Ministry of Higher Education and

Scientific Research

Babylon University

College of Engineering

Electrical Engineering Department

Design and Evaluation of Secure Communication Based on Chaos System

A Thesis

Submitted to the Department of Electrical Engineering

University of Babylon

In partial fulfillment of the requirements of the degree of Master of Science in Electrical Engineering / Electronic and Communication / Electronics

Done By

Huda Hassan Hatif

Under Supervision of

Prof. Dr. Saad Saffah Hasson

2022م 1444هـ

بسم الله الرحمن الرحيم

يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات

صدق الله العلي العظيم

المجادلة: ١١

Acknowledgements

In the name of ALLAH, the Most Gracious and the Most Merciful for giving me the determination and will to complete this research work.

I appreciate the inspiration and guidelines from my supervisor Prof. Dr. **Saad S. Hasson**, for his advice, guidance and encouragement. Without his continuous support and interest, this work would not have been the same as presented here.

I would like to extend my thanks and gratitude to the Deanship of the College of Engineering and the Presidency of the Electrical Engineering Department for the facilities and administrative procedures they provided me, which effectively contributed to the completing of the requirements of this research.

Special thanks to my dear brother **Ameer K. Jawad** for his support and advice.

Researcher

Dedication

To my parents

The first reason for my success and the most beautiful blessings of God upon me

to my husband

That great man who brought out the best in me and always encouraged me to reach my ambitions

to the pearls

Juman, Rayan

To my brothers

my support and I share my joys and sorrows.

To all my friends and to all those from whom I received advice and support;

I dedicate to you the summary of my scientific effort

Certify

I certify that this thesis entitled "Design and Evaluation of secure communication based on chaos system" was prepared by (**Huda Hassan Hatif**) under my supervision at Babylon university in partial fulfillment of the requirements for the degree of bachelor in computer engineering techniques.

Signature:

Name: Prof. Dr. Saad Saffah Hasson

(Supervisor)

Date: / /

Signature:

Name: Dr. Shamim Fadhil Abbas

(Head of Department)

Date: / /

Abstract

Many factors that must be taken considered communication systems, but two of the most important parameters are privacy and efficient transmission data. In this thesis, a secure communication system based on chaotic signals was designed and simulated to achieve the above-mentioned factors.

With regard to data security: An encryption and decryption system was built based on the Hyper Chaos system by generating random binary numbers (0,1) using three proposed methods in the research and performing an XOR operation between the random bits and the data to be encrypted after converting it to a Binary format. All three methods proved their efficiency balancing the probability of zeros and ones, and the encryption algorithm was applied to several types of images (grayscale and color images).

The simulation results proved the efficiency of the encryption system in terms of the size of keys (theoretically, the key size is close to infinity), However, in practice the key size depends on the factorial of 9 coefficients (and in a special case in the proposed system it depends on 18 coefficients) and each of them is a factorial of 10^{16} (as Prove in Matlab) and thus we will get a huge number of keys that it is difficult to calculate accurately. Also, the encrypted image given Peak-Signal-to-Noise-Ratio (PSNR) is less than 9 dB, which means that the encryption is good relatively, and also, if the image is retrieved on the receiver side, the decrypted image is clearly returned with PSNR = ∞ dB.

As for the communication system, a modulation method called Differential Chaotic Shift Keying (DCSK) was built, and an innovative method was proposed, which is transmission with Unequal Error Protection between bits (UEP) when SNR is low, some of the power is transferred from the less important bits (LSBs) to the most significant bits (MSBs). The simulation results proved the high efficiency of the proposed method compared to the traditional DCSK, with a profit gain of more than 72% using the Mean Square Error (MSE) criterion with respect to classical DCSK.

List of Contents

List of Figures

List of Tables

List of Symbols

Symbol	Definition
$\lambda_1\ \lambda_2\ \lambda_3$	The Eigen values of characteristic equation
$dx/dt\ ,\dot{x}$	state variable of the chaotic system at time
x_k	Iterative value of the chaotic map
$\grave{x}\ ,\grave{y}\ ,\grave{z}\ ,\grave{w}$	States value of the Rabinovich system
r, a, b, c, d	Parameters of the Rabinovich system
x_o, y_o, z_o, w_o	Initial condition of the Rabinovich system
N_b	Number of bits that represent each sample
M	Number of image rows
N	Number of image columns
H	histogram distribution of the original image.
Ȟ̀	histogram distribution of the encrypted image.
K, n, I, i, J & j	Loop Counters

List of Abbreviations

Abbreviation	*Definition*
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BigNum	Big Number such as 10^{12}
CM	Comparison Method
COOK	Chaotic On – Off – Keying modulation
CORR	Correlation Coefficients
CSK	Chaos Shift Keying
CSV	Chaotic State Values
CV	Comber two Vectors
Data_{sig}	2nd part of modulated bit in DCSK.
dB	Decibel
DCSK	Differential Chaotic Shaft Keying
DCSK-DIM	Differential Chaotic Shaft Keying – Dual Index Modulation
E	Entropy
EQ	Encryption Quality
eq	Equation
Fig	Figure
FM-DCSK	Frequency Modulation of DCSK
HCRS	Hyper Chaos Rebanovich System
MD	Maximum Deviation
ModBit	modulated bit
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
PV	Power Vector for Unequal Error Protection in DCSK
Rec. Image	Recovered Image
Ref_{sig}	1st part of modulated bit in DCSK (Chaotic Reference Segment)
SNR	Signal to Noise Ratio
SS	Spread Spectrum
SSIM	Structural Similarity Index
Sum	Summation
UEP	Unequal Error Protection Method

Chapter One

Introduction

1 Chapter One: Introduction

1.1 Introduction

As a result of the present digital revolution, sending and receiving data has become much more convenient and accurate. However, due to the huge advancement in means and hacking programs, it has become more difficult to protect the confidentiality of data sent from hacking. Following the development of digital applications and programs that allowed hackers to easily penetrate copyright and modify any file, preserving the copyright of data such as videos, images, documents, articles, and other types of data has become a concern for many organizations including publishing, universities, television stations, government agencies, another establishment [1].

The world community has been aware of the situation in recent years. The internet has played a part several of terrorist attacks. Where most government confidential information is transmitted over the internet, encryption is used as a defence against penetration, so the information's confidentiality is determined by the strength of the encryption system used, which is often easily broken due to advances in decoding technologies and breaking encryption algorithms. As a result, many academics and organizations have turned to methods of concealing data in ways that are difficult to identify (hiding the presence of data) [2].

Cryptography is the science and study of ways to prevent unwanted disclosure and manipulation of data in computer and communication networks [3]. There are two types of cryptographic systems: private-key cryptosystems and public-key cryptosystems. Both are controlled by keys and are based on complicated mathematical calculations [4].

Chaotic signals are a sort of wideband, non-periodic, and noise-like signals that can be used for spread spectrum (SS) transmission. In this vein, chaotic communication uses chaotic signals as carriers. it has many advantages, including simple transceiver circuits, fading mitigation in time-varying channels [5] jamming resistance with low probability of interception (LPI) [6] and secure communications [7]. As is generally known, chaotic communication systems can be classified into two groups, coherent and non-coherent schemes, depending on whether chaotic synchronization is required at the receiver terminal. [8] describes a classical coherent method called chaotic shift keying (CSK). Despite the efforts of many research colleagues to investigate effective chaos-synchronization algorithms, those methods have only achieved moderate progress [9,10], severely hampering the development of coherent chaotic communication schemes. Non-coherent techniques have attracted much attention in chaotic communication since they don't require intricate chaotic synchronization or channel state information at the receiver.

The most prominent non-coherent chaotic communication system is differential chaos shift keying (DCSK) [11], which has been extensively explored since its inception. The DCSK scheme has now taken off on a rapid development path, with a slew of worthwhile DCSK variants proposed and studied by researchers. The data rate and energy efficiency of DCSK are relatively poor since half of the bit length is spent sending non-information-bearing reference samples [12].

1.2 Historical Background

Chaos idea originated in the first run through in physics and mathematics, which serves as a historical foundation for the chaos hypothesis. Poincaré Henri, a French mathematician, first established the chaotic and chaotic dynamical systems in the 1890s. Poincaré Henri won an Oscar II award for his discovery that the conduct of the 3-body Empyreal system orbit is changing and unpredictable [13]. The Effect of the Butterfly, described by Edward Lorenz of weather behavior in 1963, is the first time Poincaré's evolution is considered account. For the first time, Lorenz used an IBM computer to model dynamical weather. The key found model is Lorenz's weather portrayal, in which he established that any small and unobserved variation will result in significant differences in reception; this is the well-known chaotic type of weather. As a result, the concept of chaos has been enlarged, with chaotic being treated as one of mathematical branches, and its benefit has been expanded in recent decades due to its vast applications [14].

The term "chaos" comes from ancient Greek, and it is used in modern physics to describe a system that has a given parameter that contains a feature of the variety's capability at any time due to various unknown rules that are difficult to clarify [15]. Chaotic behavior can be defined as an unpredictable phenomenon that emerges from a deterministic framework and behaves in a complex manner [16]. The chaotic signal generated has a periodicity conduct and no randomness. These generated signals have three apparent qualities: aperiodic signal waveform, wideband signal spectrum, and sensitivity to beginning conditions, which can be used as advantages despite its irregular shape [17, 18].

1.3 Literature Review

Image encryption and transmission using chaotic systems have piqued the interest of a many researchers, who have presented several advanced algorithms and strategies for designing durable, powerful, and high-level security. This section explores numerous ways to image encryption utilizing chaotic systems proposed in the literature.

in 2008 ***Gao and Chen*** [19] presented an encryption technique that uses a shuffling matrix to jumble the coordinates of pixels. Following shuffling, a hyper-chaotic mechanism is utilized to confuse the link between the original and encrypted images.

In 2014, ***Khanzadi et. al.*** [20] suggested an image encryption technique based on chaotic maps and employing a random bit sequence generator. To produce the requisite random bit sequences, Chaotic Logistic and Tent maps are employed. These chaotic functions permute the pixels of the plain image, which is subsequently partitioned into eight bitmap planes. Random bit and random number matrices are used to permute and substitute bits in each plane; the sematrices are the results of those functions. The permutation step for pixels and bit mappings is based on a chaotic random Ergodic matrix.

In 2015 ***Gorji et. al.*** published an image encryption approach based on Logistic and Tent chaotic maps and permutation-diffusion architecture, in which chaotic maps transform the plain-image's pixels to encrypt them. Finally, the plain-image is recreated by decrypting the encrypted image. MATLAB simulation was used to analyze the proposed system performance utilizing tests such as space key analysis, histogram analysis, key sensitivity analysis, and maximum signal-to-noise ratio.

in 2015 ***Roohbakhsh and Yaghoobi*** [22], published a color image encrypting method using chaos theory. first, press the hyper-chaos key and the second huge space key together. Various experiments were carried out on the simulation findings to assess the suggested method's security.

in 2016 ***Abdul Hassan*** [23] introduced a new hyper chaotic system that is based on Hénon and Logistic maps and has excellent capacity, security, and efficiency. In an image encryption scheme, the proposed hyper-chaos system is used to create the diffusion key. The image encryption technique, which is based on the suggested hyper-chaos system, has a huge key space, a high sensitivity of the encryption key, and good statistical properties, according to simulation testing. Various applications require different amounts of encryption and decryption time.

in 2019 ***Cai et. al.*** [24], proposed two promising differential chaos shift keying systems with dual-index modulation have been proposed and analyzed in an exhaustive manner. In the proposed systems, the overall transmitted bits are divided into the in-phase branch and quadrature branch, respectively, and then by means of dual-index modulation technique, the mapped bits of the in-phase and quadrature branches are modulated into a pair of distinguishable index symbols. Profiting from the dual-index modulation, the data rata, spectral efficiency and BER performance of the proposed DCSK-DIM systems are promoted significantly compared to the recently proposed PPM-DCSK system. Explicitly, the DCSK-DIM-I system makes a great progress in pursuit of admirable BER performance, while the DCSK-DIM-II system elevates the data rate to a great extent.

in 2000 ***Sushchik et. al.***[25] Used chaotic signals in spread-spectrum communications has a few clear advantages over traditional approaches. Chaotic signals are non-periodic, wide-band, and more difficult Used chaotic signals in spread-spectrum communications has a few clear advantages over traditional approaches. Chaotic signals are non-periodic, wide-band, and more difficult to predict, reconstruct, and characterize periodic carriers. These properties of chaotic signals make it more difficult to intercept and decode the information modulated upon them. However, many suggested chaos-based communication schemes do not provide processing gain, a feature highly desirable in spread-spectrum communication schemes. In this paper, we suggest two communication schemes that provide a processing gain. The performance of these and of the earlier proposed differential chaos shift keying is studied analytically and numerically for discrete time implementations. It is shown that, when performance is characterized by the dependence of the bit error rate on Eb\No the increase of the spreading sequence length beyond a certain point degrades the performance. For a given Eb\No, there is a length of the spreading sequence that minimizes the bit error rate.

in 2003 ***Lawrance & Ohama*** [26] explores the calculation of exact bit error rates (BERs) for some single-user chaotic-shift-keying (CSK) communications systems, in contrast to approximate Gaussian-based approximations in current use. The conventional signal-to-noise-ratio approach is shown to give only lower bounds on the BERs. An analytical Gaussian approach based on the exact mean and variance of the decoder function gives inexact results. Exact BERs are given here for several CSK systems with spreading sequences from different types of chaotic map. They achieve exactness from fully exploiting the dynamical and statistical features of the systems and the results correspond theoretically to impractically large Monte Carlo simulations. A further aspect of the paper is the derivation of likelihood optimal bit decoders, which can be superior to correlation decoders. The inapplicability of Gaussian assumptions is viewed through some exact distributional results for one system.

in 2009 ***Kaddoum et. al.***[27] present a new and accurate approach to computing the bit-error-rate (BER) performance of coherent and non-coherent chaos-based communication systems. The approach explores the dynamical properties of chaotic sequences and takes into account that the bit's energy is varying from one transmitted bit to another. Compared with other widely used approaches in the literature, the proposed methodology gives accurate results even for low spreading factors.

in 2016 ***Mahdi et. al.***[28] proposed a simple accurate analysis of the bit error rate performance for differential chaos shift keying communication system with an additive white Gaussian noise channel by using the non-central F distribution of the decision variable and assuming variable bit energy in the calculation. The new method has much higher accuracy and much lower computational complexity than the existing methods in the literature. Numerical results show that in most cases, the predicted bit error rate from the new method is indistinguishable from the simulated bit error rate, showing the effectiveness of our result.

This thesis presents a new encryption technique for images depending on the generation method of a random bit stream through a double Rabinovich hyper chaotic system. The proposed algorithm (Hyper Chaotic Rabinovich System (HCRS)) will be achieved through several methods. Each method is then examined in balanced and delayed environments.

1.4 Problem Statement

One of the most prominent problems of wireless communication systems is the problem of privacy and noise violations. With regard to the first problem, which is the violation of privacy, the research provides a secure and strong encryption system using Hyper Chaos system.

As for the second problem, a system was proposed in which the bit energy changes according to SNR, as well as according to the importance of each bit.

1.5 Aims of the Thesis

thesis aims to:

1. Explore the characteristics of chaotic systems and to build secure communication schemes using chaos.

2. Design a security communication scheme, to encrypt image based on hyper chaotic system and DCSK Based on Logistic chaotic map.
3. Use non-coherent detection receiver for DCSK to de-modulation and reconstruction original data.
4. Proposed double Hyper chaos to image encryption.
5. Propose Unequal Error Protection method to improve the performance of designed system in the presence of AWGN channel.
6. Evaluate the performance of proposed methods using MATLAB simulations.

1.6 Thesis Outline

This thesis is divided into five chapters. Among these chapters the **first chapter** which generously provides a brief introduction of the thesis.

Chapter two gives description of chaotic systems and their properties, as well as a basic theory of cryptography and its purposes and properties. Also included are highlights of the technical tests that are used to determine encryption quality.

Chapter three describes the design of the proposed image encryption algorithms. and differential chaos shift keying.

Chapter four presents the results obtained from simulations conducted in Chapter

Chapter five Contain the conclusions and future work.

Chapter Two

Theoretical Background

2 Chapter Two: Theoretical Background

2.1 Introduction

In the last decades, significant progress in communication systems needed to increase the performance and security of these systems, to transmute information from the transmitter to the receiver through any public channel.

This chapter will explain the chaotic system, type of chaotic system, hyper-chaos system, characteristics and more focus of its applications in the secure communication field.

2.2 Chaotic Signal

Non-periodic, random-like signals originating from nonlinear processes are known as chaotic signals, systems that are dynamical. A dynamical system, in general, has a fixed number of independent state variables, each of whose motions or trajectories is governed by a set of differential equations involving all of the state variables. Dynamical systems with chaotic state variables shift in a bounded, non-periodic, random-like fashion [29].

They also have a property known as sensitive dependency on initial conditions, which means that any two nearby starting conditions will easily lead to two completely uncorrelated state variable motions or trajectories. This property allows one to produce an infinite number of uncorrelated chaotic signals using different initial values from the same system [30].

The state variable of a simple second order discrete-time chaotic system. We confirm that the signal is bounded within the range [-1, + 1] here, in addition to observing its aperiodic and random existence.

2.3 Chaotic Systems

A chaotic system is a complex system with non-linear non-equilibrium dynamics process which could be characterized by the following:

- The chaotic system behavior is a collection of numerous systematic acts and each system component does not play a leading role under normal conditions.

- Chaotic systems are random and unpredictable.

- They have a higher sensitivity to the initial conditions. So, if two identical chaotic systems but with a slight difference in initial conditions, will rapidly form totally different states. [31]

The chaotic systems become widely used in information security, technology such as information encryption, and digital watermarking. the power of using chaotic system for cryptography is that the information signal in traditional methods is modulated and demodulated by using sine carrier signal, while in chaotic systems transmitter sends carrier information signal and the receiver demodulates it to resume the signal. Because of the random nature of broadband carrier of the chaotic systems, the information signal will be similar to channel noise signal. In other words, intruders (or attackers) would think the channel noise signal is noise not encrypted information. So, the use of chaotic systems in cryptography ensures the security of the information. [32]. The use of chaotic systems in cryptography has two major directions: the first one is using the chaotic system for synchronization of secure communication, while the other one is generating stream cipher or block cipher by using chaotic systems.

2.4 Chaotic Flow

Chaotic flow is a continuous-time system, and the chaotic flow signal is derived from a set of differential equations [33], i.e.

$$\dot{x} \;= \frac{d_x}{d_t} = \dot{x}(t) = f\big(x(t)\big) \tag{2.1}$$

Where $\frac{d_x}{d_t}$ and $\dot{x}$ the state vector of the system at time (t) in the dynamical system and $f(\cdot)$ is a function of any chaotic flows [33, 34]

Rössler System, Lorenz System, Chen's system, Chua system, Lü system are examples of the famous flows [33]. Rössler chaotic flow strange attracter and time series are illustrate in Figure (2.1.a) and Figure (2.1.b) [35] respectively.

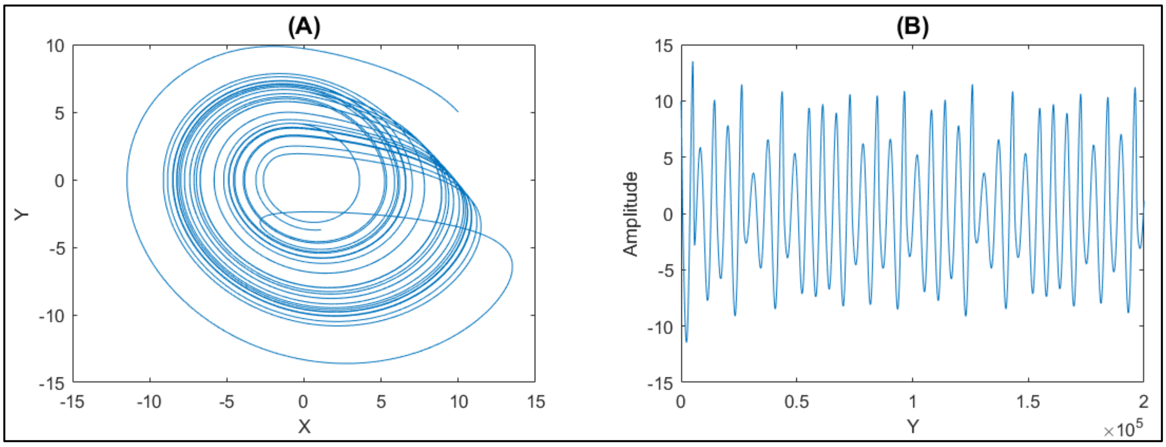

Figure 2-1: Rössler System flow (a) The strange attractor, (b) time series x(t).

2.5 Chaotic Map

A map is evolution function that exhibits some sort of chaotic behavior. Chaotic maps may be parameterized by a discrete-time. Discrete maps usually take the form of kth iterated functions. Chaotic maps often occur in the study of dynamical systems [36, 37].

$$x_k = g(x_{k-1}) \tag{2.2}$$

Where x_k is the state vector and $g(\cdot)$ denotes the iterative function which is known as chaotic map.

Here are some examples of the well-known maps:

- Standard Map
- Logistic map
- Hénon map
- cat map

Another example of well-known chaotic map is the logistic map [37], which is time series map produced as:

$$x_{n+1} = 1 - 2x_n^2 \tag{2.3}$$

The logistic map's trajectory and dynamics are shown in Figure (2.2.a) and Figure (2.2.b), respectively.

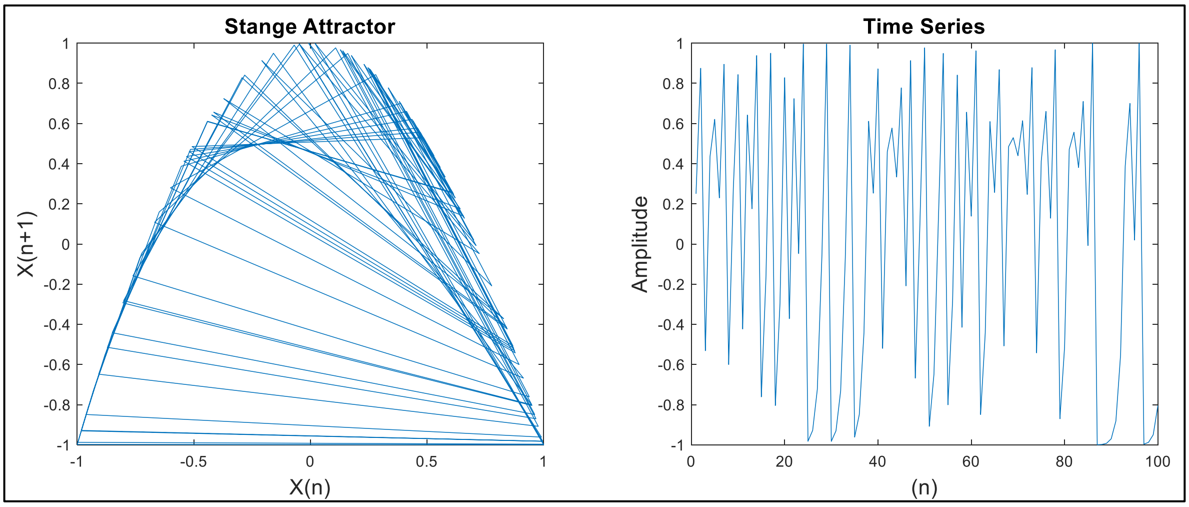

Figure 2-2: The Logistic chaotic map (a) strange attracter (b)Time series X_n Selecting of the Chaotic System [37].

To select the chaotic system, it must first specify the domain of the system if it continuous or discrete [38]. The proposed system used to encrypt a text message deals with the discrete time domain. These types in chaos encryption systems are very important for the security efficiency.

Depending on the time domain, chaotic systems divided into two types. The first one is the chaotic flow that deals with the Continuous Time Systems and the second is the chaotic map that describe the Discrete Time Systems. The chaotic system is randomly explicitly generated [39, 40].

2.6 Hyper Chaotic System

Hyper-chaos is chaotic systems that have a high sensitivity to initial conditions and system parameters, which is one of their most distinguishing characteristics. The sensitivity properties cause the trajectories of two related chaotic systems to diverge exponentially, regardless of the nearly identical initial conditions [41].

A dynamical model with at least two positive Lyapunov exponents is described as a hyper chaotic system. As a result, the dynamics of such systems will simultaneously expand in a variety of directions.

- **Hyper Chaotic Rabinovich System (HCRS)**

A continuous-time hyper chaotic autonomous system has at least four dimensions, with positive Lyapunov exponents of at least two. As a result, it benefits from increasing the system's randomness and unpredictability, which is significant in the field of secure communication. The HCRS is made up of the following equations [42]:

$$\left.\begin{aligned} \grave{x} \ &= ry - ax + yz \\ \grave{y} &= rx - by - xz \\ \grave{z} &= -dz + xy + w^2 \\ \grave{w} &= xy + cw \end{aligned}\right\} \tag{2.4}$$

Figure (2.3) shows the time series for each vector, the system parameters constrain the form of the chaotic attractor. We can observe the studied chaotic system's irregular hyper attractors simply by looking at it in fig. (2.4).

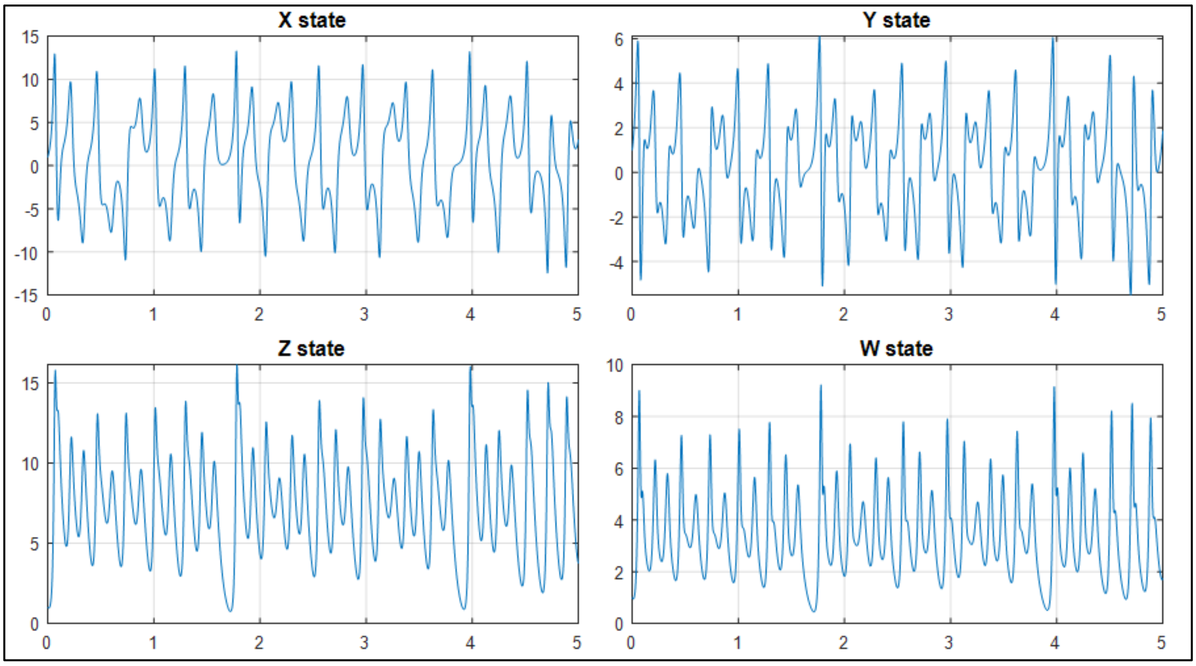

Figure 2-3: Time series for all vectors to Rabinovich system.

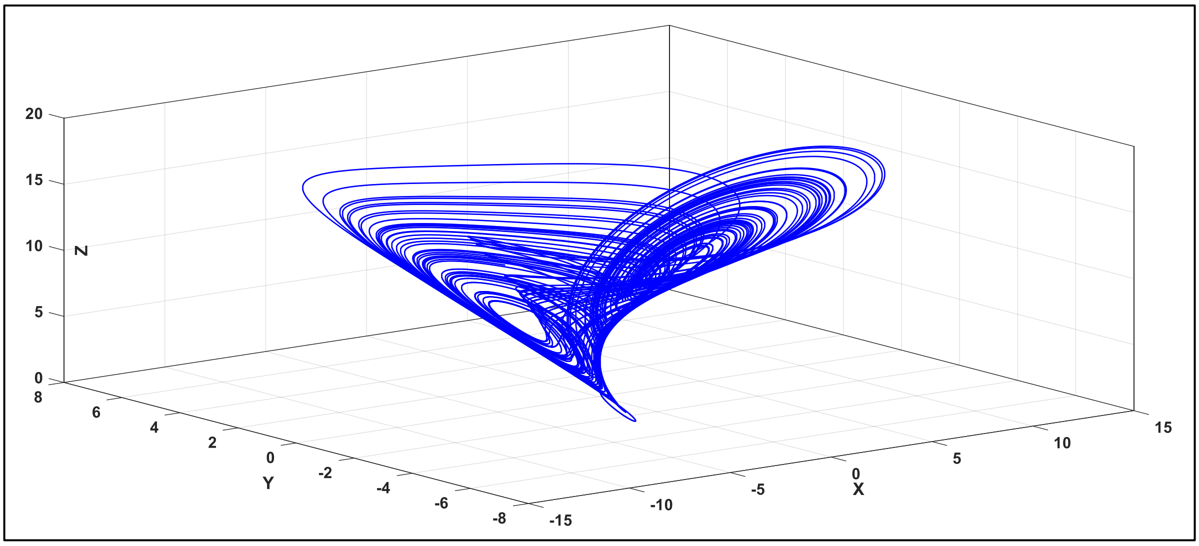

Figure 2-4: Three Dimensional portraits of Rabinovich system [37].

The Rabinovich model (eq. (2.4)) is sensitive to the system's initial conditions and parameters; it demonstrates that one of the trajectories is closely related to another but has very different characteristics. Fig. (2.5) explains the concept by displaying the state's time-domain waveform x(t) (the blue line represents the initial conditions (x_o, y_o, z_o & w_o) that's equal to (1,1,1&1) respectively, and the red line represents the initial conditions (x_o, y_o, z_o & w_o) that's equal to (1, 1, 1.000001 & 1) respectively). The difference in the initial conditions results in an absolute difference in the system's actions. Similarly, minor changes in parameters result in a totally new time series [43].

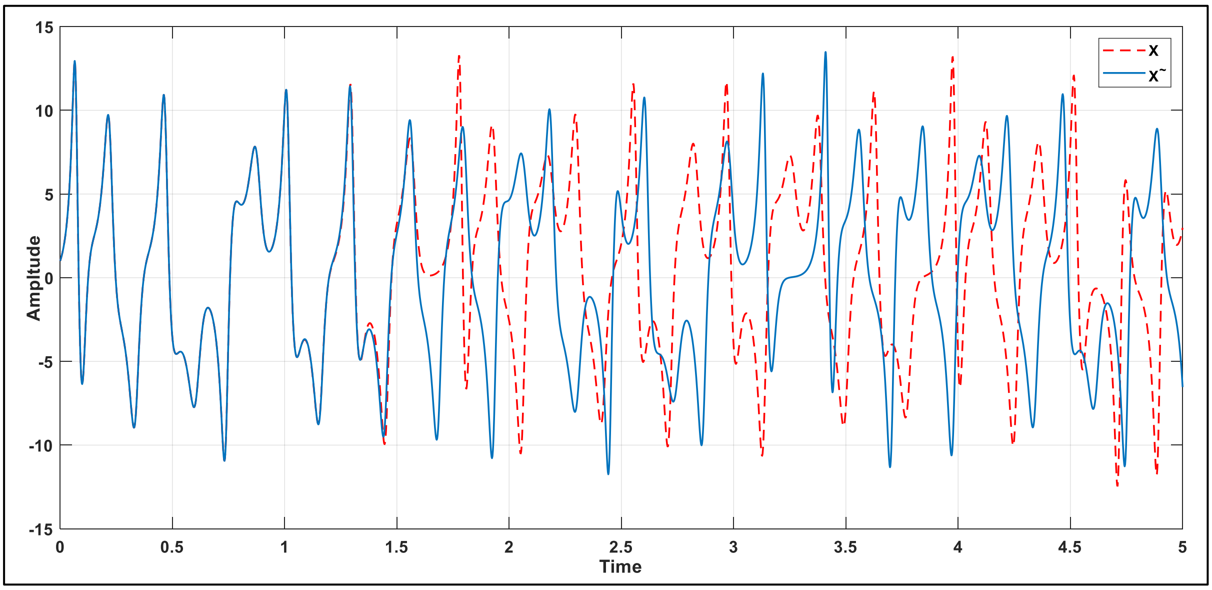

Figure 2-5: Sensitive Rabinovich system to initial condition.

2.7 The Properties of Chaotic Signals

Some important features of chaotic signals are

1- Chaotic signals have broadband spectrum; hence the presence of information does not necessarily change the properties of the signal.

2- Output power remains constant regardless of information content.

3- It is resistant against multipath fading and offers cheaper solution to traditional spread spectrum systems.

4- Chaotic signals are aperiodic; therefore, have limited predictability.

5- Chaotic signals are complex in structure and impossible to predict over long time.

6- Chaotic signals appear noise like.

7- Chaotic signal can be used for providing security at physical level.

2.8 Lyapunov Exponents

Lyapunov's characteristic exponent of this strategy is taken as a measuring element for all components of chaos and sensitivity reliance on starting states. Lyapunov normal exponents can be utilized for measuring the detachment of two close directions as far as beginning conditions. The division $\Delta(\mathrm{t})$ of such two directions is quicker with the development of time [44,46]

It may retain two points, $x_n(t)$ and $x_n(t) + \Delta x_n(t)$; they are on the attractor at time t, so that firstly:

$$x_n(t) \; = |x_n(t) + \Delta x_n(t)| << 1. \qquad (2.5)$$

$$\Delta\,(\mathrm{t}) \approx \Delta\,(0)e^{\lambda t}. \qquad (2.6)$$

In fig. (2.6), it is finding a clear definition of this principle. where λ is the Lyapunov number and $\{x_1, x_2, \ldots\ldots, x_n\}$ is the path of the *f* on the real line.

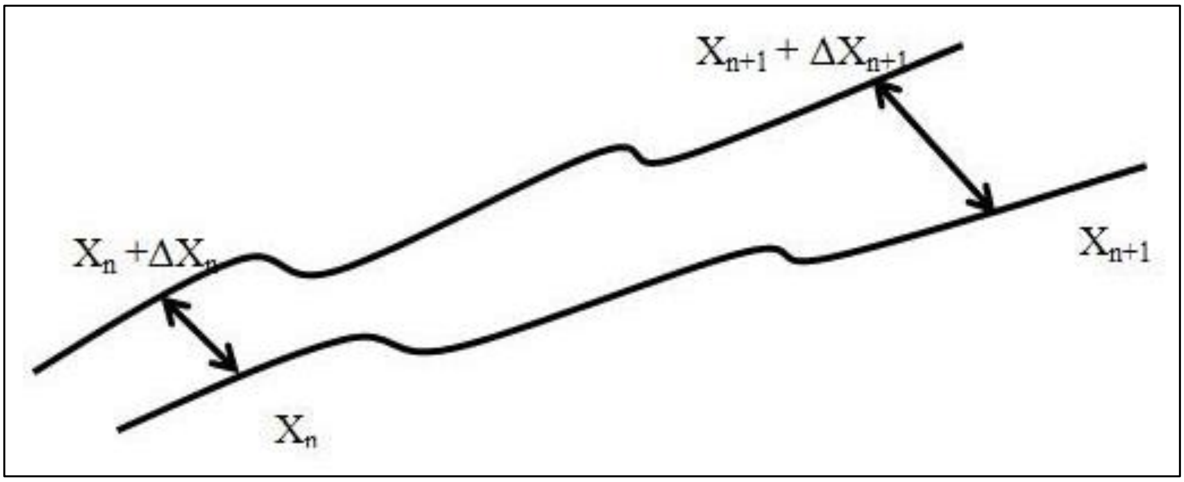

Figure 2-6: Lyapunov exponent [46].

For 1-D maps the characteristic of the Lyapunov exponent is obtained by the section$< \log\left|\frac{df}{dx}\right| >$. This way, the quantity of exponents is equivalent to the dimensionality of the stage space $(\lambda_1, \lambda_2, \lambda_3 \ldots\ldots \lambda_n)$. The exponents are sorted out on the premise of the diminishing worth, and it is generally realized that the length of the line between directions increments as $e^{\lambda_1 t}$, the areas increment as$e^{(\lambda_1+\lambda_2)t}$, and the volume increments as $e^{(\lambda_1+\lambda_2+\lambda_3)t}$, (where t denotes the continuity of time in flows while for maps denotes to the iteration index).

- There are many Lyapunov exponents for a chaotic system equal in number to the dimensionality of map. There are, for instance, a single positive Lyapunov exponent for one dimensional map and two Lyapunov exponents for the two-dimensional map as Henon map, one is negative and the other is positive. Regarding Lorenz chaotic flow, there are three exponents, positive, negative and equal to zero.
- When Lyapunov exponent is greater than zero ($\lambda > 0$), it is used as signature of chaos.
- When Lyapunov exponent is smaller than zero ($\lambda < 0$), it means that the orbit is associated to a stable fixed point or stable periodic orbit.
- While Lyapunov exponent is equal to zero ($\lambda = 0$), the orbit is a limit orbit.

2.9 Advantages and Disadvantages of Symmetric-key Encryption [47]

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the encryption/decryption would know it. In a symmetric cryptosystem, the encrypted message is sent over without any public keys attached to it.

2.9.1 The Advantages

1. To achieve large data rates, symmetric-key ciphers are designed. Hardware implementations of this form of encryption may achieve encryption rates in the hundreds of gigabytes per second, while software implementations can achieve rates in the megabytes per second range.

2. Symmetric ciphering uses keys that are quite short.
3. Different cryptographic processes, such as pseudorandom number generators, hash functions, and computationally efficient digital signature schemes, can be built using symmetric-key ciphers.
4. Symmetric-key ciphers can be symmetric-key ciphers which can be collected to obtain stronger ciphers. So, simple transformations which are relatively weak and easy to analyze, can be used to build strong product ciphers.

2.9.2 Disadvantages

1. Because the same key is used for encryption and decryption, the key must be kept secure.
2. Many key pairs must be managed in large networks. The use of the TTP (Trusted Third Party) is required for proper key management.

2.10 Asymmetric Encryption

Asymmetric encryption (also known as public key cryptography) is a type of encryption that requires two keys instead of one, the first of which is known as the public key and the second as the private key. The first is open to the public, while the second is solely available to users. This capability makes public key encryption superior to symmetric key encryption in terms of resolving the difficulty of managing secret keys, but it also makes it mathematically more vulnerable to assaults. Because it requires more computer processing capacity, asymmetric encryption is about a thousand times slower than symmetric key encryption [48].

2.11 Chaotic Image Encryption Algorithms

Changing the pixel's value and changing the pixel's position are two kinds of image encryption utilizing a chaotic encryption system. The first employs a chaotic system as a random number generator, with the resulting sequence performing a specific operation on the plain text to produce ciphertext, which alters the pixel's value. The other is used to adjust the coordinates of pixels that are affected by random chaos. From the created sequence, the chaotic systems construct a scrambling matrix.

2.11.1 Pixel value transform (changing pixel value)

Pixel value transforming is the earliest type of image encryption, in which the plaintext is converted to ciphertext by modifying the pixel values. Let A represent the original image with dimensions of M*N and S as gradation layers (for RGB, S=3), as illustrated in figure (2-7). Initial conditions and system parameters must be established as an encryption key that is utilized to generate the ciphertext when employing a chaotic system for encryption. The chaotic sequence will be formed after that. The encryption procedure will be accomplished by executing XOR operations with the original image pixels, and the encrypted image will look as pseudo-random data, due to the chaotic system's randomness. The XOR operation must be applied to the pixel value of the ciphertext for image decryption (in other words, to retrieve plaintext from ciphertext) using the same initial conditions and parameters of the chaotic systems as were used for the encryption process. [49]

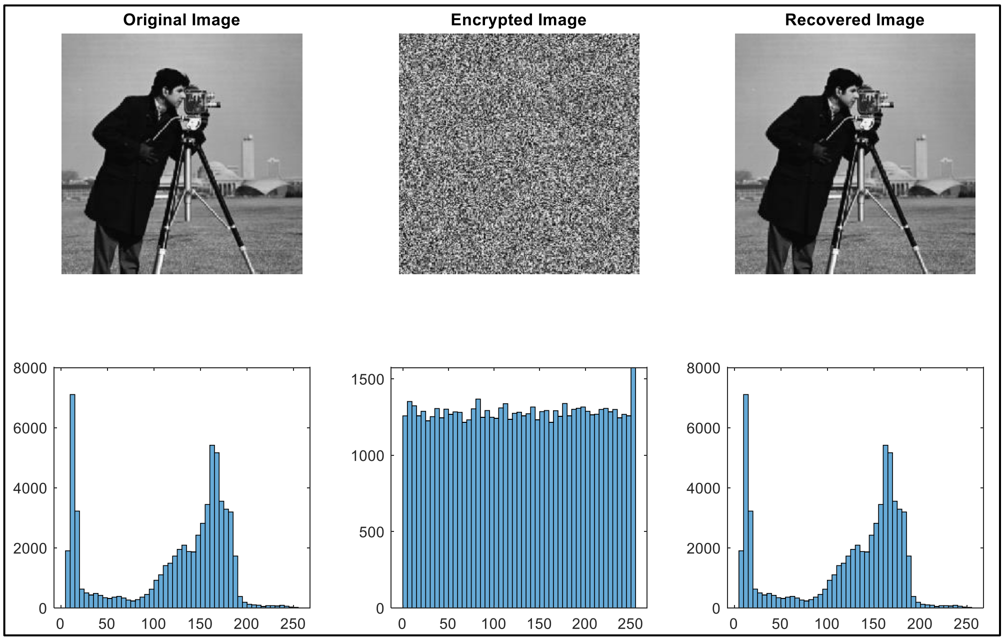

Figure 2-7: Image Encryption Based on Pixel value changing [50]

2.11.2 Pixel position transform (changing pixel coordinate)

The ciphertext formed by modifying the pixels' locations rather than their values is the second sort of digital image encryption procedure. To construct the cipher image, a two-dimensional chaotic map is used to transfer each pixel position from the plaintext to a new place. As seen in figure (2.8), this sort of encryption is also known as image scrambling.

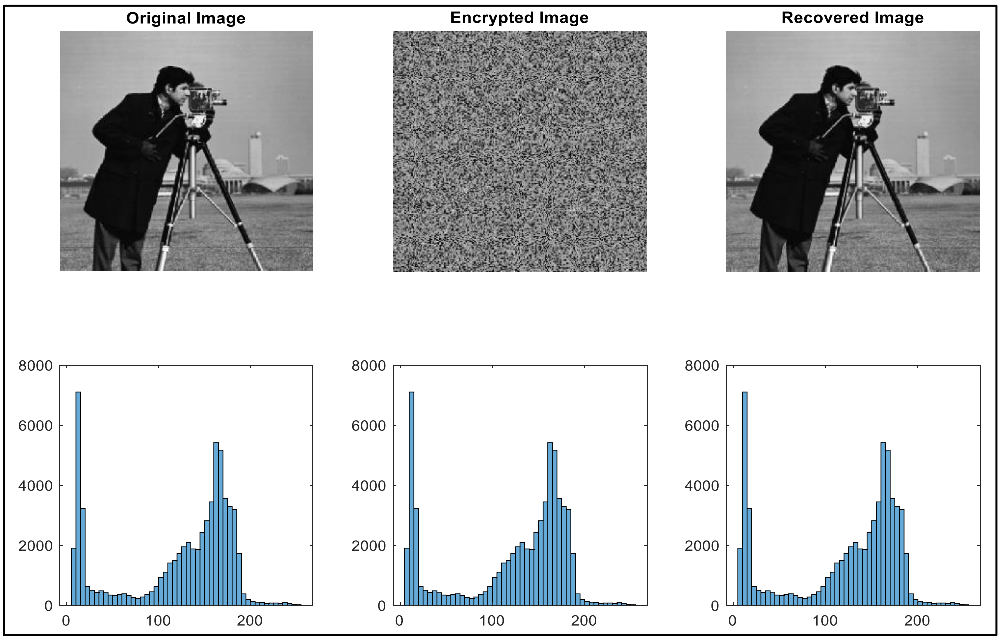

Figure 2-8: Image Encryption Based on Pixel Position Changing [50].

Many chaos-based encryption techniques are now either basic pixel location transformations or simple pixel value changes. For assaulting the ciphertext, image pixel scrambling provides useful intruder resistance, but it is regarded weak when attacking known plain text because it just alters the position of the pixels without changing their values [50].

2.12 Application of Chaos to Communications and Modulation

With their inherent broad band characteristic, chaotic signals are ideal candidates for disseminating narrowband information. As a consequence of encoding information with chaotic signals, the resulting signals are spread-spectrum signals with greater bandwidths and lower power spectral densities.

They get all the advantages of spread-spectrum signals, such as uninformed detection complexity, multipath fading mitigation, and anti-jamming. Furthermore, because of the sensitive dependence on initial conditions and parameter variations, a large number of spreading waveforms can be easily produced. As a result, confusion offers a low-cost and flexible way to communicate over a wide range of frequencies.

A variety of modulation and demodulation systems for communications have been proposed in recent years. We'll go through three different forms of communication methods that have been thoroughly researched in the following section.

2.12.1 Chaotic Analog Modulation

For transmitting analog information with chaotic signals, there are two widely discussed classes of techniques: chaotic modulation and chaotic masking. The analog signal is applied to the output of a chaotic system in the most basic form of chaotic masking. At the moment, the original based on a process known as chaos synchronization, on the receiving end the analog information is extracted after the chaotic signal is reconstructed by subtracting the incoming signal from the replicated chaotic signal.

The basic concept behind chaotic modulation is to inject analog information into a chaotic system, causing it to change its dynamics. This is typically achieved by changing a parameter of your choosing. As a consequence, the analog information is contained in the chaotic signal provided by the machine. The receiver's task is to monitor the chaotic signal's shifting dynamics and retrieve the analog information [51].

2.12.2 Chaotic Digital Modulation

Several schemes have been proposed in the past for encoding digital information with chaotic signals. In most proposed methods, the basic principle is to map digital symbols to non- periodic chaotic basis signals.

For instance, chaotic switching or chaos shift keying (CSK) maps different symbols to different chaotic basis signals, which are produced from a dynamical system using different values of a bifurcation parameter or from several different dynamical systems. If synchronized copies of the chaotic basis signals are available at the receiver, detection can be achieved by evaluating the synchronization error or based on a conventional correlator-type detector. This class of detection is known as coherent detection. Moreover, if synchronized copies of the chaotic basis signals are not available at the receiver, detection has to be done by non-coherent means [52,53].

Another widely studied modulation technique for encoding digital information is based on a differential keying approach. Known as differential chaos shift keying (DCSK). This approach involves developing a special framework for the information bit that enables non-coherent detection to be performed. Any transmitted symbol in the binary case is represented by two chaotic signal sample sets. The first is used as a reference sample collection, while the second is used to gather information. The data sample set is either an exact or reversed copy of the reference sample set, depending on the symbol sent. Demodulation is simple and can be accomplished by correlating the two chaotic sample sets. By comparing the correlator output to a threshold value, the binary symbols can be distinguished [54].

A few other digital modulation schemes derived from CSK and DCSK have also been proposed, chaotic on-off-keying (COOK), frequency-modulated

DCSK (FM-DCSK), correlation delay shift keying (CDSK) and symmetric CSK and quadrature CSK [55,56].

2.13 Chaos Shift Keying

Chaos shift keying (CSK) was first proposed by Parlitz et al. [57] and Dedieu et al. [58]. The idea is to encode digital symbols with chaotic basis signals. Figure (2.9) shows the block diagram of a typical CSK digital communication system. The operating principle can be described as follows. The transmitter consists of two chaos generators f and g, producing signals $\hat{c}$(t) and $\check{c}$(t), respectively. If a binary "+1" is to be sent during the interval $[(l-1)T_b, lT_b)$, $\hat{c}$(t) is transmitted, and if "-I" is to be sent, $\check{c}$(t) is transmitted.

In its originally proposed form, the CSK system works on the basis of the self-synchronizing property of chaotic systems. The receiver structure is shown in Figure (2.10), in which the incoming signal is used to drive two self-synchronization subsystems $\tilde{f}$ and $\tilde{g}$, which are matched to f and g, respectively. Assume that the filters at the transmitter and receiver are distortion-less and the channel is perfect. When the transmitted signal is $\hat{c}$(t), the subsystem $\tilde{f}$ will be synchronized with the incoming signal while $\tilde{g}$ does not, and vice versa. Therefore, by measuring the difference (error) between the incoming signal and the output of the self-synchronization subsystems, the transmitted symbol can be estimated. Results show that the systems work well under a noiseless condition.

In communications, correlation is a generic process that is used to evaluate the "likeness" between two signals. Clearly, for the CSK system mentioned above, instead of measuring the synchronization error, we may directly evaluate the correlation between the transmitted signal and the replica basis signals to identify the transmitted symbol. Thus, a correlator plus a decision maker forms a generic coherent receiver for the CSK system.

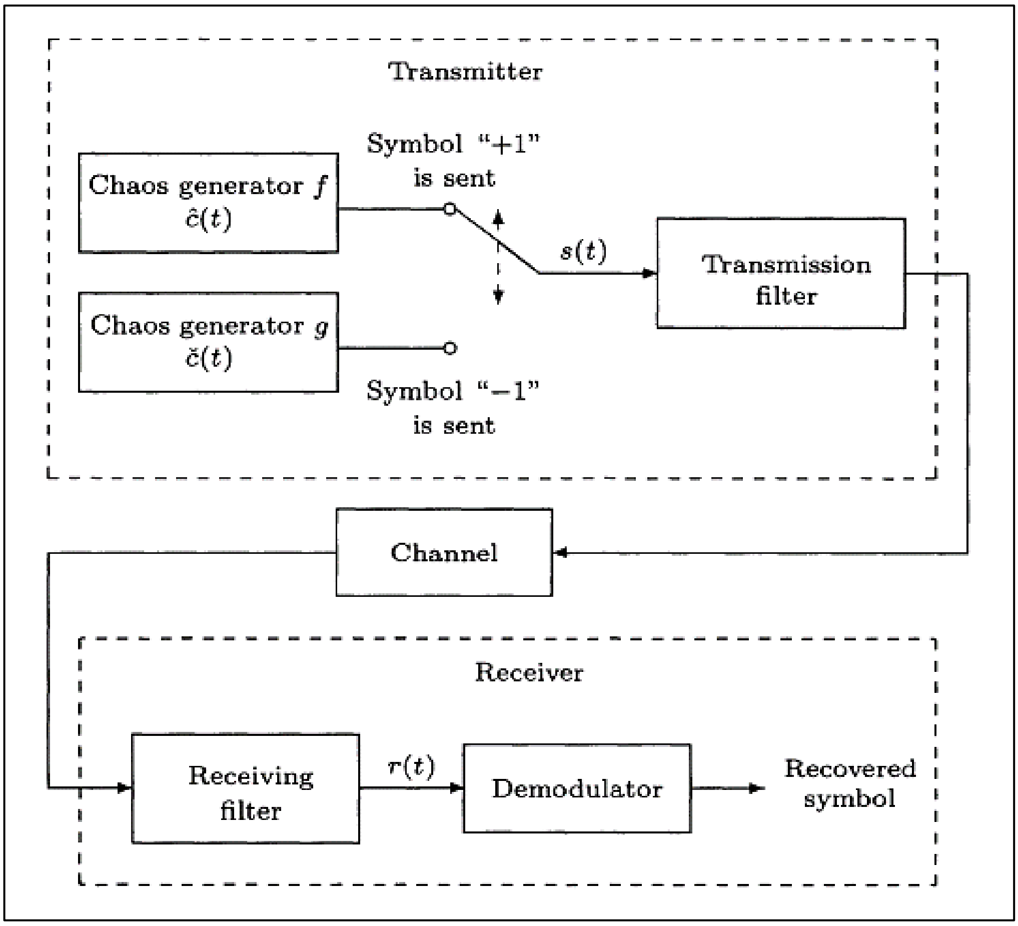

Figure 2-9: CSK digital communication system [57].

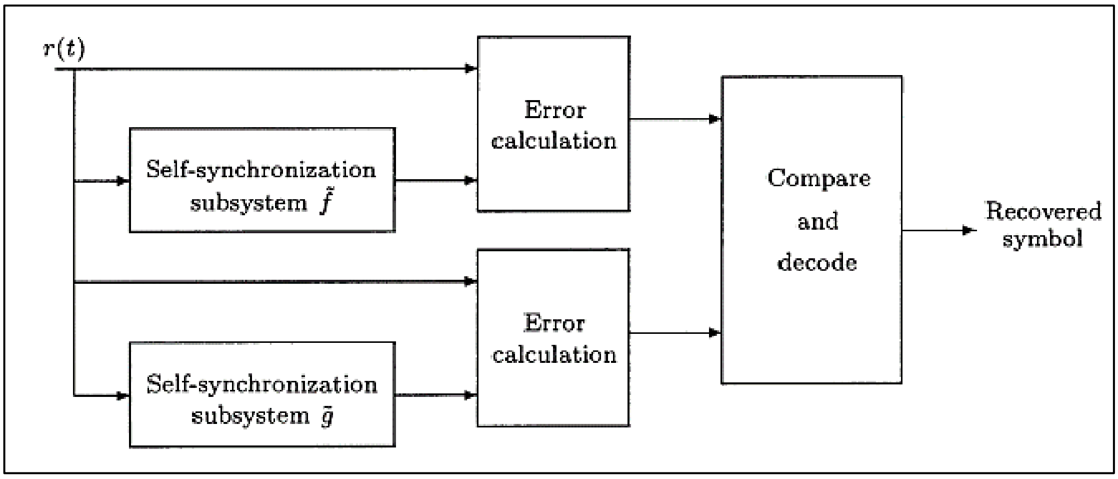

Figure 2-10: Synchronization-error-based CSK demodulation [57].

2.14 Differential Chaos Shift Keying

The differential chaos-shift-keying (DCSK) modulation scheme was proposed to facilitate non-coherent detection [59]. Figure (2.11) shows the block diagram of a DCSK modulator. In this scheme, every transmitted symbol is represented by two consecutive chaotic signal samples. The first one serves as the reference (reference sample) while the second one carries the data (data sample). If a "+1" is to be transmitted, the data sample will be identical to the reference sample, and if a "-I" is to be transmitted, an inverted version of the reference sample will be used as the data sample[59]. Usually, the reference sample is sent in the first half symbol period, and the data sample is sent in the second half symbol period. Thus, for the lth symbol period, we have

$$s(t) = \begin{cases} c(t) & for(l-1)T_b \le t < (l-\frac{1}{2})T_b \\ \pm c\left(t-\frac{T_b}{2}\right) & for(l-\frac{1}{2})T_b \le t < lT_b \end{cases} \tag{2.7}$$

if "+1" and "-1" is to be transmitted.

Figure (2.13) shows a typical sample of s(t). At the receiver, the correlation between the reference sample and the data sample is evaluated. This can be done by correlating the incoming signal with a half-symbol-delayed version of itself, as shown in Fig (2.12) The output of the correlator at the end of the lth symbol duration is given by

$$y(lT_b) = \int_{(t-\frac{1}{2})T_b}^{lT_b} r(t)r\left(t-\frac{T_b}{2}\right)dt \tag{2.8}$$

assuming that the transmitted signal is contaminated by additive noise, the correltor output is given by

$$y(lT_b) = \int_{\left(t-\frac{1}{2}\right)T_b}^{lT_b} [s(t)+\acute{n}\ (t)][s\left(t-\frac{T_b}{2}\right)+\acute{n}\ (t-\frac{T_b}{2})]dt$$

$$= \int_{\left(l-\frac{1}{2}\right)T_b}^{lT_b}\left[s(t)s\left(t-\frac{T_b}{2}\right)\right]dt + \int_{\left(l-\frac{1}{2}\right)T_b}^{lT_b}[s(t)\acute{n}\ (t-\frac{T_b}{2})]dt +$$

$$\int_{\left(l-\frac{1}{2}\right)T_b}^{lT_b}[\acute{n}\ (t)s(t-T_b/2)]dt + \int_{\left(l-\frac{1}{2}\right)T_b}^{lT_b}[\acute{n}\ (t)\acute{n}(t-T_b/2)]dt \tag{2.9}$$

where n'(t) is the noise component at the output of the receiving filter. The first term in (2.8) can be positive or negative, depending on whether a"+1" or "-I" has been transmitted. Also, all other integral terms have a zero mean. Thus, the threshold of the detector can be set optimally at zero, which is independent of the noise level [55].

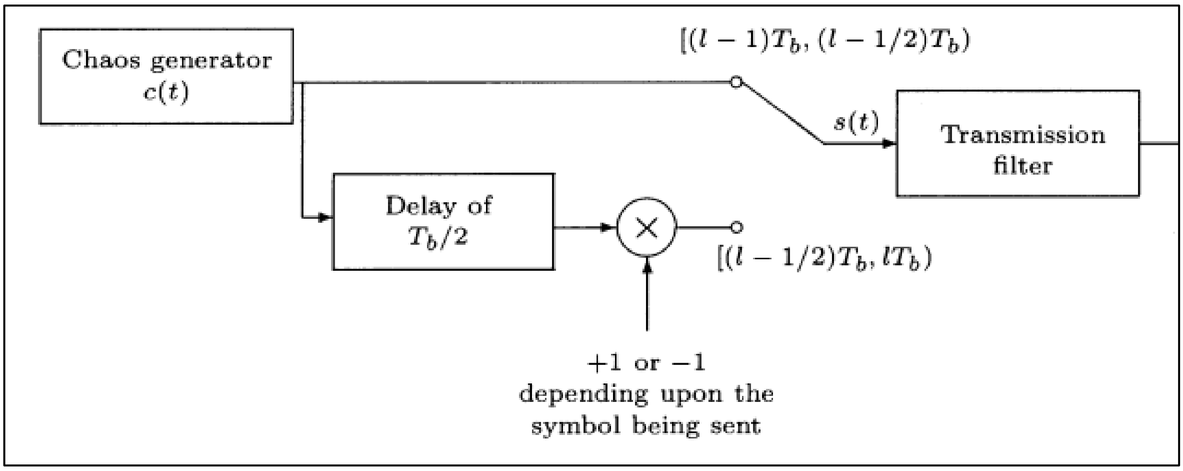

Figure 2-11: DCSK modulator [58].

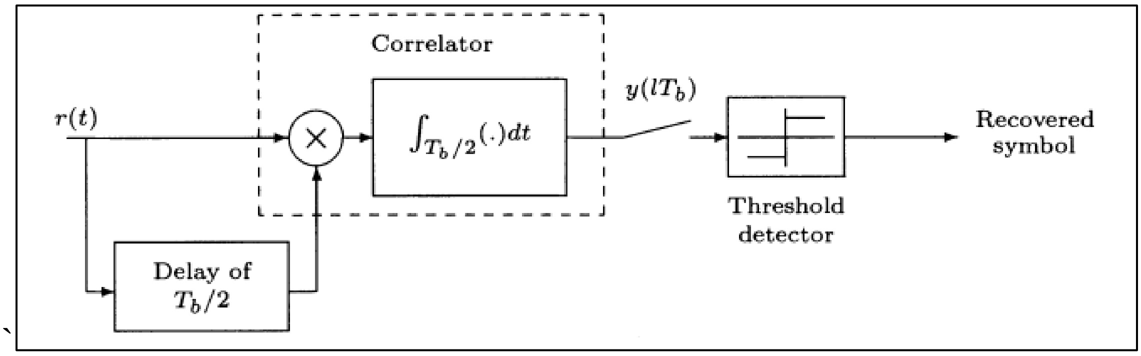

Figure 2-12: DCSK demodulator [58].

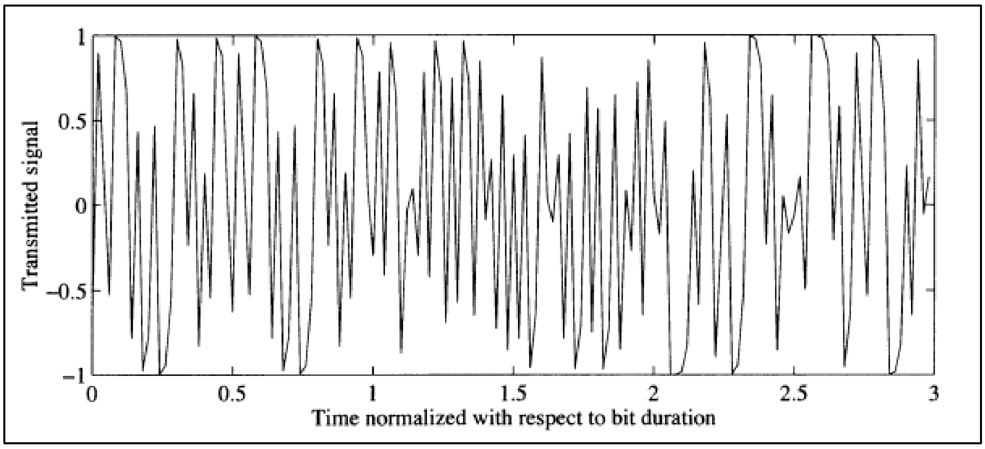

Figure 2-13: A typical transmitted DCSK signal sample.

Note that the centers of the two clusters corresponding to the two symbols are located at equal distance from zero. Thus, setting the threshold at zero is sufficient to differentiate the two symbols. If the channel is noisy, however, the two clusters widen and overlap each other, Thus, although errors are inevitable, the optimal threshold remains at zero. This is clearly an advantage of DCSK over the non-coherent CSK discussed earlier. Furthermore, DCSK is almost insensitive to channel distortion. This is because the channel usually does not vary much within a symbol period and both the reference and data samples are thus subject to the same distortion.

The main drawback of DCSK, however, is that it can only transmit at half the data rate of the other systems because it spends half of the time transmitting the non-information-bearing reference samples. One possible way to increase the data rate is to use a multilevel demodulation scheme [55]. The price to pay, however, is a more complicated system and a possibly degraded bit error performance due to the attenuation of the channel.

2.15 Image Quality Measurement Tests

In image encryption, feature skulking of the original image from visual monitoring is one of the important factors of encryption examining, but it is not enough to measure the image encryption algorithm strength. So, scientist proposed algorithms which have been adopted to measure the encryption algorithm strength. The image after encryption will be compared with itself before encryption to check the algorithm powerful, even if the change is in the pixel's value, pixel's position or both of them. Higher and irregular changes in them mean the more effective of image encryption algorithm.

There are many techniques and algorithms used for the image encryption algorithm strength measurement, these are: The Correlation Coefficient Measuring Factor, Maximum Deviation analysis, Entropy, Peak Signal-to-Noise Ratio (PSNR) and Structural similarity index measure (SSIM).

2.15.1 The Correlation Coefficient

The correlation coefficient is a statistical analysis which is used to obtain the relationship between two random variables or data sets. In image processing, it is used to obtain the similarity between two images. So, for image encryption, it is one of statistical analysis that is used to calculate the encryption algorithm strength. When the result of it equals zero, that means the images are totally different (original and the encrypted images). If it is equal to one, that means the encryption process failed to hide the details of the original image. The correlation coefficient could be obtained as follows:

$$Corr = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}((x_i - E(x)))^2} \ \sqrt{\sum_{i=1}^{N}((y_i - E(y)))^2}} \tag{2.10}$$

where $1/N \sum_{i=1}^{N} x_i$, x and y are the pixel's value of the original and the encrypted image respectively. [60]

2.15.2 Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) can be used to evaluate the encryption scheme strength by indicating the pixel's value between the original image and the encrypted image. It can be calculated by using the following equation.

$$PSNR = 10\ \log_{10}\left[\frac{M*N*255^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(x(i,j)-y(i,j)\right)^2}\right] \qquad (2.11)$$

where x and y are the original and the encrypted image respectively, (i,j) is the coordinate of the pixel and M,N are the image size. Lower PSNR means higher encryption effectively. [61]

2.15.3Maximum Deviation Analysis

Maximum Deviation analysis is a statistical analysis which is used to calculate the deviation between the original and the encrypted images. This analysis could be calculated according to the following equation:

$$MD = \frac{h_o+h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad (2.12)$$

where $h = |H - \grave{H}|$, H and H' are the histogram distribution of the original and the encrypted image. Higher MD means higher encryption degree and the encrypted image faraway (deviated) from the original one [61].

2.15.4 Entropy

One of the well-known analyses for randomness and encryption quality measurements is Information Entropy Analysis. The encryption quality could be measured by calculating the entropy of the plain image and the entropy of the cipher image, then comparing between them. The entropy of the image could be evaluated by the following equation:

$$E = \sum_{i=0}^{2^n-1}[P(i) * \log_2(\frac{1}{P(i)}) \qquad (2.13)$$

where P(i) means the symbol i probability which is expressed in bits. So, for images with gray level of 256 (0 to 255), the maximum entropy equals 8, and it is referred to as an ideal case of randomness. In general, the entropy of practical image is less than the maximum entropy. In encryption process; the entropy of the encrypted image should be ideally equal to 8. When the entropy of it is less than 8, it confirms degree predictability.

To resist the entropy attack, the entropy of the encrypted image should be close to the maximum entropy value. [61]

2.15.5 Structural similarity index measure (SSIM)

Is a method for predicting the perceived quality of digital television and cinematic images, as well as other kinds of digital images and videos. SSIM is used for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference. The SSIM index is calculated on various windows of an image. The measure between two windows x and y of common size N*N is;

$$SSIM(x, y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{2.14}$$

μ_x , μ_y pixel sample of x and y .

σ_x^2, σ_y^2 the variance of x and y , σ_{xy} the covariance of x and y.

$c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ two variables to stabilize the division with weak denominator.

L the dynamic range of the pixel-values (typically is $2^{bits\ per\ pixel} - 1$)

$k_1 = 0.01$, $k_2 = 0.03$ by default.

Chapter Three

Proposed Secure Communication Systems Based on Chaos

3 Chapter Three: Proposed Secure Communication Systems Based on Chaos

3.1 Introduction

This chapter discusses how to create a communication system that is both secure and noise resistant. First the security features of the system are based on hyper-chaotic system (Rabinovich system). Then the communication part is based on a non-coherent Differential Chaotic Shift Keying (DCSK). Finally, the image quality measure to be sent through the proposed system are given at the end of this chapter. This system's implementation and design are carried out with the help of the MATLAB software (R2019a).

3.2 The proposed System

Figure (3-1) and (3.2) depicts the suggested system model. First, both the transmitter and the receiver are aware of the image encrypted using a Hyper Chaotic (Rabinovich System) method. The encrypted image is then transmitted across the AWGN channel using DCSK.

At the receiver side, the received DCSK signal plus AWGN noise collected from the transmission channel. In the next sections the details of the algorithms to image encryption based chaotic signal. To improve the system performance the noise signal incorporated with the useful signal should be reduced. To achieve this, noise reduction schemes are proposed based on changing power between bits as depended on the weight of significant bits and named as Unequal Error Protection Chaotic Bits method (UEP). In the next sections, Simulation programs and details of these methods, as well as other basic signaling operations will be illustrated.

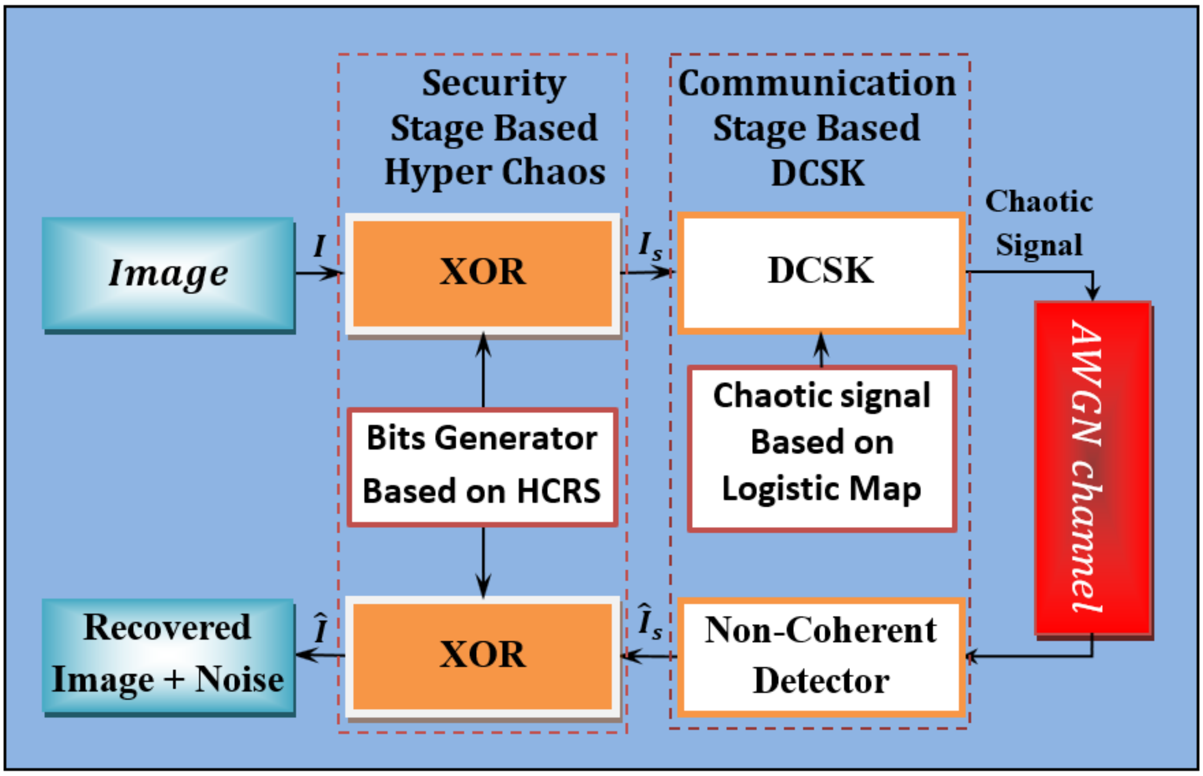

Figure 3-1: Block diagram of the proposed designed system.

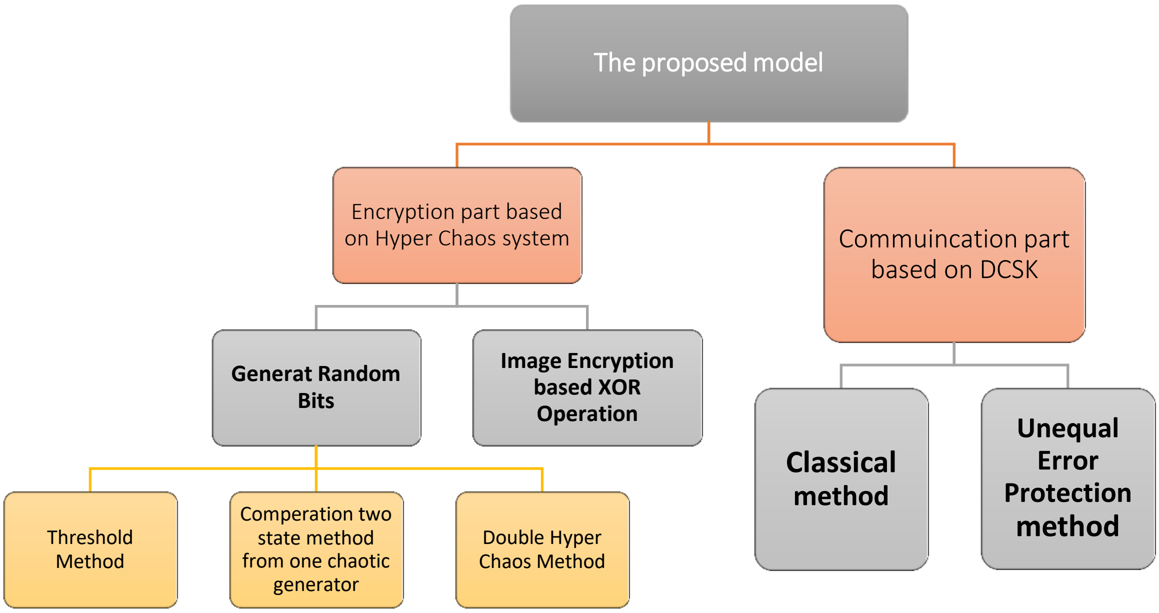

Figure 3-2: Block diagram of the proposed models.

3.3 Encryption Image Based Hyper Chaotic Rabinovich System

3.3.1 Encryption of Image

Digital image encryption is the process by which a significant image is translated into an insignificant or disordered image to strengthen the ability to protect against any attack and improve system security. One of the ways to encrypt images is changing pixel's value; this method employs a chaotic system as a random number generator, with the generated sequence performing a specific operation on the plain text to produce ciphertext, which alters the pixel's value.

The method of encoding the image in this way is summarized as follows

step 1. Generate random sequence from hyper chaos Rabinovich system.

step 2. Convert the decimal chaotic values to binary.

step 3. Converting the gray or colors images to binary form.

step 4. The method of encryption is based on XOR operations between the binary form of image and the random chaotic bits from the step 2.

step 5. Then the encrypted bits (from step 4) vector are converted to the decimal form (encrypted pixels).

step 6. Finally, converted the vector of encrypted pixels to encrypted image is same dimension of clear image. As shown in table (3.1).

Table 3-1: Encryption Sub-Image based chaotic signal and XOR.

Original Pixels (Sub-Image)	Random Bits from Chaotic Signal	Enc. Pixel (XOR Operation)
$(161)_{10} \rightarrow (10100001)_2$	$(155)_{10} \rightarrow (10011011)_2$	$(00111010)_2 \rightarrow (058)_{10}$
$(090)_{10} \rightarrow (01011010)_2$	$(115)_{10} \rightarrow (01110011)_2$	$(00101001)_2 \rightarrow (041)_{10}$
$(255)_{10} \rightarrow (11111111)_2$	$(230)_{10} \rightarrow (11100110)_2$	$(00011001)_2 \rightarrow (025)_{10}$
$(057)_{10} \rightarrow (00111001)_2$	$(180)_{10} \rightarrow (10110100)_2$	$(10001101)_2 \rightarrow (141)_{10}$
$(167)_{10} \rightarrow (10100111)_2$	$(170)_{10} \rightarrow (10101010)_2$	$(00001101)_2 \rightarrow (013)_{10}$

3.3.2 Generate Random Sequence from Chaotic Flow

This system uses three ways to generate a stream of random bits (ones and zeros) with the same properties as the PN (Pseudo Random Noise) code from the hyper-chaos on which the cryptography is based. After the input image signal is transformed into a digital image signal, this code will be exclusive or (XOR). In this framework, an HCRS will be employed to generate a stream of bits in three ways, resulting in a chaotic code that is equivalent to the PN code.

There are some typical steps in all of the suggested approach and will be clearly illustrated in the following flowchart (3-3).

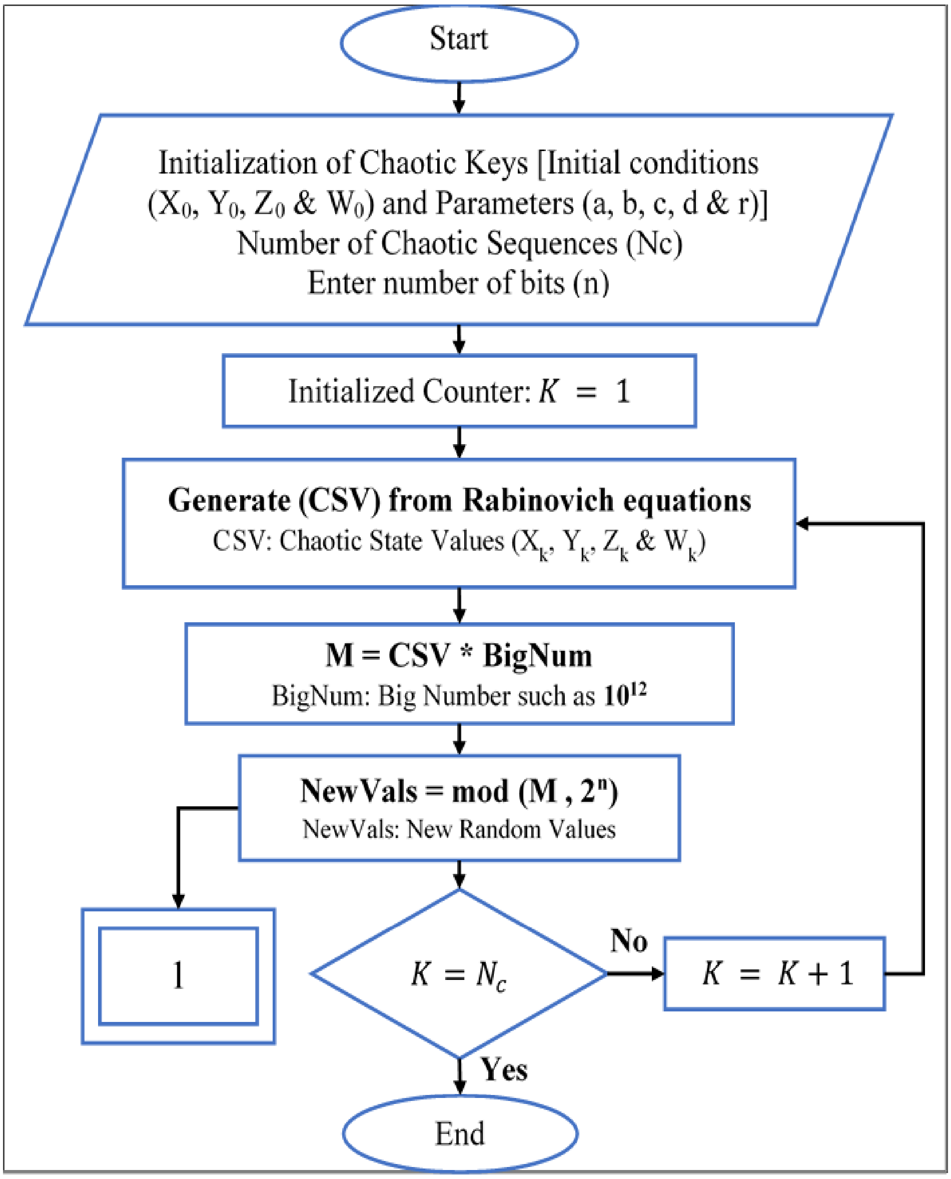
Start
Initialization of Chaotic Keys [Initial conditions
(X0, Y0, Z0 & W0) and Parameters (a, b, c, d & r)]
Number of Chaotic Sequences (Nc)
Enter number of bits (n)
Initialized Counter: K = 1
Generate (CSV) from Rabinovich equations
CSV: Chaotic State Values (Xk, Yk, Zk & Wk)
M = CSV * BigNum
BigNum: Big Number such as 10^12
NewVals = mod (M , 2^n)
NewVals: New Random Values
1
K = Nc
No
K = K + 1
Yes
End

Figure 3-3: General flowchart generating random numbers from chaos

3.3.2.1 HCRS based on Threshold Method

This method can be summarized as follows:

1. Initialized the value of all parameters and initial conditions for the chaotic system,

2. Initialized the number of bits (n) from each state value,

3. Generate four state vector Chaotic sequence (X, Y, Z & W) from differential equations of Rabinovich chaotic system,

4. To get high dynamic from the generated chaotic values, multiply by the considerable number (such 10^{12}), Divided by the maximum value (MidVal = $(2^n)/2$) and take the reminder.

5. Convert $RandVal$ from decimal form to binary by taking thresholds value if ($RandVal \geq \text{threshold}$) value the result will be 1, and if ($RandVal < \text{threshold}$) value the result will be 0.

In figure (3.4) the flowchart diagram shows all these details. While fig. (3.5) shows the signal generated by the threshold method.

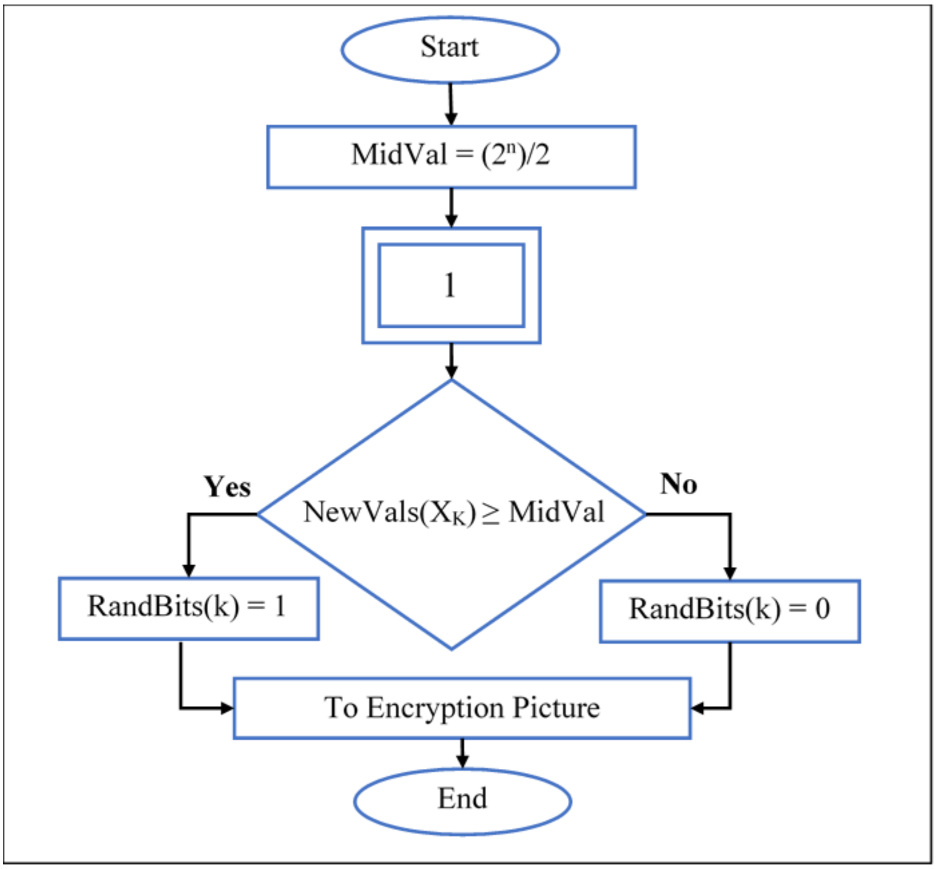

Figure 3-4: Signal flow of the Threshold Method.

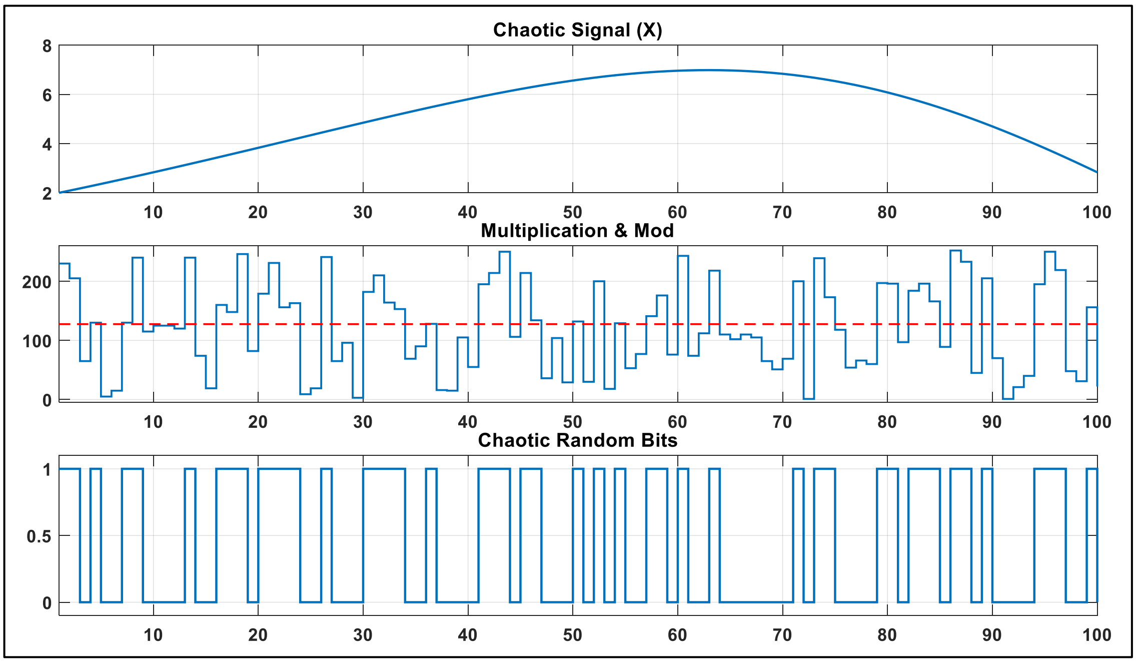

Figure 3-5: Signal graph for the Threshold Method.

3.3.2.2 HCRS based on Comber with Two Vectors (HCRS_CV)

This method includes initializing the value of all parameters and initial conditions for the chaotic system, initialized the number of bits (n) from each state value, Generate two state vector for chaotic system (X, Z) from differential equations of Rabinovich chaotic system, As mentioned previously, to get high randomness from the generated chaotic values , multiply by the considerable number (such as 10^{12}) and divided by maximum value (MaxVal=(2^{n})) and take remind number, After that, the two vectors are compared, and if (x) is greater or equal, the result is 1 on the contrary, the result is 0.

In figure (3.6) the flowchart diagram shows all these details. While fig. (3.7) shows the signal generated by the threshold method.

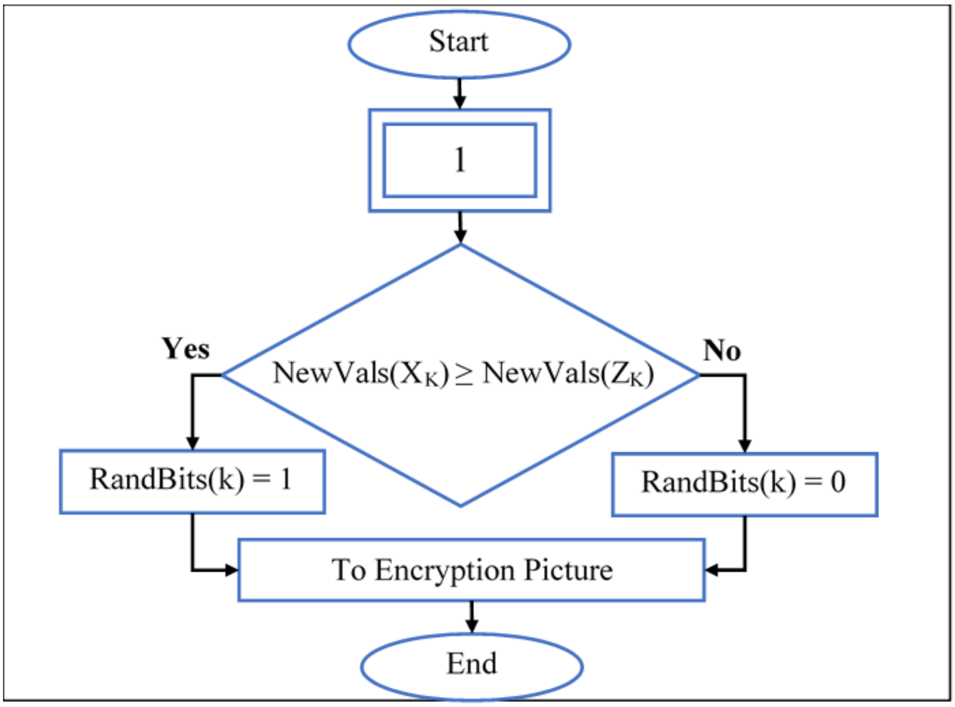

Figure 3-6: Sub-flowchart of the Comber method to generate random bits.

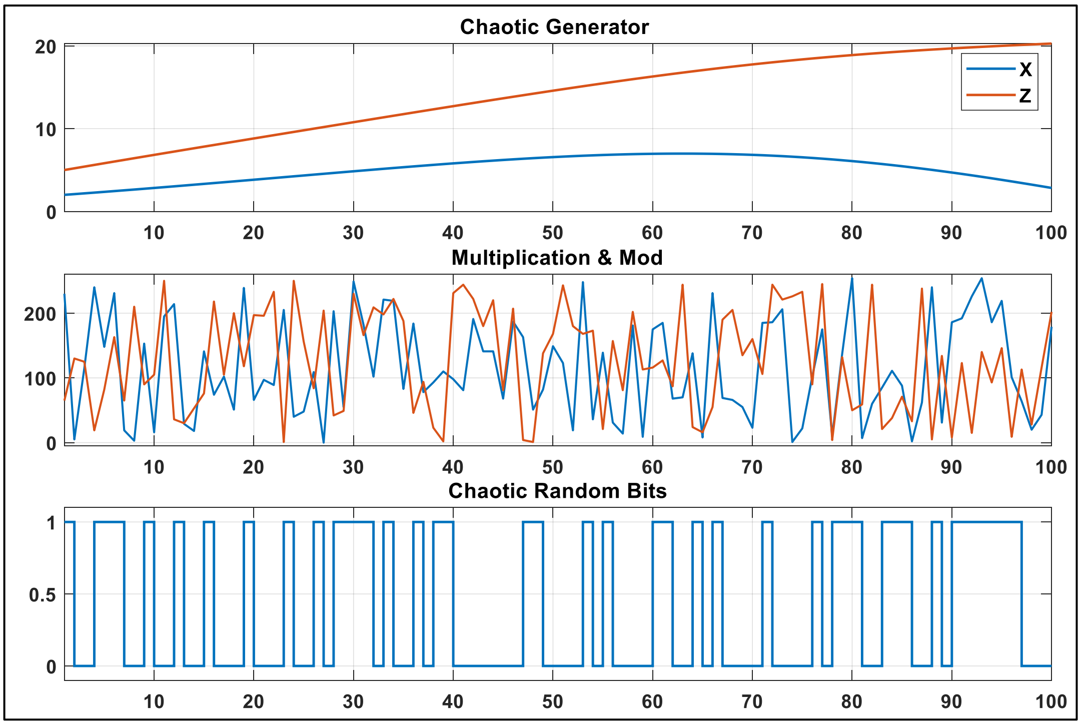

Figure 3-7: Signal graph for the Comber method.

3.3.2.3 HCRS based on Double Hyper Chaos (HCRS-DHC)

In this method, establish the values of all parameters and initial conditions of two chaotic Rabinovich systems and multiply each function by considerable number (such 10^{12}), divided by the maximum value (MaxVal = (2^n)) and take the remind number, finally compare them; if the value from the first chaotic system is greater or equal than the value from the second chaotic system, the bits are 1s. Otherwise, they are 0s, and vice versa. In figure (3.8) the flowchart diagram shows all these details. While fig. (3.9) shows the signal generated by the threshold method.

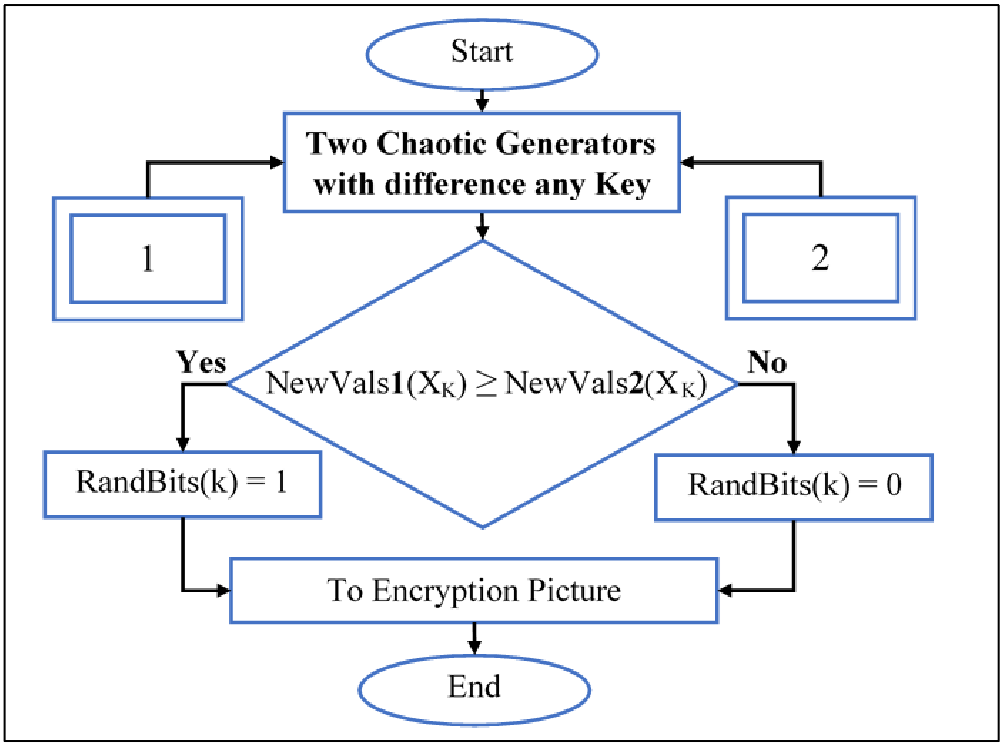
Start
Two Chaotic Generators with difference any Key
1
2
Yes
No
NewVals1(XK) ≥ NewVals2(XK)
RandBits(k) = 1
RandBits(k) = 0
To Encryption Picture
End

Figure 3-8: Sub-flowchart of the HCRS based on double Hyper Chaos

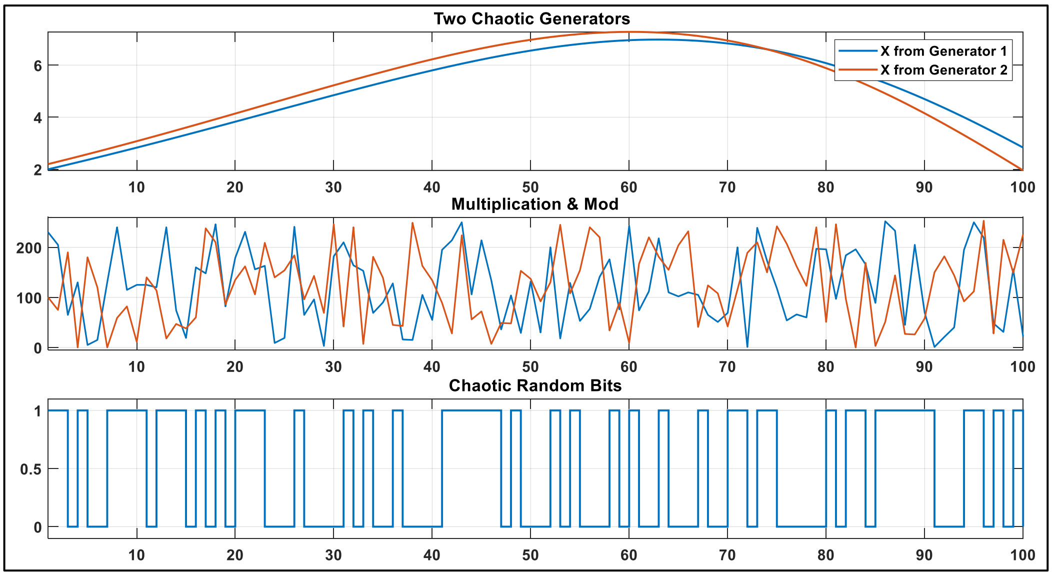

Figure 3-9: Signal graph for the HCRS based on double Hyper Chaos.

Each of these techniques must produce bits of characteristics. It's similar to the PN code. It will also appear in the results. Balance and Run are the most significant properties of the PN code. Property of balance means that the number of 1s and 0s is equal over the series, which implies the relative number of the 0's and 1's probability are 1⁄2 to each. Property of Run indicates that succession within one cycle of equivalent symbols (1's or 0's), a length series equal to the length of the Run.

3.4 Differential Chaotic Shift Keying

3.4.1 Modulation Part:

Every transmitted symbol is represented by chaotic signal samples in the differential chaos-shift-keying (DCSK), The first part is used as a reference (reference sample), and the second part is used to carry the data (data sample).

In this part:

- Convert the data bits to bipolar form
- Chaos signal is equipped with the use of Logistic map with initial condition (X_1=0.1)

$$X_{i+1} = 1 - 2X_i \tag{3.1}$$

- To prepare the reference signal Ref_{sig}, values are taken from the chaos signal of length equal to the value of beta for each bit.

  Where: Beta is equal number of chaotic samples in Ref_{sig}, and equal 0.5 Spreading factor.
- Perform a multiplication of the Ref_{sig}*bipolar data Thus, the so-called Data_{sig} is obtained.
- Modulate both the Data_{sig} and the Ref_{sig}. Then the modulation signal is sent through AWGN channel. Figure (3.10) show the idea of topic.

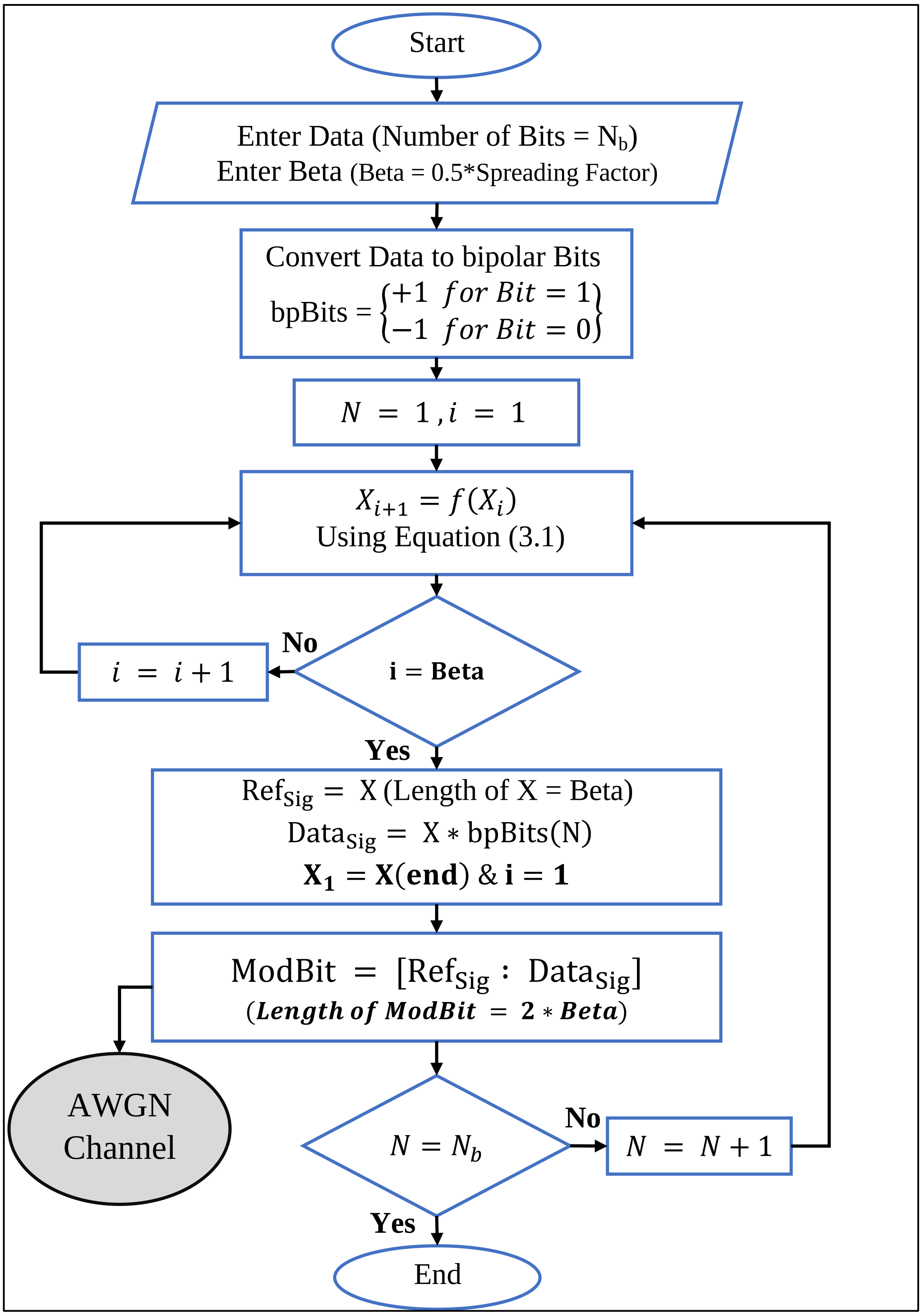
Start
Enter Data (Number of Bits = N_b)
Enter Beta (Beta = 0.5*Spreading Factor)
Convert Data to bipolar Bits
bpBits = $\begin{Bmatrix} +1 \ for\ Bit = 1 \\ -1 \ for\ Bit = 0 \end{Bmatrix}$
$N = 1, i = 1$
$X_{i+1} = f(X_i)$
Using Equation (3.1)
No
$i = i + 1$
i = Beta
Yes
$\mathrm{Ref_{Sig}} = $ X (Length of X = Beta)
$\mathrm{Data_{Sig}} = \mathrm{X} * \mathrm{bpBits(N)}$
$\mathbf{X_1 = X(end)}$ & $\mathbf{i = 1}$
$\mathrm{ModBit} = [\mathrm{Ref_{Sig}} : \mathrm{Data_{Sig}}]$
$(\boldsymbol{Length\ of\ ModBit} = \mathbf{2} * \boldsymbol{Beta})$
AWGN Channel
$N = N_b$
No
$N = N + 1$
Yes
End

Figure 3-10: The flowchart of the Transmitter side of DCSK.

3.4.2 Demodulation part

In this part, the encrypted image will be restored, knowing which bits were zero or one will do the following

$$demodulation\ signal = sum(Ref_{sig} * data_{sign}) \qquad (3.2)$$

If the result of this process is positive, then this means that it is one, and if it is negative, then it means that it is zero. To this extent, the encoded image vector was obtained.

As for decoding and getting original image we need to generate a chaos signal exactly the same as what was generated by the encryption process. By performing XOR operation between chaos signal and vector of encryption image. The flowchart in (3.11) explains the process in the receiver side and figure (3-12) is illustrates the idea of the topic.

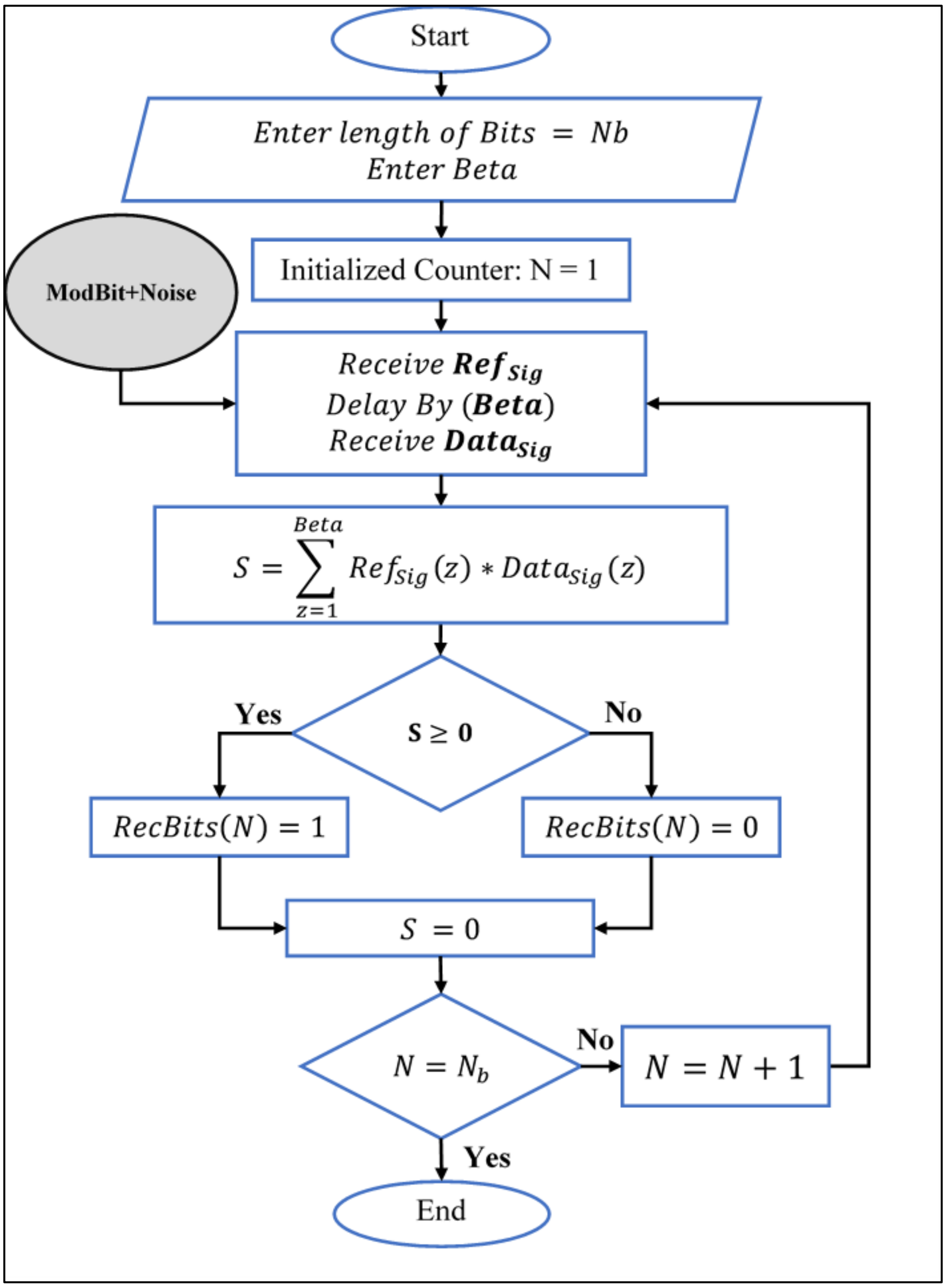
Start
Enter length of Bits = Nb
Enter Beta
ModBit+Noise
Initialized Counter: N = 1
Receive $\boldsymbol{Ref}_{Sig}$
Delay By (**Beta**)
Receive $\boldsymbol{Data}_{Sig}$
$S = \sum_{z=1}^{Beta} Ref_{Sig}(z) * Data_{Sig}(z)$
Yes
$S \geq 0$
No
$RecBits(N) = 1$
$RecBits(N) = 0$
$S = 0$
$N = N_b$
No
$N = N + 1$
Yes
End

Figure 3-11: Flowchart of Demodulation Part from DCSK

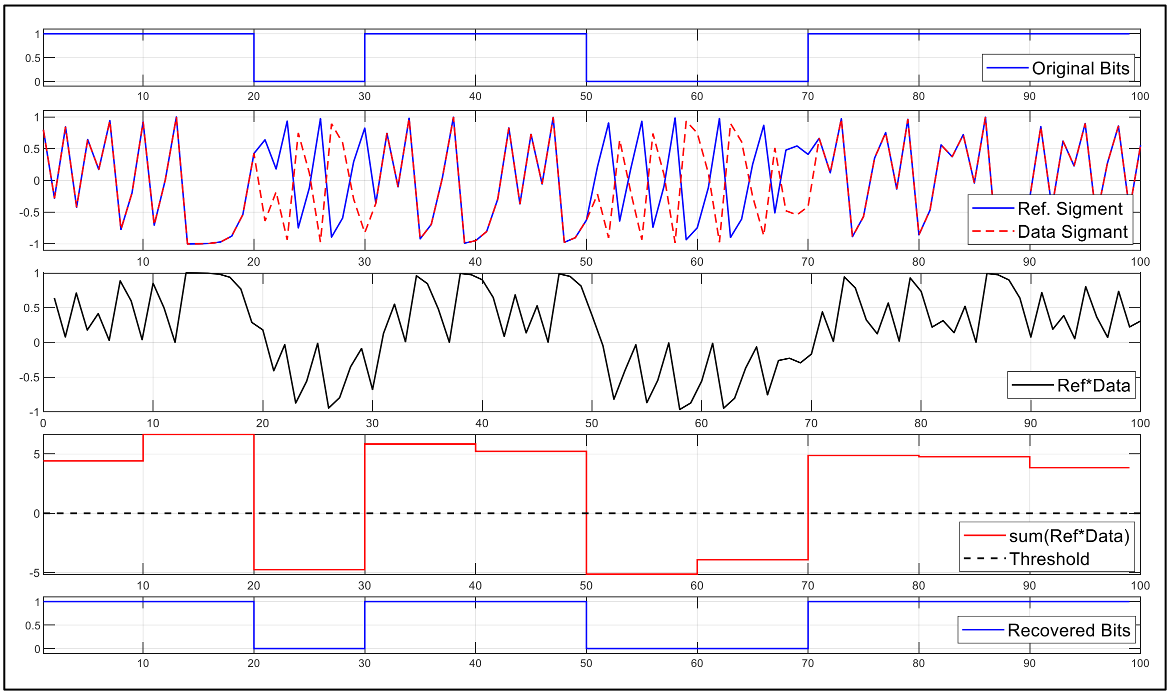

Figure 3-12: Signal graph of DCSK.

3.5 *Unequal Error Protection for DCSK signal (UEP)*

In the communication systems, UEP indicates that there are distinct bits of the transmitted signal may have different error sensitivity. The most common method is the (UEP) based on channel coding. For a variety of reasons, certain broadcast systems may not utilize channel coding. To overcome this issue, a unique strategy for achieving UEP by assigning varying power to certain bits based on their error sensitivity is presented. The optimization criteria for UEP have a significant relationship with subjective reality.

$$P = V^2/R \qquad (3\text{-}3)$$

*P = 8/R watt

It is known that the image in general consists of a pixel’s matrix and each pixel consists of 8 bits - one byte - for the gray image and 24 bits divided into three colors for the color image (RGB Image). The weight and importance of each bit in a byte varies according to the location of the bit, the most bit (MSB) being the equivalent of 2^7 =128 and the first bit (LSB) is equivalent 2^0 =1. It's means that the MSB bit = 128 times of LSB bit. As well as the rest of the bits depending on 2 to the power of n as shown below. The MSB bit equal 128 times of the first bit (LSB).

From this discrepancy in importance and power, it must be accompanied by a transgressive importance in the transmission systems, especially when the transmission medium has very bad conditions. This is what was adopted in this proposal to reduce noise. the following flowchart in fig. (3-13) clarifies more.

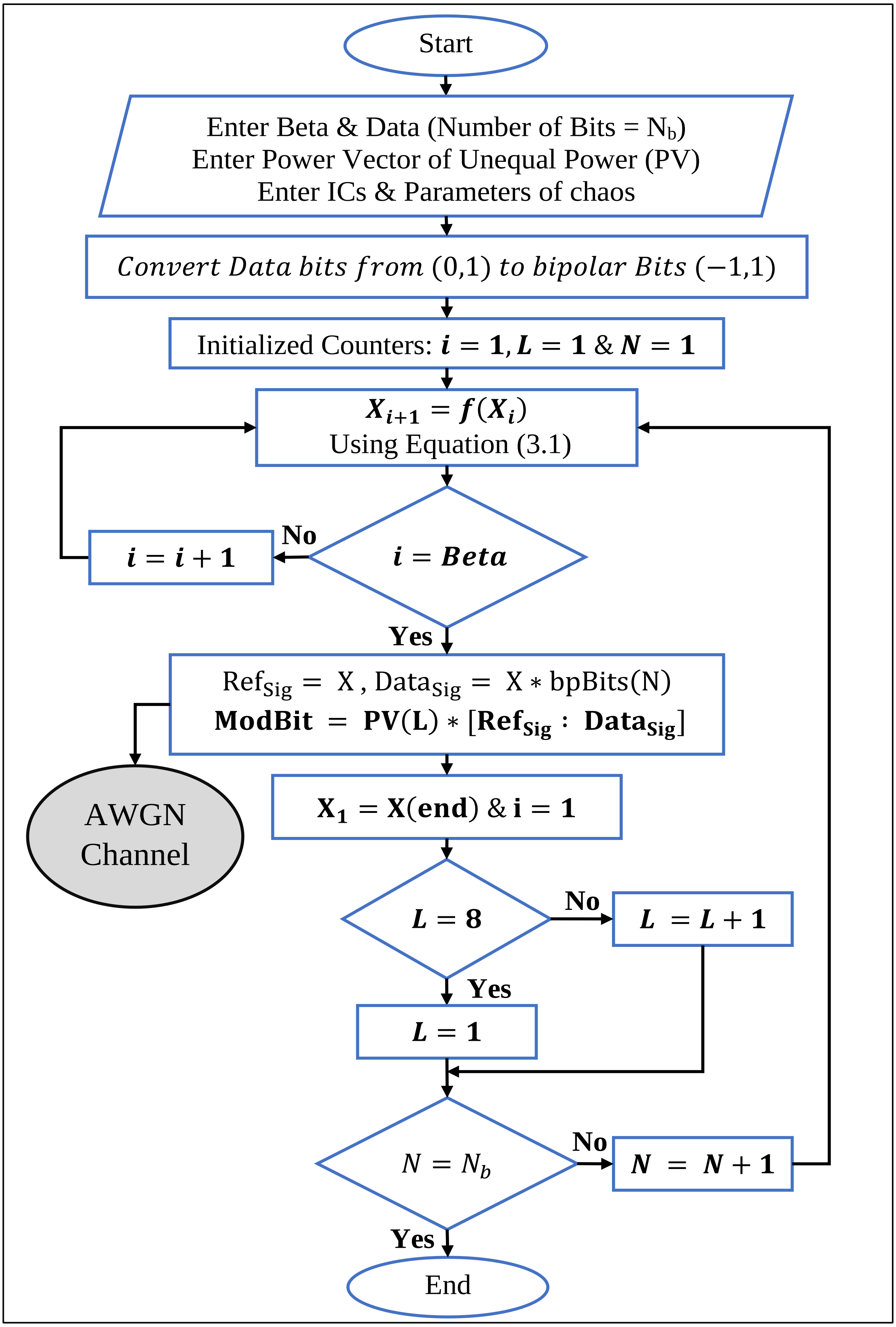
Start
Enter Beta & Data (Number of Bits = N_b)
Enter Power Vector of Unequal Power (PV)
Enter ICs & Parameters of chaos
$Convert\ Data\ bits\ from\ (0,1)\ to\ bipolar\ Bits\ (-1,1)$
Initialized Counters: $\boldsymbol{i=1, L=1}$ & $\boldsymbol{N=1}$
$\boldsymbol{X_{i+1} = f(X_i)}$
Using Equation (3.1)
$\boldsymbol{i = Beta}$
No
$\boldsymbol{i = i+1}$
Yes
$\mathrm{Ref_{Sig}} = \mathrm{X}$, $\mathrm{Data_{Sig}} = \mathrm{X} * \mathrm{bpBits(N)}$
$\mathbf{ModBit} = \mathbf{PV(L)} * [\mathbf{Ref_{Sig}} : \mathbf{Data_{Sig}}]$
AWGN Channel
$\mathbf{X_1 = X(end)}$ & $\mathbf{i = 1}$
$\boldsymbol{L = 8}$
No
$\boldsymbol{L = L+1}$
Yes
$\boldsymbol{L = 1}$
$N = N_b$
No
$\boldsymbol{N = N+1}$
Yes
End

Figure 3-13: Flowchart of the proposed Unequal Error Protection method over DCSK.

Chapter Four

Simulation Results of The Proposed System

4 Chapter Four: Simulation Results of The Proposed System

4.1 Introduction

The simulation results and a review of the system methodologies established in chapter three are presented in this chapter. present two parts of results, as follow:

1st part: - related to the image encryption part and measuring security of designed scheme based on hyper-chaos.

2nd part: - related to the communication part (DCSK) in equal and UEP and measured the quality of recovered image.

The simulation of the systems has been done using Intel ® Core i5, 4th generation (u), 2.30 GHz with MATLAB software (R2019a).

4.2 Simulation Results of Encryption Sub-System Part

4.2.1 Results simulation of the overall system based Lyapunov exponent

The Lyapunov characteristic exponent is used as a metric for all aspects of chaos and sensitivity to beginning states in this technique. Lyapunov characteristic exponents are used to measure the distance between two near trajectories in terms of initial conditions. As mentioned earlier, hyper chaotic systems have at least two positive Lyapunov exponents. As shown in figure (4.1)

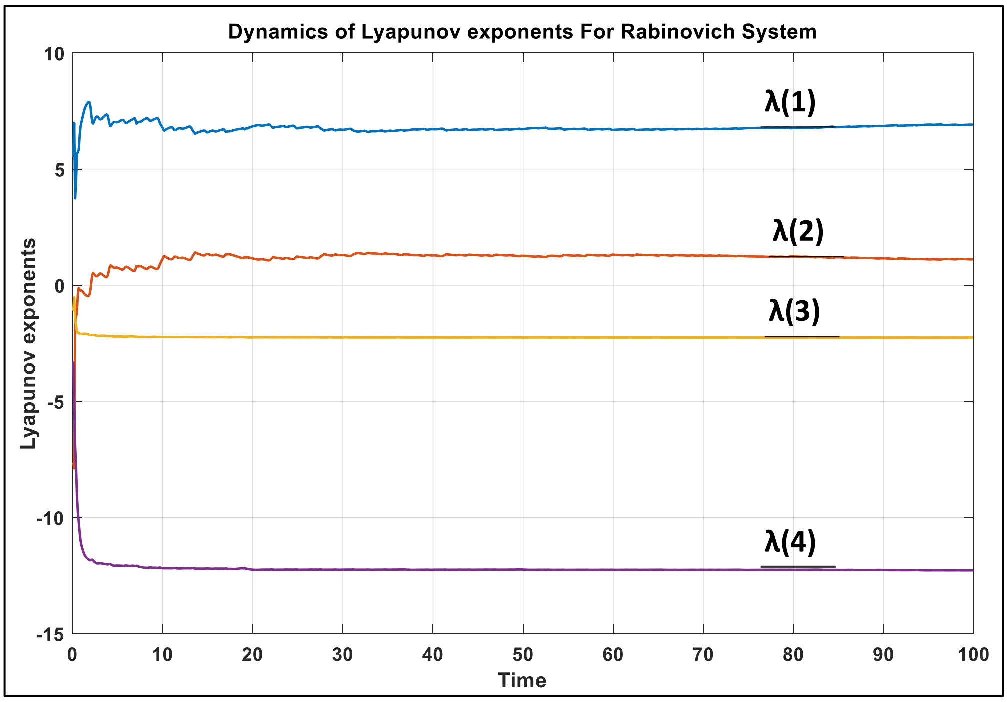

Figure 4-1: Lyapunov exponents of the chaotic Rabinovich system.

From the above figure in the HCRS, Lyapunov exponents are (6.903847, 1.123492, -2.252736, -12.274603) respectively, which means the Rabinovich is a hyper chaotic system.

4.2.2 Simulation Results of Three Approaches for Verifying the Features of a Chaotic Code

The PN code is a lengthy code containing repeating pulses. which can be hundreds of digits long. Still, the chaotic system period approaches infinite, which is its most essential attribute, and its period is unknown. As a result, the entire time will be used to double-check the one-to-zero ratio; a portion of the whole time will be used instead of it.

The partial period is balanced in all three techniques, with the number of zeros and ones nearly equal, implying that the entire period is in balance, as seen in the tables below (4-1). $lim_{t\to\infty} p_0(t) = lim_{t\to\infty} p_1(t) = 0.5$

The result of delay, balance property and number of keys for all proposed methods (Threshold method, Comber with two vector method and Double hyper chaos method) will explain in the following table (4-1).

Table 4-1: Delay, Balance and Key size to All method for Random Bit Generators.

Proposed Method	Number of bits	Delay per second	Balance property	Number of keys
Threshold Method	10^5	0.0597	0.4981	Nine dimensions of keys, 5 parameters (a, b, c, d & h) & 4 Initial Conditions (x, y, z & w)
	10^6	0.8061	0.4979	
	10^7	7.1605	0.4978	
Comber with Two Vector method	10^5	0.0582	0.5015	Nine dimensions of keys, 5 parameters (a, b, c, d & h) & 4 Initial Conditions (x, y, z & w)
	10^6	0.7878	0.5022	
	10^7	7.4139	0.5022	
Double Hyper Chaos method	10^5	0.1324	0.5026	18 dimensions of keys 5 parameters (a1, b1, c1, d1, h1, a2, b2, c2, d2 & h2) & 8 initial conditions (Xo1, Yo1, Zo1, Wo1, Xo2, Yo2, Zo2, & Wo2)
	10^6	1.5135	0.5021	
	10^7	14.1554	0.5019	

From table (4-1), Each of these methods generates a unique set of features. It's the same as the PN code. It will also show up. Balance and Run are the most important aspects of the PN code. The property of balance asserts that a series' number of 1s and 0s is equal, implying that the frequencies of the 0s and 1s are 1/2 to each other. The Run property denotes a succession of equivalent symbols (1's & 0's) with one cycle, with a length series equal to the Run's length.

All results of the three methods are almost the same, but the third method is the best because it contains more key space, for each system (five parameters and four initial conditions) for two systems, we will have eighteen key spaces Thus, this method is more reliable and safer.

4.2.3 Simulation result of image encryption algorithm

Lena image is performance image's test of the proposed algorithms as compared with the traditional schemes. Other different images are used with different dimensions to deeply evaluate the performance. Some of the images have equal dimensions, the others don't. Lena image is used in the implementation which is shown in figure (4.2) with its histogram.

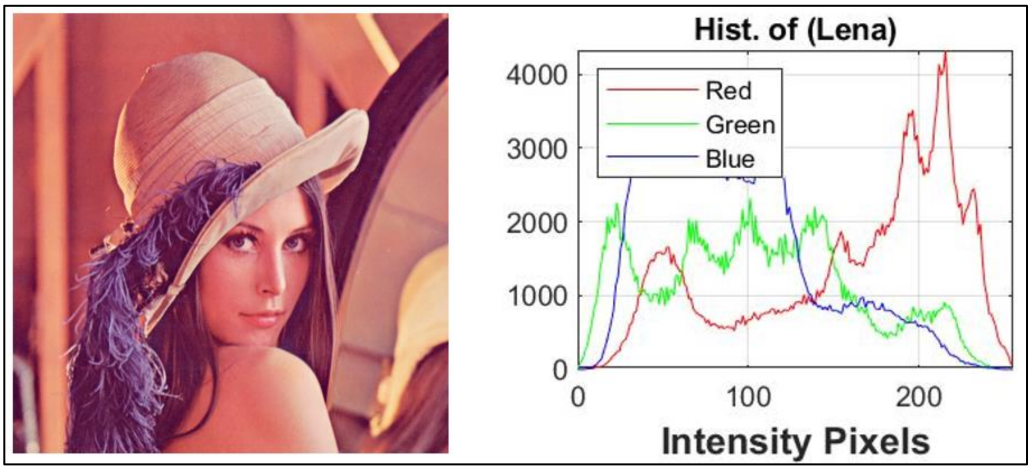

Figure 4-2: Lena Image for testing.

The use of the Lena image as a test image is crucial since it contains a variety of details, including blurred regions, uniform reigns, numerous detailed regions, high entropy, and shading. This image's features make it ideal for testing image processing methods. Other images, such as a cameraman and peppers, are utilized in image processing testing. Figure (4.3) and (4.4) show these images with their histograms.

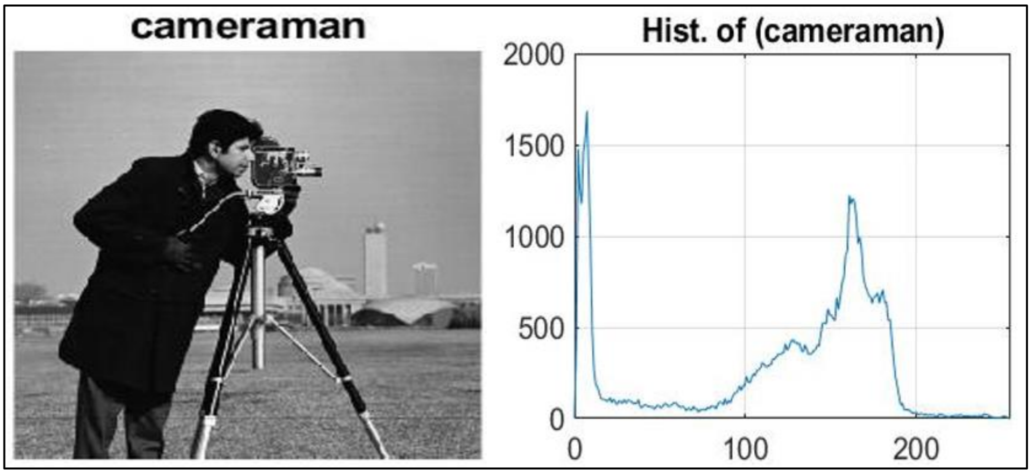

Figure 4-3: Show cameraman image with its histogram.

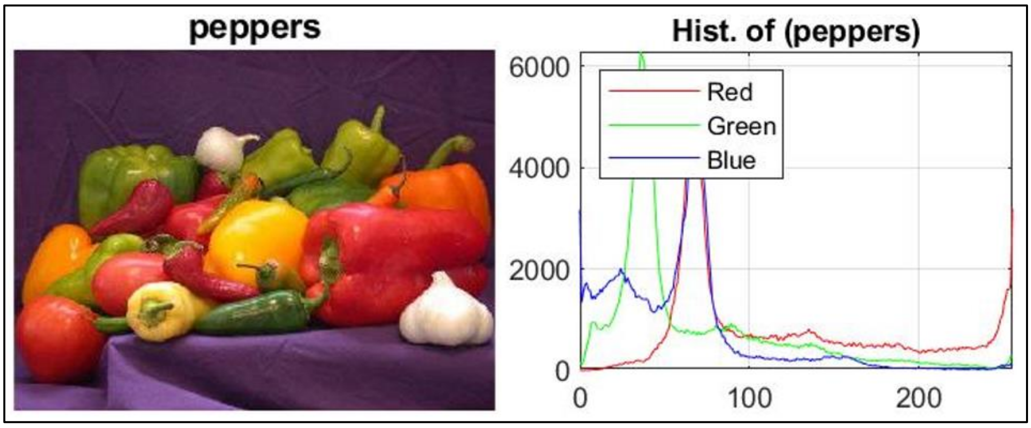

Figure 4-4: Show Peppers image with its histogram.

These images have been converted from 3D & 2D to 1D binary vector using MATLAB functions.

4.2.4 Encryption of Image

The practice of converting a major image into an insignificant or disordered image to boost the ability to protect against any assault and improve system security is known as digital image encryption. Changing the pixel's value is one approach to encrypt image; this method uses a chaotic system as a random number generator, with the created sequence executing a specific operation on the plain text to generate cipher text, which changes the pixel's value.

The method of encryption the image is summarized by performing an XOR operation between random sequence of chaotic flow and vector of image after converting it to 1D. figures below (4-5),(4-6) and (4-7) show the encrypted images.

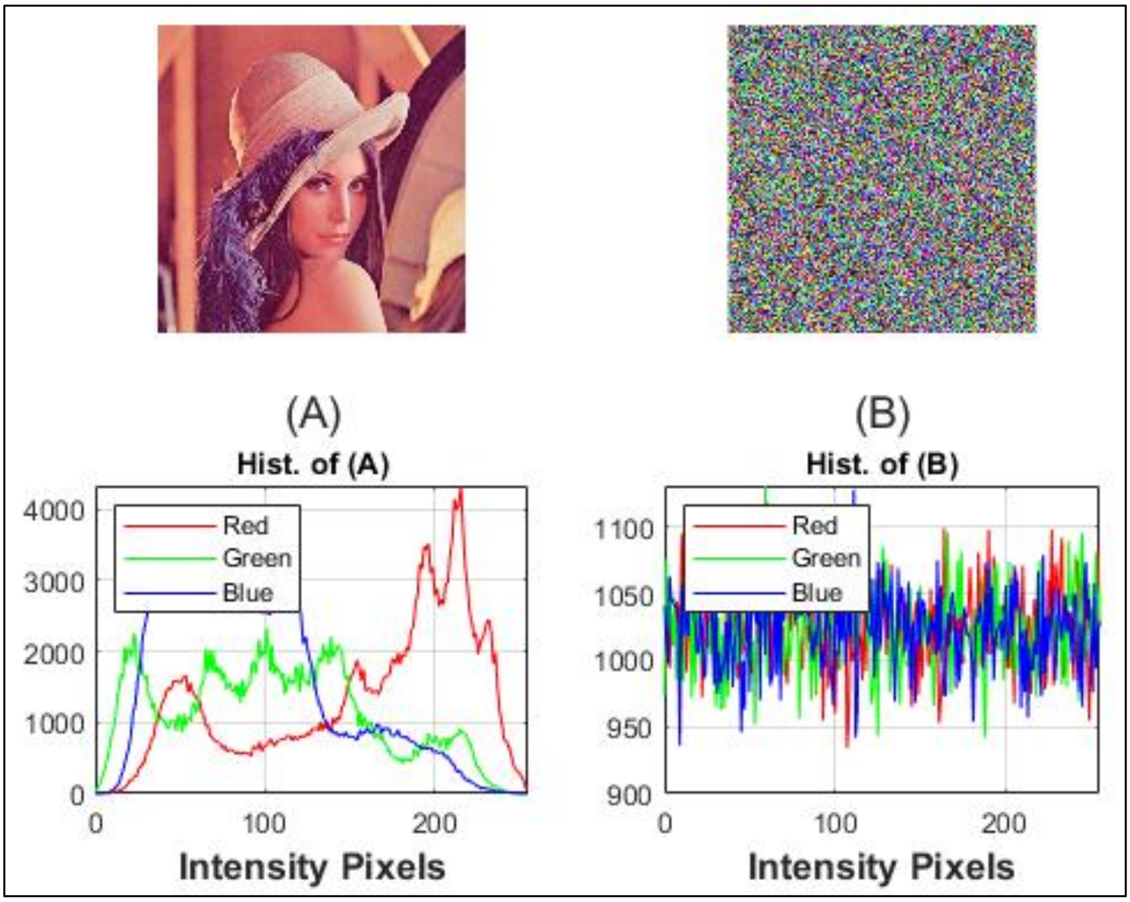

Figure 4-5: Color Image Encryption. (A) Lena Image. (B) Encrypted Image.

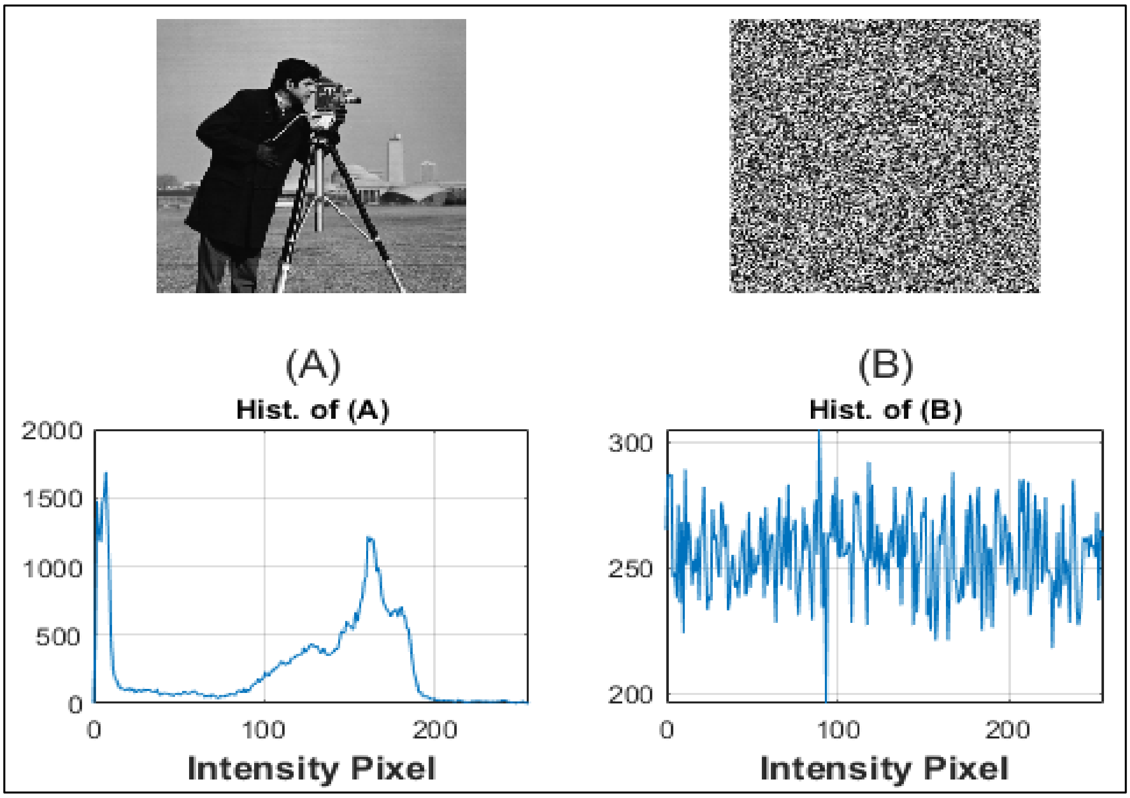

Figure 4-6: Gray scale Image Encryption. (A) Cameraman Image. (B) Encrypted Image.

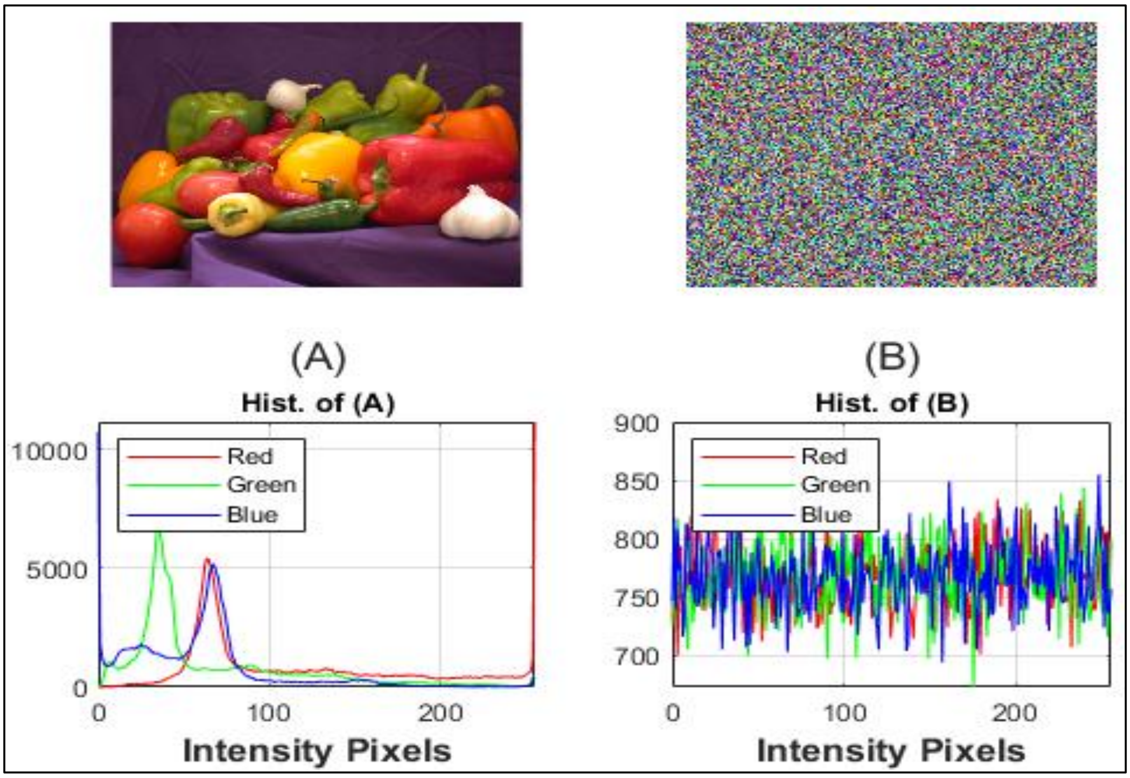

Figure 4-7: Color Image Encryption. (A)Peppers Image. (B) Encrypted Image

4.2.5 Encryption's Quality Tests

While feature skulking of the original image from visual surveillance is an important part of image encryption analysis, it is not enough to judge the image encryption scheme's strength.

As a result, scientists developed techniques for evaluating the strength of encryption schemes. To ensure that the algorithm is effective, the image after encryption will be compared to itself before encryption, regardless of whether the change is in pixel location, pixel value, or both. If there are more and irregular changes in the images, the image encryption algorithm is more effective.

The Correlation Coefficient Measuring Factor, Maximum Deviation Analysis, Entropy, PSNR, and SSIM are some methods and algorithms used to assess the strength of image encryption algorithms. The following table (4-2) show the results of encryption quality test of each image encryption by using different method of generating chaos.

From the results, it is clear that the type of the chaotic function or the method of its generation does not affect the results of the encryption, But the number of dimensions for that function or method and its parameters is directly proportional to the size of the key used for encryption.

Table 4-2: Images Encryption quality by using different method of generating random bits.

Image	Test Type	HCRS-Threshold Method	HCRS_CV	HCRS_DHC
Lena image	Correlation Co.	0.4899	0.472	0.460
	PSNR	8.615	8.599	8.630
	MDA	$3.512*10^5$	$3.389*10^5$	$3.819*10^5$
	Entropy	7.999	7.998	7.999
	SSIM	0.0078	0.0076	0.0075
Cameraman	Correlation Co.	0.5883	0.5872	0.6001
	PSNR	3.604	3.503	4.112
	MDA	$6.41725*10^5$	$6.42312*10^5$	$6.41613*10^5$
	Entropy	7.99686	7.9974	7.9987
	SSIM	0.0081	0.0079	0.0085
Peppers image	Correlation Co.	0.4177	0.4218	0.4200
	PSNR	2.844	2.798	2.832
	MDA	$4.4551*10^6$	$4.4496*10^6$	$4.45430*10^6$
	Entropy	7.9996	7.9998	7.9995
	SSIM	0.0062	0.0061	0.0064

Table (4-2) in illustrate the high security for encrypted image in all testing measurements. As PSNR less than 9dB, Entropy about 8, and SSIM is very small near by zero.

4.3 Simulation Results of DCSK Sub-System Part

4.3.1 Simulation results of traditional DCSK

Each transmitted symbol is represented by two chaotic signals in the DCSK modulation. The first signal serves as a point of reference, while the second serves as a data carrier. Each bit in the encryption image vector is transmitted a number of times in this section. Let's pretend that number is a beta, and the spreading factor equal two beta.

Then a chaos signal is formed, the length of this signal is equal to the length of the vector encoded image after iteration. The chaos signal after being repeated a beta number of times might be taken as a reference. A multiplication is done between the vector of the encoded image after iteration and the chaotic signal processed after iteration in order to acquire the data. Figure (4-8) show the transmitted bits for multi values of beta and multi levels of SNRs. And Figure (4-9) is transmitted of image in multi levels of SNRs.

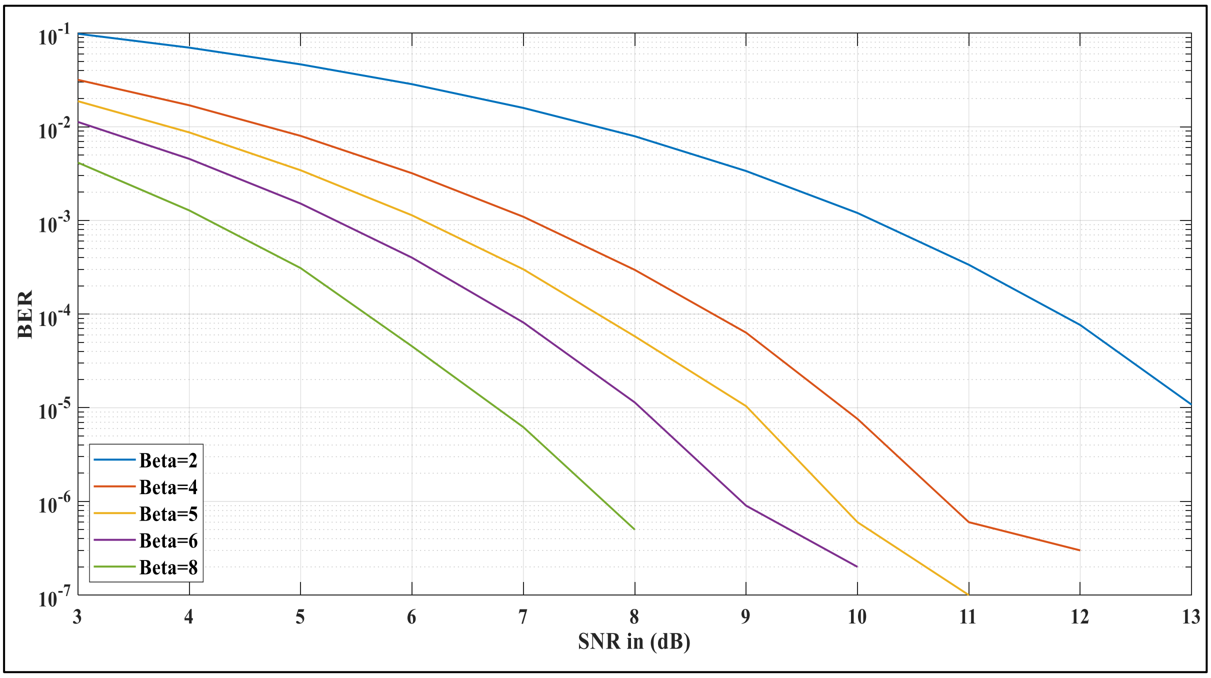

Figure 4-8: BER vs SNR carve for DCSK at multi values of Beta (2, 4, 5, 6 and 8) and SNR (from 3 to 13) dB.

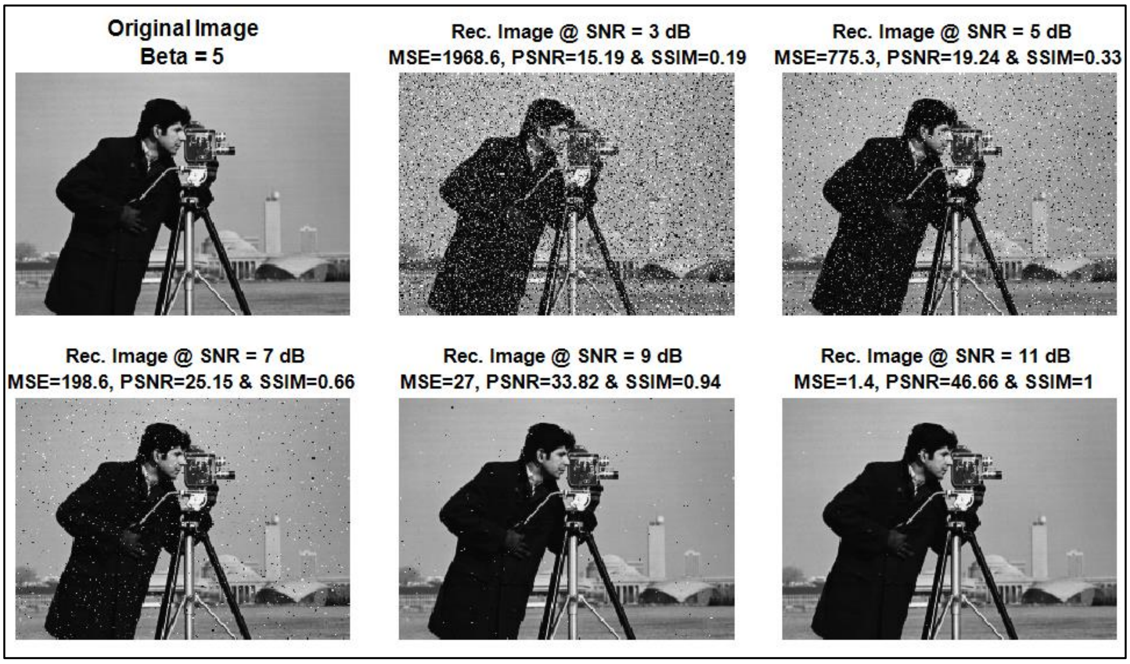
Original Image
Beta = 5
Rec. Image @ SNR = 3 dB
MSE=1968.6, PSNR=15.19 & SSIM=0.19
Rec. Image @ SNR = 5 dB
MSE=775.3, PSNR=19.24 & SSIM=0.33
Rec. Image @ SNR = 7 dB
MSE=198.6, PSNR=25.15 & SSIM=0.66
Rec. Image @ SNR = 9 dB
MSE=27, PSNR=33.82 & SSIM=0.94
Rec. Image @ SNR = 11 dB
MSE=1.4, PSNR=46.66 & SSIM=1

Figure 4-9: Transmission Image in DCSK at (Beta=5) and multi SNRs.

From the above result figures (4-8) and (4-9), it is clear that the use of classical differential chaos gives clear image when the SNR exceed the 11db, So, to treat this case, mean that to get clear image when SNR a few The proposal has been placed below.

4.3.2 Simulation Results of Proposed Unequal Error Protection of DCSK

It comprises giving one aspect of a situation higher emphasis or preference than others. In the field of digital communication, such as video or audio transmissions, individual bits of sent parameters can have different bit error sensitivity. The most common method is to use channel coding with unique error protection (UEP). For a variety of reasons, certain broadcast systems may not utilize channel coding. To address this problem, a unique method is given that accomplishes unique error protection by assigning varied power to specific bits based on their error sensitivity. The mean square error and other tests (PSNR and SSIM) between the original parameter and the decoded parameter represents the optimization criteria for Unequal Error Protection assigning which has a real attachment to perceived reality.

Figures (4-10) to (4-14) show the results of the image encoded using Multi–Unequal Error Protection distributions of DCSK with different value of signal to noise ratio.

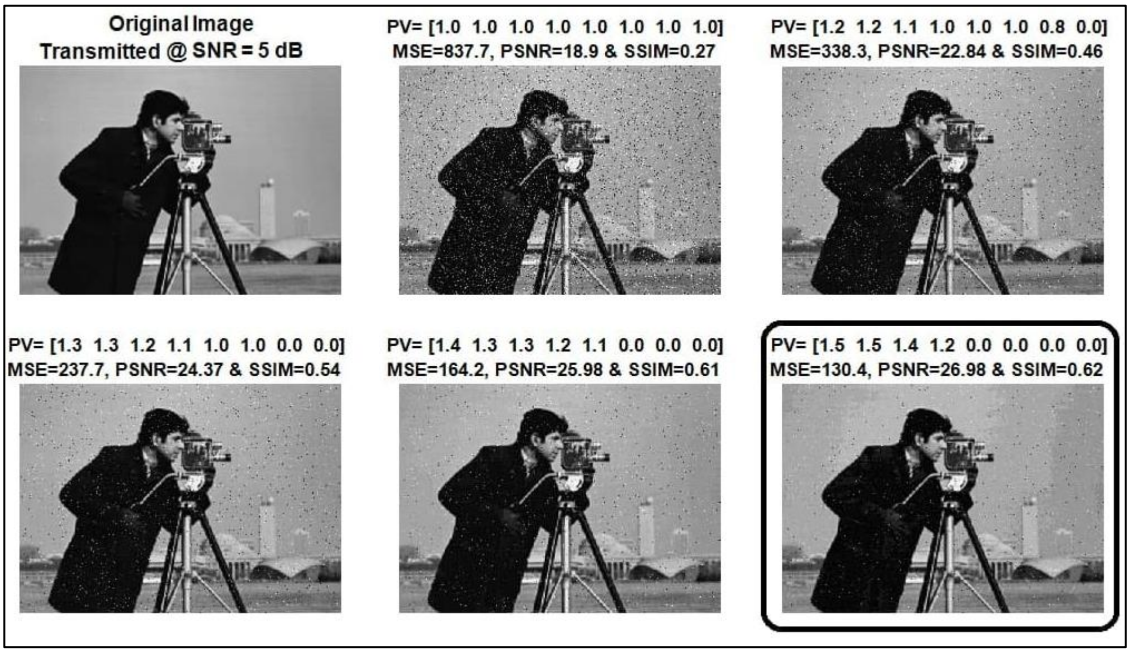
Original Image
Transmitted @ SNR = 5 dB
PV= [1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0]
MSE=837.7, PSNR=18.9 & SSIM=0.27
PV= [1.2 1.2 1.1 1.0 1.0 1.0 0.8 0.0]
MSE=338.3, PSNR=22.84 & SSIM=0.46
PV= [1.3 1.3 1.2 1.1 1.0 1.0 0.0 0.0]
MSE=237.7, PSNR=24.37 & SSIM=0.54
PV= [1.4 1.3 1.3 1.2 1.1 0.0 0.0 0.0]
MSE=164.2, PSNR=25.98 & SSIM=0.61
PV= [1.5 1.5 1.4 1.2 0.0 0.0 0.0 0.0]
MSE=130.4, PSNR=26.98 & SSIM=0.62

Figure 4-10: Multi–Unequal Error Protection distributions of DCSK at Beta = 5. Best Transmission Image at 5th Power Vector at SNR = 5dB.

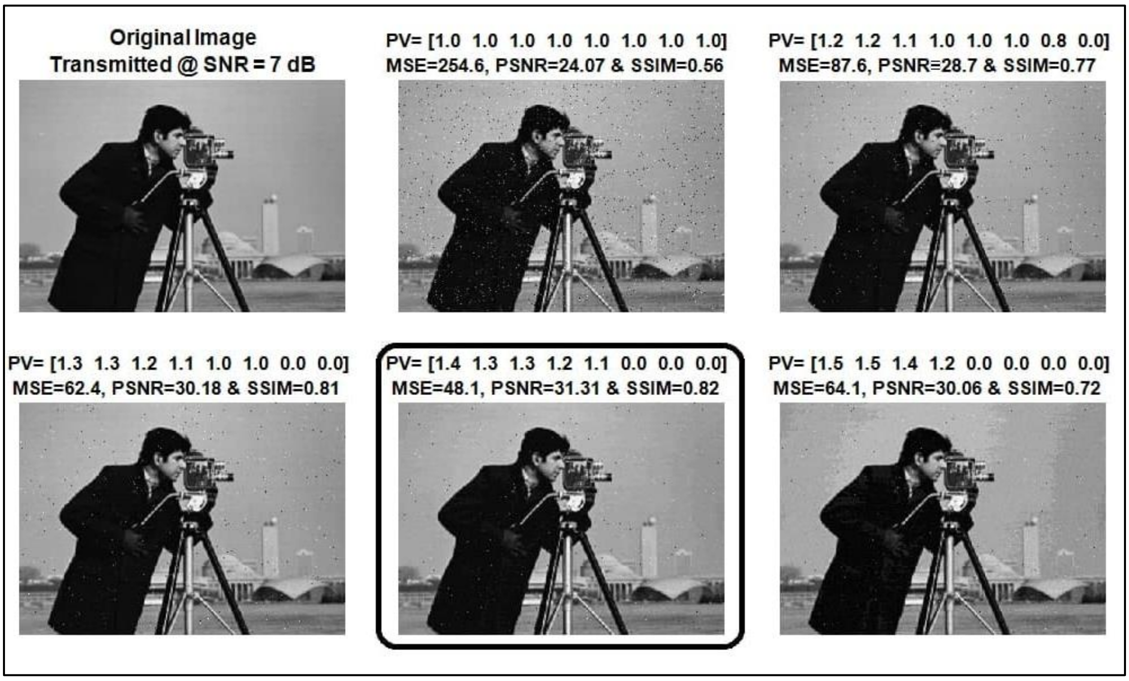
Original Image
Transmitted @ SNR = 7 dB
PV= [1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0]
MSE=254.6, PSNR=24.07 & SSIM=0.56
PV= [1.2 1.2 1.1 1.0 1.0 1.0 0.8 0.0]
MSE=87.6, PSNR=28.7 & SSIM=0.77
PV= [1.3 1.3 1.2 1.1 1.0 1.0 0.0 0.0]
MSE=62.4, PSNR=30.18 & SSIM=0.81
PV= [1.4 1.3 1.3 1.2 1.1 0.0 0.0 0.0]
MSE=48.1, PSNR=31.31 & SSIM=0.82
PV= [1.5 1.5 1.4 1.2 0.0 0.0 0.0 0.0]
MSE=64.1, PSNR=30.06 & SSIM=0.72

Figure 4-11: Multi–Unequal Error Protection distributions of DCSK at Beta = 5. Best Transmission Image at 4th Power Vector at SNR = 7dB.

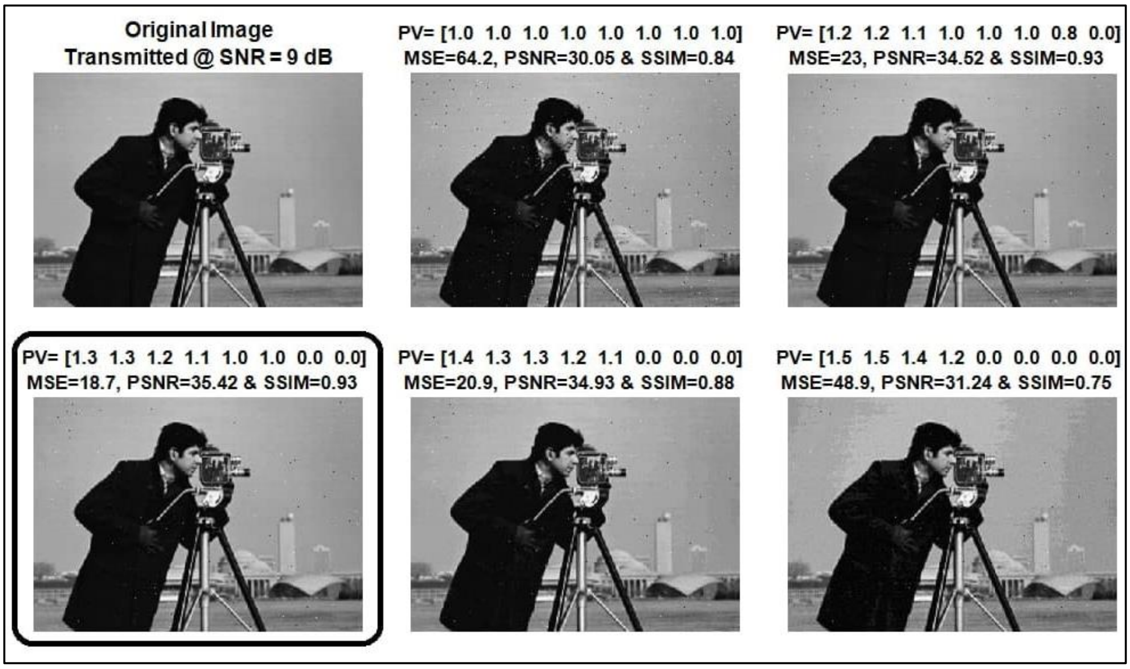
Original Image
Transmitted @ SNR = 9 dB
PV= [1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0]
MSE=64.2, PSNR=30.05 & SSIM=0.84
PV= [1.2 1.2 1.1 1.0 1.0 1.0 0.8 0.0]
MSE=23, PSNR=34.52 & SSIM=0.93
PV= [1.3 1.3 1.2 1.1 1.0 1.0 0.0 0.0]
MSE=18.7, PSNR=35.42 & SSIM=0.93
PV= [1.4 1.3 1.3 1.2 1.1 0.0 0.0 0.0]
MSE=20.9, PSNR=34.93 & SSIM=0.88
PV= [1.5 1.5 1.4 1.2 0.0 0.0 0.0 0.0]
MSE=48.9, PSNR=31.24 & SSIM=0.75

Figure 4-12: Multi–Unequal Error Protection distributions of DCSK at Beta = 5. Best Transmission Image at 3rd Power Vector at SNR = 9dB.

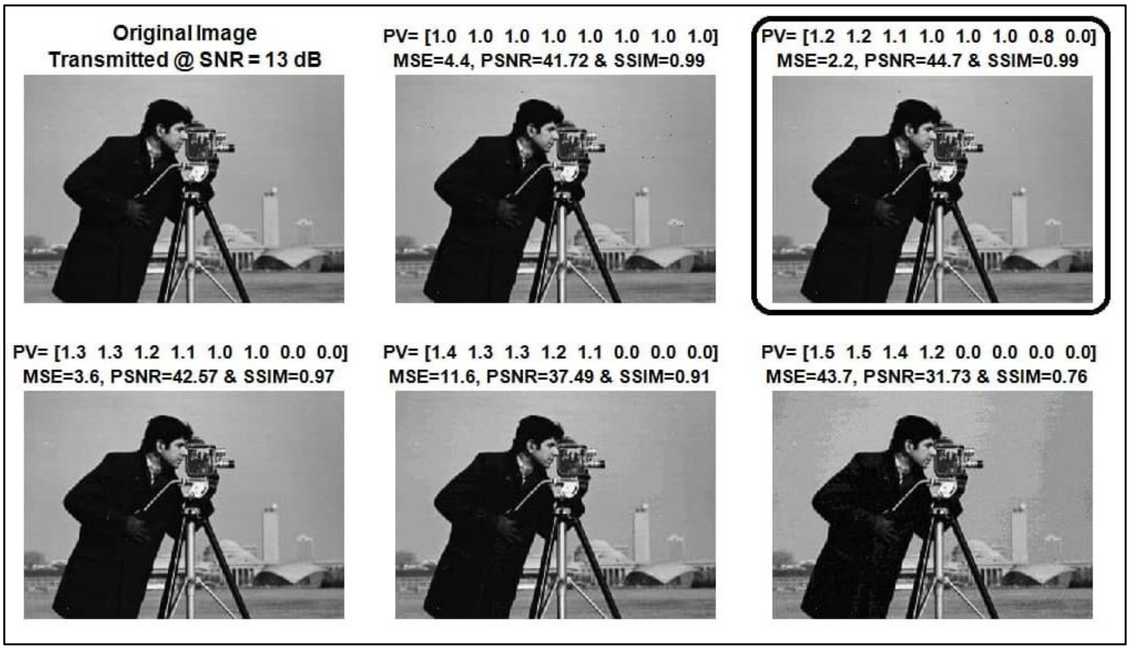
Original Image
Transmitted @ SNR = 13 dB
PV= [1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0]
MSE=4.4, PSNR=41.72 & SSIM=0.99
PV= [1.2 1.2 1.1 1.0 1.0 1.0 0.8 0.0]
MSE=2.2, PSNR=44.7 & SSIM=0.99
PV= [1.3 1.3 1.2 1.1 1.0 1.0 0.0 0.0]
MSE=3.6, PSNR=42.57 & SSIM=0.97
PV= [1.4 1.3 1.3 1.2 1.1 0.0 0.0 0.0]
MSE=11.6, PSNR=37.49 & SSIM=0.91
PV= [1.5 1.5 1.4 1.2 0.0 0.0 0.0 0.0]
MSE=43.7, PSNR=31.73 & SSIM=0.76

Figure 4-13: Multi–Unequal Error Protection distributions of DCSK at Beta = 5. Best Transmission Image at 2nd Power Vector at SNR = 13dB.

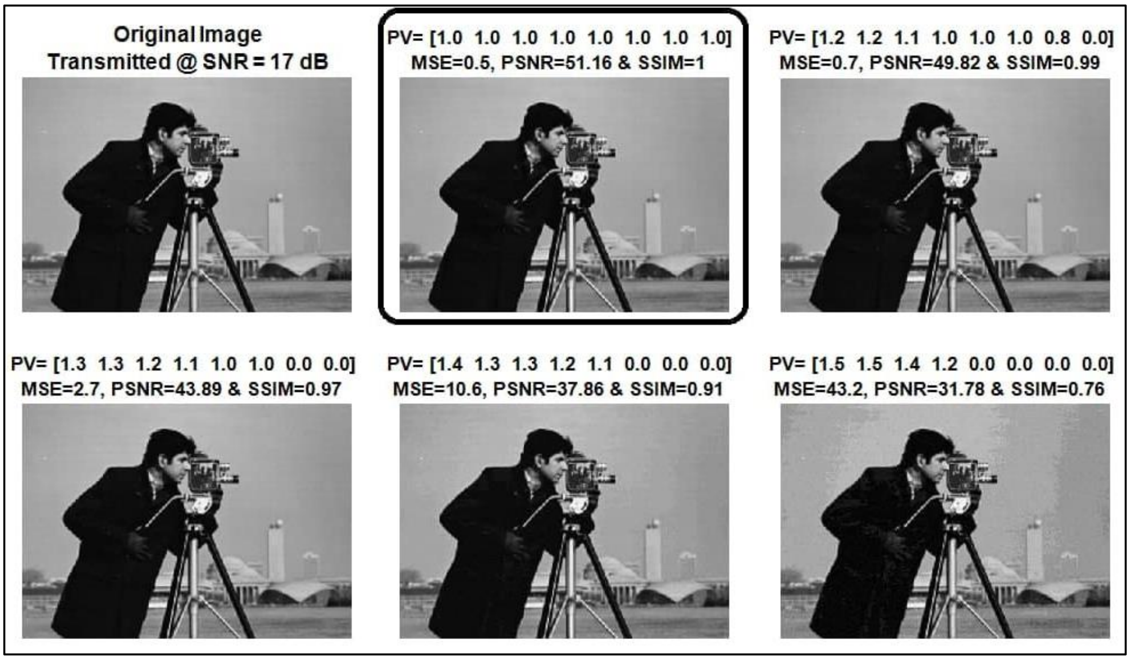
Original Image
Transmitted @ SNR = 17 dB
PV= [1.0 1.0 1.0 1.0 1.0 1.0 1.0 1.0]
MSE=0.5, PSNR=51.16 & SSIM=1
PV= [1.2 1.2 1.1 1.0 1.0 1.0 0.8 0.0]
MSE=0.7, PSNR=49.82 & SSIM=0.99
PV= [1.3 1.3 1.2 1.1 1.0 1.0 0.0 0.0]
MSE=2.7, PSNR=43.89 & SSIM=0.97
PV= [1.4 1.3 1.3 1.2 1.1 0.0 0.0 0.0]
MSE=10.6, PSNR=37.86 & SSIM=0.91
PV= [1.5 1.5 1.4 1.2 0.0 0.0 0.0 0.0]
MSE=43.2, PSNR=31.78 & SSIM=0.76

Figure 4-14: Multi–Unequal Error Protection distributions of DCSK at Beta = 5. Best Transmission Image in normal DCSK (equal power) at SNR = 17dB.

From figures (4-10) to (4-14), it is clear that the transmission with the proposed Unequal Error Protection method is very effective when the value of the SNR is low. The lower SNR value, the less important bits (LSBs) are sacrificed or neglected in favor of the more important bits (MSBs) in order to get a better transmission, as in Figures (4-10) and (4-11) and so on.

As the SNR is improving, the less significant bits are lessened until reach a stage where the SNR is high and sufficient without the need to neglect the less significant bits, and the traditional method becomes better when it is above 13dB and the beta value is 5.

Table (4-3) shows the amount of gain obtained as a result of using the proposed method.

$$MSE\ Gain\ = \frac{MSE(Normal\ DCSK) - MSE(Best\ Unequal\ Power)}{MSE(Normal\ DCSK)} \qquad (4.1)$$

$$PSNR\ Gain\ = \frac{PSNR(Best\ Unequal\ Power) - PSNR(Normal\ DCSK)}{PSNR(Normal\ DCSK)} \qquad (4.2)$$

$$SSIM\ Gain\ = \frac{SSIM(Best\ Unequal\ Power)-SSIM(Normal\ DCSK)}{SSIM(Normal\ DCSK)} \qquad (4.3)$$

Table 4-3: The gain obtained as a result of using the proposed method

SNR (dB)	Normal DCSK [1, 1, 1, 1, 1, 1, 1, 1]			Proposed Unequal Power Method			Gain (%100)		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM	MSE	PSNR	SSIM
5	841.7	18.88	0.27	**[2.4, 2.2, 1.9, 1.5, 0, 0, 0, 0]**			84.82	43.37	129.6
				127.7	27.07	0.62			
7	264.4	23.91	0.55	**[2, 1.8, 1.6, 1.4, 1.2, 0, 0, 0]**			82.03	31.2	49.09
				47.5	31.37	0.82			
9	63	30.14	0.85	**[1.7, 1.6, 1.4, 1.2, 1.1, 1, 0, 0]**			71.9	18.3	10.58
				17.7	35.66	0.93			
13	4.9	41.23	0.989	**[1.5,1.4,1.3,1.1,1,1,0.5,0.2]**			75.51	14.7	1.01
				1.2	47.29	0.999			
17	0.5	51.16	1	When SNR = 17 dB or more, the normal DCSK (equal power) became the best results from unequal power.					

Chapter Five

Conclusions and Future Work Suggestions

Chapter Five: Conclusions and Future Work Suggestions

5.1 Conclusions

5.1.1 Conclusions for Encryption Part

1. Rabinovich system has 4 initial conditions and 5 parameters, all these parameters are represented as keys in image encryption.
2. Used of more than one chaotic system for encryption increases the size of the number of keys (key space), although it does not significantly affect the increase in image distortion.
3. Rabinovich system is a kind of Chaotic Flow and therefore the change between one value and the next is minimal. Therefore, it is not possible to obtain great randomness except by sensation those few differences by multiplying the value of the chaotic system by a large number (such as 10^{12}) and then mod by small number (such as 256).
4. Theoretically, the key space in the Chaotic system is close to infinite, but in reality, it can be calculated with knowledge of the sensitivity, the rang for each initial conditions or parameters.
5. All four methods to generate random bits give good specifications rather for the balanced between zeros and ones at any given length.

5.1.2 Conclusions for Communication Part (DCSK)

1. When the value of the SNR is low, the less important bits (LSBs) are sacrificed or neglected in favor of the more important bits (MSBs)
2. Using UEP or unequal spreading factor when the SNR is low.
3. The Unequal Error Protection method is simple because does not need to be updated or modified on the receiver side in any distribution power.
4. When SNR more than 13 dB, the use of classical or equal power becomes better if the Beta = 5.

5.2 Suggestions for Future Work

1. Increasing the data rate to more than half by sending more than one bit from the same reference from the chaotic signal.
2. Hardware implementation for all or part of the system using FPGA or FPAA.
3. It was suggested to add channel coding to improve system performance.
4. It was suggested to add channel codding with the first, second and third bits of MSB, as they contain approximately 87.5% of the amount of data in all bits.

References

[1] Easttom, William. "Steganography." Modern Cryptography. Springer, Cham, 2021. 337-356.

[2] Blahut, Richard E. Cryptography and secure communication. Cambridge University Press, 2014.

[3] W. M. Hewlett, Modern Cryptography: Theory and Practice, Prentice Hall PTR, 2003.

[4] Stinson, Douglas R. "Classical cryptography." Cryptography, Theory and Practice (1995): 1-20.

[5] Xia, Yongxiang, Chi Kong Tse, and Francis Chung-Ming Lau. "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread." IEEE Transactions on Circuits and Systems II: Express Briefs 51.12 (2004): 680-684.

[6] Yu, Jin, and Yu-Dong Yao. "Detection performance of chaotic spreading LPI waveforms." IEEE transactions on wireless communications 4.2 (2005): 390-396.

[7] Lynnyk, Volodymyr, and Sergej Čelikovský. "On the anti–synchronization detection for the generalized Lorenz system and its applications to secure encryption." Kybernetika 46.1 (2010): 1-18.

[8] Cai, X., Xu, W., Wang, L., & Chen, G., “Towards high-data-rate noncoherent chaotic communication: A multiple-mode differential chaos shift keying system,” IEEE Transactions on Wireless Communications, , Vol. 20, Issue 8, pp.: 4888-4901, 2021.

[9] Pecora, L. M., and T. L. Carroll. "On the control and synchronization of chaos." Phys Rev Lett 64.7 (1990): 821-827.

[10] Kolumbán, Géza, and Michael Peter Kennedy. "Communications using chaos/spl Gt/MINUS. III. Performance bounds for correlation receivers." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 47.12 (2000): 1673-1683.

[11] H. Ma, Y. Fang, Y. Tao, P. Chen and Y. Li, "A Novel Differential Chaos Shift Keying Scheme with Transmit Diversity," in IEEE Communications Letters, vol. 26, no. 7, pp. 1668-1672, July 2022, doi: 10.1109/LCOMM.2022.3168151.

[12] Tse, C. K., and F. C. M. Lau. "Chaos-based digital communication systems." Operating Principles, Analysis Methods and Performance Evaluation (2003).

[13] Wang, Zheng, and K. T. Chau. Chaos in electric drive systems: analysis, control and application. John Wiley & Sons, 2011.

[14] Meador, Clyde-Emmanuel Estorninho. "Numerical calculation of Lyapunov exponents for three-dimensional systems of ordinary differential equations." (2011).

[15] Theodossiou, Efstratios, et al. "The notion of chaos: From the cosmogonical chaos of ancient greek philosophical thought to the chaos theory of modern physics." Facta universitatis-series: Philosophy, Sociology, Psychology and History 11.2 (2012): 211-221.

[16] Theodossiou, Efstratios, et al. "The notion of chaos: From the cosmogonical chaos of ancient greek philosophical thought to the chaos theory of modern physics." Facta universitatis-series: Philosophy, Sociology, Psychology and History 11.2 (2012): 211-221.

[17] Sardanyés i Cayuela, Josep. Dynamics, evolution and information in nonlinear dynamical systems of replicators. Universitat Pompeu Fabra, 2009.

[18] Kurian, Ajeesh P., and Sadasivan Puthusserypady. "Secure digital communication using chaotic symbolic dynamics." TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES 14.1 (2006): 195-207.

[19] Gao, Tiegang, and Zengqiang Chen. "A new image encryption algorithm based on hyper-chaos." Physics letters A 372.4 (2008): 394-400.

[20] Khanzadi, Himan, Mohammad Eshghi, and Shahram Etemadi Borujeni. "Image encryption using random bit sequence based on chaotic maps." Arabian Journal for Science and engineering 39.2 (2014): 1039-1047.

[21] Gorji, RB—Shirvani, and F. R. MH—Mooziraji. "A new image encryption method using chaotic map." Journal of Multidisciplinary Engineering Science and Technology (JMEST) 2.2 (2015): 251-256.

[22] Roohbakhsh, Danial, and Mahdi Yaghoobi. "Color image encryption using hyper chaos Chen." International Journal of Computer Applications 110.4 (2015).

[23] A. K. A. Hassan, "Proposed Hyperchaotic System for Image Encryption," (IJACSA) International Journal of Advanced Computer Science and Applications,, vol. 7, pp. 37-40, 2016.

[24] Cai, Xiangming, et al. "Design and performance analysis of differential chaos shift keying system with dual-index modulation." IEEE Access 7 (2019): 26867-26880.

[25] Sushchik, Mikhail, Lev S. Tsimring, and Alexander R. Volkovskii. "Performance analysis of correlation-based communication schemes utilizing

chaos." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 47.12 (2000): 1684-1691.

[26] Lawrance, Anthony J., and Gan Ohama. "Exact calculation of bit error rates in communication systems with chaotic modulation." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 50.11 (2003): 1391-1400.

[27] Kaddoum, Georges, Pascal Chargé, and Daniel Roviras. "A generalized methodology for bit-error-rate prediction in correlation-based communication schemes using chaos." IEEE Communications letters 13.8 (2009): 567-569.

[28] Long, Min, Yunfei Chen, and Fei Peng. "Simple and accurate analysis of BER performance for DCSK chaotic communication." IEEE Communications Letters 15.11 (2011): 1175-1177.

[29] Mahdi, Amina, Ameer K. Jawad, and Saad S. Hreshee. "Digital chaotic scrambling of voice based on duffing map." International Journal of Information and Communication Sciences 1.2 (2016): 16-21.

[30] A. K. Jawad, H. N. Abdullah, S. S. Hreshee, "Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals," Journal of American Science, Vol. 11, Issue 7, pp. 49-55, 2015

[31] Jovic, Branislav. Synchronization techniques for chaotic communication systems. Springer Science & Business Media, 2011.

[32] Skiadas, Christos H., and Ioannis Dimotikalis. Chaotic Systems: Theory and Applications. World Scientific, 2010.

[33] Hussein S. " Single Tone Direct Sequence Spread Signals Detection Based On Chaos Theory" M.Sc. Thesis, College of Engineering Al-Mustansiriya University, Department of Electrical Engineering, Iraq, Baghdad, January 2012.

[34] Gerald Teschl, “Ordinary Differential Equations and Dynamical Systems”, American Mathematical SocietyProvidence, Rhode Island, 2010.

[35] Chen, Shihua, et al. "Adaptive synchronization of uncertain Rössler hyperchaotic system based on parameter identification." Physics Letters A 321.1 (2004): 50-55.

[36] Edwardott “Chaos Dynamical Systems” CAMBRIDGE University, second edition, 2002

[37] He, Li-fang etal "A chaotic secure communication scheme based on logistic map." 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). Vol. 8. IEEE, 2010.

[38] Minai, Ali A, and Tirunelveli Anand. "Synchronizing multiple chaotic maps with a randomized scalar coupling." Physica D: Nonlinear Phenomena 125.3-4 (1999): 241-259.

[39] Mahdi, Amina, and Saad S. Hreshee. "Design and implementation of voice encryption system using XOR based on Hénon map." 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA). IEEE, 2016.

[40] Atheer M., "FBGA Based Image Encryption Using Chaotic System", Doctor Thesis in Electronic Engineering University of Technology, October 2016

[41] Al-Asady, Heba Abdul-Jaleel, Osama Qasim Jumah Al-Thahab, and Saad S. Hreshee. "Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper." Journal of Physics: Conference Series. Vol. 1818. No. 1. IOP Publishing, 2021.

[42] Samia, Rezzag. "Solution bounds of the hyper-chaotic Rabinovich system." Nonlinear studies 24.4 (2017).

[43] M. Moghtadaei and. M. H. Golpayegani, ―Complex Dynamic Behaviors of the Complex Lorenz System‖, Scientia Iranica, Vol. 19, PP. 733–738, (2012)

[44] S. H. Strogatz, "Nonlinear Dynamics and Chaos", Preseus Books Publishing, LLC, 1994

[45] K.T. CHAU, ZHENG WANG, "Chaos in Electric Drive Systems" , John wiley & soon, IEEE, 2011.

[46] W. R. Story, ―Application of Lyapunov Exponents to Strange Attractors and Intact & Damaged Ship Stability‖, M.Sc. Thesis, Blacksburg, Virginia Tech, (2009)

[47] A. Menezes, . P. van Oorschot and . S. Vanstone, Handbook of Applied Cryptography, CRC press, 1997.

[48] M. Matyas, M. Peyravian , A. Roginsky and . N. Zunic, "Reversible Data Mixing Procedure for Efficient Public-Key Encryption," Computer and Security , vol. 17, no. 3, p. 265–272, 1998.

[49] S. Chakraborty, A. Seal, M. Roy and K. Mali, "A Novel Lossless Image Encryption Method using DNA Substitution and Chaotic Logistic Map," International Journal of Security and Its Applications, vol. 10, pp. 205-216, 2016.

[50] Z. Liehuang, L. Wenzhuo, . L. Lejian and . L. Hon, "A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences," IJCSNS International Journal of Computer Science and Network Security, vol. 6, pp. 125-130, August 2006

[51] Itoh, Makoto, and Hiroyuki Murakami. "New communication systems via chaotic synchronizations and modulations." IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences 78.3 (1995): 285-290.

[52] Dedieu, Herve, Michael Peter Kennedy, and Martin Hasler. "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 40.10 (1993): 634-642.

[53] Kocarev, L. J., et al. "Experimental demonstration of secure communications via chaotic synchronization." International Journal of Bifurcation and Chaos 2.03 (1992): 709-713.

[54] Kennedy, Michael Peter, et al. "Performance evaluation of FM-DCSK modulation in multipath environments." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 47.12 (2000): 1702-1711.

[55] Kolumbán, Géza, Michael Peter Kennedy, and Leon O. Chua. "The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications." IEEE Transactions on circuits and systems I: Fundamental theory and applications 44.10 (1997): 927-936.

[56] Galias, Zbigniew, and Gian Mario Maggio. "Quadrature chaos-shift keying: theory and performance analysis." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48.12 (2001): 1510-1519.

[57] Parlitz, Ulrich, et al. "Transmission of digital signals by chaotic synchronization." International Journal of Bifurcation and Chaos 2.04 (1992): 973-977.

[58] Dedieu, Herve, Michael Peter Kennedy, and Martin Hasler. "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 40.10 (1993): 634-642.

[59] Kolumbán, Géza, et al. "Differential chaos shift keying: A robust coding for chaos communication." Proc. NDES. Vol. 96. 1996.

[60] O. M. Abu Zaid, N. A. El-Fishawy, E. M. Nigm and O. S. Faragallah, "A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security," International Journal of Computer Applications, vol. 61, pp. 29-39, 2013.

[61] J. Ahmad and F. Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes," International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS, vol. 12, pp. 18-31, 2012.

الملخص

توجد الكثير من العوامل التي يجب الاخذ بها في أنظمة الاتصالات، ولكن من اهم العوامل هما عاملان، الخصوصية والاتصال الكفوء.

في هذا البحث تم بناء نظام اتصالات يعتمد على الإشارات الفوضوية لتحقيق العوامل سالفة الذكر.

فيما يخص امنية البيانات: تم بناء منظومة تشفير تعتمد على النظام الفوضوي المركب (Hyper Chaos) وذلك بتوليد ارقام ثنائية عشوائية (٠،١) باستخدام ثلاث طرق مقترحة في البحث واجراء عملية XOR بين البتات العشوائية والبينات المراد تشفيرها بعد تحويلها الى الصيغة الثنائية (Binary form). وجيع الطرق الثلاث اثبتت كفاءتها من حيث المساواة بين احتمالية والاصفار والواحدات، وكذلك وتم تطبيق خوارزمية التشفير على عدة أنواع من الصورة (الرمادية والملونة).

اثبتت نتائج المحاكاة كفاءة منظومة التشفير من حيث حجم عدد المفاتيح فأنه (من الناحية النظرية يقترب حجم عدد المفاتيح من المالانهاية) ومن الناحية العملية يعتمد حجم عدد المفاتيح على مضروب ٩ معاملات (وبحالة خاصة في النظام المقترح ١٨ معامل) وكل واحد منهم مضروب $١٠^{١٦}$ (كما اثبت في الماتلاب) وبالتالي سنحصل على عدد مفاتيح كبير جدا يصعب حسابه بشكل دقيق. وكذلك الصورة المشفرة اعطت اقل من ٩ ديسي بيل وهذا يعني ان الصورة المشفرة مختفية الملامح بشكل تام وكذلك فان استرجاع الصورة في جهة المستلم فأن الصورة ترجع بشكل واضح تماما بقيمة لا نهائية ديسي بيل.

اما فيما يخص منظومة الاتصالات فتم بناء طريقة تضمين تسمى مفاتيح التحول الفوضوي التفاضلي DCSK (Differential Chaotic Shift Keying) وتم اقترح طريقة مبتكرة وهي الارسال بالقدرة الغير متساوية بين البتات (Unequal Error Protection Bits) عندما تكون SNR قليلة فيتم تحويل بعض من القدرة من البتات الأقل أهمية (LSBs) الى البتات الأكثر أهمية (MSBs). وأثبتت النتائج العملية الكفاءة العالية للطريقة المقترحة مقارنتاً بالطريقة التقليدية وذلك بمعدل ربح يزيد على ٧٢% بمعيار معدل الخطأ التربيعي (Mean Sequard Error - MSE).

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية الهندسة

قسم الهندسة الكهربائية

تصميم وتقييم اتصال آمن بناءً على نظام فوضوي

رسالة مقدمة الى قسم الهندسة الكهربائية في كلية الهندسة/جامعة بابل كجزء من متطلبات نيل درجة ماجستير علوم في الهندسة الكهربائية

(الكترونيك واتصالات)

من قِبل

هدى حسن هاتف

تحت اشراف

الأستاذ الدكتور سعد سفاح حسون

١٤٤٤ هـ

٢٠٢٢ م