Republic of Iraq
Ministry of Higher Education and Scientific Research
University Of Basrah
College of Computer Science and Information Technology

An Efficient Color Image Encryption Method Using DNA Sequence and Chaos Cipher

A Thesis

Submitted to the Council of the College of Computer Science and Information Technology / University of Basrah as a Partial Fulfillment of the Requirements for the Degree of M.Sc. in Computer Science in the field of Information Security

By
Ghofran Khaled Shraida
(B.Sc. Computer Science 2013)

Supervisor
Prof. Dr. Hameed Abdulkareem Younis

June 2022 A.D. Dhu Al Qa'dah 1443 H.

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ وَمَن يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ

إِنَّ اللَّهَ بَالِغُ أَمْرِهِ قَدْ جَعَلَ اللَّهُ لِكُلِّ شَيْءٍ قَدْرًا

صدق الله العلي العظيم

﴿ سورة الطلاق الاية (٣) ﴾

Supervisor's Recommendation

I certify that this thesis entitled "**An Efficient Color Image Encryption Method Using DNA Sequence and Chaos Cipher** " was made under my supervision at the Department of the College of Computer Science and Information Technology, University of Basrah, as a partial fulfillment of the requirements for the Degree of M.Sc. in Computer Science, in specific field of information security.

Signature:

Name: Prof. Dr. Hameed Abdulkareem Younis

Date:

Recommendation of Head of Dept.

In view of the available recommendations, I put forward this thesis for debate by an examine committee.

Signature:

Name: Asst. Prof. Dr. Zainab Najim Nameer

Date:

Acknowledgments

First of all, I would like to thank Almighty Allah the most merciful for all his blessings throughout my life, and for always being my strength and peace. I could not have achieved this much without the grace of Almighty Allah.

I thank the Deanship of the College of Computer Science and Information Technology represented by the Dean, Assist. Prof. Dr. Salma Abdel-Baqi Mahmoud, the Head of the Department, Assist. Prof. Dr. Zainab Najim Nameer, and the Postgraduate Rapporteur, Assist. Prof. Dr. Adalah Mahdi Jiyad.

I would like to express my sincere gratitude to all the instructors that have taught me more than just science, especially my supervisor Prof. Dr. Hameed Abdulkareem Younis, for his encouragement. He was always there whenever I found any problem. I appreciate his efforts, time, support, and guidance throughout my thesis and am proud to be a student of such a kind supervisor.

I am thankful to all of my family members for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my parents for their earnest prayers, unconditional love, and unflinching support in completing my Master degree. I would like deeply to thank my companion throughout the journey, my husband, for being a great role model and encouraging me throughout my studies; he helped, guided, and supported me in order to achieve my dream. Thanks to my brothers and my sisters who stood with me all my life.

I would like to thank my best friend for motivating me during my degree program.

Ghofran Khaled Shraida

Researcher

Contents

List of Abbreviations

Abbreviation	Definition
2D-RT	Two Dimensions Rectangular Transform
A	Adenine
AES	Advanced Encryption Standard
C	Cytosine
CML	Coupled Map Lattice
CRC32	Cyclic Redundancy Check 32
DES	Data Encryption Standard
DNA	Deoxyribonucleic Acid
DLFSR	Dynamic Linear Feedback Shift Register
DSA	Digital Signature Algorithm
ECC	Elliptic-Curve Cryptography
G	Guanine
MD4	Message-Digest 4
MSE	Mean Square Error
NCA	Nonlinear Chaotic Algorithm
NCBI	National Center for Biotechnology Information
NPCR	Number of Pixel Change Rate
PKC	Public Key Cryptography
PSNR	Peak Signal-to-Noise Ratio
PWLCM	Piecewise Linear Chaotic Map
RC4	Rivest Cipher 4
RSA	Rivest Shamir Adleman

SHA	Secure Hash Algorithm
S-Box	Substitution Box
SKC	Secret Key Cryptography
SEAL	Software-Optimized Encryption Algorithm
T	Thymine
TD-ERCS	Tangent-Delay Ellipse Reflecting the Cavity-map System
UACI	Unified Average Cipher Intensity
XOR	exclusive-OR

List of Figures

List of Tables

Abstract

The color image is the core of multimedia content; it has become an important element in information transmission. Images are being shared and distributed in various fields public uses them for bank transactions or business communications, the government uses them to share secret confidential data, and in the medical field, it is used to account for patients reports. All these require user authentication, reliability and accuracy of data and encryption techniques are valuable tools to provide that needed security. Recently, the encryption technique for color images using the chaotic system and DNA bases has drawn much attention from the research community.

The size of an image file is large, this means that encryption of digital images requires large amounts of computation. Traditional encryption techniques, like, Data Encryption Standard, and Advanced Encryption Standard are not only inefficient, but also less secure. Due to characteristics of chaos theory, such as periodicity, sensitivity to initial conditions and control parameters, and unpredictability. Hence, characteristics of DNA, such as, vast parallelism and large storage capacity making it a very promising field. The algorithms based on DNA and chaotic functions use the advantages of both fields to provide image protection in an effectively.

This thesis presents an efficient color image encryption algorithm through Lorenz hyper-chaotic system along with Rossler hyper-chaotic system and DNA cryptography. The proposed algorithm consists of three steps: Firstly, initial conditions for Lorenz hyper-chaotic system and Rossler hyper-chaotic system are set depending on the hash value of Secure Hashing Algorithm-256/384, which is generated from a plain image to avoid chosen plaintext attacks. Secondly, Lorenz hyper-chaotic system generates chaotic sequences that transform the plain color image into a confusing image. These sequences

are used to create a confusion key to scramble the three components (red, green, and blue) of a color image. Finally, a combination of following approaches is used to encrypt the scrambled components: the scrambled components and Rossler hyper-chaotic system-based key are encoded to DNA bases. Addition operations are applied between the components chaotically. XOR operations are applied between the DNA components of the image and DNA sequences that are generated based on the Rossler hyper-chaotic system. Then, decode the DNA components of the image; thus, the final encrypted image is generated.

The simulation results indicate that the suggested encryption algorithm is able to satisfy the requirements of security. Confusion and diffusion have yielded a value of entropy is 7.997 bits and the key space is 2^{200}, the correlation coefficient is nearly zero. The efficacy of the proposed method has been verified through numerous evaluations, and the results show that it is resistant and effective against attacks like statistical and brute-force attacks. Furthermore, the algorithm devised is more efficient when compared with some previous color image encryption algorithms that used chaotic maps with DNA coding.

Chapter One

General Introduction

1.1 Introduction

The exchanging information is considered an asset and it people tend to keep it safe from attacks of various types [1]. This means that only those authorized should have access to the information. To keep information safe, it must be hidden from unauthorized people. Internet networks have become an essential part of information storage, as well as, its transfer from one part of the world to another. Most of the information transferred is through Internet networks. Information could consist of, for example, text, audio, image, or video. A basic requirement of any information transfer is to keep it confidential and integral [2]. Information can be hacked at any point of transfer between the source and the destination. Internet networks face different types of information threats [3].

Images are employed in a variety of applications nowadays. In addition, many applications, such as, medical imaging systems, pay-tv, confidential video conferences, military image communications, and others, require specific and trustworthy security in the storing and transmission of digital images. Many image encryption algorithms have been proposed in order to accomplish these goals. In the field of information securing, image encryption plays a major role. The methods and algorithms for securing or encrypting images span from basic spatial domain procedures to more advance and a trustworthy frequency domain by changing the values and the positions of the pixels of the image. A technique for encrypting images consists of changing the image to a less recognizable one [4]. Then again, from an encrypted image, image decryption recovers the original image.

1.2 Overview for Materials

New technologies facilitate the generation, transmission, exchanging, and storage of large images also the need for digital rights protection becomes more urgent. In particular, the Internet provides a public network that allows illegal distribution of images much more easily.

During transmission over the global network, digital images are subject to security attacks. Therefore, information security of the digital image has become a burning research issue. There is a need to develop reliable encryption schemes to fulfill the ever-increasing security need of the increasing data of communication system. In this thesis, a multi-type chaotic map along with a DNA encoding technique has been suggested an efficient color image encryption method.

1.2.1 Chaotic Map

The study of chaos proved a better encryption technology for providing security to sensitive data that uses non-periodic signals generated by chaotic systems for encryption. A chaotic system is a nonlinear deterministic system. Chaotic maps generate chaotic pseudo-random sequences. Their constructions are incredibly complex, making analysis and predictions challenging. An uncorrelated sequence results from a minor change in the initial condition [5]. Thus, the use of chaotic systems can thereby improve the security of cryptosystems. Permutation and diffusion are the two phases of cryptography techniques based on chaotic maps [6]. During the permutation phase, chaotic sequences or matrix transformations are used to modify the positions of the pixels. Although, this permutation approach improves encryption, it is unable to change the pixel value. Because pixels are not modified, the encrypted image's histogram and the original image's histogram are identical. As a result, statistical analysis could threat its security. During the diffusion phase, chaotic sequences modify the pixel values of the plain image. In comparison to

permutation, diffusion may provide more security. As a result, several researchers have coupled permutation and diffusion to increase the level of secrecy [7]–[10]. Thus, the use of discrete chaotic maps not only helps to build a good encryption system, also, makes to obtain a good candidate for efficiency. To ensure the security of digital image information, the effective protective measure is image encryption.

1.2.2 DNA Technology

A new field quickly advancing in international researches on cryptography is using DNA to achieve better and more efficient image encryption [11]–[14]. Cryptography and molecular biology may seem incomplete, but it was discovered that these two disciplines could work together more closely. Adleman developed the field of DNA computing in 1994 [15]. Information security can be achieved via DNA cryptography and information science [16].

DNA has great advantages in dealing with large storage capacity, parallelism, and less power requirement for DNA computation [17]. DNA computing essentially uses biochemical experiments to address practical problems. However, because of the limitations of biochemical reaction conditions, such as expensive experimental equipment, environmental requirements, difficulty in extracting DNA sequence, and difficulties in controlling the concentration, temperature, and PH of the reactant, studying DNA computing is difficult. Regarding image encryption in DNA computing, researchers ignore the complex experimental links of DNA, only use DNA coding to carry image information, and design a reasonable and effective encryption algorithm.

1.3 Problem Statement and Motivations

The size of an image file is larger than other digital data like text and audio [18]. This means that encryption of digital images requires large amounts of computation; hence the need to devise special algorithms to handle this type of data. In theory, traditional encryption techniques, like, Data Encryption Standard (DES) [19], and Advanced Encryption Standard (AES) [20] are good. But most traditional encryption is developed for text data without considering the unique characteristics of image files [21]. Compared to the encryption of traditional alphanumeric data files, the encryption of images files has encountered several new challenges due to their unique characteristics, such as, the size of the images is often substantially larger than that of the text data. As a result, the encryption algorithm that encrypts the image demands a very large amount of computation. This means that the above techniques are not only inefficient, but also less secure [22]. Chaotic maps and Deoxyribonucleic Acid (DNA) technology are the two most popular topics currently used in image encryption, combined or separately. These two technologies have good security features and can be used in digital image security [23].

Chaotic systems' sensitive initial conditions, unexpected, nonperiodic, perfect statistics, and other attributes [24]–[26] enable them to construct secure cryptosystems. Many useful properties of DNA computing have been discovered [11]: high-scale computational parallelism, minimal energy loss, and a significant amount of storage space. From this point of view, the proposed encryption algorithm combines DNA coding and hyper-chaotic systems.

1.4 Literature Review

In the literature review, a great deal of studies have improved color images security. Some of the suitable methods are listed in this section.

P. Liu *et al.* [9] proposed a new color image encryption algorithm using logistic maps, spatial maps, and DNA coding. Logistic maps utilized to scramble pixels, spatial maps used to replace pixels, DNA coding, and XOR operations employed to increase the complexity of the algorithm in the suggested encryption method. This algorithm has a large key space, but the ability to resist entropy attacks and statistical attacks needs to be improved.

N. Iqbal *et al.* [27] suggested an image encryption algorithm combines chaos theory, the chess piece Castle, and DNA computing. The random numbers sequences for the mechanisms of confusion and diffusion provided via a chaotic map. The pixels from the input image confused by Castle's random movement on the imagined big checkerboard. Two sequences of random numbers and a shuffled image turned into DNA strands, then, DNA operations performed to achieve the diffusion effects. The scheme has a short processing time, but the key sensitivity and correlation between the pixels need to be improved.

X. Wu *et al.* [28] presented a new robust and lossless color image encryption algorithm based on DNA sequence operation and one-way coupled-map lattices (OCML). The plain-image was firstly decomposed into three gray-level components and were converted into three DNA matrices. Then the XOR operation was performed on the DNA matrices for two times. Next, the shuffled DNA matrices were transformed into three gray images according to the DNA decoding rules. This algorithm can effectively resist cropping and noise attacks. However, the ability of ciphertext images to resist information entropy needs to be improved.

X. Wu *et al.* [29] used Coupled Map Lattice (CML) based on the Nonlinear Chaotic Algorithm (NCA) map to present a new DNA-based color image encryption technique. The secret keys employed for updating the spatiotemporal chaotic system's parameters and initial settings. Hence, the secret keys are important in the key streams created by CML based on the NCA map. To scramble the DNA matrices, a DNA-level shuffling procedure used. This algorithm has the ability to resist differential attacks, but the ability to resist information entropy is poor.

X.-Y. Wang *et al.* [30] demonstrated a color image encryption technique. They separate the color image into three grey images (R, G, and B) and convert the images into binary matrices, and then obtain three DNA matrices by using the third DNA coding rule. Then, the DNA matrices scrambled via the chaotic sequences that generated from Lorenz chaotic system. The obtained matrices exchanged into rows matrices. By performing the fourth DNA coding rule, the encrypted image was obtained. The ability to resist the information entropy of this algorithm is good, but the ability to resist differential attacks needs to be improved.

H. R. Shakir [31] suggested a novel image encryption technique combining the Tangent-Delay Ellipse Reflecting the Cavity-map System (TD-ERCS), and DNA-sequence operations. The TD-ERCS system permuted the image pixels' locations, while DNA-sequence XOR operations diffused the plain image's pixel values. Based on results from experiments and security research, the algorithm encryption's efficiency shown to be good, but the key sensitivity needs to be improved.

H. R. Amani and M. Yaghoobi [32] developed a new adaptive encryption technique for RGB images by using hyper-chaotic with DNA sequence operations. The mapping of the Arnold cat and the image pixels' gray value

modified using a mix of three techniques: the adaptive approach, the DNA sequence, and the Chen hyper-chaotic system. The more these three strategies were combined, the more complex the algorithm becomes. This algorithm has a large key space, but the ability to resist entropy attacks and differential attacks needs to be improved.

Q. Liu and L. Liu [11] suggested a color image encryption technique using double-chaos system, bit-level DNA coding and DNA operations. The Arnold method used to shuffle the components of the plain image for this approach. Then, for the diffusion of three scrambled component sets, three sets of chaotic sequences constructed using the modified double chaos system, which consisted of Rossler hyper-chaotic mapping and Lorenz chaotic mapping using varying parameters. Then, the three image groupings diffused using DNA coding and computing, and the three factions of cipher components merged to create the final encrypted image. This algorithm is simple to implement and has large key space, but the ability to resist information entropy and differential attack needs to be improved.

H. G. Mohamed *et al.* [14] introduced a new encryption for verifying image transmission across information correspondence frameworks. With chaotic confusion procedures and the mtDNA diffusion process, they are indistinguishable, reducing equipment complexity and improving framework security. To divide each component of RGB images into n-clusters, color image encryption employed a chaotic map, then; global scrambling throughout the entire image was applied. Finally, applied intra-pixel scrambling in each cluster, resulting in very disordered pixels in the encrypted image. Then, it employed the rationale of the mtDNA to diffuse the formerly scrambled pixel values. This algorithm can effectively resist information entropy attacks. However, the ability of encrypted images to resist differential attacks needs to be improved.

T. S. Ali and R. Ali [33] introduced a new color image encryption technique. To construct a permutation vector, this approach initially used a chaotic map. This vector permutes the pixels of a plain image. After that, a chaotic map was utilized to create a Substitution Box (S-Box), which then used for substitution. After using the S-Box, the features of confusion and diffusion could be noticed. Finally, the chaotic map was used to generate a random sequence, and each pixel value was bitwise XORed with the resulting sequence. The horizontal, vertical, and diagonal relationships between close pixels have all changed significantly duo to this kind of pixel mixing, but the encryption efficiency is low and the ability to resist information entropy is poor.

1.5 The Aim of the Work

The aim of the proposed technique is to maintain a high level of robustness against cryptographic attacks. The robustness is the property that characterizes how effective the proposed algorithm is against attacks, such as, cipher text only, known plaintext, chosen cipher-text and chosen plaintext attacks.

To prove security of the proposed algorithm, differential and statistical analyses have been applied using various tools. For statistical analysis, histogram, key space, key sensitivity, information entropy, and correlations are measured for plain and encrypted images. The Mean Square Error (MSE) and the Peak Signal-to-Noise Ratio (PSNR) are calculated. For differential analysis, two proposed tests called *Number of Pixel Change Rate (NPCR) and Unified Average Cipher Intensity (UACI)* are applied. The proposed algorithm considered robust against cryptographic attacks if it passes these tests successfully.

1.6 Contributions of Thesis

The existing color image encryption algorithms mainly have the following defects through the above literature analysis: The encryption algorithm based on DNA diffusion has a single calculation method, which complexity and security are low. There is no disturb the correlation between the three channels RGB of a color image, which is vulnerable to statistical attacks. The encryption algorithm has defects in resisting conventional attacks and security is not high. In order to solve the above problems, a color image encryption algorithm combining image hashing, 4D hyperchaotic systems and dynamic DNA addition operations is proposed. The major contributions of this thesis are:

- Secure Hash Algorithm-256 (SHA-256) hash of the plain image is used to generate secret keys. As long as the original image has a slight change in one bit of pixel value, SHA-256 hash value will make a huge difference. This increase the sensitivity of the key to resist the chosen plaintext attack, also facilitate the detection and analysis of image tamper location.
- Each pixel in each channel is scrambled into a new position chaotically. The proposed algorithm uses a hyper-chaotic system to scramble each pixel. This scrambling is repeated four times using sequences generated from 4D Lorenz hyper-chaotic system.
- The proposed algorithm has used DNA operation methods by exploiting the excellent characteristics of the hyper-chaotic system such as randomness to determine the DNA operation methods randomly.

1.7 Outline of the Thesis

The arrangement of this thesis is as follows: Chapter One discusses the introduction, problem statement and motivations, overview, literature review, contributions, and aim to design a new cryptographic algorithm. Chapter Two presents basics of cryptography, the preliminaries, materials, and metrics. Chapter Three discusses a proposed method of using chaotic systems and DNA encoding rules. In Chapter Four, the results were acquired by employing conventional metrics and are quantitatively and qualitatively compared to previous algorithms. Finally, Chapter Five contains conclusions that are drawn based on the results of the image encryption method, as well as, future works.

Chapter Two

Theoretical Background

2.1 Introduction

Encryption is a method used for encoding a message, image or important information in specific method that allow only parties who have the authorization to access, and prevent the unauthorized parties from access [34]. It is generally maintaining the information confidentiality by using different algorithms that have capability for converting the information into unrecognized codes. In fact, encryption does not prevent the interference, but makes intelligible content in unreadable content. Therefore, unauthorized cannot understand the encrypted information because it appears like a mixture of symbols, numbers and unintelligible characters.

In encryption algorithm, the plain image is encrypted by algorithm steps in order to generate a ciphered image that is not be able to read only if decrypted. Technically, encryption schemes mainly employed a cryptography key that generated in a way, which it is hardly to be discovered. An authorized can easily decode the image by using the key that provided by the sender to authorized receiver and this operation called *decryption*. Five ingredients are usually used in encryption scheme [35].

1- **Plain image:** the plain image is considered original image that is entered to the scheme as input.

2- **Encryption algorithm:** the encryption scheme can perform different types of substitutions on the plain image depending on the secret keys.

3- **Secret keys:** the keys are treated as inputs for encryption algorithm. All the steps of substitution, permutation and transformation mainly depending on particular keys.

4- **Cipher image:** cipher image is considered as output of the algorithm. It mainly depends on the input image and the secret keys. For using various keys in algorithm, two various cipher image will be produced.

5- **Decryption algorithm:** decryption algorithm is usually processed as encryption algorithm but reverse way. It depends on the cipher image and the secret keys to be able to recover the plain image.

2.2 The Goal of Cryptography

Cryptography is able to provide a number of security aims in order to ensure data privacy. Because the advantages of security for cryptography, the cryptography has many applications today [36]. The goals of cryptography can be summarized as follow [37]:

1- **Confidentiality:** The transmitted data in the computer has to be accessible only to the authorized party and not accessible to unauthorized parties.

2- **Authentication:** For received information of any system, the identity for the transmitter should be checked in order to prove that the receiving information came from an authorized person.

3- **Integrity:** The authorized parties can allow making modifications to the transmitted information and it is prohibited to make modifications for other parties between the transmitter and receiver.

4- **Non-Repudiation:** The receiver and the transmitter have not to be capable to deny the sending.

5- **Access Control:** For given information, only the authorized parties are capable to access

2.3 Classification of Cryptography

Encryption techniques are used in order to ensure security when confidential information is exchanged through communication line. The encryption technique can be classified depend on large number standard methods such as classical and modern [38].

2.3.1 Classical Cryptography

The types of classical cryptography can be classified into two main types: Substitution and Transposition [39].

2.3.1.1 Substitution Cipher

Substitution is sorted into two main types [39]. The first type is the monoalphabetic cipher and when refers to a substitute cipher using a simple key. An example of a monoalphabetic is Caesar cipher. Polyalphabetic cipher is the second type of Substitution cryptography. It indicates substitute cipher alphabet that its plain seems not similar from place to another place during the process of encryption. Vigenere cipher is example of the polyalphabetic.

2.3.1.2 Transposition Cipher

Transposition cipher is a mechanism for encryption. It uses units of plain text to occupy the position. And these units can be shifted depending on system of plain text permutation that is accordingly constituted [40]. Transposition cipher has two main types of transportation: Keyless transposition and Keyed transposition. In keyless cipher, the characters are shuffled by means of implementing the plain text in specified way which it varies from the reading way. The example of keyless transportation is the rail fence cipher. In keyed transposition, the method is different in which the plain text is divided into blocks that predetermined in size. By using a key in each block, the block characters are permuted. The Columnar is an example for keyed transposition.

2.3.2 Modern Cryptography

Modern cryptography is classified according to strongly scientific methods in which the computational of encryption algorithms are produced in a sequence that supposed to be difficult to be broken. In order to designed unbreakable system, the system should be resisted to the all type of attacks. In general, information should be theoretically secure and is not provably able to be broken. Modern cryptography can be categorized in to two categories: symmetric key cryptography and asymmetric key cryptography [41].

2.3.2.1 Symmetric Key Cryptography

The vital rule in symmetric algorithms is privacy, so the key that used in encryption and decryption should be unknown to unauthorized parties. Therefore, only the authorized parties should know the secret key. It is obvious that the characterizations of symmetric key algorithms do not need to consume high computing power. DES and BLOWFISH is considering as an example for symmetric cryptography. Generally, there are two types of symmetric key: stream ciphers or block ciphers [42].

A. Stream Cipher

The stream cipher is operated in single bit or byte and the encryption process is individually applied to bits at same time [43]. This process is basically achieved when a single bit from the secret key is added to the original text. It is mentioned that the stream cipher cryptography can be classified into two types of cipher that recognized as synchronous stream and asynchronous stream cipher. In synchronous stream cipher, the encryption system is mainly depending on key. In asynchronous stream cipher, where the key is significantly depending on cipher text. Rivest Cipher 4 (RC4), Quad, and Software-Optimized Encryption Algorithm (SEAL) are a few examples of the stream ciphers.

B. Block Cipher

The ability of characteristics of block cipher allow the plaintext bits to be encrypted in both single and complete block simultaneous. By employing same key. It is obvious that all bits in plaintext of same block will depend one another during the process of encryption [44]. From the practice, the major length of block ciphers is either 128 bits (16 bytes) like AES, or 64 bits (8 bytes) like DES and 3DES. Furthermore, there are several algorithms exploited the block cipher approach. Twofish, Blowfish, RC2, RC5, Camellia, are some examples of the block ciphers.

2.3.2.2 Asymmetric Key Cryptography

In asymmetric key cryptography, various keys are used in the encryption and the decryption process. These keys are called *Public Key Cryptography* (PKC) [45]. Generally, public key used for encryption process and private key is employed for decryption process. The asymmetric key cryptography trusts mathematical functions which are simply to calculate in the encryption process but they are hardly to calculate in the decryption process. The disadvantages of PKC is the time required to whole process is high as compared with symmetric key cryptography [46]. Several algorithms used asymmetric key cryptography such as Elliptic-Curve Cryptography (ECC), Rivest Shamir Algorithm (RSA), and Digital Signature Algorithm (DSA).

2.4 Chaos Theory

The term chaos has no standard definition but it can be defined by observing, the phenomenon in nature. Chaos or randomness and order are opposites and interrelated with order. Current chaos theory is used to predict future behavior. Its use in daily life is increasing. Chaos theory is the study of complex, nonlinear and dynamic systems [47]. It is a branch of mathematics that deals with systems that appear to be orderly (deterministic) but, in fact,

harbor chaotic behaviors. It also deals with systems that appear to be chaotic, but in fact, have an underlying order. Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions, an effect which is popularly referred to as the *butterfly effect* [48].

Chaos is the science of surprises, of the nonlinear and the unpredictable. It teaches us to expect the unexpected. Chaos theory deals with the nonlinear things that are effectively impossible to predict or control, such as turbulence, weather, the stock market, our brain states and so on [49], while most traditional science deals with supposedly predictable phenomena like gravity, electricity and chemical reactions. Many natural objects exhibit fractal properties, including landscapes, clouds, trees, organs and rivers. Many of the systems exhibit complex, chaotic behavior. Recognizing the chaotic, fractal nature of our world can give us new insight, power and wisdom.

In other words, chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions and a response popularly referred to as the butterfly effect. Small differences in initial conditions, result in widely different out-comes for such dynamical systems, generally rendering long term prediction impossible. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. The deterministic nature of any system does not make them predictable. This behavior is known as *deterministic chaos* or simply *chaos*. This theory was summarized by Edward Lorenz [50].

The most important properties of chaos are following [51]. **The Butterfly Effect**: This effect shows that a small change in the initial conditions lead to drastic changes in the results. **Unpredictability**: Chaos theory shows unpredictability due to sensitivity to initial conditions. **Order/Disorder**: Chaos theory is not disorder. It explores the transitions between order and disorder,

which may occur differently. **Feedback**: Chaos theory shows feedback-response behavior. The next value is calculated using the last output as in the case of Lorenz equation.

2.5 Chaotic Maps

2.5.1 Lorenz Chaotic System

Lorenz chaotic system is a typical 3D chaotic system discovered by meteorologist E.N. Lorenz in his study of convection phenomena. Compared with low-dimensional chaotic mapping, Lorenz chaotic mapping has a more complex structure, the sequence is more random, and the key space is greatly increased. Lorenz chaotic mapping is defined as follows [50]:

$$\begin{cases} \hat{X} = a\,(Y - X) \\ \hat{Y} = cX - Y - XZ \\ \hat{Z} = XY - bZ \end{cases} \quad (2.1),$$

where X, Y, and Z are the initial conditions and a, b, and c are the control parameters. The Lorenz chaotic system is in a state of chaos when a = 10, b = 8/3, and c = 28. Figure (2.1) depicts the attractor of the Lorenz chaotic system.

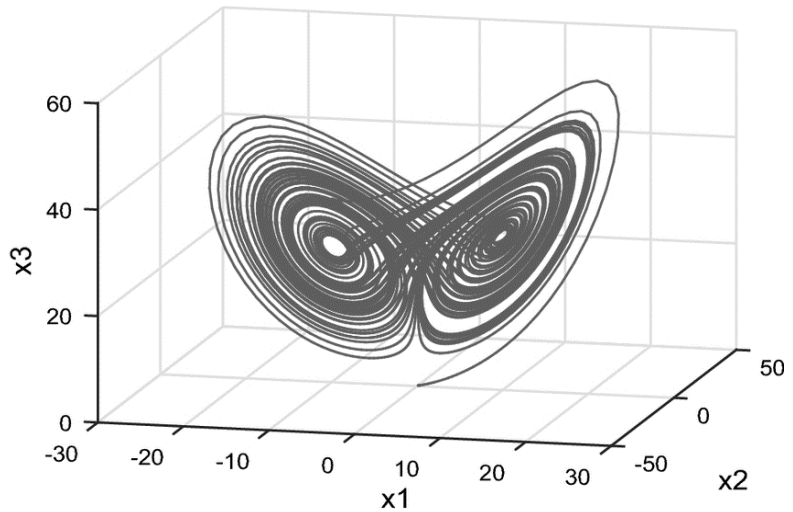


Figure (2.1): Lorenz chaotic system [52].

2.5.2 Lorenz Hyper-chaotic System

Because the chaotic sequence formed by the Lorenz hyper-chaotic system [53] has greater unpredictability and randomness, the encryption technique described in this thesis uses it to encrypt the image. By adding a nonlinear controller W to Lorenz system , the result is a new system:

$$\begin{cases} \hat{X} = a(Y - X) + W \\ \hat{Y} = cX - Y - XZ \\ \hat{Z} = XY - bZ \\ \hat{W} = -YZ + rW \end{cases} \quad (2.2),$$

where X, Y, Z, and W are the system's state variables. The system's control parameters are a, b, c, and r. The system Equation (2.2) achieves a hyper-chaotic mode when a = 10, b= 8/3, c = 28, and r is in the range (-1.52, -0.06]. To solve the system Equation (2.2), the fourth-order Runge–Kutta method is utilized [11].

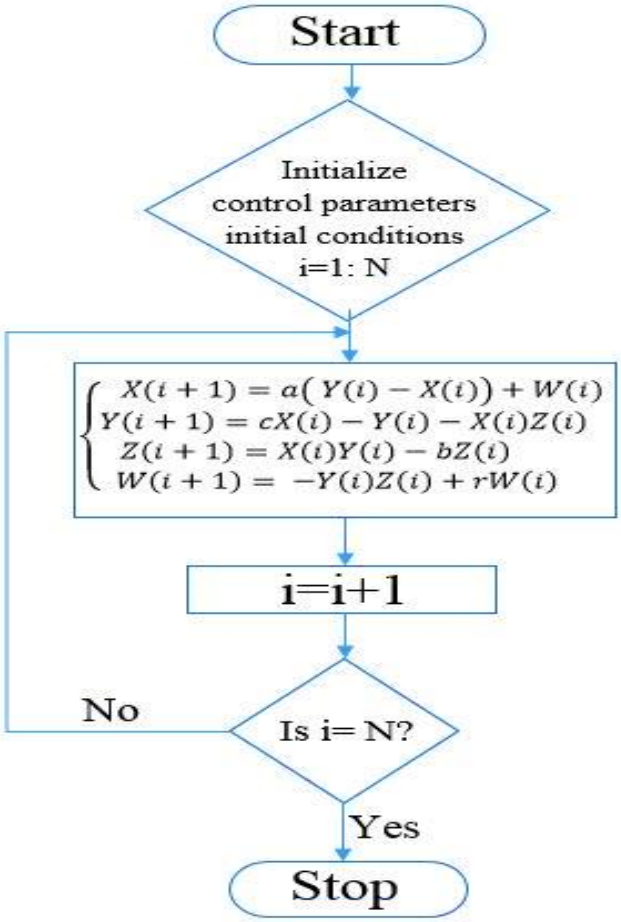


Figure (2.2): Flowchart of creation four sequences of Lorenz hyper-chaotic system.

For the initial variables (X_1, Y_1, Z_1, W_1), the four-dimensional hyper-chaotic sequence {X_i, Y_i, Z_i, W_i| i = 1, 2, 3, 4, . . ., N} can be obtained. Figure (2.2) shows the flowchart of calculating the four sequences of Lorenz hyper-chaotic system. When r = -1, the projection of the attractor of system Equation (2.2) on each plane is shown in the Figure (2.3).

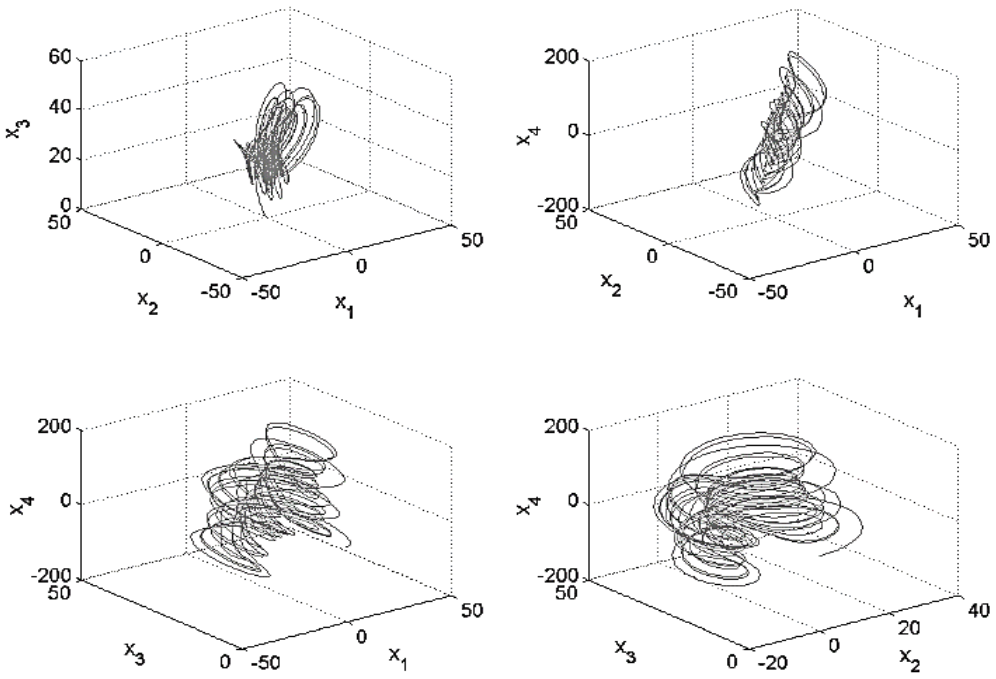


Figure (2.3): Lorenz hyper-chaotic system.

2.5.3 Rossler Chaotic System

The Rossler system is a three-dimensional chaotic system with one nonlinear term introduced by Otto Rossler in 1976 [54]. Chaos dynamics refers to the dynamical behavior of nonlinear systems that have specific specified properties with regard to time and starting circumstances. The Rossler chaotic system is calculated from the following equation:

$$\begin{cases} \hat{A} = -B - C \\ \hat{B} = A + \alpha B \\ \hat{C} = \beta + AC - \gamma C \end{cases} \quad (2.3),$$

where α, β, and γ are system parameters. When these parameters set to (α = 0.2, β = 0.2, and γ = 5.7), Rossler chaotic system is in a chaotic state. The attractor of Rossler chaotic system is shown in the Figure (2.4).

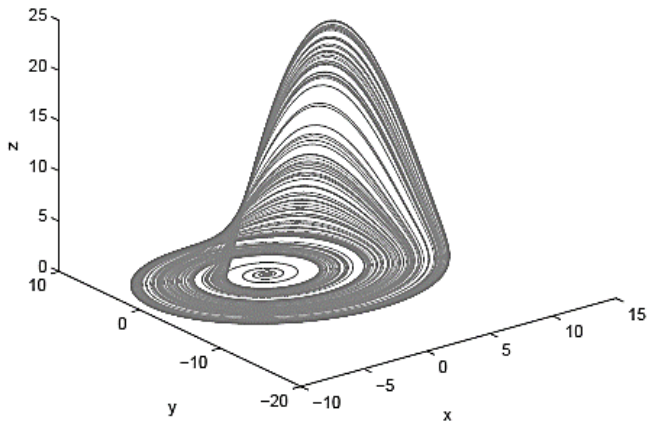


Figure (2.4): Rossler chaotic system.

2.5.4 Rossler Hyper-Chaotic System

The Rossler hyper-chaotic system [55] is a dynamic nonlinear system. It has the features of unpredictability, sensitivity to control parameters and initial conditions. Because these properties are congruent with cryptographic research, the technique is commonly utilized in image encryption [56]. The Equation (2.4) describing a Rossler hyper-chaotic system is provided below:

$$\begin{cases} \hat{A} = -B - C \\ \hat{B} = A + \alpha B + D \\ \hat{C} = \beta + CA \\ \hat{D} = \gamma D - \delta C \end{cases} \quad (2.4),$$

where (A, B, C, and D), are the state variables, and (α, β, γ, and δ), are the control parameters. When (α = 0.25, β = 3, γ = 0.05, and δ = 0.5), the above system is in a hyper-chaotic state. Figure (2.5) shows the flowchart of calculating the four sequences of Rossler hyper-chaotic system. The phase diagrams of the six planes are shown in the Figure (2.6).

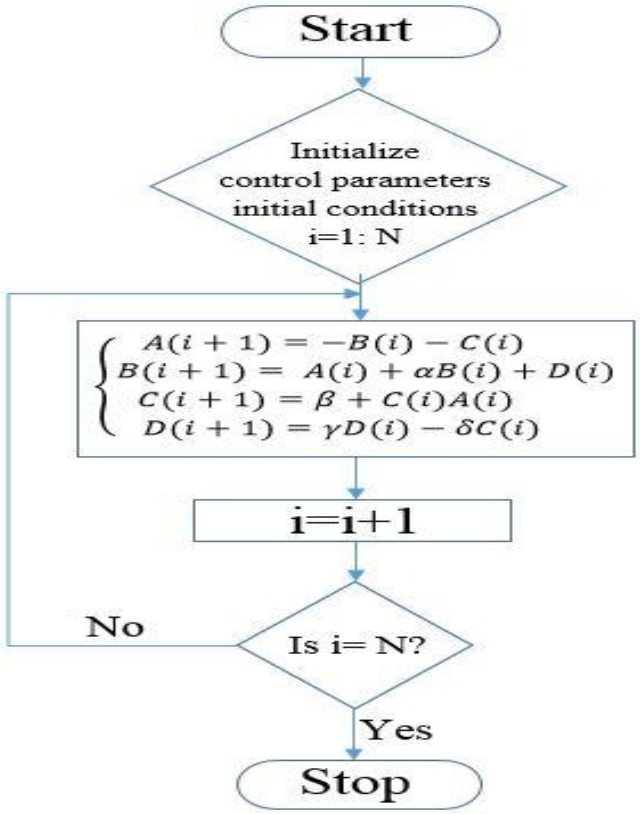


Figure (2.5): Flowchart of creation four sequences of Rossler hyper-chaotic system.

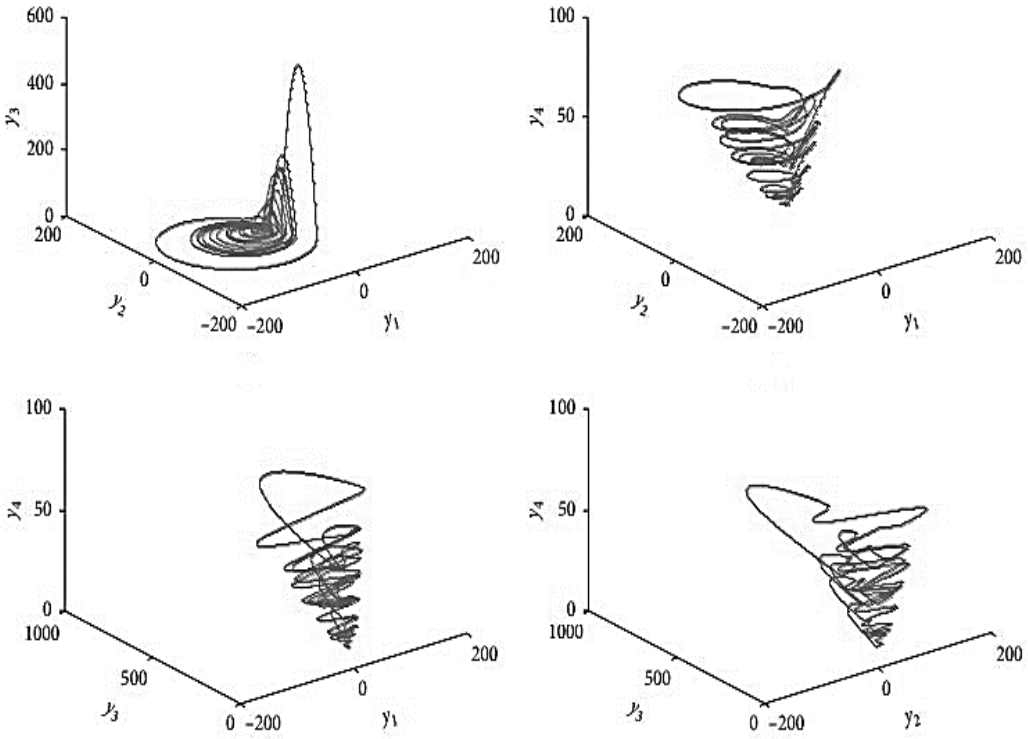


Figure (2.6): Rossler hyper-chaotic system [57].

2.6 DNA based Cryptography

DNA called as *genes* that store the information of our cells. It contains instructions for the construction and working of cells. It is the key for genetic inheritance. DNA is the source code to life. One cm^3 of DNA can store 10 terabytes of data. Figure (2.7) shows how digital data is encoded into DNA sequences and the latter is decoded and returned to digital data.

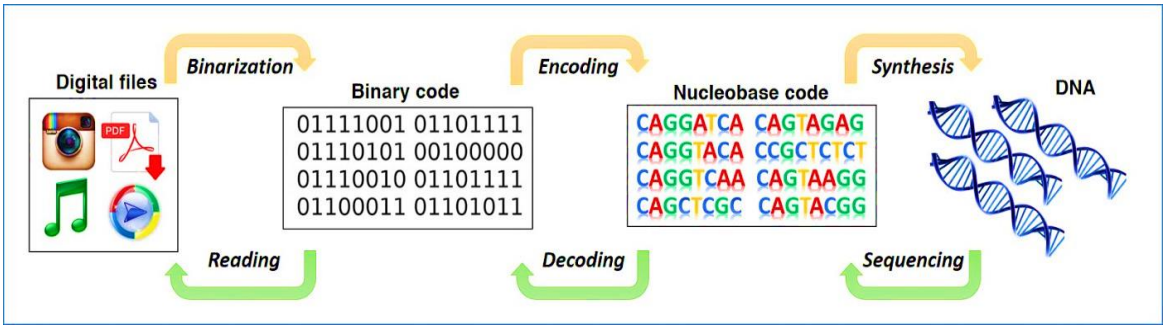


Figure (2.7): DNA and cryptography [58].

DNA and cryptography are a new field developed as a result of the advancement in DNA computation. Recently, it was discovered that DNA is able to store large amounts of data [59]. DNA cryptography is an emerging technology. It is a new technique used to store data safely in rest and in motion as well.

DNA cryptography has shown new ways to secure data. DNA provides data security with the help of its nucleotides. These nucleotides contain of four nitrogen bases, a phosphate group, and a carbon sugar which are Adenine, Cytosine, Guanine and Thymine; abbreviated as A, C, G, and T, respectively. These have a unique sequence structure, making them the basis of DNA cryptography [60]. As this DNA structure; make living things unique, likewise, using its techniques in cryptography make encryption algorithms unbreakable.

2.6.1 Properties of DNA

The use of DNA is promising, and it has the following important characteristics [59]:

1. **Data storage capacity**: DNA has a data density of around one bit per cubic nanometer, whereas traditional storage technologies require 1012 cubic nanometers to keep one bit.
2. **Data security**: Data security is demanded by society. DNA provides this ability as its unique structure makes data encryption algorithms unbreakable.
3. **Power requirement**: less power requirement is required for DNA computing because the chemical bonds of DNA work without any external power. As digital data is under consistent threat, there is a need for new approaches to secure data. Organizations need to be ahead of attackers to protect their own data and customer information to meet future needs.

2.6.2 DNA Encoding and Computing Operations

There are four DNA deoxy nucleotides which are A, G, C, and T bases. Among them G and C are complementary, so are A and T. Normally in binary system, 0 and 1 are complement to each other. Hence, 00, 11, 01, 10 can be encoded into the four bases. According to combinatorics there are 24 kinds possible DNA encoding methods. Due to complementary relationship between the four only 8 coding combinations are effective, as listed in Table (2.1).

In image encryption, the gray value of the image pixel can be expressed as its corresponding binary sequence, and then this binary sequence can easily be encoded into a DNA sequence. On the other hand, a DNA sequence can easily be translated into a pixel value. For example: a pixel value is 234 and its binary sequence 11101010. It can be encoded into a DNA sequence CTTT using DNA encoding Rule 6. And applying DNA decoding rule 3 on this sequence the retrieved pixel value is 128 [61]. Figure (2.8) explain the example in details. Figure (2.9) shows the flowchart of the DNA encoding for image pixels.

Moreover, different operations have been applied on DNA sequence to encrypt the image. As with binary numbers, the DNA sequences can be added, subtracted, and XORed in the same way, and the results are influenced by the rule that used to perform these operations. The details of the ADD DNA operation according to rule 0, XOR DNA operation according to rule 4, and SUB DNA operation according to rule 7 are shown in the Table (2.2), Table (2.3), and Table (2.4), respectively.

Table (2.1): DNA encoding rules.

Rule	**Rule 0**	**Rule 1**	**Rule 2**	**Rule 3**	**Rule 4**	**Rule 5**	**Rule 6**	**Rule 7**
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

Table (2.2): ADD operation DNA according to Rule 0.

+	**A**	**C**	**T**	**G**
A	A	C	T	G
C	C	G	A	T
T	T	A	G	C
G	G	T	C	A

Table (2.3): XOR operation DNA according to Rule 4.

⊕	**A**	**C**	**T**	**G**
A	G	T	C	A
C	T	G	A	C
T	C	A	G	T
G	A	C	T	G

Table (2.4): SUB operation DNA according to Rule 7.

+	**A**	**C**	**T**	**G**
A	T	A	G	C
C	G	T	C	A
T	A	C	T	G
G	C	G	A	T

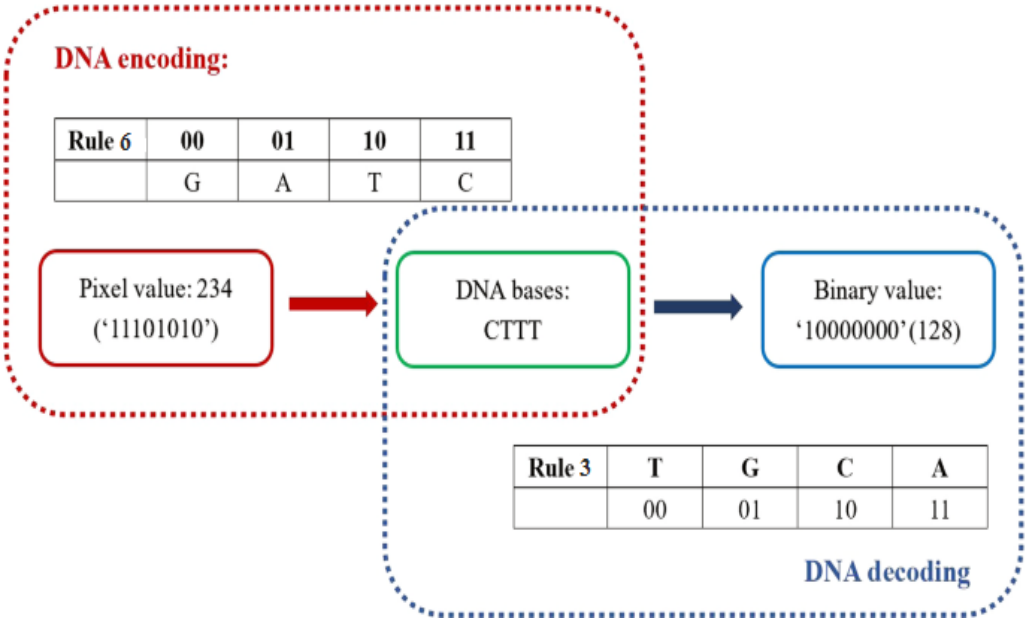


Figure (2.8): An example for DNA encoding and decoding.

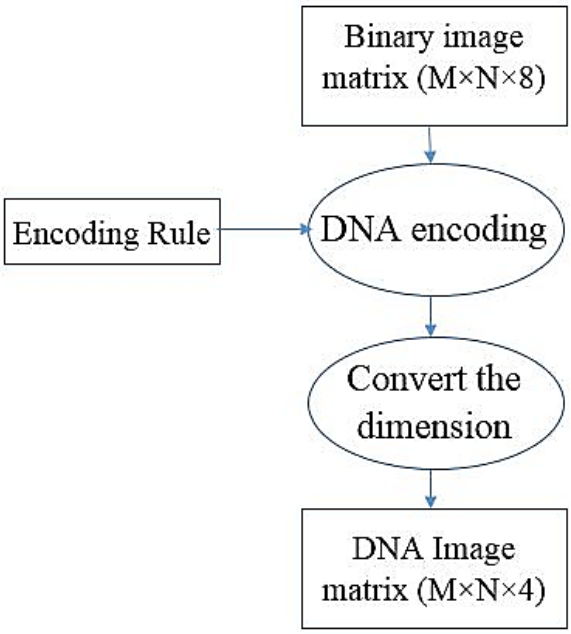


Figure (2.9): Flowchart of the DNA encoding for image pixels.

2.7 Hashing and Cryptography

A hash function cryptographic algorithm system is a technique, which accepts variable length input and produces fixed length hash value. No key is used in this method. Examples of hash function cryptographic algorithms are Message-Digest 4 (MD4), Message-Digest 5 (MD5), and SHA-2 family [62].

Hashing is used to validate the reliability of content by detecting all alterations of the content via noticeable changes to the hash output [63]. Hashing usually turns a plain text/image or password into a fixed length string of characters. Hash codes, hash values, hash sums, or simply hashes are the values returned by a hash function. A hash function may be a simple like Cyclic Redundancy Check (CRC32) or a full cryptographic function like MD5 or SHA1/2/256/384/512**.**

A hashing algorithm can always generate an 8-byte long string. It could be happen that two separate messages produce the same hash sum. It is important to note that hashing algorithms can require a key or not. If it does not require a secret key then called *keyless hashing algorithm* [64].

Hashing is basically impossible to reverse because of its internal working structure [65]. Hash functions works in an iterative mode over the input values to produce the hash chunk. In any hashing algorithm, the output of one stage is treated as the input of another stage. This process repeats itself until the final chunk is produced. Table (2.5) shows the types of SHA algorithms and its characteristics. SHA-256 and SHA-384 are used in our proposed encryption algorithm.

Table (2.5): Secure hash algorithms types [66].

Algorithm	Input message size (bits)	Output digest size (bits)
SHA-1	$<2^{64}$	160
SHA-224	$<2^{64}$	224
SHA-256	$<2^{64}$	256
SHA-384	$<2^{64}$	384
SHA-512	$<2^{64}$	512

2.8 Image Scrambling

Image scrambling is one of the way to encrypt the image data. Aim of image scrambling is to destroy the original image contents to make it difficult for the intruders to get original information out of it. So image scrambling transform the original image to random pattern image which is meaningless and imperceptible by human eyes. Recent years, many Image scrambling methods have been proposed. The evaluation of scrambling degree states the security level of the algorithm. Greater the scrambling degree higher the security of encrypted image. Objective evaluation of an scrambling algorithm can be done through changed pixel positions, entropy, correlation etc. [67]. Figure (2.10) shows the process of changing the positions of image pixels.

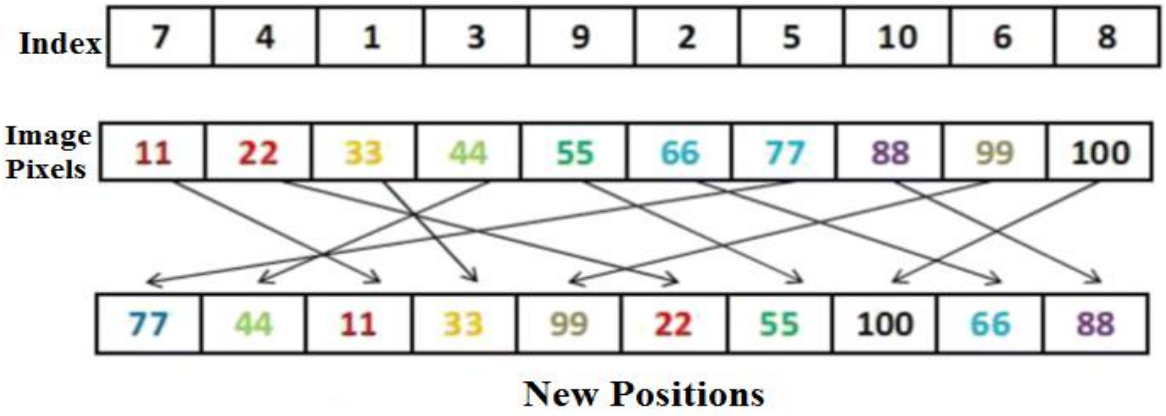


Figure (2.10): Image scrambling.

2.9 Metrics for Evaluating Encrypted Images

For verifying the security and the performance of an encryption algorithm, the algorithm has to be tested and evaluated based on the encrypted image properties. A good encryption algorithm should result in an encrypted image meeting the requirements of the following evaluation metrics [68].

The metrics may be classified into a couple of categories [69]. The first class evaluates the efficiency of the substitution process, which includes the histogram, entropy and correlation coefficients. The second group is

responsible for evaluating the ability of the approach to diffuse the original image. This group includes the MSE, PSNR, NPCR, and the UACI.

2.9.1 Key Space

The key space is the aggregate number of the diverse keys that can be utilized in the encryption and decryption techniques. For an operational cryptosystem, the key space should be huge to make exhaustion attack unfeasible; as resisting brute force attack requires a large secret key, with at least 128 effective and independent bits based on the available resources these days.

The attempts to discover the decryption key by checking all imaginable keys and the number of attempts to discover the key space of the cryptosystem is called the key space analysis. An encryption algorithm with a 128-bit key size describes a key space of 2^{128}, which takes almost 1021 years with superior computers to check all possible keys. Therefore, a cryptosystem with a key size of 128 effective and independent bits computationally sounds resistance against brute force attacks [70]. However, the encryption speed may slow down when the space of secret keys is very large.

2.9.2 Histogram

An image histogram represents the pixels values intensity distribution in an image, so to resist any statistical attack and to ensure a secure encryption system, the histogram of the encrypted image must be uniform [71]. From a mathematical standpoint, the histogram is a discrete function with gray level values ranging from 0 to L – 1 as in the following equation [72]:

$$hist(rk) = \frac{nk}{M \times N} \quad (2.5),$$

the k^{th} gray level is represented by rk, and the number of pixels in the image with that gray level value is represented by nk. M × N represents the total number of pixels in the image, and rk = 0, 1,..., L - 1. The histogram provides

an overall image description, where a narrow histogram refers to the fact that the image's visibility is poor due to the lack of contrast in the gray levels that exist in the image. Similarly, a widely distributed histogram refers to the fact that the majority of gray levels exist in the image, and therefore, the general contrast and visibility are better.

2.9.3 Information Entropy

The entropy of the information is used as a measure of the extent of the ambiguity of the system, it is a measure of unpredictability associated with a random variable and determines the quantity or the probability of the information's expected value contained in the message [73]. Through the entropy of the information can be known how to distribute the pixels values of an image [74]. The greater the value in the use of encryption, the better the outcomes. The entropy H(d) of data d is calculated using the following equation [75]:

$$H(d) = \sum_{i=1}^{2^l-1} p(d_i) log_2(\frac{1}{p(d_i)}) \quad (2.6),$$

where l is the number of digits in the image pixel gray value, and $p(d_i)$ signifies the likelihood of a pixel with value d_i occurring.

2.9.4 Correlation Coefficients

A correlation analysis determines the similarity between the cipher and the original image [76]. When the pixels' correlation coefficients in the encrypted image are as little as possible, the encryption technique of a color image must withstand statistical attacks. Equations (2.7), (2.8), and (2.9) [77] may be used to determine two neighboring pixels' horizontal, vertical, and diagonal correlation coefficients:

$$corr_{xy} = \frac{cov(x,y)}{\sqrt{\sigma_x}\sqrt{\sigma_y}} \quad (2.7)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \quad (2.8)$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{n}(x_i - \bar{x})^2 \text{ , and } \sigma_y = \frac{1}{N}\sum_{i=1}^{n}(y_i - \bar{y})^2 \quad (2.9),$$

where x and y are two neighbouring grayscale values and N is the total number of pixels in the image, $\bar{x}$ and $\bar{y}$ denote the mean value depicted in the following equation:

$$\bar{x} = \frac{1}{M \times N}\sum_{i=1}^{M \times N} x_i \quad (2.10)$$

The correlation coefficients are computed for numerous pairs of nearby (horizontal, vertical, and diagonal) pixels chosen at random from the encrypted image.

2.9.5 MSE and PSNR

We utilized the PSNR and MSE to assess the similarity between the plain image and the encrypted image for the encryption method. MSE is written as the following equation [78].

$$MSE = \frac{1}{M \times N}\sum_{a=0}^{M-1}\sum_{b=0}^{N-1}[|F(a,b) - F_0(a,b)|^2] \quad (2.11),$$

where M and N are the rows and columns of the image, respectively. F and F_0 are two images. A lower MSE value indicates that the proposed algorithm is more accurate in describing experimental data. MSE in our experiment refers to the similarity between the plain image and encrypted image, as well as, the similarity between the plain and decrypted images. In image encryption, PSNR gives the ratio between the peak signal and noise power between the original image and its encrypted form [79] . PSNR is written as the following equation [78].

$$PSNR = 10.log_{10}(\frac{peakval^2}{MSE}) \quad (2.12)$$

Peakval denotes the maximum number of image pixels; for an 8-bit integer-based image, peakval = 255. Table (2.6) shows the correct values of MSE and PSNR for the encrypted and decrypted images.

Table (2.6): The better cases for MSE and PSNR values.

Case	Image A - Image B	MSE	PSNR
1	original - encrypted	must be high	low
2	decrypted - original	must be low	high

2.9.6 Differential Attacks

The NPCR and the UACI are commonly employed to assess the robustness of encryption systems in terms of differential attacks [80]. This method can be used to find the relationship between the encrypted image and the original image. The NPCR and UACI are used to assess how one-pixel changes affect the entire encrypted images with the proposed algorithm. In other word, a single pixel alteration in the plain image causes a massive change in the encrypted image [81]. The following equations can be used to calculate NPCR, and UACI [82]:

$$NPCR = \frac{\sum_{i,j} D(i.j)}{M \times N} \times 100\% \quad (2.13)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (2.14)$$

$C_1(i,j)$ and $C_2(i,j)$ represent two encrypted images with only one pixel value change from the corresponding plain images, $D(i.j) = 0$ when it is the same value in C_1 and C_2, while, it is 1 when it is different. For every three test images, the standard predicted values of NPCR and UACI, as stated in [29], should be greater than 99.4% and 33.2 %, respectively.

Chapter Three

Proposed Encryption Algorithm Based on DNA Encoding and Hyper-chaotic Systems

3.1 Introduction

This chapter will highlight the proposed method used to build a secure color image encryption algorithm using a mixture of SHA-2, DNA encoding and hyper-chaotic systems.

The algorithm that has been proposed consists of six major steps: Key generation, Generate chaotic sequences, Scrambling, DNA encoding, Substitution, and DNA decoding.

In this chapter, we introduce the generation of the secret key based on the original image. The generation of Lorenz hyper-chaotic sequences by using the secret key and use these sequences to scramble the components of original image. It focuses on diffusion process that contains generation of Rossler hyper-chaotic sequences by using the secret key, DNA encoding/ decoding, addition operation, and xoration with Rossler hyper-chaotic sequences. The decryption process and restore the original image from the encrypted. Finally, summary is discuss.

3.2 Generation of the Secret Key

The security of the 4-D hyper-chaotic systems, which has been used in the proposed algorithm, relies on the key space of the initial key, hence the generation of the initial key is considered to be very important.

Both the sender and the recipient share a single key in this scheme. Because a single key is used for both encryption and decryption, this method is known as *Secret Key Cryptography* (*SKC*). The most desirable feature of any image algorithm is to make the secret key as strong as possible, so that, it cannot be hacked and is protected from detection by unauthorized parties. Therefore, the key is generated in a rather complex way, so that, it is difficult for an attacker to know and predict the key. The hash of the original image is used to generate the secret key. The diagram of generation of the secret key as shown in Figure (3.1). The steps for key generation are as follows:

Step1: The original key is generated by SHA-256, which is a hashing algorithm. The matrix I_0 represents the original image pixels. By hashing with SHA-256, we can obtain $K_{initail}$. What needs to be emphasized is that $K_{initail}$ is a one-time key because $K_{initail}$ varies with different images.

$$K_{initial} = f_{SHA-256}(I_0) \tag{3.1}$$

Generally, hash function generates a 256-bit hash value. Typically, this value is represented as a 64 digit hexadecimal number. It leads a significant difference between two images if there happens even one-bit alteration in the input of hash value.

Step2: To add more complexity, the initial key $K_{initail}$ is hashed with SHA-384, we can get K_{final} that contains 48 bytes.

$$K_{final} = f_{SHA-384}\,(K_{initail}) \tag{3.2}$$

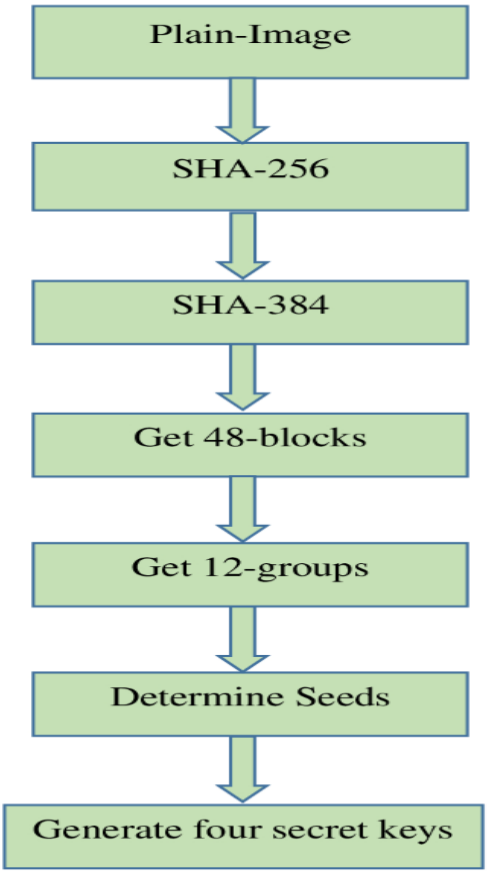


Figure (3.1): Block diagram of the secret keys generation.

Step3: The initial key can be used to get the initial parameters for a chaotic system once it is generated. A 384-bit K_i is divided into 8-bit blocks and we get 48 blocks $b_1, b_2, \ldots, b_{48}$. After that, every 4 blocks are grouped together, resulting in 12 groups, $G_1, G_2, \ldots, G_{12}$.

$$G_i = \{b_{4i-3};\ b_{4i-2};\ b_{4i-1};\ b_{4i}\},\ (1 \le i \le 12) \tag{3.3}$$

Step4: According to our chaotic systems, seeds $S_1, S_2, \ldots, S_{12}$ are determined as follows:

$$S_i = \frac{1}{2^6}\sum_{m=0}^{3} b_{4i-m}\ ,\quad (1 \le i \le 12) \tag{3.4}$$

Step5: The final keys are obtained by applying Equation (3.5) to the seeds that calculated in the previous stage:

$$\begin{cases} X_1 = A_1 = S_1 + S_2 + S_3 \\ Y_1 = B_1 = S_4 + S_5 + S_6 \\ Z_1 = C_1 = S_7 + S_8 + S_9 \\ W_1 = D_1 = S_{10} + S_{11} + S_{12} \end{cases} \quad (3.5),$$

where (X_1, Y_1, Z_1, and W_1) are the initial parameters of Lorenz hyper-chaotic system and (A_1, B_1, C_1, and D_1) are the initial parameters of Rossler hyper-chaotic system. The fundamental principle of chaos encryption is based on dynamic systems' ability to generate a sequence of random numbers, which is then utilized to encrypt images. The initial conditions that used to generate the random number sequence, have a significant impact on the final result. The sequences will be completely different if the initial conditions is slightly changed. Chaotic systems are useful for encryption because of their sensitivity to the initial conditions. The secret keys generated, in this section, were used as the initial conditions for producing chaotic sequences.

3.3 Confusion Phase

Image pixels permutation is an important role for encryption scheme. Permutation is considered as an auxiliary operation for diffusion step. Sorting permutation using hyper-chaotic systems, such as permutation used in proposed algorithm, result into image that appear as scattered pattern. This makes all pixels move in random direction and distance. It is different from Arnold cat map that approximately make all pixel move in similar direction. Despite the importance of permutation stage, the encryption system largely depends on diffusion stage.

This phase consists of two stages to obtain the permutation, the first stage includes the generation and modification of chaotic sequences and the second stage includes the scrambling process by using modified chaotic sequences.

3.3.1 Stage1

In this stage, the generation and modification of chaotic sequences are applied as following steps:

Step1: Generation of four chaotic sequences X, Y, Z, and W via a Lorenz hyper-chaotic system. This step uses the initial conditions X_1, Y_1, Z_1, and W_1 as described in the Equation (3.5). To reduce the transient effect and get a suitable pseudo-random sequence, the results of the first iterations are ignored. The system is then performed M×N times, resulting in the following four sequences:

$$\begin{cases} X = \left[\hat{X}_1, \hat{X}_2, \hat{X}_3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \hat{X}_{MN}\right] \\ Y = \left[\hat{Y}_1, \hat{Y}_2, \hat{Y}_3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \hat{Y}_{MN}\right] \\ Z = \left[\hat{Z}_1, \hat{Z}_2, \hat{Z}_3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \hat{Z}_{MN}\right] \\ W = \left[\hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \hat{W}_{MN}\right] \end{cases} \quad (3.6)$$

Step2: Apply the following equations on the sequences generated by hyper-chaotic systems X, Y, Z, and W :

$$\begin{cases} [\sim, \mathrm{Index_x}] = \mathrm{sort}(X, 'ascend') \\ [\sim, \mathrm{Index_y}] = \mathrm{sort}(Y, 'descend') \\ [\sim, \mathrm{Index_z}] = \mathrm{sort}(Z, 'ascend') \\ [\sim, \mathrm{Index_w}] = \mathrm{sort}(W, 'descend') \end{cases} \quad (3.7),$$

where $sort()$ is the sequencing index function. $\mathrm{Index_x}$, $\mathrm{Index_y}$, $\mathrm{Index_z}$, and $\mathrm{Index_w}$ represent the new sequences of X, Y, Z, and W, respectively.

3.3.2 Stage2

Color image is not immediately encryptable. As a result, the color image must be separated into R, G, and B gray images components. As an example, in Figure (3.2); we separate the image (a) of Lena in color with size 256 × 256; images in grayscale of the R, G, and B components of (a) are shown in (b), (c), and (d), respectively.

In the following steps, the position of the pixels on the original image have been scrambled based on the sequences that are produced by Lorenz hyper-chaotic system:

Step1: Suppose that a color image has the dimensions M × N, where M and N denote the image's rows (height) and columns (width).

Step2: Convert the color (RGB) image in its digital form into three 2D matrices R, G, and B for the channels of red, green, and blue, respectively, where the entries of original image in the range [0, 255]. The size of each component is M × N, where M signifies the row's number and N signifies the column's number of R, G, and B.

Step3: Scrambling the positions of pixels using the index sequences of X, Y, Z, and W sequentially for each component and obtain scrambled matrices R_s, G_s, and B_s.

Figure (3.3) shows the three components after they have been scrambled. Even though there are obvious discrepancies between the three scrambled image components (a), (b), and (c). There is still a correlation between pixels, even when human eyes cannot see the original image information.

3.4 Diffusion Phase

Because confusion is not enough, any inverse procedure that returns the pixels to their original places will declare the original image. Diffusion refers to modifying the values of pixels of an image by conducting various transformations on the pixels values. As a result, by changing the values of the pixels, the encryption operation will be strengthened and the correlation between pixels will be cancelled, resulting in an encrypted image with a uniform histogram. Scrambled image can be encrypted after applying several operations to every pixel using DNA encoding and Rossler hyper-chaotic system.

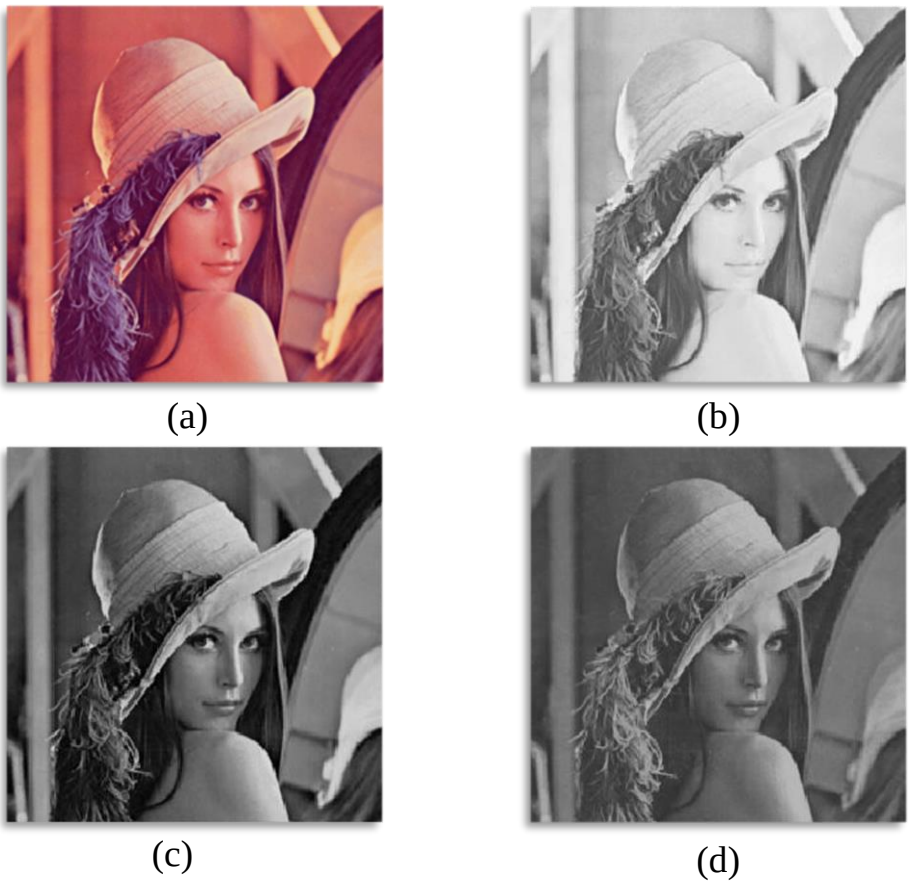


Figure (3.2): Lena image: (a) RGB Lena's image 256 × 256, (b) element of red, (c) element of green, and (d) element of blue.

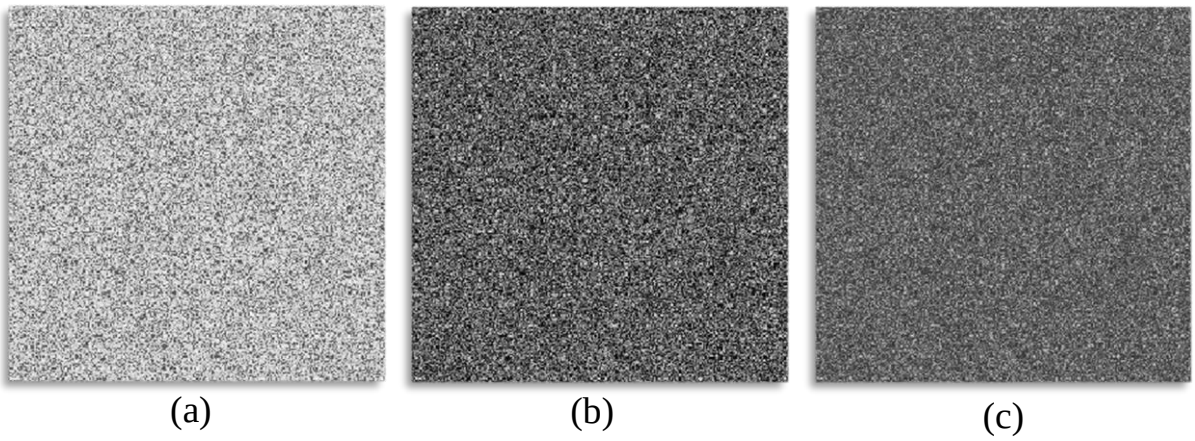


Figure (3.3): Scrambled components: (a) Red, (b) Green, and (c) Blue.

3.4.1 Chaotic Sequences Generation

Generation of chaotic sequences can be proposed as the following steps:

Step1: Using the Rossler hyper-chaotic system to create four chaotic sequences A, B, C, and D. The initial parameters A_1, B_1, C_1, and D_1 are used in this step, as specified in Equation (3.5). To decrease the transitory impact and produce a sufficient pseudo-random sequence, the results of the first iterations are ignored. After then, the system is run M × N times, resulting in the following four sequences:

$$\begin{cases} A = \left[\hat{A}_1, \hat{A}_2, \hat{A}_3, \dots\dots\dots\dots\dots\dots\dots\dots \hat{A}_{MN}\right] \\ B = \left[\hat{B}_1, \hat{B}_2, \hat{B}_3, \dots\dots\dots\dots\dots\dots\dots\dots \hat{B}_{MN}\right] \\ C = \left[\hat{C}_1, \hat{C}_2, \hat{C}_3, \dots\dots\dots\dots\dots\dots\dots\dots \hat{C}_{MN}\right] \\ D = \left[\hat{D}_1, \hat{D}_2, \hat{D}_3, \dots\dots\dots\dots\dots\dots\dots\dots \hat{D}_{MN}\right] \end{cases} \quad (3.8)$$

Step2: The first chaotic sequence A is converted into range from 0 to 7 according to the following equation.

$$\mathrm{A} = \mathrm{MOD}(\mathrm{ROUND}(\mathrm{A} * 10\hat{}4),8) \quad (3.9)$$

The resulting sequence is used in the process of determining the rule that used in the addition operation in the next stages, where the addition will be dynamic by using the chaotic sequence.

Step3: The rest of chaotic sequences B, C, and D are converted into range from 0 to 255 according to the following equation:

$$\begin{cases} \mathrm{B} = \mathrm{MOD}(\mathrm{ROUND}(\mathrm{B} * 10\hat{}4),256) \\ \mathrm{C} = \mathrm{MOD}(\mathrm{ROUND}(\mathrm{C} * 10\hat{}4),256) \\ \mathrm{D} = \mathrm{MOD}(\mathrm{ROUND}(\mathrm{D} * 10\hat{}4),256) \end{cases} \quad (3.10)$$

The three generated sequences are used in the XOR operation

3.4.2 DNA Encoding

In DNA encoding, the following steps are applied:

Step1: By converting the scrambled matrices R_s, G_s, and B_s into an 8-bit binary representation, three alternative matrices, R_{binary}, G_{binary}, and B_{binary}, can be created, all of which are of size (M, N, 8).

Step2: Each binary pixel in the three matrices R_{binary}, G_{binary} and B_{binary} being encoded into DNA using rules 5, 6, and 7 as show in Table (2.1), so that, we can get R_{DNA}, G_{DNA}, and B_{DNA}, respectively and their size is (M, N, 4).

Step3: Three alternate sequences, B_{binary}, C_{binary}, and D_{binary}, can be constructed by converting the three chaotic sequences B, C, and D into an 8-bit binary form.

Step4: By encoding each binary item in the three sequences B_{binary}, C_{binary}, and D_{binary} into DNA using rules 5, 6, and 7, we can obtain B_{DNA}, C_{DNA}, and D_{DNA}, respectively.

3.4.3 Addition and Xoration Operations

The operations of addition and xoration applied as the following steps:

Step1: The addition operation between the three matrices is done according to Equation (3.11), and the addition rule is chosen dynamically depending on the sequence A. Where the sign " + " denotes to an ADD operation.

$$\begin{cases} G'_{DNA} = R_{DNA} + G_{DNA} \\ B'_{DNA} = G_{DNA} + B_{DNA} \\ R'_{DNA} = R_{DNA} + G'_{DNA} \end{cases} \quad (3.11)$$

Step2: The XOR operation is applied between the chaotic sequences, B_{DNA} with R'_{DNA}, to get R''_{DNA}, C_{DNA} with G'_{DNA}, to get G''_{DNA}, and D_{DNA} with B'_{DNA}, to get B''_{DNA} as in Equation (3.12).Where the sign "⊕" denotes to a XOR operation.

$$\begin{cases} R''_{DNA} = B_{DNA} \oplus R'_{DNA} \\ G''_{DNA} = C_{DNA} \oplus G'_{DNA} \\ B''_{DNA} = D_{DNA} \oplus B'_{DNA} \end{cases} \quad (3.12)$$

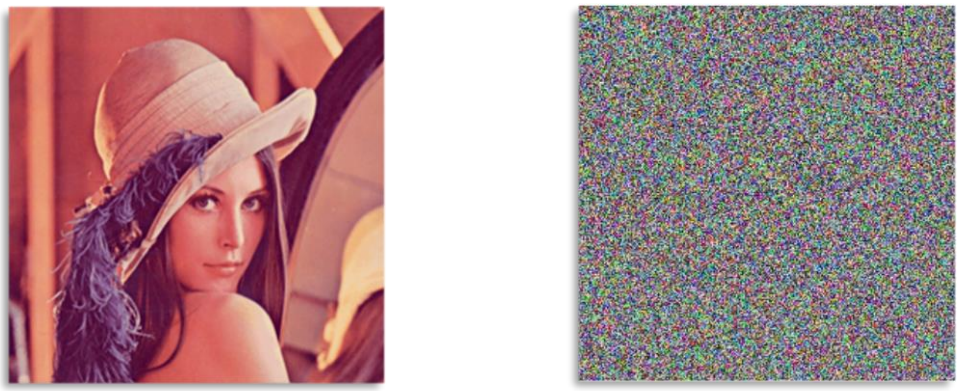
3.4.4 DNA Decoding

In DNA decoding, we applied the following steps:

Step1: The DNA encrypted matrices that obtained from previous step are decoded to binary representation by using the rules 0, 1, and 2 with. Then, the binary matrices converted into the pixel matrices R', G', and B'.

Step2: Finally, the three components are combined to form the encrypted image. Send the encrypted image, as well as, the secret keys to the recipient now.

Figure (3.4) (a), and (b) show both the plain and encrypted images, respectively. The human eye cannot identify the information because the encrypted image is not clear. Figure (2.5) show the block diagram of the proposed encryption algorithm.



(a) (b)

Figure (3.4): Result of the encryption process: (a) Original image; (b) Encrypted image.

3.5 Decryption Process

The encrypted image generated through the encryption algorithm is sent by insecure channel. As the proposed image cryptosystem is symmetric, therefore, the decryption can, also, be carried-out by using the similar steps in the opposite direction. After receiving the color (RGB) encrypted image, the recipient acquires the encryption's private keys which has been transformed through insecure channel. These keys can be employed in hyper-chaotic

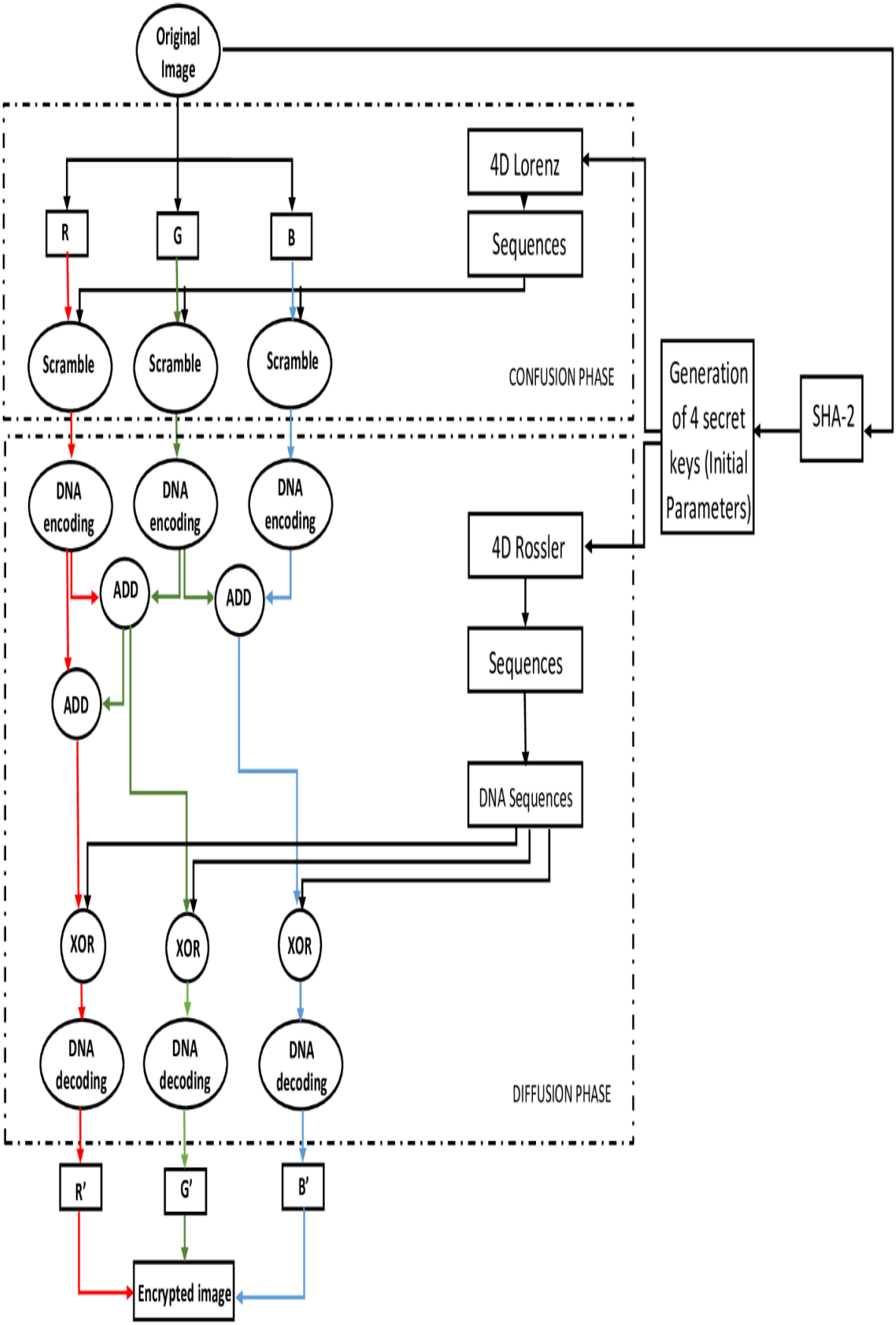


Figure (2.5): Block diagram of the proposed encryption method.

systems for the creation of random values for encryption. The pixel value is restored to its original value prior to encryption by first executing the diffusion step and then doing the confusion step to restore pixels to their original places in the image before encryption.

The decryption process of images is shown in Figure (3.6). The original color image that has been encrypted and the image that has been decrypted are shown in Figure (3.7) (a), and (b), respectively. The procedure of recovering the plain color image from the encrypted color image is given as follows:

Step1: Read the color image that has been encrypted E, and then separated into R, G, and B components.

Step2: Use four initial conditions (secret keys) and parameters in Rossler hyper-chaotic systems, for producing four sequences A, B, C, and D. To keep the values of the sequence A between [0, 7], it performs Equation (3.9). Also, to keep the values of the sequences B, C, and D between [0, 255], it performs Equation (3.10).

Step3: Convert the three encrypted image components (ER, EG, EB) and the three chaotic sequences (B, C, D) into binary matrices with length size (M × N × 8).

Step4: Encode the three binary matrices of encrypted image components according to DNA encoding by using the rules 0, 1, and 2, respectively, and get three matrices whose length is (M × N ×4).

Step5: Encode the three binary matrices of chaotic sequences according to DNA encoding by using the rules 5, 6, and 7, respectively, and get three matrices whose length is (M × N ×4).

Step6: Perform the XOR process between the matrices obtained from Step4 and the matrices obtained from Step5, then, get R'_{DNA}, G'_{DNA}, and B'_{DNA}.

Step7: The subtraction operation between the three matrices is done according to Equation (3.13), and the subtract rule is chosen dynamically depending on the sequence A. Where the sign " − " denotes to a SUB operation.

$$\begin{cases} \mathrm{R_{DNA}} = \mathrm{R'_{DNA}} - \mathrm{G'_{DNA}} \\ \mathrm{G_{DNA}} = \mathrm{G'_{DNA}} - \mathrm{R_{DNA}} \\ \mathrm{B_{DNA}} = \mathrm{B'_{DNA}} - \mathrm{G_{DNA}} \end{cases} \tag{3.13}$$

Step8: Three DNA sequences matrixes are decoded by the rules 5, 6, and 7, respectively, to obtain the R, G, and B components.

Step9: Use four initial values (secret keys) and parameters for hyper Lorenz chaotic systems for producing four sequences X, Y, Z, and W. These sequences are sorted according to Equation (3.7), as detailed in Section (3.3.1).

Step10: Select the combination (X, Y, Z, and W) in reverse order to descramble R, G, and B components.

Step11: Finally, these three matrices are recombined into a color image to create the final decrypted image.

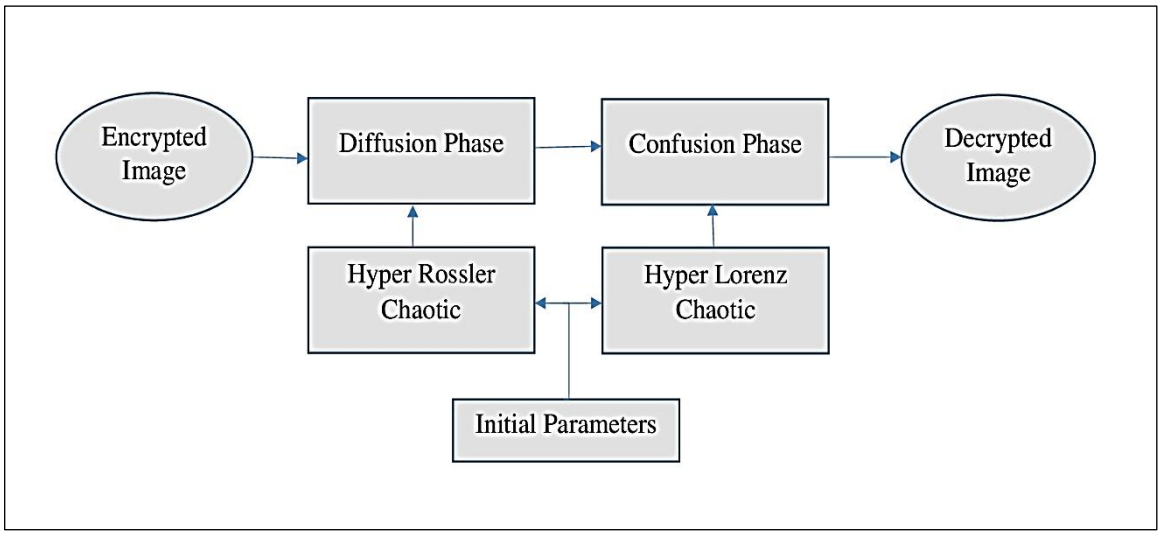
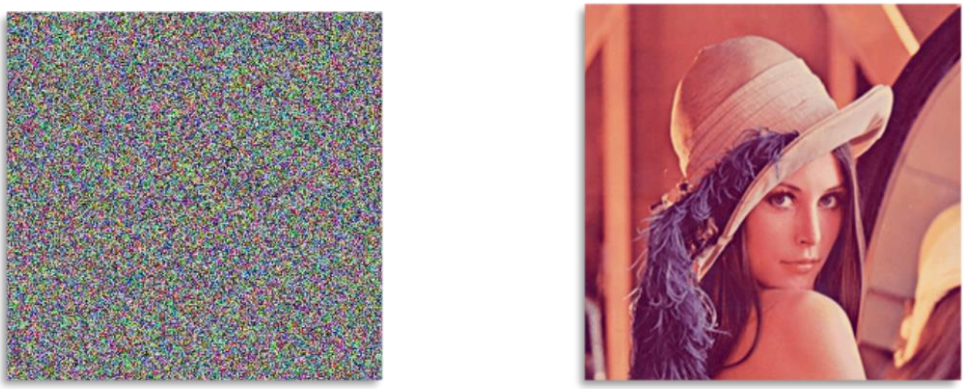


Figure (3.6): Block diagram of image decryption process.



(a) (b)

Figure (3.7): Result of the decryption process (a) Encrypted image; (b) Decrypted image.

3.6 Summary

The one-time pad encryption technique is safe, according to Shannon's theory. Because chaotic sequences formed by a chaotic system are unpredictable, and sequences generated by numerous chaotic systems combined are even more unpredictable, the multiple chaotic color encryption algorithm is classified as a one-time pad algorithm. As a result, it is clear that this algorithm has a high level of security.

Furthermore, the color image encryption algorithm proposed in this chapter, which uses chaotic sequences and DNA coding, has the following advantages:

1- The initial conditions for chaotic systems in the proposed algorithm are based on the original color image, which makes prediction more challenging.

2- Any changing in chaotic system parameter has a direct impact on the chaotic sequences. As a result, the initial values will have a huge impact on the resulting of encryption or decryption process.

3- For increased security, this algorithm does not employ the initial part of the created chaotic sequences, instead choosing the last portion of the chaotic sequences.

4- The security of the encryption algorithm is improved by using distinct encoding and decoding algorithms to encrypt the three components of color image and chaotic sequences.

5- Dynamic DNA addition operation, in which the addition rules depends on the chaotic matrix, could be added more security.

Chapter Four

Simulation Results and Security Analysis

4.1 Data Collection and Simulation Environment

The experiments are carried out to demonstrate the proposed method's performance and validity. To evaluate the encryption/decryption processes on the images, different images have been used. The four images used (Lena, Baboon, Pepper, and Flowers) are taken from USC-SIPI (http://sipi.usc.edu/database/) [83] open image repository for color (RGB) images, and two images used (all Black, all White). All the selected images are stored in PNG format 256 × 256. The implementation of the image encryption scheme is performed on the PC with MATLAB R2013a having operating system 32-bit Windows 8, Intel$^{(R)}$ Core^{TM} i5-4310U 2.60 GHz CPU with 8 GB RAM. Furthermore, a Lena 256×256 color image is utilized for comparison where the settings for executing encryption are specified as (a = 10, b =8/3, c =35, and r = -1) for hyper Lorenz chaotic system and (a = 0.25, b = 3, c = 0.05, and d = 0.5) for hyper Rossler chaotic system.

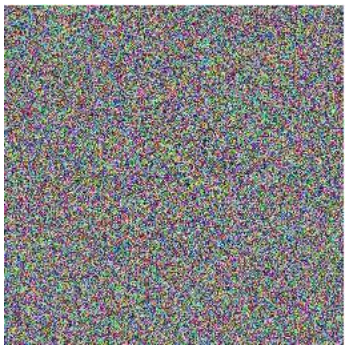
4.2 Simulation Results

An effective image encryption algorithm should be able to resist all types of attacks, including exhaustive, differential, and statistical attacks, etc. By assessing the security performance of the suggested encryption algorithm, we will demonstrate that this encryption system is sufficiently secure against various cryptographic attacks. The performance of the suggested image encryption technique is analyzed in detail. Experimental results consists of these: Performance Evaluation, Histogram Analysis, Key Space, Key Sensitivity Analysis, Information Entropy Analysis, Correlation of Adjacent Pixels, MSE and PSNR Analysis, and Attacks Analysis, they are described below.

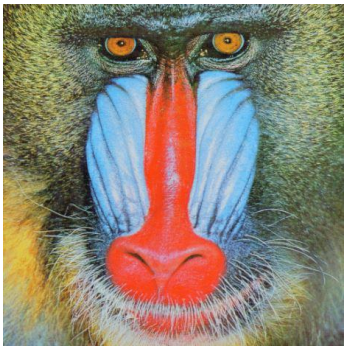
4.2.1 Performance Evaluation

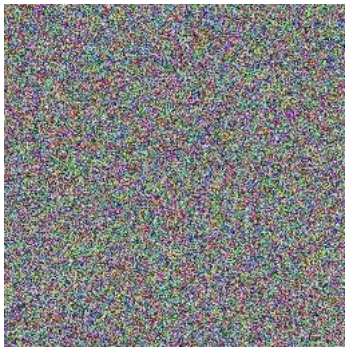
The proposed algorithm encrypted and decrypted a number of colored images, and a visual test is conducted. Figure (4.1); p(a)–p(f) plain images, Figure (4.1); e(a)–e(f) encrypted images, and Figure (4.1); d(a)–d(f) decrypted images. We were unable to extract any relevant information from the encrypted images, because they were all noise-like images, as shown in Figure (4.1). However, the decrypted images were exactly the same as the original images, demonstrating that the algorithm is secure and successful.

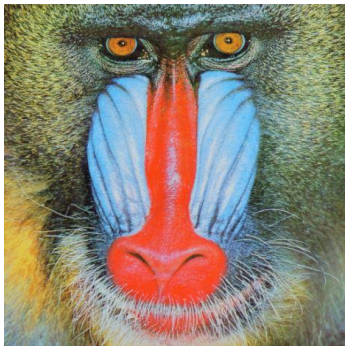

p(a)


e(a)

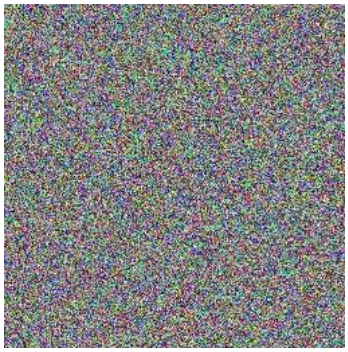

d(a)


p(b)


e(b)


d(b)


p(c)


e(c)


d(c)

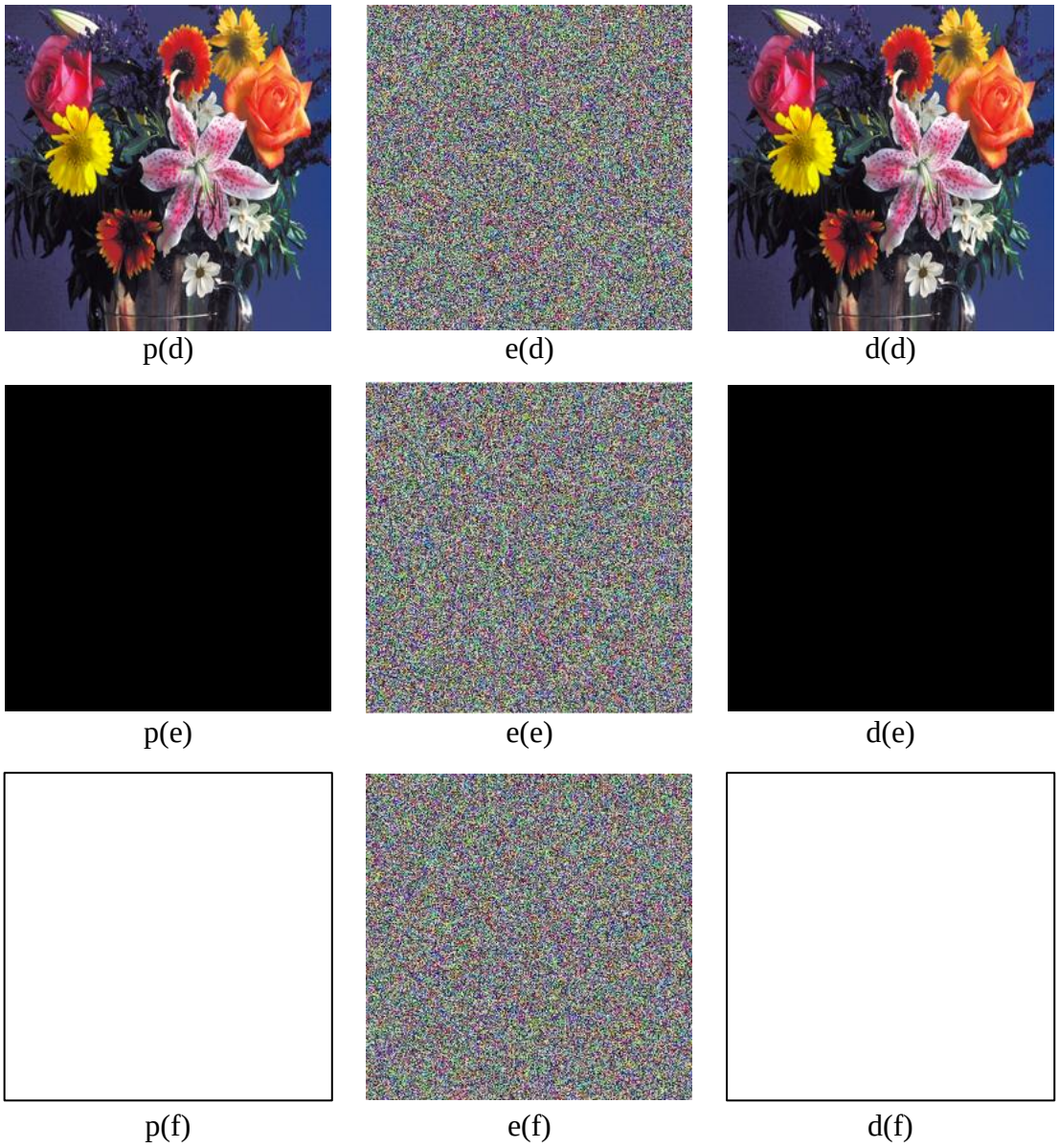


Figure (4.1): Performance evaluation of the proposed method; p(a–f) are plain images, e(a–f) are encrypted images, and d(a–f) are decrypted images.

4.2.2 Histogram Analysis

The distribution of pixels inside the image is visualized via histogram analysis, which is a useful tool for image analysis. To be strong against statistical attacks, the histogram for encrypted images should be uniformly distributed, as the most used bit in the image and its position can give some information about the key.

The Lena image is a typical example and it is used for the show histogram in Figure (4.2). Figure (4.2)-(a_0, a_1, and a_2) show the histograms for channels

(red, green, and blue) of Lina's plain image, respectively. Since, Figure (4.2); (b_0, b_1, b_2) shows the histograms of the encrypted image for channels (red, green, and blue) of Lina's image, respectively.

The encryption was highly achieved by lowering the majority of the data, as seen in the histograms. It can be concluded that the proposed algorithm is effective at thwarting the histogram attack and shows whether an attacker tries to deduce pixel data by analyzing the statistic characteristic of the image that is encrypted from the histogram. This type of attack is known as a cipher only attack, it is being resisted by this algorithm and providing no useful information to the attacker.

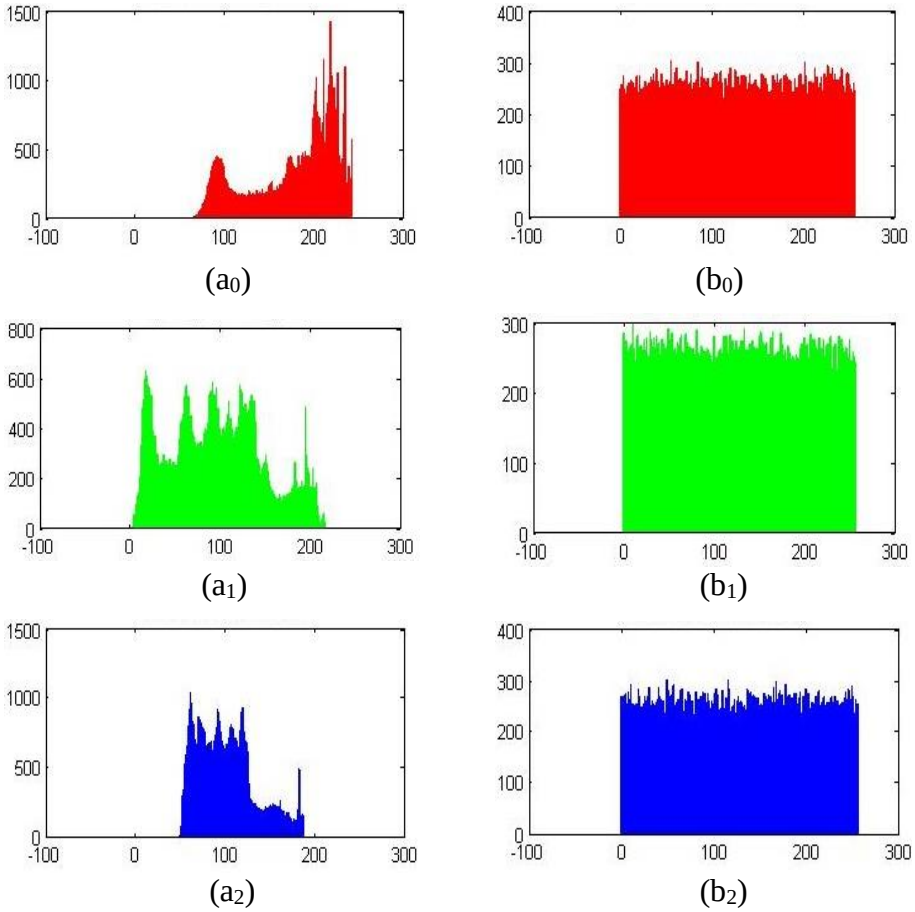


Figure (4.2): Histogram Analysis of Lena image; (a_0, a_1, a_2) the histograms for (R, G, and B) of plain image; (b_0, b_1, b_2) the histograms of the encrypted image for (R, G, and B).

4.2.3 Key Space

The key in the proposed algorithm is composed primarily of the initial parameters X_1, Y_1, Z_1, and W_1 composed of hyper Lorenz and hyper Rossler systems. Thus, if precision is set at 10^{-15}, there are 4 keys in total, which means the total key space is $10^{15\times4} = 10^{60} = (10^3)^{20} \approx (2^{10})^{20} \approx 2^{200}$ larger than 2^{128}. As a result, we have implemented an encryption algorithm with enough key space to resist various brute-force attacks.

4.2.4 Key Sensitivity Analysis

A protected algorithm must provide a wide key space to increase the resistance to brute force attacks on a cryptosystem. Furthermore, be fully sensitive to the key, which indicates that the image cannot be decrypted by minor changes in the key. This means that even a minor variation in the secret key will result in an entirely different encrypted image; in other hand, a secret key that is slightly different from the correct one will never decrypt the image and will generate a completely wrong image.

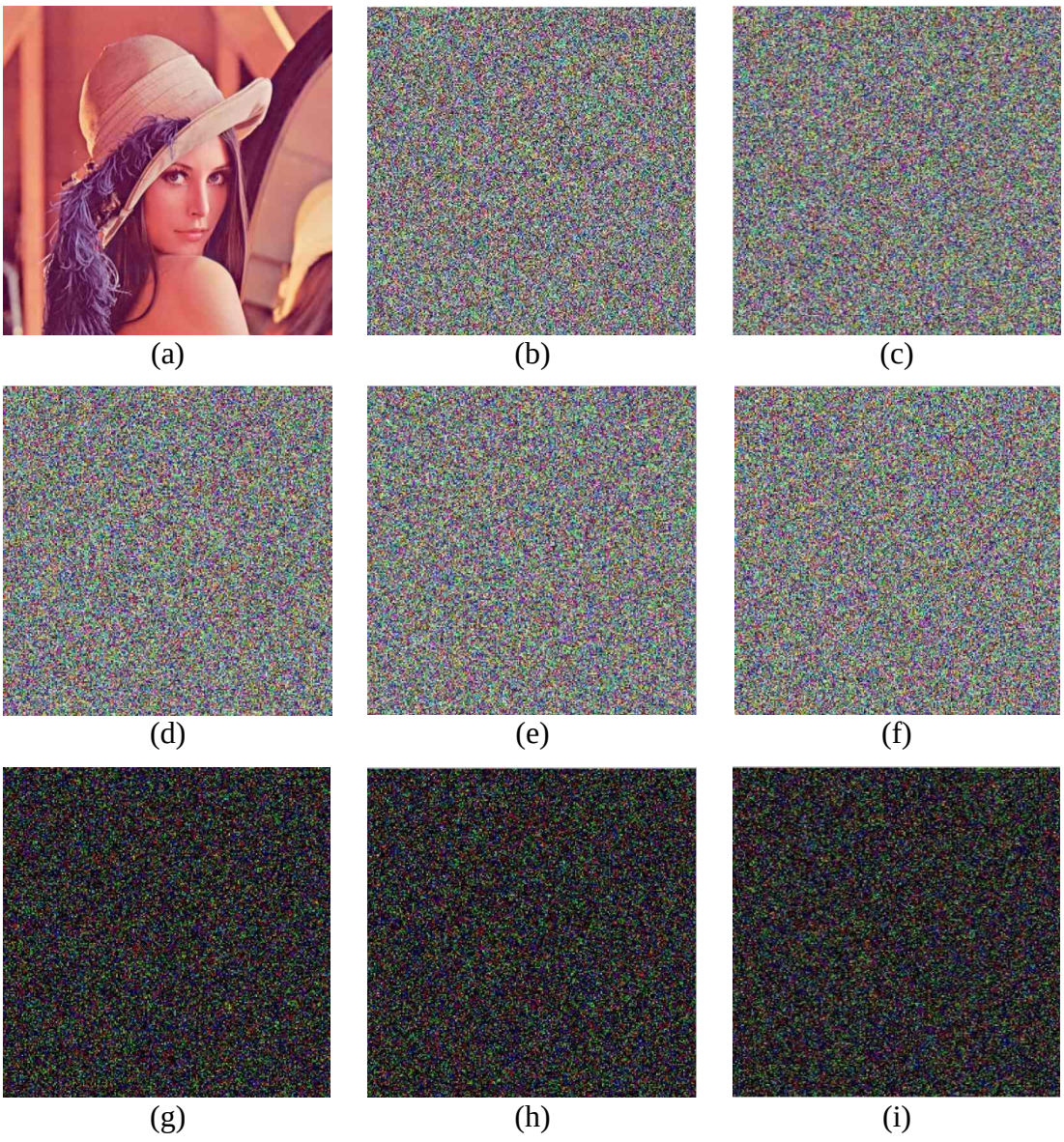
4.2.4.1 Key Sensitivity Analysis of the Encryption Process

At the encryption process, an image encryption algorithm must be sensitive enough to minor changes in the encryption key. Here, as the plain image, we utilize the Lena image from Figure (4.1) (a). To demonstrate the proposed algorithm's key sensitivity visually, one of the initial parameters is altered, while the others stay unchanged. The encryption stage's key sensitivity analysis is depicted in Figure (4.3), the NPCR for associated encrypted images of Figure (4.3) is reported in Table (4.1).

In Table (4.1), the original key of the plain image is Key, and (Key1, Key2, Key3, Key4), are four modified keys. As a result, the encrypted versions of the plain image differ from the encrypted image that has been used the original key when four slightly changed keys are utilized to encrypt it, the values of NPCR in Table (4.1) are greater than 99.6%.

Table (4.1): NPCR for encrypted images for Figure (4.3) in encryption stage.

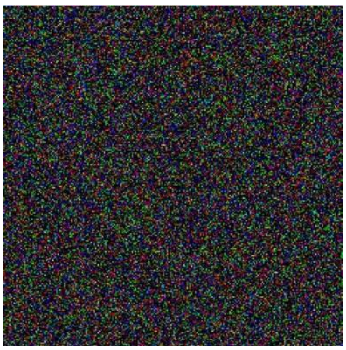
	X	Y	Z	W	NPCR (%)
Key	27.84375	31.0625	29.8125	23.640625	0
Key1	27.8437**6**	31.0625	29.8125	23.640625	99.60
Key2	27.84375	31.062**6**	29.8125	23.640625	99.61
Key3	27.84375	31.0625	29.**9**125	23.640625	99.61
Key4	27.84375	31.0625	29.8125	23.64**1**625	99.60



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)



(j)

Figure (4.3): Key Sensitivity Analysis of the Encryption Process; (a) Lena's original image; (b) encrypted image with the original encryption key; (c), (d), (e), and (f) utilizing four modified keys to encrypt the images; (g) b - c; (h) b - d; (i) b - e; (j) b - f.

4.2.4.2 Key Sensitivity Analysis of the Decryption Process

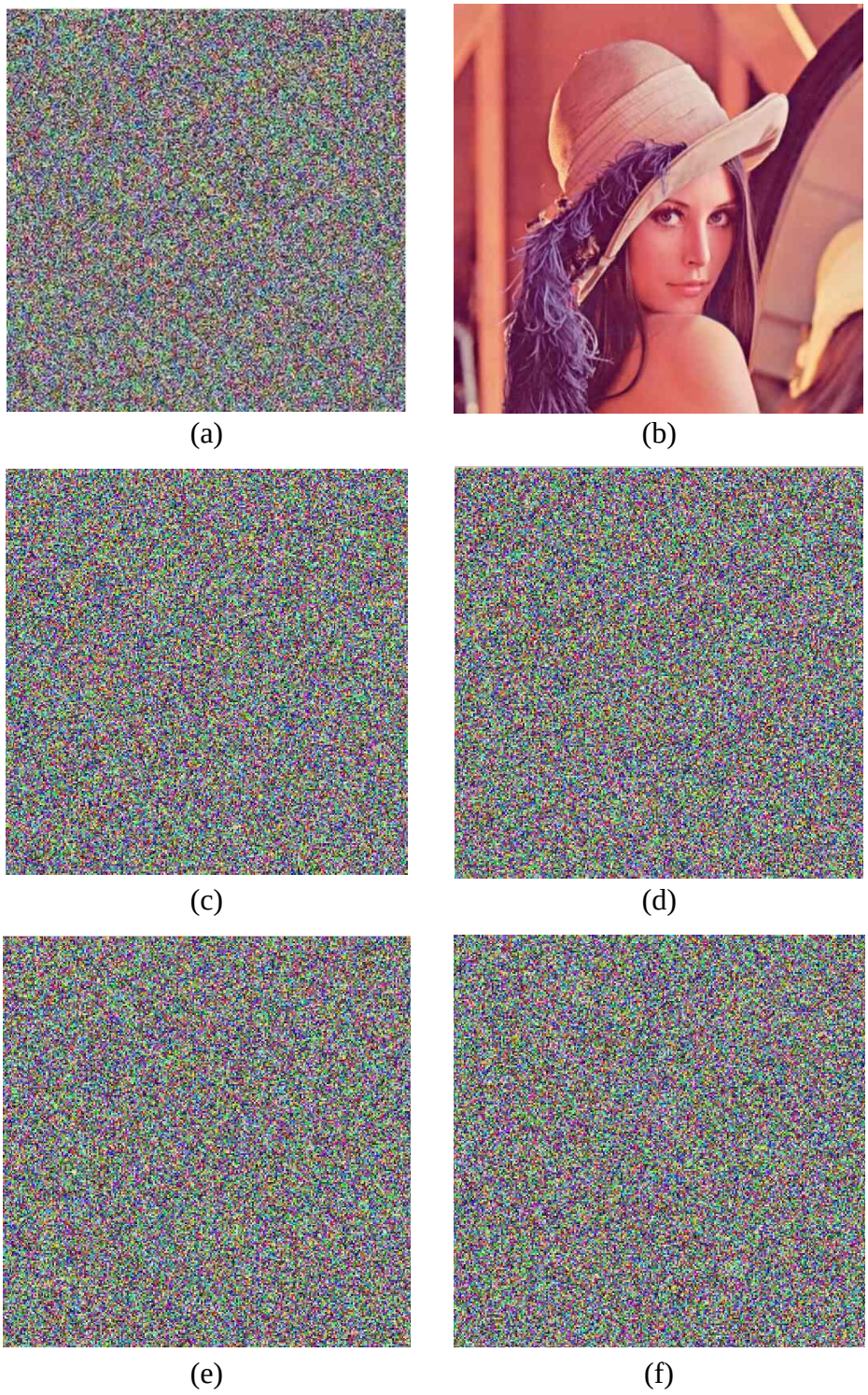
The key sensitivity in the decryption stage is shown in Figure (4.4), the NPCR for associated decrypted images of Figure (4.4) is reported in Table (4.2).

In Table (4.2), the original key is Key, (Key1, Key2, Key3, and Key4) are four modified keys. As a result, the decrypted versions of the image that is encrypt differ from the image that is plain when four slightly modified keys are used to decrypt it, the values of NPCR in Table (4.2) are greater than 99.6%.

Table (4.2): NPCR for associated decrypted images for Figure (4.4) in decryption stage.

	X	Y	Z	W	NPCR (%)
Key	27.84375	31.0625	29.8125	23.640625	0
Key1	27.843**8**5	31.0625	29.8125	23.640625	99.60
Key2	27.84375	31.062**6**	29.8125	23.640625	99.61
Key3	27.84375	31.0625	29.8**2**25	23.640625	99.60
Key4	27.84375	31.0625	29.8125	23.64063**5**	99.62

In summary, the results of the experiments reveal that the suggested technique is extremely sensitive to the secret key. Any little adjustments have an impact on the outcomes of encryption and decryption.



(a) (b)

(c) (d)

(e) (f)

Figure (4.4): Key Sensitivity Analysis of the Decryption Process; (a) Lena's encrypted image; (b) decrypted image with the original decryption key; (c) - (f) utilizing four modified keys to decrypt the image.

4.2.5 Information Entropy Analysis

Ambiguity to understand the encrypted image is one of the most important goals of image encryption. Equation (2.6) is used to compute information entropy, which is then used to test the various images.

Table (4.3) shows the results of the information entropy of all components (R, G, and B) of plain images and encrypted images. Information entropy has a theoretical value of 8 bit and the entropies are all extremely near to the optimal value of 8 bit. As a result, the proposed algorithm exhibits high encrypted image unpredictability, therefore, the proposed algorithm can resist information entropy attacks well.

4.2.6 Correlation Analysis

Neighboring pixels are significantly correlated in the horizontal, vertical, and diagonal directions of the original image. In an ideal encryption technique, the pixels in the encrypted image's correlation coefficients should be low enough to withstand statistical attacks.

Table (4.3): Information entropy analysis.

	Original image (bits)			Encrypted image (bits)		
	R_{com}	G_{com}	B_{com}	R_{com}	G_{com}	B_{com}
Lena	7.1545	7.539	6.8382	7.997	7.9972	7.9971
Baboon	7.7011	7.5129	7.7657	7.9971	7.9976	7.9973
Peppers	7.3902	7.6149	7.0968	7.9974	7.9976	7.9974
Flowers	7.4143	7.2628	7.387	7.9969	7.9965	7.997
Black	0	0	0	7.9972	7.9973	7.9972
White	0	0	0	7.9963	7.9972	7.9965
Average				7.9970		

In order to compare and analyze the neighbor pixels of the plain and encrypted images, we used 50,000 pairs of neighbor pixels that were randomly selected from the plain images and encrypted images. The correlation distribution in three directions of the two neighboring pixels is shown in Figure (4.5), Figure (4.6), and Figure (4.7). As observed, in the plain image, pixels that are adjacent to each other are highly concentrated, meaning there is a strong correlation in the plain image. In the encrypted image, the distributions of adjacent pixels are random, meaning that low correlation exists in the encrypted image.

For an original image, the correlation coefficients are close to one, while, for an encrypted image, the correlation coefficients are close to zero. Table (4.4) reveals that the encrypted image's adjacent pixels have a very low correlation and a good confusion and diffusion properties of the proposed image encryption algorithm.

Table (4.4): Correlation coefficients of the plain images and encrypted images.

	plain image			Encrypted image		
	$H_{\_dir.}$	$V_{\_dir.}$	$D_{\_dir.}$	$H_{\_dir.}$	$V_{\_dir.}$	$D_{\_dir.}$
Lena	0.968	0.986	0.954	0.0016	0.0046	-0.0006
Baboon	0.808	0.758	0.749	-0.0010	0.0026	0.0003
Peppers	0.961	0.962	0.938	-0.0007	0.0068	0.0004
Flowers	0.927	0.951	0.904	0.0046	0.0009	0.0072
Black	1	1	1	0.005	0.0008	-0.0063
White	1	1	1	-0.0007	-0.0064	0.001

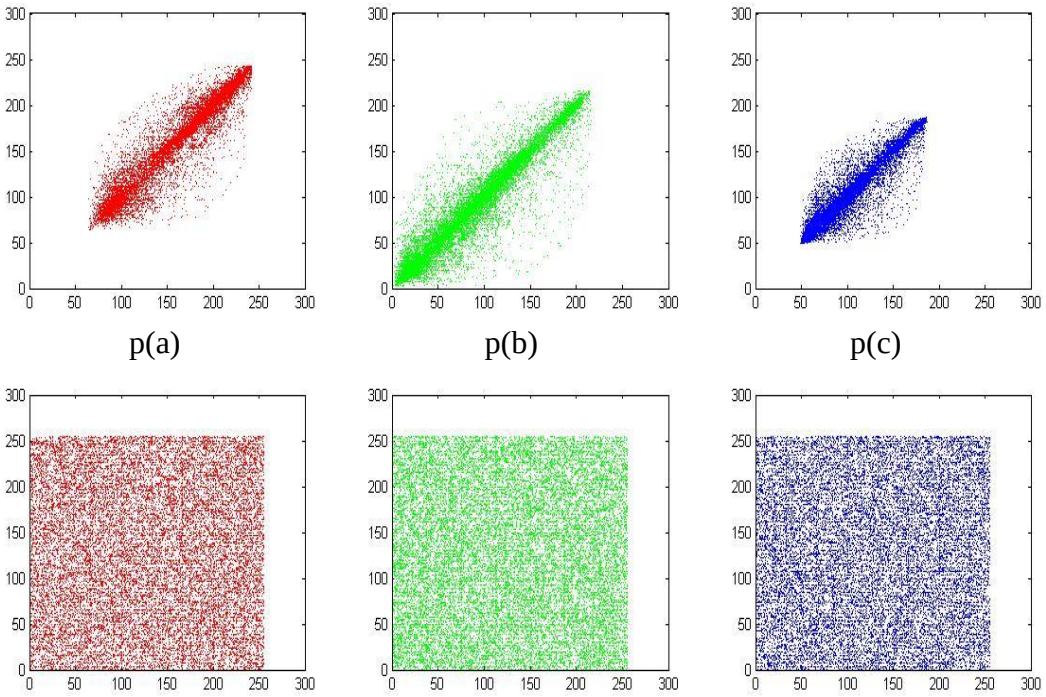


Figure (4.5): Horizontal pixel pair distribution in original and encrypted images; p(a-c) Horizontal distribution in original image, e(a-c) Horizontal distribution in encrypted image.

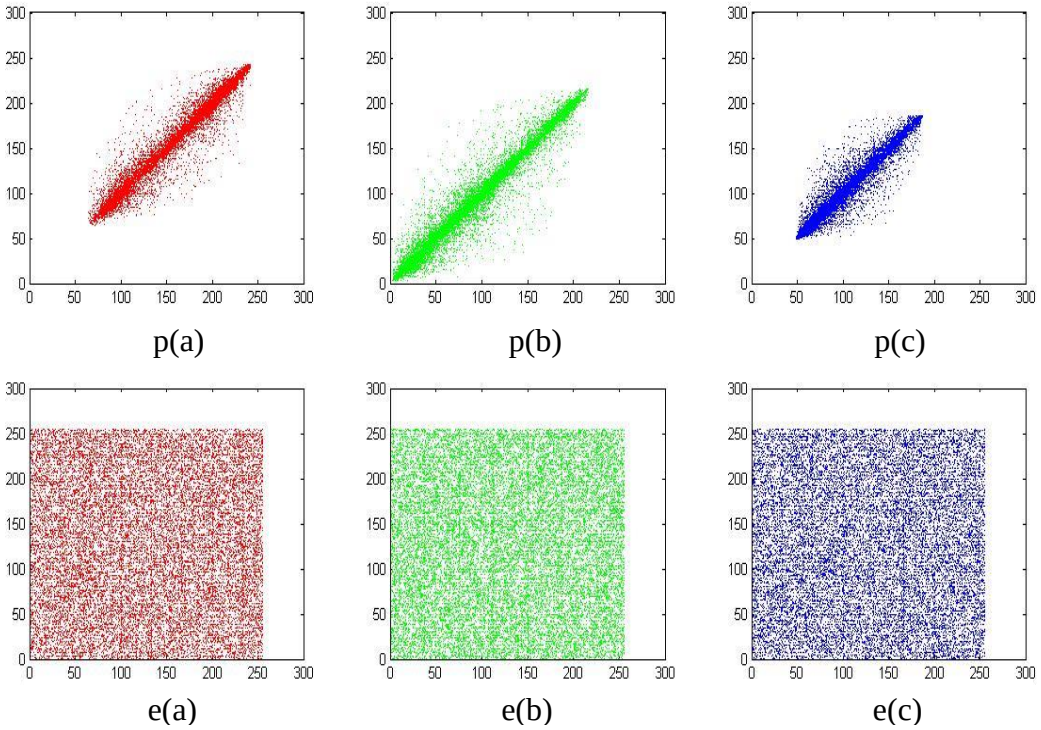


Figure (4.6): Vertical pixel pair distribution in original and encrypted images; p(a-c) Vertical distribution in original image, e(a-c) Vertical distribution in encrypted image.

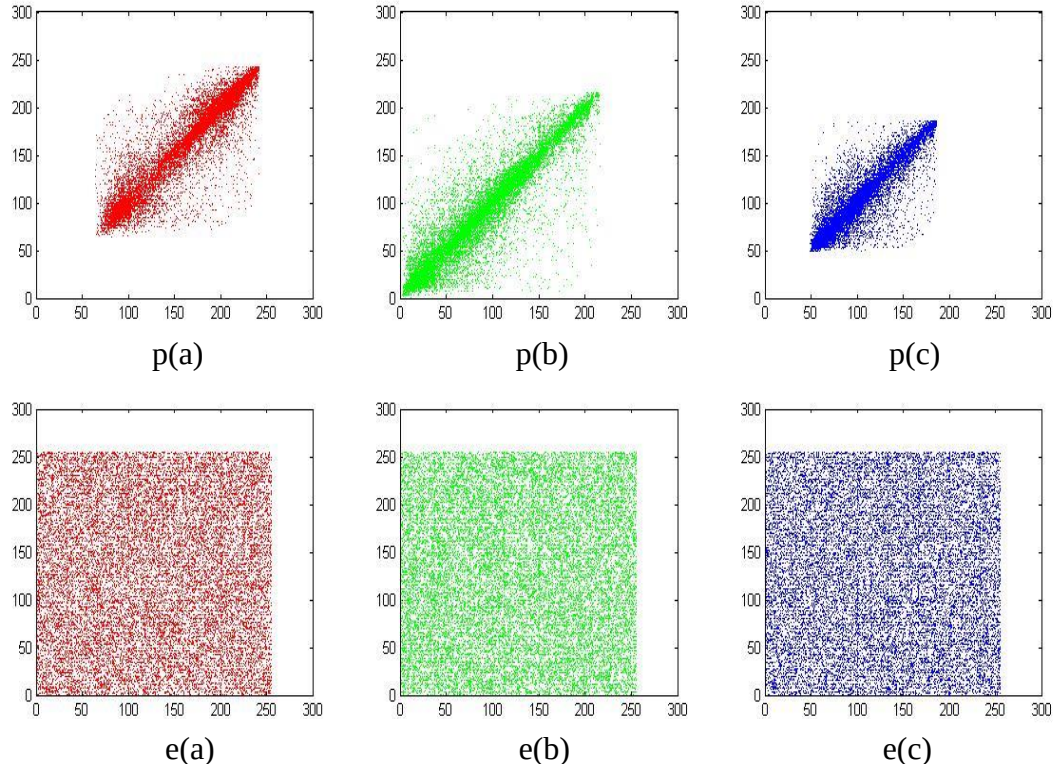


Figure (4.7): Diagonal pixel pair distribution in original and encrypted images; p(a-c) Diagonal distribution in original image, e(a-c) Diagonal distribution in encrypted image.

4.2.7 MSE and PSNR Analysis

MSE and PSNR are used to calculate the difference between the original image and the encrypted image. The quality of an image is commonly evaluated with them; Equations (2.11) and (2.12) defines MSE and PSNR, respectively. encrypted image is indistinguishable by the eye from the original, if the PSNR value is smaller than or equal to 30 dB. Otherwise, the human visual system is capable of detecting the deterioration in quality. In particular, an infinite PSNR value (MSE = 0) indicates that two images are identical. Table (4.5) shows the PSNR values for the test images created with the proposed encryption algorithm. By comparing the original and decrypted images, the PSNR values are always infinite when applying the proposed algorithm, as shown in Table (4.5). In other words, the image after decryption is identical to the original. The greater the value of MSE between the original and the encrypted images, the lower the value of PSNR, the better the encryption algorithm's security effect.

Table (4.5): The MSE and PSNR results between the original and encrypted/ decrypted images: 'O-E' Original and encrypted images and 'O-D' original and decrypted images.

	MSE(O-E)	MSE(O-D)	PSNR(O-E)(dB)	PSNR(O-D)(dB)
Lena	8906	0	8.662	∞
Baboon	8675	0	8.762	∞
Peppers	10058	0	8.168	∞
Flowers	11051	0	7.706	∞
Black	21724	0	4.761	∞
White	21740	0	4.758	∞

4.2.8 Attacks Analysis

4.2.8.1 Differential Attacks

NPCR is a method for calculating the percentage difference in number of pixels between two encrypted images as in Equation (2.13). The UACI was utilized to determine the average intensity of two encrypted images as in Equation (2.14). The capacity of encryption systems to resist differential attacks is demonstrated by their high NPCR and UACI scores.

Table (4.6) shows the results of NPCR and UACI for the proposed algorithm. The average value of NPCR and UACI for the plain images are 99.63% and 33.48%, respectively. It illustrates that NPCR and UACI are extremely close to the intended values. Even if there is only a minor difference in the plain image, it shows a different variant of the encrypted image. As a result, the suggested algorithm has a high level of plain image sensitivity.

Table (4.6): Differential attacks.

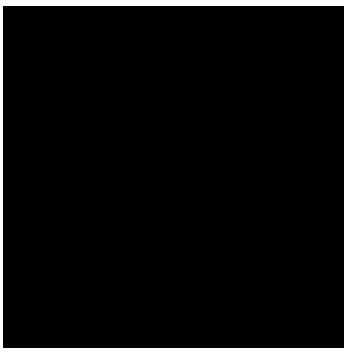
	NPCR (%)				UACI (%)			
	$R_{com.}$	G_{com}	B_{com}	Average	R_{com}	G_{com}	B_{com}	Average
Lena	99.6521	99.6292	99.6277	99.6363	33.394	33.4283	33.5255	33.4492
Baboon	99.6262	99.646	99.6475	99.6399	33.5447	33.5299	33.4846	33.5197
Peppers	99.6078	99.6414	99.6078	99.619	33.5118	33.4692	33.5301	33.5037
Flowers	99.6384	99.6109	99.6246	99.6246	33.4383	33.5318	33.6411	33.5370
Black	99.6338	99.6078	99.6857	99.6424	33.4144	33.4409	33.4828	33.4460
White	99.6216	99.6262	99.6109	99.6195	33.4775	33.3138	33.6032	33.4648
Average				99.6302	Average			33.4867

4.2.8.2 Known Plaintext and Chosen Plaintext Attacks

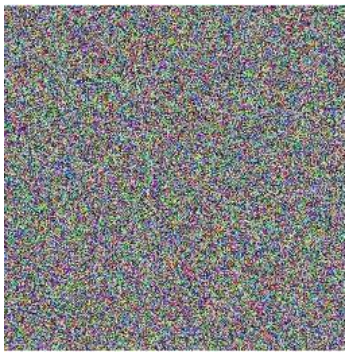
Many image encryption algorithms are vulnerable to attacks, such as, known-plaintext, chosen-plaintext, cipher-text only, and so on. To effectively withstand these attacks, the proposed algorithm addresses the following three issues. At first, for the 4D Lorenz and 4D Rossler map systems, calculating initial values is based on the SHA-256 value of the plain image. The Lorenz sequences, which are associated with the plain image, perform the shuffling. Also, the initial diffusion is performed by the diffusion key, which is built primarily from the plain image. Finally, the ADD operation rules of the image that encoded with DNA are set by Rossler sequence. If the plain image is changed, the chaotic systems have different initial values due to the use of SHA-256 values. As confusion and diffusion change, the final result changes. Therefore, the proposed approach is highly reliant on the plain image and is resistant to both knowing plaintext attack and choosing plaintext attack.

Hackers have been known to attack encryption algorithms by using special plain images, utilize all black or all white images. In reality, special images can make the permutation process invalid revealing the encryption mechanism and therefore rendering the scheme insecure. The original images, and all white and all black encrypted images, as well as, their histograms, are shown in the Figure (4.8). The size of all the images is 256 × 256. Tables (4.3) and (4.4) exhibit all black and white encrypted images' entropies and correlation coefficients, respectively.

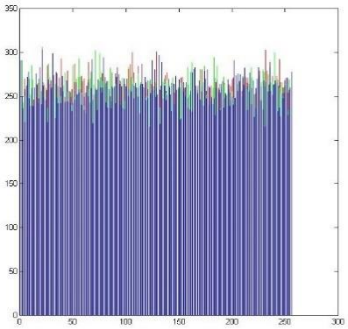
We can observe from the results that the encrypted images have a lot of noise. Additionally, they have a uniform distribution of histograms, entropies that are close to 8, and close to zero correlation coefficients. Thus, the cipher images provide no significant information for attacking the encryption system. Therefore, knowing plaintext attack and choosing plaintext attack can be effectively countered by our encryption technique.



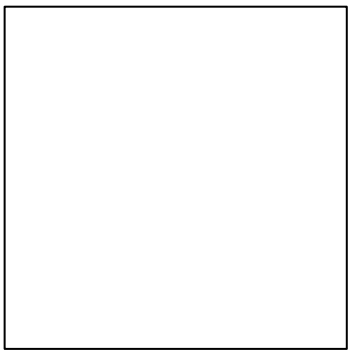
(a) All black.



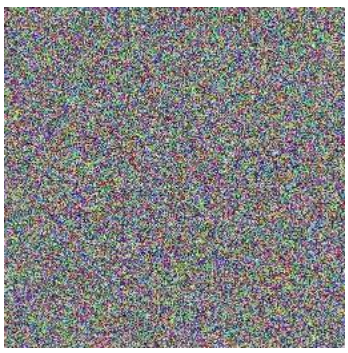
(b) All-black cipher image.



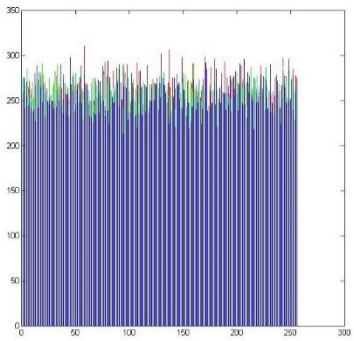
(c) The cipher image's histogram.



(d) All white.



(e) All-white cipher image.

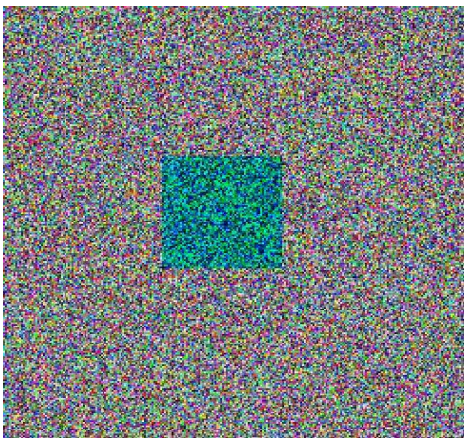


(f) The cipher image's histogram.

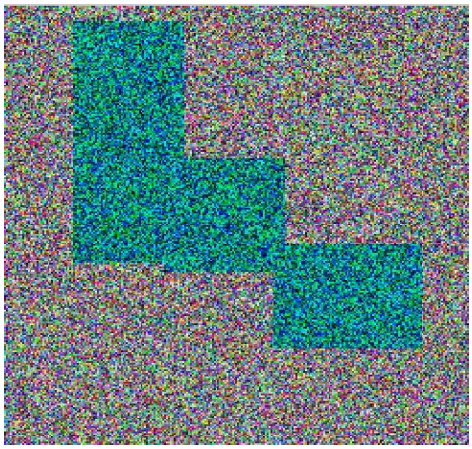
Figure (4.8): Experimental results of known plaintext attack and chosen plaintext attack.

4.2.8.3 Occlusion Attack

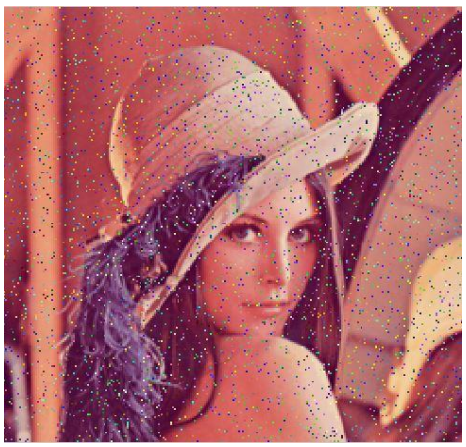
Some data may be lost during the transmission of digital images over networks due to a network congestion or a deliberate destruction. Any optimal encryption algorithm must be resistant to occlusion (data loss) attacks during transmission and storage. The occlusion attack is used to see if it is possible from encrypted images that have lost some information; we can retrieve the original images. To demonstrate the effectiveness of the proposed algorithm against this attack, some information from the encrypted Lena image has been lost, as illustrated in Figure (4.9) (a), and (b). Then, the associated decrypted images are shown in Figure (4.9) (c), and (d), respectively. The figure shows that they are still recognizably identifiable. As a result, the proposed algorithm is resistant to this attack.



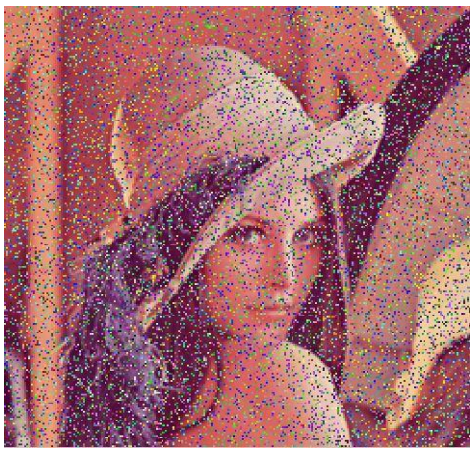
(a) (1/16) Loss data on an encrypted image.



(b) (1/4) Loss data on an encrypted image.



(c) (1/16) Loss data on a decrypted image.



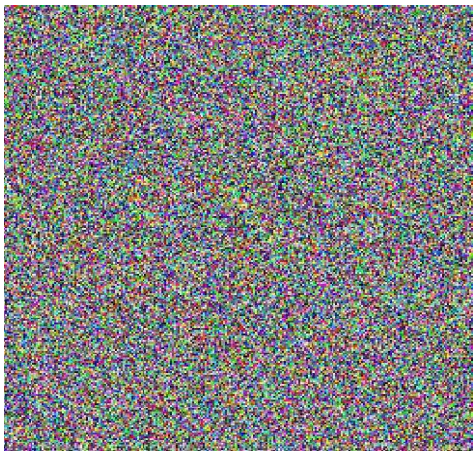
(d) (1/4) Loss data on a decrypted image.

Figure (4.9): Experimental results of occlusion attack.

4.2.8.4 Noise Attack

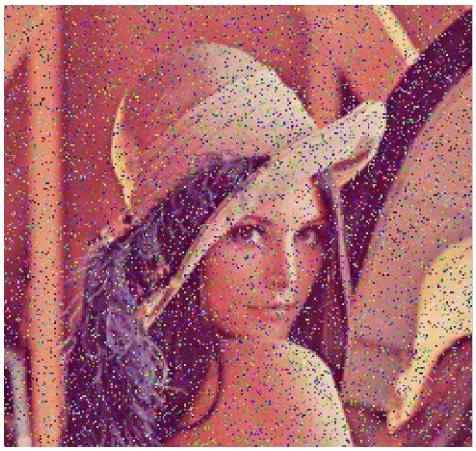
Noise will always have effect on the encrypted image in real communication channels. It is significantly more difficult to recover encrypted images when there is noise on them. Thus, the ability of encryption algorithm to withstand noise attack is, also, a significant factor to consider when evaluating their performance. Figure (4.10) (a), and (b) depicts at two distinct noise densities, encrypted-images are distorted by Salt and Pepper noise, 0.01, and 0.1, respectively. Using the proposed algorithm, noise-tainted encrypted images can be decrypted. The decrypted images are displayed in Figure (4.10) (c), and (d), respectively. From the Figure (4.10), it can be observed that even when the encrypted Lena image is tainted by noise; it can still be accurately decrypted, indicating that the majority of the information can be retrieved.

(a) 0.01 noise adding to encrypted image.



(b) 0.1 noise adding to encrypted image.

(c) Decrypted image after adding 0.01 noise.



(d) Decrypted image after adding 0.1 noise.

Figure (4.10): Experimental results of noise attack.

4.3 Running Time

The speed of the proposed encryption algorithm is a very important factor to measure the efficiency. The proposed algorithm was tested using PC with MATLAB R2013a having operating system 32-bit Windows 8, Intel$^{(R)}$ Core^{TM} i5-4310U 2.60 GHz CPU with 8 GB RAM, and Table (4.7) presents encryption and decryption running time.

Table (4.7): Running time in seconds.

Image	Encryption time	Decryption time
Lena	78	35
Baboon	79	34
Peppers	65	32
Flowers	74	33
Black	54	29
White	50	26

4.4 Comparison

The suggested image encryption algorithm is compared to the performance of competing systems based on a variety of parameters. For simplicity, the image of Lena is used for comparison. The results was shown that the proposed system outperforms other systems in terms of security. The results of the correlation comparison (colored images are calculated by averaging horizontal, vertical, and diagonal red, green, and blue components values), information entropy, NPCR, and UACI are shown in Table (4.8).

Table (4.8): Comparison analysis of Lena image.

Correlation Coefficient					
	Proposed algorithm	Ref.[11]	Ref.[9]	Ref.[27]	Ref.[29]
Corr. H.	**0.0016**	−0.0119	0.007	-0.0061	-0.0082
Corr. V.	**0.0046**	−0.0087	0.0062	0.0067	-0.0128
Corr. D.	**-0.0006**	−0.0045	0.0016	-0.0018	-0.0012
Information Entropy					
	Proposed algorithm	Ref.[11]	Ref.[9]	Ref.[29]	Ref.[28]
Entropy	**7.9971**	7.9896	7.9913	7.9896	7.9894
Differential Attacks					
	Proposed algorithm	Ref.[11]	Ref.[14]	Ref.[27]	Ref.[30]
NPCR %	**99.63**	99.61	99.61	99.61	99.59
UACI %	**33.44**	32.20	33.42	33.40	33.42

4.5 Limitations of Our Work

This thesis includes a successful implementation of the proposed image encryption algorithm. However, there are several limitations that need to be addressed in the future. The limitations could include the following:

1- Because the proposed encryption algorithm's secret keys include vital and confidential data. During the transmission of secret keys, we should keep security in mind.

2- We only applied four types of attack methods to the encrypted images in order to assess the performance of the suggested encryption method; other attack methods should be considered, so that, the robustness of the proposed algorithm may be analyzed more thoroughly.

3- In this study work, six images were employed as the dataset for image encryption; in the future, we will explore more example images.

4- The DNA-based image encryption system has a slow computational speed and take time to implement, which could make it difficult to use in practice.

4.6 Summary

As consequence of simulation results and the security analysis, two hyper-chaotic systems with DNA encoding produced an efficient color image encryption has the following results:

- It is clear that the encrypted image's histogram has been uniformly distributed. It can be concluded that the suggested algorithm is effective at thwarting the histogram attack.
- Key space of 2^{200}, which is large enough to withstand attacks.
- Sensitivity to secret keys in both stages encryption and decryption. It is reveal that any little adjustments have an impact on the encryption and decryption results.
- Entropy has average value of 7.9970, which is quite near to the optimum value. Therefore, the proposed algorithm can resist information entropy attacks well.
- The correlation between neighboring pixels has been minimized to withstand statistical attacks in the vertical, horizontal, and diagonal directions.
- Greater value of MSE between the original and the encrypted images, and lower value of PSNR, which means that the encryption algorithm's security is good.

Additionally, the experimental results showed that the proposed algorithm could withstand different attacks, such as:

- The average value of NPCR and UACI for the plain images are 99.63% and 33.48%, respectively, this means that the proposed algorithm can resist differential attacks well.
- Knowing plaintext attack and choosing plaintext attack can be effectively countered by our encryption technique.
- The proposed algorithm counters various levels of occlusion (data loss) and noise attacks.

In addition, the original image was restored without any noise and guaranteed a good degree of quality of the obtained image with infinite value for PSNR and zero for MSE when comparison the decrypted images with the original images.

Chapter Five

Conclusions and Future Works

5.1 Conclusions

This thesis has analyzed an image cryptosystem that used hyper-chaotic systems and a variety of technologies. To generate eight sequences, hyper-chaotic systems were properly utilized, four of them are used to scramble the pixel locations and break up the correlations between them (confusion process). The other four are used to change the value of pixels (diffusion process). Additional techniques, such as, SHA-256 and SHA-384 are used to work as a source of strength for plain image sensitivity by confounding the relationship between the plain image and the initial conditions values of hyper-chaotic systems. While, the technique of DNA coding is employed to improve the cryptosystem's security.

Simulations and comparisons have also verified the security of the proposed encryption algorithm from four aspects: the exhaustive attack, the statistical attack, the differential attack and the known plaintext and chosen-plaintext attacks. The algorithm has a large key space and is extremely sensitive to its keys. Thus, it can resist exhaustive attack. The histogram of the scheme is uniform. The correlation coefficient is close to 0, and the entropy value is close to 8. Thus, the scheme can resist statistical attack. Both UACI and NPCR values approach their ideal values, which illustrates that the proposed scheme can resist differential attacks. The all-white and all-black image experiment also illustrates that the proposed algorithm can resist the known-plaintext and chosen plaintext attacks. All of the above findings demonstrate that the proposed scheme is efficient and practical in communications

5.2 Future Works

The following is a summary of the thesis's future works:

1- The algorithm discussed in this thesis, also, can be extended to video and speech encryption.

2- It is advised that image encryption algorithm be combined with image data compression technology to achieve image security with suitable compression.

3- Initializing a new hyper-chaotic system with high precision control values is an important aspect of chaotic encryption for the purpose of expanding key space and increasing the security.

4- The proposed algorithm consumes elapsed time due to the complexity of the encryption algorithm, it is suggested that the system be implemented using a parallel manner, which can save time while encrypt the images.

References

[1] C. Li, G. Luo, and C. Li, “An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map.,” *Int. J. Netw. Secur.*, vol. 21, no. 1, pp. 22–29, 2019.

[2] D. A. Trujillo-Toledo, D. A. Trujillo-Toledo, O. R. López-Bonilla, E. E. García-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, E. Inzunza-González , “Real-time RGB Image Encryption for IoT Applications Using Enhanced Sequences From Chaotic Maps,” *Chaos, Solitons & Fractals*, vol. 153, pp. 111506, 2021.

[3] V. Kakkad, M. Patel, and M. Shah, “Biometric Authentication and Image Encryption for Image Security in Cloud Framework,” *Multiscale Multidiscip. Model. Exp. Des.*, vol. 2, no. 4, pp. 233–248, 2019.

[4] X. Wang and L. Liu, “Image Encryption Based on Hash Table Scrambling and DNA Substitution,” *IEEE Access*, vol. 8, pp. 68533–68547, 2020.

[5] J. Zhang and D. Huo, “Image Encryption Algorithm Based on Quantum Chaotic Map and DNA Coding,” *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 15605–15621, 2019.

[6] K. Suneja, S. Dua, and M. Dua, “A Review of Chaos Based Image Encryption,” in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019, pp. 693–698.

[7] D. Ravichandran, S. Fathima, V. Balasubramanian, A. Banu, and R. Amirtharajan, “DNA and Chaos Based Confusion-Diffusion for Color Image Security,” in *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 2019, pp. 1–6.

[8] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, “A Novel Color Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System,” *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.

[9] P. Liu, T. Zhang, and X. Li, “A New Color Image Encryption Algorithm Based on DNA and Spatial Chaotic Map,” *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 14823–14835, 2019.

[10] A. K. Shibeeb, M. H. Ahmed, and A. H. Mohammed, “A New Chaotic Image Cryptosystem Based on Plaintext-Associated Mechanism and Integrated Confusion-Diffusion Operation,” *Karbala Int. J. Mod. Sci.*, vol. 7, no. 3, pp. 2, 2021.

[11] Q. Liu and L. Liu, “Color Image Encryption Algorithm Based on DNA Coding and

Double Chaos System," *IEEE Access*, vol. 8, pp. 83596–83610, 2020.

[12] J. Wu, X. Liao, and B. Yang, "Image Encryption Using 2D Hénon-Sine Map and DNA Approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[13] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-Based Image Encryption Scheme," *Inf. Sci. (Ny).*, vol. 520, pp. 130–141, 2020.

[14] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences," *Entropy*, vol. 22, no. 2, pp. 158, 2020.

[15] L. M. Adleman, "Molecular Computation of Solutions to Combinatorial Problems," *Science (80-.).*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[16] A. Vikram, S. Kalaivani, and G. Gopinath, "A Novel Encryption Algorithm based on DNA Cryptography," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, 2019, pp. 1004–1009.

[17] S. Patel, K. P. Bharath, and R. Kumar, "Symmetric Keys Image Encryption and Decryption Uusing 3D Chaotic Maps With DNA Encoding Technique," *Multimed. Tools Appl.*, vol. 79, no. 43, pp. 31739–31757, 2020.

[18] T. Sivakumar and R. Venkatesan, "A Novel Image Encryption Approach Using Matrix Reordering," *WSEAS Trans. Comput.*, vol. 12, no. 11, pp. 407–418, 2013.

[19] F. Pub, "Data Encryption Standard (DES)," *FIPS PUB*, pp. 43–46, 1999.

[20] J. Nechvatal *et al.*, "Report on the Development of the Advanced Encryption Standard (AES)," *J. Res. Natl. Inst. Stand. Technol.*, vol. 106, no. 3, pp. 511, 2001.

[21] L. Chen, H. Yin, L. Yuan, J. A. T. Machado, R. Wu, and Z. Alam, "Double Color Image Encryption Based on Fractional Order Discrete Improved Henon Map and Rubik's Cube Transform," *Signal Process. Image Commun.*, vol. 97, pp. 116363, 2021.

[22] L. Y. Zhang; Y. Liu; F. Pareschi; Y. Zhang; K. Wong; R. Rovatti, and G. Setti, "On the Security of a Class of Diffusion Mechanisms for Image Encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, 2017.

[23] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020.

[24] A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi J. Sci.*, pp. 324–337, 2022.

[25] R. Rimani, N. H. Said, A. Ali-Pacha, and J. A. L. Ramos, "An Efficient Image

Encryption Using a Dynamic, Nonlinear and Secret Diffusion Scheme," *Baghdad Sci. J.*, vol. 18, no. 3, pp. 628, 2021.

[26] A. A. Al-Hussein, "Chaos Phenomenon in Power Systems : A Review," *Iraqi J. Elecrrical Electron. Eng.*, vol. 17, no. 2, 2021.

[27] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, and M. Hanif, "On the Image Encryption Algorithm Based on the Chaotic System, DNA Encoding, and Castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[28] X. Wu, J. Kurths, and H. Kan, "A Robust and Lossless DNA Encryption Scheme for Color Images," *Multimed. Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, 2018.

[29] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color Image DNA Encryption Using NCA Map-Based CML and One-Time Keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[30] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A Novel Color Image Encryption Scheme Using DNA Permutation Based on the Lorenz System," *Multimed. Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, 2018.

[31] H. R. Shakir, "A Color-Image Encryption Scheme Using a 2D Chaotic System and Dna Coding," *Adv. Multimed.*, vol. 2019, 2019.

[32] H. R. Amani and M. Yaghoobi, "A New Approach in Adaptive Encryption Algorithm for Color Images Based on DNA Sequence Operation and Hyper-Chaotic System," *Multimed. Tools Appl.*, vol. 78, no. 15, pp. 21537–21556, 2019.

[33] T. S. Ali and R. Ali, "A New Chaos Based Color Image Encryption Algorithm Using Permutation Substitution and Boolean Operation," *Multimed. Tools Appl.*, vol. 79, no. 27–28, pp. 19853–19873, 2020.

[34] S. Mozaffari, "Parallel Image Encryption With Bitplane Decomposition and Genetic Algorithm," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25799–25819, 2018.

[35] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, 2012, pp. 1–5.

[36] A. Kumar and N. S. Raghava, "An EfficientImage Encryption Scheme Using Elementary Cellular Automata with Novel Permutation Box," *Multimed. Tools Appl.*, vol. 80, no. 14, pp. 21727–21750, 2021.

[37] L. A. Shihab, "Technological Tools for Data Security in the Treatment of Data Reliability in Big Data Environments," *Int. Trans. J. Eng. Manag. Appl. Sci. Technol.*, vol. 11, no. 9, pp. 1–13, 2020.

[38] K. R. Saraf and M. P. Jesudason, “Encryption Principles and Techniques for the Internet of Things,” in *Cryptographic security solutions for the internet of things*, IGI Global, 2019, pp. 42–66.

[39] R. Mishra, J. K. Mantri, and S. Pradhan, “New Multiphase Encryption Scheme for Better Security Enhancement,” in *IOT with Smart Systems*, Springer, 2022, pp. 599–606.

[40] K. A. Rajan, “Use of Transposition Cipher and its Types,” *Int. J. Res. Eng. Sci. Manag.*, vol. 4, no. 11, pp. 164–165, 2021.

[41] R. R. Salavi, M. M. Math, and U. P. Kulkarni, “A Survey of Various Cryptographic Techniques: From Ttraditional Cryptography to Fully Homomorphic Encryption,” in *Innovations in Computer Science and Engineering*, Springer, 2019, pp. 295–305.

[42] B. Stoyanov and G. Nedzhibov, “Symmetric Key Encryption Based on Rotation-Translation Equation,” *Symmetry (Basel).*, vol. 12, no. 1, pp. 73, 2020.

[43] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, “The Design and FPGA-Based Implementation of a Stream Cipher Based on a Secure Chaotic Generator,” *Appl. Sci.*, vol. 11, no. 2, pp. 625, 2021.

[44] A. H. Zahid, E. Al-Solami, and M. Ahmad, “A Novel Modular Approach Based Substitution-Box Design for Image Encryption,” *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

[45] W.-L. Tai and Y.-F. Chang, “Separable Reversible Data Hiding in Encrypted Signals With Public Key Cryptography,” *Symmetry (Basel).*, vol. 10, no. 1, pp. 23, 2018.

[46] D. Suhag, S. S. Gaur, and A. K. Mohapatra, “A Proposed Scheme to Achieve Node Authentication in Military Applications of Wireless Sensor Network,” *J. Stat. Manag. Syst.*, vol. 22, no. 2, pp. 347–362, 2019.

[47] S. A. Mehdi and Z. L. Ali, “Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper-Chaotic System,” *Al-Mustansiriyah J. Sci.*, vol. 31, no. 1, pp. 54, 2020.

[48] M. Khan and F. Masood, “A Novel Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps,” *Multimed. Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, 2019.

[49] S. A. Fadhel, Z. N. Al-Kateeb, and M. J. AL-Shamdeen, “An Improved Data Hiding Using Pixel Value Difference Method and Hyperchaotic System,” in *Journal of Physics: Conference Series*, 2021, vol. 1879, no. 2, pp. 22089.

[50] E. N. Lorenz, “Deterministic Nonperiodic Flow,” *J. Atmos. Sci.*, vol. 20, no. 2, pp.

130–141, 1963.

[51] M. Kalra, S. Katyal, and R. Singh, “A Tent Map and Logistic Map Based Approach for Chaos-Based Image Encryption and Decryption,” in *Innovations in Computer Science and Engineering*, Springer, 2019, pp. 159–165.

[52] S. Vaidyanathan, V. Tech, and V. Tech, “Anti-Synchronization of the Hyperchaotic Lorenz Systems by Sliding Mode Control,” *Int. J. Comput. Sci. Eng.*, vol. 2021, no. September, 2015.

[53] X. Wang and M. Wang, “A Hyperchaos Generated from Lorenz System,” *Phys. A Stat. Mech. its Appl.*, vol. 387, no. 14, pp. 3751–3758, 2008.

[54] O. E. Rössler, “An Equation for Continuous Chaos,” *Phys. Lett. A*, vol. 57, no. 5, pp. 397–398, 1976.

[55] O. Rossler, “An Equation for Hyperchaos,” *Phys. Lett. A*, vol. 71, no. 2–3, pp. 155–157, 1979.

[56] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, “A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals,” *IEEE Access*, vol. 7, pp. 74734–74746, 2019.

[57] J. Zheng and J. Li, “Synchronization of a Class of Chaotic Systems with Different Dimensions,” *Complexity*, vol. 2021, 2021.

[58] J. K. Panjiyar, “From Punch Card to DNA Data Storage,” 2018. https://medium.com/zerone-magazine/from-punch-card-to-dna-data-storage-5c15dcc4803e.

[59] X. Zhang and Y. Hu, “Multiple-Image Encryption Algorithm Based on the 3D Scrambling Model and Dynamic DNA Coding,” *Opt. Laser Technol.*, vol. 141, pp. 107073, 2021.

[60] F. Akram, H. Ali, and A. T. Laghari, “Trends to Store Digital Data in DNA: an Overview,” *Mol. Biol. Rep.*, vol. 45, no. 5, pp. 1479–1490, 2018.

[61] S. M. Abdullah and I. Q. Abduljaleel, “Speech Encryption Technique Using S - Box Based on Multi Chaotic Maps,” *TEM J.*, vol. 10, no. 3, pp. 1429–1434, 2021.

[62] M. I. Mihailescu and S. L. Nita, “Hash Functions,” in *Cryptography and Cryptanalysis in MATLAB*, Springer, 2021, pp. 83–102.

[63] A. S. Shaik, R. K. Karsh, M. Islam, and R. H. Laskar, “A Review of Hashing Based Image Authentication Techniques,” *Multimed. Tools Appl.*, pp. 1–28, 2021.

[64] L. V Cherckesova, O. A. Safaryan, N. G. Lyashenko, and D. A. Korochentsev, “Developing a New Collision-Resistant Hashing Algorithm,” *Mathematics*, vol. 10,

no. 15, pp. 2769, 2022.

[65] G. V. Priya and K. P. Babu, "Chaos Based Encryption on Image with Hash Function Implementation," *Chaos*, vol. 2, no. 3, 2021.

[66] N. Mol, "Design of an HMAC Co-Processor Unit Based on SHA-2 Family of Hash Functions," *Int. J. Eng. Res.*, vol. 3, no. 3, 2014.

[67] R. Shelke and S. Metkar, "Image Scrambling Methods for Digital Image Encryption," in *2016 International Conference on Signal and Information Processing (IConSIP)*, 2016, pp. 1–6.

[68] Y. P. K. Nkandeu and A. Tiedeu, "An Image Encryption Algorithm Based on Substitution Technique and Chaos Mixing," *Multimed. Tools Appl.*, vol. 78, no. 8, pp. 10013–10034, 2019.

[69] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Robust Medical Image Encryption Based on DNA-chaos Cryptosystem for Secure Telemedicine and Healthcare Applications," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 10, pp. 9007–9035, 2021.

[70] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing Against Brute-Force Attack: A Hash-Based RFID Mutual Authentication Protocol Using a Secret Value," *Comput. Commun.*, vol. 34, no. 3, pp. 391–397, 2011.

[71] M. Jarjar, S. Hraoui, S. Najah, and K. Zenkouar, "New Technology of Color Image Encryption Based on Chaos and Two Improved Vigenère Steps," *Multimed. Tools Appl.*, pp. 1–25, 2022.

[72] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," *Complexity*, vol. 2020, 2020.

[73] S. Ihara, *Information Theory for Continuous Systems*, vol. 2. World Scientific, 1993.

[74] M. Zhou and C. Wang, "A Novel Image Encryption Scheme Based on Conservative Hyperchaotic System and Closed-loop Diffusion Between Blocks," *Signal Processing*, vol. 171, pp. 107484, 2020.

[75] J. Xu, B. Zhao, and Z. Wu, "Research on Color Image Encryption Algorithm Based on Bit-Plane and Chen Chaotic System," *Entropy*, vol. 24, no. 2, pp. 186, 2022.

[76] Hameed A. Yoirnis, Turki Y. Abdalla, "Hiding Processing Approaches For Digital Images Encryption Using Wavelet Transform." Basrah Journal for Engineering Science, vol. 8, no. 1, pp. 1-12, 2008.

[77] Y. Sun, H. Zhang, X. Wang, and M. Wang, "Bit-Level Color Image Encryption Algorithm Based on Coarse-Grained Logistic Map and Fractional Chaos," *Multimed.*

Tools Appl., vol. 80, no. 8, pp. 12155–12173, 2021.

[78] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain, and M. Asif, "An Efficient Image Encryption Scheme Based on Double Affine Substitution Box and Chaotic System," *Integration*, vol. 81, pp. 108–122, 2021.

[79] D. S. Laiphrakpam and M. S. Khumanthem, "Medical Image Encryption Based on Improved ElGamal Encryption Technique," *Optik (Stuttg).*, vol. 147, pp. 88–102, 2017.

[80] A.-V. Diaconu and A. C. Dascalescu, "Correlation Distribution of Adjacent Pixels Randomness Test for Image Encryption," in *Proc. Rom. Acad. Ser. A*, 2017, vol. 18, pp. 351–360.

[81] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image Encryption-then-Transmission Using DNA Encryption Algorithm and the Double Chaos," *IEEE Photonics J.*, vol. 10, no. 3, pp. 1–15, 2018.

[82] B. D. Parameshachari, "Logistic Sine Map (LSM) Based Partial Image Encryption," in *2021 National Computing Colleges Conference (NCCC)*, 2021, pp. 1–6.

[83] "The USC-SIPI Image Database." https://sipi.usc.edu/database/.

List of Publications

Accepted Papers

[1] Ghofran Kh. Shraida and Hameed A. Younis "An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences," Iraqi Journal for Electrical and Electronic Engineering.

[2] Ghofran Kh. Shraida and Hameed A. Younis "A Review of DNA-Based Color Image Encryption Algorithms," Iraqi Journal of Intelligent Computing and Informatics.

[3] Ghofran Kh. Shraida and Hameed A. Younis "Chaotic-Based Color Image Encryption Algorithms: A Review," Journal of Basrah Researches (Sciences).

المستخلص

جذبت تقنية تشفير الصور الملونة باستخدام الانظمة الفوضوية وقواعد الحمض النووي (DNA) انتباه الباحثين العلميين مؤخرًا. أصبح محتوى الوسائط المتعددة، والذي يتمثل جوهره في الصورة الملونة، عنصرًا مهمًا في نقل المعلومات. هذا يعني أنه يجب نقل محتويات الوسائط المتعددة مثل الصوت والفيديو والصور عبر قنوات الاتصال بأمان باستخدام تقنيات تشفير كفوءة.

تعد نظرية الفوضى موضوعًا شائعًا في الأنظمة الديناميكية غير الخطية نظرًا لخصائصها مثل الدورية والحساسية لمعلمات البداية والتحكم. ان الانظمة شديدة الفوضى مفيدة في إنشاء تسلسلات شبه عشوائية للتشفير. اضافة الى ذلك، فإن تقنية تشفير الحمض النووي (DNA) تمتلك خصائص مثل التوازي الواسع وسعة التخزين الكبيرة مما يجعلها مجالًا واعدًا. تستخدم الخوارزميات القائمة على الحمض النووي (DNA) والانظمة الفوضوية مزايا كلا المجالين لتوفير حماية فعالة للصور.

تقدم هذه الرسالة خوارزمية فعالة لتشفير الصور الملونة من خلال أنظمة شديدة الفوضى (Lorenz and Rossler) وتشفير الحمض النووي (DNA). ان الخوارزمية المقترحة تتكون من ثلاث خطوات:

أولاً، يتم تحديد المعلمات الأولية للأنظمة مفرطة الفوضى بالاعتماد على قيمة دالة التجزئة (SHA-256/384) والتي يتم إنشاؤها من الصورة الاصلية لتجنب هجمات النص الاصلي.

ثانيًا، يتم توليد سلاسل فوضوية من نظام Lorenz تحول الصورة الأصلية الملونة إلى صورة مشوشة عن طريق خلط مواقع البكسلات لطبقات الصورة الملونة الثلاثة (الأحمر والأخضر والأزرق) باستخدام مفتاح الخلط.

واخيرا، يتم تطبيق ترميز الحمض النووي باستخدام قواعد معينة على المكونات المشوشة والسلاسل الفوضوية المولدة من نظام Rossler. اجراء عملية الجمع بين المكونات المرمزة. وبعدها تطبيق عملية XOR بين مكونات الحمض النووي للصورة وتسلسلات الحمض النووي التي تم إنشاؤها بناءً على نظام Rossler. أخيرًا، فك تشفير الحمض النووي لمكونات الصورة، وبالتالي، يتم إنشاء الصورة النهائية المشفرة.

تظهر النتائج التجريبية أن طريقة التشفير المقترحة يمكن أن تلبي معايير الأمان المطلوبة. حيث أسفرت عن قيمة الانتروبي 7.997 بت، فضاء المفتاح 2^{200}، معامل الارتباط يقترب من الصفر. وتم التحقق من فعالية الطريقة المستخدمة من خلال العديد من التقييمات، حيث أظهرت النتائج أنها

مقاومة وفعالة ضد الهجمات منها الهجمات الإحصائية وهجمات القوة الغاشمة. علاوة على ذلك، تعد الخوارزمية المقترحة أكثر كفاءة عند مقارنتها بالعديد من خوارزميات تشفير الصور الملونة السابقة.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة البصرة
كلية علوم الحاسوب وتكنولوجيا المعلومات

طريقة تشفير صور ملونة فعالة باستخدام تسلسل الحمض النووي وتشفير الفوضى

رسالة ماجستير

مقدمة الى مجلس كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة البصرة

وهي جزء من متطلبات نيل شهادة الماجستير في علوم الحاسوب

في تخصص امنية المعلومات

من قبل

غفران خالد شريدة

(بكالوريوس علوم الحاسوب 2013)

بأشراف

أ. د حميد عبد الكريم يونس

حزيران 2022 م

ذو القعدة 1443 هـ