Ministry of Higher Education and
Scientific Research
University of Babylon
College of Science for Women
Department of Computer Science

Hybrid Method of Image Encryption Using DNA and Chaotic Map

A Thesis

Submitted to the Council of the College of Science for Women at the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Science/ Computer Science

By

Mohammed Jasim Najim Al-masoudi

Supervised by

Dr: Sahar Adill Kadhum

2022 A.D. **1444 A.H**

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿قَالُواْ سُبۡحَٰنَكَ لَا عِلۡمَ لَنَآ إِلَّا مَا عَلَّمۡتَنَآۖ
إِنَّكَ أَنتَ ٱلۡعَلِيمُ ٱلۡحَكِيمُ ٣٢﴾

صدق الله العلي العظيم

سورة البقرة/ أية (٣٢)

Supervisor Certification

I certify that this thesis entitled “Hybrid Method of Image Encryption Using DNA and Chaotic Map” was done by (Mohammed Jasim Najim Al-masoudi) under my supervision.

Signature:
Name: Asst. Prof. Dr: Sahar Adill Kadhum
Date: / /2022
Address: University of Babylon /College of Science for Women

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled “Hybrid Method of Image Encryption Using DNA and Chaotic Map” for debate by the examination committee.

Signature:

Name: Asst. Prof. Dr: Saif Alalak

Date: / /2022

Address: University of Babylon /College of Science for Women

Dedication

Thanks are to ALLAH in the first and last place, my Creator, To the teacher and messenger, Mohammed (May Allah blesses and grants him) and his progeny, who taught us the purpose of life...

To my beloved family who encourages and supports me. My dear father, mother, brothers, my wife and my children. To all the people in my life...

Iraqi martyrs who sacrificed for honor and dignity...

I dedicate this thesis.

Mohammed Jasim Najim Al-masoudi

Acknowledgments

Praise and thanks to Allah who enabled me to complete my thesis and facilitated the difficulties for me. Thanks are to all my teachers in the College of Science for Women; particularly I am highly indebted expressing my thanks to the supervisor on this thesis **Dr. Sahar Adill Kadhum** for her excellent guidance and encouragement to complete my thesis.

I would like to thank my dear father and mother, brothers, sisters, my wife, and my children for their love, patience, and understanding to spend my time on this research. This accomplishment would not have been possible without them. Finally, I would like to thank all my friends and all the people who helped me during my Master's study.

Abstract

The rapid spread of the network applications over almost all the fields of daily life requires greater security of the data. Recently, there are greater demand for digital world in different forms. Digital images are one such form that has become more important. Securing image data is challenging due computational requirements for encryption and decryption processes. Also, conventional encryption standard algorithms are not secure enough in case of digital images because of the special characteristics of the images like high redundancy of information, high correlation among the pixels. In order to cope with these concerns, innovative image encryption techniques are required such as chaotic theory, deoxyribonucleic acid molecular (DNA) concepts have become popular to ensure image security.

In this thesis, encryption/decryption methods based on a hyper-chaotic and dynamic DNA coding techniques are proposed to produce an efficient image encryption scheme. This represented in partially encrypting using 2D Henon map, DNA map, and a dynamic DNA coding; by decomposing the original greyscale image plane to two planes (MSB, LSB), where MSB is the main concern for the partial encryption algorithm. The algorithm combine chaotic theory and DNA computing under a scenario includes three types encryption algorithm (2D-Henon, DNA, and mix (Henon-DNA)), each type includes two rounds: first round: generate encryption keys. The second round: stamp the first pixel of MSB by initial value as trade stamp for this plane to be encrypted by the generated keys. The stamping step to help the receiver in checking the ciphered image if it cracked or not.

While the DNA has been used in this thesis into two directions, firstly: generate encryption keys using DNA sequential from National Center for Biotechnology Information (NCBI) maximizing the length matching algorithm to provide immunity against attacks. The second direction, as a dynamic coding

rules mechanism. This mechanism apply another secure facility in not predicating or getting the scenario of image encryption manner.

The experiments are conducted on different standard images with different characteristics. These gray images of size 256×256 of different types. To ensure improved encryption algorithm

The performance evaluation of the proposed algorithm security and effectiveness was measured through a series of tests such as: visual test presented by histogram analysis, correlation, information entropy, NPCR, UACI, and PSNR measurements applied to the three types of encryption with the comparison. The results shows in chapter four that the DNA mapping override the problems the Henon map that suffering from lack complete confusion to images of high redundancy of information, high correlation among the pixels.

Table of Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

1D	One Dimensions
2D	Two Dimensions
A	Adenine
AES	Advanced Encryption Standard
C	Cytosine
CHM	Chaotic Henon Map
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DNA	Deoxyribose Nucleic Acid
G	Guanine
HCMM	Henon–Chebyshev Modulation Map
HSM	Henon-Sine Map
LSB	Least Significant Bit
LSMM	Low Skeletal Muscle Mass
MSB	Most Significant Bit
MSE	Mean Squared Error
NCBI	National Center for Biotechnology Information
NPCR	Number Of Pixels Change Rate
PRBNG	Pseudo Random Binary Number Generator
PSNR	Peak Signal-to-Noise Ratio
ROI	Region Of Interest

RSA	Rivets Shamir and Adelman
S-box	substitution box
SHA-512	Secure Hash Algorithm-512
SIE	Selective Image Encryption
T	Thymine
UACI	unified average changing intensity

CHAPTER ONE

INTRODUCTION

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Network technologies are used for transmitting various media of digital data through them. One the digital data media is images. Nowadays transmission digital images in a network are consider a commn process, where every moment large amount of digital images are transmitted by the networks. Military images transmission requires high-security levels to prevent intruders from being violated their privacy [1]. In general, the data of an images may be secret information that candidate to unauthorized access, owners of such digital data images do not want to penetrate their images without a permission. For these reasons, securing images' contents has become an important issue [2]. Various techniques have been used to preserve image confidentiality and keep the unauthorized users far away, these techniques called security techniques. Security techniques follows into two main categories: cryptography and information hiding [1,3]. In encryption techniques, the plaintext is converted to a noise text using a key, which is not understood or predicting its content. Users cannot restore the encrypted text without knowing the key at least. Some data media like images in somehow having inherent features such as data redundancy. Bulk capacity of data, correlation among pixels is high, sensitivity is less compared to data in text a slight change in the attribute of any pixel of the image does not drastically degrade the quality of the image and this in general is difficult to handle by traditional methods [1].

While, information hiding is the technique of embedding information in a media. information hiding is divided into two techniques: Steganography and

digital watermarking [4]. The steganography technique implies a secrete message is embedded in a selected media cover so that it is not detectable. But, in a digital watermarking technique, a piece of digital data inserted in a selected media such as images, where the original and watermarked images' perceptibility are similar. Image encryption, in which the image data is manipulated a way that not authorized person cannot read the original contents [5, 6]. Different interpretation of information and new directions in developing cryptographic protocols are use on a large scale for transmitting information secretly have adopted through the age of computer development [7]. The computing power offered the possibility to build new and strong algorithms in cryptography, but conversely has a strong tool used by cryptanalysts to break the cryptosystems. This means, the explorer of finding new directions and powerful developments in ciphering techniques to fulfill the security needs of transferring digital data is a continuous process [7, 8].

Many theories and disciplines have been applied to protect sensitive data, maintain privacy or security before transmission or distribution. such as chaos theory, DNA, the quantum method. Chaotic-based methods possess intrinsic properties such as non-periodicity, random behavior, and sensitivity to control parameters and initial conditions [9].These properties enable the successful utilization in the encryption of images. Moreover, Chaotic-based encryption techniques are considered good because these techniques present a good combination of a speed, high security, complexity, reasonable computational overheads and computational power etc. [10]

Recently, DNA cryptography utilizes as an informational carrier using the molecular techniques [11]. DNA cryptography gains attention because of the vast storage capacity of DNA. The massive parallelism and ultra-low power consumption opened the door for researchers to utilize the DNA in many fields especially in security [11, 12].

1.2 Problem Statement

The encryption schemes increase the size of the data, getting additional computations that consume a lot of time, or media nature of data such as images that requires special attention, some data in somehow have inherent some features such as redundancy, bulk capacity, high correlation pixels as in images which are generally difficult to handle by traditional encryption algorithms. even in some chaotic maps such as Henon that suffers from this problem. Thus, a reliable and robust security encryption method is needed to overcome these views by expanding the era of encryption environment by merging it with new a directions such as DNA biological molecular. Where, this expansion is the thesis focal point interesting for manipulating the above problems

1.3 Objectives of the Thesis

The Objectives of this thesis is to combination the classical Henon chaotic map performance with DNA map in encrypting images that have inherent features such as redundancy, bulk capacity, and high correlation pixels by adopt function to DNA molecular mapping and to ensure the security of data that grounded on:
Firstly: Partial encryption process is implemented by:

- 2D-Henon chaotic map and DNA map
- Stamping the selected image by an invisible value, to ensure the privacy if the image has been fraud or not

Secondly, the DNA map provides:

- wider range of chaotic

Thirdly, using the dynamic DNA coding rules to:

- ensure highly data confusion
- The intruder cannot reach the coding rule used and thus, the ciphered message cannot break easily or analyzed.

1.4 Related Works

Jan and Ahmad [13], presented a technique that divide the image in a number of blocks to calculate the correlation coefficients of each block. The block of a maximum correlation coefficient values were pixel-wise XOR with the random numbers that are generated from a skew tent map based on a threshold value. Finally, the resulted image was permuted via two random generated sequences from Tangent Delay Ellipse Reflecting Cavity Map System chaotic map.

JAN and WADII [14], proposed a scheme to generate the initial conditions of the chaotic maps from a random DNA sequence although the plaintext image. The three different 1D chaotic maps were used to increase the key space. These maps were used to diffuse a plain image by selecting a block with high correlation and it is bitwise XOR with the random matrix. While, the other two chaotic breaks the correlation between adjacent pixels by confusion (using row and column shuffling). Then, the ciphered image was divided into Most Significant Bits (MSBs) and Least Significant Bit (LSBs), The host image was passed through lifting wavelet transformation, which replaced the low-frequency blocks of the host image (i.e., HL and HH) with the MSBs and LSBs of cipher text that resultd in a chaotic visual selective encrypted image

Zhen and Changgen [15], proposed an chaos encryption image scheme Using imitating jigsaw method with revolving and shifting operations. The scheme consisted of three processes: preprocessing, encryption process, and post processing. The preprocessing partitioned the original image into blocks of 64 × 64 pixels and randomly revolved and shifted under controled sequences that generated by a hyper-chaotic Lorenz system with initial conditions that were calculated by the original image and keys. The encryption process partitioned the resulted image into blocks of 32 × 32 pixels and randomly revolved and encrypted by control sequence and key blocks which were generated by the skew tent map.

In post processing, the image was partitioned into blocks of 16 ×16 pixels to randomly revolved and shifted again under control sequences which are related with encrypted image and keys to increases the diffusion characteristics.

Mohammad and Hassan [16], proposed three different styles of encryption algorithms: full, mid full, and selective. The full approach encrypts all sub-matrices of an image, while the middle-full is a middle solution between the selective and full algorithms and its goal is to conceal the type of the medical image. Selective encryption identifies a set of sub-matrices of an image according to a statistical average test, known as region of interest (ROI). In the three approaches, a high security level is ensured where each image is encrypted independently of the previous and next images. The primitives of the proposal, like permutation and substitution, depend on a dynamic key. The proposed use a round function is lightweight and applied for only one round. This reduces the latency and the required resources as compared to traditional encryption algorithms. the size of a sub-matrix is variable and can be changed according to the available memory size.

Bhagyashri and Vinay [17], proposed Partial Image Encryption using Chaos. Was proposed original greyscale image was decomposed into its corresponding binary eight bit planes then encrypted using chaotic map based on pseudorandom binary number generator (PRBNG) were encrypted using keys which were obtained by applying the recurrence relation of chaotic map. The non-selective bit along with encrypted selective bits were combined to form the final cipher image. The proposed algorithm was measured through a series of security and effectiveness measures.

Jian and Dezhi [18], proposed an image encryption method based on the combination of chaotic map and DNA coding. Firstly, the chaotic sequences generated by the Lorenz chaotic system to scramble the pixels of the image. Diffusing process was used to obtain the encrypted image using Chen's hyper-chaotic and DNA encoding, The image encryption is divided into two main parts:

scrambling and pixel diffusion. using the grayscale images of Lena and the Cameraman, with image sizes of 256 × 256. The DNA encoding rules are dynamically selected according to generated chaotic sequences.

Kumar and Raghava [19], proposed region-based selective image encryption to secure information in an efficient manner to reduced encryption time. Secrecy of unnecessary information within an image is not required for both the ends in communication. Here, security aggregated chaos-based coding with most significant bit diffusion and recentness keyless substitution cipher at the pixel level on the ROI image obtained by a hybrid region growing method. This technique significantly reduces the storage space and transmission costs.

Mutnuru and Kumari [20], proposed a new selective encryption-based security system to transfer data with protection in unsecure network. The data in the image is transmitted over a network is discriminated using DCT transform and partially encrypted using Number Puzzle technique to provides security from unauthorized access.

Akkasaligar and Biradar [21], presented a DNA cryptography and dual hyperchaotic map techniques that were proposed for digital medical image. These images had a very large size and require more computational time. To reduce computational time, a selective digital medical image encryption algorithm was used. In the proposed cryptosystem, the permutation and diffusion process were performed on selected pixels of digital medical images. The construction of DNA structure for these images, all DNA encoding rules based on the pixel position of the medical image were used. The cipher image was attained by using all DNA decoding rules based on the pixel value of the medical image.

Wonyoung and Sun-Young [22], proposed method for partially encrypting private information in images. The proposed method encrypted private information without increasing the data size, solving the problem of wasted storage space. Where, specific sections of encrypted images can be decrypted and recognized before decryption of the entire information, which

addresses the problems besetting traditional privacy masking and image encryption methods.

LIU and WANG [23], proposed an image encryption scheme combining the 5D hyper chaotic system and DNA technology. The proposed scheme is related to the plaintext and external secret key, which did not need to manage the huge amounts of dynamic secret keys and does not to design synchronization method. The proposed scheme consisted of four parts: pixel-level diffusion, pixel-level permutation, DNA-level diffusion and second permutation. In pixel-level diffusion process, chaotic sequences iterated by 5D hyper chaotic system with initial values (set as secret keys) were used to rewrite the pixel values of plaintext image and they were also used to generate second permutation rule. the pixel-level permutation rules were obtained by chaotic system with modified initial values that were related to the plaintext image and external secret key. In the DNA-level diffusion process, select a part of pixel values of the pixel-level permutated image and external secret key to generate key streams used in this level. The decryption part can obtain the selected pixel values during the decryption process, which avoids transmitting huge secret keys and synchronizing them with plaintext images. In the second permutation, rearrange the position of the selected pixel values.The related work presented dealt with part of the proposed procedures from the site of partial encryption. The below related work with another site of the proposed procedures dealing with dynamic DNA coding and Henon map.

Liu, and Ye [24], presented asymmetric image encryption algorithm based on DNA coding and hyper-chaotic system was designed. Consist of three stages. Firstly, eliminate the risk of key transmission and management, the initial values of the hyper-chaotic system were generated the RSA algorithm and the plain image, in which the sum of odd rows, even rows, odd columns, and even columns are computed respectively to extra the plain message from the plain image as input of RSA algorithm. Secondly, the pixel level permutation was performed to

confuse the image according to the chaotic sequences generated. Finally, dynamical DNA encryption was designed to diffuse the permuted image. The process of DNA encryption included DNA coding, decoding, and DNA operation. The DNA rules were generated according to chaotic sequences dynamically, rather than fixed rules with simple operation.

Yu Liu and Zheng Qin [25], presented new image encryption method based on genetic mutation, DNA coding and cascading two maps Hénon and Chebyshev map to produce a two-dimensional Hénon–Chebyshev modulation map (2D-HCMM). The proposal scheme used the 2D-HCMM to generate keys randomly, these keys were used to encrypt the image pixels, substituted by DNA coding then scrambled by genetic mutation operation.

Zheng and Liu [26], presented an image encryption scheme based on dynamic DNA sequences encryption and improved 2D-LSMM. The logistic map was used to control the input of the sine map. the encoding and operation rules of DNA sequences were determined by 2D-LSMM chaotic sequences.

QAYYUM and AHMAD [27], proposed a scheme based on two-dimensional Henon, Ikeda chaotic maps, and substitution box (S-box) transformation. Through Henon, a random S-Box is selected and the image pixel was substituted randomly, several security tests such as information entropy, histogram investigation, correlation analysis, energy, homogeneity, and mean square error were performed to analyze security and robustness of the proposed algorithm.

Wu and Liao [28], proposed a two-dimensional Henon-Sine map (2D-HSM). The new map possesses better ergodicity and pseudo ´ randomness, and its parameters gives a wider chaotic range, compared with many existing chaotic systems. applying a DNA encoding and a DNA exclusive-or (XOR) operation rule for image encryption to improve the efficiency of image permutation and diffusion. Furthermore, to protect image content while an image was transferred over the Internet.

Zhang and Han [29], presented an image encryption algorithm based on bit permutation and dynamic DNA encoding. The algorithm first uses Keccak to calculate the hash value for a given DNA sequence as the initial value of a chaotic map; second, it uses a chaotic sequence to scramble the image pixel locations, and the butterfly network was used to implement the bit permutation. The image was coded into a DNA matrix dynamic, and an algebraic operation was performed with the DNA sequence to realize the substitution of the pixels, improving the security of the encryption. Finally, the confusion and diffusion properties were enhanced by the operation of the DNA sequence and the cipher text feedback.

1.5 Thesis Organization

In addition to chapter one, the thesis is organized into four chapters as bellow:

Chapter Two presents the theoretical background the thesis related with such as, cryptography techniques, chaotic system, 2D Henon chaotic, DNA molecular structure, and coding rules.

Chapter Three presents the theoretical implementation of the proposal work includes the proposal general structure, block diagrams, flowcharts, and algorithms.

Chapter Four presents the practical implementation of the proposal work includes the experimental images, results and discussion.

Chapter Five presents the conclusion and future work.

1.6 Summary

In this chapter, a preliminaries to this thesis is given. The related works are presented. The problem is explained. The contributions of the work are presented. The aims of the thesis are stated. Finally, thesis structure is introduced.

CHAPTER TWO

THEORETICAL BACKGROUND

CHAPTER TWO

THEORETICAL BACKGROUND

2.1 Introduction

In the recent years, the traditional cryptographic systems are vulnerable to attacks, because encryption algorithms are lack for evaluation to their performance. Nowadays, new and efficient methods have suggest to developing secure technique for image encryption like chaos, DNA, and block chain. This chapter presents the theoretical background of encryption method the proposed such as, cryptology, chaos theory, DNA molecular and chaos image encryption, DNA image encryption and DNA coding.

2.2 Cryptology

Cryptology also known as cryptography is an art of achieving security and done by encoding the data in apparent nonsense manner using encryption algorithms, so that only the intended user can retrieve the original content. The term cryptography is not only providing information security, its rather one of a set of techniques Cryptography prior to the modern age was effectively synonymous with encryption. A cryptography algorithm, often known as a cipher, is a mathematical function that is used to encrypt and decrypt data. To encrypt the message, the cryptography technique uses an association key. A cryptosystem is a collection of cryptography algorithms, keys, and protocols [30].

2.2.1 Encryption Scheme Category

Full image encryption methods and selective (or partial) image encryption techniques are two types of image encryption schemes that have been developed [10,31].

A. The Full Image Encryption

Full image encryption techniques encrypt the entire image, which takes a lot of time and resources and isn't always suitable for real-time applications [10,31].

B. Partial Encryption (Selective Encryption)

Selective encryption, also known as selective decryption, is a technology that allows you to avoid encrypting the entire image (partial encryption, soft encryption or perceptual encryption). Furthermore, partial encryption uses fewer resources because it only encrypts the image's interest region. Partial image encryption techniques are computationally efficient, making them suited for real-time implementations and applications such as teleconferences and video monitoring, among others. They save time and money [31].

The main goal is to divide the image material into two interest-based sharing sections: public sharing and protected sharing. The most important property of partial encryption is that it minimizes the amount of data that is protected. In most cases, partial encryption is used in conjunction with compression. Low frequency coefficients carry the majority of the image's data, while high frequency coefficients convey the fine points. [10,32].

2.3 Cryptography and Chaos theory

Chaotic sequences have various cryptographic advantages over regular ciphers, It's also hard to challenge and extremely hard to break. As a result of these attributes, the safety efficiency of cryptography and decoding operations has significantly improved.

The main idea behind chaotic cryptography is really to encrypt plaintext with a chaotic string generated by a chaotic map in order to obtain the cipher text. After transmission, The receiver creates the very same chaotic map as that of the transmitter via chaotic synchronization, and then recovers the unencrypted from this [33].

According to existing research, the chaotic sequences generated by the chaos systems is a nonlinear string with a complex design that is difficult to analyze and predict, as well as high randomization, correlations, and difficulty, which makes it suitable for usage as a chaotic cryptographic key pattern. The chaotic sequence is an effective key sequences for the "a words a secrets" cryptography scheme, and it can also be used as a passwords method. [33].

Chaos has an exceptionally crucial role in secure communication systems because to its high sensitivities to beginning situations and chaos-inducing elements [34].

Chaos theory has been intensively researched in a variety of fields, including mathematics, physics, computer science, and engineering. Since the last two decades, many academics and cryptographers have been drawn to chaos-based image encryption. They discovered that there are some correlations between features that have analogues in chaos and cryptography. Chaotic maps and cryptographic algorithms have a striking resemblance in terms of sensitivity to initial conditions and deterministic pseudorandom behavior. Moreover, in the building of cryptographic techniques, utter confusion and diffusion are two broad good principles that result to the hiding of the statistically organization of pixel in a source images and a reduction in the statistically dependency of an input image and its encryption counterpart. The addition of a mix aspect to chaos-based cryptographic algorithms enhances the complexities of the cipher picture. [31, 35].

2.4 Chaotic maps

Chaotic systems are nonlinear systems with many complex characteristics. It has qualified features such as nonlinearity, deterministically, abnormality, and affectability to initial conditions and sensitivity[35]. Due to their high sensitivity to beginning parameters, chaotic maps could generate a large amount of randomness chaotic sequence having pseudo-random properties.Because of their

high sensitivity to initial conditions, chaotic maps can create a large number of randomness chaotic sequence with pseudo-random features.

The fluttering wings indicate a minute change in the dynamic system's initial state. This sets in motion a series of events that will lead to large future changes. This suggests that even a small adjustment in the original settings (often in the ten-millionth put a value) can have drastically different results. As a result, long-term prediction is difficult for a chaotic system in general. This means that knowing the beginning state of these systems allows us to anticipate their future behavior. This behavior is known as deterministic chaos or just chaos, and It is exhibited by chaotic maps. Any Chaotic Map can be characterized mathematically as in Equation (1).

$$X_n = f(X_{n-1}) \qquad \text{n= 1,2,3,…..} \qquad (1)$$

Where, xn is called the state of iteration n, the equation (1) is mapping the state x_{n-1} to the next state , Continuous and discrete maps are two types of such maps [36,37].

Round in cryptographic techniques correspond to recursive algorithms, are a type of discrete maps. Chaotic cryptosystems are proposed based on the resemblance between cryptography and discrete chaotic dynamic systems. Certain attributes in every maps are cryptographically equivalent to cryptography. In stream ciphers, a chaotic system is used to create a pseudo - random number stream cipher, whereas in block ciphers, the unencrypted or private key(s) are used as the beginning and controlled parameter. Eventually, the chaotic systems are subjected to some repetition in order to get the cipher-text. Cryptosystems have major challenges in terms of security and complexity. These should be considered when selecting a mapping and its encryption features [37,38].

In the confusion (pixel positions changing) and diffusion processes, the generated chaos random numbers are utilized (pixels value changing) [10].

There are a variety of chaotic maps that are one-dimensional (1D), higher-dimensional (2D), or have both dimensions, such as 1D Logistics maps, 2D Logistics maps, Intertwining Logistic maps, Quantum maps, Burger maps, Skewtent maps, Bernoulli's maps, Beta maps, and Piece wise Linear Chaotic Maps (PWLCM), and henon map, which is the one used in this proposal.

2.4.1 Chaotic Henon Map (CHM)

The Henon map looks to be one of the most well-studied instances of chaotic discrete time dynamical systems, proposed by the French astronomer scientist Michelas in 1978 as a simplification of the Lorenz chaotic system [38,31], that has the same properties and is defined by (2and3). Since the differential equations of the Lorenz system are more difficult to execute. It was obtained by stretch and folding. The model of Henon is a 2D plane that is able to stretch, fold and reverse. It presents chaotic behavior for the dynamic systems. The mathematical model is represented by the following two equations (2and3)[31]:

$$X_{n+1} = 1 - aX_n^2 + Y_n \qquad (2)$$

$$Y_{n+1} = bX_n \qquad (3)$$

Where:

X_n , y_n represent the initial values, x_{n+1}, y_{n+1} takes the values between (0,1).

(a,b) are the initial parameters, while (x0, y0) is the initial point. Through the Henon map, every pixel (x_n, y_n) is plotted to a new pixel (x_{n+1}, y_{n+1}). The Henon function shows chaotic behavior between a = 1.4 and b = 0.3, and A chaotic attraction in the shape of a corkscrew appears in the rounds. Figure (2.1) depicts the Henon map's two-dimensional layer, which is the result of a specified numbers of cycles beginning at a specific starting statement (0.1, 0.1). Any minor modifications in the starting pixel will result in significant alterations and behavior [39,37, 31].

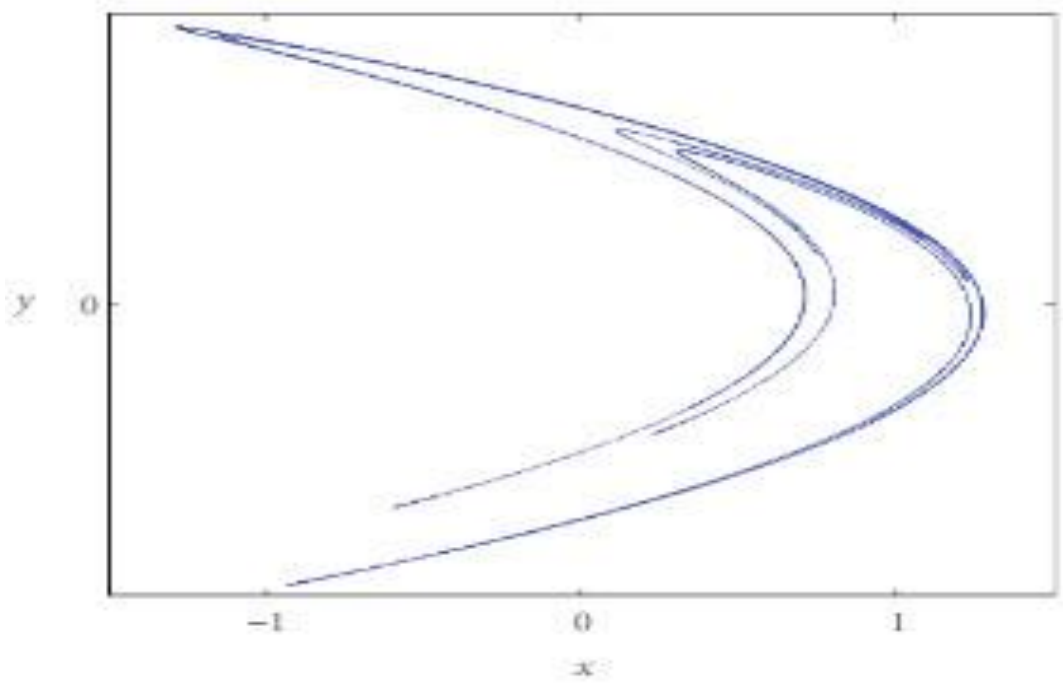


Figure (2.1): Henon Map Form [37]

2.5 Deoxyribose Nucleic Acid (DNA) Cryptography

The area of DNA encryption is a relatively recent one in the realm of data security that has a lot of potential. It combines traditional cryptographic solutions with the genetic material's strength. It is feasible to reap the benefits of traditional cryptographic techniques while also solving several of their shortcomings by incorporating DNA into conventional symmetric key cryptography. DNA can be utilized in a variety of ways to safeguard information content, including ciphering and concealing data. Secret information can be encoded in DNA structures that are tiny in size and concealed among a large number of other DNA structures [40]. This type of computation makes use of the personality capability of DNA strands as well as parallelism computing. just because matching nucleotides in DNA's design connect to one another via a single hybridization processes, it is termed self-assembling. When multiple different DNA structures hybridize at the same time, this results in parallel calculations. DNA sequences, which may be available in digital form in genetic databases, can be used to produce random numbers. [40,41]

2.6 Deoxy Nucleotide Acid (DNA) Theory

The four nucleic acid bases A (adenine), C (cytosine), G (guanine), and T (thymine) make up a DNA sequence (thymine). According to bases pairing regulations, purine adenosine (A) usually couples with purine thymine (T), and purine cytosine (C) usually pairs and purine guanine (G).It can be deduced that A and T complement each other, and G and C complement each other as well. The Watson–Crick base pairing rules are named after the two scientists who identified the structural foundation of these correlations. The DNA structure is simulated by DNA computing operations and computed by means of molecular biology. Figure (2.2) illustrate the DNA structure [42].

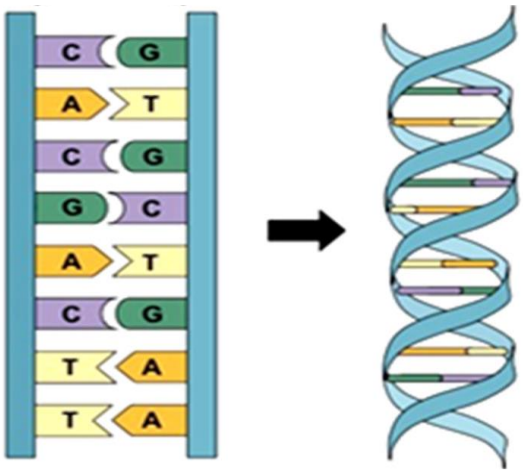


Figure (2.2): The DNA Structure [42]

2.6.1 DNA Coding

Despite the fact that DNA is made up of four fundamental nucleotides: A, T, C, and G [38], An eight - bit binary digit with the value 0 and 1 can be used to represent every pixels in image. The binary values pairing creates a complementing relationships pairing. The digit pair 00, 01, 10, and 11 can be used to encode the DNA bases A, C, G, and T. The DNA bases A, C, G, and T could be encrypted to use the digit pair 00, 01, 10, and 11. Since 00 and 11 and 01 and 10 are complimentary, the DNA letters A, C, G, and T can be encrypted to use the digit pair 00, 01, 10, and 11. With the pairing rule satisfied, 24 varieties of

this coding rules scheme can be obtained. T bases must be linked to A bases, and C bases must be linked to G bases. For example, to encode the value 147 of a pixel in an image, If a rule is selected, the value will be transformed to a binary value (10010011), and the matching DNA coding rule representation will be "GCAT." Furthermore, if a different rule is adopted, the binary number's 8-bit can be stated as "ATCG" for example. [38,43].

The coding rule scheme in DNA is either fixed or dynamic. including during the cryptography, the laws of DNA coding and functioning have remained unchanged, which is known as fixed coding. The dynamic coding, on the other hand, varies between pixels and is generated in a variety of ways. [44,45]

2.7 Image Encryption

Among the most widespread communication forms is the digital representation, and some regions have more strict cryptography regulations. The majority of traditional picture encryption algorithms rely on discrete mathematics [44]. Encryption techniques are dependent on two major processes. The initial stage is to be permuntation as to which pixel arrangements have changed. The second stage, diffusion, is dependent on modifying the values of pixels. For the protection of digital photographs, numerous encryption techniques have been develop. The general architecture of an image encryption-decryption system is shown in Figure (2.3) [30,44].

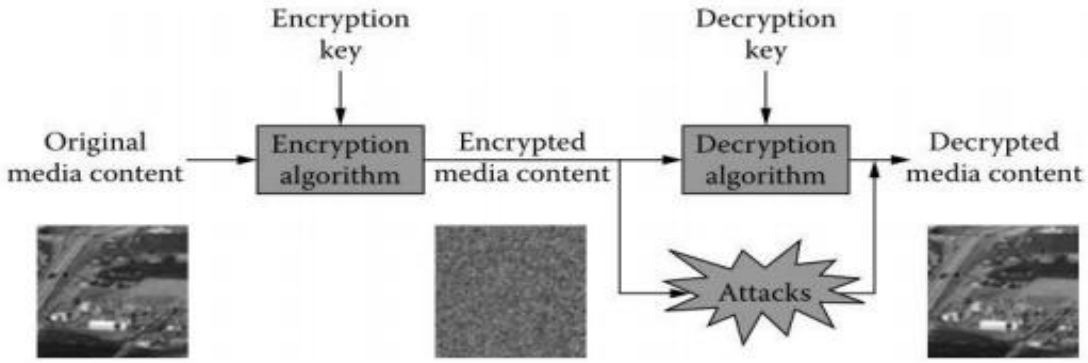


Figure (2.3): Architecture of an Image Encryption-Decryption System [30]

2.7.1. Chaos Based Image Encryption

Chaotic picture cryptography is centered on a dynamical mechanism capable of providing both speedy and secure data protections methods.[44].

Chaos has intrinsic traits including non-periodicity, random behavior, and sensitivity to control parameters and beginning conditions [35]. These qualities make it possible to use chaotic-based algorithms to encrypt photos successfully. Chaos based image encryption algorithms use pseudo random sequences generated out of a chaotic function to encrypt the plaintext. The structures of these sequences are extremely complicated and difficult to understand and predict. In the field of image encryption, these qualities are used. The most common ciphers based on chaotic maps can be divided into two types: permuntation and diffusion. To make the content unrevealed, diffusion based encryption (diffusion algorithm) modifies the pixel values. The pixels are shuffled and the pixel values are not changed in permutation or trans-positioning-based encryption (confusion algorithm). Permutation and diffusion are often combined in order to get high computational security[37].

2.7.2. DNA Based Image Encryption

Researcher has combined DNA sequencing and chaotic to create high-efficiency and safe cryptography, thanks to the massive parallelism and extraordinary information density of DNA molecules. [46,47]. The cryptography of images is dependent on a basic understanding of DNA and DNA sequence operations. [44].

DNA cryptography arose as a new cryptographic discipline as a result of DNA computer research, DNA is used as a data carrier, and systems biology technologies is used as a device for implantation. Because it is not based on complicated mathematical calculations, it is secure. Furthermore, DNA cryptography is far more suitable for high density data storage than quantum cryptography, making it the most successful encryption solution for digital

images. To construct cipher images, the basic principle underlying image encryption with DNA is to convert image pixels into DNA sequences using DNA rules and then perform various DNA operations. Figure (2.4) shows the general block diagram of existing DNA encryption system [45,30]

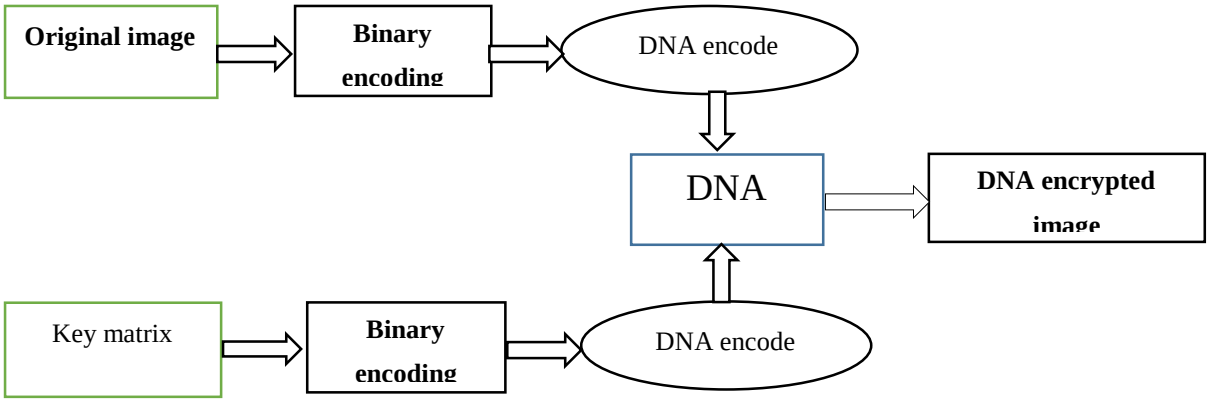


Figure (2.4): DNA Based Image Encryption System adopted from [30]

2.8 Performance Metrics

The specialization of security investigation is discovering a cryptosystem's flaw and recovering the complete ciphered message or discovering the secret key without knowing the decryption key or method. A good encryption scheme should be resistant to all known assaults, including known-plaintext, cipher text only, statistical, differential, and various brute-force attacks, there are a variety of approaches for determining what level of access the attacker has to various aspects of the cryptosystem, such as the key or plaintext.

2.8.1 Statistical Analysis

According to Shannon's hypothesis, statistical analysis can be used to analysis a variety of ciphers since the original and encrypted picture relationship can be identified by statistical analysis. As a result, The encryption algorithm should be unrecognizable from the source. There's a few ways to see if an encrypted image contains any characteristics of the original picture such as histogram[48].

- Histogram

A histogram depicts the image's gray scale brightness. For statistical strikes against that non-uniform distributions, this knowledge is extremely useful. To strengthen their susceptibility to statistical methods, images produced by a suitable encryption scheme should have uniform histograms [48].

- Correlation Analysis

Correlation coefficient analysis is a measurement of the correlation among the adjacent pixels in the image. The encryption process should break the correlation of adjacent pixels; therefore, the less correlation among adjacent pixels in the cipher image, the better the security.

This test computes the correlations between two adjacent point (vertical, horizontal or diagonal), Correlation coefficient with the range [−1,1]. It is computed according to Equations (4): [48].

$$r_{ab} = \frac{cov(a,b)}{\sqrt{D(a)D(b)}} \qquad (4)$$

Where cov(a,b) is the covariance computed according to Equation (5):

$$cov(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))(b_i - E(b)) \qquad (5)$$

The Mean computed according to Equations (6):

$$E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i \qquad (6)$$

And the standard deviation computed according to Equations (7):

$$D(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))^2 \qquad (7)$$

Even if adjacent pixels in clear images are very redundant and correlated, the pixels in the encrypted image should have as little redundancy and correlation as possible [48].

2.8.2 Entropy

The entropy of a signal is a numerical measure of its uncertainty and randomness. The degree of uncertainty of a cipher image can reflect the diffusion

performance of an image cryptosystem, and the information entropy is a measurement to indicate the uncertainty degree of the whole image information. A high entropy value indicates a signal that is less predictable.

The information entropy is given in Equation (8).

$$H(s) = \sum_{i=0}^{2^{k-1}} p(s_i) \log_2 \frac{1}{p_i} \qquad (8)$$

Where:

K: is the bit depth of the test image, e.g., K = 8 for an 8-bit gray image,

$P(s_i)$ means the probability of s_i.

In the ideal case, the information entropy of 8-bit gray image is H(s) = 8 bits [48].

2.8.3 Differential Analysis

This sort of examination focuses on the encryption algorithm's susceptibility to slight modifications, in which the attacker can make a smaller change (for example, one point) in the basic images and see what happens. The attacker must be unable to identify a compelling association between the original and encrypted images in powerful cryptosystems. Two metrics are widely used to assess a picture cryptosystem's diffusion ability: NPCR (numbers of pixels variation) with UACI (unified average change intensities). The expectation of NPCR and UACI between two random images are given in Equations (9) and (10), respective [48].

$$NPCR_E = (1 - \frac{1}{2^{\log_2 L}}) \times 100\% \qquad (9)$$

$$UACI_E = \frac{1}{L^2} (\frac{\sum_{X=1}^{L=1} x(x+1)}{L-1}) \times 100\% \qquad (10)$$

2.8.4 Peak Signal-to-Noise Ratio (PSNR)

The term Peak Signal-to-Noise Ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many

signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale [49]. The mathematical representation of the **PSNR** is as eq. (11):

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \quad (11)$$

where the **MSE** (*Mean Squared Error*) is computed by eq. (12) [49]:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (12)$$

Where:
f: represents the matrix data of our original image
g: represents the matrix data of our degraded image in question
m: represents the numbers of rows of pixels of the images and (i) represents the Index of that row
n: represents the number of columns of pixels of the image and j represents the index of that column
MAX_f : is the maximum signal value that exists in our original "known to be good" image.

2.9 Summary

This chapter presented the background of the proposed outline, like cryptology, chaos theory, DNA molecular, and chaos image encryption, DNA image encryption, and DNA coding. Finally, it presented some performance metrics can be used to measure the performance of proposed method like , Histogram analysis, and correlative analysis, entropy, PSNR, MSE.

CHAPTER THREE

THE PROPOSED SYSTEM

CHAPTER THREE

THE PROPOSED SYSTEM

3.1 Introduction

This chapter, clarify the theoretical part of the proposed system. In particular, it deals with ciphering the grayscale data image partially; using chaos theory and DNA coding techniques. The layout of this chapter describes the workflow stages of the proposal. This layout represented by the block diagrams, algorithms and their explanations.

3.2 The Proposed System Structure

The proposed system structure consist from two sites: transmitter and receiver, deals with two types of chaos (Henon map and DNA map with dynamic DNA coding technique). The DNA map is a focal point in the proposal, where it was employed in a new direction different from what the researchers has dealt with in terms of its use in encryption, hiding and other applications. The proposal used the DNA as chaos map and a dynamic coding used to supported the chaos behavior. The Henon map is selected here one of a known standard chaos to illustrate the comparison between the DNA and Henon behavior from the view of a chaos. The usage of these maps illustrated in the block diagram of figure (3.1).

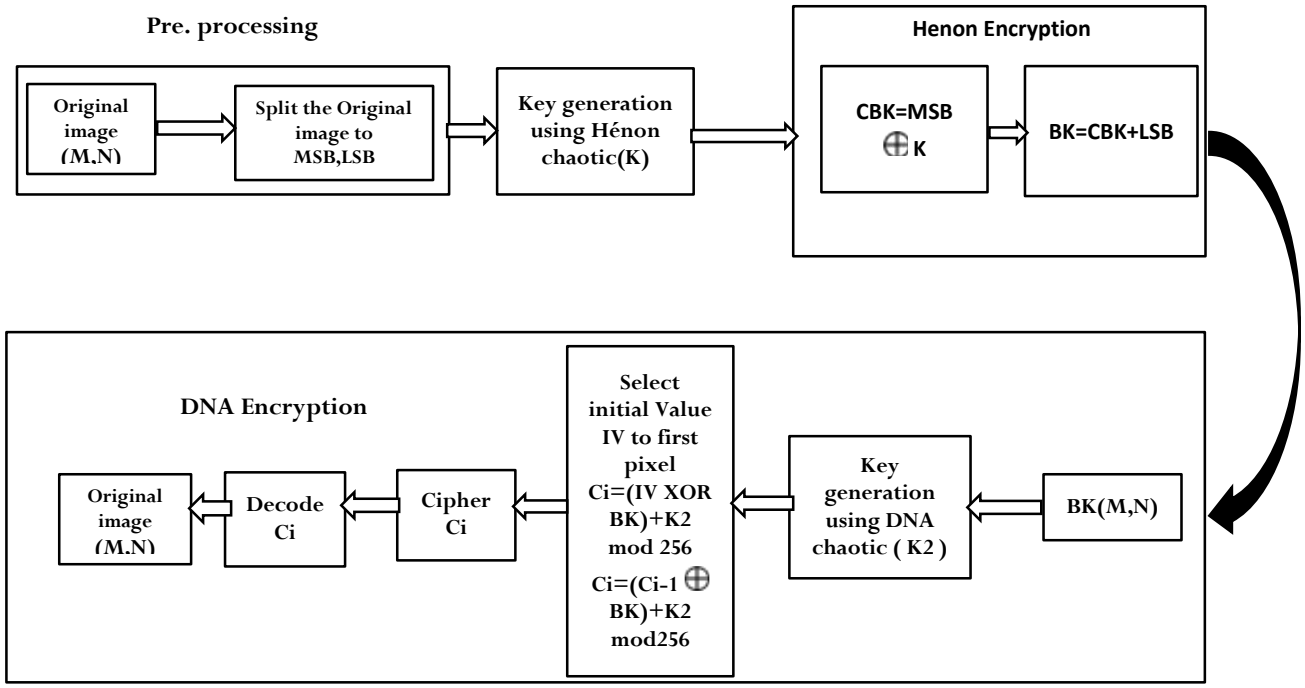


Figure (3.1): The Proposed System Block diagram

3.3 Proposed System Stages

The proposed system work flow at transmitter site pass through two main stages:

3.3.1 Preparing Stage

This stage prepares the plain image for the encryption stage. Thus, this stage represents the base for the whole proposal procedure which includes:

A. Image Plain Processing

The aim of this process is to determine the significant bits of gray image plane includes: *Image plane Decomposition process.*

B. Image Plain Decomposition Process

The gray image plain composes of intensity pixels that are quantized into levels ranging from 0 to 255 of an integer number. Each pixel value will be converted to its corresponding binary form of 8 bit.The next step is to divided the pixel plane to two planes (MSB, LSB). Algorithm (3.1) illustrate this step.

Algorithm (3.1): Preparing Stage

Input: plain image (g) of size (mxn)

Output: Partitioned g to (MSB, LSB) planes

Step 1: Partition image (g) to two planes

```
For i = 0:m-1
    For j = 0:n-1
        Each pixel value P in g[i, j] decomposed to its
          corresponding 8- bit binary
        split plane of 8- bit binary to two planes: (MSB, LSB)
    end
end
```

3.3.2 Encryption Stage

This stage includes three types of encryption: Henon map, DNA map, and mixing encryption (two maps). Although, the DNA coding rule used here is a dynamic coding rule instead of fixed coding. The procedure of these encryption techniques are explained in bellow.

A. Henon Encryption Process

This step includes ciphering the image partially using Henon map. The procedure is illustrated in figure (3.2).

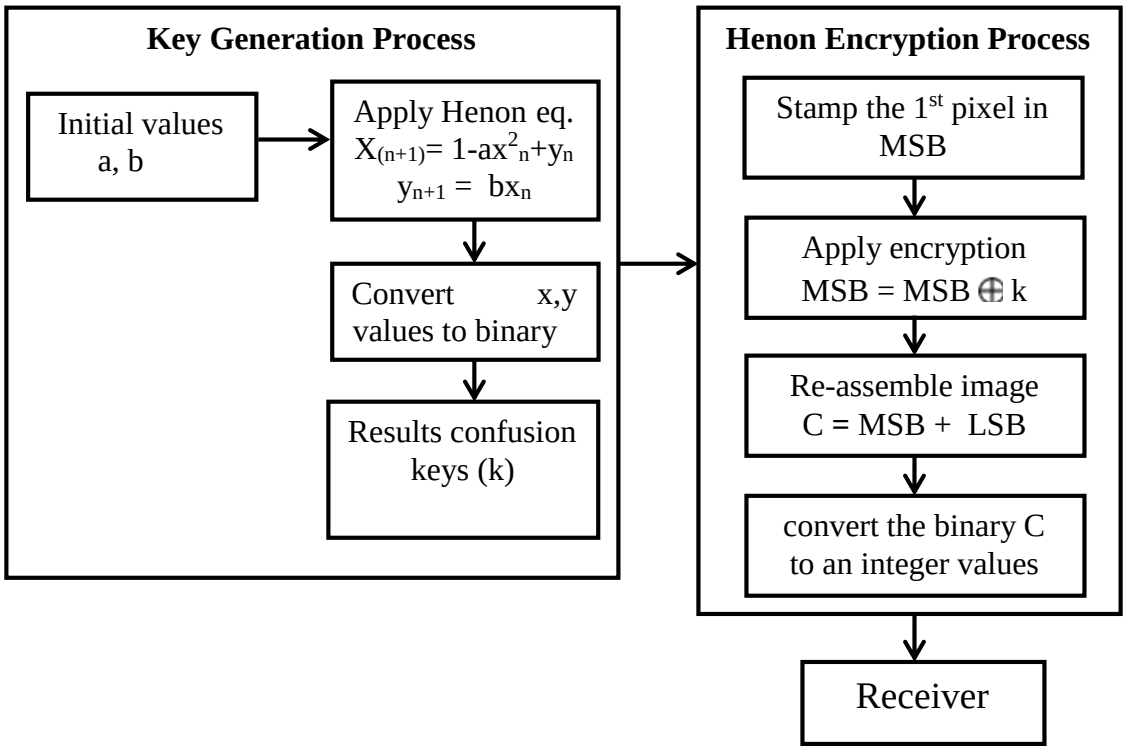


Figure (3.2): Layout Steps of Henon Encryption

The values of (a=1.4 and b=0.3).This process includes of:

- Key Generation Process

To generate ciphering keys a Henon map is used to encrypt the MSB. Algorithm (3.2) constructed to explain this process.

Algorithm (3.2): Key Generation Process

Input: image of (m,n), initial values (a=1.4, b=0.3)
Output: stream of encryption keys (k)

Step 1: For i = 1: mn
Step 2: For x = 0 : m-1
Step 3: For y = 0 : n-1
Step 4: $x_{(n+1)}= 1-ax^2_n+y_n$ // henon eq. (1)
Step 5: $y_{(n+1)} = bx_n$ (2)

Step 6: generate sequence of bits

IF $x_{(n+1)} > y_{(n+1)}$
k(i) =1
else
IF $x_{(n+1)} \leq y_{(n+1)}$
k(i) = 0
end
end
end
end
end

Step 7: the result is stream of K ={$k_0, k_1, k_2, ..., k_{n-1}$ }

- Encryption Process

To get a ciphered image, encryption process must be applied. In this work, the encryption is supported by a stamping trade. This stamping is produced by XOR initial value (v) with the first pixel in MSB plane, this value represent as a trade for this plain and provides the receiver a checking mechanism to test the ciphered f it has been cracked or not. The workflow of this process is illustrated in algorithm (3.3).

Algorithm (3. 3): Encryption Process

Input: K sequence**,** random initial value (v), gMSB(m,n) and gLSB (m,n)
Output: stamped ciphered image

Step 1: get g(MSB)
Step 2: processing the MSB part only

gMSB[1,1] = v ⊕ gMSB[1,1] (3)

Step 3: For x = 1:mn
Step 4: For y = 1:mn
Step 5: gMSB [x,y]= gMSB[x,y] ⊕ k[x,y] (4)
Step 6: end
Step 7: end

// re-assemble MSB with LSB to get the ciphered image

Step 8: C = gMSB + gLSB

// generating ciphered image

Step 9: encode the binary ciphered image (C) to its corresponding integer values

B. DNA Cryptography

To provide the chaos based cryptosystem more securing, DNA technology is applied because of its characteristics such as parallelism, and huge storage. The proposed used the DNA into two directions as a: DNA map and dynamic coding rule. Figure (3.3) explain the DNA cryptography layout.

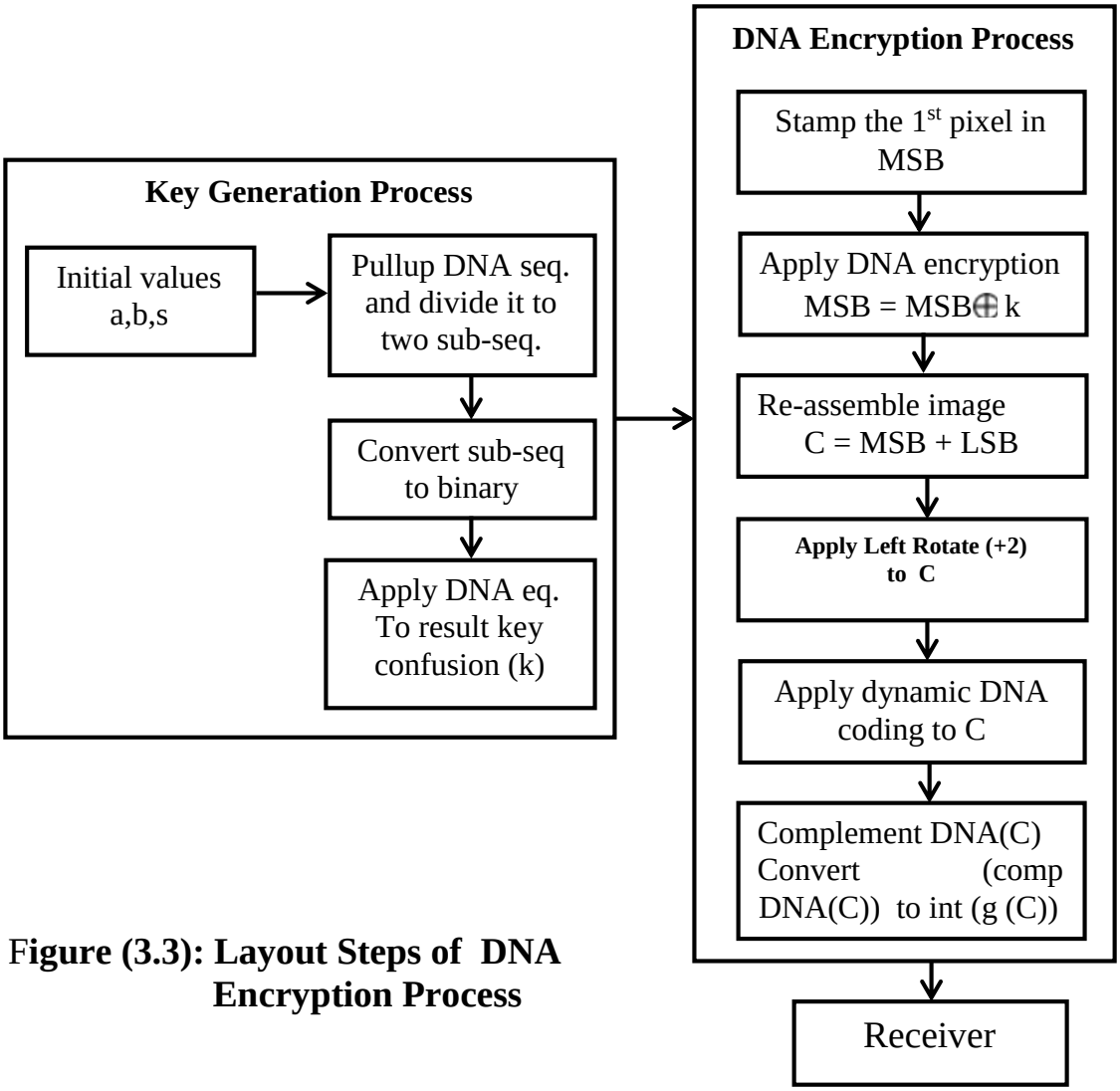


Figure (3.3): Layout Steps of DNA Encryption Process

- DNA Coding Table

Constructing a DNA coding table is a necessity step to convert the DNA bases to a binary bits or vice versa. The type of DNA coding table used in this proposal is shown in table (3.1).

Table (3.1): DNA Coding

DNA Base	Binary Value
A	**11**
C	**10**
G	**00**
T	**01**

- Key Generation Process

This process produce a stream of keys to produce a first type of encryption. Producing ciphered keys are explained in algorithm (3.4):

Algorithm (3.4): Key Generation Process

Input: DNA seq., seed value (23), initial values (a=21,b=31)
Output: stream of ciphered keys

Step 1: pullup a DNA sequence from NCBI db.

Step 2: increase the DNA sequence by 4 to proportion the image size

Step 3: divide the sequence into subsequences, each subsequences is converted to a binary according to table (3.1) generating a sub-sequences of $N=\{N_0,N_1,\ldots, N_{n-1}\}$ of binary values

Step 4: apply DNA map to generate stream of confusion keys using eq. (5) with seed value (s), and two parameters (a,b):

For i = 0 to n-1 such that $0 \leq i \leq n$

$$k_i = (((s_i \oplus N_i) \times a)+b) \bmod 2^8 \qquad (5)$$

end // for

Step 5: the result is a stream of K ={$k_0, k_1, k_2, ..., k_{n-1}$ }

- DNA Encryption

To perform this step, coding rule table must be prepared because it is used during the encryption process, although procedure of coding method must prepare. The procedure of encryption process is illustrated in algorithm (3.5).

Algorithm (3.5): DNA Encryption Process

Input: gray image [g(MSB) and g(LSB)], K sequence**,** initial value (v=41)
Output: partial ciphered image

Step 1: get g(MSB)
Step 2: select initial value (v) added to the first pixel in g(MSB) producing a trade stamp for the image computed by: //trade stamp for the 1st pixel

$$\boldsymbol{C_0 = [(IV \oplus P_0) + K_0] mod 2^8 \ , \quad i = 0} \qquad (6)$$

Step 3: produce partial ciphered image by apply eq. (7)
For i = 1:mn

$$\boldsymbol{C_i = [(C_{i-1} \oplus P_i) + K_i] mod 2^8 \ , \quad 1 \leq i < mn} \qquad (7)$$

end
end

Step 4: C = g(MSB) + g(LSB)

Step 5: For i = 1 to mn

For j = 1:4
C[i,j]= [left shift by 2 (C[i,j])]
end
end
// re-assemble MSB with LSB to get the ciphered image
Step 6: Encode each value of the sequence C into integer
Step 7: convert each value of the sequence C into DNA code using dynamic coding as in algorithm (3.6) and DNA rule table (3.2) and stored in X
Step 8: apply the base pairing complement on sequence X
Step 9: Convert the sequence X into a 2D matrix and converted to a values to generate encrypted

- DNA Dynamic Encoding Method

To get a strong confusion to the image pixels, a DNA dynamic mechanism is used, thereby spreading the effect of plain image through encryption to enhance the security. The type of DNA coding rule table used in this thesis has been constructed in table (3.2).The process of dynamic DNA encoding scheme is explained in an example below in figure (3.4), algorithm (3.6) describe the procedure of coding the ciphered message to DNA using dynamic rule.

Table (3.2): DNA Rules

Code/Rule	A	T	C	G
Rule 1	**00**	**10**	**11**	**01**
Rule 2	**00**	**01**	**11**	**10**
Rule 3	**01**	**00**	**10**	**11**
Rule 4	**01**	**00**	**11**	**10**
Rule 5	**10**	**11**	**00**	**01**
Rule 6	**10**	**01**	**00**	**11**
Rule 7	**11**	**01**	**10**	**00**
Rule 8	**11**	**10**	**01**	**00**

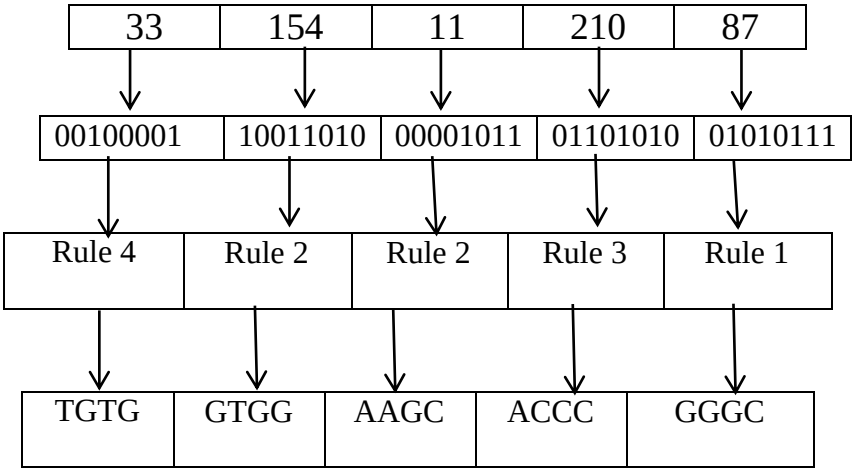


Figure (3.4): Example of Dynamic DNA Encoding

Algorithm (3.6): Dynamic DNA Coding Rule Process
Input: C sequence, table (3.2) **Output:** DNA ciphered image
Step 1: consider each value in C sequence **Step 2:** apply eq. (8) to assign a rule from table (3.2) $$\boldsymbol{Rule - No. = mod(Q, 8) + 1} \quad \textbf{(8)}$$ **Step 3:** encode the C sequence to a DNA coding according to Rule-No. in table (3.2) **Step 4:** the result is a DNA ciphered sequence

C. Mixing Encryption (Henon-DNA Encryption)

This type of encryption consists of applying the two maps in encryption process in two levels: the first level apply the Henon map to the plain image. The output of this level will be input to the next level (DNA map), the result of these levels are ciphered image of (Henon-DNA Encryption). The initial value (v) will be applied to the first level of encryption (Henon map) only.

3.4 Receiver Site

At this site, the transmitter has to send important parameters on agreed secure channel in a table in order to retrieve the ciphered image by the receiver using the transmitter two stages but in a reverse order. After conducting several experiments on different values, the best results were obtained using the important parameters listed in table (3.3) such as:

Table (3.3): Base Parameters

Parameter Name	Value
Seed value	23
Stamp value	41
a,b	21,31

According to encryption method type used, the receiver has to apply the inverse steps of encryption method i.e. (decryption process). These types are:

3.4.1 Henon Decryption Process

In order to decrypt the ciphered message encrypted by Henon map, the receiver has to trace back the encryption algorithm for this map in an inverse steps. The first step in decryption process is key generation step done first explained in algorithm (3,2). While, decryption process illustrated in algorithm (3.7).

Algorithm (3. 7): Decryption Process

Input: K sequence**,** initial value (v), ciphered g(m,n)
Output: plain image

Step 1: split the ciphered image g to (MSB) and (LSB)

// processing the MSB part only

Step 2: decrypt (MSB) by apply eq. (4)

For i = 1:mn such that $1 \leq i \leq mn$
  For j = 1:4
    MSB [i,j]= MSB[i,j] $\oplus$ k[i,j] (4)
  end
end
Step 3: gMSB[1,1] = v $\oplus$ gMSB[1,1] (3)

// re-assemble MSB with LSB to get the ciphered image

Step 4: C = gMSB + gLSB

// generating binary image

Step 5: encode the binary image (C) to its corresponding integer values

3.4.2 DNA Decryption Process

To decrypt the DNA ciphered image required two steps:

- Generate ciphered keys as in algorithm (3,4)
- Apply DNA Decryption Process as in algorithm (3.8)

Algorithm (3.8): DNA Encryption Process

Input: ciphered image (g), K sequence**,** initial value (v)
Output: partial ciphered image

Step 1: convert g(m,n) to DNA coding using dynamic coding rules as in algorithm (3.5) and DNA rule table (3.2) and stored in C
Step 2: apply the base pairing complement on sequence C

Step 3:split the ciphered image g to (MSB) and (LSB)

Step 4: decrypt (MSB) by apply eq. (7)

For i = 1:mn such that $1 \le i \le mn$

For j = 1:4

$$C[i,j]= [C[i,j] \oplus (gMSB[i,j]) - k_{(i \bmod n)})] \bmod 2^8 \quad (7)$$

end // for

end // for

Step 5: For i = 1: mn

For j = 1:4

C[i,j]= [right shift by 2 (C[i,j])]

end // for

end // for

Step 6: apply the initial value (v) to the first pixel in g(MSB) computed by eq. (6)

$$c_0 = [v \oplus (P_0 - k_0)] \bmod 2^8 \quad (6)$$

// re-assemble MSB with LSB to get the ciphered image

Step 7: C = g(MSB) + g(LSB)

Step 8: Encode each value of the sequence C to corresponding integer value

Step 9: Convert the sequence X into a 2D matrix and converted to a values to generate encrypted

3.4.3 Mix (Henon-DNA) Decryption Process

Applying this type of decryption to retrieve the plain message required:

- Apply algorithm (3.8) without step 6 (stamp value). The result of this step will be the input to the next step.
- Apply algorithm (3.7)

The output of this level will be the plain image

3.5 Summary

This chapter presented the proposed system which encrypt the message inside a grayscale image by a secure and an efficient manner. It contains three techniques. A first technique is Henon Chaos Encryption Method, a second technique is DNA map Encryption Method , and the third technique is the mix of Henon Chaos Encryption Method with DNA map Encryption Method. Each

technique contains two phases one to encrypt the plain message (encryption process) and other to retrieve the secret message (decryption process).

CHAPTER FOUR

IMPLEMENTATION AND RESULT ANALYSIS

CHAPTER FOUR

IMPLEMENTATION AND RESULT ANALYSIS

4.1 Introduction

This chapter presents the proposed practical section. Includes the implementation of the system and the obtained results with performance metrics for analyzing the results. These metrics are explained in chapter two.

The system has been implement on laptop included: Processor: Intel core i5, Operating system: Windows 10 platform. The proposed system programmed using MATLAB software version R2017b.The experimental results were analyzed to clarify the results by some performance metrics discussed in chapter two; these metrics are Histogram analysis, Correlation analysis, Quality metrics (NPCR and UACI), Entropy, and PSNR analysis.

4.2 Proposed System Implementation

The proposed implementation system based on hyper encryption chaos. The hyper encryption chaos includes 2D-Henon mapping and mapping called DNA map with DNA dynamic coding rules. There are three types of encryption: Henon map encryption, DNA map encryption, and mix (Henon-DNA) maps encryption.

4.3 The Material of the Test

The tests are carried out on a variety of standard gray images ’of size 256×256, with varying properties including more features and huge sections of the same hue. These images are ‘Lena’, ‘Baboon’, ‘cameraman’, ‘A’, ‘Duck’ and ‘Nike as shown in Figure (4.1).

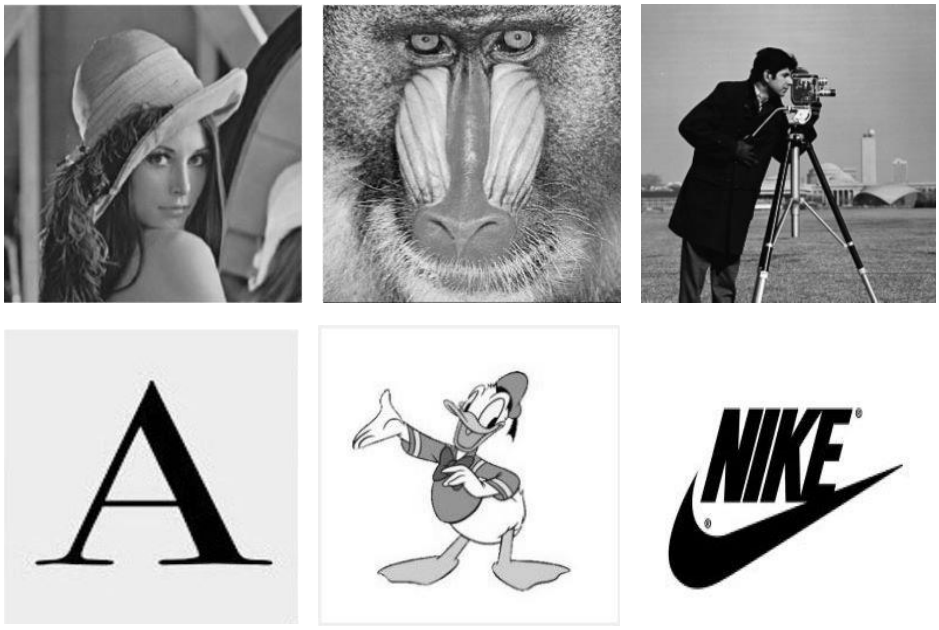


Figure 4.1: Selected Test Images.

4.4 Encryption/ Decryption Processes

To explain the ability of the proposed in encrypting original images and retrieving them using the three types of encryption algorithms: Henon, DNA, and mix (Henon- DNA) maps respectively. Figure (4.2. (a-c)) presents this ability for the three encryption algorithms.

4.4.1 Henon Encryption/ Decryption Processes

Original image **ciphered image** **decryption image**

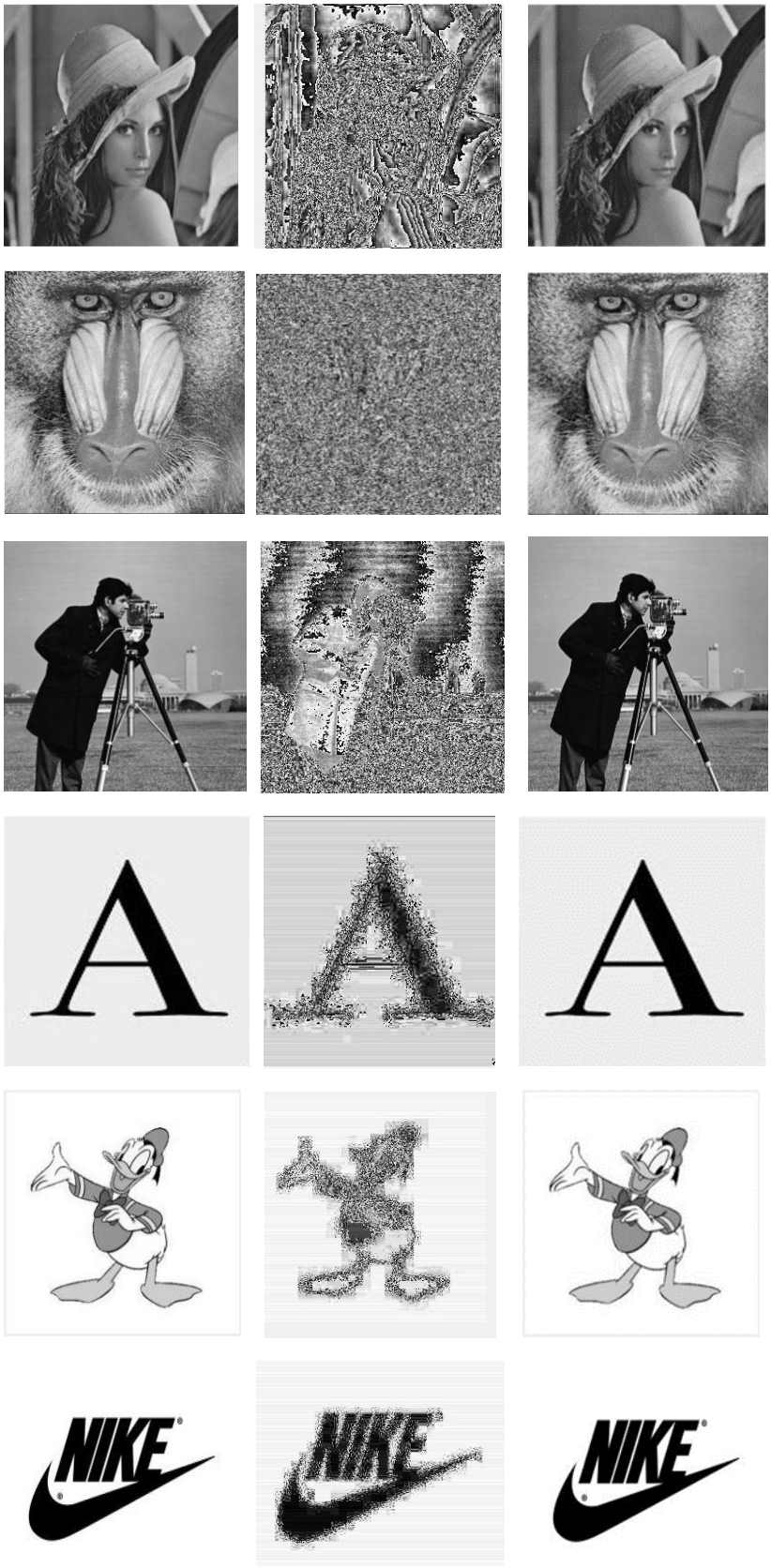


Figure (4.2.a): Henon Encryption/ Decryption Processes

4.4.2 DNA Encryption/ Decryption Processes

Original image **ciphered image** **decryption image**

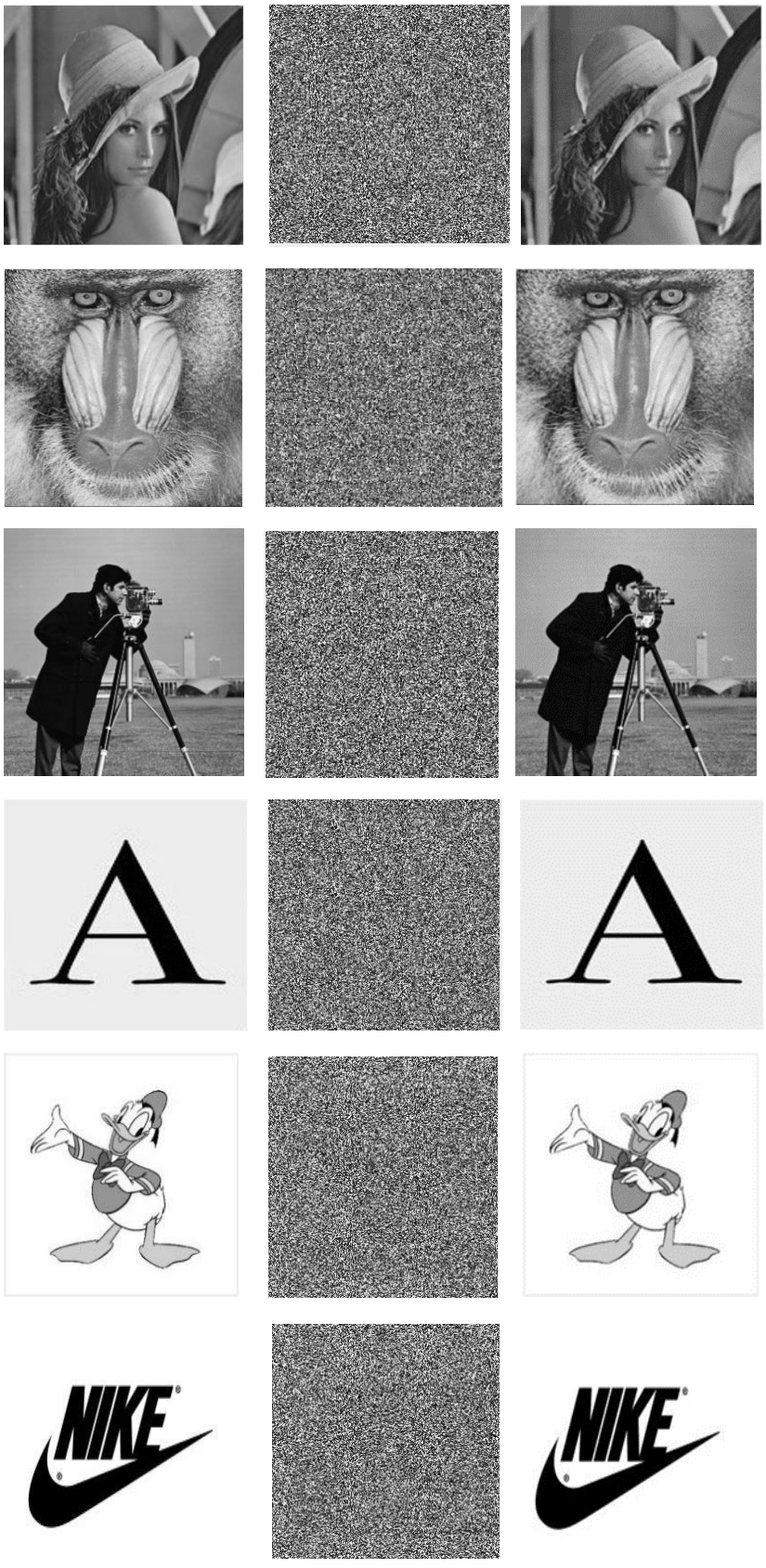


Figure (4.2.b): DNA Encryption/ Decryption Processes

4.4.3 Mix (Henon-DNA) Maps (Encryption/ Decryption) Processes

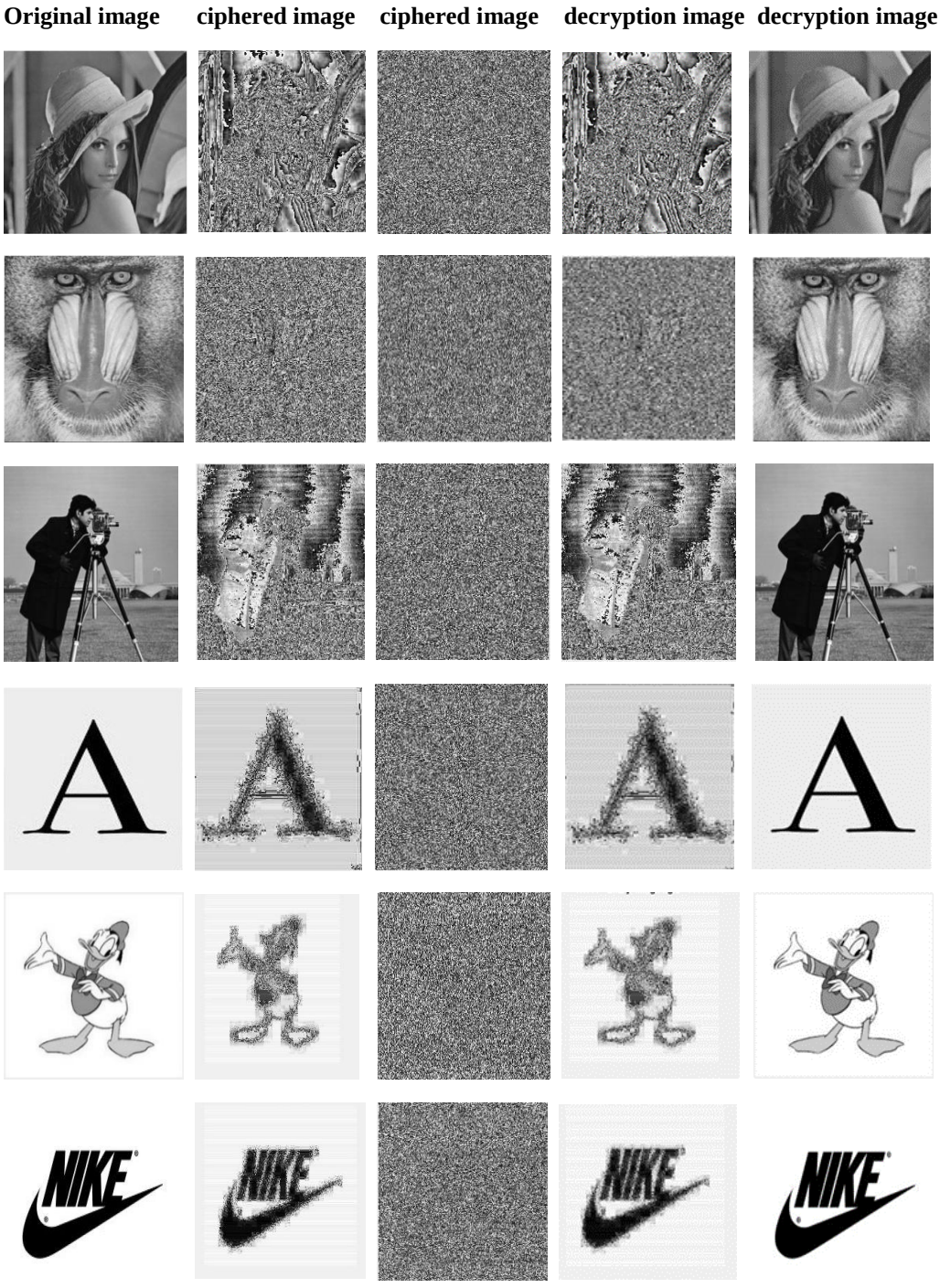
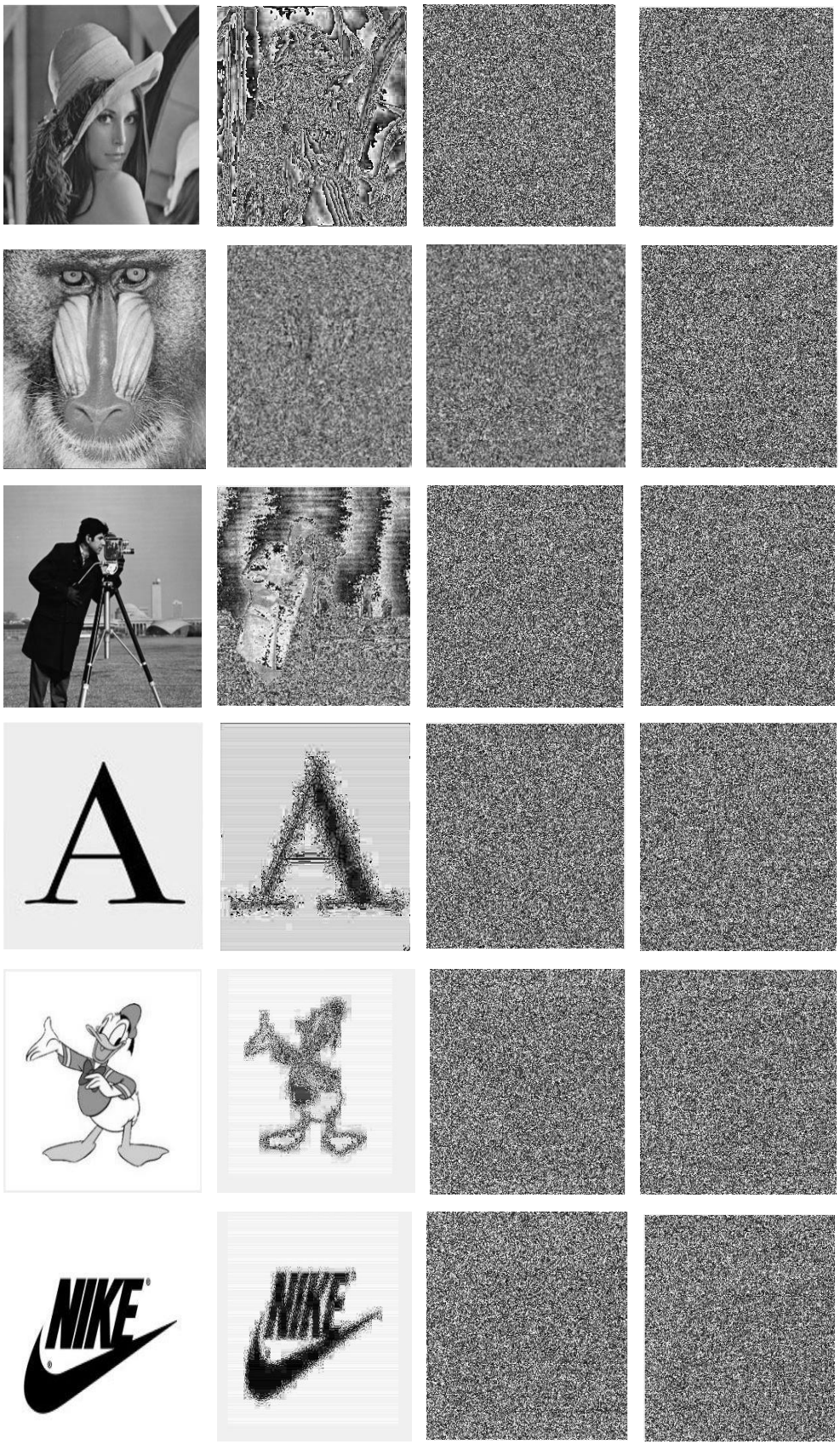


Figure (4.2.c): Mix (Henon-DNA) Encryption/ Decryption Processes

Figure (4.3) shows a comparisons between the original image shows the three types of encryption algorithms: Henon, DNA, and mix (Henon- DNA) maps respectively



(a) **(b)** **(c)** **(d)**

Figure (4.3): (a) original image. (b) Henon encrypted image map. (c) DNA encryped image map. (d) Mix (Henon-DNA) Encrypted image maps

The encrypted images and the input images have no links, as can be seen in the diagram above in Figure (4.3). As a result, the cryptography performance is satisfactory. Also it can be seen that the Henon map is not suitable for all images such as 'A', 'Duck', and 'Nick'. While the rest images good.

4.5 Performance Metrics

To evaluate the security and cryptography performances, several measurement metrics are used as bellow:

4.5.1 Statistical Analysis

Several metrics used for this type analysis such as:

A. Visual Histogram Test

Using the proposed method, examined the histograms of several images as well as their crypto algorithms, the used images 'Lena,' 'Baboon,' ' cameraman' 'A,' 'Duck,' and 'Nike Coronary', as well as their histograms and their encryption equivalents are shown in Figures (4.4), (4.5), and (4.6) for the three types of encryption algorithms. Clearly, the encryption images graphs are symmetrical and differ significantly from those of their matching the original images.

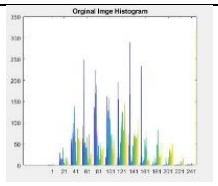
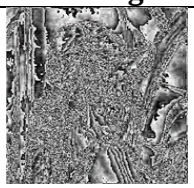
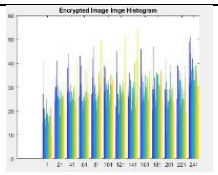
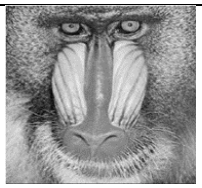
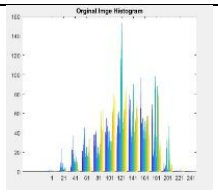
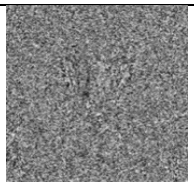
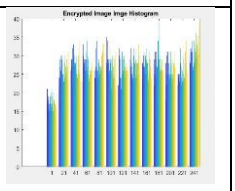
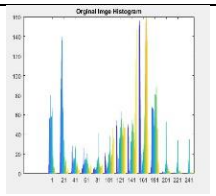
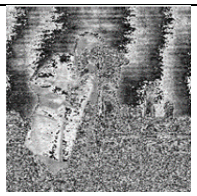
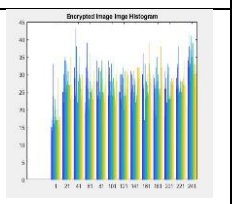
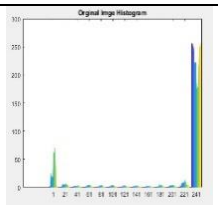
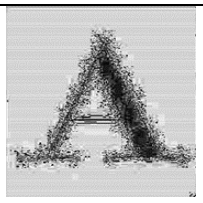
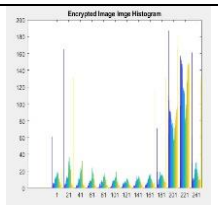
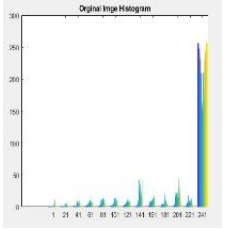
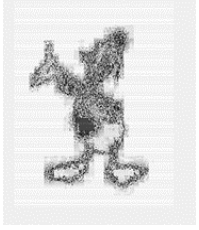
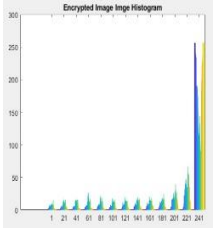
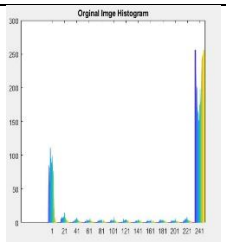
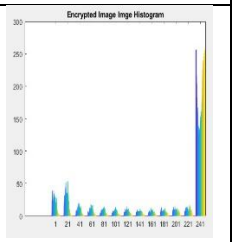
Image	Original Image	Histogram	Encryption Image	Histogram
Lena				
Baboon				
cameraman				
A				
Duke				
Nike				

Figure (4.4): Histogram of (Original / Encrypted) Images using Henon map.

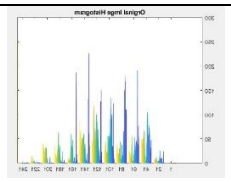
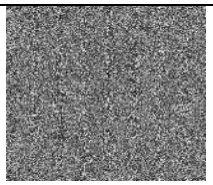
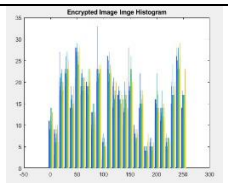
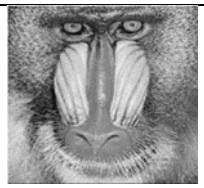
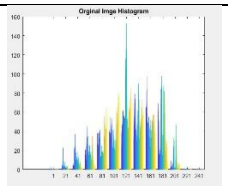
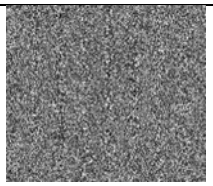
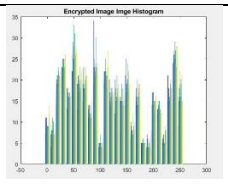
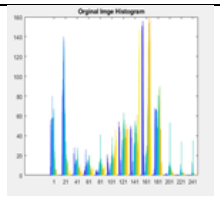
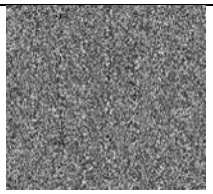
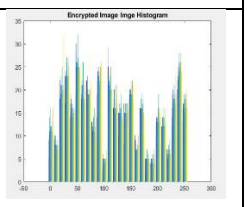
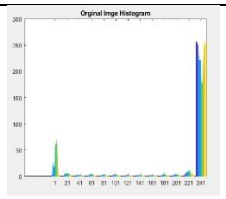
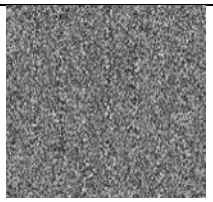
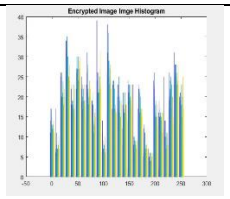
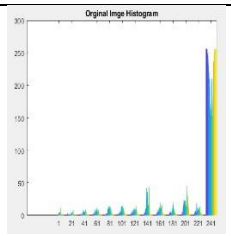
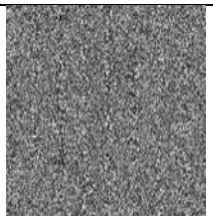
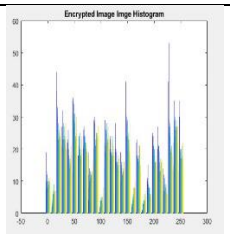
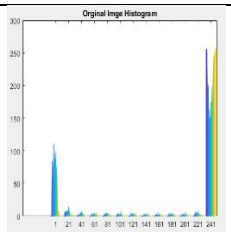
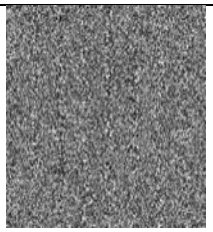
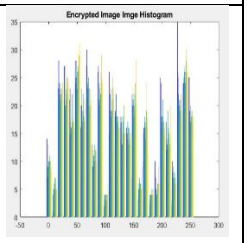
Image	Original Image	Histogram	Encryption Image	Histogram
Lena				
Baboon				
camerama n				
A				
Duke				
Nike				

Figure (4.5): Histogram of (Original / Encrypted) Images Using DNA map.

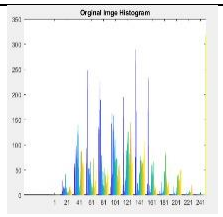
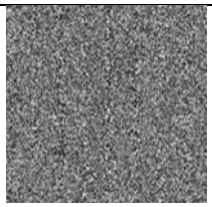
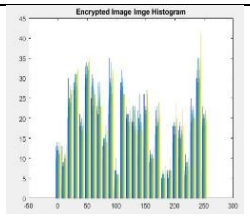
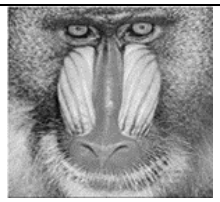
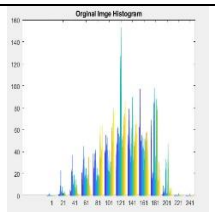
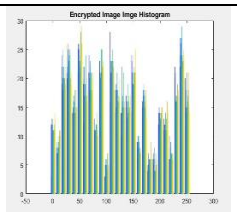
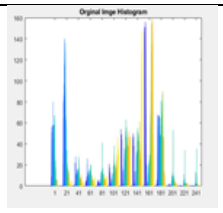
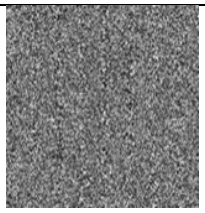
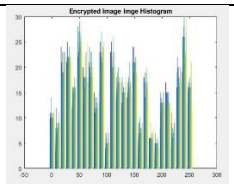
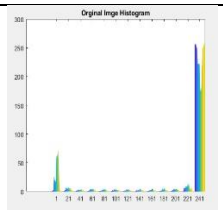
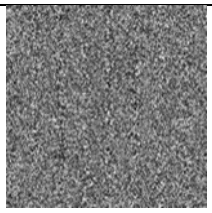
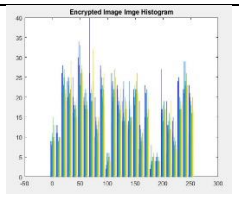
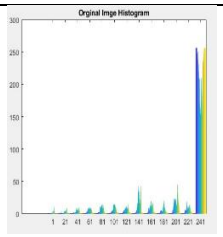
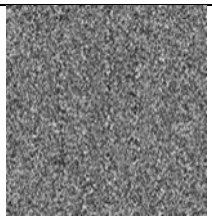
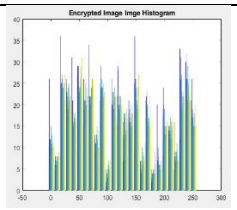
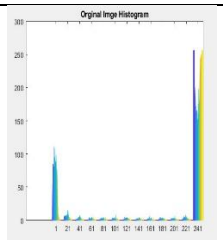
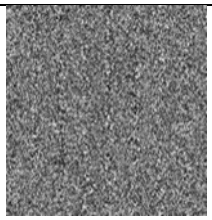
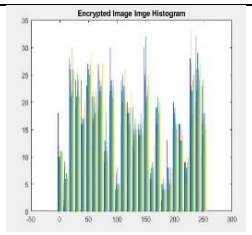
Image	Original Image	Histogram	Encryption Image	Histogram
Lena				
Baboon				
camera man				
A				
Duke				
Nike				

Figure (4.6): Histogram of Original Images and Encrypted Images using Mixing Algorithm (Henon –DNA) maps

B. Keys Space Analysis

The complete group of keys that can be utilized in the cryptography system is referred to as the secret key. A good image encryption methods should have plenty of key space and make attacks impossible. This analysis for:

- Henon map

In the proposed encryption technique, Henon map is used whose initial conditions are computed to produce secret key. The key size of the suggested cryptography consists of the following elements: initial conditions (v), and (a,b). Where a, b ∈ (0.3, 1.4). All this makes the possibility of a successful brute force attack low but not for all grey images (the images that has a high correlation adjacent pixels as in mage (character A, Duck, Nike).

- DNA Map

The key size of the suggested cryptography using DNA map consists of the following elements: The initial value (v), prime numbers p1 and p2, seed value (s), DNA dynamic rules, and adapting Shifting-Complement operations. All these makes the possibility of a successful brute force attack is low.

- Henon-DNA Maps

Further, in the proposed encryption technique, two types of maps are used whose initial conditions are computed differently using secret keys. The key size of the suggested cryptography consists of the following elements: the initial value (v), initial conditions (a, b), where a, b ∈ (0.3, 1.4) to generate Henon ciphered keys. The prime numbers p1 and p2, seed value (s), keys (k) to generate DNA ciphered keys, with the dynamic rules and shift-complement operations. All this makes the possibility of a successful brute force attack impossible and low.

C. Keys Sensitivity Analysis

For a good image encryption technique, encryption must be highly sensitive to the secret key. This analysis for:

- Henon map

Any change of the initial (v) and (a,b) in the secret key should produce an entirely different cipher image.

- DNA Map

Any change in the prime numbers p1 and p2, the initial value (v), seed value (s), consist the secret key that reflects on dynamic rules should produce an entirely different cipher image.

- Henon-DNA Maps

Any change in initial values for each map producing their secret keys with the adaptive operations should produce an entirely different cipher image.

4.5.2 Correlation

The relationship among neighboring visual pixel image and their encryption images is clarified in this section. Pixel values are very close to neighboring pixel values in a horizontally, vertically, and diagonally directions in an original image. Leads to a fact, that the relation between adjacent pixels is strong.

This gap can be used by the cipher agent to encrypt files. This interpreted that the adjacent pixels in the encoded model must be mutually independent.

Figure (4.7 (a-c)) illustrate the correlated coefficient (horizontal, vertical, and diagonal) for ‘Lena’, ‘Baboon’, ‘cameraman, ‘A’, ‘Duck’ and ‘Nike encrypted by Henon, DNA, and Mixing maps. As it could be observed in the graph, the encryption images correlations are close to zero as shown in table (4.1. (a-c)).

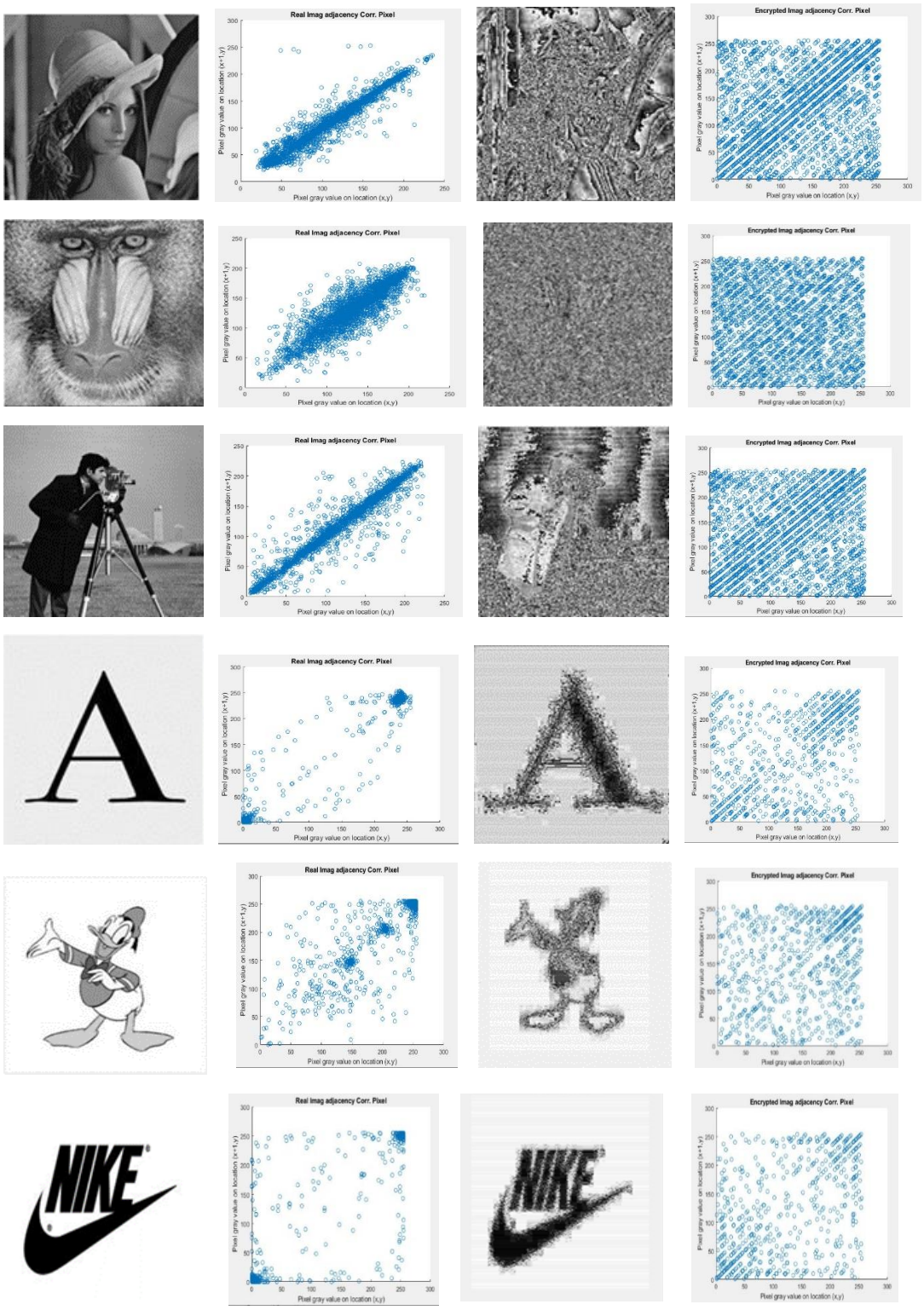
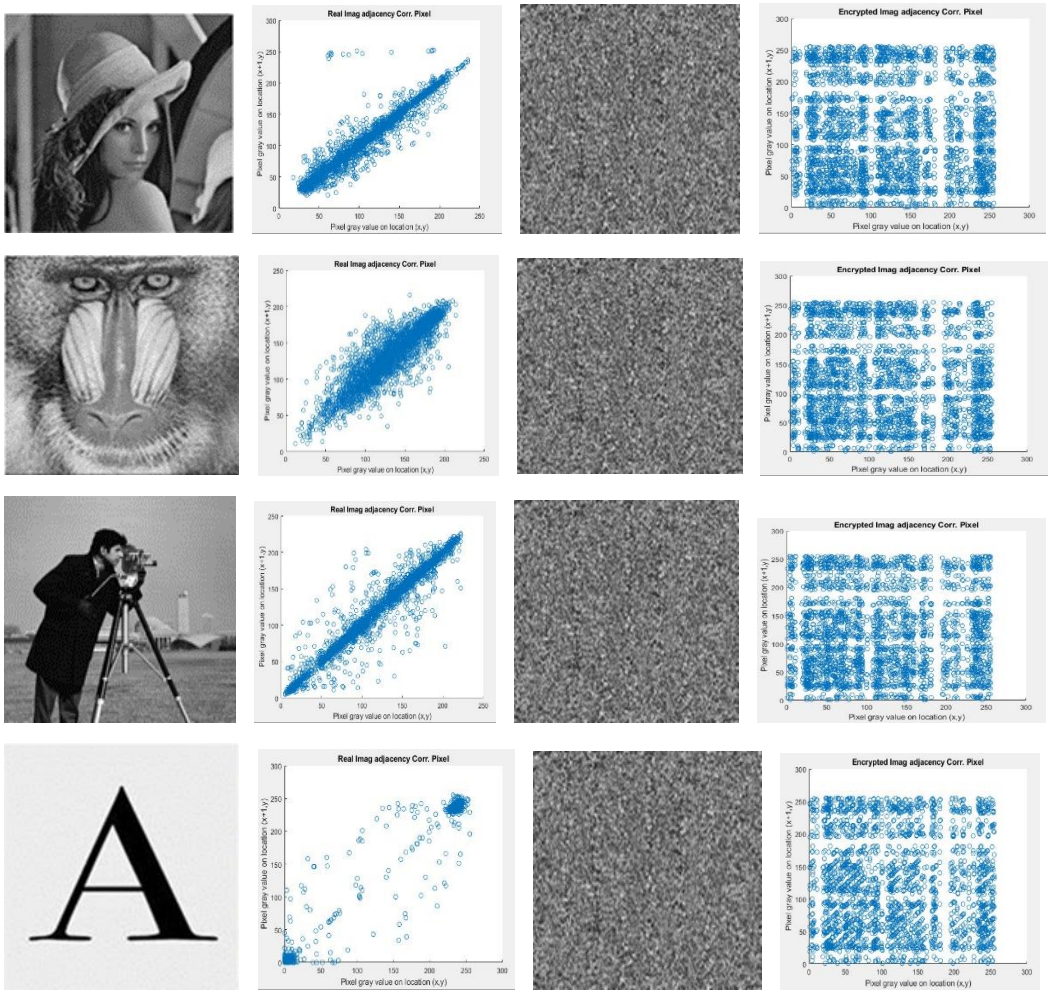


Figure (4.7.a): Correlation Coefficient of (Original / Encryption) Images by Henon map

Table (4.1.a): Correlation Coefficient of (Original / Encryption) Images by Henon map

Images	Original Image			Encryption Image		
	horizontally	vertically	Diagonally	horizontally	vertically	diagonally
Lena	0.95394	0.97336	0.9237	0.24534	0.36438	0.18505
Baboon	0.87353	0.82969	0.7833	0.013428	0.02673	0.0016369
cameraman	0.96115	0.96831	0.93277	0.21461	0.23569	0.15377
A	0.98297	0.98095	0.96566	0.66242	0.67734	0.58691
Duke	0.88419	0.8844	0.7987	0.63669	0.63293	0.62097
Nike	0.96867	0.98597	0.94496	0.88516	0.89361	0.86717



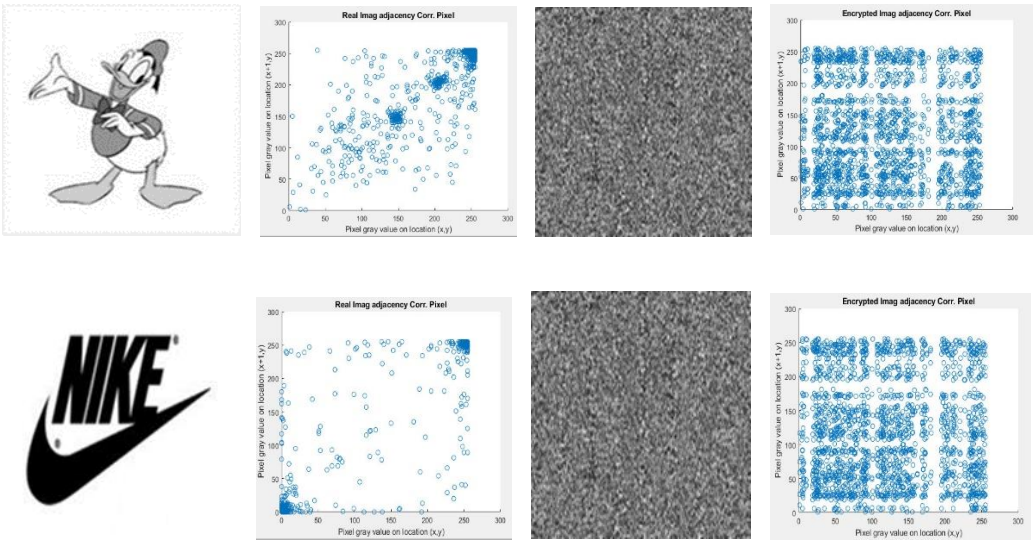


Figure (4.7.b): Correlation Coefficient of Original / Encryption Images by DNA map

Table (4.1.b): Correlation Coefficient of Original / Encryption Images by DNA map

Images	Original Image			Encryption Image		
	Horizontally	Vertically	Diagonally	Horizontally	Vertically	Diagonally
Lena	0.93704	0.97336	0.90711	0.0015677	-0.0021355	-0.0007801
Baboon	0.92585	0.90676	0.87573	-0.004076	-0.001575	0.00017506
cameraman	0.97046	0.9778	0.9512	-0.0089118	-0.0021154	-0.0068662
A	0.98294	0.98095	0.96564	-0.015049	0.0088718	-0.0053998
Duke	0.90448	0.90467	0.83342	0.001649	-0.0009813	0.0063782
Nike	0.96869	0.98597	0.94499	-0.0061715	0.0081078	0.010269

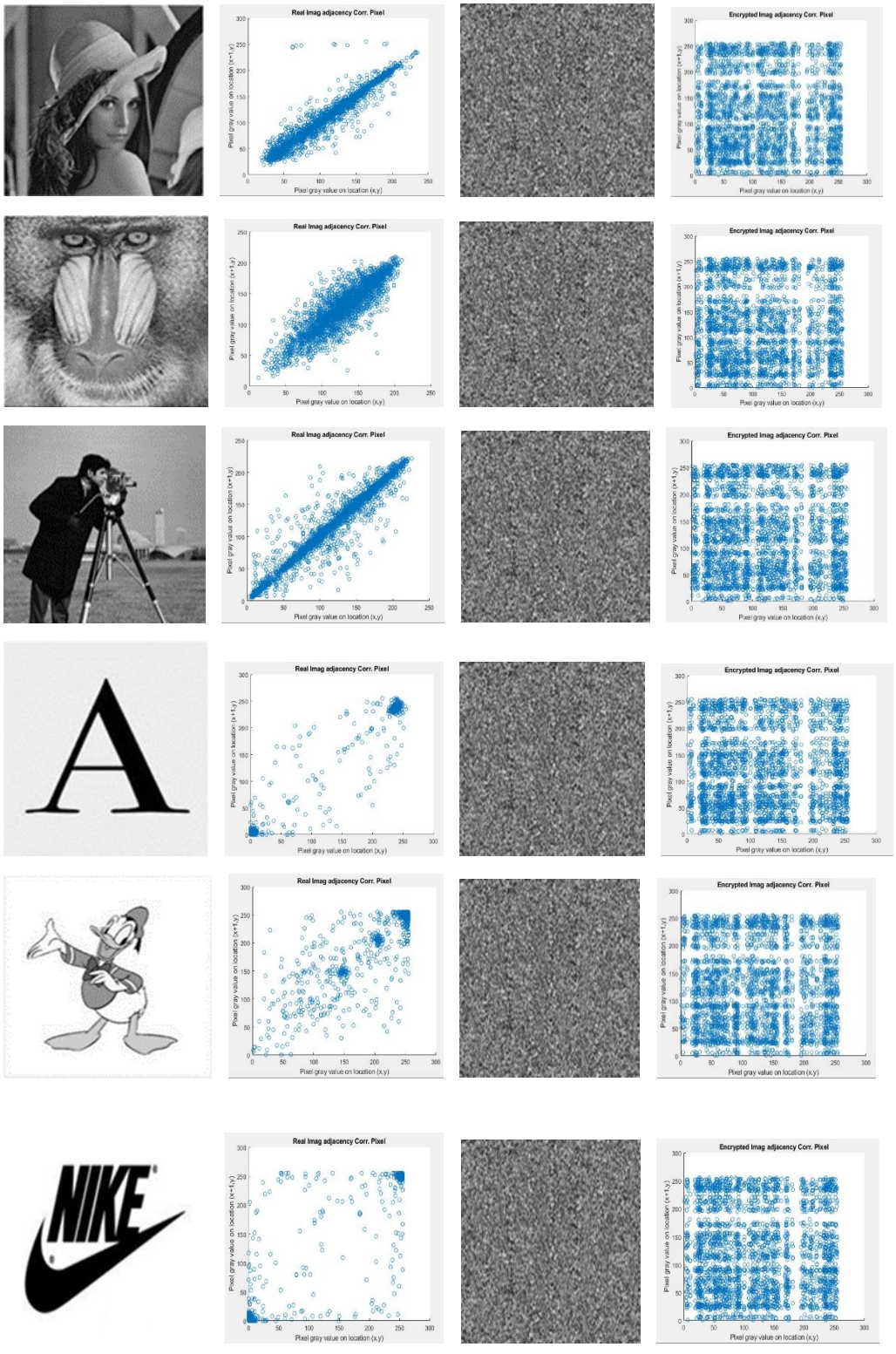


Figure (4.7.c): Correlation Coefficient of (Original / Encryption) Images by Mixing (Henon-DNA) maps

Table (4.1.c): Correlation Coefficient of Original / Encryption Images by Mixing (Henon-DNA) maps

Images	Original Image			Encryption Image		
	Horizontally	Vertically	Diagonally	Horizontally	Vertically	Diagonally
Lena	0.95394	0.97336	0.9237	0.0037672	-0.0042593	-0.00073818
Baboon	0.87353	0.82969	0.7833	-6.8349e-5	0.0035117	0.0036929
Cameramn	0.96115	0.96831	0.93277	-0.0028766	-0.0048235	-0.0028002
A	0.98297	0.98095	0.96566	-0.0064071	0.0012578	0.0084741
Duke	0.88419	0.8844	0.7987	-0.0042939	0.0063209	0.004516
Nike	0.96867	0.98597	0.94496	0.0052204	0.007194	-0.0024449

The suggested encryption algorithm meets the criteria of zero correlations and is extremely resistant to correlations-based attack.

4.5.3 Entropy Measurement

Entropy is a statistical measure of randomness, If all pixels occur with same possibility, the perfect entropy is reached, implying that the pixel distributions is regular. The maximal entropy, or perfect entropy, is $\log^2 = 8$ bits. Table (4.2) shows that the mean and variation of the entropy of the various algorithm. The proposed encryption solution achieves a means entropy that is extremely near to 8, indicating that our cryptosystem has good diffusion performance.

Table (4.2): Entropy of: original image, Henon encrypted images, DNA encrypted images, Mixing (Henon-DNA) encrypted images

Image	original image	Henon encrypted images	DNA encrypted images	Mixing encrypted images
Lena	7.4159	7.9649	7.485	7.4756
Baboon	7.2357	7.9873	7.4847	7.4747
cameraman	7.5829	7.9891	7.4858	7.4797
A	2.824	5.589	7.405	7.3313
Duke	2.8289	5.3496	7.1857	7.2977
Nike	2.1911	5.0534	7.1114	7.2914

4.5.4 NPCR – UACI

The encryption algorithm is very sensitive to minor change in the source images, which is a suitable encryption strategy (e.g., a single pixel change). Two typical quantified measurements are used in this context: NPCR (amount of pixels variation) and UACI (Overall area change percentage). The NPCR is used to count the variation of different pixel. The UACI, on the other hand, describes the average intensities values.

Table (4.3) shows the mean and variance for the UACI and NPCR for the three types of encryption methods. As a result, the suggested technique is extremely sensitives to slight change in the source image's pixels.

Table (4.3): UACI and NPCR of: (A) Henon encrypting images, (B) DNA encrypting images, and (C) Mixing Henon-DNA encrypting images

Image	A		B		C	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.5445	28.6992	99.5099	28.6833	99.6340	28.7051
Baboon	99.6094	27.3071	99.6094	28.0547	99.3394	28.2453
cameraman	99.6088	30.0289	99.6058	29.9399	99.6675	29.894
A	99.6074	15.6547	99.6093	45.5172	99.4394	45.3982
Duke	99.5094	11.0044	99.6064	47.8573	99.6453	48.5184
Nike	99.4494	8.5687	99.6394	49.4731	99.6744	50.0003

4.5.5 Peak Signal-to- Noise Ratio (PSNR)

Peak signal to noise ratio (PSNR) is used to show the quantitative analysis of the encryption techniques. The higher the PSNR, the closer the encoded image is to the original image. Where, the high PSNR value should correlate with a higher quality image. Whenever the PSNR is low as possible, the encryption scheme is good. The measurement of PSNR for the ciphered images using Henon, DNA, and mixing (Henon- DNA) maps are shown in table (4.4).

Table (4.4): PSNR Comparison between the ciphered images by Henon, DNA, and Mixing (Henon-DNA) maps

Image	PSNR of Henon map	PSNR of DNA map	PSNR of Mixing (Henon-DNA) maps
Lena	**9.1861**	**9.0825**	**9.079**
Baboon	**9.7186**	**9.5554**	**9.502**
cameraman	**8.7529**	**8.824**	**8.8275**
A	**12.4437**	**5.3998**	**5.4069**
Duke	**14.3483**	**4.9989**	**4.913**
Nike	**16.0929**	**4.7438**	**4.7005**

4.5.6 Execution Time

The amount of time required by the proposal algorithm to execute both encryption and decryption process is shown in table (4.5). The execution time is calculated in seconds.

Table (4.5): Amount of Time Encryption by proposed system

Image	Encryption by Henon map Time in Sec.	Encryption by DNA map Time in Sec.	Encryption by Mixing (Henon-DNA) maps Time in Sec.
Lena	**14.938**	**168.036**	**214.126**
Baboon	**13.032**	**167.606**	**198.132**
cameraman	**12.984**	**171.053**	**211.620**
A	**14.595**	**170.353**	**195.101**
Duke	**12.268**	**175.260**	**201.861**
Nike	**12.170**	**166.519**	**195.774**

4.6 Comparative Analysis

In this section, a comparison between the proposed system and [14] from the measurements bellow:-

4.6.1 Entropy

Comparison between the proposed system and [14] of entropy for two images (lena, cameraman), Entropy is a statistical indicator of randomness. If all pixels

occur with the same probability, perfect entropy is attain, indicating that the distribution of pixels is regular. Tables (4. 6) illustrate the comparisons.
, and correlation coefficients for two images (lena, cameraman). Tables (4.(6,7,8,9,10)) illustrate the comparisons.

Table (4.6) Comparison of Entropy between the proposed system and [14]

Image	Entropy in the proposed system			Entropy [14]	Status
	Henon	DNA	Mixing		
Lena	7.9649	7.485	7.4756	7.5892	different
cameraman	7.9891	7.4858	7.4797	7.1096	different

4.6.2 UACI and NPCR

Comparison between the proposed system and [14] of UACI and NPCR for two images (lena, cameraman) A good encryption method is one in which the encryption algorithm is extremely sensitive to even little changes in the source images. Tables (4.7),(4.8) illustrate the comparisons.

Table (4.7) Comparison of UACI and NPCR between the proposed system (Lena) and [14]

Image	UACI and NPCR in the proposed system (Lena)			UACI, NPCR [14]	Status
	Henon	DNA	Mixing		
UACI	28.6992	28.6833	28.7051	27.5706	different
NPCR	99.5445	99.5099	99.6340	90.1978	different

Table (4.8) Comparison of UACI and NPCR the proposed system (cameraman) and [14]

Image	UACI and NPCR in the proposed system (cameraman)			UACI , NPCR and [14] (cameraman)	Status
	Henon	DNA	Mixing		
UACI	30.0289	29.9399	29.894	28.8406	different
NPCR	99.6088	99.6058	99.6675	91.7114	different

4.6.3 Correlation Coefficients

Comparison between the proposed system and [14] of Correlation Coefficients for two images (lena, cameraman). It is made clear how surrounding visual pixel images relate to their encryption images. Tables (4.9),(4.10) illustrate the comparisons.

Table (4.9): Comparison of Correlation Coefficient between the proposed system (Lena) and [14]

Image	Correlation Coefficient of (Lena) in the proposed system			Correlation Coefficient [14] (Lena)	Status
	Henon	DNA	Mixing		
Horizontally	0.24534	0.0015677	0.0037672	-0.0041	different
Vertically	0.36438	-0.0021355	-0.0042593	-0.0037	different
Diagonally	0.18505	-0.0007801	-0.00073818	-0.0065	different

Table (4.10): Comparison of Correlation Coefficient between the proposed system (cameraman) and [14]

Image	Correlation Coefficient of (cameraman) in the proposed system			Correlation Coefficient [14] (cameraman)	Status
	Henon	DNA	Mixing		
Horizontally	0.21461	-0.0089118	-0.0028766	-0.0015	different
Vertically	0.23569	-0.0021154	-0.0048235	-0.0143	different
Diagonally	0.15377	-0.0068662	-0.0028002	-0.0236	different

4.7 Summary

This chapter presented implement and discussion for the results of the proposed system techniques. The proposed system techniques have been compared with other well-known techniques and evaluating its performances by some metrics

such as (PSNR, MSE, Histogram, and Correlation). Example for implementation of the proposed method has been presented. The experimental results show that the power of the proposed system techniques had encrypt and decrypt the secret message with a high level of security.

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

5.1 Introduction

A good image encryption technique needs to be faster, meet real time constraints and robust against various attacks. The efficient storage and representation of data in encryption is important. A number of chaos and DNA based encryption schemes have been implemented in this thesis which are secure and suitable for image encryption. In this thesis, some contributions have been made to combine Henon image encryption with DNA map. In this chapter, the entire work of the proposed thesis is concluded and the possibilities of future works for the applications that can be implemented by the proposal techniques.

5.2 Conclusion

1- Unknowing which coefficient were partially encrypted by the intruder gives the proposal algorithm an efficiency in providing strength security.

2- Employing DNA random mapping, because it possesses better flexibility and pseudo-randomness, and its parameters have a wider range of mapping.

3- Using the dynamic DNA coding rules, the encryption process becomes more complicated and harder to predicate because of the procedure mechanism applied in this thesis.

5.3 Future Work

The proposed system can be investigated as a future work for:

- Implementing other types of chaos
- Colored images, videos, audios data.

REFERENCES

REFERENCES

[1] Chen, Y., Xie, S., & Zhang, J. (2022). A hybrid domain image encryption algorithm based on improved henon map. Entropy, 24(2), 287.

[2] " District, W. S., & Jolaade, I. A. Information Security and Corporate Performance of Public Organisations in Ogun.

[3] Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. Entropy, 23(3), 341.

[4] Megías, D., Mazurczyk, W., & Kuribayashi, M. (2021). Data Hiding and Its Applications: Digital Watermarking and Steganography. Applied Sciences, 11(22), 10928.

[5] Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. IEEE Access, 8, 166589-166611.

[6] Kesa, N. R. K. (2018). Steganography a data hiding technique.

[7] Ali M. N, Gil M. M, (2020). Analysis of design goals of cryptography algorithms based on different components. 77(23), 31397-31426.

[8] Latif, I. H. (2020, February). Time evaluation of different cryptography algorithms using labview. In IOP Conference Series: Materials Science and Engineering (Vol. 745, No. 1, p. 012039). IOP Publishing.

[9] Shaukat, S., Arshid, A. L. I., Eleyan, A., SHAH, S. A., & AHMAD, J. (2020). Chaos theory and its application: An essential framework for image encryption. Chaos Theory and Applications, 2(1), 17-22.

[10] Khan, J. S., Ahmad, J., Ahmed, S. S., Siddiqa, H. A., Abbasi, S. F., & Kayhan, S. K. (2019). DNA key based visual chaotic image encryption. Journal of Intelligent & Fuzzy Systems, 37(2), 2549-2561.

[11] Kolate, V., & Joshi, R. B. (2021). An Information Security Using DNA Cryptography along with AES Algorithm. Turkish Journal of Computer and Mathematics Education, 12(1S), 183-192.

[12] Al-Mahdi, H., Alruily, M., Shahin, O. R., & Alkhaldi, K. (2019). Design and analysis of DNA encryption and decryption technique based on asymmetric cryptography system. International Journal of Advanced Computer Science and Applications, 10(2).

[13] Khan, J. S., & Ahmad, J. (2019). Chaos based efficient selective image encryption. Multidimensional Systems and Signal Processing, 30(2), 943-961.

[14] Khan, J. S., Boulila, W., Ahmad, J., Rubaiee, S., Rehman, A. U., Alroobaea, R., & Buchanan, W. J. (2020). DNA and plaintext dependent chaotic visual selective image encryption. IEEE Access, 8, 159732-159744.

[15] Li, Z., Peng, C., Tan, W., & Li, L. (2021). An effective chaos-based image encryption scheme using imitating jigsaw method. Complexity, 2021.
[16] Noura, M., Noura, H., Chehab, A., Mansour, M. M., Sleem, L., & Couturier, R. (2018). A dynamic approach for a lightweight and secure cipher for medical images. Multimedia Tools and Applications, 77(23), 31397-31426.
[17] Pandurangi, Bhagyashree & Sangolli, Vinay & Patil, Meenakshi. (2020). Fast Partial Image Encryption using Chaos. 3. 19-24.
[18] Zhang, J., Hou, D., & Ren, H. (2016). Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system. Mathematical Problems in Engineering, 2016.
[19] Kumar, A., & Raghava, N. S. (2020). Selective colour image encryption using Hénon chaotic system with a keyless substitution cipher. Engineering and Applied Science Research, 47(1), 66-76.
[20] Mutnuru, S., Sah, S. K., & Kumar, S. P. (2020). Selective encryption of image by number maze technique. Int. J. Cryptogr. Inf. Secur, 10(2), 1-10.
[21] Akkasaligar, Dr. Prema & Biradar, Sumangala. (2020). Selective medical image encryption using DNA cryptography. Information Security Journal: A Global Perspective. 29. 1-11. 10.1080/19393555.2020.1718248.
[22] Jang, W., & Lee, S. Y. (2020). Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment. International Journal of Distributed Sensor Networks, 16(3), 1550147720914779.
[23] Liu, L., Wang, D., & Lei, Y. (2020). An image encryption scheme based on hyper chaotic system and DNA with fixed secret keys. IEEE Access, 8, 46400-46416.
[24] Liu, M., & Ye, G. (2021). A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm. Mathematical Biosciences and Engineering, 18(4), 3887-3906.
[25] Liu, Y., Qin, Z., Liao, X., & Wu, J. (2020). A chaotic image encryption scheme based on Hénon–Chebyshev modulation map and genetic operations. International Journal of Bifurcation and Chaos, 30(06), 2050090.
[26] Zheng, J., & Liu, L. (2020). Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Processing, 14(11), 2310-2320.
[27] Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Masood, F., Khan, F., & Buchanan, W. J. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. IEEE Access, 8, 140876-140895.

[28] Wu, J., Liao, X., & Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. Signal processing, 153, 11-23.
[29] Zhang, X., Han, F., & Niu, Y. (2017). Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding. Computational intelligence and neuroscience, 2017.
[30] Saranya, M. R., Mohan, A. K., & Anusudha, K. (2014, November). A composite image cipher using DNA sequence and genetic algorithm. In 2014 International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1022-1026). IEEE.

[31] Tresor, L. O., & Sumbwanyambe, M. (2019). A selective image encryption scheme based on 2d DWT, Henon map and 4d Qi hyper-chaos. IEEE Access, 7, 103463-103472.

[32] Soleymani, A., & Nordin, M. J. (2021). Selective Image Encryption Based On Chaotic Maps And Elliptic Curve Cryptography.

[33] Hu, Y., & Tian, R. (2020). Image encryption and decryption based on chaotic algorithm. Journal of Applied Mathematics and Physics, 8(9), 1814-1825.
[34] Fang, J. S., Tsai, J. S. H., Yan, J. J., Chiang, L. H., & Guo, S. M. (2022). Secure Data Transmission and Image Encryption Based on a Digital-Redesign Sliding Mode Chaos Synchronization. Mathematics, 10(3), 518.
[35] Yousif, B., Khalifa, F., Makram, A., & Takieldeen, A. (2020). A novel image encryption/decryption scheme based on integrating multiple chaotic maps. AIP Advances, 10(7), 075220.

[36] May, R. (1976). Simple mathematical models with very complicated dynamics. Nature, 261: 459-467.

[37] Soleymani, A., Nordin, M. J., & Sundararajan, E. (2014). A chaotic cryptosystem for images based on Henon and Arnold cat map. The Scientific World Journal, 2014.
[38] Zhang, J., Hou, D., & Ren, H. (2016). Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system. Mathematical Problems in Engineering, 2016.

[39] Dena, A., & Salah, A. (2018). Image encryption algorithm based on RC4 and Henon map. J Theor Appl Inf Technol, 96(21), 7065-7076.

[40] Mondal, M., & Ray, K. S. (2019). Review on DNA cryptography. arXiv preprint arXiv:1904.05528.

[41] Geeksforgeeks.org Sovereign Corporate Tower, (2021).DNA Cryptograph.18 Oct. Sector-136, Noida, Uttar Pradesh - 201305
[42] Khalifa, A. (2021). A secure steganographic channel using DNA sequence data and a bio-inspired XOR cipher. Information, 12(6), 253.

[43] Liu, M., & Ye, G. (2021). A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm. Mathematical Biosciences and Engineering, 18(4), 3887-3906.
[44] Zheng, J., & Liu, L. (2020). Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Processing, 14(11), 2310-2320.
[45] Rehman, A., Liao, X., Kulsoom, A., & Abbas, S. (2015). Selective encryption for gray images based on chaos and DNA complementary rules. Multimedia Tools & Applications, 74(13).
[46] Akhavan, A., Samsudin, A., & Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. Optics & Laser Technology, 95, 94-99.
[47] Liao, X., Hahsmi, M. A., & Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik-International Journal for Light and Electron Optics, 153, 117-134.

[48] Li, Z., Peng, C., Tan, W., & Li, L. (2020). A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation. Applied Sciences, 10(21), 7469.
[49] " Instruments, N. (2013). Peak signal-to-noise ratio as an image quality metric.

الـخـلاصـــــــــة

يتطلب الانتشار السريع لتطبيقات الشبكة في جميع مجالات الحياة حماية أكبر للبيانات. في الآونة الأخيرة، هناك طلب متزايد على العالم الرقمي بأشكاله المختلفة. الصور الرقمية هي أحد الأشكال التي أصبحت أكثر أهمية. يمثل تأمين وحماية بيانات الصورة تحديًا للمتطلبات الحسابية الواجبة لعمليات التشفير وفك التشفير. كما أن الخوارزميات القياسية للتشفير التقليدية ليست آمنة بدرجة كافية في حالة الصور الرقمية بسبب خصائص الصور مثل التكرار العالي للمعلومات والارتباط العالي بين وحدات البيكسل. ومن أجل التعامل مع هذه المخاوف، فإن تقنيات تشفير الصور المبتكرة مطلوبة مثل النظرية الغير منتظمة، وأصبحت المفاهيم للحمض النووي (DNA) شائعة لضمان أمان وحماية الصورة.

في هذه الرسالة، تم اقتراح طرق التشفير / فك التشفير القائمة على تقنيات تشفير DNA map لإنتاج مخطط فعال لتشفير الصور. يتمثل هذا في التشفير الجزئي باستخدام خريطة Henon ثنائية الأبعاد وخريطة DNA وتشفير DNA الديناميكي؛ عن طريق تحليل مستوى الصورة الأصلي ذي التدرج الرمادي إلى مستويين (MSB، LSB) ، حيث يكون MSB هو الشاغل الرئيسي لخوارزمية التشفير الجزئي. تجمع الخوارزمية بين النظرية الغير منتظمة وحساب الحمض النووي في إطار سيناريو يتضمن ثلاثة أنواع من خوارزمية التشفير (2D-Henon و DNA و (mix (Henon-DNA)، كل نوع يتضمن جولتين: الجولة الأولى: إنشاء مفاتيح التشفير. الجولة الثانية: ختم البكسل الأول من MSB بالقيمة الأولية كختم تجاري لهذا المستوى ليتم تشفيره بواسطة المفاتيح التي تم إنشاؤها. خطوة الختم لمساعدة المتلقي في فحص الصورة المشفرة إذا كانت سليمة أم لا.

بينما تم استخدام الحمض النووي في هذه الرسالة في اتجاهين ، أولاً: إنشاء مفاتيح تشفير باستخدام تسلسل الحمض النووي من المركز الوطني لمعلومات التكنولوجيا الحيوية (NCBI) لأنشاء خوارزمية مطابقة الطول مع الصورة الاصلية لتوفير مناعة ضد الهجمات. الاتجاه الثاني ، كآلية ديناميكية لقواعد الترميز. تعمل هذه الآلية على إضافة مرفقًا آمنًا آخر في عدم توقع أو الحصول على سيناريو طريقة تشفير الصور.

تجرى التجارب على صور قياسية مختلفة بخصائص مختلفة. هذه الصور الرمادية بحجم ٢٥٦ × ٢٥٦ من أنواع مختلفة. لضمان تحسين خوارزمية التشفير

تم قياس أداء أمان وفعالية الخوارزمية المقترحة من خلال سلسلة من الاختبارات مثل:

histogram analysis, correlation, entropy, NPCR, UACI, and PSNR

الاختبارات مطبقة على ثلاثة أنواع من التشفير مع المقارنة.

تظهر النتائج في الفصل الرابع أن DNA map يتجاوز مشاكل Henon map التي تعاني من ضعف في الانتشار الكامل لصور التكرار العالي للمعلومات ، والارتباط العالي بين وحدات البكسل.

وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية العلوم للبنات
قسم علوم الحاسوب

الطريقة الهجينة لتشفير الصور باستخدام الحامض النووي والخريطة الفوضوية

رسالة

مقدمة إلى مجلس كلية العلوم للبنات -جامعة بابل وهي جزء من متطلبات نيل شهادة الماجستير في العلوم/علوم الحاسبات

من قبل

محمد جاسم نجم المسعودي

بإشراف

أ.م.د. سحر عادل كاظم

٢٠٢٢