

Multimedia Security Using Chaotic Map

A Dissertation submitted in partial fulfillment of the requirement for the
award of the degree of

MASTER OF TECHNOLOGY
(INFORMATION SYSTEMS)

Submitted By:

BRIJESH KUMAR PATEL

(Roll No. – 2K12/ISY/07)

Under the esteemed guidance of

Dr. N. S. RAGHAVA

Associate Professor



DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI-110042
SESSION: 2012-2014

CERTIFICATE

This is to certify that the thesis entitled “**Multimedia Security using Chaotic Map**” submitted by **Brijesh Kumar Patel (2K12/ISY/07)** to the 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.

Dr. N. S. Raghava
Project Guide
Associate Professor
Department of Information Technology
Delhi Technological University
Shahbad Daultpur, Bawana road, Delhi 110042

Date:

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 **Dr. 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 express my gratitude towards my **parents & staff** of Delhi Technological University for their kind co-operation and encouragement which helped me in the 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.

Brijesh Kumar Patel
Roll No.: 2K12/ISY/07
M. Tech (Information Systems)
Department of Information Technology
Delhi Technological University

ABSTRACT

The meaningful exchange of information between two or more entities is known as communication. Multimedia documents such as text, audio, video are the main forms of information in communication, which required transferring information from one place to another. In this era of e-communication, the first concern is about the security of the content which is shared during communication. While the information is on the net, it is impossible to keep track of the path of the information or the copying of information is going through. Security is a continuous process by which data can be secured from several active and passive attacks. There are a number of security techniques by which we can ensure the integrity, confidentiality and authentication of the information. Cryptography is one of the primitive methods to secure information from eavesdroppers, hackers or intruders. The encryption technique protects the confidentiality of a message or information. Since, there are limited encryption algorithms, but vast 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 confusion and 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 is created by shuffling the image pixels in a specific order for several iterations. To reduce the volume of multimedia information during transmission Discrete Fourier Transform (DCT) is applied. 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 the digital transmission world. The proposed method proved to produce good results for gray as well as color images.

CONTENTS

CERTIFICATE.....	i
ACKNOWLEDGEMENT.....	ii
ABSTRACT.....	iii
CHAPTER 1	
INTRODUCTION	1
1.1 SECURITY.....	1
1.2 NETWORK SECURITY.....	1
1.3 INFORMATION SECURITY.....	2
1.4 BASIC PRINCIPALS OF INFORMATION SECURITY.....	3
1.4.1 Confidentiality	
1.4.2 Authentication	
1.4.3 Integration	
1.4.4 Non-Repudiation	
1.4.5 Availability	
1.4.6 Access Control	
1.5 ATTACKS IN INFO AND NETWORK SECURITY.....	7
1.5.1 Active Attacks	
1.5.2 Passive Attacks	
1.5.3 Distributed Attack	
1.5.4 Insider Attack	
1.5.5 Close-in Attack	
1.5.6 Phishing Attacks	
1.5.7 Hijack Attack	
1.5.8 Spoof Attack	
1.5.9 Buffer Overflow	
1.5.10 Exploit Attack	
1.5.11 Password Attack	

1.6	NETWORK SECURITY MODEL.....	10
1.7	MULTIMEDIA.....	12
1.8	CRYPTOGRAPHY.....	13
	1.8.1 Typical cryptography	
	1.8.2 Categories of cryptography	
1.9	SYMMETRIC KEY CRYPTOGRAPHY.....	16
1.10	PUBLIC-KEY CRYPTOGRAPHY.....	19
1.11	CRYPTANALYSIS.....	21
1.12	SIGNIFICANT TERMS.....	22
	1.12.1. Cryptosystem	
	1.12.2. One time pad	
	1.12.3. Eavesdropping	

CHAPTER 2

CHOAS AND CRYPTOGRAPHY.....	24
2.1 INTRODUCTION.....	24
2.2 CHOAS THEORY.....	25
2.2.1 History of chaos theory	
2.3 CHAOS-BASED CRYPTOGRAPHY.....	27
2.4 CHOATIC MAPS.....	29
2.4.1 One-Dimension chaotic maps	
2.4.2 Two-Dimension chaotic maps	
2.5 ATTRACTOR.....	33

CHAPTER 3

LOGISTIC MAP AND DISCRETE COSINE TRANSFORM.....	34
3.1 LOGISTIC MAP.....	34
3.2 RANDOM NUMBER GENERATOR.....	35
3.1.1 Random number generator	
3.1.2 Pseudorandom number generator	
3.3 CONFUSION AND DEFUSION.....	36

3.4	IMAGE COMPRESSION AND DISCRETE COSINE TRANSFORM.....	37
3.4.1	IMAGE COMPRESSION	
3.4.1.1	Need for image compression	
3.4.1.2	Principle behind compression	
3.4.2	TYPES OF IMAGE COMPRESSION	
3.4.3	DISCRETE COSINE TRANSFORM (DCT)	
CHAPTER 4		
	RELATED WORK.....	42
CHAPTER 5		
	PROPOSED ALGORITHM FOR ENCRYPTION.....	44
5.1	MOTIVATION.....	44
5.2	PROPOSED METHOD.....	44
5.3	PROPOSED ALGORITHM.....	45
CHAPTER 6		
	EXPERIMENTAL RESULTS AND DISCUSSION.....	49
6.1	STATISTICAL ANALYSIS.....	52
6.1.1	Histogram analysis	
6.1.2	Information entropy analysis	
6.1.3	Key sensitivity test	
6.1.4	Mean value analysis	
6.1.5	Encryption key randomness analysis	
6.2	EXPERIMENTAL RESULTS ON DIFFERENT IMAGES.....	58
6.3	COMPARISONS OF VARIOUS QUALITY PRAMETERS FOR ENCRYPTION FOR DIFFERENT CHAOTIC MAPS.....	59
6.3.1	Variation in entropy with iteration for different images.	
6.3.2	Mean Square Error Analysis for different chaotic maps	
6.3.3	Peak signal to noise ratio comparison of different Chaotic maps.	

- 6.3.4 Unified Average Change in Intensity
- 6.3.5 Number of Pixel Change Rate
- 6.3.6 Time complexity analysis for different chaotic map

CHAPTER 7

CONCLUSION AND FUTURE WORK73

- 7.1 CONCLUSION.....73
- 7.2 FUTURE WORK.....74

REFERENCES75

LIST OF FIGURES

Fig. No.	Title	Pg. No.
1.1	Loss of confidentiality	3
1.2	Absence of Authentication.	4
1.3	Loss of integrity	5
1.4	Establishing Non-repudiation.	6
1.5	Attack on Availability	6
1.6	Network security model	11
1.7	General architecture of multimedia information system	13
1.8	Block diagram of cryptography	15
1.9	Symmetric key encryption process.	16
1.10	Stream Cipher	17
1.11	Block Cipher	18
1.12	Simplified Data Encryption Standard.	19
1.13	Asymmetric key cryptography process.	20
1.14	Diffie-Hellman Process	21
1.15	One-time pad or Verman cipher	23
2.1	Comparison between chaotic systems and cryptographic algorithms	28
2.2	Attractor in dynamic space	33
3.1	Bifurcation diagram for Logistic map	34
3.2	Variation of Logistic map with iterations	35
3.3	Image compression model	38
3.4	Input images and DCT	40
3.5	SNR v.s. No. of coefficients	41
5.1	Input Image	45
5.2	Image after first iteration	45

5.3	Flow chart of proposed algorithm	46
5.4	Shuffled image after fifth iteration	47
6.1	Bifurcation diagram of logistic map	49
6.2	Encryption by Chaotic Logistic map	50
6.3	Decryption by chaotic Logistic map	51
6.4	Histogram analysis for encryption process	52
6.5	Histogram analysis for decryption process	53
6.6	Key sensitivity analysis	55
6.7	Mean value analysis of original image and encrypted image	56
6.8	Encryption key randomness analysis	57
6.9	Variation in entropy with iteration of Henon map	62
6.10	Variation in entropy with iteration of Tent map	62
6.11	Variation in entropy with iteration for Logistic map	63
6.12	Entropy comparison for different chaotic map	63
6.13	MSE for Logistic map	64
6.14	MSE for Tent map	65
6.15	MSE for Henon map	65
6.16	MSE comparisons for different chaotic maps	65
6.17	PSNR for Logistic map	66
6.18	PSNR for Tent map	66
6.19	PSNR for Henon map	67
6.20	Comparisons of PSNR for different chaotic maps	67
6.21	UACI value for Henon map	68
6.22	UACI value for Logistic map	68
6.23	UACI value for Tent map	69
6.24	UACI value comparison of different chaotic maps	69
6.25	NPCR value for Logistic map	70
6.26	NPCR values for Tent map	70
6.27	NPCR values for Henon map	71
6.28	NPCR value comparisons for different chaotic maps	71
6.29	Time complexity analysis of different chaotic map	72

LIST OF TABLES

Table no.	Topic	Page no.
Table 1	Graphical representation of different Chaotic maps	30
Table 2	Entropy analysis	54
Table 3	Experimental results on different images	58
Table 4	Test images used to perform various encryption qualities parameter test	61
Table 5	MSE for different chaotic maps	64
Table 6	PSNR value comparison for different chaotic maps	66
Table 7	UACI value comparison for different chaotic maps	68
Table 8	NPCR values for different chaotic maps	70
Table 9	Time Complexity for different chaotic map	71

CHAPTER - 1

INTRODUCTION

1.1 SECURITY

Security is the degree of resistance to, or protection from, harm. It can be applied to any valuable and vulnerable, such as a person, nation, dwelling, community, or organization. The process of protecting hardware and software resources from intruders, eavesdroppers, hackers or attackers is known as computer security. A hacker is an individual who finds out loop wholes in a computers system or computer network and seeks an unauthorized 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 unauthorized access. In computer, security is broadly divided into two categories

- Network Security
- Information Security

1.2 NETWORK SECURITY

Network Security [1] [2] is the policies and provisions implemented by a network administrator to avert unauthorized access to computer resources and computer network. All the users can generate their own or are assigned user name and password that permit them to get info and other resources within their domain of authority. Network security includes public and private, networks, which are used in communications and transactions among individuals, businesses and government activities. It is used in various fields like private enterprises, educational institutions and government organizations. As does network security title explains: It provides safety to the network infrastructure parallel overseeing operations being done.

1.3 INFORMATION SECURITY

It is also known as InfoSec. Information security is the practice of shielding data from disruption, obliteration, illicit access, perusal. InfoSec is a general term that can be used nonetheless of the form the data may take physical, electronic, etc..

Two significant facets of data safety are:

1. IT SECURITY

It is also known as computer safety. IT Security is a data safety mechanism implemented in technology most frequently in certain forms of the computer system. It is vital to make a note that a computer system does not really limited to a home desktop. Any device with a processor and some memory can be designated as the computer. These devices cover a wide range of appliances such as non-networked stand-alone devices as like calculators, to networked mobile calculating maneuvers such as tablet computers and Smartphones.

2. INFORMATION ASSURANCE

It is the process of making confirmation that gen is not lost, when critical matters happen. These problems comprise, but are not restricted to: disasters which may be natural or human, malfunctioning of computer or server, physical burglary, or other instance, where the information has the possibility of being vanished. Meanwhile utmost of the data is kept on computers in our modern epoch; info security is characteristically dealt with by IT security experts.

1.4 BASICS PRINCIPLES OF INFORMATION SECURITY

- **Confidentiality**
- **Authentication**
- **Integrity**
- **Nonrepudiation**

- **Availability**
- **Access Control**

1.4.1 CONFIDENTIALITY

Confidentiality is a kind of promise or set of rules that restricts access and puts restrictions on certain kind of information. When communication takes place over an insecure network, only the projected recipient should be able to access the contents of the message. The information should not be accessible to any unauthorized recipient. In figure 1.1, user A sends data to intended user B. Confidentiality [8] is compromised when unauthorized user C reads the message.

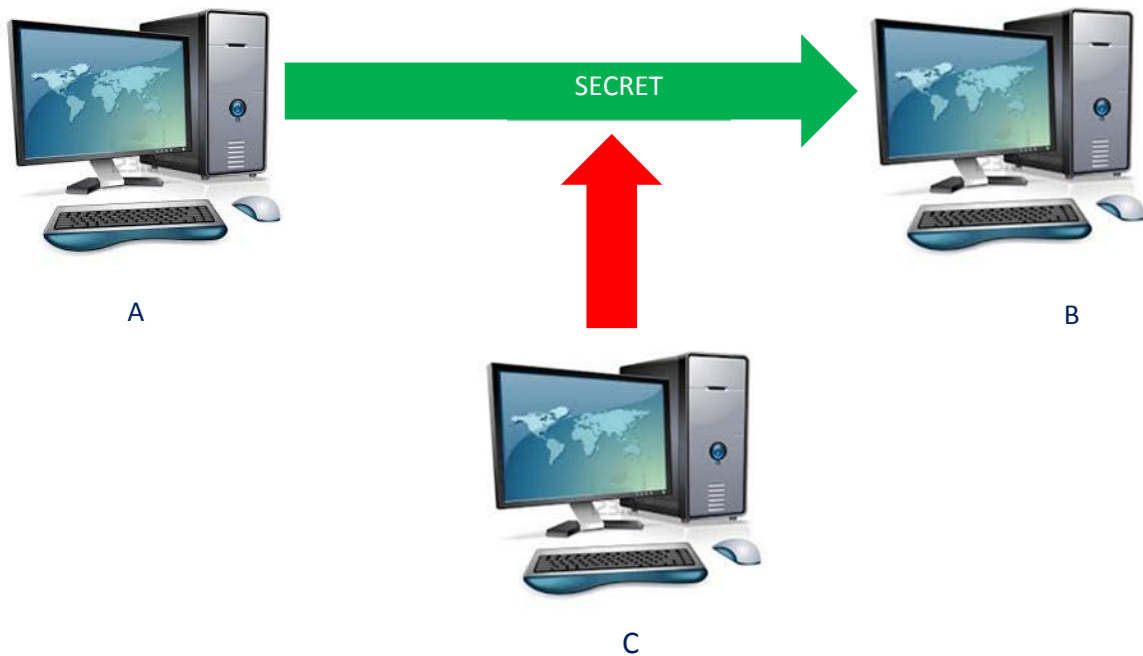


Figure 1.1: Loss of confidentiality

1.4.2 AUTHENTICATION

In data safety, it is obligatory to make confirm that the data which may be physical or electronic are unaffected. It is also essential for legitimacy to certify that both participating entities are who they entitle to be. One of the techniques applied for

information authentication is by "digital signatures", which give confirmation that the information is original and it was sent by the person having the appropriate validation key. Authentication mechanisms help to establish proof of identities. This process of authentication confirms that the source of the info is correctly recognized. For example, if a message received by user B says that it is originated from user A but actually the message was sent by user C, this kind of attack is called absence of authentication, as shown in figure 1.2. This type of attack is also called fabrication.

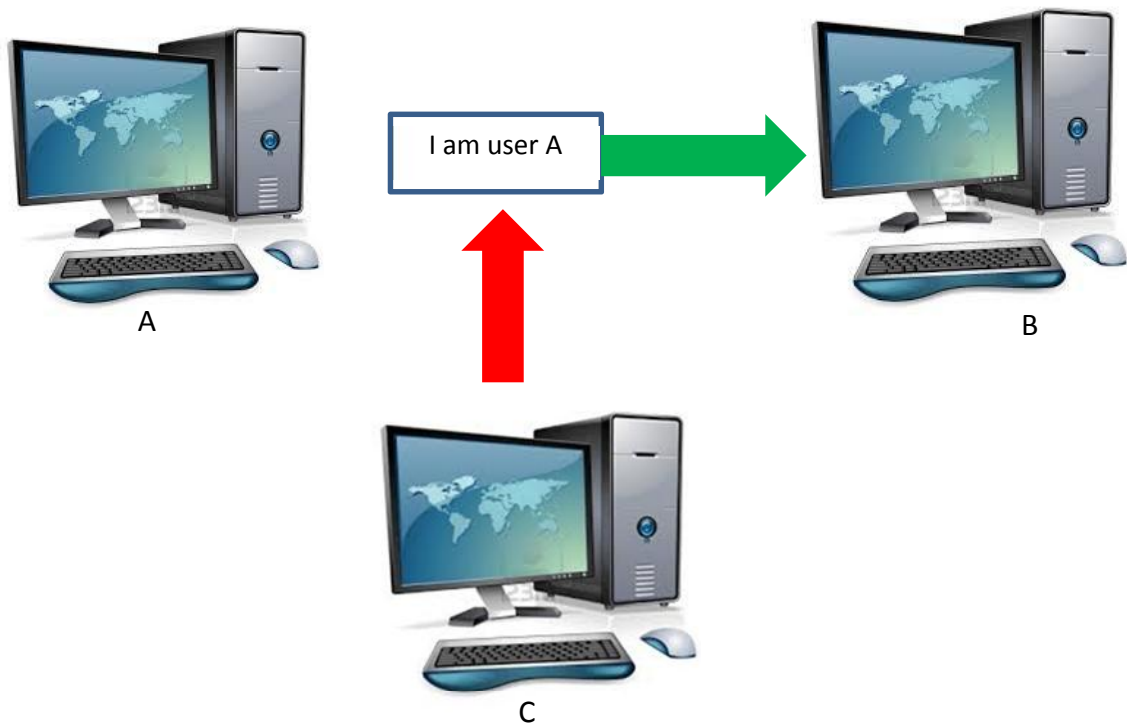


Figure 1.2: Absence of Authentication

1.4.3 INTEGRITY

The process of making confirmation that the data acquired is exactly same as sent by an accredited entity is called integrity. Figure 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 the possibility that the message has been altered resulting in a loss of integrity.

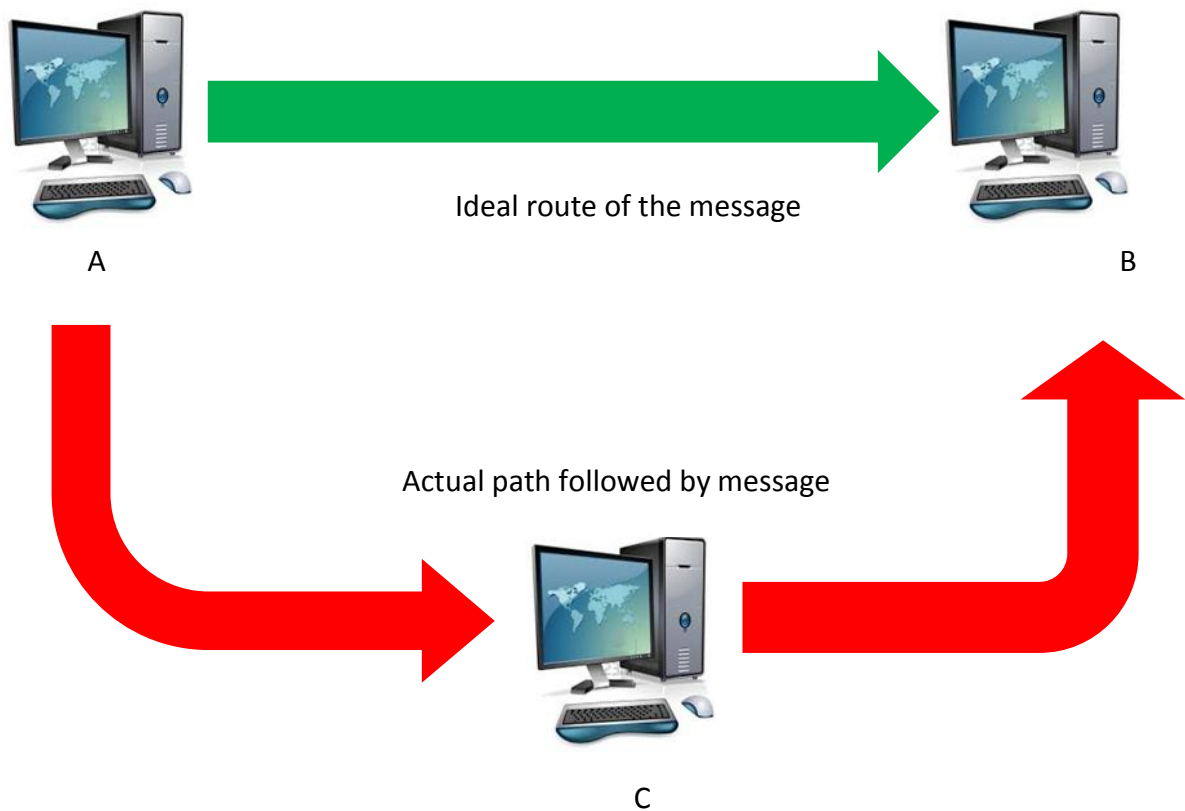


Figure 1.3: Loss of Integrity

1.4.4 NON-REPUDIATION

Nonrepudiation means one entity of the transaction cannot refuse having received a transaction or information and nor can the other communicating person refused having sent an information. Non-repudiation does not allow the sender of a message to deny the claim of not sending that message.

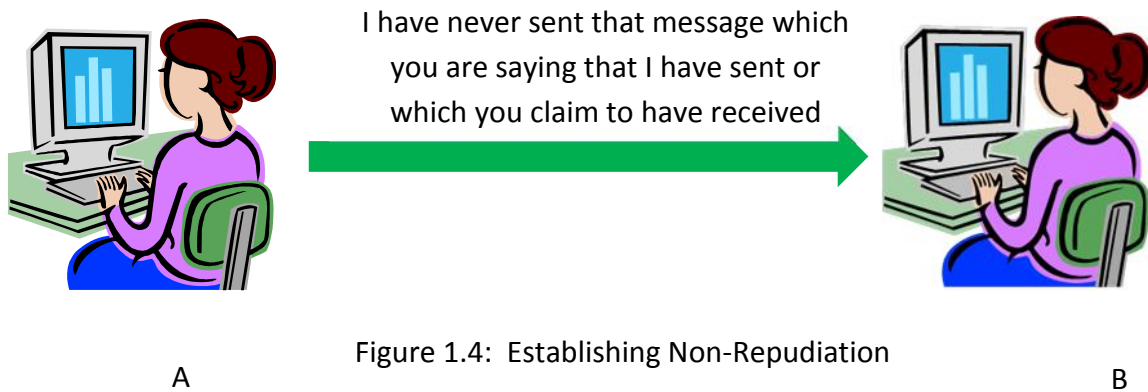


Figure 1.4: Establishing Non-Repudiation

1.4.5 AVILABILITY

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

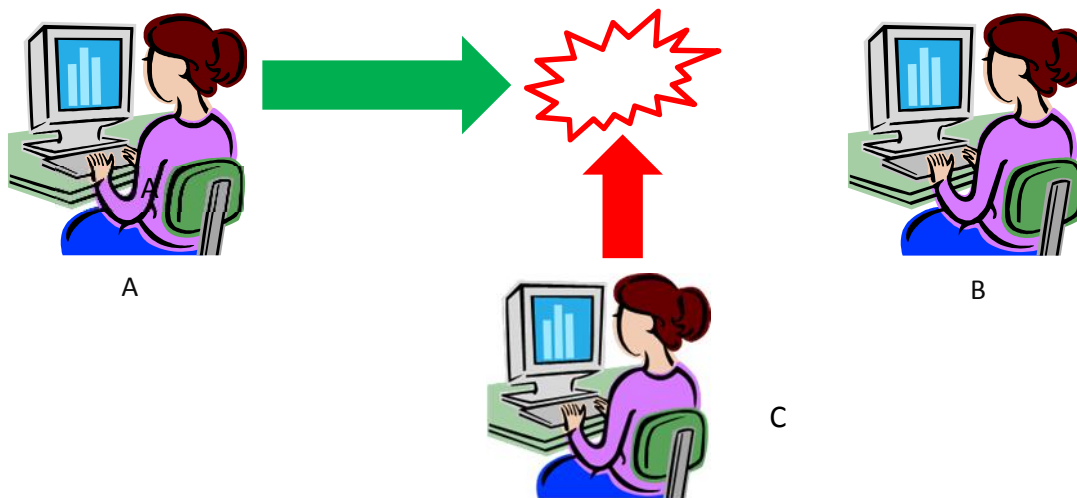


Figure 1.5: Attack on Availability

1.4.6 ACCESS CONTROL

Access control is the branch of gen security and physical security. It is the selective constraint to access information or other resources. The process of accessing may mean entering, using or consuming. This prevents from unauthorized use of a resource.

1.5 ATTACKS IN INFORMATION AND NETWORK SECURITY

Any attempt by an unauthorized user to acquire access to any information and other resources by compromising its security [3] is called a security attack. A system which may be a computer or other electronic devices must be able to diminish the damage and able to convalesce rapidly when they occur. Following classes of attacks exist in information systems, described below in detail.

- Active Attack
- Distributed Attack
- Close-in Attack
- Insider Attack
- Spoof Attack
- Hijack Attack
- Phishing Attacks
- Buffer Overflow
- Password Attack
- Exploit Attack

1.5.1 ACTIVE ATTACK

Active attacks are the actions that attempt to bypass the secured system. Active attack can be performed via stealth, viruses, Trojan horses. Active attacks include some variation of the information sequences or the creation of false stream, to introduce malicious code,

and to modify or steal information. It is difficult to prevent active attacks. A masquerade happens, when one user pretends to be some other user.

1.5.2 PASSIVE ATTACK

The goal in case of a passive attack is to simply get the information that is being transmitted. Attacker monitors the traffic. Passive attacks are difficult to detect as the attacker only sniffs the data without doing any modifications in data. This attack can be prevented by the means of encryption.

1.5.3 DISTRIBUTED ATTACK

This kind of attack requires that the contender introduce enigma, like backdoor program or a Trojan horse, to a “trusted” software or component that will next time distributed to several other firms and group of users. Distributed attacks insert faulty code like a back door in a software or hardware to acquire illicit entry to a system or information later.

1.5.4 INSIDER ATTACK

It comprises individual from the inside of an organization, like a disgruntled employee. To attack any network infrastructure, insider attacks can be malicious or non-malicious. In case of malicious, insider deliberately damage info, eavesdrop or steal it. Insider attacker can use the information in a fraudulent manner or repudiate access to some other legitimate users.

1.5.5 CLOSE-IN ATTACK

This kind of network attack includes somebody endeavoring to get physically close to the systems or data in a network. Close physical proximity has gained thru surreptitious admittance into an open access, network or both.

One of the prevalent methods of close in attack is the social engineering. In case of social engineering attack, the hacker compromises the network resources thru social interaction with a person, an e-mail or a message.

1.5.6 PHISHING ATTACK

In case of this kind of attack, the cracker generates a bogus website that guises just as a widespread website, for example the banking website or FLIPKART E-shopping website. In phishing, hacker sends an e-mail message or text message to the intended group of users and trying to trick the user so that they may click the specified link by the attacker, which leads to the bogus websites. Next time, when the legitimate user tries to log on with their detail info, the hacker archives the user vital information such as username and password and thereafter attempts that gen on the factual website.

1.5.7. HIJACK ATTACK

It is kind of attack, where a hacker have controlled a session among two interacting parties and disrupt the other person from the communication. The first person yet believes that he/she is talking to the genuine party and may send confidential info to the hacker by coincidence. It can also be considered as the man in the middle attack.

1.5.8 SPOOF ATTACK

In the spoof attack, hackers modify the address of incoming packets of a message, which makes the sender or receiver to think that the message is arriving from some different address. Spoof attack is mainly performed to bypass the firewall security of a network and gain access to the private information of an organization.

1.5.9 BUFFER OVERFLOW

In this type of bout, the attacker directs more gen to an application than is anticipated. A buffer overflow attack typically happens, when the attacker gains administrative control of the security system in a shell.

1.5.10 EXPLOIT ATTACK

In this kind of bout, the attacker has knowledge about a safety issue inside a piece of software, an operating system or application and controls that gene by exploiting the weakness.

1.5.11 PASSWORD ATTACK

Password bout is carried out by cracking the passwords stored in a network database. There are mainly three major categories for password attack: first is brute force attack, second dictionary attack and a hybrid bout. A brute-force bout is occurring, when the invader tries each and every probable combination of characters that can be used in the password. A dictionary bout usages a file of word list. The word list file is a list of possible passwords.

1.6 NETWORK SECURITY MODEL

In this model [13], as shown in figure 1.6, the two entities participated in the communication tend to send messages via an information channel. A logical gene network is established between them by defining a route over internet from source to target. In order to protect the information from intruders, the entities involved will perform some sort of security-related transformations on the message to be forwarded using some form of undisclosed information. Such activities may involve the use of a

Trustworthy Third Party to whom some responsibilities such as distribution of secret information or authorization/authentication are entrusted to.

There are four essential jobs involved in developing a security service using this model:

1. A procedure for carrying out the safety connected conversion.
2. Create the furtive information required by that procedure
3. Method for sharing and distribution of confidential gen.
4. A procedure to be applied by two entities that utilizes the safety system and confidential gen to achieve a particular safety service.

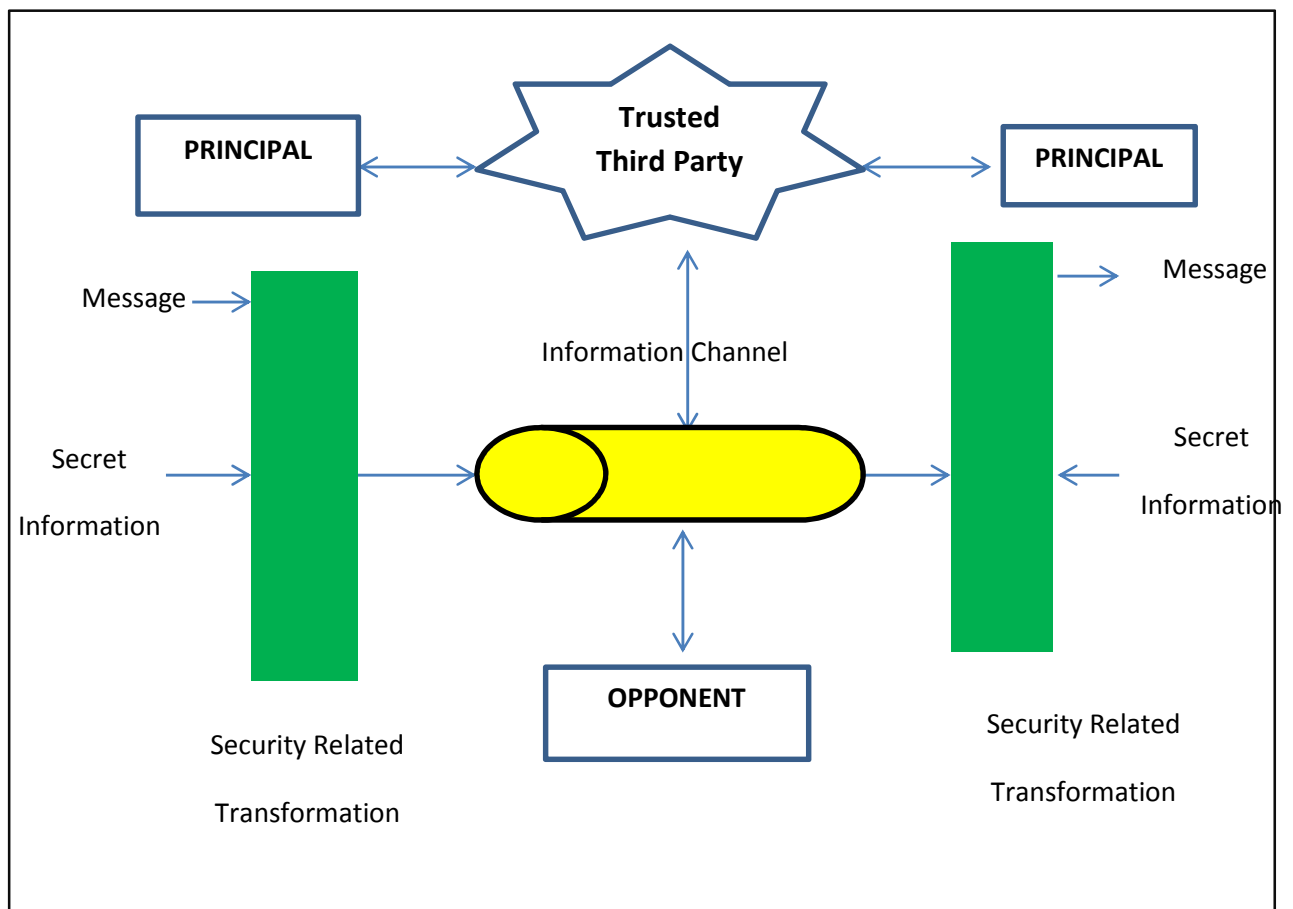


Figure 1.6: Network Security Model

1.7 MULTIMEDIA

The term multimedia [4] was devised by Bob Goldstein on July 1966, at the opening of his "LightWorks at L'Oursin" demonstration in Southampton, Long Island. Multimedia 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 information or content that uses an amalgamation of different document 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 the Internet needs high level of protection from intruders [5].

Now-a-days digital images are used frequently for communication. Telecommunication systems and digital information's development have 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 unauthorized 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 the gen has been compromised or not. Digital signatures are used to confirm the legitimacy and veracity of the message. It verifies the origin of the message and also prevents the sender from later denying that he sent the message. Multimedia finds its application in numerous fields as mentioned below

- Creative Industries
- Commercial Uses
- Entertainment and Fine Arts
- Education
- Business
- Journalism
- Industries

- Scientific research
- Medicine
- Disabilities, etc.

The general architecture of multimedia system is described in the figure 1.7.

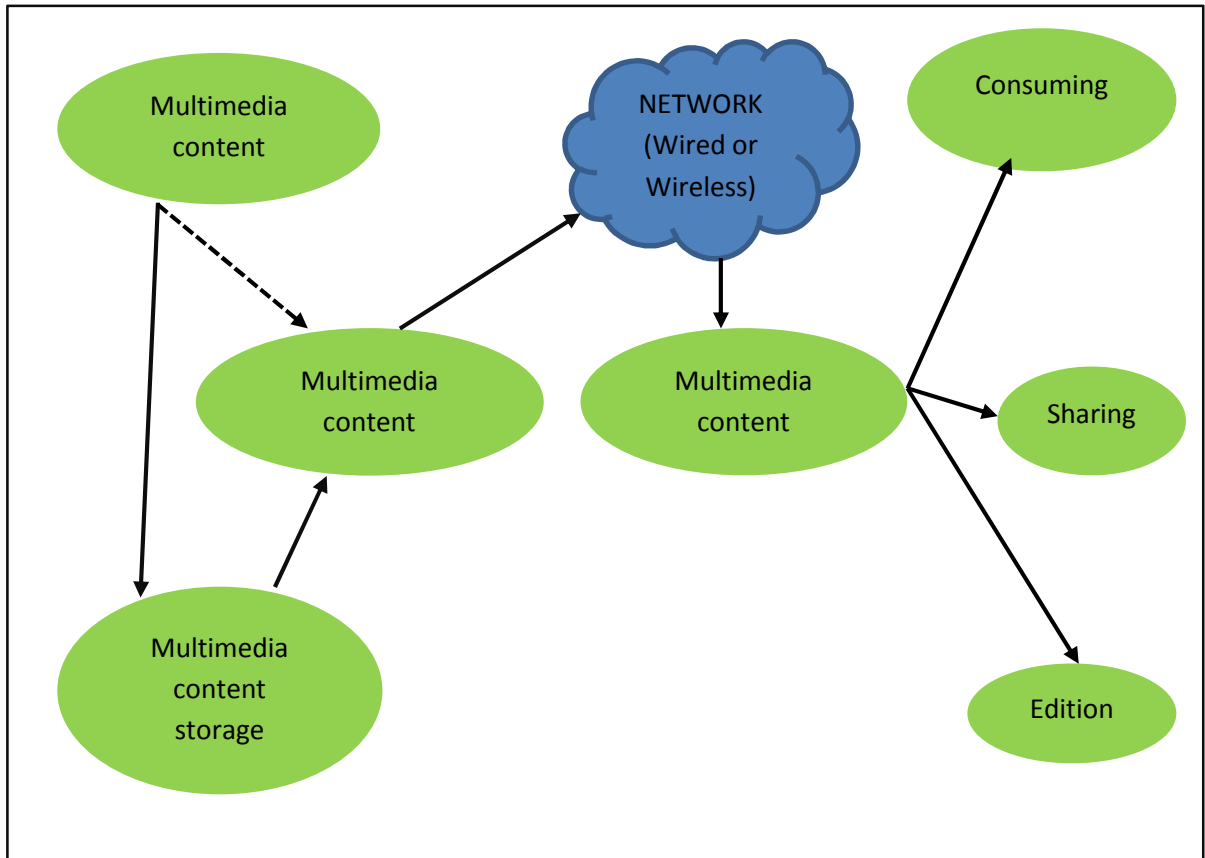


Figure 1.7: General architecture of multimedia system

1.8 CRYPTOGRAPHY

Cryptography [6] [7] is the science of securing gen by encoding it to a non-readable form. Cryptography is synonymous to encryption. This process is systematic and well-structured and is associated with several aspects of info safety, like integrity, authentication, confidentiality and non-repudiation. Widely used applications of cryptography comprise ATM cards, security pass codes, computer passwords, and electronic trade.

Historically, encryption was used by militaries and governments for a long time to facilitate clandestine communication. But now it is widely used in shielding gen within several varieties of civilian systems.

The one who encrypts the message needs to share the decoding practice required to recuperate the genuine info only with envisioning recipients, and thereby prohibiting undesirable people to decrypt the message. Cryptography techniques were used since World War I to communicate the messages secretly. As the technology is growing, the ways used to perform cryptology have become progressively multifaceted and it's utility more prevalent.

1.8.1 TYPICAL CRYPTOGRAPHY

The earlier methods of clandestine writing needed slightly more effort than that of a local pen and paper analogy since utmost people could not read. Actual cryptography [10] [14] was required for more literate opponents. The foremost traditional cipher forms are transposition ciphers, which reorganize or shambles the sequence of letters in information (For example, 'hello India' becomes 'ehloInidai' in a simple reordering pattern.

The simple process of cryptography could not provide much confidentiality from opponents. Caesar cipher was an early substitution cipher scheme, in which every letter in the plaintext was switched by a letter certain fixed sites in the alphabetic sequences. According to Suetonius, long back ago, Julius Caesar applied the Caesar cipher method with a shift of three to link with his generals.

The cryptography scheme can be explained as follows

Input message is specified in the form of plain text 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 described below as

$$C = E * K_e(P) \dots \dots \dots (I)$$

Where,

K_e is the key for encryption and $E ()$ is the function of encryption.

In the same way, the decryption process is described as

$$P=D*K_d(C) \dots \dots \dots (II)$$

Where,

K_d is the key for decryption and $D()$ is the function for decryption.

When both the keys, encryption key and the decryption keys, are same, i.e. $K_e = K_d$, the encryption is known as symmetric cipher or private-key cipher. For private-key ciphers, key for encoding and decoding key must be conveyed from the sender to the receiver through different secret channels. When key for encryption is different from decryption key, i.e. $K_e \neq K_d$, the cipher is known as public-key cryptography. For public-key encoding ciphering technique, each communicating entity has a distinct set of keys. The encryption key K_e is published and distributed to all the parties, and the decryption key K_d is kept private. Here, the advantage lies in the fact that no additional secret medium is required for secret transfer.

1.8.2 CATEGORIES OF CRYPTOGRAPHY

In cryptography, encoding is the procedure of encryption of information or messages in such a manner that eavesdroppers or attackers not able to read it, but only those authorized people can read the message correctly who have been passed on with the details about the encryption algorithm and the secret key. There exist two fundamental types of encryption process:

- Public key cryptography.
- Symmetric-key cryptography.

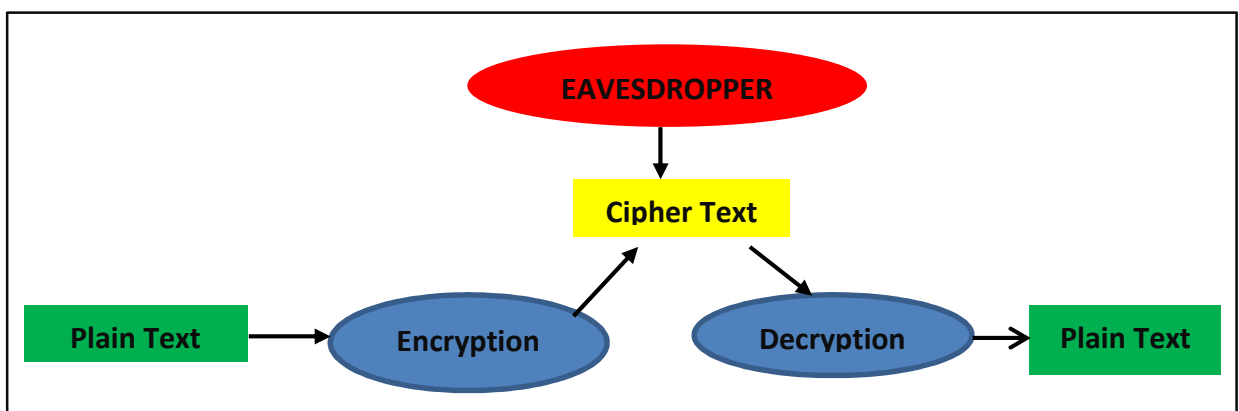


Figure 1.8: Block diagram of cryptography

1.9 SYMMETRIC-KEY CRYPTOGRAPHY

In this method of encryption, the same key is utilized for encoding as well as for the process of decoding of the message. Hence, the sender and receiver must share the secret key before they desire to transfer info among them. In symmetric-key [10] encryption process, the key for encryption is published for everyone to encode messages. Though, only the receiving entity admittance to the decoding key and is able to read the encoded messages. Public-key ciphering technique is a comparatively fresh invention. Earlier, all encoding process has been symmetric-key or private key systems.

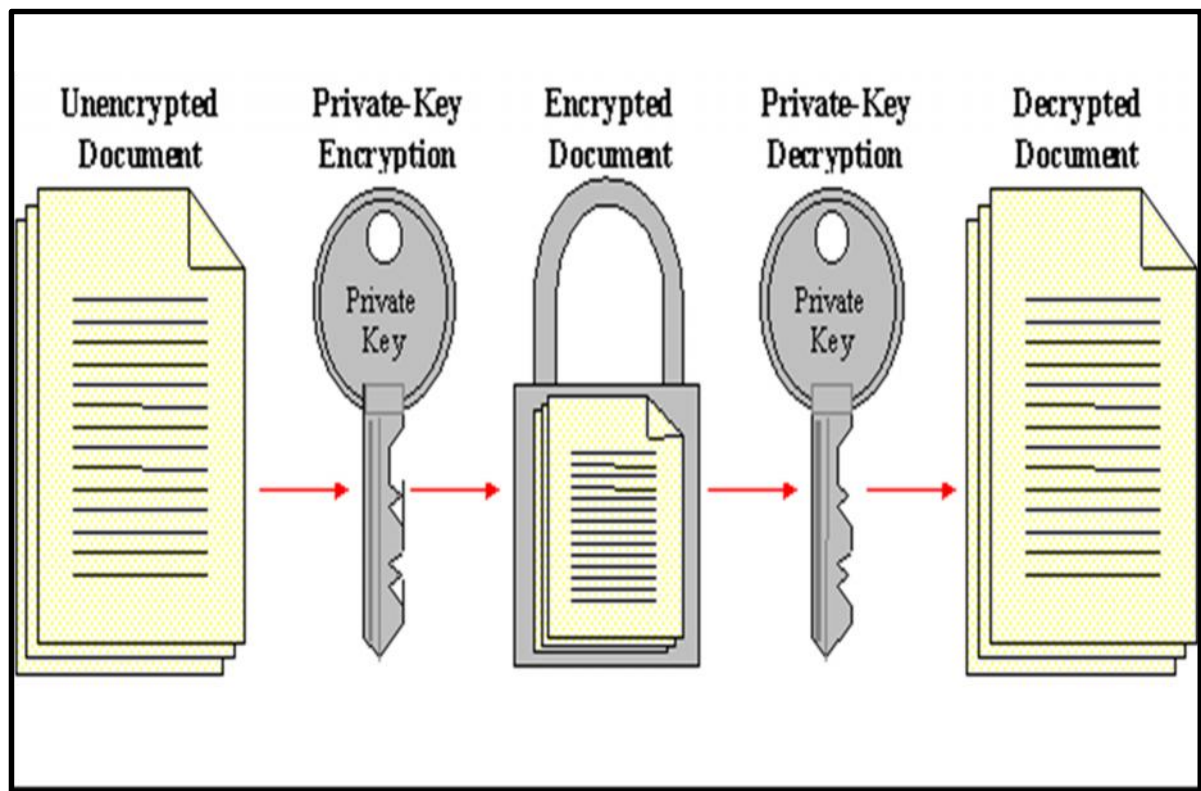


Figure 1.9: Symmetric Key Encryption process

SYMMETRIC KEY ALGORITHM

These algorithms are a set of procedures or methods of cryptography that uses the same encoding keys for both encoding of messages and for the process of decoding of cipher text. The keys will be same or there can be modest conversion to go amid the two keys. This requirement that the sender and receiver have admittance to the secret key is one of the major hitches of symmetric key encoding, when compared to any other public-key encoding procedure.

TYPES OF SYMMETRIC KEY ALGORITHM

It can use either stream cipher or block cipher. A stream cipher [16] is a symmetric key encoding process in which a stream of plaintext is combined with a pseudorandom cipher stream or key stream as shown in figure 1.10. All plaintext digits are encrypted one at a time with the equivalent digit of the key stream, which produces digit of cipher text sequences. The encryption of every digit depends on the present state so it is also called a state cipher. In general, a digit is typically a set of bits and the process for combining is an exclusive-or (XOR) operation.

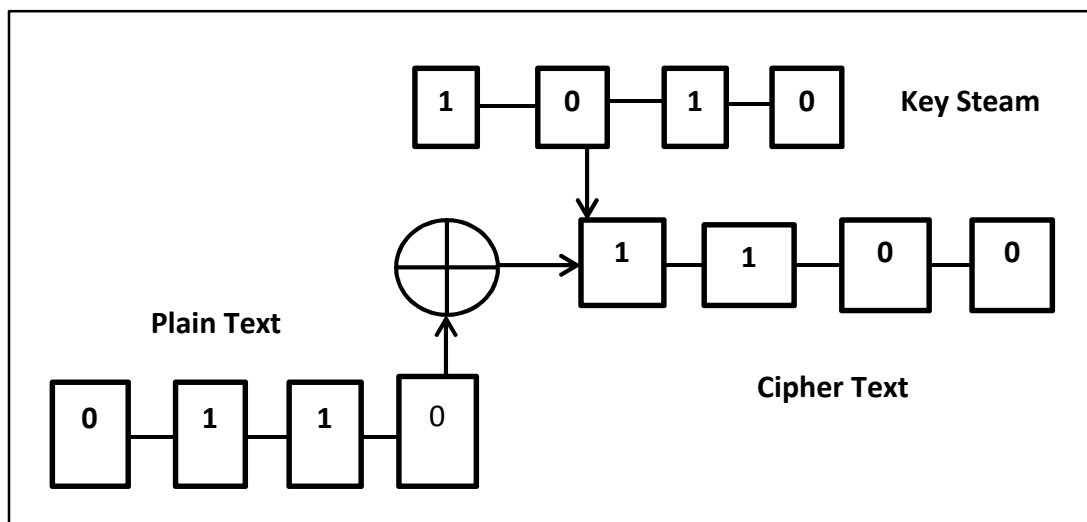


Figure 1.10: Stream cipher

The pseudorandom key is generated in sequence from a random seed by using digital shift registers. The random seed acts as the cryptographic key for decrypting the cipher text stream. Stream ciphers have a completely different process from block ciphers. Block ciphers applied to larger blocks of data to a static and unwavering transformation. A block cipher primeval is utilized in a way that it behaves excellently as a stream cipher. Block cipher encryption process is shown in Figure 1.11.

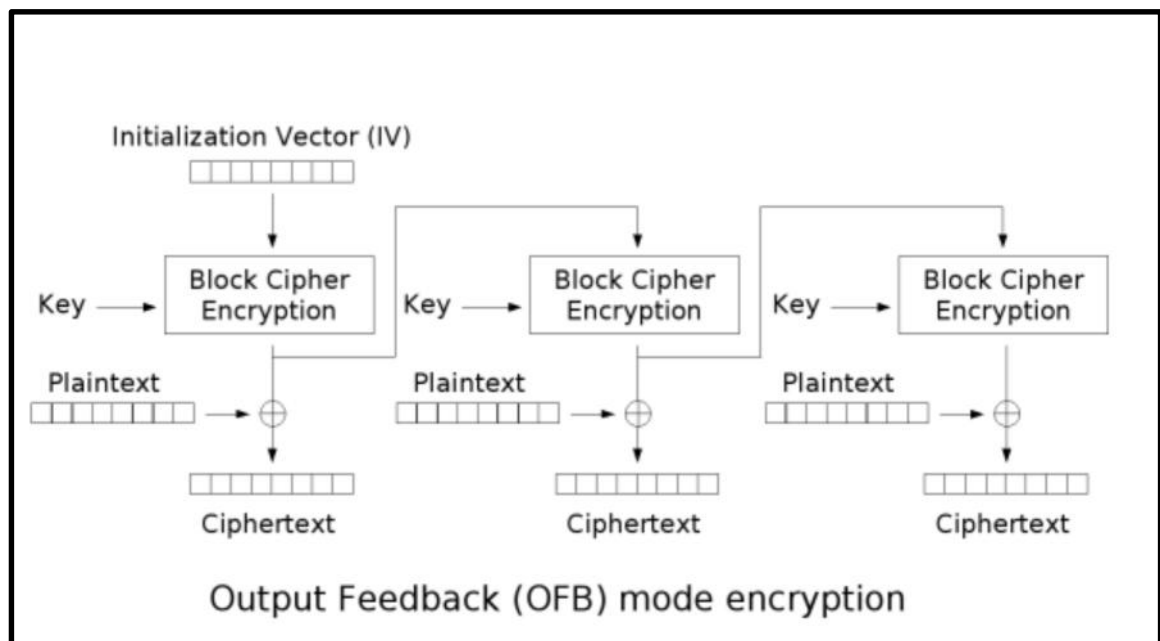
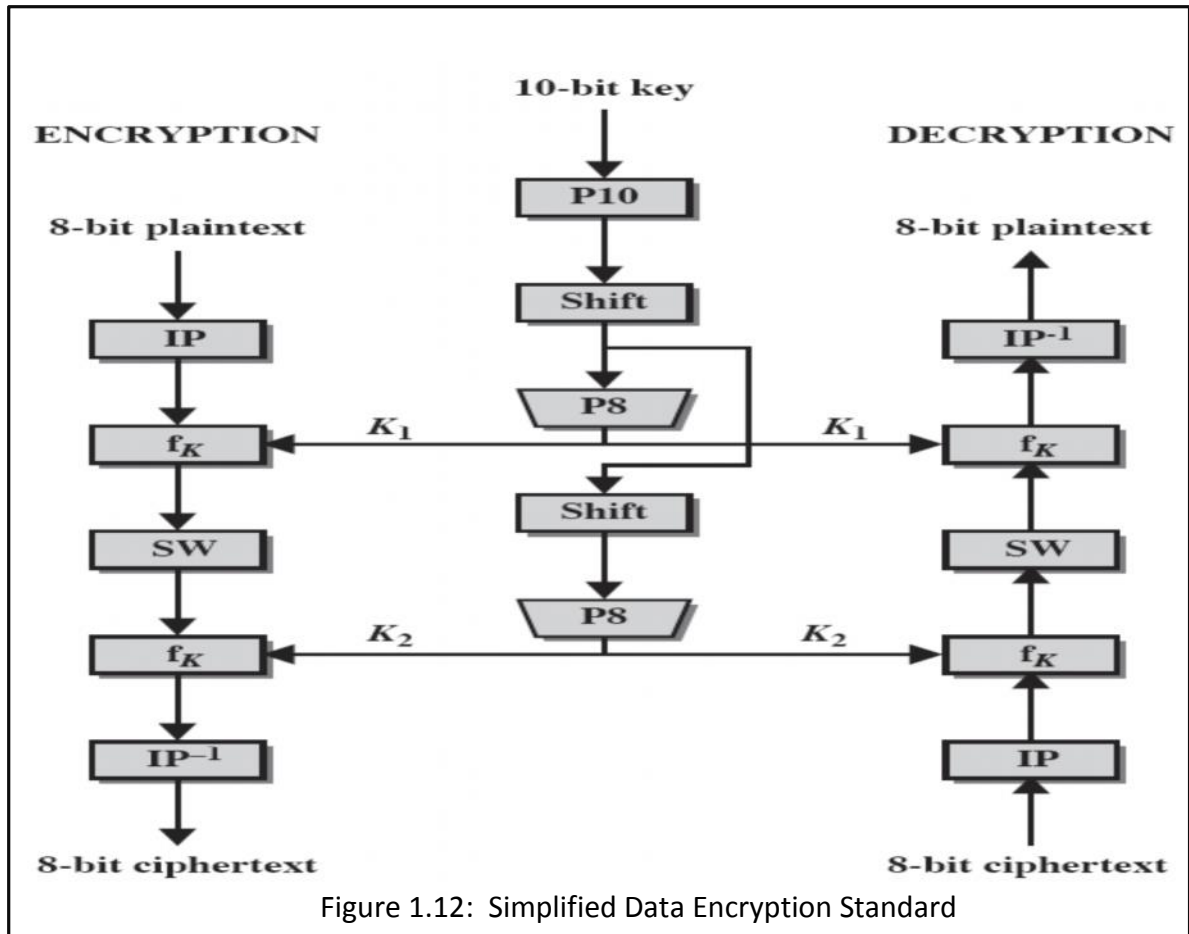


Figure 1.11: Block Cipher

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 lesser hardware complexity. Though, stream ciphers, if used incorrectly, are prone to serious security problems. To overcome this drawback, the same starting seed must never be used twice.

All conventional encryption procedures are built on two categories of modification of the data: substitution and permutation.

In case of substitution: each portion of the plaintext is projected into another portion. Whereas in case of a permutation: the letters in the plain text are reorganized. A simplified DES procedure is shown in the Figure 1.12 below.



1.10 PUBLIC-KEY CRYPTOGRAPHY

Symmetric-key or Private-key cryptosystems [12] utilize the same secret key for encoding and decoding of data, may be a message or information have a dissimilar key than the others.

In 1976, Whitfield Diffie and Martin Hellman anticipated the notion of public key cryptography or asymmetric key crypto system. Diffie–Hellman is a key exchange protocol, which provides a solution to allow two parties to secretly share encryption keys.

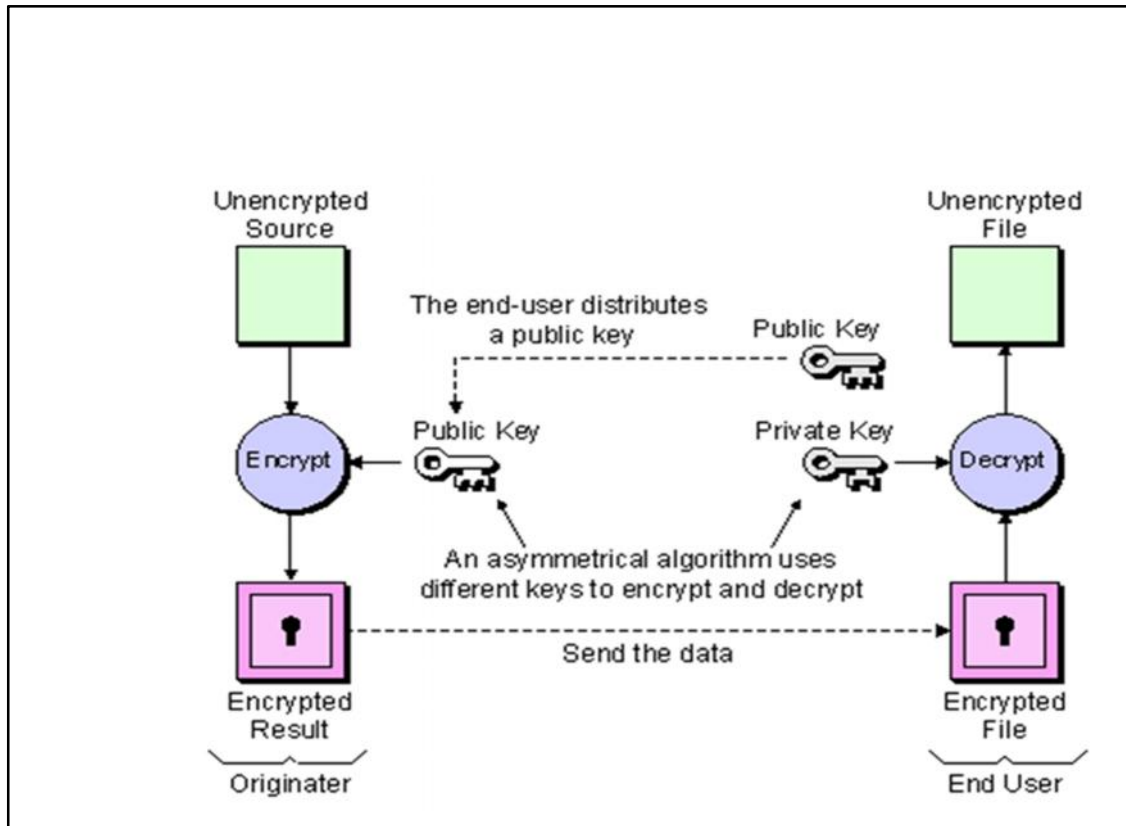


Figure 1.13: Public Key Cryptography Process

In the process of Diffie Hellman key exchange, every communicating entity generates a pair of public and secret key and share the public key. Afterwards procurement of a genuine set of one another's public key, Alice and Bob can calculate a mutual clandestine offline and the shared clandestine can be utilized as the key in the process of symmetric encoding.

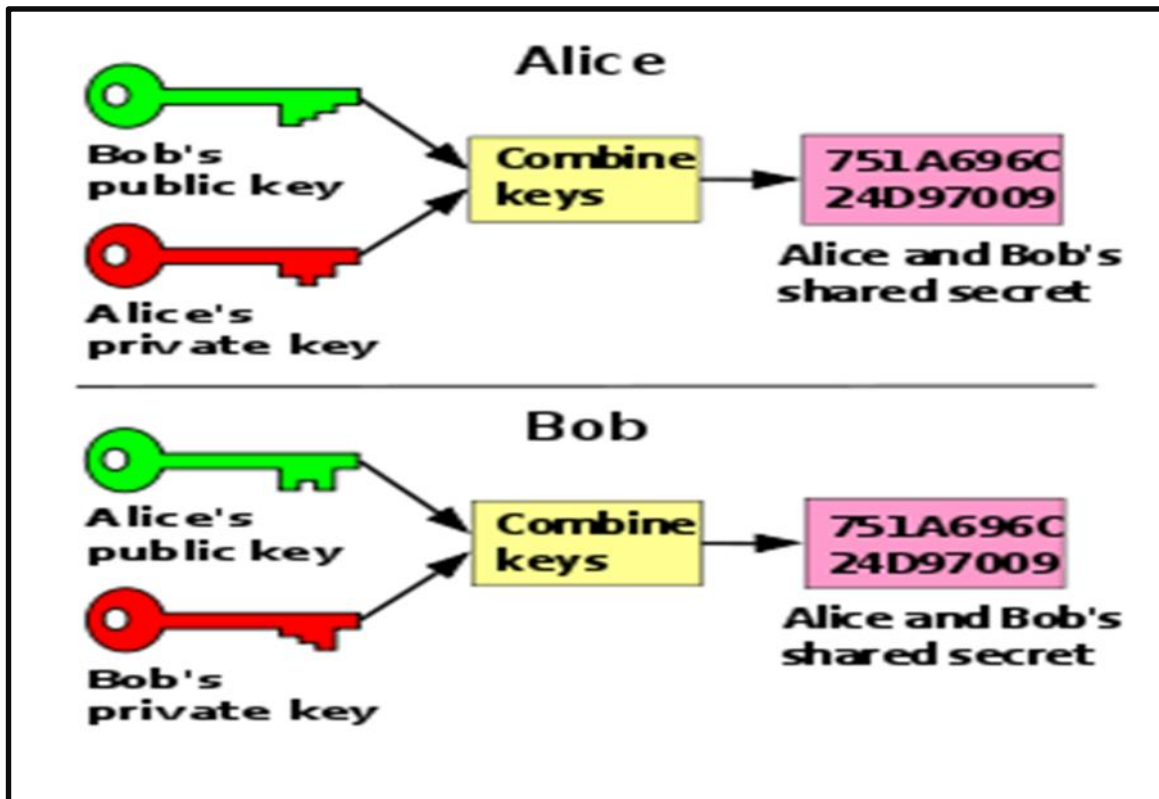


Figure 1.14: Diffie-Hellman Process

1.11 CRYPTANALYSIS

It is the process of study of ciphers, or confidential coding system, with a target of discovering flaws in them that grant access to derive plain text from the cipher text, without inevitably having the knowledge of the algorithm or key. This is known as breaking the cryptosystem or cipher text.

There are several methods for performing cryptanalysis, subject to what right the cryptanalyst has to the cipher text, plain text or any other aspects of the cryptosystem.

1.12 SIGNIFICANT TERMS

1.12.1 CRYPTOSYSTEM

The word cryptosystem is utilized as synonym for cryptographic scheme. A cryptographic scheme is any system, which consist of cryptography like a system for secure electronic mail which includes cryptographic hash functions, key management, methods for digital signatures, and so on. In the perspective of cryptography, a cryptosystem denotes a set of processes require to implement a particular procedure of encryption and decryption.

1.12.2 EAVESDROPPING

Eavesdropping is an unethical act of interfering in-between and sneakily listening to a secret exchange. This can be considered as a passive attack if third party tries only to observe the flow and get information. If it attempts to modify the info or affects the flow of data, then eavesdropping is categorized as active attack. Eavesdropping can be done by monitoring Internet conversations or telephone network by a third party.

1.12.3 ONE-TIME PAD

One-time pad [13] is a process of encoding, which is difficult to break if used correctly. Cipher text is obtained by encrypting each bit from the plaintext from modular addition to secret random key of the same length as the plaintext. It is impossible to decrypt cipher text without prior knowledge of encryption the key. This is possible only if the key is truly random, and of the same size that of plain text, never reused in part or whole, and kept clandestine. For easy disguise, the pad is sometimes abridged to a very small size in a manner that it can be used only with the help of a powerful magnifying glass.

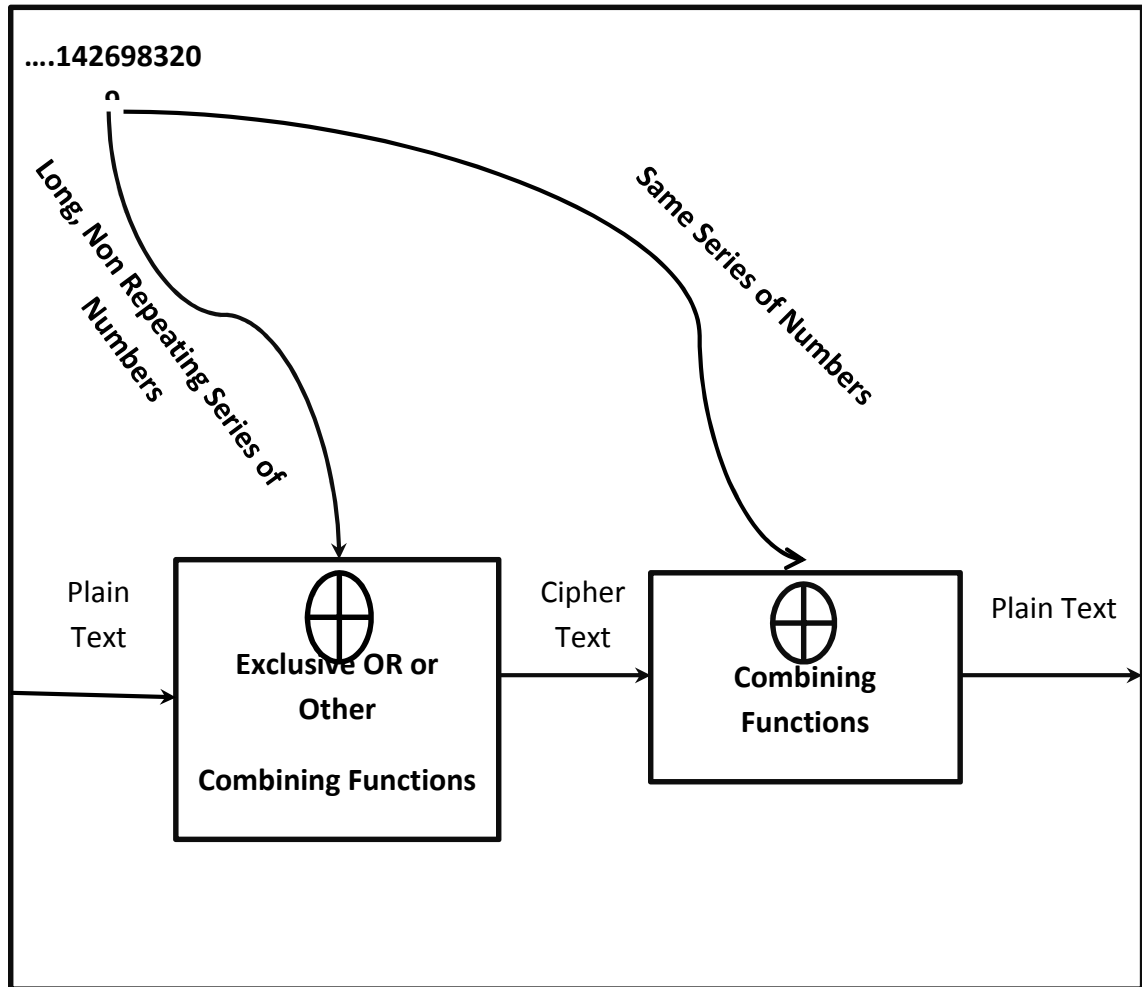


Figure 1.15: One-Time Pad or Verman Cipher

CHAPTER - 2

CHAOS AND CRYPTOGRAPHY

2.1 INTRODUCTION

In the past few decades, chaotic signal [17] [18] 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 behavior.

Chaos theory is a part of mathematics that defines the multifaceted active systems which is highly delicate to their initial parameters. Eventually, each and every result depends on these initial parameters.

Chaos theory is used in numerous disciplines, counting engineering, meteorology, economics, biology and physics. There exist several kinds of chaotic systems which inherit the property of chaos theory. Chaotic systems like 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 maps define the randomness in the attractor field depending upon these initial parameters. Chaos theory is a mathematical physics, which has been driven by Edward Lopez. It is stated as follows:

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

On 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 the past few decades, chaotic systems were applied in cryptography to secure multimedia over insecure network. A chaotic system based on confusion and diffusion was developed in 1989 [19]. Although it was already being used for cryptographic system, but there was no theorem to prove authenticity of the chaotic map. Chaotic systems [20] 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 [21]. The parameters in chaotic maps are meaningful if they are real numbers [22], which can be used in the cryptographic algorithms as encryption and decryption keys. Chaotic systems have possible applications in such cryptography procedures as the hash function, block cipher and pseudorandom number generator. Over the last two decades, there has been fabulous concern in utilizing chaotic systems to design secure cryptographic algorithms [23].

2.2 CHAOS THEORY

A system is called a chaotic system, if it is subtle to initial circumstances and topology. This theory is named so due to the fact that the systems described by this theory [24] [25] are apparently topsy-turvy, but in reality, chaos theory is regarding discovery the essential order in ostensibly random data. Researchers have studied chaos theory in numerous domains, such as electronic systems, climate and weather and lasers.

A chaotic system is modest, dynamical and non-linear 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 [26]. On the other hand, in classical science of the previous states, whereas there is always a mathematical equation to determine the system evolution[27]. 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 behavior, and completely deterministic nature. The chaotic conduct can be perceived in many different systems such as electronic systems, lasers, climate and economics [28].

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 behavior, but completely deterministic in nature: the behavior of chaotic systems is purely deterministic but seems to be random. Hence, for same initial values the chaotic system produces the same set of output values again and again. Furthermore, the chaotic systems are dynamical structures that are described by differential equations and the previous state identifies the next step.

2. Sensitivity dependence on the initial circumstances:

The initial state is the stage from which the system starts. Dynamical systems evolve entirely differently over time, even with slight changes in the initial state [29]. 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 systems.

3. Unpredictable:

The future conditions of the chaotic system are very difficult to envisage in the long term as stated in. 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 issues related to weather forecasting, which cannot be solved on its own with a group of twelve reckonings to model the weather [30]. Nevertheless, this computer platform could only predict supposedly what the weather might be. Once he desired to see a specific order again. He started solving the problem in the intermediate of the series, instead of starting from the start, consequently he entered the number off his printout and set free to run. The output sequence evolved to be different. This process is similar to chaos theory, is also identified as subtle dependency on initial conditions. Slight alterations in the preliminary circumstances can lead to a drastic alteration in the long term comportment of a system. Such minute difference in a measurement might be well-thought-out as background noise or experimental noise. These things are nearly not possible to avoid in even the most secluded lab. From this clue, Lorenz stated that it is not possible to forecast the weather precisely. Though, this

unearthing led Lorenz on additional characteristics of what eventually came to be recognized as chaos theory.

2.3 CHAOS-BASED CRYPTOGRAPHY

The relationship between conventional cryptography algorithms and chaos-based cryptography algorithms are very important in order to understand the differences and similarities among cryptography algorithms and chaotic systems. Old and traditional cryptographic system were based on integer number system whereas chaotic systems [31] 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 [32].

➤ **Block Cipher Based on Chaotic Systems**

A block cipher is a transformation function that maps, units of plaintext bits to cipher text bits of the identical unit size underneath the control of the secret key. The decryption method divides the input cipher text 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 furthestmost widely-used hash functions employed in numerous safety applications and etiquettes. Since SHA-1 was attacked in 2005, many researchers have been working on designing a new, alternative secure hash function [33].

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

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

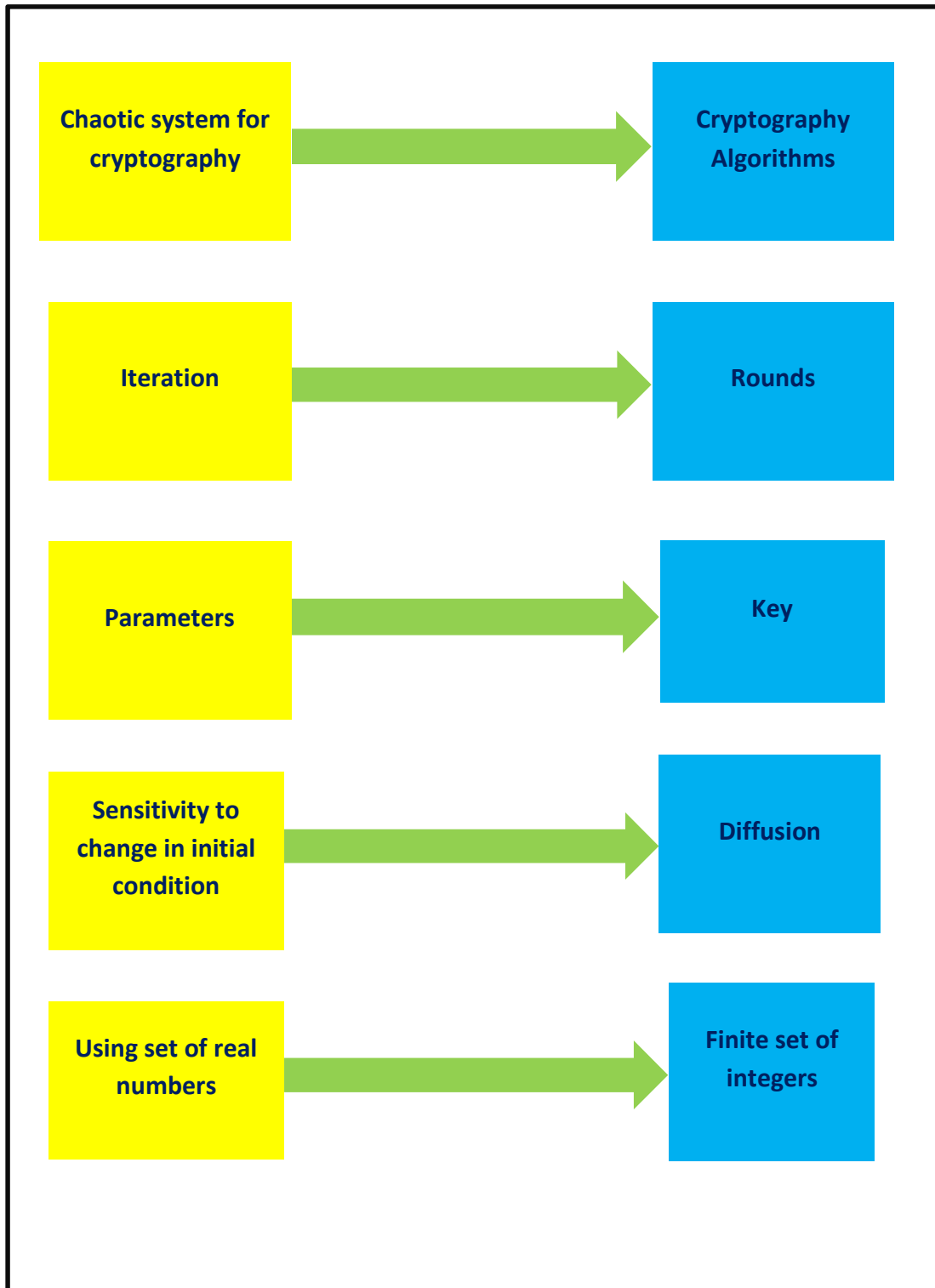


Fig. 2.1: Comparison between Chaotic System and Cryptographic

2.4 CHAOTIC MAPS

These are the varieties maps that show some kind of chaotic behavior. It can be parameterized by continuous time or discrete time variables. Discrete maps habitually take the method of repeated functions. Chaotic maps frequently befall in the field of dynamical schemes. Where on one hand, 1-D chaotic maps are used and applied on data sequence or upon the document and on the other hand 2-D or greater order chaotic maps are employed for image encryption, the reason being that the image pixels can be considered as a 2D sequence of pixels. Literatures upon chaos consist of common terms such as maps. 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

This type of maps 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. A list of some of

One-dimensional chaotic maps are given below:

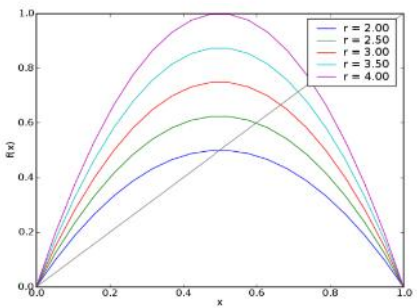
- Complex Squaring Map
- Complex Quadratic Map
- Duffing Equation
- Gauss Map
- Interval Exchange Map
- Logistic Map
- Tent Map
- Van Der Pol Oscillator

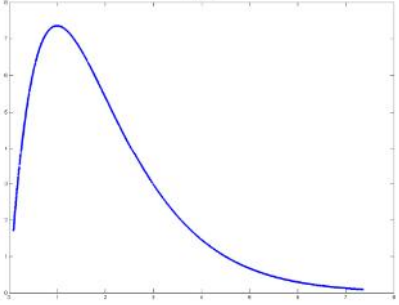
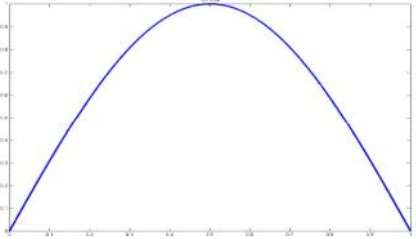
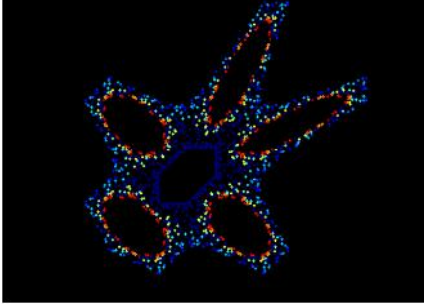
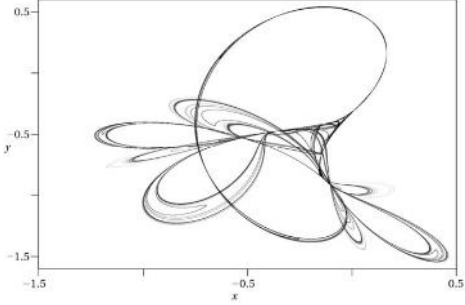
2.4.2 Two-dimensional Chaotic Maps

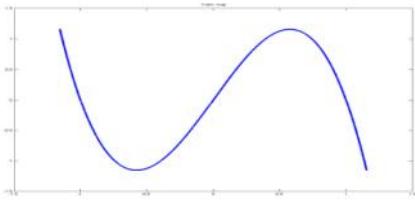
These maps deals with more than one variable quantity. Two-dimensional chaotic maps exist as an object in a three-dimensional space, where x and y axis indicates the ruling equation of the chaotic map and z-axis is the temporal axis. A list of some of two dimensional chaotic Maps is given below:

- Ikeda Map
- Baker's Map
- Duffing map
- Exponential Map
- Henon Map
- Horseshoe Map
- Arnold's Cat map

Table 1: Graphical representation of different chaotic maps

CHAOTIC MAP	EQUATION FOR MAP	PLOT
LOGISTIC MAP	$X_{n+1} = rX_n(1 - X_n)$	

<p>RICKERS MAP</p>	$X_{n+1} = R(X_n)$ <p>Where $R(X) = Xe^{p-X}$</p> <p>on $[0 \]$</p>	
<p>SINE MAP</p>	$X_{n+1} = \sin(\pi X_n)$	
<p>GINGERBREAD MAN MAP</p>	$X_{n+1} = 1 - Y_n + X_n $ $Y_{n+1} = X_n$	
<p>TINKERBELL MAP</p>	$X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n$ $Y_{n+1} = 2X_nY_n + cX_n + dY_n$	

CUBIC MAP	$X_{n+1} = 3X_n(1 - X_n)^2$	
------------------	-----------------------------	--

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 sequence, even though other parameters are not repeated or duplicated repeated. An attractor is a set of variables which evolves in discrete dynamical system. These sets 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 [38] can be a curve point and a complicated way of fractal structure is known by strange attractor.



Figure 2.2: Attractor for dynamic system

A dynamic type of equilibrium is known as Strange Attractor. The dissimilarity amid a Strange Attractor and an Attractor is that, Strange Attractor signifies some kind of trajectory upon which a system goes from situation to situation without ever settling down, where an Attractor embodies a state to which a system finally settle down.

CHAPTER - 3

LOGISTIC MAP

AND

DISCRETE COSINE TRANSFORM

3.1 LOGISTIC MAP

The word chaos means randomness in the system. It is the measurement of disorder into a system. In case of data encryption it can be considered as how much cipher block is sensitive to the initial settings of the chaotic maps. Chaotic map [41] [42], which we have applied in our proposed method of multimedia encryption, is mathematically represented by the formula given below

$$F(X_n) = a * X_n * (1 - X_n) \quad (1)$$

$$F(X_{n+1}) = F(X_n) \quad (2)$$

Here X_n represents the chaotic sequence [43], which lies between zero and one, as shown in Fig 2. The preliminary condition in case of the logistic map is for $n=0$, $X_0 \in [0, 1]$. The parameter 'a' is a real number in the range of 0 and 4, i.e. $a \in [0, 4]$. After a lot of research, researchers have found that system is chaotic for 'an' in the range from $3.56994 < a < 4$. For the value of 'a' beyond 4, the value of X leaves ranges [0, 1]. And X_n diverges for almost all initial values of X_0 . Depending on the values of a., X has different nature, which are shown in the Fig. 2.

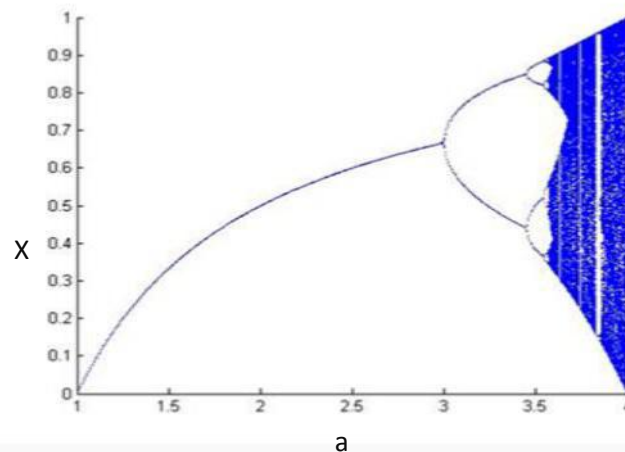


Fig. 3.1 Bifurcation diagram for logistic map

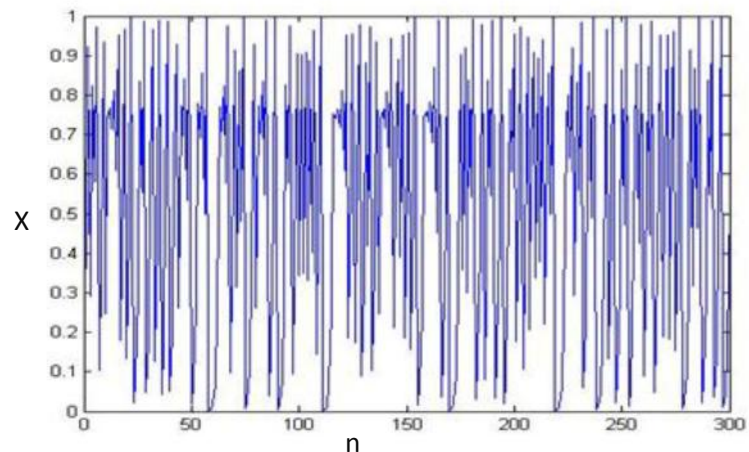


Fig. 3.2 Variations of Logistic map with iterations

3.2 RANDOM NUMBER GENERATOR

There are mainly two kinds of random number generators:

- Random number generator
- Pseudorandom random number generator

3.2.1 Random number generator

It is an algorithm or a device that generates a series of binary bits that are statistically independent from each other. Random number generators are utilized in many cryptography algorithms. They provide a high level of security for various cryptographic systems such as DES secret key, prime numbers in the RSA algorithm, and prime numbers in a digital signature.

3.2.2 Pseudorandom number generator (PRNG)

PRNG is a procedure that devises a binary bit sequence that is approximately haphazard. All the processes are governed in a deterministic manner. The input parameter of the PRNG is called a seed and the yield is known as binary series.

The PRNG generates a sequence of length l which is not random. It collects all small truly random bits 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.

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

In stream cipher algorithms, pseudorandom number generators (PRNGs) results are mainly used as a key stream that simply XOR with plain text to generate the cipher text using other encoding process. Moreover, it is very important to generate the secret keys and initialization variables by PRNGs.

3.3 CONFUSION AND DEFUSION

Cryptography algorithms are designed based on confusion and diffusion. In 1949, Claude Shannon introduced the terms 'confusion' and 'diffusion', which are considered to be a very important aspect of designing a secure encrypted message [43]. Shannon's theory aims to deduce the possibility of cipher text attack based on plain text statistical analysis.

Some cryptanalysts use their prior knowledge of plaintext statistical characteristics to make the 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.

Therefore, Shannon suggested that the cipher text should be independent of the key used and also the cipher text should be independent of the plaintext. Diffusion is nothing but hiding the relationship amid the plaintext and cipher text. Changing one bit in plain text

can affect more than half of the cipher text bits. Confusion can be termed as hiding the relationship amid the statistics of cipher text 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 cipher text, while confusion prevents the cryptanalyst from finding any relationship amid the cipher text and the used key.

Hash functions are similar to conventional encryption methods in a way that they need the influence of the whole input message to be spread into the hash value space. In an ideal hash function, there should be a complex relationship between bits in input message and the 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.

3.4 IMAGE COMPRESSION AND DISCRETE COSINE TRANSFORM

3.4.1 IMAGE COMPRESSION

3.4.1.1 Requirement for image compression

The necessity for picture compression becomes obvious, when the required bits per image is calculated from quantization techniques and archetypal sampling rate. For example, contemplate the broadcast of lower quality 512 x 512 x 8 bits per pixel x 3-color audiovisual picture in phone line in a 96000 bauds modem, the communication would require nearly 11 minutes for a solo picture, which is not acceptable for utmost applications.

3.4.1.2 Principles behind compression

The picture compression research objective is to decrease the quantity of bits needed to present a picture by eliminating the spectral and spatial redundancies up to the extent it is probable.

Data redundancy is the crucial matter in digital image compression. If N_1 and N_2 symbolize the number of gen units in the input image and compressed picture, then the compression ratio Cr will be

$$Cr = N_1 / N_2;$$

And comparative data redundancy R_d of the input picture can be formulated as

$$R_d = 1 - (1 / Cr);$$

Three cases rise here:

- (1) If $N_1 = N_2$, then $Cr = 1$, therefore $R_d = 0$, which infers that input picture do not hold several redundancy among pixels.
- (2) If $N_1 \gg N_2$, then Cr , therefore $R_d > 0$, which suggests a significant amount of redundancy in the input picture.
- (3) If $N_1 \ll N_2$, then $Cr > 0$ and therefore R_d - which implies that the compressed picture contain more data than the input picture.

3.4.2 TYPES OF IMAGE COMPRESSION

Lossless versus Lossy compression:

In the Lossless compression practice, the reassembled picture, later compression, is mathematically indistinguishable to the input picture. Lossless compression is favored for archival purposes in applications like medicinal pictures, methodological portrayals, etc. Though, lossy systems can achieve considerable compression. Lossy approaches are predominantly appropriate for natural pictures like snapshots in applications, where minute damage of reliability is satisfactory to acquire a generous discount in bit rate.

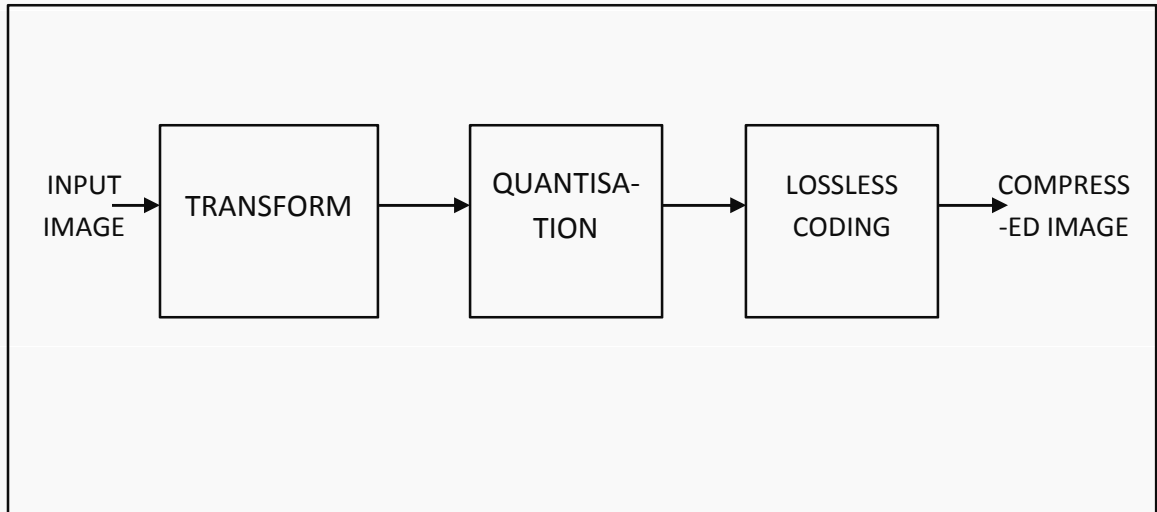


Fig. 3.3 Image compression Model

3.4.3 DISCRETE COSINE TRANSFORM

Discrete cosine transform (DCT) splits the picture into components of distinct frequencies, where a smaller amount of frequency of lesser concern is rejected via quantization. However, essential frequencies were utilized to recover the picture at the time of decompression. In comparison to any other reliable transforms, DCT has several benefits:

- (1) DCT can be employed in a single integrated circuit;
- (2) DCT has the capability to keep the utmost of the gen in fewer coefficients;
- (3) It lessens blocking artifacts that occur, when margins among sub pictures become noticeable.

FORWARD 2D-DCT TRANSFORM

$$C(u, v) = D(u)D(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \dots \dots \dots (3)$$

Where,

$$u, v = 0, 1, 2 \dots N-1$$

INVERSE 2D-DCT TRANSFORM

$$F(x, y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} D(u)D(v)D(u, v) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \dots(4)$$

Where,

$$D(u) = (1/N)^{1/2} \text{ for } u = 0$$

$$D(u) = (2/N)^{1/2} \text{ for } u = 1, 2, 3, \dots, N-1$$



Fig. 3.4 (a) Input Image

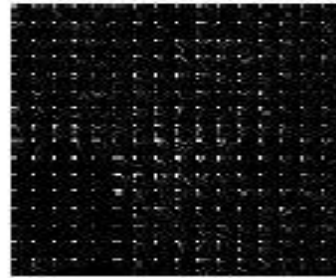


Fig. 3.4 (b) After 8X8 DCT



Fig. 3.4 (c) Input Image

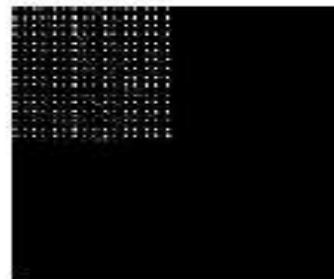


Fig. 3.4 (d) After 4X4 DCT



Fig. 3.4 (e) Input Image



Fig. 3.4 (f) After 4X4 DCT



Fig. 3.4 (g) Input Image



Fig. 3.4 (h) After 8X8 DCT

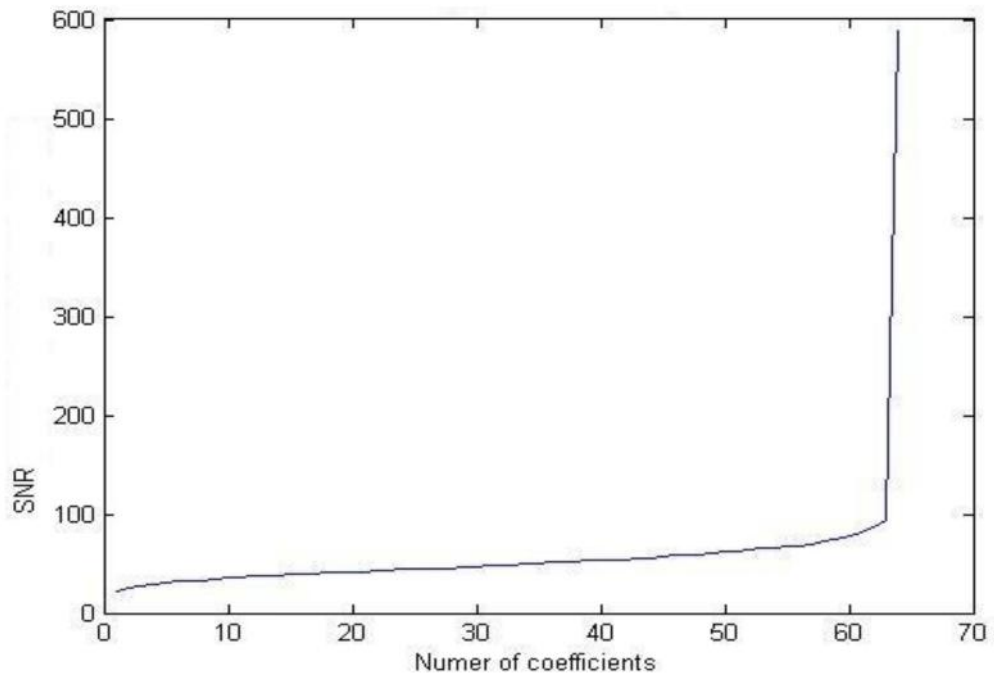


Fig. 3.5 SNR vs. No. of coefficients

CHAPTER - 4

RELATED WORK

In this section, a literature review of various techniques and methods of digital image security is done. There are two ways of Image encryption, one is done in Spatial Domain and another in Frequency Domain. In the cryptography scheme, Spatial Domain is used more frequently rather than frequency domain. When these digital images are encrypted with traditional cryptography schemes, they have slow speed due to the large size of data. With the introduction of Chaos theory and its applications, a new aspect of secure cryptography has emerged.

Cryptography scheme is mainly two types: one is symmetric key cryptography scheme and another one is known as private key cryptography scheme. The symmetric key cryptography scheme is achieved by two ways: one is stream cipher and another is a block cipher.

The most popular symmetric key cryptography is DES (data encryption algorithm). It is the FIPS or federal information processing standard; it shows DEA originated at IBM. It was accepted in 1977 as standard by the United States (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 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.

Edward Lorenz examined chaos theory by describing a simple model of Weather prediction which was a first numerical model to detect chaos in a non-linear dynamical system.

In Lorenz's findings some equations gave rise to some surprisingly complex behavior and chaotic behavior depends on the initial condition. In [49], Hadamard analyzed 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 the mathematical literature where system results appear random 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 utilized to create a random binary sequence to produce the cipher text.

In 1989, Matthews published the first chaos-based stream cipher algorithm 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 key stream. In CPRNGs, many chaotic systems have been utilized including Piecewise non-linear chaotic map, Logistic map, Tent map, and Henon attractor.

In [54], Chen et al. Presented symmetric image encryption process, which is based on 3D chaotic maps. Wang et al. [55] introduced a 3D Cat map centered symmetric picture encoding process.

Joint picture encoding process built on diffusion mapped disorder and hyper chaotic systems, encoding system are also presented in [56] [57]. Though, the encryption mathematics based on 3D chaotic cat maps is a computationally costly procedure. And the key size is not independent.

Chen Wei-bin and Zhang Xin [58] in 2009 anticipated a picture encoding process based on the Arnold cat map with the Henon chaotic system. Several experiments are done by him that shows the efficiency of secure encryption algorithm.

CHAPTER - 5

PROPOSED ALGORITHM FOR ENCRYPTION

5.1 MOTIVATION

The present development of networked multimedia systems has amplified the requirement for the safety of digital media. This is mainly significant for the security 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 numbers so it's easy to formulate and generate keys which are random in behavior. Chaotic map is totally different from traditional cryptography schemes which are unpractical on images. Chaos maps truly work on one time pad scheme, so it is just impossible for cryptanalysis to decode the cipher image because of these properties of chaotic systems. Computable cost, complexity and other factors increase the use of chaotic systems.

5.2 PROPOSED METHOD

I propose an efficient algorithm for multimedia security, which provides better security than earlier chaotic based encryption systems. Multimedia encryption using our proposed method is a four-step process. In the first we create confusion by changing bit positions in the input image. In the next step a block of random numbers is created by applying iterations as many times as the image size. Then the XOR operation is applied to generate the cypher text (encrypted image). Finally, discrete cosine transform (DCT) is applied to shrink the volume of data by compression. In the decryption, we performed reversed of the encoding process at the receiver's end.

5.3 PROPOSED ALGORITHM

The proposed algorithm for multimedia encryption is a five-step process

1. Divide the input image into four equal components.
2. Image is shuffling to create confusion.
3. Encryption of information using a logistic map.
4. DCT is applied to the encrypted image for compression.
5. Step 1-4 is applied in reverse order to get the original image.

I. IMAGE SHUFFLING PROCESS

Step: 1

In the first iteration split the original image into four equal components and interchange them diagonally.



Fig. 5.1 Input image



Fig. 5.2 Image after first Iteration

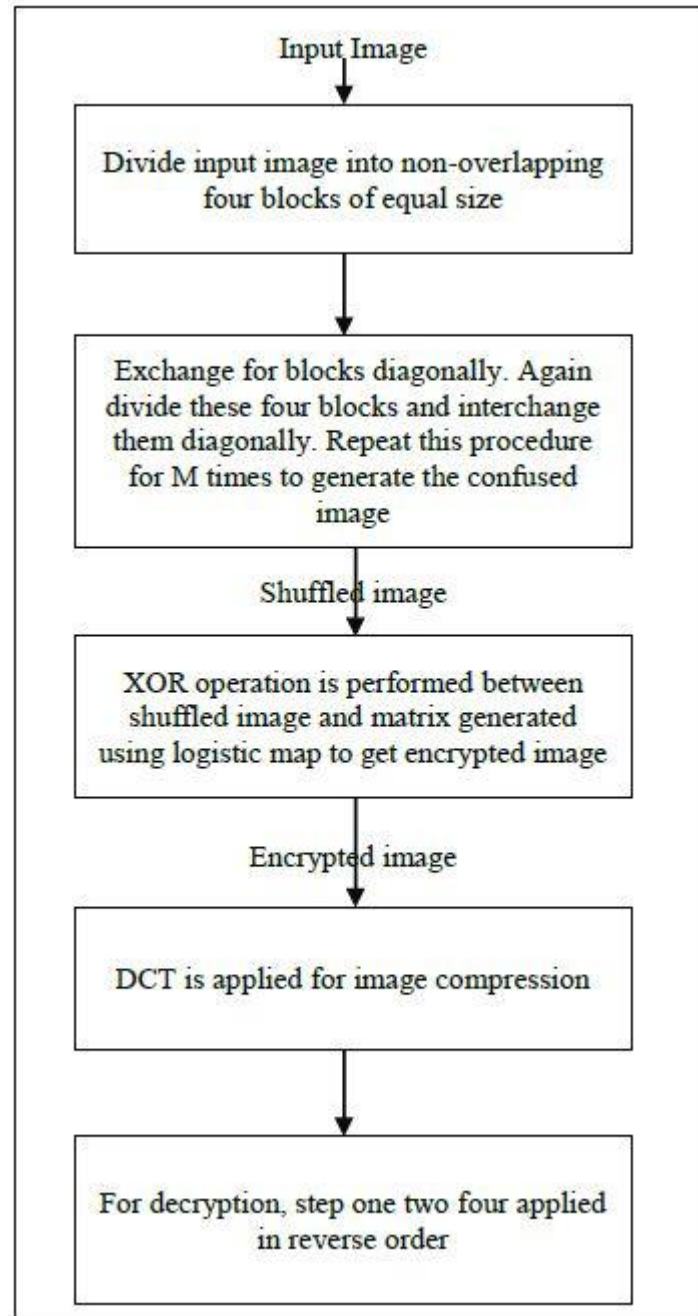


Fig. 5.3 Flow chart of proposed algorithm

Step: 2

Now, in the second, third, fourth and fifth iterations, again divide the each component of the shuffled image into four components and interchange them diagonally.

Step: 3

Repeat step number one, for N (where N is an integer) iterations to generate shuffled image.



Fig. 5.4 Shuffled image after fifth iteration

II. ENCRYPTION USING CHAOTIC LOGISTIC MAP

Shuffled image is encoded applying the pseudorandom sequence derived from the chaotic logistic map.

Step: 1

Choose the initial value of the constant parameters 'a' and X_0 for chaotic logistic map. These parameters act as secret symmetric key for data encryption using logistic map.

Step: 2

Logistic map work as a key stream generator for message encoding . The dimensions of the stream depend upon the dimensions of images taken during the encryption procedure. If the image size is $M \times N$, then the number of logistic sequence will be $M \times N$ obtained by equation (1), where each element in the sequence is normalized in the range of 0-255.

Step: 3

Encoding is done by bitwise Exclusive-OR operation between shuffled image and sequence generated in step 2.

Step: 4

Discrete cosine transform (DCT) is applied to the encrypted image, for compression.

Step: 5

At the receivers end, step 1-4 are applied in reverse manner.

CHAPTER - 6

EXPERIMENTAL RESULTS

Experimental results of the proposed image encryption process are illustrated to appreciate the effectiveness of the proposed algorithm with gray and color images.

The MATLAB 7.5 software was used for implementing this code. Grayscale is typically the favored form for image processing. The color images can be disintegrated and processed as three separate grayscale images.

Here, test image of size 256×256 is shown in Fig. 6.2 (a). The initial constraints for Logistic map are chosen as $a = 3.999$ and $X_0 = 0.1$ to make the chaotic system. Secret symmetric key for encryption is a combination of $X_n = 0.1$ and $a = 3.999$.

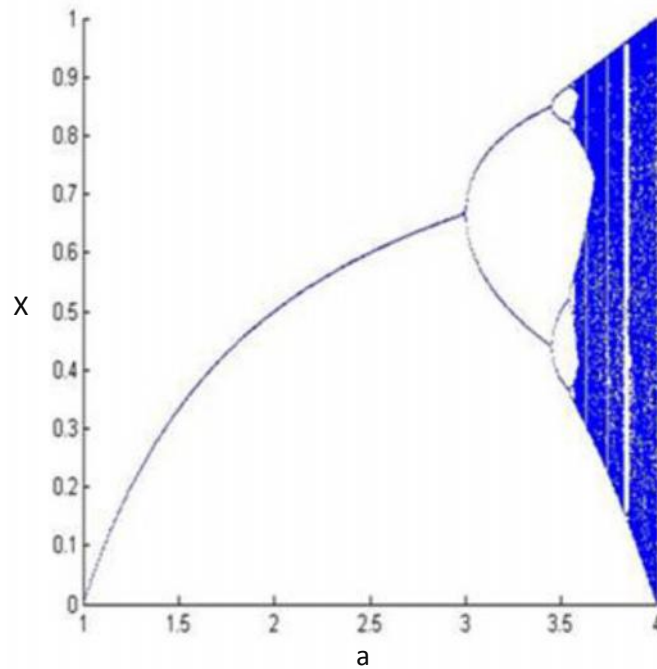


Fig. 6.1 Bifurcation diagram of Logistic map

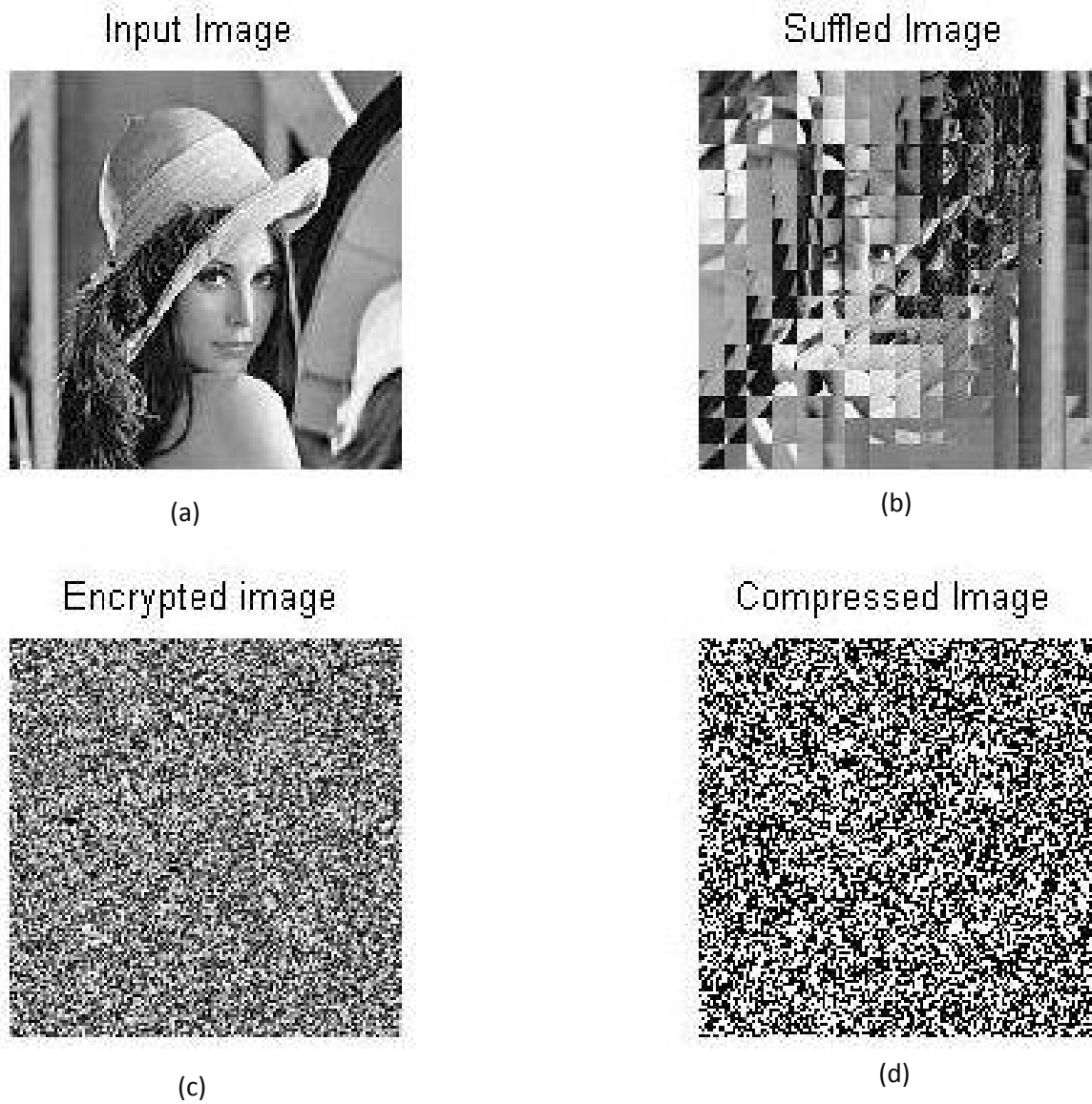
1. ENCRYPTION OF IMAGE

Fig. 6.2 Encryption by Chaotic Logistic system. (a) Input image (b) Shuffled image
(c) Encrypted image (d) Compressed image.

2. DECRYPTION OF IMAGE

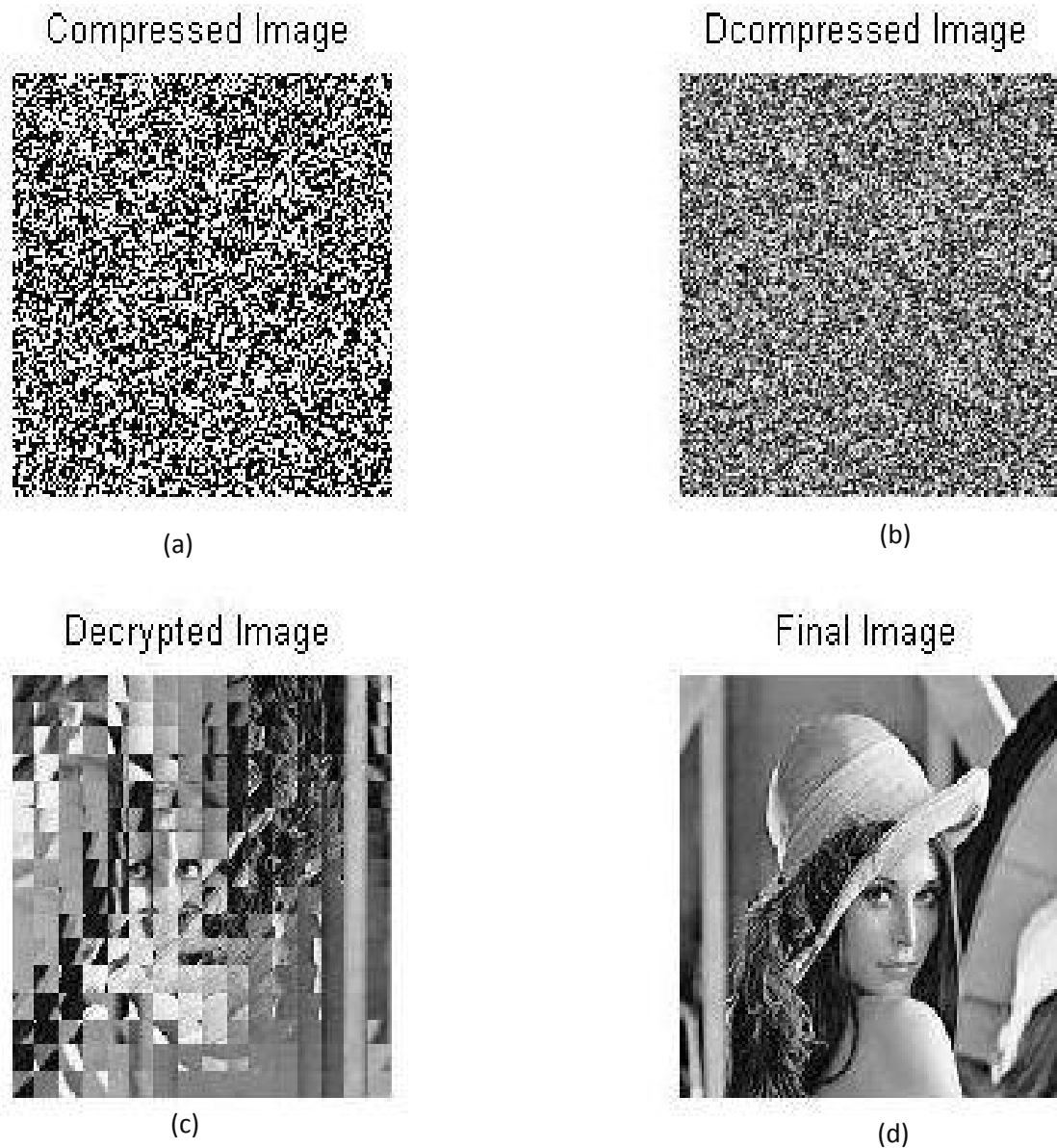


Fig. 6.3 Decryption by chaotic Logistic map.(a)Compressed image,(b)Decompressed cipher shuffled image (c) Shuffled image, (d) Output image after applying the shuffling algorithm in reverse order.

6.1 STATISTICAL ANALYSIS

6.1.1 HISTOGRAM ANALYSIS

The histogram is a graphical representation of pixel intensity of an image. There are 256 distinct probable intensities for an 8-bit grayscale image, so the histogram will graphically exhibit 256 numbers showing the dissemination of pixels amongst those grayscale images.

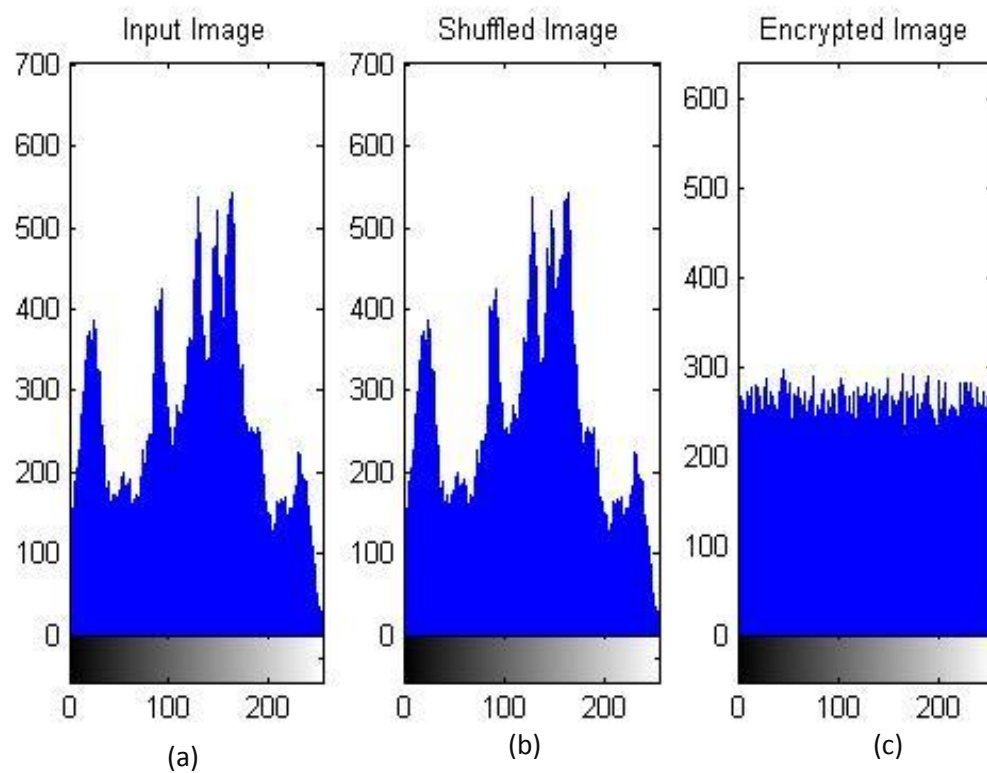


Fig. 6.4 (a), Fig. 6.4 (b) and Fig. 6.4 (c) are the histograms of original images, shuffled image and encrypted image respectively.

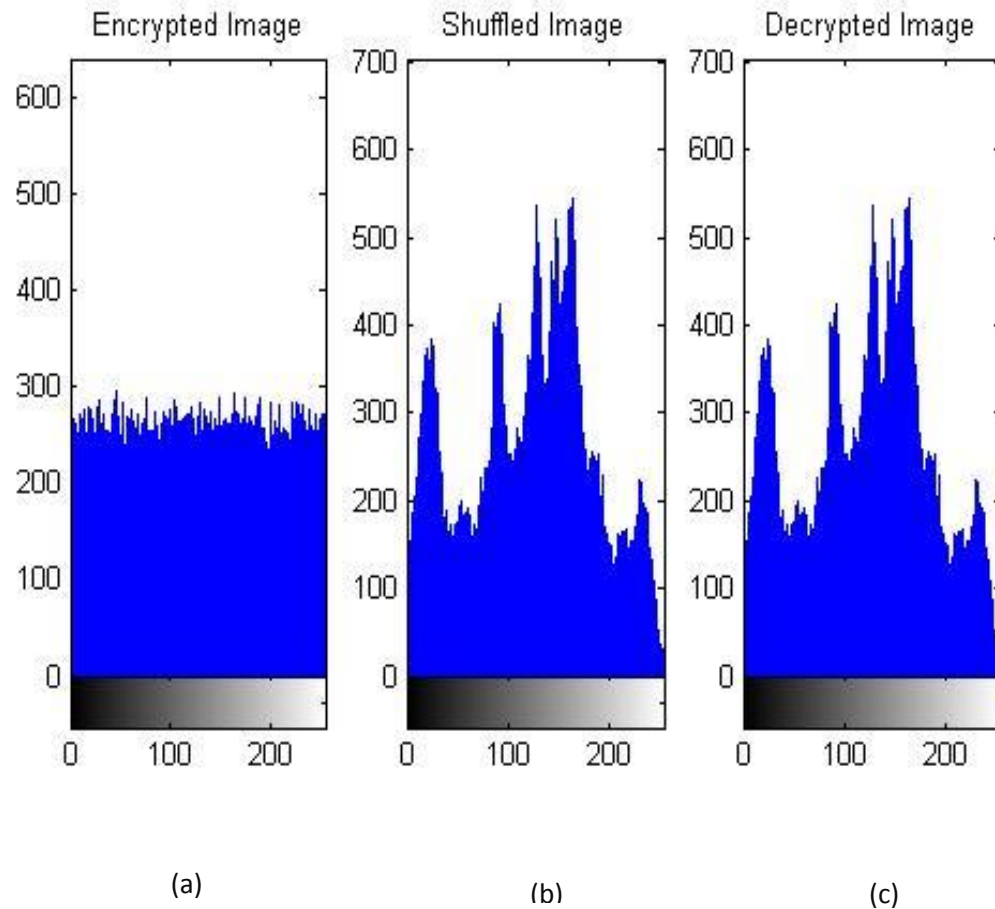


Fig. 6.5 Histogram analysis: (a) Histogram of cipher image, (b) Histogram of shuffled image, (c) Histogram of image after applying the shuffling algorithm in reverse order.

It is analyzed from Fig. 6.4, that there exists a uniform dissemination of grayscale values in cipher image, and considerably changed from histograms of the original image. In the original image some of the grayscale values do not exist in the range of 0 to 255 but in encrypted image, grayscale values exist uniformly in the range 0 to 255. Therefore, it is proved that the encrypted image does not help intruders to deploy a statistical attack on encryption technique.

6.1.2 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 measurement of randomness that can be used to depict the texture of the input image.

Entropy is defined as

$$H = -\sum (p_i \cdot \log_2(p_i)) \quad \text{eqn.(3)}$$

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

Table 2: Entropy analysis

	Input Image	Encrypted Image	Output Image
Entropy	7.8439	7.9990	7.8440

6.1.3 KEY SENSITIVITY TEST

For secure encoding, the key should be sensitive to large spaced key size to avoid every kind of conceivable attack. Randomness is the key point of the logistic map. To test the sensitivity of the key involved, a minute variation was done in original secret key by changing X_0 from 0.1 to 0.10001. As a result, it is not possible to obtain the original image at the receiver's end.

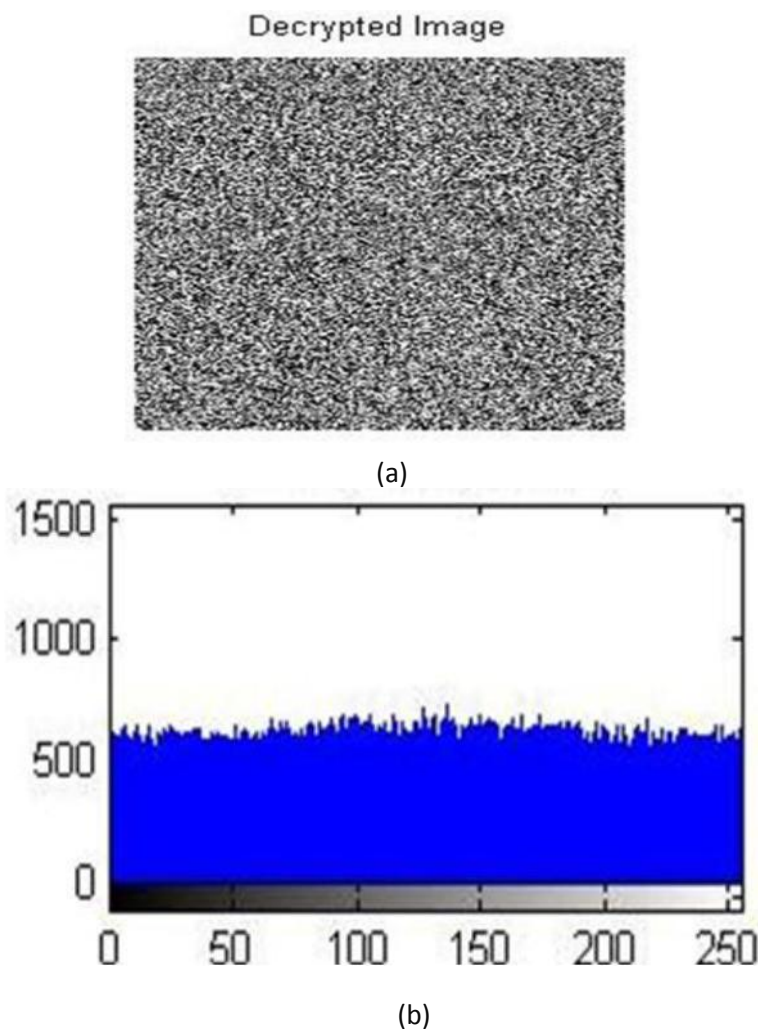


Fig. 6.6 Key sensitivity analysis: (a) Decrypted image after slight variation in key (b) histogram of decrypted image.

6.1.4 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 the uniform distribution of gray levels along all vertical lines of the encrypted image. Figure 6.7 shows the mean value obtained from the encrypted gray scale images by applying the proposed encryption method. Here red line is for the original image and the green line is for encrypted image. The mean value across the image remains nearly consistent and close to each other.

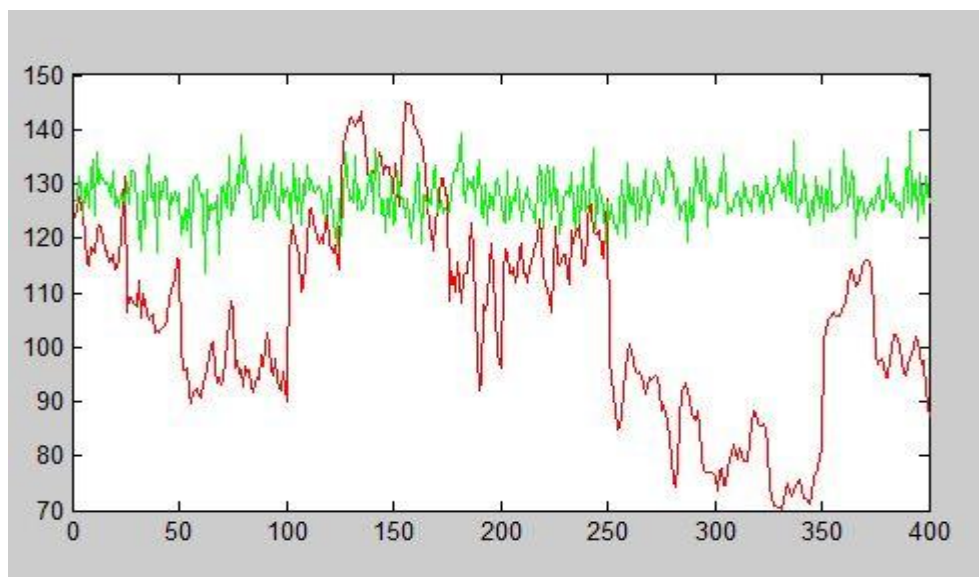


Fig. 6.7 Mean values of original image and encrypted image

6.1.5 ENCRYPTION KEY RANDOMNESS ANALYSIS

For better performance of the proposed algorithm, key values generated from chaotic maps should differ from neighboring keys to a larger extent. Here, from the figure 6.7 it's clear that following property is satisfied by the key generated using a chaotic logistic map.

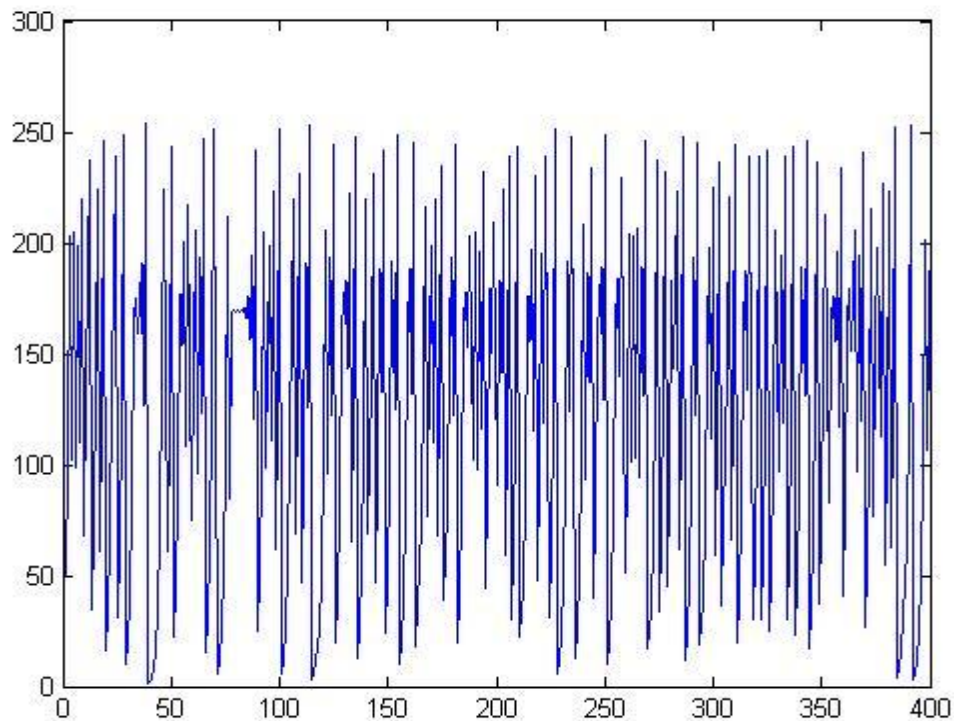











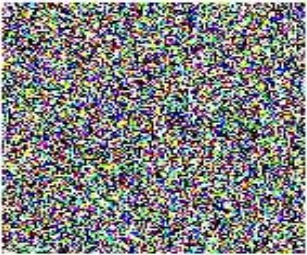









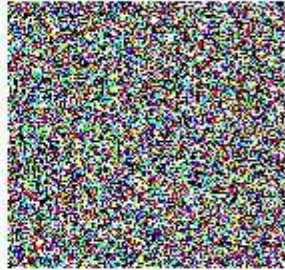




Fig. 6.8 Encryption key randomness analysis

6.2 EXPERIMENTAL RESULTS ON DIFFERENT IMAGES

Table 3: Experimental results on different images

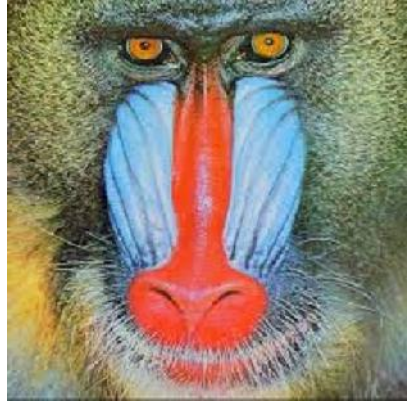


<p>Input Image</p> 	<p>Suffled Image</p> 
<p>Ciphered Image</p> 	<p>Comperessed Image</p> 
<p>Comperessed Image</p> 	<p>Decompressed Image</p> 
<p>Decrypted Image</p> 	<p>Final image</p> 

<p>Input Image</p> 	<p>Suffled Image</p> 
<p>Ciphered Image</p> 	<p>Comperessed Image</p> 
<p>Comperessed Image</p> 	<p>Decompressed Image</p> 
<p>Decrypted Image</p> 	<p>Final image</p> 

<p>Input Image</p> 	<p>Suffled Image</p> 
<p>Ciphered Image</p> 	<p>Compressed Image</p> 
<p>Compressed Image</p> 	<p>Decompressed Image</p> 
<p>Decrypted Image</p> 	<p>Final image</p> 

6.3 COMPARISON OF VARIOUS QUALITY PRAMETERS FOR ENCRYPTION USING DIFFERENT IMAGES FOR CHAOTIC MAPS

Table 4: Test images used to perform various encryption quality parameter test

6.3.1 Variation in entropy with iteration for different images

Expected entropy for a good encryption algorithm should be 8, in the image encryption process using henon map, Tent map and Logistic map its nearly 8. As the number of iterations increases in the proposed confusion process, the entropy of the encrypted image also increases.

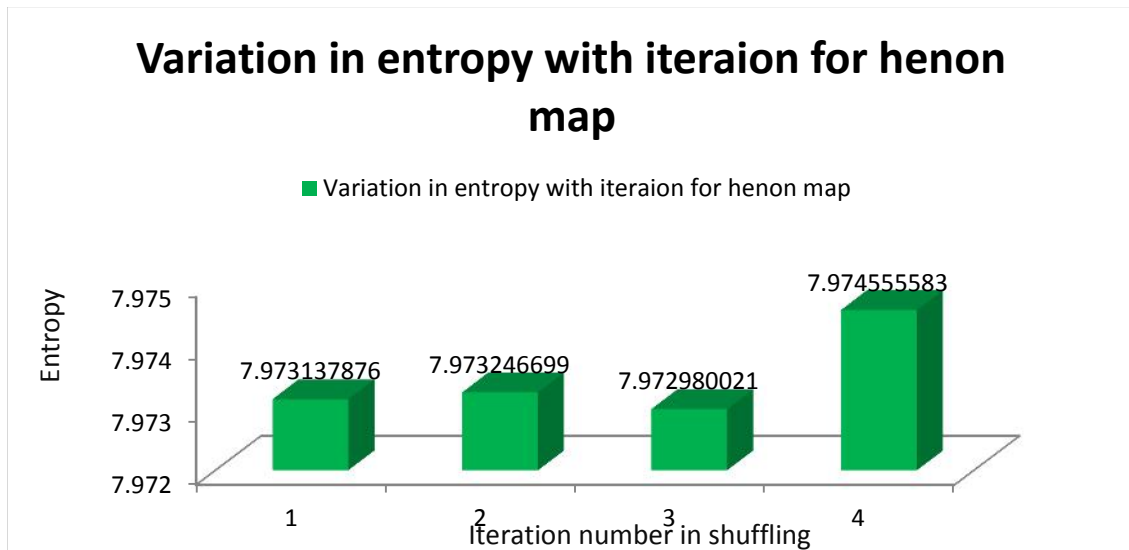


Fig. 6.9: Variation in entropy with iteration of henon map

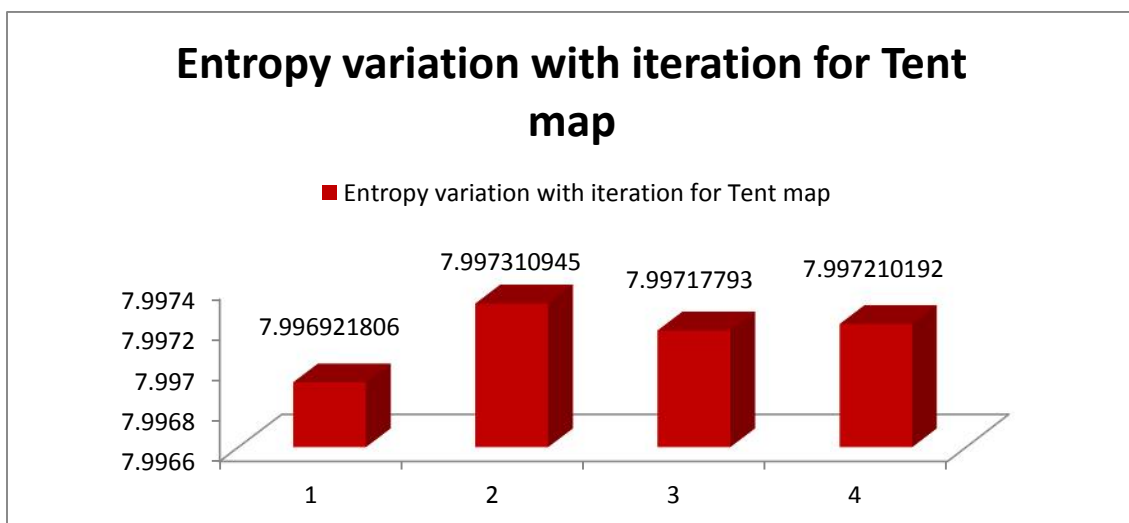


Fig. 6.10: Variation in entropy with iteration of Tent map

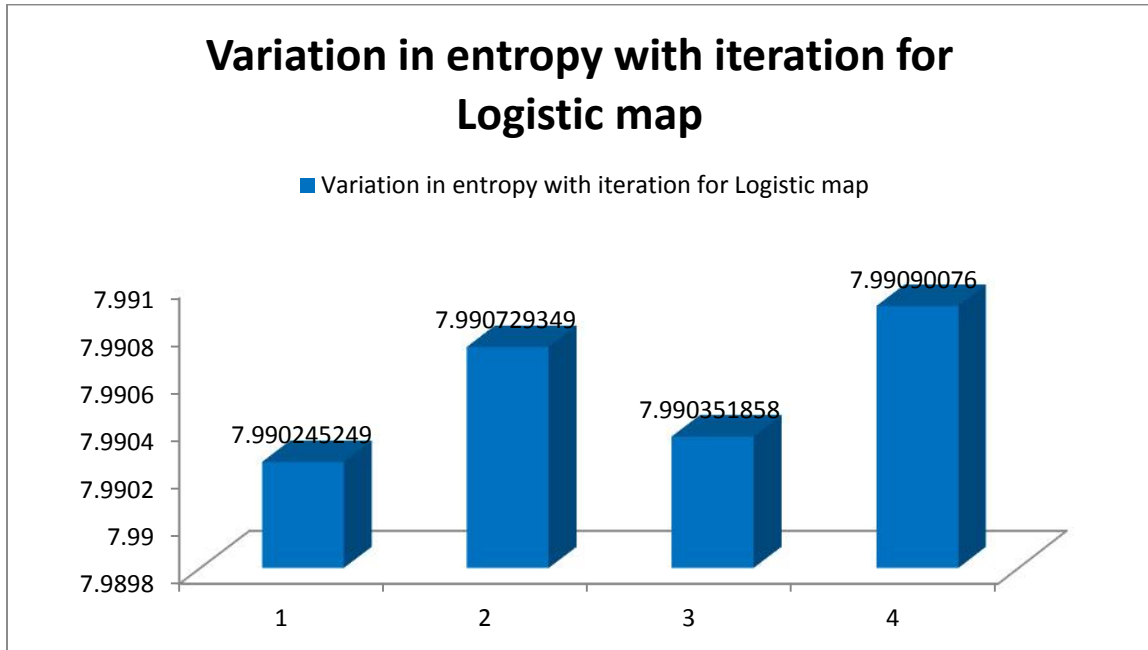


Fig. 6.11 Variation in entropy with iteration for Logistic map

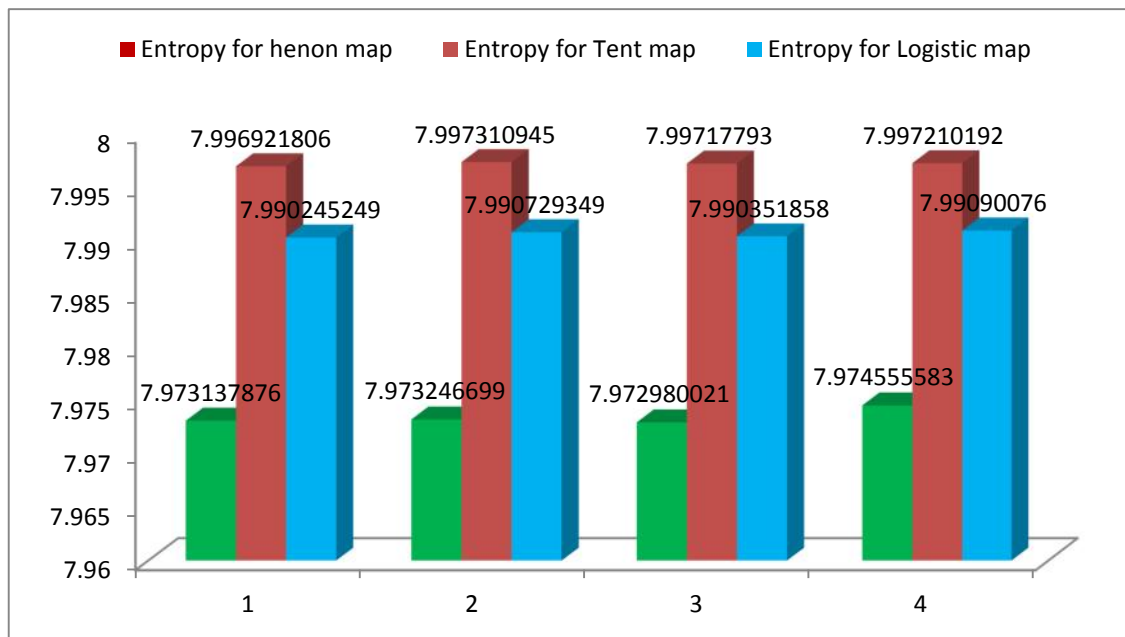


Fig. 6.12 Entropy comparison for different chaotic map

6.3.2 Mean Square Error Analysis for different chaotic maps (MSE)

Mean square error (MSE) between two images is given by the following equation

$$MSE = \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |c(i,j) - p(i,j)|^2 \right\} / (M * N)$$

Where, C(i, j) and P(i, j) are pixels of the encrypted image and input image respectively.

MSE is used to calculate Peak signal to noise ratio (PSNR). Smaller the values of PSNR, better the encryption quality of the encryption algorithms.

Table 5: MSE for different chaotic maps

IMAGE NAME	LOGISTIC MAP	TENT MAP	HENON MAP
Lena	9.11E+03	9.62E+03	9.05E+03
Baboon	5.64E+03	6.85E+003	5.17E+03
Dtu	1.97E+04	1.77E+04	1.93E+04
Camera man	9.55E+03	9.78E+03	9.04E+03
Nature	9.47E+03	9.57E+03	8.44E+03

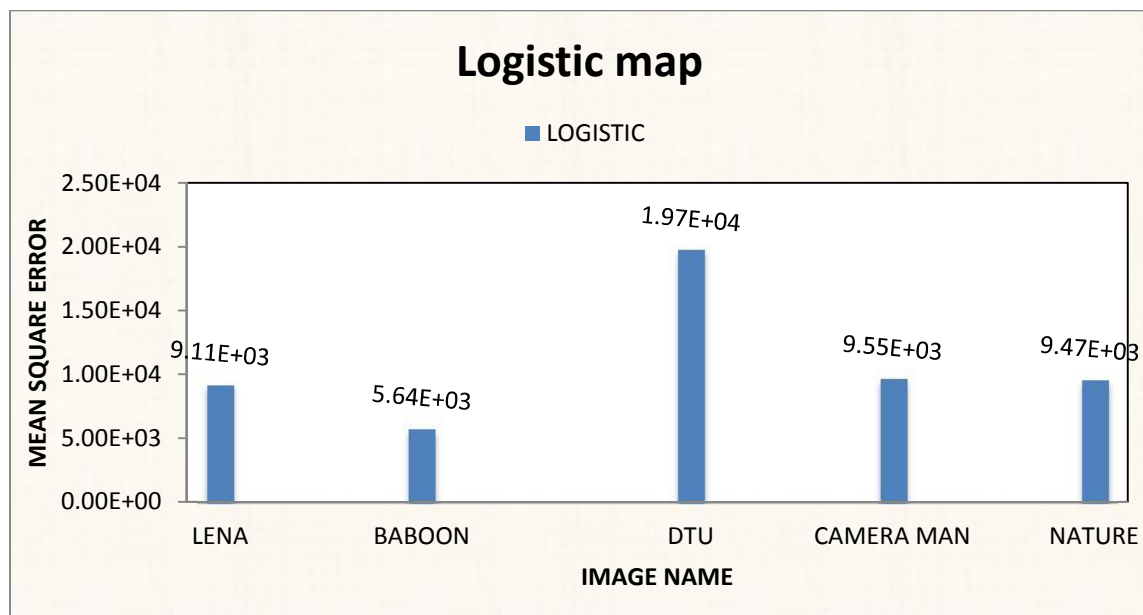


Fig. 6.13 MSE for Logistic map

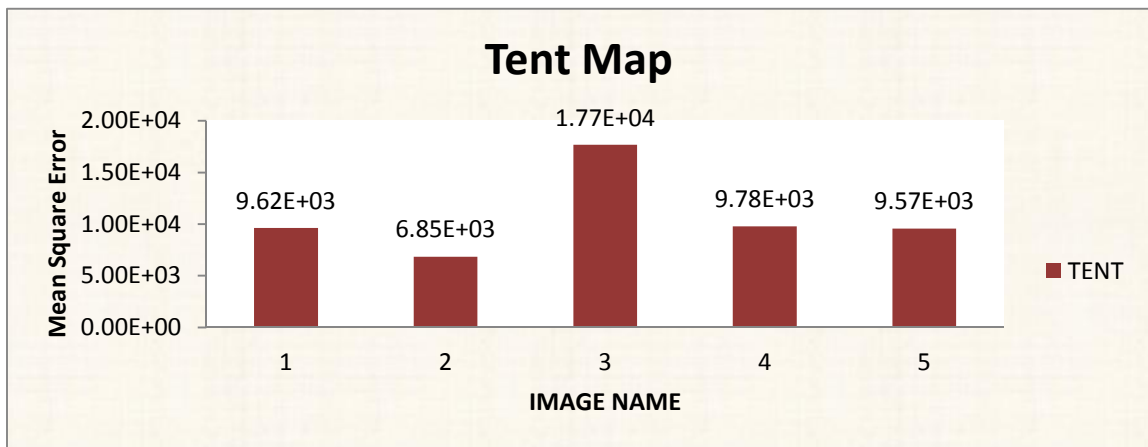


Fig. 6.14 MSE for Tent map

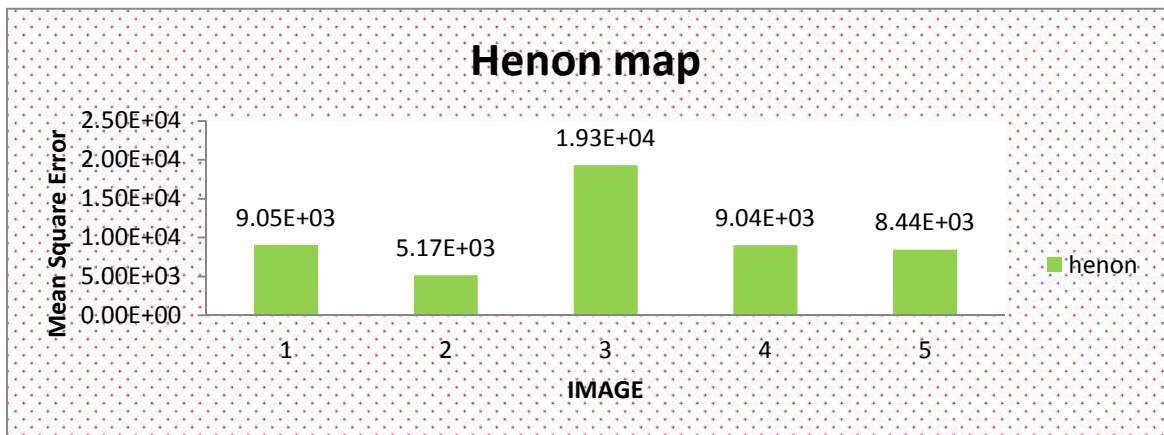


Fig. 6.15 MSE for Henon map

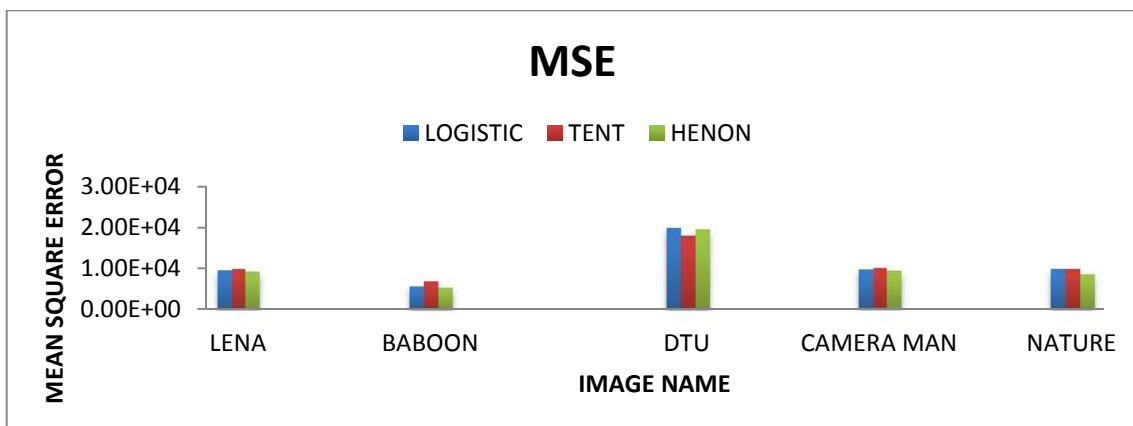


Fig. 6.16 MSE comparisons for different chaotic maps

6.3.3 Peak signal to noise ratio comparison of different chaotic maps (PSNR)

PSNR is calculated with the help of MSE. The lesser value of PSNR is expected for better image encryption.

Table 6: PSNR value comparison for different chaotic maps

IMAGE NAME	LOGISTIC MAP	TENT MAP	HENON MAP
Lena	8.5677	8.3311	8.5977
Baboon	10.655	99.80E+00	11.0271
Dtu	5.2305	5.6908	5.3043
Camera man	8.3640	8.2598	8.6027
Nature	8.4006	8.3574	8.9021

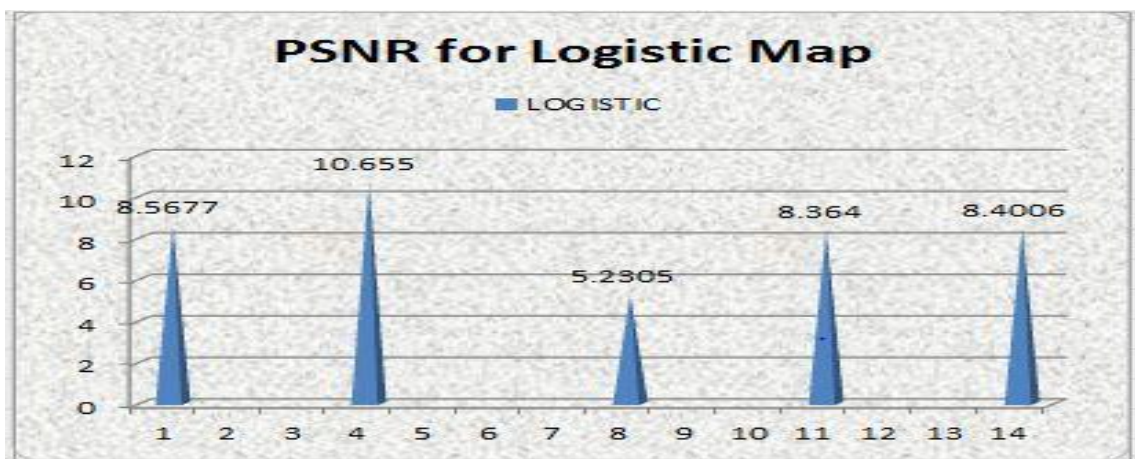


Fig. 6.17 PSNR for Logistic map

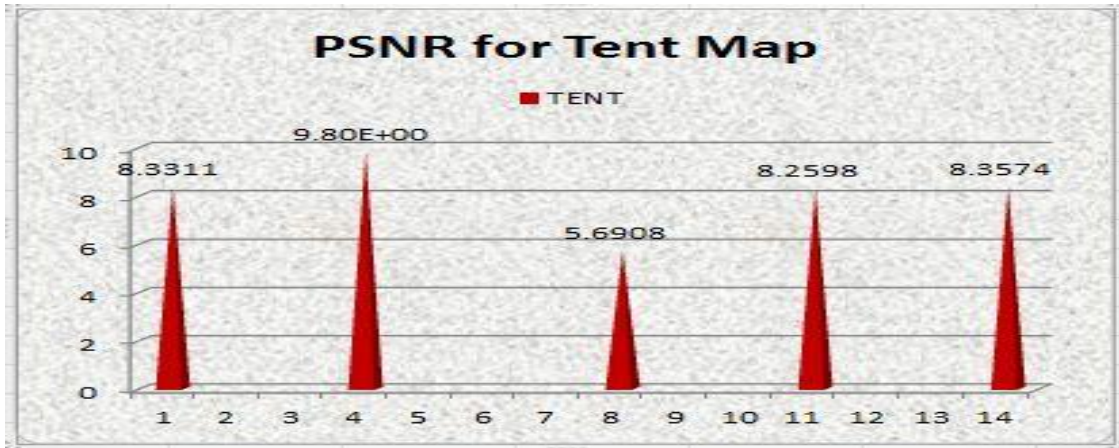


Fig. 6.18 PSNR for Tent map

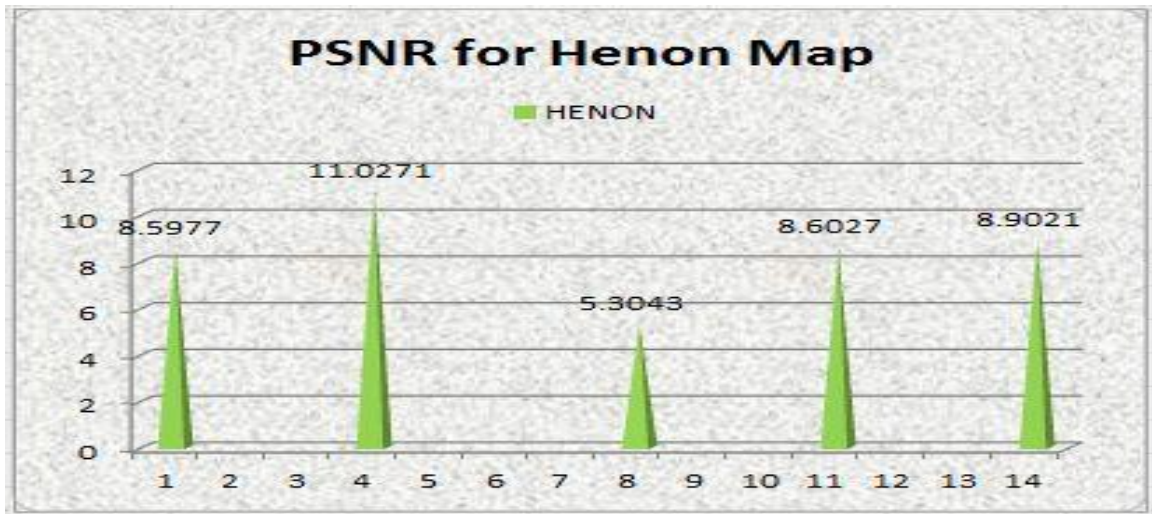


Fig. 6.19: PSNR for Henon Map

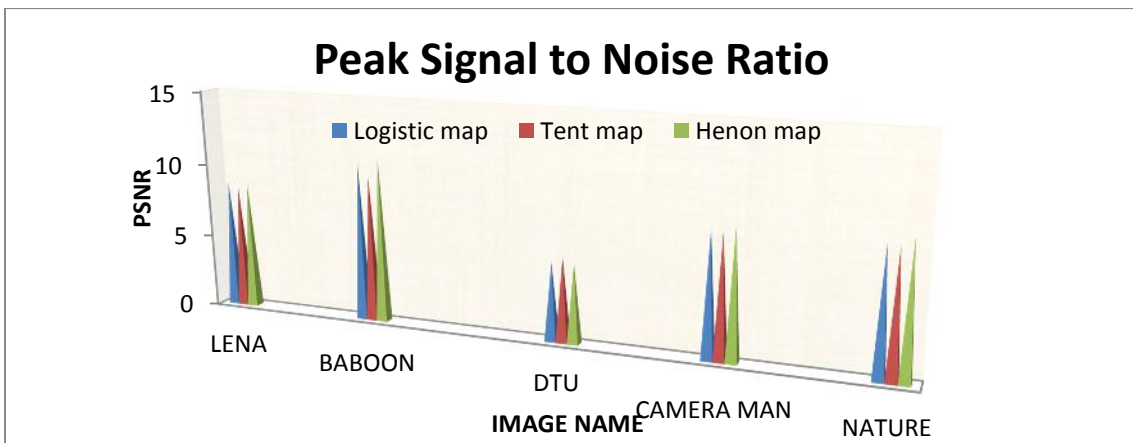


Fig. 6.20: Comparisons of PSNR for different chaotic maps

6.3.4 Unified Average Change in Intensity (UACI)

UACI is used to test the one pixel change in the encrypted image. UACI is mathematically represented by the formula

$$UACI = [\sum_{i,j} \left\{ \frac{|C1(i,j) - C2(i,j)|}{256} \right\} * 100\%] / (M * N)$$

Where, C1(i, j) and C2(i, j) are the encrypted image from the input images which have one pixel difference.

M*N is the size of the image.

Table 7: UACI value comparison for different chaotic maps

IMAGE NAME	LOGISTIC MAP	TENT MAP	HENON MAP
Lena	30.5687%	31.0516%	39.6753%
Baboon	24.0767%	27.2941%	22.7415%
Dtu	45.1275%	43.9174%	42.9872%
Camera man	31.6277%	31.2765%	30.8844%
Nature	31.4095%	31.4125%	29.1222%

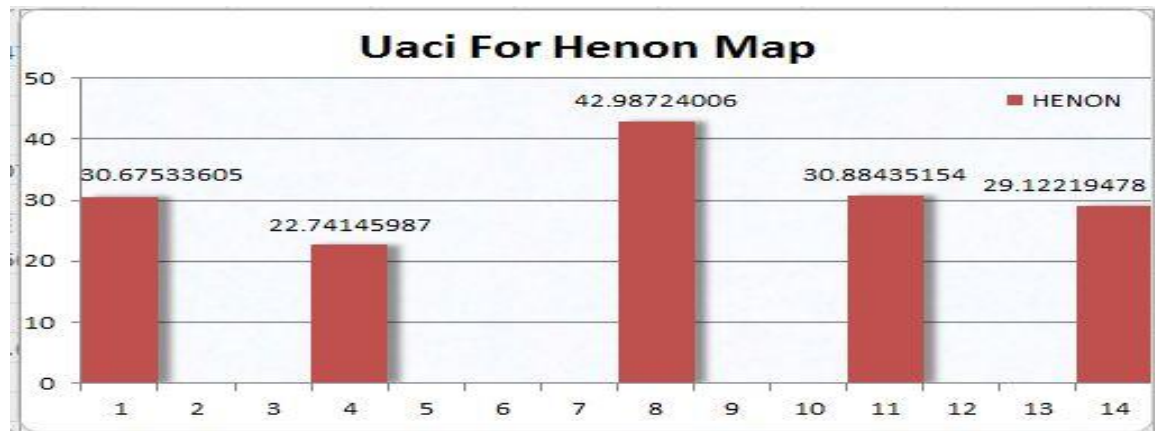


Fig. 6.21 UACI value for Henon map

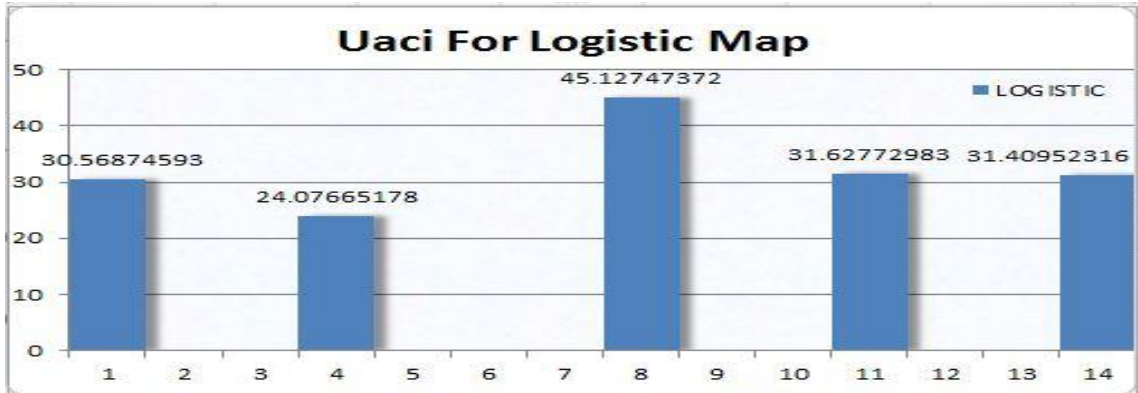


Fig. 6.22 UACI value for Logistic map

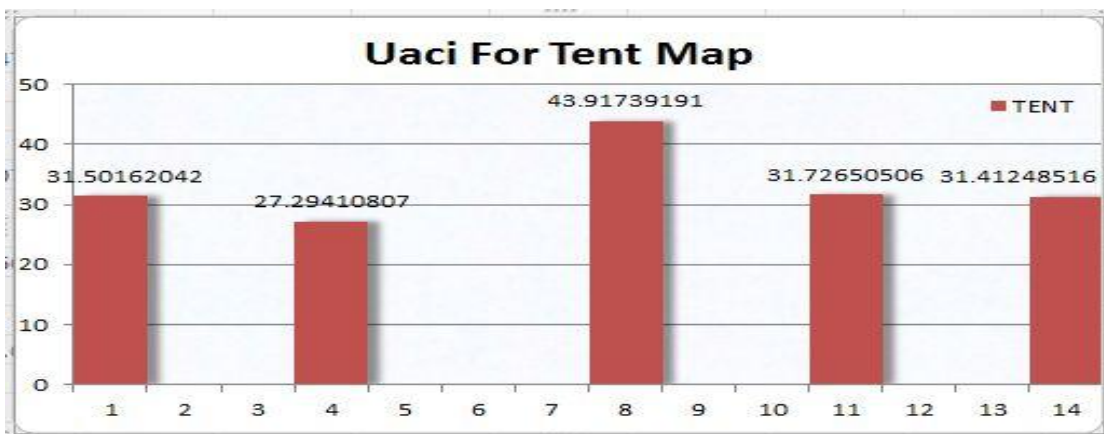


Fig. 6.23 UACI value for Tent map

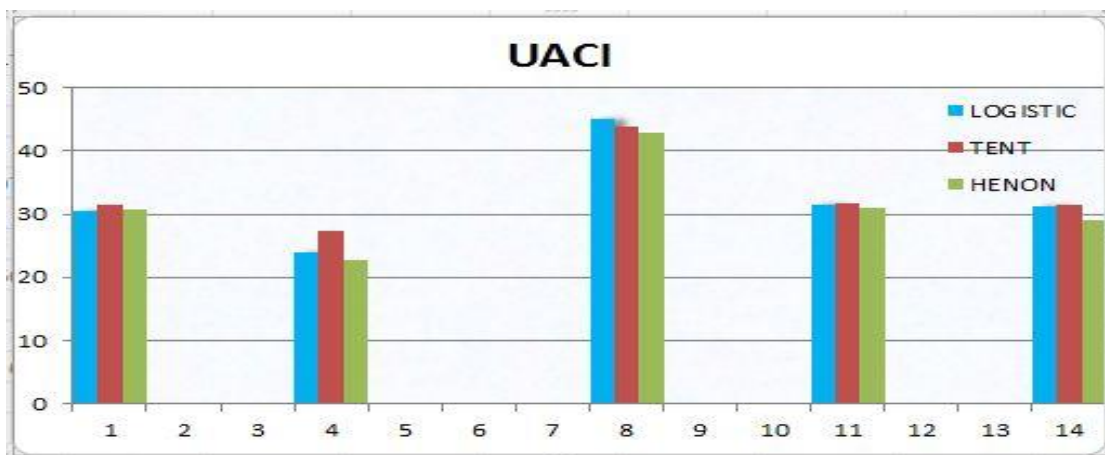


Fig. 6.24 UACI value comparison of different chaotic maps

6.3.5 Number of Pixel Change Rate (NPCR)

NPCR is the measure of change in the encrypted image, when there is one pixel change in the input image. Mathematically, NPCR is given by the equation

$$NPCR = \sum_{i,j} D(i,j) / (M \times N)$$

Where, $D(i, j) = 1$, if $\{C1(i, j) = C2(I, j)\}$

And $D(i, j) = 0$, if $\{C1(i, j) \neq C2(i, j)\}$

$C1(i, j)$ and $C2(i, j)$ are the encrypted images with one pixel difference in the input image.

$I = 0, 1, 2, \dots, M-1$.

$J = 0, 1, 2, \dots, N-1$.

$M \times N$ is the size of the input and encrypted image.

Table 8: NPCR values for different chaotic maps

IMAGE NAME	LOGISTIC MAP	TENT MAP	HENON MAP
Lena	99.5987%	99.6353%	99.5987%
Baboon	99.4720%	99.5941%	99.4812%
Dtu	99.0707%	99.6536%	88.8582%
Camera man	99.6628%	99.5728%	99.6902%
Nature	99.6048%	99.6109%	99.5178%

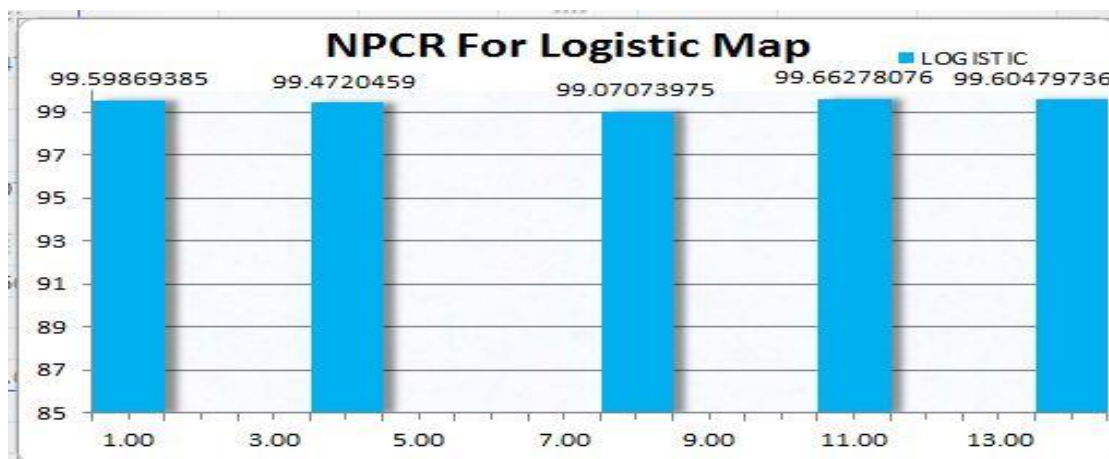


Fig. 6.24 NPCR value for Logistic map

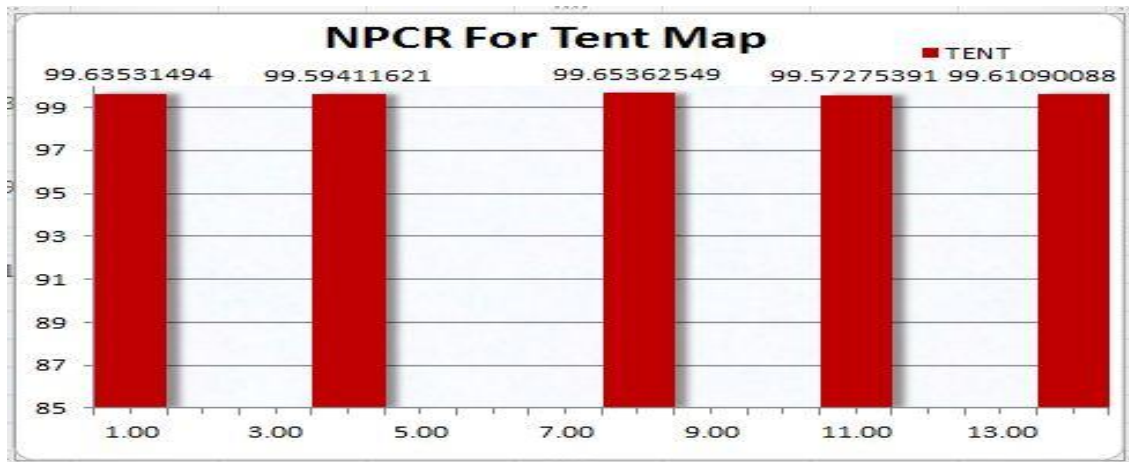


Fig. 6.25 NPCR values of Tent map

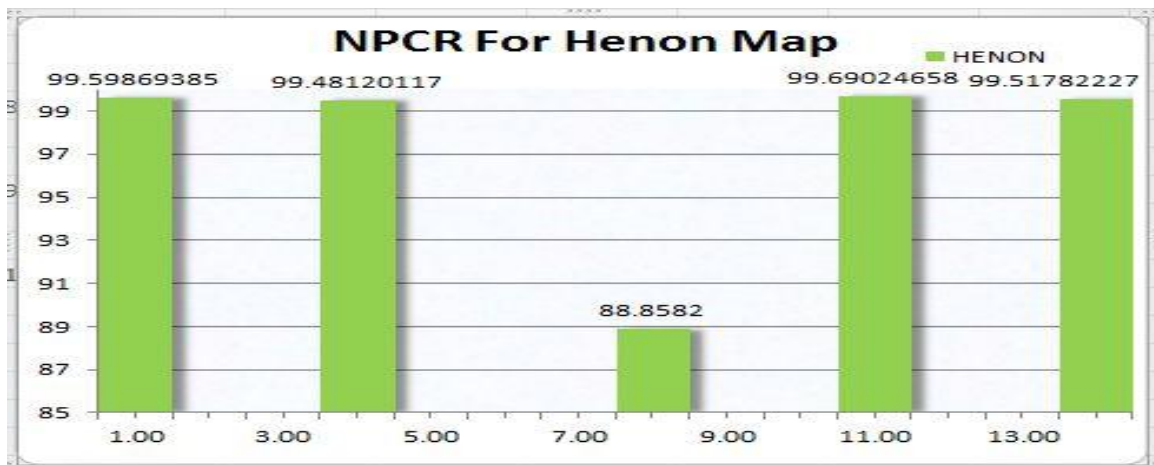


Fig. 6.26: NPCR values of Henon map

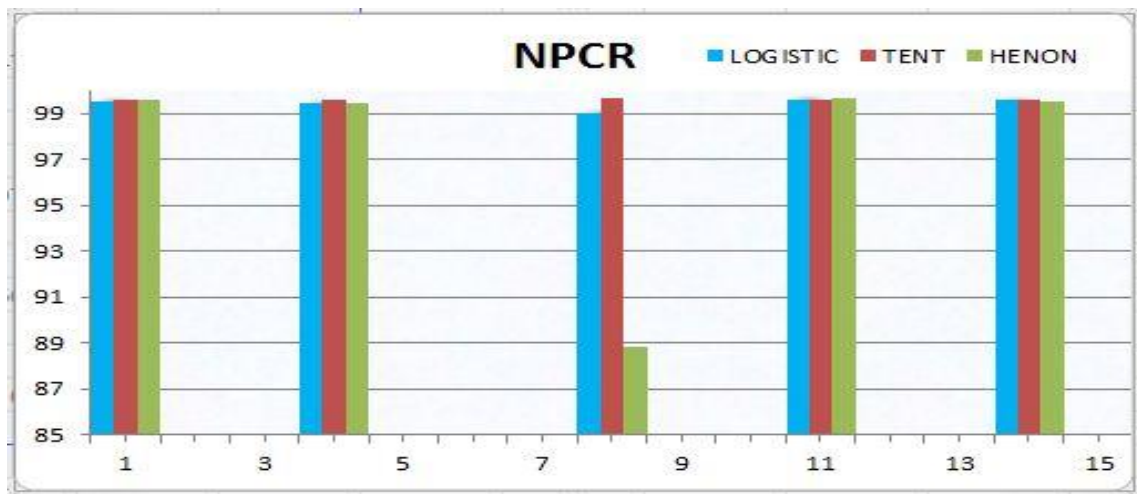


Fig. 6.27: NPCR value comparisons for different chaotic maps

6.3.6. Time complexity analysis for different chaotic map

Table 9: Time Complexity for different chaotic map

Chaotic map name	Encryption Time (in second)	Decryption Time (in second)
Logistic map	0.240	0.263
Tent map	0.090	0.217
Henon map	0.819	0.616

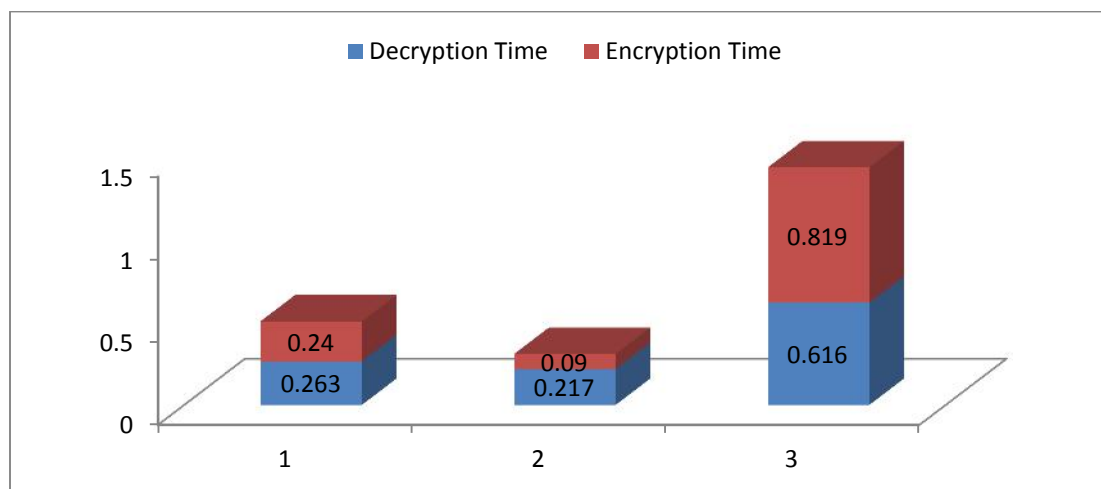


Fig. 6.28 Time complexity analysis of different chaotic map

From all the above quality parameters for image encryption, It is shown that the Tent map gives the best performance, followed by Logistic map and then it's the performance of Henon map.

CHAPTER - 7

CONCLUSION AND FUTURE WORK

7.1 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 the eavesdropper 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 from one position to a new position and diffusion is increased through a byte sequence generated through Chaotic Logistic system.

So, both the processes of increasing confusion and diffusion resulted in increasing the security of cryptosystem. A Stream cipher is achieved by performing the XOR operation between images and byte stream of the Chaotic Logistic 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 the proposed algorithm. Statistical analysis like histogram analysis, information entropy analysis, key sensitivity test, mean value analysis and key randomness analysis gives a judgmental result of encryption cryptosystem.

Proposed algorithm when run on several images indicates that this chaotic system is applicable for all kinds of images.

7.2 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 a high level of security.
- In this thesis, the proposed work is based on symmetric key cryptography. This work can be extended further for asymmetric key cryptography.
- The Chaotic Logistic system is not the only chaotic system which is dynamic. Other chaotic systems are also available which could be used in cryptography.

REFERENCES

- [1] N. S. Raghava, Ashish Kumar, "IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE", International Journal of Computer Science Engineering and Information Technology Research (IJCEITR)ISSN(P): 2249-6831; ISSN(E): 2249-7943Vol. 3, Issue 5, Dec 2013, 11-18.
- [2] Liu Chunli, Liu DongHui, "Computer Network Security Issues and Countermeasures", IEEE Symposium on Robotics and Applications (ISRA), 2012.
- [3] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition. New York: John Wiley & Sons, 1996.
- [4] Susanne Boll, "MultiTube—Where Multimedia and Web 2.0 Could Meet", IEEE Computer Society, 2007.
- [5] Lian S., DimitrisKanellopoulos, G. R., "Recent Advances in Multimedia Information System Security", Informatica 33 (2009), 2009.
- [6] Whitfield Diffie, Martin E. Hellman, "New Directions In Cryptography", IEEE Transactions On Information Theory, Vol. It-22, No. 6, November 1976.
- [7] 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.
- [8] 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.
- [9] HassenRedwan and Ki-Hyung Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", Japan-China Joint Workshop on Frontier of Computer Science and Technology, 2008.
- [10] G. Jakimoski, L. Kocarev, "Block encryption ciphers based on chaotic maps", IEEE Transaction on Circuits System-I, 48 (2002) 163-169.
- [11] Menezes A., P.V. Oorschot, S. Vanstone, Handbook of Applied Cryptography", FL: CRC Press, Boca Raton, 1997.
- [12] Diffie w. Bell-Northern Res., Mountain View, CA, USA, "The first ten years of publickey cryptography", Proceedings of the IEEE (Volume: 76, Issue: 5).

- [13] 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.
- [14] 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.
- [15] http://www.ieeeeghn.org/wiki/index.php/Cryptography#Classical_cryptography
- [16] Lamba, C.S. "Design and Analysis of Stream Cipher for Network Security", Communication Software and Networks, 2010. ICCSN '10.
- [17] G. Jakimoski and L. Kocarev., "Analysis of recently proposed chaos-based encryption Algorithm", Physics Letters, A, 2001.
- [18] 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
- [19] Matthews R., "On the derivation of a chaotic encryption algorithm," Cryptologia 1989;8(1):29–41, 1989.
- [20] Wikipedia,Chaos theory,http://en.wikipedia.org/w/index.php?title=Chaos_theory&oldid=264934743.
- [21] Kocarev L., "Chaos-based cryptography: a brief overview overview", Circuits and Systems Magazine, IEEE, 2001. 1(3): p. 6.
- [22] 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.
- [23] 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.
- [24] G. Jakimoski, L. Kocarev., "Analysis of recently proposed chaos-based encryption algorithm", Physics Letters,A,2001.
- [25] 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.

- [26] 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.
- [27] Alligood K.T., T.D. Sauer, J.A. Yorke, "Chaos an Introduction to Dynamical Systems", First ed. 1996, New York: Springer-Verlag.
- [28] 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.
- [29] Parker T.S. and L.O. Chua, "Practical Numerical Algorithms for Chaotic Systems", Firsted. 1989,New York Berlin Heidelberg: Springer-Verlag New York Inc.
- [30] <http://www.imho.com/grae/chaos/chaos.html>.
- [31] Kocarev L., "Chaos-based cryptography: a brief overview". Circuits and Systems Magazine", IEEE, 2001. 1(3): p. 6.
- [32] Muhammad KhurramKhan, Jiashu Zhang, "Investigation on Pseudorandom Properties of Chaotic Stream Ciphers," IEEE, 2006.
- [33] X. Wang, Y.L.Y., H. Yu, "Finding collisions in the full SHA1", Eurocrypt 2005, 2005.
- [34] 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.
- [35] 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.
- [36] 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.
- [37] Hazarika, N., Saikia, M., "A Novel Partial Image Encryption using Chaotic Logistic Map", Signal Processing and Integrated Networks (SPIN), 2014

- International conference on digital signal processing. 10.1109/SPIN.2014.6776953, pp. 231- 236.
- [38] Qiu Run-he, Cao Yun, Fu Yu-Zhen, “Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption” 2011 4th International Congress on Image and Signal Processing. 10.1109/CISP.2011.610030, pp. 629-632.
- [39] Hongjun Liu, Xingyuan Wang, “Triple-image encryption scheme based on one-time key stream generated by chaos and plain images”, Journal of Systems and Software, Volume 86, Issue 3, March 2013, pp. 826-834.
- [40] Yunpeng Zhang Fei Zuo, Zhengjun Zhai, CAI Xiaobin, “A New Image Encryption Algorithm Based on Multiple Chaos System ”, International Symposium on Electronic Commerce and Security. 10.1109/ISECS.2008.142, pp. 347-350.
- [41] Tiegang Gao, QiaoLun GU, Zengqiang Chen, Renhong Cheng, “An Improved Image Encryption Algorithm Based on Hyper-chaos*”, 2009 Fourth International Conference on Innovative Computing, Information and Control 10.1109/ICICIC.2009.88, pp. 1281-1284.
- [42] N. K. Pareek, Vinod Patidhar and K.K. Sud “Image encryption using chaotic logistic map”, Image and Vision Computing 24 (2006) 926-934, received 10 August 2004; received in revised form 11 August 2005; accepted 6 February 2006.
- [43] Weihai Li, Nenghai Yu, “A ROBUST CHAOS-BASED IMAGE ENCRYPTION SCHEME”, Multimedia and Expo, 2009.ICME2009.IEEE International Conference. 10.1109/ICME.2009.5202674, pp. 1034-1037.
- [44] Ashtiyani, M., Electr. Eng. Dept., IHU, Tehran, Birgani, P.M., Hosseini, H.M., “Chaos-Based Medical Image Encryption Using Symmetric Cryptography”, Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008, 10.1109/ICTTA.2008.4530291, pp 1-5.
- [45] WANG Juan, “Image Encryption Algorithm Based on 2-D Wavelet Transform and Chaos Sequences”, Computational Intelligence and Software Engineering, 2009. CiSE 2009, 10.1109/CISE.2009.5362955, pp. 1-3

- [46] Guosheng Gu, Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm", *Innovative Computing, Information and Control*, 2006.ICICIC '06, 10.1109/ICICIC.2006.46, pp.492-495.
- [47] Hegui Zhu, Cheng Zhao, Xiangde Zhang, "A novel image encryption-compression scheme using hyper-chaos and the Chinese remainder theorem", *Signal Processing: Image Communication*, Volume 28, Issue 6, July 2013, pp. 670-680
- [48] Gan Yu, Yongjun Shen; Guidong Zhang; Yanhua Yang, "A Chaos-based Color Image Encryption Algorithm", *Computational Intelligence and Design (ISCID)*, 10.1109/ISCID.2013.13, pp. 92-95.
- [49] Miles E. Smland Dennis K. Branstad, "The Data Encryption Standard: Past and Future", *Proceedings of the IEEE*, VOL. 76, NO. 5, MAY 1988.
- [50] Poincaré J.H., *Sur le problème des trois corps et les équations de la dynamique. Divergence des séries de M. Lindstedt* *Acta Mathematica*, 1890. 13: p. 1-270,
- [51] Alligood K.T., T.D. Sauer, and J.A. Yorke, "Chaos an Introduction to Dynamical Systems", First ed. 1996, New York: Springer-Verlag.
- [52] 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.
- [53] Wolfram S. "Cryptography with cellular automata", in *Advances in Cryptology - Crypto'85, Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 1985.
- [54] 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.
- [55] K. Wang, W. Pei, "On the security of 3D Cat map based symmetric image encryption scheme", *Physics Letters A.*, pp. 432-439, May. 2005.
- [56] 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.
- [57] 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.

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