Chapter1
Introduction

1.1Overview

The presence of computer networks has prompted new problems with security and privacy. Having a secure and reliable means for communicating with images and video is becoming a necessity and its related issues must be carefully considered. Hence, network security and data encryption have become important. The images can be considered nowadays, one of the most usable forms of information. Image and video encryption have applications in various fields including Internet communication, multimedia systems, medical imaging, telemedicine and military communication. There are two types of applications for information transmission over the Internet. The first ones are the online applications, which consider the speed as the main issue. The second ones are web pages, which consider the security as the main issue.

We are living in the information age; we need to keep information about every aspect for our lives. In other words, information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. During the last two decades, computer networks created a revolution in the use of information. Authorized people can send and receive information from a distance using computer networks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity, when it is needed (availability). Although the three previously mentioned requirements have not changed, they now have some new dimensions. Not only should information be confidential, when it is stored in a computer; there should also be away to maintain its confidentiality, when it is transmitted from one computer to another. Information transmitted over computer networks nowadays is not only text, but also audio, image, and other multimedia types. The field of multimedia security has matured in the last decade to provide a class of tool-sets and design insights for the protection and enhancement of digital media under a number of diverse attack scenarios. Research in multimedia security was first motivated, in part, by the increasing use of digital means to communicate, store and represent

entertainment information such as music and video. The digital form allowed the perfect duplication of information and almost seemless manipulation and tampering of the data. This created new types of security attacks not (as seriously) addressed in the past by the entertainment industry. The paradigm shift from analog to digital multimedia for entertainment has had an enormous impact for artists, publishers, copyright holders and consumers alike providing flexible and more accessible business models. In such a setting, one natural question that arises is the security and confidentiality of a digital packet of multimedia information.

1.2 Research Motivations

In the digital world nowadays, the security of digital image has become more and more important because of the advances in communication technology and multimedia technology. We can realize that more and more researches have been developed for security issues to protect the data from possible unauthorized instructions. The security of digital images involves several different aspects, including copyright protection, authentication, confidentiality, and access control. Generally, the copyright protection is addressed by digital watermarking, which embeds the owner's private information, called the watermark, into the original image and extracts it from a questionable image when the ownership needs to be resolved. On the other hand, content confidentiality and access control are addressed by encryption, through which only authorized parties holding decryption keys can access content in clear text. In this regard, a direct solution is to use an encryption algorithm to encrypt the data, directly. This solution has led to the number-theory-based encryption algorithms such as the Data Encryption Standard (DES), AES, which is a symmetric encryption algorithms and the RSA algorithm, developed by Rivest, Shamir and Adleman, which is an asymmetric encryption algorithm. However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as the bulk data capacity and high redundancy, which are troublesome for traditional encryption. Moreover, these encryption schemes require extra operations on compressed image data, thereby demanding long computational time and high computing power. In real-time communications, due to their low encryption and decryption speeds, they may introduce significant latency. Innovative encryption techniques need to be developed for effective data encryption

for financial institutions, E-commerce, and multimedia applications. For future Internet applications on wireless networks, encryption techniques for multimedia applications need to be studied and developed. In this thesis, we focus on the subject of image encryption.

1.3 Basic Concepts of Cryptography

Image security is based on cryptography. In fact, some basic concepts from cryptography are used as building blocks (primitives) for applications in image security.

1.3.1 Goals of Cryptography

Cryptography is a study of techniques (called cryptosystems) that are used to accomplish the following four goals:

- Confidentiality
- Data integrity
- Authentication
- Non-repudiation.

A study of techniques used to break existing cryptosystems is called *Cryptanalysis*. Since cryptography and cryptanalysis are greatly dependent on each other, people refer to *cryptology* as a joint study of cryptography and cryptanalysis. Now Let us try to understand all four goals of cryptography.

Confidentiality refers to the protection of information from unauthorized access. An undesired communicating party, called adversary must not be able to access the communication material. This goal of cryptography is a basic one that has been always addressed and enforced throughout the history of cryptographic practice.

Data integrity ensures that information has not been manipulated in an unauthorized way. If the information is altered, all communicating parties can detect this alteration.

Authentication methods are studied in two groups; entity authentication and message authentication. Entity authentication is the process whereby one party is assured of the identity of a second party involved in a protocol, and that the second has actually participated immediately prior to the time the evidence is acquired. Message

authentication is a term used analogously with data origin authentication. It provides data origin authentication with respect to the original message source and data integrity, but no uniqueness and timeliness guarantees.

Non-repudiation means that the receiver can prove to everyone that the sender did indeed send the message; i.e., the sender cannot claim that he or she didn't encrypt and/or sign certain digital information.

Fortunately, modern cryptography has developed techniques to handle all four goals of cryptography.

1.3.2 Principles of Encryption

The basic idea of *encryption* is to modify the message in such a way that only a legal recipient can reconstruct its content. A discrete-valued cryptosystem can be characterized by:

a set of possible plaintexts, P.

a set of possible ciphertexts, C.

a set of possible cipher keys, K.

a set of possible encryption and decryption transformations, E and D.

An encryption system is also called a cipher, or a cryptosystem. The message for encryption is called plaintext, and the encrypted message is called ciphertext. Denote the plaintext and the ciphertext by P and C, respectively. The encryption procedure of a cipher can be described as:

$C = E_{Ke}\ (P)$

where K_e is the encryption key and E is the encryption function. Similarly, the decryption procedure is defined as:

$P = D_{Kd}\, C$

where K_d is the decryption key and D is the decryption function. The security of a cipher should only rely on the decryption key, since an adversary can recover the

plaintext from the observed ciphertext once he gets K_d. Fig. 1.1 shows a block diagram for encryption/decryption of a cipher.

Fig. 1.1 Encryption/Decryption of a cipher

1.4 Classification of Encryption Algorithms

Encryption algorithms can be classified in different ways; according to structures of the algorithms, according to keys, or according to the percentage of the data encrypted.

1.4.1 Classification According to Encryption Structure

Encryption algorithms can be classified according to encryption structure into block ciphers and stream ciphers.

A block cipher is a type of symmetric-key encryption algorithms that transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length. The fixed length is called the block size. For many block ciphers, the block size is 64 or 128 bits. The larger the block size is, the more secure is the cipher, but the more complex are the encryption, decryption algorithms and devices. Modern block ciphers have the following features:

1. Variable key size.

2. Mixed arithmetic operations, which can provide non-linearity.

3. Data-dependent rotations and key-dependent rotations.

4. Lengthy key schedule algorithm.

5. Variable plaintext/ciphertext block sizes and variable number of rounds.

Block ciphers can be characterized by:

1. Block size. Larger block sizes mean greater security.

2. Key size. Larger key sizes mean greater security.

3. Number of rounds. Multiple rounds increase security.

4. Encryption modes. They define how messages larger than the block size are encrypted.

Unlike block ciphers that operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits. So, stream ciphers can be designed to be exceptionally fast, much faster than a typical block cipher. Generally, a stream cipher generates a sequence of bits as a key (called keystream) using a Pseudo Random Number Generator (PRNG) that expands a short secret key (e.g., 128-bits) into a long string (keystream) (e.g., 106 bits), and the encryption is accomplished by combining the keystream with the plaintext. Usually, the bitwise XOR operation is chosen to perform ciphering, basically for its simplicity. Stream ciphers have the following properties:

1. They don't have perfect security.

2. Security depends on the properties of the PRNG.

3. The PRNG must be unpredictable; given consecutive sequence of output bits,the next bit must be hard to predict.

4. Typical stream ciphers are very fast.

Today, there is no stream cipher that has emerged as a standard. The most widely used stream cipher is the RC4. The stream ciphers may be employed in many applications such as in Transport Layer Security (TLS), Wired Equivalent Privacy (WEP).

1.4.2 Classification According to Keys

According to keys, there are two kinds of ciphers following the relationship of Ke and Kd . When $Ke = Kd$, the cipher is called a private-key cipher or a symmetric cipher. For private-key ciphers, the encryption/decryption key must be transmitted from the sender to the receiver via a separate secret channel. When $Ke = Kd$, the cipher is

called a public-key cipher or an asymmetric cipher. For public-key ciphers, the encryption key *Ke* is published and the decryption key *Kd* is kept private, for which no additional secret channel is needed for key transfer. In conventional encryption as shown in Fig. 1.2, the sender encrypts the data (plaintext) using the encryption key and the receiver decrypts the encrypted data (ciphertext) into the original data (plaintext) using the decryption key. In symmetric encryption, both encryption and decryption keys are identical. Fig. 1.3 shows the public key encryption (asymmetric encryption), in which the encryption and decryption keys are different. Instead of one key, there are two different keys; a public (*Ke*) and a private (*Kd*). Public key cryptography solves the problem of conventional cryptosystems by distributing the key. Table 1.1 shows a comparison between symmetric encryption and asymmetric encryption.

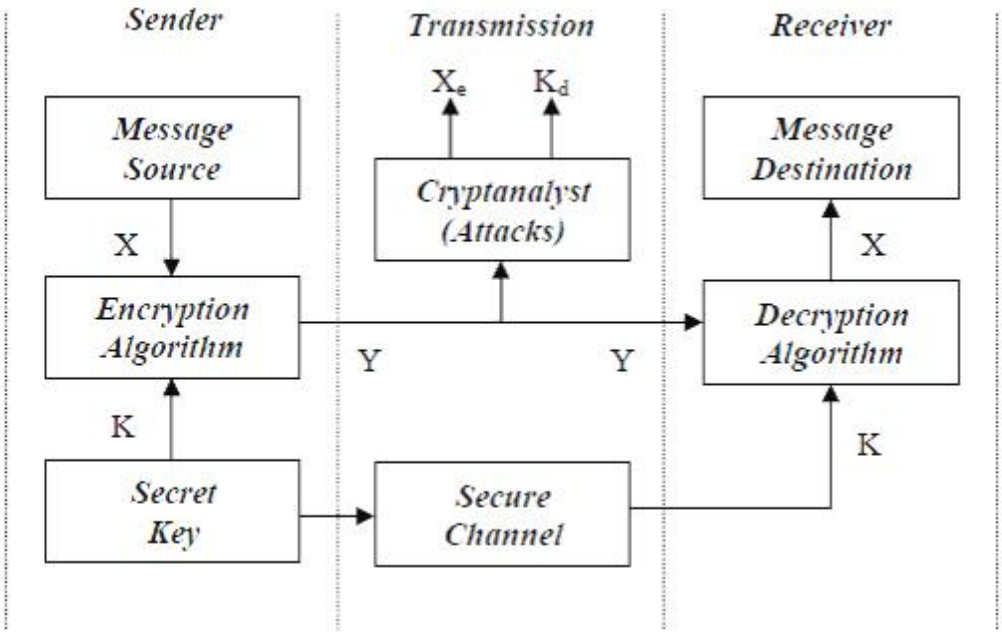


Figure 1.2: Model of symmetric encryption.

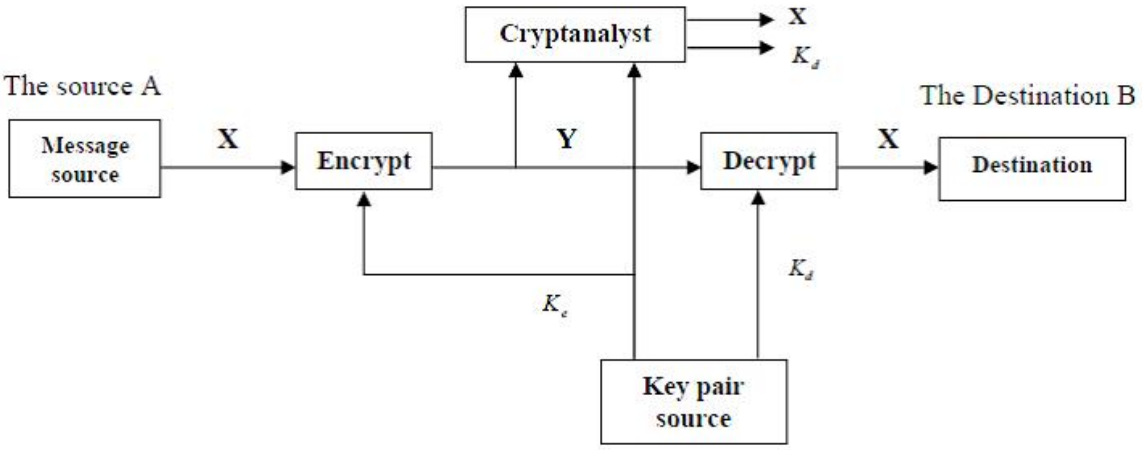


Fig. 1.3 Asymmetric key encryption

In general, there are two types of cryptosystems:

(1) Symmetric (private) key cryptosystems.

(2) Asymmetric (public) key cryptosystems.

Most people have chosen to call the first group simply symmetric key cryptosystems, and the popular name for the second group is just public key cryptosystems.

Table 1.1. Comparison between symmetric encryption and asymmetric encryption

Conventional Encryption (Symmetric Encryption)	Public-key Encryption (Asymmetric Encryption)
requirements to work: 1. The same algorithm with the same key can be used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	requirements to work: 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys.
requirements for security: 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no	requirements for security: 1. the decryption key must be kept secret. 2. It must be impossible or at least

other information is available. 3. Knowledge of the algorithm plus samples of the ciphertext must be insufficient to determine the key.	impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm, the encryption key and samples of the ciphertext must be insufficient to determine the decryption key.

1.4.3 Classification According to Percentage of Encrypted Data

With respect to the amount of encrypted data, the encryption can be divided into full encryption and partial encryption (also called selective encryption), according to the percentage of the data encrypted.

1.5 Cryptanalysis

Cryptanalysis is the art of deciphering an encrypted message as a whole or in part, when the decryption key is not known. Depending on the amount of known information and the amount of control over the system by the adversary (cryptanalyst), there are several basic types of cryptanalytic attacks. Some of the most important ones, for a system implementer, are described below and they are summarized in Table 1.2.

Cipher text-only attack. The adversary only has access to one or more encrypted messages. The most important goal of a proposed cryptosystem is to withstand this type of attacks.

Brute force attack: This is a type of ciphertext-only attacks. It is based on exhaustive key search, and for well-designed cryptosystems should be computationally infeasible.

Known-plaintext attack: In this type of attacks, an adversary has some knowledge about the plaintext corresponding to the given ciphertext. This may help him to determine the key or a part of the key.

Chosen-plaintext attack: Essentially, an adversary can feed the chosen plaintext into the black box that contains the encryption algorithm and the encryption key. The black box spits out the corresponding ciphertext, and the adversary may use the

accumulated knowledge about the plaintext - ciphertext pairs to obtain the secret key or at least a part of it.

Chosen-ciphertext attack: Here, an adversary can feed the chosen ciphertext into the black box that contains the decryption algorithm and the decryption key. The black box produces the corresponding plaintext, and the adversary tries to obtain the secret key or a part of the key by analyzing the accumulated ciphertext – plaintext pairs.

Type of attacks	Pre-requisites for the cryptanalyst
Ciphertext only	1- Encryption algorithm. 2- Ciphertext to be decoded
Known plaintext	1- Encryption algorithm. 2- Ciphertext to be decoded. 3- Plaintext message together with its corresponding ciphertext generated with the secret key.
Chosen ciphertext	1- Encryption algorithm. 2- Ciphertext to be decoded. 3- Reported ciphertext chosen by cryptanalyst together with its corresponding plaintext generated with the decryption algorithm and the decryption key.
Chosen plaintext	1- Encryption algorithm. 2- Ciphertext to be decoded. 3- Reported plaintext chosen by cryptanalyst together with its corresponding ciphertext generated with the encryption algorithm and the encryption key.

1.6 Chaos and Its Use in Cryptography

Chaos theory has been established since 1970s in many different research areas, such as physics, mathematics, engineering, and biology, etc. The most well known characteristics of chaos are the so called "butterfly-effect" (sensitivity to initial conditions), and the pseudo-randomness generated by deterministic equations. (Many fundamental properties of chaotic systems have their corresponding counterparts in

traditional cryptosystems. Chaotic systems have several significant features favourable to secure communications, such as ergodicity, sensitivity to initial conditions, control parameters and random like behavior. With all these advantages, scientists expected to introduce new and powerful tools of chaotic cryptography. So, chaos may become a new rich source of new ciphers.

1.6.1 Similarity between Chaos and encryption

Figure 1.4 summarizes similarities and differences between chaotic maps and cryptographic algorithms. Chaotic maps and cryptographic algorithms (or more generally maps defined on finite sets) have some similar properties: sensitivity to a change in initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods. Encryption rounds of a cryptographic algorithm lead to the desired diffusion and confusion properties of the algorithm. Iterations of a chaotic map spread the initial region over the entire phase space. The parameters of the chaotic map may represent the key of the encryption algorithm. An important difference between chaos and cryptography is that encryption transformations are defined on finite sets, while chaos has meaning only on real numbers. Moreover, for the time being, the notions of cryptographic security and performance of cryptographic algorithms have no counterpart in chaos theory.

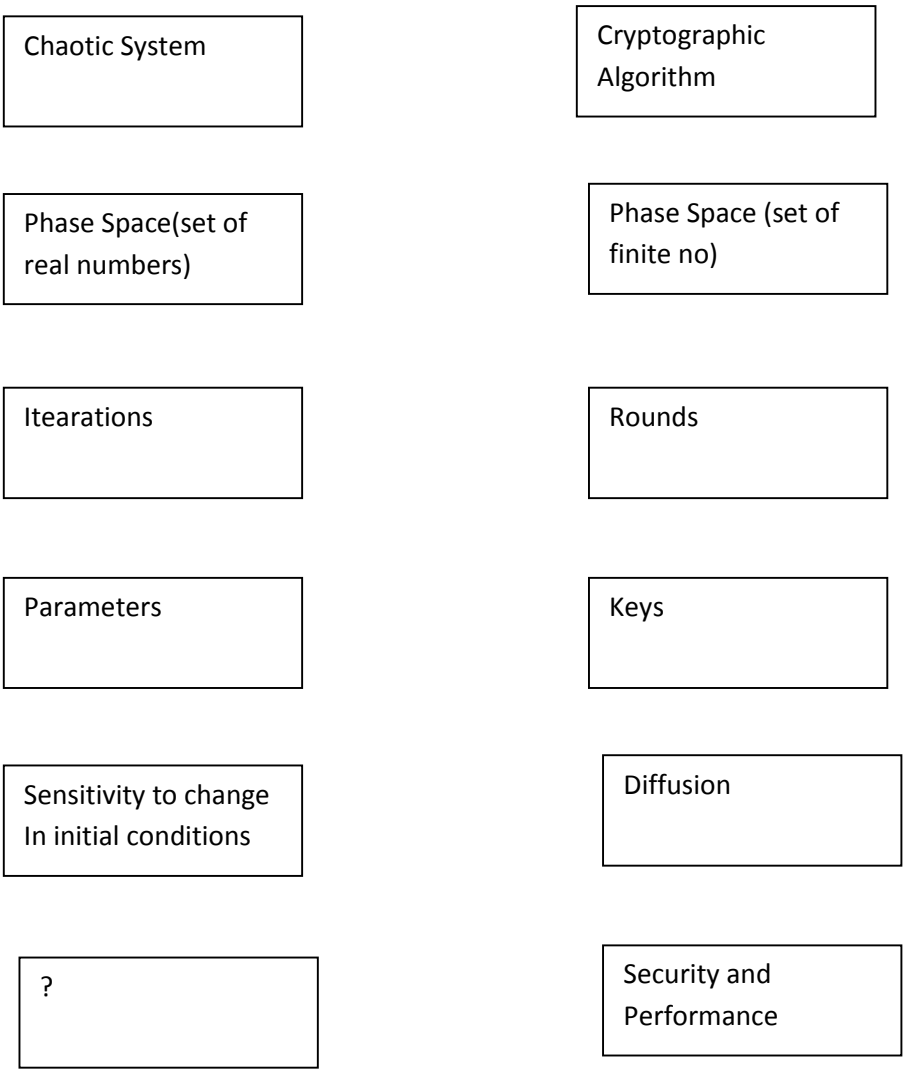


Figure 1: Similarities and differences between chaotic systems and cryptographic algorithms.

1.6.2 The Properties of Chaos

The basic properties of chaotic systems are deterministic, the sensitivity to initial conditions and parameters, the ergodicity and the topological transitivity. Deterministic means that chaotic systems have some determining mathematical equations ruling their behavior. The sensitivity to initial conditions means that, when a chaotic map is iteratively applied to two initially close points, the iterations quickly diverge, and become uncorrelated in the long term. Sensitivity to parameters causes the properties of the map to change quickly, when slightly perturbing the parameters, on which the map depends. Hence, a chaotic system can be used as a pseudorandom number generator. Topological transitivity is the tendency of the system to quickly scramble up small portions of the state space into an intricate network of filaments.

Local, correlated information becomes scattered all over the state space. The ergodicity property of a chaotic map means that if partitioning the state space into a finite number of regions, no matter how many, any orbit of the map will pass through all these regions. The ergodicity of a chaotic map is ensured by the topological transitivity property.

1.7 Problem Formulation

For large image, traditional image encryption algorithm such as data encryption standard (DES) is not suitable because of the weakness of low-level efficiency. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. 1-D chaotic systems such as logistic map are widely used, with the advantages of high-level efficiency and simplicity. But their weakness, such as small key space and weak securities, is also disturbing. During decryption the exact decryption is not possible in this method as pixels value will be floating point by thus algorithm and because of that some data loss occurs. Because of exponential sensitivity of chaotic maps, it makes a proper decryption of the original image impossible. A more frequently used 2D chaotic map is Arnold's chaotic map. Although it has proved itself to a good efficiency yet security is always a concern. The key generated for encryption of image can be hacked or guessed by intruder. It should also show more key sensitivity. A small change in key should affect the encrypted image.

1.8 Objective

Keeping above problems in mind, first of all various literatures available on chaos mapping encryption will be studied. During my work logistic map will be improved to make it non linear so that encryption key generated by this is unpredictable to hackers and it shows very less periodicity. More detailed description about modified logistic map is discussed in chapter 4. This modified logistic key is diffused into arnold's cat map scrambled image. Following will be key objectives which will be followed in thesis work:

- There are various chaotic maps available. Study of frequently used chaotic maps for image encryption will be done.

- A new modified chaos based on non linear chaos algorithm will be developed. Most of them are used in 1-D. So a modified chaos algorithm by combining Arnold's cat map and non linear logistic map will be developed and tested on parameters like resistivity to attack, histogram and correlation.
- A Graphical User Interface for the proposed algorithm will be designed in MATLAB.

1.9 Organisation of Thesis

Complete thesis has been divided into 6 chapters. Chapter 1 gives introduction about the topic which is followed by literature review in chapter 2. Chapter 3 discusses about chaos theory and various chaotic maps available. Proposed work in thesis in described in chapter 4 and results are discussed in 5^{th} chapter followed by conclusion in chapter 6.

Chapter 1: gives introduction about topic. It tells about encryption available and basic of chaos theory.

Chapter 2: it discussed the work done recently on image encryption using chaotic maps

Chapter 3: what are chaotic maps from information theory point of view and how many chaotic maps are available are discussed here.

Chapter 4: described the proposed work with problems in previous techniques in detail with graphical understanding.

Chapter 5: results are discussed here.

Chapter 6: conclusion and future scope.

Chapter2

Literature Review

1. In this paper [1] recent image encryption techniques have been discussed. Some of the techniques used to encrypt entire image bit sequence and some of them perform selective encryption i.e only selected part of image is encrypted. In block based encryption technique they reduce the correlation among the pixels and increase entropy. Some the technique uses genetic algorithm for encryption are also discussed. The image encryption algorithm which uses genetic algorithm for encryption have maximum entropy and gives less correlation coefficient. So if any encryption technique is combined with genetic algorithm technique we will get the maximum result. One of the technique which is based on DNA sequencing is useful for big image encryption and it reduces the encryption time of big image .The techniques which are chosen provide the security.
2. In this proposed[2] method genetic algorithm is used to obtain optimum result and in the last stage best cipher image is selected based on calculation of correlation coefficient and entropy. The image having lowest correlation coefficient and highest entropy is selected as best cipher image. In this paper first time genetic algorithm is used first time for encryption of images. Entropy and correlation coefficient obtained by using this method are 7.9978 and -0.0009 respectively.
3. In this paper[3] various image encryption schemes have been classified and analyzed with respect to various parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security and concluded that spatial domain schemes are generally faster but security level is low. In spatial domain, the scheme mentioned was good as far as compression friendliness, security and speed is concerned. While in frequency domain, scheme maintained good performance from security point of view.
4. In this[4] work MIE and VC algorithms have been improved by adding compression capability. As it can be seen from the experimental results jpeg with quality parameter set to 100 does not compress grayscale image, besides

size of the grayscale image increases, because noise in the image cannot be compressed productively. Quality setting set to 90 or below reaches good compression ratios. However jpeg was not suitable for color images (even with quality set to 100) because of the loss in the color. Thus PNG lossless compression was ideal for color image compression with MIE. VC is not a lossless encryption in nature, thus compression algorithm have to chosen carefully. Lossless PNG compression for gray-level and color images has a big compression ratio because it has only one color plane to encrypt and saves storage space and network bandwidth up to 92,4%.

5. An[5] image encryption scheme based on the 3D sawtooth map is proposed in this paper. The 3D sawtooth map is utilized to generate chaotic orbits to permute the pixel positions and to generate pseudo-random gray value sequences to change the pixel gray values. The image encryption scheme is then applied to encrypt the secret image which will be imbedded in one host image. The encrypted secret image and the host image are transformed by the wavelet transform and then are merged in the frequency domain. Experimental results show that the stego-image looks visually identical to the original host one and the secret image can be effectively extracted upon image processing attacks, which demonstrates strong robustness against a variety of attacks.
6. This paper[6] presents a new nonlinear chaotic algorithm. Its structural parameters and initial value can all be used as encryption key in chaotic cryptosystems. Experimental analysis demonstrates that the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. It is particularly suitable for Internet image encryption and transmission applications. Although the algorithm presented in this paper aims at the image encryption, it is not just limited to this area and can be widely applied in other information security fields.
7. This paper [7] introduces a new parametric switching chaotic system (PSCS) and its corresponding transforms for image encryption. The proposed PSCS has a simple structure and integrates the Logistic, Sine and Tent maps into one single system. The PSCS shows more general properties, including the Sine and Tent maps as special instances. It has complex chaotic behaviours.

A novel image encryption algorithm is introduced using the proposed PSCS and its transforms. Simulation results and security analysis are given to demonstrate that the proposed algorithm can encrypt different types of images with a high level of security.

8. The[8] security of Fridrich's algorithm against brute-force attack, statistical attack, known-plaintext attack and select plaintext attack is analyzed by investigating the properties of the involved chaotic maps and diffusion functions. Based on the given analyses, some means are proposed to strengthen the overall performance of the focused cryptosystem.
9. This paper[6] presents a new nonlinear chaotic algorithm (NCA) which uses power function and tangent function instead of linear function. Its structural parameters are obtained by experimental analysis. And an image encryption algorithm in a one-time-one password system is designed. The experimental results demonstrate that the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. Compared with some general encryption algorithms such as DES, the encryption algorithm is more secure.
10. In this paper[9], the security of the image encryption algorithm MCKBA/HCKBA has been studied in detail. Based on some properties of a composite function composed of modulo addition and XOR operation known-plaintext attack and an improved chosen-plaintext attack were provided to determine an equivalent secret key of MCKBA/HCKBA. The cryptanalysis provided in this paper sheds some light on breaking other encryption schemes based on multiple combination of the modulo addition and XOR operations.
11. This paper[7] introduces a new parametric switching chaotic system (PSCS) and its corresponding transforms for image encryption. The proposed PSCS has a simple structure and integrates the Logistic, Sine and Tent maps into one single system. The PSCS shows more general properties, including the Sine and Tent maps as special instances. It has complex chaotic behaviors. A novel image encryption algorithm is introduced using the proposed PSCS and its transforms. Simulation results and security analysis are given to demonstrate that the proposed algorithm can encrypt different types of images with a high level of security.

12. In this article[10], chaos based cryptography is discussed from a point of view which is closer to the spirit of both cryptography and chaos theory than the way the subject has been treated recently by many researchers.
13. The proposed[8] image encryption system is analyzed thoroughly in this paper. Through studying the strengths of the confusion and diffusion properties, its security against statistical attack, known-plaintext attack, select-plaintext attack and so on, some enhancement means are proposed to improve the cryptosystem, and some advices is given to select suitable chaotic map, diffusion function and iteration time.
14. This paper[11] proposed a novel image encryption algorithm, called ECKBA. The security level is enhanced and it security came from the following changes to the original algorithm: a larger key space, a more chaotic one dimensional map, and the use of a multi-round SP-network.
15. In this paper[12], it has been pointed out that the RCES/RSES image encryption method recently proposed is not secure enough against the known/chosen-plaintext attacks, and that the security against brute-force attack was overestimated. Both theoretical and experimental analyses have been given to support the feasibility of the known/chosen-plaintext attacks. The insecurity of RCES is caused by a careless design, and some principles on good design of secure image encryption schemes can be learned from the weakness of RCES.
16. In this paper[13] author examined one of the recently proposed chaotic image encryption algorithms, based on chaotic map lattices (CML). He showed certain problems with the chaotic map, as well as errors in the designed algorithm. Then proposed a way to improve it and present a new version of algorithm and its implementation and the results of a security analysis and a comparison of both schemes was shown.
17. In this paper[14], first, for the resistance to differential attack and linear attack, statistic properties of discrete exponential chaotic maps has been presented. In virtue of that, a spatial S-box is designed, and then, author design a key scheme for the resistance to statistic attack and grey code attack. This scheme can resist to the error function attack (EFA) which be regarded as a very effective attack recently. Finally, Experimental and analytic results show that this scheme is efficient and highly secure.

18. Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. Image security has found a great need in many applications where the image is to be protected from unauthorized access. Encryption is one of the ways to ensure high security. In recent years, encryption technology has been developed and many image encryption methods have been used. . Encryption and decryption consume a considerable amount of time. So there is a need for an efficient algorithm. This paper proposed three different image encryption techniques for colour image.
19. This paper takes intelligent security car as the research background, aiming to find a image encryption algorithm to realize the car in the image secure transmission of wireless transmission network based on open protocols, with good safety and high real-time. this passage is based on the analysis of the existing encryption algorithms of traditional and new image, select the digital image encryption technology based on chaotic system, And put forward a Multiple chaotic image encryption method which is fit for this project, After analysis and test, the algorithm satisfies the requirements of safety and real-time.
20. In order to improve performance and security of image encryption algorithm effectively based on chaotic sequences, an extended chaotic sequence generating method is generated based on logistic chaotic system using Bernstein form Bézier curve generating algorithm. To test the pseudorandom performance of the extended chaotic sequence, we also analyze random performance, autocorrelation performance,and balance performance of the extended chaotic sequence. Simulation results show that the extended chaotic sequence generated using our method is pseudorandom and its correlation performance and balance performance are good. As an application, we apply the extended chaotic sequence in image encryption algorithm, the simulation results show that the performance of the encrypted image using our method is better than that using logistic chaotic sequence.
21. Hyper-chaos has more than one positive Lyapunov exponents and it has more complex dynamical characteristics than chaos. Hence it becomes a better choice for secure image encryption schemes. In this paper, 3D Arnold cat map can be applied in image encryption, and it has more security and better

effect. However, its period is fixed. The original image will be returned to itself if iterating some times. On the basis of 3D Arnold cat map, it presented an algorithm of image encryption which separates the original image to many same blocks and no period. Theoretical and experimental analyses both confirm the security and the validity of the proposed algorithm.

22. Chaotic algorithm is a well-used method in the real-time secure image transmission systems. Research's are using this algorithm in encryption and decryption process. Even though it is applicable in many areas there are some disadvantages of security means low security to the sending information (others can easily decrypt the code). Now almost all images are in colour space and my project encrypt the color images by considering the each colour (R, G and B). In this paper I am going to change the image pixels position by which we can get high security and more difference between the original image and cipher image. Currently this algorithm is only applicable to only still colour images but in this paper I am going to develop encryption and decryption process for moving images such as videos by using chaotic algorithm. Finally I am going to compare the histograms also to demonstrate the encryption between the plain image and encrypted image. The main advantage of the paper is we can use longer key space and this process takes very less time. By using this algorithm we are going to encrypt and decrypt the color image. After taking color image we separate the red, green and blue components and after that we are going to confuse the red, green and blue components and we encrypt the image with another gray scale image. In decryption process we are going to undiffused the red, green and blue components and by using histograms we are going to compare the image histograms before encryption and after decryption.
23. In recent years, information security essential in various arenas like internet communication, multimedia systems, medical imaging, tele-medicine and military communication. However, most of them faced with some problems such as the lack of robustness and security. In this letter, after reviewing the main points of the chaotic trigonometric maps and the coupled map lattices, we introduce the scheme of chaos-based image encryption based on coupled map lattices. The scheme decreases periodic effect of the erotic dynamical

systems in the chaos-based image encryption. To evaluate the security of the encrypted image of this scheme, the key space analysis, the correlation of two adjacent pixels and differential attack were performed. This scheme tries to improve the problem of failure of encryption such as small key space and level of security.

24. This paper proposes a high security image encryption technique using logistic map. The proposed image encryption algorithm is described in detail along with its security analysis such as key space analysis, statistical analysis and differential analysis. A comparison in terms of correlation between the initial and transformed images, Number of pixels change rate and unified average changing intensity is also done. The present algorithm has been tested using different images to prove that the encryption method has a great potential and has a good ability to achieve the high confidential security
25. In this paper a chaos-based image encryption algorithm was proposed in the security weaknesses of the proposal. By applying chosen plaintext and known-plaintext attacks, we show that all the secret parameters can be revealed.
26. Recently, an image encryption scheme based on logistic map was proposed. It has been reported by a research group that its equivalent secret key can be reconstructed with only one pair of known-plaintext and the corresponding cipher-text. Utilizing stable distribution of the chaotic states generated by iterating the logistic map, this paper further demonstrates that much more information about the secret key can be derived under the same condition.
27. This paper proposes the chaotic encryption algorithm based on 3D logistic map, 3D Chebyshev map, and 3D, 2D Arnolds cat map for color image encryption. Here the 2D Arnolds cat map is used for image pixel scrambling and 3D Arnold's cat map is used for R, G, and B component substitution. 3D Chebyshev map is used for key generation and 3D logistic map is used for image scrambling. The use of 3D chaotic functions in the encryption algorithm provide more security by using the, shuffling and substitution to the encrypted image. The Chebyshev map is used for public key encryption and distribution of generated private keys
28. Chaos theory has significantly contributed towards the development of fast and secure image encryptionalgorithms. Authors in [1] proposed an efficient

and secure approach for image encryption based on chaotic logistic maps.The algorithm uses an 80-bit secret key and two chaotic logistic maps, whose initial conditions are derived using the secret key. Depending upon the outcome of logistic maps, algorithm performs any of eight different types of operations on different pixels. To make the algorithm more robust, secret key is modified after encrypting a block of 16-pixels. This paper proposes enhancements in the mentioned algorithm to make it more efficient and secure. The security analysis of the algorithm establishes its utility in real-time image encryption.

29. Information security is concerned with maintaining the secrecy, reliability and accessibility of data. The main objective of information security is to protect information and information system from unauthorized access, revelation, disruption, alteration, annihilation and use. This paper uses spatial domain LSB substitution method for information embedding and Arnold's transform is applied twice in two different phases to ensure security. The system is tested and validated against a series of standard images and the results show that the method is highly secure and provides high data hiding capacity.

Chapter 3

Chaos Theory

Chapter 1 provided brief information about the chaotic theory. There are various chaotic maps are available so problem raised which one to choose. How chaotic maps are chosen is discussed in this chapter but before that chaotic map is discussed form information theory point of view.

3.1 Chaos from an Information Theory Point of View [12]

Chaos theory, as a branch of the theory of nonlinear dynamical systems, has brought to our attention a somewhat surprising fact: low-dimensional dynamical systems are capable of complex and unpredictable behavior. What is the origin of chaos in deterministic systems? For simplicity we consider here a discrete-time dynamical system defined by iteration of the function F: $X \rightarrow X$, X — RN. The set of points $\{x, F(x), F2(x), \ldots\}$ is called a trajectory (or orbit) of the initial condition x. We assume that F has a chaotic attractor. Informally, an attractor is called chaotic if the motion on it is unpredictable: two nearby states on the attractor have different and unrelated behavior within the attractor. The evolution of a deterministic system is completely determined by the vector field F and the initial condition x. However, to specify completely the initial condition an infinite amount of information and a measuring system with an infinite precision are required, which are both intractable. What are the effects of a measuring system's finite precision? Measuring an initial (and future) state is equivalent to partitioning the state space into a finite number of regions, and observing the evolution in this macroscopic world. Any set of a finite number of disjoint regions which cover the state space is called a partition of the system. The process of partitioning the state space, assigning symbols to every region from the partition, and the resulting macroscopic dynamics are called symbolic dynamics. If the system is chaotic, then different initial states belonging to the same region will produce different observations at some later time. From the viewpoint of our measuring system, identical macroscopic initial states evolve differently. A loss of

determinism occurred, and transitions between the regions of the partition can only be specified by means of probabilities. Partitioning of the state space turns the deterministic chaotic system into an ergodic information source which can be analyzed in terms of information theory. The Kolmogorov-Sinai entropy (denoted by hKS) is the measure of asymptotic rate of creation of information by iterating F. Systems with positive entropy are usually considered as chaotic. The unpredictability of chaotic trajectories is caused by exponential separation of nearby points. Unpredictability means uncertainty; therefore, one should expect that the entropy of a dynamical system is related to its positive Lyapunov exponents. This deep mathematical result is rigorously proven only for so called Sinai-Ruelle-Bowen measure. From the viewpoint of any measuring device, if the dynamical system produces unpredictable sequences, then the dynamical system is called chaotic. While the motion of the dynamical system in the continuous (microscopic) state space is deterministic, its motion in the partitioned (macroscopic) space is stochastic and the trajectories are sequences of symbols. On the basis of the knowledge of the past coarse-grained trajectory of the system we can predict its future macroscopic states only in probabilistic terms. Turning a deterministic chaotic system into an information source via partitioning of the state space is not in collision with Shannon's note that a deterministic system cannot generate information. Actually, a chaotic system does not generate information, that is, its evolution is completely determined by its initial state. A chaotic system merely converts the information about its initial state into a form which is visible to the measuring system. Every letter in the coarse-grained trajectory, which is a sequence of letters, brings an additional amount of information about the initial state. The word random in deterministic dynamical systems is linked to incompressibility of information: a trajectory of the system is termed random when the shortest program that generates it has (essentially) the same size as the trajectory itself. The trajectory of a point $\boldsymbol{x}$ is called random if its algorithmic complexity is positive. The following theorem is of essential significance in this case: For chaotic systems the trajectories of almost all state points $\boldsymbol{x} \in X$ are random and their algorithmic complexity is equal to the Kolmogorov-Sinai entropy hKS. As a disturbing consequence, no finite computer program can produce or predict a chaotic trajectory, or in other language, for any additional bit of the initial state, a computer program can output only one additional bit about the chaotic trajectory. Clearly, positive algorithmic complexity of almost all initial states does not suffice for the

randomness of trajectories of a dynamical system; for example a dynamical system with a stable equilibrium would contradict such a conjecture. What is the source of the unpredictability and information generation of a chaotic behavior? The finite precision of any real measuring system and the sensitive dependence of a chaotic evolution to a change in initial states combine to an inability for long-term prediction of chaotic behavior. Hopefully, this section resolves the juxtaposition of three seemingly contradictory terms: “random”, “deterministic” and “chaos”. Determinism of the defining equations implies existence and uniqueness of solutions, but it does not imply computability of solutions.

3.2 Chaotic Maps

below given table shows the various chaotic maps available for rncryption with their dimensionality.

Table 3.1 : Chaotic Maps © Wikipedia

Map	Time domain	Space domain	Number of space dimensions	Also known as
Arnold's cat map	discrete	Real	2	
Baker's map	discrete	Real	2	
Bogdanov map				
Chen-Lee system	continuous	Real	3	
Chossat-Golubitsky symmetry map				
Circle map	discrete	Real	1	
Complex Cubic map				

Map	Time domain	Space domain	Number of space dimensions	Also known as
Complex quadratic map	discrete	Complex	1	gives rise to the Mandelbrot set
Complex squaring map	discrete	Complex	1	
Degenerate Double Rotor map				
Double Rotor map				
Duffing equation	continuous	Real	1	
Duffing map	discrete	Real	2	
Dyadic transformation	discrete	Real	1	2x mod 1 map, Bernoulli map, doubling map, sawtooth map
Exponential map	discrete	Complex	2	
Gauss map	discrete	Real	1	mouse map, Gaussian map
Generalized Baker map				
Gingerbreadman map	discrete	Real	2	

Map	Time domain	Space domain	Number of space dimensions	Also known as
Gumowski/Mira map				
Hitzl-Zele map				
Horseshoe map	discrete	Real	2	
Hénon map	discrete	Real	2	
Hénon with 5th order polynomial				
Ikeda map	discrete	Real	2	
Interval exchange map	discrete	Real	1	
Kaplan-Yorke map	discrete	Real	2	
Linear map on unit square				
Logistic map	discrete	Real	1	
Lorenz attractor	continuous	Real	3	
Lorenz system's Poincare Return map				
Lozi map	discrete	Real	2	
Nordmark truncated map				

Map	Time domain	Space domain	Number of space dimensions	Also known as
Pomeau-Manneville maps for intermittent chaos	discrete	Real	1 and 2	Normal-form maps for intermittency (Types I, II and III)
Pulsed rotor				
Quasiperiodicity map				
Rabinovich-Fabrikant equations	continuous	Real	3	
Random Rotate map				
Rössler map	continuous	Real	3	
Shobu-Ose-Mori piecewise-linear map	discrete	Real	1	piecewise-linear approximation for Pomeau-Manneville Type I map
Sinai map - See [1]				
Standard map, Kicked rotor	discrete	Real	2	Chirikov standard map, Chirikov-Taylor map
Symplectic map				
Tangent map				
Tent map	discrete	Real	1	
Tinkerbell map	discrete	Real	2	

Map	Time domain	Space domain	Number of space dimensions	Also known as
Triangle map				
Van der Pol oscillator	continuous	Real	1	
Zaslavskii map	discrete	Real	2	
Zaslavskii rotation map				

Chapter4

Proposed Work

In previous chapter, work done by many researchers on image encryption using various chaos algorithms was discussed. In this chapter arnold's cat map along with modified logistic map will be discussed. In my work image encryption is done by collectively use of arnol'd cat map and modified logistic map.

4.1 Arnold's Cat Map and Logistic Map

Logistic mapping is a typical representative of the chaotic mapping. Although it is one dimensional mapping, the control effect is very good. The Logistic equation is shown as follows:

$x_n = rx_n(1 - x_n)$ n=0,1,2……. (4.1)

In the formula, x_n is the variable, as well as r is the system parameter in which $r\epsilon(0,4] and\ x_n\epsilon[0,1]$.. When 1<$r < 3$, the solution of the system is fixed point. When $r = 3$ the formula starts the transition state, when r =3.5699456, the system enters a chaotic state. As is often the case in dynamical systems theory, the action of the logistic map can not only be represented algebraically, as in Eq. 4.1, but also geometrically. Given a point xn, the graph of the logistic map provides y = f(xn). To use y as the starting point of the next iteration, we must find the corresponding location in the x space, which is done simply by drawing the line from the point [xn, f(xn)] to the diagonal y = x. This simple construction is then repeated, as illustrated in Fig. 4.1(a, b).

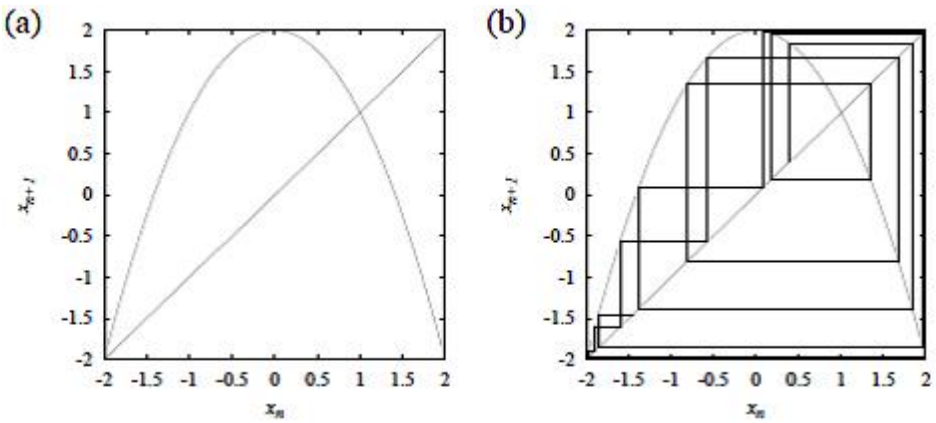


Figure 4.1: (a) Graph of the logistic map for $r = 2$. (b) Graphical representation of the iteration of equation 4.1 []

The various behaviors displayed by the logistic map are easily explored, as this map depends on a single parameter r. As illustrated in Fig. 4.2, one finds quickly that two main types of dynamical regimes can be observed: stationary or periodic regimes on the one hand, and "chaotic" regimes on the other hand. In the first case, iterations eventually visit only a finite set of different values that are forever repeated in a fixed order. In the latter case, the state of the system never repeats itself exactly and seemingly evolves in a disordered way, as in Fig. 4.2(b).

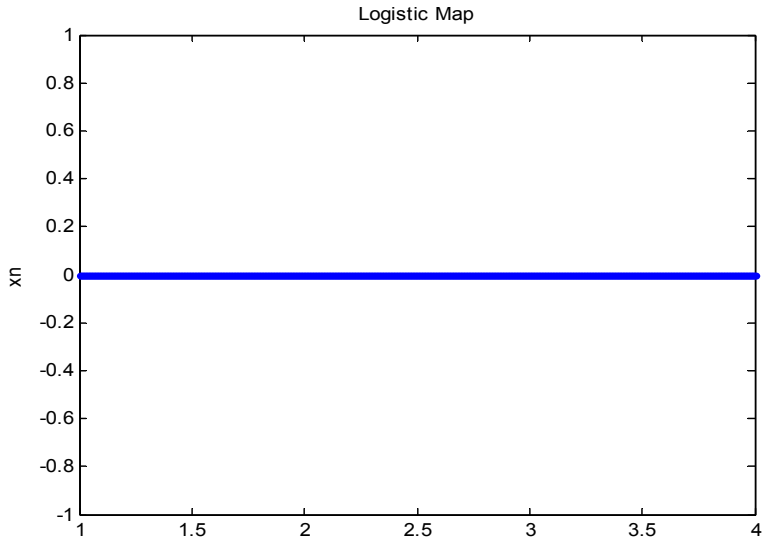


Figure4.2(a): stationary regime, r= 0.5

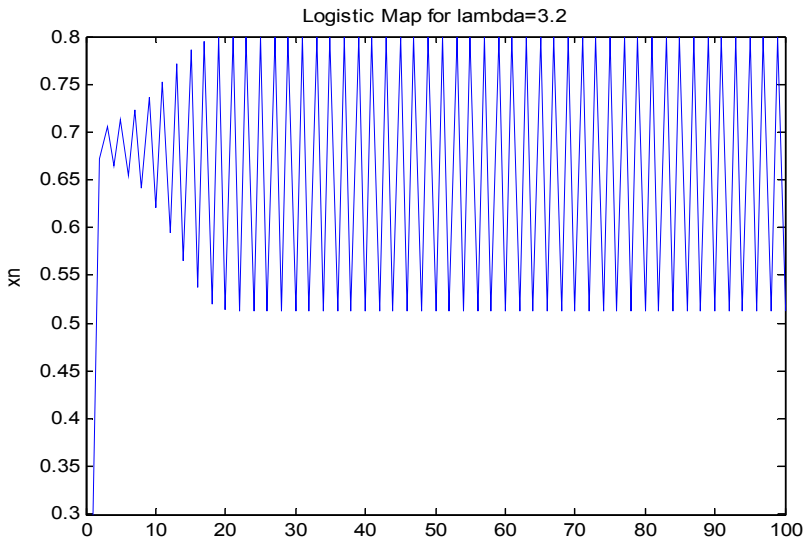


Figure 4.2(b): periodic regime of period 5

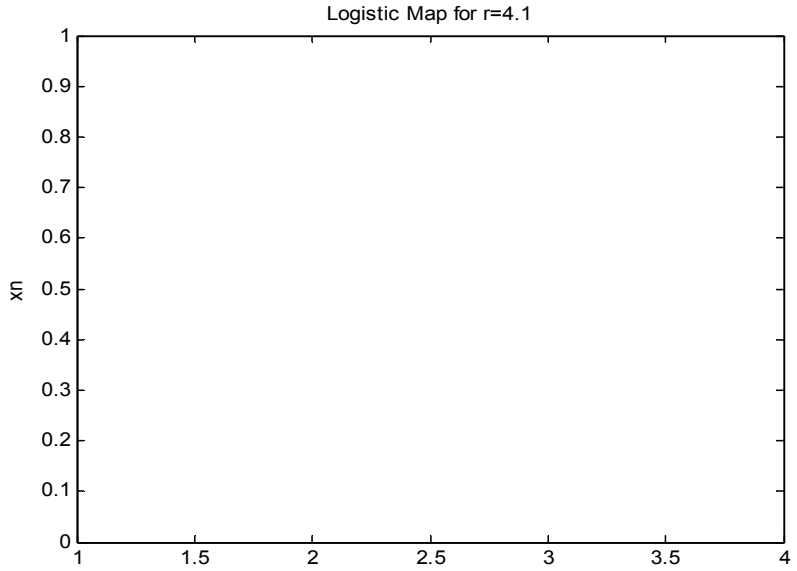


Figure 4.2(c) : logistic map for r>4

By varying the parameter *r*, the following behavior is observed:

- With *r* between 0 and 1, the population will eventually die, independent of the initial population.
- With *r* between 1 and 2, the population will quickly approach the value $\frac{r-1}{r}$, independent of the initial population.
- With *r* between 2 and 3, the population will also eventually approach the same value $\frac{r-1}{r}$,, but first will fluctuate around that value for some time. The rate of convergence is linear, except for *r*=3, when it is dramatically slow, less than linear.
- With *r* between 3 and $1+\sqrt{6}$ (approximately 3.44949), from almost all initial conditions the population will approach permanent oscillations between two values. These two values are dependent on *r*.
- With *r* between 3.44949 and 3.54409 (approximately), from almost all initial conditions the population will approach permanent oscillations among four values. The latter number is a root of a 12th degree polynomial.
- With *r* increasing beyond 3.54409, from almost all initial conditions the population will approach oscillations among 8 values, then 16, 32, etc. The lengths of the parameter intervals which yield oscillations of a given length

decrease rapidly; the ratio between the lengths of two successive such bifurcation intervals approaches the Feigenbaum constant $\delta = 4.66920$. This behavior is an example of a period-doubling cascade.

- At r approximately 3.56995 is the onset of chaos, at the end of the period-doubling cascade. From almost all initial conditions we can no longer see any oscillations of finite period. Slight variations in the initial population yield dramatically different results over time, a prime characteristic of chaos.

- Most values beyond 3.56995 exhibit chaotic behaviour, but there are still certain isolated ranges of r that show non-chaotic behavior; these are sometimes called *islands of stability*. For instance, beginning at $1 + \sqrt{8}$ (approximately 3.82843) there is a range of parameters r which show oscillation among three values, and for slightly higher values of r oscillation among 6 values, then 12 etc.

- The development of the chaotic behavior of the logistic sequence as the parameter r varies from approximately 3.56995 to approximately 3.82843 is sometimes called the Pomeau–Manneville scenario, which is characterized by a periodic (laminar) phase interrupted by bursts of aperiodic behavior. Such a scenario has an application in semiconductor devices. There are other ranges which yield oscillation among 5 values etc.; all oscillation periods occur for some values of r. A period-doubling window with parameter c is a range of r-values consisting of a succession of sub-ranges. The k^{th} sub-range contains the values of r for which there is a stable cycle (a cycle which attracts a set of initial points of unit measure) of period $c2^k$. This sequence of sub-ranges is called a cascade of harmonics. In a subrange with a stable cycle of period $c2^{k*}$ there are unstable cycles of period $c2^k$ for all $k<k*$. The r value at the end of the infinite sequence of sub-ranges is called the point of accumulation of the cascade of harmonics. As r rises there is a succession of new windows with different c values. The first one is for $c = 1$; all subsequent windows involving odd c occur in decreasing order of c starting with arbitrarily large c.

- Beyond $r = 4$, the values eventually leave the interval [0,1] and diverge for almost all initial values as shown in figure 4.2(c).

For any value of *r* there is at most one stable cycle. A stable cycle attracts almost all points. For an *r* with a stable cycle of some period, there can be infinitely many unstable cycles of various periods.

A bifurcation diagram summarizes this. The horizontal axis shows the values of the parameter *r* while the vertical axis shows the possible long-term values of *x*.

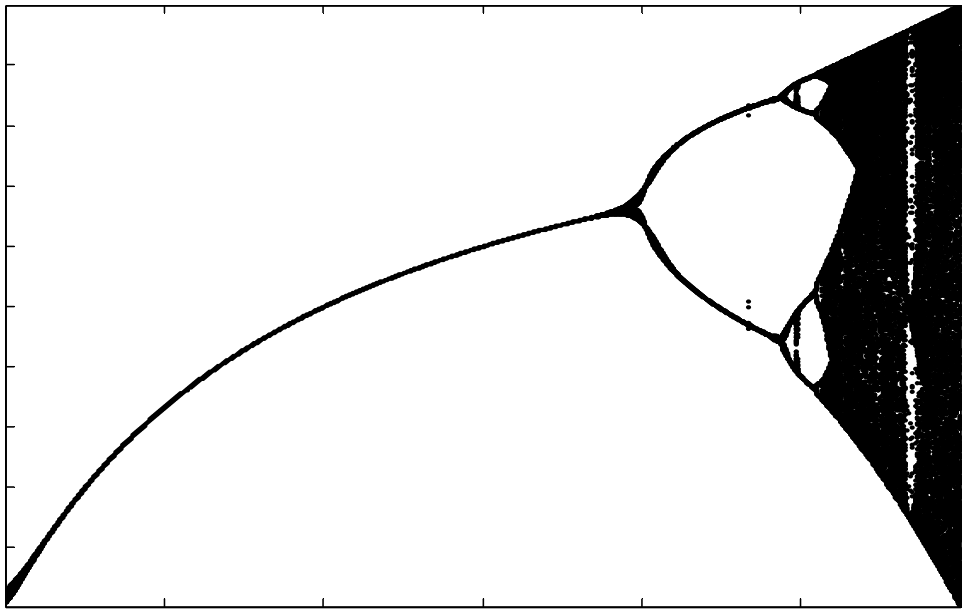


Figure 4.3: Bifurcation diagram of Logistic map

The bifurcation diagram is a self-similar: if you zoom in on the above mentioned value *r* = 3.82843 and focus on one arm of the three, the situation nearby looks like a shrunk and slightly distorted version of the whole diagram. The same is true for all other non-chaotic points. This is an example of the deep and ubiquitous connection between chaos and fractals.

From above discussion it has been found out that:

1) The Logistic map does not satisfy uniform distribution property. When r= [0, 3.6) the points concentrate on several values and could not be used for encryption purpose.
2) Cryptosystems based on Logistic map has small key space and weak security.

So in my proposed work these drawbacks of logistic map have been removed by ***Modified Logistic Map***. In this non linear function has been adopted to change the

value of key continuously for security enhancement. So the modified logistic map is defined as the tangent function of x_n as

$$x_{n+1} = r.tg(\alpha x_n).(1 - x_n)^{\beta} \quad \text{.....(4.2)}$$

The ranges of parameters r, a and b will be discussed as follows. Firstly, they are positive. Secondly, the absolute value of the slope of the curve at fixed point should not be less than 1, and xn+1 > xn when xn = 1/(1 + b), therefore r may be defined as

$$r = \mu.ctg\left(\frac{\alpha}{1+\beta}\right).(1+\frac{1}{\beta})^{\beta} \;;\; \mu > 0 \qquad (4.3)$$

Finally, parameter l is obtained by experimental analysis; as a result, $\mu = 1 - \beta^{-4}$. So the NCA map is defined as follows:

$$x_{n+1} = (1-\beta)^{-4} ctg\left(\frac{\alpha}{1+\beta}\right).(1+\frac{1}{\beta})^{\beta}.tg(\alpha x_n).(1-x_n)^{\beta}$$

(4.4)

where xn ϵ (0, 1), a ϵ (0, 1.4], b ϵ [5, 43], or xn ϵ (0, 1), a ϵ (1.4, 1.5], b ϵ [9, 38], or xn ϵ (0, 1), a ϵ (1.5, 1.57], b ϵ [3, 15]. The ranges of a and b are obtained by iteration experimental analysis.

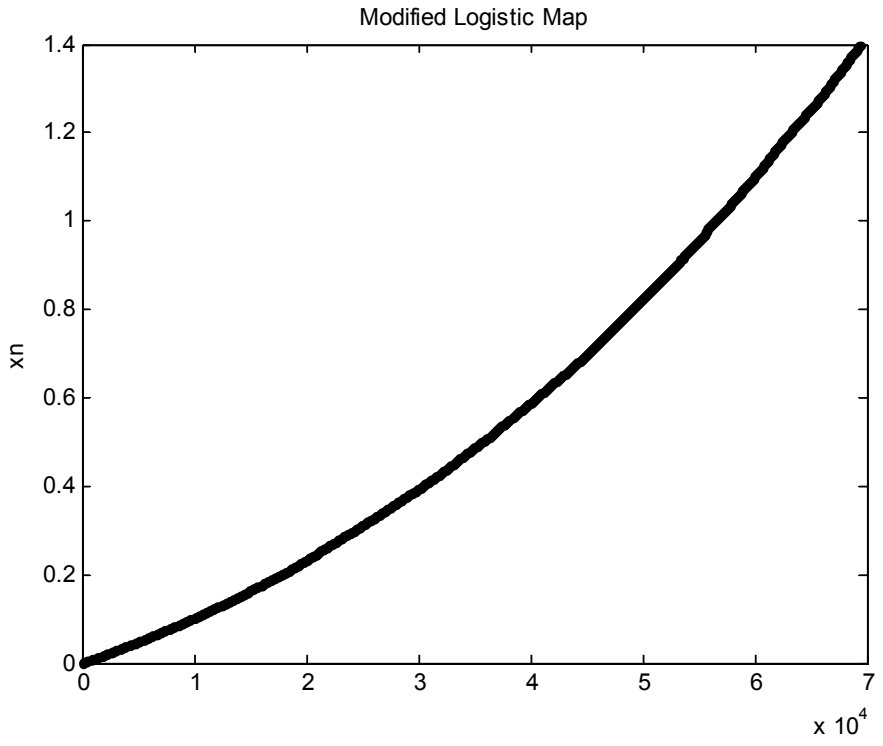


Figure 4.4: Modified Logistic map

Since this logistic map is one dimensional and one dimensional chaotic map always suffer from weak security and low key space even after sufficient improvement. So in my work logistic map is combined with arnold's 2D cat map to overcome these weakness.

Arnold's cat map's feature is that image being apparently randomized by the transformation but returning to its original state after a number of steps. As can be seen in the figure 4.5, the original image of the cat is sheared and then wrapped around in the first iteration of the transformation. After some iterations, the resulting image appears rather random or disordered, yet after further iterations the image appears to have further order—ghost-like images of the cat, multiple smaller copies arranged in a repeating structure and even upside-down copies of the original image—and ultimately returns to the original image.

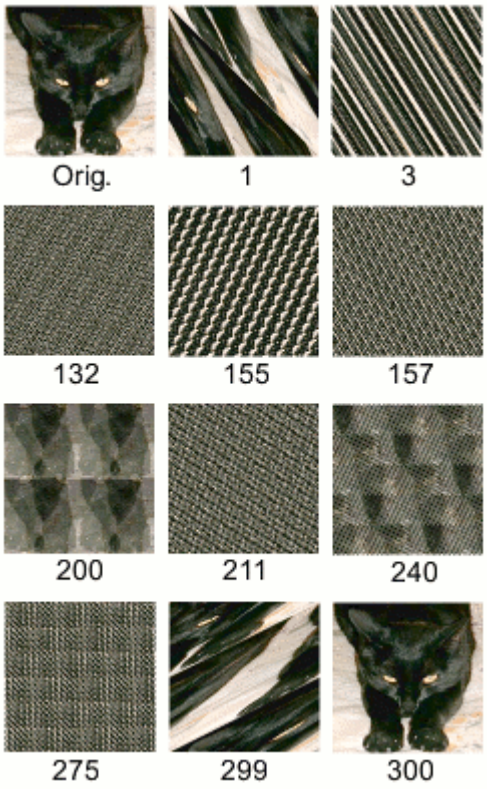


Figure 4.5: Arnold's cat map scrambling image

Arnold map was firstly proposed by Arnold in 1968, an equation of two-dimensional Arnold map is shown below (MathWorld2007):

$$\begin{cases} x_{n+1} = (x_n + y_n) mod 1 \\ y_{n+1} = (x_n + k * y_n) mod 1 \end{cases} \quad (4.5)$$

Where notation '*x*mod1'means to take the fractional part of a real number *x* only by adding or subtracting an appropriate integer; therefore(*x*n, *y*n)is confined in a unit square of [0,1]×[0,1]. The transforming formula 4.6 in matrix form is shown as below

When *k*=2

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} = c \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod1 \qquad (4.6)$$

Firstly, the determinant of matrix *C* is stretched by linear transformation and then folded by modulo operation, thus the Arnold map in figure 4.6 is an area-preserving map and the determinant of its linear transformation matrix, too. The map appears to be in chaotic states; and it is an one-to-one map; hence, the watermark pixels of different positions will be moved to different embedding positions. Formula 4.6 defines matrix *C* where |*C*| = 1, the Arnold map is an area-preserving map without attractor. Meanwhile, the Arnold map is a one-to-one map, each point in unit matrix is uniquely transformed to another point in the same identity matrix. Arnold map has a very typical characteristic of chaotic motion: stretching (*x*, *y* can be larger after multiplying by matrix *C*) and folding (*x*, *y* can be withdrawn back to the identity matrix by taking its modulo).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} = c \begin{bmatrix} x_n \\ y_n \end{bmatrix} modN \qquad (4.7)$$

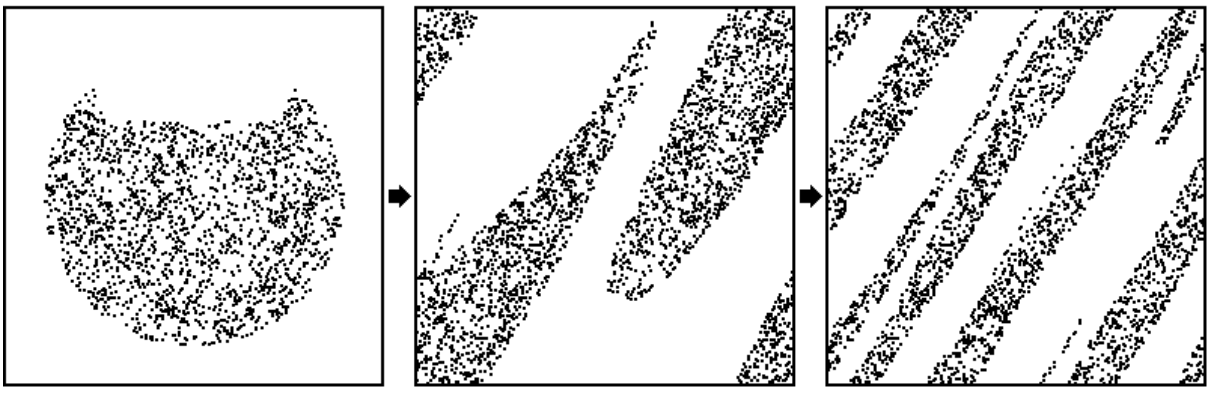


Figure 4.6: Arnold's Cat map

The above Arnold map is formulized as follows. Firstly, the phase space is generalized to [0, 1, 2,…*N*-1] × [0, 1, 2,…*N*-1], that is only positive integers from 0 to *N*-1are taken; second, it is generalized to two-dimensional invertible area-preserving equation as in formula 4.8.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} = c \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod(N+1) \quad (4.8)$$

Where *a*, *b*, *c*, and *d* are positive integers, and |*C*| = *ad*−*bc*= 1 holds. Therefore, in this context, only three out of these four parameters are independent, say, we can let *a*, *b* and *c* be independent while *d* depends on the area condition |*C*|.

4.2 Steps for Image Encryption

Cat map scrambling is used to scramble image in image encryption. It enhances the security of encrypted image. For this purpose the key is generated with help of modified logistic map, that key is now more sensitive to a bit change and key space is also increased. By using this key the resulting encrypted image will have desired properties. Step to encrypt image as per my proposed algorithm are as:

- Database of various images to be loaded as image encryption give different results depending upon type of image. For this we have selected two RGB images of size 200*200 & 300*300 and one gray image of Leena.
- Arnold's 2D cat map is used to scramble the image, for this the coefficients values are taken as
  A=1, b= 20, c=10 and d=b*c+1
- Iterations are done thrice for scrambling.
- The encryption key is generated by modified logistic map having non linear equations by 10000 iterations of equation.
- To diffuse the key into scrambled image XORing operation is used. Every column of scrambled image matrix is XORed with column of encrypted key.
- The thus encrypted image is checked on parameters of histogram, correlation coefficient and key sensitivity.

The flow chart of steps is shown in figure 4.7

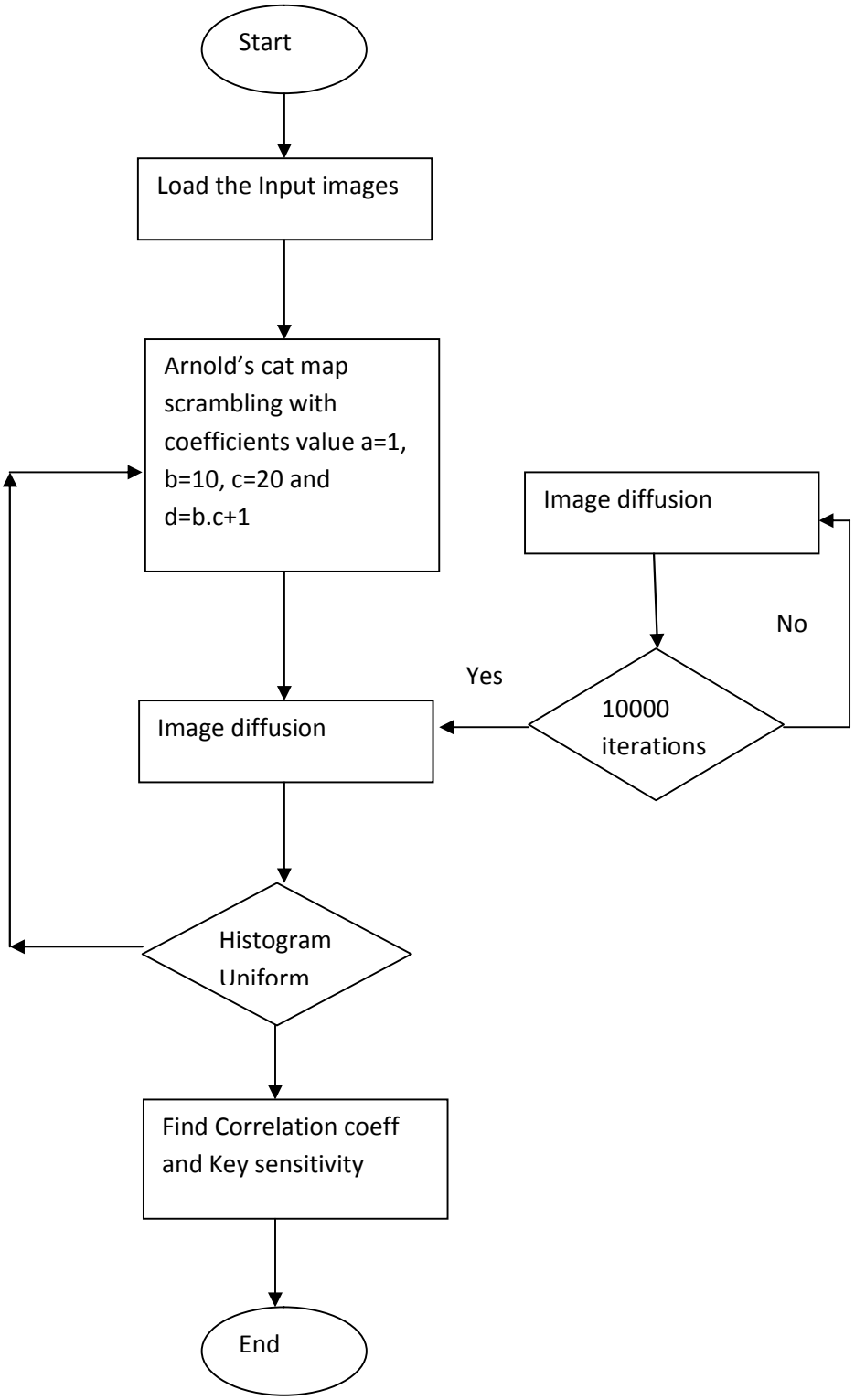


Figure 4.7: Flow Chart of Image encryption by modified logistic map and arnold's cat map.

Chapter 5

Results & Discussion

MATLAB R2009b's image processing toolbox has been used in image encryption. Image Processing Toolbox™ provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Many toolbox functions support multicore processors, GPUs, and C-code generation. Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions and apps let you explore images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest (ROIs). The toolbox supports workflows for processing, displaying, and navigating large images.

Three types of images are loaded for image encryption. Initially RGB image of 200 * 200 pixels is loaded as shown in figure 5.1. For image encryption the RGB image has to be converted into gray scale image as gray scale images are intensity images which are single sampled, that's why processing on these is quite easier. Figure 5.2 shows the gray scale image of image shown in figure 5.1.

Figure 5.1: Loaded Image of 200*200 pixels

Figure 5.2: gray scale converted image of 5.1

As discussed, encrypted key is generated by modified logistic map which is having large key space than logistic map. Moreover the key generated by logistic map is periodic in nature which can be cracked by intruder whereas modified logistic map generated a non periodic and large key as shown in figure 5.3.

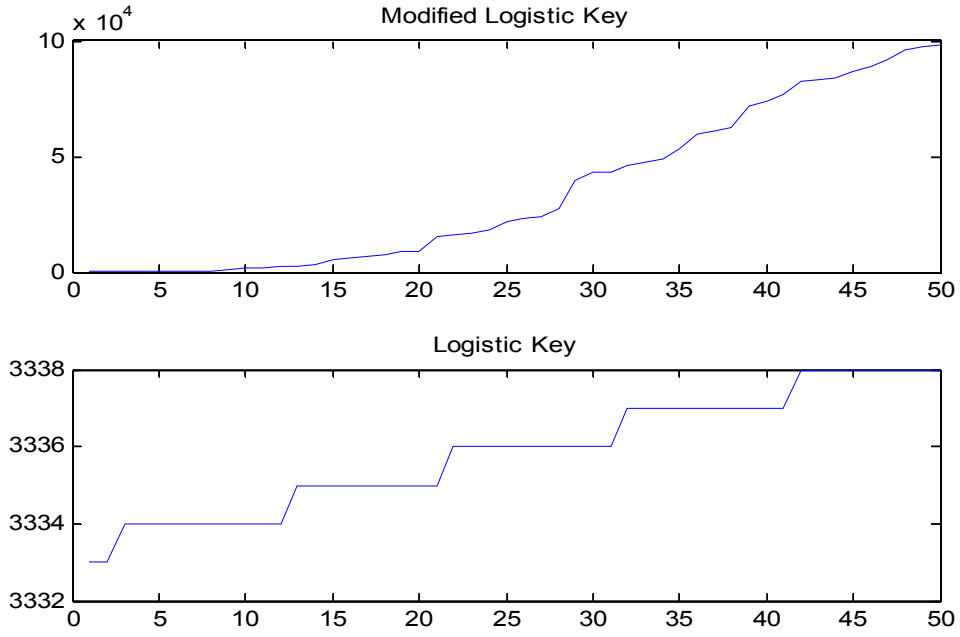


Figure 5.3: plot of 50 samples of modified logistic and logistic key

Above plot clearly shows the non periodicity of modified logistic key as well as when scale along y axis is noticed then large key space property in modified logistic map is proved. Keys generated in above both cases are in range between 0 and 1 and initial value x_0 is taken as 0.3 after hit and trial observations.

Table 1: Key samples for both key generation methods

Key	Modified Logistic	Logistic
1	4	3333
2	24	3333
3	36	3334
4	74	3334
5	216	3334
6	249	3334
7	319	3334
8	658	3334
9	751	3334
10	1795	3334
11	1914	3334
12	2206	3334
13	2815	3335
14	3435	3335
15	5170	3335
16	5756	3335
17	6548	3335
18	7516	3335
19	8757	3335
20	8974	3335
21	15168	3335
22	16117	3336
23	17048	3336
24	18411	3336
25	21579	3336
26	23069	3336
27	24284	3336
28	27619	3336
29	39412	3336
30	42980	3336
31	43090	3336
32	46380	3337
33	47833	3337
34	48624	3337
35	53268	3337
36	59690	3337
37	60750	3337
38	62375	3337
39	72084	3337
40	73683	3337
41	76556	3337
42	82707	3338
43	82902	3338
44	84066	3338
45	86559	3338
46	88796	3338
47	91546	3338
48	96229	3338
49	97633	3338
50	98432	3338

Variation in modified logistic key is more than logistic key, which make it robust to attackers. But before diffusing key with cover image, cover image is scrambled first by Arnold's cat map as security in 1 D is always questioned and doubtful. So a 2D arnold's cat map first scramble the image. From the literature review it is clear that arnold's scrambling is done three times to make it robust as shown in figure 5.4.

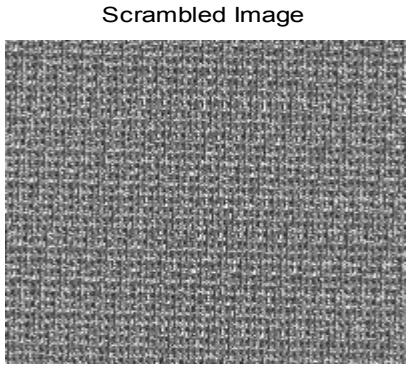


Figure 5.4: Arnold's scrambled image

The image histogram of scrambled image with cover image is shown in figure 5.5. histogram of image should be uniform if it is encrypted. Figure 5.5 shows energy distributed in scrambled image and cover image is still same except the representation of image.

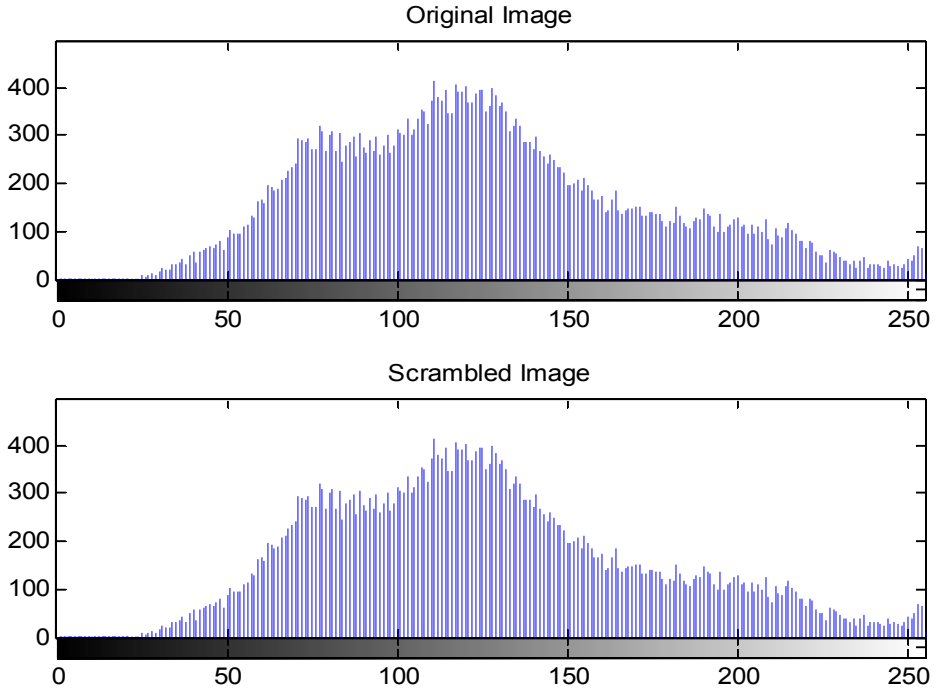


Figure 5.5: Histogram of cover and scrambled image

Now diffusion of encrypted key is done by XOR operation. XOR operation has the advantage that if key is known then output XORED with key will give the input image. It reduces the complexity in decryption process. The encrypted image and histogram is shown in figure 5.6(a) and (b).

Figure 5.6(a): Encrypted Image after scrambling

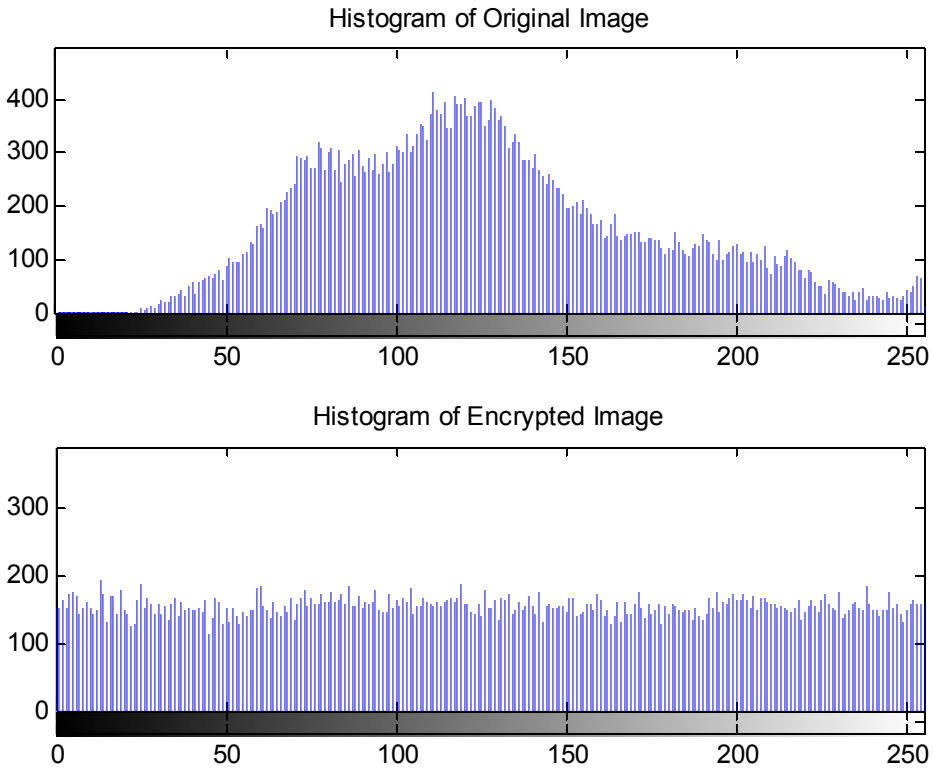


Figure 5.6(b): Histogram showing energy distribution after encryption

Above figure satisfy the condition of uniform histogram after encryption. It makes difficult to hacker to guess image as energy is now distributed in whole image

uniformly. This is the basic condition of image encryption which is fulfilled by our proposed work. Histogram of simple logistic key encryption of same image is shown in figure 5.7 and now no word require to explain the difference.

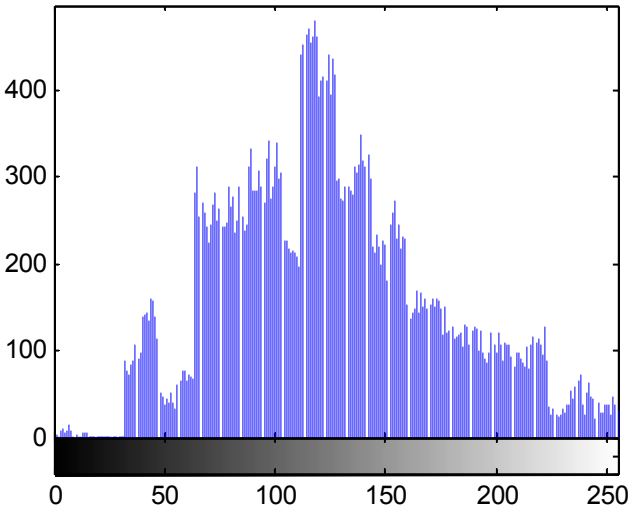


Figure 5.7: Histogram of encrypted image of simple logistic map

Security analysis of encryption algorithm is done with correlation coefficients of adjacent pixels. Lower the correlation higher is the secure. To check the security horizontal correlation coefficient is separately found out and vertical separately as shown in figure 5.8. above plot in 5.8 shows the highly correlated value of original image pixel with neighbouring pixel whereas lower plot is not much correlated.

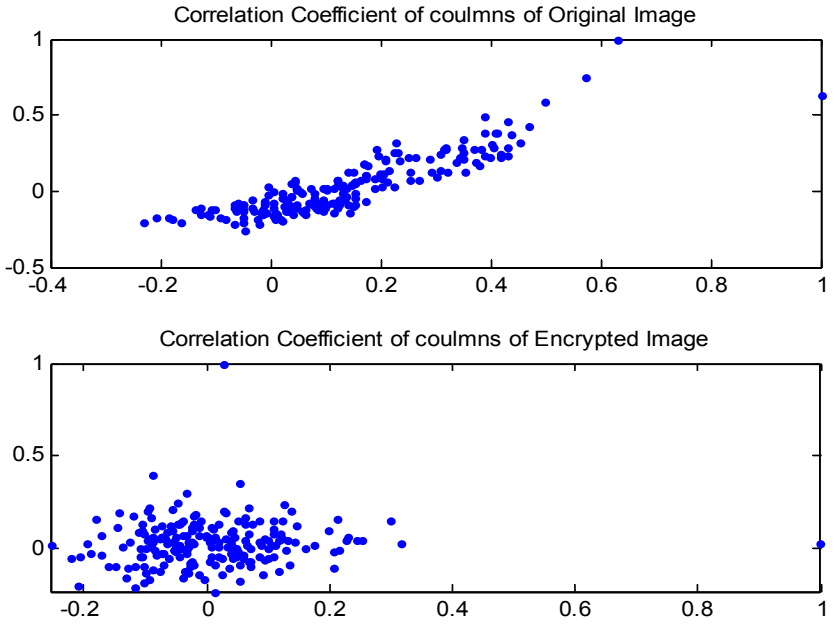


Figure 5.8 (a): Vertical correlation coefficient

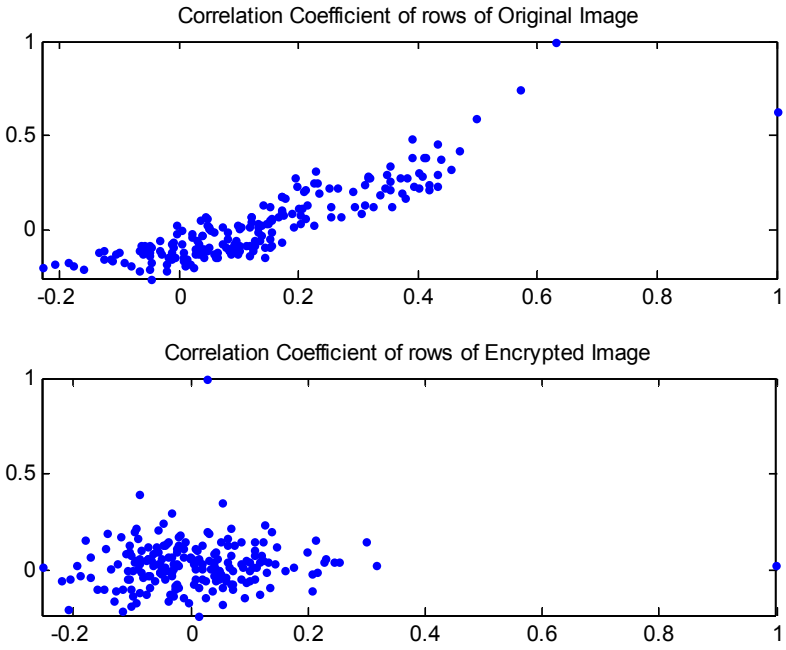


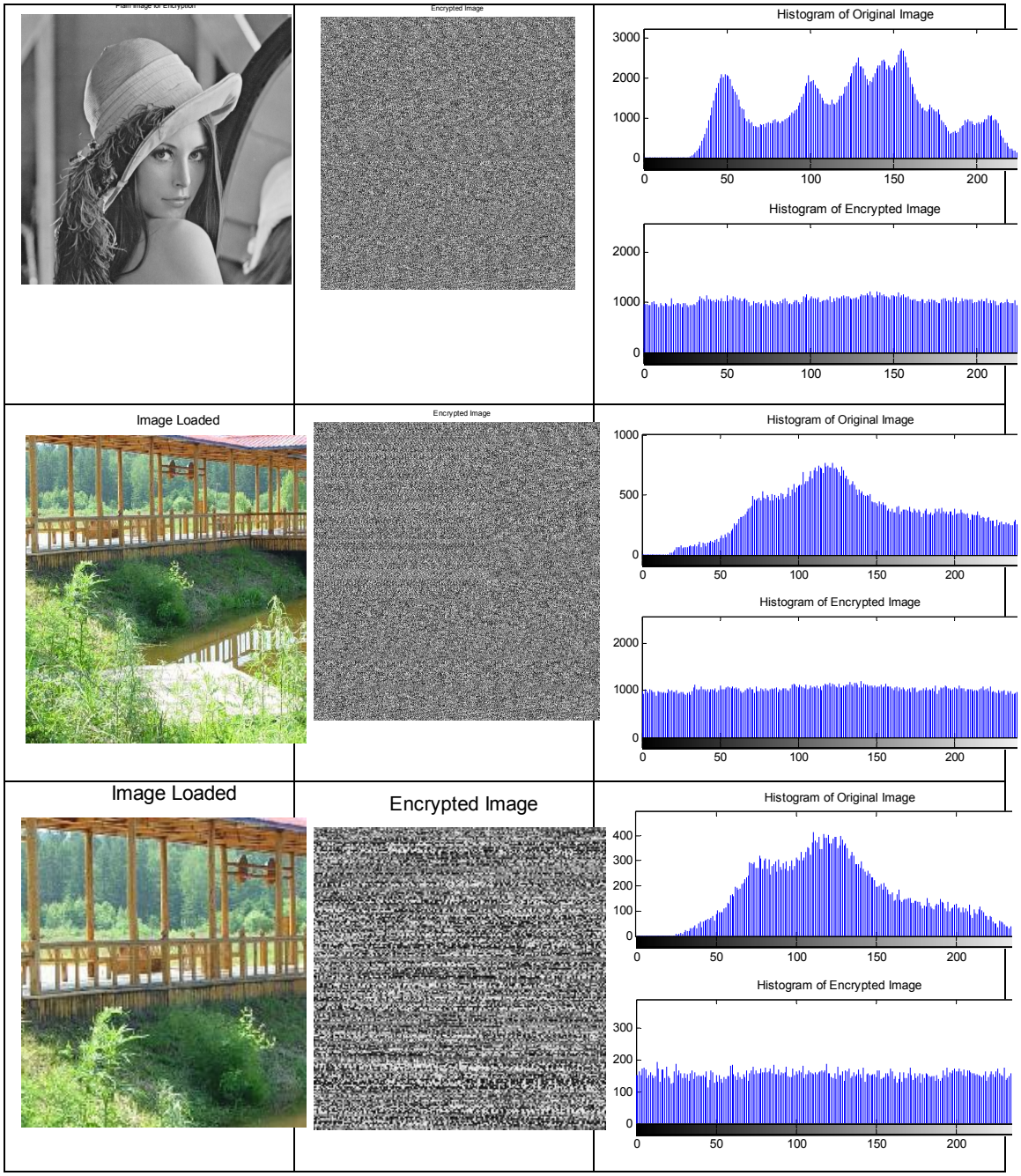
Figure 5.8(b): Horizontal Correlation Coefficient

The third image uploaded in code is of Leena gray scale image. The horizontal and vertical correlation coeff is shown in table 5.2. leena image is having lowest correlation coeff . Thus encryption makes it more secure.

Table 5.2: Horizontal and vertical correlation coeff

	Horizontal Correlation coeff	Vertical Correlation coeff
200*200 image	0.0752	0.0752
400*400 image	0.1165	0.1165
512*512 image	-0.0564	-0.0564

Table 5.3 below shows the encrypted image with their histogram of three images taken as input and shows that histogram of encrypted image is uniform in every case irrespective of input image.



The other major parameter to check the feasibility of algorithm is key sensitivity. Key sensitivity represents the change in encrypted image with a small change in key. If key sensitivity is high then encrypted image will be more secure as for decryption purpose exact key will be required, if key is displaced by even a single bit then image will change. Below given tables 5.4 the encrypted image's vertical correlation coefficients for 3 iterations of Arnold's cat map respectively. Three different key have been used for key sensitivity purpose.

Table 5.4: vertical Correlation coefficients for different key

512*512 (Image size)	0.0234	0.0344	0.0133
300*300	-0.0029	0.0053	0.0290
200*200	0.0406	-0.0065	0.0817

Chapter 6

Conclusion & Future Scope

In this work we have enhanced the work done on Arnold's cat mp encryption. The key used for encryption requires security and unpredictability. This work is done with help of modified logistic map. The key objective of this work was to study different chaotic map encrypting algorithms and to modify logistic map. It was concluded form literature review that security is enhanced if multidimensional chaotic mapping is used. The single dimensional logistic map is used to just produce encryption key. Even, weaknesses of simple logistic map is also identified in our work. Simple logistic map was periodic in nature and can be predicted easily by a smart hacker. So the periodicity is removed by using non linear equation in logistic map. Key generated by this is diffused into confused image by Baker's cat map. Results are checked on various parameters like histogram analysis, correlation coefficients etc. uniformity of encrypted image histogram shows the effectiveness of the proposed algorithm.

In spite of all this, we note that a lot of work can still be done in this area. We now summarize some of the directions in which we propose to proceed.

- Mathematical analysis of the chaos of the higher dimensional Arnold's maps is yet to be explored. The encryption of image after higher oreder scrambling by Arnold's cat ma is yet to be observed.
- We wish to explore the application of fractional chaos in the encryption scheme. For this, we first need to get the fractional counterparts of the Arnold's map and verify that the properties of chaos are retained.
- We have incorporated the diffusion mechanism into confusion. However, efforts must be put into exploring the possibility of using chaotic substitutions for the diffusion mechanism. The main criterion for this exploration should be the speed and efficiency with which the diffusion can be achieved using the chaotic maps.
- In natural sciences, lots of diffusion phenomena are modeled by differential equations. We wish to explore the applicability of these models in the diffusion process of encryption schemes. Further, we can utilize fractional

calculus to create fractional diffusion equations and investigate the applicability of these equations for diffusion process for encryption.

- Our method of encryption in ideally suited for implementation in embedded systems where memory is at a premium and the processor is slow. In such cases, we must resort to calculating the permutation each time. This calls for a trade off between speed of the cipher and strength

References

1. Varsha S.Nemade and R.B.Wagh," Review of different image encryption techniques" Proceedings of " National Conference on Emerging Trends in Computer Technology (NCETCT-2012)" Held at R.C.Patel Institute of Technology, Shirpur, Dist. Dhule,Maharashtra,India. April 21, 2012

2. Shubhangini P.Nichat, Prof.Mrs.S.S.Sikchi," Image Encryption using Hybrid Genetic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013 ISSN: 2277 128X

3. Jolly Shah and Dr. Vikas Saxena," Performance Study on Image Encryption Schemes" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

4. Pia Singh, Prof. Karamjeet Singh, " Image Encryption And Decryption Using Blowfish Algorithm In Matlab" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013

5. Ruisong Ye and Wenping Yu," An Image Hiding Scheme Using 3D Sawtooth Map and Discrete Wavelet Transform" I.J. Image, Graphics and Signal Processing, 2012, 6, 52-60

6. Haojiang Gao , Yisheng Zhang, Shuyun Liang, Dequn Li," A new chaotic algorithm for image encryption" ©2005 Published by Elsevier Ltd.

7. Yicong Zhou, Long Bao, C. L. Philip Chen," Image Encryption Using a New Parametric Switching Chaotic System" ©2011 Published by Elsevier Ltd.

8. Shiguo Lian, Jinsheng Sun, Zhiquan Wang," Security Analysis of A Chaos-based Image Encryption Algorithm" The paper was accepted by Phisica A, Elsevier Science, 2005.

9. Chengqing Li,Yuansheng Liu, Leo Yu Zhang, and Michael Z. Q. Chen," Breaking a chaotic image encryption algorithm based on modulo4 addition and XOR operation,July 27, 2012

10. Ljupcˇo Kocarev," Chaos-Based Cryptography: A Brief Overview,1531636X/10/$10.00©2001IEEE

11. Daniel Socek, Shujun Li, Spyros S. Magliveras and Borko Furht," Enhanced 1-D Chaotic Key-Based Algorithm forImage Encryption,(2004-05).

12. Shujun Li, Chengqing Li, Guanrong Chen and Kwok-Tung Lo," Cryptanalysis of RCES/RSES Image Encryption Scheme,FernUniversit¨at in Hagen, Lehrgebiet Informationstechnik, Universit¨atsstraße 27, 58084 Hagen,Germany.

13. K. Jastrzebski , Z. Kotulski ," ON IMPROVED IMAGE ENCRYPTION SCHEME BASEDON CHAOTIC MAP LATTICES,*ENGINEERING TRANSACTIONS Engng. Trans.* 57, 2, 69–84, 2009

14. Linhua Zhang, Xiaofeng Liao, Xuebing Wang," An image encryption approach based on chaotic maps, Accepted 14 September 2004

15. Rajinder Kaur1, Er. Kanwalpreet Singh," Comparative Analysis and Implementationof Image Encryption Algorithms, IJCSMC, Vol. 2, Issue. 4, April 2013, pg.170 – 176

16. Shuai Wang, Wei Sun1,, Yinan Guo1, Haiqun Yang1and Shuming Jiang," Design and Analysis of Fast Image Encryption Algorithm based on Multiple Chaotic Systems in Real-time Security Car, International Journal of Security and Its Applications Vol.7, No.6 (2013),

17. ZHANG Xuefeng ,FAN Jiulun ," Extended Logistic Chaotic Sequence and Its Performance Analysis, TSINGHUA SCIENCE AND TECHNOLOGYISSN 1007-0214 28/49 pp156-161Volume 12, Number S1, July 2007

18. Pan Tian-gong and Li Da-yong," A Novel Image Encryption Using Arnold Cat, International Journal of Security and Its Applications Vol.7, No.5 (2013)

19. M.Surya Bhupal Rao, DrV.S.GiridharAkula," CHAOTIC ALGORITHMS USED FOR ENCRYPTION ANDDECRYPTION ON MOVING IMAGES, Volume 2, No.8, August 2013International Journal of Advances in Computer Science and Technology.

20. Sodeif Ahadpour, Yaser Sadra," A Chaos-based Image Encryption Scheme using Chaotic Coupled Map Lattices**.**

21. Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi," An Image Encryption Process based on Chaotic Logistic Map, March 20, 2014.

22. Cahit Cokal, Ercan Solak,"Cryptanalysis of a chaos-based image encryption algorithm, Physics Letters A 373 (2009) 1357–1360

23. Chengqing Li ,Tao Xie , Qi Liu," Cryptanalyzing an image encryption scheme based onlogistic map, Jan 17 2013.

24. Pawan N. Khade and Prof. Manish Narnaware," 3D Chaotic Functions for Image Encryption, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

25. Ravindra K. Purwar, Priyanka," An Improved Image Encryption Scheme UsingChaotic Logistic Maps, International Journal of Latest Trends in Engineering and Technology (IJLTET).

26. Minati Mishra, Ashanta Ranjan Routray, Sunit Kumar," High Security Image Steganography withModified Arnold's Cat Map, *International Journal of Computer Applications (0975 – 8887)Volume 37– No.9, January 2012.*