An Image Encryption Technique using Chaotic map and DNA Sequence Operation

---

A Thesis submitted to the Faculty of Engineering & Technology, Jadavpur University in partial fulfillment of the requirements for the Degree of Master of Engineering in Software Engineering

By

HASIBUL RAHAMAN

Examination Roll Number: M4SWE19021

Registration Number: 140976 of 2017-2018

Class Roll Number: 001711002020

Under the Guidance & Supervision of

Mr. Sujit Kumar Das

Assistant Professor

Department of Information Technology

Jadavpur University

Department of Information Technology
Faculty of Engineering and Technology
Jadavpur University (Salt Lake Campus)
Kolkata-700098

2019

Jadavpur University
Department of Information Technology
Faculty of Engineering & Technology

Certificate of Recommendation

I hereby recommend that the thesis, entitled ***"An Image Encryption Technique using Chaotic map and DNA Sequence Operation"*** *prepared by* ***Hasibul Rahaman*** *(Examination Roll Number:* M4SWE19021*, Registration Number:* 140976 *of* 2017-2018*), under my supervision, be accepted in partial fulfillment of the requirements for the Degree of* ***Master of Engineering*** *in* ***Software Engineering*** *from the* ***Department of Information Technology*** *under* ***Jadavpur University****.*

.....

Mr. Sujit Kumar Das

Asst. Professor, Dept. of Information Technology,
Jadavpur University

Counter Signed by:

.....

Head of the Department

Department of Information Technology, Jadavpur University

.....

Dean

Faculty of Engineering and Technology, Jadavpur University

Jadavpur University
Department of Information Technology
Faculty of Engineering & Technology

Certificate of Approval

The foregoing thesis, entitled as ***" An Image Encryption Technique using Chaotic map and DNA Sequence Operation"*** *is hereby approved by the committee of final examination for evaluation of thesis as a creditable study of an engineering subject carried out and presented by* ***Hasibul Rahaman*** *(Examination Roll Number:* M4SWE19021, *Registration Number:* 140976 *of* 2017-2018*) in a manner satisfactory to warrant its acceptance as a perquisite to the Degree of Master of Software Engineering. It is understood that by this approval, the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the thesis only for the purpose for which it is submitted.*

.....

Signature of External Examiner

.....

Signature of Supervisor

Mr. Sujit Kumar Das
Asst. Professor, Dept. of Information Technology,
Jadavpur University

Jadavpur University
Department of Information Technology
Faculty of Engineering & Technology

Declaration of Originality and Compliance of Academic Ethics

I hereby declare that this thesis contains literature survey and original research work by the undersigned candidate, as a part of his Master of Engineering in Software Engineering.

All information in this document has been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all the material and results are not original to this work.

Name (in Block Letter): **HASIBUL RAHAMAN**

Exam Roll Number: **M4SWE19021**

Class Roll Number: **001711002020**

Thesis Title: ***An image Encryption Technique using Chaotic map and DNA Sequence Operation.***

Signature with Date:

Acknowledgement

First of all , I would like to express my profound to my thesis supervisor, ***Mr. Sujit Kumar Das,*** *Assistant professor, Department of Information Technology, Jadavpur University, Kolkata for his outstanding guidance and support during my thesis work. I have been benefited greatly from working under his guidance. His constant motivation and support has been invaluable throughout my studies at Jadavpur University, Kolkata. Without his sustained effort, encouragement and guidance, this project would not have been taken shape. I am grateful to him for the knowledge he imparted and all the necessary facilities he provided to me that led to successful completion of my thesis.*

I would also like to thank our Head of the Information Technology Department, Dr. B. Sardar for his excellent guidance and kind co-operation during the entire study at Jadavpur University, Kolkata.

Let me take this opportunity to spcially thank all the faculty members of Information Technology Department who have directlyor indirectly co-operated and encouraged me during my study course. I wish to extend my sincere thanks to all the staffs and library staff of Jadavpur University, Kolkata, who helped me during the course of my study.

Finally I would like to thank my parents, my family and friends for their constant love and support and for providing me with the opportunity and the encouragement to purse my life goals. Lastly, I would like to thank The Almighty for providing me with this opportunity at Jadavpur University.

HASIBUL RAHAMAN

Abstract

In this thesis, we proposed an image encryption scheme based on Two-dimensional Henon map, four-dimensional hyperchaotic Lorenz system and DNA encoding operation. The proposed image encryption algorithm mainly divided into three main parts. Firstly, we generate a two dimensional random matrix as the same size of the plain image by successive iteration through Henon mapping. Then, the image is divided into some block and we set block size. Next, we select the DNA encoding and decoding method of each sub-block of plaintext image and the random matrix and the DNA operation between the two sub-blocks through the random sequence generated by the four-dimensional hyperchaotic Lorenz system. Finally, we combine all encrypted sub-blocks to get cipher image. We have performed key space analysis, key sensitivity analysis and statistical analysis to demonstrate the security of the proposed image encryption scheme. Experimental result and security analysis proved that the proposed image encryption scheme not only has a good encryption effect but also capable of effectively resisting brute-force attack, statistical attack and differential attack.

Keywords: Image Encryption, Henon Mapping, Hyperchaotic Lorenz system, DNA Encoding, DNA sequence operation, Runge-Kutta method, Security Analysis.

Contents

Topics **Page No.**

List of Tables

List of Figures

Chapter-1
Introduction

1.1 Overview

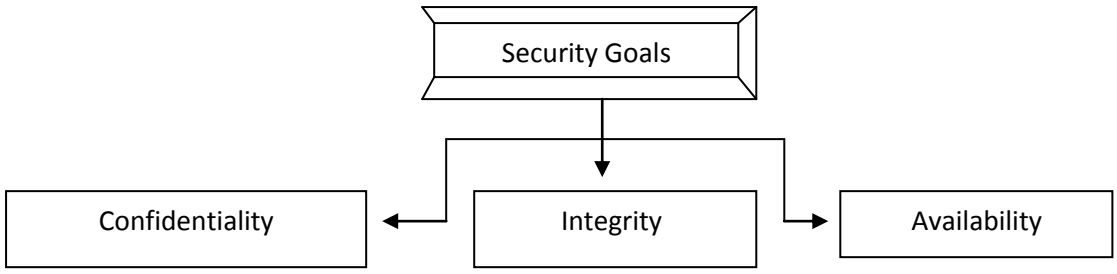
Due to the quick development of network technology and innovation in technologies, images are broadly used in wireless communication, multimedia systems, medical imaging, telemedicine, and military communication. So images can now be considered one of the most usable forms of information. So, the security of the image is very important. Using communication networks, authorized people can send and receive information from a distance. Since the internet is not a secure communication channel. When image sends on the internet, it may be possible that some secret or confidential images can be accessed, stolen or modified by the unauthorized people. The security of digital images involves several different aspects including copyright protection, authentication, confidentiality, and access control. To be secure, information needs to be hidden from unauthorized access that is called confidentiality, protected from the unauthorized change that is integrity and available to an authorized entity, when it is needed that is called availability. So at different stages, namely generation, storing, transmission or distribution of digital images, confidentiality is required. There are various techniques available to ensure the privacy and security of digital images during the transmission. Some popular techniques are image encryption, steganography, secret image sharing and digital watermarking. Among them, image encryption is one of the widely used and popular technique. Like a traditional cryptographic method, image encryption is a process which converts a plain image to an unreadable format which called cipher image. There is some existing text base encryption algorithm which are Data Encryption Standard(DES), AES which is a symmetric encryption algorithm. However, these encryption schemes appear not to be idle for image encryption, due to some inherent characteristic of images, such as high redundancy, the bulk data capacity which are problematic for traditional encryption. Moreover, these, ciphers require high computing power, high computational time and an extra operation on compressed image data. The ciphers are preferable for real-time image encryption which takes a lesser amount of time at the same time without compromising the security.

1.2 Image encryption

Image encryption is the process of encoding image in such a way that eavesdroppers or hackers can not read it, but authorizes parties can read it. The primary thought in the image encryption is to transmit the image safely over the system so no unapproved client can ready to decode the image. The image is encrypted using an encryption algorithm, rotate it into an unreadable image, in an encryption scheme. This is usually done with the use of encryption keys, which specifies how the image is to be encoded. Any adversary that can see the encrypted image should not be able to determine anything about the original image. However using a decryption algorithm, an authorized party is able to decode the encrypted image. That usually requires a secret decryption key, so adversaries do not have access. Basically, two categories of image encryption method: Frequency domain methods and Spatial domain methods. In the frequency domain method, the coefficients of the frequencies of the images are converted. The pixels of the images are straightly manipulated in the form of reducing the correlation among the pixels in the spatial domain method. Normally, the image encryption method in the spatial domain consists of two phases confusion and diffusion. In the confusion phase, the locations of the pixels values are changed. In the diffusion phase, the value of pixels is changed. Nowadays, a number of different techniques have been used to encrypt images such as Chaotic system Optical transform Wave transform, Cellular automata, and Scan pattern and DNA computing.

1.3 Image encryption security goals

There are basically three security goals in image encryption: confidentiality, integrity, and availability. They are described as follows.



1.3.1 Confidentiality

Confidentiality refers to the protection of information from unauthorized access. An undesired communicating party, called an adversary, must not be able to access the communication material. Confidentiality is the most common aspect of information security. It is not only applied for the storage of information but also applies to the transmission of information. That means we need to conceal it during the image transmission.

1.3.2 Integrity

Information needs to be changed constantly. Integrity means that these changes need to be done only by authorized entities and through the authorized mechanism. Integrity violation is not necessarily the result of a malicious act, an interruption in the system may also create unwanted changes in the information.

1.3.3 Availability

The third component of information security is availability. The information created and stored needs to be available to authorized entities. Information is useless if it is not available. Information needs to be changed constantly, which means it must be accessible to authorized entities.

1.5 Research Motivation

Due to the increase of the use of technology in every situation of life, in the field of transportation, communication, medicine and military, the main item to be transmitted in the fields in the digital image. The digital image contains many important critical information like military information, bank swift, etc. Due to this importance, the transmitted digital image became unsecured in the communication and transportation medium because many attackers target these images whenever possible worldwide in different ways. Thus it is urgent to find latest and upgrade methods to protect these digital images and their content from any type of attack.

1.6 Organization of Thesis

The complete thesis is organized in five chapters.

Chapter 1, gives the introduction to the topic. It discusses the image encryption security goal and discusses the parameters which consider for security of image encryption.

Chapter 2, represents details literature review about different image encryption scheme suggested by different researchers. It discusses review on chaos-based image encryption scheme, Cellular automata base image encryption scheme, Scan base, Wave transmission base and DNA computing based image encryption scheme.

Chapter 3 discusses two-dimensional Henon mapping, Four-dimensional Hyperchaotic Lorenz system, Runge-Kutta method, and DNA sequence Operation.

Chapter 4, represents the proposed image encryption technique.

Chapter 5, represents experimental result and security analysis such as keyspace, key sensitivity, histogram analysis, correlation coefficient, and information entropy and It also discuss comparisons of previous image encryption method with the proposed work in this thesis.

Chapter 6, represents the conclusion and future work.

Chapter-2

Literature Review

In this chapter, we discuss the basic concept of Chaos theory and properties of chaotic sequence. we review a number of image encryption technique proposed by different authors. We review Chaos-based image encryption technique, Cellular automata based image encryption technique, Scan pattern and Wave transmission based image encryption technique. We discuss the basic concept of DNA Computing. Finally, we review the image encryption technique based on DNA operation.

2.1 Chaos Theory

Chaos theory is now being applied to various field of engineering, basic science like physics, philosophy related to the field of economics and also mathematics. Here the focus is on the behavior of dynamic systems that are highly sensitive to an initial condition commonly referred to as the butterfly effect. A small variation in the initial conditions yields diverging results. The systems are deterministic without the involvement of random elements. Deterministic nature makes the system predictable. Chaotic behavior is also evident in natural systems like the weather. In common usage, "Chaos" means "a state of disorder".

2.2 Chaotic Sequence

A chaotic sequence is non-periodic, non-converging sequence and exhibits noise like behavior. The initial value can be varied to produce a number of uncorrelated random-like, yet reproducible and deterministic signal sequences. These sequences called the chaotic sequences are real-valued sequences which can be converted into integer-valued sequences during image encryption which are effective for pixel permutation. One of the simplest and most widely studied nonlinear dynamic systems capable of exhibiting chaos is the logistic map.

2.3 Basic properties of a Chaotic System

For any dynamic function f mapping $X \to X$ to be classified as chaotic, it must have the following properties:

- f is topologically transitive.
- f has a sensitive dependence on the initial condition.
- Periodic point is dense in X

Consider a function $f(x) = \mu \times (1-x)$ where μ is the control parameter. This function maps $[0,1]$ to $[0,1]$ and matches all the above criteria.

Sensitivity to initial condition: Sensitivity to initial conditions means that each point in a chaotic system is arbitrarily closely approximated by other points with significantly different future paths or trajectories. Thus, an arbitrarily small change, or perturbation, of the current trajectory may lead to significantly different future behavior. Sensitivity to initial conditions is popularly known as the "butterfly effect", so-called because of the title of a paper given by Edward Lorenz in 1972.

Dense periodic point: A set is called dense when there is another number between any two numbers. For example, between 1 and 1.1there is1.05. But between 1 and 1.05 there is1.005. Therefore, a dense set has an infinite number of point.

2.4 Chaos-based Image Encryption Technique

Since the 1970s Chaos theory has been established in many types of research areas such as engineering, biology, mathematics, and others. Butterfly effect (sensitivity to initial condition) is the most well-known characteristic of Chaotic system. By deterministic equation, pseudorandomness is generated in a chaotic system. Chaotic systems have several significant features such as random-like behavior, sensitivity to the initial condition, control parameters and ergodicity. In recent years, several chaos-based .image encryption schemes have been developed. Fridrich [1] demonstrated the image encryption technique based on 2D standard Baker map in 1998. Mainly, pixel diffusion and chaotic permutation are two phases of this encryption algorithm. A chaotic map such as the baker map, cat map, and the standard map is used to permute the image pixels in the first phase. A certain discretized one-dimensional chaotic map is used to change the pixels gray values in a sequential manner in

the second phase. In [2] an image encryption scheme is demonstrated based on the chaotic standard map. This encryption algorithm mainly consists of three parts a key generator, a diffusion function, and a confusion function. In confusion process, a modified standard map was used. In diffusion steps, a logistic map was used. A key stream is generated in each round which determines the parameters of the logistic map and standard map. A chaos-based image encryption algorithm with variable control parameters is proposed in [3]. This algorithm can be considered an upgraded version of permutation-diffusion architecture. A chaotic map is used to determine the control parameters of baker map, cat map and standard map in each permutation round. The key stream which is generated from another chaotic map is used in the diffusion phase. Wang, Yong, et al. [4] proposed image encryption based on the chaotic sequence. Here at first, they divided the image into blocks of pixels. After that spatiotemporal chaotic system is used to generate a pseudorandom sequence. The blocks are diffuse and shuffle using a pseudorandom sequence. The pixels valued are changed. N Khade, Pawan, et al. [5] proposed image encryption based on 3D Chaotic function. In this method, they used 3D, 2D Arnold's cat map, 3D Logistic map, and 3D Chebyshev map for color image encryption. Here they used 2D Arnolds Cat map for image pixel scrambling. Here they used 3D Chebyshev map for key generation. They used 3D Logistic map for image scrambling. Here they used 3D Arnolds Cat map for Red, Green and Blue component substitution. In this algorithm, they used both Confusion and Diffusion phase this makes this algorithm very secure. Wang, Xingyuan, et al. [6] proposed new image encryption based on dynamic S-boxes. At first, by chaotic system S-boxes are constructed. The initial states of the chaotic system and the parameters are generated for the first S-box using the last pixel value of the plain image and an external 256-bit key. According to row and adjacent row, the image pixels are divided into several groups. After that, a new S-boxes are generated for each group. The correlation between vertical pixels is reduced in this way. The authors have used the same method on columns in order to reduce the correlation between adjacent horizontal pixels. In order to get a large keyspace, the authors used an external 256-bit secret key. Tang, Zhenjun, et al. [7] proposed image encryption based on block shuffling and Chaotic map. At first, they divided the input image into the overlapping block. After that, they used a Chaotic map to make a small size square matrix. With the help of Arnold transform, the square matrix is further scrambled to generate a set of secret matrics. Finally, they perform exclusive OR operation between the image block and corresponding elements of a random secret matrix to encrypt each block. Hua, Zhongyun, et al [8] proposed image encryption based on two dimensional(2D) chaotic map, also called the 2D Sine Logistic modulation map (2D-SSLM).

Sine Logistic modulation map is derived from Sine and Logistic maps which are a 1D chaotic map. Here they used chaotic magic transform(CMT) for image encryption. The images pixels are shuffled quickly in both row and a column direction at the same time using chaotic magic transform. They also proposed a CMT based image encryption algorithm (CMT-IEA) integrating 2D-SLMN and CMT. Lu, Xu, et al. [9] proposed image encryption based on piecewise linear chaotic maps (PWLCM). Before confusion and defusion phase they convert the plain image into two binary sequences using bit plane decomposition method. They introduce a new mutual diffusion strategy between the sequence in the diffusion phase. In the diffusion phase, a little modification in the plain text image can cause a large number of binary value will be changed in the cipher sequence. In the confusion phase by the control of the piecewise linear chaotic map, they swap the binary element between the two sequences. In ref. [10] proposed image encryption based on Chaotic system and Permutation – Substitution network. Here they used four cryptographic phases, which are diffusion, substitution, diffusion, and permutation. At first, they used a new chaotic map for diffusion phase. Then they used strong S-boxes for substitution phase. After that Chaotic Logistic map is used for the diffusion phase. Finally, a permutation function is used to accomplish a block permutation phase to enhance the statical performance of encryption algorithm. Li, Yueping, Chunhua Wang, et al. [11] proposed hyper-chaos based image encryption using bit-level permutation and pixel-level permutation. Here Bit-level permutation is used to scramble the image. After that, they used pixel –level permutation. Bit-level permutation and Pixel level permutation are combined together can secure the security of the cryptosystem. Finally, they add the pixel after pixel level permutation in the diffusion phase. The algorithm is safer compared to exiting hyper chaos-based image encryption algorithm because they used bit-level permutation and pixel-level permutation. In ref. [12] proposed image encryption based on Line and Chaos map. In the image, the encryption algorithm line map is used to shuffle the pixels. Here Line map is a chaos base map. At first, the plain image is converted to a binary image. The initial value of the skew tent chaotic system is used to generate the secret key. The encryption and decryption both processes used the secret key. In this algorithm, they generate three chaotic sequences for image encryption.

2.5 Image Encryption Techniques based on Cellular Automata

Cellular automata are one of the simplest and fast random numbers generators which offer advantages of random behavior and greater sensitivity to initial conditions in very low computational overhead. In [13] Bakhshandeh, et al. proposed new image encryption based on reversible memory cellular automata and chaotic map. The initial condition of the chaotic maps is the secret key used in this algorithm. At first, a piecewise linear chaotic map is used to confuse the plain image in the permutation phase. To obtain an efficient and secure algorithm, they used a reversible memory cellular automata as well as a logistic map in the diffusion phase. Niyat, Abolfazl Yaghoutiet al. [14] proposed a color image encryption based on Cellular automata and hybrid hyper-chaotic system. In this algorithm, they used confusion and diffusion method. By chaos mapping, the positions of the original image pixels are replaced in confusion step. The logistic map is used to initialize one-dimensional-uniform cellular automata. Using non-uniform cellular automata they created a key image. The chaotic map is used to perform pixel permutation, which reduces the correlation between adjacent pixels. A value is selected randomly from the key image using Chen hyper-chaotic function which is used for encryption purpose. In ref. [15] proposed secure image encryption based on cellular automata and chaotic skew tent map. In this scheme, cellular automata are used to generate a pseudo-random number sequence(PRNS). The plain image is first permuted using the pseudo-random number sequence to remove the high correlation among the adjacent pixels. The cellular automata have a fixed keyspace like 128-bit or 256-bit. By the skew tent map, a single random number generated. Then the permuted image is encrypted based on a single random number. Cellular automata are used with chaotic skew tent map to create a huge key space. Therefore a combination of cellular automata and chaotic skew tent map gives a faster PRNS generator and higher keyspace which makes the algorithm more secure.

2.6 Image Encryption Technique based on Scan Pattern

The scan pattern is a formal language-based two-dimensional spatial-accessing methodology to generate a wide range of scanning paths to permute the pixels of an image. It is also defined as, scanning of a two-dimensional array in which each element of the array is accessed exactly once. The pixels of an original image are permuted to obtain the scrambled image using a scan pattern. Scan patterns are usually used to permute the pixels of an image. In [16], a novel image encryption method was proposed using transposition method, circular

shift, and scan pattern. The scan pattern generated by the notion of Kth smallest and stack dynamically used to permutate the pixels of the original image. The transposition and circular shift are done by shuffling key. The shuffling key is generated from the original image. The shuffling key is used for both row and column permutation and for both row and column circular shift and bitwise XOR operation. In [17], proposed image encryption based on SCAN pattern and basic XOR operation. In this method, at first, the original image is divided into a number of blocks. After that, the blocks are shuffled by the SCAN pattern to build a newly transformed image. Then pixels of each block are repositioned by scan pattern again for reaching more entropy. After that, the newly transformed image performed basic XOR operation for better encryption. For both encryption and decryption side, they used a 128-bit secret key. This encryption algorithm reduces the relationship among image elements by increasing the entropy value of the encrypted image as well as reducing the correlation among the adjacent pixels. Sivakumar et. al. [18] proposed a novel image encryption method based on a hybrid scan and a random number. This image encryption method mainly consists of three stages namely, pre-processing, pixel permutation with calligraphy based scan and pixel permutation with calligraphy based diagonal scan. The pixel position of the original image is permuted with calligraphy based scan and calligraphy based diagonal scan to obtain a scrambled image. The calligraphy scan combined with diagonal scan to permute the pixels block in the permutation stage. Using the Blum Blum Shub (BBS) generator, the random number is generated. The random number generated from the BBS generator and the scrambled image using XOR operation to obtain a cipher image. In [19] proposed image encryption based on scanning technique and cell shuffling. This proposed encryption method mainly contains two-step. In the first stage, the image is divided into a number of blocks then shuffle the original image. After the blocks shuffle the image structured are changed and then scan pattern is applied. In the second stage, the wave spiral scan pattern is applied to get the encrypted image.in this stage, the first scan pattern is applied before cell splitting and shuffling. In [20] proposed a new image encryption method using a circle. This encryption method mainly consists of two-phase confusion and diffusion phase. They have taken points on the perimeter of a circle to define the permutation. In the confusion phase, they have applied geometric properties of the circle for pixel position changing. They permute bit position of pixels to change pixel value in the diffusion phase.

2.7 Image Encryption Techniques based on Wave Transmission

In [21] proposed a block image encryption scheme based on Wave transmission and chaotic system. Using chaotic system a random sequence is generated. The chaotic sequence is used to find the source point of the wave and produced a diffusion matrix for modular operation. The keystream is dependent on both the secret key and the plain image in the encryption process. There are mainly three parameters in the wavefunction source point, wavelength, and amplitude. Liao, Xiaofeng, et al. [22] proposed a novel image encryption scheme based on self-adaptive Wave transmission. Wave transmission encryption is a way to change the gray-level values of pixels by simulating Wave transmission. Self-adaptive is carried out by partition an image into two equal part. Then the information of one part encrypts the other part. In this algorithm, the information of one part is used to control the amplitude of the wave when encrypting the other part. An image is divided into two equal part, during encryption. Both parts are encrypted by using wave transmission encryption with four waves whose amplitudes are determined by the other one. Wen Chen [23] proposed a novel image encryption method using three-dimensional space. In 3-D space, each input image is divided into a series of particle-like points distributed. All generated particle-like points are simultaneously encrypted into a phase-only mask. In [24] proposed a new asymmetric optical image encryption scheme based on an improved amplitude-phase retrieval algorithm. An iterative amplitude and phase retrieval process are selected to encode a primary image into real-valued ciphertext using two random phase masks that serve as public encryption keys. The private key generated in the encryption processes used to perform one-way phase modulation. Using conventional double random phase encoding architecture the decryption process is implemented optically.

2.8 DNA Cryptography

DNA cryptography is one of the rapidly emerging technologies where DNA is used as an information carrier. The vast parallelism, extraordinary information density, exceptional energy efficiency inherent in DNA molecules are searched for cryptographic purposes such as image encryption, authentication, signature so on. A gram of DNA contains 10^{21} DNA bases and can store 10^{8} terabytes of memory. DNA bases computation takes less time to compare to another algorithm. In this technique, bases of DNA are arranged random order and plaintext bits can be stored successfully using these bases. DNA chains have a large scale of parallelism and its computing speed could reach up to 1 billions of times per second

computations. A security system may have many weak spots like the place where the cipher is stored. DNA cryptography solves such problem. The data is secured either inside the DNA or using DNA sequences to create encrypted text which can only be decrypted if the key and current sequence is known.

2.9 Image Encryption using DNA Operation

Adleman first introduced DNA computing into the encryption field in 1994. DNA computing created a new stage of information processing. DNA computing is applied in cryptography for huge storage, massive parallelism, and ultra-low power consumption. DNA coding has a strong parallel computing capability. Recently, DNA based image encryption has become more and more popular [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]. Generally, DNA-based image encryption categorized into two phases: At first, using DNA encoding theory to encode plain image pixels into a DNA sequence. Then a gray pixel value is decomposed into four DNA elements which can increase the efficiency of image confusion and diffusion. Secondly, the encoded plain image pixels generate a key image based on DNA operation rules and form the cipher image. Wang, Xing-Yuan, et al. [25] proposed image encryption based on Chaotic sequence and DNA sequence operation.The pseudorandom sequences produced by the spatiotemporal chaos system is used to perform bitwise exclusive OR operation on the pixel of the plain image. After that, using DNA encoding rule, a DNA matrix is obtained by encoding the confused image. After that, the row and column of the DNA matrix are permuted. At last, using DNA decoding rule they decode the confusing DNA matrix. Finally, get the cipher image. Zhang, Qiang, et al. [26] proposed new image encryption based on hyper-chaotic system and DNA sequence operation. At first, by encoding the key image and the original image, they obtained two DNA sequence matrices. After that by Chen's hyper-chaotic map, they generated the hyper-chaotic sequence. Chen's hyper-chaos system is used to permutate the DNA matrics. By using DNA sequence addition operation, they XOR the random DNA matrix and the scrambled DNA matrix. Finally, By the DNA decoding rule, they get the encrypted image by decoding the DNA sequence matrix. Wu Xiangjun et al. [27] proposed a color image encryption based on one-dimensional chaotic map and DNA sequence operation. The secret keys and the plain image is used to generate the key streams from a 1D chaotic system. After that by the DNA encoding rule, the key streams and the plain image are transformed into the DNA matrix. After that, they perform XOR operation and DNA complementary rule on the DNA matrices to get the scrambled

DNA matrices. After that DNA matrix divided into the equal block. Then the blocks are shuffled randomly. Then they perform DNA XOR operation and addition operation on the DNA matrix and get encoded DNA matrix. Finally, by the DNA decoding rule, they convert the encoded DNA matrix to cipher image. Guesmi, R., et al. [28] proposed image encryption based on the Secure Hash Algorithm and DNA sequence operation. The plain image hash valued is used to generate the initial value of the Lorenz system. The one time key from the plain image and the secret hash key are generated using a secure hash algorithm. The encrypted key is a hash value. The chaotic sequence is used to shuffle the pixels in the diffusion process. Three sequences are generated using the Lorenz system. The red, blue, and green component of the image are shuffled by the three sequences. In the confusion process the pixel values of the image R, G, B component is scrambled using DNA XOR and then encrypt the scrambled image. Zhen, Ping, et al. [29] proposed secure image encryption based on Spatiotemporal chaotic system and Logistic chaotic system. Here they used Logistic chaotic map to generate a DNA matrix. Then DNA matrix which is generated from the Logistic map is used to perform DNA addition operation with the encoded image. The Spatiotemporal chaotic map is used to resist from chosen -plaintext attack. Wu, Xiangjun, et al. [30] proposed a color image encryption based on NCA map-based CML and one-time key and DNA sequence operation. In this algorithm at first, they used NCA map-based CML to generate the key streams. The system parameters are updated using the hash function SHA-512. The plain image decomposed into the red, green and blue component. By using DNA encoding rule the component are converted into three DNA matrices. After that, a new DNA matrix is formed to combine three DNA matrix. Then they perform column-wise and row-wise permutation on DNA matrix. Then the DNA matrix is divided into three equal blocks. After that, they perform DNA subtraction, XOR, and addition operation on those blocks. Finally, according to the DNA decoding rule, they transform the DNA matrix into the decimal matrix. Zhang, Xuncai, et al. [31] proposed new image encryption based on dynamic DNA encoding and chaotic system. At first, the hash value for a given DNA sequence is calculated using Keccack method. The hash value is used as the initial value of the chaotic map. Using a chaotic map they generate a chaotic sequence. After that, the image pixels locations are scrambled using the chaotic sequence. The bit permutation is implemented using the butterfly network. The image is coded into a dynamic DNA matrix. After that, they perform an algebraic operation on the DNA sequence. By the operation of the DNA sequence and the ciphertext feedback, the confusion and diffusion properties of the algorithm are enhanced. In ref. [32] proposed image encryption based on DNA complementary rule and

chaotic maps. At first, a piecewise linear chaotic map (PWLCM) is used to generate a one-dimensional array. Using one-dimensional array the row and column of the original image are permuted. By the DNA encoding rule, each pixel of the original image is encoded into four nucleotides. After that using DNA complementary rule, each nucleotide is transformed into its base pair for randoms times. By Chebyshev maps, the times is generated. They used the MD5 hash of the plain image to generate the initial values and parameters of the chaotic map. Wu, Jiahui et al. [33] proposed new image encryption based on DNA approach and 2D Henon-Sine map. By combining the Henon map and the Sine map, the authors designed a 2D Henon Sine map. The 2D Henon Sine map has better ergodicity, a wider chaotic range compare to another chaotic map. The DNA rules are controlled by the 2D Henon Sine map. In this algorithm, the DNA approach is used to diffuse the image pixels. Using two-dimensional Henon Sine map permuted the image pixels. Chai, Xiuli, et al. [34] proposed new image encryption based on DNA sequence operation and chaotic sequence. At first, a DNA matrix is formed by encoding the plain image. After that, the authors performed a wase-based permutation scheme on a DNA matrix. Using Logistic chaotic map, the chaotic sequence is generated. The chaotic sequence is applied for column circular permutation and row circular permutation. The SHA 256 hash of the plain image is used to calculate the initial values and parameters of the chaotic system. At DNA level row by row image diffusion method is applied. By the hamming distance of the plain image, the initial value and system parameters of the chaotic system is renewed. Finally, the cipher image is obtained by decoding the diffused of the DNA matrix.Zhan, Kun, et al. [35] proposed image encryption based on four-dimensional hyperchaotic sequence and DNA sequence. At first, a pseudorandom sequence is generated using a four-dimensional hyper-chaotic sequence. The hyperchaotic sequence is applied in each step: GBS, DNA addition, DNA complementation, and the binary XOR. All pixels values valued of an input image are converted into a serial binary digit stream. By the hyperchaotic sequence, the bitstream is scrambled globally. To obtain a robust encryption performance DNA algebraic operation and complementation are performed between the hyperchaotic sequence and DNA sequence.

Chapter-3

Preliminaries

In the previous chapter, work done by many types of research on image encryption using various algorithms was discussed. In this chapter, we discuss two-dimensional Henon mapping and four-dimensional hyperchaotic Lorenz systems. We explain DNA encoding and decoding operation, DNA addition, DNA subtraction, and DNA XOR operation. In my work, image encryption is done by the use of two-dimensional Henon mapping, four-dimensional hyperchaotic Lorenz systems, and DNA encoding operation.

3.1 Two-dimensional Henon map

We have seen that chaotic systems have many unique properties such as sensitivity to the initial condition, topological mixing, unpredictability, and ergodicity. These properties are very useful for image encryption concept. For image encryption scheme the concept of the chaotic system is very popular. In this thesis, we introduce the two-dimensional Henon map. We use two-dimensional Henon map to develop our image encryption algorithm. The Henon map defined on a two-dimensional plane is a nonlinear discrete-time dynamical system. In 1976 the Henon map has been introduced and studied for the first time by Henon [50]. The Henon map is a two-dimensional nonlinear discrete chaotic map. Some properties of the Henon map are sensitivity to the initial condition, ergodic and unpredictability. These properties of the Henon map are very useful for our image encryption scheme. The Henon map is a two-dimensional iterated map defined by Equation (3.1).

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{3.1}$$

Where x, y represents the iteration values, n represents the number of iteration. a, b are two control parameters, $a \in (0,1.4), 0.2 < b \leq 0.314$. The Henon mapping system can be a chaotic state when $a = 1.4$ and $b = 0.3$.

The initial value x_0 and the initial value y_0 represent the key. The choice of $a=1.4$ and $b=0.3$ values were in a way such that they are very small enough. So that x_i and y_i were folded and do not extend to infinity, but the values not too small to lose the line structure of the attractor. The attractor of this map is shown in Figure 1. We observed that the system points did not breakout to infinity and remained inside the square. The quadrilateral is pulled and closed by the Henon map at each iteration until the geometrical attractor is achieved.

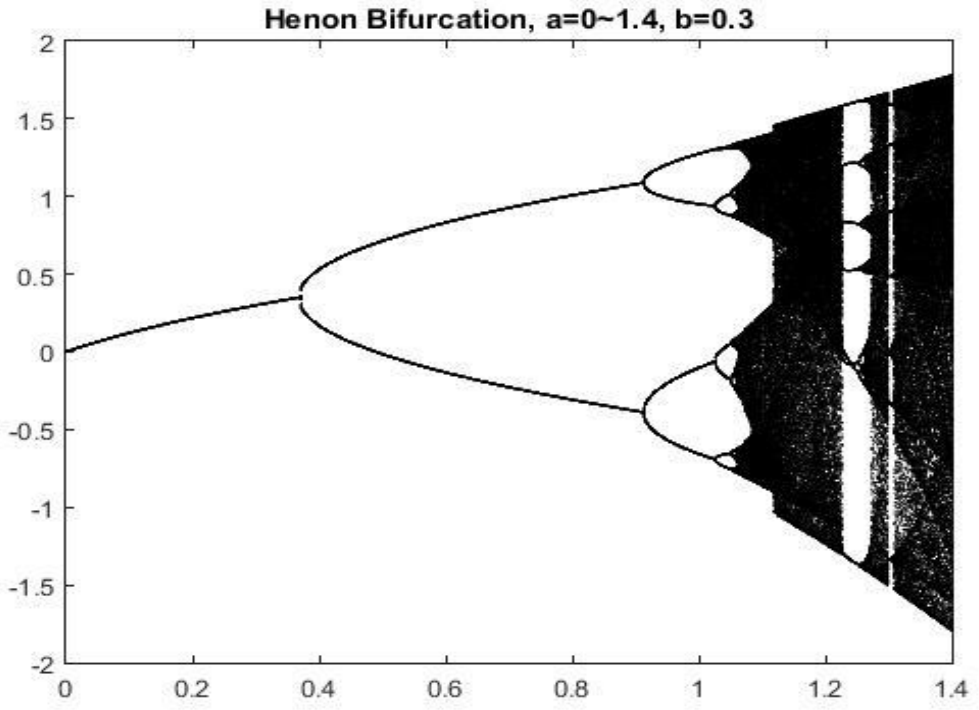


Figure 3.1: Bifurcation diagram of the Henon map

Table 3.1: Different regions in the bifurcation diagram of the Henon map

Nature of the dynamic behavior	Henon map	
	a	b
Fixed point	$0 \le a \le 0.35$	0.3
Period–doubling cascade	$0.35 < a \le 1.06$	0.3
Chaotic Attractor	$1.06 < a \le 1.22$	0.3
Fixed point	$1.22 < a \le 1.27$	0.3
Chaotic Range	$1.27 < a \le 1.44$	0.3

3.2 The Hyper-chaotic Lorenz system

In this encryption algorithm, we use hyper-chaotic sequences which generated from Lorenz hyper-chaotic system to encrypt the image. In [49] Hyper-chaotic Lorenz system is described as Equation (3.2).

$$\begin{cases} \dot{x} = a(y - x); \\ \dot{y} = cx - dy - xz; \\ \dot{z} = bz + xy + w; \\ \dot{w} = -rw + kyz; \end{cases} \tag{3.2}$$

Where x, y, z, and w are space coordinates; a, b c d r and k are parameters; and the dot denotes derivative with respect to time t . When parameters a = 21.7, b = 7.3, c = 6.6, d = -2, $r = 0.1$ and $k = -9.5$ four-dimensional Lorenz hyper-chaotic system is in the chaotic state and can generate four chaotic sequences. The corresponding Lyapunov exponents of this hyperchaotic attractor are λ_1 = 1.1625, λ_2 = 0.1392, λ_3= -0.0003, λ_4 = −28.3942. Because the hyper-chaos has two positive Lyapunov exponents, a hyper-chaotic system's prediction time s often shorter than that of a chaotic system. As a result, it is often regarded as safer than chaos for designing security algorithms. Here, we take the four-order Runge–Kutta method to solve the equations. We set the initial condition (x_0, y_0, z_0, w_0) and can obtain four hyper chaotic sequences $\{(x_i, y_i, z_i, w_i) \mid i = 1, 2, 3, ...\}$. These hyper chaotic sequences are very sensitive dependence on initial condition (x_0, y_0, z_0, w_0) and non-periodicity. We set initial condition value according to the equation and integration step $h = 0.002$. We solve the equation and get the first 5096 real values. After that we, remove first 1000 value for better randomness. We get 4096 real values of each sequence. Finally, we get four sequences with good randomness.

3.3 Fourth-order Runge-Kutta Method

To solve the fourth-order hyperchaotic Lorenz system in this image encryption algorithm we use the fourth order Runge-Kutta method. Fourth order Runge-Kutta method is described by the Equation (3.3).

$$\begin{cases} x_{n+1} = x_n + (h/6)(K_1 + 2K_2 + 2K_3 + K_4) \\ y_{n+1} = y_n + (h/6)(L_1 + 2L_2 + 2L_3 + L_4) \\ z_{n+1} = z_n + (h/6)(M_1 + 2M_2 + 2M_3 + M_4) \\ w_{n+1} = w_n + (h/6)(N_1 + 2N_2 + 2N_3 + N_4) \end{cases} \tag{3.3}$$

Where

$$\begin{cases} K_1 = a(y_n - x_n) \\ K_2 = a\left[(y_n + hK_1/2) - (x_n + hK_1/2)\right] \\ K_3 = a\left[(y_n + hK_2/2) - (x_n + hK_2/2)\right] \\ K_4 = a\left[(y_n + hK_3) - (x_n + hK_3)\right] \end{cases}$$

$$\begin{cases} L_1 = cx_n - dy_n - x_n z_n \\ L_2 = c(x_n + hL_1/2) - d(y_n + hL_1/2) - (x_n + hL_1/2)(z_n + hL_1/2) \\ L_3 = c(x_n + hL_2/2) - d(y_n + hL_2/2) - (x_n + hL_2/2)(z_n + hL_2/2) \\ L_4 = c(x_n + hL_3) - d(y_n + hL_3) - (x_n + hL_3)(z_n + hL_3) \end{cases}$$

$$\begin{cases} M_1 = bz_n + x_n y_n + w_n \\ M_2 = b(z_n + hM_1/2) + \left[(x_n + hM_1/2)(y_n + hM_1/2)\right] + (w_n + hM_1/2) \\ M_3 = b(z_n + hM_2/2) + \left[(x_n + hM_2/2)(y_n + hM_2/2)\right] + (w_n + hM_2/2) \\ M_4 = b(z_n + hM_3) + \left[(x_n + hM_3)(y_n + hM_3)\right] + (w_n + hM_3) \end{cases}$$

$$\begin{cases} N_1 = -rw_n + ky_n z_n \\ N_2 = -r(w_n + hN_1/2) + k\left[(y_n + hN_1/2)(z_n + hN_1/2)\right] \\ N_3 = -r(w_n + hN_2/2) + k\left[(y_n + hN_2/2)(z_n + hN_2/2)\right] \\ N_4 = -r(w_n + hN_3) + k\left[(y_n + hN_3)(z_n + hN_3)\right] \end{cases}$$

3.4 DNA sequence operation

3.4.1 DNA encoding and decoding rule for images

DNA computing is a form of computing which uses DNA, biochemistry and molecular biology, instead of the traditional silicon-based computer technologies. DNA computing, or more generally, biomolecular computing, is a fast developing inte rdisciplinary area. With the rapid development of DNA computing, the researchers presented many biological operations and algebra operations based on the DNA sequence. A DNA sequence consists of four nucleic acid bases A(adenine), C(cytosine), G(guanine) and T(thymine), where A and T are complementary pairs, and C and G are complementary pairs. In the binary number 0 and 1 are complementary pairs, so 00 and 11 are complementary pairs, and 01 and 10 are complementary pairs. Using the similarity and uniqueness of complementary properties, we link the binary and DNA together. The range of pixel values is 1-255, and we use at least 8-bit binary number to express decimal number 255, which is the biggest one among the pixel value, so we use an 8-bit binary number to represent one-pixel value. There are 24 types of encoding rules using the four bases A, C, G, and T to encode 00, 01, 10 and 11. But there are only 8 of them which can be seen in Table 3.2 satisfying the Watson-Crick complementary rule.

Example: The binary pixel value of an image is [00111010], so the corresponding DNA sequence is [ATGG] according to the first encoding rule, similarly according to the seventh decoding rule, the decoding sequence is [01101111].

Table 3.2: Eight kinds of DNA encoding rules

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

3.4.2 Addition and Subtraction algebraic operation for DNA sequence

With the rapid developments of DNA computing, some biology operations and algebraic operations based on DNA sequence are reported by researchers (King and Gaborit, 2007, Baum, 1996), such as addition and subtraction operations. Addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction in the binary. Corresponding to 8 kinds of DNA encoding schemes, there also exist 8 kinds of DNA addition rules and 8 kinds of DNA subtraction rules.

For Example: Taking two DNA sequences [TCGA] and [GTAC] we select one type of addition operation shown in Table 3.3 to add them and we get a sequence [AGGC]. Similarly, we can also get the sequence [GTAA] by subtracting the sequence [ATCG] from [GACT]. The subtraction operation is shown in Table 3.4 Seen from Table 3.3, Table 3.4, the base in each row or column is unique. In other words, the results of the addition operation and subtraction operation are unique. In this paper, we will use these addition or subtraction rules to scramble images' pixel values.

Table 3.3: Addition operation for DNA sequences.

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

Table 3.4: Subtraction operation for DNA sequences.

--	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

3.4.3 XOR algebraic operation for DNA sequences.

XOR operation for DNA sequences is performed according to traditional XOR in the binary. Corresponding to eight kinds of DNA encoding schemes, there also exist eight kinds of DNA XOR rules. In this paper, we used the XOR operation to fuse the original image.

For example, there are two DNA sequences [GACT] and [ATGC], we select one type of XOR operation which is shown in Table 3.5 to XOR them, and we get a sequence [GTTG] as the result. The XOR operation is reflexive. So, we also can get the sequence [GTTA] by sequence [GACT] XOR sequence [ATGT] under the XOR operation. From Table 3, we can see that anyone base in every row or column is unique, in other words, the results of XOR operation is one and only. In this paper, we will use this XOR operation rule to scramble the pixel values of the original image.

Table 3.5: XOR operation for DNA sequences.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	C	A	G
T	T	T	G	A

Chapter-4

The Proposed Image Encryption Process

The block diagram of Image Encryption Process

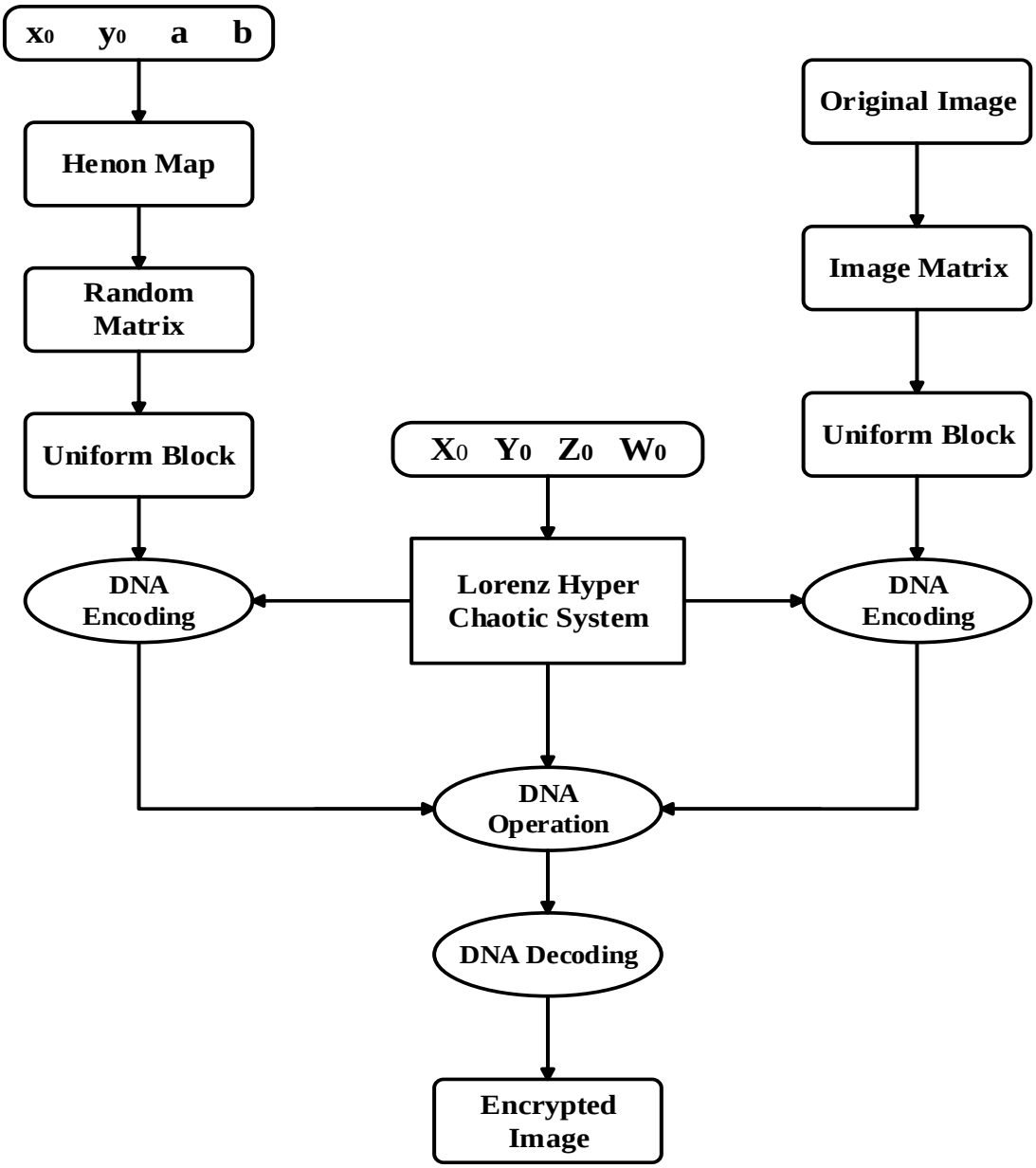


Figure 4.1 : The Block Diagram of Proposed Image Encryption Process

4.1 Generation of the secret key

The initial values of two-dimensional Henon map and four-dimensional hyperchaotic Lorenz systems are used as the secret key of the proposed image encryption algorithm. The plain image is used to produce the initial values of the Henon map and Lorenz hyperchaotic system. The initial values x_0 and y_0 of Henon map are generated according to Equation (4.1) and (4.2).

$$x_0 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} I(x,y)}{255 \times M \times N} \tag{4.1}$$

$$y_0 = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} I(x,y)}{255 \times M \times N} \tag{4.2}$$

Where $I(x,y)$ represents the gray value of the pixel at the (x,y) position of the image. The initial values $X(0), Y(0), Z(0), \mathrm{W}(0)$ of Lorenz hyperchaotic system are calculated according to Equation (4.2)

$$\begin{cases} X(0) = \dfrac{\sum I_1(x,y)}{3 \times M \times N} \\ Y(0) = \dfrac{\sum I_2(x,y)}{3 \times M \times N} \\ Z(0) = \dfrac{\sum I_3(x,y)}{3 \times M \times N} \\ W(0) = \dfrac{\sum I_4(x,y)}{3 \times M \times N} \end{cases} \tag{4.3}$$

4.2 Hyperchaotic Sequence Generations

We use the four-dimensional hyperchaotic Lorenz system discussed in section 3.2 to generate the pseudorandom sequence. The hyperchaotic generation process contains four steps.

Step 1: Input the initial condition (x_0, y_0, z_0, w_0) and set the step size $h = 0.0002$ and $N_0 = 1000$. The control parameters $a = 21.7, b = 7.3, c = 6.6, d = -2, r = 0.1$ and $k = -9.5$ are set.

Step 2: Iterate the hyperchaotic Lorenz system for $N_0 + \left(\frac{M}{q} \times \frac{N}{q}\right)$ times by Runge-Kutta method. Four sequences $\{x_i\}, \{y_i\}, \{z_i\}, \{w_i\}$ will be generated and the length of each sequence is $N_0 + \left(\frac{M}{q} \times \frac{N}{q}\right)$. Then we remove first N_0 numbers for each sequence for better randomness.

Step 3: Transform the first sequence $\{x_i\}$ into integer sequence $\{Q_i\}$ according to the Equation (4.4).

$$Q_i = \mathrm{mod}\left(floor\left(x_i \times 10^4\right), 8\right) + 1 \tag{4.4}$$

Step 4: Transform the second sequence $\{y_i\}$ into integer sequence $\{R_i\}$ according to the Equation (4.5).

$$R_i = \mathrm{mod}\left(floor\left(y_i \times 10^4\right), 8\right) + 1 \tag{4.5}$$

Step 5: Transform the third sequence $\{z_i\}$ into integer sequence $\{S_i\}$ according to the Equation (4.6).

$$S_i = \mathrm{mod}\left(floor\left(z_i \times 10^4\right), 3\right) \tag{4.6}$$

Step 6: Transform the fourth sequence $\{w_i\}$ into integer sequence $\{T_i\}$ according to the Equation (4.7).

$$T_i = \mathrm{mod}\left(floor\left(w_i \times 10^4\right), 8\right) + 1 \tag{4.7}$$

4.3 Image Encryption Algorithm

The image encryption algorithm is divided into three main parts.

At first a random matrix as the same size of the plaintext image is generated by successive iteration through Henon mapping, given the initial value x_0, y_0 and the parameter a and b. Next according to the random sequence generated by the Lorenz hyperchaotic system, the DNA encoding and decoding method of each sub-block of the random matrix and the plaintext image is selected. After that Selecting the DNA operation between the two sub-block of the plaintext image and the random matrix through the random sequence generated by the Lorenz hyperchaotic sequence. Finally, we combine all encrypted sub-blocks to get cipher text image.

4.3.1 The specific steps of the image encryption algorithm are as follow:

Input: Grayscale image I, the initial value of the two-dimensional Henon map x_0, y_0 and the parameter a, b initial value of the Lorenz hyperchaotic system $X(0), Y(0), Z(0), \mathrm{W}(0)$ are the input.

Output: encrypted image.

Step 1: Input the grayscale plain image I with size $M \times N$ where M and N are the image dimensions of rows and columns, respectively.

Step 2: We used the Henon map to generate a chaotic sequence. The parameter a is set to 1.4 and b is set to 0.3 and the initial value x_0 and y_0 is generated according to Equation (4.1) and (4.2). After that, the Henon map is successively iterated $5000 + M \times N$ times. Then we remove the first 5000 elements to get better randomness and we get the sequence $\{p_i\}$.

Step 3: Each element in the sequence $\{p_i\}$ needs to be transformed to be an integer in the range of 0 to 255, in order to be able to perform DNA encoding, according to Equation (4.8) the sequence is converted into a two-dimensional random matrix D of order $M \times N$.

$$p_i = \mathrm{mod}\left(ceil\left(p_i \times 10^3\right), 256\right) \tag{4.8}$$

$ceil(x)$ represents the smallest integer not less than x .

Step 4: The size of the block is set to $q \times q$. Image can be divided into $M/q \times N/q$ blocks.

Step 5: The initial values and parameters of Lorenz hyperchaotic system are set according to Equation (4.3). Then we solve the Lorenz hyperchaotic system equation by the fourth-order Runge-Kutta method to obtain four sequences $\{Q_i\}$, $\{R_i\}$, $\{S_i\}$ $\{T_i\}$ and the length of each sequence is $M/q \times N/q$.

Step 6: $\{Q_i\}$ determine the DNA encoding mode of each sub-block of image I. So, Q_i has only 8 possibilites, the DNA encoding method of the $i-$th sub-block in I is Q_i. According to the value of the sequence Q_i and the DNA encoding rule in Table 3.2 each pixel value in the block is encoded into a DNA sequence and the DNA matrix X_1 is generated. An 8-bit gray value is converted A, C, G, and T every two bits. Each sub-block is seperated into groups of two bit faces and four matrices of the same size are obtained, converted into DNA sequences, and four matrices are arranged side by side. That is, if the input matrix size is $M \times N$, the output matrix size is $M \times 4N$.

Step 7: $\{R_i\}$ determine the DNA encoding mode of each sub-block of random matrix D. So, R_i has only 8 possibilities, the DNA encoding method of $i-$th sub-block in D is R_i. According to the value of the sequence R_i and the DNA encoding rule in Table 3.2 each pixel in the block is encoded into DNA sequence and the DNA matrix X_2 is generated.

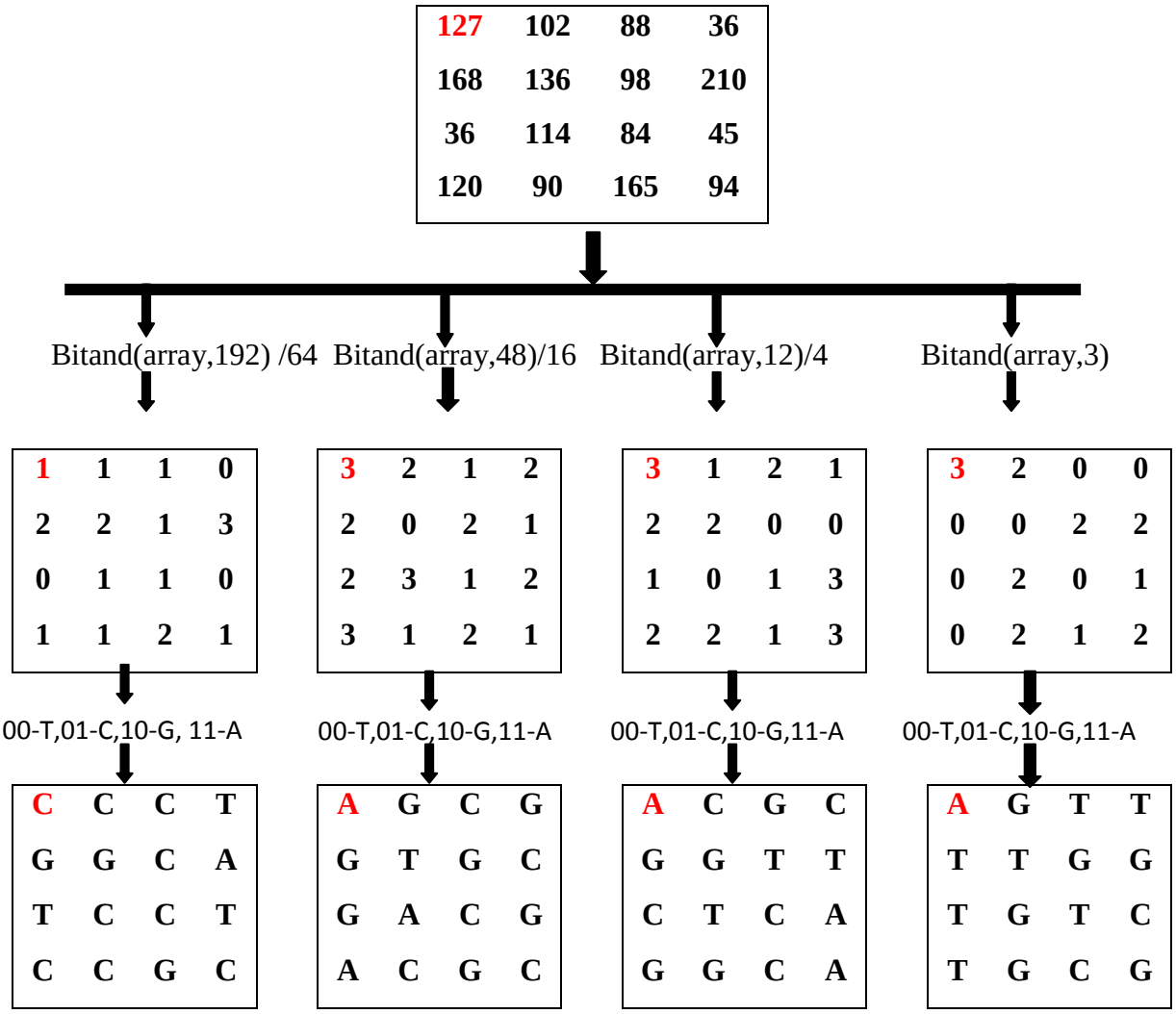
Step 8: $\{S_i\}$ determines the DNA operation between the blocks corresponding to image I and random matrix D. Here $\{S_i\}$ is composed of only three elements: $0, 1,$ and 2. There are three cases to discuss: $i)$ if $S_i = 0$ then we take the DNA addition operation between two DNA sequence. $ii)$ if $S_i = 1$ then we take the DNA subtraction operation between two DNA sequence. $iii)$ if $S_i = 2$ then we take the DNA XOR operation between two DNA sequence.

Step 9: To obtain a better diffusion effect, the relationship between the current image block encryption result and the previous image block encryption result is also determined by $\{S_i\}$. Take $S_i = 0$ as an example, then

$$X_i = X_{i-1} + I_i + D_i \tag{4.9}$$

Step 10: $\{T_i\}$ determine the DNA decoding method of the DNA sequence obtained by the calculation. So, T_i has only 8 possibilities, the DNA decoding method of i −th sub-block is T_i. That is, according to the value of the sequence $\{T_i\}$ and DNA decoding rule in Table 3.2, each DNA sequence is decoded into binary . The decoded binary is converted to decimal to obtain the final encrypted image.

4.4 DNA Encoding Process:



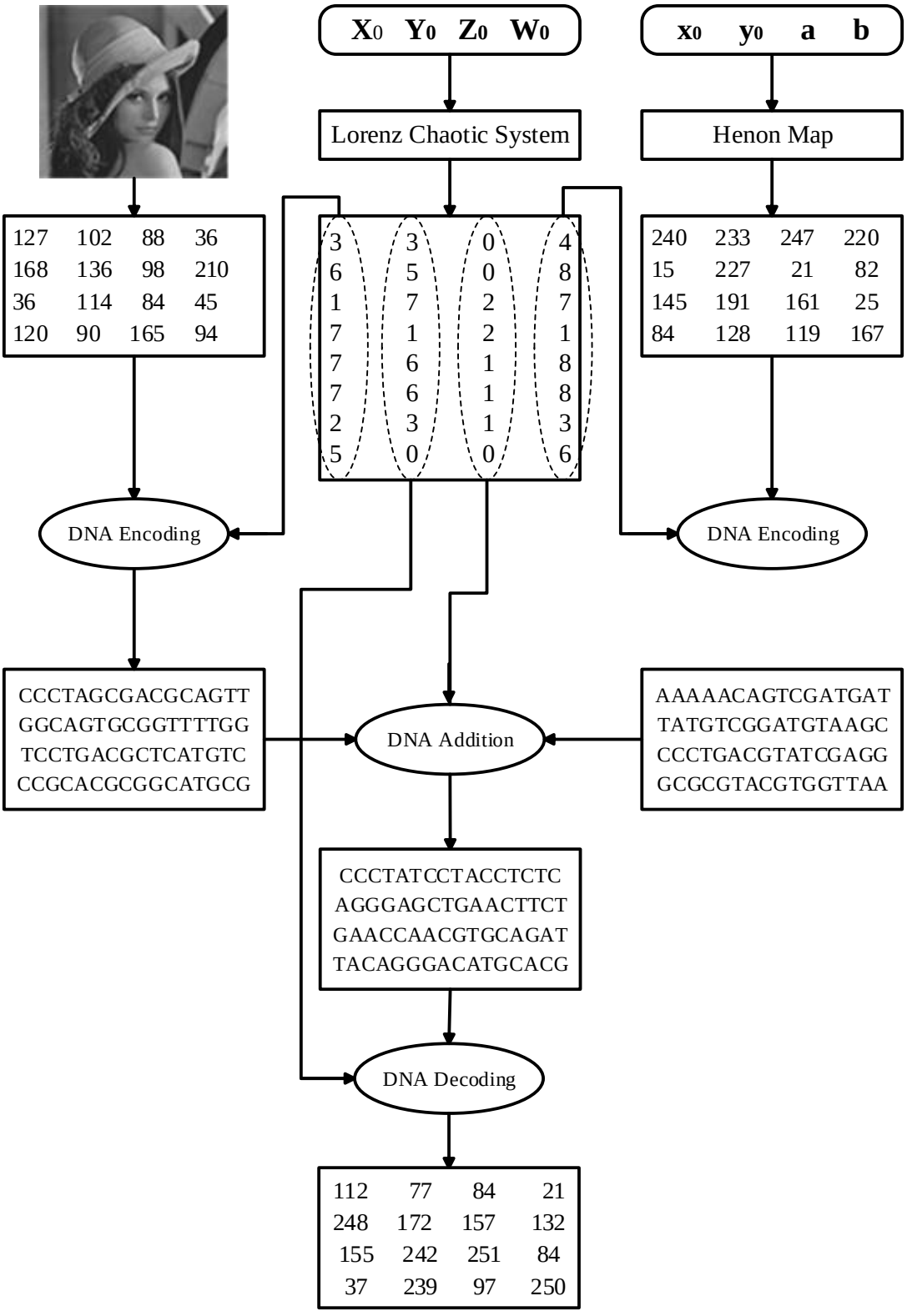
Example of DNA encoding for One pixel : Suppose pixel value 127

Bitand (127, 192) / 64 = Bitand(01111111, 11000000) / 64 = 64 / 64 = 1

Bitand (127,48) / 16 = Bitand(01111111,00110000) / 16 = 48 / 16 = 3

Bitand (127,12) / 4 = Bitand (01111111, 00001100) / 4 = 12 / 4 = 3

Bitand (127,3) = Bitand (01111111, 00000011) = 3, we get the sequence 1,3,3,3 , According to third Dna encoding rule 00-T, 01-C, 10-G, 11-A, So we get DNA sequence CAAA.



A Simple Example of proposed Image Encryption Process

4.5 Image Decryption Process

The decryption process is the inverse of the image encryption process. The step of the encryption process will be executed in reverse order in the decryption process. Only the block diagram of the decryption process is given below. It can be seen that the decryption block diagram is almost same encryption diagram, except the position of plain and cipher image, are changed.

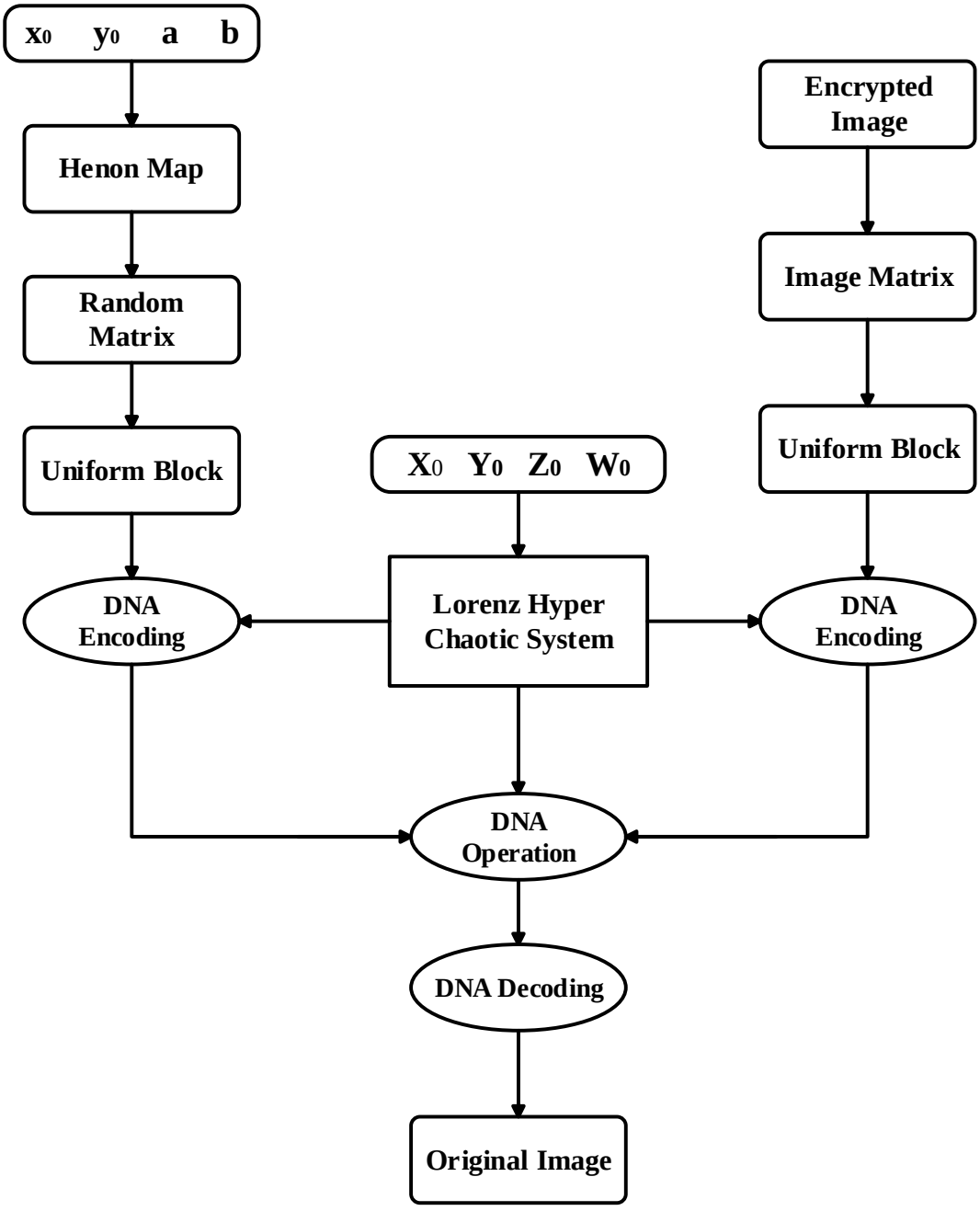


Figure 4.3: Block Diagram of Image Decryption Process

Chapter-5

Experimental Results and Security Analysis

5.1 Simulation Result

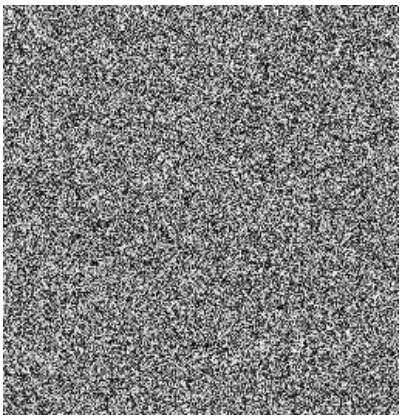
In this section, simulation results will be demonstrated to test the performance of our proposed image encryption algorithm. We use Matlab 2015a to run the encryption and decryption algorithm. In this experiment for testing purpose, we have taken five grayscale images of size 256×256, namely "Lena", "Lake", 'Baboon", "Peppers", and "Barbara". The plain Lena image and corresponding cipher image are shown in Figure 5.1. The plain Lake image and corresponding cipher image are displayed in Figure 5.2. Figure 5.3, Figure 5.4, Figure 5.5, Figure 5.6 represents the simulation result of Baboon, Peppers and Barbara images. The parameters of the experiment are set as follows: block size 4×4, two-dimensional Henon mapping parameters $a = 1.4$ and $b = 0.3$, Four-dimensional hyperchaotic Lorenz system parameters $a = 21.7,\ b = 7.3,\ c = 6.6,\ d = -2, r = 0.1$ and $k = -9.5$. The key consists of the initial value $x_0,\ y_0$ of Henon map and $x(0), y(0), z(0), w(0)$ of Lorenz hyperchaotic system. The initial values of the Henon map and Lorenz hyperchaotic system are generated from the plaintext image. From the simulation results, it is clear that the encrypted image appears to be really noisy and proving that we cannot obtain any information from the encrypted image. This shows that our algorithm has a good encryption effect. Also from the encrypted image, we saw that by using the right secret key we can obtain the good decryption images.

System specification used

In this work to implement and test the proposed image encryption scheme, the following specification has been used in the computer system.

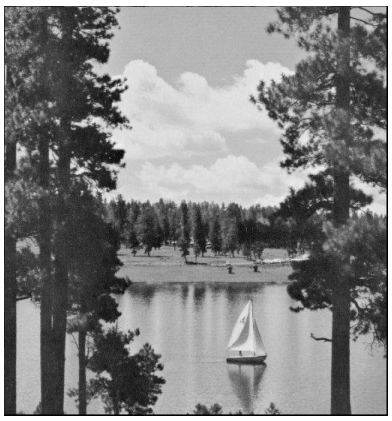
- ✓ PC with core i3
- ✓ Hard Disk 500GB
- ✓ RAM 4.00GB
- ✓ Windows 8.1 Professional, 64bit.

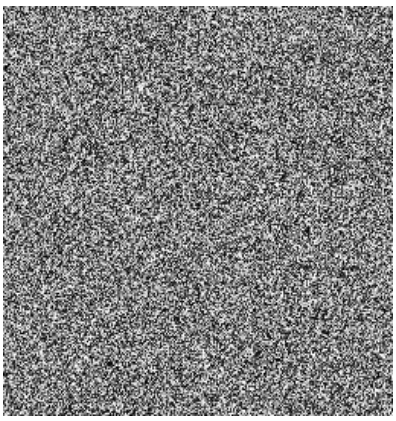

Plain image Lena


Correponding cipher image


Decrypted image

Figure 5.1: Simulation result of the Lena image.


Plain image Lake


Corresponding cipher image

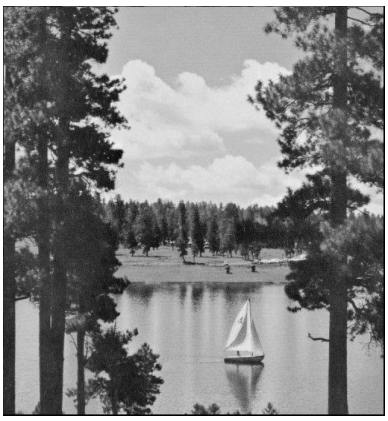
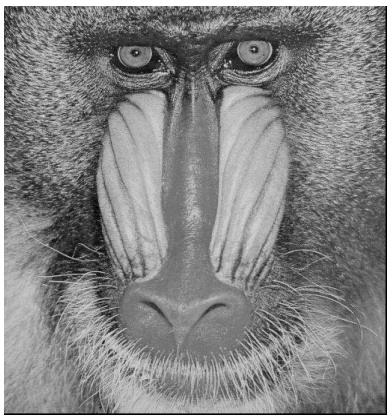
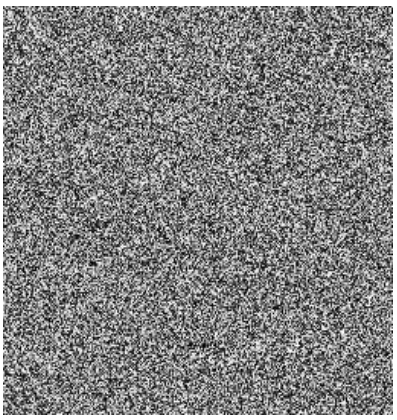

Decrypted image

Figure 5.2: Simulation result of the Lake image.


Plain image Baboon


Corresponding cipher image

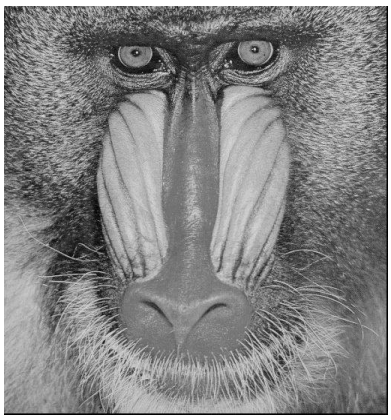
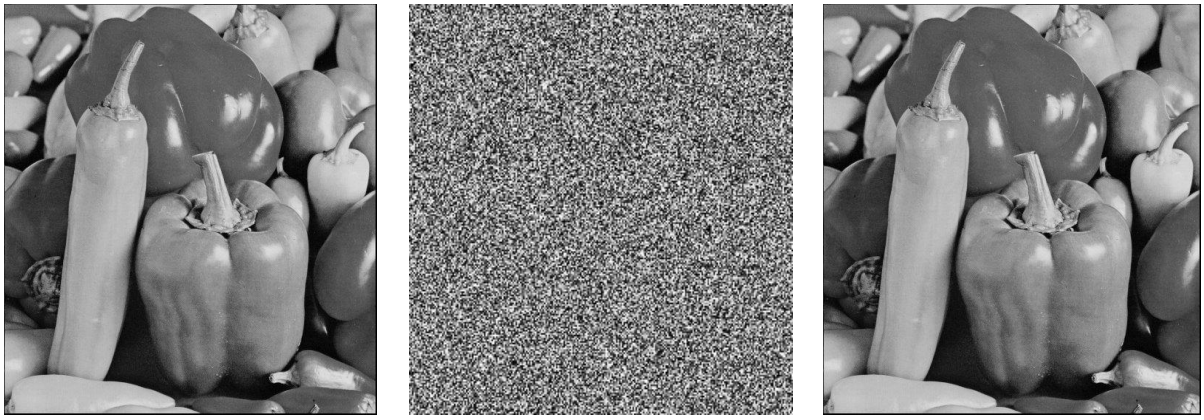
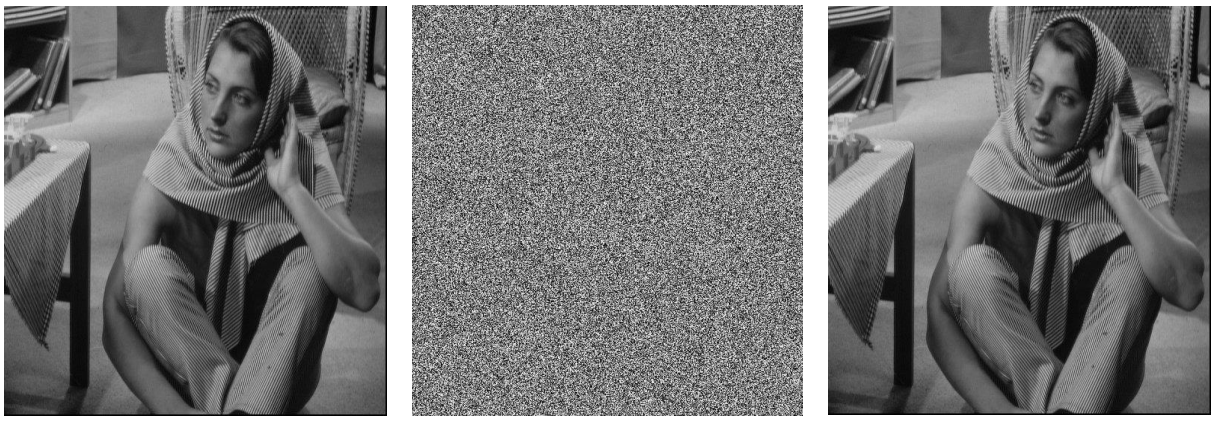

Decrypted image

Figure 5.3: Simulation result of the Baboon image.



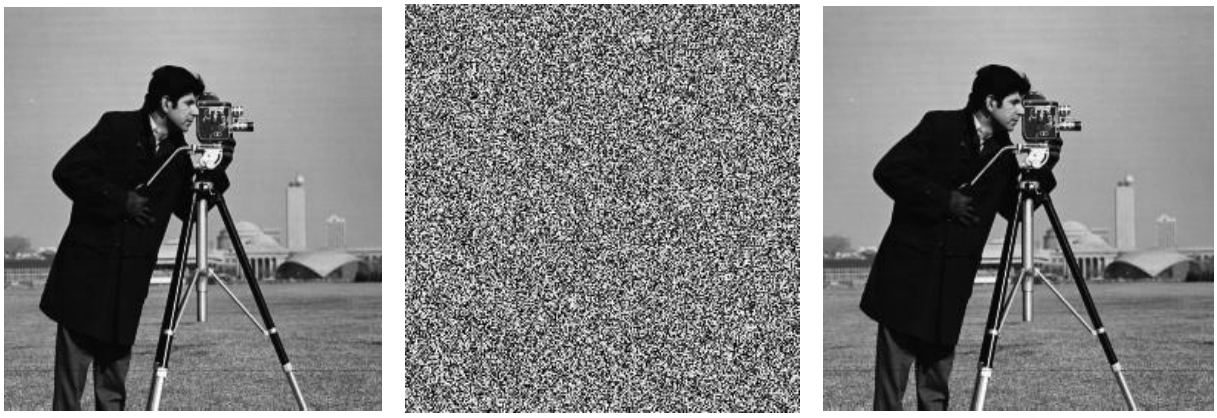
Plain image Pappers Corresponding cipher image Decrypted image

Figure 5.4: Simulation result of the Peppers image.



Plain image Barbara Corresponding cipher image Decrypted image

Figure 5.5: Simulation result of the Barbara plain image.



Plain image Cameraman Corresponding cipher image Decrypted image

Figure 5.6: Simulation result of the Cameraman image.

5.2 The Security Analysis

It is well known that a good encryption scheme should be robust of all kinds of attacks such as brute-force attack, differential attack, statistical attack, and plaintext attack. In this section, we discuss the security analysis of the proposed image encryption scheme such as key space analysis, key sensitivity analysis with respect to the key and plaintext and statistical analysis, etc. to prove that our proposed image encryption scheme is secure against the most common attacks.

5.2.1 Security key analysis

An ideal image encryption scheme should have a large enough key space and extreme sensitivity to the key to resisting brute-force attack. We will analyze the key space and the sensitivity of the security key.

5.2.1.1 Key space analysis

Key space size is the total number of different keys which can be used in the encryption process. It is well known that a for a good encryption algorithm key space should be large enough to make brute-force attack not effective. It is generally considered that the key space must be at least 2^100. The secret keys used in the proposed encryption scheme is the initial values of the Henon map and Lorenz hyperchaotic system. So, there are six secret keys $\left(x_0, y_0, x(0), y(0), z(0), w(0)\right)$. According to standard 64-bit IEEE floating-point, computation precision of the floating point is 10^-15. So, Henon map possible initial value x_0 is 10^-15 and y_0 is 10^-15 and four-dimensional Hyperchaotic Lorenz system possible initial values $x(0)$ is 10^-15, $y(0)$ is 10^-15, $z(0)$ is 10^-15 and $w(0)$ is 10^-15. So, the total key space of the proposed image encryption scheme is 10^15*10^15*10^15*10^15*10^15*10^15 =10^90 $\approx$ 2^299. In addition, the parameters a, b, c, d, r, k can also be used as keys to further expand the key space. The total key space is larger than 2^100. So, the key space of our proposed image encryption scheme is large enough to resist all kinds of brute-force attacks and can provide a high-security level.

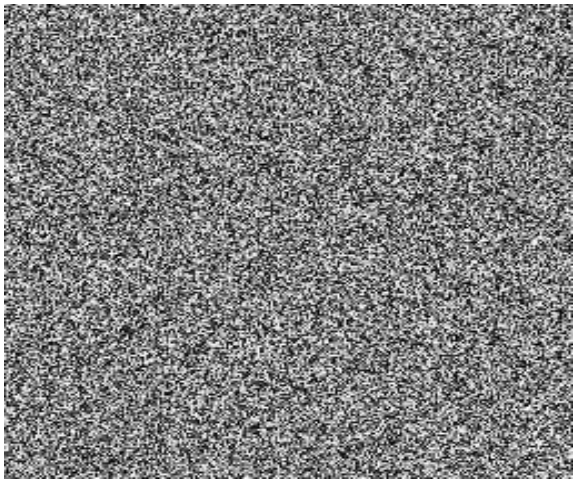
5.2.1.2 Key sensitivity analysis

A well-designed image encryption scheme should be sensitive with respect to the secret key, that is to say, a very little change in the secret key should produce a completely different cipher image. Generally, there are two ways to test the key sensitivity of image encryption. One is the plain image cannot be recovered from the cipher image if there is slightly difference the encryption and decryption keys. Other is completely different cipher image should be produced when slightly differences keys are used to encrypt the same plain image. For testing the key sensitivity of the proposed image encryption scheme, we used a slight difference decryption key. Using the initial value $x_0 = 0.3751$ for the encryption of the Lena image, we have obtained the encrypted image shown in Fig 5.6. The decrypted image is shown in Fig. 5.7, if $x_0 = 0.3751$ is used. Using $x_0 = 0.37510000001$ and another secret key unchanged the decrypted image is shown in Fig. 5.7. Fig 5.7 Illustrates that we correctly decrypt the image only when the encryption keys and the decryption keys are the same. Otherwise, as long as there is a minor difference in the key, we can not correctly extract the original image. Thus, we can see that our proposed image encryption scheme has the secret key sensitivity which demonstrated that it has the ability to resist exhaustive attack.

5.2.2 Statistical Analysis

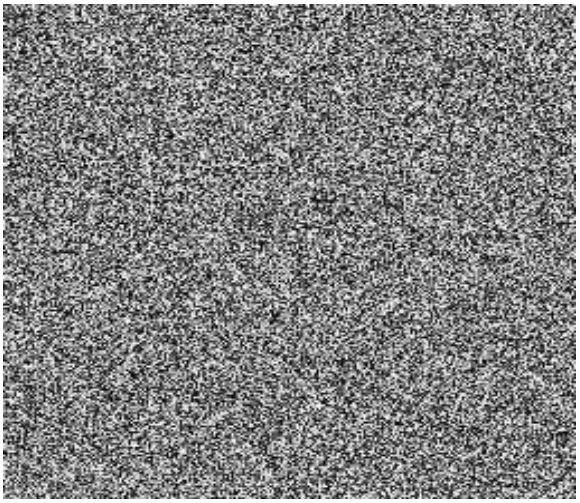
It is well known that many image encryption algorithms have been successfully analyzed with the help of statistical analysis and several statistical attacks have been considered on them. Therefore, an ideal image encryption algorithm should be robust against any statistical attack. To prove the robustness of our proposed image encryption algorithm, we have performed statistical analysis by calculating the histograms, the information entropy and the correlations of two adjacent pixels in the encrypted images.

(a) Original image



(b) Encrypted image with $x_0 = 0.3751$

(c) Decrypted image with $x_0 = 0.3751$

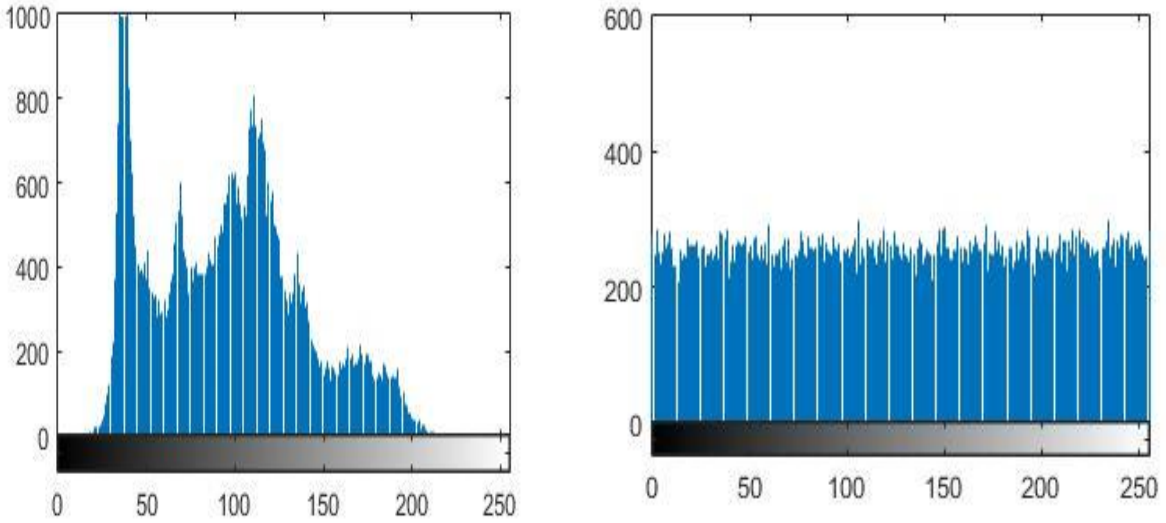


(d) Decrypted image with $x_0 = 03751000001$

Figure. 5.7: Key sensitivity tests results

5.2.2.1 Histogram Analysis

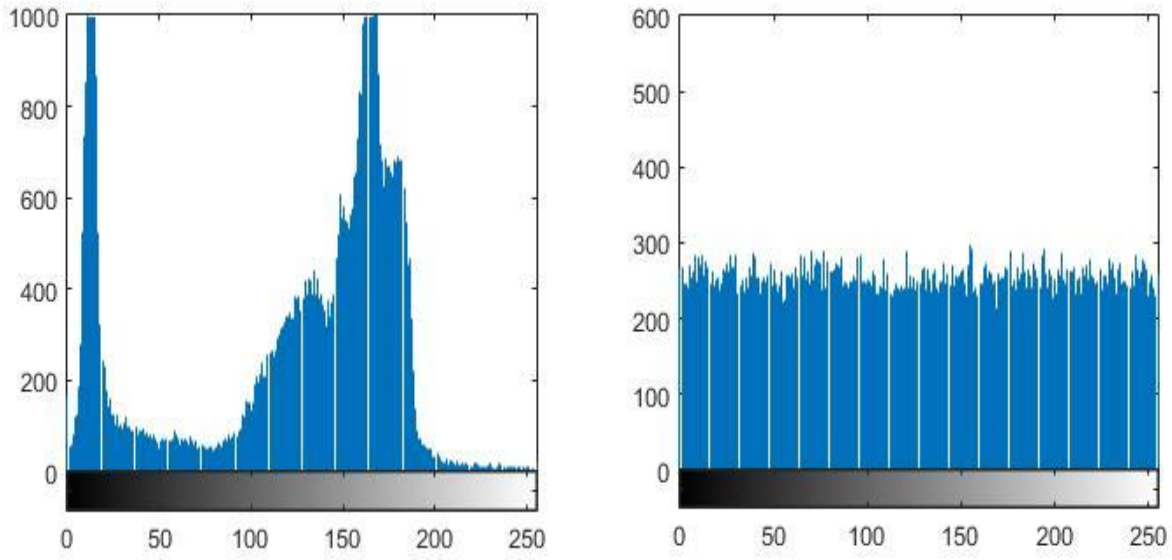
The histogram of an image refers to a graph of the pixel intensity values. The histogram is a graph showing the number of pixels in an image at different intensity values found in the image. There are 256 different possible intensities, in an 8-bit grayscale image. So, the histogram will display 256 numbers showing the distribution of pixels amongst those grayscale values. The histogram displays the nature of the distribution of image pixels, whether the distribution is either uniform or non-uniform. It is important to ensure that the original images and the encrypted images do not have any statical similarities. For a strong image encryption algorithm, the histogram of a plain image and the encrypted image must have considerable differences. The histogram of the original and corresponding encrypted Lena, Cameraman, Lake, Baboon, Peppers and Barbara images are given in below figure.



Lena Image Histogram

Encrypted Lena image Histogram

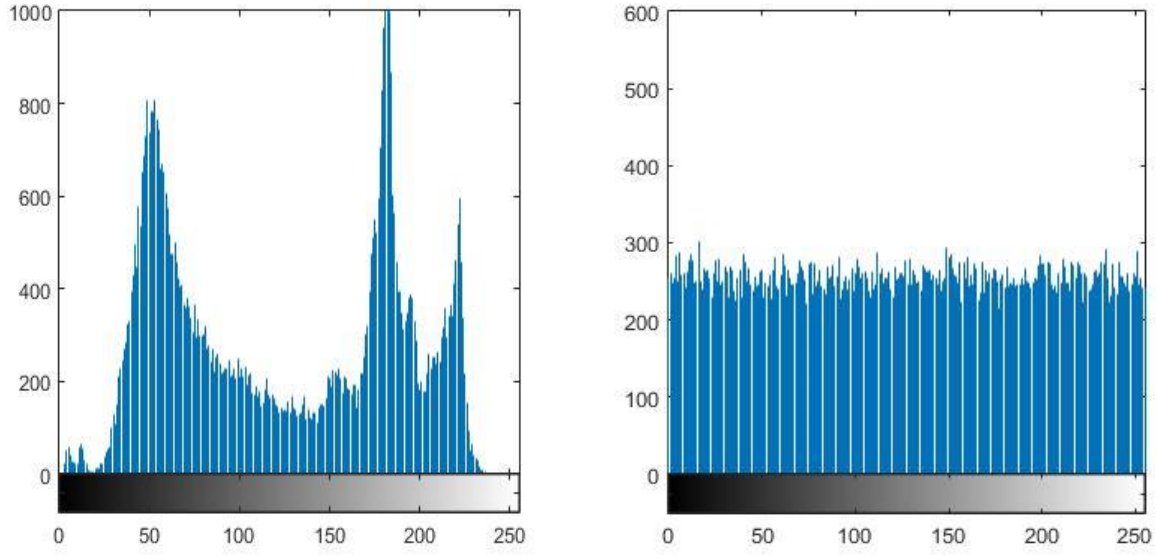
Figure 5.8: Histogram analysis result of plain and encrypted Lena image



Cameramn Image Histogram

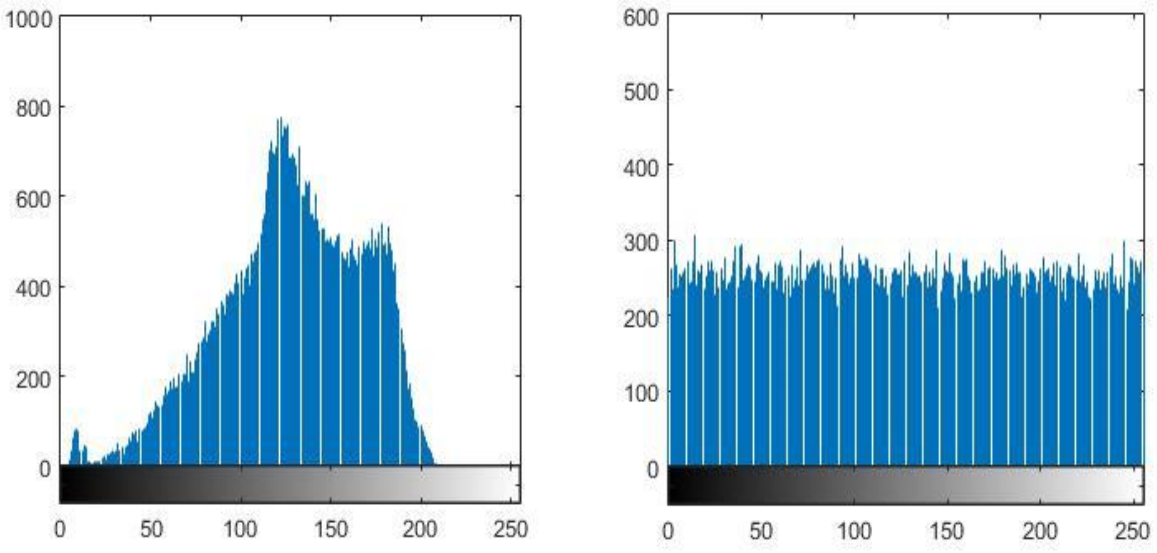
Encrypted Cameraman Image Histogram

Figure 5.9: Histogram analysis result of plain and encrypted Cameraman image



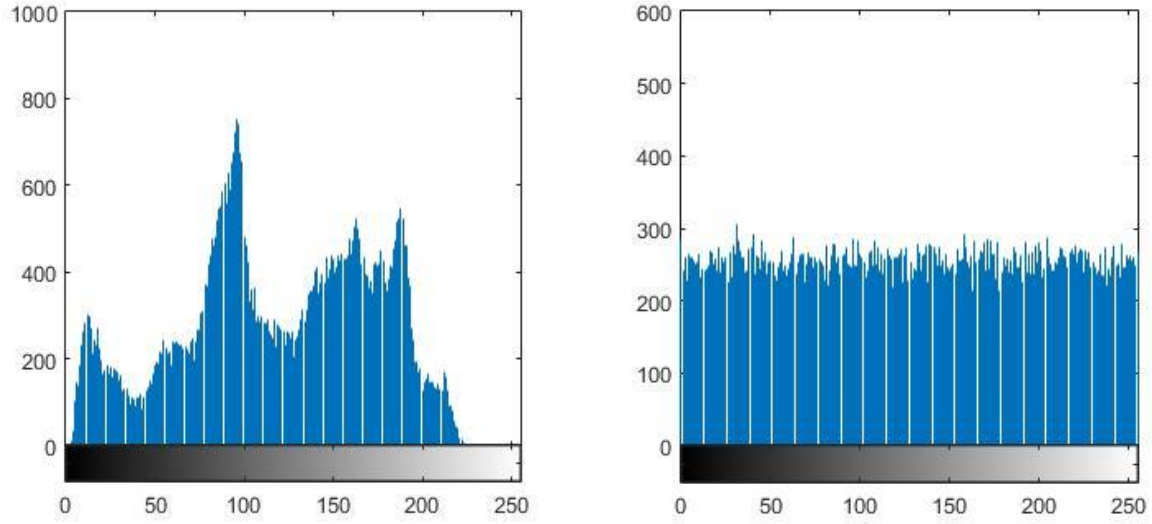
Lake image Histogram Encrypted Lake image Histogram

Figure 5.10: Histogram analysis result of Plain and Encrypted Lake image



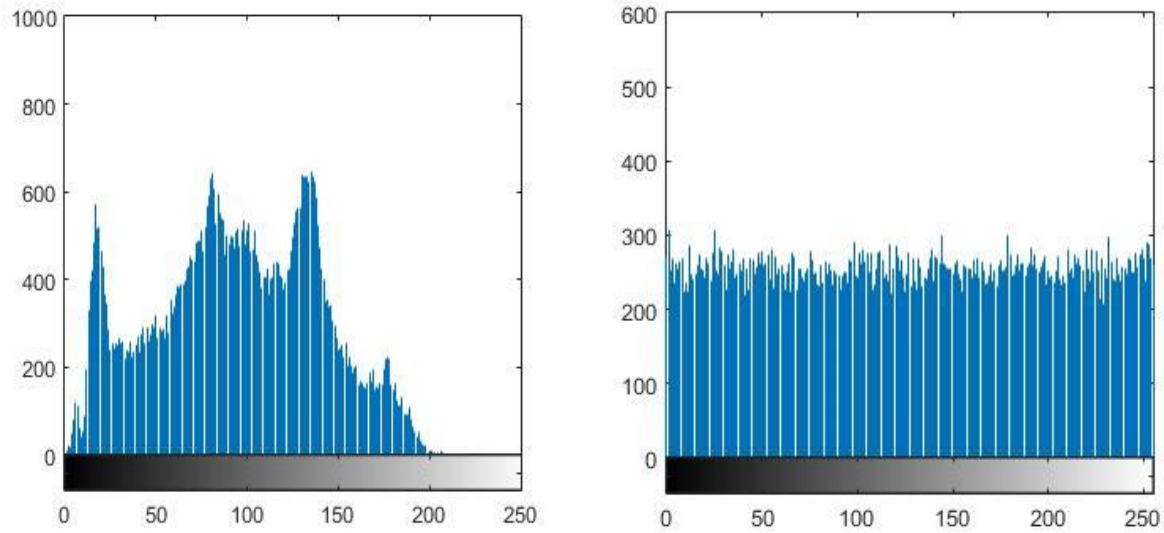
Baboon image Histogram Encrypted Baboon image Histogram

Figure 5.11: Histogram analysis result of plain and encrypted Baboon image



Peppers image Histogram | Encrypted Peppers image Histogram

Figure 5.12: Histogram analysis result of plain and encrypted Baboon image



Barbara image Histogram | Encrypted Barbara image Histogram

Figure 5.13: Histogram analysis result of plain and encrypted Barbara image

From all the histogram figure it is clear that the histograms of the encrypted image are flat and the gray-scale values are uniformly distributed over the entire encrypted image. Thus, our proposed image encryption scheme resists statistical attack based on analysis of histogram of cipher image.

5.2.2.2 Correlation Coefficient Analysis

The correlation coefficient is a useful measure to judge the security level of any image encryption scheme. It is used to find the degree of similarity between the original image and the corresponding encrypted image and between adjacent pixels of the encrypted image. Correlation is a measure of the relationship between two variables or pixels in an image. There is a very close correlation between them if the two pixels are the two neighbouring pixels in an image. If the two pixels are not neighbouring pixels then it is said that they are less correlated. This is called adjacent pixels correlation. There is a strong correlation between adjacent pixels, in an original image. By knowing the value of neighbor pixels strong correlation helps to predict the value of a pixel. In the case of the encrypted image, the strong correlation is not expected. So, the correlation between adjacent pixels should be lower. Generally, correlation along three directions namely diagonal, horizontal and vertical are calculated. The correlation coefficient of the plain image is always nearly equal to 1 while that of the cipher image correlation coefficient greatly reduced to close 0. For experimental purpose, we took both original and cipher image. Then the correlation coefficients $r_{x,y}$ of two adjacent pixels are calculated according to the following formulas:

$$r_{ab} = \frac{\operatorname{cov}(a,b)}{\sqrt{D(a)}\sqrt{D(b)}} \tag{5.1}$$

Where,

$$\operatorname{cov}(a,b) = \frac{1}{n}\sum_{i=1}^{n}\left(a_i - E(a)\right)\left(b_i - E(b)\right)$$

$$E(a) = \frac{1}{n}\sum_{i=1}^{n} a_i,\ E(b) = \frac{1}{n}\sum_{i=1}^{n} b_i$$

$$D(a) = \frac{1}{n}\sum_{i=1}^{n}\left(a_i - E(a)\right)^2,\quad D(b) = \frac{1}{n}\sum_{i=1}^{n}\left(b_i - E(b)\right)^2$$

Here, a and b in the above expression are the two adjacent pixels of the image and n is the number of pair of pixels in the image. $cov(a,b)$ is the covariance between a and b and $E(a)$ and $D(a)$ are the mean and standard deviation of the pixel values of a_i and b_i respectively. We randomly selected 5000 pairs of adjacent pixels (in horizontally, vertically and diagonally) within an image to compute the coefficient of correlation for plain image and encrypted image.

Table 5.1 reports the correlation coefficient of several plain images and those of their cipher image. From table 5.1 it is clearly seen that pixels of the original image are highly correlated whereas in the encrypted image correlation are very low. The graphical view of relation sheep between the adjacent pixels in horizontal, vertical, and diagonal direction in the original and encrypted Lena image is shown in Figure 5.14. The correlation coefficient between adjacent pixels can be shown using a scatter diagram. From Figure 5.12 it may be noted that the scatter diagram of the plain image is settled along the diagonal $(y = x)$ line, which signifies that adjacent pixels are highly correlated. Scattered diagram distributed over the entire region, in case of the encrypted image which implies that the value of a pixel can not be predicted from its neighbor pixels. So, the encrypted image adjacent pixels are uncorrelated.

Table 5.1: Result of correlation coefficient analysis of plain and cipher image.

Image	Direction		
	Horizontal	Vertical	Diagonal
Lena plain image	0.9659	0.9458	0.9287
Lena cipher image	0.0017	-0.0053	-0.0013
Lake plain image	0.9392	0.9482	0.9104
Lake cipher image	0.0046	-0.0076	-0.0072
Baboon plain image	0.7974	0.8392	0.7642
Baboon cipher image	-0.0012	-0.0063	-0.0049
Peppers plain image	0.9449	0.9476	0.9128
Peppers cipher image	0.0010	0.0021	0.0064
Barbara plain image	0.9468	0.9277	0.9028
Barbara cipher image	0.0063	-0.0053	-0.0023
Plain Cameraman image	0.9518	0.9352	0.9048
Cameraman cipher image	0.0056	0.0029	-0.0063

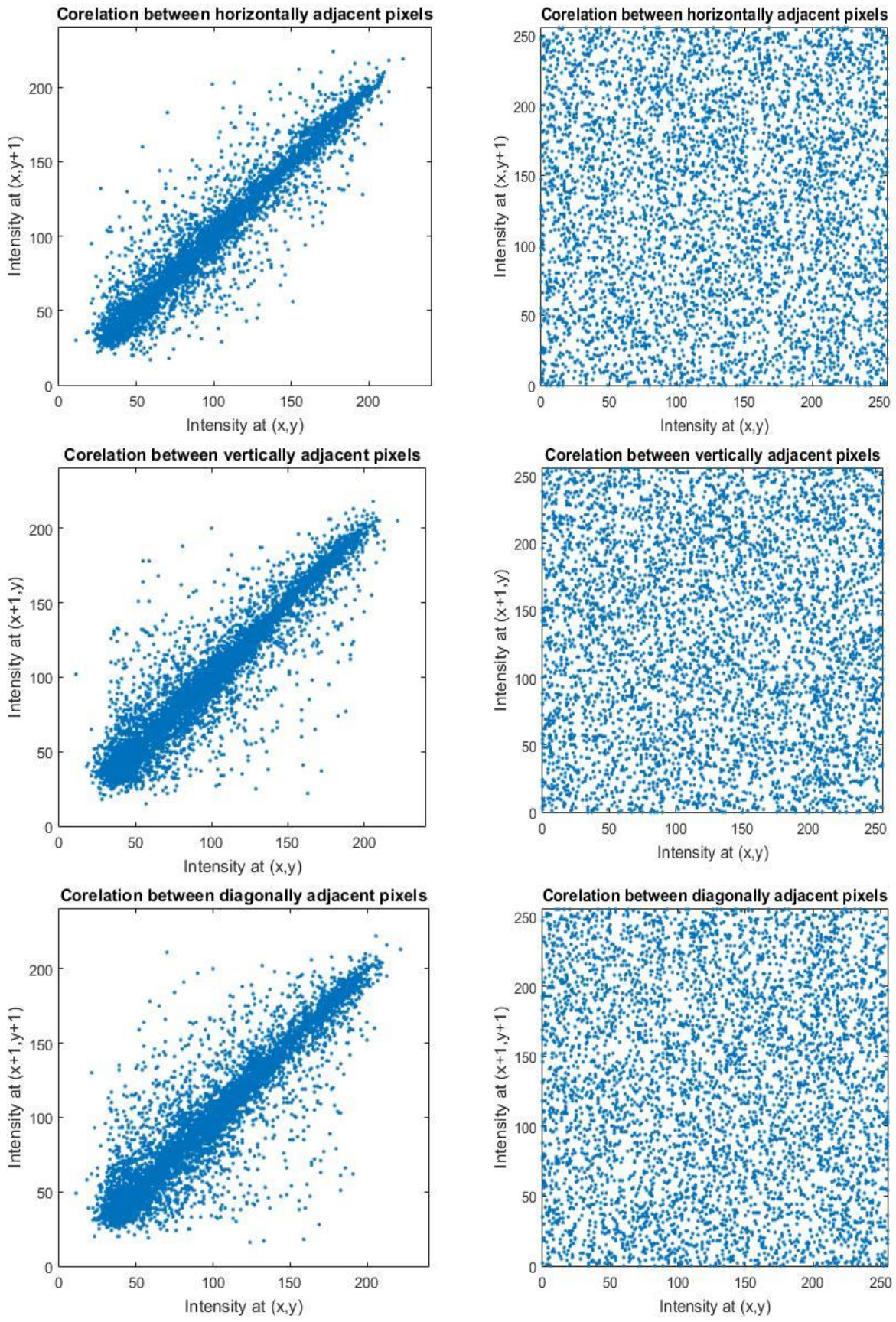


Figure 5.14: Correlation of adjacent pixels original and encrypted Lena image

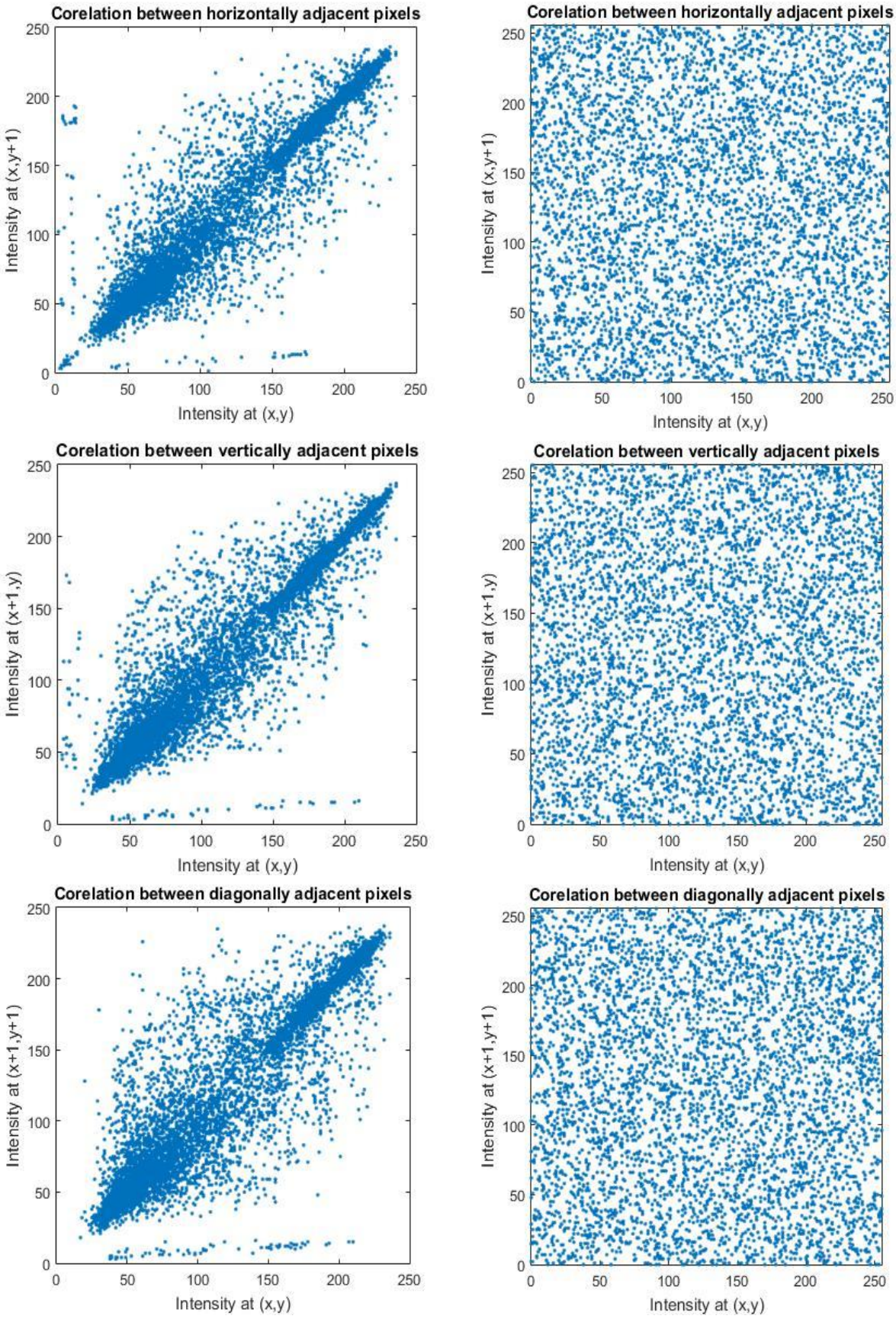


Figure 5.15: Correlation of adjacent pixels original and encrypted Lake image

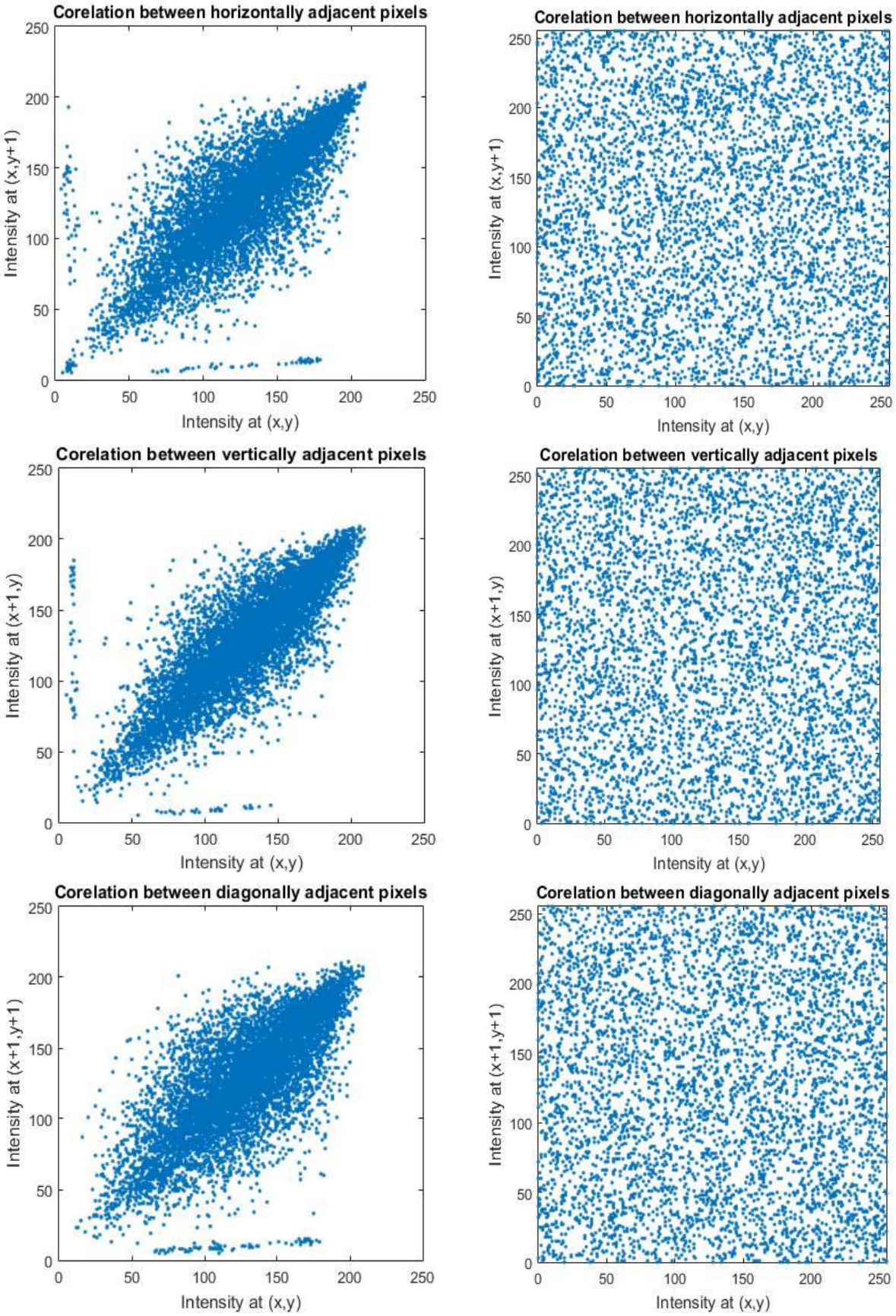


Figure 5.16: Correlation of adjacent pixels original and encrypted Baboon image

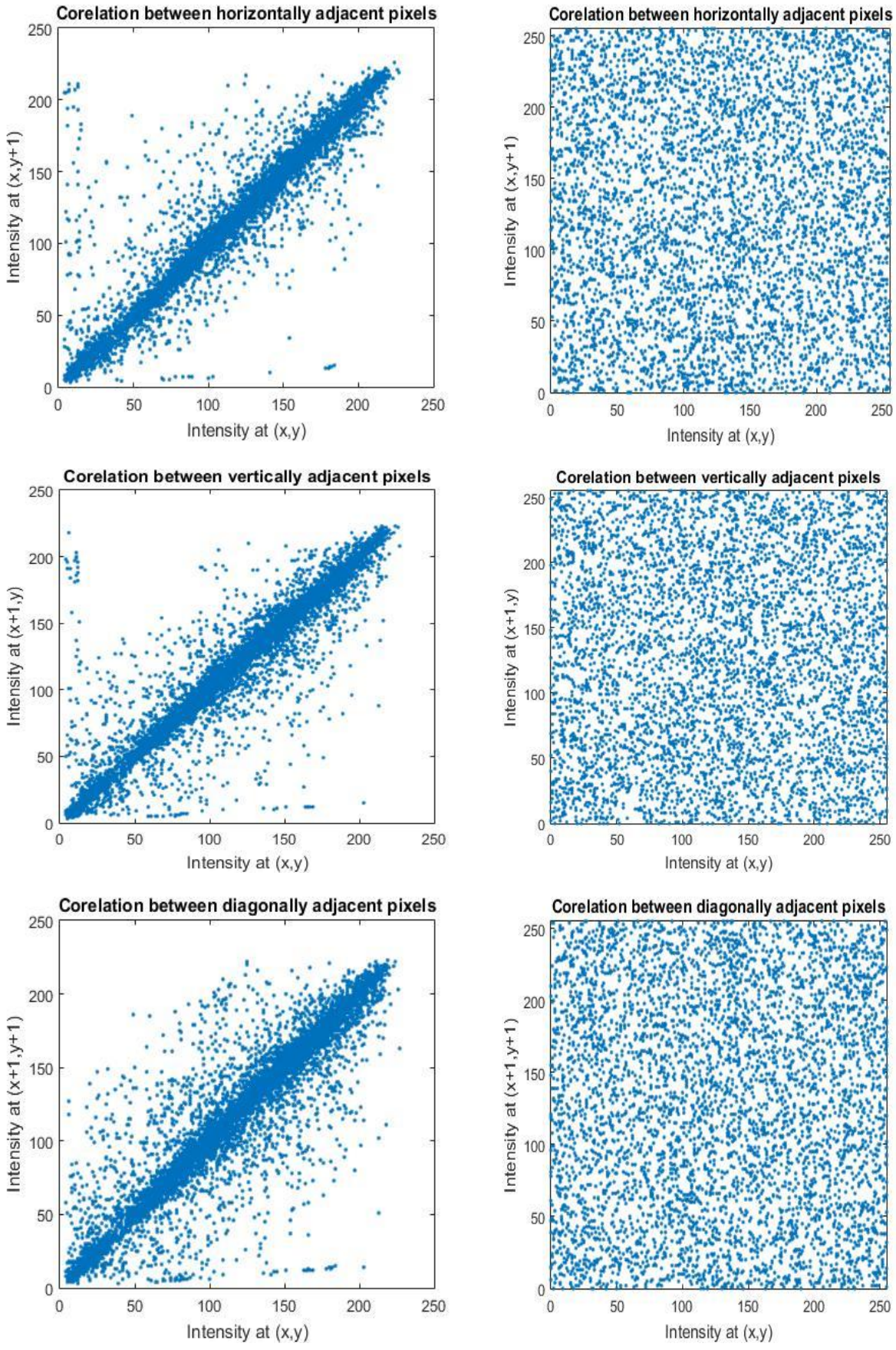


Figure 5.17: Correlation of adjacent pixels original and encrypted Peppers image

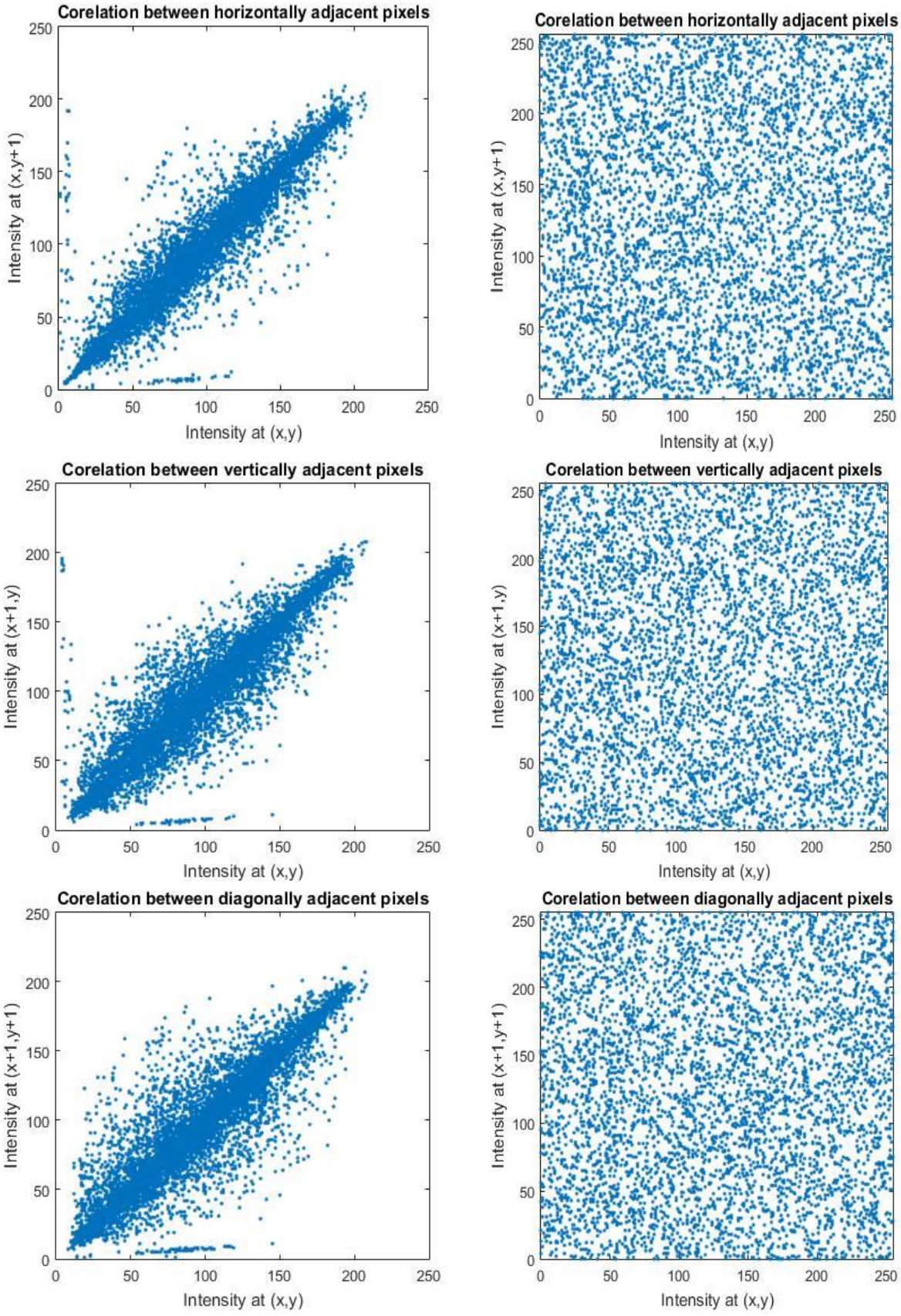


Figure 5.18: Correlation of adjacent pixels original and encrypted Barbara image

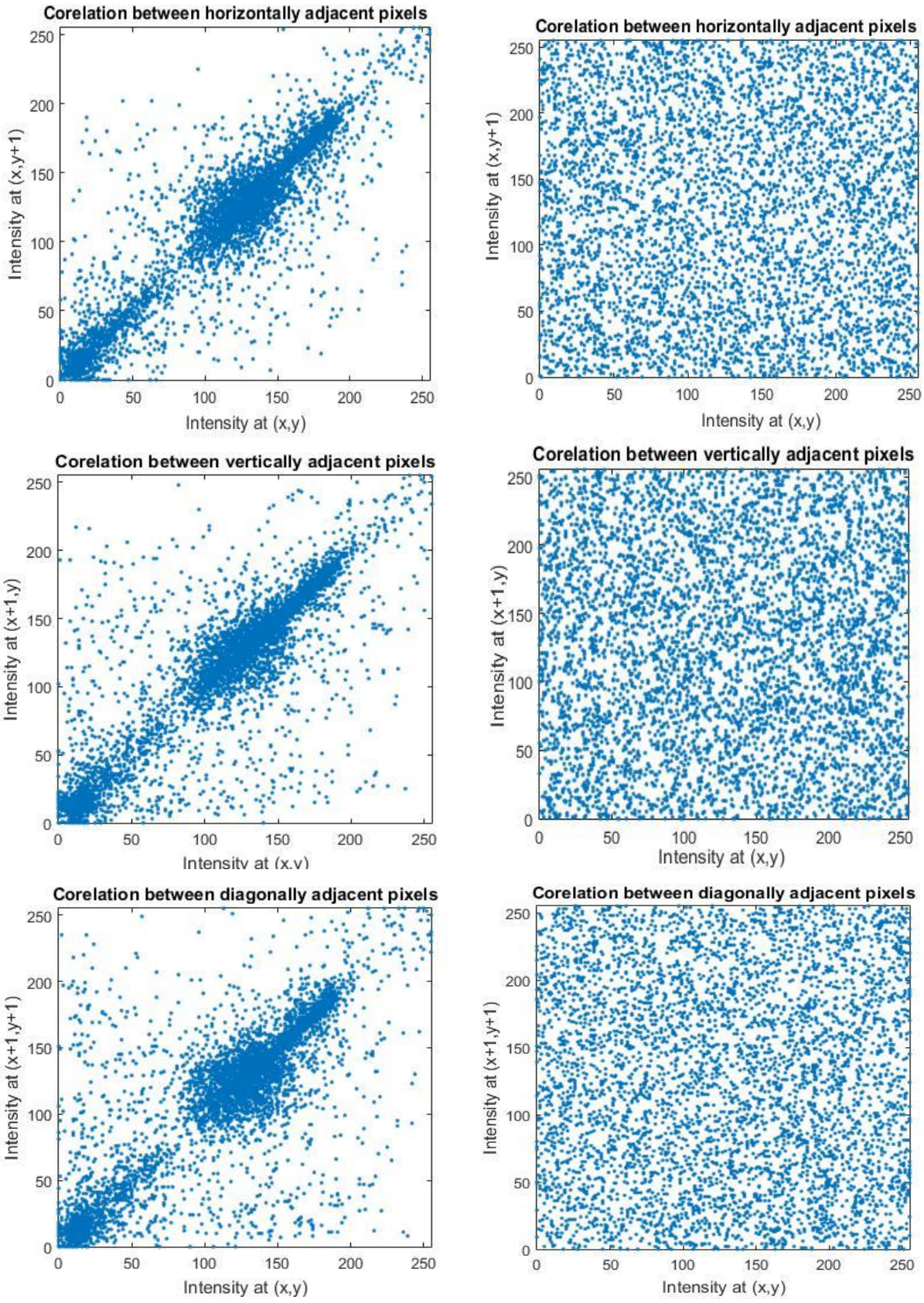


Figure 5.19: Correlation of adjacent pixels original and encrypted Cameraman image.

It is clear from Table 5.1 and Fig.5.14, Fig.5.15, Fig. 5.16, Fig. 5.17, Fig. 5.18 and Fig. 5.19 that the correlation coefficients of the plain images are close to one and the correlation coefficient of the cipher image are near to zero. Therefore, we conclude that adjacent pixels of the plain image are highly correlated. In case of cipher image correlations between adjacent pixels are negligible. Finally from the entire figure we observed that the correlation between adjacent pixels in the all the encrypted image is reduced and hence the proposed image encryption method resists the statistical attacks.

5.2.2.3 Information Entropy Analysis

It is well known that Information Entropy is one of the most important criteria to test the image randomness. Information entropy is defined to express the degree of uncertainties in the system. We can use it to express the uncertainties of the image information. Information entropy is used to measure the uniform distribution of pixel gray-level in the image. If the entropy is bigger, the uncertainty of the image is greater. A gray-scale image has possible intensity values ranging from 0 to 255 which can be encoded by 8 bit. For a gray-scale image, the ideal entropy value is 8 and it corresponds to a perfect noise-image. Thus, for strong image encryption algorithm, the entropy of encrypted image should be as close to 8 as possible. According to Shannon's theory, the entropy $H(m)$ of a message source m can be given by

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} \tag{5.2}$$

Where $p(m_i)$ is the probability of symbol m_i and N is the number of bits for each symbol m_i. We can get the ideal entropy for a random image with 256 gray levels is 8 according to the equation. The information entropy of the plain and cipher images generated from our algorithm are listed in Table 5.2. For the image "Lena", the entropy of the encrypted image shown is Figure 5.1 is 7.9975, which is close to 8 and demonstrates that the cipher image close to a random image. We also conduct the entropy analysis on other "Lake", "Peppers", "Baboon", "Barbara" images and the calculates results are listed in Table 5.2, which are very close to the theoretical value of 8.

Table 5.2: Results of information entropy analysis of plain and cipher image

Entropy analysis	Size	Original image	Cipher image
Lena	256*256	7.2283	7.9975
Lake	256*256	7.4706	7.9972
Baboon	256*256	7.2589	7.9970
Peppers	256*256	7.5877	7.9969
Barbara	256*256	7.4237	7.9973
Cameraman	256*256	7.1048	7.9974

5.2.3 Differential attack: NPCR and UACI

A general requirement for all image encryption schemes is that the encrypted image is significantly different from his original version. The differential attack is to study how a small change in a plain image can affect the corresponding cipher image. A good image encryption approach should have the ability to resist differential attacks that is to say a small change (even if changing a bit) in a plain image can cause great change in the cipher image. Two of the most popular indices to quantify the performance of resisting differential attacks in image encryption are the number of pixels change rate (NPCR) and the unified average changing intensity(UACI). The NPCR measures the percentage of different pixel numbers and UACI measures the average intensity of differences between two images. The NPCR and UACI values are calculated as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{5.3}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{\left|E_1(i,j) - E_2(i,j)\right|}{255}\right] \times 100\% \tag{5.4}$$

Where, M and N are the width and height of the image and $E_1(i,j)$ $E_2(i,j)$ denotes the pixel values of the *ith* row and *jth* column of images of E_1 and E_2 respectively and $D(i,j)$ is difference array, it can be calculated by

$$D(i,j) = \begin{cases} 1, & if\ E_1(i,j) = E_2(i,j) \\ 0, & if\ E_1(i,j) \neq E_2(i,j) \end{cases}$$

It is clear that in order to resist differential attack the NPCR and UACI values should be large enough for an ideal image encryption scheme. NPCR and UACI of "Lena", "Lake", "Baboon", "Peppers", and "Barbara", "Cameraman" are listed in Table 5.3. From the result in Table 5.3, it is clear that NPCR value is very close to 100% and UACI is about 33%, which demonstrated that the proposed image encryption technique has a strong ability to resist differential attack.

Table 5.3: Resistance to differential attack analysis

Images	NPCR	UACI
Encrypted image Lena	99.6262	33.8254
Encrypted image Lake	99.6460	33.8919
Encrypted image Baboon	99.6094	33.3162
Encrypted image Peppers	99.6552	33.3756
Encrypted image Barbara	99.6231	33.5166
Encrypted Cameraman image	99.6429	33.4709

5.3 Comparison with some existing image encryption scheme

In this section, we compare our proposed image encryption scheme with some other existing image encryption scheme. The comparison of adjacent pixel correlation obtained by our proposed image encryption scheme and the existing schemes are listed in Table 5.4 for Lena image.

Table 5.4: Comparison of correlation coefficient test on encrypted Lena image

Encryption Methods	Direction		
	Horizontal	Vertical	Diagonal
Ref. [36]	0.0214	0.0465	-0.0090
Ref. [38]	-0.0288	0.0145	0.0365
Ref. [37]	0.0039	-0.0314	0.0158
Ref. [39]	0.4968	0.4938	0.0480
Proposed	0.0017	-0.0053	-0.0013

From the result in Table 5.4, it is clear that the correlation between adjacent pixels in encrypted Lena images is optimal and close to zero and it is observed that the obtained correlation coefficient values are better than the image encryption method in [36, 37, 38, 39].

The comparison of adjacent pixel correlation obtained by our proposed image encryption scheme and the existing schemes are listed in Table 5.5 for Lake image.

Table 5.5: Comparison of correlation coefficient test on encrypted Lake image.

Encryption Methods	Direction		
	Horizontal	Vertical	Diagonal
Ref. [39]	0.4996	0.5029	0.0647
Ref. [40]	0.0118	0.0100	-0.0274
Ref. [41]	0.0231	0.0140	0.0097
Proposed	0.0046	-0.0076	-0.0072

From the result in Table 5.5, it is clear that the correlation between adjacent pixels in encrypted Lake image is optimal and close to zero and it is observed that the obtained correlation coefficient values are better than those image encryption method in [39, 40, 41].

The key space supported by the proposed image encryption method and other existing method is listed in Table 5.6.

Table 5.6: Comparison of key space

Encryption method	Keyspace
Ref. [39]	2^187
Ref. [41]	2^276
Ref. [42]	2^80
Ref. [43]	2^216
Ref. [11]	2^273
Ref. [44]	2^129
Proposed method	2^299

The comparison of information entropy obtained by our proposed image encryption method and existing image encryption method are listed in Table 5.7.

Table 5.7: Comparison of information entropy value

Entropy	Images			
	Lena	Peppers	Baboon	Barbara
Ref. [51]	7.9907	7.9900	7.9912	7.9907
Ref. [52]	7.9914	7.9955	7.9944	7.9954
Ref. [32]	7.9874	7.9860	-	7.9867
Ref. [45]	7.9895	7.9915	-	-
Ref. [46]	7.9923	-	7.9925	-
Ref. [47]	7.9915	-	7.9869	-
Ref. [48]	-	7.9958	7.9938	-
Proposed	7.9975	7.9969	7.9970	7.9973

From Table 5.7 it is observed that result obtained by proposed image encryption technique is acceptable and better than those image encryption method in [32, 45, 46, 47, 48, 51, 52].

The comparison of NPCR and UACI value obtained by our proposed image encryption method and existing image encryption method are listed in Table 5.8.

Table 5.8: Comparison of NPCR and UACI value for Baboon image.

Algorithm	NPCR	UACI
Ref. [44]	97.89	32.61
Ref. [40]	99.53	33.61
Ref. [48]	99.10	33.25
Proposed	99.60	33.31

From Table 5.8 it is observed that result obtained by proposed image encryption technique is acceptable and better than those image encryption method in [40, 44, 48].

Chapter-6

Conclusion & Future Scope

6.1 Conclusion

In this thesis, we proposed an image encryption scheme based on Two-dimensional Henon map, four-dimensional hyperchaotic Lorenz system and DNA encoding operation. In order to extend the scope of secret in this thesis, we used two-dimensional Henon map and four-dimensional hyperchaotic Lorenz system. The proposed image encryption technique mainly divided into three main parts. At first, a random matrix as the same size of the plain image is generated through successive iteration by Henon mapping and we set the initial value and parameter of Henon map. After that, we solve the four-dimensional hyperchaotic Lorenz System using a fourth order Runge-Kutta method to obtain four sequences. According to the first and second random sequence generated by Lorenz hyperchaotic system and DNA encoding rule, each sub-block of the image and each sub-block of the random matrix is encoded into a DNA sequence and DNA matrix generated. Using third random sequence, we perform DNA addition, subtraction and XOR operation between two DNA matrixes. Using four random sequences and DNA decoding rule each DNA matrix is decoded into binary. The decoded binary is converted to decimal to obtain the final encrypted image. We have performed key space analysis, key sensitivity analysis, and statistical analysis to demonstrate the security of the proposed image encryption scheme. The image encryption technique has a large key space and too much sensitive to its keys, thus, it can resist brute-force attack. The correlation coefficient of the proposed image encryption scheme is close to 0 and histogram of the proposed scheme is uniform and entropy value is close to 8, thus the proposed image encryption scheme can resist statistical analysis. NPCR value is very close to 100% and UACI is about 33%, which demonstrated that the proposed image encryption technique has a strong ability to resist differential attack. we compare our proposed image encryption scheme with some other existing image encryption scheme. Finally, we conclude with the remark that our proposed image encryption scheme is expected to be useful for real-time image encryption and transmission applications.

6.2 Future Scope

The proposed image encryption technique has been applied on a grayscale image, which can be extended to color image.

Using communication network authorizes people can send and receive digital video. Since the internet is not a secure communication channel. During digital video transmission, it may be possible that some secret video image can be accessed, stolen or modified by the unauthorized people. So, during transmission some encryption methodologies are needed that can protect digital video from attacks. So our proposed algorithm can be applied for the video image.

Proposed work is done in the spatial domain in this thesis. Using wavelets it can be extended in the frequency domain to increase the speed and reduce the storage requirement for the image.

References

[1] Fridrich, Jiri. "Symmetric ciphers based on two-dimensional chaotic maps." International Journal of Bifurcation and Chaos 8.06 (1998): 1259-1284.

[2] Lian, Shiguo, Jinsheng Sun, and Zhiquan Wang. "A block cipher based on a suitable use of the chaotic standard map." *Chaos, Solitons & Fractals* 26.1 (2005): 117-129.

[3] Wang, Yong, et al. "A chaos-based image encryption algorithm with variable control parameters." Chaos, Solitons & Fractals 41.4 (2009): 1773-1783

[4] Wang, Yong, et al. "A new chaos-based fast image encryption algorithm." Applied soft computing 11.1 (2011): 514-522.

[5] N Khade, Pawan., and Manish Narnaware. "3D chaotic functions for image encryption." International Journal of Computer Science Issues (IJCSI) 9.3 (2012): 323.

[6] Wang, Xingyuan, and Qian Wang. "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos." Nonlinear Dynamics 75.3 (2014): 567-576.

[7] Tang, Zhenjun, Xianquan Zhang, and Weiwei Lan. "Efficient image encryption with block shuffling and chaotic map." Multimedia tools and applications 74.15 (2015): 5429-5448.

[8] Hua, Zhongyun, et al. "2D Sine Logistic modulation map for image encryption." Information Sciences 297 (2015): 80-94.

[9] Xu, Lu, and et al. "A novel bit-level image encryption algorithm based on chaotic maps." Optics and Lasers in Engineering 78 (2016): 17-25

[10] Belazi, Akram, Ahmed A. Abd El-Latif, and Safya Belghith. "A novel image encryption scheme based on substitution-permutation network and chaos." Signal Processing 128 (2016): 155-170.

[11] Li, Yueping, Chunhua Wang, and Hua Chen. "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation." Optics and Lasers in Engineering 90 (2017).

[12] Zhou, Guomin, et al. "A novel image encryption algorithm based on chaos and Line map." Neurocomputing 169 (2015): 150-157.

[13] Bakhshandeh, Atieh, and Ziba Eslami. "An authenticated image encryption scheme based on chaotic maps and memory cellular automata." Optics and Lasers in Engineering 51.6 (2013): 665-673.

[14] Niyat, Abolfazl Yaghouti, Mohammad Hossein Moattar, and Masood Niazi Torshiz. "Color image encryption on hybrid hyper-chaotic system and cellular automata." Optics and Lasers in Engineering 90 (2017): 225-237.

[15] Mondal, Bhaskar, Shrey Singh, and Prabhakar Kumar. "A secure image encryption scheme based on cellular automata and chaotic skew tent map." Journal of Information Security and Applications 45 (2019): 117-130.

[16] Sivakumar, T., and R. Venkatesan. "A novel approach for image encryption using dynamic SCAN pattern." *IAENG International Journal of Computer Science* 41.2 (2014): 91-101.

[17] Rad, Reza Moradi, Abdolrahman Attar, and Reza Ebrahimi Atani. "A new fast and simple image encryption algorithm using scan patterns and xor." *International Journal of Signal Processing, Image Processing and Pattern Recognition* 6.5 (2013): 275-290.

[18] Sivakumar, T., and R. Venkatesan. "A Novel Image Encryption Using Calligraphy Based Scan Method and Random Number." KSII Transactions on Internet & Information Systems 9.6 (2015).

[19] Singar, Chandra Prakash, Jyoti Bharti, and R. K. Pateriya. "Image encryption based on cell shuffling and scanning techniques." 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE). IEEE, 2017.

[20] Das, Sujit Kumar, and Bibhas Chandra Dhara. "A new image encryption method using circle." 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017.

[21] Ye, Guodong. "A block image encryption algorithm based on wave transmission and chaotic systems." Nonlinear Dynamics 75.3 (2014): 417-427.

[22] Liao, Xiaofeng, Shiyue Lai, and Qing Zhou. "A novel image encryption algorithm based on self-adaptive wave transmission." Signal Procssing 90.9 (2010): 2714-2722.

[23] Chen, Wen. "Optical multiple-image encryption using three-dimensional space." IEEE Photonics Journal 8.2 (2016): 1-8.

[24] Wang, Y., C. Quan, and C. J. Tay. "Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm." Optics and Lasers in Engineering 78 (2016): 8-16.

[25] Wang, Xing-Yuan, Ying-Qian Zhang, and Xue-Mei Bao. "A novel chaotic image encryption scheme using DNA sequence operations." *Optics and Lasers in Engineering* 73 (2015): 53-61.

[26] Zhang, Qiang, Ling Guo, and Xiaopeng Wei. "A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system." Optik-International Journal for Light and Electron Optics 124.18 (2013): 3596-3600.

[27] Wu Xiangjun, Haibin Kan, and Jürgen Kurths. "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps." Applied Soft Computing 37 (2015): 24-39.

[28] Guesmi, R., et al. "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2." *Nonlinear Dynamics* 83.3 (2016): 1123-1136.

[29] Zhen, Ping, et al. "Chaos-based image encryption scheme combining DNA coding and entropy." Multimedia Tools and Applications 75.11 (2016): 6303-6319.

[30] Wu, Xiangjun, et al. "Color image DNA encryption using NCA map-based CML and one-time keys." Signal Processing 148 (2018): 272-287.

[31] Zhang, Xuncai, Feng Han, and Ying Niu. "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding." *Computational intelligence and neuroscience*2017 (2017).

[32] Liu, Hongjun, and Xingyuan Wang. "Image encryption using DNA complementary rule and chaotic maps." Applied Soft Computing 12.5 (2012): 1457-1466.

[33] Wu, Jiahui, Xiaofeng Liao, and Bo Yang. "Image encryption using 2D Hénon-Sine map and DNA approach." Signal Processing 153 (2018): 11-23.

[34] Chai, Xiuli, Yiran Chen, and Lucie Broyde. "A novel chaos-based image encryption algorithm using DNA sequence operations." Optics and Lasers in Engineering 88 (2017): 197-213.

[35] Zhan, Kun, et al. "Cross-utilizing hyperchaotic and DNA sequences for image encryption." Journal of Electronic Imaging 26.1 (2017): 013021

[36] Zhen, Ping, et al. "Chaos-based image encryption scheme combining DNA coding and entropy." Multimedia Tools and Applications 75.11 (2016): 6303-6319.

[37] Zhang, Xuncai, Zheng Zhou, and Ying Niu. "An image encryption method based on the feistel network and dynamic DNA encoding." IEEE Photonics Journal 10.4 (2018): 1-14.

[38] Yavuz, Erdem, et al. "A chaos-based image encryption algorithm with simple logical functions." Computers & Electrical Engineering 54 (2016): 471-483.

[39] Gong, Lihua, et al. "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform." Optics & Laser Technology 103 (2018): 48-58.

[40] Liu, Xingbin, et al. "Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model." IEEE Access (2019).

[41] Zhou, Nanrun, et al. "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing." Optics & Laser Technology 82 (2016): 121-133.

[42] Enayatifar, Rasul. "Image encryption via logistic map function and heap tree." International Journal of Physical Sciences 6.2 (2011): 221-228.

[43] Song, Chun-Yan, Yu-Long Qiao, and Xing-Zhou Zhang. "An image encryption scheme based on new spatiotemporal chaos." Optik-International Journal for Light and Electron Optics 124.18 (2013): 3329-3334.

[44] Enayatifar, Rasul, et al. "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata." Optics and Lasers in Engineering 71 (2015): 33-41.

[45] Huang, Xiaoling, and Guodong Ye. "An image encryption algorithm based on hyper-chaos and DNA sequence." Multimedia tools and applications 72.1 (2014): 57-70.

[46] Guan, Mengmeng, Xuelin Yang, and Weisheng Hu. "Digital image encryption using chaotic DNA encoding in frequency-domain." Tenth International Conference on Graphics and Image Processing (ICGIP 2018). Vol. 11069. International Society for Optics and Photonics, 2019.

[47] Das, Subhajit, Satyendra Nath Mondal, and Manas Sanyal. "A Novel Approach of Image Encryption Using Chaos and Dynamic DNA Sequence." 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, 2019

[48] Enayatifar, Rasul, et al. "Image encryption using a synchronous permutation-diffusion technique." Optics and Lasers in Engineering 90 (2017): 146-154.

[49] Chen, Yuming. "The existence of homoclinic orbits in a 4D Lorenz-type hyperchaotic system." Nonlinear Dynamics 87.3 (2017): 1445-1452.

[50] Sprott, J. C. "High-dimensional dynamics in the delayed Hénon map." Electronic journal of theoretical physics 3.12 (2006): 19-35.

[51] Tang, Zhenjun, et al. "Reversible data hiding with differential compression in encrypted image." Multimedia Tools and Applications 78.8 (2019): 9691-9715.

[52] Rajagopalan, Sundararaman, et al. "YRBS coding with logistic map–a novel Sanskrit aphorism and chaos for image encryption." Multimedia Tools and Applications 78.8 (2019): 10513-10541.