REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

SECURING CRITICAL INFORMATION: AN IMAGE CRYPTOGRAPHY DIGITAL BASED ON MULTI LEVEL CRYPTOGRAPHIC

Lina Jamal IBRAHIM

Master's Thesis

Supervisor

Prof. Dr. Osman Nuri UÇAN

Istanbul, 2022

SECURING CRITICAL INFORMATION: AN IMAGE CRYPTOGRAPHY DIGITAL BASED ON MULTI LEVEL CRYPTOGRAPHIC

Lina Jamal IBRAHIM

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled SECURING CRITICAL INFORMATION: AN IMAGE CRYPTOGRAPHY DIGITAL BASED ON MULTI LEVEL CRYPTOGRAPHIC prepared by LINA JAMAL IBRAHIM and submitted on 08/08/2022 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

_____

Prof. Dr. Osman Nuri UCAN

Supervisor

Thesis Defense Committee Members:

Prof. Dr. Osman Nuri UCAN	Faculty of Engineering and Natural Sciences, Altinbas University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Faculty of Engineering and Natural Sciences, Altinbas University	_____
Assoc. Prof. Dr. Adil Deniz DURU	Faculty of Sport Sciences, Marmara University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master thesis.

Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Lina Jamal IBRAHIM

Signature

DEDICATION

I devote and pledge this research work to my father and mother to help me in my hard times, for their patience, encouragement, and support; without their presence in my life, this research would not have been completed after God

PREFACE

First and foremost, all praise and thanks are due to Allah, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him). Next, I would like to thank my supervisor, Prof. Dr. Osman Nuri UCAN, for his patience and advice to complete this research; Then I would like to express my sincere appreciation to all the friends who advised me and provided me with moral support while preparing for this research work. Finally, I am grateful to all my family members for their support. I would like to thank my parents for their patience, encouragement, support and understanding.

ABSTRACT

SECURING CRITICAL INFORMATION: AN IMAGE CRYPTOGRAPHY DIGITAL BASED ON MULTI LEVEL CRYPTOGRAPHIC

IBRAHIM, Lina Jamal,

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

Supervisor: Prof. Dr. Osman Nuri UÇAN

Date: 08 / 2022

Pages: 117

The importance of image encryption has considerably increased specially after the spectacular growth of internet of things (IoT) and due to the simplicity of capturing and transferring digital images. Although there are several encryption approaches, chaotic with image cryptography is considered the most appropriate approach for image applications due to its sensitivity to starting conditions and control parameter value. This research aims at generating an encrypted image free of statistical information to make cryptanalysis infeasible. Therefore, a new method was introduced in this thesis called Multi-layer Chaotic Maps (MLCM) based on confusion and diffusion. Basically, the confusion method uses the Sensitive Logistic Map (SLM), Hénon Map, and the additive white Gaussian noise to generate random numbers to be used in the pixel permutation method. However, the diffusion method uses Extended Bernoulli Map (EBM), Tinkerbell, Burgers, and Ricker maps to generate the random matrix. The correlation between adjacent pixels was minimized to have a very small value (x10-3). Besides, the keyspace was extended to be very large (2^450) considering the key sensitivity to hinder brute force attack. Finally, a histogram was idealized to be perfectly equal in all occurrences and the resulted information entropy was equal to the ideal value (8), which means that the resulted encrypted image is free of statistical properties in terms of the value of the histogram and the value of information entropy. Based on the findings, the high randomness of the generated random sequences of the proposed confusion and diffusion methods is capable of producing a robust image encryption framework against all types of cryptanalysis attacks.

Keywords: Cryptography, Chaotic Maps, Sensitive Logistic Map, Extended Bernoulli Map

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

1D	:	One Dimension
2D	:	Two Dimensions
3D	:	Three Dimensions
4D	:	Four Dimensions
AE	:	Authenticated Encryption
AES	:	Advanced Encryption Standard
ARX	:	Add Rotate XOR
AWGN	:	Additive White Gaussian Noise
BRC	:	Bit-Chaotic-Rearrange
CBC	:	Cipher-Block Chaining
CC	:	Correlation Coefficient
CFB	:	Cipher Feedback
CIA	:	Confidentiality, Integrity and Availability
CNN	:	Convolutional Neural Network
C-SPIHT	:	Color Set Partitioning in Hierarchical Tree
CTR	:	Counter
DCT	:	Discrete Cosine Change
DES	:	Data Encryption Standard

DNA	:	Deoxyribonucleic Acid
DWT	:	Discrete Wavelet Transform
EBM	:	Extended Bernoulli Map
ECB	:	Electronic Codebook
FFT	:	Fast Fourier Transformation

1. INTRODUCTION

1.1 INTRODUCTION

Increasing dependence on multimedia data in different programs and methods, such as defense ministry, communication fields, medical, education stages, and social network (chatting programs), results in increasing threats to such data. The image is the major and common multimedia type used in internet, because of the it is transmitted in easy way over network [1]. In other side, the request to transfer the image within the ensure way has also become hot subject, and cryptography is the choose as secure way to transfer the image data. Current cryptography techniques such as (RSA, Triple DES, and new version of AES) are inappropriate for image cryptography because of the huge amount of size and noteworthy redundancy of image information [2]. In addition, there are many limitations and disadvantage such as the demand for a powerful calculation program and time requirement, so, such that these techniques have a low level of efficiency [3]. The image cryptography is defined as the utilize of a set of steps named algorithm to convert the original image into a coded image in such a manner that no one can recover it [4]. Recently, numerous methods have been introduced to encrypt image, using chaotic map (Chaos map) to improve the efficient [5]. The chaotic maps were first introduced in the (1970s) for utilize in mathematics, physics, and engineering fileds. The chaotic map methods are common and popular because of their sensitivity, randomness and unpredictability [7]. Also, chaotic systems are similar to noisy methods because they are unpredictable, random, and sensitive to starting conditions (initial point) and control parameters in all pixels [8]. Therefore, chaotic methods have been used in cryptography widely nowadays [9]. Also, chaotic methods are useful for cryptography because they show to be random information. The major difference between chaotic methods and chaotic encryption is that chaotic encryption has defined by a finite set and chaotic methods can define via real numbers [11].

1.2 PROBLEM BACKGRUOND

In image encryption, the predictive of new pixel's position within a condition for random function s*ti*ll need full concern [12][13]. A random function may be used to produce a key that

can be used for both encryption and decryption, and this function should be strong and dependable [14]. The correlation of individual pixels can be mapped under this key. Previously more effort was spent in this regard to improve the confusion to avoid any tamper detection, but still, need to trick the warden and aggressor. Recently, more work was put into improving the confusion to avoid any tamper detection. These works are used different approaches to deceive the warden and attacker. In contrast to confusion which takes into account pixel position, the diffusion stage is in charge of altering pixel value [16]. Due to the image's histogram's direct effect, changing these values is crucial. A consistent histogram for the produced cipher image has received a lot of attention from algorithms in recent years. The diffusion method should efface the histogram of the cipher image to eliminate the statistical aspects of the encrypted image in order to defend against statistical assaults. However, an encrypted image of 8 has to have an information entropy of 8. The image histogram and information entropy are closely related concepts [17]. Information entropy indicates the erratic distribution of pixel values. The information entropy should be near the optimum value (8) ineffective image encryption techniques, and when it is 8, this denotes a truly random sample [18]. Many methods accomplish security in the field of image encryption, but the chaotic method is the best method since it shares the same cryptographic properties [19][20]. Nowadays, numerous chaos-based image encryption techniques use the Shannon (1949) confusion and diffusion process to create safe image encryption systems. Despite being excellent, some suggested approaches nevertheless run across several issues. For instance, in the algorithm proposed by Qais and Aouda [21], both chaotic methods (Rössler and Lorenz) are utilized with a cryptography system. Generally, utilizing two, three, or more chaotic methods in one scheme is highly uncommon [22]. Both methods of Rössler and Lorenz basically work with three parameters or variables. Therefore, the proposed work security is improved due to the parameters being worked based on six variables, so it is highly the level of security. This work is used to shuffle the pixels of the image and modify its grayscale value during the different number of loops before storing the randomized pixels of the image. The main operation used in cryptography is the XOR operation in most of the methods. In proposed work, the size keyspace is pretty within increasing the initial value to six numbers instead of three numbers within each chaotic system. Additionally, because the suggested approach just performs an XOR operation between the plain image and the

random one without changing the image's pixels, the predicted correlation value between the adjacent pixels of the encrypted image will be modest. The suggested framework deals with the bit-level of image pixels and the random sequences produced by the employment of two logistic maps in both confusion-diffusion processes. The two random sequences are created utilizing two beginning conditions and two control parameters as part of the proposed method's first phase. The image pixels are permuted using the first of these created sequences. In order to do the permutation, the image is first transformed from a two-dimensional matrix into a one-dimensional array and then this array is rearranged in accordance with the randomness order of the random sequence. The output array will be examined to produce a bit-level matrix (each element in this array will be analyzed into its bits component). The bit-level matrix element will be permuted using the second chaotic sequence that was produced by applying the second starting condition and second control parameter. The analysis produced by this approach falls short of picture encryption security standards since the histogram's anticipated result will not be particularly uniform. To reduce the complexity of image encryption, Abhinav and Verma [24] proposed a simple image encryption method using CWT which means complex wavelet transformation. In present work, the original image used Wavelet Transformation for image transformation. secondly, the chaotic map was used for pixel scrambling based on the Arnold method. Although the suggested image encryption method is a simple method, it expects to obtain low results in terms of histogram analysis .As mentioned in the above brief survey, the development of encryption methods for the secure transmission of images over the internet still faces many remaining challenges and one of the main challenges in encryption algorithms is the generation of random numbers known as encryption keys, where these random numbers must satisfy several principles of unpredictability, long series period and the ability to regenerate these sequences many times. The initial key is another issue in the image encryption field and the criteria of this issue are based on the key size, key sensitivity, level of randomness, and regenerating ability. The statistical properties of the cipher image such as the correlation between adjacent pixels, the correlation coefficient between plain and cipher images, histogram, and information entropy are considered important issues in the field of image encryption. Also, the ability to withstand differential attacks has become a very critical issue, especially after the increased interest in such attacks. These challenges and issues can be explained in detail as

follows: In the field of cryptography, random number generator plays an essential role and the ciphertext properties fully depend on the generated key [25]. The random number generator is basically used to generate the secret key to be used later in the encryption algorithm and to produce the desired random keys. There are generally two types of these generators. The first one is the True Random Number Generator (TRGN). To produce randomness in this type a non-deterministic source (entropy source) should be sampled and processed outside the computer [26]. Actually, it is very simple to get a source of entropy, like the keystrokes time interval or some variations of mouse movement. In practice, it is difficult to get entropy by tracking user inputs, while keystrokes are often buffered by the operating system after collecting several keystrokes to be sent to a waiting program. The radioactive source is considered a really good entropy generator. Another good entropy source is the noise of the atmosphere that can be acquired by radio [27]. The output of TRNG is sometimes used directly as the random number or sometimes used as the input of the Pseudo-Random Number Generator (PRNG). To use it directly (no extra processing implemented to it), it should satisfy randomness criteria. For encryption purposes, some of the entropy sources (e.g. time/date vectors) are sometimes predictable; it can lighten the predictability by the combination of different types of sources [28]. However, there are still weak and drawbacks in using TRNG in cryptography fields and this weakness and drawback is the time consumption required to produce TRNG, which makes this generator undesirable when a large size random sequence is required. In addition, TRNG is deficient when it is evaluated by using statistical tests. The second type is Pseudo-Random Number Generator (PRNG). In this type of random number generator, one or more values can be used as the input (seed) to produce pseudorandom series of unpredictable behavior as the output [29]. Randomness and unpredictability are the properties of the used seed value itself, and typically PRNG output is deterministic, and it is a function of the seed. The term pseudorandom is an indication of the deterministic nature of the used process, and because of this nature, the pseudo-random sequence is reproducible by using the same seed value [30]. Thus, the used seed should be saved if reproducing or validation process is required. It is worth noting that the pseudorandom number series is most often more random than the true random numbers generated from physical sources. Another feature of the PRNG that makes it more usable is that each of the generated pseudorandom number values is fully dependent on random

input that is already generated by the previous implementation of the PRNG. The correlation between input and output can be eliminated by using PRNG rather than TRNG. Thus, the random series generated by PRNG is better in terms of statistical properties in addition to the short time of implementation [31]. In cryptographic applications, both TRNG and PRNG are produced random bit series and sometimes it combines these random bits into random blocks. The most important properties of the produced random series are randomness and unpredictability [32]. Randomness can be explained as the result of flipping of fair (unbiased) coin which has two faces labeled “0” and “1” and the flipping process is independent of the previous result i.e., the current flip result is not affected by the previous result and would not affect the next result. Thus, the perfect random generator is resulted from the unbiased (fair) coin flip, since the distribution of zero and one values is random and [0, 1] are distributed uniformly. Each bit in the random series is generated independent of the other elements of the same random series, and the next value in the series cannot be predicted, regardless of how many bits have already been generated. Unpredictability is the second property of the produced random series. For cryptographic applications, both TRNG and PRNG must be unpredictable. In PRNG, if the seed value is unknown, the next generated value will be unpredictable, a feature known as forwarding unpredictability. The knowledge of any value in the random series should not lead to revealing the seed value (also, it should be unpredictable in a backward direction). There should be no clear correlation between the seed and any value in the generated series and the appearance probability of each element in the generated random series should be equal to 50% [33]. Key security is the procedure to be taken to ensure the confidentiality of the used key. There are two main issues in the key security field, which are key space and key sensitivity. The key space can be defined as the total number of possible keys that can be used to decrypt the ciphertext [32]. The key space size is an important criterion in the field of cryptography and in a good encryption system, the large key space indicates good resistance against brute force attacks [34]. In addition, powerful cryptography (encryption) must have a power encryption key (secret key) which means the encryption key should be bigger than 2^100 [32], with the indicator indicating the bits numbers of a secret key. The large cryptography key is provided powerful security against different types of attacks such as the Brute Force Attacks (BFA) [35]. Therefore, the design of an encryption system must consider the size of the key space. In a brute

force attack, the cryptanalyst tries different keys and may eventually guess the true key, thus a large key space size makes this type of attack infeasible. Key sensitivity is another issue related to key space size. In key sensitivity criteria, any slight change in the used key, even by one bit, should produce totally different encrypted image [36]. Therefore, key sensitivity issues must be considered in the design of any image encryption system. The statistical properties of cipher images can be exploited by cryptanalysts to decipher the encryption algorithm [37]. Correlation between adjacent pixels in the cipher image, correlation coefficient between cipher and plain image, histogram, and information entropy are the most important statistical features in the image encryption field. A good encryption system should obliterate all statistical features of the plain image because the cryptanalyst always tries to find any weakness in the encryption system to use in his analysis. There are several types of statistical-based attacks such as Histogram analysis, in which the plain image consists of semantic information which can be analyzed according to the frequency of the gray level. Thus, it is very important to deface the histogram of the plain image by the use of a strong encryption method. In correlation analysis, similar to the histogram, the correlation between adjacent pixels can reveal good statistical information about the plain image and call also reflect the relationship between the adjacent pixels. This type of information (correlation) can be minimized by suggesting a powerful encryption method [38].

Differential analysis is a general form of cryptanalysis, and it is primarily developed to be applicable for a block cipher, but recently several differential attack methods have been designed especially for stream cipher analysis [39]. In this analysis type, the cryptanalysis tries to find any relationship between two cipher images produced by making a one-pixel value alteration of the plain image before implementing the encryption process. If a significant difference between the two cipher images is obtained, the encryption method is differential attack proof, otherwise, it is easy to reveal good information of the plain image [40].

1.3 PROBLEM STATEMENT

Despite the use of traditional image encryption techniques to encrypt images with a security level, there are a number of problems that should be fixed to produce better-encrypted images. The creation of random keys for encryption and decryption procedures is the fundamental

difficulty addressed by inventors of image encryption [41]. The system's security is impacted by unexpected number generation, which is taken into account by the random number generator. In order to make the cipher image as chaotic as feasible, randomization is crucial in image encryption [42]. Due to the traditional random function, the system is resistant to statistical attacks that attempt to quantize the location of the pixel between the encryption and decryption processes [43]. Most of the studies in the last decade emphasized that good encryption is based on the correlation of pixels inside the image. The majority of research conducted over the past ten years has underlined the importance of pixel correlation as the foundation for effective encryption. Obviously, the simple image's complex pixel distribution results in a greater correlation. Therefore, randomizing the position of each pixel when encrypting and reconstructing cipher images might result in a cluttered image [44]. The rearranging of the pixels inside the picture increases security and prevents statistical assaults [45].

The significance of key space is to enable an encryption system to be more dependable and safer [46]. It the unavoidable for both confusion and diffusion to have such huge starting sizes, especially when employing 2D random key generation [47]. The encryption images should be taken into account by the image histogram and information entropy [48]. The histogram should be uniformed, and the entropy should be increased as the statistical assault is more sensitive to entropy values [49]. Additionally, every little alteration in the plain image must result in a large difference in the encrypted image. So, these results are related to a strong image encryption framework in order to prevent differential attacks [50].

1.4 RESEARCH GOAL

The goal of this research is to design and develop an image encryption framework with high-quality criteria. This can be achieved by increasing key space size, generating random keys with high randomness levels, obliterating the statistical properties of the encrypted image in addition to increasing robustness against differential attack.

1.5 RESEARCH OBJECTIVES

The following goals must be accomplished in order to reach the research aim.

i. To introduce a novel framework for image encryption based on two security procedures and idealize the erasure of statistical features such as information entropy and histogram.

ii. To enhance the confusion and diffusion processes based on a new random number generator with chaotic maps and additive white Gaussian noise is proposed.

iii. To provide a straightforward and effective diffusion technique for boosting resistance to differential analysis.

1.6 RESEARCH SCOPE

In order to achieve the desired goals and objectives of this research, it is very important to define the research scope, which can be explained by the following points:

i. SIPI is the dataset used to test the proposed framework. This dataset contains many images that are suitable to implement the proposed system. In addition to the SIPI dataset, the system performance is tested using three images taken via a mobile camera.

ii. Different image sizes such as 256*256, 512*512, 1024*1024 pixels are used to test the system Grayscale and 24-bit-colored images are also used.

iii. System testing is carried out using various performance analysis techniques, such as the US National Institute of Standards and Technology's random number generating test (NIST),

iv. key space, key sensitivity, image histogram (IH), Quantitative histogram (QH) by variance metric, information entropy analysis, the correlation between adjacent pixels by correlation, the correlation coefficient between plain and cipher images, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), and differential analysis such as Number of Pixels Change Rate (NPCR) with Unified Average Changing Intensity (UACI).

1.7 RESEARCH SIGNIFICANCE

The proposed image encryption system will achieve cipher images with a better security level, and this is done by introducing of the new process in the proposed encryption system to idealize histogram and information entropy, using new random number generators with large the key space, increasing robustness against the differential attack. The significance of the study is not only by the implementation in the field of image encryption, as it can also be used in other cryptography fields. The proposed random number generators have good quality in terms of the randomness criteria, and this can make the proposed generators useable in the fields that require random number generators like complete randomized design, computer simulation, statistical sampling, and in other fields where unpredictable sequences are desired.

1.8 THESIS ORGANIZATION

The proposed research is presented through this thesis and organized into six chapters, which can be outlined as follows:

Chapter 1: In this chapter, an introduction to the proposed research was done including problem formulation and a description of a research goal, objectives, scope, and significance.

Chapter 2: In this chapter, previous studies and related issues are discussed in detail.

Chapter 3: General research framework, the datasets used in the system testing, and the techniques used to evaluate the system are presented.

Chapter 4: The implementation of chaotic maps within confusion and diffusion process are mentioned in this chapter.

Chapter 5: Performance evaluation and security attacks of the proposed method are explained in this chapter.

Chapter 6: Contributions and future works of the proposed research are elaborated in this chapter.

2. LITERATURE REVIEW

2.1 INTRUDECTION

In this chapter, a comprehensive literature review is provided to identify the research questions and set the objectives. Image encryption can be defined as the art of converting a plain image into coded form in a way there is no one can restore it else than the intended receiver only [51]. Demand expansion on finding secure methods to protect the information of images is coming from the escalation of image applications and image transfer over the internet and open networks and due to the existence of critical information included by these images. Image encryption is one of the most effective ways to protect such information (images) and it has applications in many fields such as military communications, medical imaging, multimedia systems, internet communications, and so [52]. The methods of text encryption can be used in the image encryption field but with significant drawbacks due to several reasons such as the large size of the images when compared to the text size which causes long time consumption, the other reason is that the decrypted text should be equal to the encrypted test while it is not necessary for image encryption. Cryptography has been beginning thousands of years ago until the last decades and it uses the old methods of encryption or what is well known by classical cryptography, using pen and paper is the best way to implement this type of cryptography or some time by using simple mechanical aids. The development of mechanical and electromechanical instruments such as the Enigma rotor machine in the early 20th century leads to making cryptography more sophisticated and more efficient. The new developments in electronic systems and the fast revolution in the computing field make encryption methods more complex. On the other side, the progress in cryptography methods and instruments paralleled with the increase of cryptanalysis (breaking of encrypted media) methods. The multimedia files such as text, audio, image, or video can be protected by security systems and these security systems can be divided into cryptography and information hiding. Cryptography is used to code the information while information hiding is the concealing of information files inside the cover files and there are two main types of data hiding which are watermarking and steganography. The main difference between these security systems is the applications they design for them. Figure 2.1 illustrates these security systems.

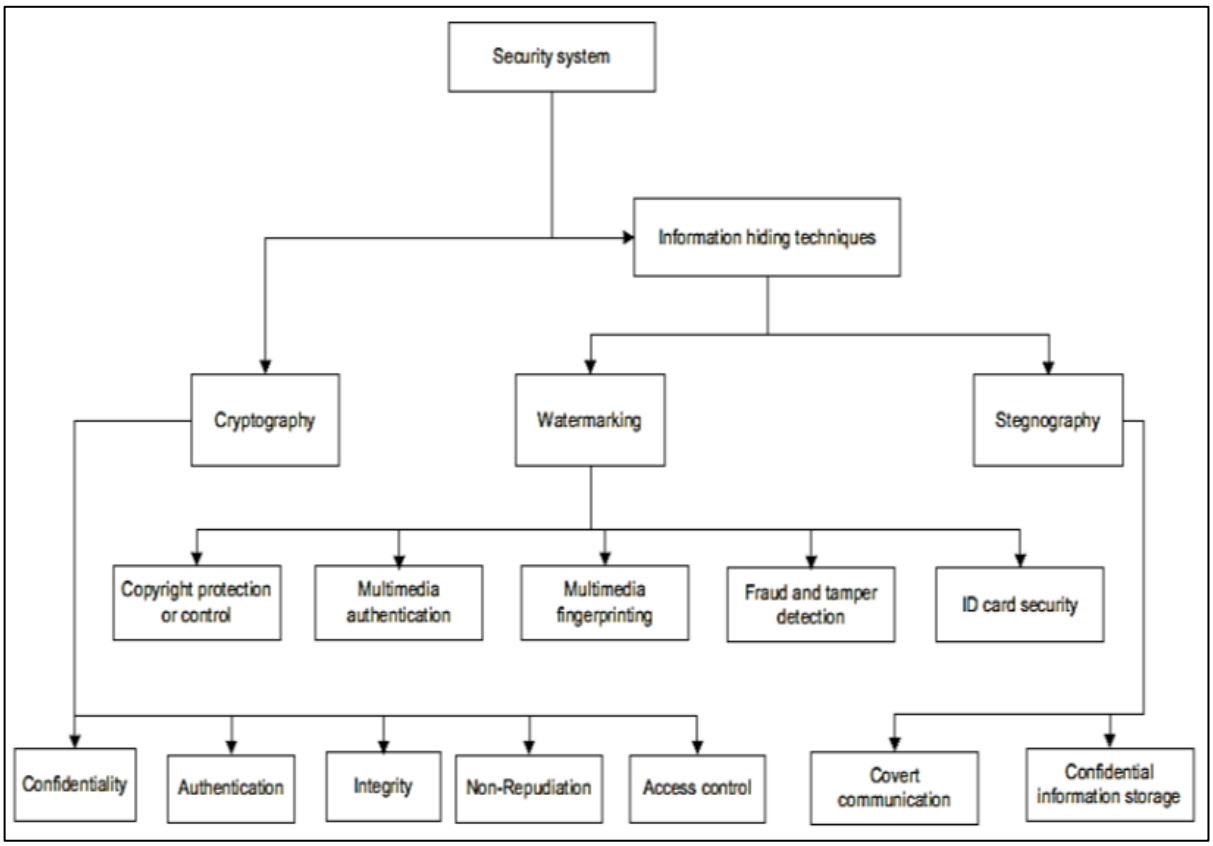


Figure 2.1: General Classifications for Security Systems [44]

2.1 CRYPTOGRAPHY DOMAINS

Implementation of a cryptosystem can be done in different domains such as spatial, frequency, and hybrid domains. Each of these domains can be explained as follows.

2.2.1 Spatial Domain

In the spatial domain, the pixel information in terms of pixel value and location in the plain image will be considered to perform the encryption procedure directly on this pixel. The image encryption function can be expressed as shown in Equation 2.1.

$$E(x, y) = f[I(x, y)] \tag{2.1}$$

Where (x, y) is the output encrypted image, $I(x, y)$ is the input plain image, f is the encryption

function applied on the plain image over the (x,y) neighborhood. The spatial domain is the original image space in which any changes in the scene S will directly cause equal changes in the captured image I. Distance in S (in any distance unit) is represented by pixels inside I.

2.2.2 Frequency Domain

In the frequency domain (also called the transformation domain), the cover image is analysed arithmetically to a string of frequencies (transformation channels), these transformation channels have two major ingredients which include the amplitudes and the phases shifting. In all alterations within the spatial domain, the cover image outputs indirect will alteration in its presentation transformation domain. The transformation domain is partitioned into main two ingredients and these ingredients are (high-frequency) ingredients that present as sharp edges and noise of the original image whilst the (low-frequency) ingredient corresponds to the smooth regions.[53].

2.3 CHQOS-BASED IMAGE ENCRYPTION

Chaos-Based or chaotic image encryption is an implementation of image encryption depending on mathematical chaos theory. This encryption technique is very safe to encrypt images before transferring over the internet and open networks. The cryptography researchers gave great effort to obtain a secure and efficient random number generator to encrypt the messages. Chaos theory was discovered in 1969 by Edward N. Lorenz. By 1970, chaos theory has established in many research areas such as physics, mathematic, biology, engineering, philosophy, and economics [54]. Because there is no common acceptable mathematical definition for chaos, it can be said the dynamical system is chaotic if it has the following properties:

a. It must be topologically mixing.
b. It must be very sensitive to initial condition and control parameters.
c. The periodic orbit of the dynamical chaotic system must be dense.

The topologically mixing property is to ensure the chaotic map ergodicity; this means if the state space is partitioned into regions with a finite number, all maps' orbits will pass through all of these regions. The sensitivity to the initial conditions and control parameters means any alight

changes in these inputs should produce output with a significant difference [55]. Since the 1990s, researchers in the cryptography field noticed that there is a close relationship between cryptography and chaos. The difference between chaos and cryptography is chaos is useful in a continuous field while cryptosystem is implemented in a finite system. Although that the cryptosystem and chaos are closely related, many chaos properties such as sensitivity to initial conditions and mixing, actually match with the cryptography properties. Table 2.1 illustrates the coincide between chaos and cryptography.

Table 2.1: Properties Coincide between Chaos and Cryptography.

Chaotic system	Cryptography Algorithms
Phase space: set of real numbers	Phase space: finite set of integers
Sensitive to initial conditions and parameters	Diffusion
parameters	Key
Iterations	Rounds

2.4 CONFUSION AND DIFFUSION

Shannon in 1949 suggested a process of diffusion and confusion to achieve an ideal security system in his famous paper entitled (communication theory of secrecy systems). The main aim of this suggestion is to deter statistical attacks. In image encryption, the meaning of diffusion process is the changing of image pixel values in proper way to diffuse the frequencies of these image pixels of the plain image over several pixel values of the cipher image, to achieve cipher image free of statistical features such as histogram or information entropy, to make meaningful statistical attack much more cipher images are needed. While in the confusion process the image pixel's location will be changed to cancel the relationship between the plain and cipher image [56]. By implementing the confusion process the key seems to be not related simply to the cipher image and each pixel in the cipher image should depend on part of the key [57].

2.5 CRYPTANALYSIS

Cryptanalysis can be defined as a technique used by attackers or hackers to break coded data without prior knowledge about the used key. Cryptanalysis is derived from the Greek word kryptós which means “hidden” and the word analýein which means “to unite” or “to lose”. It is used to decrypt the cipher information by analyzing the flow in the used algorithm to understand the hidden aspect included in the system [58]. Friedrich Kasiski considers as the first one who broke the Vigenere cipher at World War I. Before that, the Vigenere cipher was used for about two centuries to communicate securely [59]. To hander, the cryptanalysis attacks asymmetric cipher was introduced at last decades. In this type of cryptography, there are two keys (private and public keys) and the key was increased dramatically as in 1980 the key space was 150 digits then early at the 21st century the key space increased to be 700 digits. After the ending of the world war, all governments have their own agency or cryptographer team that is responsible for the decoding of cipher messages by implementing the cryptanalysis methods [60].

2.6 RANDOM KEY GENERATING

The main issue in the random function is the key, which is reflecting how to start generating random numbers from the beginning without repetition. The random key considers the first step to start generating other numbers in the series. A key is used to encrypt and decrypt whatever data is being encrypted /decrypted [61]. A program used to generate keys is called a key generator. The secret key is mandatory for encryption algorithms and the success of encryption is dependent on it, even it considers more important than the encryption algorithm itself, this is because of three reasons which are: The encrypted message cannot be decrypted without knowing the correct secret key, brute-force can be hander by increasing the keyspace size, and encryption with strong key is difficult to be attack and vice versa [62]. The used keys should be absolutely independent of the content of the plain text and the use of different keys lead to producing different ciphertext for the same plain text. This can be achieved only by using the correct key. The secrete key is divided into the public-key algorithm and the private key algorithm. The public key algorithm or asymmetric encryption algorithm used one key for the encryption process which is called the public key while the second key is used for the decryption

process. The public key will be distributed to all network users while the decryption key or private key is only owned by the related recipient [63]. In symmetric-key encryption algorithms, the key used in the encryption process is the same key used in the decryption process. Therefore, it is known only by the sender and receiver, and it should be maintained. The sensitive issue for the symmetric keys is that they should be always secret [64]. Thus, it should be highly protected and shared securely. The implementation of the symmetric keys is broadly used in the image encryption field. Figure 2.2 explains the encryption and decryption process in symmetric and asymmetric encryption algorithms. The public key algorithms need more complex computations; therefore, it is not preferred in the field of multimedia protection [65].

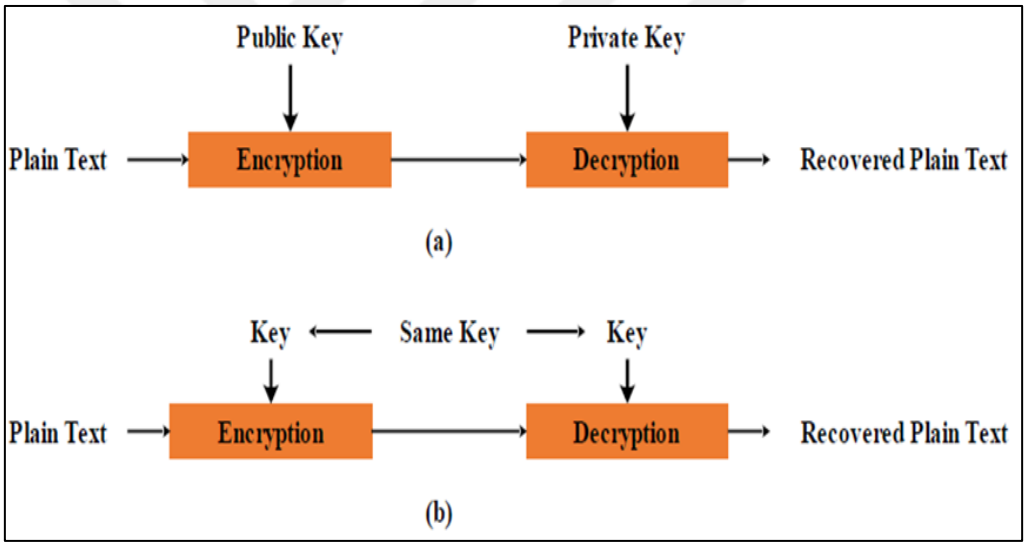


Figure 2.2 Encryption Key Types (a) Asymmetric Key (b) Symmetric Key.

The key generating methods can be described by the traditional encryption algorithms such as AES, RC4, and RC5. Random number generation is the generation of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance, usually through a random-number generator [66]. The distribution of the random keys reflects the behavior of the generated random numbers. The chaotic maps are unpredictable sequences of real numbers that can be normalized to be between 0 and 1. A distribution of values is clustered around an average (referred to as the “mean”) is known as a “normal” distribution or it can also be called the

Gaussian distribution [67]. In terms of entropy, the quality of image encryption is commonly measured by the information entropy over the ciphertext image. The expression of the degree of uncertainty in a system can be measured by the information entropy parameter [2] Sometimes entropy is defined as the degree of randomness or disorder in the system, therefore information entropy is suitable for use in the evaluation of image encryption systems [68]. Information entropy indicates the distribution of colors in an image and a good, ciphered image is an image with an equal distribution of color values or gray values in grayscale images. According to Stoyanov and Kordov [69], they consider the following assumptions:

"Let us consider that there are 256 values of the information source in red, green, blue, and grey colors of the image with the same probability. We can get the perfect entropy H(X) = 8, corresponding to a truly random sample". The differential analysis is another issue in the field of image encryption. In differential analysis, the cryptanalysis may make a slight change (e.g., modify only one pixel) of the encrypted image, and then observes the change of the result [70]. In this way, he may be able to find out a meaningful relationship between the plain-image and the cipher-image. If one minor change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then this differential attack would become very inefficient and practically useless [71].

2.6.1 Random Key Generating in AES Algorithm

Advanced Encryption Standard (AES) is a block symmetric cipher designed to be used instead of Data Encryption Standard (DES) and it is adopted for encrypting data in many applications. It has a variable key length of 128,192 or 256 bits and the size of the encrypted data block is 128 bits, the encryption process is within 10, 12, or 14 rounds which depend on the key size. AES encryption algorithm is flexible and fast for the block cipher, it can be implemented in various models such as CBC, ECB, OFB, CFB, and CTR. They work in certain operation modes as a stream cipher [72]. In the AES algorithm, the key used for encryption is the same used for decryption, and it only accepts a block size of 128 bits, therefore AES is considered a symmetric block cipher [73]. There are three versions of the AES algorithm (AES-128, AES-192, and AES 256) each one of these versions has its own name which is driven by the used key size [74]. In

addition, the number of needed rounds to implement this encryption algorithm is dependent on the key size i.e., if the key size is 128 the number of rounds is 10 while for key sizes 192 and 256 the round's number is 12 and 14 respectively. Figure 2.3 demonstrates the operation of the AES encryption algorithm [28].

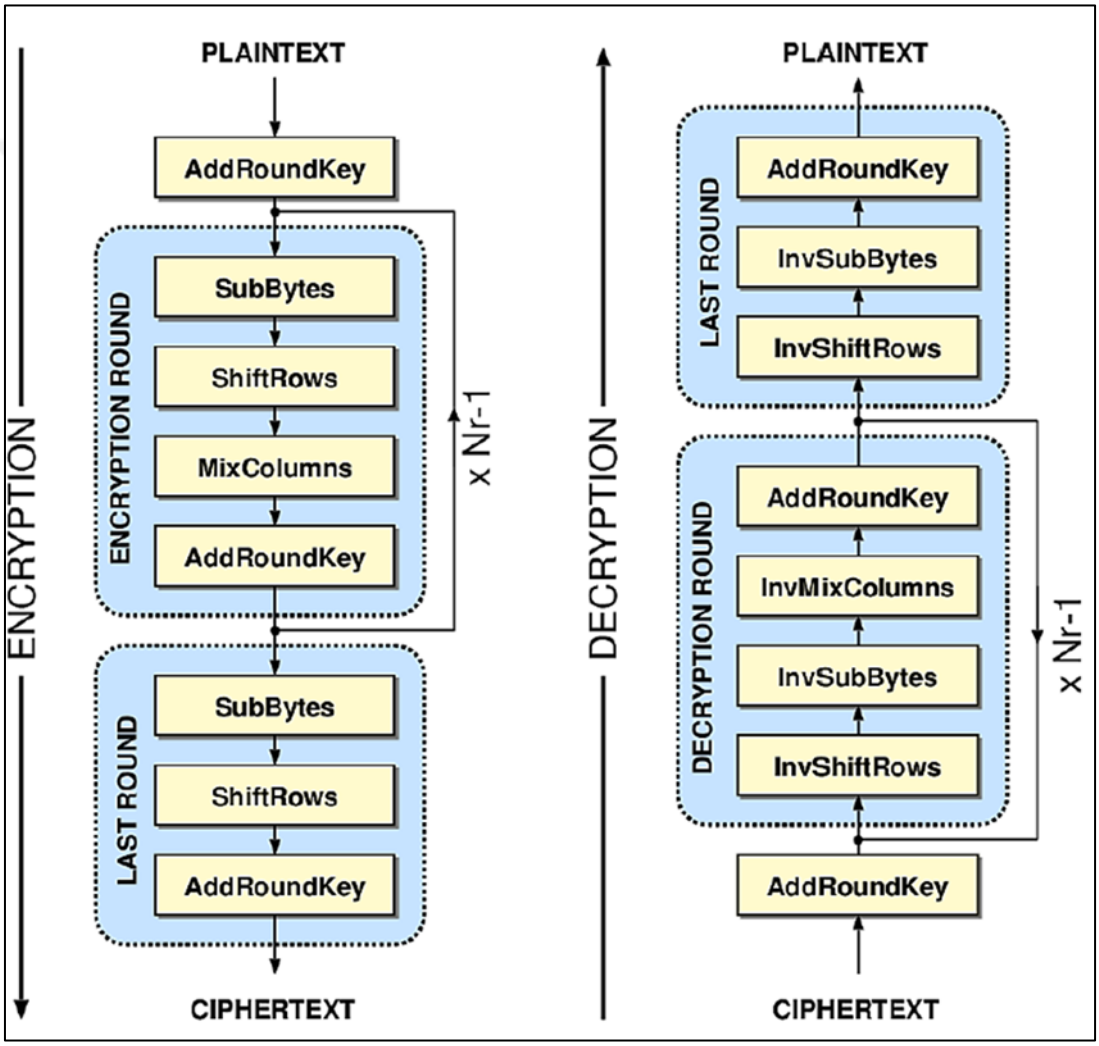


Figure 2.3 General Flowchart of AES Encryption Algorithm [28]

A new image encryption method was introduced by Ran et al. [44] by integrating several encryption methods including AES, Blowfish, RC6, and Serpent, the sensitive blocks are encrypted in this method while four different patterns are used to rescan the insensitive blocks. Based on the importance, and by using edge detection technique each block is classified into

significant or insignificant classes. To reduce the computational cost and to maximize the protection for sensitive information this algorithm applies different security levels for each block class. The small predictability level will prevent the attacker to snap off any information about the cipher image [26].

2.6.2 Secret Key of RC5 And RC6 Algorithms

RC5 consider as a parameterized encryption algorithm, RC5 is flexible in both security level and performance characteristics, because in this encryption algorithm all of the numbers of rounds, block size, and key size are variables [40]. Simplicity is the most important feature of RC5 and the encryption process is based on three operations: addition, exclusive-or, and rotation. Simplicity in design and simplicity in the analysis is provided by the RC5 design. In addition, heavy use of the rotations of data-dependent is another characteristic feature in the encryption, and this is very useful in the hindering of linear and differential attacks. Rivest [65] is the official name of the RC5 stream cipher, it is more efficient and more useable in the real-time fields and based on random permutation implementations. According to a different analysis, the period number of the cipher is more than 100. Due to their absolute performance, RC4 and RC5 become members of the cryptographic community. The basic flow process of RC5 is shown in Figure 2.4.

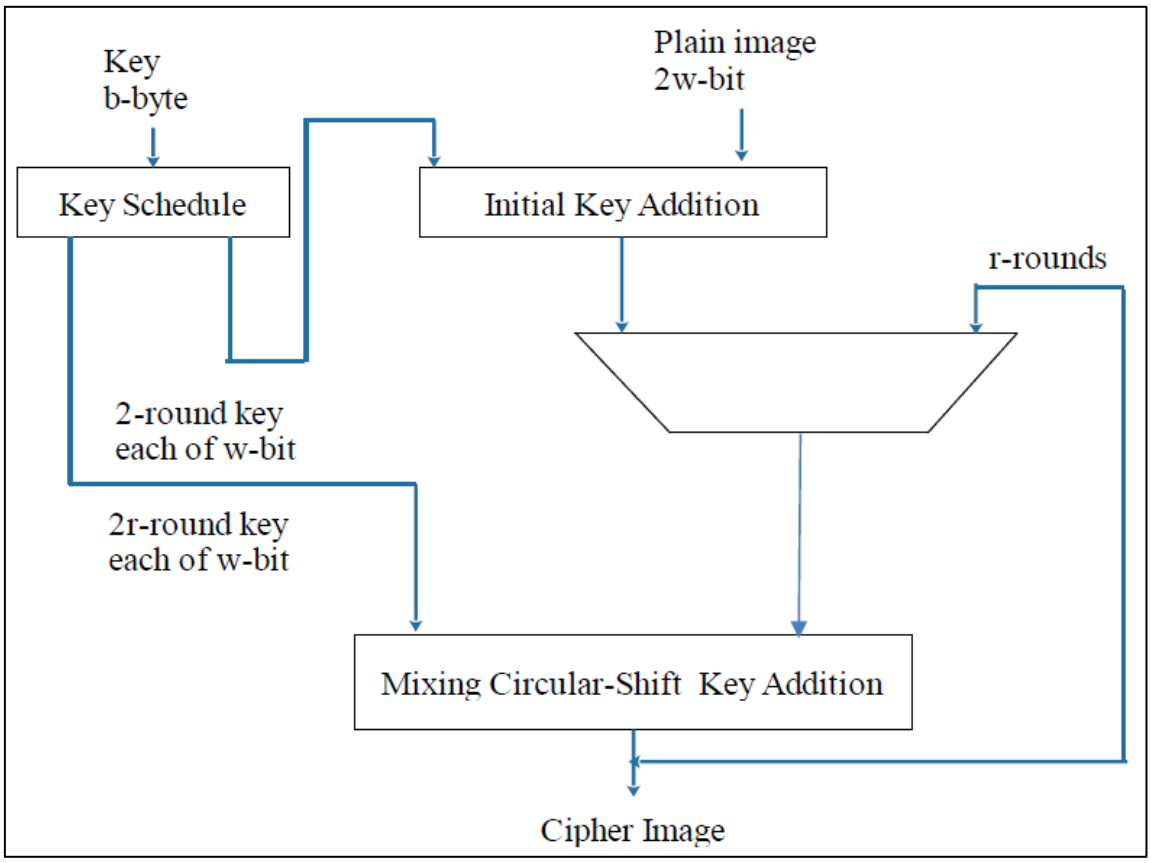


Figure 2.4: General Block Diagram for RC5 Algorithm [44]

A partial and fast image encryption technique was proposed by Sasidharan and Philip [31] this technique is based on DWT and RC4 stream cipher. In this technique, the image is converted into the frequency domain using DWT and the approximation matrix (low-frequency band) was used to protect the critical image information by implementing the RC4 algorithm, the rest image information is shuffled by the using shuffle algorithm. An XOR operator is implemented between the low-frequency band component and the RC4 keystream. Two issues were achieved by implementing this technique, which is reducing the required time by encrypting part of the image and increasing the security by shuffling the rest image. Faragallah [21] use RC5 to encrypt the images by extracting the image header and dividing the image data into 16-bit blocks. RC5 is performed on all 16-bit blocks sequentially until the end of the bitstream of image data. The secret key is developed as n random binary words sequence which consists of three simple

algorithms (initialization, mixing, and conversion). Table 2.2 show a summary of the key space size for AES, RC4 and RC5 encryption Algorithms.

Table 2.2: Summary of Key Space Size of Traditional Encryption Algorithm

Traditional Algorithm	Key Space Size
AES	128
RC4	Variable
RC5	Variable & > 100

Other researchers suggest their own random generators such as Jallouli et al., [50] the proposed a new pseudo-random number generator based on three chaotic maps Skewtent, Piece Wise Linear Chaotic (PWLCM), and Logistic maps, these maps are weakly coupled and implemented with finite precision. A chaotic multiplexing technique is also included. The proposed pseudo-random number generator is achieved by iterating three chaotic maps which are Skewtent, PWLCM, and Logistic maps by coupling them weakly with a coupling matrix. Also, a technique of chaotic multiplexing is used [54]. The proposed pseudo-random number generator uses three initial conditions (one for each map) also the control parameters for the used maps and coupling matrix must be specified. All of the initial conditions and control parameters were initiated by the use of the Linux kernel [3]. New pseudo-random number generator algorithm proposed by Hanis et al., [71] the new key is generated by using a novel modified convolution and chaotic mapping technique. First of all, initial condition and control parameters for the logistic map are specified to generate two random sequences, after that a convolution process is implemented on these two generated sequences to produce a new random sequence. The convolution is done on the binary sequences therefore it can be said the process is a binary convolution. The distribution of the random keys reflects the behavior of the generated random numbers. The chaotic map is an unpredictable sequence of real numbers that can be normalized to be between 0 and 1. A distribution of values is clustered around an average (referred to as the “mean”) is known as a “normal” distribution or it can also be called the Gaussian distribution [52].

2.7 EXISTING TECHNIQUES USED IN THE PROPOSED METHOD

Two chaotic maps are used in the proposed confusion method. The chaotic logistic map is modified to be more suitable for the proposed method. Sensitive Logistic Maps (SLM) and Hénon Maps in addition to additive white Gaussian noise are used in the proposed confusion method while in the diffusion method Bernoulli map is modified to Extended Bernoulli Map (EBM) and Tinkerbell, Burger, Ricker maps used to obtain random sequences with better criteria. The following sections explain the chaotic maps and additive white Gaussian noise used in the proposed framework.

2.7.1 Chaotic Logistic Map

Chaos is a general phenomenon that occurs in deterministic nonlinear systems and is characterized by a great sensitivity to the beginning circumstances and unpredictable and random behavior. In 1963, Edward N. Lorenz made the discovery [33]. The logistic map is a second-degree polynomial, and it is a kind of one-dimensional map. The first description for a logistic map was in May 1976, after that it was widely used in image encryption because it is a simple mathematical model with very complicated dynamics [29]. A logistic chaotic map can be described by Equation 2.2.

$$X_{n+1} = rX_n(\mathbf{1} - \boldsymbol{x_n}) \qquad (2.2)$$

where r is the control parameter of the logistic map and r ϵ (0,4), n=1,2,3, … and X1 are the initial conditions or seed value, and its value is (0< X1<1). To turn the logistic map into a chaotic map r must be arranged between 3.5699 and 4 (Liu and Miao, 2016). Figure 2.5 shows the behavior of a logistic map where r=3.99 and X1=0.5.

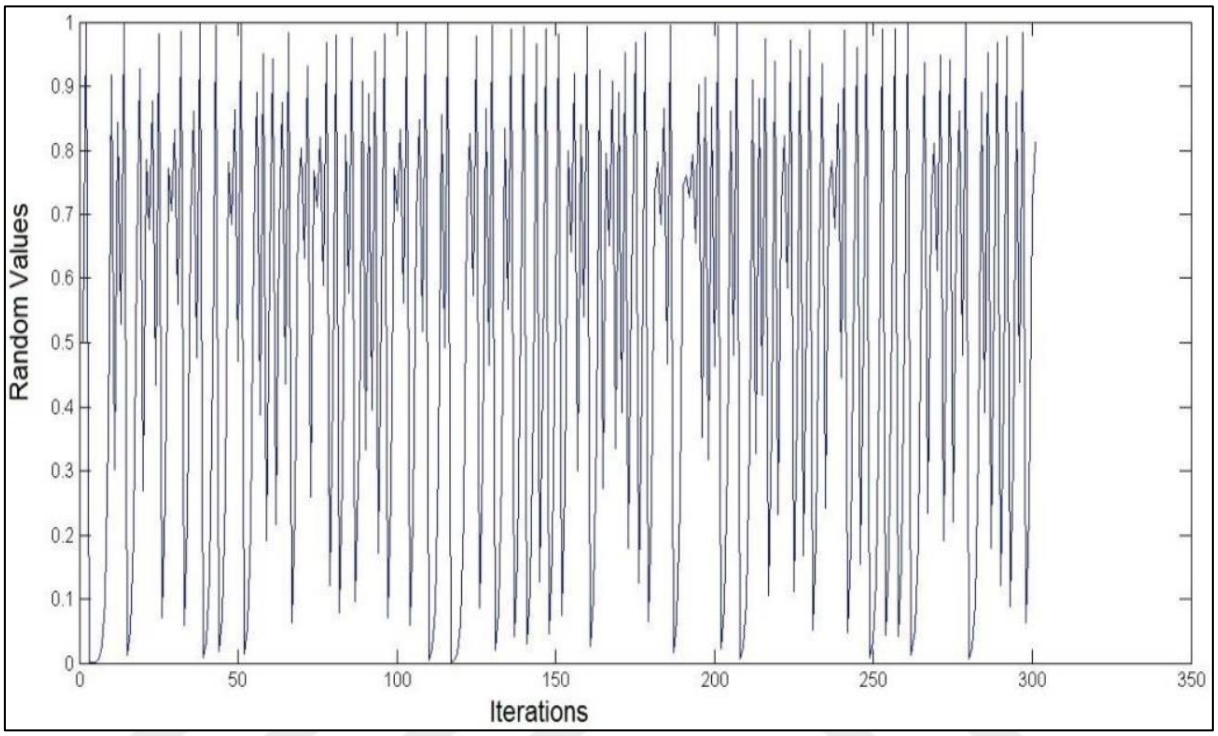


Figure 2.5: The behavior of logistic map [36]

The cobweb diagram of a logistic map illustrates the dynamical behavior of the chaotic logistic map [37] and can be seen in Figure 2.6.

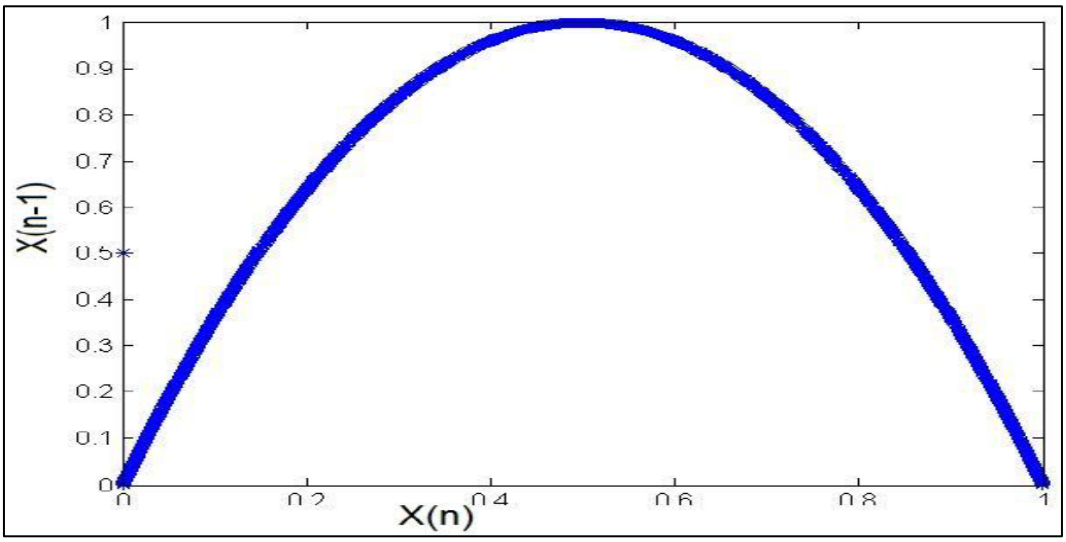


Figure 2.6: The cobweb diagram of the logistic map [37]

A cobweb diagram is a visual tool used in mathematics to study the behavior of dynamical systems and one-dimension iterated systems such as chaotic maps [36].

2.7.2 Hénon Map

The Hénon map was introduced by Michel Hénon as a simplified model of the Lorenz model [33], and due to the good chaotic behavior and specifications of the Hénon map, especially its high sensitivity to initial conditions [33], it is considered one of the best dynamical systems. This is demonstrated by Equation (2.3) and Equation (2.4).

$$X_{n+1} = 1 - aX_n^2 + Y_n \quad (2.3)$$

$$Y_{n+1} = bX_n \quad (2.4)$$

where a and b are the control parameters and X, and Y are the initial circumstances. T*h*e sy*st*em achieves strong chaotic behavior when (a = 1.4 and b = 0.3). The Hénon map response to initial conditions with control parameters (a=1.4, b=0.3) is shown in Figure 2.7.

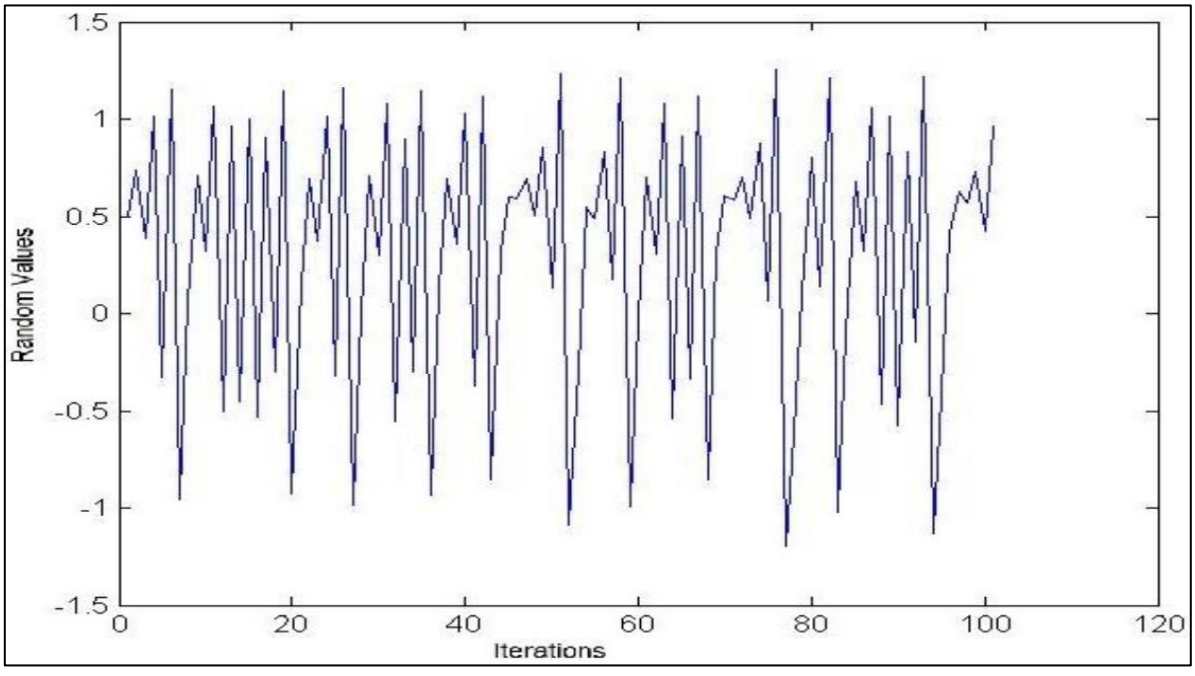


Figure 2.7: Hénon Map Response [43]

The Hénon map converges to a strange attractor. This attractor can be visualized by considering arbitrary initial conditions using computer code [43]. The plotting between Xn and Yn used to obtain the attractor is shown in Figure 2.8.

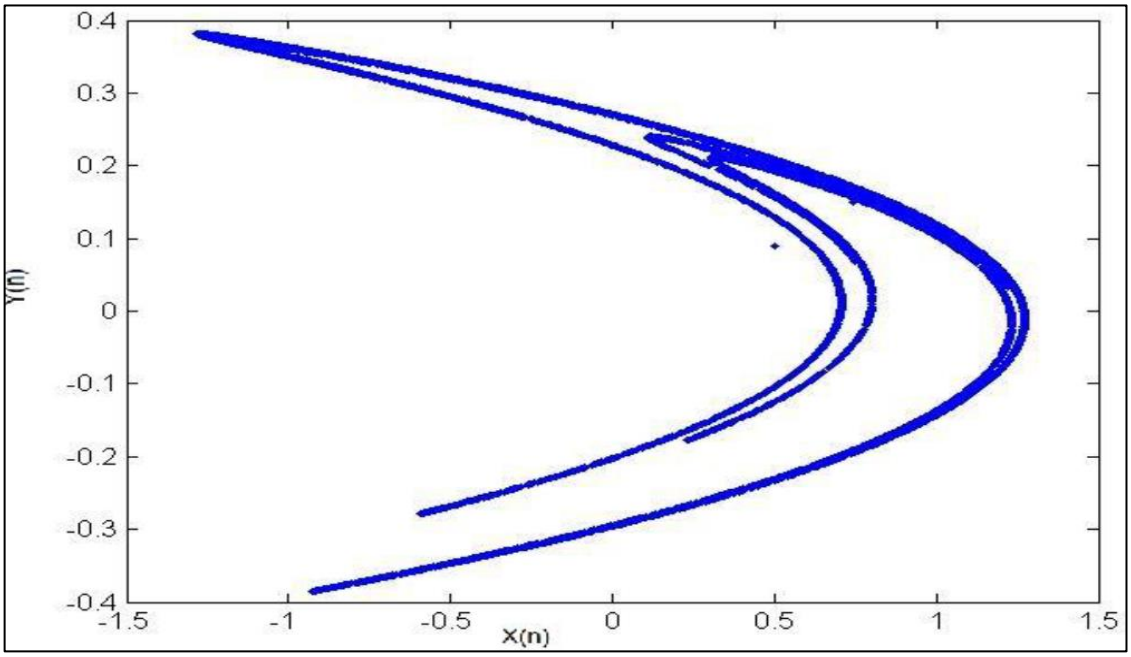


Figure 2.8: Hénon Map Attractor [43]

2.7.3 Additive White Gaussian Noise (AWGN)

The goal of this study is to design image encryption systems with high criteria and to achieve this goal various issues must be considered [45]. The removal of the statistical properties of the cipher image is very important and correlation is one of the most important of these statistical properties. To dissolve correlation between adjacent pixels of the plain image, and because whole image encryption is fully controlled by a random key, the random number generator must have a minimum correlation. Thus, additive white Gaussian noise was used to achieve this objective, because there is a zero correlation between the values of this type of noise [44].

Noise is undesirable, inevitable, and corrupts the visual quality of the acquired images [44]. There are several types of noise such as salt and pepper, Gaussian, Shot, and anisotropic noise.

Gaussian noise is one of the most important noise types and it is defined as a statistical noise with probability density functions similar to the normal distribution [45]. Sometimes Gaussian noise is defined as noise with a distribution of Gaussian amplitude. The Gaussian noise distribution function is explained by Equation (2.5).

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (2.5)$$

where σ and μ are the standard deviation and the average of the noise, respectively. When μ is equal to zero will produce AWGN, which is considered a special type of Gaussian noise. The effect of AWGN on a sine wave is shown in Figure 2.9.

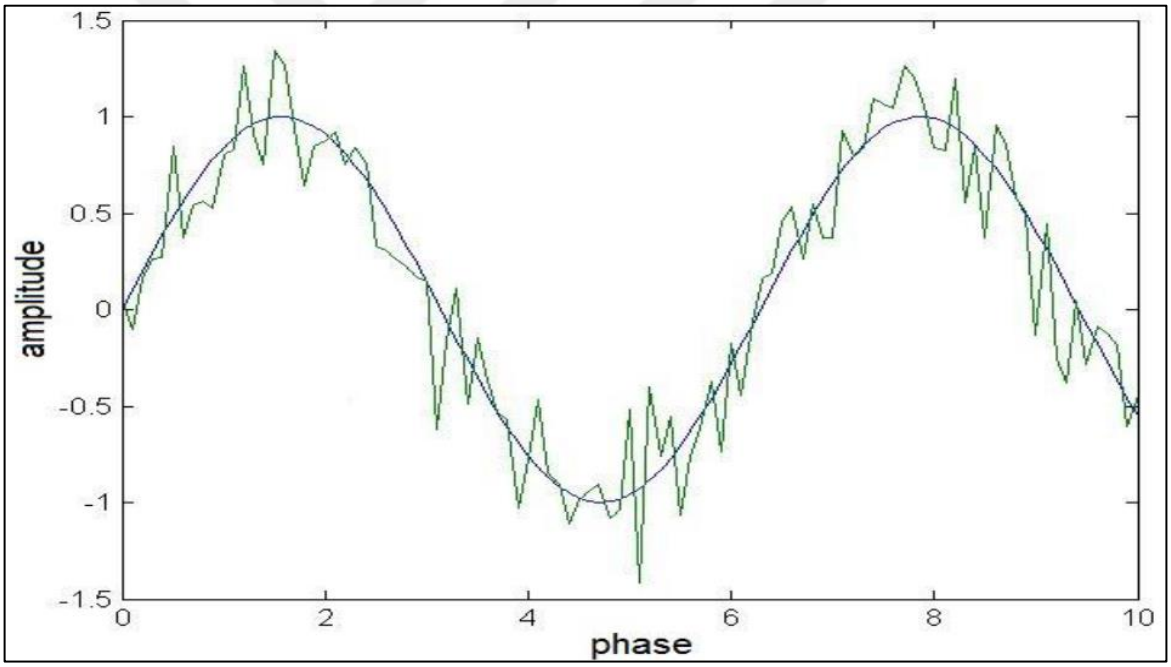


Figure 2.9: The effect of AWGN on a sine wave [45]

As shown in Figure 2.9, the average AWGN is equal to zero and there is no correlation between these values. All image pixel values will deviate from their original values when AWGN is implemented for this image [43]. Equation 2.6 shows the process of such implementation.

$$I(X,Y) = I_0(x,y) + N(x,y) \quad (2.6)$$

Where Io is the original image, N is the AWGN, and I is the resulting image at location (x, y).

2.7.4 Bernoulli Map

For all dynamical systems, Bernoulli maps transform inputs as an output value for use as new input values for the next iteration []. Famously known as dyadic transformation, doubling map, or saw tooth map and it can be written as seen in Equation (2.7). The response of Equation (2.7) is shown as in Figure 2.10, and the behavior of the successive iteration (cobweb diagram) is seen in Figure 2.11.

$$X_n = (2 * X_{n-1}) mod\ 1 \qquad (2.7)$$

The response of Equation (2.7) is shown in Figure 2.10.

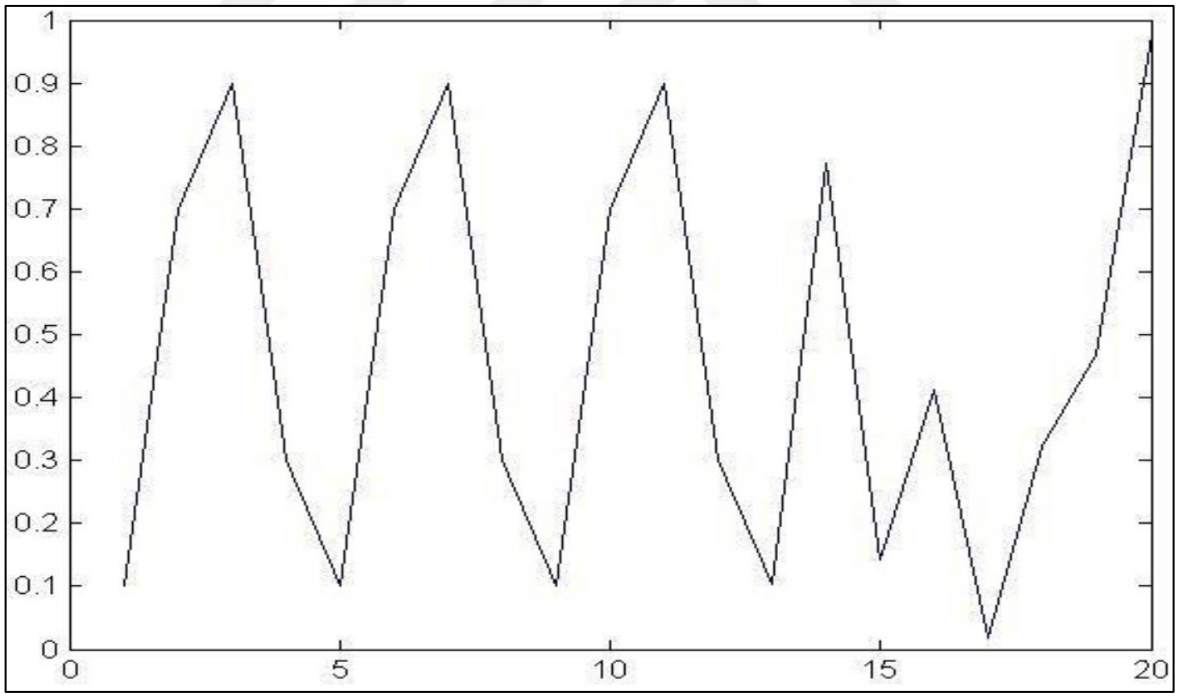


Figure 2.10: Bernoulli map response [62]

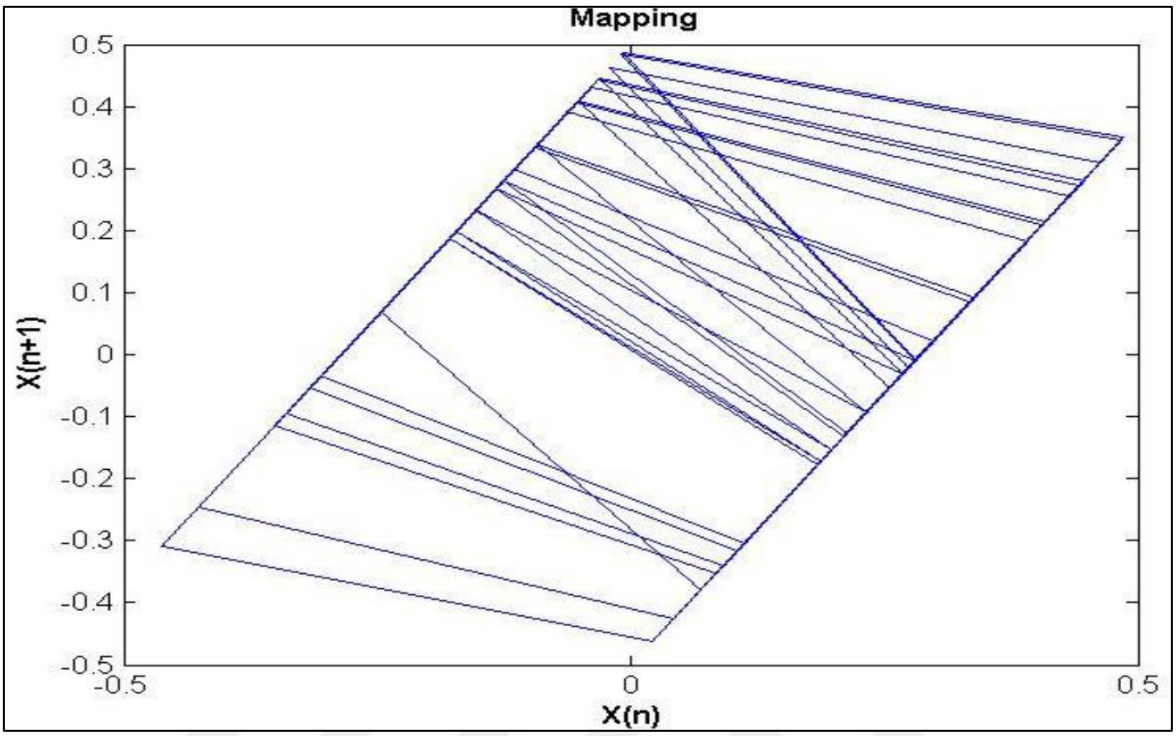


Figure 2.11: Bernoulli successive iterations behavior [62]

As seen in Equation (2.7), Bernoulli maps use one secret key as an input for the random number generator, which considers relatively short keys and is easy to be attacked by brute force. To avoid such weakness an amendment was proposed in this study [63].

2.7.5 Tinkerbell Map

A Tinkerbell Map is a discrete Two-Dimensional system that is generated by implementing Equation (2.8) and Equation (2.9) [63] [64]

$$X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n \quad (2.8)$$

$$Y_{n+1} = 2X_n Y_n + cX_n + dY_n \quad (2.9)$$

Both the response and the behavior of successive iteration of Equation (2.8) and Equation (2.9) are seen within figure 2.12 and figure 2.13, respectively.

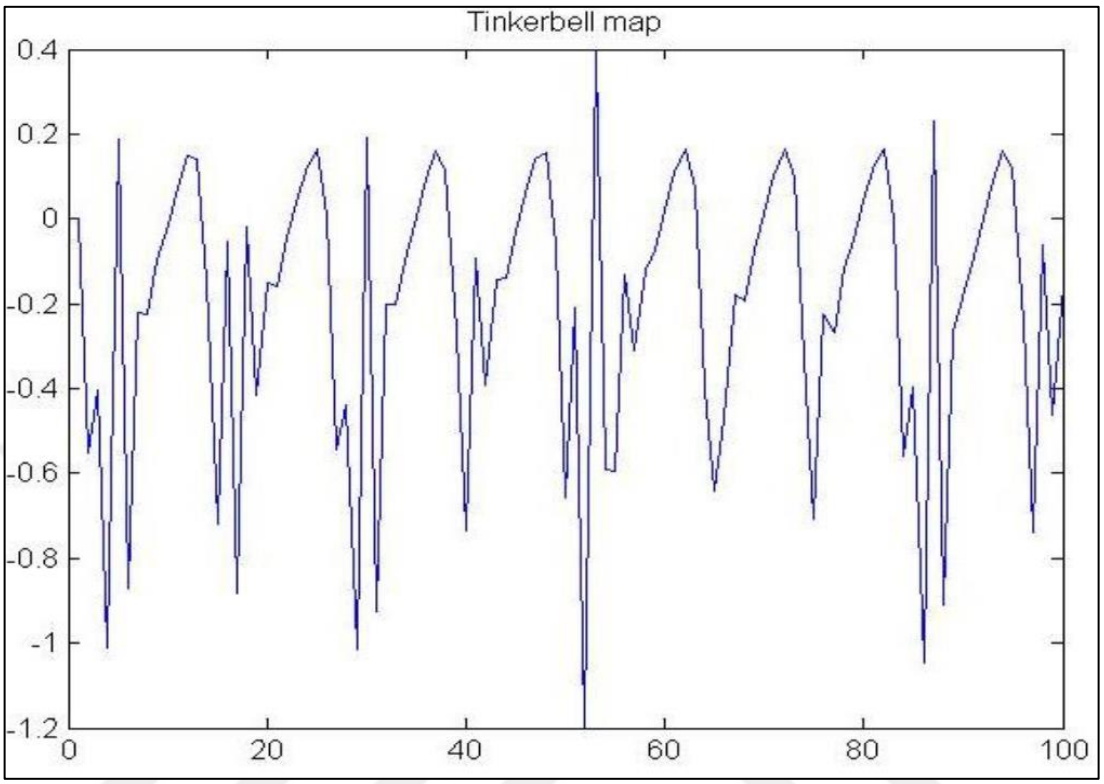


Figure 2.12: Response of Tinkerbell Map [59]

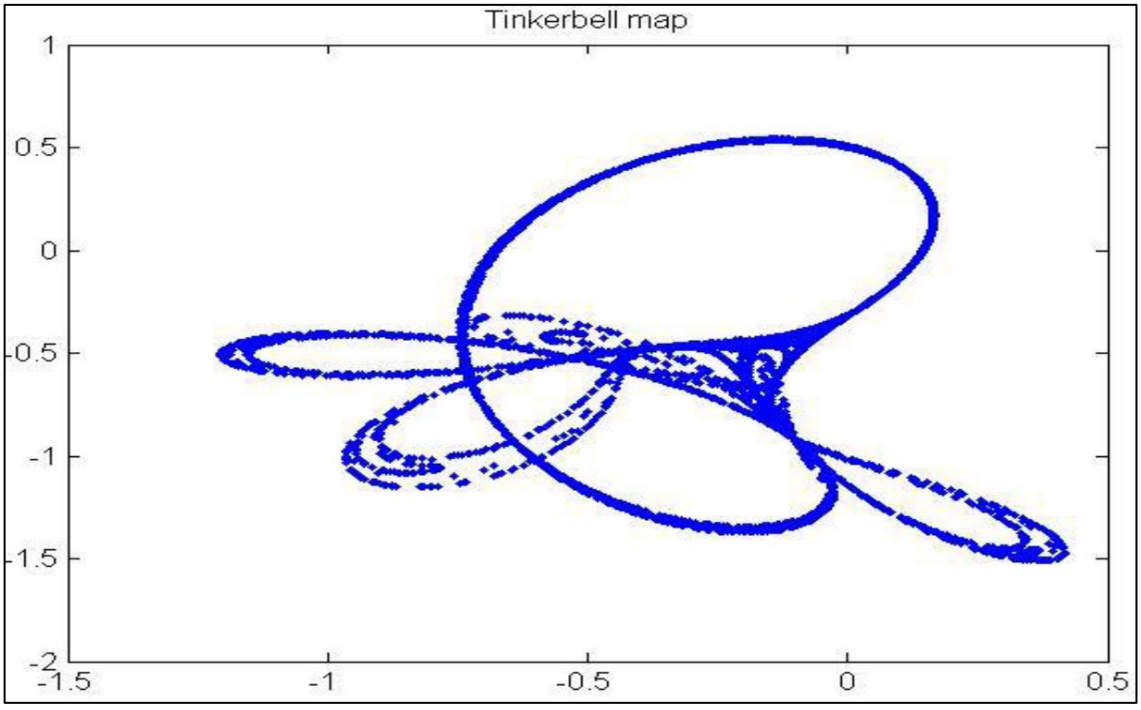


Figure 2.13: Behavior of Successive Iteration of Tinkerbell Map [57]

The origin name of Tinkerbell is unknown, but the behavioral drawing of successive iterations shown in Figure 2.13 is similar to the movement of Tinker Bell over Cinderella castle in the famous Disney cartoon. Equation (2.8) and Equation (2.9) were studied as a special case in detail by Nusse and Yorke [58] and they found that 64 periods, 10 unstable periodic orbits, and one strange attractor when the parameters of both above mentioned equations are (a = 0.9; b = −0.6; c = 2; d = 0.5) [58].

2.7.6 Burgers Map (BM)

A BM is produced by the discre*tiz*ation of the pair of diff*ere*ntial equations. It used to explain the importance of bifurcation in hydrodynamic flow, Equation 2.10 and Equation 2.11 are Burger's map equations and there are two control parameters that control the behavior of this map.

$$X(n+1) = (a * Xn) - (Yn)\text{^}2 \quad (2.10)$$

$$Y(n+1) = (b * Yn) - (Xn * Yn) \quad (2.11)$$

These two equations exhibit chaotic behavior when a = 0.75 and b = 1.75. The chaotic behavior is seen clearly in the response plot shown in Figure 2.14 and the plot of successive iteration behavior is shown in Figure 2.15.

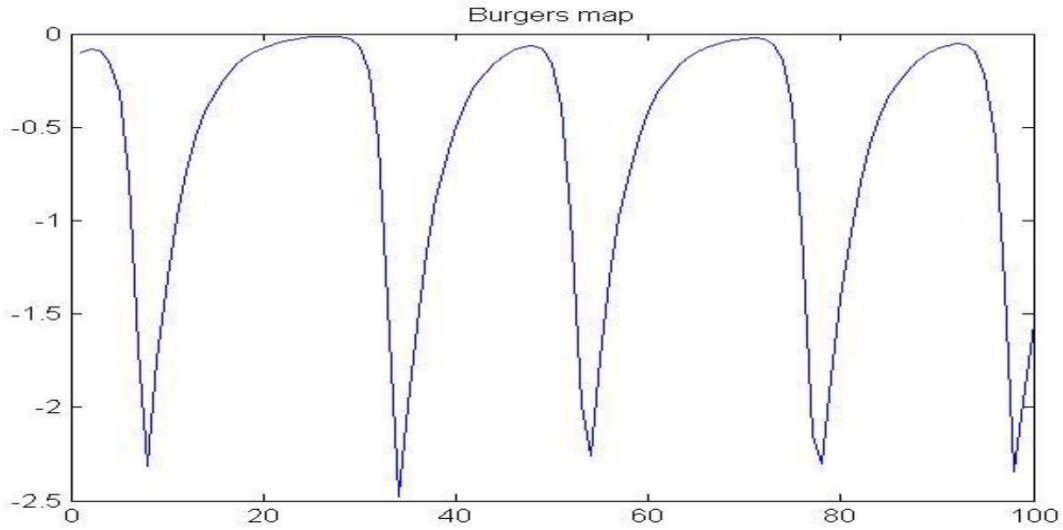


Figure 2.14: Chaotic Response of Burgers Map [22]

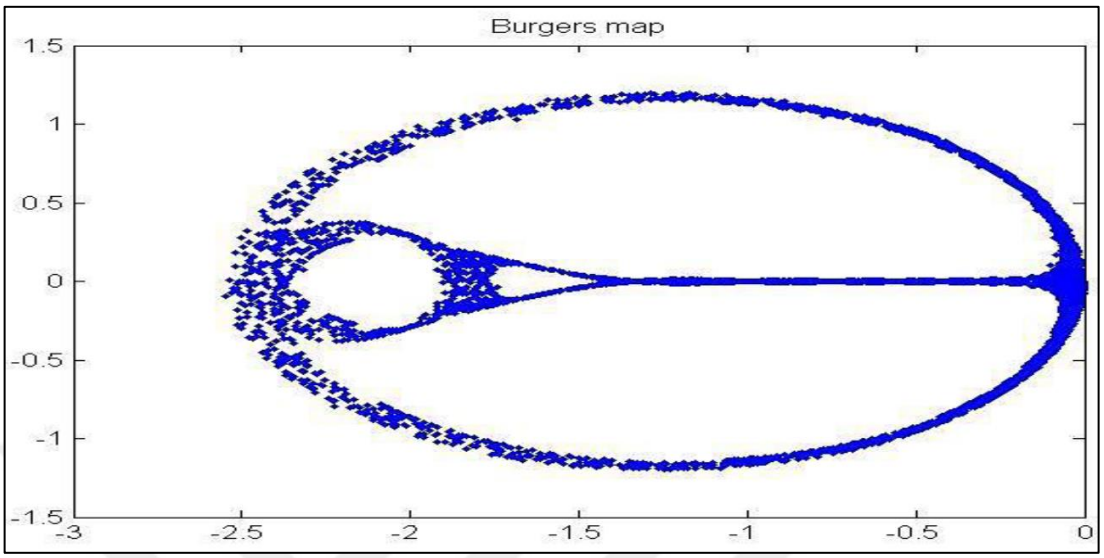


Figure 2.15: Chaotic Behaviour of Successive Iteration of Burgers Map [22]

2.7.7 Ricker Map

There is a long history of using Ricker models to study the dynamics of single-species populations [23]. W. E. Ricker was an important founder of fisheries science. He proposed the Ricker model in 1954 to predict the number of fish that will be present in a fishery and this model is expressed in Equation 2.12.

$$X_{n+1=}X_n e^{r(1-\frac{X_n}{k})} \qquad (2.12)$$

where r and k are control parameters (controlling growth rate and carrying capacity, respectively). The behavior of Equation 2.12 becomes unstable when (r > 2) and the dynamics of the Ricker model become oscillatory in the second period. Sufficiently increasing the growth control parameter (r) leads to unpredictable dynamics (chaotic). The response and behavior of successive iterations of the Ricker map are seen in fig*ur*e 2.16 and fi*gur*e 2.17, respectively.

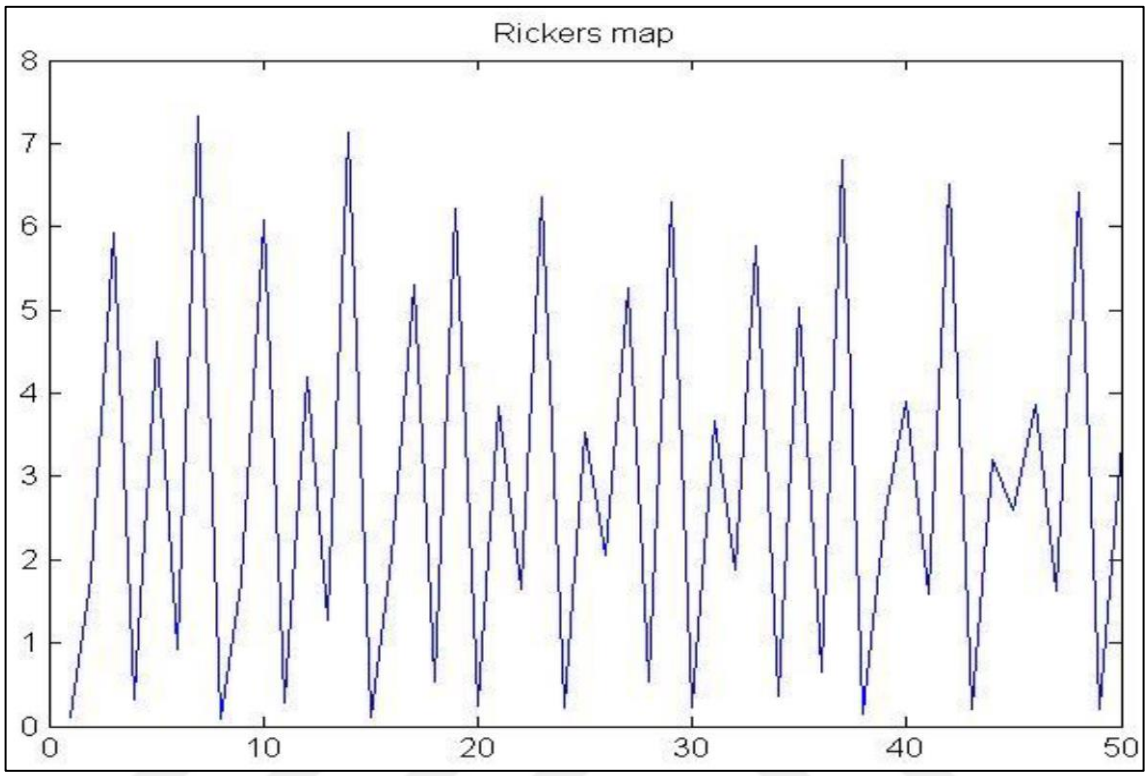


Figure 2.16: Response of Ricker Map [23]

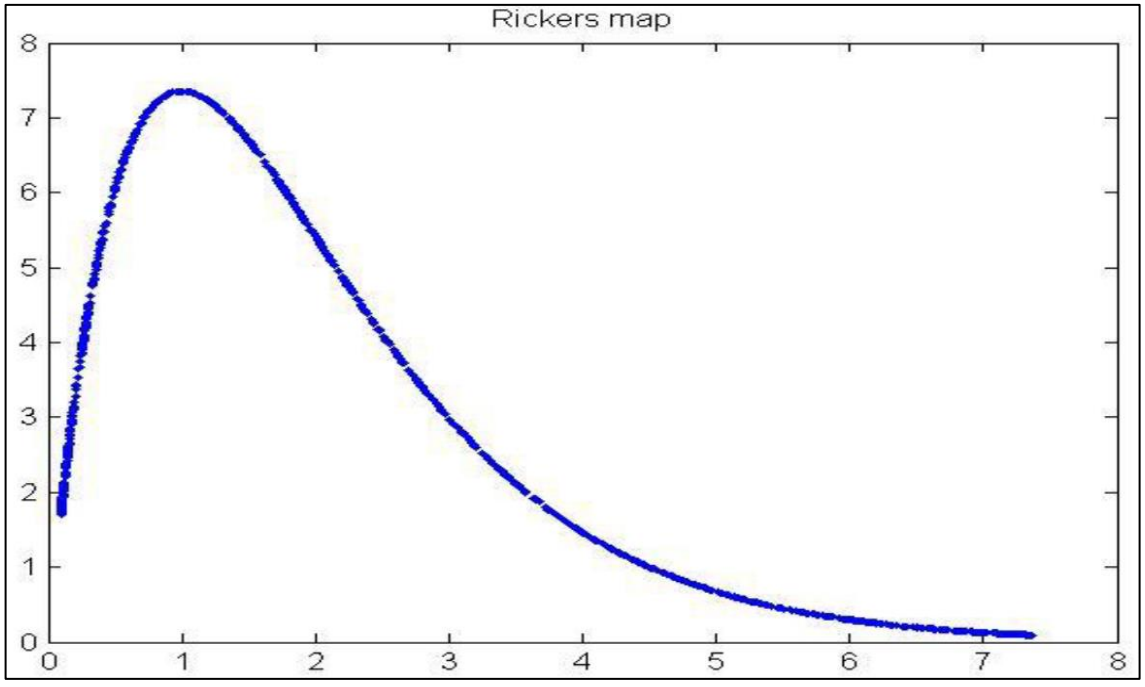


Figure 2.17: Behavior of Successive Iterations of Ricker Map [23]

The image encryption process mostly contains two main stages which are confusion and diffusion, with the proposed method one more stage added to the main framework [24]. The first stage of confusion involved two sub-process, previously random generators suffer from weaknesses in randomness and size of keyspace, with the proposed method random functions become strong and unpredictable especially in terms of keyspace size to make solving like this function almost impossible. The same meaning with the confusing process and correlation of adjusting pixels also improved with the proposed method, not like literature studies. With reference to the diffusion stage same as the previous stage when considering a strong random function [23]. In addition, to improve by adding Internal Interaction between Image Pixels. The most important difference with previous studies is one extra stage to improve image encryption. This stage includes idealizing the histogram to be in alignment for tackling the attacker and increasing the entropy value till reaches 8 value which is considered the top best value.

2.8 IMAGE ENCRYPTION TECHNIQUES

Several traditional image encryption techniques will be summarized in this chapter, this discussion will focus on the full image encryption frameworks. As mentioned earlier full image encryption type is divided into spatial, frequency, and hybrid domains, and Table 2.3 will be summarized the existing methods.

Table 2.3: The summarized of existing methods.

Authors/Year	Method	Dataset	Performance	Remarks
(Yadav *et al.*, 2013)	Three phases. -Use hash function to generate shift table. -Use the generated table in the rows and columns shuffling -Use AES algorithm for encryption process	RGB 300X300	Speed: 0.703s NPCR:99.6689 UACI:27.7599 Key Space: N/A Correlation: -0.041 Entropy: 7.9985	-Fast encryption -High resistance to differential attack -because of only one secret are used it is easy to be attacked.
(Wang and Wang, 2014)	Three phases -Generate dynamic S-box based on logistic and Kent chaotic maps. -Divide image into blocks - Encrypt each block by use its S-box.	Grayscale 256X256	Speed: 1.0740s NPCR:99.61 UACI:33.42 Key Space:2256 Correlation: 0.0137 Entropy: 7.9971	-Need for large memory size, due to the use of many S-boxes. - Large Key space make brute force attack infeasible. - Moderate speed.

Table 2.3: The summarized of existing methods. ."tables continued"

(Mishra *et al.*, 2014)	Two phases - Use 2-D cat map to shuffle image - Use 1-D logistic map encrypt image.	Grayscale 128X128	Speed: N/A NPCR: N/A UACI: N/A Key Space: 2112 Correlation: 0.0095 Entropy: 7.9892	-Acceptable key space size. -high key sensitivity. -resist entropy attack.
(Tong *et al.*, 2014)	Three phases -Use feedback register and chaotic map to generate random sequence. -Use 3-D Backer chaotic map to shuffle image pixels. -use the random sequence to encrypt the image.	RGB 256X256	Speed: N/A NPCR: N/A UACI: N/A Key Space: N/A Correlation: 0.0153 Entropy: 7.999	-High security level -fast encryption process -Limit selection of initial condition.

Table 2.3: The summarized of existing methods."tables continued"

(Zhou *et al.*, 2014)	Two phases -Image shuffling. -Encrypt image by using of generated secret key which based on chaotic map.	Grayscale 256X256	Speed: N/A NPCR: N/A UACI: N/A Key Space: N/A Correlation: 0.002 Entropy: 7.9975 7.9971	-Fast image encryption. -Large key space. -Moderate security level.
(Bora *et al.*, 2015)	Three used methods -Blowfish algorithm -Cross chaos method -Blowfish-cross encryption method	Grayscale 256X256	Speed: 86.012s NPCR:99.56 UACI:30.91 Key Space: N/A Correlation: -0.01	-Impossible to retrieve plain image with the key absent. -Not suitable for real time implementations.

Table 2.3: The summarized of existing methods. ."tables continued"

Hua et al .2020	two-dimensional logistic tent modular map (2DLTMM)	Grayscale 256X256	Speed: 0.0779 s NPCR: 99.61 UACI: 33.46 Key Space: N/A Correlation: 0.002 Entropy:7.99841	-Limit selection of initial condition. -Fast encryption - High resistance to differential attack
Xian et al.,2022	Fractal sorting matrix -Global chaotic pixel diffusion	Grayscale 256X256	Speed: 0.0779 s NPCR: 99.60 UACI: 33.4723 Key Space: N/A Correlation: 0.002 Entropy: 7.9971	-High security level -fast encryption process -Not suitable for real time implementations

3. METHODOLOGY

3.1 INTRODUCTION

This chapter is dedicated to explaining the methodology used to achieve the objective of the proposed research. The reasons behind approaches choice, the proposed model designing, formulas that have been used to form the proposed model, selection of dataset that used to implement the proposed model and the evaluation methods and its formulas will be described in this chapter. Achieving the best results in image encryption criteria is the main goal of the proposed framework. The general frameworks of the traditional chaos-based image encryption include two processes, while the number of processes in the proposed one is three as it will discuss later in this chapter. Achieving the demands of image encryption objectives will depend on how much the proposed framework will meet the desired criteria, and in this research, there are several suggested contributions to fulfill these goals. The first process is designed for the reason of achieving the dissolving of high correlation between neighbor pixels. In this process Amended Logistic Map with Hénon map are used to increase dissolving of neighbor image pixels, While in the second processor image. Diffusion process a set of chaotic maps was used to modify the pixels value. Finally, an additional process was proposed in this research to achieve histogram alignment for the cipher image. The implementations of this process produce encrypted images with a full uniform histogram and perfect entropy. The concepts of image encryption and the implemented contributions lead to achieving a powerful image encryption framework, details of the proposed framework and the evaluation methods in addition to the dataset that had been used in this research will be explain in more detail in this chapter.

3.2 RESEARCH FRAMEWORK

The improvement of the existed image encryption framework is the main goal of the proposed research, and to verify this aim a research framework should be proposed to control all research processes. The framework of this research is containing three main processes in addition to the preprocessing, evaluation, and decryption processes. Each one of the main processes is containing one or more contributions. In the evaluation process, several methods are used to

evaluate the proposed framework. The first process is the image pixel permutation or image confusion process, the image confusion is the process of shuffling image pixels to destroy the relationship between the neighbored pixels or dissolve the correlation among pixels adjacent for encrypted image. There are two sub-proces are included in this process which is (dynamic key generating for confusion process and confusion sub-process). The dynamic key is generated by using two chaotic maps and additive white Gaussian noise, the first chaotic map is the Hénon map, while the second is the Amended logistic map. The second process or diff*usi*on pr*oce*ss is the main goal of this process is to change the pixels value randomly. The histogram of the encrypted image after the accomplishment diffusion process should be almost uniform as much as possible to resist any clue of the plain image information from the encrypted one. In the diffusion process, four chaotic maps in addition to the additive white Gaussian noise will be used to form the random diffusion key, these four chaotic maps are, Amended Bernoulli, Tinkerbell, Burgers, and Ricker maps. The first step in the process of generating diffusion random matrix is to generate four random series one for each of the previously mentioned maps, the size of each of these series are equal to the size of the plain image (M x N) where M and N are equal to the image dimensions, Amended Bernoulli map will be used to control the selection process of the elements of the desired random key from the rest used maps, after finishing this process an additive white Gaussian noise will be added to this key series. then an XOR operation is done between each randomly successive rows and columns with double times. Finally, the XOR operator will implement the resulting diffusion matrix and the scrambled image. The new process which is the histogram alignment process was added to the proposed research the aim of adding this process is to perfectly uniformize the histogram of the encrypted image also the information entropy will be idealized. Finally, evaluation of the proposed framework will be done by using several image encryption methods such as NIST, keyspace, key sensitivity, differential attack, histogram, entropy, correlation analysis, structural similarity, encryption quality, MSE, and Peak Signal to Noise Ratio (PSNR). The main difference or main contribution of the proposed framework in comparison with the existed frameworks is that the additional process (histogram alignment process), in addition to the Amendment of both of chaotic logistic map (LM) and chaotic Bernoulli map (BEM) and also the use of additive white Gaussian noise. In the existed image e*nc*ryption framework, that is based on chaotic maps, there are only two

processes which are the image confusion process and the image diffusion process. The proposed framework shows large size of key space and better result in the dissolving of correlation between adjacent pixels also perfect histogram uniformizing and perfect entropy, figure 3.1 illustrate the framework of the proposed research.

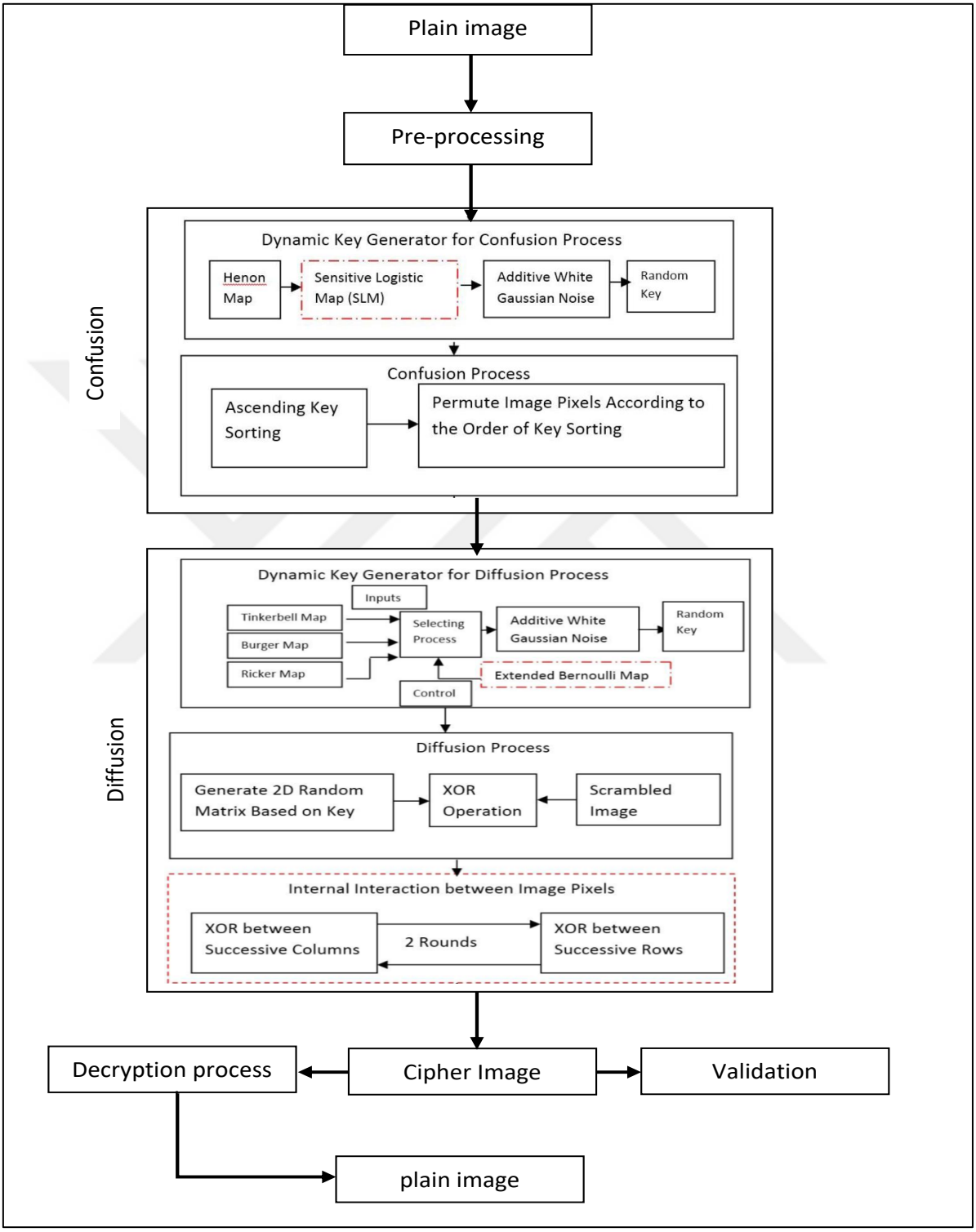


Figure 3.1: General Framework for the Proposed Research.

The first process in the proposed framework is the confusion process in the above framework the random generator based on Sensitive Logistic Map (SLM) is proposed to achieve sensitive and unpredictable random key to be used in the confusion process which will be responsible for the minimizing of correlation between adjacent pixels for the cipher image. While in the diffusion process the Extended Bernoulli Map (EBM) and Internal Interaction between Image Pixels (IIIP) was proposed to improve the performance of the diffusion process by increasing key randomness and maximizing resistance against differential attack.

3.3 PRE-PROCESSING

This section of the process is in charge of selecting and evaluating the chosen image before carrying out any action. In beginning, an image will be selected from the chosen dataset if the chosen image is 8-bit grayscale the proposed framework will deal with it directly, while in 24-bit RGB images analysis of its RGB channels should be implemented to deal with each channel separately. After complete separation, store each image channel in a separate 8-bit matrix with dimensions matching those of the original image after full separation. The implementation of this part produces three channels image, each of which is an 8-bit image. The figure 3.2 illustrates this procedure.

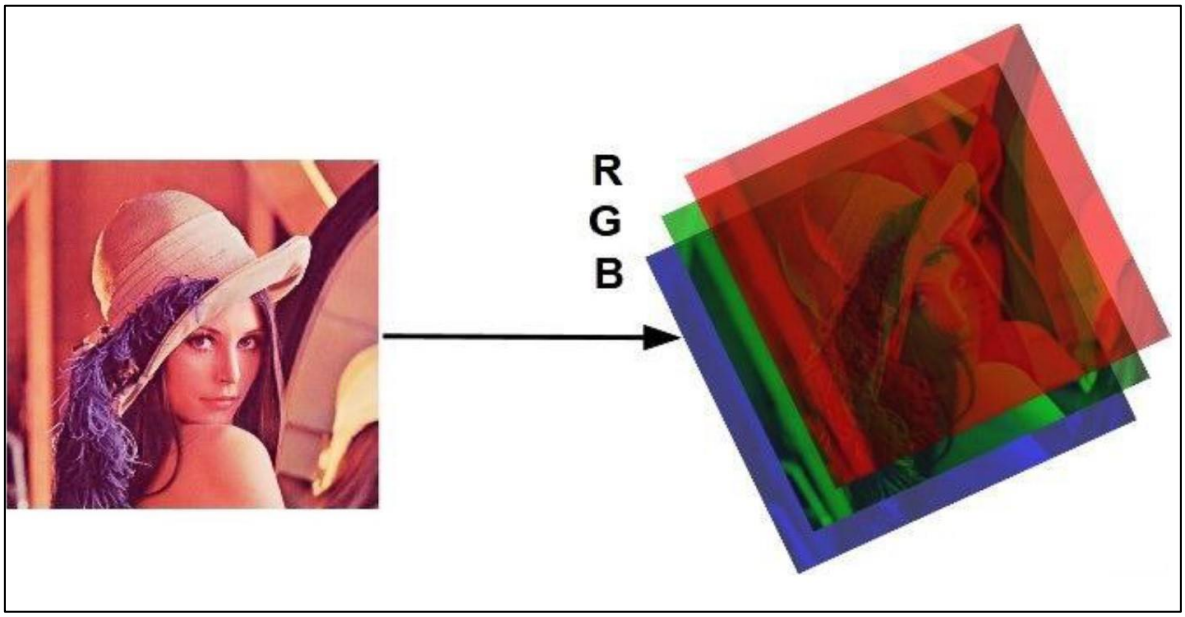


Figure 3.2: Illustrate analysis of RGB channels.

3.4 CONFUSION METHOD

Confusion method is divided into two main processes, which are dynamic key generating process and confusion process. Following is an explanation for these to processes.

3.4.1 Dynamic Key Generator for Confusion Process

Dynamic key generating is very important and essential in image encryption system [43], in proposed framework different chaotic maps are used. For confusion process, Hénon and amended logistic maps was used together to form the random key, in addition to these maps additive white Gaussian noise was added to the random key in reason of producing confusion random key with high randomness criteria. The dynamic key generator for confusion process can be explained as following:

a. Generate random number series by implement Hénon map. The length of this series is equal to the number of plain image rows.
b. Use each one of these generated numbers as initial value for amended logistic map.
c. Implement amended logistic map several times, the number of these implementation times is equal to the length of the random series that had been produced from chaotic Hénon map (equal to the row numbers of plain image) and use one element of random Hénon random series as initial value for each implementation of amended logistic map.
d. The length of each produced series from the implementation of amended logistic map is equal to the number of plain image's columns.
e. The produced random numbers will be as a two dimensions random key.
f. An additive white Gaussian noise will be added to the two dimensions random key to produce the random key of confusion process to be used in the confusion part.

Producing of random key for confusion process can be more explained by following numerical example:

a. Let's try to produce random key to confuse an image with dimensions of (4×4) pixels.
b. To confuse such image a random key with 4×4 dimension should be produced.

c. First step is to choose initial value to be as an input of Hénon map, and this value will be equal to (0.323) in this example. Implementing of Hénon map to series and the elements of this key series should be equal to the number of rows of desired image (which 4 random elements).

Table 3.1 illustrates the generated random key for Hénon map produce the auto generated random key

Table 3.1: The generated random key for Hénon map.

0.323
0.210
0.986
0.763

a. Using of the generated column to be as initial inputs for amended logistic map.

b. Generate multi random keys by implement amended logistic map four times using of the four elements of generated random series of Hénon map as initial inputs for amended logistic map. Table 3.2 illustrates the generated random key for amended logistic map.

Table 3.2: The generated random key for amended logistic map.

0.323	0.977	0.543	0.432
0.210	**0.391**	**0.433**	**0.675**
0.986	**0.854**	**0.942**	**0.329**
0.763	**0.492**	**0.657**	**0.261**

Additive white Gaussian noise will be interacting with the above random key to produce the final confusing random key. As illustrated in Table 3.3.

Table 3.3: Generation of random key for confusion process.

0.423	0.832	0.592	0.377
0.267	**0.409**	**0.477**	**0.600**
1.033	**0.950**	**0.871**	**0.432**
0.709	**0.438**	**0.732**	**0.321**

In this process randomness increased to improve confusion stage by change logistic map to Sensitive Logistic Map (SLM).

3.4.2 Confusion Process

Confusion is the part of image encryption framework that is responsible for achieving the dissolving of the high correlation between adjacent pixels in the plain image [45]. The method for dissolve this correlation is by applies permutation of pixels locations in plain image using the generated random key to control the whole process of this part. After create Two Dimensional random key, all pixels of the original image will be shuffled according to the 2-D random number key. At beginning we sort random key matrix in ascending order, the order of indices of the random key will be scrambled, and the plain image will undergo the same scrambling process that happen to the random key, so the indices of both of scrambled key and scrambled image will be same. Figure 3.3 illustrates this process.

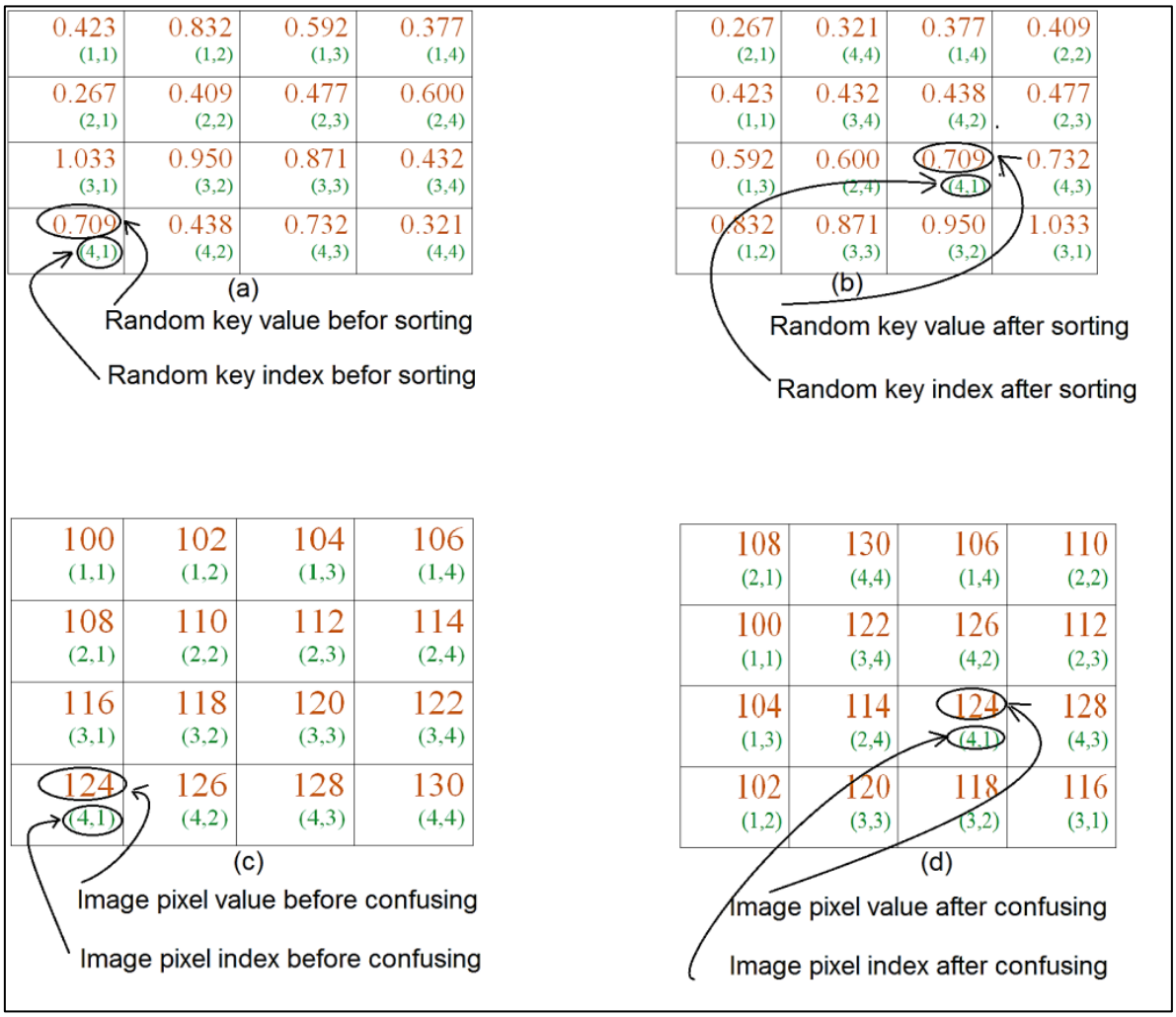


Figure 3.3: The confusion process. (a) random key before sorting (b) random key after sorting (c) image before confusion (d) image after confusion.

The image resulted by applying confusion part will show less correlation between the adjacent pixel, due to the shuffling of these pixels' locations with random manner.

In other side the histogram of the resulted image will still be same as the histogram of the plain image because the image pixel values does not changed. Only the pixel's location is changed in this framework part. Confusion process mainly relies on logistic map to reposition the pixels as correlation process. In this regard changing pixel position is important to avoid statistical attack [48].

3.5 DIFFUSION METHOD

Diffusion method consists of three main phases which are the dynamic key generator phase, internal interaction between image pixels phase and diffusion process phase, following is an explanation for these three phases.

3.5.1 Dynamic Key Generator for Diffusion Process

Four of chaotic maps will be used to generate random key for diffusion process in addition to these chaotic maps an additive white Gaussian noise will be implemented to produce random key. Amended Bernoulli, Tinkerbell, Burgers, and Ricker maps will be exploited to generate diffusion random key. In proposed framework all of amended Bernoulli, Tinkerbell, Burgers and Ricker maps will generate its own random series the size of each of these series is equal to M x N size when M and N are the dimensions of the plain image. After generating these series, random key will select from Tinkerbell, Burgers, and Ricker maps series, and the process of selection is controlled by Amended Bernoulli map. The selection of the random key will be depending on the values that has been generated from the implementation of Amended Bernoulli map i.e. when the value of control series is equal to a certain condition, the selection of random key will be either from Tinkerbell map, Burgers or Ricker maps. After forming the random matrix an additive Gaussian noise will be added to this matrix to generate the random key that will used in the diffusion process. Figure (3.4) shows the random key generating process. In Figure 3.4, random key control the selection process according to Algorithm 3.1.

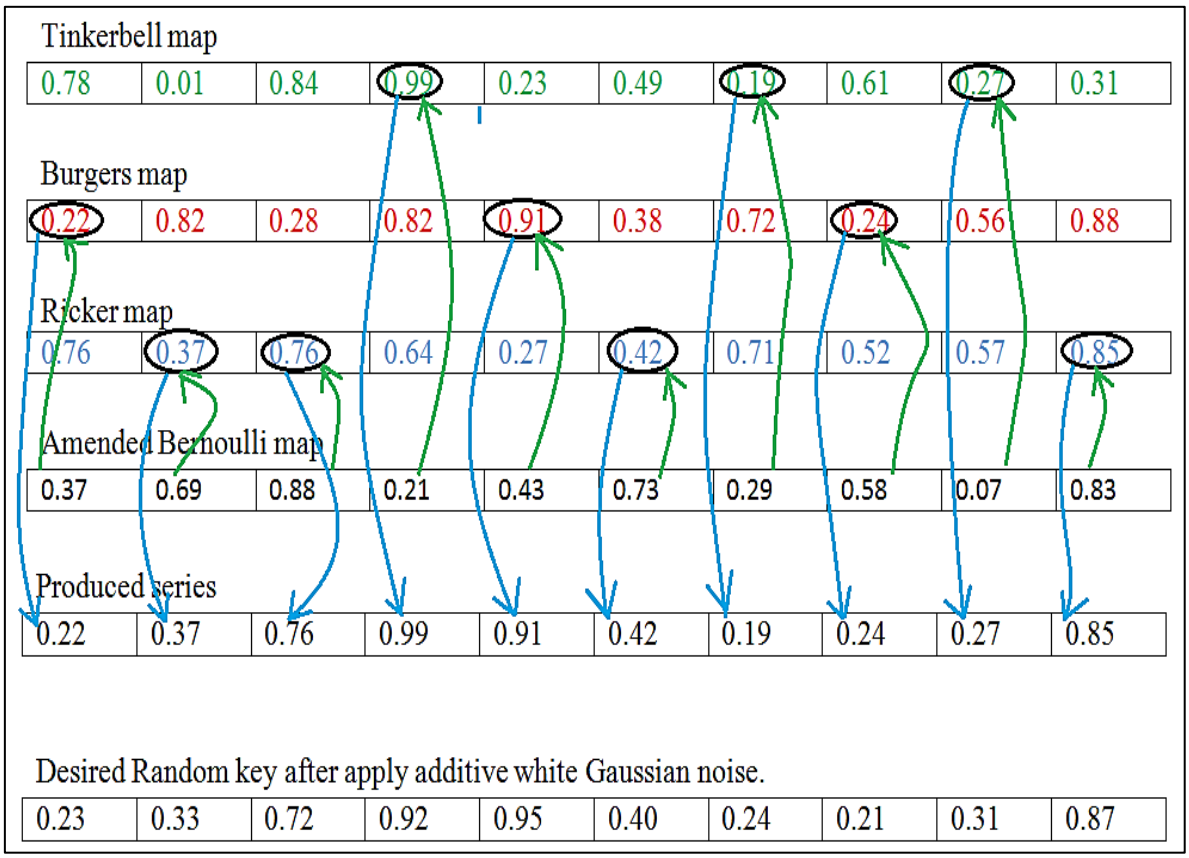


Figure 3.4: Random key generating process for diffusion process.

Algorithm 3.1: Random Element Selecting Process

Input: Four (RND) vectors

Output: one (RND) Vector

Begin

{For all RND vectors **do**

If Amended Bernoulli > 0.34 **then** select element from Tinkerbell vector

If 0.34 = < Amended Bernoulli < 0.67 **then** select element from Burger vector

Else the selected element is from Ricker vector**}**

End

3.5.2 Internal Interaction Between Image Pixels

Due to the growing interest in the development of differential attack by the cryptanalysis and to increase the resistance against such attacks, this study proposes simple and effective process to produce robust method against the differential attack. In differential attack the cryptanalysis tries to make small difference in plain image and encrypt this altered image, then by studying the relationship between the encrypted images and their corresponding plain image he try to find a patterns to exploit it later in his attack. In the proposed method the process of Internal Interaction between Image Pixels will make any slight change in plain image even in one pixel leads to produce encrypted image totally different from the encrypted image that produce from the encryption of plain image, or in other words the proposed method will be very sensitive to any change in plain image. The Internal Interaction between Image Pixels method can be achieved as follows:

At first, use the generated two dimensions random numbers matrix for diffusion process to control the entire process by use of the random numbers of the first row and first column to index the sequence of the columns and rows respectively. An XOR operation will be implemented between each two successive (according to random indexing) pixels in horizontal direction then in vertical direction, and to ensure that the effect of any small change in the plain image will totally affect the produced encrypted image, the process should be repeated twice. With proposed method 2D random used to improve the random function with key space. Choosing new random method leads to increase possibility of ambiguity pixel's locations [8]. With previous work there is a chance for cryptanalysis to discover pixel map.

3.5.3 Diffusion Process

The main purpose of diffusion process is to obliterate the image information, and this can be achieved by altering of the image pixel values with proper method. Histogram is one of the main criteria for image diffusion process, and the uniform histogram is desired in this image encryption process. In proposed framework, to achieve main aims of the diffusion process, the random matrix numbers that has been generated from previous section will converted from fractal numbers that has been arranged between (0) and (1) to an integer number arranged

between (0) and (255) With an equal number of appearances for each of these numbers. The resulted matrix will be the key for diffusion part. Diffusion is how to change image's statistical information especially the histogram information by altering image pixels values. In proposed framework, the generated key with equal number of appearances for each of the key elements is the main reason to get the almost uniform histogram for the encrypted image after diffusion process. Implementation of XOR operator between the generated diffusion random key and the image that resulted from confusion process (scrambled image) is the main process in this part of image encryption. The histogram of resulted image after diffusion process is almost uniform also for entropy is close to 8. Which means it is very difficult for cryptanalysis to reveal the plain image from the encrypted image that resulted from diffusion process. To prevent any attempt from the cryptanalysis to attack the encrypted image by using of most attacks methods especially the methods based on statistical features of encrypted image, a new part which is responsible for destroying any statistical features in terms of entropy and histogram for the encrypted image. This part will explain in detail in following.

Internal Interaction between Image Pixels (IIIP) allow the system to avoid deferential analysis. This process runs simultaneously with the proposed Extended Bernoulli Map (EBM) to achieve better performance with diffusion stage.

3.6 DATASET

In image encryption systems a dataset is defined as a set of images, which is used to verify the proposed study and to benchmark the observations of this study with the already existing literature. Many images are used as datasets in the literature, where each researcher achieved results based on a dataset. This study follows the same strategy to evaluate and benchmark the experimental results obtained using the proposed method. Colour (red, green, and blue) and grey scale images are used. In these each pixel in the image consists of 24 bits, in which 8 bits are allocated to each colour. Image encryption methods treat each part separately as new pixels, because the illumination of each colour (part) is different from other pixels. The worthiness of the proposed framework is further demonstrated by the selection of several images from the SIPI standard dataset including Girl, Tiffany, Elaine, Cameraman, Lena, Baboon, and Man as

shown in Figure 3.5.

Figure 3.5: Selected Standard SIPI dataset used in the proposed framework (a) Girl (b) Tiffany (c) Elaine (d) Cameraman (e) Lena (f) Baboon (g) Man. [10]

The images selected from the SIPI dataset have different sizes and contain both RGB and grayscale images (Girl is RGB with size of 256*256 pixels, Tiffany is RGB with size of 256*256 pixels, Elaine and Lena are grayscale with size of 512*512, Baboon is RGB with size of 512*512 pixels and Man is grayscale with size of 1024*1024 pixels). System performance was tested using three images taken via mobile. This was deemed to be more realistic and biased free, which allowed the system to adopt real images as illustrated in Figure 3.6.

Figure 3.6: Images Taken by Mobile Camera (a) Cactus (b) Dolls (c) City used in the system performance evaluation.

All images taken by a mobile phone are RGB (coloured) and the size is 512*512 pixels. This study uses the SIPI image dataset with variable image types (grayscale and colored) and the size

of used SIPI images are different (256 x 256, 512 x 512 and 1024 x 1024) in addition to three colored image that captured by mobile camera of the size of 512 x 512 (Cactus, Dolls and City). The implementation of the proposed framework is started by generate random number sequence for confusion method to be used later in the confusion process. The random number generator for diffusion method is the first process in diffusion process. Then by the using of generated random number the Internal Interaction between Image Pixels (IIIP) method will be implemented.

3.7 PERFORMANCE EVALUATION

Many image encryption systems have been proposed to achieve high image encryption criteria. Researchers in image encryption always focus on how to encrypt images with secure methods. There are several methods to evaluate image encryption systems. The following section provides explanations of these methods.

3.7.1 Random Number Generation Test

To evaluate the randomness of the generated number there are (15) different tests, which are included in the NIST Test Suite, one of which is the ability to test random keys produced either from physical or logical generators of arbitrary lengths. These tests are based on several different types of non-randomness that can occur in the generating key sequences [11]. These tests are:

i - The Frequency (Monobit) Test
ii- Frequency Test within a Block
iii- The Runs Test
iv- Tests for the Longest-Run-of-Ones in a Block
v- The Binary Matrix Rank Test
vi- The Discrete Fourier Transform (Spectral) Test
vii- The Non-overlapping Template Matching Test
viii- The Overlapping Template Matching Test
ix- Maurer's "Universal Statistical" Test

x- The Linear Complexity Test

xi- The Serial Test

xii- The Approximate Entropy Test

xiii- The Cumulative Sums (Cusums) Test

xiv- The Random Excursions Test

xv- The Random Excursions Variant Test

3.7.2 Key Space Analysis (KA)

The key space analysis is a list of indispensables trying to guess the true decryption analysis keys. Powerful cryptography (encryption) must have a power encryption key (secret key) which means the encryption key should be bigger than 2^100 [4], with the indicator indicating the bits numbers of a secret key. In good encryption systems, the large key space indicates good resistance and high strength against Brute Force Attacks (BFA) [5].

3.7.3 Key Vulnerability Analysis (KVA)

The secret keys (cryptography keys) used for cryptography make strong cryptography. The simple modification in a cryptography key or secret key will represent a different cryptography image. Therefore, the security level in the image cryptosystem is dependent on the keys used in the system and the measurement of the robustness of the system. Finally, any modification in the cryptography key gives a different process in the encryption and decryption procedure and the original image will not be rebuilt probably [8].

3.7.4 Correlation Between Adjacent Pixels

It is well known that the most successful methods of encrypted image attacks are statistical-based attacks, and to encrypt images with secure methods the encrypted image must resist statistical attacks. To ensure that the used encryption method is performed against statistical attacks a correlation between the horizontal, vertical and diagonal directions must be calculated for adjacent pixels in both plain and encrypted images [6]. To ensure robustness against statistical correlation attacks for the proposed image encryption framework, Equations (3.1),

(3.2), (3.3), and (3.4) are used in the calculation of image correlation.

$$cor = \frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \quad (3.1)$$

Where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - x')^2 \quad (3.2)$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(yi - y')^2 \quad (3.3)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(xi - x')(yi - y') \quad (3.4)$$

3.7.5 Color Image Histogram Analysis

The image histogram is the description of occurrence frequency for each pixel value in an image. The histogram of the encrypted image must be fully statistically different from the histogram of the plain image and should be uniform to avoid statistical histogram attacks [13].

In image histogram plots, each bar represents a specific number of occurrences for the corresponding pixel value. In 8-bit greyscale images the pixels value are arranged from 0 (which represents a black pixel) and 255 (which represents a white pixel) as explained in Figure 3.7.

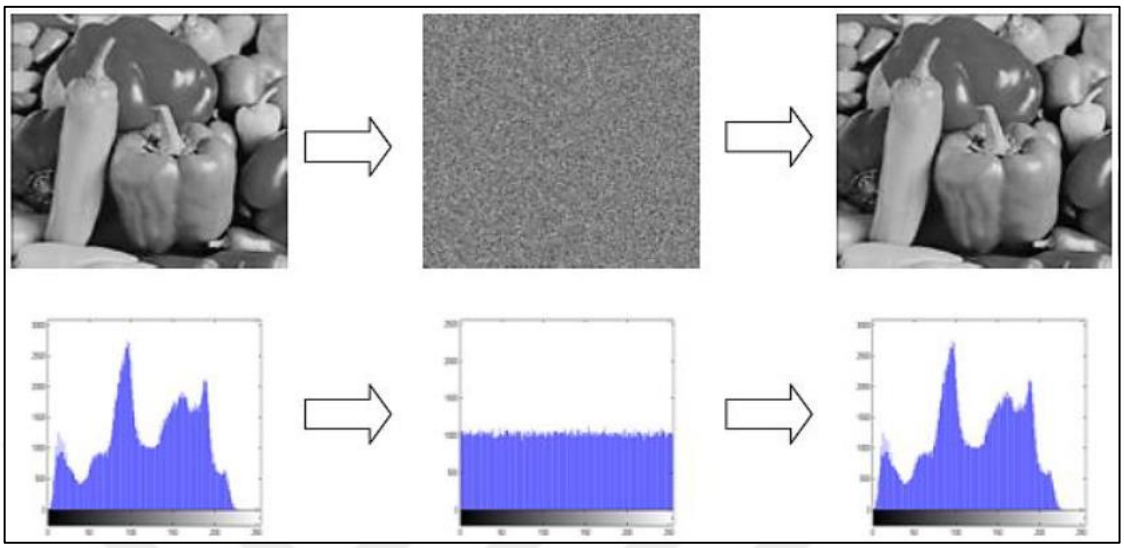


Figure 3.7: The histogram for plain, encrypted and decrypted images.

3.7.6 Information Entropy Analysis

Information entropy (IE) is utilized to compute uncertain societies and associations among different random values [53]. According to computing the IE to a greyscale image, the result can be equal to 8 sh, or Bits. The Image cryptography has to produce a cryptography image within the Entropy Value (EV) similar to the greyscale image value [27]. Information entropy can be calculated using Equation (3.5):

$$H(m) = \sum_{i=0}^{M-1} P(mi) \log_2 \frac{1}{P(mi)} \qquad (3.5)$$

where M is the whole number of pixels, mi symbolizes the possibility of occurrence of symbol mi and log denotes the base 2 logarithm so that the entropy is expressed in binary mode. The amount of information entropy in a perfect random image is 8. When the cipher image entropy is close to 8, this indicates that the cipher images are almost random, and the used algorithm is secure against entropy-based attacks.

3.8 SUMMARY

This chapter illustrates the proposed framework using image confusion, image diffusion, and histogram alignment. Image confusion or pixel permutation is the method of how to change image pixels' locations randomly to dissolve correlations between adjacent image pixels. In the confusion process, Hénon map, amended Logistic Maps, and white Gaussian noise are used to generate random keys. A diffusion process was used to randomly alter pixel values. Amended Bernoulli, Tinkerbell, Burgers, and Ricker maps in addition to additive white Gaussian noise were used to generate a diffuse random key. An XOR operator between the scrambled image and the diffusion random key was used to diffuse the image. The third or final process is a histogram alignment process, in which the histogram and entropy of the ciphered image are perfected as desired. SIPI was the dataset used to test the proposed framework. And this dataset contains many images that are suitable for implementing the proposed framework. Several evaluation methods are explained in this chapter and these methods were used to evaluate the proposed framework.

4. CHAOTIC MAPS IN CONFUSION AND DIFFUSION PROCESS

4.1 INTRODUCTION

This chapter deal details the confusion and diffusion methods to achieve study objectives. Chaos-based image encryption systems are composed of confusion and diffusion methods. Confusion methods are responsible for minimizing correlations between adjacent pixels of the encrypted image by randomly changing the locations of plain image pixels, while the diffusion method is responsible of changing image pixels values randomly. Successful image encryption methods hide visual information and the statistical characteristics of the plain image to make any attempt to reveal the image infeasible. While the process of image diffusion is the most effective method to hide the statistical information of an encrypted image and it complements the image confusion process to achieve encrypted images with high criteria [15]. Firstly, the proposed confusion method consists of two main processes. First, the random number generating process consist of the amendment of logistic map equation to improve the sensitivity of the well-known logistic map and using Hénon map, Sensitive Logistic Map (SLM), and additive white Gaussian noise (AWGN) to perform random number generator. Second, image pixel permutation units are used as random numbers in the process of changing the locations of each plain image pixel to increase the performance of the proposed study. Secondly, the diffusion method consists of random number generation and the diffusion process.

4.2 CHAOTIC MAPS USED IN THE PROPOSED CONFUSION METHOD

Two chaotic maps are used in the proposed confusion method. The Sensitive Logistic Maps (SLM) and Hénon map in addition to additive white Gaussian noise are used in the proposed confusion method to obtain random sequences with better criteria. The following sections explain the proposed SLM.

4.2.1 The Proposed Sensitive Logistic Map (SLM)

To achieve the research objectives, an amendment to the logistic map was proposed in this study. This new form of logistic map aims to increase the randomness of the confusion process by increasing sensitivity to initial conditions. To achieve this goal a multiplication between the output of each iteration of the logistic map with an integer K (which must be >1) to increase the difference between the input and output values for each iteration. Multiplication will make the resulted values exceed the boundaries of the logistic map i.e. the output will be greater than 1. The logistic map is an iterated equation, and the output of each iteration will be the input for the next iteration. The input limits for the logistic map are greater than (0) and smaller than (1), which leads to some imperfection. Therefore, to solve this problem a modulus of (1) was used to make the resulting values within an acceptable range (0 < X < 1). Equation 4.1 shows the proposed Sensitive Logistic Map (SLM).

$$X_{n+1=}\big(rXn(1-Xn)\big) * K \ mod \ 1 \qquad (4.1)$$

Introducing a new parameter (K) to SLM will produce dynamical systems with more randomness by applying multiplication between (rXn(1−Xn)) and K (which is >1) to amplify the result of each iteration to produce a more sensitive random number generator. K parameter used to increase the sensitivity of the new iteration to the old input that resulted from the previous iteration. While (mod 1) is to reduce the accumulation when feedback the result to the equation of random generator keep the range of random number between 0 and 1 to avoid the over exceed the range. The response of the proposed SLM shows significant differences between the behavior of the original logistic map and the behavior of the proposed SLM in Figure 4.1.

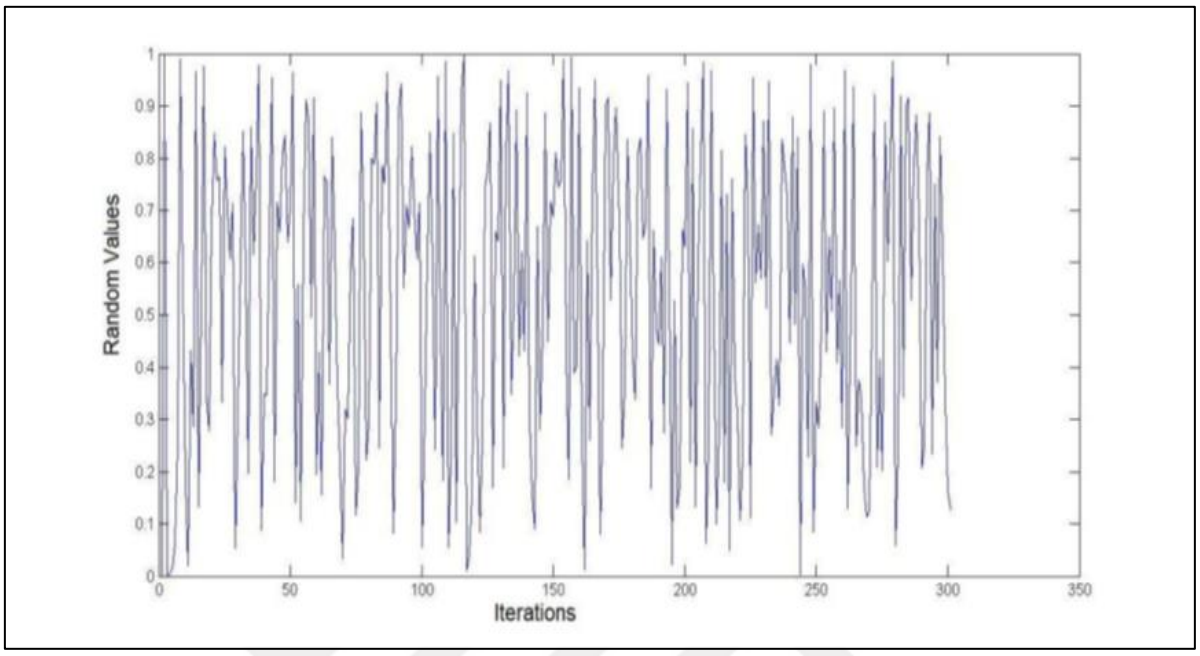


Figure 4.1: SLM Response.

While the cobweb diagram for SLM shows the dynamical behavior of the proposed map, Figure 4.2 indicates chaotic behavior for the proposed method.

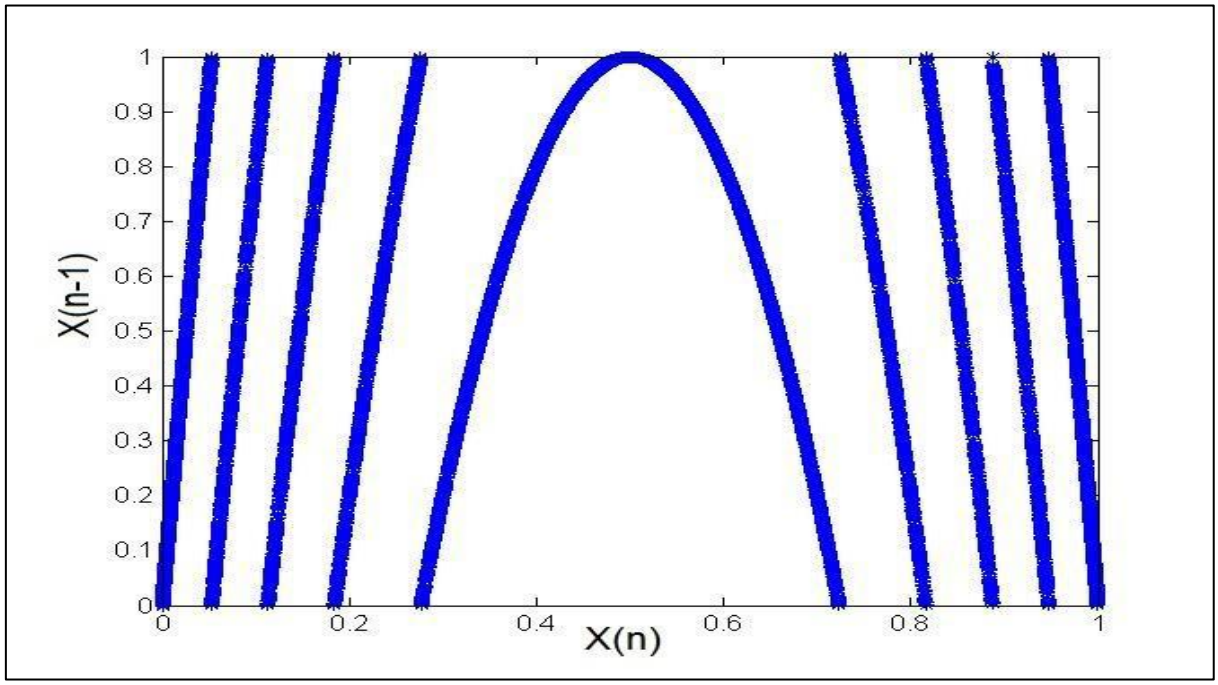


Figure 4.2: SLM Cobweb Diagram.

The differences in both the response, cobweb diagram of the logistic map, and SLM increase the randomness of the produced random sequences.

4.3 GENERAL FRAMEWORK FOR THE CONFUSION METHOD

Image confusion is the process of minimizing the relationship between the cipher image and plain image [19]. The proposed confusion process consists of two sub-processes, which are a random number generator and a confusion process. The random number generator is based on two chaotic maps (Hénon and SLM) in addition to AWGN. To generate useful random numbers a special combination of three methods is proposed in this research. The generating of random number generator for the confusion method can be seen in Figure 4.3.

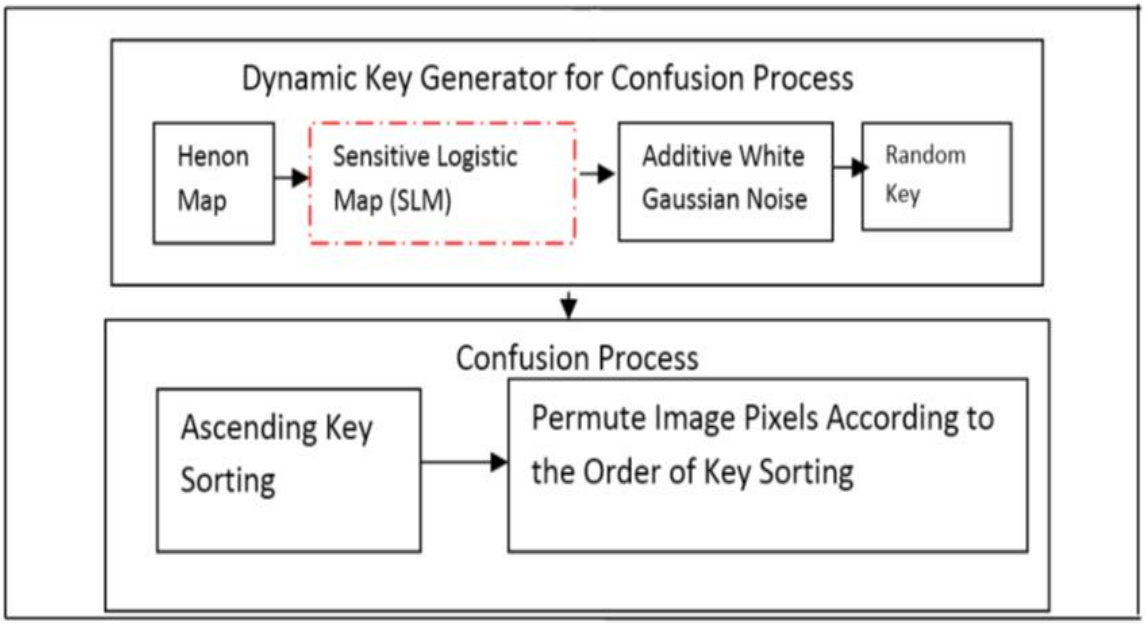


Figure 4.3: General Framework for confusion process.

At first, the initial conditions and control Parameters are initiated manually to be used as the inputs for the Hénon map.

The output of the Hénon map is a random sequence consisting of random numbers equal to the number of image rows as seen in Figure 4.4.

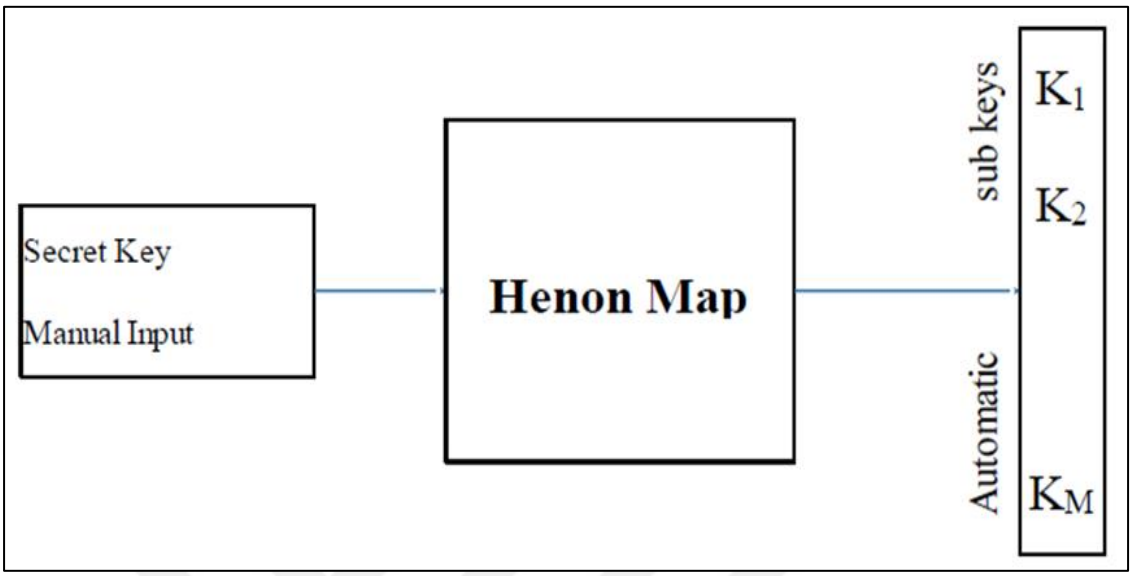


Figure 4.4: The process of generating automatic sub-keys.

The proposed SLM was used in the second phase of the random key generator. The generated sub-keys (K1 to KM) were used as inputs in the proposed SLM to generate a random sequence for each row and the size of each of these sequences was equal the size of the plain image columns, which is N. Figure 4.5 explains this process.

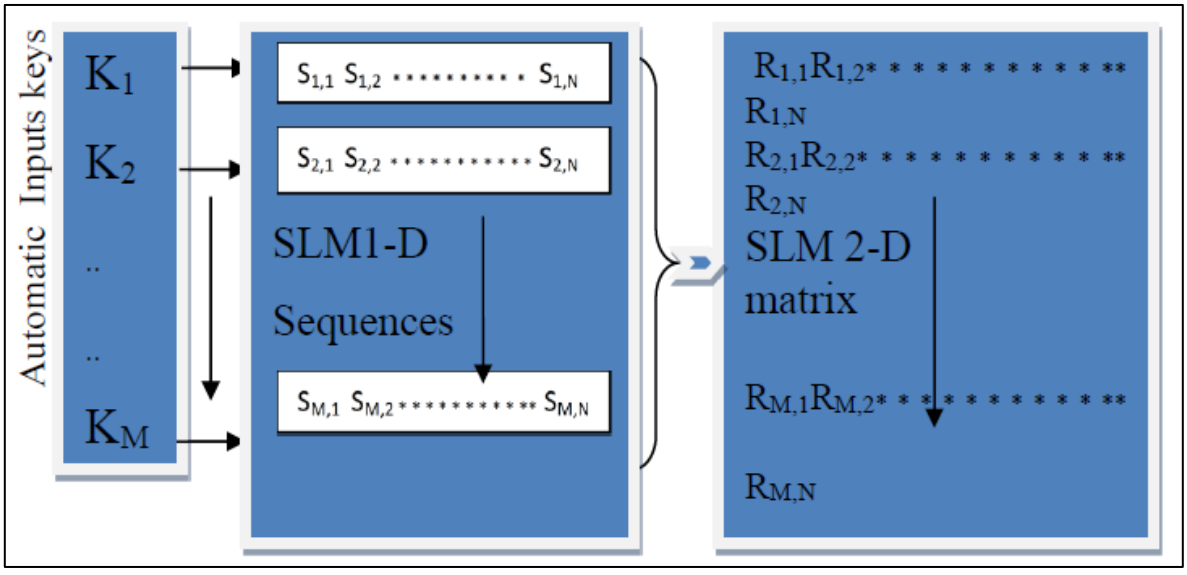


Figure 4.5: Using of Automatic Key to be as SLM Inputs.

Where K is the sub-key, S is the random number sequence generated by SLM, and R is a two-dimension random number matrix assembled from random sequences.After obtaining the random matrix from executing the Hénon map and the proposed SLM to increase the quality of the random number generator, an additive white Gaussian noise was implemented to the random matrix as shown in Figure 4.6.

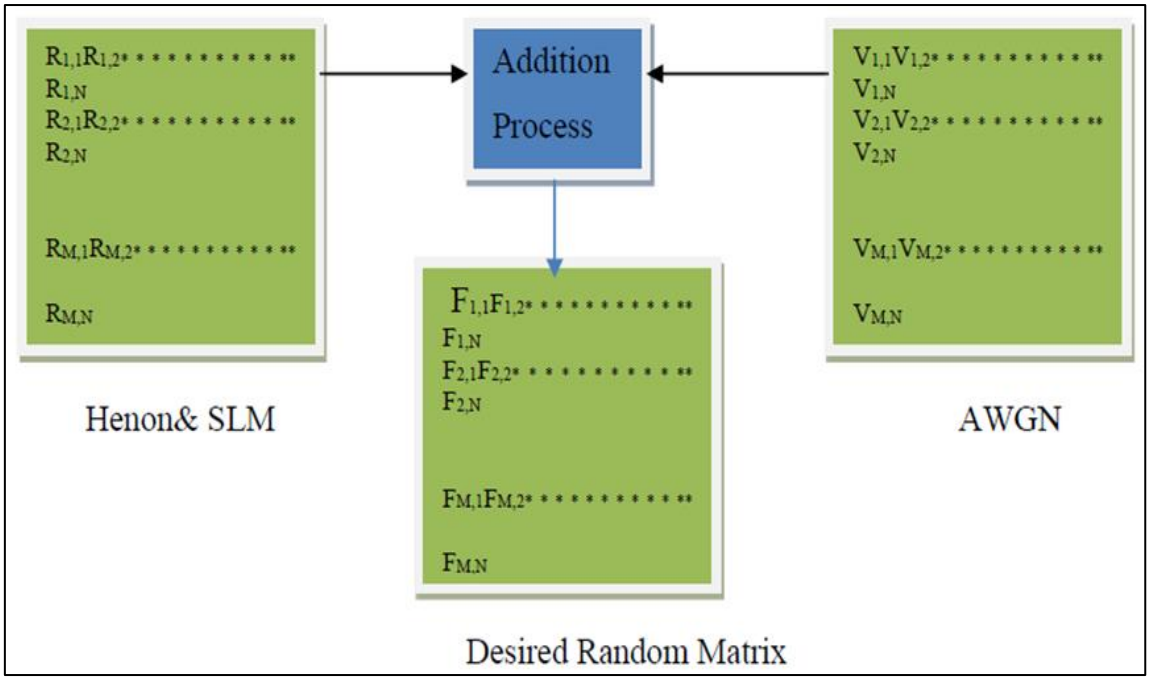


Figure 4.6: Final Random Matrix for confusion process.

where V is a two-dimensional matrix of additive white Gaussian noise and F is the final random matrix to be used in the confusion process to control image permutation.

4.4 CONFUSION PROCESS

The confusion process is a description of the image permutation method. In this study, image pixels were scrambled to reduce the high correlation between adjacent pixels to increase resistance to statistical attacks. To accomplish this goal this study proposed the creation of a random matrix, which is already explained in detail, and this matrix is dedicated to controlling

pixel scrambling in the image confusion process. The first step of the confusion process is to convert a two dimensions random number matrix into a One-Dimensional random array as illustrated in Figure 4.7.

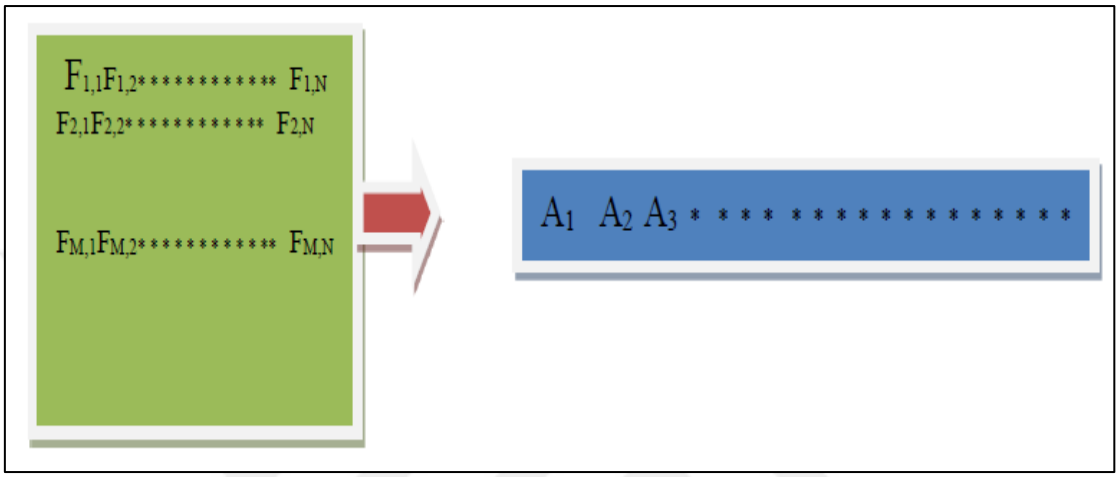


Figure 4.7: Two Dimensions to One Dimension Random Matrix Conversion.

After the conversion process ascending sorting was implemented to the one-dimension random array to consider the new order of the old indices of the sorted array (when any value in the random array changes its location to the new location in the sorted array the original index of this value before sorting follows the value to the new location). A table of three variables was created as shown in Figure 4.8.

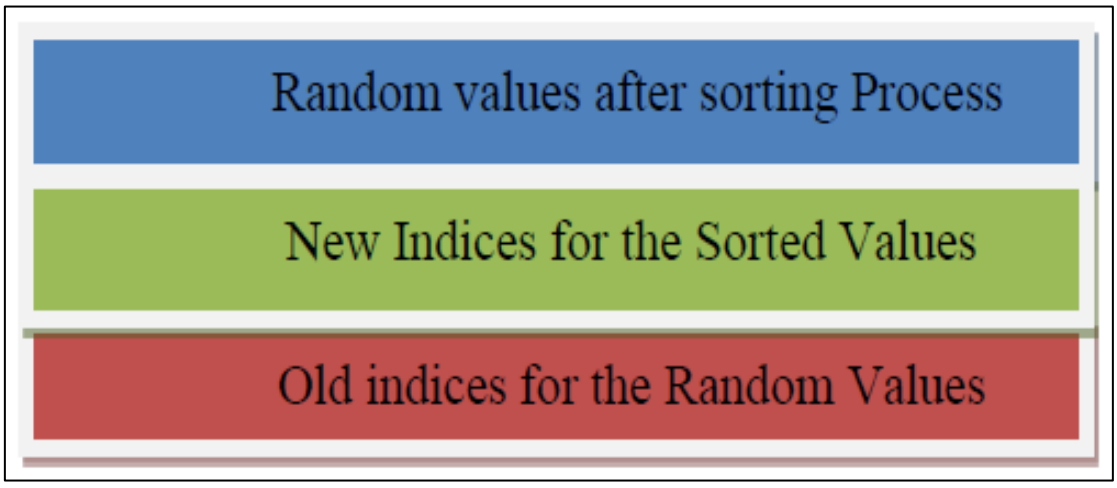


Figure 4.8: Table of the Random Array Fields after the Sorting Process.

Thus, random values and their new indices are in ascending order, but the old indices are ordered in a random way, therefore it is necessary to create a lookup table consisting of old indices against new indices. The new step is the conversion of the plain image from a two dimensions matrix into a one-dimensional array with the same size as the sorted random array. Although the conversion process makes reshapes the plain image the correlations between successive elements in the new one-dimension image array are still high. To minimize this high correlation the image pixels are scrambled using the previously mentioned lookup table to change the location of pixels in the one-dimensional image array to a new location. To get the scrambled image conversion from the one-dimensional image array after scrambling into a two-dimension scrambled image was made. The scrambled image is considered as an intermediate encrypted image with the minimum correlation between adjacent pixels, but other characteristics like the histogram and information entropy are still the same.

4.5 GENERAL FRAMEWORK FOR DIFFUSION PROCESS

For the obliteration of the statistical information of the encrypted image, the diffusion process is considered the most important process in all chaotic image encryption systems. This study suggests a new diffusion process to achieve image encryption frameworks with high criteria. Several points have been considered in the proposed diffusion process such as increased keyspace, key sensitivity, removal of histogram and information entropy, and increased resistance to differential attacks. To achieve all these goals this study proposes the framework seen in figure 4.9

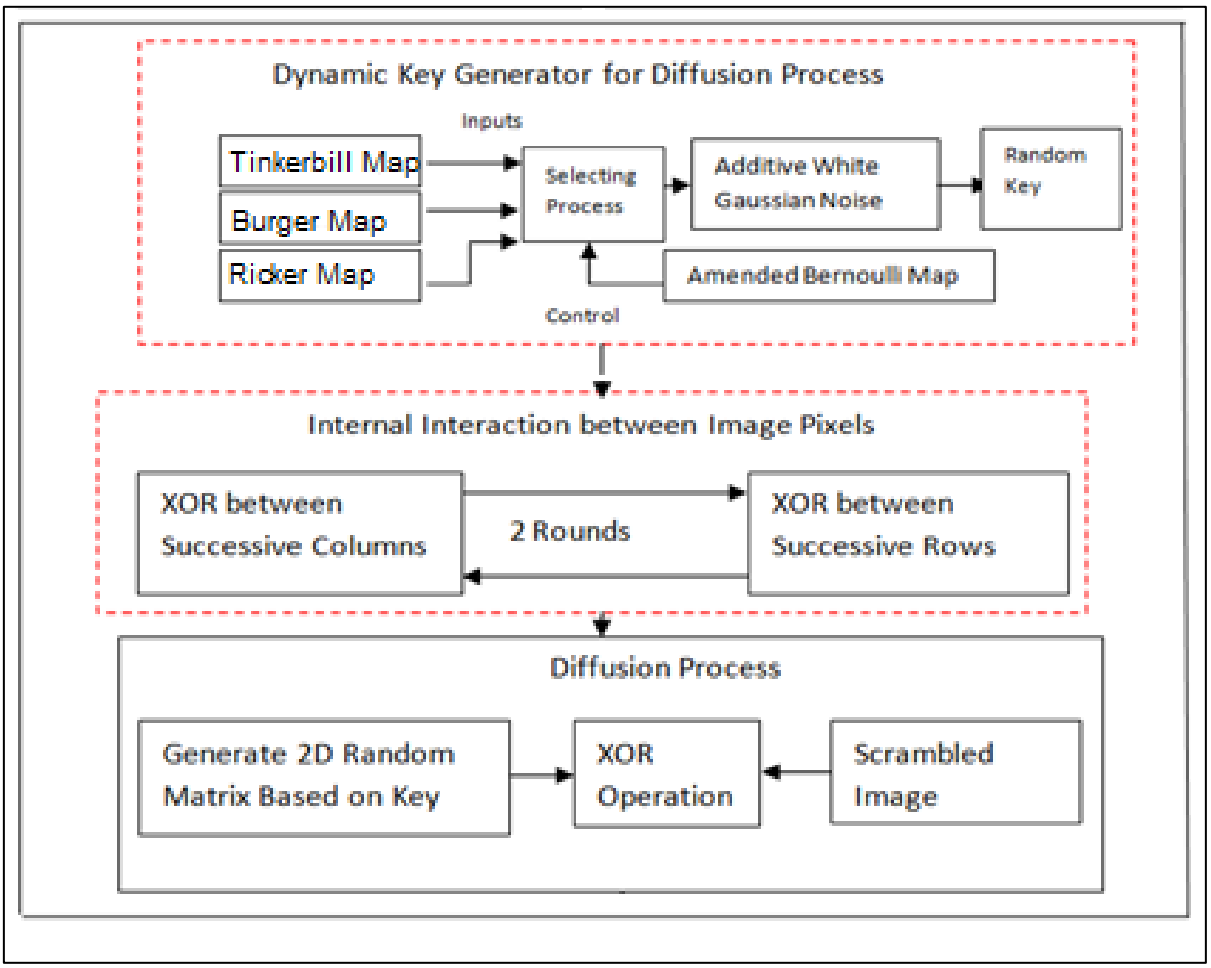


Figure 4.9: Framework of Image Diffusion Method.

The proposed framework for the diffusion method consists of three sub-processes which are random number generator process, Internal Interaction between Image Pixels (IIIP) sub-process, and diffusion process. The random number generator is designed by the use of the channel hopping technique which is performed by implementing the Tinkerbill map, Burger map, and Ricker map in addition to the Extended Bernoulli Map (EBM) which is used to control the selection process. IIIP method is proposed to achieve robust image encryption method against differential attack this process is proposed by this research while the diffusion process is implemented to efface the statistical properties of the encrypted image by the execution of XOR operator between the image generated from the IIIP process and the random matrix that derived from the random number generator.

4.6 RANDOM NUMBERS GENERATOR FOR DIFFUSION

The generating of random numbers with high-security criteria is considered essential for all image encryption processes and the quality of the resulting encrypted image follows the quality of the random number generator [28], therefore this study focuses on how to generate random numbers suitable for the image diffusion process. This study proposes a random number generator for the diffusion process based on hopping between multiple chaotic maps and additive white Gaussian noise. To generate random numbers for the diffusion process four chaotic maps are used, which are Extended Bernoulli Map (EBM), Tinkerbell, Burgers, and Ricker maps, in addition to additive white Gaussian noise. More explanations for the Extended Bernoulli Map are as follows:

4.7 EXTENDED BERNOULLI MAP

Brute force attacks are famous in cryptanalysis for attacking encrypted information and the most effective technique used to make such attacks infeasible is increasing secret keyspace as much as possible. In this study, two techniques are used to increase keyspace. One of these techniques is by implementing multiple chaotic maps with consideration for key sensitivity, while the other technique is by proposing an amendment to the Bernoulli map increases the keyspace of the proposed generator. Bernoulli map uses one initial key as the input and this study suggests increasing the initial values to two as seen in Equation (4.2).

$$X_n = \left(2 * (X_{n-1}) + (X_{n-2})\right) mod\ 1 \qquad (4.2)$$

In addition to the increasing of key space size by increasing the total number of initial conditions, the response of the proposed Extended Bernoulli Map (EBM) shows more randomness and more unpredictable behavior which achieved because the generating is dynamical for both of initial conditions which affect the whole random number generating process. The existence of two initial conditions with variable values (for each iteration) causes dynamical behavior of these initials which increases randomness and unpredictability for the generated random key.

The response of Equation (4.2) is shown in Figure 4.10 and the behavior of the successive iteration (control parameter = 0.62) is seen in Figure 4.11

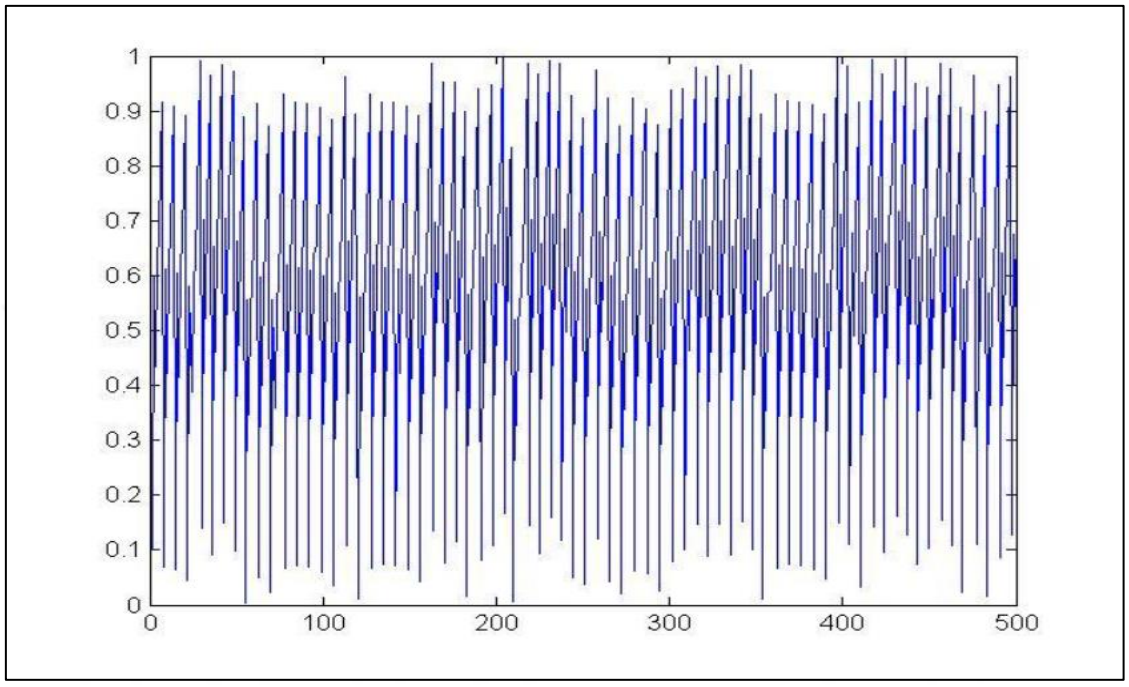


Figure 4.10: Response of Extended Bernoulli Map.

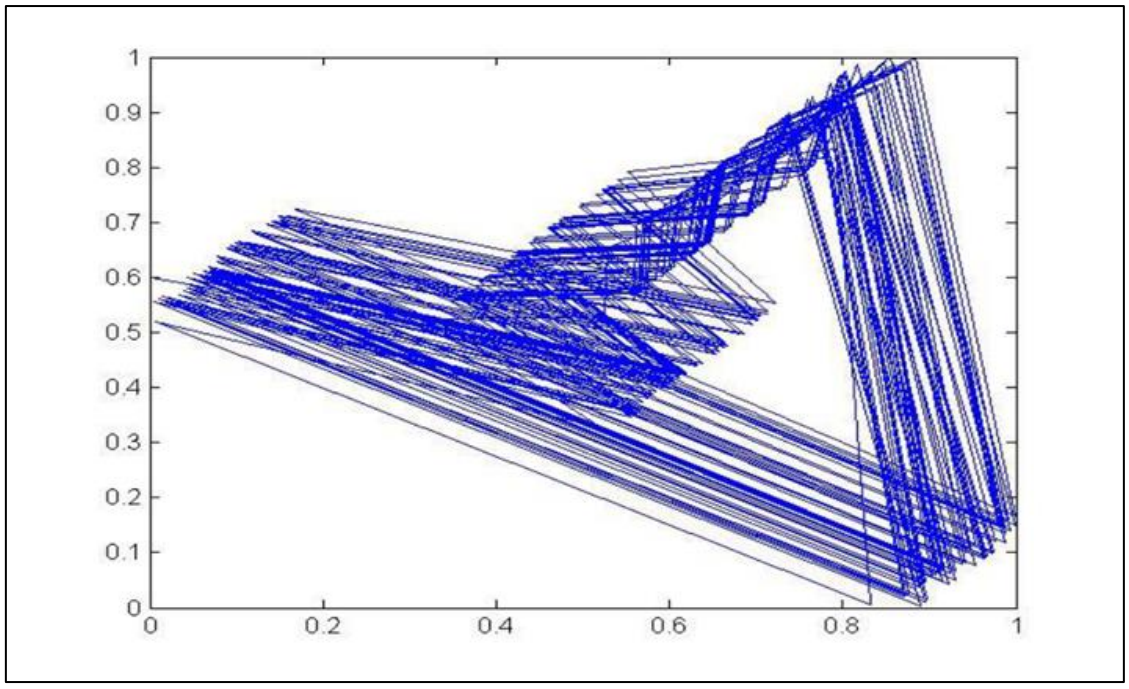


Figure 4.11: Successive Iterations Behaviour of Extended Bernoulli Map.

In addition to increasing key space, the randomness of the proposed Extended Bernoulli Map (EBM) is also increased as shown in figure 4.10 and Figure 4.11.

4.8 DIFFUSION PROCESS

This study suggests two random number generators for the confusion process (already explained in previous chapters) and the diffusion process. As mentioned earlier four chaotic maps are used, and these maps are the Extended Bernoulli Map (EBM), Tinkerbell, Burgers, and Ricker maps in addition to additive white Gaussian noise. The used technique to produce random numbers is channel hopping. After the selection process, additive white Gaussian noise is used on selected random numbers. The process of selecting random numbers is as follows:

At first, four sequences (VEx_B,VT, VB, and VR, which belong to the Extended Bernoulli Map (EBM), Tinkerbell, Burgers and Ricker maps, respectively) are generated by the initial conditions and control parameters for these four chaotic maps.The length of each of these sequences is N*M where N and M are the rows and column numbers, respectively for the image to be encrypted. Random number values will be chosen from one of the sequences of the three used chaotic maps (Tinkerbell, Burgers, and Ricker maps), and the Extended Bernoulli Map is used to control the value selecting process. The last step in the random number generating process is the implementation of additive white Gaussian noise (w) to the selected random sequence (V). The resulting sequence (R) is the desired random number sequence, which will be used in the process of image diffusion. The generation of random number sequences is explained in Figure (4.12).

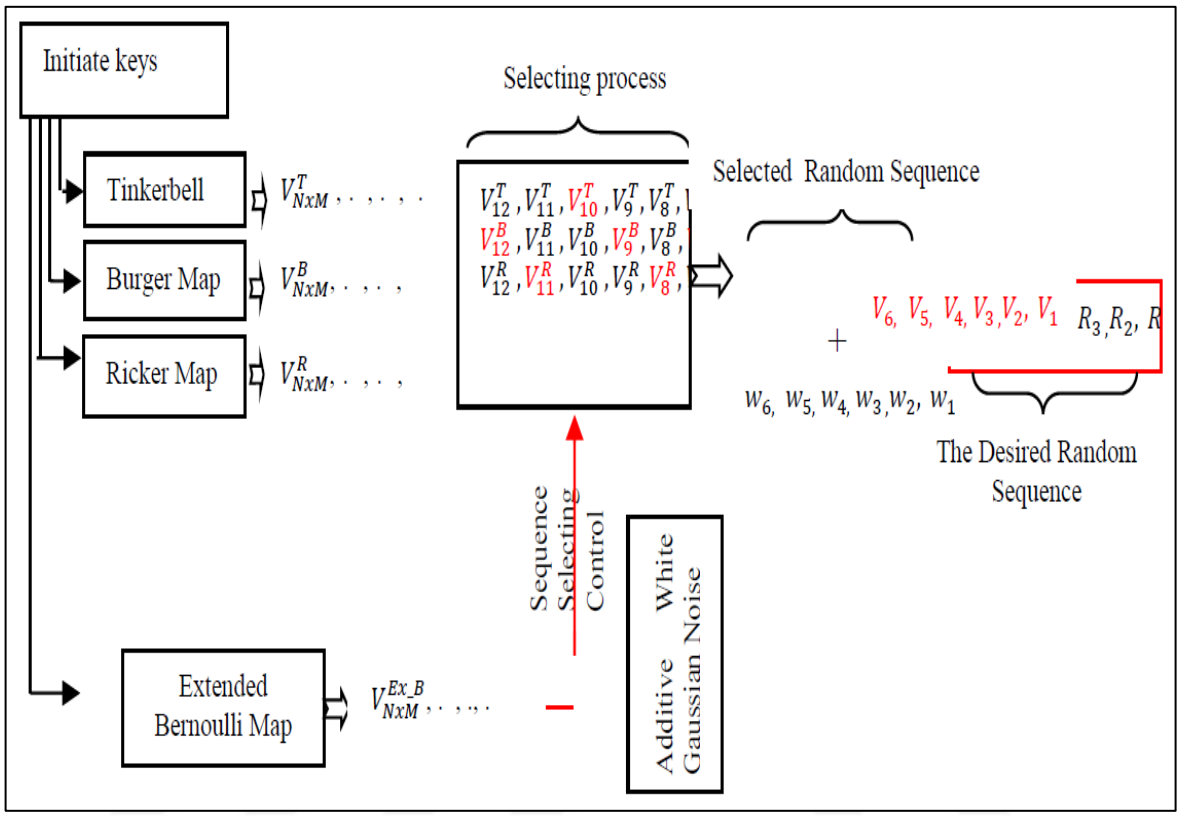


Figure 4.12: Channel Hopping Process.

After generating the desired random sequence, a conversion from one dimension into two dimensions matrix is implemented and the dimensions of the produced matrix are the same dimensions as the plain image (M × N) to be encrypted.

4.9 INTERNAL INTERACTION BETWEEN IMAGE PIXELS

Nowadays the importance of differential attacks has increased due to its high performance in cryptanalysis and researchers have concentrated on developing new techniques based on this type of attack. This study suggests a technique to resist this type of attack. The proposed technique is simple and depends on a produced random number matrix. In a differential attack cryptanalysis encrypts an image multiple times with the same encryption method and the same control parameter and initial conditions but every time it makes a slight change (one pixel) to the plain image, after which a number of encrypted images are created for comparison purposes to find relationships between the plain image and the encrypted image. To resist this type of attack encryption methods should produce significant differences between encrypted images

after making minor alterations [31]. This study suggests implementing XOR operators between image pixels. The first row and first column of the random number matrix are used to control the XOR operation. The implementation of XOR operators is done between each column and it's successive (according to the random order obtained from the first row in the random matrix) column. Then the XOR operator is implemented for the first row and it's successive (according to the random numbers obtained from the first column of the random matrix) rows.

To ensure any minor changes in the original image after even o*n*e-pi*xe*l alterations produce significant changes within the encrypted image, this study suggests the XOR implementation process is repeated twice. A numerical example to explain the proposed technique is as follows:

Suppose the plain image is a 4 x 4-pixel image and the random order for the columns is (4,1,3, and 2) and the random order for the rows is (2,4,1, and 3), which were obtained from the first row and first column of the random matrix, respectively. This procedure is illust*rat*ed in fig*u*re 4.13.

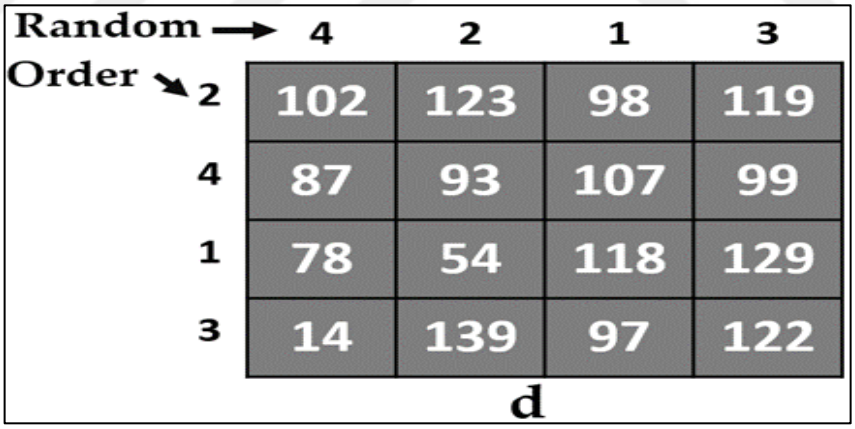


Figure 4.13: 4 × 4 plain image.

The first process was done by implementing XOR operators between the values of the second column (first column in random order) as seen in Figure 4.13 and the values of the fourth column (second column in random order). The resulting values will replace the values of the fourth column while the values of the second column will stay the same. After that, a new implementation of the XOR operator is done between the new values of the fourth column and the values of the third column (the random order for the third column is three) and the resulting

values will replace the values of the third column. Then with the same process, XOR operations will take place between the first and third columns, the values of the first column will be updated by the new values. Finally, XOR operations will be done between the first and second columns (fourth and first random columns order). The resulting values will be saved in the second column instead of the old values. The same procedure will be done between the successive (in random order) rows. After completing the first round of XOR operations between successive columns and successive rows, another implementation of the same process was done to ensure that any change of even one pixel will affect the entire image as shown in Figure 4.14.

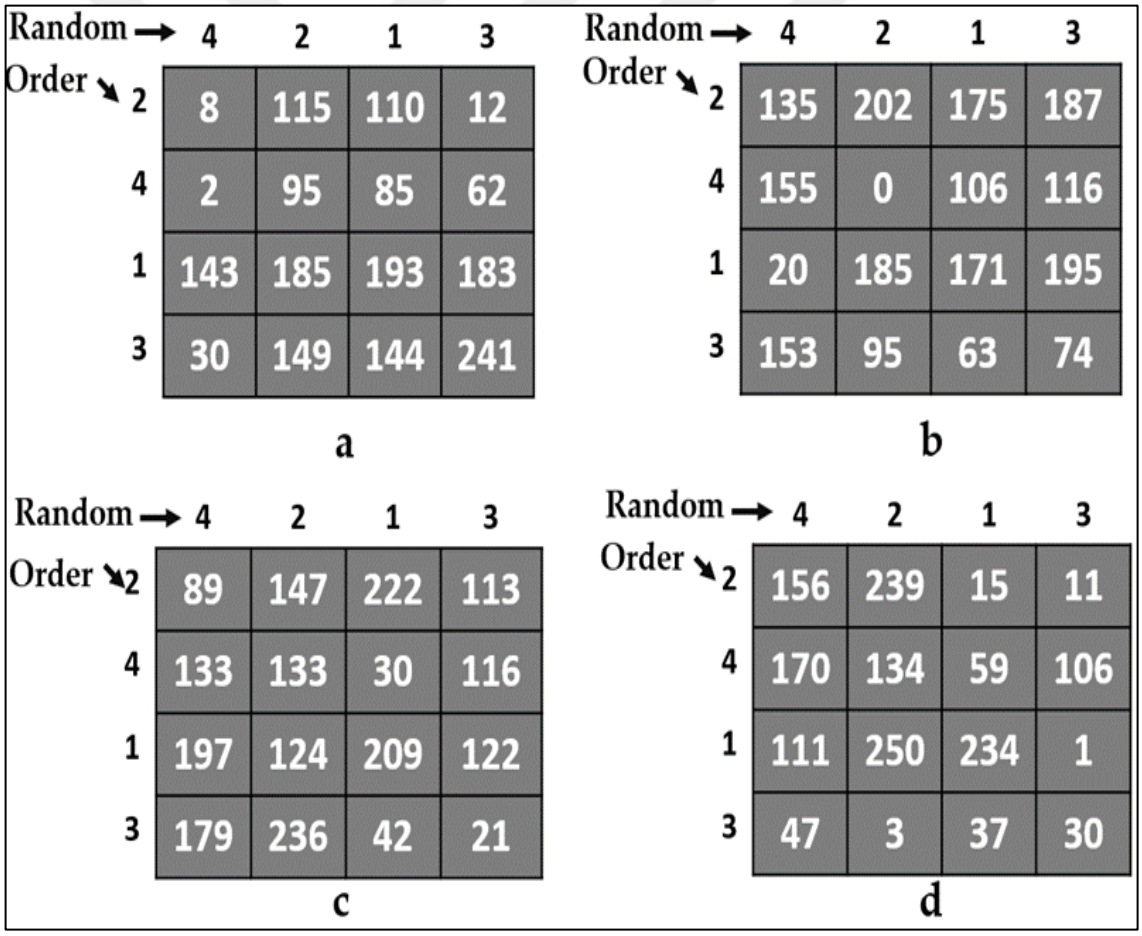


Figure 4.14: Implementation of XOR operators between (a) successive columns, (b) successive rows, (c) second round successive columns, (d) and second round successive rows.

To verify the performance of the proposed method against differential attacks, only one pixel in the original image (the pixel located at the address (2, 3)) was changed from 107 to 152 as seen in Figure 4.15. After that, the implementation of XOR operations will take place between successive columns and successive rows. This process is repeated for the second round as shown in Figure 4.16.

Random → / Order ↘	4	2	1	3
2	102	123	98	119
4	87	93	152	99
1	78	54	118	129
3	142	139	97	122

Figure 4.15: The altered image matrix.

The red value in Figure 4.15 is the altered value, while the red values in Figure 4.16 represent changes in the resulting image due to the small alterations in the original image after two rounds of XOR operations.

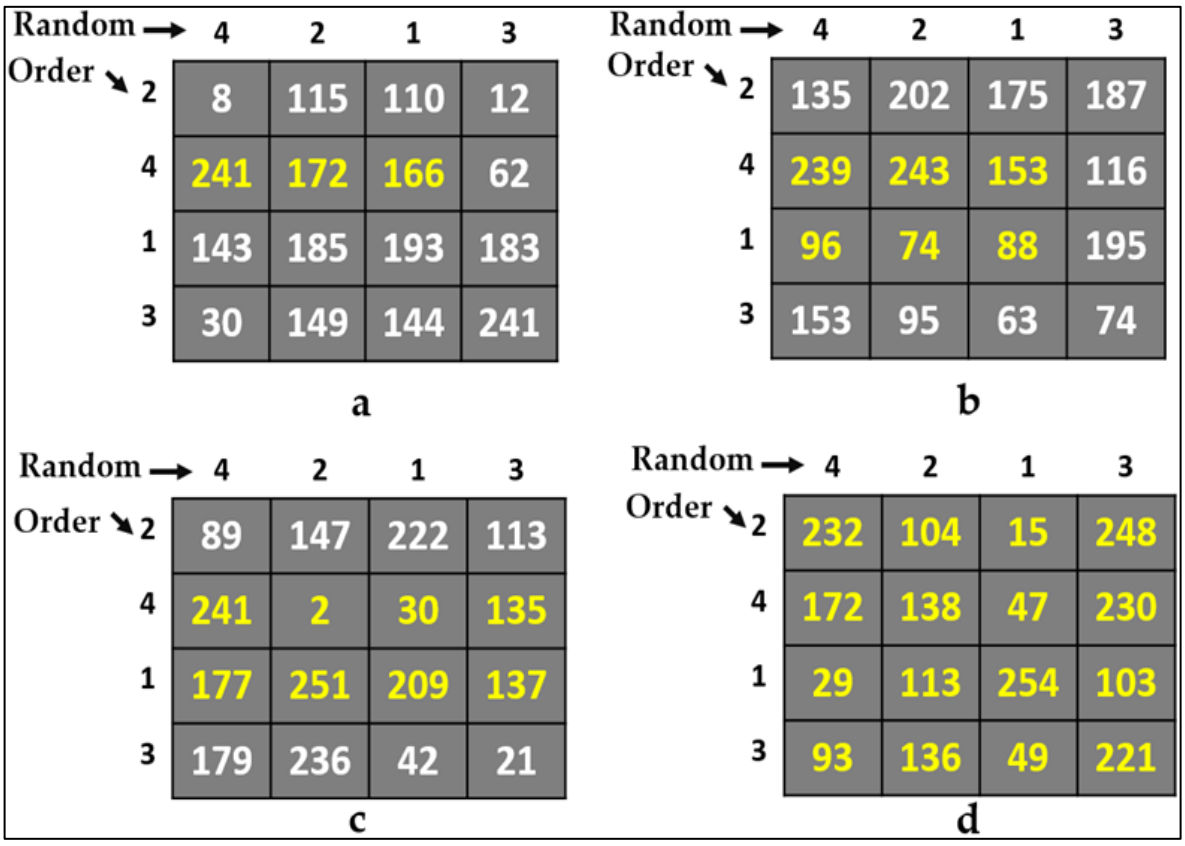


Figure 4.16: Changes due to the Small Alterations in the Original Image.

By altering the pixel located at the address (2, 3) as seen in Figure 4.15 leads to significant changes in the resulting image as shown in Figure 4.16 (d). Because in differential attacks cryptanalysis makes small changes to the plain image and encrypts it to find patterns or relationships between the plain image and its encrypted images, significant changes make differential attacks infeasible [13] and it clear that the resulting images are entirely different from those encrypted without any pixel alterations.

4.10 DECRYPTION PROCESS FOR DIFFUSED IMAGE

The first step in the decryption of diffused image is the generation of a random key using as inputs the same initial keys and control parameters used in the generation of random key for the image diffusion process. After generating the random key, the process of internal interaction between image pixels will be reversed by implementing XOR operators between successive (in

reverse of the random order) rows in the diffused image, starting with implementing XOR operators between the first row and the last row of the random order. The result of XOR process will be saved in the first row. The second process is done by conducting the same process between the last row and the second to last row. The result is saved in the last row. The XOR process will be continued until the first and first rows. Operations between these two rows and their result will be saved in the second row. XOR operations will be done to successive rows as mentioned above in the same order (according to the random numbers) as the first round of the XOR process. The second round is implemented the same as the as first round on the image resulting from the first round.

4.11 DECRYPTION PROCESS FOR CONFUSED IMAGE.

The decryption process for the confused image will recover the plain image. To achieve this there are a several processes that must be done. The random number generator used in the confusion method must have the same initial conditions and control parameters used generate same random key used in the encryption process. The generated random key must be sorted in ascending order while keeping the old index, in addition to the new index of the sorted key. The new and old indices are used to permute the confused image by permuting the pixels of the old index to the new index. By following this process for all image pixels, the plain image will be recovered from the confused image.

5. EXPERIMENTAL RESULT AND DISCUSSION

5.1 INTRODUCTION

In this chapter, the detailed results and necessary empirical preparations to verify the efficiency of the proposed methods are reported, and several methods of evaluation are used to make comparisons with recent image encryption methods. A standard image dataset was used to verify the performance of the proposed method. Evaluation using image encryption methods is more complex because parameters that control the whole image encryption framework overlap with each other to produce the desired encrypted image. To overcome this complexity methods of evaluating image encryption methods are concerned with different issues in the encryption system. For example, the NIST evaluation method is used to evaluate key randomness. NIST is a package consisting of several statistical methods and each of these statistical methods is responsible for verifying that the key sequence does not include any non-random elements. The second issue in image encryption evaluation is initial key security because some cryptanalysis attacks like brute force attacks try to reveal plain images from encrypted images by trying to use all possible combinations of key data. To resist this type of attack a long and sensitive key is required [41]. Therefore, key space and key sensitivity are evaluated to verify the performance of image encryption systems in terms of key security. Another image encryption issue is the statistical properties of the ciphered image. When a critical ciphered image is transferred between two authorized entities it is very easy for cryptanalysis to receive the image, especially after the spread of internet usage in recent years. Cryptanalysis tries to exploit statistical information that is collected from the ciphered image to reveal the plain image. To verify that the performance of the proposed image encryption framework achieved the desired criteria, multiple statistical evaluation methods such as the correlation between adjacent pixels, image histogram, and information entropy were implemented. In addition to these evaluation methods, MSE and PSNR were used to calculate the quality of the ciphered image. Finally, evaluation for hindering differential attacks was done using the Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) techniques to verify that the proposed image encryption system is robust against such attacks. All researchers in image encryption focus on

how to encrypt images with secure methods. To achieve the security and effectiveness of the proposed algorithm, we have performed many experiments on general image sets and representative experimental images.The MATLAB 2019 was used to implement the proposed scheme. The PC configuration included a 3.20 GHz CPU, 8 GB RAM (2400 MHz), and Microsoft Windows 10. The following section provides explanations of these methods.

5.2 RANDOMNESS ANALYSIS OF THE GENERATED NUMBER

To ensure the randomness of the proposed system the US National Institute of Standards and Technology (NIST) package was used. NIST is a statistical test suite used to analyze the randomness of true-random and pseudo-random number generators [33]. Implementing the NIST test for each file of random bits produced a summary report. Each test was run on a large number of bits sets from the tested file. P-value and proportion are two results from NIIST that indicate the randomness of the proposed random number generator. P-value is a statistical result from each NIST test. To explain this using an example, suppose that the P-value is equal to 0.97, this means that 97% of random sequences produced by the tested random number generator were better than the sequences produced by an ideal random number generator. Therefore, a large P-value indicates greater randomness. Proportion is an indication of the number of p-values over a 0.01 confidence interval and it is equal to the number of test sequences that pass the randomness test. This research includes two random number generators, the first one is a combination of Hénon maps, Sensitive Logistic Maps (SLM), an additive white Gaussian noise. It is used in the confusing process and NIST results for this generator are shown in Table 5.1.

Table 5.1: NIST results for the random number generator proposed for the confusion method.

	Statistical test	P-Value	Proportion
1	Frequency	0.9834	0.9991
2	Block Frequency	0.7344	1.000
3	Runs Template	0.9660	0.9983
4	Longest-Run	0.6265	0.9989
5	Binary Matrix	0.9884	0.9923
6	Fast Fourier Transform (FFT)	0.5491	0.9989
7	Non-Overlapping	0.9386	0.9995
8	Overlapping	0.8774	0.9957
9	Universal	0.9989	0.9984
10	Linear Complexity	0.8183	1.000
11	Serial	0.8686	0.9978
12	Approximate Entropy Information	0.9776	0.9994
13	Cusum Template	0.6473	0.9969
14	Random Excursions Template	0.9593	0.9997
15	Random Excursions Variant	0.9674	0.9997

To verify that the proposed random number generator for the confusion process is better than recent methods a comparison was done between the NIST results for the proposed random number generator and recent methods as shown in Table 5.2.

Table 5.2: Comparison between proposed random number generator for the Confusion method and two recent methods.

		Hani's et al. [71]		**Jallouli et al. [54]**		**Proposed scheme**	
	Statistical test	**P-Value**	**Proportion**	**P-Value**	**Proportion**	**P-Value**	**Proportion**
1	Frequency	**0.33**	**0.96**	**0.97**	**0.99**	**0.98**	**0.99**
2	Block Frequency	**0.67**	**0.99**	**0.05**	**0.99**	**0.73**	**1.00**
3	Runs Template	**0.93**	**0.99**	**0.53**	**1.00**	**0.96**	**0.99**
4	Longest-Run	**0.45**	**0.99**	**0.29**	**0.99**	**0.62**	**0.99**
5	Binary Matrix	**0.16**	**0.99**	**0.96**	**0.97**	**0.98**	**0.99**
6	Fast Fourier Transform (FFT)	**0.19**	**0.99**	**0.38**	**0.97**	**0.54**	**0.99**
7	Non-Overlapping	**0.79**	**0.99**	**N/A**	**N/A**	**0.93**	**0.99**
8	Overlapping	**0.12**	**0.99**	**0.63**	**0.98**	**0.87**	**0.99**
9	Universal	**0.35**	**0.98**	**0.23**	**0.98**	**0.99**	**0.99**
10	Linear Complexity	**0.31**	**0.97**	**0.29**	**0.99**	**0.81**	**1.00**
11	Serial	**0.96**	**0.97**	**0.60**	**1.00**	**0.86**	**0.99**
12	Approximate Entropy Information	**0.07**	**0.97**	**0.93**	**0.99**	**0.97**	**0.99**
13	Cusum Template	**0.73**	**0.97**	**N/A**	**N/A**	**0.64**	**0.99**
14	Random Excursions Template	**0.73**	**1.00**	**0.31**	**0.99**	**0.95**	**0.99**
15	Random Excursions Variant	**0.91**	**1.00**	**0.29**	**0.99**	**0.96**	**0.99**

The diffusion process for the proposed method is based on its own random number generator, which consists of an Extended Bernoulli Map (EBM), Tinkerbell, Burgers, and Ricker maps in addition to additive white Gaussian noise. To verify that the proposed random number generator for the diffusion process met image encryption criteria a NIST analysis was implemented for

this generator and the results of this implementation are shown in Table 5.3

Table 5.3: NIST results for the random number generator proposed for the diffusion method.

	Statistical test	P-Value	Proportion
1	Frequ*en*cy	**0.99**	**1.00**
2	Block Fr*equ*ency (BF)	**0.75**	**0.99**
3	Runs Template	**0.97**	**0.99**
4	Longest-Run	**0.67**	**1.00**
5	Binary Matrix	**0.98**	**0.99**
6	Fast Fourier Transform (FFT)	**0.59**	**0.99**
7	Non-Overlapping	**0.82**	**0.99**
8	Overlapping	**0.87**	**0.99**
9	Un*iver*sal	**0.66**	**0.97**
10	L*in*ear C*om*plexity	**0.47**	**0.99**
11	Serial	**0.91**	**1.00**
12	Approximate Entropy Information	**0.97**	**0.99**
13	Cusum Template	**0.92**	**0.99**
14	Random Excursions Template	**0.89**	**0.99**
15	Random Ex*cursi*ons Variant (REV)	**0.94**	**0.99**

To verify that the proposed random number generator for the diffusion process is better in term of randomness criteria a comparison with two recent methods is shown in Table 5.4.

Table 5.4: Comparison between proposed random number generator for the Diffusion method and two recent methods.

		Hanis et al. [71]		Jallouli et al.,[54]		Proposed scheme	
	Statistical test	**P-Value**	**Proportion**	**P-Value**	**Proportion**	**P-Value**	**Proportion**
1	Frequency	**0.33**	**0.96**	**0.97**	**0.99**	**0.99**	**1.00**
2	Block Frequency	**0.67**	**0.99**	**0.05**	**0.99**	**0.75**	**0.99**
3	Runs Template	**0.93**	**0.99**	**0.53**	**1.00**	**0.97**	**0.99**
4	Longest-Run	**0.45**	**0.99**	**0.29**	**0.99**	**0.67**	**1.00**
5	Binary Matrix	**0.16**	**0.99**	**0.96**	**0.97**	**0.98**	**0.99**
6	Fast Fourier Transform (FFT)	**0.19**	**0.99**	**0.38**	**0.97**	**0.59**	**0.99**
7	Non-Overlapping	**0.79**	**0.99**	**N/A**	**N/A**	**0.82**	**0.99**
8	Overlapping	**0.12**	**0.99**	**0.63**	**0.98**	**0.87**	**0.99**
9	Universal	**0.35**	**0.98**	**0.23**	**0.98**	**0.66**	**0.97**
10	Linear Complexity	**0.31**	**0.97**	**0.29**	**0.99**	**0.47**	**0.99**
11	Serial	**0.96**	**0.97**	**0.60**	**1.00**	**0.91**	**1.00**
12	Approximate Entropy Information	**0.07**	**0.97**	**0.93**	**0.99**	**0.97**	**0.99**
13	Cusum Template	**0.73**	**0.97**	**0.83**	**0.98**	**0.92**	**0.99**
14	Random Excursions Template	**0.73**	**1.00**	**0.31**	**0.99**	**0.89**	**0.99**
15	Random Excursions Variant	**0.91**	**1.00**	**0.29**	**0.99**	**0.94**	**0.99**

As seen in Table 5.4, the proposed random number generator for the diffusion process is better than the random number generator proposed by [71] and [54]. Due to the proposed generating technique and the proposed EBM which produce a random sequence with high randomness criteria the proposed random number generator for the diffusion process achieves randomness criteria better than recent methods.

5.3 KEY SPACE ANALYSIS

Ideal key generators for encryption purposes should use large key spaces to ensure that brute force attacks or exhaustive attacks are not possible. Key generators with key spaces smaller than 2^{128} are not acceptable because it is not sufficiently secure [20]. In the proposed system six chaotic maps are used to increase the security of the key generator and the precision of each initial value is equal to 10^{15}, therefore the key space for the proposed system can be calculated as seen in Table 5.5.

Table 5.5: The key spaces for proposed scheme.

Chaotic Map	Number of Initial Values	Key Space (Decimal)	Key Space (Binary)
Hénon	2	10^{30}	2^{100}
Amended Beroulli	2	10^{30}	2^{100}
Tinkerbell	2	10^{30}	2^{100}
Burger	2	10^{30}	2^{100}
Ricker	1	10^{15}	2^{50}
Total	9	10^{135}	2^{450}

Table 5.6: Comparison between the proposed scheme and several recent methods based on Key space size.

	Method	Key Space Size
1	Enayatifar et al.,	2^{240}
2	Choi et al.,	2^{448}
3	Bashir et al.,	2^{212}
4	Kulsoom et al.,	2^{167}
5	Kar et al.,	2^{256}
6	Proposed Method	2^{450}

5.4 CORRELATION COEFFICIENT BETWEEN ORIGINAL AND ENCRYPTED IMAGES

The evaluation of Correlation Coefficient (CC) is responsible for measuring closeness between plain images and related ciphered images [21]. The calculation of CC is done using Equations (5.1), (5.2), and (5.3):

$$A' = \frac{1}{M\ x\ N}\sum_{i=1}^{M}\sum_{j=1}^{N} A_{ij} \tag{5.1}$$

$$B' = \frac{1}{M\ x\ N}\sum_{i=1}^{M}\sum_{j=1}^{N} B_{ij} \tag{5.2}$$

$$CC = \sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{ij} - A'_{ij}\right)\left(B_{ij} - B'_{ij}\right)$$

$$\Big/\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N} A_{ij} - A'_{ij}\right)^2\left(\sum_{i=1}^{M}\sum_{j=1}^{N} B_{ij} - B'_{ij}\right)^2} \tag{5.3}$$

Here, A and B represent the plain and ciphered image, respectively. M and N are the dimensions of both plain and ciphered images, respectively. When CC is close to zero there is a significant difference between the plain and ciphered image, which indicates the strength of the encryption method. The correlation of adjacent pixels is a statistical property of a ciphered image. Therefore, cryptanalysis always tries to exploit such properties when attacking ciphered images, especially images that show obvious statistical properties. To verify the proposed method a metric was used to analyze the correlation of adjacent pixels. In plain images the correlation of adjacent pixel values should be close to 1 while the correlation of a successfully ciphered image should be close to zero [31]. The confusion process is concerned with weakening high correlations between adjacent pixels. Therefore, a good confusion process produces ciphered image with smaller correlations between adjacent pixels. The proposed encryption system was implemented on a SIPI standard image dataset and three datasets taken from a mobile phone. Implementing correlation equations is done by choosing 5000 pixels randomly from the image and analyzing correlations between these pixels and pixels that are located beside these pixels in the horizontal, vertical, and diagonal directions. Table 5.7 shows the correlation of adjacent

pixels for the plain images chosen from the SIPI dataset in addition to the three images taken by a mobile camera.

Table 5.7: Correlation of adjacent pixels for plain-Images.

	Image Name	Image Type	Size	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
1	Girl	RGB	256 × 256	0.9893	0.9688	0.9610
2	Tiffany	RGB	256 × 256	0.9426	0.9682	0.9945
3	Elaine	grayscale	512 × 512	0.9519	0.9801	0.9724
4	Cameraman	grayscale	256 × 256	0.9682	0.9583	0.8569
5	Lena	grayscale	512 × 512	0.9785	0.9880	0.9855
6	Baboon	RGB	512 × 512	0.5119	0.6024	0.6876
7	Cactus	RGB	512 × 512	0.9763	0.9902	0.9848
8	Dolls	RGB	512 × 512	0.9847	0.9903	0.9624
9	City	RGB	512 × 512	0.9738	0.9824	0.9572
10	Man	grayscale	1024 × 1024	0.9889	0.9932	0.9789

Table 5.7 show that the correlation for the plain image is very high because the difference among a value of pixels, and the neighbour pixels is very small at smooth areas while the difference is increasing at sharp edges, and it is clear which a smooth region (area) in the used images is greater than the sharp edge therefore the correlation is very high (close to one).

For baboon the correlation relatively low because the ratio of smooth area and sharp edge is close to one. Table 5.8 display a co*rr*elation bet*wee*n adjacent pixels for encrypted image resulting from the proposed encryption system on different RGB and grey scale images chosen from the SIPI dataset in addition to the three images taken by mobile phone.

Table 5.8: Correlation between adjacent pixels for the encrypted image.

	Name	Image Type	Size	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
1	Girl	RGB	256 × 256	0.002713	-0.000792	0.001218
2	Tiffany	RGB	256 × 256	-0.000982	-0.002321	0.001821
3	Elaine	grayscale	512 × 512	0.003541	-0.000721	0.001298
4	Cameraman	grayscale	256 × 256	0.00111	-0.002107	-0.007655
5	Lena	grayscale	512 × 512	0.000732	0.000391	0.000320
6	Baboon	RGB	512 × 512	0.000643	0.000433	-0.002219
7	Cactus	RGB	512 × 512	-0.007272	0.006551	0.002221
8	Dolls	RGB	512 × 512	-0.002117	0.000457	-0.002994
9	City	RGB	512 × 512	-0.008188	-0.002218	0.000221
10	Man	grayscale	1024 × 1024	0.003232	-0.000233	0.002229

As it seen in Table 5.8 the correlation between adjacent pixels for the encrypted image is very low due the implementation of the proposed confusion method scrambles the image pixels randomly and the relation between the adjacent pixels in horizontal, vertical and diagonal directions is in random order because the difference is highly increases, highly decreases, slowly increases or slowly decreases.To verify the new image encryption system a comparison between the results of proposed system and the results of several recent methods is shown in Table 5.9.

Table 5.9: Correlation between adjacent pixels for the encrypted image and Existing methods.

Method	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Choi *et al.*,	-0.003	-0.004	-0.009
Enayatifar *et al.*,	0.0008	0.0021	0.0005
Bashir *et al.*,	0.0238	-0.0182	0.0073
Kulsoom *et al.*,	0.0027	0.0005	-0.0045
Kar *et al.*,	-0.0076	-0.0034	-0.0074
Proposed Method	**0.000732**	**0.000391**	**0.00032**

Table5.9 shows that the proposed method is better than other recent methods in terms of correlation. The image used in this comparison is a Lena 512 * 512 grayscale image.

5.5 INFORMATION ENTROPY ANALYSIS

Information Entropy is used to measure uncertain associations between random variables [41]. A greyscale image has a theoretical entropy value of 8 bits. Image encryption algorithms should produce an encrypted image with an entropy value similar to greyscale values [28][29]. Information entropy can be calculated using Equation 16:

$$H(m) = \sum_{i=0}^{m-1} P(m_i) log_2 \frac{1}{P(m_i)} \quad (5.4)$$

where M is the whole number of pixels, (mi) symbolizes the possibility of occurrence of symbol (mi) and log denotes the base 2 logarithm so that the entropy is expressed in binary mode. The amount of information entropy in a perfect random image is 8. When the cipher image entropy is close to 8, this indicates that the cipher images are almost random, and the used algorithm is secure against entropy-based attack. The amount of information entropy in a perfect random image is 8 [26]. Table 5.10 shows the entropy results for the proposed image encryption system.

Table 5.10: The Entropy outcome for the proposed work.

Image Name (IM)	*Image Type*	Size	Entropy
Girl	***RGB***	**256 × 256**	8
Tiffany	***RGB***	**256 × 256**	8
Elaine	***grayscale***	**512 × 512**	8
Cameraman	***grayscale***	**256 × 256**	8
Lena	***grayscale***	**512 × 512**	8
Baboon	***RGB***	**512 × 512**	8
Cactus	***RGB***	**512 × 512**	8
Dolls	***RGB***	**512 × 512**	8
City	***RGB***	**512 × 512**	8
Man	***grayscale***	**1024 × 1024**	8

Table 5.10 shows that the proposed system produces encrypted images with perfect results in terms of entropy evaluation (8) regardless of image size or type.

In recent image encryption systems, entropy is always close to 8 but it is not equal to 8. This can be seen in Table 5.11.

Table 5.11: Entropy results for the proposed image encryption and existing methods.

Method	(Enayatifar *et al.*)	(Choi *et al.*,)	(Bashir *et al.*,)	(Kulsoom *et al.*)	(Kar *et al.*)	Proposed method
Average Entropy	**7.9994**	**7.8198**	**7.9992**	**7.9972**	**7.9872**	**8.0**

5.6 QUANTITATIVE HISTOGRAM ANALYSIS

Image histogram is the description of occurrence frequencies for each pixel value in an image. The histogram of the encrypted image should be fully statistically different from the histogram of the plain image and should be uniform to avoid statistical histogram attack [16]. In image histogram plots, each bar represents specific number of occurrences for the corresponding pixel value. In 8-bit greyscale images the pixels value is arranged from 0 (which represents a black pixel) and 255 (which represents a white pixel) [14]. If the histogram of the generated encrypted image is absolutely flat which indicates that the histogram is in perfect result as it desired. Histogram of encrypted image represents the sternness of the encryption method against statistical attack. Therefore, the quantitative analysis is important to estimate the value of uniform pixels distribution [9] this quantitative test can be performed by the using of variance metric. The equation 5.5 is used to calculate the variance of encrypted image.

$$Var\ (H) = \frac{1}{n^2}\sum_{i=1}^{n}\frac{(H_i - H_j)}{2} \qquad (5.5)$$

where Hi, Hj represents occurrence of different pixel values (i, j).

The histogram variance results for the tested images are tabulated in Table 5.12 and this table show that the variance of all of these tested images is equal to zero which means that the uniformity distribution of the proposed method is ideal and the statistical attack for the proposed method is infeasibl.

Table 5.12: Variance of the encrypted image.

Image Name	Image Type	Size	Variance
Girl	*RGB*	*256 × 256*	*0*
Tiffany	*RGB*	*256 × 256*	*0*
Elaine	*grayscale*	*512 × 512*	*0*
Cameraman	*grayscale*	*256 × 256*	*0*
Lena	*grayscale*	*512 × 512*	*0*
Baboon	*RGB*	*512 × 512*	*0*
Cactus	*RGB*	*512 × 512*	*0*
Dolls	*RGB*	*512 × 512*	*0*
City	*RGB*	*512 × 512*	*0*
Man	*grayscale*	*1024 × 1024*	*0*

As seen in Table 5.12 there is no variance in the histograms for all encrypted images regardless the size or type (RGB or grayscale) because the occurrences frequency is fixed for all events. A comparison with other approaches is conducted to show that the suggested method's quantitative histogram analysis is superior to other ways as seen in Table 5.13.

Table 5.13: Comparison between variance of proposed method and existing recent methods.

Method	(Enayatifar *et al.*, 2017)	(Choi *et al.*, 2016)	(Bashir *et al.*, 2016)	(Kar *et al.*, 2017)	Proposed Method
Variance	5118.094	977.02	5554.82	1209.4	**0**

The proposed method is better than all of the old methods in terms of variance results as seen in the above table because the proposed method achieve ideal histogram, but all other methods did not achieve such histogram.

5.7 MSE AND PEAK SIGNAL TO NOISE RATIO ANALYSIS

Mean Square Errors (MSE) between plain and ciphered images are used to evaluate the reliability of the proposed framework. This evaluation was achieved by implementing Equation 5.6:

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}(a(i,j) - b(i,j)^2) \quad (5.6)$$

where M and N are the dimensions of both the plain and ciphered images, a (i, j) and b (i , j) are pixels value in the i row and j column for the plain and ciphered images. Larger MSEs provide better image encryption security [17].

Furthermore, peak signal to noise ratio or PSNR is used to evaluate the quality of the proposed image encryption framework, which is done by implementing Equation 5.7:

$$PSNR = 10log_{10}\frac{(I_{max}^2)}{MSE} \quad (5.7)$$

where Imax is the maximum possible pixel value of an image. A minimum PSNR value between plain and ciphered images indicates great differences and good encryption. To evaluate MSE and PSNR calculations were made using both plain and encrypted images.

A big MSE and a small PSNR are desirable for encryption. The evaluation results for MSE and PSNR are shown in Table 5.14.

Table 5.14: MSE and PSNR results for the proposed method.

Image Name	Image Type	Size	MSE	PSNR
Girl	RGB	**256 × 256**	**12748**	**7.07**
Tiffany	RGB	**256 × 256**	**9274**	**8.45**
Elaine	grayscale	**512 × 512**	**8679**	**8.74**
Cameraman	grayscale	**256 × 256**	**13418**	**6.85**
Lena	grayscale	**512 × 512**	**13728**	**8.19**
Baboon	RGB	**512 × 512**	**7984**	**8.95**
Cactus	RGB	**512 × 512**	**6816**	**9.79**
Dolls	RGB	**512 × 512**	**8567**	**8.80**
City	RGB	**512 × 512**	**10332**	**7.98**
Man	grayscale	**1024 × 1024**	**9924**	**8.16**

To verify the proposed method in terms of the MSE and PSNR results, Table 5.15 illustrates a comparison of the proposed method with several recent image encryption methods.

Table 5.15: Comparison of MSE and PSNR for the proposed method and existing recent methods.

Method	MSE	PSNR
(Gu et al.)	9595	8.31
(Kar et al.)	9551	8.33
(Bashir et al.)	9465	8.37
Proposed Method	**9864**	**8.19**

In Table 5.15, both of the proposed methods and other recent methods used a grayscale Lena image with a size of 512*512 pixels.

Table 5.14 and Table 5.15 show that the MSE and PSNR of the proposed framework is achieve good results and it is better than the current methods MSE indicates the difference between the plain image and the encrypted image, and the largest value is the better. PSNR is indicates the similarity between plain image and encrypted image the smallest value is better in results because it means the similarity is at minimum.

5.8 DIFFERENTIAL ANALYSIS

The most useful security analysis for differential attack in image encryption is Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR focuses on the total absolute number of changed pixels during a differential attack, while UACI is concerned with the average change in a pair of ciphered pixels.

Suppose c1 and c2 are ciphered images before and after small changes are made to the plain image. The pixel value at grid (i,j) in c1 and c2 are denoted as c1(i, j) and c2 (i, j) and a bipolar array D is defined in Equation 5.8. The NPCR and UACI are mathematically defined by Equation 5.9 and 5.10, respectively.

$$D(i,j) = \begin{cases} 0, if\ c1(i,j)=c2(i,j) \\ 1, if\ c1(i,j)\neq c2(i,j) \end{cases} \quad (5.8)$$

$$NPCR = \frac{1}{M*N}\sum_{i,j}^{M,N} D(i,j) * 100\% \quad (5.9)$$

$$UACI = \frac{1}{M*N}\sum_{i,j}^{M,N} \frac{|c1(i,j)-c2(i,j)|}{255} * 100\% \quad (5.10)$$

where M and N are the width and height of c1 and c2.

The Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity

(UACI) techniques were used to analyze the security of the image encryption methods in terms of differential attacks. The results for the proposed method are shown in Table 5.16.

Table 5.16: NPCR and UACI for proposed method.

Image Name	Image Type	Size	NPCR	UACI
Girl	RGB	256 × 256	99.63	33.87
Tiffany	RGB	256 × 256	99.81	33.92
Elaine	grayscale	512 × 512	99.65	34.39
Cameraman	grayscale	256 × 256	99.59	33.30
Lena	grayscale	512 × 512	99.83	34.10
Baboon	RGB	512 × 512	99.66	33.52
Cactus	RGB	512 × 512	99.63	33.37
Dolls	RGB	512 × 512	99.67	33.32
City	RGB	512 × 512	99.91	34.65
Man	grayscale	1024 × 1024	99.65	33.35

The results of the differential attack analysis show that the value of NPCR is >99.6 and UACI is >33.3. Therefore, the proposed method is very sensitive to a small change in the plain image.

A comparison between the proposed method and recent methods is shown in Table 5.17 This comparison shows that the results for the proposed method are better than the results of other recent methods in terms of differential attack resistance.

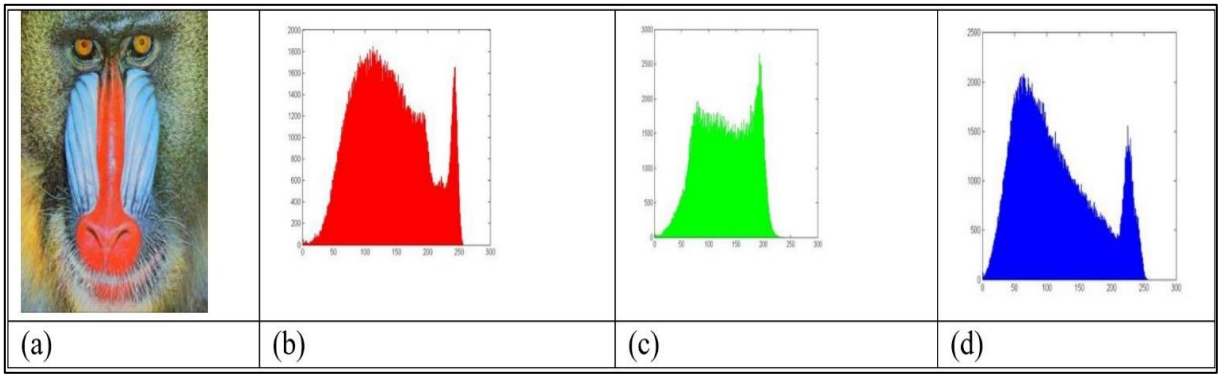
Table 5.17: NPCR and UACI Comparison between the proposed method and recent methods.

	Method	NPCR	UACI
1	(Enayatifar *et al.*, 2017)	99.63	33.59
2	(Choi *et al.*, 2016)	99.60	28.62
3	(Bashir *et al.*, 2016)	72.24	20.06
4	(Kulsoom *et al.*, 2016)	99.61	28.60
5	(Kar *et al.*, 2017)	99.69	33.50
6	**Proposed Method**	**99.83**	**34.10**

The NPCR reflect the ratio of the pixel affected by tiny change in plain image the ratio is > 99 which means more than 99% of image pixels is changed when small change made to the plain image while UACI reflect the average of the effect of this change to all image pixels.

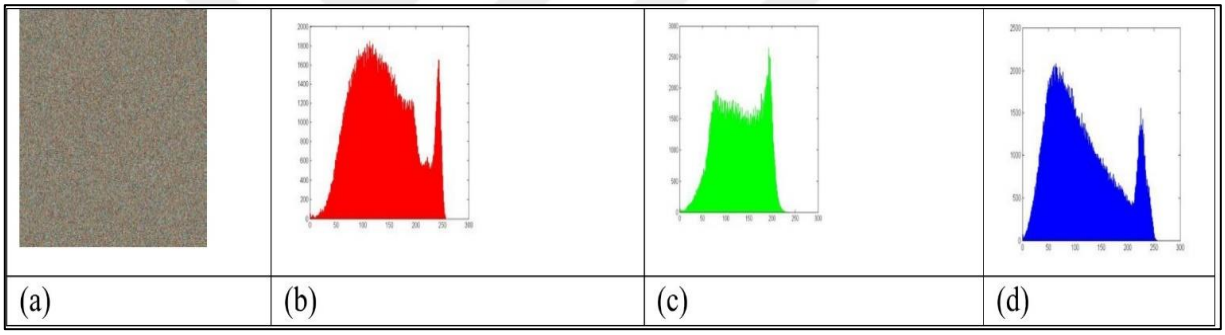
5.9 HISTOGRAM ANALYSIS

In this section performance result of the proposed confusion method for histogram analysis. The intended empirical results of the implementation of the confusion method minimized correlations between adjacent pixels for the confused image, while the other results such as histogram and information entropy are still the same as the plain image. The confusion method is responsible for breaking correlations between image pixels by redistributing pixels inside the image coordinates. Figure 5.1 shows the plain image (baboon) with 512*512pixel dimensions and its related RGB histogram components. While figure 5.2 shows the encryption image histogram of baboon image.



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

Figure 5.1: Plain image and its RGB Histogram (a) Baboon Image (b)(c)(d) RGB Histogram Components.



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

Figure 5.2: Confused Baboon Image and its RGB Histogram (a) Confused Image (b)(c)(d) RGB Histogram Components.

5.10 SUMMARY

This chapter verified the proposed encryption system and compared it to several recent methods. Because there is no specific definition or aspect for randomness the evaluation of the encryption system was complicated and needed multiple calculations, and this study use multiple methods to ensure that the proposed encryption system is better in terms of image encryption criteria. The random number keys, key security, statistical properties, the quality of the ciphered image, and resistance against differential attack were analyzed to verify the proposed system. A comparison with several recent methods was also conducted. The results achieved by analysis show that the proposed image encryption system is better in all criteria and has ideal results for both histogram and information entropy were achieve.

6. CONCLUSION AND FUTURE WORKS

6.1 INTRODUCTION

In this chapter the contribution, conclusion and future work are discussed for proposed method. To achieve the ideal results in image encryption field, a new encryption framework was proposed in this study, and several contributions. Ordinary chaotic image encryption frameworks have two processes, the confusion process and the diffusion process. The proposed framework proposed a new process for confusion and diffusion processes. In the proposed image confusion process, a Sensitive Logistic Map (SLM) was proposed to achieve more sensitivity to the initial conditions along with different chaotic maps. While in the proposed diffusion process Extended Bernoulli Map (EBM) was proposed to achieve random number generator with high randomness criteria and long key space size to increase the security of the diffusion process, in addition, a method of Internal Interaction between Image Pixels (IIIP) was proposed to increase the resistance against differential attack. The study contributions can be listed as follows:

6.2 IMAGE ENCRYPTION FRAMEWORK BASED ON THREE PROCESSES

Different contributions are introduced within the proposed work. These contributions are presented in confusion and diffusion procedure. The confusion procedure consists of different chaotic maps used to generate the random and chaos key. This key is used during the encrypted process to get the cipher images. The result of the confusion stage becomes the input to the diffusion procedure. the diffusion procedure consists of different chaotic maps which are used to generate a random and chaotic key. This key is used with the diffusion process to encrypt the resulting image of the confusing process. A sensitive Logistic Map (SLM) is proposed in this research to increase the randomization during the key generation. Also, Extended Bernoulli Map (EBM) is proposed from the original Bernoulli Map algorithm to increase the randomization of the proposed key

6.2.1 Sensitive Logistic Map (SLM)

The new Sensitive Logistic Map (SLM) shows more sensitivity to the initial conditions and control parameters. Both the original and amended chaotic logistic map are shown in Equation (6.1) and Equation (6.2).

$$x^{n+1} = rx^n(1 - x^n) \quad (6.1)$$

$$x^{n+1} = rx^n(1 - x^n) * m \; mod \; k \quad (6.2)$$

where n and k are integers and m is greater than one. In the proposed amended chaotic logistic map, it is clear that there are two additional control parameters that lead to increase security. Also, the behavior of the proposed map is more sensitive to initial condition, because of the multiplication by m parameter. Also, the using of modulus operation increase the randomness of the proposed SLM.

6.2.2 Extended Bernoulli Map (EBM)

A new method based on the Bernoulli map was proposed in this study. Equation (6.3) and Equation (6.4) show both the original and Extended Bernoulli Map (EBM) sequentially. EBM equation has two initial conditions, meaning that the key space size of the new equation is duplicated and according to that the security of the generator will be increased.

$$x^{n+1} = kx^n \; mod \; 1 \quad (6.3)$$

$$X_n = \big(2 * (Xn - 1) + (Xn - 2)\big) \; mod 1 \quad (6.4)$$

where n and k are integer and xn, xn−1 are the initial values. The amendment of the Bernoulli map makes generated numbers more random because the output of each iteration is depending on two random inputs instead of one random input for the Bernoulli map.

6.2.3 Internal Interaction Between Image Pixels (IIIP)

To achieve image encryption system with high resistance to the differential attack, a simple and efficient method was proposed this method is named Internal Interaction between Image Pixels (IIIP). In this method an XOR operator is implemented between each two successive (randomly) rows and each two successive (randomly) column twice times to ensure that any slight change in any pixel of plain image will produce significant change in the ciphered image.

6.3 FUTURE WORK

Today image encryption is essential especially in critical fields and too many researchers focus on encryption frameworks that produce encrypted images with highly secure criteria. In this study, some of these criteria were achieved with perfect results, while the rest had very good results. To idealize correlation criteria the additional process proposed in this study can be used by carefully selecting two values to implement XOR operations to achieve ideal correlation results. The investigation of new chaotic maps with large key space requirements is important to avoid complexity when using large keys because existing methods focus on merging multiple chaotic maps to create large key spaces.

6.4 CONCLUSION

Despite Shannon (1949) proposed that the ideal secrecy system for cryptography is consist of two main processes which are confusion and diffusion, but such system is not achieved yet. The proposed study show that the achieving of ideal secrecy system is done along with a new confusion and diffusion processes. The execution of the presented work obtains better results in histogram analysis and information entropy for the resulting image. Also, the rest statistical properties such as correlation between adjacent pixels, Variance, MSE and PSNR of the ciphered image obtain significant enhancement. The proposed SLM and EBM methods enhance the key security by increase key space size with maintain key sensitivity. High correlations between neighbouring pixels are broken by the suggested confusion process, whereas the proposed diffusion process improves resistance to differential attack while also erasing the

statistical characteristics of the encrypted image.

REFERENCES

[1] Lai Q, Wan Z, Zhang H, Chen G. "Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption." *IEEE Transactions on Neural Networks and Learning Systems*. Feb 10.2022.

[2] Wang X, Yin S, Shafiq M, Laghari AA, Karim S, Cheikhrouhou O, Alhakami W, Hamam H. "A new V-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption." *Security and Communication Networks.* Feb 14;2022.

[3] Gong LH, Luo HX, Wu RQ, Zhou NR." New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG." *Physica A: Statistical Mechanics and its Applications.* Apr 1;591:126793.2022.

[4] Hua Z, Zhu Z, Yi S, Zhang Z, Huang H. "Cross-plane colour image encryption using a two-dimensional logistic tent modular map." *Information Sciences*. Feb 6;546:1063-83.2021.

[5] Wang X, Yang J. "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient." *Information Sciences*. Aug 1; 569:217-40.2021.

[6] Bentoutou Y, Bensikaddour EH, Taleb N, Bounoua N. "An improved image encryption algorithm for satellite applications." *Advances in Space Research*. Jul 1;66(1):176-92.2020.

[7] Pourasad Y, Ranjbarzadeh R, Mardani A. "A new algorithm for digital image encryption based on chaos theory." *Entropy*. Mar;23(3):341.2021.

[8] Hua Z, Zhu Z, Yi S, Zhang Z, Huang H. "Cross-plane colour image encryption using a two-dimensional logistic tent modular map." *Information Sciences*. Feb 6; 546:1063-83.2021.

[9] Farah MB, Guesmi R, Kachouri A, Samet M. "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation." *Optics & Laser Technology*. Jan 1; 121:105777.2020.

[10] Zhang L, Zhang X. “Multiple-image encryption algorithm based on bit planes and chaos.” *Multimedia Tools and Applications*. Aug;79(29):20753-71.2020.

[11] Yasser I, Khalifa F, Mohamed MA, Samrah AS. “A new image encryption scheme based on hybrid chaotic maps.” *Complexity*. 2020 Jul 25;2020.

[12] Farah MA, Farah A, Farah T.“An image encryption scheme based on a new hybrid chaotic map and optimized substitution box.” *Nonlinear Dynamics.* Mar;99(4):3041-64.2020.

[13] Wang X, Gao S.“Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory.” *Information sciences*. Jan 1; 507:16-36.2020.

[14] Kaur M, Singh D, Uppal RS.” Parallel strength pareto evolutionary algorithm-II based image encryption.” *IET Image Processing*. Apr 30;14(6):1015-26.2020.

[15] Song W, Zheng Y, Fu C, Shan P.” A novel batch image encryption algorithm using parallel computing.” *Information Sciences*. May 1; 518:211-24.2020.

[16] Wang X, Gao S.” Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network.” *Information sciences*. Oct 1; 539:195-214.2020.

[17] Kumar M, Lahcen R, Mohapatra RN, Alwala C, Kurella S.” Review of image encryption techniques.” J. *Comput. Eng..;*14(1):31-7.2020.

[18] Jithin KC, Sankar S.” Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set.” *Journal of Information Security and Applications*. Feb 1; 50:102428.2020.

[19] Farah MB, Guesmi R, Kachouri A, Samet M.” A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation.” *Optics & Laser Technology*. Jan 1; 121:105777.2020.

[20] Jiang N, Dong X, Hu H, Ji Z, Zhang W.” Quantum image encryption based on Henon mapping.” *International Journal of Theoretical Physics*. Mar;58(3):979-91.2019.

[21] Alsafasfeh QH, Arfoa AA.” Image encryption based on the general approach for multiple chaotic systems.” J. *Signal Inf. Process*. Aug 31;2(3):238-44.2011.

[22] Abundiz-Pérez F, Cruz-Hernández C, Murillo-Escobar MA, López-Gutiérrez RM, Arellano-Delgado A.” A fingerprint image encryption scheme based on hyperchaotic Rössler map.” *Mathematical Problems in Engineering*. Jan 1;2016.

[23] Liu R, Tian X.” New algorithm for color image encryption using chaotic map and spatial bit-level permutation.”

[24] Jain A.” Pixel chaotic shuffling and Arnold map-based Image Security Using Complex Wavelet Transform.” *Journal of Network Communications and Emerging Technologies* (JNCET).;6(5):8-11.2016.

[25] Luo Y, Ouyang X, Liu J, Cao L, Zou Y.” An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system.” *Soft Computing*. Jan 9:1-27.2022.

[26] Taha MS, Rahem MS, Hashim MM, Khalid HN.” High payload image steganography scheme with minimum distortion based on distinction grade value method.” *Multimedia Tools and Applications*. Mar 25:1-34.2022.

[27] Al-Roithy BO, Gutub A. “Remodeling randomness prioritization to boost-up security of RGB image encryption.” *Multimedia Tools and Applications*. Jul;80(18):28521-81.2021.

[28] Bhowmick A, Sinha N, Arjunan RV, Kishore B.” Permutation-Substitution architecture-based image encryption algorithm using middle square and RC4 PRNG.” *In International Conference on Inventive Systems and Control (ICISC)* Jan 19 (pp. 1-6). IEEE.2017

[29] ElBeltagy M, Alexan W, Elkhamry A, Moustafa M, Hussein HH.” Image Encryption Through Rössler System, PRNG S-Box and Recamán's Sequence.” *In IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* Jan 26 (pp. 0716-0722). IEEE.2022.

[30] Chen E, Min L, Chen G.” Discrete chaotic systems with one-line equilibria and their application to image encryption.” *International Journal of Bifurcation and Chaos*. Mar;27(03):1750046.2017.

[31] Gutub A, Al-Roithy B.” Varying PRNG to improve image cryptography implementation.” *Journal of Engineering Research*. Sep 1;9(3A).2021.

[32] Al-Roithy B, Gutub A.” Trustworthy image security via involving binary and chaotic gravitational searching within PRNG selections.” Int. J. Comput. Sci. *Network Secur. (IJCSNS*). Dec;20(12):167-76.2020.

[33] Annadurai S, Manoj R, Jathanna RD.” A novel self-transforming image encryption algorithm using intrinsically mutating PRNG.” InProceedings of First International Conference on Smart System, *Innovations and Computing* (pp. 203-214). Springer, Singapore.2018.

[34] Sani RH, Behnia S, Akhshani A.” Creation of S-box based on a hierarchy of Julia sets: image encryption approach.” *Multidimensional Systems and Signal Processing*. Jun 23:1-24.2021.

[35] Man Z, Li J, Di X, Liu X, Zhou J, Wang J, Zhang X. “A novel image encryption algorithm based on least squares generative adversarial network random number generator.” *Multimedia Tools and Applications*. Jul;80(18):27445-69.2021.

[36] Broumandnia A.”Designing digital image encryption using 2D and 3D reversible modular chaotic maps.” *Journal of Information Security and Applications*. Aug 1; 47:188-98.2019.

[37] Hanis S, Amutha R.” A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure.” *Nonlinear Dynamics*. Jan;95(1):421-32.2019.

[38] Alawida M, Teh JS, Samsudin A.” An image encryption scheme based on hybridizing digital chaos and finite state machine.” *Signal Processing*. Nov 1; 164:249-66.2019.

[39] Kaur M, Singh S, Kaur M, Singh A, Singh D.” A Systematic Review of Metaheuristic-based Image Encryption Techniques.” *Archives of Computational Methods in Engineering*. Oct 28:1-5.2021.

[40] Luo Y, Yu J, Lai W, Liu L.” A novel chaotic image encryption algorithm based on improved baker map and logistic map.” *Multimedia Tools and Applications*. Aug;78(15):22023-43.2019.

[41] Shaukat S, Arshid AL, Eleyan A, SHAH SA, AHMAD J.” Chaos theory and its application: An essential framework for image encryption.” *Chaos Theory and Applications*. Jun 30;2(1):17-22.2020.

[42] Zhou N, Chen W, Yan X, Wang Y.” Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system.” *Quantum Information Processing*. Jun;17(6):1-24.2018.

[43] Chen LP, Yin H, Yuan LG, Lopes AM, Machado JA, Wu RC.” A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations.” *Frontiers of Information Technology & Electronic Engineering*. Jun;21(6):866-79.2020.

[44] Girdhar A, Kumar V.” A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences.” *Multimedia Tools and Applications*. Oct;77(20):27017-39.2018.

[45] Mondal B, Kumar P, Singh S.” A chaotic permutation and diffusion-based image encryption algorithm for secure communications.” *Multimedia Tools and Applications*. Dec;77(23):31177-98.2018.

[46] Ahmad J, Hwang SO.” A secure image encryption scheme based on chaotic maps and affine transformation.” *Multimedia Tools and Applications*. Nov;75(21):13951-76.2016.

[47] Guesmi R, Ben Farah MA, Kachouri A, Samet M.“Hash key-based image encryption using crossover operator and chaos.” *Multimedia tools and applications*. Apr;75(8):4753-69.2016.

[48] Parvin Z, Seyedarabi H, Shamsi M.” A new secure and sensitive image encryption scheme based on new substitution with chaotic function.” *Multimedia Tools and Applications.* Sep;75(17):10631-48.2016.

[49] Kumari M, Gupta S, Sardana P.” A survey of image encryption algorithms.” *3D Research.* Dec;8(4):1-35.2017.

[50] Li C, Lin D, Lü J, Hao F.” Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography.*” IEEE multimedia*. Oct 17;25(4):46-56.2018.

[51] Li C, Luo G, Qin K, Li C.” An image encryption scheme based on chaotic tent map.” *Nonlinear Dynamics*. Jan;87(1):127-33.2017.

[52] Wang X, Wang S, Zhang Y, Guo K. “A novel image encryption algorithm based on chaotic shuffling method.” *Information Security Journal: A Global Perspective*. Jan 2;26(1):7-16.2017.

[53] Wang J, Wang QH, Hu Y.“Image encryption using compressive sensing and detour cylindrical diffraction.” *IEEE Photonics Journal*. Apr 30;10(3):1-4.2018.

[54] Chai X.” An image encryption algorithm based on bit level Brownian motion and new chaotic systems.” *Multimedia Tools and Applications*. Jan;76(1):1159-75.2017.

[55] Huang H, Yang S.” Colour image encryption based on logistic mapping and double random-phase encoding.” *IET Image Processing*. Mar 30;11(4):211-6.2017.

[56] Zhao T, Ran Q, Yuan L, Chi Y, Ma J.” Security of image encryption scheme based on multi-parameter fractional Fourier transform.” *Optics Communications*. Oct 1; 376:47-51.2016.

[57] Yap WS, Phan RC, Goi BM, Yau WC, Heng SH. “On the effective subkey space of some image encryption algorithms using external key.” *Journal of Visual Communication and Image Representation*. Oct 1; 40:51-7.2016.

[58] Yavuz E, Yazıcı R, Kasapbaşı MC, Yamaç E.” A chaos-based image encryption algorithm with simple logical functions.” *Computers & Electrical Engineering*. Aug 1; 54:471-83.2016.

[59] Niyat AY, Moattar MH, Torshiz MN.” Color image encryption based on hybrid hyper-chaotic system and cellular automata.” *Optics and Lasers in Engineering*. Mar 1; 90:225-37.2017.

[60] Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JB.” Fusion of confusion and diffusion: a novel image encryption approach.” *Telecommunication Systems.* May;65(1):65-78.2017.

[61] Gong LH, He XT, Cheng S, Hua TX, Zhou NR.” Quantum image encryption algorithm based on quantum image XOR operations.” *International Journal of Theoretical Physics*. Jul;55(7):3234-50.2016.

[62] Arif J, Khan MA, Ghaleb B, Ahmad J, Munir A, Rashid U, Al-Dubai A.” A Novel Chaotic Permutation–Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution.” *IEEE Access*. Jan 26.2022.

[63] Ametepe AF, Ahouandjinou AS, Ezin EC.” Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks.” *Wireless Networks*. Apr;28(3):991-1001.2022.

[64] Shah AA, Adeel A, Ahmad J, Al-Dubai A, Gogate M, Bishnu A, Diyan M, Hussain T, Dashtipour K, Ratnarajah T, Hussain A.” A Novel Chaos-based Light-weight Image Encryption Scheme for Multi-modal Hearing Aids.” *arXiv preprint arXiv*:.05662. Feb 11.2022.

[65] Chhabra S, Lata K.”Towards the enhancement of AES IP security using hardware obfuscation technique: A practical approach for secure data transmission in IoT.*” Security and Privacy*.: e233.

[66] Ali NA, Rahma AM, Shaker SH.”Survey on 3D Content Encryption.” *iJIM*.;15(15):115.2021.

[67] Msekh ZA, Msekh AA.” Design and Implementation Wireless Sensor Node with Security Algorithm Based on Microcontroller ESP8266.” *InMicro-Electronics and Telecommunication Engineering* (pp. 363-371). Springer, Singapore.2022.

[68] Ravichandran D, Banu S A, Murthy BK, Balasubramanian V, Fathima S, Amirtharajan R. “An efficient medical image encryption using hybrid DNA computing and chaos in transform domain.” *Medical & Biological Engineering & Computing*. Mar;59(3):589-605.2021.2021.

[69] Sahasrabuddhe A, Laiphrakpam DS. “Multiple images encryption based on 3D scrambling and hyper-chaotic system.” *Information Sciences*. Mar 1; 550:252-67.2021

[70] Montero-Canela R, Zambrano-Serrano E, Tamariz-Flores EI, Muñoz-Pacheco JM, Torrealba-Meléndez R.” Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks.” *Ad Hoc Networks*. Feb 1; 97:102005.2022.

[71] Anandkumar R, Kalpana R.“Designing a fast image encryption scheme using fractal function and 3D Henon Map.” *Journal of Information Security and Applications*. Dec 1; 49:102390.2019.

[72] Jiang N, Dong X, Hu H, Ji Z, Zhang W.” Quantum image encryption based on Henon mapping.” *International Journal of Theoretical Physics*. Mar;58(3):979-91.2019.

[73] Adhikari S, Karforma S.” A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence.” *International Journal of Information Technology*. Aug;13(4)