T.C

ALTINBAS UNIVERSITY

Information Technologies

STUDY & DEVELOPMENT OF CRYPTOSYSTEMS FOR 3D IMAGE BASED ON CHAOTIC SYSTEMS

Ali Ismail Jadaan

Master Thesis

Supervisor

Asst. Prof. Dr. Sefer KURNAZ

Istanbul 2019

STUDY & DEVELOPMENT OF CRYPTOSYSTEMS FOR 3D IMAGE BASED ON CHAOTIC SYSTEMS

by

ALI ISMAIL JADAAN

Information Technologies

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2019

--

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

ALI ISMAIL JADAAN

DEDICATION

I would like to dedicate this work to my lovely family and specially my mother, for their invaluable efforts when I felt hopeless and weak in solving problems.

ACKNOWLEDGEMENTS

In the name of Allah: the Beneficent and the Merciful_ Praise and Gratitude be to Allah forgiving me strength and guidance: so that this thesis can be finished accordingly would like to thank my supervisors: Asst. Prof. Dr. Sefer KURNAZ Please let me express my deep sense of gratitude and appreciation to both of you for the knowledge: guidance and unconditional support you have given me. I wish you all the best and further success and achievements in your life.

ABSTRACT

STUDY & DEVELOPMENT OF CRYPTOSYSTEMS FOR 3D IMAGE BASED ON CHAOTIC SYSTEMS

Ali Ismail Jadaan
M.Sc., Information Technologies, Altınbas University,
Supervisor: Asst. Prof. Dr. Sefer KURNAZ
Date: July,2019
Page: 67

In this work, a novel pixel permutation -diffusion method for image encryption. The output trajectory of chaotic system is very unpredictable. Therefore, based on the unpredictable character, we use the chaotic sequences generated by chaotic systems as encryption codes (keys) and then implement the digital-color (rgb) image encryption with high confidential security. Encryption algorithm is divided into two parts, permutation process and diffusion process. In the permutation process, the algorithm introduces plain-text feedback mechanism that makes the permutation effect not only associated with the chaotic sequences, but also related to plain-text, in this stage, image is scrambled in row then in column using Aizawa and TSUCS chaotic systems respectively. And in the diffusion process, Sun Wan chaotic systems sequence are used to effectuate XOR operation of pixels and chaos values to get final encrypted image. By several experimental tests such as histogram analysis, key space analysis, and statistical analysis shows that the proposed algorithm for an image cryptosystem provides an efficient and secure way for image encryption.

Keywords: Chaos Encryption, Image Encryption, 3D Chaos System

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

TSUCS	:	Tree Scroll unified Chaos System
NDLS	:	Non-Linear Dynamical Systems
UACI	:	Unified Average Changing Intensity
NIST	:	National Institute of Standards and Technology
AES	:	Advanced Encryption Standard
DSA	:	Digital Signature Algorithm

LIST OF SYMBOLS

∀	:	The universal quantifier
∃	:	The existential quantifier.

1. INTRODUCTION

This chapter describes the status of information hiding technology. It will serve as an introduction to the background of this research. The motivation of the research, the research problems of existing image encryption schemes technologies. The chapter finished with in brief introduction of the overall structure of this thesis.

1.1 BACKGROUND

With the rapid development of information technology, multimedia documents have become a central element in the various fields of application. Indeed, they are tools of essential work in biomedical, in satellite and astronomical imagery, in film production, or in industrial computer science. This phenomenal development has not been done without the concern of illegal manipulation since anyone can easily copy, modify and distribute digital images without the risk of damaging them. These illicit manipulations are a central problem for the security of any system: the state, a company, or an individual. Hence, the importance of protecting these multimedia documents against unauthorized access or distribution.

Therefore, how to effectively protect copyright and the security of information has become an urgent practical problem. Traditional encryption techniques can simply guarantee the security of digital media information during transmission; however, there are still some limitations to protecting the integrity of digital media content and preventing unauthorized copying.

In recent years, several image encryption algorithms have been proposed. Image encryption techniques mix the pixels of the standard image and reduce the association between the pixels, so that any opponent cannot modify the encrypted image. The chaotic encryption method seems to be much better day after day. Chaos-based cryptographic algorithms are one of the newest and most effective ways to develop secure image encryption techniques.

1.1 RESEARCH MOTIVATIONS

With the growing popularity of network and the development information processing, a high percentage of digital image information transmission in the network are related to personal privacy and confidential secrets. It is undoubtedly important to ensure information security. Data encryption is an important measure to ensure data security in a network environment; however, at this stage, most of the encryption and authentication password system structures are text messages, because digital images involve large amount of data and high redundancy; current encrypting methods have more or less shortcomings. Thus, to ensure secure transmission of images in the network, the new study of digital image encryption method, has become an urgent need. This thesis introduces a new technology that combines the image processing technologies with the modern chaotic cryptography technology.

Through computer networks, it is very convenient for people to work and to have access to study resources; resource sharing has become much easier. But, people have to face various security problems in the meantime. According to statistics worldwide, a hacking incident takes place nearly every 20 seconds. A variety of security incidents result in the loss of over $17 billion in the U.S every year. [1] Information hacking incident has increased 250% in the past 5 years, nearly 99% of big companies suffer a variety of hacking incidents, and even RAS securities websites were attacked.

The complexity and the flexibility of network environment determine the existence of network security threats. Digital images in network transmission are prone to a variety of man-made attacks, including information theft, data tampering, data deletion, and virus attacks, which cause huge losses to the information owners. Therefore, how to ensure information security of the image has become a hot issue.

Cryptographic techniques can be used primarily to protect information security. A sound password system can not only guarantee the confidentiality of information, but is useful to ensure the integrity and authenticity of information. The chaotic encryption technology is an emerging encryption technology that uses chaotic signals generated by chaotic system for encryption, which has fine features of the password such as being a class of random chaos, and extremely sensitive to initial conditions. Thus, the use of chaotic signals can help build a good encryption system. Besides, the chaotic encryption

system can be simply implemented and run fast; it is suitable for image encryption with large amount of data. [2]

To ensure the security of digital image information, there are two effective protective measures. The first one is digital watermarking technology, which embeds a watermark in an entire image to effectively protect digital copyright. But this method is not able to change the appearance of an image, which is not suitable for the confidential needs of image. The other method is image encryption. Through encrypting operations of this method, the original image is transformed to information similar to channel random noise, and such random noise is not recognizable to people who do not have the encryption key. With the fast growth of networking technology, image encryption techniques have good application prospects.

For image encryption, people used to encrypt image by traditional encryption algorithms. Based on the secret keys used in the processes of encryption and decryption, traditional encryption method can be divided into asymmetric-key cryptography (also known as secret key and public-key) and symmetric-key cryptography [2] . Symmetric-key cryptography algorithm uses the same key for encryption and decryption , and only communicating parties know the secret key, which can encrypt or decrypt message, such as DES (Data Encryption Standard), and IDEA (International Data Encryption Algorithm). In an asymmetric key encryption, the encryption and the decryption keys are different. Encryption key is known to everyone and only the intended recipient has the key to decrypt the message. The typical algorithms such as RSA (invented by Rivest, Shamir and Adleman) and ElGamal are typical samples of this type. In theory, the image can be encrypted through traditional encryption techniques, but most traditional encryption technologies are based on text design without considering the inherent characteristics of images, thus, using the above approach is not only inefficient but less secure. To solve these problems, many scholars turn to image encryption algorithms. Some of their typical approaches will be introduced in the following:

- **Arnold transforms:**

Arnold transform can be considered as stretching, compressing, folding and matching processes. Through these processes, *S* point in discrete digital image matrix can be rearranged. Discrete digital image is a kind of finite set. The result of such transforms

can cause chaotic of position changes of pixels in *S* set. But the repeated iterations of such finite set is periodical; therefore, reversion phenomena will occur after finite iterations, which is called Poincare recurrence theorem. [3] Thus, if encryption algorithm is obtained, plain text can be recovered by any status of cipher text performing iterations. The type of attack often last very short time, which means the breaches of security and confidentiality exist. On the other hand, there are some shortcomings similar to Arnold transform existing in Hilbert pixel replacement encryption. Although these replacement technologies do not have much cipher features, they can effectively scramble input sequence of plain text, which can effectively cover up statistic characteristics of the plain text in order to resist statistic attacks. Hence, even though the Arnold transform can structure one of replacement parts of space; it is not suitable to be an independent cryptosystem.

- **SCAN language encryption:**

SCAN language is an efficient two-dimensional spatial data access technology. [4] It can conveniently generate massive scanning paths or space-filling curves, which can transform two-dimensional image data to one-dimensional data sequence, and then use different scanning word to represent different image cipher text. Commercial encryption algorithms such as DES and IDEA are two example algorithms. This type of encryption algorithm does not compress data for original image data, but scanned text words can be compressed without losses. In general, this algorithm is normally used to process massive data, although lossless compression is applied for scanning words. Under normal circumstances, compression ratio is not high; it can only utilize the convenience that SCAN language transforms 2D data to 1D data. Data security depends on common commercial cipher. During the encryption process, 2D data should be transformed to 1D data first; thus, pretreatment window time is needed, decrypted data needs to be rearranged, and the efficiency is not high. Like RSA, DES and AES algorithms, the SCAN algorithm is also one of block encryption. Compared with streaming encryption, block encryption is a direct method, but the biggest problem is that it requires as small a secret key as possible, so that memory space and operation time can be minimized. [5] SCAN language encryption is classified as three types; they are scan patterns, partition patterns and mixed patterns.

- **Chaotic encryption techniques:**

Since 1992, chaotic secure communication has evolved for generations. Chaotic masking and chaotic shift keying belongs to the first generation of chaotic secure communication technology; the security is not strong, and its practicability is greatly retarded. Chaotic modulation is the second generation of chaotic secure communication technology. Although the safety of the second generation is better than the first, it still falls short of customer satisfaction. The third generation is chaotic encryption technology. This method combines the benefits of chaos and cryptography, and it has a very high safety performance. It is followed by synchronization pulse of chaotic communication, which is the fourth generation of chaotic secure communication an tis technology will be the center of our interest in tis work .

1.2 RESEARCH PROBLEM

In order to design hyperchaotic scrambling system for digital images, the following problems will be addressed in this research work.

(1) What's algorithm suitable to scrambling

The lack of robustness and security are important problem for secret key, but the development of communication technology requires, these problems will not solve. We found single chaotic system is simple than hyperchaotic system. A single chaotic system is easy to implement; because of this, it can easily be cracked, as well as limited by the computer word length. The scrambling image will return to its original state that after a certain number of iterations from the single chaotic system. The hyperchaotic system has complex characteristics and unpredictable.

(2) How to improve algorithm for digital image encryption:

The hyperchaotic encryption speed is slower than simple chaotic. For now, the development of technology depends more and more on the digital image and high resolution photo are required for sharp reproduction in our life. The encryption process can take a long time or outage. Therefore, building a highly agile control system that hyperchaotic algorithm is used to improve secret key space, randomly and encryption

speed. Chapter 4 will illustrate this problem and make specific improvements.

(3) What's better technology to hidden image?

Chaos theory is a branch of mathematics that deals with non-linear phenomena. These phenomena include weather, financial markets, organizational behavior, predicting epileptic seizures, fractals and other complex real-world physical phenomena. Chaotic phenomena are characterized by the fact that they are seemingly random, but have a precise mathematical formulation. Hence, given some other parameters they are repeatable/reproducible/predictable and yet apparently random. The properties required by cryptography are readily satisfied by chaotic functions via their properties of (a) sensitive dependence on initial conditions (function parameters), (b) topological transitivity and (c) erodicity (randomness). This makes chaos theory a good, attractive option for cryptography. Thus we see that Chaos theory has come a long way from the time a butterfly flapped its wings in the minds of Feigenbaum and Lorentz, especially in its application to cryptography and to image encryption.

(4) How to test the performance evaluation of proposed algorithms

Based on these results, performance evaluation of proposed encryption algorithms are the chaotic scrambling and the watermark encryption. By comparing the analysis result with the bit error rate and normalized correlation for the scrambled image and original image, and the extracted image and host image.

1.3 RESEARCH OBJECTIVES

A wide range of applied multimedia delivery in the future network is becoming increasingly prevalent. Information security problems have also become increasingly prominent especially image cryptography for secure transmission. However, traditional encryption methods for digital image are limited. Therefore, it is necessary to explore new features for image encryption. Chaotic encryption is a new technology that develops rapidly in recent years. The technology, with its features of simplicity, fast encryption, and high security, is very suitable for image encryption. However, due to short development time, it is still not perfect and needs to be further studied. This major work is divided into studying the origin of chaos and conducting simulation

algorithm. Through analyzing and summarizing, the pros and cons for various algorithms can be obtained. Based on the modern cryptography, a more multi-dimensional chaotic image encryption system is designed; in-depth exposition of some key issues on the system will be made, such as achieving multi-dimensional chaotic system and specific steps of the encryption process.

In order to employ chaos theory to a larger extent, we try and combine the confusion and diffusion mechanisms using some chaotic functions. When we consider the binary representation of the intensities of the image at each pixel location, we observe that every image is inherently 3D in nature. The working of the diffusion mechanism - a substitution function of the gray level intensities - motivated us combine confusion and diffusion by a common mechanism on the 3D view of the image, using chaos theory. In summary, we provide a

- Mathematic study of multidimensional chaotic systemes and Performance in image encryption.
- Way to integrate confusion and diffusion mechanisms.

1.4 STRUCTURE OF THE THESIS

Chapter (1) introduces the background of the information hiding technologies, the motivations of the research, the research problems, objectives, methodology and the structure of the thesis. Chapter (2) describe fundamental concept and definition of cryptography theory, chaos concept basis and connection between cryptography and chaos. Chapter (3) presents a literature review of chaotic theories, chaotic cipher algorithms, and chaotic encryption algorithm problems. Chapter (4) proposes to encrypt images based on a hyperchaotic systems.

2. PRELIMINARY KNOWLEDGE

In this chapter the relationship between cryptographic and chaotic systems is analyzed. Main definitions about cryptography and chaotic dynamics are discussed.

2.1 CRYPTOGRAPHY

Cryptography is the study of mathematical techniques related to the aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Practical cryptography is the study of the methods of the encryption of the information, creation of the digital signature, the control of the keys and the certificates. Cryptanalysis is the opposite of the cryptography. Cryptanalysis studies the decryption of the cipher information without knowledge of the key. Cryptology is a part of the mathematics study about the mathematical footing of the cryptography and cryptanalysis methods. In the currently section some preliminary knowledge about cryptography is introduced.

2.2 CRYPTOGRAPHICAL SYSTEM

As mentioned, a cryptosystem is a system in which information can be made meaningless to all people except the intended reader. In a cryptosystem, the sender (usually called Alice) encrypts a plaintext to a ciphertext before sending and the receiver (usually called Bob) decrypts the ciphertext to obtain the plaintext, see Fig. 1 The term plaintext means the original message or information, which can be a company business plan or a personal medical record, etc., the encryption process make the original information unreadable to general readers. The ciphertext is the encryption process's output which is not recognizable. The decryption process converts the ciphertext back to plaintext for the intended readers.

From the mathematical point of view, the cryptosystem $S = (X, Y, K, f)$ fi is the transformation of the information $f: X \times K \to Y$, defined on the spaces X, Y, K which was the initial states, the final states and the keys respectively. Condition x ∈ X encode some useful information. In the computer cryptography spaces X ⊂ {0, 1} ∗, Y ⊂ {0, 1} ∗, K ⊂ {0, 1} ∗, and the transformation f is given by the algorithm realized with a

Turing machine. The transformation f can be considered as the iteration function of the Cryptographical algorithm (Fig. 1). In this case, the cryptosystem generates the sequences of states $x_0, x_1, x_2, x_2, \ldots x_i$, where $x_i = f(x_{i-1}, k)$, $x_0 \in X$, $k \in K$. This sequence is called a trajectory or the orbit of the system. The overall orbit is determined by the initial state x0 of the system and the parameter k. Such a subsequent transformation of some state by the application of the same primitive function can be seen in the block ciphers, stream ciphers, pseudo-random bit generators, etc. Thus a cryptosystem can be understood as a dynamic system $S = (f, X, K)$, Ki with a nonlinear function f, the state space X, and the parameter space K. As it will be shown below, the requirements for cryptosystems are interrelated with the properties of the chaotic systems.

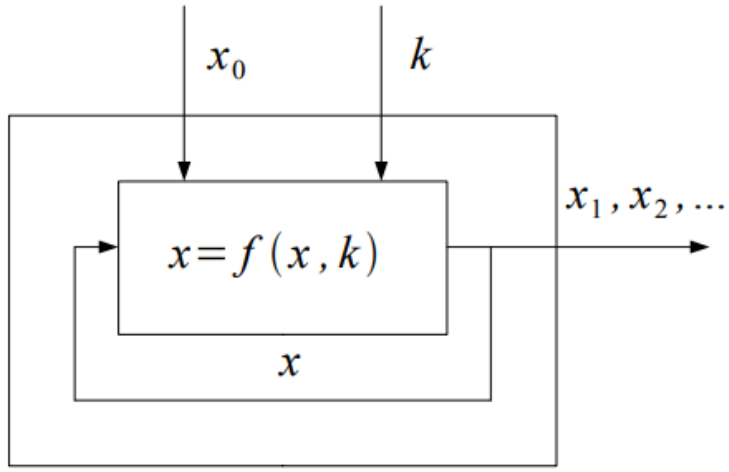

Figure 2.1: The Cryptographical system.

2.3 MAIN DEFINITIONS RELATED TO CRYPTOGRAPHY

Main definitions related to cryptography are presented below [6]:

- A Denotes a finite set called the alphabet of definition. For example, $A = \{0,1\}$, the binary alphabet, is a frequently used alphabet of definition. Note that any alphabet can be encoded in terms of the binary alphabet. For example, since there are 64 binary

strings of length six, each letter of the Czech alphabet can be assigned a unique binary string of length six.

- M Denotes a set called the message space. M consists of strings of symbols from an alphabet of definition. An element of M is called a plaintext message or simply a plaintext. For example, M may consist of binary strings, computer code, English text, etc.

- C Denotes a set called the ciphertext space. C consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for M. An element of C is called a ciphertext.

- K denotes a set called the key space. An element of K is called a key.

- Each element $e \in K$ uniquely determines a bijection between M and C, denoted byE_e. E_e Is called an encryption function. Note that E_e must be a bijection, i.e. one-to-one mapping as the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext.

- For each d ∈ K, D_d denotes a bijection from C to M (i.e., D_d: $C \rightarrow M$). Dd is called a decryption function or decryption transformation.

- The process of applying the transformation E_e to a message $m \in M$ is usually referred to as encrypting m or the encryption of m.

- The process of applying the transformation D_d to a ciphertext c is usually referred to as decrypting c or the decryption of c.

- An encryption scheme consists of a set $\{E_e$: e ∈ K$\}$ of encryption transformations and a corresponding set $\{D_d$: d ∈ K$\}$ of decryption transformations with the property that for each e ∈ K there is a unique key $d \in K$ such that $D_d = E_e^{-1}$; that is, $D_d(E_e(m)) = m$ (1)

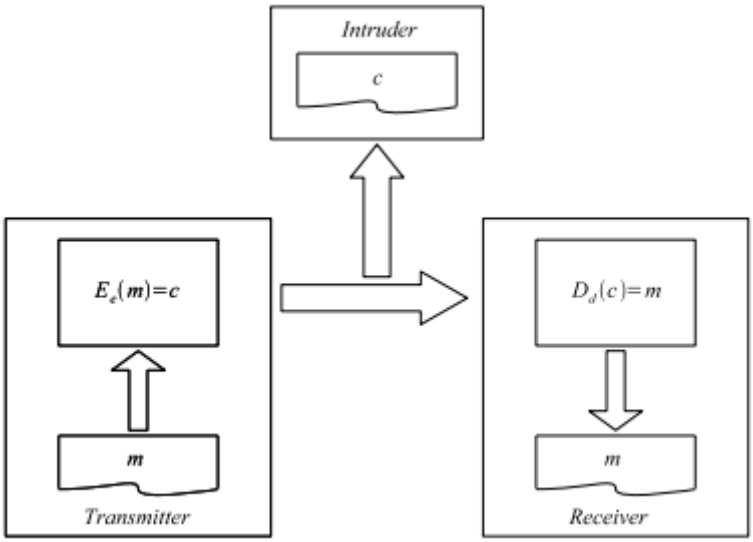

Figure 2.2: The classical encryption/decryption scheme.

For all m ∈ M. An encryption scheme is sometimes referred to as a cipher.

- The keys e and d in the preceding definition are referred to as a key pair and sometimes denoted by (e, d). Note that e and d could be the same. If e = d, then the cryptosystem is refereed as the symmetric one.

- To construct an encryption scheme requires one to select a message space M, a ciphertext space C, a key space K, a set of encryption transformations $\{E_e : e \in K\}$, and a corresponding set of decryption transformations $\{D_d : d \in K\}$.

- Fig. 1.2 illustrates the classical encryption/decryption scheme.

2.4 ENCRYPTION SCHEMES, THEIR CLASSIFICATIONS AND PROPERTIES

Encryption scheme can be written in the following form:

$$S = (E, D, M, C, K), \tag{2.2}$$

where, E : M∗ × K → C∗ and D : C ∗ × K → M∗ , such that for each key e ∈ K exists a unique key d ∈ K and $D_d = E_e^{-1}$, thus

$$\forall m \in M, e \in K \quad \exists d \in K : \quad m = D(E(m, e), d), \tag{2.3}$$

Practically, scheme is assigned by algorithms E, D and spaces M, C, K.

Encryption systems can be classified on the basis of methods of key distribution, or structure of the encryption algorithm. According to the key distribution, encryption systems are categorized as symmetric systems and asymmetric systems

2.4.1 Private Key Cryptosystems

In the private key cryptosystem or symmetric systems, shown in Fig. 3, all users in the communication network (Bob, and Alice in this example) share the same key (Ke = Kd). Both encryption and decryption are done using this key. This type of systems depends on the assumption that the adversaries cannot obtain the secret key which is not always practical. Examples of symmetric encryption are: the Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and RC4.

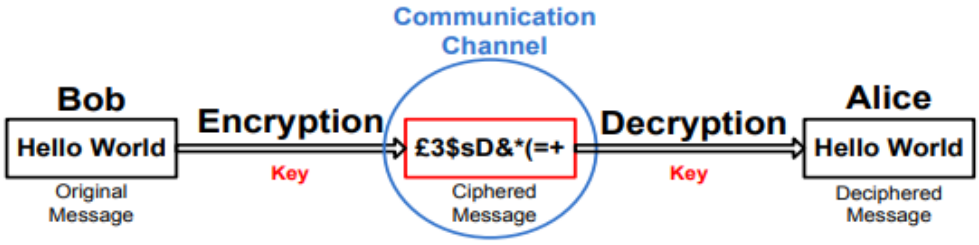

Figure 2.3: Private key cryptosystem scheme

In terms of the output data, symmetric encryption systems can be classified into block ciphers or stream ciphers:

- **Stream ciphers**

A stream cipher is a type of private key encryption where the stream cipher algorithm generates key stream. The key stream bits and the plaintext bits are combined together, usually with the exclusive-or (XOR) operation, and then the result for this combination is the ciphertext. Stream ciphers are considered much faster with lower hardware cost than the block cipher algorithms [7].

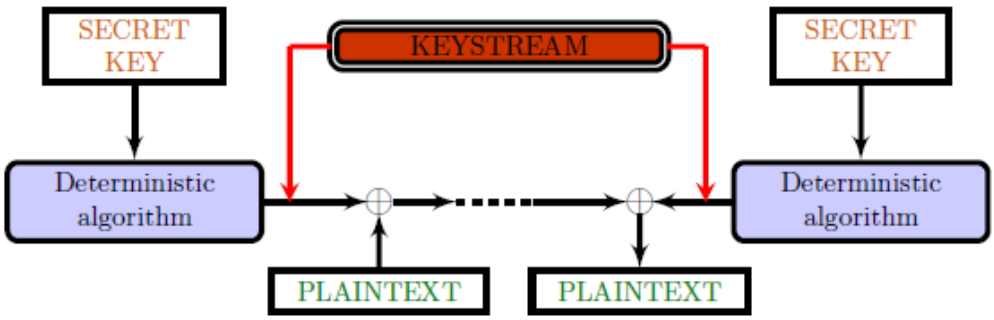

Figure 2.4: Stream chiper

- **Block Ciphers**

A block cipher is a private key encryption that encrypts a fixed-length block of plaintext into same length of ciphertext block. The encryption and decryption in the block cipher are performed by using the same secret key. Typically, a block cipher that takes the input 64-bit block of plaintext must produce the output 64-bit block of ciphertext

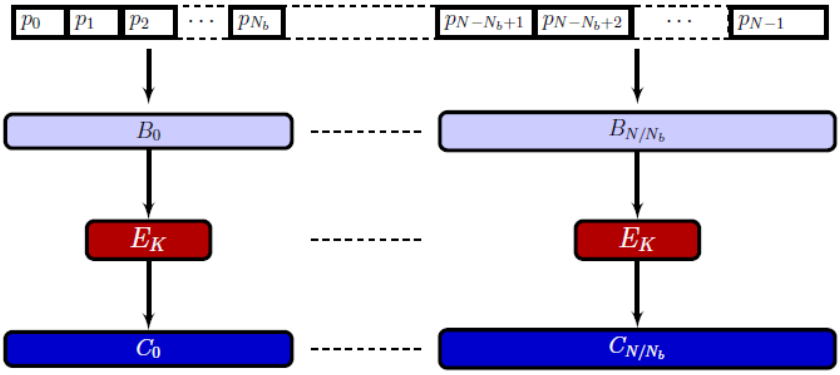

Figure 2.5: Block cipher.

2.4.2 Public Key Cryptosystems

On the other hand Public key cryptosystem or asymmetric systems, shown in Fig. 6, depend on different class of mathematical transformations in which each user in the network has two keys: public and private keys. The public key of each node is announced to every other node whereas the private key is hidden. Messages are encrypted using the receiver's public key and can only be decrypted by corresponding private key (Ke ≠ Kd). The keys are related mathematically through an irreversible function and thus the private key cannot be derived from the public key. Examples of private key encryption are: Digital Signature Algorithm (DSA), and RSA.

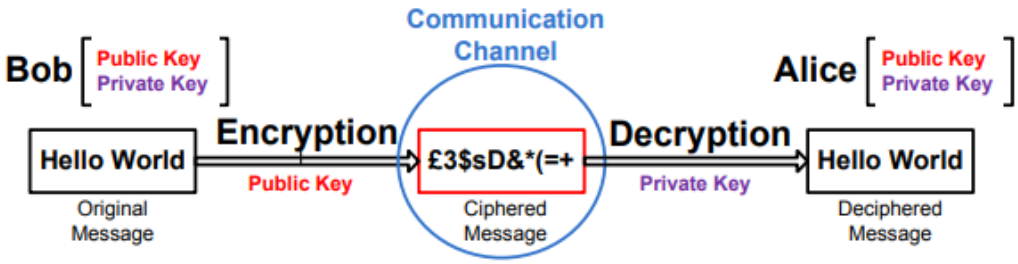

Figure 2.6: Asymmetric systems

2.5 CHAOS AND CRYPTOGRAPHY

In this section, the definitions of the dynamic and chaotic systems are introduced. The

relationship between the properties of chaotic and cryptographic systems is going to be discussed as well.

2.5.1 Dynamical Systems

In many cases, systems that behave close to linear are more predictable, i.e. the output is a direct function of the input. As the nonlinearities of a system become stronger, those outcomes become less predictable. This is the case for dynamical systems that exhibit chaotic behavior. Dynamical systems are mathematical models that provide a rule for how the system changes relative to time [8]. The state of a dynamical system can be visualized as a point and the phase-space of the system is the set of all possible states. In many cases, a dynamical system is the approximation of a system's true dynamics which can be altered by interactions with other systems or by time scales that cannot be incorporated into the model. These time scale changes are often very slow and are therefore incorporated as parameters. The set of all possible parameters is often refered to as the parameter space or control space. There are two types of dynamical systems, discrete-time and continuous-time. Continuous-time dynamical systems can be represented by a system of first order differential equations, $\dot{x}(t) = F'(x(t))$ and are often referred to as flows.

(1) Continuous dynamical system S =< X, K, f >, depending on the parameters, can be presents by the following equation:

$$\frac{dx}{dt} = f(x,k),\ x \epsilon K \in R,\ k \in K \in R \qquad (2.4)$$

Where $f: X * K \rightarrow Y$ is smooth vector function, X is a state space and K is a space of the control parameters. For every initial condition x0 system satisfies the condition of the existence and uniqueness of solutions x (t, x0),

Where x (0, x0) = x0. Curve φt (t, x0) which corresponds to the solution is called a trajectory.

(2) A discrete-time, dynamical system can be presented by the following iteration function:

$$x_{n+1} = f(x_n, k), x_n \in X \in R,\ k \in K\ \in R,\ n = 1, 2,\ .... \qquad (2.5)$$

Where xi are discrete states of the system. Trajectory φ (i, x0) is a sequence of x0, x1,

x2.... It easy do note, that equation (5) resembles a Cryptographical iteration function used in the pseudo-random number generators, block ciphers, etc. (see Fig. 5). Iterative transformation of the information, depends on the control parameter, used in both of the dynamical and Cryptographical systems. Further, the control parameter k in the definitions of the system < X, f > and iteration function f(x), will be omitted.

2.5.2 Chaotic System

Chaos is the phenomenon of apparently random or unpredictable behavior in deterministic systems, it refers to the irregular output of deterministic system whose behavior is difficult to predict because there are so many variable or unknown factors. These systems' state evolves with time and exhibit dynamics and high sensitivity to initial conditions. As a result of this sensitivity, which manifests itself as an exponential growth of perturbations in the initial conditions, the behavior of chaotic systems appears to be random [10], [11]. This happens even though these systems are deterministic, meaning that their future dynamics are fully defined by their initial conditions, with no random elements involved. This behavior is known as deterministic chaos, or simply chaos [12]. This kind of systems can be a simple non-linear equation or a complex prediction mathematical model.

Sensitivity to initial conditions means that each point in such a system is arbitrarily closely approximated by other points with significantly different future trajectories. Thus, an arbitrarily small perturbation of the current trajectory may lead to significantly different future behavior.

Chaos is defined as the property exists in deterministic nonlinear dynamical systems that show random behavior. A dynamical system is referred to a mathematical model, usually for natural phenomena, includes the set of all possible states of the system in addition to a fixed set of equations describing the evolution of the solution with time [36]. Chaotic systems are deterministic since the future behavior of the solution at any state is fully determined by its fixed equations. Nonetheless, the behavior is unpredictable due to the strong dependence of such system on the initial conditions producing an exponential divergence in the solutions [37]. Chaotic dynamical systems can either be continuous or discrete. Continuous dynamical systems can be expressed

as follows:

$$\frac{dx}{dt} = f(x,p),\ x \in X \subseteq \mathbb{R}, p \in P \subseteq \mathbb{R} \quad (2.6)$$

where f is the function determining the behavior of the system, X is the set of the possible state space and P is the space of control parameters. The curve ϕ(t,x) corresponds to the evolution of the system over time and is called the trajectory or orbit. Similarly, discretetime dynamical systems can be expressed as follows:

$$x_{n+1} = F(x_n, \delta),\ n = 1, 2, \ldots \quad (2.7)$$

Where the state variable x and the system parameter δ are scalars, i.e., $x, \delta \in \mathbb{R}$, and f is mapping function defiened in the real domain $\mathbb{R} \rightarrow \mathbb{R}$.

From Eq. (7), it can be seen that one-dimensional chaotic maps refer to those with the relation where the value of xn+1 is determined only by xn. More specifically, this is known as recurrence relation. In chaotic dynamics, iteration is involved, which means to evaluate the map f over and over. [13, 14] For example, logistic chaotic map is one-dimensional chaotic map.

2.5.2.1 Logistic chaotic map

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst. Mathematically, the logistic map is written by:

$$x_{n+1} = r x_n (1 - x_n) \quad (2.8)$$

Where:

x_n is a number between zero and one, and represents the ratio of existing population to the maximum possible population at year n, and hence x_0 represents the initial ratio of population to maximize population (at year 0). r is a positive number, and represents a combined rate for reproduction and starvation.

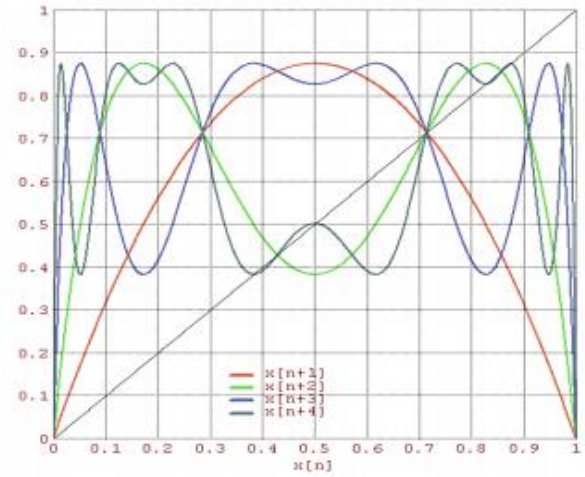

Figure 2.7: Logistic function for r=3.5 after first 3 iterations

2.5.3 Features of Classically Chaotic Motion

Compared with linear systems and other nonlinear systems, the chaotic system has its own characteristics. The main features are:

- Initial value of the sensitivity**:**

Chaos is easy to recognize using initial-value of the sensitivity. With the passage of time, any two adjacent initial conditions will show itself independent of the time. There is sensitive dependence on initial conditions everywhere, e.g. in the famous 'butterfly effect' theory;

- Properties of being bounded:

Chaotic is bounded; its movement is always been limited to a definite region, which is known as chaotic domain;

- Periodicity:

The chaotic motion is ergodic in its chaotic attractor domain, or chaotic in a finite time, where the chaotic orbit passes every state point in the chaotic region, but will never stay at a certain state point;

- Randomness:

Under certain conditions, the situation may change in a qualitative way or make the system chaotic but a status may arise or may not appear;

- Local Instability:

A chaotic system is sensitive to the initial conditions and parameters. Fig. 8 shows the output plot of two orbits of the logic map with red line (r=3.9995) and blue line (r=3.9994), starting with same initial condition $x0 = 0.567021$

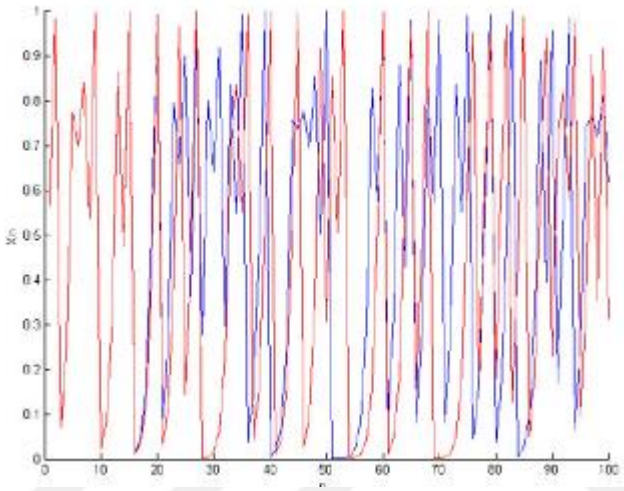

Figure 2.8: Orbits 100 iterations of logistic map using two different System parameter (r)

Fig. 9 shows the output plot of two orbits of the logic map with red line ($x0 = 0.567021$) and blue line ($x0 = 0.567020$) , starting with same r= 3.9995.

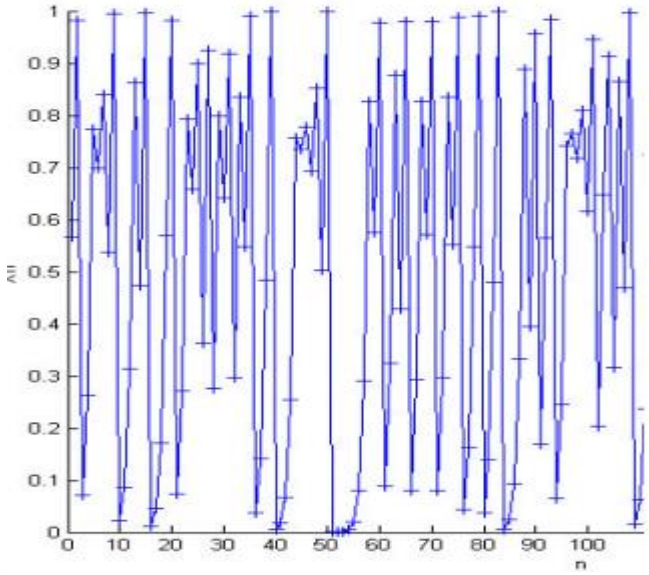

Figure 2.9: Orbits 100 iterations of logistic map using two different initial

- Stochasticity:

The output of normal deterministic dynamic system is easily predictable. However, for a chaotic dynamic system, the output behavior is random-like and hard to predict in long term. Fig.10 shows the random-like output of a logistic map $x0 = 0.565$ and $r = 3.9995$.

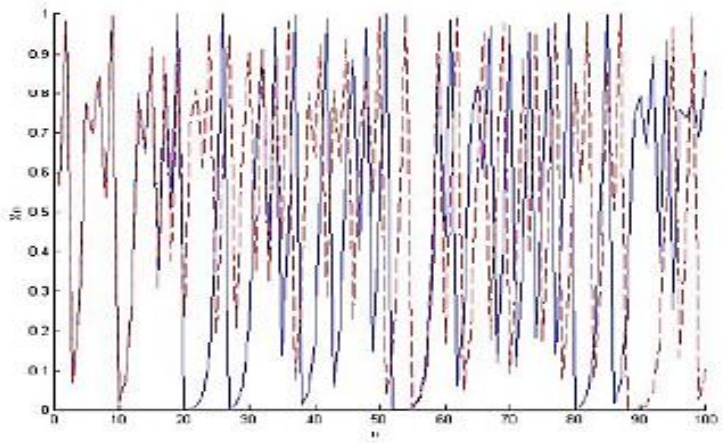

Figure 2.10: Orbits 200 iterations of logistic map using the initial condition = 0.565 with constant system parameter (r= 3.9995)

- Ergodicity:

For a normal deterministic dynamic system, its output is usually periodicity. However, for a chaotic dynamic system, the system output is ergodic (non - periodic).

- Self-similarity:

The progression of the system, in time or space, demonstrates the similar presence at dissimilar scales of observation. This distinguishing feature creates the system to appear auto-repetitive at dissimilar scales of observation [15].

- Universal application:

The so-called universal application refers to demonstrate certain common characteristics for different systems when they approach the chaotic state. They would not be affected by specific parameters of the system or the equation to change;

- Fractal dimension:

It is a geometric feature of a point set in n-dimensional space. It has the infinitely divisible structure.

- Long-term unpredictability :

Because initial conditions are confirmed to a limited precision, the initial conditions of small differences could have enormous consequences, so it is not possible to predict long-term future of a chaotic system at the dynamics;

2.6 CHAOTIC SYSTEM FOR CRYPTOGRAPHY

Because a chaotic system is sensitive to initial conditions, small errors in some initial values errors can be enlarged by system. Therefore, the system development in anticipating is unpredictable; also because chaotic sequence has good statistical properties, it can generate random numbers. These characteristics are well suited to sequence encryption technology. According to the information theory of mathematician Shannon's when some methods are used to produce a random sequence, the sequence can only be identified by the key. Any input of a slight change may lead to a significant effect, thus the sequence can be encrypted. [16] A chaotic system can precisely meet such requirement.. Owing to the characteristics of a chaotic system, its numerical distribution does not conform to the principle of probability statistics and no stable probability distribution characteristic can be obtained. In addition, a chaotic number set

is real valued, and can be extended to the complex value domain. Therefore, employing the principle of the chaos theory to encrypt the data can guard against attacks like frequency and exhaustive attack, so that it is difficult to analyze and decipher the password.

There are some similar properties between chaotic systems and traditional cryptographic algorithms. In cryptographic algorithms, diffusion and confusion are applied on plaintext over the encryption rounds of the algorithm. In chaotic systems, similar things happen on the initial input parameters. After a sufficiently large number of iterations, an input parameter will be eventually spread over the entire phase space through the random-like orbit over iterations. The stochasticity property of a chaotic system is similar to the diffusion and confusion properties of cryptographic algorithms. For cryptographic algorithms, in order to decrypt the ciphertext to the original plaintext correctly, the same key should be used in both encryption and decryption. This is just similar to the requirement that chaotic systems need the same input parameter to reproduce the same output orbit. In this case, the system parameters and initial conditions can be considered as the private key of a chaotic cryptosystem. The table 1 summaries the common relationship which promotes chaos theory into practical cryptographic design [17, 18].

Table 2.1: Similarities and differences between chaos and cryptography

Chaotic system	**Traditional cryptosystems**
Ergodicity	Confusion
Sensitivity to initial condition and system parameters	Diffusion
Parameters	Encryption key
Iterations	Cipher rounds

In other words, confusion in traditional cryptosystems causes plaintext transforming to random ciphertext such that there should be no repeated pattern in the ciphertext. By the same token, the trajectories of chaotic systems pass through all points f the phase space generally with uniform distribution, which means, it is very difficult to predict the final position of one point from its initial position. It is indeed the concept of ergodicity which can be associated with confusion in cryptosystems.

To develop a good cryptosystem, anther essential design principle is the property of diffusion. By doing so, a totally different ciphertext is resulted no matter how one bit of key or plaintext is changed. This implies that the system is sensitive to plaintext and its encryption key. On the other hand, recall that the chaotic systems highly depend on initial conditions and parameters. A small variation in any of the system parameters or initial points leads to the trajectories diverged significantly. In this regard, chaotic systems and cryptosystems can naturally benefit from each other.

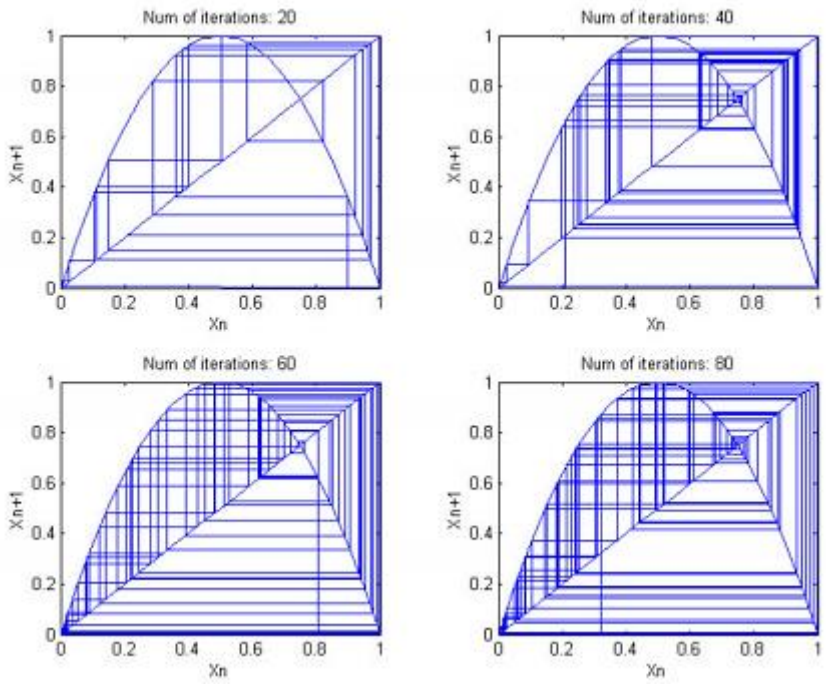

Figure 2.11: The orbits of the logistic map at different number of iterations

2.6.1 Comparison Of Chaotic And Cryptographic Properties

In the review article of 2006, Alvarez & Li have made the comparison between the two very clearly [19]:

- Periodicity, Mixing property and Auto- similarity in chaotic compare with the confusion in cryptography where the output of the system seems similar for any input.

- Sensitivity to introductory conditions and control parameters in chaotic relate to Diffusion in cryptography where a small difference in the input produces a very different output.

- Deterministic property of chaotic relate to deterministic pseudo randomness where a deterministic procedure is one that produces pseudo randomness.

- Complexity of chaotic relates to algorithmic complexity of cryptography where a simple algorithm produces highly complex outputs.

2.6.2 Performance Evaluation of Chaotic Encryption Algorithm

According to some studies of pseudorandom bit generator using the statistical test suite of the U.S. National Institute of Standards and Technology (NIST), a chaotic encryption algorithm should be divided into three parts: security, costs and applicability. (Andrew *et al.*, 1997) They introduce a Lorenz chaotic encryption algorithm, and set a standard of encryption algorithm, to compare the current encryption algorithms.

- Security analysis

First of all, the chaotic system is very sensitive to the parameters and the initial values; it can provide a large key collection to fully satisfy the meet for the encryption. Through examining the binary sequence generated by the chaotic system, the distribution of 0 and 1, when the run-length meets the requirement of random sequence, it can be treated as random sequence. Secondly, chaotic encryption is a kind of stream encryption; so it invulnerable to attacking methods that aim at grouped encryption. Besides, for attacking

methods aiming to decipher text, it is not impossible to guess the key through XOR operation because of the unidirectional and iterative nature of chaotic signals.

- Cost analysis

Algorithm cost includes time cost and spacing cost. Time cost includes time of preparation and time of encryption. Usually, preparation time prior to the encryption is used to create sub-key encryption; encryption time is mainly used for the exchange of deciphered text data under encryption control. As a king of stream encryption, chaotic encryption has short preparation time. Since XOR operation is carried out each bit of data, time is mainly spent on the generation of key stream. Compared with current popular grouped encryption algorithms, it takes much less time. Run-state space refers to the temporary space needed by the algorithm during the encryption process. Because chaotic encryption algorithm has no *S*-box spaces, few temporary variables, and it is able to generate key stream by cycling, which requires less space to store variables, therefore, it occupies less space during run-time, which suggests it is outstanding on spacing costs.

- Applicability:

The encryption and decryption processes of chaotic encryption algorithm can be reused; thus, the occupied space is compressed. It has good applicability to both hardware and software of information security. The algorithm has been implemented by using C++ and JAVA. DSP is designed and developed based on such an algorithm.

2.7 CONCLUSION

This chapter introduced some preliminary knowledge about cryptography and chaotic dynamics. The main purpose was to show that there is close relation between cryptography and dynamical systems theory. Therefore, methods from automatic control theory can be considered for application in cryptography. The analogy between dynamical systems theory and cryptography is readily illustrated by Tab.1

3. IMAGE ENCRYPTION USING CHAOS: RELATED WORK

With the increasing reliance on communications via the Internet and networks, many forms of data, such as text, audio, image and video, can be transmitted digitally, images being the most widespread and oldest encryption techniques such as: AES, DES, RSA, etc. are not applicable in image encryption. This problem has been solved using chaos encryption, which is an acceptable form of encryption for image data. Sensitivity to initial conditions and control parameters makes chaos encryption suitable for image applications. This study discusses various techniques of encryption of chaos. This chapter presents a literature review on chaos-based image encryption and cryptosystem analysis methods.

3.1 IMAGE ENCRYPTION

Image data characteristics are totally different from text data in terms of the nature of the bits constituting image pixels and accordingly in terms of the security requirements in encryption algorithms. Some features of image data are summed in [38] as: high redundancy, bulk capacity, uneven distribution of color intensities, and strong correlation between pixels in the horizontal, vertical, and diagonal orientations. Such characteristics impose the following challenges in the image encryption [38]: 1. Bits in the ciphered image should appear random with uniform histogram and do not imply any statistical relationship about the original image. 2. Correlation in the ciphered image is kept minimal in all directions. 3. Encryption is done for the whole image with equal security levels. Perhaps the most important requirement in image encryption is to satisfy the confusion and diffusion properties identified by Shannon [16]. Confusion in image encryption refers to changing the value of each pixel in the original image through a complex transformation. The relationship between original pixels and the corresponding ciphered ones cannot be determined easily. Diffusion refers to the property of dividing the influence of each bit in the original image over many bits in the ciphered image. Consequently a change in one bit in the original image results in a completely different ciphered image.

3.2 CHAOTIC IMAGE ENCRYPTION

The properties of chaos comprise unpredictable behavior, deterministic dynamics, and non-linear transform and can be used for chaotic image encryption. This concept leads to techniques that can simultaneously offer security functions and an overall visual check, which might be appropriate in some applications. Digital images are widely used in various applications, like military, legal and medical systems and these applications necessitate controlling access to images and providing the means to validate integrity of images.

Block encryption is a scheme in which the plain text is divided into blocks of fixed length, and encryption of one block is done at a time. Whereas, stream ciphers are based on generating an "infinite" cryptographic key stream, and use this key stream to encrypt one bit or byte at a time. The Table 1 shows the review of Block and Stream cipher image encryption schemes considering the parameters discussed by the various researchers in their work.

3.3 ARCHITECTURE OF CRYPTO CHAOTIC IMAGE SYSTEMS

A typical architecture of existing chaos-based image cryptosystems is shown in Fig. 12. It consists of two stages, namely; confusion and diffusion stages. In the confusion stage, permutations of image pixels are done in a secret order, without changing their values. The purpose of the diffusion stage is to change the pixel values sequentially so that a small change in one pixel is spread out to many pixels, with anticipation to the whole image. To décor relate the affiliation between adjacent pixels, the confusion stage is performed n times, where n is usually larger than 1, followed by the diffusion stage. The complete n-round confusion and single round diffusion repeat form times, with m usually larger than 1, so as to get an acceptable level of security. The parameters of the chaotic maps leading the permutation and the diffusion should better be dissimilar in different rounds. This is obtained by a round key generator with a seed secret key as input.

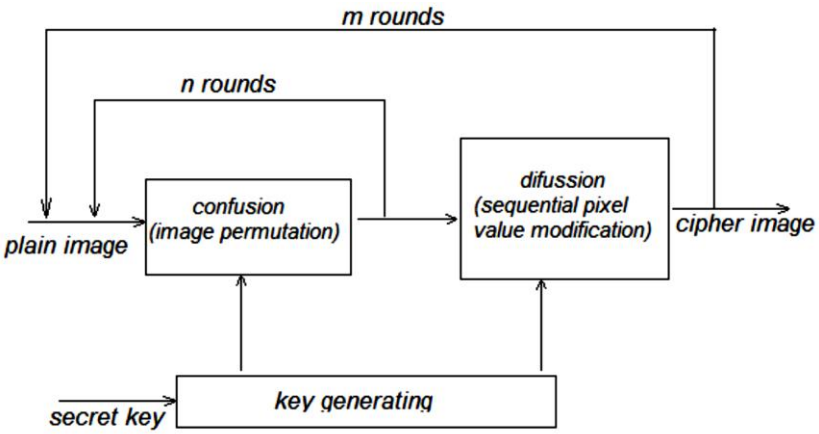

Figure 3.12: Schéma général de cryptage d'images basé sur le chaos

3.3.1 Criteria for Analyzing an Image Encryption Algorithm

- Key space:

The size of the key space is the number of encryption / decryption key pairs that are available in the encryption system [20]. A necessary but not sufficient condition for an encryption scheme to be sure is that the key space is large enough to provide security against brute force attack.

- The histogram:

The histogram is used to represent the graphical distribution of pixels in an image by plotting the total number of pixels at each gray level value. In an image processing context, the histogram of an image designates a histogram of is a graph illustrating the number of pixels in an image at each intensity value found in that image. In an image encryption context, the histogram of the encrypted image must be uniform so that an adversary cannot extract any information from this histogram [21]. Pixel intensity values.

- Correlation:

Correlation is a technique that makes it possible to compare two images to estimate the displacements of the pixels of an image relative to another reference image. Adjacent pixels in a standard image have a strong correlation. A good image encryption scheme

should remove such a correlation to ensure security against statistical analysis. In order to test the correlation between two images, 10,000 pairs of two adjacent pixels are randomly selected in the three directions; horizontal, vertical and diagonal from the components R, G, B of the clear image and its encrypted image and the correlation coefficients of each pair were calculated using the following formulas:

$$\text{coefficient de corrélation} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{3.9}$$

Where covariance of x, y is: The result of the calculation is a real value belonging to the interval [0,1]. If the coefficient is 1 then the two images are equal. Otherwise, If the value obtained is 0 or close to 0 then the two images are different [21].

- Entropy:

The entropy of an information is the amount of information encompassed or released by an information source. In particular, the more redundant the source, the less information it contains. High entropy values show a high degree of randomness; and for any message coded on M bits, the upper limit of the entropy is M. The formula used to compute the entropy of a source m is as follows:

$$H(M) = \sum_{i=0}^{2^n-1} p(m_i) \log_2\left(\frac{1}{p(m_i)}\right) \tag{3.10}$$

Where P (Ci) represents the probability of occurrence of the symbol Ci, M × N is the total number of symbols. For an 8-bit gray-scale image, the theoretical maximum entropy value is 8 bits / symbol, which occurs when all pixel values are equiprobable or the histogram is flat. The entropy of the image shows the distribution of the value of the gray level. The uniform distribution of gray levels indicates higher entropy. So for a crypto system of perfect image encryption the value of the entropy must be very close to 8 for each plane.

- Differential attacks:

In order to detect the relationship between the original image and the encrypted image, an opponent makes a small change on the clear image, then uses the encryption algorithm to encrypt the image before and after the change, in order to test how a small change in the original image affects the encrypted image. This kind of attack is called

differential attack.

To ensure the security of an image encryption scheme against differential analysis, two quantitative measures are used: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI).

The NPCR represents the rate of different pixels between the two encrypted images, while the UACI represents the difference of the average intensity. The formula used to calculate these two percentages is defined as follows:

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \quad (3.11)$$

$$UACI = \frac{1}{M \times N} [\sum_{i,j} \frac{c1(i,j) - c2(i,j)}{255}] \times 100\% \quad (3.12)$$

3.4 IMAGES BASED CHAOS ENCRYPTION SCHEMES

Obtaining a consistent method for encryption has always been necessary even in the past. Expertise has improved to take into account simpler and improved encryption and transmission, so that it has also enabled the development of interception and cryptanalysis.

Several image encryption algorithms based on conventional encryption methods (RSA, DES and AES) are present but have failed since digital images are characterized by high redundancy, high correlation and large size. Therefore, a special interest is needed when encrypting this data. According to Shannon [16]: confusion (substitution) and diffusion (permutation) are the two main methods for eliminating high redundancies and high correlation. Confusion creates a strong relationship between the key and the ciphertext. On the other hand, the diffusion reduces the redundancy of the plaintext in the propagation on the total ciphertext.

In recent years, encryption technology has been developed rapidly and many image encryption methods have been put forward. The chaos-based image encryption technique is a new encryption technique for images. It uses a random sequence of chaos to encrypt the image, which is an effective way to deal with the intractable problem of fast, highly secure image encryption.

The advantage of using chaos in secure communication is to obtain additional unpredictability and randomness in the data.

In this part we present various techniques of image encryption based on chaos by classifying encryption techniques according to two main categories such as flow and block encryption schemes.

3.4.1 Block Image Encryption Schemes

- Image Encryption Using Random Bit Sequence Based on Chaotic Maps 2014

Himan Khanzadi et al. [22], proposed an algorithm for image encryption using the random bit sequence generator based on chaotic maps. To generate random bit sequence, chaotic logistic and tent maps are used and pixels of the plain image are permuted using these chaotic functions. The image is partitioned into eight bit map planes and in each plane, bits are permuted and substituted according to random bit and random number matrices. Based on the chaotic random Ergodic matrix, the pixels and bit maps permutation are evaluated. Performance of the scheme is evaluated using chi-square test, correlation coefficient, number of pixel of change rate (NPCR), unified average changing intensity (UACI), and key space. The histogram of encrypted image is approximated by a uniform distribution with low chi-square factor. Experimental results and analysis shows that the scheme exhibits good properties to resist attacks. Total key space is 2∧2,160, which is large enough to resist any bruteforce attack.

- Image Encryption Block-Wise with Multiple Chaotic Maps for Permutation and Diffusion, 2016:

Gopalakrishnan and al. [23] have suggested another algorithm for image encryption based on various chaotic maps. The algorithm integrates the notion of permutation of pixel positions. The encryption process consists of dividing the original image into 8×8 size blocks, and then different chaotic cards are used for five steps of the proposed encryption algorithm. First, the cubic map is used to swap the pixels that are contained in the blocks. Second, the Henon map was used to broadcast the permuted pixels. Third, a quadratic map has been worked on to swap the blocks. Fourth, a logistics map was used to swap all the entire pixels of an image. Finally, the Henon map was applied to diffuse the permuted image using the XOR operation.

- Image Encryption Based on Diffusion and Multiple Chaotic Maps,2011:

G.A. Sathishkumar and al. [24] proposed encryption algorithm belongs to the category of the combination of value transformation and position permutation In this , two different types of scanning methods are used and their performances are analyzed. In the typical schematic of the proposed method first, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using logistic map sub key and in its transformation leads to diffusion process. Third, sub keys are generated by four different chaotic maps and images are treated as a 1D array by performing Raster scanning and Zigzag scanning. The scanned arrays are divided into various sub blocks. Then for each sub block, position permu action and value transformation are performed to produce the encrypted image. The sub keys are generated by applying the suitable chaotic map banks. Based on the initial conditions, the generated chaotic map banks are allowed to hop through various orbits of chaotic maps. The hopping pattern is determined from the output of the previousmap.Hence for each sub block various chaotic mapping patterns are applied which further increases the efficiency of the key to be determined by the brute force attack. In each orbit, a sample point is taken and used as key for a specific block and a condition to choose the particular orbit in a particular map is adopted. Then, based on the chaotic system, binary sequence is generated to control the bit-circulation functions for performing the successive data transformation on the input data. In addition to chaotic features of mixing, unpredictable, and extreme sensitive to initial seeds, through multiple chaotic maps and orbits hopping mechanism spread out the pseudo random number base to a wide flat spread spectrum in terms of time and space.

- A Novel Image Encryption Algorithm Based on Bit-level Improved Arnold Transform and Hyper Chaotic Map, 2015

Bouslehi Hamdi et al. [25] invented a 4-dimensional hyper-chaotic system from Lorenz's chaotic system to perform image encryption. Hyper chaotic sequences generated with a new method are used to generate key sequences that are used for image encryption. This article has followed the same method of chaos encryption as the majority of the work in

the block encryption process but the deference lies in the process of permuting pixels in the image. First the image is broken into four blocks and the image pixels are switched using a random function and linear permutation function diagonal permutation, the logic function "XOR" and the changing intensity function. Security analysis, including randomness, entropy of information and key sensitivities. The randomness of the proposed system increases the robustness of the algorithm.

- A new image encryption method: Parallel sub-image encryption with hyper chaos, 2012:

Omid Mirzaei and al. [26] proposed an image encryption scheme, based on a total pixel mixing and parallel encryption algorithm. The image encryption algorithm combines the Lorenz and Chen chaotic systems to confuse the relationship between the original image and the encrypted image. The size of the original grayscale image is M × N. The original image is first divided into 4 subpictures, then the position of each subpicture is altered randomly using the logistic map by the then a total confusion matrix is used to mix the position of the pixels in the entire image, then the sub-images are encrypted simultaneously in parallel. The security analysis is done by key space analysis, key sensitivity test, adjacent pixel similarity and encryption speed.

3.4.2 Stream Image Encryption Scheme

- An efficient chaotic image encryption algorithm based on a generalized Arnold map, 2012:

Guodong Ye and Kwok-WoWong [27], proposed an efficient image encryption algorithm using the generalized Arnold map. The conventional confusion-diffusion architecture is adopted, in which the keystream used depends on the plain-image. Two stages, i.e., permutation and diffusion are composed in the algorithm. To substantially reduce the correlation between adjacent pixels, a total circular function rather than the traditional periodic position permutation is used in the permutation stage. Whereas,

double diffusion functions like positive and opposite module are utilized with a novel generation of the keystream in the diffusion. Experimental result and analysis show that the scheme can resist known- and chosen-plaintext attacks. In future, the scheme can be extended to adopt other chaotic systems by simply changing the generation of the chaotic sequences in the confusion stage. As mentioned by the authors, the scheme can also adopt high-dimensional chaotic systems such as Chen's system, spatial chaotic system, and 3D cat map.

- Designing a multi-scroll chaotic system by operating Logistic map with fractal process, 2017

Nabil Ben Slimane et al. [28] ont présente un nouveau système chaotique basé sur le processus fractal de Julia, les attracteurs chaotiques et la carte logistique dans un ensemble complexe. L'algorithme de cryptage se compose de deux étapes principales: la confusion et la diffusion. L'analyse de sécurité, y compris l'analyse des attaques différentielles, les tests statistiques, l'analyse des espaces clés, le test d'entropie de l'information et le temps de fonctionnement.

- New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos, 2013:

LEI Li-hong and al. [29] proposed a new image encryption algorithm based on logistic map and hyperchaotic systems, two kinds of keys were produced by using logistic chaotic iteration and hyper chaotic systems. The two kinds of keys are alternately used in the image encryption process, so the the encryption keys have a better random distribution. The encryption algorithm introduced Ciphertext cross-diffusion to increase the ciphertext sensitivity .The simulation results of the experiment showed the evenly distributed ciphertext pixels, the large key space, the small correlation of neighbor ciphertext pixels, highly sensitive keys and so on. Therefore, the algorithm has some potentiality in the field of image secure storage and image secure communication.

- Multi chaotic systems based pixel shuffle for image encryption, 2009

C.K. Huang and H.H.[30] Nien introduces a new pixel shuffle technique with multi chaotic systems for the image encryption. Since the chaotic system is highly sensitive to initial values and system parameters, meanwhile, has an enormous key space, the proposed method combined with four chaotic systems and pixel shuffle can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. We conduct FIPS PUB 140-1, correlation coefficient, NPCR, and UACI to test on the security analysis and the distribution of distinguished elements of variables for the encrypted image. The adopted examples show the highly confidential encrypted images and demonstrate a good potential in the application of the digital-color image encryption [2].

- A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme, 2014

Xianhan Zhang and Yang Cao [31] suggested a one-dimensional chaotic map which exhibits a larger maximal Lyapunov exponent, indicating better properties of the chaotic map. A new algorithm based on this new chaotic map is used in image encryption, providing a brand new way to encrypt images. It also entails another classical map: Arnold's Cat Map, through which the coordinates of the target image's grey value matrix will be changed to another. Here, the safety of the image is largely strengthened and guaranteed.

- A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map, 2012

XiaoJun Tong and al. [32] proposed encryption algorithm includes two parts: firstly, the positions of the original image pixels are permuted by Baker map; secondly, the values of the permuted pixels are encrypted by multiple chaotic map The security analysis of the proposed image encryption is discussed here, such as sensitivity analysis, statistical analysis, sp800-22 testing, and entropy testing and so on to prove that the proposed encryption scheme is secure against the most common attacks. A fast image encryption scheme is proposed which utilizes dynamical multiple-chaotic map confuse the

relationship between the cipher image and the plain image. Baker map is used to permute the positions of image pixels in the spatial-domain and the mixing of confusion and diffusion can produces more randomness. The experimental results demonstrate that image encryption technique has advantages of high-level security, such as high robust against statistic attacks and the precision of cipher be sensitive to the secret key approach to 10-14. At the same time, the probability of precision degradation is lower than simple-chaotic map encryption scheme and has high encryption than other famous encryption methods .

3.5 COMPARAISON AND ANALYSIS

The schemes discussed in the previous section are compared and analyzed here in this section. The security of image encryption schemes can be determined by some tests. These tests include key space tests, statistical tests and differential tests. We have considered only those tests in which plain image 'lena' is used such that uniformity for comparison can be achieved. Based on the test parameters, table 2 and 3 below shows the comparison between various schemes discussed in the previous section.

Table 3.2: Comparison of different block encryption techniques

Block encryption scheme					
S. No	**Parameter**	**[22]**	**[23]**	**[25]**	**[26]**
1	Method	random bit sequence generator and based on chaotic maps	Multiple chaotic maps	Arnold transform and hyper chaotic maps	Hyper chaos systems
2	Histogram distribution	Fairly Uniform	Fairly Uniform	Fairly Uniform	Fairly Uniform
3	Key Space	2^{212}	-	2^{200}	2^{296}
4	Correlation of adjacent pixels (Horizontal)	0.00059387	-0.0021	-0.0023	−0.0893
	Vertical	0.0041	0.0023	-0.00005121	0.0034
	Diagonal	0.0048	0.0132	-0.0015	0.0010
5	NPCR	99.61	99.27	99.6056	-
6	UACI	33.35	33.46	33.5842	-
7	Advantage	High level security	Fast encryption speed	good, resistance to brute-force attack,	Big space sequence
8	Disadvantage	Limited key space	Limited perceptual quality.	Plain-image must be square size	Bed resistance to brute-force attack,

It can be analyzed from table 2 that the schemes exhibit good properties to resist different attacks. Some schemes [22] and [26] possess good properties to resist statistical attacks as their correlation values are very close to zero as compared to other ones. Whereas on the other side, other schemes [22] and [25] have good resistance to differential attacks.

Table 3.3: Comparison of different stream encryption techniques

Stream encryption scheme					
S. No	Parameter	[27]	[28]	[29]	[32]
1	Method	generalized Arnold map	chaotic attractors and Logistic map in a complex set	Arnold transform and hyper chaotic maps	Logistic Map and Tent Map
2	Histogram distribution	Fairly Uniform	Fairly Uniform	Fairly Uniform	Fairly Uniform
3	Key Space	-	10^{84}	10^{44}	10^{14}
4	Correlation of adjacent pixels (Horizontal)	−0.06153	0.002951	0.1257	0.0076856231
	Vertical	0.07700	0.010921	0.0581	0.0128994115
	Diagonal	−0.07236	0.000289	0.0504	0.0129194833
5	NPCR	99.774	99.6188	99.42	99.51
6	UACI	34.339	33.4773	27.78	33.44
7	Advantage	High level security	Fast encryption speed	Good key space	high robust statistic attacks
8	Disadvantage	Limited key space	-	Not resistible for statics attacks	Limited key space

3.6 DISCUSSION

Ensuring the security of digital images distributed or saved in a non-network is strongly related to the image encryption algorithm used. However, current encryption techniques, such as AES, DES, and RSA, are not suitable for image data encryption and cannot guarantee the privacy and security of data due to the size and redundancy of images. In order to overcome this problem, several image encryption cryptosystems have been proposed based on different techniques and strategies. Nevertheless, most of these cryptosystems suffer from one or more problems such as low sensitivity to clear image

variation, restricted key space [24] [25], weak keys and equivalent keys. Irresistibility to clear text attack known and irresistibility to clear text attack chosen.

Chaos-based algorithms have shown remarkable properties in many aspects related to security, complexity, performance, speed, and so on. The possibility of self-synchronization of chaotic oscillations has triggered a flood of work on the application of chaos in cryptography.

The fundamental characteristics of chaotic maps have absorbed the consciousness of cryptographers because they have many properties such as erodicity, sensitivity to initial conditions, nonlinear, deterministic, complex behavior, and so on. Most properties are related to certain requirements such as mixing and spreading cryptography

According to the Chaos Encryption Technique Literature Study, it has been concluded that encryption methods based on chaotic systems [31] [32] despite its advantages for the image security chain pose major problems:

(1) Encryption methods based on one-dimensional (1D) continuous chaotic systems show the problem of low key space in front of the huge amount of information transmitted and the lack of control parameters for secure encryption against the attack. Brute force.

(2) the existing system will take a lot of computing time that the inapplicable for real-time systems or modern communication systems so are not effective for network systems

(3) Currently, most studies on chaotic encryption technology are based on one dimension and two dimensions. Some studies suggest that the confidentiality of the low dimension is not sufficient. Numerous small-scale chaotic encryption solutions have been proposed in recent years, but all of them have more or less gaps in confidentiality. It is generally accepted that many current chaotic encryption solutions have security vulnerabilities.

To improve security, the following methods can be considered:

(1) Design quasi-chaotic sequences with complex and dynamic behavior, a long time. Thus, the development of a multi-dimensional chaotic encryption system is essential to the design of a robust chaotic encryption system, and the design of high-quality chaotic sequences is essential to the development of a high-quality chaotic encryption system.

(2) Explore the possibility of using chaotic or chaos-based encryption techniques to protect remote sensing satellite images and provide a high level of security in an efficient and reliable manner.

3.7 CONCLUSION

Dans ce chapitre on a donné un aperçu sur les concept fondamentale de la cryptographie en présentant la relation ente eu la théorie de chaos en en premier lieu ensuite on a présenté une revue de littérature sur les différents méthodes de cryptage de l'image numérique basé sur les systèmes chaotiques ainsi les paramètres de performance et d'évaluation de sécurité existants par la suite on a élaboré une étude comparative en se basant dans cette étude sur les paramètres d'évaluations considère et la méthode utilisé pour chaque article afin de dégager les inconvénient des algorithme dans une problématique .

4. STUDY AND DEVELOPMENT OF NEW COLOR IMAGE ENCRYPTION SCHEME BASED ON MULTIDIMENSIONAL CHAOTIC SYSTEMS

This chapter is intended for our research contributions in the field of image encryption. This is a new symmetric encryption scheme based on the stream encryption scheme and which makes a strong relationship between the encrypted image and the secret key to prevent knowledge of the clear image without the knowledge of the key. The proposed encryption algorithm is based on three-dimensional chaotic systems and the permutation-diffusion structure. Unlike permutation-based cryptographic systems with small key spaces, the proposed image encryption algorithm has a large key space. Thus, it prevents brute force analysis. The results of the simulation show the efficiency and safety of our proposed system. In addition, the AES algorithm and other symmetric algorithms have been investigated and the comparison with the proposed algorithm shows the superiority of the proposed scheme. On the other hand, the calculation of the number of primitive instructions of the proposed schema asserts that our contribution is the fastest by comparing it with recently proposed algorithms.

4.1 CHAOTIC SYSTEMS

Chaos theory is a field of study in mathematics which studies the behavior of dynamical systems that are highly sensitive to initial values and parameters—an effect which is popularly referred to as the butterfly effect. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general.

In mathematics, a chaotic map is a map that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Continuous maps usually take the form of iterated functions. Their properties are similar to confusion and diffusion cryptography properties, so they have been used to build good cryptosystems. Furthermore, these properties make chaotic cryptosystems robust against statistical attacks. Chaotic maps often occur in the study of dynamical systems.

In this section we present a mathematic study for continuous chaotic system used in our cryptosystem for color image

4.1.1 Aizawa Attractor

The Aizawa attractor is a system of equations that, when applied iteratively on three-dimensional coordinates, evolves in such a way as to have the resulting coordinates map out a three dimensional shape, in this case a sphere with a tube-like structure penetrating one of it's axis. The Aizawa attractor is a special case of the Lorenz attractor [34] . The equations themselves are fairly straightforward:

$$\begin{cases} \frac{dx}{dt} = (z-\beta)x - \delta y \\ \frac{dy}{dt} = \delta x + (z-\delta)y \\ \frac{dz}{dt} = \gamma + \alpha z - \frac{z^3}{3} - (x^2+y^2)(1+\epsilon z) + \sigma z x^3 \end{cases} \quad (4.13)$$

for $(x, y, z) \in \mathbb{R}$ and parameters $\alpha, \beta, \gamma, \delta, \rho$ and ϵ Commonly used values of the parameters in visualizations are $\alpha = 0.95; \beta = 0.7 ; \delta = 3.5; \epsilon = 0.25; \gamma = 0.6$; and $\sigma = 0.1$. The solution to the Aizawa equation (13) with these parameters and initial value $x_0 = (0.1,0,0)$ is pictured in Figure 13.

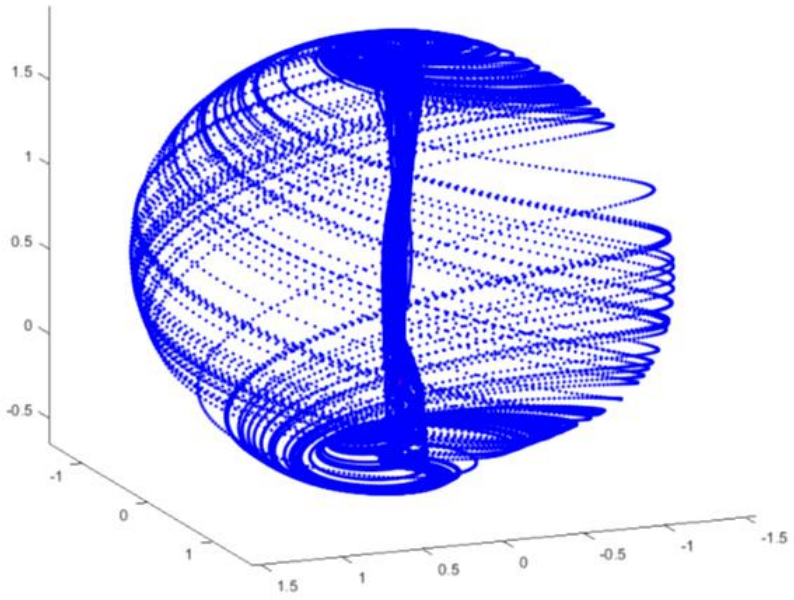

Figure 4.13: Aizawa Attractor α=0.95

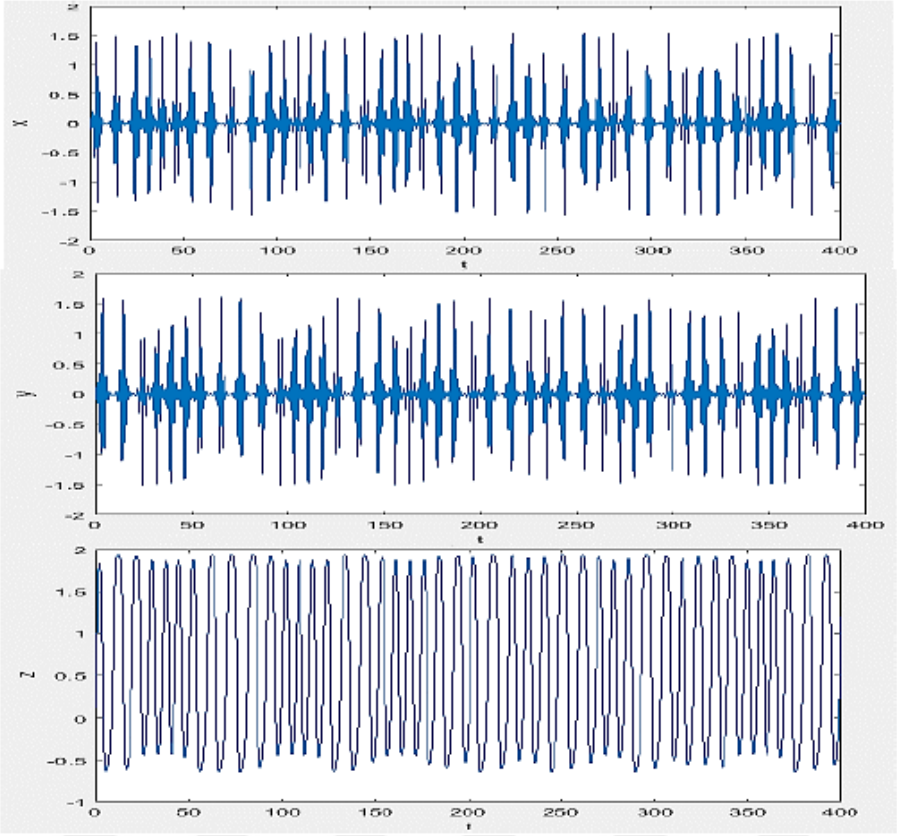

Figure 2.14: Evolution of the axes in time

4.1.2 Three Scroll Unified Chaotic System 1

The unified three-scroll chaotic system (TSUCS) was introduced by Lin Pan, Wuneng Zhou, Jian'an Fang and Dequan Li in 2010 [33]. The system is described by the following three-dimensional equations:

$$\begin{cases} \frac{dx}{dt} = a(y - x) + dxz \\ \frac{dy}{dt} = bx - xz + fy \\ \frac{dz}{dt} = -ex^2 + xy + cz \end{cases} \quad (4.14)$$

In (10), x, y, z are state variables and a, b, c, d, e, f, are positive constant system parameters. The system shows a chaotic attractor (see figure. 15) if the value of the system parameter is chosen as follows:

a = 40, b = 55, c = 11/6, d = 0.16, e = 0.65, f = 20 (4.10)

For mathematical simulations, the initial state value of the chaotic system (14) is assigned as follows: x (0) = 0.0001, y (0) = 0.0001, z (0) = 0.0001 (4.11)

Figure (15) shows the 3D view of the attractor of the new chaotic system (14) of the three-scroll attractor on the three coordinate planes.

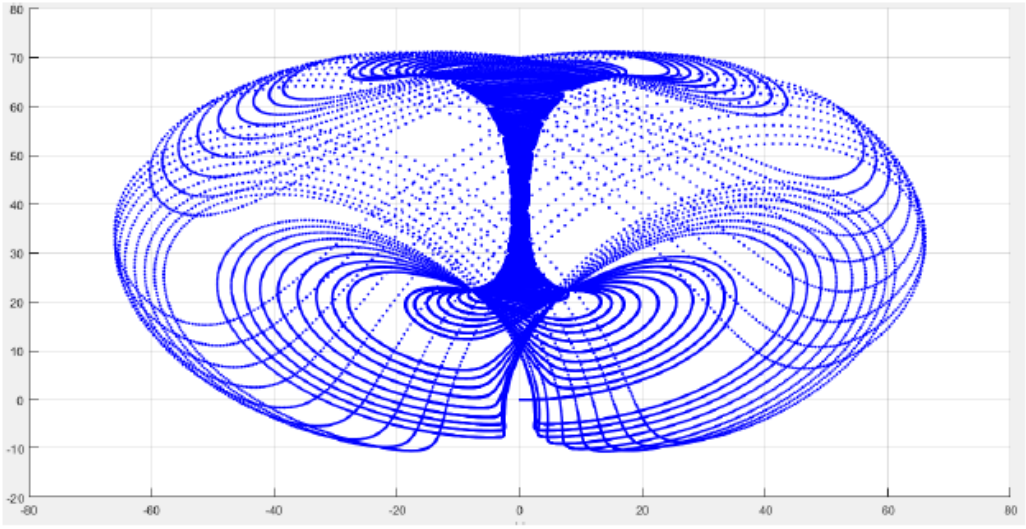

Figure 4.15: TSUCS attractor in 3D

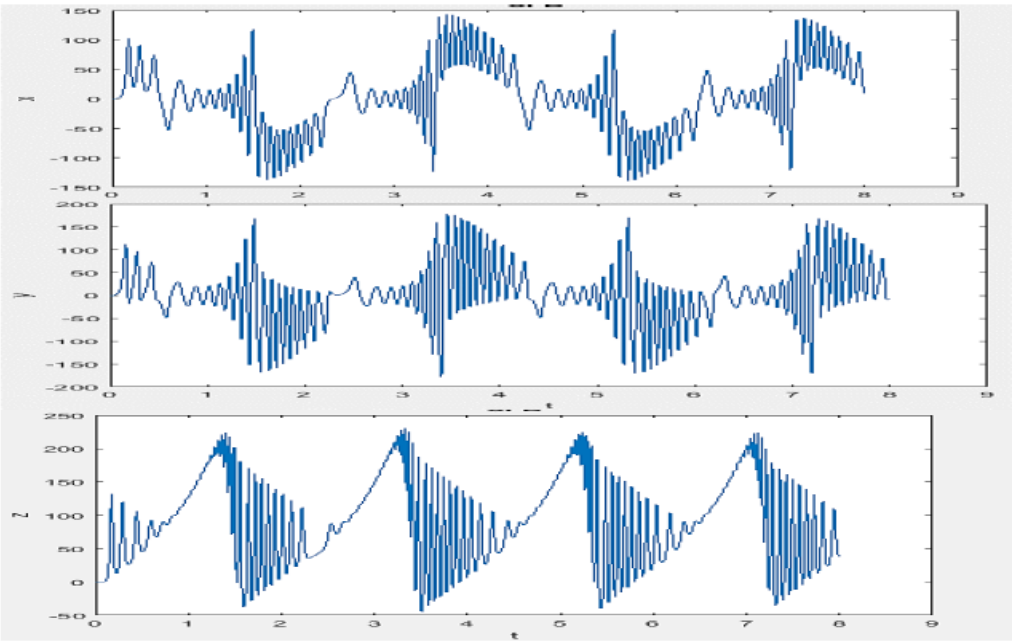

Figure 4.16: Evolution of the axes in the time of Three Scroll Unified Chaotic System attractor

4.1.3 Wang Sun Four Scroll Chaotic System

In 2009, Wang et al. discovered a chaotic four scroll system, which is given by the three-dimensional system of the following nonlinear differential equation:

$$\begin{cases} \frac{dx}{dt} = ax + cyz \\ \frac{dy}{dt} = bx + dy - xz \\ \frac{dz}{dt} = ez + fxy \end{cases} \quad (4.15)$$

In (15), x, y, z are state variables and a, b, c, d, e, f, are constant system parameters. The system (15) shows a chaotic attractor (see figure) if the value of the system parameter is chosen as follows:

a = 0.2, b = -0.02, c = 1.0, d = -0.4, e = -1.0, f = -1.0 (4.18)

For mathematical simulations, the initial state value of the chaotic system is assigned as follows: x (0) = 0.1, y (0) = 0.1, z (0) = 0.1 (4.19)

Figure (17) shows the 3D view of the attractor of the new chaotic system (15) of the four-volute attractor on the three coordinate planes.

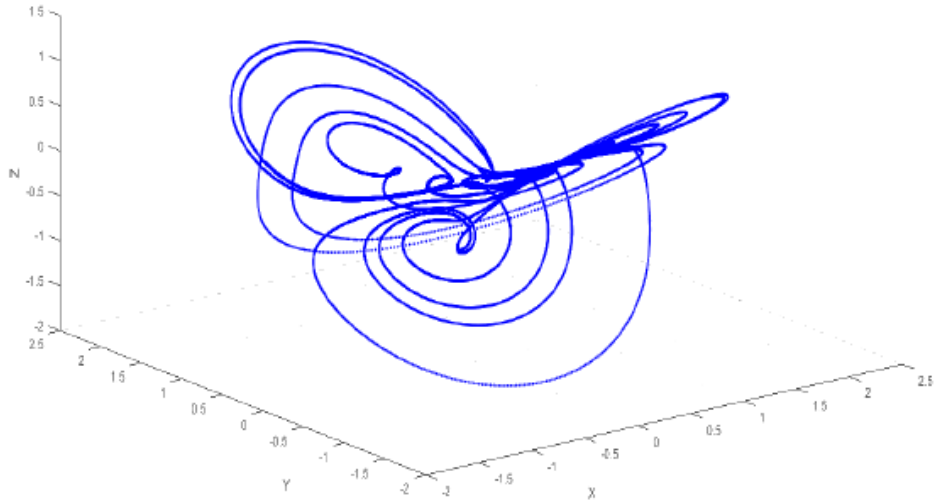

Figure 4.17: Strange attractor of the Wang Sun chaotic system

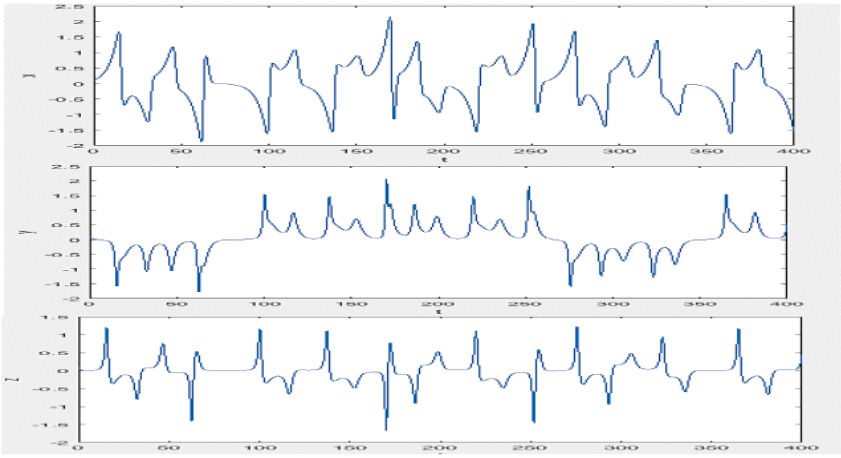

Figure 4.18: Evolution of the axes in time of Wang Sun attractor

4.1.4 Discussion Of Choice Of Systems

(1) Compared to common chaotic maps, hyper-chaotic systems need more parameters and have more complex dynamic behaviors that are unpredictable.

(2) Large key space withstands brute force attacks

(3) The systems are sensitive to slight changes in the original condition the system is resistant to synchronous attack of adaptive parameters because of its complex three-dimensional structure the systems have 3 chaotic sequences

4.2 PROPOSED SYSTEM

Since the chaotic system is highly sensitive to initial values and system parameters, meanwhile, has an enormous key space. The proposed algorithm for image encryption is based on Shanon idea of confusion and diffusion [16], that is, combining the substitution and permutation network (S–P network), which is also now the base of modern block ciphers. In addition to the S–P network, random noise is also added to decorrelate the plain image pixels. Thus, there are three modules of the anticipated technique, addition of noise, Permutation and Substitution.

In this section, a new color image encryption algorithm based on hyperchaotic chaotic systems and permutation-diffusion structure has been proposed. In the rows and

columns permutation process, we use the chaotic sequences generated from Aizawa and TSUCS chaotic systems to permute the first unit and spread the influence to the following other units. Therefore the permutation effect relies on both the keys and plain image. The key stream in the diffusion process depends on both the key (the initial value and the control parameters of the hyperchaotic system) and the permuted image. The key space is large enough to resist brute-force attacks. Statistical analysis shows that the scheme can protect the image from the statistical attack very well. The scheme possesses high key sensitivity and gets a good ability to resist differential attack. It can avoid the chosen plain-text and chosen cipher-text attack. With high-level security, it can be widely used in the Internet applications, such as Internet secure image communications.

4.3 ALGORITHM DESIGN

The design of the proposed algorithm (AIST) is explained in this section. The first three subsections provide design details step by step. The last subsection illustrate the overall workflow of the algorithm.

4.3.1 Encryption Process

The encryption process involves scrambling of rows and columns based on the chaotic sequence generated by the Aizawa and TSUCS attractor followed by XOR'ing the pixels with the pseudorandom numbers generated by Wan Sun Four scroll chaotic system

4.3.1.1 Row scrambling algorithm

The detailed description of the rows scrambling algorithm is composed of seven steps:

- *Step 1*. Iterate the hyper chaotic system by using Eq. (13) for L_0 times to get rid of transient effect, where L_0 is a constant. Continue to iterate the system for L times, where L is the max (X, Y, Z) for digital image$P(X, Y, Z)$, and obtain chaotic three sequences which everyone has L elements. Select three sequences and modify them by using the following formula:

$$x = mod((abs(x) - floor(abs(x))) \times 10^{15}, L \qquad (4.16)$$

- *Step 2*: Transform the original image into matrix of three dimension to get $A(i,j)$, $B(i,j)$ and $C(i,j)$

- *Step 3*. Split each matrix ($A_{X1\times Y1}$, $B_{X2\times Y2}$, $B_{X3\times X3}$) into M units. Each row is a unit, and any of the ith row is represented as $P_i, i=1,2,...M,$ (4.17)

- *Step 4*. Select the three chaotic sequences which were derived from Step 1, truncate them with the length N to get vector_row1, vector_row2 and vector_row3.

- *Step 5*. $i = 1$.

- *Step 6*. For each matrix, all elements in the Pi are permuted by the vectors vector_row1, vector_row2 and vector_row3 according to the following formula (18) and obtain the new three row of permutation image.

$$p_i^r(j) = t\_row(j)) \text{ , } j = 1, 2, \ \dots, N \qquad (4.18)$$

- *Step 7*. Then the p_i^r derived from Step 6 is sorted according to the method mentioned above to obtain a new three vectors, which will be used to permute the next row.

- *Step 8*. $i = i + 1$; Go to step 6 until i reaches M. Then, we get the row scrambled image P_r.

//The goal of the process is to changing pixels positions of color image by scrambling pixel values in rows using three pseudorandom sequences generated by Aizawa attractor//

Algorithm 1 Row Scrambling Algorithm : $y_{(i,:)} = [x0y0z0]$

while $count \leq n$ **do**
  $Q_1 = y_{(i-1,3)} - b - dy_{(i-1,2)}$
  $Q_2 = y_{(i-1,1)} + (y_{(i-1,3)} - b)y_{(i-1,2)}$
  $Q_3 = e + ay_{y(i-1,3)} - 3(y_{(i-1,3)})^2(1 + ey_{(i-1,3)}) + fy_{y(i-1,3)}(y_{(i-1,1)})^4$
  $y_{(i,:)} = y(i-1,:) + h * ydt$
  $p_{(i,:)} = unit8(floor(mod(y(i,:) * 10^15, 256)))$
end while
$w_1 = y(:,1)$, $w_2 = y(:,2)$, $w_3 = y(:,3)$
$A = I(:,:,1)$, $B = I(:,:,2)$, $C = I(:,:,3)$
$[X_1Y_1] = size(A)$, $[X_2Y_2] = size(B)$, $[X_3Y_3] = size(c)$
$i = 1$
for $j \leftarrow 1$ to Y **do**
  $R1(j) = A(W_1(i))$
  $R2(j) = B(W_2(i))$
  $R3(j) = C(W_3(i))$
  $W_1(i) = R1(j)$
  $W_2(i) = R2(j)$
  $W_3(i) = R3(j)$
  $i = i + 1$
  $T_1(:,:,1) = I_1(1,:,i)$
  $T_2(:,:,2) = I_2(1,:,i)$
  $T_3(:,:,3) = I_3(1,:,i)$
  end

4.3.1.2 Column scrambling algorithm

The detailed description of the columns scrambling algorithm is composed of seven steps:

- *Step 1*. Iterate the hyper chaotic system by using Eq. (14) for L_0 times to get rid of transient effect, where L_0 is a constant. Continue to iterate the system for L times, where L is the max (X, Y, Z) for digital image$P(X, Y, Z)$, and obtain chaotic three sequences which everyone has L elements. Select three sequences and modify them by using the following formula (16):

$$x = mod((abs(x) - floor(abs(x))) \times 10^{15}, L \qquad (4.16)$$

- *Step 1*. intercept a subsequence of length M to get a vector_col1, vector_col2 and vector_col3

- *Step 2*: Transform the scrambled image into matrix of three dimension to get A, B and C

- *Step 3*. Split the row scrambled image p^r into N units. Each column is a unit, and any of the ith column is represented as $p_j^r, j = 1, 2, \ldots, N$. (4.19)

- *Step 4*. j=1.

- *Step 5*. According to the following formula (20), all elements in p_j^r are permuted by the vector vector_col1, vector_col2 and vector_col3. Then we obtain the new ith column in permutation image.

$$p_j^{r\acute{e}}(j) = p_j^r = \left(t_{col(i)}\right), \ i = 1,2, \ldots, M \qquad (4.20)$$

- *Step 6*.P_i^{rc} Was sorted according to the method mentioned above to get a new vector t_col, which will be used to permutated the next column.

- *Step 7*. $i = i + 1$; Repeat the step 4 and 5 until i reaches N.Then, we get the permuted image P_{rc}.

//after realizing the scrambing in row in this process we aim to change pixels position by scrambling pixels value in column using three pseudorandom sequences generated by TSUCS system.//

Algorithm 2 Column Scrambling Algorithm : $y_{(i,:)} = [x0y0z0]$

while $count \leq n$ **do**
  $Q_1 = a(y_{(i-1,2)} - y_{(i-1,1)}) + dy_{(i-1,1)}y_{(i-1,3)}$
  $Q_2 = by_{(i-1,1)} - y_{(i-1,1)}y_{(i-1,2)} + fy_{(i-1,3)}$
  $Q_3 = -ey^2_{(i-1,2)} + y_{(i-1,1)}y_{(i-1,2)} + cy_{(i-1,3)}$
  $y_{(i,:)} = y(i-1,:) + h * ydt$
  $p_{(i,:)} = unit8(floor(mod(y(i,:) * 10^15, 256)))$
end while
$w_1 = y(:,1)$, $w_2 = y(:,2)$, $w_3 = y(:,3)$
$A = I(:,:,1)$, $B = I(:,:,2)$, $C = I(:,:,3)$
$[X_1Y_1] = size(A)$, $[X_2Y_2] = size(B)$, $[X_3Y_3] = size(c)$
  $j = 1$
for $i \leftarrow 1$ to X **do**
  $R1(i) = A(W_1(j))$
  $R2(i) = B(W_2(j))$
  $R3(i) = C(W_3(j))$
  $W_1(j) = R1(i)$
  $W_2(j) = R2(i)$
  $W_3(j) = R3(i)$
  $j = j + 1$
  $S_r(:,:,1) = I_1(:,1,i)$
  $S_r(:,:,2) = I_2(:,1,i)$
  $S_r(:,:,3) = I_3(:,1,i)$
  end

4.3.1.3 Substitution algorithm

This process is consist in changing pixels value by calculation pseudorondom numbers from Wang Sun system and XOR'ring these number with pixels value.//

Input: Shuffled image

Output: Encrypted image

Step 1: Calculate pseudorandom numbers from Four Scroll attractor (x_k, y_k, z_k)

Step 2: Calculate these number to get three matrix

$$Inew_1(i,j),\ Inew_2(i,j),\ Inew_3(i,j) \qquad (4.21)$$

Step 3: Transformation of image in tree matrix $A(i,j)$, $B(i,j)$, $C(i,j)$

Step 4. Do XOR operation with (A, B, C) in points (i, j) and $Inew_1$, $Inew_2$ *and* $Inew_1$, Hence(I_{n1}, I_{n2}, I_{n3}) is obtained

$$I_{n1} = A(i,j) \oplus Inew_1(i,j) \tag{4.22}$$

$$I_{n2} = B(i,j) \oplus Inew_2(i,j) \tag{4.23}$$

$$I_{n3} = C(i,j) \oplus Inew_3(i,j) \tag{4.24}$$

Step 5: Transformation of matrix to get final encrypted image

$$I = reshape(I_{n1}, I_{n2}, I_{n3}) \tag{4.25}$$

//This process is consist in changing pixels value by calculation pseudorondom numbers from Wang Sun system and XOR'ring these number with pixels value.//

Algorithm 3 Substitution algorithm : $y_{(i,:)} = [x0y0z0]$,$[XYZ] = size(I)$

while $count \leq n$ **do**
  $Q_1 = ay_{(i-1,1)} + cy_{(i-1,2)}y_{(i-1,3)}$
  $Q_2 = by_{(i-1,1)} + dy_{(i-1,2)} - y_{(i-1,1)}y_{(i-1,3)}$
  $Q_3 = ey_{(i-1,3)} + fy_{(i-1,1)}y_{(i-1,2)}$
  $y_{(i,:)} = y(i-1,:) + h * ydt$
  $p_{(i,:)} = unit8(floor(mod(y(i,:) * 10^15, 256)))$
end while
$x = p(:,1)$, $y = p(:,2)$, $z = p(:,3)$
$A = I(:,:,1)$, $B = I(:,:,2)$, $C = I(:,:,3)$
$[X_1Y_1] = size(A)$, $[X_2Y_2] = size(B)$, $[X_3Y_3] = size(c)$
$Len = 0$
for $i \leftarrow 1$ to X **do**
  $Inew1 = x(Len+1 : Len+Y)$
  $Inew2 = y(Len+1 : Len+Y)$
  $Inew3 = z(Len+1 : Len+Y)$
  $Len = Len + Y1$
end for
$A = I(:,:,1)$
$B = I(:,:,2)$
$C = I(:,:,3)$
$I_{n1} = bitxor(Inew_1, A)$
$I_{n2} = bitxor(Inew_2, B)$
$I_{n3} = bitxor(Inew_2, C)$
$I(:,:,1) = I_{n1}$
$I(:,:,2) = I_{n2}$
$I(:,:,3) = I_{n3}$
end =0

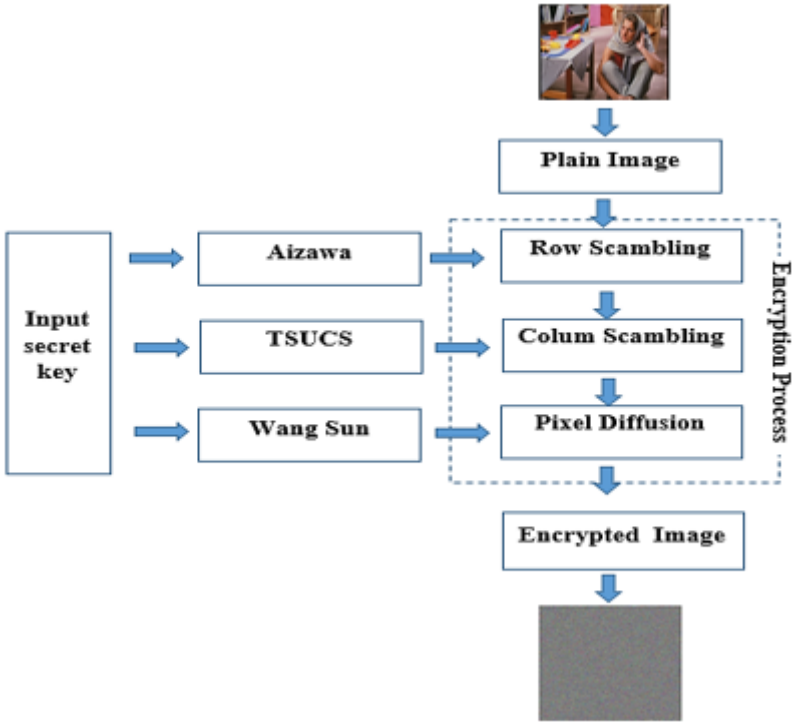

Figure 4.19: Process of encryption

4.3.2 Decryption Algorithm

The decryption process involves XOR'ing pixels with the pseudorandom numbers generated by the Wan Sun attractor followed by the inverse column row scrambling operation.

Input: Encrypted image

Output: Decrypted image

Step 1: Read encrypted image

Step 2: Using Wan Sun generate pseudorandom numbers (xk)

Step 3: XOR pixel values with Xk generated from Wang Sun Attractor.

Step 4: Use the numbers from TSUCS (Three Scroll Unified Chaotic System) for inverse column scrambling.

Step 5: Use the numbers from Aizawa Attractor for inverse row scrambling.

4.4 EXPERIMENT RESULT

In order to verify the validity of the algorithm, we encrypt image whose size is 320x 256 x 3 in the MATLAB simulation environment.

Figure 4.20: Original images

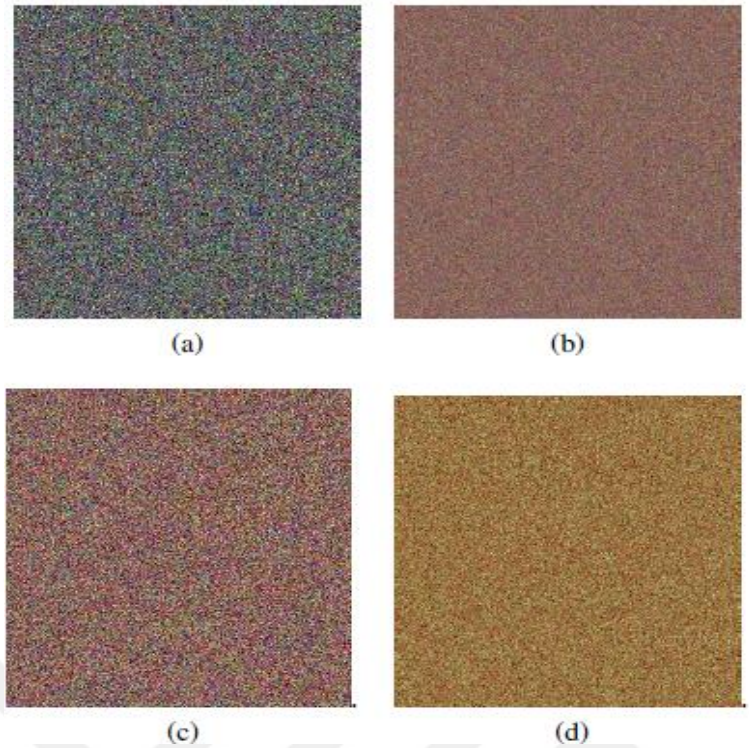

Figure 4.21: Encrypted images

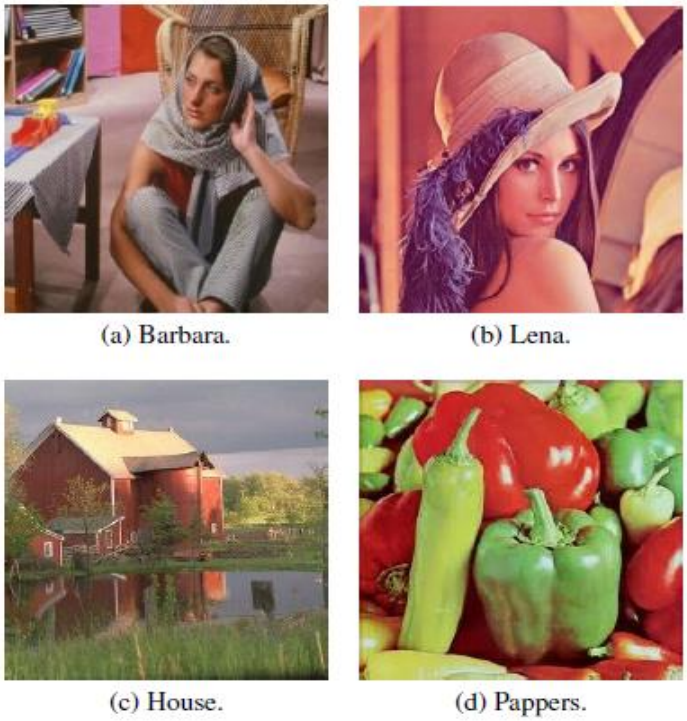

Figure 4.22: Decrypted images

The result of encryption is shown in Fig.21, while Fig.20 gives the original image. A good encryption scheme should have efficient security proprieties, such as large key space to resist brute-force attacks and high sensitivity to the secret keys.

Different security analysis, such as statistical analysis, key space analysis, entropy, NPCR, UACI and speed analysis are computed to prove the efficiency of our encryption scheme and the potential of the proposed chaotic maps.

4.5 ENCRYPTION PERFORMANCE ANALYSIS

4.5.1 Key Space Analysis

For the Wang Sun chaotic map, the sensitivity of the control parameters and initialization values is considered 10^{20}. Therefore, the space of each initialization value is10^{20}. While the control parameters a, b, c, d, e, f is in the range (-0.02, 0.5), then the key space for each is 0.5×10^{16}. Thus, the key space of the proposed schema is 0.125×10^{16}. It is large enough to ensure the resistance of the scheme against brute force attacks.

4.5.2 Visual Analysis

The purpose of the visual tests is to high the presence of similarities between a clear image and its number. Figure.21 shows that the encrypted images do not contain any features of the standard images. Visual tests were performed on different images, sizes and formats, and showed that there was no perceptual similarity.

4.5.3 Correlation Analysis

Correlation between two vertically adjacent pixels and two horizontally adjacent pixels in a single image and an encrypted image are considered in this investigation. We calculate the correlation coefficients of the adjacent pixels for the single image and the encrypted image for the Barbara image. It is well known that adjacent image pixels are strongly correlated in horizontal, vertical directions (x, y). Such a high correlation property can be quantified by means of correlation coefficients that are given by:

$$Cr_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4.21}$$

Where Cr is the Correlation Coefficient x and y are the horizontal and vertical directions.

Table 4 summarizes the auto correlation values for horizontal, vertical, and diagonal orientations of the original and ciphered image for all color components. Fig. 23 depicts the effect of encryption on the auto correlation in the horizontal dimension for all colors. The same trend is also noticed on vertical and diagonal dimensions. Cross correlation coefficient between the ciphered image and the original are found to be - 0.0041, 0.002, and 0.0032 for RGB colors respectively. Low coefficient values imply that the stream cipher implements the robust confusion and diffusion algorithm implemented in the proposed system which efficiently prevents any information leakage regarding pixel correlations.

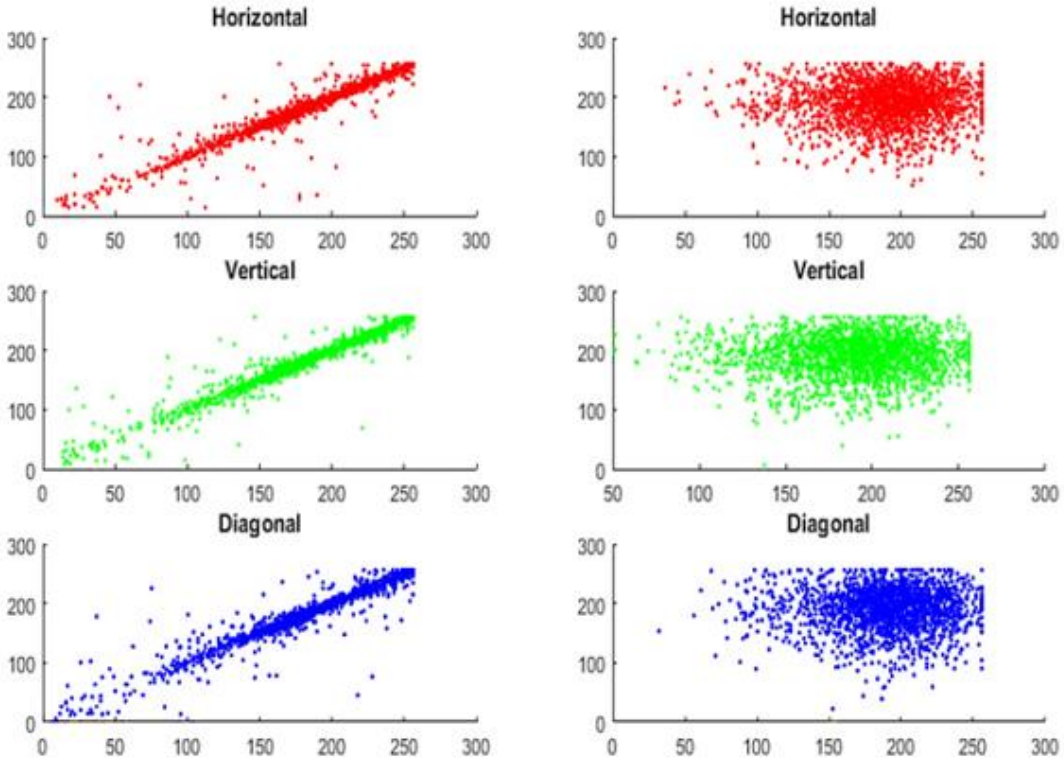

Figure 4.23: Pixel correlation diagram

Table 4.4: Pixel correlation diagram

Direction	Original image			Encrypted image		
	R	G	B	R	G	B
Horizontal	0.9530	0.9422	0.9257	-0.0042	-0.0024	0.0087
vertical	0.9350	0.9204	0.8955	-0.0013	-0.0096	0.0009
Diagonal	0.9125	0.9512	0.9220	-0.0027	-0.0003	0.0038

Table 1 show the coefficients of the correlations measured by the clear images are close to 1 while the ciphered images are close to 0, based on the results obtained we can affirm that the proposed algorithm has successfully removed the correlation of the adjacent pixels

4.5.4 Histogram Analysis

The histogram of the encrypted image as shown in Figure 24 is uniform, significantly different from that of the original image, and has no statistical resemblance to the ordinary image and therefore provides no indication for use a statistical attack on the present image encryption procedure. Therefore, a statistical attack on the proposed image encryption procedure is difficult.

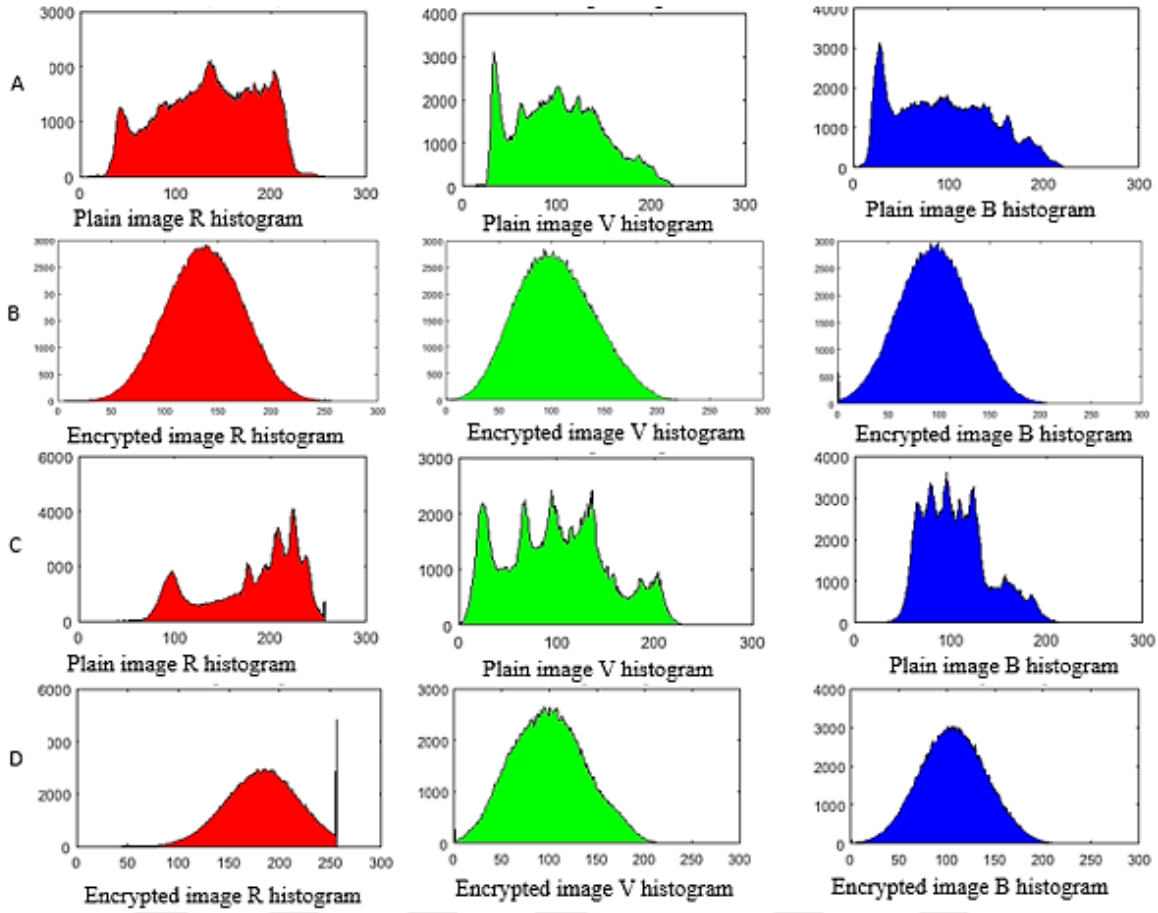

Figure 4.24: Histograms: (A) histogram of original image Lena, (B) histogram of encrypted image Lena histogram of original (C) image Barbara, (D) histogram of encrypted image Barbara.

4.5.5 Analysis of The Entropy of Information

Entropy values of the ciphered image compared to the original are shown in Table 5 for all color components. Low entropy values in the original image reflect the high predictability in the image data. However, high entropy values in the ciphered image imply the randomness levels achieved by the proposed stream cipher.

Table 4.5: Analysis of the information entropy of the algorithm

	Lena			**Barbara**		
Color	**R**	**G**	**B**	**R**	**G**	**B**
Entropy of information	7.5562	7.5243	7.5318	7.4757	7.4688	7.4462

4.5.6 Differential Attacks Analysis

In image encryption, the cipher resistance to differential attacks is commonly analyzed via the number of pixels change rate (NPCR) and unified average changing intensity (UACI) tests. NPCR represents the percentage of different pixel numbers between the plane image and the encrypted image, and UACI represents the average intensity differences between the plane image and the encrypted image or between two encrypted images.

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \quad (4.22)$$

$$UACI = \frac{1}{M \times N} [\sum_{i,j} \frac{c1(i,j) - c2(i,j)}{255}] \times 100\% \quad (4.23)$$

Where M and N represent the width and height of the image respectively. Two images were used in the tests. The first image is the original image, and the other is obtained by changing the value of the last pixel with a difference of 1. We encrypt the two images using the same encryption key to obtain the corresponding images C1 and C2.

Both NCPR and UACI tests are conducted 500 times with inputs having only one bit change randomly in only pixel with an arbitrary location. Table 6 depicts the mean values of the NCPR and UACI tests for all color components. Results reflect the effect of using the chained confusion algorithm implemented in the system in which changing one bit in the input affects the chaotic sequence from generator resulting in completely different output.

Table 4.6: Results of number of pixels change rate, unified average changing intensity

Image	**Lena.png**			**Barabara.png**		
Color	**R**	**G**	**B**	**R**	**G**	**B**
NPCR	99.4619%	99.4157%	99.4315%	99.4402%	99.4720%	99.4922%
UACI	33.5596%	33.5702%	33.6317%	33.4569%	33.5113%	33.4437%

4.5.7 Discussion

The algorithm gathers 3 types of chaotic systems (mono scroll, three scroll and 4 scroll) which presents a new method of exploitation of the permutation-diffusion encryption structure. The system used in this algorithm was invented recently and based on 3-dimensional equations Moreover, compared to common chaotic maps, hyper-chaotic systems need more than parameters and have more complex dynamic behaviors that are unpredictable the proposed algorithm to a stronger property and a larger key space. Theoretical analysis and experimental results show that the image encryption system offered at a high security level and excellent

4.6 COMPARISON

The following table 7 illustrates the comparison results between the proposed algorithm and the algorithm of reference [4] at the differential attack resistance level. The results show showed that the proposed algorithm had modified many pixels and their values for single images. Compared to the algorithm in reference [4], the average NPCRs of each component of the images tested are greater than 99.4%, which is much higher than them, and the average UACIs are efficiently modified, which makes it possible to resist differential attacks.

Table 4.7: Result of comparison between the algorithms

Algorithme	**Image**	NPCR (%)			UACI (%)		
		R	**G**	**B**	**R**	**G**	**B**
Proposed	**Lena.png**	99.4619	99.4157	99.4315	33.4969	33.5113	33.4437
Ref [35]	**Lena.png**	99.58649	99.21722	98.84796	33.48347	33.46399	33.26891

4.7 CONCLUSION

In this paper we have introduced a new secure and efficient technique that provides color image encryption. In order to overcome the weakness of one-dimensional card-based encryption systems with small key spaces, the proposed image encryption algorithm has a large key space and can successfully prevent brute force attack. Security analysis simulations were performed to ensure the effectiveness of the proposed system against statistical analysis, key space analysis, sensitivity analysis, and so on. Based on the results obtained, we can say that the proposed scheme is suitable for image encryption applications. In the following chapter, we will introduce our second contribution, which consists of a cryptosystem for digital images based on confusion-diffusion architecture using chaos theory.

5. DISCUSSION AND FUTURE RESEARCH

The amount of visual information available in digital format has grown exponentially in recent years due to the wide availability of equipment's such as digital cameras and camera phones, changes in the way people socially interact by setting up community web pages, wide spread use of the Internet in all types of personal and business activities, and developments in high speed transmission of digital images with high reliability.

However the wide accessibility of the Internet and its connected hosts and availability of technology to capture network traffic or penetrate hosts have made digital images vulnerable to unauthorized access while in storage and during transmission over a network. Hence users of the Internet and application that use or process digital images need to address security issues to protect commercial value of images and also ensure user privacy and other issues.

Apart from the above security related issues, numeric image trading has become a mainstream trade in cyber space and pay-after-trial services of digital multimedia are in wide practice. For example, thumbnail versions of images are used to provide previews to customers prior to the transaction in order to have a choice of selection. Current practices include showing only a small tile (thumbnail) of the original image, showing a lower-resolution version of the full image, showing the original image overlaid with a visible watermark image, or partial encryption of the images allowing only for a low visibility level than the original image.

Among these schemes, except for the method using partial encryption, other methods can be successfully attacked to obtain the original image by watermark removal, image enhancement, etc. In this context, image encryption becomes important in achieving the security requirements listed earlier to protect commercial interests and ensure privacy.

The objective of the research presented in this thesis is to propose an image encryption technique which is capable of encrypting an image effectively and securely with a predefined visibility level. Unlike a conventional symmetric key encryption scheme, apart from the input plaintext image and the secret encryption key, there will be a third input defining the visibility level of the output ciphertext image. This research studies the use of chaos theory in implementing such an encryption scheme and proposes a concrete image encryption scheme using 3D chaotic maps called Ikeda map and the Kaplan-Yorke map achieving the stipulated objective.

5.1 CONCLUSION

This project introduces our proposal color image encryption scheme, which is a new secure and efficient technique that provides color image encryption. In order to overcome the weakness of one-dimensional card-based encryption systems with small key spaces, the proposed image encryption algorithm has a large key space and can successfully prevent brute force attack. Security analysis simulations were performed to ensure the effectiveness of the proposed system against statistical analysis, key space analysis, sensitivity analysis, and so on. Based on the results obtained, we can say that the proposed scheme is suitable for image encryption applications. In the next chapter, we will introduce our second contribution, which consists of a cryptosystem for digital images based on confusion-diffusion architecture using chaos theory.

5.2 PERSPECTIVE WORK

Although the proposed contributions are quite effective, the solutions obtained are not optimal. However, there are several points that can be improved.

(1) The use of the notion of parallelism, the purpose of which is to process the images in a simultaneous manner, will make it possible to optimize the execution time of the two propositions. On the other hand it is very important to use another development tool and programming language more advanced and powerful. In addition, an image compression approach must be combined with the proposed schemes to optimize the image transmission time as well as its storage.

(2) The future research study will focus on the realization of encryptions for both video and audio files. Shifting to further strengthen the security of chaotic encryption.

(3) The combination of chaotic encryption and image data compression technology. We can consider the image of information is encrypted and appropriate to introduce a certain loss of data. How to use chaotic system properties of the design more secure, more efficient chaotic image data. It is a promising research direction.

(4) The study of realization of chaotic encryption technology has provided an effective tool for both chaotic encryption and chaotic confidential communications. Some researchers have proposed to implement chaotic confidential communications and chaotic encryption by using very-large-scale integration (VLSI) technology; such a technology is believed to have tremendous potential for future research work.

REFERENCES

[1] Chia, P., et al.(2003), Understanding Organizational Security Culture. Information Systems: The Challenges of Theory and Practice. *Las Vegas, USA, Information Institute.*

[2] Lin, Q.H., et al. (2004), Secure Image Communication Using Blind Source Separation, *Proceeding of IEEE 6th CAS Symp.on Emerging Technologies: Mobile and Wireless COMM*, pp.261-264.

[3] Huang, F., and Feng, Y. (2007), Novel 2D chaotic map based on image segmentation and image encryption approach, *Proceeding of Opt. Précis. Eng*., pp. 1096-1103.

[4] Kachris, C. (2003), Chapter 3 The SCAN Algorithm**,** *Design and FPGA Implementation of the SCAN Encryption Algorithm.*

[5] Kachris, C., et al. (2003), A Reconfigurable Logic-based Processor for the SCAN Image and Video Encryption Algorithm, *International Journal of Parallel Programming*, Vol.31, No.6, pp.489-504.

[6] Menezes, A. J., Vanstone, S. A., and Oorschot, P. C. V. Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[7] M. Robshaw, "Stream Cipher", RSA Laboratories Technical Report TR- 701, Version 2.0, July 1995

[8] S. EUBANK AND D. FARMER, 1989 Lectures in Complex Systems, vol. 2 of *The Proceedings of the 1989 Complex Systems Summer School*, Addison-Wesley Publishing Company, Santa Fe, New Mexico, June 1989, lectures An Introducion to Chaos and Randomness, pp. 75–190.

[9] Batterman, R. W. (1993), Defining Chaos, *Philosophy of Science*, pp. 43-66.

[10] Vinod Patidar, N. K. Pareek, G. Purohit and K.K.Sud, " Modified substitutiondiffusion image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, 2009 [

[11] JiWon Yoon, ,Hyoungshick Kim , " An image encryption scheme with a pseudorandom permutation based on chaotic maps", *Communications in Nonlinear Science and Numerical Simulation,* 2010

[12] Zbigniew Kotulski, Janusz Szczepański," Discrete chaotic cryptography", Ann. Physik, vol. 6, pp. 381-394, 1997

[13] R. Schmitz and J. Franklin, "Use of Chaotic Dynamical Systems in Cryptography" , vol. 338, pp. 429-441, 2001.

[14] Fangjun Huang, Zhi-Hong Guan, "Cryptosystem using Chaotic Keys", *Chaos Soliton Fractals*, Vol. 23, No. 3, pp. 851-855, 2005

[15] Fabre, C. (2011). Chaos Game 2D/3D, from the Wolfram Demonstrations Project

i. http://demonstrations.wolfram.com/ChaosGame2D3D/

[16] Shannon, C.E. (1948), A mathematical theory of communication, *Proceeding of The Bell System Technical Journal*, 27 (3) 379-423. 623-656.

[17] [17]L. Kocarev, "Chaos-Based Cryptography: A Brief Overview", IEEE Circuits and System Magazine, Vol. 1 , No. 3, pp. 6-21, 2001.

[18] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic cryptosystems: Cryptanalysis and identifiability," *in IEEE Tran. Circuits and Systems* I , vol. 53, no. 12, pp. 2673- 2680,2006

[19] Alvarez, G., Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos, World Scientific*, Vol. 16, pp 2129-2151.

[20] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed. Image encryption using stream cipher based on nonlinear combination generator with enhanced security. *New Trends in Mathematical Sciences*. 2013; 1(1): 10-19.

[21] Beloucif Assia. Contribution à l'étude des mécanismes Cryptographiques. Université de Batna 2. Faculté de mathématiques et d'informatique. 2016

[22] H. Khanzadi, M. Eshghi and S.E. Borujeni, Image encryption using random bit sequence based on chaotic maps, *Arabian Journal for Science and engineering*, vol. 39, no. 2, pp. 1039-1047, 2014.

[23] Gopalakrishnan, T., and S. Ramakrishnan. "IMAGE ENCRYPTION IN BLOCK-WISE WITH MULTIPLE CHAOTIC MAPS FOR PERMUTATION AND DIFFUSION." *ICTACT Journal on Image & Video Processing* 6.3 (2016).

[24] Sathishkumar, G. A., & Sriraam, D. N. (2011). Image encryption based on diffusion and multiple chaotic maps. *arXiv preprint arXiv:1103.3792*.

[25] Ni, Z., Kang, X., & Wang, L. (2016, August). A novel image encryption algorithm based on bit-level improved Arnold transform and hyper chaotic map. In *2016 IEEE International Conference on Signal and Image Processing (ICSIP)* (pp. 156-160). IEEE.

[26] Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, 67(1), 557-566.

[27] Ye, G., & Wong, K. W. (2012). An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear dynamics*, *69*(4), 2079-2087.

[28] Slimane, N. B., Bouallegue, K., & Machhout, M. (2017). Designing a multi-scroll chaotic system by operating Logistic map with fractal process. *Nonlinear Dynamics*, *88*(3), 1655-1675.

[29] Li-Hong, L., Feng-Ming, B., & Xue-Hui, H. (2013, June). New image encryption algorithm based on logistic map and hyper-chaos. In *2013 International Conference on Computational and Information Sciences* (pp. 713-716). IEEE.

[30] Huang, C. K., & Nien, H. H. (2009). Multi chaotic systems based pixel shuffle for image encryption. *Optics communications*, *282*(11), 2123-2127.

[31] ZHANG, Xianhan et CAO, Yang. A novel chaotic map and an improved chaos-based image encryption scheme. *The Scientific World Journal*, 2014, vol. 2014.

[32] Tong, X., Liu, Y., Zhang, M., & Wang, Z. (2012, October). A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map. In *2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science* (pp. 285-289). IEEE.

[33] PAN, Lin, ZHOU, Wuneng, FANG, Jian'an, *et al*. A new three-scroll unified chaotic system coined. *International Journal of Nonlinear Science*, 2010, vol. 10, no 4, p. 462-474.

[34] Michael S. Gagliardo, 3D Printing Chaos**,** *Bridges 2018 Conference Proceedings, 2018.*

[35] Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Journal of Systems and Software, 85(2), 290–299, (2012).

[36] T.S. Parker and L.O. Chua, "Chaos: A tutorial for engineers," Proceedings of the IEEE, vol. 75, no. 8, pp. 982-1008, 1987.

[37] C. Werndl, "What are the new implications of chaos for unpredictability?," British J. for the Philosophy of Sci., vol. 60, no. 1, pp. 195-220, 2009.

[38] E. B. Corrochano, Y. Mao, and G. Chen, "Chaos-based image encryption," in Handbook of Geometric Computing.: Springer Berlin Heidelberg, 2005, pp. 231- 265