Int. J. Nonlinear Anal. Appl. 13 (2022) 2, 1591–1615
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.6571

MLCM: An efficient image encryption technique for IoT application based on multi-layer chaotic maps

Kadhum Al-Majdi[a], Ahmed H. Salman[b,*], Noor Alhuda F. Abbas[b], Mohammed M. Hashim[c], Mustafa S. Taha[d], Abdullah A. Nahi Alrabeeah[d], Salim Saleh[d,e]

[a]*Ashur University College, Baghdad, Iraq*

[b]*Department of Computer Technologies Engineering, AL-Esraa University College, Baghdad, Iraq*

[c]*Faculty of Engineering, Uruk University, Baghdad, Iraq*

[d]*Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq*

[e]*Department of Mathematics, Hodeidah University-Hodeidah, Yemen*

(Communicated by Madjid Eshaghi Gordji)

Abstract

The importance of image encryption has considerably increased especially after the dramatic evolution of the internet of things (IOT) and due to the simplicity of capturing and transferring digital images. Although there are several encryption approaches, chaos-based image encryption is considered the most appropriate approach for image applications because of its sensitivity to initial conditions and control parameters. This research aims at generating an encrypted image free of statistical information to make cryptanalysis infeasible. Therefore, a new method was introduced in this paper 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 $\left(2^{450}\right)$ 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 histogram and 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: IoT applications, Chaotic Maps, Image encryption, Logistic Map, Bernoulli Map
2020 MSC: Primary 90C33, Secondary 26B25

[*] Corresponding author

Email addresses: dr.kadhum@au.edu.iq (Kadhum Al-Majdi), ahmed@esraa.edu.iq (Ahmed H. Salman), nooralhuda@esraa.edu.iq (Noor Alhuda F. Abbas), comp.mmh@gmail.com (Mohammed M. Hashim), mustafa@moti.oil.gov.iq (Mustafa S. Taha), eng.abdullahnahi@gmail.com (Abdullah A. Nahi Alrabeeah), salem.saleh@cihanuniversity.edu.iq (Salim Saleh)

Received: January 2022 *Accepted:* March 2022

1 Introduction

Recently, the Internet of Things (IoT) is used and grown fast because of the creation of data communication and might be supposed as a description of ubiquitous computing due to the IoT being used directly with user involvement to the continuously interconnected collaborative working devices (sensor devices) without users interaction [18, 45]. The rapid development of IoT applications makes its communication and transmission security issues more attractive [2, 7, 23, 33]. Therefore, it is very necessary to implement effective security and confidentiality technology for the transmis- sion in IoT [29, 43, 46]. Such security can be provided using security features such as information security techniques (steganography, watermarking, and encryption) with IoT systems. Encryption can be defined as the art of converting a plain object into coded form in a way there is no one can restore it else than the intended receiver only [2]. The demand to transfer the images in a secure manner has also increased, and encryption is the preferred method to securely transfer image data. Current encryption techniques such as AES, DES, and RSA are unsuitable for image data encrypting because of the huge size and noticeable redundancy of image data [12, 25]. In addition, there are several drawbacks and weakness such as the requirement for a powerful computing system and high computational time, thus the implementation of these techniques cause a low level of efficiency and cannot guarantee data confidentiality and security [21, 42].

Confusion and diffusion methods have been used in conventional image encryption methods. One of the most important stages in image encryption is confusion which is considered about pixels position in the plain image. Many efforts tried to kill the pixel's neighbor dependence by exchanging the positions under certain conditions to maintain the correlation of the pixels [26]. Predictive of new pixel's position under the condition of random function still need more concern [15]. Correlation of sit pixels can be mapped under the key generated from random function and this function should be strong and reliable for using the generated key in both encryption and decryption processes [28]. The confusion process is responsible for good cipher image produced from the encryption process and any weakness in this stage will affect the security of the system [5, 41]. 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.

On the contrary of confusion which considers pixels position, the diffusion stage is responsible for changing pixels value [24]. Altering such values is essential due to the direct influence of the histogram of the image. In yesteryears many algorithms tremendous attention to making a uniform histogram for the generated cipher images. The pixel's value getting between 0-255, histogram de- picts these values as graph and briefness of such value is not easy. To overcome statistical attacks diffusion process should efface histogram of cipher image to obliterate any statistical properties of the encrypted image. On the other hand, information entropy of encrypted image of 8 is needed. Information entropy reflects the uncertainty distribution of pixel values and it is highly related to the image histogram. When changing pixels value the distribution of pixel values to that. And in successful image encryption methods, the information entropy should be close to the ideal value (2.3), while when the information entropy is equal to 8 this will indicate a truly random sample [13].

Despite the use of conventional image encryption methods to encrypt images with a high-security level, there are several issues that should be improved to achieve better-encrypted image quality. The main challenge faced by image encryption designers is the generation of random keys to be used in encryption and decryption processes [14]. Random generator considers the gist of the confusion process, generating unpredictable numbers affect the security of the system. Hence, randomness is important in image encryption to make the cipher image messy as possible [13]. The conventional random function makes the system robust against any statistical attack [9] to quantize the position of the pixel between encryption and decryption process.

Most of the studies in the last decade emphasized that good encryption is based on the correlation of pixels inside the image. Obviously, the complex distribution of the pixels in the plain image gives a better correlation. It's evident that messy images can be achieved by randomizing pixel positions during encryption and how reconstructing cipher images [6]. Reposition of pixels inside the image makes more secure and cipher image stop against statistical attacks [32]. Increasing keyspace in an encryption system allows it to be more secure and reliable, hence the importance of key space [11]. So large initial size in both confusion and diffusion it is inevitable, especially when using 2D random key generating [38].

Image histogram and information entropy of the cipher images should be considered [44]. The statistical attack is more sensitive to entropy values, thus equalization of pixel values by uniforming the histogram and increasing the entropy is utmost [17]. Also, to avoid the differential attacks, in a good image encryption framework, any slight difference in the plain image must cause a significant difference in their encrypted image [4, 30].

In this paper, a new image encryption framework with high-quality criteria is proposed. 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 attacks. The main contribution of the new framework is the addition of a new process for confusion and diffusion. The confusion method uses the proposed Sensitive Logistic Map (SLM) along with Hénon Map and the additive white Gaussian noise to generate random numbers to be used in the pixel permutation method. While, diffusion method uses the Tinkerbell, Burgers, Ricker maps along with the proposed Extended Bernoulli Map (EBM) have been exploited to generate the random matrix. Internal Interaction between Image Pixels (IIIP) was used to implement XOR operator between the random matrix and scrambled image. 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.

2 Overview

This section provided the research domains and the existing methods which are used in this re- search. Image encryption can be defined as the art of conversion a plain image into coded form in a way there is no one can restore it else than the intended receiver only [17]. 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 machines 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. Demand expansion on finding secure methods to protect the information of images is coming from the escalation of image applications and image transferring over 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 on [35]. The methods of text encryption can be used in image encryption field but with significant drawbacks due to several reasons such as the large size of the images when it 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 not necessary in image encryption.

2.1 Cryptography Domains

Implementation of a cryptosystem can be done in different domains such as spatial, frequency, and hybrid domains [50]. Each of these domains can be explained as follows.

2.1.1 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 $E(x, y)$ 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 [47]. 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 [34]. Distance in S (in any distance unit) is represented by pixels inside I.

2.1.2 Frequency Domain

In frequency, domain image analyzed mathematically to series of frequencies, each of these frequencies has two main components which are the amplitude and the phase shift. Any changes in spatial domain image produce indirect changes in its frequency domain representation. The information of the frequency domain is divided into two main components, and these components are high-frequency components that represent sharp edges and noise of the plain image while the low-frequency component corresponds to the smooth area [3].

2.1.3 Hybrid Domain

The hybrid domain is the combination of both previous domains. The wavelet change and disordered guide have been proposed for image encryption as stated in [1] aged utilizing wavelet decay for preparing to guide all basic data which consists of a low recurrence sub-band. Thusly, amazing turbulent encryption is grasped for scrambling the low recurrence with the wavelet coefficients. Meanwhile, XOR is used for the high recurrence band which takes a shot of the image. Moreover, the wavelet amusement is grasped for disseminating of the encrypted data using a low recurrence band. The Arnold scrambling technique has been used for the output of the repeated wavelet image which is later diffused with encryption technique. However, the execution time of the system for encryption of images requires 0.266 seconds to the provided key length is 2,128.

2.2 Chaotic-Based Image Encryption

Chaotic-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 [1]. 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:

- It must be topologically mixing.
- It must be very sensitive to initial condition and control parameters.
- 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 [16].

2.3 Confusion and Diffusion

Shannon in 1949 suggested a process of diffusion and confusion to achieve an ideal security sys- tem 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 the 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 the meaningful statistical attack much more cipher images are needed. While in the confusion process the image pixels' location will be changed to cancel the relationship between the plain and cipher image. 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 [10].

2.4 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.

2.4.1 Chaotic Logistic Map

Chaos can be defined as a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit high sensitivity to initial conditions and have random behavior. It was discovered by Edward N. Lorenz in 1963. 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 [22]. A logistic chaotic map can be described by Equation 2.2.

$$x_{n+1} = rx_n\left(1 - x_n\right) \tag{2.2}$$

where r is the control parameter of the Iogistic map and $r \in (0.4), n = 1, 2, 3, \ldots$, and x_1 are the initial conditions or seed value and its value is $0 < x_1 < 1$. To turn the logistic map into a chaotic map r must be arranged between 3.5699 and 4 [40].

2.4.2 Hénon Map

The Hénon map was introduced by Michel Hénon as a simplified model of the Lorenz model, and due to the good chaotic behavior and specifications of the Hénon map, especially its high sensitivity to initial conditions [48]. It is considered one of the best dynamical systems. This is demonstrated by Equation 2.3 and Equation 2.4

$$x_{n+1} = 1 - 2ax_n + y_n \tag{2.3}$$

$$y_{n+1} = bx_n \tag{2.4}$$

where x and y are the Initial conditions, a and b are the control parameters. The system achieves strong chaotic behavior when $a = 1.4$ and $b = 0.3$. The Hénon map response to initial conditions with control parameters ($a = 1.4$ and $b = 0.3$ [27]).

2.4.3 Additive White Gaussian Noise

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 [8].

Noise is undesirable, inevitable, and corrupts the visual quality of the acquired images . 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 a normal distribution [31]. Sometimes Gaussian noise is defined as noise with a distribution of Gaussian amplitude. The Gaussian noise distribution function is explained by Equation 2.5.

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

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 considered a special type of Gaussian noise [20].

2.4.4 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 2.6 [49].

$$x_n = (2x_n - 1) \bmod 1 \tag{2.6}$$

2.4.5 Tinkerbell Map

A Tinkerbell Map is a discrete two-dimensional system that is generated by implementing Equation 2.7 and Equation 2.8 [19].

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \tag{2.7}$$

$$y_{n+1} = 2x_n y_n + cx_n + dy_n. \tag{2.8}$$

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 (2.7) and Equation (2.8) were studied as a special case in detail by Nusse and Yorke in 1997 and they found that 64 periods, 10 unstable periodic orbits, and one strange attractor when the parameters of both above-mentioned equations are $a = 0.9, b = -0.6, c = 2, d = 0.5$ [36].

2.4.6 Burgers Map

Burgers Map is produced by the discretization of a pair of coupled differential equations. It is used to explain the importance of bifurcation in hydrodynamic flow [39]. Equation 2.9 and Equation 2.10 are Burgers map equations and there are two control parameters that control the behavior of this map.

$$x_{n+1} = ax_n - y_n^2 \tag{2.9}$$

$$y_{n+1} = by_n - (x_n y_n) \,. \tag{2.10}$$

These two equations exhibit chaotic behavior when $a = 0.75$ and $b = 1.75$.

2.4.7 Ricker Map

There is a long history of using Ricker models to study the dynamics of single-species populations [37]. 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 2.11

$$x_{n+1} = x_n e^{r\left(1-\frac{x_n}{k}\right)} \tag{2.11}$$

where r and k are control parameters (controlling growth rate and carrying capacity, respectively). The behavior of Equation 2.11 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).

3 Proposed Method

The improvement of the image encryption framework is the main goal of the proposed research. The proposed framework is containing three main processes preprocessing, encryption and decryption. 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 which is discussed in section 4. The figure 1. illustrates the main proposed framework.

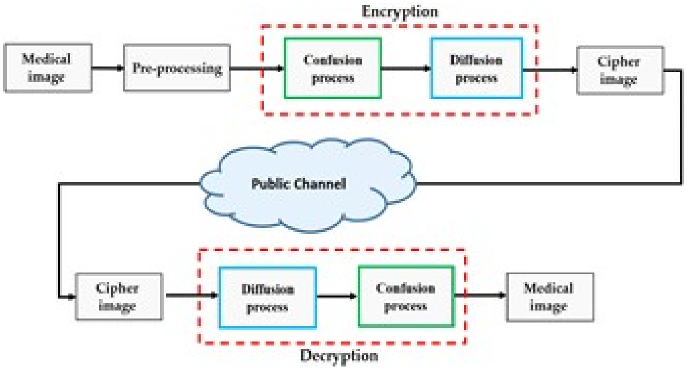


Figure 1: main framework of proposed scheme

3.1 Pre-processing process

This part of the framework is responsible for choosing and analyzing the chosen image before implementing any action on it. 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-bits RGB images analysis to its RGB channels should be implemented to deal with each channel separately.

After complete separation, store each image channel in a single 8-bits matrix with dimensions equal to the dimension of the original image. The implementation of this part produces three channels image and each of these channels is the 8-bit image. Figure 2. illustrates this procedure.

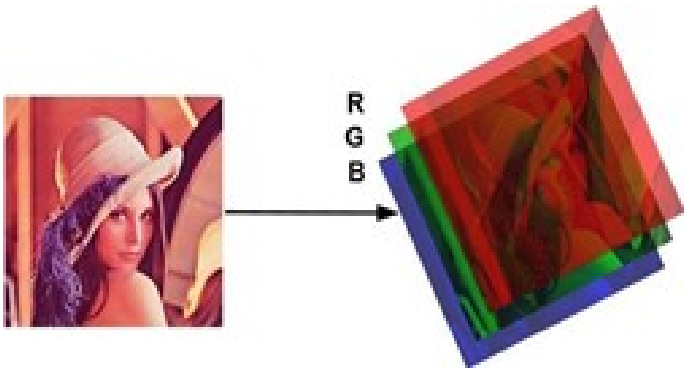


Figure 2: Illustrate analysis of RGB channels

3.2 Encryption process

Although there are several encryption approaches, chaos-based image encryption is considered the most appropriate approach for image applications because of its sensitivity to initial conditions and control parameters. Confusion and diffusion methods have been used in proposed image encryption to bypass statistical attacks. The below subsection is discussed the encryption process.

3.2.1 Chaotic Maps Used in the Proposed Confusion Method

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

3.2.2 Sensitive Logistic Map (SLM)

To achieve the research objectives, an amendment to the logistic map was proposed in this research. 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 it 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 resulted values within an acceptable range $0 < x < 1$. Equation (3.1) shows the proposed Sensitive Logistic Map (SLM).

$$x_{n+1} = \left(rx_n\left(1 - x_n\right)\right) k \bmod 1 \tag{3.1}$$

Introducing a new parameter K to SLM will produce dynamical systems with more randomness by applying multiplication between $\left(rx_n\left(1 - x_n\right)\right)$ 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 3. While the cobweb diagram for SLM shows the dynamical behavior of the proposed map, in figure 4 indicates chaotic behavior for the proposed method. The differences in both the response, cobweb diagram of the logistic map, and SLM increase the randomness of the produced random sequences.

3.2.3 Confusion Method

In the encryption method, the first step is the image pixel permutation or image confusion method. Image confusion is the process of shuffling image pixels to destroy the relationship between the neighbored pixels or dissolve the correlation between adjacent pixels of the encrypted image. There are two subprocess are included in this process which is (dynamic key generating for confusion process and confusion process) as seen in figure 5.

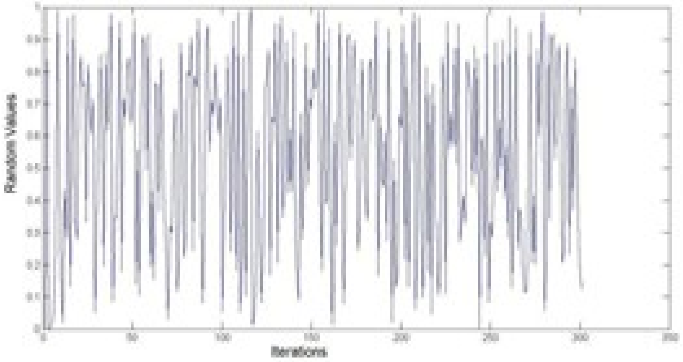


Figure 3: SLM Response

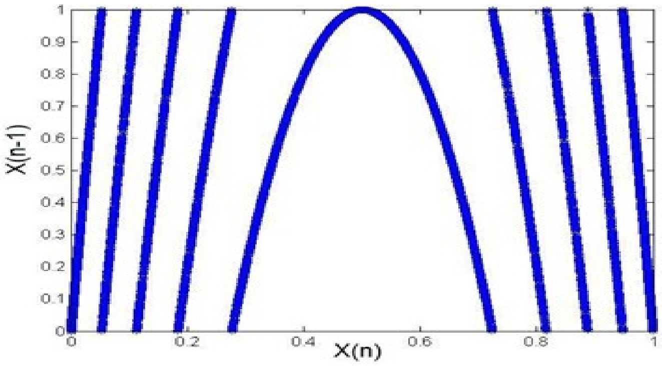


Figure 4: SLM Cobweb Diagram

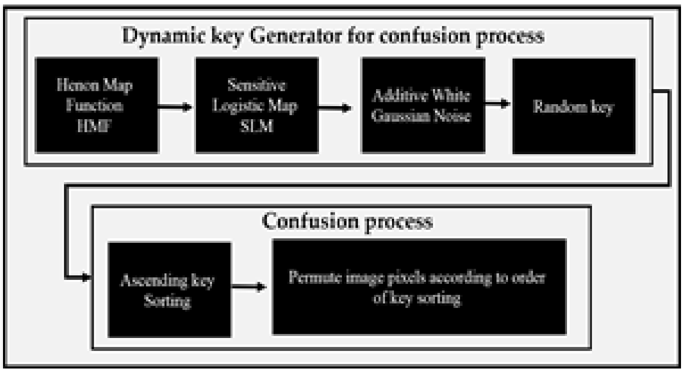

Dynamic key Generator for confusion process
Henon Map Function HMF
Sensitive Logistic Map SLM
Additive White Gaussian Noise
Random key
Confusion process
Ascending key Sorting
Permute image pixels according to order of key sorting

Figure 5: General framework for confusion method

3.2.4 Dynamic Key Generator for Confusion Method

The dynamic key generating is very important and essential in image encryption systems [32]. In the proposed framework different chaotic maps are used. In the dynamic key, H*é*non and amended logistic maps were used together to generate 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. At firs the initial conditions and control Parameters are initiated manually to be used as the inputs for H*é*non map. The output of H*é*non map is a random sequence consists of random numbers equal to the number of image rows as seen in Figure 6.

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 7. explains this process. 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.

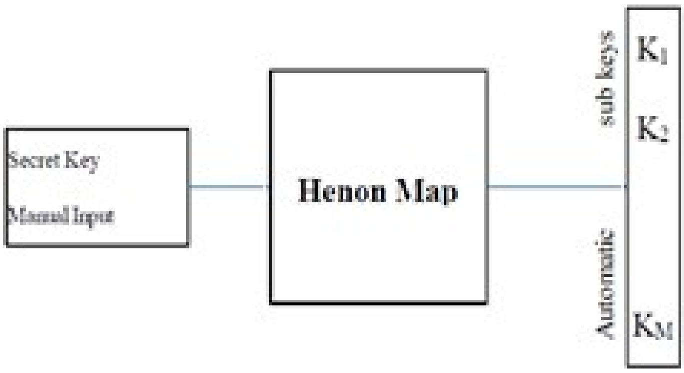


Figure 6: The process of generating automatic sub-keys

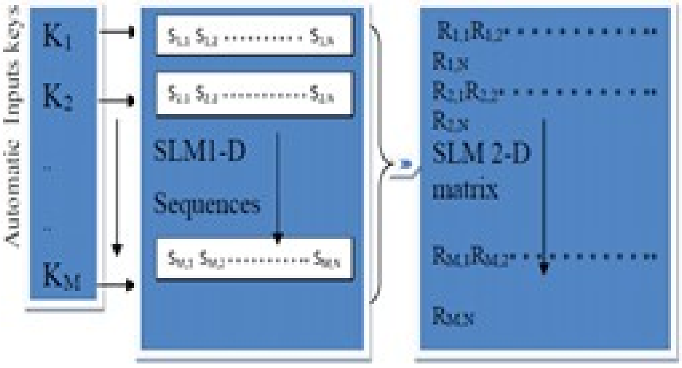


Figure 7: Using of Automatic Key to be as SLM Inputs

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 8, 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.

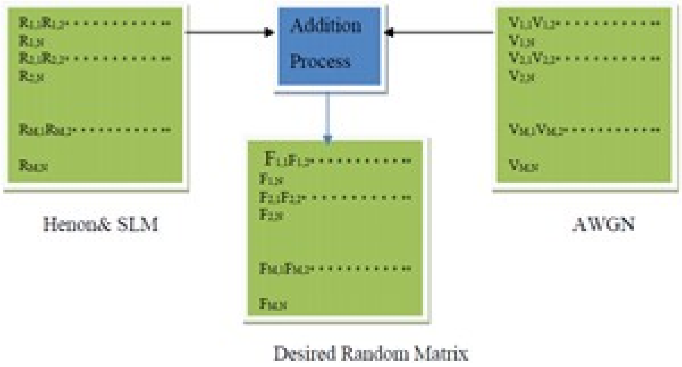


Figure 8: Final Random Matrix for confusion Process

3.2.5 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 it 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 dimension random array as illustrated in Figure 9.

After the conversion process ascending sorting was implemented to the one dimension random array to consider

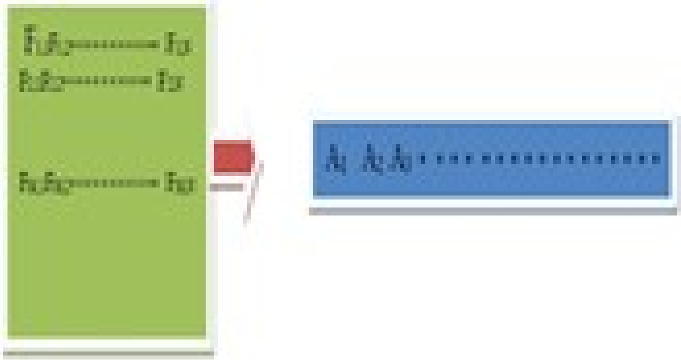

$F_{11}F_{12}$.............F_{1x}
$F_{21}F_{22}$.............F_{2y}
$F_{n1}F_{n2}$.............F_{nz}
A_1 A_2 A_3 ....

Figure 9: Two Dimensions to One Dimension Random Matrix Conversion

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 10.

Random values after sorting Process
New Indices for the Sorted Values
Old indices for the Random Values

Figure 10: 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 is 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 dimension array with the same size of the sorted random array. Although the conversion process make 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 dimension image array to a new location. To get the scrambled image a conversion from the one dimension image array after scrambling into a two dimension scrambled image was made. The scrambled image is considered as an intermediate encrypted image with minimum correlation between adjacent pixels, but another characteristics like the histogram and information entropy are still the same.

3.2.6 Chaotic Maps Used in the Proposed Diffusion Method

Four different chaotic maps are used to generate random numbers for the diffusion process. The chaotic maps are the Extended Bernoulli Map (EBM), Tinkerbell, Burgers and Ricker maps, in addition to additive white Gaussian noise. The below section is explained in details the proposed Extended Bernoulli Map.

3.2.7 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 are increasing secret key space as much as possible. In this study two techniques are used to increase key space. 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 increase the key space 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 3.2.

$$x_n = (2\,(x_{n-1} + (x_{n-2}))) \bmod 1 \tag{3.2}$$

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) show more randomness and more unpredictable behavior which achieved because the generating is dynamical for both of initial conditions which effect the whole random number generating process. The existence of two initial conditions with variable values (for each iteration) cause dynamical behavior of these initials which increase randomness and unpredictability for the generated random key.

The response of Equation (3.1) is shown in Figure 11 and the behavipr of the successive iteration (control parameter = 0.62) is seen in Figure 12.

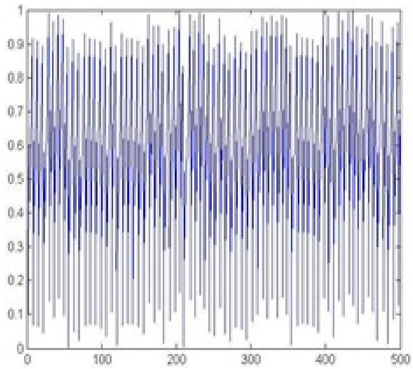


Figure 11: Response of Extended Bernoulli Map

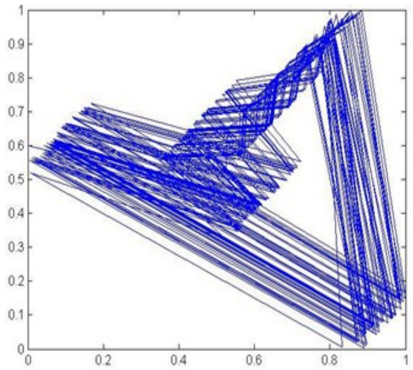


Figure 12: Successive Iterations Behaviour of Extended Bernoulli Map

In addition to increasing key space the randomness of the proposed Extended Bernoulli Map (EBM) is also increased as shown in Figure 11 and Figure 12.

3.2.8 Diffusion Method

In order to obliteration of the statistical information of the encrypted image the diffusion process is used. 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 has been considered in the proposed diffusion process such as increased key space, 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 13.

The proposed framework for 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 dynamic key generator is designed by the using of channel hopping technique which performed by implement Tinkerbill map, Burger map and Ricker map in addition to the Extended Bernoulli Map (EBM) which used to control the selection process. IIIP

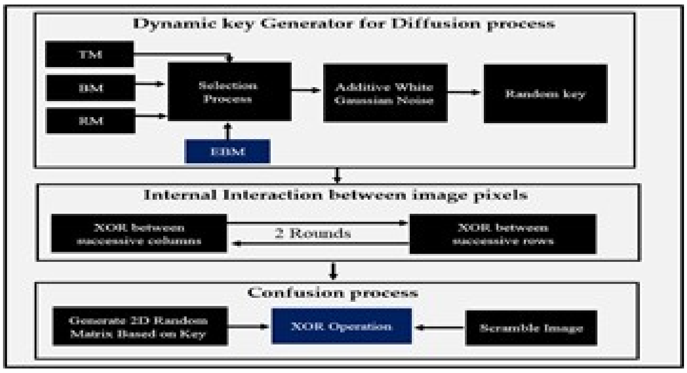

Dynamic key Generator for Diffusion process
TM
BM
RM
Selection Process
EBM
Additive White Gaussian Noise
Random key
Internal Interaction between image pixels
XOR between successive columns
2 Rounds
XOR between successive rows
Confusion process
Generate 2D Random Matrix Based on Key
XOR Operation
Scramble Image

Figure 13: Framework of Diffusion Method

method is proposed to achieve robust image encryption method against differential attack this process is proposed by this research. Lastly, the diffusion process is implemented to efface the statistical properties of the encrypted image by the by the execution of XOR operator between the image generated from IIIP process and the random matrix that derived from the random number generator.

3.2.9 Dynamic Key Generator for Diffusion Method

As mentioned earlier four chaotic maps are used to generate keys. The channel hopping technique is used to produce random key numbers. 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 $\mathbb{M}$ where N and M are the row and column numbers, respectively for the image to be encrypted. Random number values will be chosen from one of 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 14. 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.

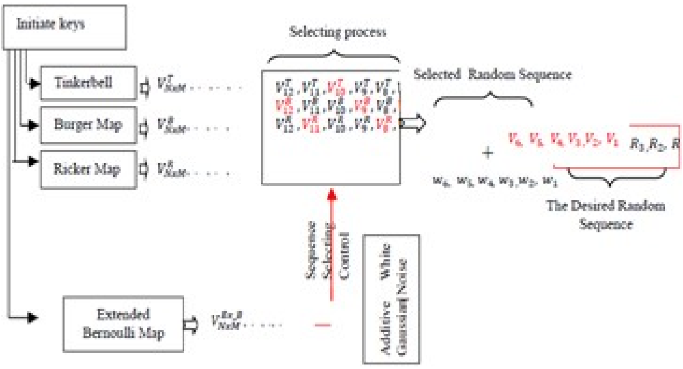


Figure 14: Channel Hopping Process

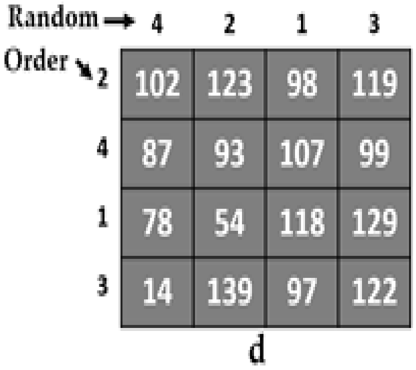
3.2.10 Internal Interaction between Image Pixels

Nowadays the importance of differential attacks has increased due to its high performance in crypt- analysis and researchers have concentrated on developing new techniques based on this type of attack. To resist this type of attack, the encryption methods should produce significant differences between encrypted images after making minor alterations.

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 plain image after even one-pixel alterations produce significant changes in 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 × 4-pixels 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 is illustrated in Figure 15. 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 15 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. Then, 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.

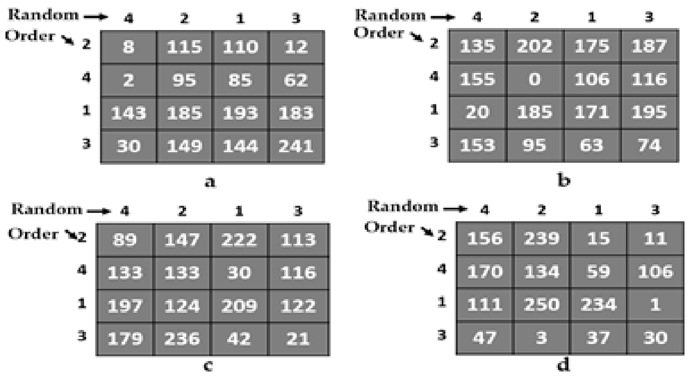


Random → Order ↘	4	2	1	3
2	102	123	98	119
4	87	93	107	99
1	78	54	118	129
3	14	139	97	122

d

Figure 15: 4 × 4 plain image

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 16. To verify the performance of the proposed method against differential attacks, only one pixel



Random → Order ↘	4	2	1	3
2	8	115	110	12
4	2	95	85	62
1	143	185	193	183
3	30	149	144	241

a

Random → Order ↘	4	2	1	3
2	135	202	175	187
4	155	0	106	116
1	20	185	171	195
3	153	95	63	74

b

Random → Order ↘	4	2	1	3
2	89	147	222	113
4	133	133	30	116
1	197	124	209	122
3	179	236	42	21

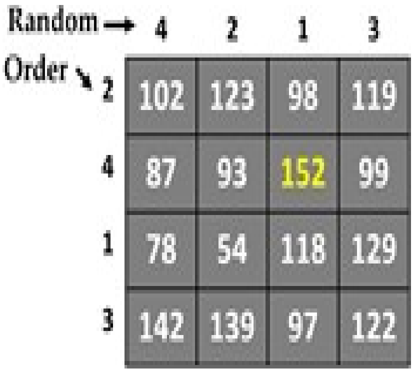
c

Random → Order ↘	4	2	1	3
2	156	239	15	11
4	170	134	59	106
1	111	250	234	1
3	47	3	37	30

d

Figure 16: Implementation of XOR operators between (a) successive columns, (b) successive rows, (c) second round successive columns, (d) and second round successive rows

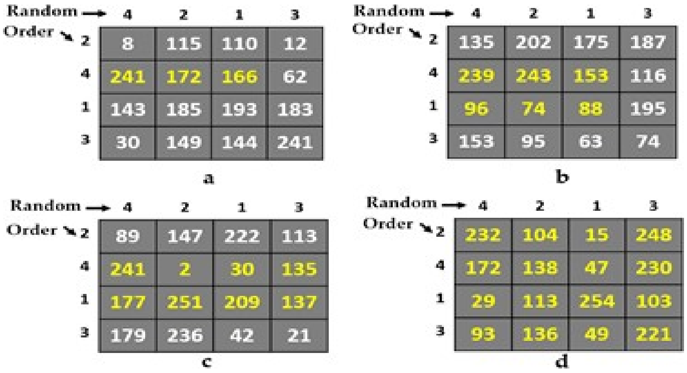
in the original image (the pixel located at the address (2, 3)) was changed from 107 to 152 as seen in Figure 17. After that the implementation of XOR operations will take place between successive columns and successive rows. This process is repeated for the second round as shown in Figure 17. The red value in Figure 15 is the altered value, while the red values in Figure 16 represent changes in the resulting image due to the small alterations in the original image after two rounds of XOR operations.



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

Figure 17: The altered image matrix

By altering the pixel located at the address (2, 3) as seen in Figure 18 leads to significant changes in the resulting image as shown in Figure 5.8(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 is clear that the resulting images are entirely different from those encrypted without any pixel alterations.



Random →	4	2	1	3
Order ↘ 2	8	115	110	12
4	241	172	166	62
1	143	185	193	183
3	30	149	144	241

a

Random →	4	2	1	3
Order ↘ 2	135	202	175	187
4	239	243	153	116
1	96	74	88	195
3	153	95	63	74

b

Random →	4	2	1	3
Order ↘ 2	89	147	222	113
4	241	2	30	135
1	177	251	209	137
3	179	236	42	21

c

Random →	4	2	1	3
Order ↘ 2	232	104	15	248
4	172	138	47	230
1	29	113	254	103
3	93	136	49	221

d

Figure 18: Changes due to the Small Alterations in the Original Image

3.2.11 Diffusion process

In the proposed framework, to achieve the main aims of the diffusion process, the random matrix numbers that have been generated from the previous section will be converted from fractal numbers that have been arranged between (0) and (1) to an integer number arranged between (0) and (255) With an equal number of appearance for each of these numbers. The resulted matrix will be the key for the diffusion part.

Diffusion is used to change the image's statistical information, especially the histogram information by altering image pixels values. In the proposed framework, the generated key with an 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 the diffusion process.

Implementation of the XOR operator between the generated diffusion random key and the image that resulted from the confusion process (scrambled image) is the main process in this part of image encryption. The histogram of the resulting image after the diffusion process is almost uniform also for entropy is close to 8. Therefore, it is very difficult for cryptanalysis to reveal the plain image from the encrypted image that resulted from the diffusion process.

3.3 Decryption Method

To ensure that the proposed method is secure the decryption process follows specific methods. In the proposed framework there are two steps to decrypt the ciphered image, each of these parts is responsible for decrypting one of the encryption parts. The final part of the encryption process should be the first part of the decryption process and vice versa.

3.3.1 Decryption Process for Diffused method

The first step in the decryption of diffused images 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 explained in 5.4. 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 first round on the image resulting from the first round. Finally, an XOR operation is performed between the resulting image and the random key matrix generated by Algorithm 5.1 to recover the image that was used as the input for the diffusion method (confused image).

3.3.2 Decryption Process for Confused method.

The decryption process for the confused image will recover the plain image. To achieve this there are several processes that must be considered. The random number generator used in the confusion method must have the same initial conditions and control parameters used to generate the 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 confusing image.

4 Experimental result

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.

4.1 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 [34]. 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

Table 1: NIST results for the random number generator proposed for the confusion method. To verify

N	Statistical test	P-value	Proportion
1	Frequency	0.98	0.99
2	Block Frequency	0.73	1.00
3	Runs	0.96	0.99
4	Longest-Run	0.62	0.99
5	Binary Matrix Rank	.098	0.99
6	FFT	0.54	0.99
7	Non-overlapping Template	0.93	0.99
8	Overlapping Template	0.87	0.99
9	Universal	0.99	0.99
10	Linear Complexity	0.81	1.00
11	Serial	0.86	0.99
12	Approximate Entropy	0.97	0.99
13	Cusum	0.64	0.99
14	Random Excursions	0.95	0.99
15	Random Excursions Variant	0.96	0.99

generator are shown in Table 1. 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 2.

Table 2: Comparison between proposed random number generator for the Confusion method and two recent methods.

N	Items	Hanis et al.		Jallouli et al.,		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	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 Rank	0.16	0.99	0.96	0.97	0.98	0.99
6	FFT	0.19	0.99	0.38	0.97	0.54	0.99
7	Non-overlapping Template	0.79	0.99	N/A	N/A	0.93	0.99
8	Overlapping Template	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	0.07	0.97	0.93	0.99	0.97	0.99
13	Cusum	0.73	0.97	N/A	N/A	0.64	0.99
14	Random Excursions	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 (ABM), 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 3.

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 4.

As seen in Table 7.6, the proposed random number generator for the diffusion process is better than the random number generator proposed by [3, 1]. 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.

Table 3: NIST results for the random number generator proposed for the diffusion method.

N	Statistical test	P-Value	Proportion
1	Frequency	0.99	1.00
2	Block Frequency	0.75	0.99
3	Runs	0.97	0.99
4	Longest-Run	0.67	1.00
5	Binary Matrix Rank	0.98	0.99
6	FFT	0.59	0.99
7	Non-overlapping Template	0.82	0.99
8	Overlapping Template	0.87	0.99
9	Universal	0.66	0.97
10	Linear Complexity	0.47	0.99
11	Serial	0.91	1.00
12	Approximate Entropy	0.97	0.99
13	Cusum	0.92	0.99
14	Random Excursions	0.89	0.99
15	Random Excursions Variant	0.94	0.99

Table 4: Comparison between proposed random number generator for the Diffusion method and two recent methods.

N	Items	Hanis et al.[54]		Jallouli et al.,[55]		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	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 Rank	0.16	0.99	0.96	0.97	0.98	0.99
6	FFT	0.19	0.99	0.38	0.97	0.59	0.99
7	Non-overlapping Template	0.79	0.99	N/A	N/A	0.82	0.99
8	Overlapping Template	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	0.07	0.97	0.93	0.99	0.97	0.99
12	Cusum	0.73	0.97	0.83	0.98	0.92	0.99
14	Random Excursions	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

4.2 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 2128 are not acceptable because it is not sufficiently secure [14]. 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 (1015), therefore the key space for the proposed system can be calculated as seen in Table 5.

Table 5: The key spaces for proposed scheme.

N	Chaotic Map	Number of Initial Values	Key Space (Decimal)	Key Space (Binary)
1	Hnon	2	1030	2100
2	Amended Beroulli	2	1030	2100
3	Tinkerbell	2	1030	2100
4	Burger	2	1030	2100
5	Ricker	1	1015	250
6	Total	9	10135	2450

The length of the key space for the proposed system is 2450 which is represented a large key. Therefore, the brute force attacks to break the proposed system are infeasible. The initial condition of SLM is not considered in Table 7.7 because this initial condition is initiated automatically using the output values from the Hénon map it cannot be used as an initial condition. In addition to key space, there are numerous control parameters related to the maps used in this study, which cannot be underestimated. These control parameters will increase possible key combinations. A comparison between the proposed method and several recent methods is in Table 6.

Table 6: Comparison between the proposed scheme and several recent methods based on Key space size.

N	Method	Key Space Size
1	Enayatifar et aL.	2240
2	Choi et al., 2016	2448
3	Bashir et al., 2018	2212
4	Kulsoom et al., 2020	2167
5	Kar et al., 2021	2256
6	Proposed Method	2450

4.3 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 3.2, 4.1, and 4.2.

$$\mathbf{A}' = \frac{1}{M \times N} \sum_{i=1} M \sum_{j=1} N A_{ij} \tag{4.1}$$

$$\mathbf{B}' = \frac{1}{M \times N} \sum_{i=1} M \sum_{j=1} N B_{ij} \tag{4.2}$$

$$CC = \frac{\sum_{i=1} M \sum_{j=1} N (A_{ij} - \mathbf{A}'_{ij})(B_{ij} - \mathbf{B}'_{ij})}{(\sum_{i=1} M \sum_{j=1} N A_{ij} - \mathbf{A}'_{ij})^2 (\sum_{i=1} M \sum_{j=1} N B_{ij} - \mathbf{B}'_{ij})^2} \tag{4.3}$$

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 [35]. 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 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 7. show that the correlation for the plain-image is very high because the difference between the 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 that the smooth 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 8. shows the correlation between adjacent pixels for the 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. As it seen in Table 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

Table 7: Correlation of adjacent pixels for plain-Images.

N	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 8: Correlation between adjacent pixels for the encrypted image.

N	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

Table 9: Correlation between adjacent pixels for the encrypted image and Existing methods.

N	Method	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
1	Choi et al., 2016	-0.003	-0.004	-0.009
2	Enayatifar et al., 2017	0.0008	0.0021	0.0005
3	Bashir et al., 2016	0.0238	-0.0182	0.0073
4	Kulsoom et al., 2016	0.0027	0.0005	-0.0045
5	Kar et al., 2017	-0.0076	-0.0034	-0.0074
6	Proposed Method	0.000732	0.000391	0.00032

comparison between the results of proposed system and the results of several recent methods is shown in Table 9

Table 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.

4.4 Information Entropy Analysis

Information Entropy is used to measure uncertain associations between random variables[15]. 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 [9, 30]. Information entropy can be calculated using Equation 4.4

$$H(m)=\sum_{i=0} P\left(m_i\right) \log_2 \frac{1}{P\left(m_i\right)} \tag{4.4}$$

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 [9]. Table 10 shows the entropy results for the proposed image encryption system. Table 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 11. 4.5 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 [12]. In image histogram plots, each bar represents 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) [21]. 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 [29] this quantitative test can be performed by the using of variance metric. The equation 4.5 is used to calculate the variance of encrypted image.

Table 10: Entropy results for the proposed image encryption.

N	Image Name	Image type	Size	Entropy
1	Girl	RGB	256 256	8
2	Tiffany	RGB	256 256	8
3	Elaine	grayscale	512 512	8
4	Cameraman	grayscale	256 256	8
5	Lena	grayscale	512 512	8
6	Baboon	RGB	512 512	8
7	Cactus	RGB	512 512	8
8	Dolls	RGB	512 512	8
9	City	RGB	512 512	8
10	Man	grayscale	1024 1024	8

Table 11: Entropy results for the proposed image encryption and existing methods.

Method	Enayatifar et al., (2017)	Choi et al., (2016)	Bashir et al., (2016)	Kulsoom et al., (2016)	Kar et al., (2017)	Proposed Method
Average Enrtopy	7.9994	7.8198	7.9992	7.9972	7.9872	8.0

$$\mathrm{Var}(H) = \frac{1}{n^2} \sum_{i=1} n \frac{(H_i - H_j)}{2} \tag{4.5}$$

where H_i, H_j represents occurrence of different pixel values (i, j). The histogram variance results for the tested images are tabulated in Table 12. and this table show that the variance of all of these tested images are equal to zero which means that the uniformity distribution of the proposed method is ideal and the statistical attacks for the proposed method is infeasible. As seen in Table 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. To verify that the quantitative histogram analysis for the proposed method is better than other methods a comparison will be held with several recent method as seen in Table 13. 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 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 5.1.

$$MSE = \frac{1}{M \times N} \sum_{i=1} M \sum_{j=1} N \left(a(i,j) - b(i,j)\right)^2 \tag{5.1}$$

Table 12: Variance of the encrypted image.

N	Image Name	Image type	Size	variance
1	Girl	RGB	256 256	0
2	Tiffany	RGB	256 256	0
3	Elaine	grayscale	512 512	0
4	Cameraman	grayscale	256 256	0
5	Lena	grayscale	512 512	0
6	Baboon	RGB	512 512	0
7	Cactus	RGB	512 512	0
8	Dolls	RGB	512 512	0
9	City	RGB	512 512	0
10	Man	grayscale	1024 1024	0

Table 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

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 ith row and jth column for the plain and ciphered images. Larger MSEs provide better image encryption security [42].

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 5.2.

$$PSNR = 10 \log_{10} \frac{\left(I_{\max}^2\right)}{MSE} \tag{5.2}$$

where $I_{\max}$ 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 14.

Table 14: MSE and PSNR results for the proposed method.

N	Image Name	Image type	Size		MSE	PSNR
1	Girl	RGB	256	256	12748	7.07
2	Tiffany	RGB	256	256	9274	8.45
3	Elaine	grayscale	512	512	8679	8.74
4	Cameraman	grayscale	256	256	13418	6.85
5	Lena	grayscale	512	512	13728	8.19
6	Baboon	RGB	512	512	7984	8.95
7	Cactus	RGB	512	512	6816	9.79
8	Dolls	RGB	512	512	8567	8.80
9	City	RGB	512	512	10332	7.98
10	Man	grayscale	1024	1024	9924	8.16

To verify the proposed method in terms of the MSE and PSNR results, Table 15 illustrates a com- parison of the proposed method with several recent image encryption methods.

Table 15: Comparison of MSE and PSNR for the proposed method and existing recent methods.

Method	MSE	PSNR
1 (Gu et al., 2016)	9595	8.31
2 (Kar et al., 2016)	9551	8.33
3 (Bashir et al., 2016)	9465	8.37
4 Proposed Method	9864	8.19

In Table 15. both of the proposed methods and other recent methods used a grayscale Lena image with a size of 512 × 512 pixels. Table 14. and Table 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.

$$D(i,i) = \begin{cases} 0, & \text{if} \quad c_1(i,j) = c_2(i,j) \\ 1 & , \text{if} \quad c_1(i,j) = c_2(i,j) \end{cases} \tag{5.3}$$

$$NPCR = \frac{1}{M \times N} \sum_{ij} M, ND(i,j) \times 100\% \tag{5.4}$$

$$UACI = \frac{1}{M \times N} \sum_{ij} M, N \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\% \tag{5.5}$$

where M and N are the width and height of c_1 and c_2.

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 16.

Table 16: NPCR and UACI for proposed method.

N	Image Name	Image Name	Size		NPCR	UACI
1	Girl	RGB	256	256	99.63	33.87
2	Tiffany	RGB	256	256	99.81	33.92
3	Elaine	grayscale	512	512	99.65	34.39
4	Cameraman	grayscale	256	256	99.59	33.30
5	Lena	grayscale	512	512	99.83	34.10
6	Baboon	RGB	512	512	99.66	33.52
7	Cactus	RGB	512	512	99.63	33.37
8	Dolls	RGB	512	512	99.67	33.32
9	City	RGB	512	512	99.91	34.65
10	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 17. This comparison shows that the results for the proposed method are better than the results of t other recent methods in terms of differential attack resistance. All data shown in Table 7.19 resulted from the implementation of encryption processes using a grayscale 512 × 512 Lena image. Table 7.20 and table 7.21 show good results in terms of withstanding against differential attack and show that the proposed method is better than other methods for hindering such attacks. 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.

Table 17: NPCR and UACI Comparison between the proposed method and recent methods.

N	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

6 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 research show that the achieving of ideal secrecy system in cryptography can be performed with the new processes of confusion and diffusion. The implementation of the proposed framework obtains ideal results in histogram and information entropy for the cipher 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. Despite the differential analysis is very interested attack but the proposed framework resolves this issue by the proposing of IIIP method. In general, the proposed framework consists of two process (confusion and diffusion) with new methods instead of one processes of conventional image encryption frameworks. The proposed confusion process is responsible on the breach of high correlations of the adjacent pixels. Finally, the proposed diffusion process increases withstanding against differential attack in addition to efface the statistical properties of the encrypted image.

References

[1] M.Z. Abdullah and Z.J. Khaleefah, *Design and implement of a hybrid cryptography textual system*, Int. Conf. Engin. Technol. (ICET), 2017, pp. 1–6.

[2] M.A. Al-Khasawneh, I. Uddin, S.A.A. Shah, A.M. Khasawneh, L. Abualigah and M. Mahmoud, *An improved chaotic image encryption algorithm using hadoop-based mapreduce framework for massive remote sensed images in parallel iot applications*, Cluster Comput. **25** (2022), no. 2, 999–1013.

[3] X. Bai, L. Zhang, J. Li, Z. Yu, Z. Yang, Y. Wang, X. Chen and X. Zhou, *Coherent imaging of objects through thin-layer highly scattering medium based on optical encryption*, Optics Commun. **506** (2022), 127558.

[4] E. Balamurugan, L.R. Flaih, D. Yuvaraj, K. Sangeetha, A. Jayanthiladevi and T.S. Kumar, *Use case of artificial intelligence in machine learning manufacturing 4.0*, Int. Conf. Comput. Intell. Knowledge Econ. (ICCIKE), 2019, pp. 656–659.

[5] M. Budiman, *A neural cryptography approach for digital image security using vigenere cipher and tree parity machine*, J. Phys.: Conf. Ser. **1898** (2021), 012039.

[6] J. Choi and N. Y. Yu, *Secure image encryption based on compressed sensing and scrambling for internet-of-multimedia things*, IEEE Access **10** (2022), 10706–10718.

[7] V. Dahiphale, G. Bansod, and J. Patil, *Anu-ii: A fast and efficient lightweight encryption design for security in iot*, Int. Conf. Big Data, IoT and Data Sci. (BID), 2017, pp. 130–137.

[8] K. Dharavathu and S.A. Mosa. *Efficient transmission of an encrypted image through a mimo–ofdm system with different encryption schemes*, Sens. Imag. **21** (2020), no. 1, 1–31.

[9] R. Durga, E. Poovammal, K. Ramana, R.H. Jhanveri, S. Singh and B. Yoon. *Ces blocks-a novel chaotic encryption schemes based blockchain system for an iot environment*, IEEE Access **10** (2022), 11354–11371.

[10] M. Farah, A. Farah and T. Farah, *An image encryption scheme based on a new hybrid chaotic map and optimized substitution box*, Nonlinear Dyn. **99** (2020), no. 4, 3041–3064.

[11] V. Gaur, R.K. Gujral, A. Mehta, N. Gupta and R. Bansal, *Enhanced digital image encryption using sine transformed complex chaotic sequence*, Proc. Int. Conf. Artific. Intell. Appl., 2021, pp. 149–160.

[12] A. Hafsa, A. Sghaier, J. Malek, and M. Machhout, *Image encryption method based on improved ecc and modified aes algorithm*, Multimedia Tools Appl. **80** (2021), no. 13, 19769–19801.

[13] M. Hashim, M.S. Taha, A.H.M. Aman, A.H.A. Hashim, M.S.M. Rahim and S. Islam, *Securing medical data transmission systems based on integrating algorithm of encryption and steganography*, 7th Int. Conf. Mechatronics Engin. (ICOM), 2019, pp. 1–6.

[14] M.M. Hashim, A.K. Mohsin and M.S.M. Rahim, *All-encompassing review of biometric information protection in fingerprints based steganography*, Proc. 3rd Int. Symp. Comput. Sci. Intell. Control, 2019, pp. 1–8.

[15] Z. Hu and S. Kais, *A quantum encryption design featuring confusion, diffusion, and mode of operation*, arXiv preprint arXiv:2010.03062, (2020).

[16] Z. Hua, Y. Zhou and H. Huang, *Cosine-transform-based chaotic system for image encryption*, Inf. Sci. **480** (2019), 403–419.

[17] S.T. Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish and M.M. Fouda, *A new image encryption algorithm for grey and color medical images*, IEEE Access **9** (2021), 37855–37865.

[18] J. Khan, J. P. Li, B. Ahamad, S. Parveen, A.U. Haq, G.A. Khan and A.K. Sangaiah, *Smsh: Secure surveillance mechanism on smart healthcare iot system with probabilistic image encryption*, IEEE Access 8 (2020), 15747–15767.

[19] P.R. Krishna, C.V.S. Teja and V. Thanikaiselvan, *A chaos based image encryption using Tinkerbell map functions*, Second Int. Conf. Electron. Commun. Aerospace Technol. (ICECA), 2018, pp. 578–582.

[20] K.S. Kumar, G. Sreenivasulu and S. V. Rajan, *Block based svd approach for additive white gaussian noise level estimation in satellite images*, 3rd Int. Conf. Comput. Sustain. Glob. Dev. (INDIACom), 2016, pp. 1464–1468.

[21] T. M. Kumar, K.S. Reddy, S. Rinaldi, B.D. Parameshachari and K. Arunachalam, *A low area high speed fpga implementation of aes architecture for cryptography application*, Electron. **10** (2021), no. 16, 2023.

[22] V. Kumar and A. Girdhar, *A 2d logistic map and lorenz-rossler chaotic system based rgb image encryption approach*, Multimedia Tools Appl. **80** (2021), no. 3, 3749–3773.

[23] B. Li, Y. Feng, Z. Xiong, W. Yang and G. Liu. *Research on ai security enhanced encryption algorithm of autonomous iot systems*, Inf. Sci. **575** (2021), 379–398.

[24] W. Li, X. Chang, A. Yan and H. Zhang, *Asymmetric multiple image elliptic curve cryptography*, Optics Lasers Engin. **136** (2021), 106319.

[25] C.-H. Lin, G.-H. Hu, C.-Y. Chan and J.-J. Yan, *Chaos-based synchronized dynamic keys and their application to image encryption with an improved aes algorithm*, Appl. Sci. **11** (2021), no. 3, 1329.

[26] A.A. Maryoosh, Z.S. Dhaif and R.A. Mustafa, *Image confusion and diffusion based on multi-chaotic system and mix-column*, Bull. Electric. Engin. Inf. **10** (2021), no. 4, 2100–2109.

[27] M.M. Matalgah and A.M. Magableh, *Simple encryption algorithm with improved performance in wireless communications*, IEEE Radio Wireless Symp., 2011, pp. 215–218.

[28] A.N. Mazher and J. Waleed, *Implementation of modified gso based magic cube keys generation in cryptography*, Eastern-Eur. J. Enterprise Technol. **1** (2021), no. 9, 43–49.

[29] S. Medileh, A. Laouid, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan and O.A. Khashan, *A flexible encryption technique for the internet of things environment*, Ad Hoc Networks **106** (2020), 102240.

[30] G. Ming, *Eagle: A new symmetric encryption algorithm against any linear attacks and differential attacks (the existence of one-way function means p!= np)*, preprint.

[31] P. Mohanakrishnan, K. Suthendran, S. Arumugam and T. Panneerselvam. *Mixed noise elimination and data hiding for secure data transmission*, Int. Conf. Theor. Comput. Sci. Discrete Math. 2016, pp. 156–164.

[32] A. S. Muhammad and F. Özkaynak, *Siea: secure image encryption algorithm based on chaotic systems optimization algorithms and pufs*, Symmetry **13** (2021), no. 5, 824.

[33] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S.W. Baik, *Secure surveillance framework for iot systems using probabilistic image encryption*, IEEE Trans. Ind. Inf. **14** (2018), no. 8, 3679–3689.

[34] R. Munir. *A block-based image encryption algorithm in frequency domain using chaotic permutation*, 8th Int. Conf. Telecommun. Syst. Serv. Appl.(TSSA), 2014, pp. 1-5.

[35] P.S.K. Oberko, V.-H.K.S. Obeng, and H. Xiong, *A survey on multi-authority and decentralized attribute-based encryption*, J. Ambient Intell. Humanized Comput. **13** (2022), no. 1, 515–533

[36] A. Ouannas, A.-A. Khennaoui, S. Bendoukha, T.P. Vo, V.-T. Pham and V.V. Huynh, *The fractional form of the tinkerbell map is chaotic*, Appl. Sci. **8** (2018), no. 12, 2640.

[37] A. G. Radwan, *On some generalized discrete logistic maps*, J. Adv. Res. **4** (2013), no. 2, 163–171.

[38] A. Sahasrabuddhe and D.S. Laiphrakpam, *Multiple images encryption based on 3d scrambling and hyper-chaotic*

system, Inf. Sci. **550** (2021), 252–267.

[39] R. Senkerik, M. Pluhacek, I. Zelinka and Z.K. Oplatkova, *Utilization of the discrete chaotic systems as the pseudo random number generators*, Modern Trends Tech. Comput. Sci., Springer, Cham, 2014, pp. 155–164.

[40] A.A. Shah, S.A. Parah, M. Rashid and M. Elhoseny, *Efficient image encryption scheme based on generalized logistic map for real time image processing*, J. Real-Time Image Process. **17** (2020), no. 6, 2139–2151.

[41] M.H. Shukur, *Design a mobile medication dispenser based on iot technology*, 3rd Int. Conf. Commun. Engin. Comput. Sci. (CIC-COCOS19), 2019.

[42] M.S. Taha, M.S.M. Rahim, S.A. Lafta, M.M. Hashim and H.M. Alzuabidi, *Combination of steganography and cryptography: A short survey*, IOP Conf. Series: Mater. Sci. Engin. **518** (2019), 052003.

[43] M.S.H. Talpur, M.Z.A. Bhuiyan and G. Wang. *Shared–node iot network architecture with ubiquitous homomorphic encryption for healthcare monitoring*, Int. J. Embed. Syst. **7** (2015), no. 1, 43–54.

[44] A. Toktas, U. Erkan and D. Ustun. *An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using abc algorithm*, Nonlinear Dyn. **105** (2021), no. 2, 1885–1909.

[45] D. Trujillo-Toledo, O. López-Bonilla, E. Garcia-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, and E. Inzunza-González, *Real-time rgb image encryption for iot applications using enhanced sequences from chaotic maps*, Chaos, Solitons Fractals **153** (2021), 111506.

[46] A.S. Unde and P. Deepthi. *Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia iot*, IEEE Trans. Circ. Syst. II: Express Briefs **67** (2019), no. 1, 167–171.

[47] H. Wang, J. Wang, Y.-C. Geng, Y. Song and J.-Q. Liu, *Quantum image encryption based on iterative framework of frequency-spatial domain transforms*, Int. J. Theor. Phys. **56** (2017), no. 10, 3029–3049.

[48] J. Wu, X. Liao and B. Yang, *Image encryption using 2d hénon-sine map and dna approach*, Signal Process. **153** (2018), 11–23.

[49] W. Zhang, Z. Zhu and H. Yu, *A symmetric image encryption algorithm based on a coupled logistic–bernoulli map and cellular automata diffusion strategy*, Entropy **21** (2019), no. 5, 504.

[50] X. Zhang, G. Zhu and S. Ma, *Remote-sensing image encryption in hybrid domains*, Optics Commun. **285** (2012), no. 7, 1736–1743.