T.C.

ALTINBAŞ UNIVERSITY

Electrical and Computer Engineering

IMPROVING OF PERMUTATION AND DIFFUSION STEP FOR CHAOS BASED IMAGE ENCRYPTION USING MULTIPLE HYPER-CHAOTIC SYSTEMS AND DIFFERENT TECHNIQUES

Mustafa Kamil Khairullah

Master Thesis

Supervisor

Prof. Dr. Oguz Bayat

Istanbul, (2019)

IMPROVING OF PERMUTATION AND DIFFUSION STEP FOR CHAOS BASED IMAGE ENCRYPTION USING MULTIPLE HYPER-CHAOTIC SYSTEMS AND DIFFERENT TECHNIQUES

by

Mustafa Kamil Khairullah

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering
in partial fulfillment of the requirements for the degree of
Master of Science

ALTINBAŞ UNIVERSITY

2019

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of .....

Academic Title Name SURNAME Co-Supervisor	Academic Title Name SURNAME Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

Academic Title Name SURNAME	Faculty, University	_____
Academic Title Name SURNAME	Faculty, University	_____
Academic Title Name SURNAME	Faculty, University	_____
Academic Title Name SURNAME	Faculty, University	_____
Assoc. Prof. Name SURNAME	Faculty, University	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of .....

Approval Date of Graduate School of
Science and Engineering: ____/____/____

_____
Academic Title Name SURNAME
Head of Department

_____
Academic Title Name SURNAME
Director

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

Mustafa Kamil Khairullah

DEDICATION

I would like to dedicate this work to my first teacher, my mother, my first supporter and role model, my father and my companion throughout the journey. Without you, this dream would never come true and to my brothers and my sisters who stood with me in order to achieve my dream.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all the instructors that have taught me more than just science, especially my supervisor Prof. Dr. Oguz Bayat and my co-advisor Prof. Dr. Mohammed Ahmed Abdala, for all the time, support and guidance provided to me along the journey to accomplish this work. Thank you all for all the knowledge and advice that made me overcome all the difficulties that I have faces.

ABSTRACT

IMPROVING OF PERMUTATION AND DIFFUSION STEP FOR CHAOS BASED IMAGE ENCRYPTION USING MULTIPLE HYPER-CHAOTIC SYSTEMS AND DIFFERENT TECHNIQUES

Khairullah, Mustafa Kamil Khairullah

M.Sc. Electrical and Computer Engineering, Altınbaş University,

Supervisor: Prof. Dr. Oguz Bayat

Date: May/2019

Pages: 52

Beside the fast development of data transmission, data encryption becomes more motivated for researchers. A major drawbacks of chaos-based image encryption are weak complexity in diffusion stage and low-key space as compared with modern cryptosystem. In this research, two effective algorithms for permutation-diffusion stages of image cryptosystem is proposed by employing two hyper-chaotic systems. These systems are utilized for the purpose of permuting and diffusing the original image pixels by generating all the encryption parameters. Lagrange equation and MD5 are considered as an auxiliary tool only used to confuse the connection between the input image and the secret keys which are intended for used in the encryption algorithm. For both algorithms, two stages of encryption are used in the proposed encryption algorithms Firstly, the sequences of the two hyper-chaotic systems are correctly merged in order to generate hybrid sequences used to permute image pixels: secondly, the hybrid hyper-chaotic sequences are properly applied with a view to generate the modified sequences that especially used for encrypting the image pixels with two rounds. The experimental results indicate that the suggested encryption algorithms are able to satisfy the requirements of security. Moreover, the proposed schemes increase key space and security and reaches minimum number of correlation coefficient.

Keywords: image encryption, image security, hyper-chaotic system, lazy wavelet transform, MD5, diffusion stage, permutation stage, cryptography.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
IDEA	International Data Encryption algorithm
TDES	Triple data encryption standard
AES	Advanced Encryption Standard
LE	Lyapunov Exponent
MD5	Message Digest Algorithm 5
LWT	Lazy Wavelet Transform
RC4	Rivest Cipher 4
PRGA	Pseudorandom Generation algorithm
ECC	Elliptic Curve Cryptography
PKC	Public Key Cryptography
RGB	Red, Green, Blue
CMYK	Cyan, Magenta, Yellow, black
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
CC	Correlation Coefficient
MAE	The Mean Absolute Error
NPCR	Number of Pixel Change Rate
UACI	Unified Averaged Changed Intensity
TIFF	Tagged Image File Format
LI	Lagrange Interpolation
PNG	Portable Graphics Format

1. INTRODUCTION

Along with instantaneous development of technologies in diverse aspect, image security is becoming essential, particularly in the online transaction. Despite the fact that a large number of cryptosystems have been constructed, the demands to establish a novel and developed encoding algorithm are increased [1]. Nowadays, the technologies of communication, specially the internet, are transmitted various types of digital data. Digital images are significantly increased among these transmitted data [2]. Therefore, preservation of information security in efficient way has significantly become functional problem. Countless of ciphering techniques are simply able to ensure the security of digital information in the period of transmission. Despite that, the protection of the digital contents that transmitted through online transaction is limit. Besides immediate increase of development for technology in digital data transmission, image protection technology has become indispensable. Generally, a quite number of algorithms are intended for used in text data. In other word, the encryption algorithms that are convenient to use in textual data are not appropriate to use in image and multimedia, this is because the huge data of image and the constrains of real time [5-6-7]. Consequently, large number of algorithms are not favorable for image for instant, data encryption standard (DES), international data encryption algorithm (IDEA), Triple data encryption standard (TDES) and advanced encryption standard (AES) [8]. These algorithms are considered to be inappropriate for image encryption for two obvious reasons. The first and essential reason is that the size for image is obviously large in comparison with the size of text. Along with the bulk data of image, traditional algorithms probably take highly extended time to execute. The second reason is that the recovered text should be identical to the its corresponding original texts. In image encryption the fully identically is not substantial between original image and recovered image. The recovered image that has insignificant distortion is considered passable for human perception. [9-10].

1.1 PROBLEM DEFINITIONS

Various problems are associated with image encryption system. such as problems that related to low key space and low stage of security which are significantly occurred by low dimensional chaotic maps [11], the problems of longer time consuming are generally occurred in algorithm that used additional steps of diffusions particularly in algorithm that used DNA technology and

the algorithms used bit-level permutation [12-13], the problems associated with the cost required for implementation are usually happened in algorithm that used optical technology and the problems of unwanted complexity that possibly increase the time with no sturdy security and this types of problems are happened in algorithms that use wavelet technology [14].

1.2 CONTRIBUTION OF THESIS

The research contains five main contributions, the first contribution is how to implement fast and secure image encryption algorithm in order to produce algorithm along with extremely large key space, high reliability, high entropy, valid ratio of correlation coefficient (CC), large sensitivity to the initial secret keys, large sensitivity to changing one bit in original image pixels, high ability for resisting various types of attacks and high quality of decryption.

The second contribution, increasing the key space efficiently by producing hybrid sequences that are generated by merging two sensitive hyper-chaotic systems.

The third contribution, find a new relation between input image and secret keys by using message digest algorithm 5 (MD5) in order to produce different key for each input image.

The forth contribution, developing a permutation stage for image encryption for the purpose of achieving best encryption result.

The fifth contribution, raising the security by employing lazy wavelet transform (LWT) through separating the image pixels according to their indices to the odd indices and even indices, lazy wavelet transform (LWT) allows to encrypt the pixel by a key and the adjacent pixel is encrypted by another key in order to confuse the correlation for adjacent pixels.

1.3 THESIS ORGANIZATION

The proposed research is consisted from six chapters, chapter two is intended to describe an overview and literature review that related to image encryption, in chapter three, an introduction about chaos theory, lazy wavelet transform and massage digest algorithm 5 (MD5), in chapter 4 the proposed algorithms, in chapter 5, the security analysis and results discussion for proposed algorithms. Eventually, chapter 6 is described the conclusion and suggestion work for future.

2. LITERATURE REVIEW

2.1 OVERVIEW

Encryption is a method used for encoding a message, image or important information in specific method that allow only parties who have the authorization to access, and prevent the unauthorized parties from access. Encryption is generally maintaining the information confidentiality by using different algorithms that have capability for converting the information into unrecognized codes. In fact, encryption does not prevent the interference, but makes intelligible content in unreadable content. Therefore, unauthorized cannot understand the encrypted information because it appears like a mixture of symbols, numbers and unintelligible characters. In encryption algorithm, the plain text or the plain image is encrypted by algorithm steps in order to generate a ciphered text or ciphered image that is not be able to read only if decrypted. Technically, encryption schemes mainly employed a cryptography key that generated in a way which it is hardly to be discovered. An authorized can easily decode the text or image by using the key that provided by the sender to authorized receiver and this operation called decryption. Five ingredients are usually used in encryption scheme as illustrated in figure 2.1 [15].

1. Plain text or plain image: the plain text/image is considered original message/image that is entered to the scheme as input.
2. Encryption scheme: the encryption scheme can perform different types of substitutions on the plain image depending on the secret keys.
3. Secret keys: the keys are treated as inputs for encryption algorithm. All the steps of substitution, permutation and transformation mainly depending on particular keys.
4. Cipher text or cipher image: cipher text/image is considered as output of the algorithm. It mainly depends on the input text/image and the secret keys. For using various keys in algorithm, two various cipher text/image will be produced.
5. Decryption algorithm: decryption algorithm is usually processed as encryption algorithm but reverse way. It depends on the cipher text/image and the secret keys to be able to recover the cipher text/image.

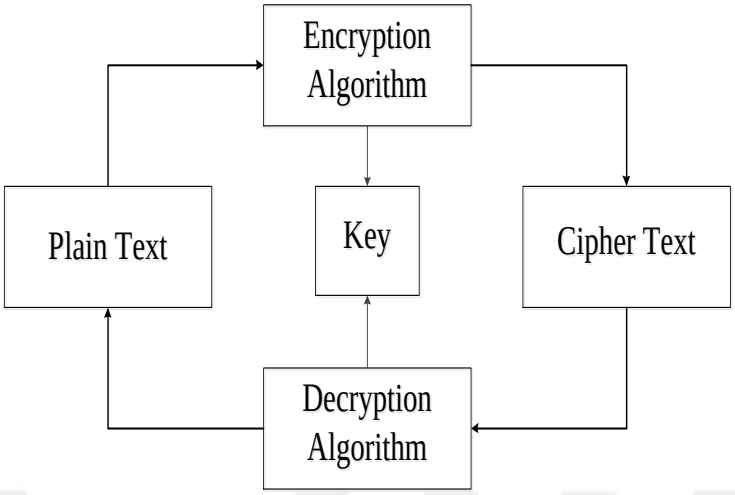


Figure 2.1: Block diagram for cryptography process.

2.2 PURPOSE OF CRYPTOGRAPHY

Cryptography is able to provide a number of security aims in order to ensure data privacy. Because the advantages of security for cryptography, the cryptography has many applications today [16]. The goals of cryptography can be summarized as follow.

2.2.1 Confidentiality

The transmitted data in computer has to be accessible only for the authorized party and not accessible for unauthorized parties.

2.2.2 Authentication

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

2.2.3 Integrity

The authorized parties can allow to make modification to the transmitted information and its prohibited to make modification for other parties between the transmitter and receiver.

2.2.4 Non Repudiation

The receiver and the transmitter have not to be capable to deny the sending.

2.2.5 Access Control

For given information, only the authorized parties are capable to access.

2.3 DIFFUSION AND CONFUSION

From the one of most essential papers on theoretical foundations for the science of cryptography, Shannon gave two fundamental properties which an efficient cryptosystem has to have hinder statistical analysis. This statistical analysis are diffusion and confusion. The diffusion is a term refers to a slight change in characters of the original texts is able to change a large number of characters in the cipher texts, and similarly, the change in the characters of the cipher text can change a large number in original image.

Confusions means that the proposed key cannot relate in easy way for the cipher text. In other words, all character for cipher text has to depend on diverse parts of the keys.

2.4 CLASSIFICATION OF CRYPTOGRAPHY

Encryption techniques are used in order to ensure security when confidential information is exchanged through communication line. The encryption technique can be classified depend on large number standard methods such as classical and modern [17].

2.4.1 Classical Cryptography

The types of classical cryptography can be classified into two main type: Substitution and Transposition [18].

2.4.1.1 Substitution cipher

Substitution is sorted into two main types [19]. The first type is he monoalphabetic cipher and it refers to a substitute cipher used simple key. The example of monoalphabetic is Caesar cipher. Polyalphabetic Cipher is the second type of Substitution cryptography. It indicates substitute cipher alphabet that its plain seems not similar from place to another place during the process of encryption. Vigenere Cipher is example of the Polyalphabetic.

Transposition cipher is a mechanism for cryptography process. It uses units of plain text to occupy the positions. And these units can be shifted depending on system of the plain text permutation that is accordingly constituted.

2.4.1.2 Transposition cipher

Transposition cipher is a mechanism for encryption. It uses units of plain text to occupy the position. And these units can be shifted depending on system of plain text permutation that is accordingly constituted [20]. Transposition cipher has two main types of transportation: keyless transposition and Keyed transposition. In keyless cipher, the characters are shuffled by means of implementing the plain text in specified way which it varies from the reading way. The example of keyless transportation is the rail fence cipher. In keyed transposition the method is different in which the plain text is divided into blocks that predetermined in size. By using a key in each block, the block characters are permuted. The Columnar is an example for keyed transposition.

2.5 MODERN CRYPTOGRAPHY

Modern cryptography is classified according to strongly scientific methods in which the computational of encryption algorithms are produced in a sequence that supposed to be difficult to be broken. In order to designed unbreakable system, the system should be resisted to the all type of attacks. In general information should be theoretically secure and is not provably able to be broken. modern cryptography can be categorized in to two categories: symmetric key cryptography and asymmetric key cryptography [21].

2.5.1 Symmetric Key Cryptography

The vital rule in symmetric algorithms is the privacy, so the key that used in encryption and decryption should be unknown for unauthorized parties. Therefore, only the authorized parties should know the secret key. It is obvious that the characterizations of symmetric key algorithms don’t need to consume high computing power. DES, CAST5, and BLOWFISH is considering as an example for symmetric cryptography. Generally, there are two types of symmetric key: stream ciphers or block ciphers [22].

2.5.1.1 Stream cipher

The stream cipher is operated in single bit or byte and the encryption process is individually applied to bits at same time. This process is basically achieved when a single bit from the secret key is added to the original text. It is mentioned that the stream cipher cryptography can be classified into two types of cipher that recognized as synchronous stream and asynchronous stream cipher. In synchronous stream cipher, the encryption system is mainly depending on key. In asynchronous stream cipher, where the key is significantly depending on cipher text. For instance: RC4, Salsa20, ISAAC, Quad, SEAL. Rivest Cipher 4 (RC4) is encryption algorithm based on use of random permutation. Two main process are included for encryption and decryption procedures. The first process is considered as scheduling algorithm for key (KSA) that gives the ability to change the key length from 1-256 bytes. The second process is considered as the pseudorandom generation algorithm (PRGA). due to the changeable key, RC4 is widely used in cryptography [23].

2.5.1.2 Block cipher

The ability of characteristics of block cipher allow the plaintext bits to be encrypted in both single and complete block simultaneous. By employing same key. It is obvious that all bits in plaintext of same block will depend one another during the process of encryption. From the practice, the major length of block ciphers is either 128 bits (16 bytes) like in advanced encryption standard (AES) or 64 bits (8 bytes) of block cipher such as data encryption standard (DES) and triple DES (3DES). Additionally, a large number of algorithms used block cipher technique. for example, Blowfish, Twofish, RC2, RC5, Camellia, CAST-128, IDEA, ARIA, Skipjack, SEED, TEA and XTEA. DES was developed by IBM team in 1974 and it was become a national standard in 1997, for this reason it is considered as first encryption standard by NIST (National Institute of Standards and Technology). DES is a 64-bit block cipher with 56 key length. The DES is jointly consist from as sixteen block cipher rounds. Practically, proportional correlation is discovered between rounds number and the amount of needed time for discovering the key through brute-force attack usage. in the other word, increasing in number of rounds lead to increase algorithm safety. DES has been widely used in many applications such as commercial applications and Military applications [24].

2.5.2 Asymmetric Key Cryptography

In asymmetric key cryptography, various keys are used in the encryption and the decryption process. These keys are called Public Key Cryptography (PKC). Generally, public key used for encryption process and private key is employed for decryption process. Basically, the asymmetric key cryptography trusts mathematical functions which are simply to calculate in the encryption process but they are hardly to calculate in the decryption process. The disadvantages of PKC is the time required to whole process is high as compared with symmetric key cryptography. several algorithms used asymmetric key cryptography such as ECC, RSA, DSA, Merkle's Puzzles, El Gamal and Diffie Hellman [25]. Elliptic Curve Cryptography (ECC) is rely on elliptic curves in limited domains. Elliptic Curve Cryptography is individually put forward technique by Neal Koblitz and Victor Miller in 1985. many facilities are provided by ECC for public key cryptosystems like providing smaller and faster key for public encryption system. The key length of ECC is 160-bit and it is considered as safer than 1024-bit key in RSA algorithm [26].

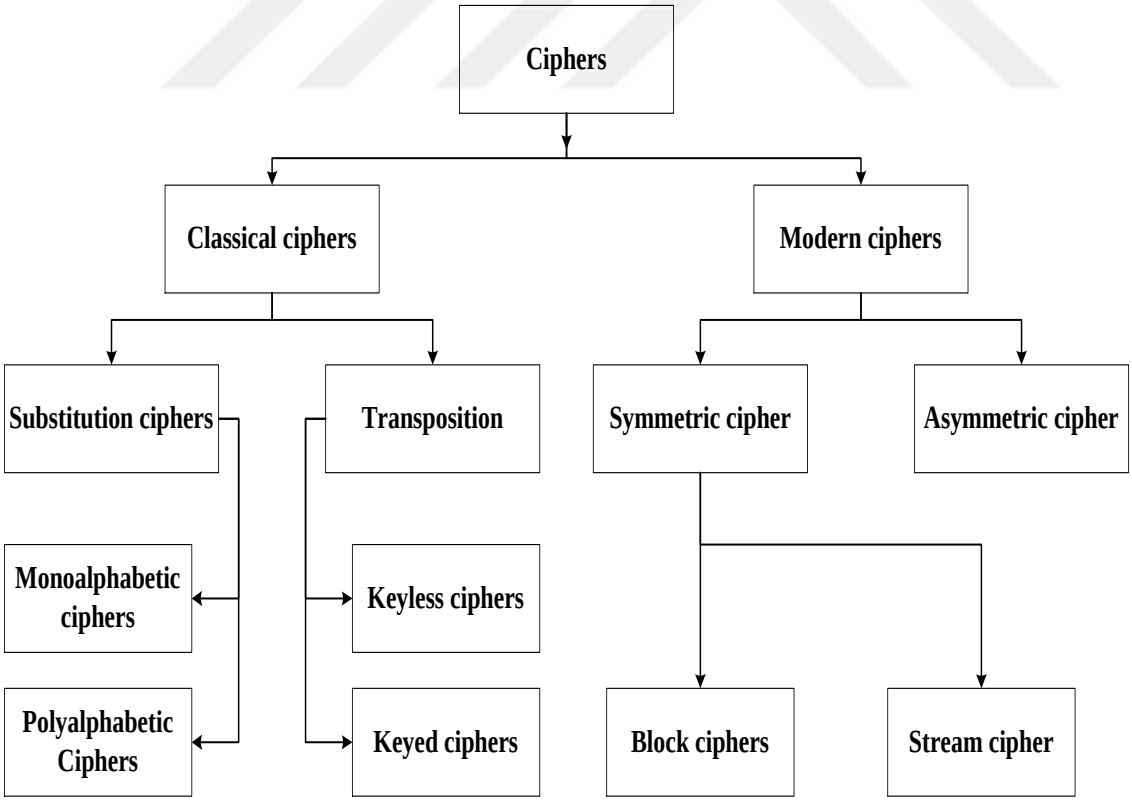


Figure 2.2: Classification of cryptography [27].

2.6 CHAOTIC TECHNIQUES

In the last few years, a variety of image encryption system that utilized chaos have widely been established in view of efficient properties of chaotic systems [28]. Chaotic properties have met the requirements of image encryption systems for instant, the sensitivity of chaotic system to its initial condition value, random results and no periodicity. In spite of the good inherited properties of chaotic systems, they are examined as not secure for the reasons that chaotic systems are produced weak security and small key space. In parallel with the evolution of chaos theory application, hyper-chaotic systems are interested additional consideration. Many encryption algorithms used hyper-chaotic systems are emerged to decrease the cons of encryption systems based on chaotic system [29]. Hyper-chaotic systems are evaluated as safer than chaotic system for used in cryptography [30].

In 2006, the authors produced an image encryption algorithm that used to permute and substitute image pixels for the purpose of presenting a strong algorithm for image encryption. A cross sampling disposal and improved treatment is also presented to enhance the characteristics of pseudorandom chaotic sequences [31].

In 2010, an algorithm based on logistic chaotic map and LSB was introduced for RGB images. Firstly, the one-dimensional map is employed to generate three sequences, these sequences used for permuted the R, G and B, where R, G and B two- dimensional matrices. Finally, using hiding technology of LSB to embed the permuted image in the carrier image in order to transmit the image securely [32].

In 2014, the authors were arranged an algorithm based on two process. A pseudo-random key is generated from hyper-chaotic system. The initial states of hyper-chaos are practically derived by applying long external key that consist from 256 bit by employing algebraic function. For the purpose of increasing the stage of security, the secret keys are related to input image. Eventually the date of image is smashing by modify every pixels value in order to crack the correlation of image pixels and to produce ciphered image [33].

In 2016, the authors were introduced an encryption scheme based on chaos theory. The encryption algorithm utilized two independent chaotic maps, these independent function are very sensitive to initial states. The chaotic function used to verify principle of chaotic encryption (confusion and diffusion). The first chaotic function used for shuffling. The second one is used for altering the values of image [34].

In 2018, a parallel scheme for image ciphering that utilized linear chaotic map (PWLCM) and hyper-chaotic map was proposed. By using novel quantification method two decimal

numbers are founded depending on input image and input external key. They are intended for used as initial states and parameters for linear map and hyper map. The maps control the processes of permutation and diffusion in order to create ciphered image [35].

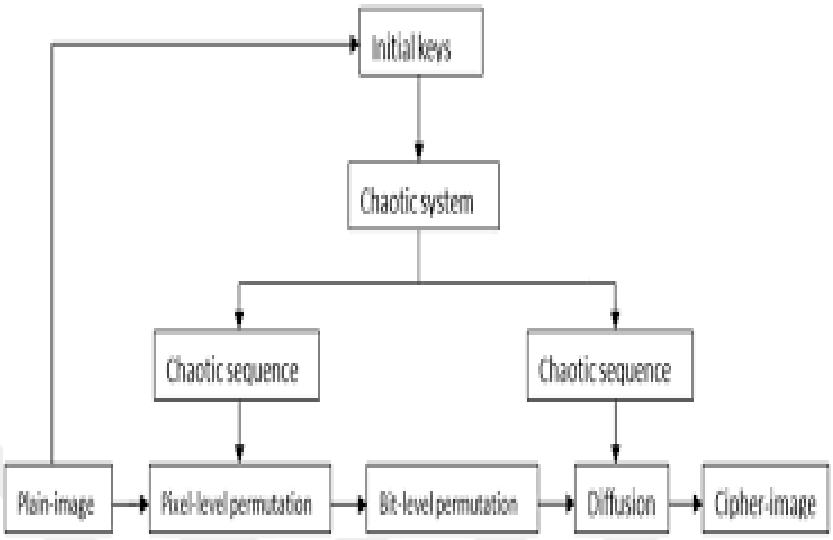


Figure 2.3: An example for chaotic encryption [36].

2.7 HYBRID TECHNIQUES

hybrid technologies for image encryption system that merge the advantages of different cryptography technologies have been proposed.

In 2015, the authors presented encryption algorithm for image protection. The algorithm mainly based on cyclic shift and chaotic system that are employed for the purpose of encryption. The cyclic shift is used in order to produce scrambled image by generating random integer number and the chaotic system is utilized for further process of encryption. Moreover, the initial states of chaotic system are effected by scrambled image. The keys that used in this algorithm are produced by chaotic system [37].

In 2016, a scheme for image ciphering was proposed depending on hyper-chaos theory and DNA techniques. Input image is firstly encoded by DNA substitution and Hyper-image permutation. Both operation intended to eliminate the connection between pixels in the ciphered image and the connection between the bits in individual pixel. The hyper-random sequences used in permutation matrix process and in determining the substitution process [38].

In 2017, an encryption system for image security was produced by combining hyper-chaotic system and DNA technology. Practically, the system encrypts the image by four

steps, first step is intended to create a random sequence (pseudorandom sequence) for the purpose of using in all the steps; second steps, simple diffusion applied for spreading simple change in individual pixel; third step, whole the plain image is encoded by the rules and operation of DNA technology; in last steps, the 2d and 3d permutation will be performed for image [39].

In 2019, an encryption scheme used for protecting the images was presented. The algorithm mainly depending on chaotic map (skew tent map) and cellular automata. The cellular automata mainly used the initial vectors that generated from chaotic map in order to produced random sequence (PRNS). By using random sequences, the input image is permuted to smash the correlation coefficient in adjacent pixels for whole image. The chaotic map is utilized to engender single chaotic number that employed to encrypt the permuted image [40].

3. METHODOLOGY

3.1 MOTIVATION

Along with the fast developing of information transmission in the different networks, a huge number of transmission information are becoming related to confidential secret and personal privacy. Undoubtedly, it is important to preserve the security of transmission. Data encryption is considered as the most important measure to protect data security in the network. The majority of these data are images. Therefore, there is an important need to ensure the image security and preventing an authorized person from accessing. As stated by statistics worldwide, a hacking incident nearly occur every 20 seconds. the loss of over $17 billion in the U.S is resulted by different security incidents every year. The hacking incident of information is significantly increased in last few years [41]. Almost all of famous companies are suffered from a large number of hacking incidents. In this research, two new methods are proposed that combine between image processing technologies and the modern technology of chaotic cryptography.

3.2 DIGITAL IMAGE

Digital image is considered as a representation of the real image like a number of set which is able to be stored through digital computer. The digital image is generally translated into very small areas named pixels. A number of or a set of numbers describe the pixel the properties (color, brightness) of pixels. All of number are usually arranged in arrays of rows and column. There are diverse basic properties for digital images. For instant, binary images can only describe the black and white colors, a color images are described by three colors for the RGB (Red, Green, Blue) system color or four color for CMYK (Cyan, Magenta, Yellow, black) system color [42-43].

3.3 CHAOS THEORY

Chaos theory is one of the most recent theories of physics. It constantly deals with the subjects of nonlinear (dynamic) sentences which constantly exhibit a kind of random (chaotic) behavior, this random (chaotic) behavior is generally occurred in case of inability for determining the initial conditions or it is caused from the physical nature of quantum mechanics. The theory of chaos generally attempts to explore the latent hidden system. Chaos theory is mainly observed by chaotic systems that are extremely sensitive to their initial

conditions. In this apparent randomization that exhibit in many random systems such as weather forecasts, fluid, the solar system, market economy, financial movement, and population growth. chaos theory aims for establishing regular rules for the study of random systems. Over the last few years, chaos theory has been widely invested in the science of cryptography for example, image encryption algorithms, text encryption schemes, ticking functions, random digital generators with high security, watermark images algorithm and stenography algorithms. The majority of these algorithms rely on single-sided random maps. The image encryption algorithms have commonly known as chaos based image encryption. A large part of chaos based image encryption algorithms used symmetric cryptography methods. For chaos based encryption schemes, the parameters and the initial states of chaotic maps are considered as private (secret) keys [44]. The term chaos does not mean no system, but on the contrary it represents a characteristic of the system that seeks to invent a new language of the system, so chaos theory has become scientifically useful not only as a contribution to support the chaotic systems, but it can generate new ideas also. The theory of chaos was born as result of observing weather patterns, and it became very applicable in various application. The benefit from chaos theory include many applications such as geology science, biology, microbiology, mathematics, science of computer, economics, money management, algorithm trading, philosophy, anthropology and physics, population dynamics, psychology, and robotics [45-46].

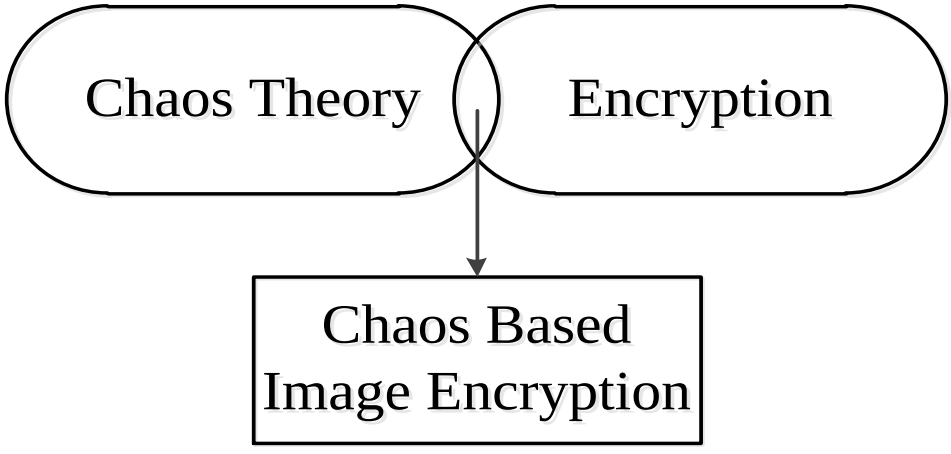


Figure 3.1: Chaos based image encryption illustration.

3.3.1 Chaotic Systems

The chaotic systems are defined as complex systems appear high sensitivity to initial values, like weather and economy. Chaotic system is produced a high level of error in the valid prediction of behavior in system's future [47]. The sensitive nature for initial condition in the chaotic systems is commonly known as *butterfly effect*. The phenomenon of chaos was first observed in model of weather by Lorenz in 1963 [48]. Due to the interesting nonlinear phenomenon, chaotic system is properly studied during the last three decades. Chaotic systems are widely used in several applications like ecological systems, chemical systems, secure communications, physical systems, etc. Chaotic systems are divided into two groups according to Lyapunov exponent (*LE*). Firstly, the systems that exhibit chaos phenomena with one positive Lyapunov exponent (*LE*), these systems are called chaotic system; Secondly, the systems that exhibit chaos with two or more than two Lyapunov exponent (*LE*), these systems are defined as hyper-chaotic systems [49]. The hyper-chaotic systems are robustly sensitive for the value of initial control and their evolution function, due to the deep inherent characteristic of hyper-chaos functions. In other words, it means slight variation in initial parameters leads to enormous variation in value generated through evolution function. Hyper-chaotic is basically characterized as high capacity, high efficiency and high security. Hyper-chaotic systems potentially have broad applications in neural network, nonlinear circuit, laser, biological systems and secure communications. The hyper-chaotic phenomenon observed for the first time by Rössler in 1979 [50].

3.3.2 The Exponent of Lyapunov for Chaos Identification in Systems

The exponent method of Lyapunov is considered as a significant tool for quantifying chaos. Practically, LYAPUNOV EXPONENT (LE) is used for measuring the rates for convergence of nearby trajectories or divergence of nearby trajectories [51]. The negative values of LYAPUNOV EXPONENTS (LE) demonstrate convergence, While the positive values indicate divergence (chaos behavior). In other word, a positive LYAPUNOV EXPONENT (LE) is studied as a definition sign of chaotic behavior. THE LYAPUNOV EXPONENTS (LE) magnitude indicates the time scale in which chaos behavior can be estimated in case of the positive exponent and negative exponent. practically, LYAPUNOV EXPONENTS (LE) are a measurement of how the nearby trajectories can rapidly converge or diverge. For high dimensional systems, one positive number of LYAPUNOV EXPONENT (LE) refers to chaotic while two positive number of LYAPUNOV EXPONENT (LE) refer to hyper-chaotic.

3.3.3 Features of Chaotic Motion

The chaotic system has a very special Characteristics in comparison with other systems (linear and nonlinear systems) [52]. The main Characteristics are

1. The movement of chaotic is limited on a specific region (the chaotic movement is bounded). Which is usually known as the domain of chaotic. This property also known as bounded region for chaotic.
2. Periodicity: it is known that the motion of chaotic is ergodic in the behavior domain in which the chaotic orbit is not settled in specific state point.
3. Randomness; the motion of chaotic is random under specific condition.
4. Sensitivity; chaos sensitivity is simple to notice by using initial states values. Two adjacent initial states will be independent in behavior with the time.

Unpredictability for long-term, due to the initial states condition that are limited in precision, small difference in initial states can lead to huge consequences. For this reason, the prediction.

3.3.4 Performance Evaluation for Chaotic Technique Schemes

The chaotic encryption can be evaluated according to many studies on pseudorandom bit generator by using National Institute of Standards and Technology (NIST) tests. The security, costs and applicability are main evaluation parts that should be considered [53].

1. Security analysis

Firstly, the sensitivity of chaotic systems is significantly high for any minor change in initial values, this property is able to provide a large key space that properly satisfied the requirements of cryptography.

the chaotic sequence is treated as random sequence according to examine of the binary sequence that generated from chaotic equations.

Secondly, the chaotic encryption is considered as a type of stream cipher. Consequently, the attack methods that aim to decipher the ciphered image will not success to discover the secret key due to the unidirectional nature of chaotic systems.

2. Cost analysis

Chaotic cipher has a very short preparing time because of the chaotic encryptions are significantly used XOR operation that carried out each bit of data and have no large number of rounds. the time of chaotic cipher is mostly spent on key generating. In comparison with

other existing methods, chaotic encryption takes very short time. In addition, chaotic cipher has few temporary space during the process of encryption, this because the chaotic ciphers have no S-box and it can produce key stream through cycling.

3. Applicability

The applicability of chaotic encryption is good for both software and hardware. The chaotic algorithm is able to be implemented by C++, MATLAB, JAVA and FPGA.

3.4 XOR CIPHER

XOR operation is widely used in cryptosystem particularly in diffusion steps. XOR process is able to adjust pixel value and smash the connection between neighboring pixels. In other terms, in diffusion stage, plain image pixels are changed in value sequentially by XOR function in order to construct cipher image and for improving its histogram. Ciphered image can be encrypted after applying XOR operation to every pixel using a suggested key. With a view to recover the original image, merely reapplying the XOR operation with the same key. Backward XOR operation means the pixel that XORed with key is re-XORed with the pervious encrypted pixel.

3.5 LIFTING IN LAZY WAVELET

Lifting scheme represents a method for enhancing wavelet properties using so called lifting steps. The lifting scheme use for both designing wavelets and performing the discrete wavelet transform. The implementation of the lifting scheme wavelet is not complicated. Lazy wavelet or polyphase transform is a second generation of Discrete wavelet transform that used to split odd and even samples. The constructions of the Lazy wavelet transform (LWT) derived from spatial domain. It is used for extracting the input signals $x[n]$ into the even and odd polyphase components as in Eq. (3.1) [54-55]. Fig. (3.2) shows the construction of lazy wavelet transform.

$$X1 = x[2n]$$

$$X2 = x[2n+1] \tag{3.1}$$

The representation of z-domain for the even and odd polyphase components is:

$$X1 = \sum_{n} x(2n) z^{-n}$$

$$X2 = \sum_n x(2n+1)z^{-n} \tag{3.2}$$

The z-transform of the input signal as the dilated sum version of z-transform of polyphase component is:

$$X(z) = \sum_n x(2n)z^{-2n} + \sum_n x(2n+1)z^{-2n+1}$$

$$= X1(z^2) + z^{-1}x2(z^2) \tag{3.3}$$

Lazy wavelet transform has some properties that correspond to image encryption system like speed, integer results of wavelet, etc. These properties are very effective with image encryption system. Lazy wavelet introduces faster calculation of wavelet transform and integer results of wavelet as compared with other types of wavelet transform.

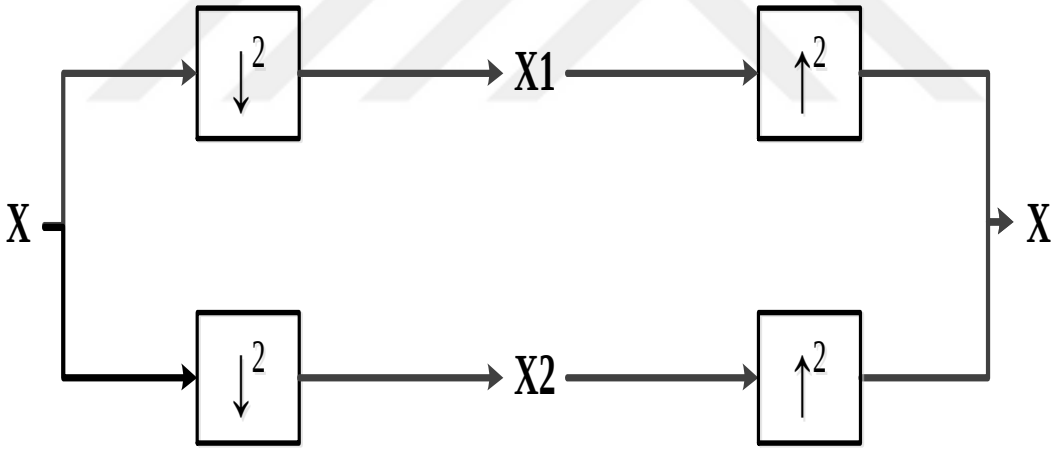


Figure 3.2: The construction of lazy wavelet and inverse lazy wavelet [56].

3.6 MD5

Message Digest Algorithm (MD5) is studied as a type of hash function which is broadly used in encryption algorithm. MD5 generates 128 bits presented as 32 digits of hexadecimal number [57]. As a result of its valuable feature of encryption security, even with slight change is able to lead to big difference between two encrypted image. The initial condition values of the hyper-chaotic systems are produced by MD5. The MD5 can be denoted by Eq. (3.4).

$$x_o = mod(D1 \oplus D2 \oplus D3 \oplus D4), 256/255 \quad (3.4)$$

x_o represents the state condition value of hyper-chaotic system, $D1$, $D2$, $D3$ and $D4$ are values of MD5 extracted from original image. The MD5 value that extracted from original image consist from 128 bits in order to generate $D1$, $D2$, $D3$ and $D4$. For instant, assume the value of MD5 is $q_1 q_2 q_3 \dots \dots q_{126} q_{127} q_{128}$, $D1$ is equal to $q_1 q_2 \dots \dots q_{31} q_{32}$, $D2$ is equal to $q_{33} q_{34} \dots \dots q_{63} q_{64}$, $D3$ is equal to $q_{65} q_{66} \dots \dots q_{95} q_{96}$ and $D4$ is equal to $q_{97} q_{98} \dots \dots q_{127} q_{128}$.

4. SIMULATION MODEL

4.1 PROPOSED ALGORITHM 1

In the first algorithm, an effective permutation-diffusion stages for image cryptosystem is proposed by employing two hyper-chaotic systems and Lagrange polynomial interpolation. These systems are utilized for the purpose of permuting and diffusing the original image pixels by generating all the encryption parameters. Lagrange equation is considered as an auxiliary tool only used to confuse the connection between the input image and the secret keys which are intended for used in the encryption algorithm. Two stages of encryption are used in the proposed encryption algorithm as shown in Figure 4.1: Firstly, the sequences of the two hyper-chaotic systems are correctly merged in order to generate sequences used to permute image pixels by different rule: secondly, the hyper-chaotic sequences are properly applied with a view to generate the modified sequences that especially used for encoding the image pixels with two rounds.

4.1.1 Hyper-Chaotic Systems

Hyper-chaotic systems are robustly sensitive for its own initial control value; this is because its extraordinary evolution functions. In other words, it means a slight variation in the initial parameters leads to enormous variation in value generated through hyper-chaotic function. As a result of the deep inherent characteristic of hyper-chaos functions, hyper-chaotic systems potentially have broad applications in secure communications and image encryption. In the proposed algorithm, two hyper chaotic systems are used. The first hyper chaotic system can be defined in Eq. (4.1) which is modeled by [58].

$$\begin{aligned} \dot{x_1} &= a_1(y_1 - x_1) \\ \dot{y_1} &= b_1 x_1 - x_1 z_1 - c_1 y_1 + w_1 \\ \dot{z_1} &= x_1 z_1 - d_1 z_1 \\ \dot{w_1} &= -k_1 y_1 + r_1 w_1 \end{aligned} \tag{4.1}$$

Where (a_1, b_1, c_1, d_1, k_1, r_1) are control parameters, and (x_1, y_1, z_1, w_1) are state variables. When $a_1 = 12$, $b_1 = 23$, c_1=1 , $d_1 = 2.1$, $k_1 = 6$ and $r_1 = 0.2$, the Eq. (4.1) is considered as hyper-chaotic along with two positive Lyapunov ($LE1 = 0.1740, LE2 = 0.1314, LE3 =$

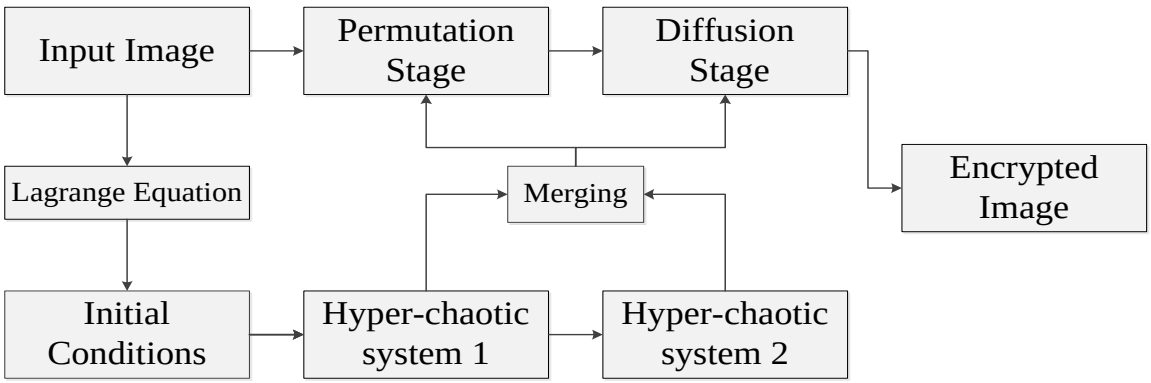


Figure 4.1: Encryption steps of proposed algorithm1.

$0.000, LE4 = -15.6059$). The behavior of Eq. (1) are shown in figures 4.2 (a) and figure 4.2 (b). The second hyper-chaotic system is modeled by [59] and can be described as in Eq. (4.2).

$$\begin{aligned} \dot{x_2} &= a_2(y_2 - x_2) + y_2 z_2 \\ \dot{y_2} &= c_2 x_2 - y_2 - x_2 z_2 + w_2 \\ \dot{z_2} &= x_2 y_2 - b_2 z_2 \\ \dot{w_2} &= -x_2 z_2 + r_2 w_2 \end{aligned} \tag{4.2}$$

Where (a_2, b_2, c_2, r_2) are system parameters, and (x_2, y_2 , z_2, w_2) are state variables. The second system is hyper-chaotic when $a_2 = 35$, b_2 =8/3, c_2=55 and r_2=1.5 and its behavior is shown in figures 4.2.(c) and figure 4.2 (d) . The Eq. (4.2) has two positive Lyapunov ($LE1 =$ $1.4944, LE2 =$ 0.5012 , $LE3$ $0.000, LE4 = -38.9264$).

4.1.2 Permutation Stage

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

In proposed permutation algorithm, the colored input image $V_{M,N,3}^{RGB}$will be separated in to matrices ($V_{M,N}^{R}$, $V_{M,N}^{G}$, $V_{M,N}^{B}$), according to its color component. $V_{M,N}^{R}$ matrix is represent red

color, $V_{M,N}^{G}$matrix is represent green color and $V_{M,N}^{B}$, is represent blue color. M and N indicate the number of rows and columns respectively. The three matrices $V_{M,N}^{R}$, $V_{M,N}^{G}$ and $V_{M,N}^{B}$ are reshaped into one-dimension matrix (vector).

$$V_r = \{r_1, r_2, \dots \dots r_{M \times N}\}$$

$$V_g = \{g_1, g_{2,} \dots \dots g_{M \times N}\} \tag{4.3}$$

$$V_b = \{b_1, b_{2,} \dots \dots b_{M \times N}\}$$

where r_i, g_i and b_i denote pixel index value of image color (Red, Green, Blue) components between 0-255 receptively. The eight hyper-chaotic sequences $(\dot{x_1}, \dot{y_1}, \dot{z_1}, \dot{w_1}, \dot{x_2}, \dot{y_2}, \dot{z_2}, \dot{w_2})$ can be generated by repeating Eq. (4.1) and Eq,(4.2) $(M \times N)/2$ times. The values of initial condition for hyper-chaotic systems will be chosen according to following equations.

$$V_{sum} = sum(V_{M,N,3}) \tag{4.4}$$

$$P(\breve{x}) = \sum_{j=1}^{2} \breve{y}_j \, L_{n,j} \tag{4.5}$$

$$L_{n,j}(\breve{x}) = \prod_{\substack{k=1 \\ k \neq j}}^{2} \frac{V_{sum} - \breve{x}_k}{\breve{x}_j - \breve{x}_k} \tag{4.6}$$

Where $\breve{x}$ and $\breve{y}$ are random values. In order to generate robust hybrid sequence. The hyper-chaotic sequences are combined as in the following equations.

$$x(1{:}\,2{:}\,M \times N) = x_1$$

$$x(2{:}\,2{:}\,M \times N) = x_2 \tag{4.7}$$

$$y(1{:}\,2{:}\,M \times N) = y_1$$

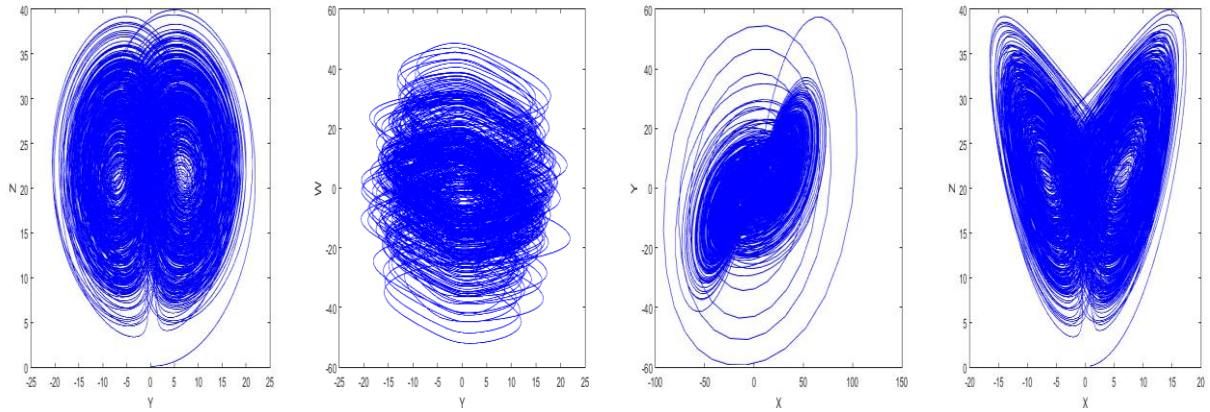
$$y(2{:}\,2{:}\,M \times N) = y_2 \tag{4.8}$$

$$z(1{:}\,2{:}\,M \times N) = z_1$$

$$z(2{:}\,2{:}\,M \times N) = z_2 \tag{4.9}$$

$$w(1{:}\,2{:}\,M \times N) = w_1$$

$$w(2{:}\,2{:}\,M \times N) = w_2 \tag{4.10}$$



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

Figure 4.2: Hyper-chaotic attractors of algorithm 1, (a) y-z plane of system1, y-w plane of system1, (d) x-y plane of system2, (d) x-z plane of system 2.

The sequences which are produced from hyper-chaotic systems are sorted in ascend way as in Eq. (4.11):

$$\begin{aligned} [F_1, L_1] &= sort\ (x_1 - w_1) \\ [F_2, L_2] &= sort\ (y_1 - w_1) \\ [F_3, L_3] &= sort\ (z_1 + w_1) \end{aligned} \tag{4.11}$$

L_1, L_2 and L_3 are new sequences after sorted. F_1, F_2, and F_3 represent index value of L_1, L_2 and L_3 respectively. Permute the pixels of image according to Eq. (4.12) by selecting the index of sorted sequences.

$$\begin{aligned} PE_R(i) &= P_R\ (F_1(i)) \\ PE_G(i) &= P_G\ \big(F_2(i)\big) \\ PE_B(i) &= P_B\ (F_3(i)) \\ i &= 1,2, \dots M \times N \end{aligned} \tag{4.12}$$

4.1.3 Diffusion Stage

In diffusion stage, plain image pixels are changed in value sequentially by XOR function in order to construct cipher image and for improving its histogram by two rounds. Ciphered image can be encrypted after applying XOR operation to every pixel using a suggested key.

4.1.3.1 First round

In first round of diffusion stage, the hyper-chaotic sequences are specifically modified according to Eq. (4.13) For more efficacious security.

$$\begin{aligned} X_x(i) &= mod(floor(x(i)) \times N1)\,, W1) \\ Y_y(i) &= mod(floor(y(i))\ \times N2)\,, W1) \\ Z_z(i) &= mod(floor(z(i))\ \times N3\ ), W1) \\ W_w^1(i) &= mod(floor(w(i)\ \times N4)\,, N\ \times\ M) \end{aligned} \tag{4.13}$$

Where i is 1,2,……$M \times N$, $N1, N2$ and $N3$ are large numbers (greater than 1000). $W1$ should be within 256. XOR operation will be applied between the permuted vectors and with the modified sequences as in Eq. (4.14). Where $\oplus$ denotes XOR operation.

$$\begin{aligned} PP_r^1(i) &= PE_R(i) \oplus X_x(W_w^1(i)) \\ PP_g^1(i) &= PE_G(i) \oplus Y_y(W_w^1(i)) \\ PP_b^1\ (i) &= PE_B(i) \oplus Z_z(W_w^1(i)) \end{aligned} \tag{4.14}$$

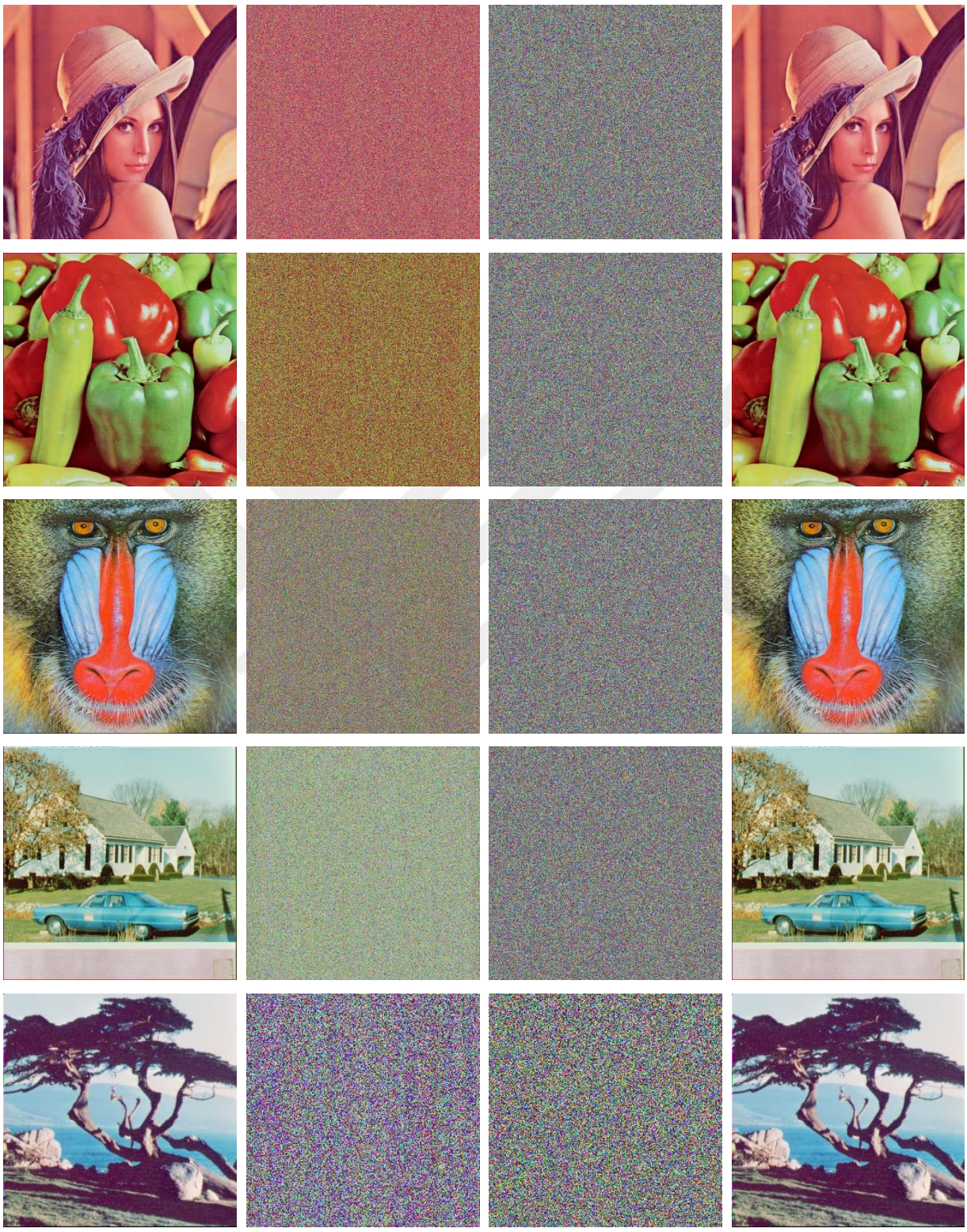
4.1.3.2 Second round

with the aim of increasing the security level of proposed algorithm, we will use more than one round in diffusion stage. The value of $W_w^2$is generated according to Eq. (4.15).

$$W_w^2(i) = mod(floor((w_2(i) + 128) \times N5\ ), N\ \times\ M) + 1 \tag{4.15}$$

It is obvious, that the XOR operations for second round are modified as in Eq. (4.16). Then convert the vectors (PP_r^2, PP_g^2, PP_b^2) into the 2-diminsional matrices ($EV_{M,N}^R$, $EV_{M,N}^G$., $EV_{M,N}^B$). Eventually, the matrices are merged in order to produce the final encrypted image $EV_{M,N,3}$. Decryption steps are similar to encryption steps but in reverse order. The results that related to encrypted and decrypted images are shown in figure 4.3.

$$\begin{aligned} PP_r^2\ (i) &= PP_r^1(i) \oplus\ X_x(W_w^2(i)) \\ PP_g^2(i) &= PP_g^1\ (i) \oplus Y_y(W_w^2(i)) \\ PP_b^2\ (i) &= PP_b^1(i) \oplus Z_z(W_w^2(i)) \end{aligned} \tag{4.16}$$



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

Figure 4.3: Encrypted and decrypted image for proposed algorithm 1 (a) plain images, (b) permuted images, (c) encrypted images, (d) decrypted images.

4.2 PROPOSED ALGORITHM 2

In this algorithm, an enhanced permutation-diffusion for encryption system was produced depend on combination of two hyper-chaotic systems in order to produce hybrid sequences with lazy wavelet and MD5. Two chaotic systems expand merits of massive key space and provide high level of security. While lazy wavelet provides high scale of complexity in order to produce efficient image encryption system. This proposed system consists from permutation and diffusion stages as shown in figure 4.4. In permutation stage, the position of pixels in original image is shuffled by key sequence that created by hybrid sequences. In diffusion stage, the value of pixels is modified by employing backward XOR after lazy wavelet takes place. The MD5 is used extracting bits from original image in order to use in the initial condition value of the hyper-chaotic-systems. The prime contribution in this algorithm is the application of combined hyper chaotic systems and performing lazy wavelet with diffusion stage to present solid key space and sufficient complexity.

4.2.1 Hyper-Chaotic Systems

In our proposed encryption algorithm 2, two hyper chaotic sequences are used that produced from useful hyper-chaotic systems. A first system can be described as in Eq (4.17) which is modeled by [60].

$$\begin{aligned} \dot{x_1} &= a_1(y_1 - x_1) \\ \dot{y_1} &= c_1 x_1 - y_1 - x_1 z_1 + w_1 - d_1 \\ \dot{z}_1 &= -b_1 z_1 + x_1 y_1 \\ \dot{w_1} &= m_1 y_1 + w_1 - n_1 {x_1}^3 \end{aligned} \tag{4.17}$$

In Eq. (2), a, b, c, d, m and n are the system parameters and x, y, z, w are state variables. When a = 10, b = 2, c = 28, d = 0.1, m = 27, n = 0.5 and the initial condition x (0) = 1, y (0) = 0, z (0) = 0, w (0) = 0, the first system is hyper chaotic and has two positive Lyapunov $LE1$ =0.5602, $LE2$ =0.0445, $LE3$ =0, $LE4$ =−12.6016. Attractors of system (2) are shown in Figure 4.5 (a) and figure 4.5 (b). Second system can be defined as in Eq. (4.18) modeled by [61].

$$\begin{aligned} \dot{x_2} &= a_2(y_2 - x_2) \\ \dot{y_2} &= c_2 y_2 - x_2 z_2 + w_2 \\ \dot{z_2} &= -b_2 z_2 + x_2 y_2 \end{aligned} \tag{4.18}$$

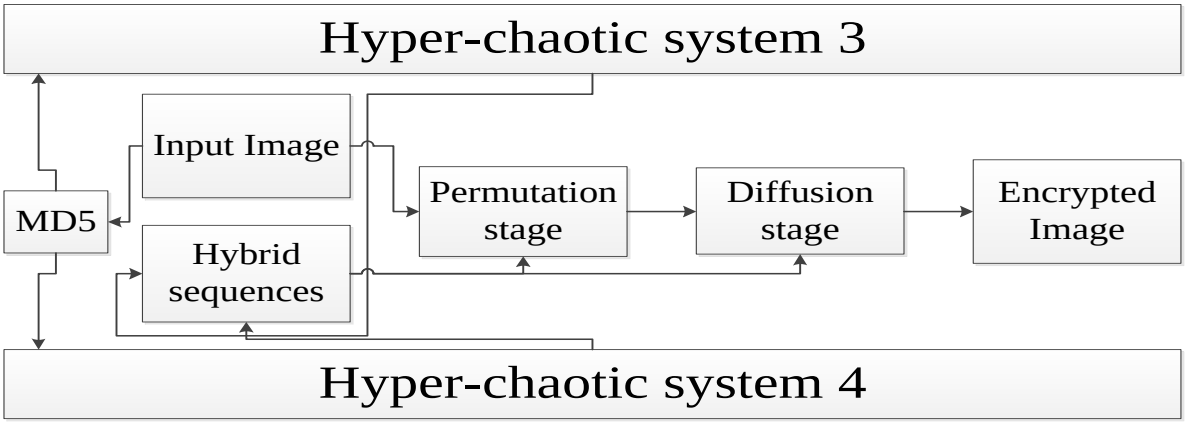


Figure 4.4: Encryption steps of proposed 2.

$\dot{w}_2 = -k_2 x - k k_2 y$

In Eq. (1), a, b, c, $k1$ and $k2$ are the system parameters and x, y, z, w are state variables. When a = 30, b = 3, c = 20, $k1$ = 2, $k2$ = 2 and the initial condition x (0) = 1, y (0) = 0, z (0) = 0, w (0) = 0, the second system is hyper chaotic and has two positive Lyapunov $LE1$ =1.4106, $LE2$ =0.1232, $LE3$ =0, $LE4$ =−20.5339. Chaotic attractors of the second system are shown in figure 4.5 (c) and figure 4.5 (d) The values of initial condition for hyper chaotic systems will be chosen according to MD5 algorithm as in following equations.

$$MD5 = mod(D1 \oplus D2 \oplus D3 \oplus D4), 256/255 \quad (4.19)$$

Where $D1, D2, D3\ and\ D4$ are bits extracted from original image.

4.2.2 Generating Hybrid Hyper-Chaotic Sequences

In order to increase the sensitivity, key space (i.e. by having more state variables and parameters), system complexity, encryption system resistance and security, the sequences that produced from Eq. (4.17) are merge with the sequences that produced from Eq. (4.18) to produce a new hybrid hyper-chaotic sequences as described in the following:

$$A = \sin(x_1) + k_2 \quad (4.20)$$

$$B = \cos(x_1) + c_2 \quad (4.21)$$

$$C = \text{abslote}\ (\sin(z_2)) + b_1 \quad (4.22)$$

$$D = \text{abslote}\ (\cos(z_2)) + a_1 \quad (4.23)$$

$$\dot{x_1}(i) = D(i-1)(y_1(i) - x_1(i))$$

$$\dot{y_1}(i) = c_1 x_1(i) - y_1(i) - x_1(i) z_1(i) + w_1(i) - d_1(i)$$

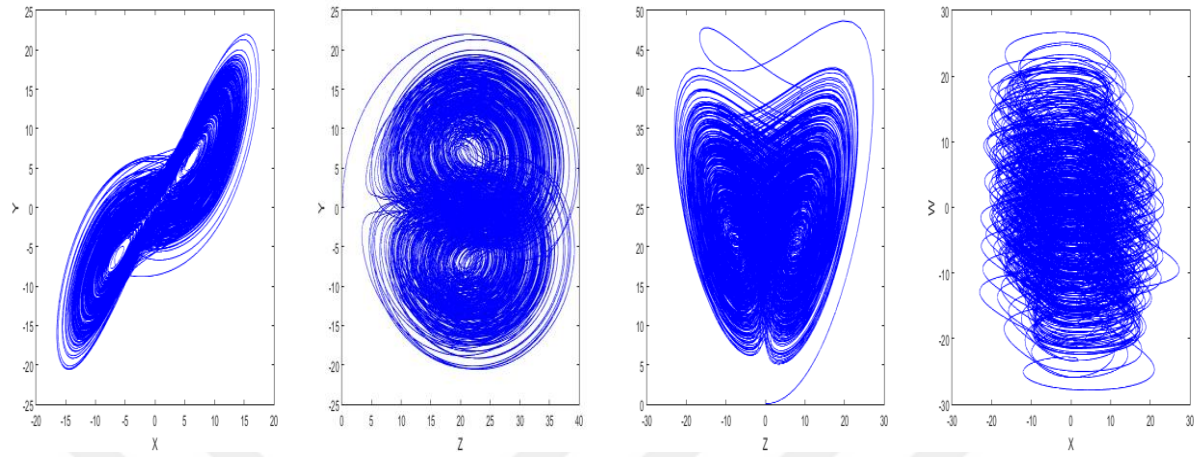


Figure 4.5: Hyper-chaotic attractors of algorthm1, (a) x-y plane of system3, x-z plane of first system, (d) x-z plane of system4, (d) x-w plane of system 4.

$$\begin{aligned}
\dot{z}_1(i) &= -C(i-1)z_1(i) + x_1(i)y_1(i) \\
\dot{w_1}(i) &= m_1 y_1(i) + w_1(i) - n_1 {x_1}^3(i) \\
\dot{x_2}(i) &= a_2(y_2(i) - x_2(i)) \\
\dot{y_2}(i) &= A(i-1)y_2(i) - x_2(i)z_2(i) + w_2(i) \\
\dot{z_2}(i) &= -b_2 z_2(i) + x_2(i)y_2(i) \\
\dot{w_2}(i) &= -B(i-1)x(i) - kk_2 y(i)
\end{aligned} \tag{4.24}$$

Where i =2……,$M \times N/2$. These sequence are modified in order to be appropriate for permutation and diffusion stages as in the following equations.

$$\begin{aligned}
X_x^1(i) &= mod(floor(x_1(i) \times N1), W1) \\
Y_y^1(i) &= mod(floor(y_1(i) \times N2), W1) \\
Z_z^1(i) &= mod(floor(z_1(i) \times N3), W1) \\
W_w^1(i) &= mod(floor(w_1(i) \times N4), (N \times M)/2) \\
X_x^2(i) &= mod(floor(x_2(i) \times N5), W1) \\
Y_y^2(i) &= mod(floor(y_2(i) \times N6), W1) \\
Z_z^2(i) &= mod(floor(z_1(i) \times N7), W1) \\
W_w^2(i) &= mod(floor(w_2(i) \times N8), (N \times M)/2)
\end{aligned} \tag{4.25, 4.26}$$

where$N1, N2, N3, N4, N5, N6, N7$ and $N8$ are large numbers (greater than 1000). $W1$ and $W2$ should be within 256.

4.2.3 Permutation Stages

In order to permute image pixels, a new approach used to shuffle rows and columns separately. The permutation used in proposed algorithm 2 is considered as modified version of the permutation that used in []. For row shuffle, we select a hybrid sequence generated from hyper-chaotic systems. The rows will be shuffled to up if the hybrid sequence is even and will be rotated down if the hyper-chaotic sequence is odd. This shuffle makes all rows move in different directions and different distances. Column permutation is basically similar to row permutation, the column will be shuffled to the right or left according to hybrid sequence that produced from chaotic and hyper-chaotic systems. The columns also will be shuffled into different directions and distances. The permutation process is an auxiliary process used for confusing the relationship between pixels for the purpose of reducing correlation between pixels.

The color input image $V^{rgb}\ (M, N, 3)$ is separated into 3 matrices (Red, Green, Blue). $V^{r}\ (M, N)$ represents red color, $V^{g}(M, N)$ represents green color and $V^{b}\ (M, N)$ represents blue color, where M denotes to the number of rows and N denotes to the number of columns of the image size. The permutation hybrid sequences that used for permutation stage will be generated according to the following Equations.

$$P_r(i) = X_x^1(Z_z^1(i) + Y_y^2(i)) \tag{4.27}$$

$$P_c(i) = Y_y^1(Z_z^1(i) + Z_z^2(i)) \tag{4.28}$$

The rows are permuted according to P_r. If the value of $P_r(i)$ is even, the rows of each color channel will be permuted according to Eq. (4.29). If the value of $P_r(i)$ is odd, the rows of each color channel will be permuted according to Eq. (4.30).

$$\begin{cases} VP_R^r(i,j) = V^r\big(i, j + P_r(i)\big) & if\ \ j + P_r(i) \le M \\ VP_R^r(i,j) = V^r(i, j + P_r(i) - N) & if\ \ j + P_r(i) > M \end{cases}$$
$$\begin{cases} VP_R^g(i,j) = V^g\big(i, j + P_r(i)\big) & if\ \ j + P_r(i) \le M \\ VP_R^g(i,j) = V^g(i, j + P_r(i) - N) & if\ \ j + P_r(i) > M \end{cases} \tag{4.29}$$
$$\begin{cases} VP_R^b(i,j) = V^b\big(i, j + P_r(i)\big) & if\ \ j + P_r(i) \le M \\ VP_R^b(i,j) = V^b(i, j + P_r(i) - N) & if\ \ j + P_r(i) > M \end{cases}$$

$$\begin{cases} VP_R^r(i) = V^R\big(i, j - P_r(i)\big) & if\ \ j - P_r(i) \ge 1 \\ VP_R^r(i) = V^R(i, j - P_r(i) + N) & if\ \ j + P_r(i) < 1 \end{cases}$$

$$\begin{cases} VP_R^g(i) = V^G\big(i, j - P_r(i)\big) & if\ \ j - P_r(i) \geq 1 \\ VP_R^g(i) = V^G(i, j - P_r(i) + N) & if\ \ j + P_r(i) < 1 \end{cases}$$
$$\begin{cases} VP_R^b(i) = V^B\big(i, j - P_r(i)\big) & if\ \ j - P_r(i) \geq 1 \\ VP_R^b(i) = V^B(i, j - P_r(i) + N) & if\ \ j + P_r(i) < 1 \end{cases} \quad (4.30)$$

Depending on the value of P_c, the rows of each channel color will be permuted, the Equations (4.31) are used if the value of $P_c$is even. If the value of $P_c$is odd, the columns will be permuted according to Equations (4.32).

$$\begin{cases} VP_C^r(i,j) = VP_R^r(i - P_c(i), j) & if\ \ i - P_r(i) \geq 1 \\ VP_C^r(i,j) = VP_R^r(N + i - P_c(i), j) & if\ \ i - P_r(i) < 1 \end{cases}$$
$$\begin{cases} VP_C^g(i,j) = VP_R^g(i - P_c(i), j) & if\ \ i - P_r(i) \geq 1 \\ VP_C^g(i,j) = VP_R^r(N + i - P_c(i), j) & if\ \ i - P_r(i) < 1 \end{cases} \quad (4.31)$$
$$\begin{cases} VP_C^b(i,j) = VP_R^b(i - P_c(i), j) & if\ \ i - P_r(i) \geq 1 \\ VP_C^b(i,j) = VP_R^b(N + i - P_c(i), j) & if\ \ i - P_r(i) < 1 \end{cases}$$

$$\begin{cases} VP_C^r(i,j) = VP_R^r\big(i, j - P_c(i)\big) & if\ \ i + P_c(i) \leq N \\ VP_C^r(i,j) = VP_R^r(i, j + P_c(i) - N) & if\ \ j + P_c(i) > N \end{cases}$$
$$\begin{cases} VP_C^g(i,j) = VP_R^g\big(i, j - P_c(i)\big) & if\ \ i + P_c(i) \leq N \\ VP_C^g(i,j) = VP_R^g(i, j + P_c(i) - N) & if\ \ j + P_c(i) > N \end{cases} \quad (4.32)$$
$$\begin{cases} VP_C^b(i,j) = VP_R^b\big(i, j - P_c(i)\big) & if\ \ i + P_c(i) \leq N \\ VP_C^b(i,j) = VP_R^b(i, j + P_c(i) - N) & if\ \ j + P_c(i) > N \end{cases}$$

4.2.4 Diffusion Stage

The three matrices P_R, P_G and P_B are reshaped into one-dimension matrix (vector).

$$\begin{aligned} VP_C^r &= \{r_1, r_2, \dots \dots r_{M \times N}\} \\ VP_C^g &= \{g_1, g_{2,} \dots \dots g_{M \times N}\} \\ VP_C^b &= \{b_1, b_{2,} \dots \dots b_{M \times N}\} \end{aligned} \quad (4.33)$$

where r_i, g_i and b_i denote pixel index value of image color (red, green, blue) components between 0-255 receptively. Apply LWT for each permuted vector (PE_R, PE_G, PE_B). Each vector will produce two vectors (PE_R^{even} , PE_R^{odd}), (PE_G^{even} , PE_G^{odd}) and (PE_B^{even} , PE_B^{odd}) as shown in

Eq. (4.32) below. XOR operation will be applied between the vectors produced from applying LWT and with the modified hyper-chaotic sequences as in the following equations.

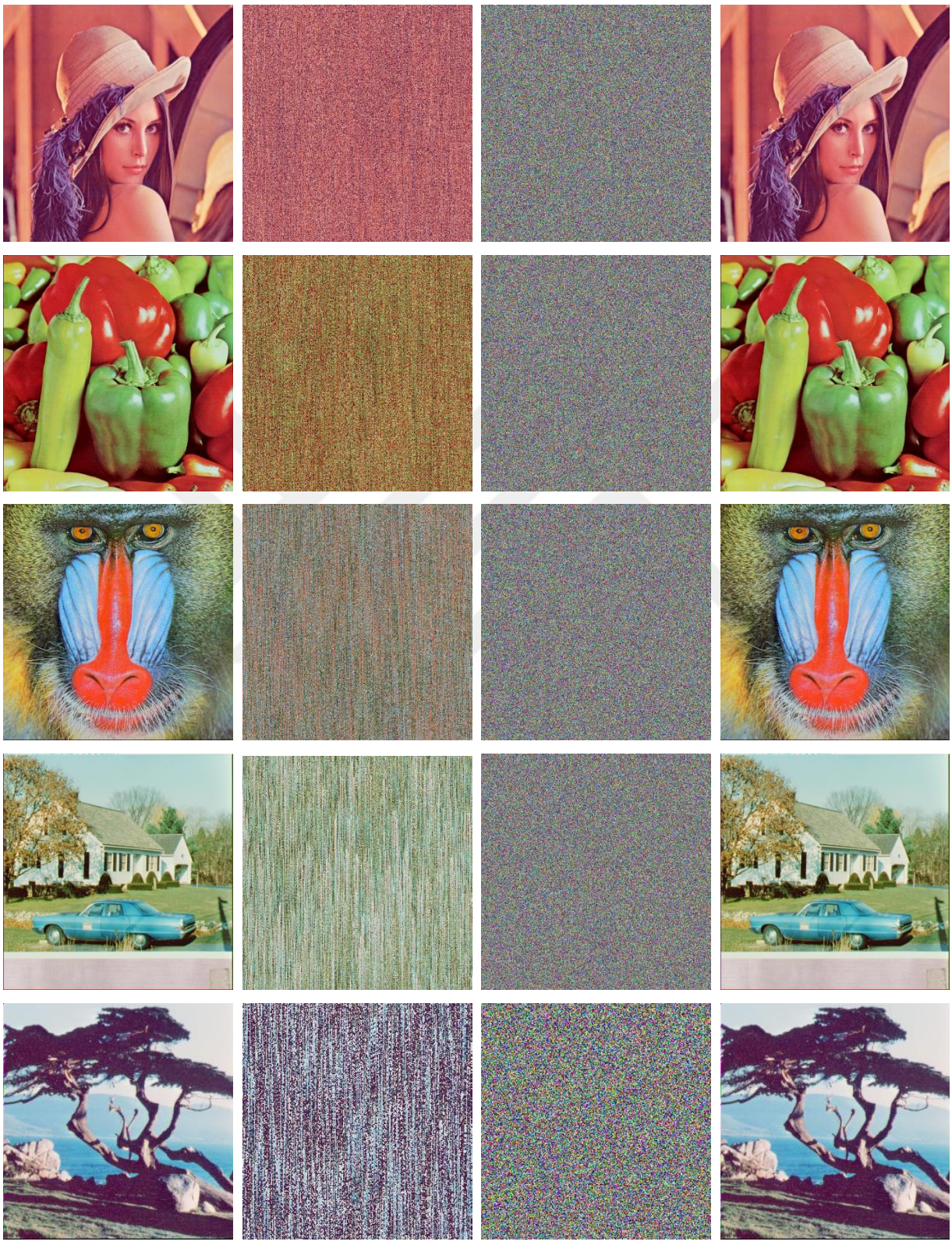
$$\begin{aligned} VP_C^r &\dashrightarrow [PE_R^{even}(j), PE_R^{odd}(j)] \\ VP_C^g &\dashrightarrow [PE_G^{even}(j), PE_G^{odd}(j)] \\ VP_C^b &\dashrightarrow \left[PE_B^{even}(j), PE_B^{odd}(j)\right] \\ j &= 1,2,\dots\dots(M \times N)/2 \end{aligned} \tag{4.34}$$

$$\begin{aligned} PP_R^{even}(1) &= PE_R^{even}(1) \oplus x_x^1(1) \\ PP_G^{even}(1) &= PE_G^{even}(1) \oplus x_x^1(1) \\ PP_B^{even}(1) &= PE_B^{even}(1) \oplus x_x^1(1) \\ PP_R^{odd}(1) &= PE_R^{odd}(1) \oplus Y_y^1(1) \\ PP_G^{odd}(1) &= PE_G^{odd}(1) \oplus Y_y^1(1) \\ PP_B^{odd}(1) &= PE_B^{odd}(1) \oplus Y_y^1(1) \end{aligned} \tag{4.35}$$

$$\begin{aligned} PP_R^{even}(j) &= PE_R^{even}(j) \oplus x_x^1(j) \oplus PP_R^{even}(j-1) \\ PP_G^{even}(j) &= PE_G^{even}(j) \oplus x_x^1(j) \oplus PP_G^{even}(j-1) \\ PP_B^{even}(j) &= PE_B^{even}(j) \oplus x_x^1(j) \oplus PP_B^{even}(j-1) \\ PP_R^{odd}(j) &= PE_R^{odd}(j) \oplus Y_y^1(j) \oplus PP_R^{odd}(j-1) \\ PP_G^{odd}(j) &= PE_G^{odd}(j) \oplus Y_y^1(j) \oplus PP_G^{odd}(j-1) \\ PP_B^{odd}(j) &= PE_B^{odd}(j) \oplus Y_y^1(j) \oplus PP_B^{odd}(j-1) \end{aligned} \tag{4.36}$$

where $j = 2,3,\dots\dots(M \times N)/2$ and $\oplus$ denotes XOR operation. If inverse LWT is applied as in Eq. (4.37), three vectors will be produced (LL_R, LL_G, LL_B). Then, convert vectors to matrix of 2-dimension. Finally Combine the image colors to get the final encrypted image $V(M, N, 3)$ the encrypted images are shown in Fig. 4. Decryption steps must be done in a similar way to that of encryption steps but in reverse way.

$$\begin{aligned} \left[PP_R^{even}(j), PP_R^{odd}(j)\right] &\dashrightarrow V_R \\ \left[PP_G^{even}(j), PP_G^{odd}(j)\right] &\dashrightarrow V_G \\ \left[PP_B^{even}(j), PP_B^{odd}(j)\right] &\dashrightarrow V_B \end{aligned} \tag{4.37}$$



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

Figure 4.6: Encrypted and decrypted image for proposed algorithm 2 (a) plain images, (b) permuted images, (c) encrypted images, (d) decrypted image.

5. ANALYSIS OF RESULTS AND DISCUSSION

The image encryption algorithms are basically implemented by using MATLAB 8.5.0 (R2015a). The lena image is selected from database provided by Fabien a. p. petitcola (https://homepages.cae.wisc.edu/~ece533/images/). The selected lena image is stored in PNG format. All the rest of images have been chosen from USC-SIPI database (http://sipi.usc.edu/database/). The selected images have been stored in the format of TIFF.

5.1 ANALYSIS OF KEY SPACE

Key space interprets entire number of the keys probability for the image encryption system. Resistant key should be large enough to prohibit brute-force attacks [62]. In proposed algorithm, the secret key is the initial value of the two systems. Therefore, the number of secret keys for proposed algorithm 1 is 18 (a_1, b_1, c_1, d_1, k_1, r_1, a_2, b_2, c_2, r_2, x_1, y_1 , z_1, w_1, x_2, y_2 , z_2, w_2) and if their precision is 10^{-14}, key space is $=10^{18^{14}} = 10^{252}$. The number of secret keys for proposed algorithm 2 is 19 (a_1, b_1, c_1, d_1, m_1, $n_1, a_2, b_2, c, k1, kk_2, x_1$, y_1, z_1, w_1, x_2, y_2, z_2, w_2). So, the key space is $=10^{18^{14}} = 10^{266}$. The key space that used in both algorithms is sufficiently large to endure exhausted attack as compared with existing system.

5.2 HISTOGRAM

Histogram analysis has been performed to confirm the enhanced method for encrypted image and plain image. A histogram illustrates the distribution of image pixel values [63]. For ideal image encryption algorithm, the encrypted image histogram should be sufficiently uniform to resist statistical attack. Figure 5.1 shows the histograms for plain and encrypted images for both algorithms. Figure 5.1 indicates that the histograms are completely uniform for the encrypted image for both algorithms. The equation employed to check the histogram uniformity is described by Chi-square test as:

$$x^2 = \sum_{i=1}^{256} \frac{(v_i - 256)^2}{256} \tag{5.1}$$

i represents gray level number, v_i indicates the occurrence frequencies of gray level. Low values refer to accurate uniformity. The Chi-square test values for original and encrypted image are tabulated in table 5.1 and table 5.2.

5.3 CORRELATION OF ADJACENT IMAGE PIXELS

Due to the very strong correlation between adjacent pixels in images, an efficient image encryption system should evict the correlation in ciphered image. A typical system should produce low correlation between adjacent encrypted image pixels. The following equation is used for studying the correlation for adjacent pixels in horizontal, vertical and diagonal direction.

$$E(x) = \frac{1}{N}\sum_{i-1}^{N} x_i$$

$$(x) = \frac{1}{N}\sum_{i-1}^{N}\left(x_i - E(x)\right)^2$$

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

$$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \tag{5.2}$$

Where x and y represent values of two adjacent image pixels and N is the number of adjacent image pixels which is selected to evaluate the correlation. Figure 5.2 (a), (b) and (c) shows the correlation coefficients of adjacent pixels for horizontal, vertical and diagonal direction of the original image. Figure 5.2 (d), (e) and (f) illustrates the correlation of adjacent pixels for horizontal, vertical and diagonal direction of ciphered image that produced from proposed algorithm 1. Figure 5.2 (g), (h) and (i) illustrates the correlation of adjacent pixels for horizontal, vertical and diagonal direction of ciphered image that produced from proposed algorithm 2. After using the two hyper chaotic systems for permutation, the correlation coefficient minimizes and the relations between encrypted image pixels are difficult to predict. Proposed scheme reduces the correlation coefficient and statistical attacks is prevented due to reduction validation of proposed scheme to correlation coefficient. Table 5.3 reveals correlation coefficients for plane images and their ciphered images. Table 5.3 results indicate that proposed scheme reaches littlest

correlation coefficients in different directions and the resistance ability of statistical attack is robust [64].

5.4 INFORMATION ENTROPY

The information entropy is a measurement of distribution image pixels. Information entropy is deemed to be most predominate criterions of randomness. Information entropy can be described as:

$$H(s) = \sum_{i=0}^{2^M-1} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{5.3}$$

Where $P(s_i)$ is the probability of the symbol s_i and 2^M represents the total number of states in information source. Ideal information entropy should be $H(s)$ = 8. Therefore, efficient entropy value should be close to 8 to indicates the effectiveness of encryption system. In our two proposed system, the hybrid hyper-chaotic sequence which introduced by two hyper chaotic systems is employed for higher randomized encryption. The values of entropy are shown in fourth column of table 5.4 and table 5.5 [65].

5.5 MEAN SQUARE ERROR, PEAK SIGNAL TO NOISE RATIO AND CORRELATION BETWEEN ORIGINAL AND ENCRYPTED IMAGE

Mean square error (MSE), peak signal to noise ratio ($PSNR$) and correlation (CC) are employed for evaluating proposed algorithms reliability . MSE is measured by using the following equation.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \big(a(i,j) - b(i,j)\big)^2 \tag{5.4}$$

Where M and N refer to the size of the image, while $a(i,j)$ and $b(i,j)$ represent pixels location for original and encrypted image, respectively. *MSE* should be large for strong secure scheme [66]. The values are reported in second column of table 5.4 and table 5.5. $PSNR$ can be described by:

$$PSNR = 10 \log_{10} \frac{I_{max}^2}{MSE} \tag{5.5}$$

I_{max}refers to maximum image pixel value. The lowest $PSNR$ interprets the major variance between encrypted image and its original. $PSNR$ values are tabulated in third column of table

5.4 and table 5.5. Correlations coefficient (CC) is analyzed for variant original/cipher images by performing 2D CC for plain image and its correspond encrypted image [67]. The CC can be calculated as in the following equation:

$$CC = \sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij} - \bar{A})(B_{ij} - \bar{B}) \Big/ \sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij} - \bar{A})^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij} - \bar{B})^2\right)} \qquad (5.6)$$

here, A and B indicates the original image and the cipher-image respectively, while $\bar{A}$ and $\bar{B}$ denote to mean values of the matrix's elements for A and B, respectively. M and N represent the height and width of the image, respectively. CC values are shown in the fifth column of table 5.4 and table 5.5. As a consequence, the calculated CC is nearly equal to 0 for both algorithm. The original image and encrypted image are unquestionably different.

5.6 DIFFERENTIAL ATTACK

5.6.1 Plain Text Sensitivity

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are widely used for the purpose of evaluation the robustness of encryption systems in term of differential attacks [68]. NPCR is generally used to calculate the percentage of the difference in number of pixels for two ciphered images and UACI used to calculate average intensity between two ciphered images as in Eq. (5.7) and Eq. (5.8). In other word, change in one pixel in the original image leads to enormous change in encrypted image [69]. high NPCR and UACI score illustrate the reliability of encryption systems to resist differential attacks. The results test is listed in table 5.4 and table 5.5.

$$D(i,j) = \begin{cases} 1, & c_1(i,j) = c_2(i,j) \\ 0, & c_1(i,j) \neq c_2(i,j) \end{cases}$$

$$NPCR = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100\% \qquad (5.7)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\% \qquad (5.8)$$

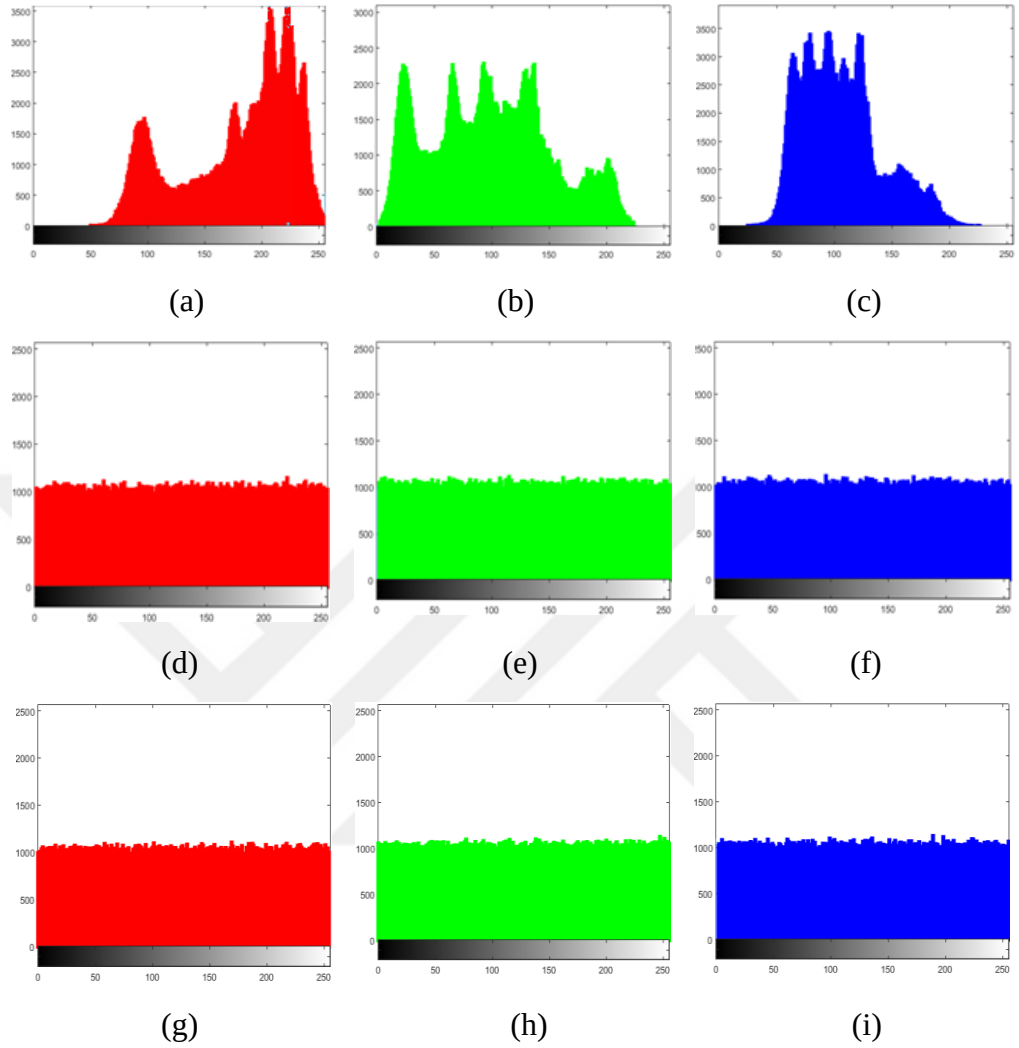


Figure 5.1: Histograms for the plain image and its encrypted: (a), (b), (c) histograms that related to original image for each color, (d), (e), (f) histograms that related to encrypted image of proposed algorithm1 for each color, (g), (h), (i) histograms that related to encrypted image of proposed algorithm2 for each color.

Table 5.1: Chi-square test for proposed algorithm 1.

Image	Original image			Encrypted image		
	R	G	B	R	G	B
Lena	252093	120279	346358	224.048	232.085	250.972
Peppers	213187	318382	491428	282.175	243.548	232.199
Baboon	82839.7	142808	79942.6	265.982	249.753	252.302
House	192029	332540	248006	261.078	247.560	232.384

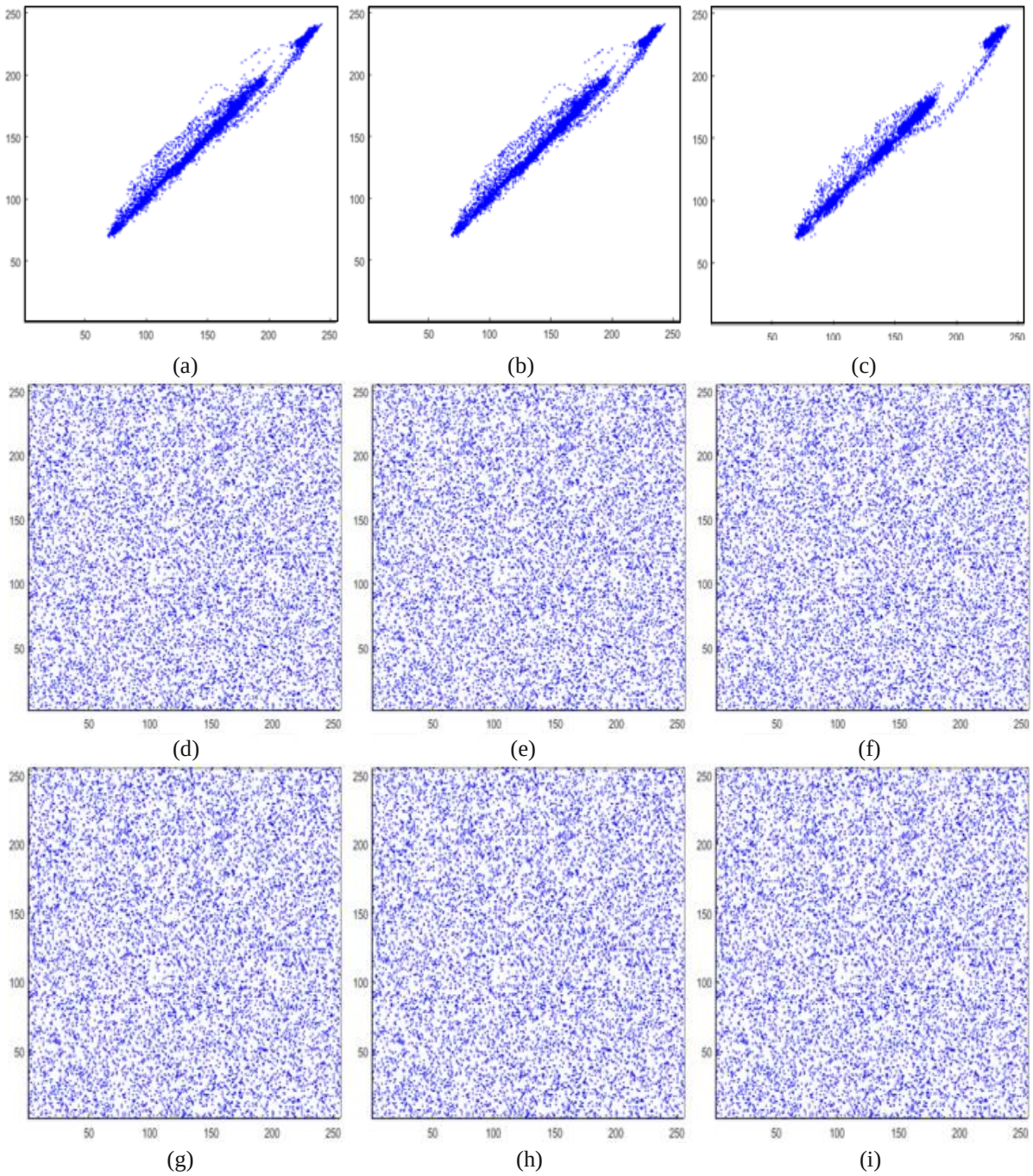


Figure 5.2: Correlarion coefficient of adjecent pixels: (a) correlarion for horizental pixels (plain image), (b) correlarion for vertical pixels (plain image) , (c) correlarion for diagonal pixels (plain image) , (d) correlarion for horizental pixels (encrypted image of proposed algorithm 1), (e) correlarion for vertical pixels (encrypted image of proposed algorithm 1), (f) correlarion for diagonal pixels (encrypted image of proposed algorithm 1), , (g) correlarion for horizental pixels (encrypted image of proposed algorithm 2), (h) correlarion for vertical pixels (encrypted image of proposed algorithm 2), (i) correlarion for diagonal pixels (encrypted image of proposed algorithm 2).

Table 5.2: Chi-square test for proposed algorithm 2.

Image	Original image			Encrypted image		
	R	G	B	R	G	B
Lena	252093	120279	346358	226.509	256.404	257.058
Peppers	213187	318382	491428	305.900	257.306	233.810
Baboon	82839.7	142808	79942.6	264.562	247.244	270.459
House	192029	332540	248006	278.244	270.304	251.709

Table 5.3: Correlation of adjacent pixels for proposed algorithm 1 and 2.

Image	Original image			Encrypted image of algorithm 1			Encrypted image of algorithm 2		
	H	V	D	H	V	D	H	V	D
Lena	0.97734	0.98808	0.96978	-0.00038	-0.00008	0.00048	-0.00063	0.00001	-0.00349
Peppers	0.97861	0.98197	0.96944	0.00084	0.00004	-0.00057	0.00046	-0.00254	- 0.00153
Baboon	0.90467	0.85201	0.82384	0.00078	0.00065	0.00028	-0.00054	0.00051	0.00812
House	0.95926	0.95986	0.92623	-0.00084	0.00012	0.00080	0.00097	-0.00138	0.01905

5.6.2 Mean Absolute Error (MAE)

The Mean Absolute Error (MAE) test is another examination used to prove the validation of encryption systems toward differential attack [70]. MAE can be described as in the following Eq.

$$MAE = \frac{1}{M \times N} \sum_{i,j} |C\ (i,j) - P(i,j)| \tag{5.9}$$

M and N refers to number of rows and columns. C is the encrypted image and P is the original image. In order to reach better encryption security, large value of MAE is needed. Table 5.4 and table 5.5 shows the values of MAE.

5.6.3 Key Sensitivity Test

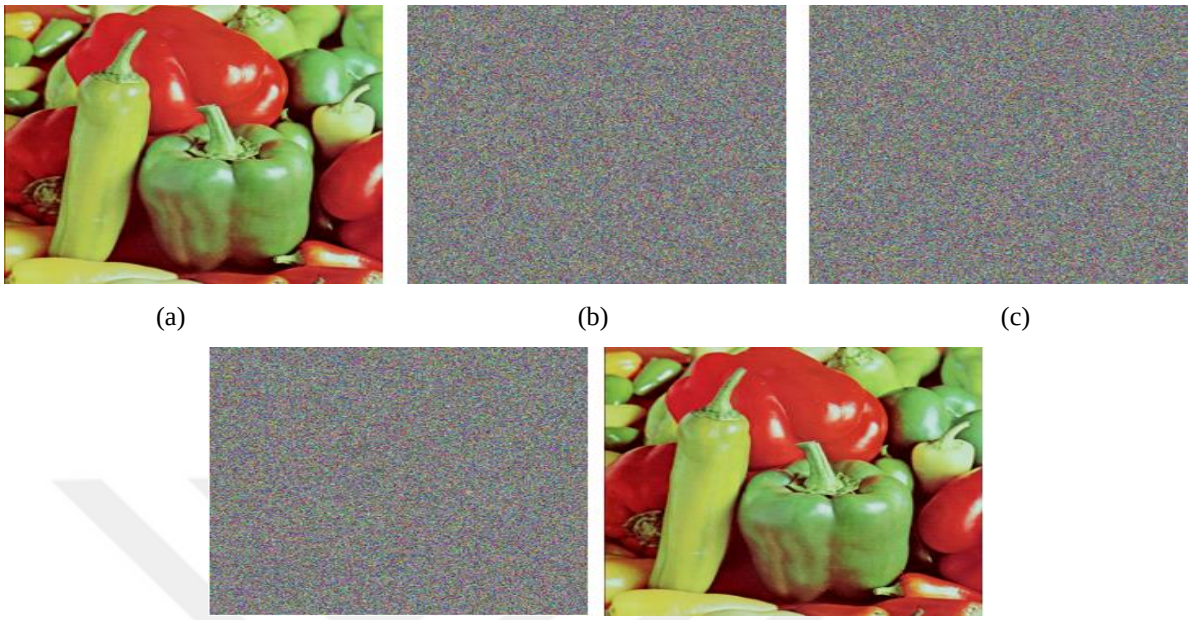
An efficient image encryption system is obligated to be sensitive for encryption key. In other word, a very minor change that occurred in secret key, the recovered image is not able to recover correctly [71]. With the aim of testing the sensitivity of the systems secret key, input image is encrypted by suggested key, the ciphered image will be decrypted with different wrong keys.

The wrong key is same the proposed key but with minor change. For proposed algorithm 1, the propose key is x_1,=1.011 $y_1 = 0.1, z_1 = 0.1, w_1 = 0.1, x_2 = 1, \mathrm{y}_2 = 0.1\ , z_2 = 0.1, w_2 = 0.1, a_1$= 12, $b_1 = 23$, $c_1 = 1$, $d_1 = 2.1$, $k_1 = 6$, $r_1 = 0.2, a_2$= 35, b_2= 8/3, c_2= 55, $r_2 = 1.5$, $\breve{x} = (0.06,6.001)$ and $\breve{y} = (-1,0.0001)$. The wrong key 1 is x_1,=1.011 $y_1 = 0.1, z_1 = 0.1, w_1 = 0.1, x_2 = 1, \mathrm{y}_2 = 0.1\ , z_2 = 0.1, w_2 = 0.1, a_1$=12+$10^{-14}$, $b_1 = 23$, $c_1 = 1$, $d_1 = 2.1$, $k_1 = 6$, $r_1 = 0.2, a_2$= 35, b_2= 8/3, c_2= 55, $r_2 = 1.5$ $\breve{x} = (0.06,6.001)$ and $\breve{y} = (-1,0.0001)$. The wrong key 2 is x_1,=1.011 $y_1 = 0.1, z_1 = 0.1, w_1 = 0.1, x_2 = 1, \mathrm{y}_2 = 0.1\ , z_2 = 0.1, w_2 = 0.1, a_1$= 12, $b_1 = 23$, $c_1 = 1$, $d_1 = 2.1$, $k_1 = 6$, r_1= 0.2, a_2= 35+10^{-14},b_2= 8/3, c_2= 55, $r_2 = 1.5$ $\breve{x} = (0.06,6.001)$ and $\breve{y} = (-1,0.0001)$. Figure 5.3 shows the results of decrypted image by secret keys with minor change for proposed algorithm1.

For proposed algorithm 2, the proposed key is a_1=10, b_1=2, c_1=28, d_1=0.1, m_1=27, n_1=0.5, a_2=30, b_2=3, c_2=20, k_2=2, kk_2=2, x_1=1, y_1=0.1, z_1=0.1, w_1=0.1, x_2=1, y_2=0.1, z_2=0.1and w_2=0.1. The wrong key1 is a_1=10, b_1=2+10^{-14}, c_1=28, d_1=0.1, m_1=27, n_1=0.5, a_2=30, b_2=3, c_2=20, k_2=2, kk_2=2, x_1=1, y_1=0.1, z_1=0.1, w_1=0.1, x_2=1, y_2=0.1, z_2=0.1and w_2=0.1. The wrong key2 is a_1=10, b_1=2, c_1=28, d_1=0.1, m_1=27, n_1=0.5, a_2=30, b_2=3, c_2=20, k_2=2+10^{-14}, kk_2=2, x_1=1, y_1=0.1, z_1=0.1, w_1=0.1, x_2=1, y_2=0.1, z_2=0.1and w_2=0.1. Figure 5.4 shows the results of decrypted image by secret keys with minor change for proposed algorithm2.

5.7 DECRYPTION QUALITY

CC is used for evaluation of the decryption quality. For a valid decryption, CC should be 1or close to one [72]. In order to test the quality of decrypted image, the CC is applied between the decrypted image and the plain image. The valuation results are tabulated in table 5.4 and table 5.5. The results of tables state that every decryption process is precise. In other word, decrypted images are fully identical to the corresponding plain images.



(a) (b) (c)

(d) (e)

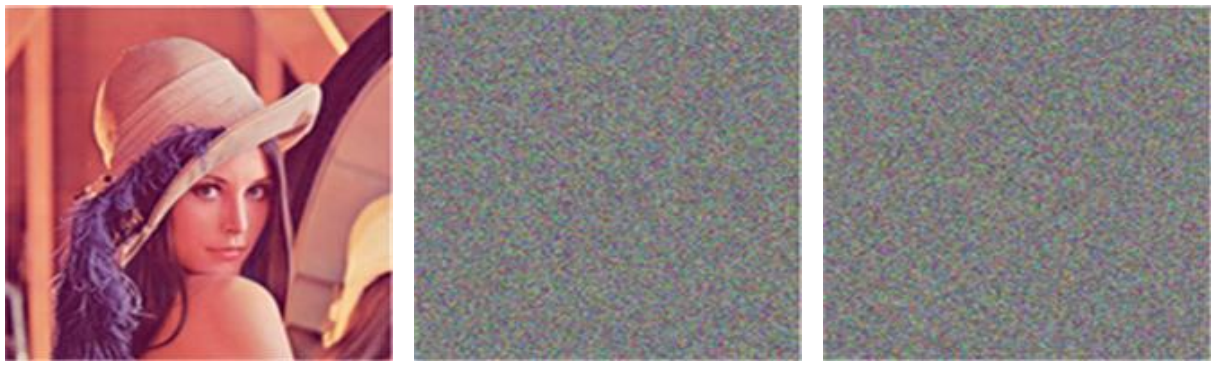
Figure 5.3: Key sensitivity test for proposed algorithm1 (a) input image, (b) encrypted image, (c) decrypted image with wrong key1, (d) decrypted image with wrong key 2, (e) decrypted image with proposed key.

Table 5.4: Encryption and decryption quality parameters for proposed algorithm 1.

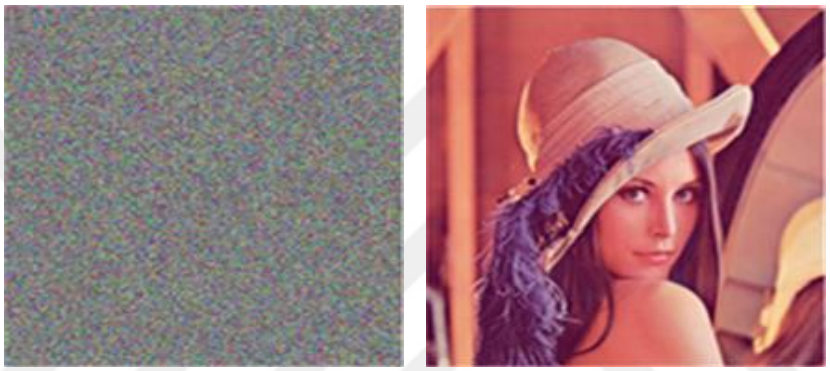
Image	Encryption quality				Differential attack			Decryption quality
	MSE	PSNR	Entropy	CC	MAE	NPCR	UACI	CC
Lena	48.3660	8.6233	7.9994	0.00142	77.526	99.60%	33.57%	1
Peppers	42.9385	8.0752	7.9993	-0.00045	82.231	99.61%	33.27%	1
Baboon	38.6173	8.7808	7.9993	-0.00037	76.305	99.62%	33.35%	1
House	25.4544	8.4812	7.9993	-0.00039	78.666	99.61%	33.39%	1

Table 5.5: Encryption and decryption quality parameters for proposed algorithm 2.

Image	Encryption quality				Differential attack			Decryption quality
	MSE	PSNR	Entropy	CC	MAE	NPCR	UACI	CC
Lena	48.4704	8.6219	7.9993	0.00049	76.359	99.60%	32.87%	1
Peppers	43.0041	8.0630	7.9993	-0.00305	82.343	99.59%	33.11%	1
Baboon	38.430	8.7733	7.9993	-0.00056	76.359	99.61%	33.45%	1
House	25.4816	8.4716	7.9993	-0.00040	78.787	99.59%	33.77%	1



(a) (b) (c)



(d) (e)

Figure 5.4: Key sensitivity test for proposed algorithm2 (a) input image, (b) encrypted image, (c) decrypted image with wrong key1, (d) decrypted image with wrong key 2, (e) decrypted image with proposed key.

5.8 NOISE ATTACK

In the interest of appraising the strength of proposed system against noise, the following sequence was carried out. The plain image is encrypted by encryption scheme. A density (0.5) of salt and pepper is added to the encrypted image. Then, the plain image is recovered from noisy encrypted image [73]. The results for both algorithms are shown in Figure 5.5.and figure 5.6.

5.9 DATA LOSS ATTACK

The data (for each color pixels) in the middle of the encrypted image with 20 * 20 window were extracted through substituting the data by zeros. Then, reconstructed the original image from encrypted image within data loss [74]. Fig.10 shows the results. It is recommended that the

suggested algorithm is able to hold against varied attacks (noise attack and data loss attack) in spatial domain.

(a) (b) (c)

Figure 5.5: Recovered images after salt and pepper noise is added: (a) salt and ppepper with density 0.05, (b) salt and ppepper with density 0.1, (c) salt and pepper with density 0.5.

(a) (b) (c)

Figure 5.6: Recovered images after salt and pepper noise is added: (a) salt and ppepper with density 0.05, (b) salt and ppepper with density 0.1, (c) salt and pepper with density 0.5.

5. 10 Comparison

Different performance of other system based diverse criteria are compared to proposed image encryption scheme performance. For simplicity, we will compare different images with different sizes. The results reveal that the proposed system holds preferable security performance compared with other systems, but it is not necessary the best. Table 5.6 shows the comparison results for correlation (for colored image the average of R, G and B color is calculated for horizontal, vertical and diagonal direction), information entropy and key space respectively.

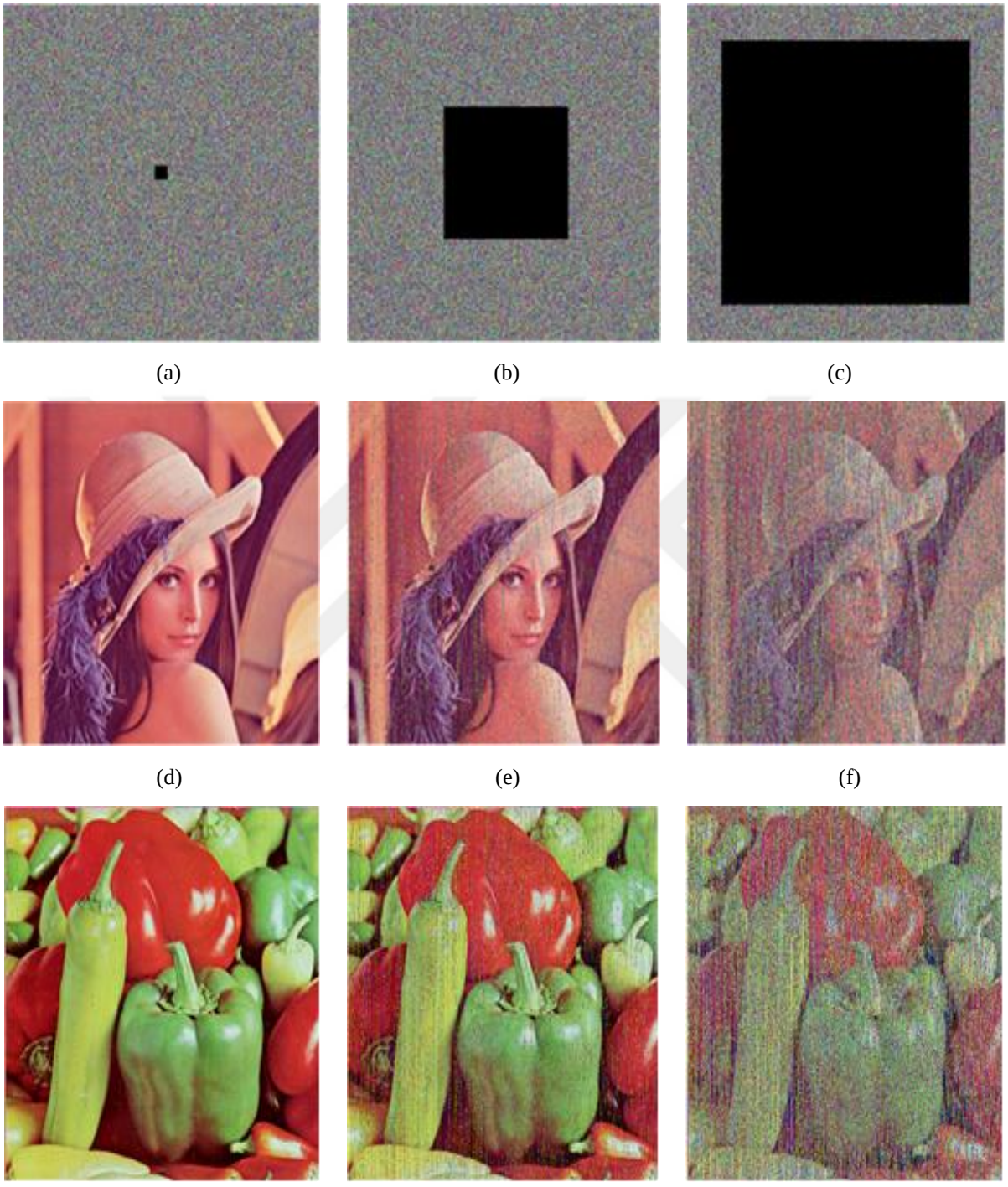


Figure 5.7: Data lose attacks test: (a) encrypted image with data lose (20 × 20), (b) encrypted image with data lose (200 × 200), (c)) encrypted image with data lose (400 × 400), (d) recovered image of (a) by algorithm 1, (e) recovered image of (b) by algorithm 1, (f) recovered image of (c) by algorithm1, (g) recovered image of (a) by algorithm 2, (h) recovered image of (b) by algorithm 2, (i) recovered image of (c) by algorithm2.

Table 5.6: Comparison of proposed algorithm with other algorithms.

Algorithm	Image	Size	Correlation coefficient (average)			Entropy	Key space
			Horizontal	Vertical	Diagonal		
Proposed 1	Lena	512×512	-0.00038	-0.00008	0.00145	7.9994	10^{252}
Proposed 1	Peppers	512×512	0.00084	0.00004	-0.00416	7.9993	10^{252}
Proposed 1	Baboon	512×512	0.00078	0.00065	-0.00398	7.9993	10^{252}
Proposed 2	Lena	512×512	-0.00063	0.00001	-0.00349	7.9993	10^{266}
Proposed 2	Peppers	512×512	0.00046	-0.00254	- 0.00153	7.9993	10^{266}
Proposed 2	Baboon	512×512	-0.00054	0.00051	0.00812	7.9993	10^{266}
Ref.[62]	Lena	256×256	-0.0057	-0.0074	0.0010	7.9977	10^{84}
Ref.[64]	Lena	512×512	0.0022	0.0001	-0.0017	7.9972	_
Ref.[64]	Baboon	512×512	-0.0008	0.0002	-0.0006	7.9972	_
Ref.[72]	Lena	512×512	0.0008	0.0008	0.0005	7.9979	2^{512}
Ref.[72]	Peppers	_	0.0001	0.0003	0.0089	7.9973	2^{512}
Ref.[75]	Lena	512×512	0.0010	-0.0008	0.0008	7.9977	2^{186}
Ref.[76]	Lena	512×512	-0.0685	0.0857	0.0059	7.9992	4.2×10^{122}
Ref.[77]	Lena	256×256	-0.0041	0.0023	0.0040	7.9972	10^{105}

6. CONCLUSION

During recent years, the applications of chaos theory have made accomplishment, and have been vastly implemented in the field of network and communication security. Some extent of chaotic encryption system doesn't execute basic cryptography principles, and encrypted image that produced by these systems are simple to be recover. This research has analyzed an image cryptosystems depending on hyper-chaotic systems and different technologies. Hyper-chaotic systems are properly used to generate eight sequences that used to permute image pixels and change the value of pixels. MD5 and Lagrange interpolation equation are an additional technique employed to give the strength for plain image sensitivity by confusing the relation between original image and initial condition values of hyper-chaotic systems. While the technique of lazy wavelet transform (LWT) is used to increase the security of cryptosystem. Consequently, two hyper-chaotic systems result better key space, better sensitivity to secret keys and better security. As consequence of experimental results and the security analysis, it is obvious that histogram of encrypted images has been uniformly distributed for encrypted image and correlation for adjacent pixel is reduced in vertical, horizontal and diagonal direction for both algorithms. The value of entropy for both algorithms is 7.9993 which is quite close to the ideal value. Additionally, experimental results illustrate that proposed schemes are able to resist against different intensity of noise and data lose attack.

The future works of this research can be summarized as follow:

1. The study of future research will mainly focus on the achievement of encryption system for video and audio files.
2. it is recommended Utilize the technology of image encryption system with the technology of image data compression in order to ensure the security of image with proper compression.
3. The study for hardware implementation of hyper-chaotic encryption technology is able to provide an efficient tool for both encryption system and confidential communication through different networks. Some researchers have tended to implement chaotic cryptosystem by employing Field Programmable Gate Array (FPGA) technology, while other researchers used Very Large Scale Integration (VLSI) technology for implementing cryptosystems.

4. initialize a new hyper-chaotic system with high precision of control values are essential part for chaotic encryption for the propose of increasing the key space and security.
5. In spite of validation of executed time for both algorithms (less than 1 second for both proposed algorithms), it is recommended to implement the chaotic system by using parallel method that can save more time to construct cipher images especially with high dimensions' image. The researcher is able to implement a cryptosystem in parallel method by using Compute Unified Device Architecture that invited by NIVDIA [78] as programing interface.

REFERENCES

[1] D. Kong, L. Cao, X. Shen, H. Zhang, and G. Jin, "Image encryption based on interleaved computer-generated holograms," *IEEE Trans. Ind. Informatics*, vol. 14, no. 2, pp. 673–678, 2018.

[2] U. Coruh and O. Bayat, "Hybrid Secure Authentication and Key Exchange Scheme for M2M Home Networks," *Secur. Commun. Networks*, vol. 2018, 2018.

[3] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, vol. 133, no. 1, p. 6, 2018.

[4] O. N. Uçan, O. Bayat, and M. B. Çoşkun, "Development and evaluation of the authentication systems by using phase-only correlation palm print identificaton methods," in *2017 International Conference on Engineering and Technology (ICET)*, 2017, pp. 1–4.

[5] M. Van Droogenbroeck and R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," *ACIVS Adv. concepts Intell. Vis. Syst. Proc.*, pp. 90–97, 2002.

[6] S. Fong, P. B. Ray, and S. Singh, "Improving the lightweight video encryption algorithm," in *proceeding of iasted international conference, single*, 2002, pp. 25–28.

[7] Y. A. Alsultanny, "Testing Image Encryption by Output Feedback (OFB)," *J. Comput. Sci.*, vol. 4, no. 2, p. 125, 2008.

[8] J. Jan, *Medical image processing, reconstruction and restoration: concepts and methods*. Crc Press, 2005.

[9] H.-M. Yuan, Y. Liu, L.-H. Gong, and J. Wang, "A new image cryptosystem based on 2D hyper-chaotic system," *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 8087–8108, 2017.

[10] D. Salomon, *Coding for data and computer communications*. Springer Science & Business Media, 2006.

[11] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *Springerplus*, vol. 5, no. 1, p. 289, 2016.

[12] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimed. Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, 2017.

[13] G. Ye, K. Jiao, C. Pan, and X. Huang, "An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map," *Secur. Commun. Networks*, vol. 2018, 2018.

[14] C.-L. Li, H.-M. Li, F.-D. Li, D.-Q. Wei, X.-B. Yang, and J. Zhang, "Multiple-image encryption by using robust chaotic map in wavelet transform domain," *Optik (Stuttg).*, vol. 171, pp. 277–286, 2018.

[15] W. Stallings, *Cryptography and Network Security: Principles and Practices 4th edition*. 2005.

[16] M. Khan and T. Shah, "A Literature Review on Image Encryption Techniques," *3D Research*, vol. 5, no. 4. 2014.

[17] A. Al-Vahed, and S. Haddad, "An overview of modern cryptography. *Tools Appl.*, vol. 1, no. 1, pp. 55-61, 2011.

[18] Q.-A. Kester, "A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher," *arXiv preprint arXi*, pp. 1307–7786, 2013.

[19] G. Shanmugam, R. M. Low, and M. Stamp, "Simple substitution distance and metamorphic detection," *J. Comput. Virol.*, vol. 9, no. 3, pp. 159–170, 2013.

[20] M. Heydari, G. L. Shabgahi, and M. M. Heydari, "Cryptanalysis of transposition ciphers with long key lengths using an improved genetic algorithm," *World Appl. Sci. J.*, vol. 21, no. 8, pp. 1194–1199, 2013.

[21] Z. Mahmood, J. L. Rana, and A. Khare, "Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)," *Int. J. Comput. Appl.*, vol. 50, no. 19, 2012.

[22] K. Patel and S. Belani, "Image encryption using different techniques: A review," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 1, pp. 30–34, 2011.

[23] S. Charbathia and S. Sharma, "A Comparative Study of Rivest Cipher Algorithms," *Int. J. Inf. Comput. Technol.ISSN*, pp. 0974–2239, 2014.

[24] K. S and Muruganandam A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System," *Int. J. Sci. Eng. Res.*, vol. 2, no. 11, pp. 24–31, 2014.

[25] S. Purevjav, T. Kim, and H. Lee, "Email encryption using hybrid cryptosystem based on Android," in *International Conference on Advanced Communication Technology, ICACT*, 2016.

[26] A. Soleymani, M. J. Nordin, and Z. M. Ali, "A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field," *J. Image Graph.*, vol. 1, no. 1, pp. 43–49, 2013.

[27] O. F. Mohammad, M. Shafry, M. Rahim, S. Rafeeq, M. Zeebaree, and F. Y. H. Ahmed, "A Survey and Analysis of the Image Encryption Methods," *International Journal of Applied Engineering Research,* vol. 12, no. 23, pp. 13265-13280, 2017.

[28] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[29] H. Hermassi, R. Rhouma, and S. Belghith, "Improvement of an image encryption algorithm based on hyper-chaos," *Telecommun. Syst.,* vol. 52, no. 2, pp. 539–549, 2013.

[30] S. Yanchuk and T. Kapitaniak, "Chaos – hyperchaos transition in coupled Rössler systems," *Physics Letters A,* vol. 290, no. 3-4, pp. 139–144, 2001.

[31] G. Gu and G. Han, "An enhanced chaos based image encryption algorithm," in *First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06),* 2006, vol. 1, pp. 492–495.

[32] Z. Aihong, L. Lian, and Z. Shuai, "Research on method of color image protective transmission based on Logistic map," *ICCASM 2010 - 2010 Int. Conf. Comput. Appl. Syst. Model. Proc.*, vol. 9, no. Iccasm, pp. 266–269, 2010.

[33] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, 2014.

[34] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Comput. Electr. Eng.*, vol. 54, pp. 471-483, 2016.

[35] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, 2018.

[36] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, no. August 2016, pp. 238–246, 2017.

[37] X. Y. Wang, S. X. Gu, and Y. Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, pp. 126–134, 2015.

[38] S. Zhang and T. Gao, "An image encryption scheme based on DNA coding and permutation of hyper-image," *Multimed. Tools Appl.*, vol. 75, no. 24, pp. 17157–17170, 2016.

[39] T. Li, M. Yang, J. Wu, and X. Jing, "A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing," *Complexity*, vol. 2017, 2017.

[40] B. Mondal, S. Singh, and P. Kumar, “A secure image encryption scheme based on cellular automata and chaotic skew tent map,” *J. Inf. Secur. Appl.*, vol. 45, pp. 117–130, 2019.

[41] P. A. Chia, S. B. Maynard, and A. B. Ruighaver, “Understanding organizational security culture,” *Proc. PACIS2002. Japan*, vol. 158, 2002.

[42] R. C. Gonzalez and R. E. Woods, “Digital image processing [M],” *Publ. house Electron. Ind.*, vol. 141, no. 7, 2002.

[43] A. S. Glassner, *Principles of digital image synthesis: Vol. 1*, vol. 1. Elsevier, 1995.

[44] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps,” *Chaos, Solitons and Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[45] M. A. Hernández-Acosta, M. Trejo-Valdez, J. H. Castro-Chacón, C. R. Torres-San Miguel, H. Martínez-Gutiérrez, and C. Torres-Torres, “Chaotic signatures of photoconductive Cu_2ZnSnS_4 nanostructures explored by Lorenz attractors,” *New J. Phys.*, vol. 20, no. 2, p. 023048, 2018.

[46] C. Kyrtsou and W. C. Labys, “Evidence for chaotic dependence between US inflation and commodity prices,” *J. Macroecon.*, vol. 28, no. 1, pp. 256–266, 2006.

[47] S. H. Kellert, *In the wake of chaos: Unpredictable order in dynamical systems*. University of Chicago press, 1993.

[48] A. M. Goulielmos and M. Psifia, “A study of trip and time charter freight rate indices: 1968–2003,” *Marit. Policy Manag.*, vol. 34, no. 1, pp. 55–67, 2007.

[49] J. Fell, J. Röschke, and P. Beckmann, “Deterministic chaos and the first positive Lyapunov exponent: a nonlinear analysis of the human electroencephalogram during sleep,” *Biol. Cybern.*, vol. 69, no. 2, pp. 139–146, 1993.

[50] O. E. Rossler, “An equation for hyperchaos,” *Phys. Lett. A*, vol. 71, no. 2–3, pp. 155–157, 1979.

[51] A. Wolf, “Quantifying chaos with Lyapunov exponents,” *Chaos*, vol. 16, pp. 285–317, 1986.

[52] P. Wu, “Research on digital image watermark encryption based on hyperchaos,” 2013.

[53] A. B. Watson and J. A. Solomon, “Model of visual contrast gain control and pattern masking,” *JOSA A*, vol. 14, no. 9, pp. 2379–2391, 1997.

[54] W. I. M. Sweldens, “The lifting scheme: A construction of second generation wavelets,” *SIAM journal on mathematical analysis*, vol. 29, no. 2, pp. 511–546, 1998.
[55] W. Sweldens, “The lifting scheme: A custom-design construction of biorthogonal wavelets,” *Appl. Comput. Harmon. Anal.*, vol. 3, no. 2, pp. 186–200, 1996.
[56] P. Balakrishnan, “Design and Implementation of Lifting Based Daubechies Wavelet Transforms Using Algebraic Integers.” University of Saskatchewan, 2013.
[57] R. Rivest, “The MD5 message-digest algorithm,” 1992.
[58] Y. Li, X. Liu, G. Chen, and X. Liao, “A new hyperchaotic Lorenz-type system: Generation, analysis, and implementation,” *Int. J. Circuit Theory Appl.*, vol. 39, no. 8, pp. 865–879, 2011.
[59] N. Yujun, W. Xingyuan, W. Mingjun, and Z. Huaguang, “A new hyperchaotic system and its circuit implementation,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 11, pp. 3518–3524, 2010.
[60] S. Jafari, S. T. Kingni, S. Vaidyanathan, C. Volos, and V.-T. Pham, “A no-equilibrium hyperchaotic system with a cubic nonlinear term,” *Opt. - Int. J. Light Electron Opt.*, vol. 127, no. 6, pp. 3259–3265, 2015.
[61] S. Pang and Y. Liu, “A new hyperchaotic system from the Lü system and its control,” *J. Comput. Appl. Math.*, vol. 235, no. 8, pp. 2775–2789, 2011.
[62] Q. Zhang, L. Liu, and X. Wei, “Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps,” *AEU-International J. Electron. Commun.*, vol. 68, no. 3, pp. 186–192, 2014.
[63] X. Zhang, W. Nie, and Y. Ma, “Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box,” *Multimed. Tools Appl.*, vol. 76, no. 14, pp. 15641–15659, 2017.
[64] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, “Color image encryption based on hybrid hyper-chaotic system and cellular automata,” *Opt. Lasers Eng.*, vol. 90, pp. 225–237, 2017.
[65] H. Zhu, C. Zhao, and X. Zhang, “A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem,” *Signal Process. Image Commun.*, vol. 28, no. 6, pp. 670–680, 2013.
[66] A. Sinha and K. Singh, “A technique for image encryption using digital signature,” *Opt. Commun.*, vol. 218, no. 4–6, pp. 229–234, 2003.
[67] F. Özkaynak and A. B. Özer, “Cryptanalysis of a new image encryption algorithm based on chaos,” *Optik (Stuttg).*, vol. 127, no. 13, pp. 5190–5192, 2016.
[68] A. V. Diaconu and A. C. Dascalescu, “Correlation distribution of adjacent pixels randomess test for image encryption,” *Proc. Rom. Acad. Ser. A - Math. Phys. Tech. Sci. Inf. Sci.*, vol. 18, pp. 351–359, 2017.

[69] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li, and Y. Liu, “Image encryption-then-transmission using DNA encryption algorithm and the double chaos,” *IEEE Photonics J.*, vol. 10, no. 3, pp. 1–15, 2018.

[70] M. Mikhail, Y. Abouelseoud, and G. El Kobrosy, “Two-phase image encryption scheme based on FFCT and fractals,” *Secur. Commun. Networks*, vol. 2017, 2017.

[71] C. Zhu and K. Sun, “Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps,” *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[72] B. Norouzi and S. Mohammad, “A novel image encryption based on hash function with only two-round diffusion process,” *Multimedia systems,* vol. 20, no. 1, pp. 45–64, 2014.

[73] C. H. Yuen and K. W. Wong, “A chaos-based joint image compression and encryption scheme using DCT and SHA-1,” *Appl. Soft Comput. J.*, vol. 11, no. 8, pp. 5092–5098, 2011.

[74] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, “Image encryption using P-Fibonacci transform and decomposition,” *Opt. Commun.*, vol. 285, no. 5, pp. 594–608, 2012.

[75] F. Özkaynak, A. B. Özer, and S. Yavuz, “Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences,” *Opt. Commun.*, vol. 285, no. 24, pp. 4946–4948, 2012.

[76] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, “Image Encryption with Double Spiral Scans and Chaotic Maps,” *Secur. Commun. Networks*, vol. 2019, 2019.

[77] X. Li, Z. Xie, J. Wu, and T. Li, “Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations,” *Complexity*, vol. 2019, 2019.

[78] C. Nvidia, “Compute unified device architecture programming guide,” 2007.