IMAGE SECURITY USING HENON CHAOTIC MAP

Thesis Submitted in Partial Fulfillment of the Requirement for the Award of the degree of

MASTER OF TECHNOLOGY
IN
INFORMATION SYSTEM

SUBMITTED BY

ASHISH KUMAR
(2K11/ISY/03)

UNDER THE GUIDANCE OF

N. S. RAGHAVA
(ASSOCIATE PROFESSOR)

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI-110042
(2011-2013)

CERTIFICATE

This is to certify that the thesis entitled **"Image Security using Henon Map"** submitted by **Ashish Kumar (2K11/ISY/03)** to Delhi Technological University, Delhi for the award of the degree of **Master of Technology** is a bona fide record of research work carried out by him under my supervision.

The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

N.S. Raghava
(Associate Professor)
Department of Information Technology
Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and **Delhi Technological University**. I would like to extend my sincere thanks to all of them.

I am highly indebted to **N.S. Raghava** (***Project guide)*** for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my special gratitude and thanks to **Prof. O.P. Verma *(Head of Dept.)*** for giving me such an opportunity to work on the project.

I would like to extend my gratitude towards my **parents** & **staff** of Delhi Technological University for their kind co-operation and encouragement which helped me in completion of this project.

My thanks and appreciations also go to my **friends and colleagues** in developing the project and people who have willingly helped me out with their abilities.

Ashish Kumar
Roll No.: 2K11/ISY/03
Dept. of Information Technology
Delhi Technological University

ABSTRACT

Communication is a meaningful exchange of information between two or more entities. Images and documents travel widely and rapidly, in multiple manifestations, through email and across the Internet. In this era of e-communication i.e. electronic transmission of information that has been encoded digitally (as for storage and processing by computers), the first concern is about the security of the content which is shared during communication. While the information is over net, it is next to impossible to keep a track of where the information or the copy of information is going through. Security is a continuous process via which data can be secured from several active and passive attacks. Several security techniques can be used to ensure the integrity, authentication and confidentiality of the information. Cryptography is one of the primitive way to secure the information from hackers or intruders. Encryption technique protects the confidentiality of a message or information which can be in the form of multimedia (text, image, and video).Since there are limited encryption algorithm but humongous key space, therefore, the secrecy of encryption depends on the secret key. In this work, a new symmetric image encryption algorithm is proposed based on Henon’s chaotic system with byte sequences applied with a novel approach of pixel shuffling of an image which results in an effective and efficient encryption of images. Confusion and diffusion are increased by shuffling the image pixels in a specific order for several iterations. Statistical analysis, experimental analysis of key sensitivity and measurement of encryption quantity proved that the proposed image encryption algorithm resulted in a new dimension for secure image transfer in digital transmission world. The proposed method proved to produce good results for gray as well as color images.

CONTENTS

CHAPTER 6

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

INTRODUCTION

1.1 SECURITY

Security is a continuous process of protecting the resources of computer system from hackers or attackers. A hacker is someone who exploits weaknesses in a computer system or computer network and seeks an unauthorised access to its data. Resources that need to be protected may be physical or non-physical. Physical resources comprise of computer peripherals and non-physical data consists of data and information. In distributed computer system, several computers are connected to each other through a network. Here, the data or information over network needs higher protection from unauthorised access. There are two categories of security in computer system.

- Information security
- Network security

1.2 INFORMATION SECURITY

Information security can be described as protection of information or data from unauthorised access, disclosure and modification regardless of the form of data.

Two main aspects of information security are:

- **IT security**: It is also referred to as computer security. This security is applied to technology or some form of computer system. IT security has a major role in any enterprise due to use of several old and new technologies. These technologies need to be kept safe and secure from malicious cyber-attacks or any breach of information.
- **Information assurance**: It is an act of protecting the data which has the potential of being lost when some critical issues arise. These issues include server malfunction, physical theft. If the data is lost once, it can lead to heavy losses to the organisation. One

of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

1.3 NETWORK SECURITY

Network security [1] consists of many policies adopted by a network administrator to protect the public and private network. These policies prevent and monitor unauthorized access, modification, misuse, or denial of a computer network and network-accessible resources. Network security focuses on the data in a network. Every user in a network is assigned an ID and password which allows them to access information and other programs. Network security covers a variety of computer networks, both private and public, that are used in everyday jobs conducting transactions and communications among several businesses, government agencies and individuals.

1.4 PRINCIPLES OF SECURITY

1.4.1 Confidentiality

When communication takes place over an insecure network only the intended recipient should be able to access the contents of the message. The information should not be accessible to any unauthorized recipient. In fig 1.1, user A sends data to intended user B. Confidentiality [8] is compromised when unauthorized user C reads the message.

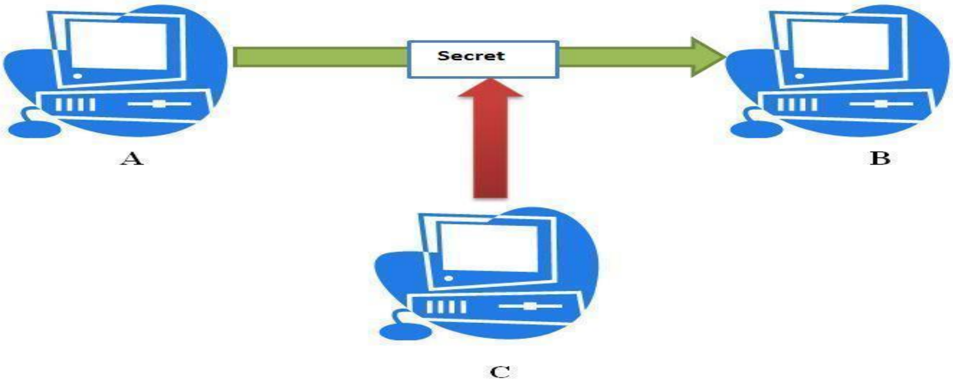


Fig. 1.1 Loss of confidentiality.

1.4.2 Authentication

Authentication [8] mechanisms help to establish proof of identities. This process of authentication ensures that the origin of the message is correctly identified. For example, if a message received by user B says that it is originated from user A but actually the message was send by user C, this kind of attack is called absence of authentication, as shown in fig. 1.2. This type of attack is also called fabrication.

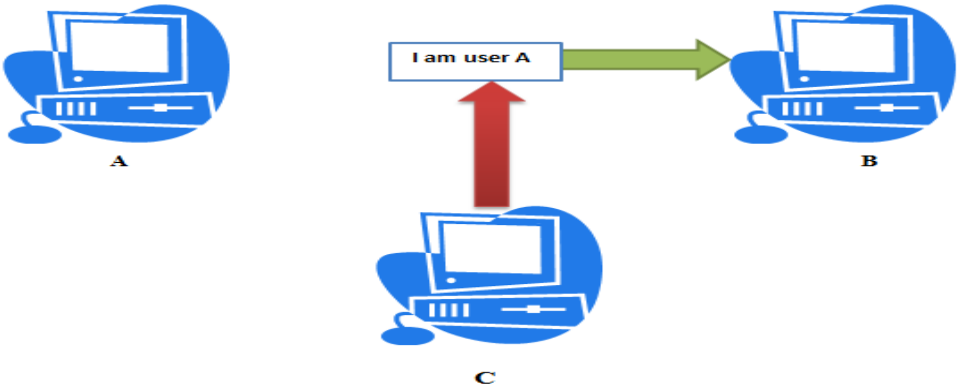


Fig. 1.2 Absence of Authentication.

1.4.3 Integrity

The assurance that the data received is exactly as sent by an authorized entity is called integrity [8]. Fig. 1.3 shows a way to detect the possibility of loss of integrity. A message from user A should go directly to user B but if it follows a route via user C, it is likely that the message has been altered resulting in loss of integrity.

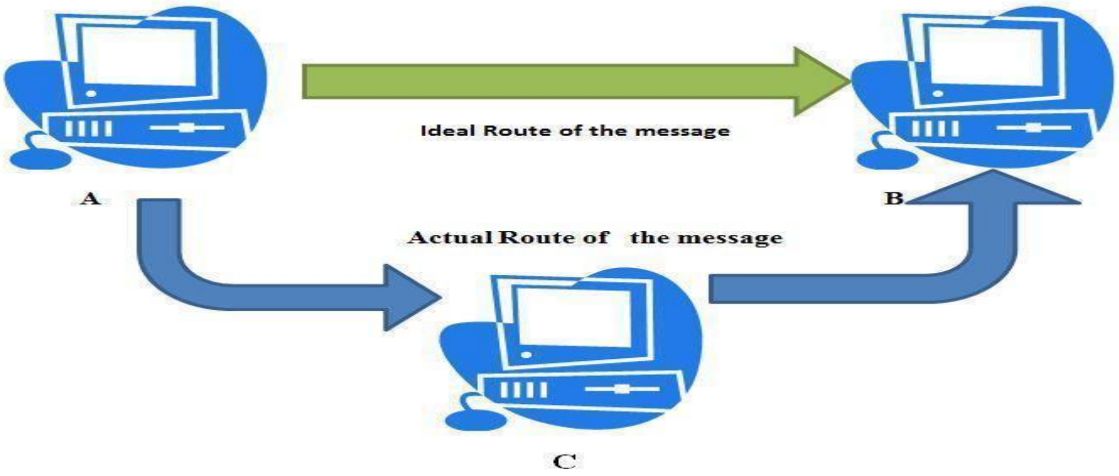


Fig. 1.3 Loss of integrity.

1.4.4 Non-Repudiation

It may happen that a user sends a message and then refuses that he had sent that message, or any user refuses to have received the message even if he had read it. Non-repudiation [8] does not allow the sender of a message to refuse the claim of not sending that message.

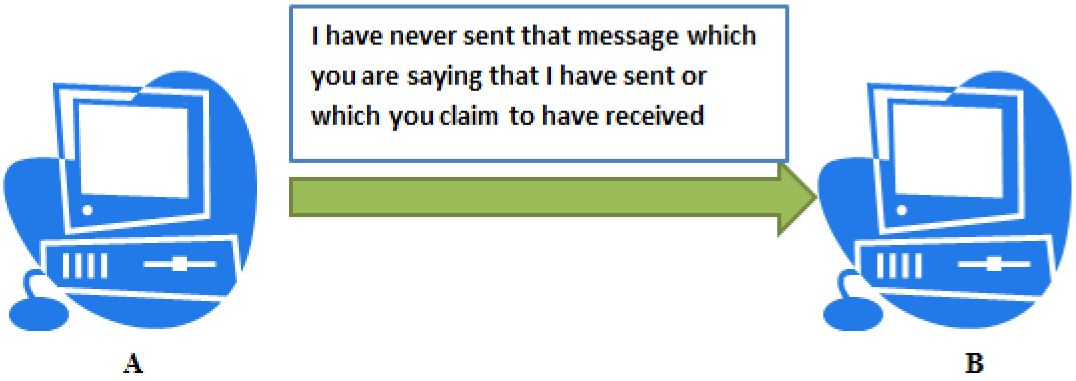

I have never sent that message which you are saying that I have sent or which you claim to have received
A
B

Fig. 1.4 Establishing Non-repudiation.

1.4.5 Availability

This type of attack is known as interruption. As shown in fig. 1.5, user A fails to access some resources of user B or fails to contact server due to the intentional action of unauthorized user C is known as attack on availability.

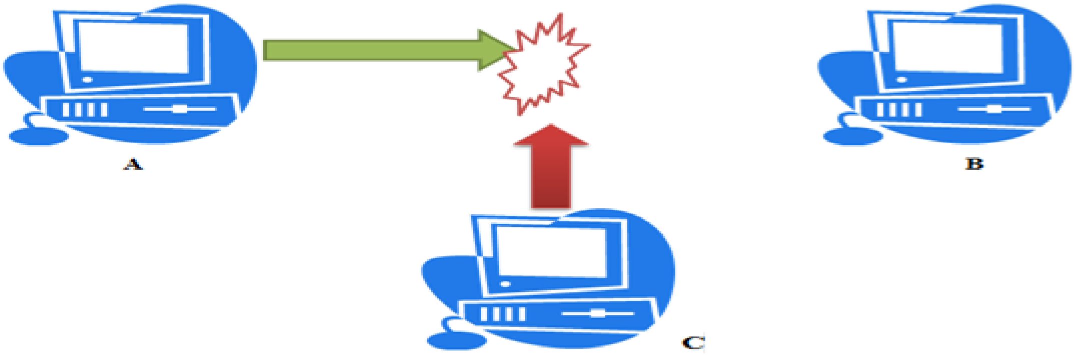


Fig. 1.5 Attack on Availability

1.4.6 Access Control

It determines who should be able to access the message or what the users assessing the resources can do. This prevents from unauthorized use of a resource.

1.5 SECURITY ATTACKS

Any attempt by an unauthorised user to gain access to any information by compromising its security [2] is called a security attack. Classes of attack might include passive monitoring of communications, close-in attacks, active network attacks, exploitation by insiders, and attacks through the service provider. A system must be able to limit damage and recover rapidly when they occur. There exist two types of security attacks:

1.5.1 Passive Attacks

The goal of the attacker is to simply get the information that is being transmitted. Attacker monitors the traffic. Passive attacks include monitoring of unprotected communications, traffic analysis, decrypting weakly encrypted traffic, and capturing all the authentication information such as passwords. Passive attacks are difficult to detect as the attacker only sniffs the data without doing any modifications in data. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user. This attack can be prevented by the means of encryption.

1.5.2 Active Attacks

Active attacks are the actions that attempt to bypass the secured system. This can be done through viruses, worms, stealth, or Trojan horses. Active attacks involve some modification of the data stream or the creation of false stream, to introduce malicious code, and to steal or modify information. It is difficult to prevent active attacks. These attacks include masquerade, replay, and modification of messages and denial of service. A masquerade takes place when one user pretends to be some other user. It can further lead to other active attacks. Replay involves the capture of data and its subsequent retransmission which produces an unauthorized effect.

1.6 NETWORK SECURITY MODEL

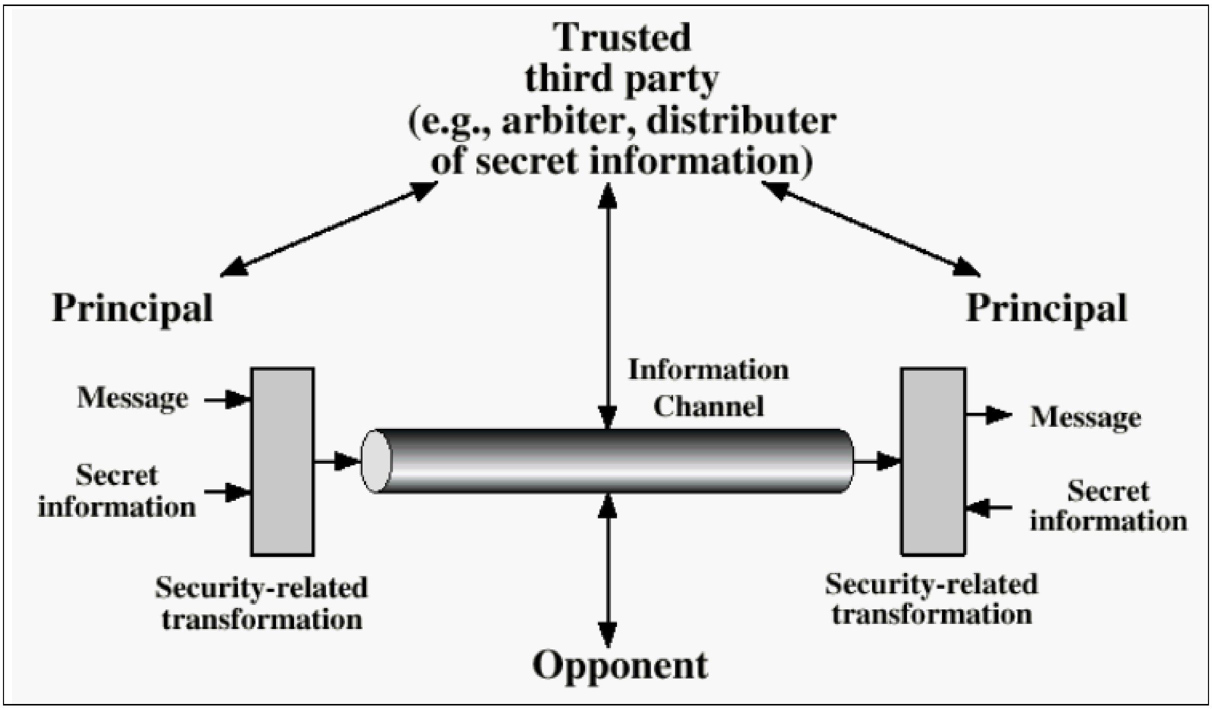


Fig. 1.6 Network security model.

In this model [13], the two entities involved in communication tend to send messages via a information channel. A logical information channel is established by defining a route through the internet from source to destination. In order to protect the information from intruders, the entities involved will perform some sort of security-related transformations on the message to be sent using some form of secret information. Such activities may involve the use of a Trusted Third Party to whom some responsibilities such as distribution of secret information or authorisation/authentication are entrusted to.

There are four essential tasks involved in designing a security service using this model:

1. An algorithm for performing the security related transformation.
2. Generate the secret information required by that algorithm
3. Method for distribution and sharing of secret information.
4. A protocol to be used by two entities that utilises the security algorithm and secret information to achieve a particular security service.

1.7 MULTIMEDIA

Multimedia [3] is an emerging field that deals with different forms of information such as text, images, audio and videos in an integrated manner. Multimedia is any media and content that uses a combination of different content forms. With the advancement of devices to display multimedia and enabling them to transfer it from one location to another has resulted in spreading of danger over their security issues. Any information shared over Internet needs high level of protection from intruders [4]. Now-a-days digital images are used frequently for communication.

Telecommunication systems and digital information's development has opened a wide range of new possibilities. Billions of people are getting connected to each other through the internet and exchange large amount of private data or information over the network. It becomes very important to secure such sensitive information from unauthorised users. Digital information has the advantage that it can be transmitted in different ways but a drawback is that it can be copied easily on a USB-stick or on a hard drive. Also exactly the same information can be sent over a wireless network or over an optical fiber. The transmission of data is efficient, fast and easy. When a sender sends some message, it becomes very important that the receiver can check whether the integrity of message has been compromised or not. Digital signatures are used to ensure the authenticity and integrity of the message. It verifies the origin of message and also prevents the sender from later denying that he sent the message.

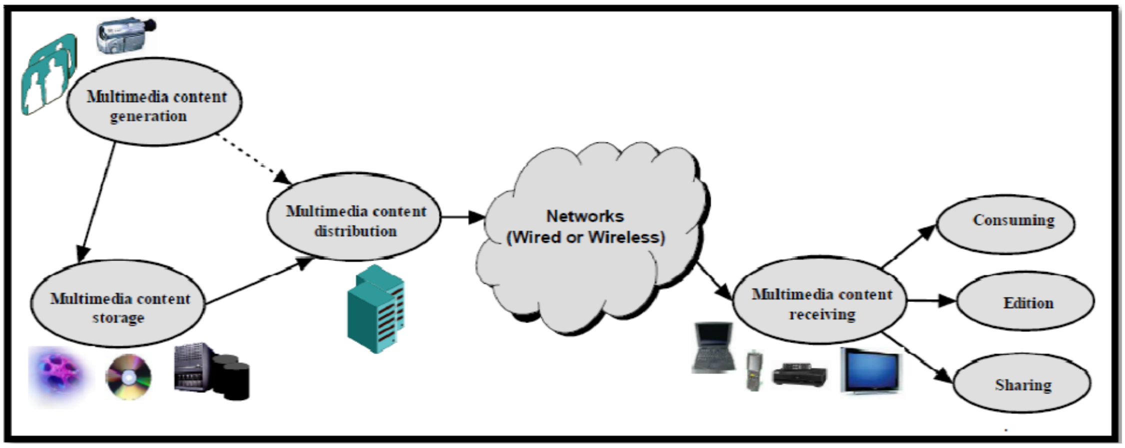

Multimedia content generation
Multimedia content distribution
Networks (Wired or Wireless)
Multimedia content storage
Multimedia content receiving
Consuming
Edition
Sharing

Fig. 1.7General architecture of multimedia information system [2].

1.8 CRYPTOGRAPHY

Cryptography is the art and science of securing information by encoding it to a non-readable form [6] [7]. Cryptography is synonymous to encryption. This process is systematic and well-structured and is related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. Widely used applications of cryptography include ATM cards, security pass codes, computer passwords, and electronic commerce.

Historically, encryption was used by militaries and governments for a long time to facilitate secret communication. But now it is widely used in protecting information within many kinds of civilian systems. For instance, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for securing some of their data in transit, and 53% utilized encryption for securing their data in storage. Encryption can also be used to protect the data which is “at rest” i.e. the files on computers and storage devices. Data at rest or the confidential data such as customers' personal records needs to be protected from being exposed through loss or theft of laptops or backup drives. Encryption of such files at rest helps protect them when physical security measures fail. Another example of using encryption on data at rest is Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering.

The one who encrypts the message needs to share the decoding technique needed to recover the original information only with intended recipients, thereby prohibiting unwanted people to decrypt the message. Cryptography techniques were used since World War I to communicate the messages secretly. As the technology is growing, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography methods are entirely based on mathematical theory. Cryptographic algorithms are designed around computational hardness assumptions, which make them practically hard to break by the hackers. Although, theoretically it is possible to break such a system but it is infeasible to do so by any known practical means. Therefore, these schemes are termed computationally secure. One-time pad is an example of information-theoretically secure schemes that provably cannot be broken even with unlimited computing power. But these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

1.8.1 CLASSIC CRYPTOGRAPHY

The earliest forms of secret writing required little more than local pen and paper analogy since most people could not read. Actual cryptography [10] [14] was required for more literate opponents. The main classical cipher types are transposition ciphers, which rearrange or shuffles the order of letters in a message (e.g., 'hello india' becomes 'ehlolnidai'' in a trivially simple rearrangement scheme), and substitution ciphers, which methodically replace letters or groups of letters with other letters or groups of letters (e.g., 'hello india' becomes 'idmmojoejb' by replacing each letter with the one following it in the Latin alphabet).

Simple versions of cryptography could not provide much confidentiality from opponents. *Caesar cipher was* an early substitution cipher scheme, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. According to Suetonius, long back ago, Julius Caesar used ceasar cipher method with a shift of three to communicate with his generals.

The **cryptography scheme** can be described as follow.

Input message is given in the form of plaintext denoted by P or plain image which is then processed with the help of an encryption system comprising of an encryption algorithm. The encrypted message is called cipher text denoted by C.

The encryption procedure can be described as **C = E Ke(P)**, where Ke is the encryption key and E() is the encryption function. In the same way, decryption procedure is described as **P = D Kd(C)**, where Kd is the decryption key and D() is the decryption function.

When both the keys, encryption key and the decryption keys, are same i.e. Ke = Kd, the cipher is called a symmetric cipher or a private-key cipher. For private-key ciphers, the encryption decryption key must be transmitted from the sender to the receiver via a separate secret channel.

When encryption key is different from decryption key i.e. Ke ≠ Kd, the cipher is called a public-key cipher or an asymmetric cipher. For public-key ciphers, each party has a distinct pair of keys. The encryption key***Ke*** *is published* and distributed to all the parties, and the decryption key ***Kd*** *is kept private*. Here, the advantage lies in the fact that no additional secret channel is needed for key transfer.

According to the encryption structure, ciphers can be divided into two classes: stream ciphers and block ciphers. Stream ciphers encrypt the plaintext with a pseudo-random sequence (called key stream) controlled by the encryption key. Block ciphers encrypt the plaintext block by block, and each block is mapped into another block of same size.

1.8.2 TYPES OF CRYPTOGRAPHY

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or attackers cannot read it, but only those authorized parties can read the message correctly who have been passed on with the details about the encryption algorithm and the secret key. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary having access to ciphertext should not be able to determine anything about the original message. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

There exist two basic types of encryption schemes:

- Symmetric-key cryptography
- Public key Cryptography

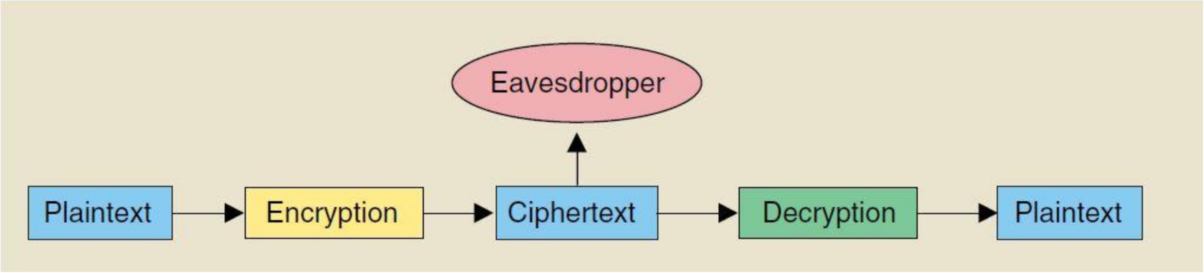


Fig. 1.8 Block diagram of cryptography.

1.9 Symmetric-key Cryptography

In this scheme, the same key is used for encryption as well as decryption of the message. Thus sender and receiver must share the secret key before they wish to communicate. In symmetric-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention. Earlier, all encryption schemes have been symmetric-key (also called private-key) schemes.

Symmetric key [9] ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. In stream cipher, plaintext is encrypted by pseudorandom bit key stream. Stream cipher is also known as state cipher.

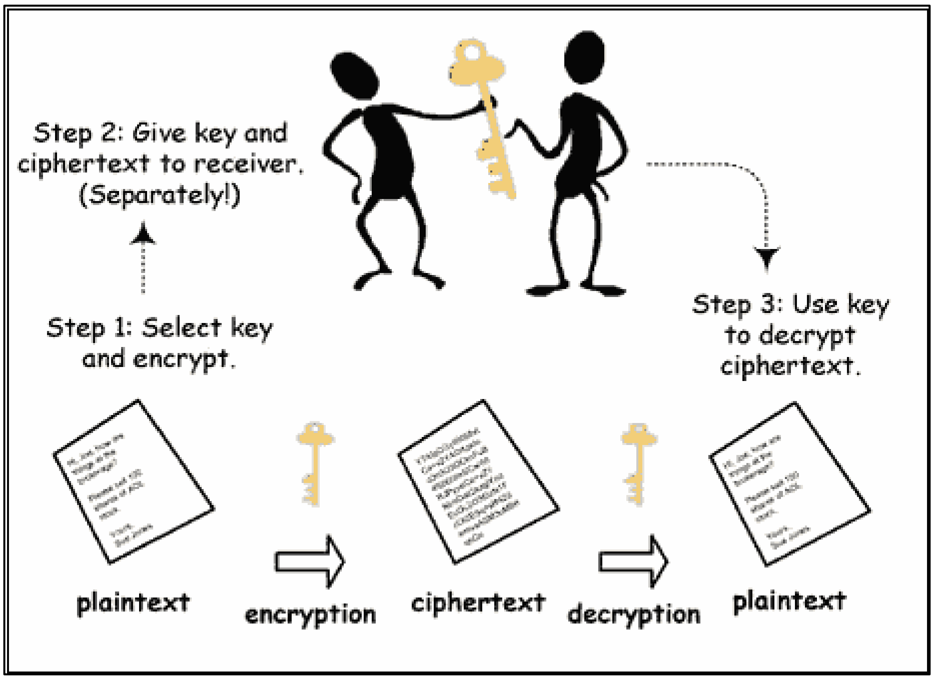

Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Fig. 1.9 Symmetric key encryption process.

❖ Symmetric-key Algorithms

Symmetric-key algorithms are a class of algorithms for cryptography that uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. This requirement that sender and receiver have access to the secret key is one of the main drawbacks of symmetric key encryption, when compared to public-key encryption.

❖ Types of symmetric-key algorithms

Symmetric-key encryption can use either **stream ciphers** or **block ciphers**. Stream ciphers encrypt the digits (typically bytes) of a message one at a time. Block ciphers take a number of bits; blocks of 64 bits have been commonly used; and encrypt them as a single unit. Padding the plaintext may be required to ensure that it is a multiple of the block size. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

A stream cipher [15] is a symmetric key cipher in which a stream of plaintext digits is combined with a pseudorandom cipher digit stream (keystream) as shown in fig. 1.10. Each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, which gives a digit of the ciphertext stream. The encryption of each digit is dependent on the current state so it is also called a state cipher. In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR).

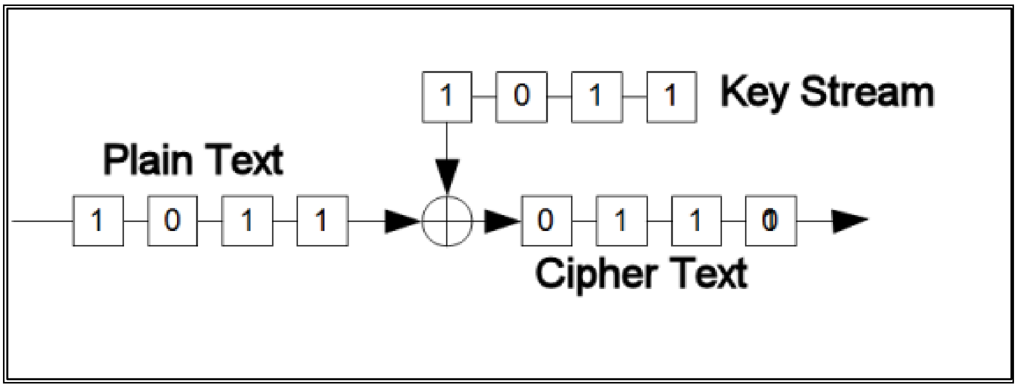


Fig. 1.10 Stream Cipher

The pseudorandom key stream is typically generated serially from a random seed value using digital shift registers. The random seed value serves as the cryptographic key for decrypting the cipher text stream.

Stream ciphers have a completely different approach from block ciphers. Block ciphers deals with large blocks of digits with a fixed and unvarying transformation. A block cipher primitive is used in such a way that it acts effectively as a stream cipher.

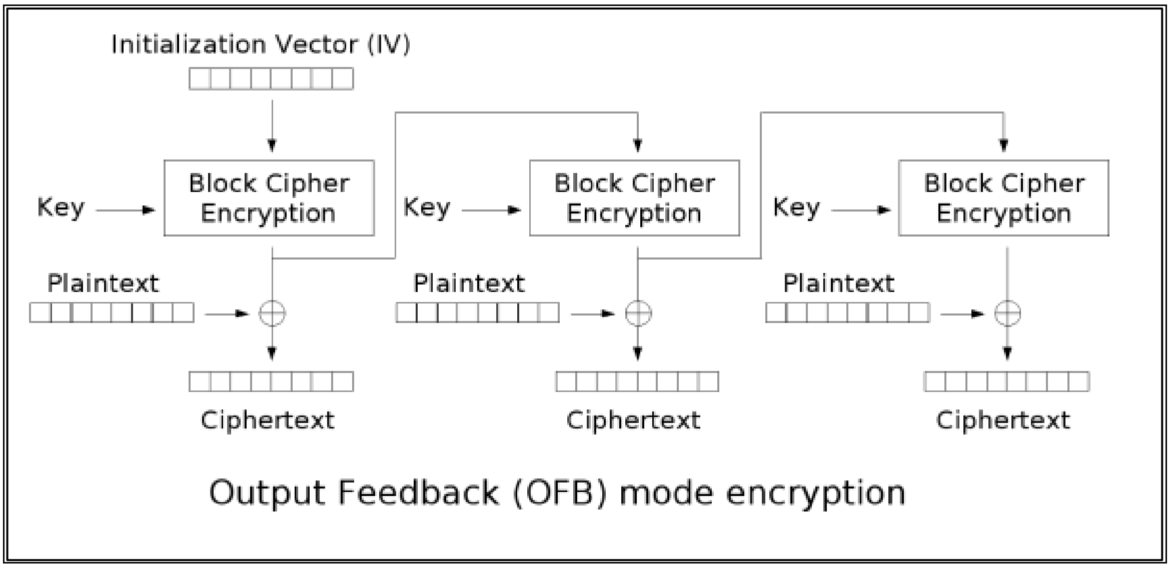


Fig. 1.11 Block Cipher

Stream ciphers have several advantages when compared to block ciphers. Stream ciphers are faster as they have higher computational speed than block ciphers. They have lower hardware complexity. However, stream ciphers, if used incorrectly, are prone to serious security problems. To overcome this drawback, the same starting state (seed) must never be used twice.

Stream ciphers, involves an arbitrarily long stream of key, which is combined with the plaintext bit-by-bit or character-by-character, almost similar to the one-time pad. In stream cipher, the output stream is generated based on a hidden internal state. This internal state changes when the cipher operates. That internal state is initially set up using the secret key material. RC4 is a commonly used stream cipher. Block ciphers can be used as stream ciphers.

US government established some cryptography standards. The **Data Encryption Standard (DES)** and the **Advanced Encryption Standard (AES)** are designated block cipher designs which have been meeting these standards. After the AES was adopted DES's designation was finally withdrawn. DES is quite popular and is used across a wide range of applications, from e-mail privacy and secure remote access to ATM encryption. Many other block ciphers have been designed and used, with substantial variation in quality.

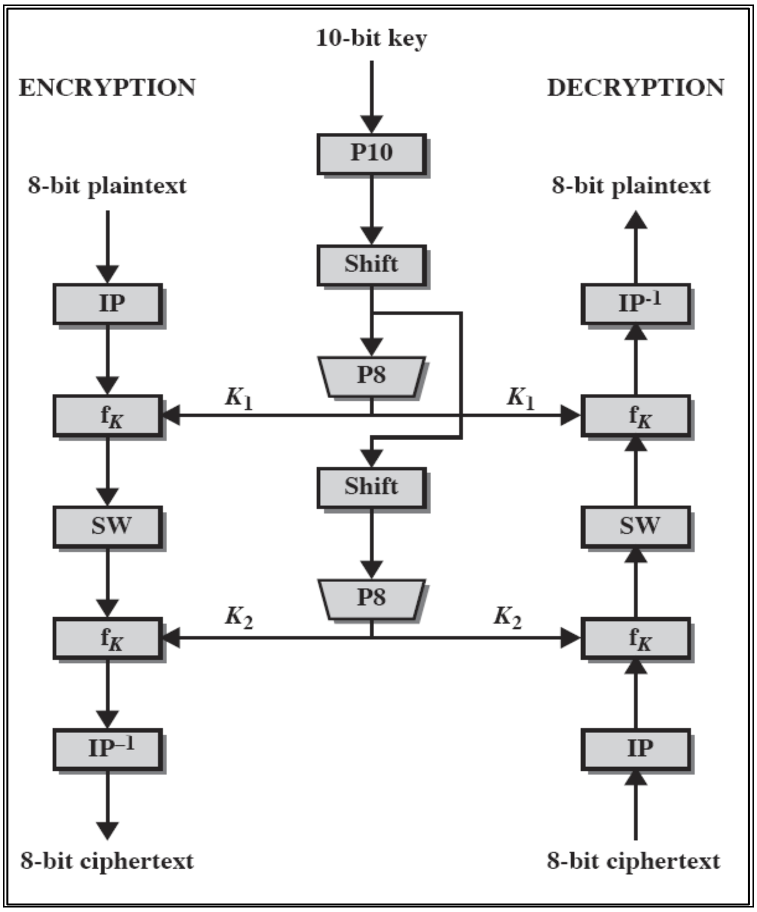


Fig. 1.12 Simplified Data Encryption Standard.

1.10 PUBLIC-KEY CRYPTOGRAPHY

Symmetric-key cryptosystems [11] use the same secret key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A considerable disadvantage of symmetric ciphers is the key management necessary to use them securely. A different key is required for each distinct pair of communicating parties, and perhaps each ciphertext exchanged as well. With the increase in the square of the number of network members, the number of keys required increases. This quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely sharing a secret key between two communicating parties, when a secure channel does not exist between them, also presents a considerable practical obstacle for cryptography users in the real world.

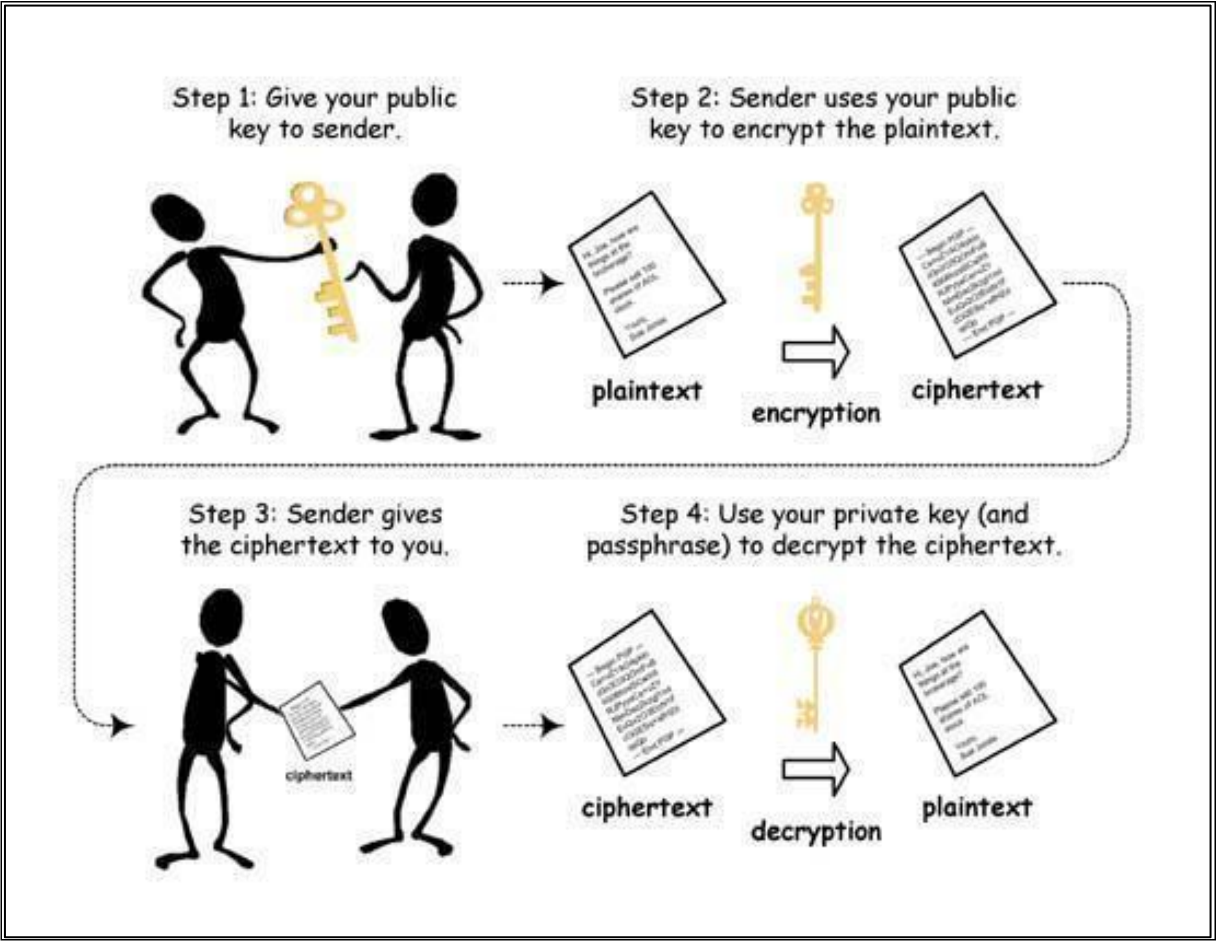

Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
ciphertext
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

Fig. 1.13 Asymmetric key cryptography process.

In 1976, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* cryptography or asymmetric key cryptography. In this, two different but mathematically related keys are used. One is public key and the other one is private key. A public key system is constructed in such a way that calculation of private key is computationally infeasible from the public key, in spite of the fact that they are necessarily related. Instead, both the keys are generated secretly, as an interrelated pair.

In public-key cryptosystems, the public key can be distributed freely to all the parties in the network, whereas private key is kept secret. The public key is used for encryption by the sender, while the *private* or *secret key* is used for decryption by the intended receiver.

Diffie–Hellman [62] is a key exchange protocol which provides a solution to allow two parties to secretly share encryption keys.

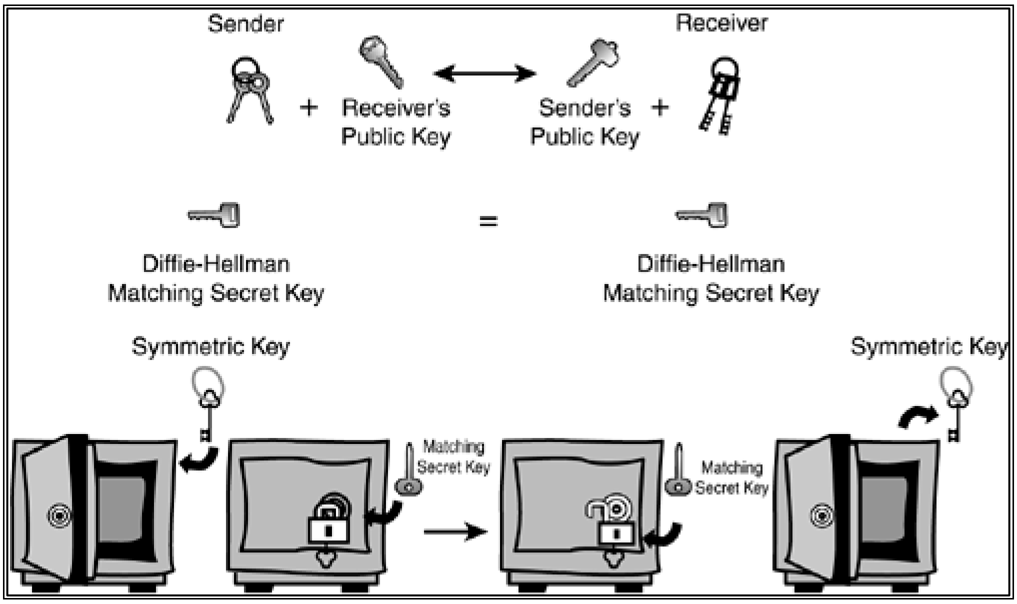


Fig. 1.14 Diffie-Hellman Process

1.11 CRYPTANALYSIS ATTACK

❖ Brute-force attack

Brute-force attack or **exhaustive key search** is a cryptanalytic [5] attack that can, be used against any encrypted data. It consists of systematically checking all possible keys until the correct key is found. In the worst case, this would result in traversing the entire search space. This attack is not possible for data encrypted in an information-theoretically secure manner. Such an attack is the only hope for intruders when it is not possible to take advantage of other weaknesses in an encryption system that would make the task easier.

❖ Cryptanalysis

Cryptanalysis is the art and science which deals with defeating cryptography techniques to recover information, or forge information that will be accepted as authentic. It is nothing but analysing cryptographic systems in order to study the hidden aspects of the systems. Cryptanalysis is used to break cryptographic security systems and gain access to the contents of encrypted messages, even for unknown cryptographic key.

In addition to the analysis of cryptographic algorithms, cryptanalysis also includes the study of side-channel attacks that do instead of targeting weaknesses in the cryptographic algorithms themselves, exploit the weaknesses in their implementation.

The methods and techniques of cryptanalysis have changed drastically through the history of cryptography, even though the target has been the same. Adapting to increasing cryptographic complexity, ranging from very primitive pen-and-paper methods, through the machines like Bombes and Colossus computers at Bletchley Park in World War II, to the schemes of present which are mathematically advanced, methods for breaking modern cryptosystems mostly involve pure mathematics for solving carefully constructed problems, the best-known being integer factorization.

1.11.1 Types of Cryptanalysis Attack

Cryptanalysis attacks are based on the amount of information known to the cryptanalyst. In general, it is assumed that the opponent knows the encryption algorithm. One possible attack is brute force attack but if key space is very large then it becomes impractical to try all the possible keys. Therefore, the opponent must rely on an analysis of ciphertext itself. A weak algorithm fails to withstand a ciphertext-only attack. An encryption algorithm is designed to withstand a known-plaintext attack. It is very difficult to estimate the amount of effort required to cryptanalyze ciphertext successfully.

Here, four type of cryptanalysis attack are described below [5]:

- **Cipher text-only:** It is the easiest to defend against as the opponent is having no other information except for the ciphertext. He is assumed to have has access only to a set of ciphertexts.

- **Known-plain text:** The opponent captures one or more plaintext messages and their encryptions which makes it possible to deduce the key on the basis of the way in which plaintext is transformed.

- **Chosen-plaintext:** If analyst is able to choose the message to be encrypted and gets source system to insert that message into the system, then this attack is possible as now analyst may deliberately pick patterns that can be expected to reveal the structure of key.

- **Chosen-cipher text:** The analyst gathers information by choosing a ciphertext and obtaining its decryption under an unknown key. He enters one or more chosen ciphertexts into system and obtains the resulting plaintexts. By combining these pieces of information he tries to reveal the hidden secret key.

1.12 KEY TERMS

1.12.1 Cryptosystem

The term cryptosystem is used as synonym for cryptographic system. A cryptographic system is any computer system that involves cryptography like a system for secure electronic mail which includes cryptographic hash functions, key management, methods for digital signatures, and so on. In the context of cryptography, a cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. A cryptosystem consists of three algorithms: one for key generation, one for encryption, and one more algorithm for the decryption. But mostly, the term cryptosystem is used when the key generation algorithm is important. Breaking a cryptosystem is not restricted to breaking the underlying cryptographic algorithms because cryptographic systems are made up of cryptographic primitives, and are usually rather complex. Usually, it is far easier to break the system as a whole, e.g., through the misconceptions of users in respect to the cryptosystem. The systematic arrangement of cipher text can stand for the security.

1.12.2 One-Time Pad

In cryptography, the one-time pad [12] is a type of encryption which is impossible to crack if used correctly. Ciphertext is obtained by encrypting each bit from the plaintext by a modular addition with a bit from a secret random key (or *pad*) of the same length as the plaintext. It is impossible to decrypt ciphertext without knowing the key. This is possible only if the key is truly random, as large as the plaintext, never reused in whole or part, and kept secret. For easy disguise, the pad was sometimes reduced to a very small size such that it can be used only with the help of a powerful magnifying glass.

One-time pads were sometimes printed onto sheets of highly flammable nitrocellulose in order to increase their secrecy. In early implementations, the key was distributed as a pad of paper, so that the top sheet could be easily torn off and destroyed after its use. However, practical problems prevented one-time pads from being widely used.

Some authors use the terms Vernam cipher and one-time pad synonymously. One-time pad was first described by Frank Miller in 1882, and then it was re-invented in 1917. It is derived from the Vernam cipher, named after one of its inventors, Gilbert Vernam. Vernam's system was a cipher that combined a message with a key read from a punched tape. The original form of Vernam's system was vulnerable to attacks as the key was reused whenever the key tape's loop made a full cycle. Joseph Mauborgne recognized that if the key tape were totally random, cryptanalysis would be impossible which lead to introduction of one-time pad.

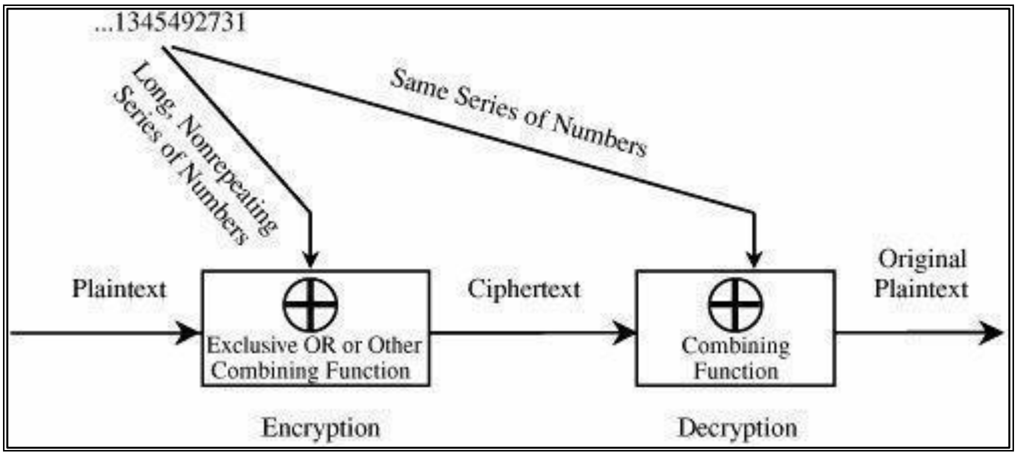


Fig. 1.15 One-time pad or Verman cipher

1.12.3 Eavesdropping

Eavesdropping is an unethical act of interfering in-between and sneakily listening to a private conversation. This can be considered as passive attack if third party attempts only to observe the flow and gain knowledge of information. If it attempts to alter the data or affects the flow of data then eavesdropping is categorised as active attack. Eavesdropping can be done by monitoring of telephone and Internet conversations by a third party. An intruder can eavesdrop the information over telephone lines (also known as wiretapping), instant messaging, emails and other methods of communication considered private. The wire tap received its name because, in older days, the monitoring circuit was applied to the wires of the telephone line being monitored and drew off or tapped a small amount of the electrical signal carrying the conversation. Now, eavesdropping is extended to the attack that steals the information from any network or device.

CHAPTER-2

CHAOS AND CRYPTOGRAPHY

2.1 INTRODUCTION

In past few decades, chaotic signal [16] [17] is widely used in cryptography system. **Chaos** is a Greek word which means unpredictable and is studied under the non-linear dynamic system. Chaotic systems are popular for their randomness and non-predictable behaviour. Chaos theory is a part of mathematics that define the complex dynamic systems which is highly sensitive to their initial parameters. Eventually, each and every result depends on these initial parameters.

Chaos theory is used in several disciplines including meteorology, engineering, economics, physics, and biology. There exist several kinds of chaotic systems which inherit the property of chaos theory. Chaotic systems such as Logistic map, Henon map, Tent map, Lorenz attractor, Rossler attractor, and Piecewise linear chaotic map are popular for their property and randomness. Orbit of these map define the randomness in attractor field depending upon these initial parameters. Chaos theory is a mathematical physics which has been driven by Edward Lopez. It is stated as follow:

"Chaos: When the present determines the future, but the approximate present does not approximately determine the future".

In traditional cryptography system, it was difficult to secure large size of multimedia from intruder or attackers and calculation of mathematical equation (built-in Encryption technique) was not so easy. In past few decades, chaotic systems are used in cryptography to secure multimedia over insecure network. A chaotic system based on confusion and diffusion was developed in 1989 [18]. Although it was already being used for cryptographic system but there was no theorem to prove authenticity of the chaotic map. Chaotic systems have attracted the cryptography due to the characteristics such as sensitivity, non-liner, unpredictability, and random-look nature, deterministic and easy to reconstruct after filling in the multimedia [19]. The parameters in chaotic maps are meaningful if they are real numbers[20], which can be used in the cryptographic algorithms as encryption and decryption keys. [21]. Chaotic systems have potential applications in such cryptography algorithms as block cipher, stream cipher, hash function, and pseudorandom number generator. Over the last two decades, there has been tremendous interest in utilizing chaotic systems to design secure cryptographic algorithms [22].

2.2 CHAOS THEORY

A system is called a chaotic system if it is sensitive to initial conditions and topology. This theory is named so due to the fact that the systems described by this theory [23] [24]are apparently disordered, but in reality, chaos theory is about finding the underlying order in apparently random data. Researchers have studied chaos theory in numerous fields, such as electronic systems, fluid dynamics, climate and weather, and lasers.

A chaotic system is a simple, non-linear and dynamical in nature. The deterministic regulations are those that determine the current state uniquely mix, and if periodic orbits are dense and random. Moreover, chaotic systems are deterministic i.e. having a great sensitivity to initial small changes in an initial value might generate small differences in the result [25].

On the other hand, in classical science from the previous states, whereas there is always a mathematical equation to determine the system evolution [26]. From the previous definitions of deterministic and dynamical systems, we cannot say that the randomness is not allowed. As the parameters are changed, the bifurcation in dynamic differential equation changes the number of solutions. Chaotic maps have been an active research area due to their characteristics, such as sensitivity to the initial value, complex behaviour, and completely deterministic nature. The chaotic behaviour can be observed in many different systems, such as electronic systems, fluid dynamics, lasers, weather, climate and economics [27].

Generally, chaotic maps define infinitely large fields of real numbers. The most important characteristics of chaotic systems are as follows:

1. **Chaotic maps are random in behaviour but completely deterministic in nature:** the behaviour of chaotic systems is purely deterministic but seems to be random.

Hence, for same initial values the chaotic system produces same set of output values again and again. Furthermore, the chaotic systems are dynamical systems that are described by differential equations or iterative mappings, and the previous state specifies the next state [25] [27] [26].

2. **Sensitivity dependence on the initial conditions:** Initial state is the state from which the system starts. Dynamical systems evolve entirely differently over time even with slight changes in the initial state [28]. If the initial variables are initialized to 0.01 and 0.2 for a chaotic system, and then slightly changed to 0.01000001. It will not produce same key stream as generated by previous initial value of chaotic system.

3. **Unpredictable:** The future states of the chaotic system are very difficult to predict in the long term as stated in [25]. In chaotic maps, even if the current state of the chaotic system is known it is useless trying to predict the next state of the system.

2.2.1 HISTORY OF CHAOS THEORY

In 1960, Lorenz was busy working on the problem of weather prediction which cannot be solved on its own with a set of twelve equations to model the weather [29]. However this computer program could only predict theoretically what the weather might be. Once he wanted to see a particular sequence again. He started solving the problem in the middle of the sequence, instead of starting from the beginning so he entered the number off his printout and left to let it run. The output sequence evolved to be different. It diverged from the initial pattern, ending up wildly different from the original. Eventually, he found that the computer stored the numbers to six decimal places in its memory. In order to save paper, he only had it print out three decimal places. The original sequence had the number equal to 0.506127, and he typed only the first three digits, 0.506. Instead of getting a sequence very close to the original sequence, the new output sequence was entirely different. This effect is known as the **butterfly effect**. The computed difference in the starting points of the two curves is so small that it is comparable to a butterfly flapping its wings. This phenomenon, common to chaos theory, is also identified as sensitive dependence on initial conditions. Slight change in the initial conditions can result in drastic change in the long-term behaviour of a system.

Such a small amount of difference in a measurement might be considered as background noise, experimental noise, or an inaccuracy of the equipment. These things are impossible to avoid in even the most isolated lab. From this idea, Lorenz stated that it is impossible to predict the weather accurately. Though, this discovery led Lorenz on to other aspects of what eventually came to be known as chaos theory.

2.3 CHAOS-BASED CRYPTOGRAPHY

The relationship between conventional cryptography algorithms and chaos-based cryptography algorithms is very important in order to understand the similarities and differences between cryptography algorithms and chaotic systems[30]. Old and traditional cryptographic system was based on integer number system whereas chaotic systems used floating point numbers for encryption transformation. Initial parameter is a meaningful term which associates to encryption key or decryption key in cryptography algorithms. The three most common cryptography primitives are block cipher, hash function and pseudorandom number generator [31].

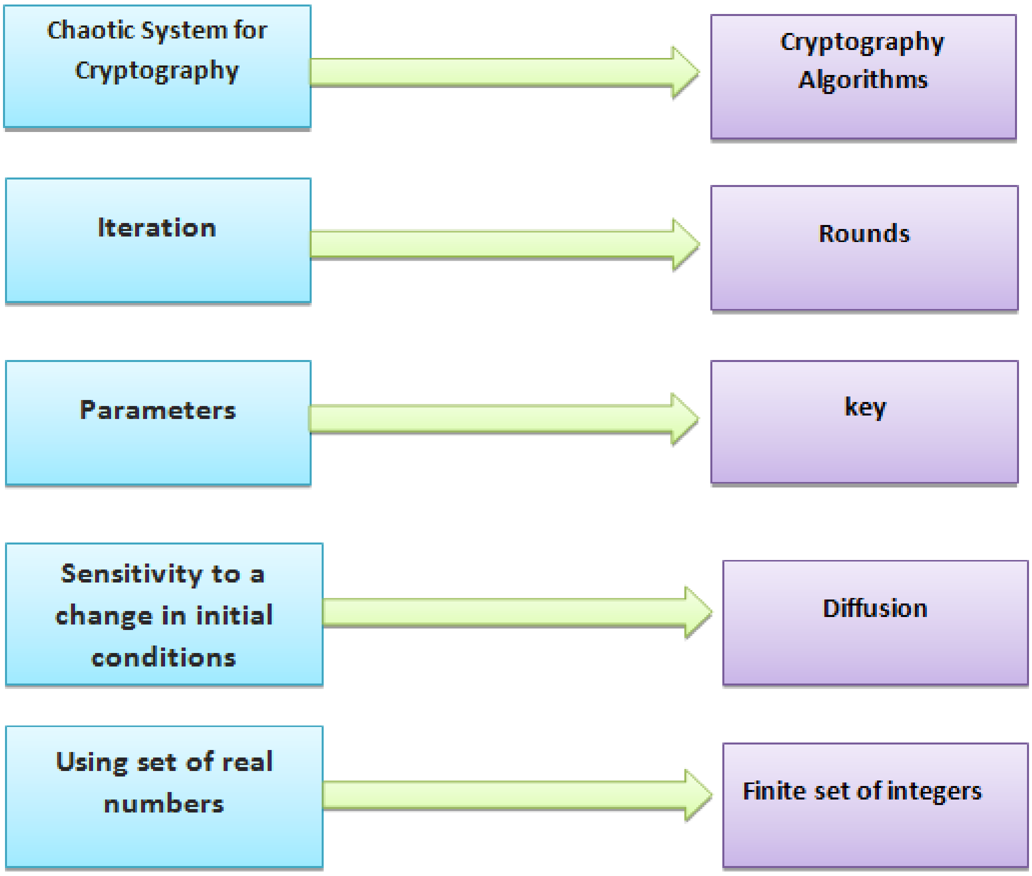

Chaotic System for Cryptography
Cryptography Algorithms
Iteration
Rounds
Parameters
key
Sensitivity to a change in initial conditions
Diffusion
Using set of real numbers
Finite set of integers

Fig. 2.1 Comparison between chaotic systems and cryptographic algorithms.

- **Block Cipher Based on Chaotic Systems**

  A block cipher is a transformation function that maps units of plaintext bits to ciphertext bits of the same unit size under the control of the secret key. The decryption method divides the input ciphertext into blocks of equal length and then applies the decryption function to each block using the same shared secret key.

- **Hash Function Based on Chaotic Systems**

  SHA-1 is one of the most widely-used hash functions employed in numerous security applications and protocols. Since SHA-1 was attacked in 2005, many researchers have been working on designing a new, alternative secure hash function [32].

- **Random Number Generators Based on Chaotic Maps**

  Chaotic systems generate unpredictable results so many researchers started working in chaotic systems to design pseudorandom number generators [33] [34] [35]. Results of Pseudorandom number generators (PRNGs) are mainly used on stream cipher algorithms as key streams that simply XOR with plaintext to generate the correspondence ciphertext using any mode of operation [108]. Moreover, it is very important to generate the secret keys and initialization variables by PRNGs [36].

2.4 CHAOTIC MAPS

A chaotic map is a map that exhibits some sort of chaotic behavior. It can be parameterized by a discrete time or a continuous time parameter. Discrete maps habitually take the form of iterated functions. Chaotic maps frequently occur in the study of dynamical systems. Where on one hand, 1-D chaotic maps are used and applied on data sequence or upon a document and on the other hand 2-D or higher dimensional chaotic maps are employed for image encryption, the reason being that the image pixels can be considered as a 2D array of pixels. Literatures upon chaos consist of common terms such as map. A map is nothing but a function whose value is uniquely determined by one or more input variables.

2.4.1 One-Dimensional Chaotic Maps

A one dimensional map deals with only one physical quantity. It is a rule relating that feature's value at one time to its value at another time. Graphical representations of these data are common in nature. Traditionally, the input or older value is across horizontal axis and the corresponding output value or function is represented on the vertical axis. List of some of one-dimensional chaotic maps is given below:

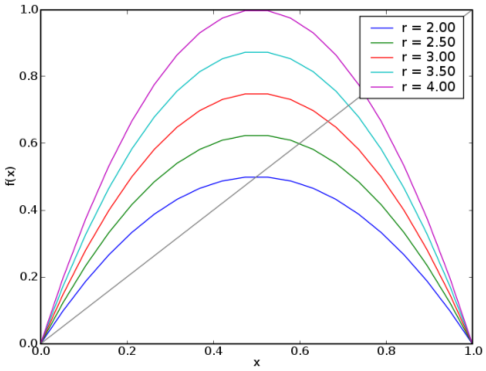
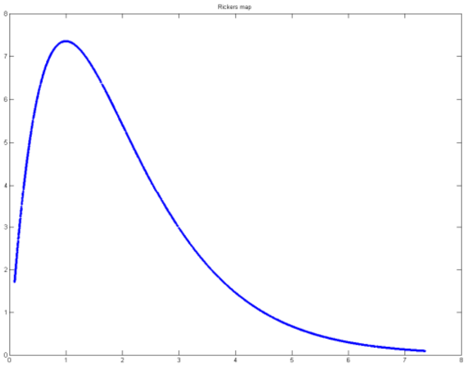
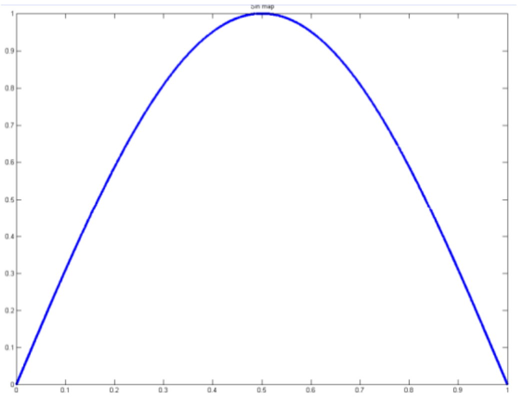
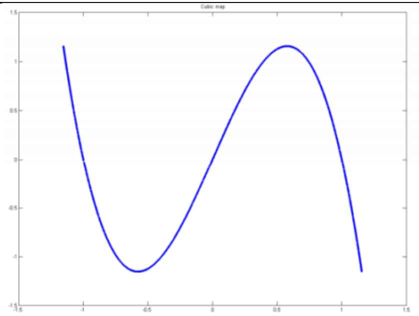
Complex Squaring Map

- Complex Quadratic Map
- Duffing Equation
- Gauss Map
- Interval Exchange Map
- Logistic Map
- Tent Map
- Van Der Pol Oscillator

2.4.2 Two-Dimensional Chaotic Maps

A two-dimensional map deals with more than one variable quantity. Two-dimensional chaotic maps exists as an object in a three-dimensional space, where x and y axis indicates the ruling equation of the chaotic map and z-axis is the temporal axis. List of some of two-dimensional chaotic Maps is given below:

- Arnold's Cat Map
- Baker's Map
- Duffing Map
- Exponential Map
- Henon Map
- Horseshoe Map
- Ikeda Map
- Kaplan-Yorke Map
- Tinkerbell Map

CHAOTIC MAP	EQUATION FOR MAP	PLOT
Logistic Map	$x_{n+1} = rx_n(1 - x_n)$	
Rickers' Map	$x_{n+1} = R(x_n)$ Where, **R(x)=xe**$^{p-x}$on [o,∞]	
Sin Map	$x_{n+1} = \sin(\pi x_n)$	
Cubic Map	$x_{n+1} = 3x_n(1 - x_n)^2$	

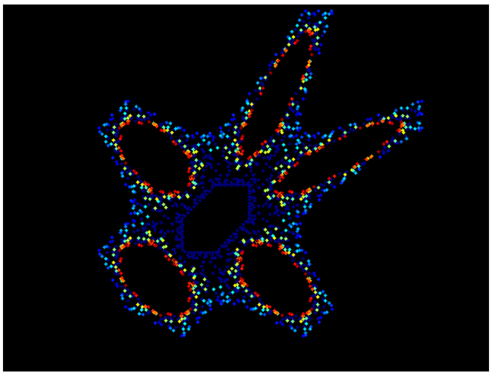
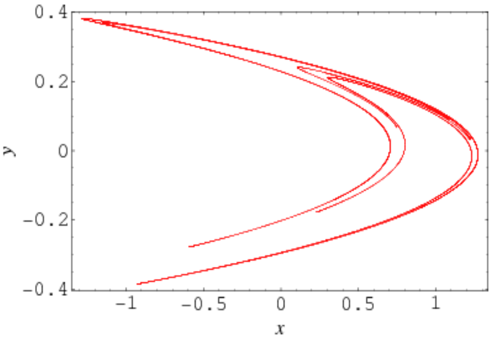
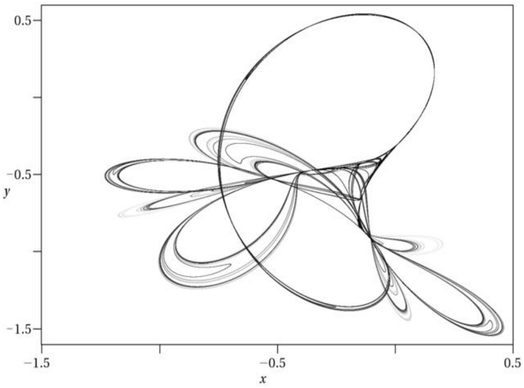
Gingerbread man Map	$\begin{cases} x_{n+1} = 1 - y_n + \lvert x_n \rvert \\ y_{n+1} = x_n \end{cases}$	
Henon Map	$\begin{cases} x_{n+1} = 1 + y_n - ax^2 \\ y_{n+1} = bx_n \end{cases}$	
Tinkerbell Map	$\begin{cases} x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} = x_{n+1} = 2x_n y_n + cx_n + dy_n \end{cases}$	

Table 1: Graphical representation of different Chaotic maps.

2.5 ATTRACTOR

Chaotic systems are too complex to visualize through naked eyes. But certain techniques are available by which we can abbreviate them into one point graph. Earlier researchers began to discover that the complex systems undergo some kind of cycle, even though other parameters are not duplicated or repeated. Attractor is a set of variables which evolves in discrete dynamical system. These set of variables moves dynamically with time and are closely related to each other. They are represented algebraically with vector dimension. In short, attractor is a region in n dimensional space. The region growing of attractor depends on the variable dimensional set. The attractor of dynamic process can be visualized geometrically in fig. 2.2. An attractor [37] can be a curve point and a complicated way of fractal structure is known by strange attractor.

Fig. 2.2 Attractor for dynamic system

A dynamic kind-of equilibrium is called a Strange Attractor. The dissimilarity between an Attractor and a Strange Attractor is that an Attractor represents a state to which a system finally settles, whereas a Strange Attractor represents some kind of trajectory upon which a system runs from situation to situation without ever settling down.

2.6 HENON MAP

The Henon map is a 2-Dimensional iterated map with chaotic behaviour proposed by a French astronomer Michel Henon in 1976 as a simplified model of the Poincare map for the Lorenz model. Two dimensional discrete-time nonlinear dynamical Henon chaotic map [38] [39] generates pseudo-random binary sequence which has been described as below:

$$\mathbf{X_{n+1} = 1+Y_n - aX_n^2}$$

$$\mathbf{Y_{n+1} = bX_n n=}\mathit{0, 1, 2\ldots} \qquad \text{eqn.(1)}$$

Here a and b are the two bifurcation parameters to control the Henon map. Parameter b is a measure of the rate of area contraction (dissipation). For b = 0, the Henon map reduces to a quadratic map, which is conjugate to the logistic map. X_1 and Y_1 are the coordinates of a point in the real plane and the property that the contraction is independent of these coordinates. Henon map is defined in the discrete time domain and in most common cases they are described by iterated functions.

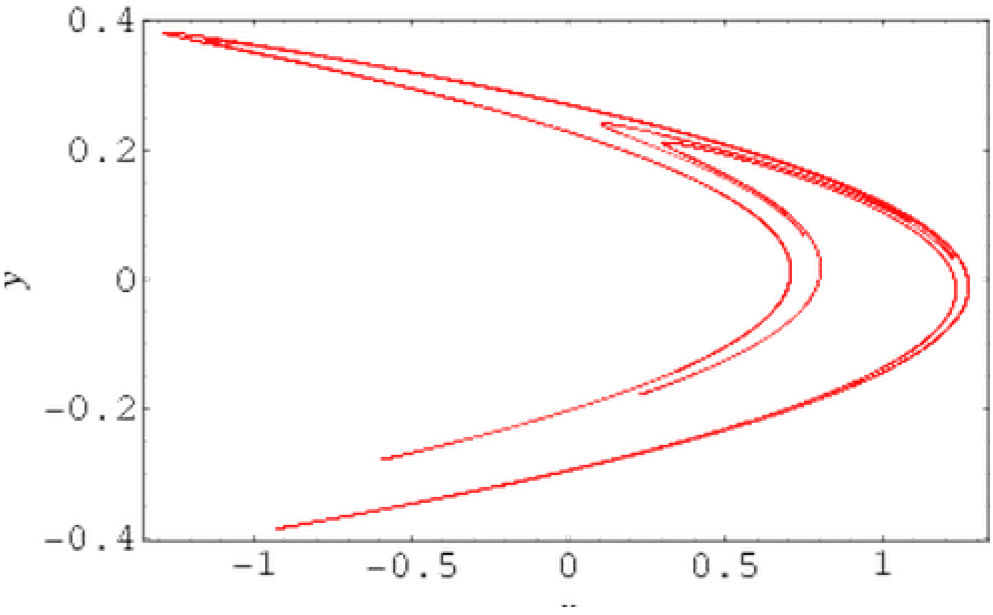


Fig. 2.3 A 2-D representation of Henon map.

Here, the parameters, *a* and *b* are of prime importance as the dynamic behaviour of system depends on these values. The system cannot be chaotic unless the values of *a* and *b* are 1.4 and 0.3 respectively. For some different values of *a* and *b* the map may be chaotic, intermittent, or obtain to a periodic orbit. Initial points X_1 and Y_1 [40] work as a symmetric key for chaotic cryptographic system used for encryption at sender's end and decryption at receiver's end.

$$\mathbf{X_{n+1} = 1+Y_n - 1.4X_n^2}$$

$$\mathbf{Y_{n+1} = 0.3X_n} \qquad \text{eqn.(2)}$$

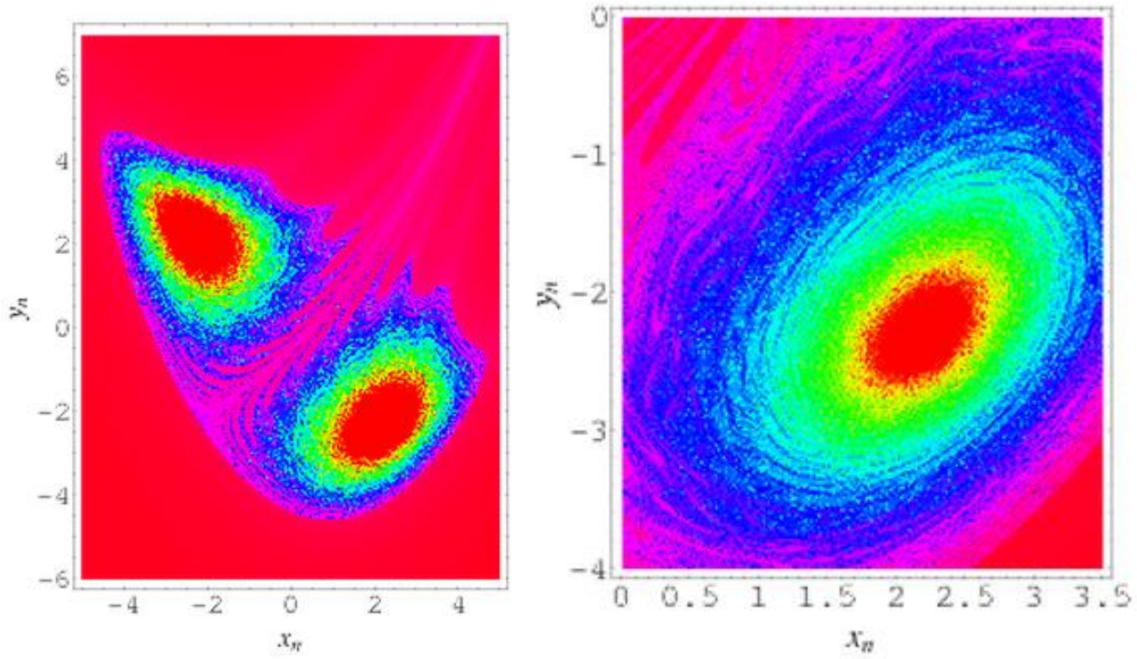


Fig.2.4The strange attractor illustrated above is obtained for a=1.4 and b=0.3

Since, Henon map is deterministic so decryption of the cipher image will reconstruct the original image at receiver's end with the same initial points X_1 and Y_1. Thus, sensitivity of key and encryption algorithm together contributes to avoid all kind of cryptanalysis attacks [5].

2.7 RANDOM NUMBER GENERATORS

There exist two types of random number generators:

- **Random number generator** - Random number generator is an algorithm or device that generates a sequence of binary bits that are statistically independent from each other [34].

  Random number generators are used in many cryptography algorithms and applications [34] [35] [36]. They provide high level of security for many cryptographic systems such as DES secret key, prime numbers in RSA algorithm, and prime numbers in digital signature.

- **Pseudorandom number generator**- A pseudorandom number generator (PRNG) is a procedure that produces a binary bit sequence that is approximately random [41]. All the processes are governed in deterministic manner. The input parameter of PRNG is called a seed and the output is called a binary sequence.

The PRNG generates sequence of length 1 which is not random. It collects all small truly random bit and expands it to a larger sequence of length l. Therefore, the PRNG sequence cannot be distinguished from the truly random sequence. Specific statistical tests and analysis are done to confirm the randomness of PRNG output [41].

Randomly chosen seeds play an important role in generating the sequence for these seeds (s, s+1, s+2,..) with the help of one-way function. Also, hash function and block cipher algorithms can be implemented to generate random bit sequence.

In stream cipher algorithms, pseudorandom number generators' (PRNGs) results are mainly used as a key streams that simply XOR with plain text to generate the ciphertext using any encryption algorithm Moreover, it is very important to generate the secret keys and initialization variables by PRNGs

2.8 CONFUSION AND DIFFUSION

Cryptography algorithms are designed based on confusion and diffusion [42]. In 1949, Claude Shannon introduced the terms ‘confusion’ and ‘diffusion’, which are considered to be a very important aspect for designing a secure encrypted message [43]. Shannon’s theory aims to deduce the possibility of ciphertext attack based on plaintext statistical analysis. Some cryptanalysts use their prior knowledge of plaintext statistical characteristics to make base of their attacks. In some languages, plaintext of different letters or words has a frequency distribution, which could be the starting point to find the used key or part of it [6]. Therefore, Shannon suggested that the ciphertext should be independent of the key used and also the ciphertext should be independent of the plaintext. Diffusion is nothing but hiding the relationship between the plaintext and ciphertext. Changing one bit in plaintext can affect more than half of the ciphertext bits. Confusion can be termed as hiding the relationship between the statistics of ciphertext and the key used so that it is sufficiently complicated to obscure any attempt to find the key. The principle of diffusion prevents the cryptanalyst from finding any relationship between the plaintext and the ciphertext, while confusion prevents the cryptanalyst from finding any relationship between the ciphertext and the used key.

Hash functions are similar to conventional encryption methods in a way that they require the influence of the whole input message to be spread into the hash value space. In an ideal hash function, there should exist a complex relationship between bits in input message and corresponding bits in hash value. Therefore, each bit has a 50% probability of changing and any bit change in the input message should affect at least half the hash value bits.

CHAPTER-3
RELATED WORK

In this section, a literature review of various techniques and methods on digital image security is done. There are two way of Image encryption, one is done in spatial domain and another in frequency domain. In cryptography scheme, spatial domain is used frequently rather than frequency domain. When these digital images are encrypted with traditional cryptography schemes, they have slow speed due to large size of data. With the introduction of Chaos theory and its applications, a new aspect of secure cryptography has emerged. According to [6], cryptography scheme has two types: one is symmetric key cryptography scheme and another one is known as private key cryptography scheme. Symmetric key cryptography scheme is achieved by two ways: one is stream cipher and another is block cipher.

The most popular symmetric key cryptography is DES (data encryption algorithm) [44]. It is the name of federal information processing standard (FIPS) 46-3; it shows DEA originated in IBM. It was adopted in 1977 as a standard by US Government for all commercial and unclassified information.

In the last decade, chaotic systems are actively working in cryptography system. Chaos theory has generated revolutionary changes in cryptography schemes with less complexity of encryption algorithm. Authors and researchers are doing a great work and giving a new dimension to cryptography with the help of chaos theory. In [45] Poincare published an article on the equations of the dynamics and the three-body problem, which simplified the way of looking at the complicated continuous trajectories from differential equations [46].

Edward Lorenz [47] [48] examined chaos theory by describing a simple model of Weather prediction which was first numerical model to detect chaos in a non-linear dynamical system. In Lorenz’s findings some equations gave rise to some surprisingly complex behaviour and chaos behaviour dependent on the initial condition. In [49], Hadamard analysed the sensitivity to the initial conditions and unpredictability of special systems, and called this the geodesic flow. Poincare proved that chaos sensitivity depends on initial conditions and gives unpredictable results in 1908. The word ‘chaos’ was first introduced into mathematical literature where system results appear random [49] by Li and Yorke in 1975.

The first published paper on ciphers based on a dynamical system was presented by Wolfram in 1985. He proposed a stream cipher algorithm based on cellular automation [50] which is used to generate a random binary sequence to produce the ciphertext.

In 1989, Matthews published the first chaos-based stream cipher algorithm [51] and suggested a chaotic function to generate a random sequence as system keys instead of pads. Matthews utilized characteristics of chaotic system to generate a random sequence with sensitivity to any change in the initial parameters.

In the literature, many chaotic pseudorandom number generators (CPRNGs) are used to implement cipher algorithms to generate the keystream [36]. In CPRNGs, many chaotic systems have been utilized including Piecewise non-linear chaotic map, Logistic map, Tent map, and Henon attractor.

In [52], Chen at el. presented symmetric image encryption scheme based on 3D chaotic cat maps. Wang at el. [53] introduced a 3D Cat map based symmetric image encryption method. Combined image encryption algorithm based on diffusion mapped disorder and hyper chaotic systems encryption scheme are also presented in [54][55]. However, the encryption arithmetic based on 3D chaotic cat maps is a computationally expensive process. And the key space is not independent.

Chen Wei-bin and Zhang Xin [56] in 2009 proposed an image encryption algorithm based on Arnold cat map with Henon chaotic system. Initially, Arnold cat map was used to shuffle the image pixels followed by using Henon map for encryption pixel by pixel. Several experiments are done by him that shows the efficiency of secure encryption algorithm.

MintuPhilipand and Asha Das [57], conducted a survey on various image encryption methodology and analysed the performance of past chaotic image encryption schemes.

Huang at el. [58] in 2009, proposed a novel Multi chaotic systems based pixel shuffling method for color image encryption.

In [59], author proposed and described Dynamical Properties of the Henon Map.Fethi Belhouche at el. [60] in 2004, proposed a method for binary image transformation using two dimensional chaotic maps. In this method, he produced almost uncorrelated images using Henon chaotic map for required image transformation. Jiansheng Guo at el. [61] in 2010 , introduced a method for breaking chaotic encryption based on Henon map, in which they analysed the efficiency of 2-D Henon chaotic system and figured out two weaknesses stating that confusion process do not destroys the correlation of images and the transform function is unbalanced.

CHAPTER-4

PROPOSED ALGORITHM FOR ENCRYPTION

4.1 MOTIVATION

The recent growth of networked multimedia systems has increased the need for the protection of digital media. This is mainly important for the protection of digital images being shared electronically. Image security involves the confidentiality, integrity and authentication of an image. Several encryption algorithms are known and are used widely. It takes a great effort to increase the key space. Chaotic maps have various properties which are used for increasing confusion and diffusion process in multimedia cryptography. Primitive keys used for encryption which were easy to get disclosed are getting replaced with more complex and mathematically generated highly secure keys. As chaotic maps are mathematical in nature and work on real number so it's easy to formulate and generate keys which are random in behavior. Chaotic map are totally different from traditional cryptography schemes which are unpractical on images. Chaos maps truly works on one time pad scheme, so it is just impossible for cryptanalysis to decode the cipher image because of these properties of chaotic system. Computable cost, complexity and other factors increase the use of chaotic system. Without such methods, placing images on a public network puts them at risk of several active and passive attacks and alteration.

4.2 PROPOSED ALGORITHM

The inputs to the chaotic Henon system are: the image to be encrypted and the initial values of Henon map which is treated as a key. In this project we use *I* to denote an image of size m×n where *m* and *n* represents rows and columns of an image respectively. F(x, y) represents the gray scale value of a pixel at position x and y. In proposed approach, first of all, the image pixels are shifted from one place to new place according to a novel shuffling method. For accurate shuffling, padding is required in image. After applying this method on input image, Henon chaotic map is used to generate binary sequence with a novel approach of encryption technique at sender’s end.

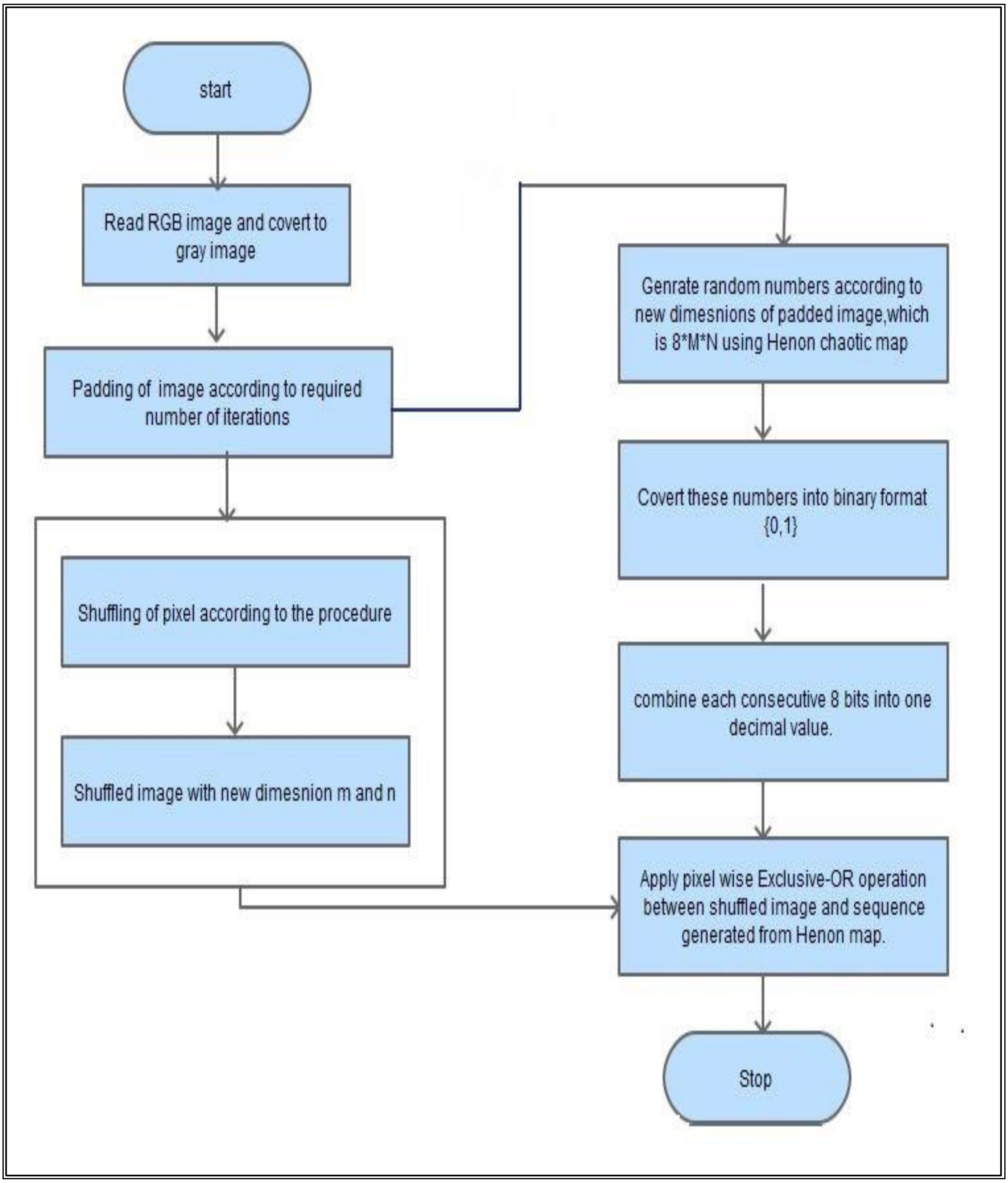

start
Read RGB image and covert to gray image
Padding of image according to required number of iterations
Shuffling of pixel according to the procedure
Shuffled image with new dimesnion m and n
Genrate random numbers according to new dimesnions of padded image,which is 8*M*N using Henon chaotic map
Covert these numbers into binary format {0,1}
combine each consecutive 8 bits into one decimal value.
Apply pixel wise Exclusive-OR operation between shuffled image and sequence generated from Henon map.
Stop

Fig. 4.1 Flowchart for proposed algorithm

A. SHUFFLING OF IMAGE PIXELS

Step 1.PADDING OF IMAGE

❖ Algorithm For Padding

The number of iteration for shuffling depends on size of the image. Number of rows and column are the primary concern for this process and these factors defines Size of padding and number of padded array. Required algorithm for padding is given below:

```
for i=1 to k
        if   $m /2^k ==0$
                No padding required in image
        Else
                I+ [$2^{k-1}$] number of padding with size [1,n] =new dimension of image;
                $m=m+2^{k-1;}$
                n=n;

        if   $n/2^k ==0$
                No padding required in image
        Else
                I+ [$2^{k-1}$] number of padding with size [m,1] =new dimension of image;
                m=m;
                $n=n+2^{k-1;}$
end
```

Zero padding consists of appending zeros to an Image. Padding size of an image depends on the number of iterations. Pad size is a vector of non-negative integers that specifies the amount of padding to add and the dimension along which to add it. If number of rows and columns are not divisible by 2^k, where, k=1,2…,n according to iteration then padded array with zero element in input image. The value of an element in the vector specifies the amount of padding to be added. The order of the element in the vector specifies the dimension along which to add the padding.

1. If number of rows are not divisible by 2^k, where, k=1, 2…,n is the number of iteration of pixel shuffling then add (2^{k-1}) zero matrix with size of [1, n]. After padding, even numbers of rows are obtained and image can divide into quadrants uniformly. This is also applicable for the columns. The new size of image will be (m+1)×n.
2. If the number of columns is not divisible by 2^k , k=1,2…,n then number of zero matrix (2^{k-1}) in [m,1] fashion padded to image now (2^{k-1}) column in image now the size of image m*(n+1) . After doing this black boundary attached in image with even number of rows and columns.

- **Example Of Padding For Iteration First**

1. If numbers of rows are not divisible by 2 then we add a zero matrix with size of [1, n]. After padding this we get even number of rows so we can divide our matrix accurately. It also depends on number of columns. Now the new size of (m+1)*n.
2. After checking for the number of rows we check number of columns. If number of columns is not divisible by 2 then, we pad zero matrix in [m, 1] fashion in order to get one more column in image. Now size of the image is m*(n+1). After doing this we get even number of rows and columns.

Step 2.SUCCESSIVE ITERATIONS FOR SHUFFLING PIXELS

Shuffling is useful to disturb the correlation among the adjacent pixels. One of these features is that the image is being apparently randomized by the transformation and returning to its original state after a number of steps. Multiple smaller copies arranged in a repeating structure and even upside-down copies of the original image—and ultimately return to the original image. Here Shuffling of the image depends upon the number of rows and columns. Divide the image into four parts. If the number of rows and columns are not divisible by 2^k , k=1,2…,n then zero bits are padded in image according to step1. Here, shuffling of pixel is done in two steps.

a) For each iteration, a quadrant is subdivided into equal sub-quadrants.
b) For the k^{th} iteration, if it is odd then rotation of quadrant is in clockwise direction and shifted into a new place otherwise in anti-clockwise direction.

To illustrate this process, two iterations are represented by the fig.4.5.

❖ FIRST ITERATION

Initially, divide the image in four quadrants and then rotate each quadrant in clockwise direction. As shown in fig.4.2, TL shifts to TR position, TR shifts to BR position, BL shifts to TL position and last quadrant of image BR shifts to BL position.

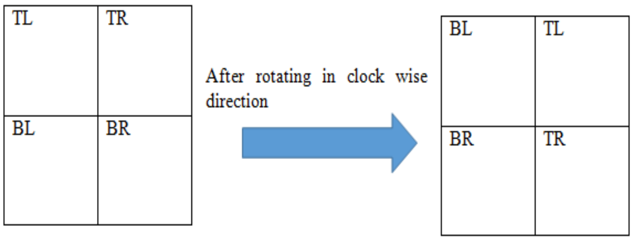
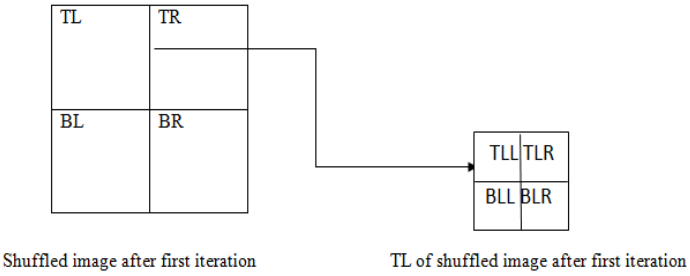


Fig. 4.2Image quadrants after first iteration

❖ SECOND ITERATION

Now each quadrant of shuffled image obtained after first iteration is further divided into sub-quadrant and follows the same procedure which is illustrate in Fig. 4.4, but in anti-clock wise direction.



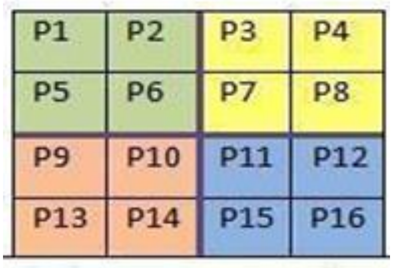
Shuffled image after first iteration

TL of shuffled image after first iteration

Fig. 4.3 Representssub-quadrants of a quadrant.

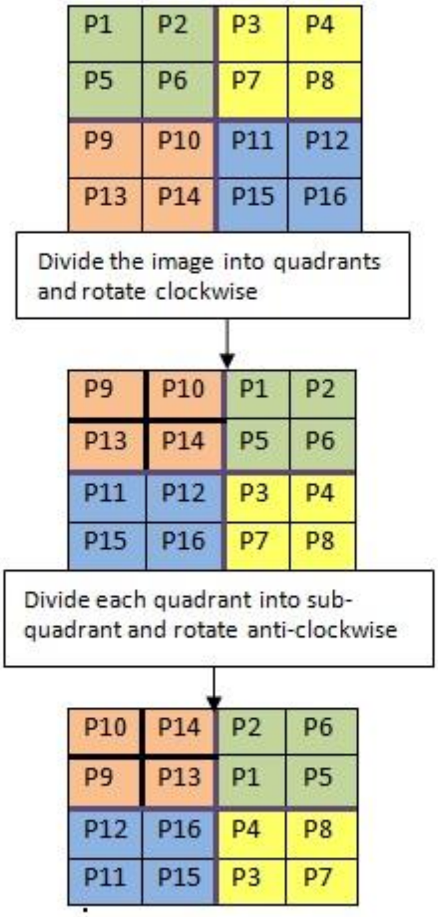
EXAMPLE:

To understand the property and phenomena of shuffling procedure, an example is illustrated below. Size of the image is 4×4, so number of pixel in image are 16. In first step, image has been divided into four equal quadrant then these quadrants are shifted in clockwise direction. In the next step these quadrants are further divided into sub-quadrant and shuffled in anti-clock wise direction.



P1	P2	P3	P4
P5	P6	P7	P8
P9	P10	P11	P12
P13	P14	P15	P16

Fig. 4.4 Represents initial position of pixels denoted by P



P1	P2	P3	P4
P5	P6	P7	P8
P9	P10	P11	P12
P13	P14	P15	P16

Divide the image into quadrants and rotate clockwise

P9	P10	P1	P2
P13	P14	P5	P6
P11	P12	P3	P4
P15	P16	P7	P8

Divide each quadrant into sub-quadrant and rotate anti-clockwise

P10	P14	P2	P6
P9	P13	P1	P5
P12	P16	P4	P8
P11	P15	P3	P7

Fig. 4.5 Shuffled image after two iterations

B. IMAGE ENCRYPTION BY HENON CHAOTIC SYSTEM

Henon map is a kind of mathematical function which works on the initial parameter. With the help of Henon map random sequences can be generated. It is a discrete-time dynamical system. It depends on two parameters, *a* and *b*, which have values of *a* = 1.4 and *b* = 0.3for the **classical Henonmap**. For the classical values the Hénon map is chaotic. For other values of *a* and *b* the map may be intermittent, chaotic, or converge to a periodic orbit. A summary of the type of behavior of the map at different parameter values may be obtained from its orbit diagram.

$$X_{n+1} = 1+Y_n - 1.4X_n^2$$

$$Y_{n+1} = 0.3X_n \qquad \text{eqn.(3)}$$

The shuffled image is encrypted using pseudo-random binary sequence generated by taking key values for Henon map.

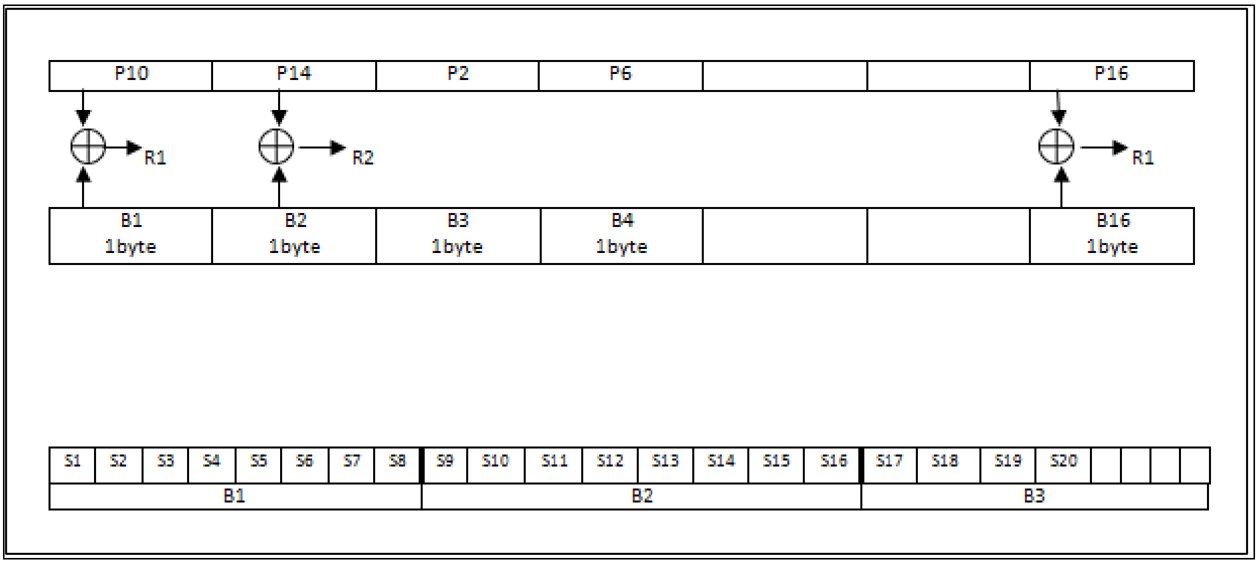
Step 1: Choose the initial value of (X_1, Y1) for Henon map. This value works as an initial secret symmetric key for Henon map.

Step 2: Henon map works as a key stream generator for cryptosystem. The size of sequence depends upon the size of image. If the image size is m×n then the number of henon sequence will be 8×m×n as obtained by equation (3).

Step 3: Experimental analysis conclude [11] that cut-off point, 0.3992, has been determined so that the sequence is balanced. The decimal values are then converted into binary values depending upon this threshold value.

$$Z_i = \begin{cases} 0 \; if \; Xi \leq 0.3992 \\ 1 \; if \; Xi \geq 0.3992 \end{cases} \qquad \text{......... eqn.(4)}$$

Step 4: Henon sequence is then reduced by combining each consecutive 8 bits into one decimal value.



. **Fig. 4.6Encryption with byte sequence**

Step 5: Encryption is done by bitwise Exclusive-OR operation between shuffled image and sequence generated in step 4 as shown in fig. 4.6. Confusion has done by permutation of pixel and diffusion has done by encryption technique.

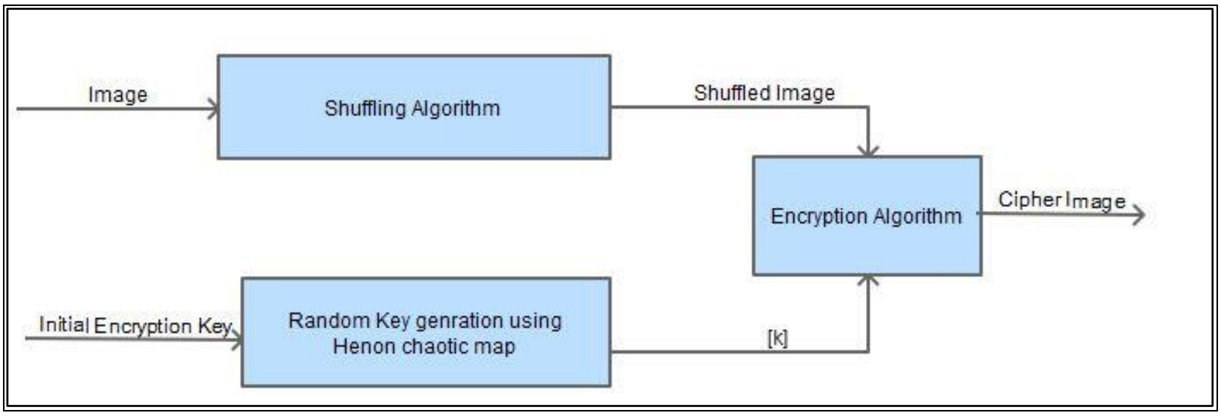


Fig. 4.7 Encryption process

C. DECRYPTION OF ENCRYPTED IMAGE

Since, the chaotic system behaviour is deterministic so reconstruction of image using the same key (X_1, Y_1) at decryption end gives the shuffled image. This shuffled image is further arranged in an order exactly opposite of the way done for encryption. Finally, the original image is obtained at receiver's end. As seen in fig. 4.8, initial keys are obtained at receiver's end along with cipher text. Henon sequence is generated with initial keys, encrypted image and Henon map go through Ex-or operation and result in shuffled image. Further shuffling of pixels in shuffled image in reverse direction produces the original image.

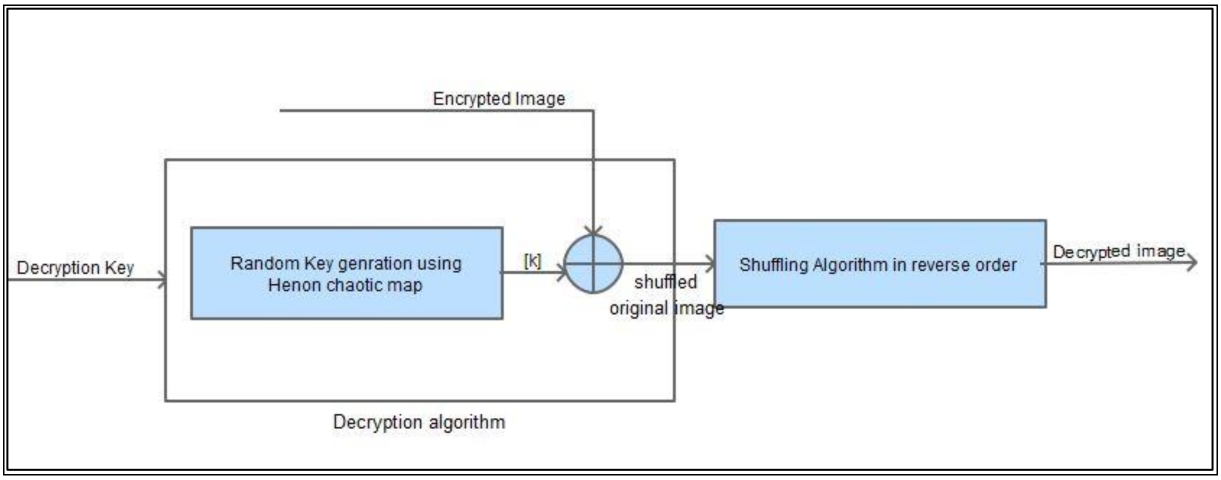


Fig. 4.8Decryption process

CHAPTER-5

EXPERIMENTAL RESULTS AND DISCUSSION

In this section, experimental results of the proposed image encryption algorithm are illustrated to appreciate the efficiency of proposed algorithm with gray and color images. The MATLAB 7.9 software was used for implementing this code. Grayscale is usually the preferred format for image processing. Color images can be decomposed and handled as three separate grayscale images.

Here, test image of size 204×204 is shown in Fig.5.2 (a). The initial parameters for Henon map are chosen as a=1.4 and b=0.3 to make the system chaotic. Secret symmetric key for encryption is a combination of X_1=0.01and Y_1=0.02.Fig.5.2 (b) and Fig.5.2(c) illustrates shuffled image after first iterations and second iteration of shuffling respectively.And the resulted encrypted image has shown in Fig.5.2 (d).

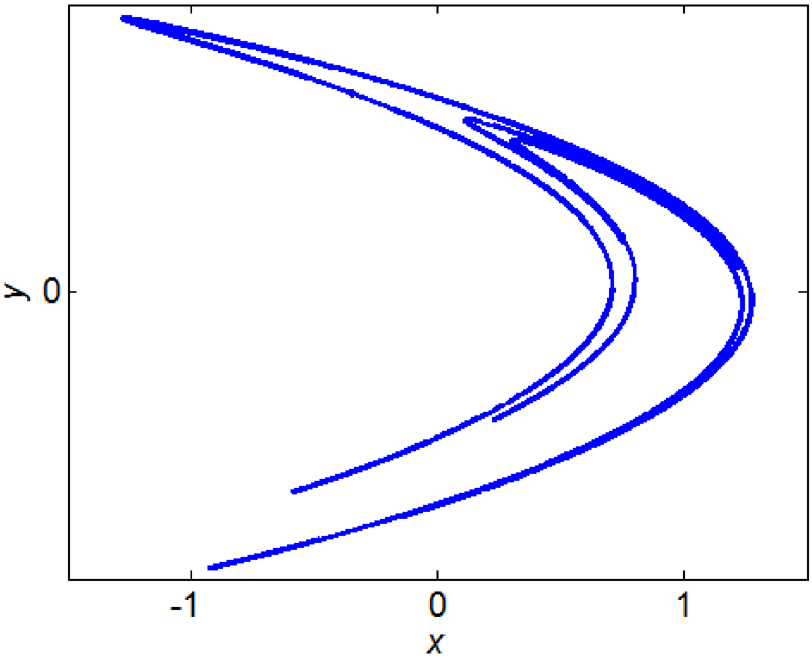
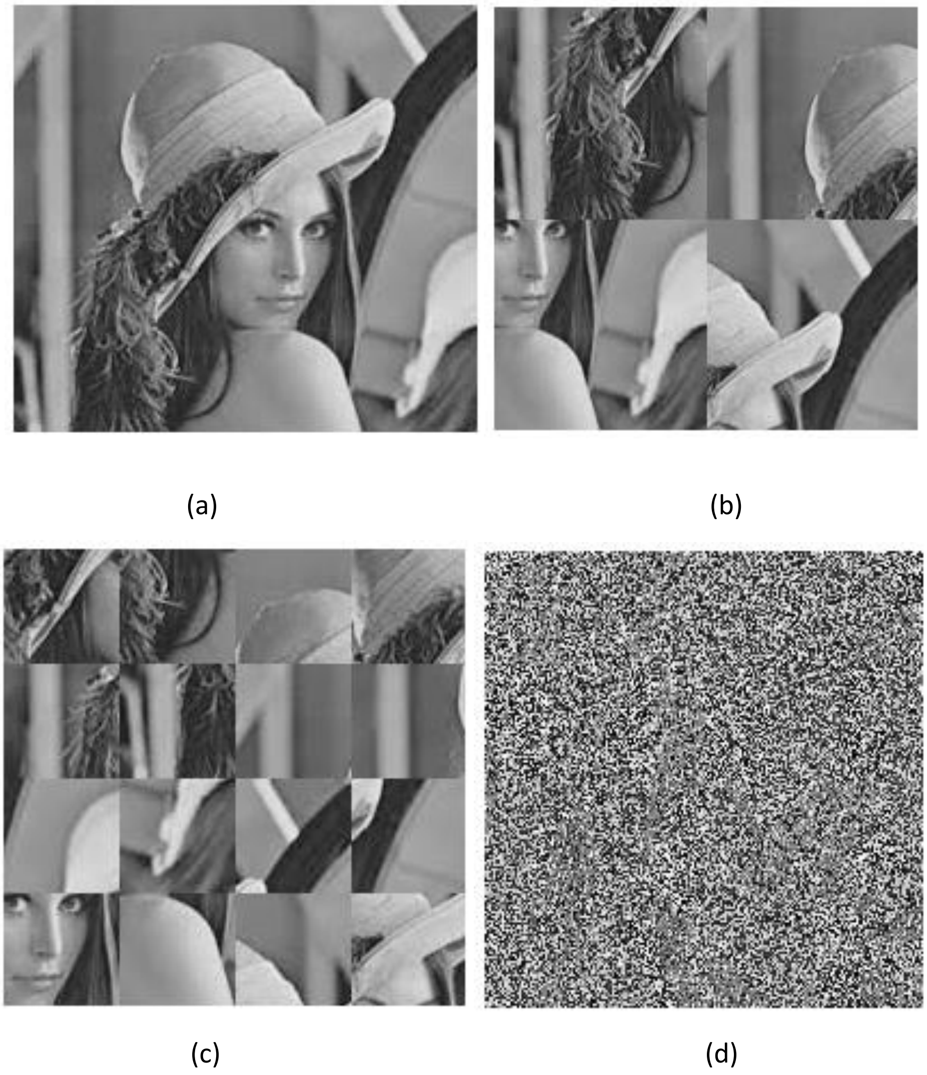


Fig. 5.1 Plot of Henon map

❖ ENCRYPTION OF IMAGE

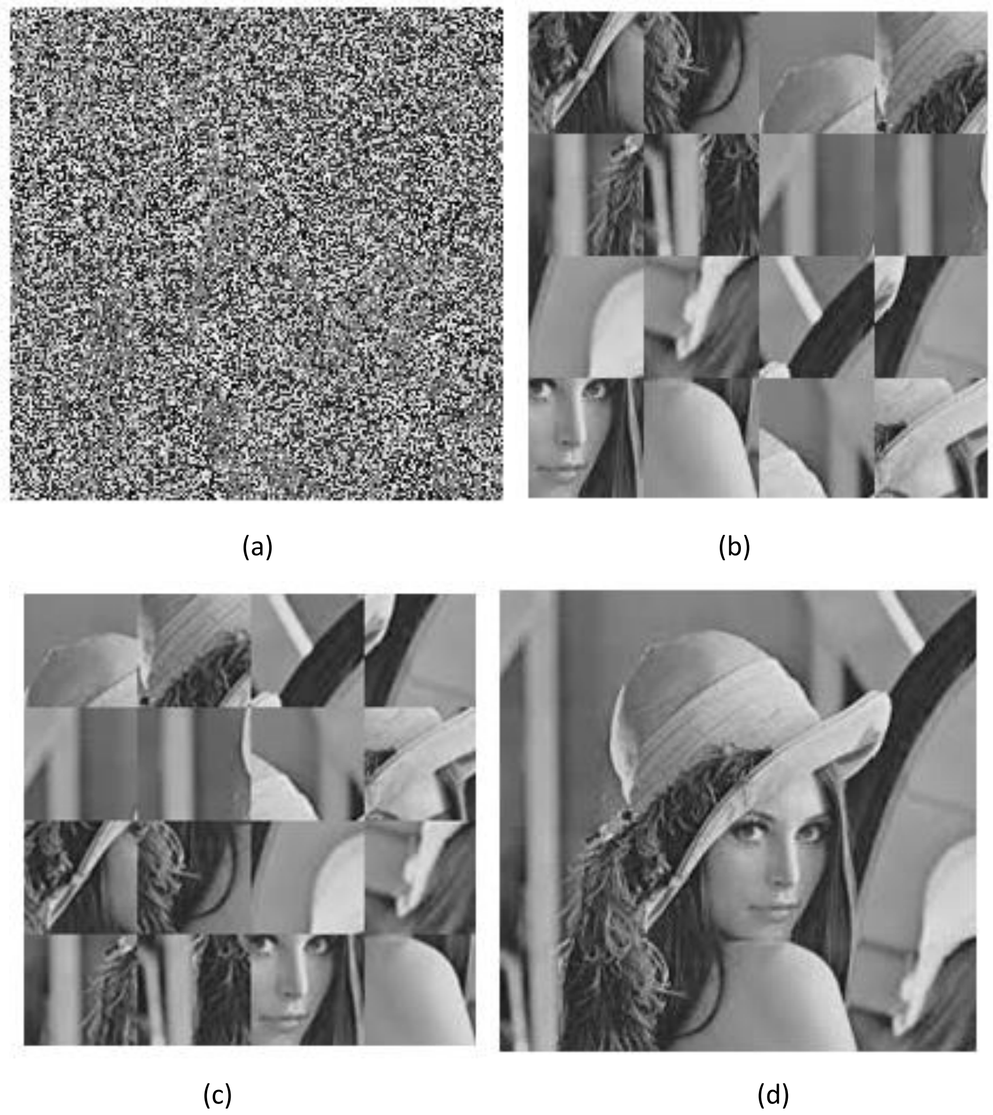


(a) (b)

(c) (d)

Fig. 5.2 Encryption by Henon chaotic system. (a) Original image (b) Shuffled image after first iteration (c) Shuffled image after second iteration and (d) Cipher image.

❖ DECRYPTION OF IMAGE



(a) (b)

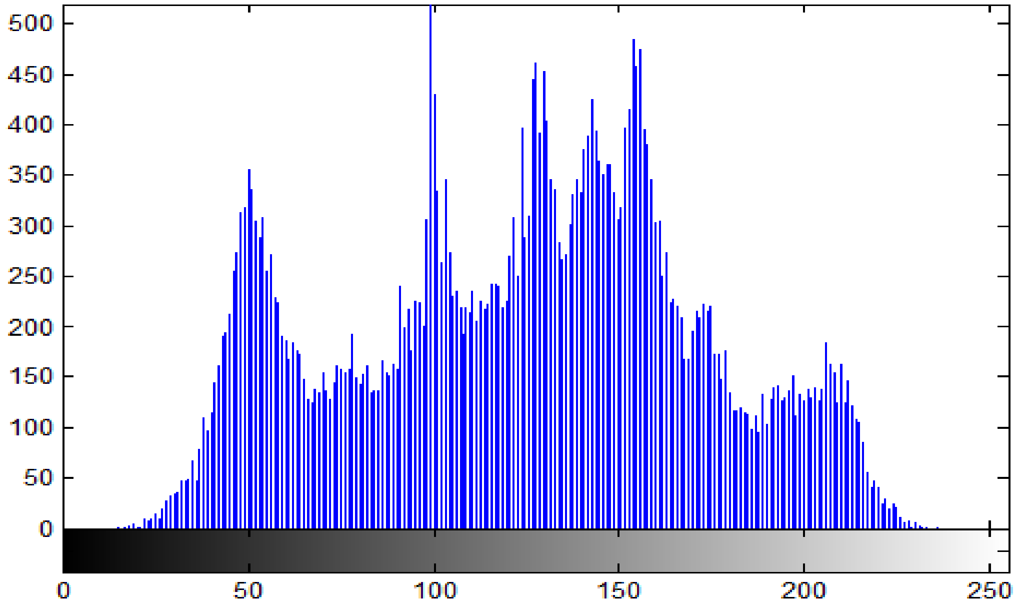
(c) (d)

Fig. 5.3 Decryption by Henon chaotic system. (a) Cipher image(b)Decrypted shuffled image (c) Shuffled image after applying shuffling algorithm in reverse order (d) original image.

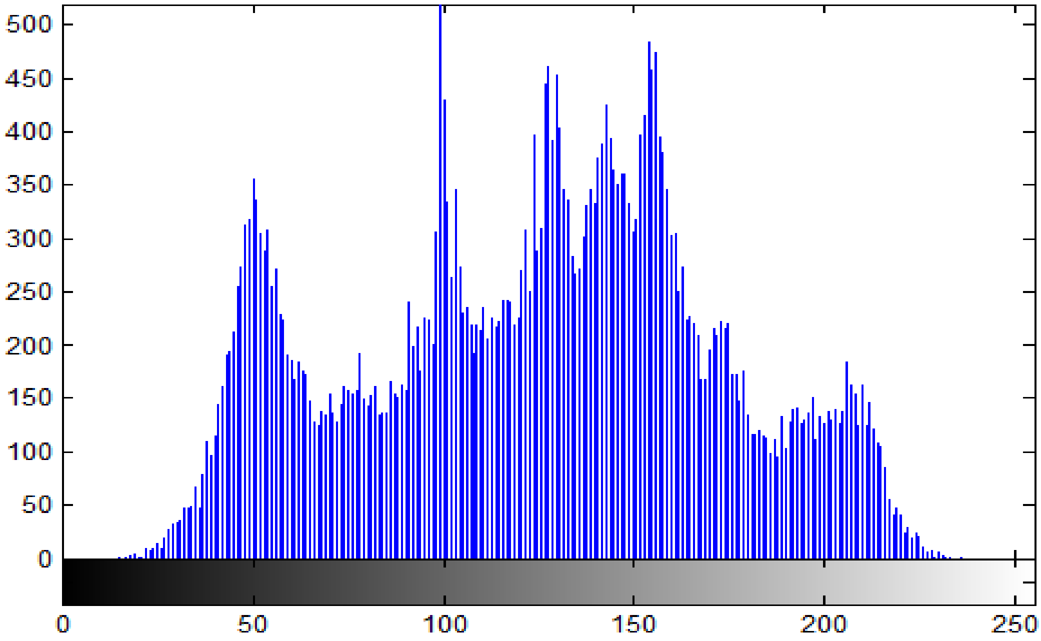
5.1 STATISTICAL ANALYSIS

A. HISTOGRAM ANALYSIS

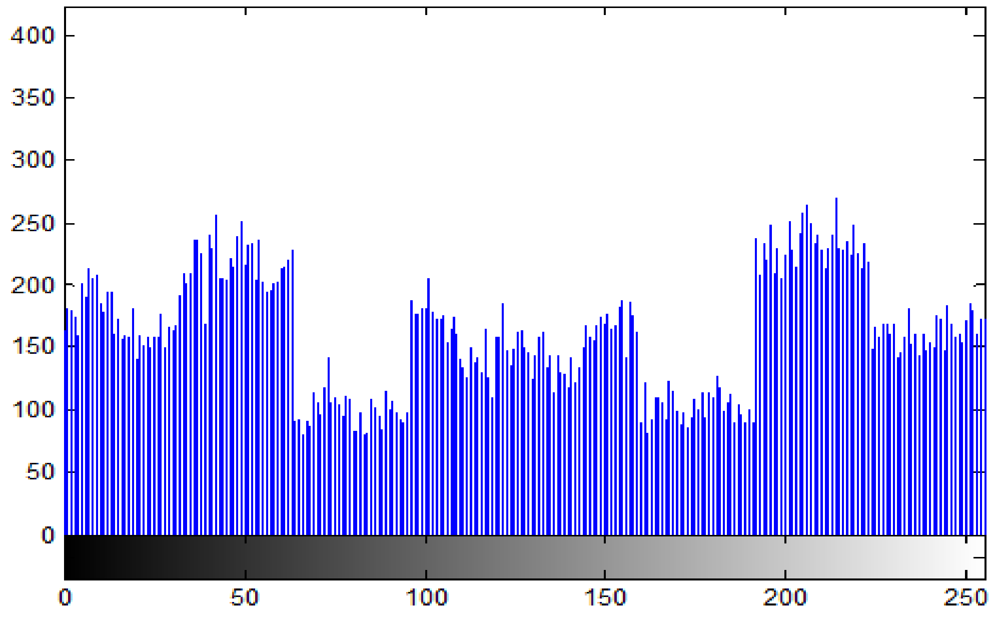
The histogram of an image is graphical representation of pixel intensity values. There are 256 different possible intensities for an 8-bit grayscale image, so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values.



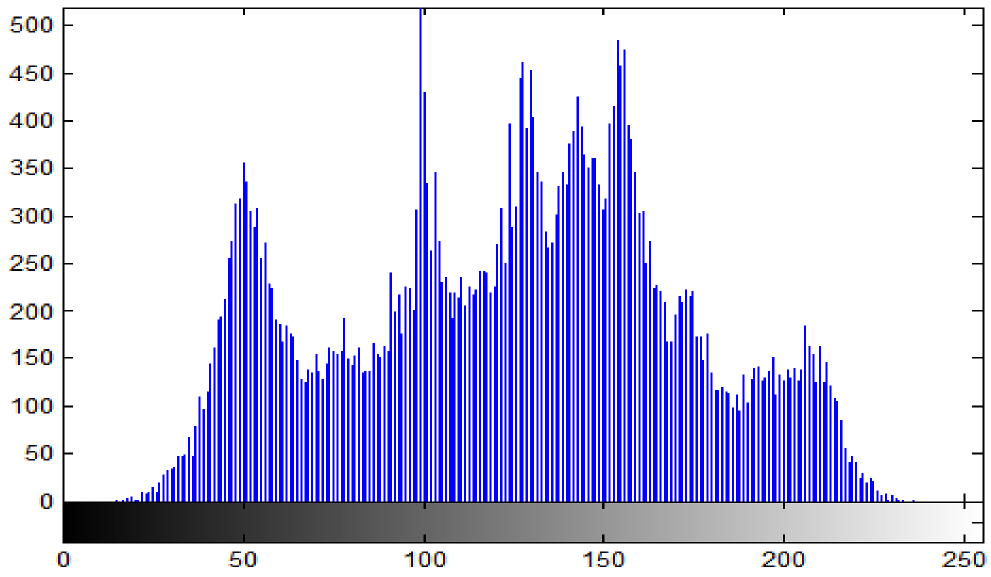
(a)



(b)



(c)



(d)

Fig. 5.4 Histogram analysis: (a) histogram of original image(b) histogram of shuffled image (c) histogram of cipher image (d) histogram of decrypted image.

It is analysed from Fig. 5.4, that there exists uniform distribution of gray scale values in cipher image, and significantly different from histograms of original image. In the original image some of the gray scale values do not exist in the range of 0 to 255 but in encrypted image gray-scale values exist uniformly in the range 0 to 255. Therefore, it is proved that the encrypted image does not help intruders to employ statistical attack on encryption procedure.

B. INFORMATION ENTROPY ANALYSIS

Information entropy is defined by the degree of uncertainties in the encryption system. It is used to calculate the Effectiveness of image encryption algorithm. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as

$$H= -\text{sum}\ (p.*\log2\ (p)) \qquad \text{eqn.(5)}$$

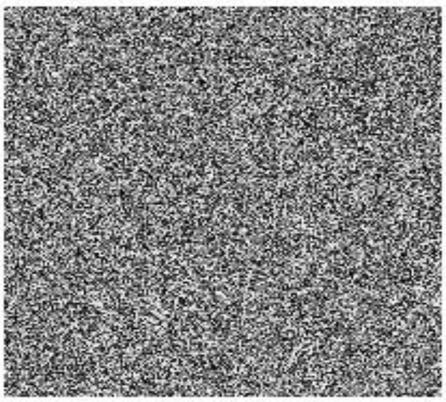
Ideal entropy of an encrypted image should be equal to 8, which corresponds to a random source. Practically, information entropy is less diverse than the ideal one. The values calculated in Table 1 are very close to the ideal value.

	Original image	After first iteration	After second iteration
Entropy	7.4521	7.9406	7.9383

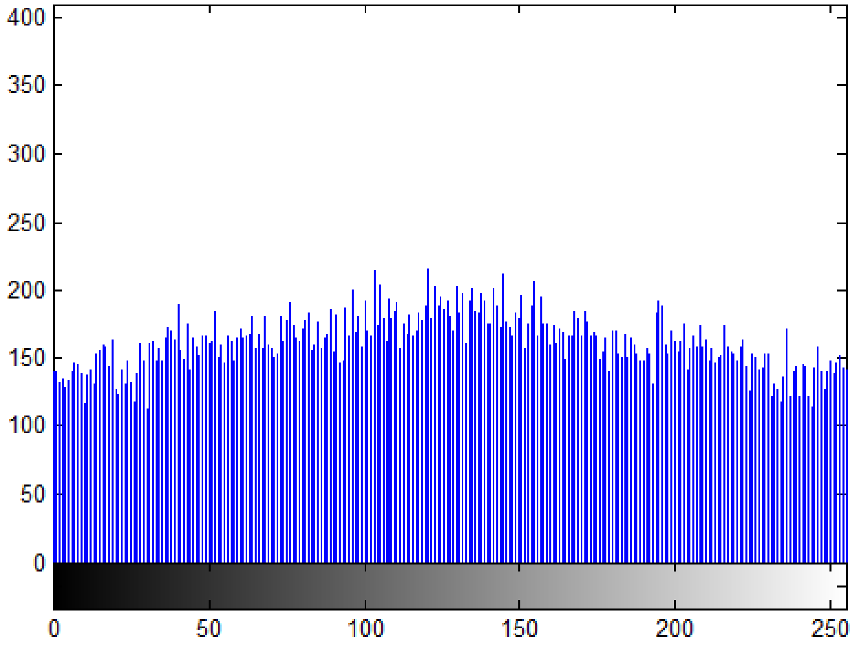
Table 2: Entropy analysis

C. KEY SENSITIVITY TEST

For secure encryption, the key should be sensitive with large space key size to resist all kind of brute force attack. Randomness is the key point of Henon map. To test the sensitivity of the key involved, a minute variation was done in original secret key by changing it from x(1)=0.01 and y(1)=0.02 to x'(1)=0.010001 and y'(1)=0.020001. As a result, it was not possible to obtain the original image at receiver's end without knowing the decryption key.



(a)

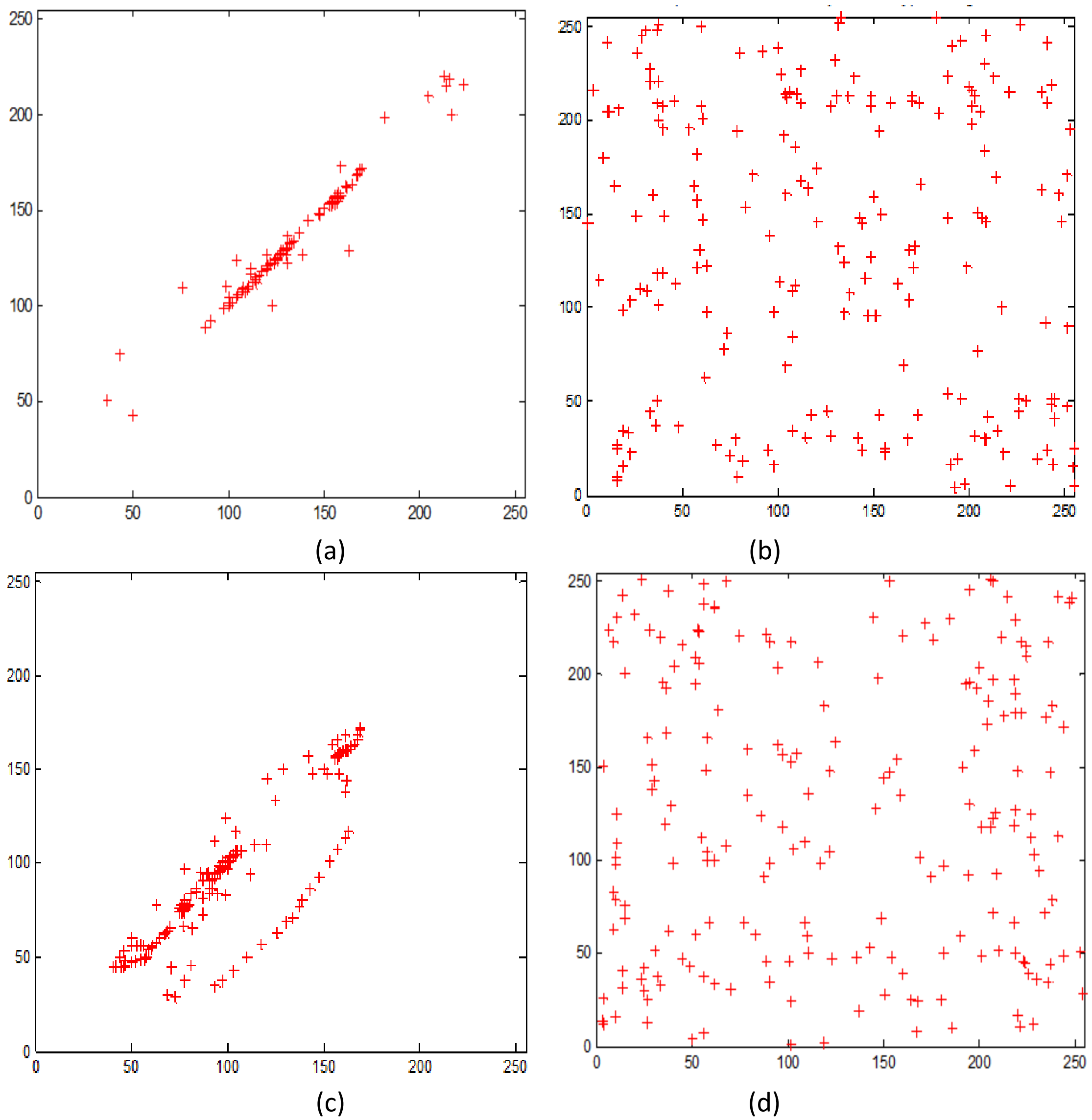


(b)

Fig. 5.5 Key sensitivity analysis: (a) Decrypted image after slight variation in key (b) histogram of decrypted image.

D. ADJACENT PIXEL CORRELATION ANALYSIS

Adjacent pixel correlation is a measure of relationship between two variables. There is very close correlation between the two neighboring pixels in an image. The correlation coefficient Cr, is computed for 1000 adjacent pixels using direct MATLAB command.



(a) (b)

(c) (d)

Fig. 5.6Correlation analysis. (a)Pixel value in original image for 4th row and 5th coloumn (horizontally) (b) Pixel value correlation in encrypted image (horizontally) (c) Pixel value correlation in original image (vertically) (d) Pixel value correlation in encrypted image (vertically).

E. MEAN VALUE ANALYSIS

Mean value analysis is done to verify the distribution of mean pixel gray value in every vertical line of an image. It also gives the average intensity of pixels along the horizontal direction in the image. In a plain image, the mean value differs along the horizontal direction and has wide variations in the mean across the width of the image.

In an encrypted image the mean value along the horizontal direction should remain consistent, which indicates uniform distribution of gray levels along all vertical lines of the encrypted image. Figures 5.7 show the mean value obtained from the encrypted gray scale images by applying the proposed encryption method. Here red line is for original image and blue line is for encrypted image.The mean vauel across the image remains nearly consistent and close to each other.

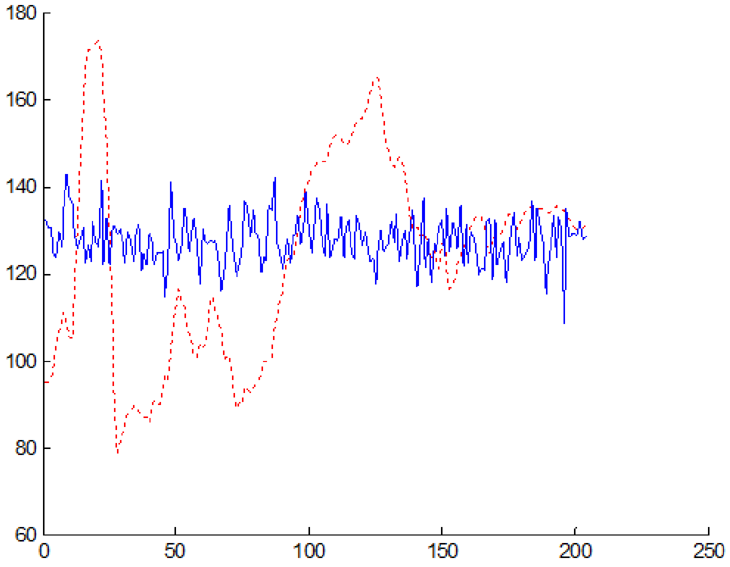
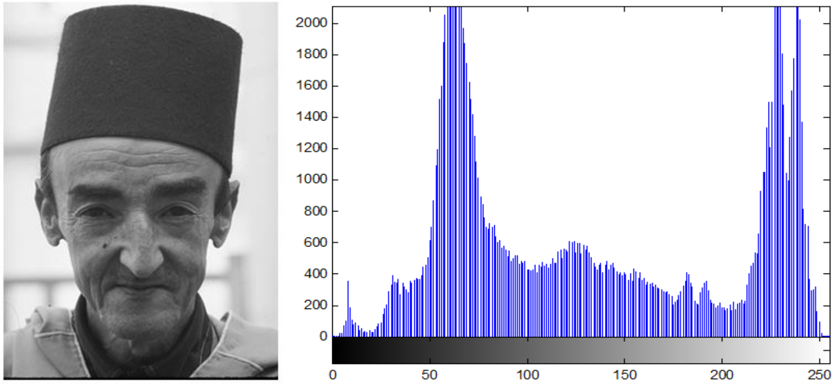


Fig. 5.7Mean value of original image and encrypted image.

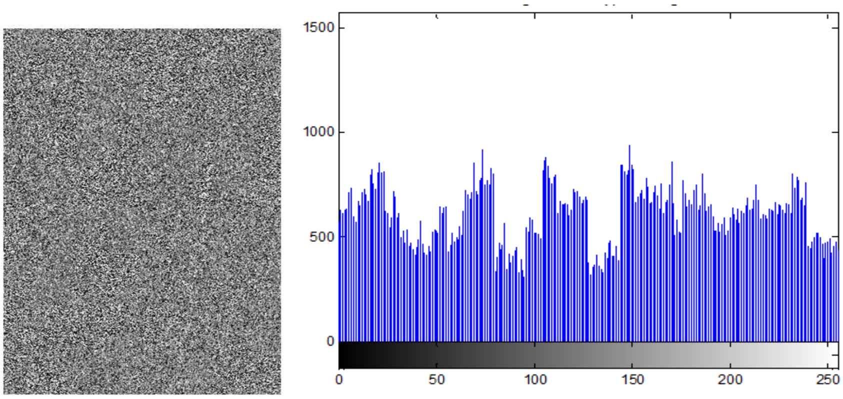
5.2 EXPERIMENATAL RESULTS ON DIFFERENT GRAY IMAGES

Following are the results obtained by applying proposed algorithm on differentgray images. Here (a) represents original image and its histogram, (b) represents encrypted image and its histogram and (c) represents decrypted image and its histogram.

A.



B.



C.

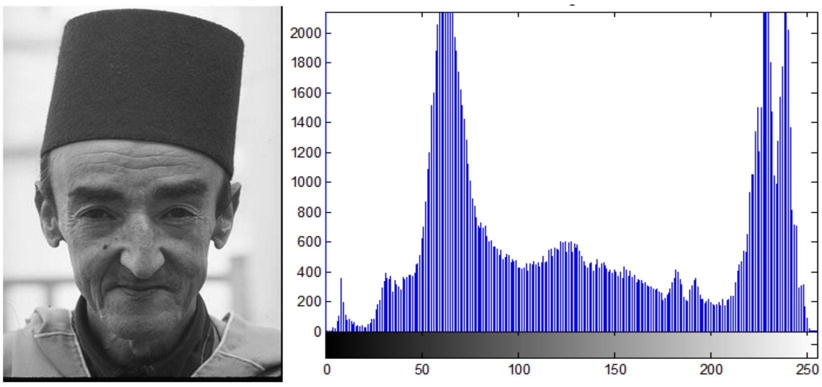
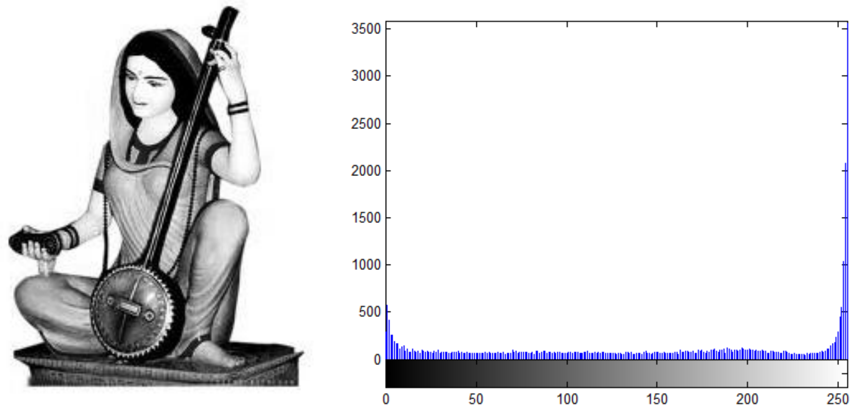
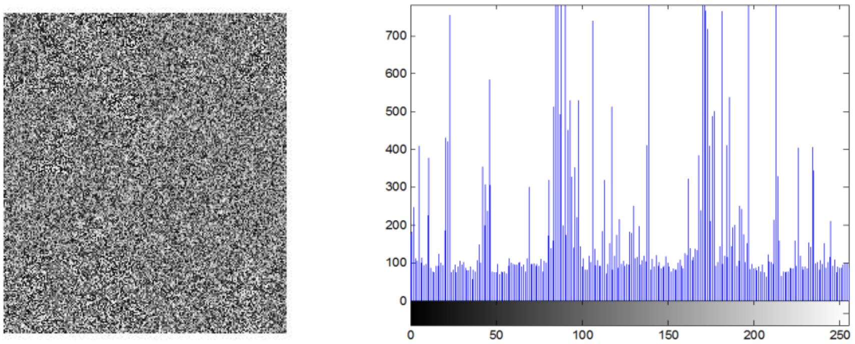


Image size	238×212
Entropy of Original Image	7.43
Entropy of Encrypted image	7.93
Encryption Quality	438.009

A.



B.



C.

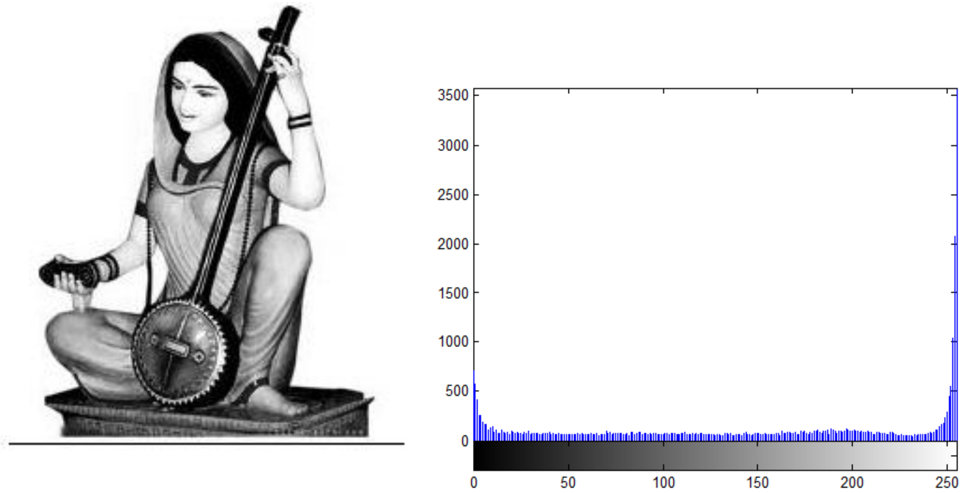
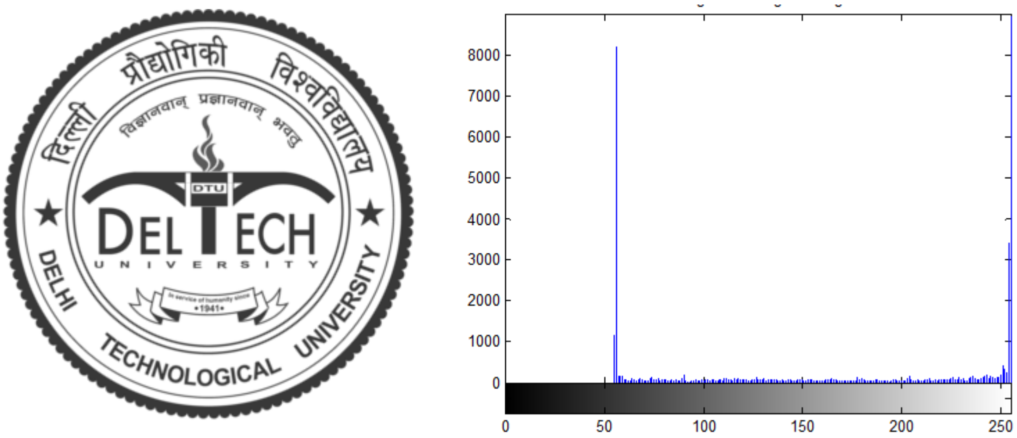
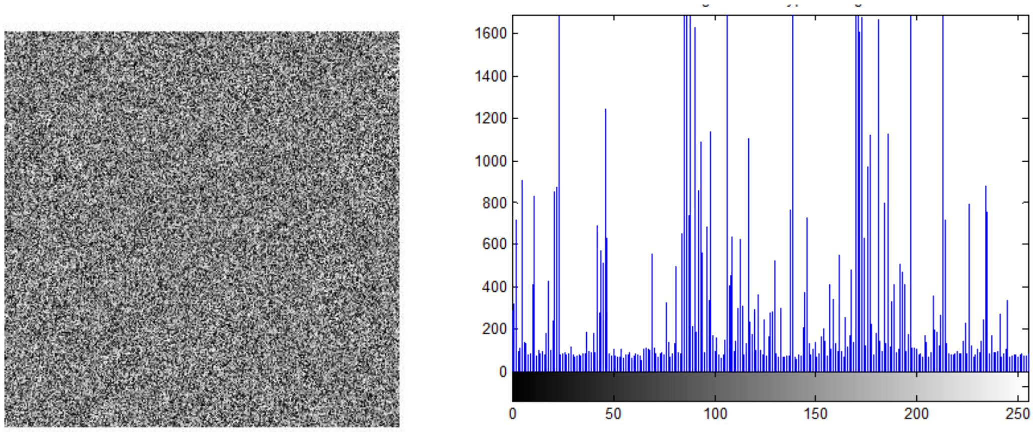


Image size	238×212
Entropy of Original Image	5.1417
Entropy of Encrypted image	7.38
Encryption Quality	225.98

A.



B.



C.

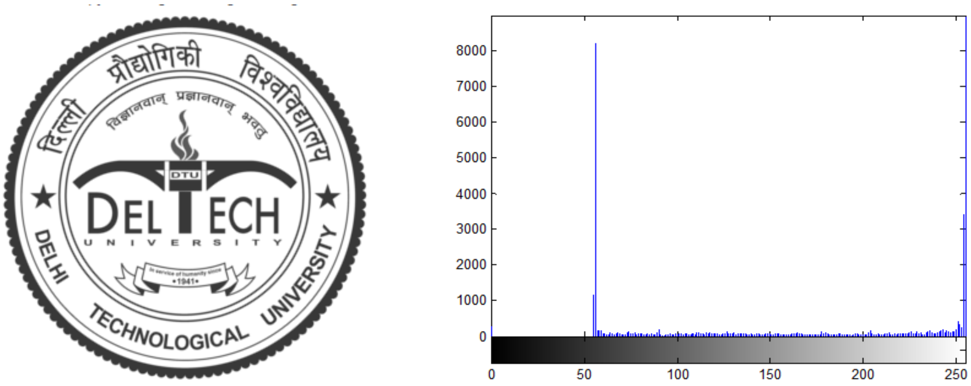
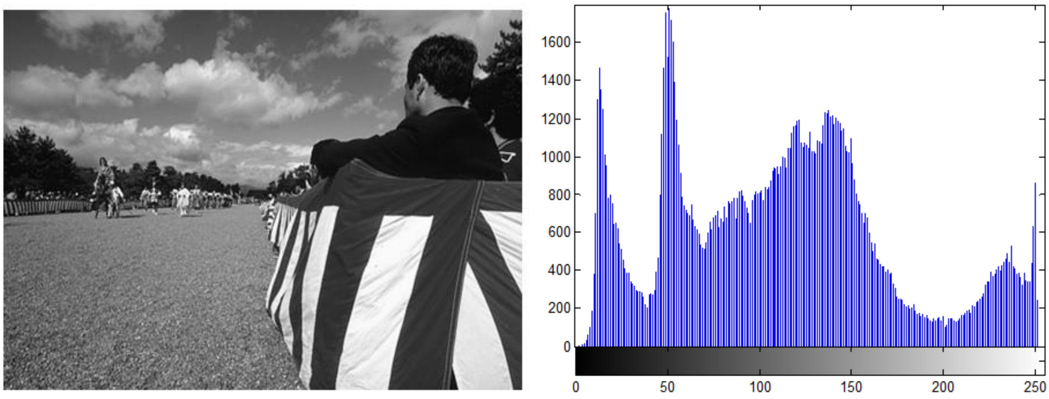
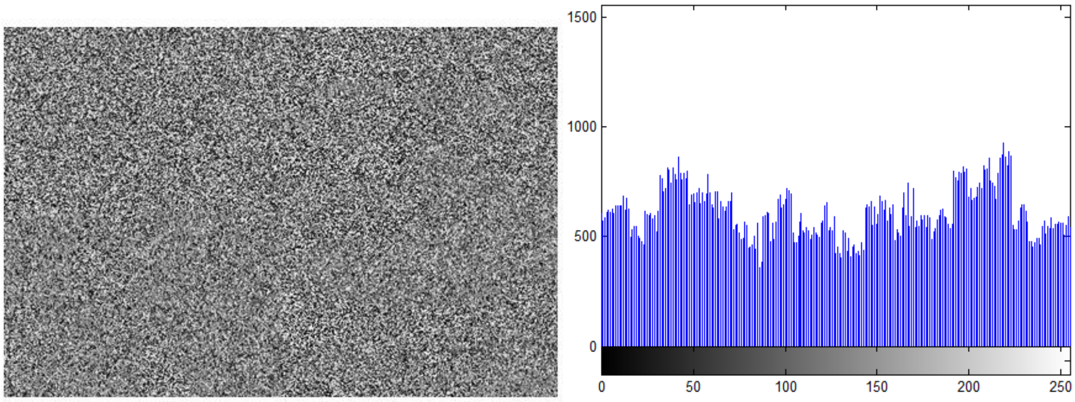


Image size	300×300
Entropy of Original Image	3.1767
Entropy of Encrypted image	6.95
Encryption Quality	563.16

A.



B.



C.

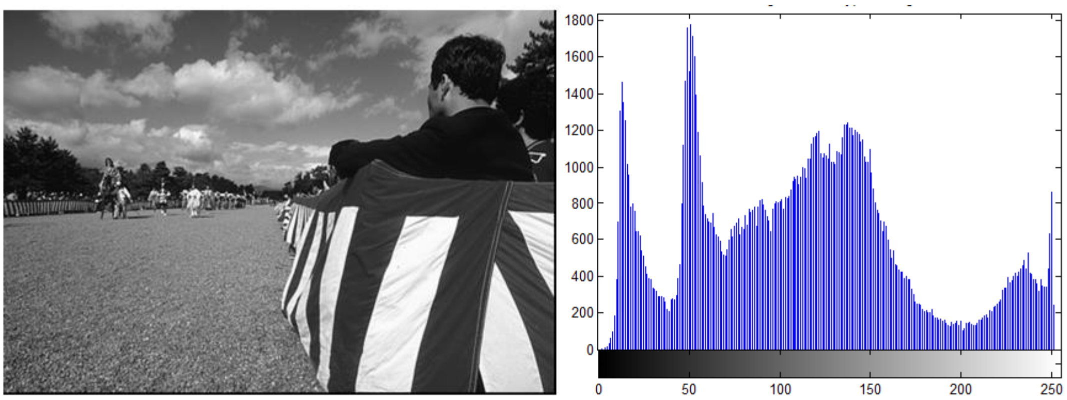
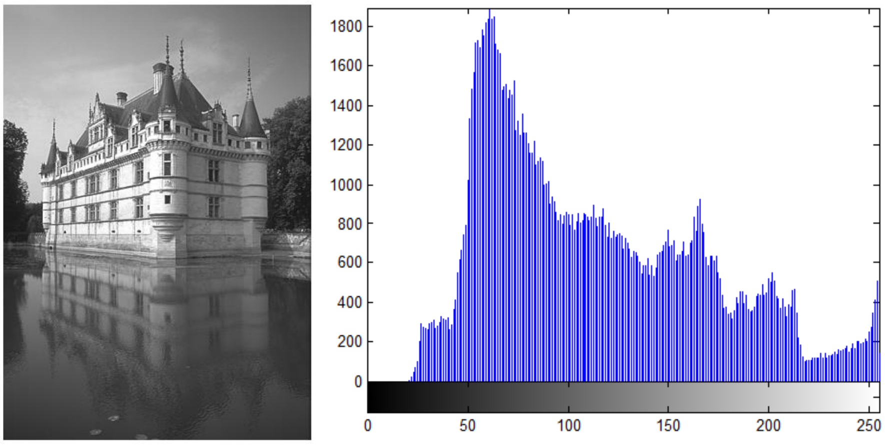
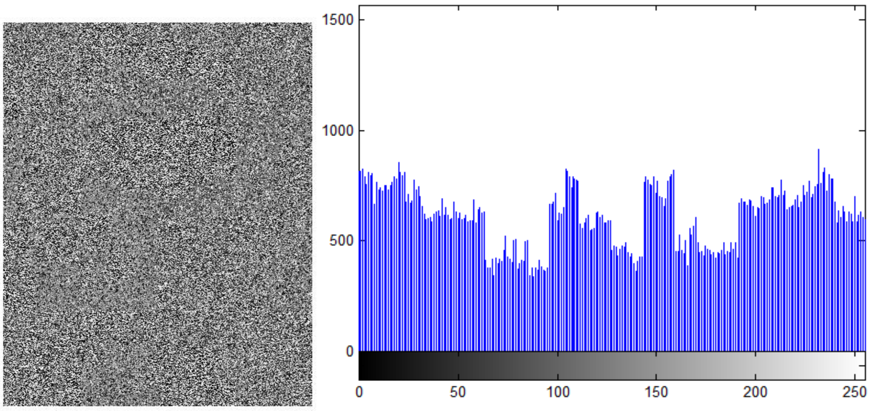


Image size	321×481
Entropy of Original Image	7.67
Entropy of Encrypted image	7.98
Encryption Quality	372.25

A.



B.



C.

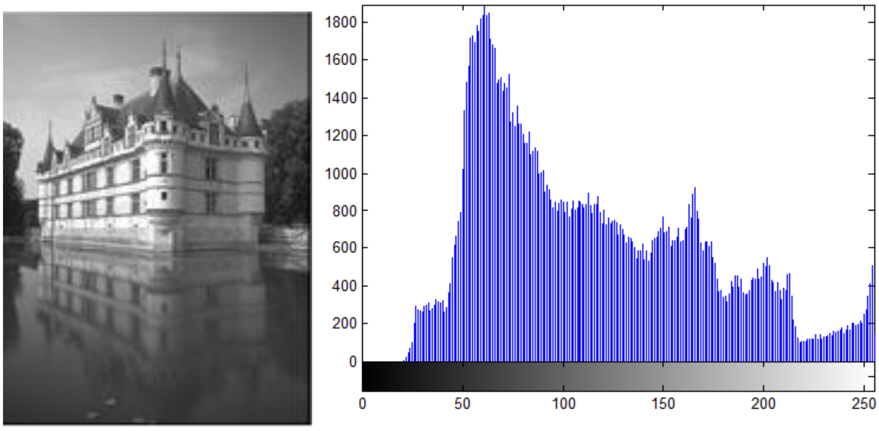
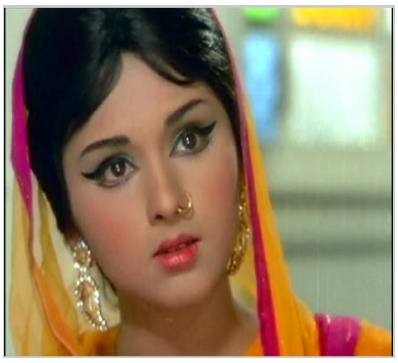
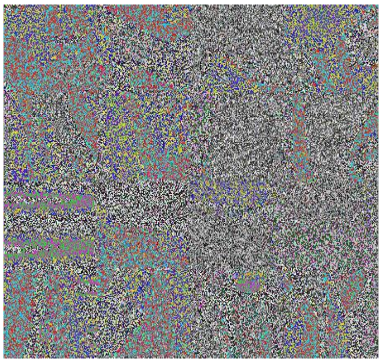


Image size	481×321
Entropy of Original Image	7.56
Entropy of Encrypted image	7.98
Encryption Quality	425.6133

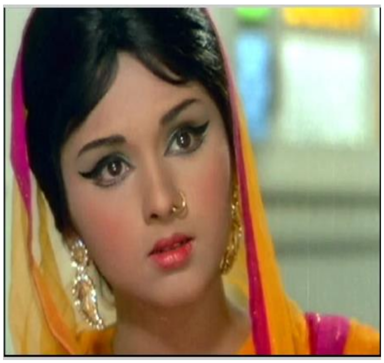
5.3 EXPERIMENATAL RESULTS ON DIFFERENT COLOR IMAGES



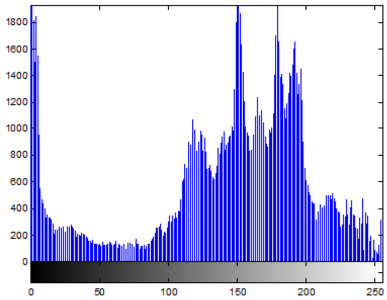
Original image



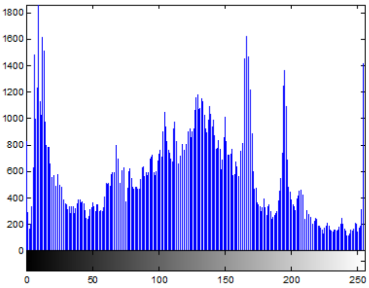
Encrypted image



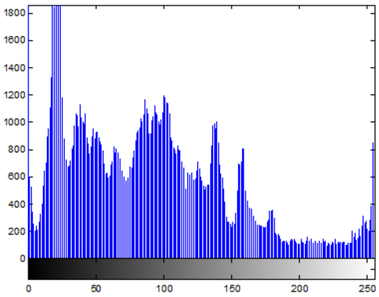
Decrypted image



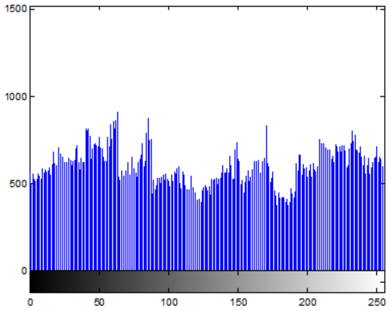
Histogram of red channel in original image



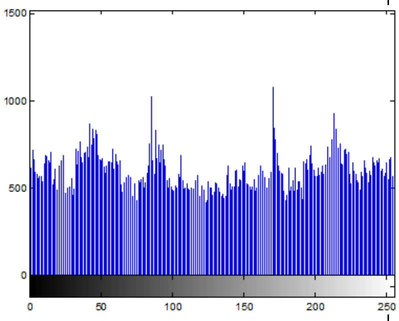
Histogram of green channel in original image



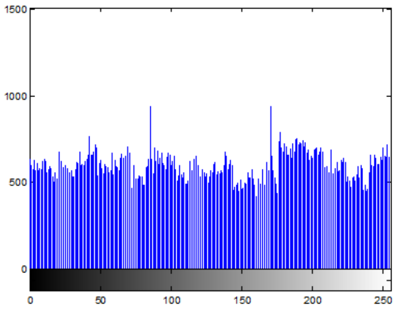
Histogram of blue channel in original image



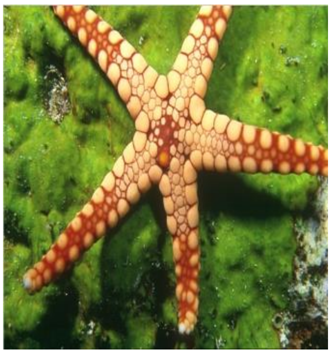
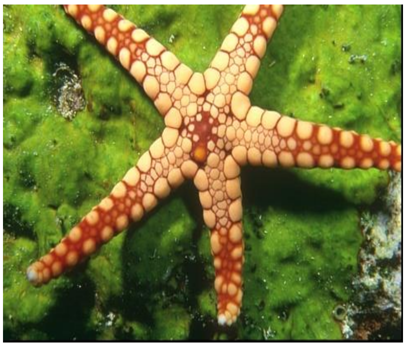
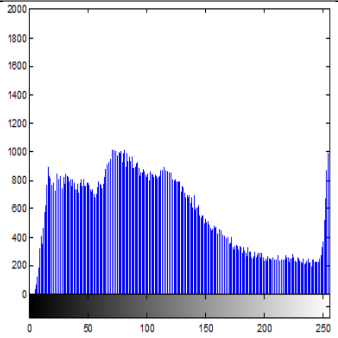
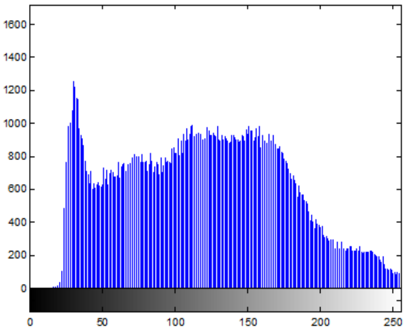
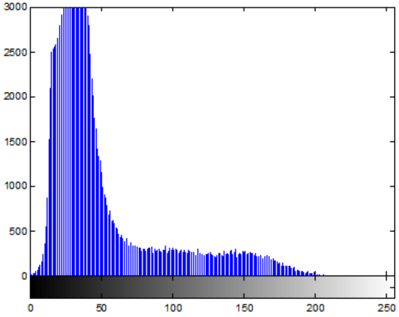
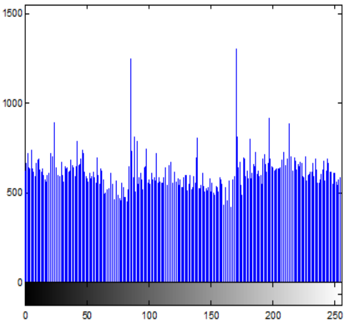
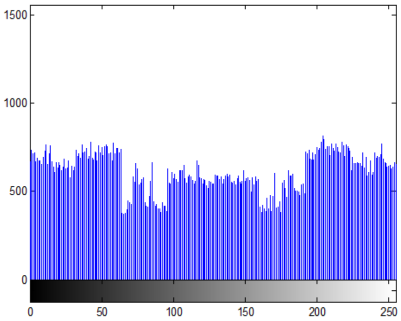
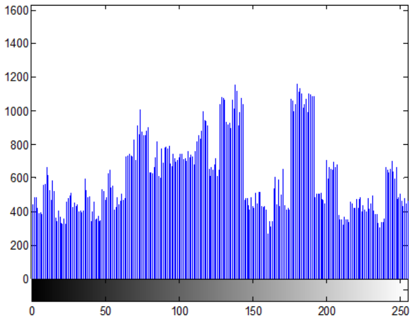
Histogram of red channel in encrypted image

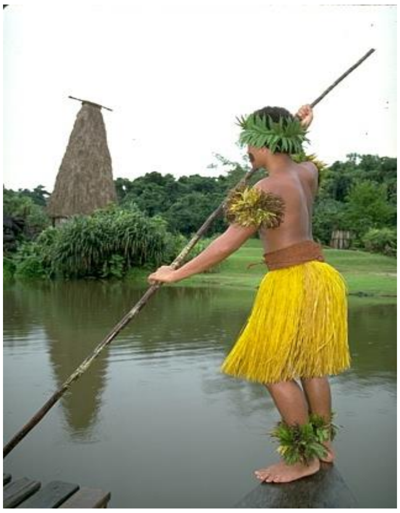
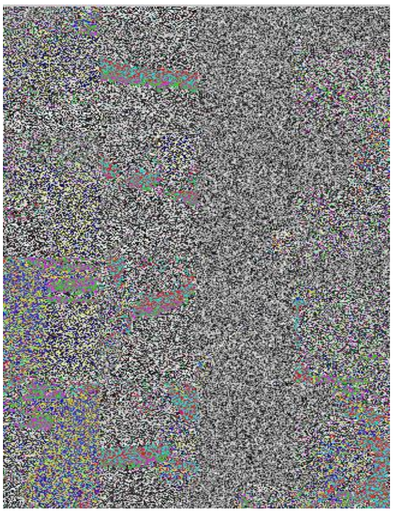
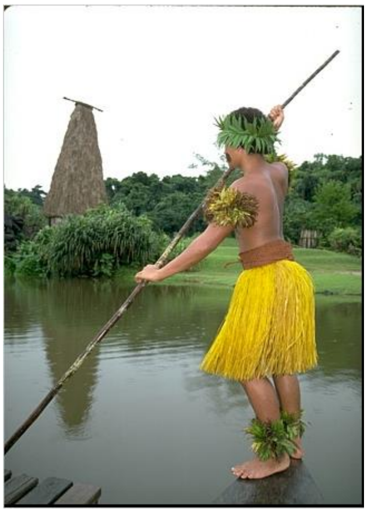
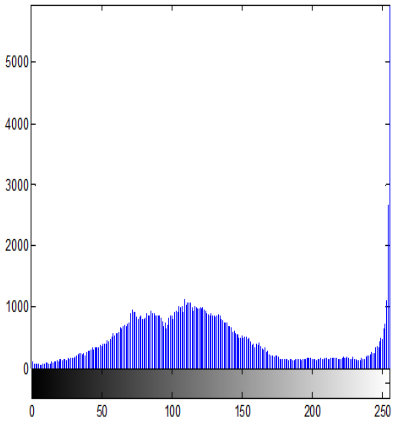
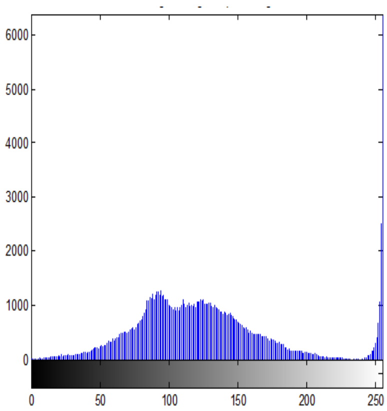
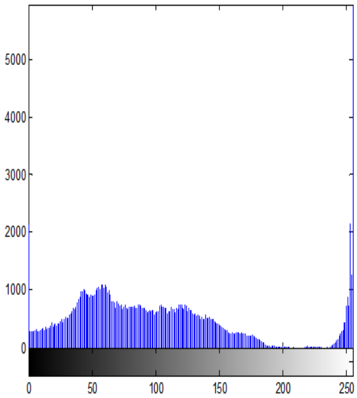
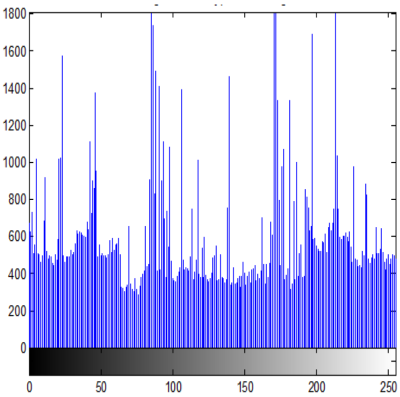
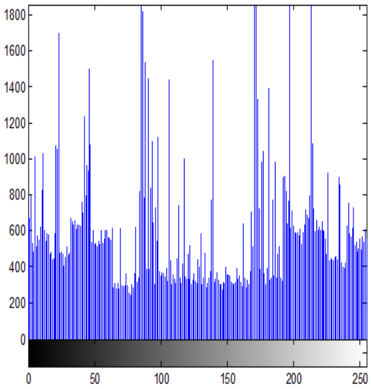
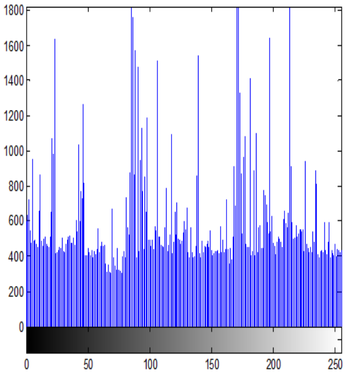


Histogram of green channel in encrypted image

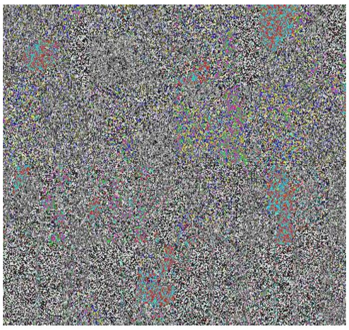


Histogram of blue channel in encrypted image

 Original image	 Encrypted image	 Decrypted image
 Histogram of red channel in original image	 Histogram of green channel in original image	 Histogram of blue channel in original image
 Histogram of red channel in encrypted image	 Histogram of green channel in encrypted image	 Histogram of blue channel in encrypted image

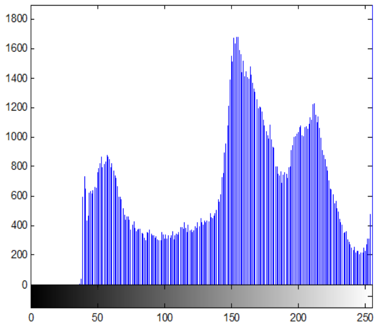
 Original image	 Encrypted image	 Decrypted image
 Histogram of red channel in original image	 Histogram of green channel in original image	 Histogram of blue channel in original image
 Histogram of red channel in encrypted image	 Histogram of green channel in encrypted image	 Histogram of blue channel in encrypted image

Original image

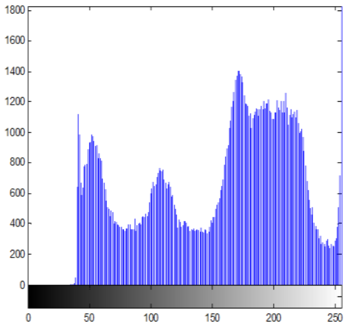


Encrypted image

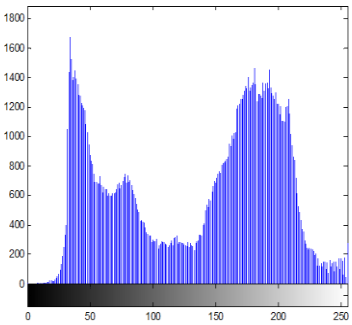
Decrypted image



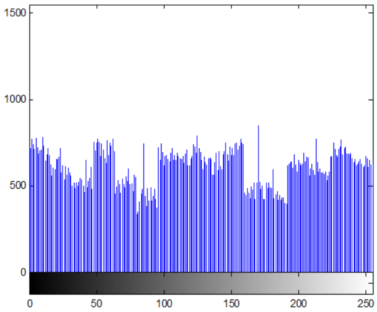
Histogram of red channel in original image



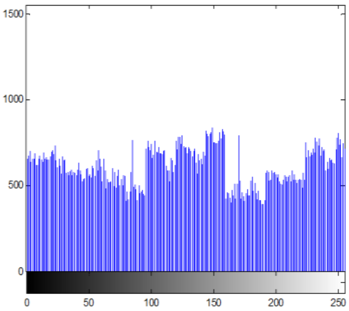
Histogram of green channel in original image



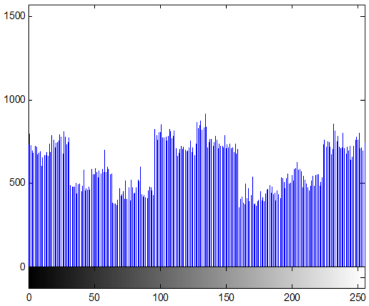
Histogram of blue channel in original image



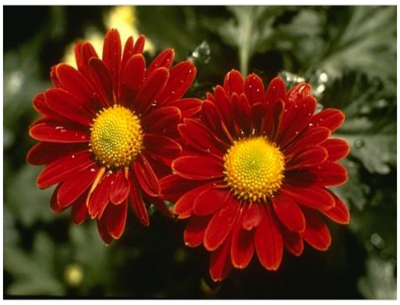
Histogram of red channel in encrypted image



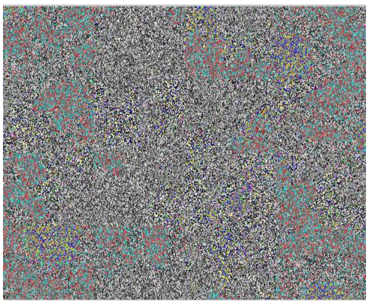
Histogram of green channel in encrypted image



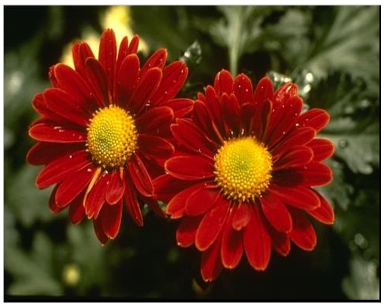
Histogram of blue channel in encrypted image



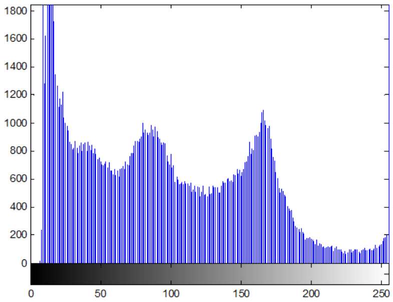
Original image



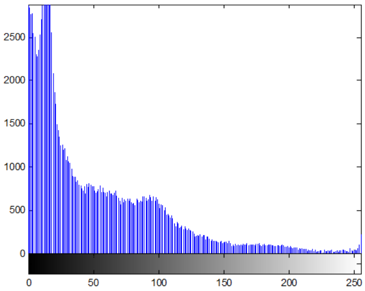
Encrypted image



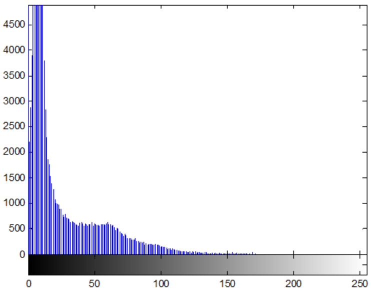
Decrypted image



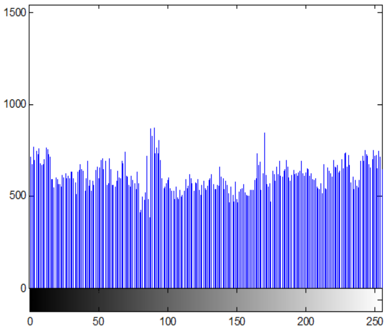
Histogram of red channel in original image



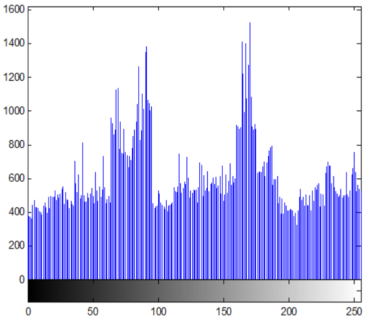
Histogram of green channel in original image



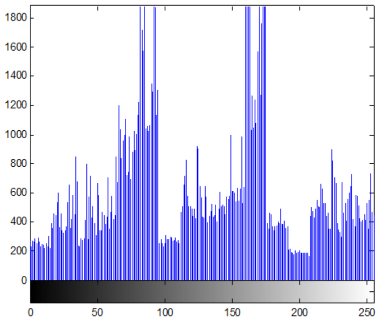
Histogram of blue channel in original image



Histogram of red channel in encrypted image



Histogram of green channel in encrypted image



Histogram of blue channel in encrypted image

CHAPTER-6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

This thesis deals with an introduction to image cryptography schemes. In this work, an image security method is proposed and applied to several images. The results thus obtained and statistical analysis confirmed a higher level of security of images which ensures that eavesdrop cannot cryptanalysis the cipher image. Here, the security relies on a secret key along with the image encryption technique. Chaos is known for randomness, so it is highly secured. Confusion is increased by shuffling pixel form one position to a new position and diffusion is increased through byte sequence generated through Henon chaotic system. So, both the processes of increasing confusion and diffusion resulted in increasing the security of cryptosystem. Stream cipher is achieved by performing XOR operation between image and byte stream of Henon chaotic system which is equivalent to one time pad.

In this thesis, Image encryption is done on gray images as well as on color images in a well suited environment. Experimental results of the proposed image encryption algorithm are illustrated to appreciate the efficiency of proposed algorithm. Statistical analysis like histogram analysis, information entropy analysis, key sensitivity test, correlation analysis, mean value analysis and image encryption quality analysis gives a judgemental result of encryption cryptosystem. Proposed algorithm when run on several images indicates that this chaotic system is applicable for all kind of images.

6.2 FUTURE WORK

This Encryption technique can improve in various aspects such as increasing efficiency, computational complexity and security.

- Future research can be conducted to exploit the proposed pseudo random number generator in security systems and application to increase randomness and provide high level of security.
- Since prime numbers have a various application so this technique can be used as a Prime number generator.
- In this thesis, proposed work is based on symmetric key cryptography. This work can be extended further for asymmetric key cryptography.
- Henon chaotic system is not the only chaotic system which is dynamic. Other chaotic systems are also available which could be used in cryptography.

REFERENCES

[1] Liu Chunli, Liu DongHui, “Computer Network Security Issues and Countermeasures”, *IEEE Symposium on Robotics and Applications (ISRA)*, 2012.

[2] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", *2nd Edition. New York: John Wiley &Sons*, 1996.

[3] Susanne Boll, “MultiTube–Where Multimedia and Web 2.0 Could Meet”,*IEEE Computer Society*, 2007.

[4] Lian S., DimitrisKanellopoulos, G. R., “Recent Advances in Multimedia Information System Security”, *Informatica 33 (2009)*, 2009.

[5] Whitfield Diffie, Martin E. Hellman,“New Directions In Cryptography”,*IEEE Transactions On Information Theory*, Vol. It-22, No. 6, November 1976.

[6] G. Chen, Y. Mao, C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”,*Chaos Solitons Fractals 21 (2004) 749-761*, 2004.

[7] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, “A fast chaotic encryptions scheme based on piece wise nonlinear chaotic maps,” *Physics Letters, A, 366 (2007) 391–396, 2007.*

[8] HassenRedwan and Ki-Hyung Kim, "Survey of Security Requirements, Attacks andNetwork Integration in Wireless Mesh Networks”, *Japan-China Joint Workshop on Frontier of Computer Science and Technology*, 2008.

[9] G. Jakimoski, L. Kocarev, “Block encryption ciphers based on chaotic maps”,*IEEE Transaction on Circuits System-I.*, 48 (2002) 163-169.

[10] Menezes A., P.V. Oorschot, S. Vanstone, Handbook of Applied Cryptography",*FL: CRC Press, Boca Raton*, 1997.

[11] Diffie w. Bell-Northern Res., Mountain View, CA, USA,"The first ten years of public-key cryptography", *Proceedings of the IEEE* (Volume: 76, Issue: 5).

[12]Songsheng Tang Fuqiang Liu, "A one-time pad encryption algorithm based on one-way hash and conventional block cipher", Consumer Electronics, Communications and Networks (CECNet), 2012.

[13] Ohta T., Chikaraishi T., “Network security model”, Networks, International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', *Proceedings of IEEE Singapore International Conference on* (Volume: 2)”, 1993.

[14] http://www.ieeeghn.org/wiki/index.php/Cryptography#Classical_cryptography

[15]Lamba, C.S. “Design and Analysis of Stream Cipher for Network Security”,*Communication Software and Networks*, 2010. ICCSN '10.

[16] G. Jakimoski and L. Kocarev., “Analysis of recently proposed chaos-based encryption algorithm”,*Physics Letters, A*,2001.

[17] A.T.Parker and K.M.Short, “Reconstructing the keystream from a chaotic encryption scheme”,*IEEE transaction on circuit and systems-I*,485(5),2001

[18]Matthews R., “On the derivation of a chaotic encryption algorithm,” *Cryptologia 1989;8(1):29–41*, 1989.

[19] Wikipedia. Chaos theory. http://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=264934743.

[20] Kocarev L., "Chaos-based cryptography: a brief overview", *Circuits and Systems Magazine, IEEE*, 2001. 1(3): p. 6.

[21] MaqablehM., A.B. Samsudin, M.A. Alia, "New Hash Function Based on Chaos Theory",*(CHA-1). IJCSNS International Journal of Computer Science and Network Security 2008*. 8(2): p. 20-26, 2008.

[22] Tao Y., W. Chai Wah, L.O. Chua, "Cryptography based on chaotic systems",*IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1997. 44(5): p. 469-472.

[23] G. Jakimoski, L. Kocarev., “Analysis of recently proposed chaos-based encryption algorithm”,*Physics Letters*,A,2001.

[24] A.T.Parker and K.M.Short, “Reconstructing the keystream from a chaotic encryption scheme”,*IEEE transaction on circuit and systems*-I,485(5),2001.

[25] Bertuglia C.S. and F. Vaio, "Nonlinearity, Chaos & Complexity The Dynamics of Natural and Social Systems", First ed. 2005, *United States: Oxford University Press Inc.*

[26] Alligood K.T., T.D. Sauer, J.A. Yorke, "Chaos an Introduction to Dynamical Systems", First ed. 1996, *New York: Springer-Verlag*.

[27] Zeng X., R.A. Pielke, R.Eykholt, "Chaos theory and its application to the Atmosphere", *Bulletin of the American Meteorological Society*, 1993. 74(4): p. 631-639.

[28] Parker T.S. and L.O. Chua, "Practical Numerical Algorithms for Chaotic Systems", First ed. 1989,*New York Berlin Heidelberg: Springer-Verlag New York Inc*.

[29] http://www.imho.com/grae/chaos/chaos.html.

[30] Kocarev L., "Chaos-based cryptography: a brief overview". Circuits and Systems Magazine", *IEEE*, 2001. 1(3): p. 6.

[31] Muhammad KhurramKhan, Jiashu Zhang, "Investigationon Pseudorandom Properties of Chaotic Stream Ciphers,” *IEEE*, 2006.

[32] X. Wang, Y.L.Y., H. Yu, "Finding collisions in the full SHA1", *Eurocrypt 2005*, 2005.

[33] Kocarev L. and G. Jakimoski, "Pseudorandom bits generated by chaotic maps", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2003. 50(1): p. 123-126.

[34] Dabal P., and R.Pelka. "A chaos-based pseudo-random bit generator implemented in FPGA device", Design and Diagnostics of Electronic Circuits &Systems (DDECS), *IEEE 14th International Symposium*, 2011.

[35] Shujuna L., M. Xuanqinb, and C. Yuanlong. "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", in Progress in Cryptology - INDOCRYPT 2001, LNCS. 2001. *Berlin: Springer-Verlag*.

[36] Stojanovski T. and L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2001. 48(3): p. 281.

[37] Luonan Chen, Kazuyuki Aihara, "Strange Attractors in Chaotic Neural Networks", *IEEE Transactions on Circuits And Systems—I: Fundamental Theory And Applications*, VOL. 47, NO. 10, OCTOBER 2000

[38] E. Petrisor, "Entry and exist sets in the dynamics of area preserving Henon map",*Chaos, Solitions and Fractals*, pp.651-658, Oct 2003.

[39] L. Guo, Z. Shi-ping, X. De-ming, L. Jian-wen, "An Intermittent Linear Feedback Method for controlling Henon-like Attractor",*Journal of Applied Science*, pp. 288-290, Dec.2001.

[40] D.Erdmann and S. Murphy, "HENON STREAM CIPHER",*Electronics Letters*, 23rdapril 1992 vol. 28 no.9

[41] AndrewRukhin, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *in NIST Special Publication* 800–22 Revision 1a. 2010.

[42] BarisCoskun, N.M., "Confusion/Diffusion capabilities of some robust hash functions", 40th annual conference, *IEEE conference proceedings: information sciences and systems*, March 2006.

[43] Shannon C., "Communication Theory of Secrecy Systems", *Bell Systems Technical Journal*, 1949.

[44] Miles E. Smldand Dennis K. Branstad, "The Data Encryption Standard: Past and Future",*Proceedings of the IEEE*, VOL. 76, NO. 5, MAY 1988.

[45] Poincaré J.H., Sur le problème des trois corps et les équations de la dynamique. Divergence des séries de M. LindstedtActaMathematica, 1890. 13: p. 1–270,

[46] Alligood K.T., T.D. Sauer, and J.A. Yorke, "Chaos an Introduction to Dynamical Systems", First ed. 1996, *New York: Springer-Verlag*.

[47] Solari H.G., M.A. Natiello, and G.B. Mindlin, "Nonlinear Dynamics-A Two-way Trip from Physics to Math", 1 ed. 1996: *Institute of Physics Publishing*.

[48] Lorenz E.N., "Deterministic NonperiodicFlow", *Journal of Atmospheric Sciences*, 1963. 20.

[49] Zeng X., R.A. Pielke, and R. Eykholt, "Chaos theory and its application to the Atmosphere", *Bulletin of the American Meteorological Society*, 1993. 74(4): p. 631-639.

[50] Wolfram S. "Cryptography with cellular automata", in Advances in Cryptology - Crypto’85, Lecture Notes in Computer Science. *Spinger-Verlag, Berlin*, 1985.

[51] Matthews R.A.J., "On the derivation of a chaotic encryption algorithm",*Cryptologia*, 13(1): p. 29–42, 1989.

[52] G. Chen, Y. Mao, K. Charles, “A symmetric image encryption scheme based on 3D chaotic cat maps”,*Chaos, Solutions & Fractals*, pp. 749-761, Dec. 2004.

[53] K. Wang, W. Pei, “On the security of 3D Cat map based symmetric image encryption scheme”,*Physics Letters A.*, pp. 432-439, May. 2005.

[54] S.-M. Chang, M.-C.Li, W.-W.Lin, “Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications”,*Nonlinear Analysis*, pp. 869–880, Jan. 2009.

[55] H. Lian-xi, L. Chuan-mu, L. Ming-xi, “Combined image encryption algorithm based on diffusion mapped disorder and hyperchaotic systems”,*Computer Applications*, pp. 1892-1895, Aug. 2007.

[56]Chen Wei-bin, Zhang Xin, “Image Encryption Algorithm Based on Henon Chaotic System”, *IEEE*, 978-1-4244-3986-7/09, 2009.

[57]Mintu Philip, Asha Das, ”Survey: Image Encryption using Chaotic Cryptography Schemes”, IJCA Special Issue on “Computational Science- New Dimensions & Perspectives” Nccse, 2011.

[58] C.K. Huang, H.H. Nien, “Multi chaotic systems based pixel shuffle for image encryption”,*Optics communications*, 282(2009) 2123-2127, 2009.

[59] WadiaFaid Hassan Al-Shameri, “Dynamical Properties of the Hénon Mapping”,*Int. Journal of Math.Analysis*, Vol. 6, no. 49, 2419 – 2430, 2012.

[60] FethiBelkhouche, UvaisQidwai, Ibrahim Gokcen, Dale Joachim, “Binary Image Transformation using Two-Dimensional Chaotic Maps”, *Proceedings of 17th International Conference on Pattern Recognition, IEEE*.

[61] JianshengGuo, ZhenzhenLv, Lei Zhang, “Breaking a chaotic Encryption Based on Henon Map”,*Third International Symposium on Information Processing, IEEE*, 2010.

[62] Harn L., Mehta M. , Wen-Jung Hsin, "Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)”,*Communications Letters, IEEE* (Volume:8 , Issue: 3) 2004.