Robust Chaos Image Encryption System using Modification Logistic Map, Gingerbread Man and Arnold Cat Map

Robust Chaos Image Encryption System

Lina Jamal Ibrahim[1], John Bush Idoko[2], Almuntadher M. Alwhelat[3]
Department of Computer Science, Dijlah University College, Baghdad, Iraq[1, 3]
Applied Artificial Intelligence Research Centre, Department of Computer Engineering,
Near East University, Nicosia 99138, Turkey[2]

***Abstract*—In the field of security, the information must be protected from unauthorized use because it contains a great deal of sensitive information especially in images. Image encryption is now recognized as an outstanding strategy for protecting images from attackers. Despite numerous advancements, an efficient image encryption method remains essential to achieve high image security. Therefore, an accurate encryption algorithm requires a formidable random key generator and regeneration abilities. In addition, a new strategy for confusion and diffusion with different processes. To accomplish these objectives, a framework for image encryption with three main phases has been created. Firstly, a new key generator was created with a high level of randomness based on different chaotic maps and the proposed Modification Logistic Map function. Secondly, the confusion phase has been proposed based on sorting the key generator ascending and then permuting the image pixels according to the sorting key. Lastly, the confusion phase has been presented based on generating the Gingerbread Man Method (GGM), Arnold Cat Map (ACM) transform and, XOR between the confused image and Arnold image. The ACM is used to remove flat areas from the image. Various parameters were used to assess the experimental result. In conclusion, it has been confirmed that the suggested picture encryption approach is a solid success in the field of encryption.**

***Keywords*—Arnold cat map; confusion; diffusion; image encryption; modification logistic map**

I. Introduction

Due to the rapid growth of electronic information over the internet, this information needs some protection techniques to secure the transfer of it, especially images because of easy transfer and widely used [1]. Different techniques have been used to secure the information but encryption techniques are the most popular ones. Encryption is essentially a technique for converting data from plaintext, which can be read, into ciphertext, which is encrypted and cannot be read. With an encryption key and a decryption key, respectively, users can access both encrypted and decrypted data [2]. The encryption method is widely used to protect the images in the computer and internet networks from unauthorized access [3].

The main elements of the encryption algorithm are a set of random numbers called encryption keys or key generators. These sets must achieve multiple principles such as unpredictability, including initial key space or size, and randomness, and regenerate these sequences multiple times. Thus, mainly these keys rather than encryption algorithm components decide encryption system security because it is easier to protect and easier to modify whenever compromised [6, 7].

These are considered to be the major difficulties often faced by encryption system designers [10]. Several designers used a large initial key including sets of parameters or parts of images. However, these keys are considered to be a drawback in encryption systems because they are very difficult to forward to the other parties [13]. Also, there are several researchers used additional methods to expand the generated key to fit the image size, which will cost a computation process and increase the complexity [8, 12, 9]. Therefore, called the need to use the random number generator and expander that overcome the previously mentioned difficulties.

The diffusion is described as a process of obscuring the relationship between the key and the plain image, in which the former is simply uncorrelated to the latter [5], whereas reshuffling bits of the plain image so that any redundancy in the plain image pixels are spread out over the cipher image.

The modern diffusion methods are based on the substitution technique, where a look-up table called SBox is used [4, 12]. To alter the value of the pixel, this work performs the diffusion process in two steps. The first phase involved applying the bitwise XOR operator to the gingerbread man image that was impacted by the Arnold cat map. When combined with the appropriate encryption key, the XOR logic operator is an ideal way to modify pixel values while maintaining the capacity to reconstruct the original pixel value. A pixel circular-shifting technique is used in the second step.

The Arnold Cat Map is a special type of chaotic map used to disturb the high correlation among pixels and scramble the positions of the pixels in an image matrix. The Arnold cat map is characterized by significant attributes, where the image pixels' position can be rearranged. However, after a definite number of iterations, the map revisits a similar pixel location leading to the creation of an original image [5, 12].

The multi-colour gingerbread man is thought to be a two-dimensional chaotic map that exhibits chaotic behavior in certain areas while maintaining stability in others [30, 32]. The stable hexagonal zone forms the gingerbread man's belly, while five other domains produce the head, arms, and legs. Points with stable orbits form all of these regions. On the other hand, the existence of any point slightly outside of this domain results in a chaotic path. Therefore, the gingerbread man's chaotic map is considered a good chaotic map when we use ACM.

This research primary goal is to improve encryption quality by raising the effectiveness and capabilities of existing image encryption techniques. Based on previous related work [4, 6, 9], different problems were addressed by suggested method.

The good encryption scheme was reflected in evaluation performance of the designed method; therefore, the obtained results is a mirror of the goodness of encryption scheme. One of encryption tests and most famous where used in most of research paper in image encryption filed is a histogram analysis. Histogram imitate the pixel's values and group them according to their values to produce a peak of values plotted in figures, an excellent diffusion phase can change the histogram shape from peaks model to smooth one or changing the entire histogram shape, the perfect example of histogram illustrate in [13], where decompose the image to their basic RGB colour channel and employed to find three histograms figures for each colour.

The designing of novelty encryption scheme for secured image transmitted over the internet remains a challenging in confusion and diffusion parts. The previous image encryption methods [4, 6, 7] give a brief background for research gaps are identified which are structured in the form of the remaining problems. Therefore, it needs to develop a novel scheme for image encryption where this scheme is combine a several methods to obtain a secure image, because the encryption scheme contains several parts such as generating encryption key, permutation and diffusion.

Excellent encryption quality still requires a strong image encryption technology, despite significant advancements. Thus, an astonishing random key with a great expansion method, a modest starting size and regeneratable capacity, enhanced confusion and diffusion techniques are all necessary for a highly secure encryption process. Three main phases of an image encryption technique were created to accomplish these goals. The proposed work consists of different novelty and contributions. These contributions are explained in the next Section II. Section III depicts some important related works. The proposed method is presented in Section IV. Experimental results are displayed in Section V, and the summary of this research is presented in Section VI.

II. Contribution

The goal of creating an image encryption system is to improve the method's intended encryption quality. This was accomplished by resolving issues raised by earlier research and offering potential solutions to overcome current limitations. Most recently, the earlier [6, 9] work that was detailed in the study review and problem background alluded to the primary difficulties that encryption system designers encountered. These issues were taken into consideration for the research's problem statement and were summed up in terms of encryption key, confusion, and diffusion, with a detailed description provided below. The encryption key needs to meet a number of strict requirements, including the initial key size, randomness, expanding mechanism, and capacity to regenerate [10, 11]. However, there is a need for major increases to the initial key size [14, 19].

Furthermore, it will be simple to cope with the growing method's requirement for additional algorithms and the small initial key size when saving and distributing to other parties. Many researchers have concentrated on confusion [18, 19], while other researchers have concentrated on diffusion [12, 14, 18] to create an accurate encryption scheme. The Shannon theorem states that both confusion and diffusion are necessary for the development of a good cryptography system to obtain a decent encryption system [19]. The proposed image encryption method consists different contributions. The below points explain briefly the proposed contributions:

- The present work introduces an improvement of the chaotic logistic map called the Modification Logistic Map (MLM). The MLM intends to increase the variability of the disorientation process by enhancing its sensitivity to initial conditions.
- In the second contribution, different chaotic maps have been used to propose a new random number for the confusion method. The proposed random number consists of Modification Logistic Map (MLM), Hénon Map Function (HMF), and the AWGN.
- The last contribution is related to the diffusion procedure. Based on diffusion method, every pixel in the image must be modified. Different technique was used within the diffusion method such as the Arnold Cat Map and Gingerbread Man and the proposed circular shifting method. These techniques were used to improve the performance of the diffusion method.

III. Related Works

In the field of image encryption, numerous methods for achieving security have been suggested, but the chaotic method is ideally appropriate due to the shares of the same cryptography characteristics [14, 15, and 17]. Nowadays, numerous chaotic-based image encryption techniques employ the confusion and diffusion technique [19] in order to produce reliable image encryption methods. Despite the fact that the proposed methods are effective, they still face a variety of obstacles. For instance, the study in [18] suggested an image-chaos method that employed chaotic mapping by associating each pair of pixels within an image with equivalents in the same image". Pixels are swapped utilizing a matrix that is created using the principles of a logistic map [19–33]. The suggested approach is both straightforward and productive. The suggested approach was assessed utilizing a correlation method that revealed the correlation between the degree of shuffling and the shuffling numbers. However, the key space of the suggested method does not meet the security requirement, as it is less than the acceptable size. Consequently, brute-force attacks will jeopardize the transmission of the encrypted image.

The encryption method suggested by [34] employs both a Rossler chaotic structure and a Lorenz chaos system. Using two or more chaotic systems in an algorithm is extremely uncommon. According to Zhu [17], chaotic behavior in the long term is periodic and dependent on initial variables. Due to the suggested approach employing the operation known as XOR between the plain image and the random image without permuting the image's pixels, the correlation among adjacent pixels of the encrypted image is expected to be less secure.

To decrease the intricacy of image encryption, Ahmad et al. [35] suggested a straightforward image encryption algorithm using dual-tree complex wavelet transformations (DT-CWT). The first step in this structure is the wavelet transformation of a simple image, followed by a pixel chaos scrambling for approximation and an Arnold transformation for the finer details. Even though the proposed image encryption approach is an easy approach, it is anticipated that the histogram analysis will yield poor results.

As outlined in the preceding overview, the creation of encryption approaches to secure the transfer of images over the internet still encounters numerous obstacles. The creation of random numbers, or encryption keys, is the primary challenge of encryption methods. The primary key is an additional problem in the field of image encryption, with criteria based on the key size, key sensitivity, degree of randomness, and capacity to regenerate [1, 4, 7, 8].

Within the context of image encryption, statistical properties for cipher outcomes including information entropy, the correlation between neighboring pixels, the histogram, and the correlation coefficient between plain and cypher images are regarded as significant issues [3, 2, 10, 14]. Furthermore, given the growing interest in differential attacks, the capacity to resist them has emerged as a crucial concern [16, 34]. Table I illustrate the list of abbreviations.

TABLE I. THE LIST OF ABBREVIATIONS OF PROPOSED WORK

List of Abbreviations		
1.	AWGN	Additive White Gaussian Noise
2.	MLM	Modification Logistic Map
3.	HMF	Hénon Map Function
4.	ACM	Arnold Cat Map
5.	GGM	Gingerbread Man Method
6.	SSIM	Structure Similarity Index Measure
7	PSNR	Peak Signal to Noise Ratio Analysis
8	MSE	Mean Square Errors
9.	DT-CWT	Dual-Tree Complex Wavelet Transformations

IV. IMAGE ENCRYPTION METHODOLOGY

The proposed method used different contributions to improve image encryption. The reverse steps of the proposed procedure were used to obtain the original image after encryption. The proposed method introduces a solution with a justified approach to the problems mentioned in the introduction. The guideline of the proposed research is described in Table II.

A. Image Pre-processing

The main phase of the proposed research is the preprocessing phase. In this phase, the input data must be manipulated and prepared before the next phase. The current study utilizes image preprocessing, which is divided into stages containing choosing the primary key and the original image, as depicted in “Fig. 1, Fig. 2 and Table II.

1) Primary key chosen: The selection of the starting key location from the Henon map function leads to the starting point of the preparation phase. “Fig. 1”, depicts a diagram of the beginning key choice process.

2) Original image chosen: In this research, the original image is selected from the SIPI dataset to be encrypted. “Fig. 2”, depicts examples of normal choosing color and grayscale images. The SIPI dataset includes three image sets categorized by the size of the image, with each of them containing both color and grayscale images [6].

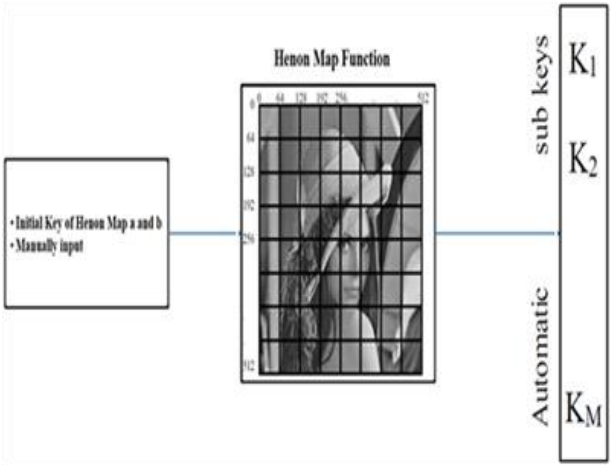


Fig. 1. Depicts a diagram of the beginning key.

Select Image

Fig. 2. The SIPI dataset image [6].

TABLE II. THE GUIDELINE OF THE PROPOSED RESEARCH

Procedure	Process activity	Objectives	Method
Phase 1 Pre-processing	• Choose an initial position for the generator. • Select plain image from data set.	Initiate the method by seed key and desire image.	• Keying the x and y position. • Determine the proper plain image.
Phase 2 Key generation	• Generate a new key based on different chaotic maps. • Expansion the key to the plain image size.	To generate an encryption key.	• Used different chaotic maps. • Proposed Modification logistic map (MLM).
Phase 3 Confusion	Ascending Key sorting. permute the image pixels according to the sorting key.	To change the pixels' position and dissolve the correlation between adjacent pixels.	- Direct swap between pixels based on the generated key. • Improved confusion method.
Phase 4 Diffusion	• Generate ginger bread man image. • Apply Arnold transform on ginger bread man image. • XOR between confused image and Arnold image. • Apply pixel rotation method.	To alter the image's pixel values and dissolve the correlation among adjacent pixels.	• Generate ginger bread man image from the same initial value in preprocessing. • Scramble the ginger image pixels by apply Arnold transform. • Apply XOR Arnold and confused image. • Shifting the binary corresponding of the XORed image pixels by amount of key value based on the rotation method.

B. *The Proposed Modification Logistic Map (MLM)*

In the suggested work, the enhanced version of the logistic map (LM) named a Modification logistic map (MLM) was suggested to increase the random number. The MLM attempts to enhance the random number of the confusion method by adding more sensitivity to primary conditions. Therefore, to accomplish this objective, multiply the output of each iteration of the LM by a number S (which needs to be greater than 1) to enhance the disparity between each loop value for input and output. Multiply will cause the resulting values to exceed the limits of the LM, meaning the output will be in excess of 1. The LM input limits are higher than (0) and less than (1), resulting in some imperfection. In order to address this issue, the mod {1} is employed to ensure the output degrees fall within a permissible range {0<Z<1}. The suggested Modification Logistic Map (MLM) is depicted in Formula 1.

$$Z_{(n+1)=}\big(rZn(1-Zn)\big) * S\ mod\ 1 \qquad (1)$$

The new criteria (S) to MLM will introduce dynamical application with more random number by employing multiply among (rZn(1−Zn)) , and S (when S >1) to amplify the outcome for each loops to introduce a more sensitive randomizes number generator. The addition of a new parameter (S) to MLM will increase the randomness of the dynamic system by multiplying (rZn (1Zn)) by S (which is greater than 1) to generate a more sensitive random number creator. The S value is utilized to enhance a new loop sensitivity to the old input from the preceding iteration. Although (mod 1) is used to minimize accumulation when feedback on the outcome of a random number creator equation keeps the range for random numbers from 0 to 1, preventing the range from being exceeded.

C. *Key Generation*

The proposed key generator is created using different chaotic maps. These chaotic maps consist of Hénon, MLM, and AWGN ma functions. The combination of three maps is useful to generate a completely random key. "Fig. 3", shown the process of the key generator in the proposed research.

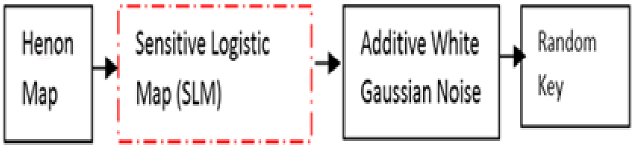


Fig. 3. The random key generation is based on different chaotic maps.

At first, the initial conditions and control Parameters are initiated manually to be used as the inputs for the Hénon map. The random sequence made up of random integers equal to the number of image rows as seen in "Fig. 4" is the result of the Hénon map.

The random key generator's second phase made use of the suggested MLM. Every row in the proposed MLM had a random sequence produced for it based on the generated sub-keys (K1 to KM), each of whose size was equal to the number of columns in the plain image N. "Fig. 5" describes the procedure mentioned previously.

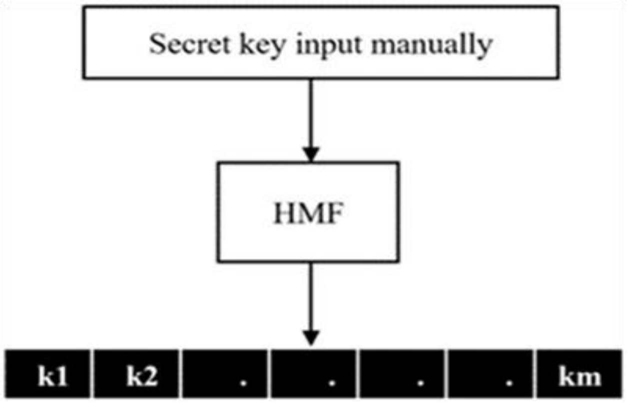


Fig. 4. The process of generating automatic sub-keys.

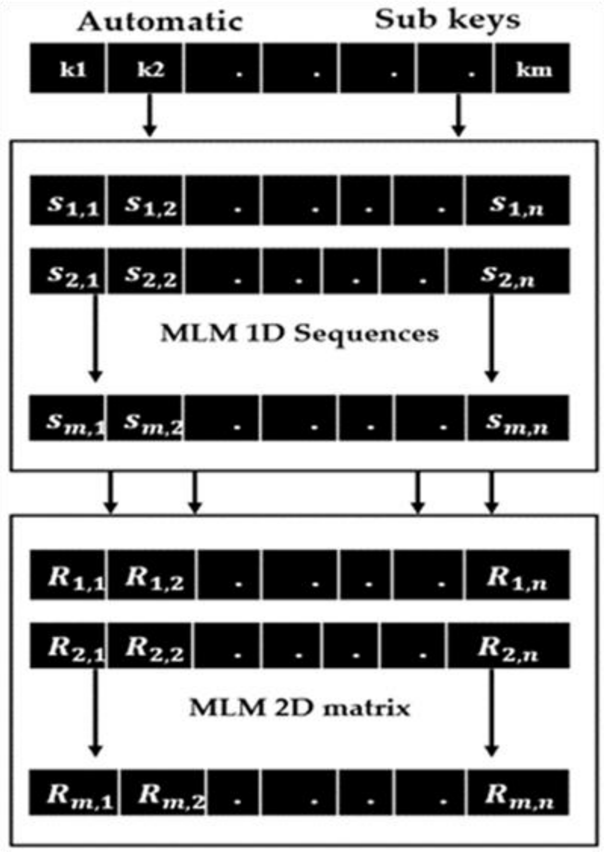

Automatic
Sub keys
k1
k2
km
$s_{1,1}$ $s_{1,2}$ $s_{1,n}$
$s_{2,1}$ $s_{2,2}$ $s_{2,n}$
MLM 1D Sequences
$s_{m,1}$ $s_{m,2}$ $s_{m,n}$
$R_{1,1}$ $R_{1,2}$ $R_{1,n}$
$R_{2,1}$ $R_{2,2}$ $R_{2,n}$
MLM 2D matrix
$R_{m,1}$ $R_{m,2}$ $R_{m,n}$

Fig. 5. Demonstrates automatic key used with MLM inputs.

Where S is the random number sequence produced by MLM, R is a two-dimensional random number matrix put together using random sequences, and K is the sub-key. An AWGN was used to create the random matrix depicted in "Fig. 6" after the random matrix was obtained by running the Hénon map and the suggested MLM to improve the random number generator's quality.

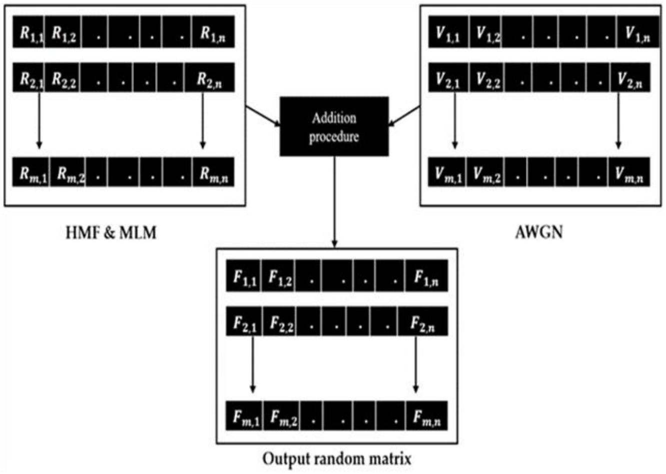

$R_{1,1}$ $R_{1,2}$ $R_{1,n}$
$R_{2,1}$ $R_{2,2}$ $R_{2,n}$
$R_{m,1}$ $R_{m,2}$ $R_{m,n}$
HMF & MLM
Addition procedure
$V_{1,1}$ $V_{1,2}$ $V_{1,n}$
$V_{2,1}$ $V_{2,2}$ $V_{2,n}$
$V_{m,1}$ $V_{m,2}$ $V_{m,n}$
AWGN
$F_{1,1}$ $F_{1,2}$ $F_{1,n}$
$F_{2,1}$ $F_{2,2}$ $F_{2,n}$
$F_{m,1}$ $F_{m,2}$ $F_{m,n}$
Output random matrix

Fig. 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.

D. *Proposed Confusion Method*

The process of reducing the similarity between the encrypted and original images is known as image confusion [18]. The proposed confusion method used the proposed random key generator and the confusion process. "Fig. 7" shows the proposed confusion method based on proposed work.

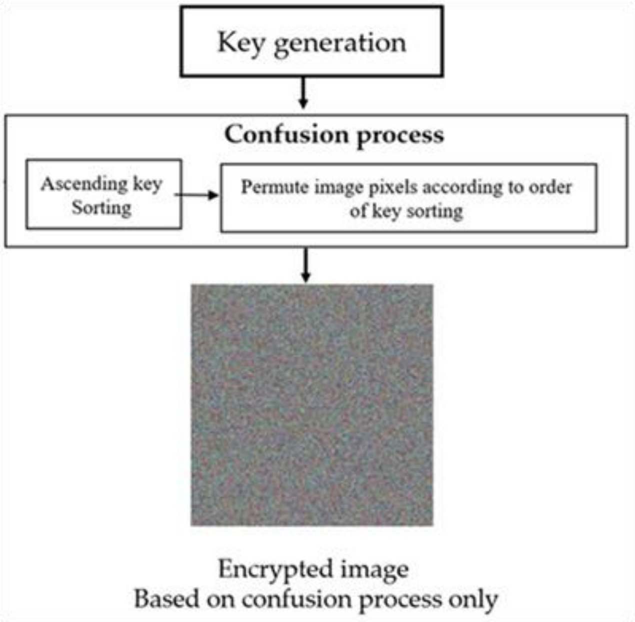

Key generation
Confusion process
Ascending key Sorting
Permute image pixels according to order of key sorting
Encrypted image
Based on confusion process only

Fig. 7. Proposed confusion method.

The proposed confusion method is start with key generation step which describe in section "C" The key generation is created based on proposed MLM and different chaotic maps. The combination of three maps is useful to generate a completely random key. The second step of proposed confusion method is confusion process as illustrate in "Fig. 7". The picture permutation method is described by the confusion process. The purpose of this study was to strengthen resistance against statistical attacks by reducing the high correlation between nearby pixels by scrambling the image pixels. In order to achieve this goal, the study suggested creating a random matrix, which is already thoroughly detailed. The purpose of this matrix is to regulate pixel scrambling during the process of visual confusion. As shown in "Fig. 8," the initial stage of the confusion process is to transform a two-dimensional random number matrix into a one-dimensional random array.

A one-dimension random array was converted, and then sorted ascendingly to account for the new order of the old indices of the sorted array (a value in the random array moves to a new location within the sorted array, and the value's original index from before sorting follows the value to the new location). Three variables were put into a table, as Fig. 9 illustrates.

Because of this, random values and their new indices are arranged in ascending order, but the old indices are arranged randomly; as a result, a lookup table comparing the old and new indices must be created. The new phase involves transforming the two-dimensional matrix plain picture into a one-dimensional array the same size as the sorted random array. Using the previously mentioned lookup table, the picture pixels are jumbled to alter the location of each pixel in the one-dimensional image array and reduce strong correlation. After the image was jumbled, a two-dimensional image array was created in order to obtain the jumbled image conversion.

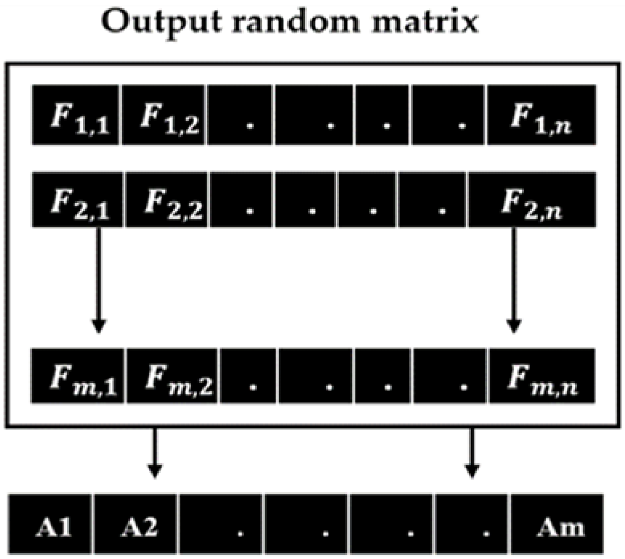


Fig. 8. Two dimensions to one dimension random matrix conversion.

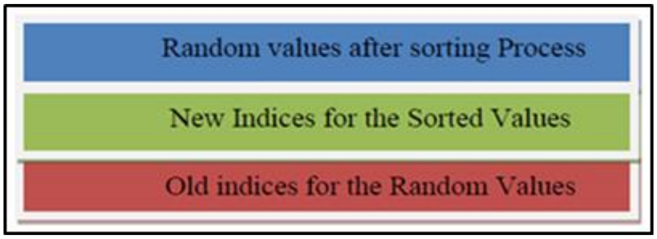

Random values after sorting Process
New Indices for the Sorted Values
Old indices for the Random Values

Fig. 9. Table of the random array fields after the sorting process.

E. Proposed Diffusion Method

The link between the key and the plain picture is said to be obscured by the diffusion process [14]. By changing the values of the pixels, the diffusion approach modifies the statistical properties of picture pixels. Therefore, the good histogram and entropy statistics findings are a reflection of the diffusion technique's effectiveness. The diffusion method is carried out in this work in two phases to change the value of the pixels. The bitwise XOR operator was used in the first stage to apply the Arnold cat map on the gingerbread man picture. The XOR operation is an ideal method to change the values of pixels while still being able to return them when fed the correct key generator. A pixel circular-shifting method is used in the second stage. Below is a description of these two steps.

1) Gingerbread Man Method (GMM): The two-dimensional chaos maps known as the multi-color GMM behave in a chaotic manner in specific fields while becoming static in others [12]. Five additional domains provide the legs, arms, and head of the gingerbread man, while the stable hexagonal sector forms the body of the figure. These all originate from points in stable orbits. On the other hand, every point that occurs within this domain but is immediately outside of it causes the trajectory to become chaotic. The geometric appearance of the GMM is created by using the relationships as shown Eq. (2) and Eq. (3). Algorithm 1 represents the pseudocode that produces from the GMM image.

$$Z(v + 1) = 1 - L(v) + |Z(v)| \tag{2}$$

$$L(v + 1) = Z(v) \tag{3}$$

Algorithm 1: GMM for image

```
INPUT   Starting value (X-position, Y-position)
BEGIN
    $X\ original \leftarrow X - position;$
    $Y\ original \leftarrow Y - position;$
    $For\ I = 1 \rightarrow Z;\ Increase\ via\ 1$
    Do
        $For\ I = 1 \rightarrow N;\ Increase\ via\ 1$
        Do
            $GMM\ (X\ original, Y\ original) \leftarrow Print\ color\ Dot;$
            $X\ New \leftarrow 1 - Y\ origin + Abs\ (X\ original);$
            $Y\ New \leftarrow X\ original$
            $X\ original \leftarrow X\ New$
            $Y\ original \leftarrow Y\ New$
        End J
    End I
END
OUTPUT  GMM image (Z, N)
```

2) Arnold Cat Map (ACM): This is a special type of chaotic map used to disturbed the high level of correlation between pixels and scramble the positions of the pixels in an image matrix. The mathematical expression for generating Arnold cat map yields in Eq. (4) and Eq. (5):

$$X\_New = (P\_1\ x\ X\_(original\ ) + P\_2\ x\ Y\_(original\ ))\ Mod\ (M) \tag{4}$$

$$Y\_New = (P\_3\ x\ X\_(original\ ) + P\_4\ x\ Y\_(original\ ))\ Mod\ (M) \tag{5}$$

where, M determines the size of the square image in 1D and P1, P2, P3 and P4 are the parameters for adjusting the chaotic behaviors and producing a good set of random occurrences with excellent characteristics of randomness, erotic, and the sensibility to the original value. The pseudocode for the creation of the ACM is represented by Algorithm 2.

Algorithm 2: ACM creation

```
INPUT   Parameter set (P1, P2, P3, P4), image (Z, N), image
        size (M)
BEGIN
    For I=1 → Z; Increase via 1
    Do
        For J=1 → N; Increase via 1
```

```
Do
    $X_{New1} \leftarrow (P_1 \, x \, X_{\text{original}} + P_2 \, x \, Y_{\text{original}})$ Mod (M)
    $Y_{New1} \leftarrow (P_3 \, x \, X_{\text{original}} + P_4 \, x \, Y_{\text{original}})$ Mod (M)
    $X_{New2} \leftarrow (P_3 \times X_{New1} + P_1 \times Y_{New1})$ Mod (M)
    $Y_{New2} \leftarrow (P_4 \times X_{New1} + P_2 \times Y_{New1})$ Mod (M)
    $X_{New3} \leftarrow (P_4 \times Y_{New2} + P_3 \times Y_{New2})$ Mod (M)
    $Y_{New3} \leftarrow (P_2 \times Y_{New2} + P_1 \times Y_{New2})$ Mod (M)
    $X_{New4} \leftarrow (P_2 \times X_{New3} + P_4 \times Y_{New3})$ Mod (M)
    $Y_{New4} \leftarrow (P_1 \times X_{New3} + P_3 \times Y_{New3})$ Mod (M)
    ACM image ($X_{New4}, Y_{New4}$) ← Image (I, J);
End J
End I
END
OUTPUT    ACM image (Z, N)
```

3) Bitwise Exclusive-OR Logic Operator: The implementation of bitwise XOR logic operator in encryption algorithms makes the operation reversal unfeasible in the absence of any information involving the initial values of one of the two used arguments such as a key or plain image. The applied XOR logic operation can be expressed mathematically as Eq. (6):

$$XOR(x,y) = 2\left[\left[\left(\left[\frac{x_{Bit}}{2}\right] mod2\right) + \left(\left[\frac{y_{Bit}}{2}\right] mod2\right)\right] mod2\right] \quad (6)$$

Where x and y are two arguments want to be applied XOR between them. Furthermore, the XOR logic operator between two images with the same dimension size guaranty one hundred present that all image pixels value will be changed to the new values. In the image encryption process the XOR operation selects each pixel of image and an encryption key to converting them to an equivalent binary byte. Then the XOR logic operator is applied on them to produce a new binary combination that represents a pre-encrypted image.

V. Experimental Results

This section outlines the findings from tests done on the suggested picture encryption technology and other analysis. The tests are performed using pictures from the SIPI standard dataset that range in size from (256x256), (512x512), to (1024x1024) pixels in both greyscale and color.

Key generation and image encryption performance of the proposed work is assessed using several metrics. Different metrics are used to examine the performance of the proposed image encryption. In addition, this section provides a benchmarking with several robust and recent types of research in terms of evaluation performance of encryption methods and reliable publishing sources. The equations from 1 to 10 On Table III illustrates the different evaluation parameters used to evaluate the propose work. The performance testing and evaluation equations of the proposed method are displayed on Table III.

A. Nist Test Suite

NIST evaluation is commonly used to evaluate the randomness of a string of characters with a total of 15 procedures. The outcome of the evaluation value is referred to as the P-value and represents the extent of sequence randomness which can be beneficial for specific purposes. If the P-value for a sequence is greater than 0.001, it is deemed random. While, when a P-Value less than 0.001value is deemed there is no random. Table IV illustrates the NIST outcome of the proposed research for Lena image grayscale.

B. Differential Attack

The suggested method needs to be sensitive to simple original images and resistant to differential assault. The differential attack has been determined using the total amount of pixels that change NPCR along with UACI. The proposed result of the differentiated attack is shown in Table V.

C. Size of (Keyspace)

The encryption keyspace refers to the collection of keys that are able to be used for encryption objectives. The extent of the keyspace has an effect on the security of the method used for encryption. In order to withstand brute-force attacks, an efficient encryption method requires a keyspace larger than 2100 bits (Table VI).

D. Analysis of Enformation Entropy

Another measure of the strength of a cryptosystem is the information entropy, which verifies the randomness of the key sequences. The information entropy indicator is used to determine the probability of occurrence change for all pixel values in the encrypted image, ambiguity being one of the biggest challenges in any image encryption. The optimal conditions exist when the probability of each pixel value is identical and the entropy value is approximately equal to 8. Table VII presents a summary of the determined entropy values for the encrypted image corresponding to the chosen input images, which are compared to the most current published value.

E. Universal Image Quality Index (UIQI)

The primary purpose of the human visual system is to derive structural information from the viewing area, for which the human visual system is highly adapted. Consequently, an evaluation of structural distortion must offer a reasonable approximation to perceived image deformation. In this method, the obtained results between plain, cipher, and recovered images are tabulated in Table VIII.

The main observation from Table VIII is that image pixels are generally non-stationary while image quality is often also space variant. In execution, it is typically desired to assess an entire image by measuring statistical characteristics locally and then combining them. “Fig. 10” and “Fig. 11” display the Q values of universal quality measurement between plain and cipher images achieved by the proposed encryption system.

TABLE III. THE PERFORMANCE TESTING AND EVALUATION EQUATIONS OF THE PROPOSED METHOD

Differential Attack	$D(i,j) = \{ \begin{smallmatrix} 0 & r_1 (I,J) = r_2 (I,J) \\ 1 & r_1 (I,J) \neq r_2 (I,J) \end{smallmatrix} \}$ (1) $\text{NPCR} = \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} D(I,J)}{W * H} * 100\%$ (2) $\text{UACI} = \frac{\sum_{I=1}^{W} \sum_{J=1}^{H} \lvert r_1 (I,J) - r_2 (I,J) \rvert}{255 * w * h} * 100\%$ (3) Where w stands for the image's width and h for its height, representing the two different encrypted images that make up r_1 and r_2. The obtained values of NPCR are theoretically close to (99%) while the NPCR > (100%), whereas the UACI ideal values are close to 33% [9].
Information entropy	$h(s) = \sum_{i=0}^{2^{m-1}} (P(s_i) \log_2 \frac{1}{P(s_i)}$ (4) Where (s_i) refers to the probability that a given symbol s_i will occur, and 2^m is the grayscale value of the image, which ranges from (0-255). Ideally, the entropy value of a cypher image should equal h. (s) =(8).
SSIM	$C_1 = (K_1 L)^2,\ C_2 = (K_2 L)^2$ (5) $\text{SSIM (P. C)} = \frac{(2\,P\,C + C_1) * (2\,cov + C_1)}{(P^2 + C^2 + C_1) * (\sigma_p^2 + \sigma_c^2 + C_2)}$ (6) where C_1 and C_2 are two variables to stabilize the division with weak denominator, L denotes dynamic range of plain image, k1 = 0.01 and k2 = 0.03 by default. P and C denote the plain and cipher image, respectively. Also, the $\sigma_p^2 + \sigma_c^2$ denotes the variance original and encrypted image res*pecti*vely, cov denotes the covariance of cipher image.
UNIVERSAL IMAGE QUALITY INDEX	$\sigma_x^2 = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2 ,\ \sigma_y^2 = \frac{1}{n-1} \sum_{i=1}^{n} (y_i - \bar{y})^2$ (7) $\sigma_{x,y} = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})$ (8) Then, we can compute $Q = \frac{4\sigma_{xy}\,\bar{x}\,\bar{y}}{(x^2 - \bar{y}^2)\,(\sigma_x^2 - \sigma_y^2)}$ (8) The Q can be decomposed into three components as $Q = \frac{\sigma_{xy}}{\sigma_x \sigma_y} * \frac{2\bar{x}\,\bar{y}}{\bar{x}^2 - \bar{y}^2} * \frac{2\sigma_x\,\sigma_y}{\sigma_x^2 - \sigma_y^2}$ (9) This quality index depicts any distortion as a three-factor mix. $Q = Correlation \times Luminance \times Contrast$ (10)
MSE AND PSNR	$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (a(i,j) - b(i,j))^2$ (11) $PSNR = 10 \log_{10} \frac{(I_{max}^2)}{MSE}$ (12)

TABLE IV. SHOWS THE NIST RESULTS FOR THREE DIFFERENT IMAGE SIZE

NIST test	**Lena grayscale image**		
	256 X 256 Size	***512 X 512 Size***	***1024 X 1024 size***
Test Name	*P-Value*	*P-Value*	*P-Value*
Entropy Approximate	0.7023	0.4077	0.3797
Frequency Block	0.6893	0.4902	0.8922
Cumulative Sums	0.7935	0.7896	0.8106
Discrete Fourier Transform	0.4838	0.4107	0.3399
Frequency	0.3963	0.3943	0.3956
Complexity of Linear	0.5693	0.5507	0.6809
Run Longest	0.5525	0.5487	0.5588
Non-Overlapping Template	0.8802	0.7097	0.8116
Template Overlapping	0.7235	0.8012	0.8020
Random Excursions	0.4899	0.4296	0.6895
RANK	0.4123	0.4397	0.8612
RUNS	0.8971	0.9124	0.8083
SERAIL	0.5021	0.5902	0.5511
Statistical Universal	0.7809	0.7421	0.8312

TABLE V. THE OUTCOME OF NPCR AND UACI UTILIZING DIFFERENT APPROACHES VERSUS THE PROPOSED RESEARCH

Images	**Ref [11]**		**Ref [16]**		**Suggested work**	
	NPCR value	***UACI value***	***NPCR value***	***UACI value***	***NPCR value***	***UACI value***
Lena	99.7004	33.3392	99.5035	33.2116	99.8994	33.2912
Tiffany	99.7956	33.1682	NA	NA	99.8387	33.1005
Girl	99.7875	33.2094	99.7028	33.3296	99.8948	33.3841
F16	NA	NA	NA	NA	99.7075	33.1022
Peppers	99.7753	33.5123	NA	NA	99. 8074	33.3226
Jelly Bean	NA	NA	NA	NA	99.7829	33.1044
Elaine	99.8944	33.2836	99.782	33.5358	99.8976	33.2823
Baboon	99.7345	33.3815	NA	NA	99.7102	33.1452
Splash	99.6279	33.5264	NA	NA	99.9883	33.1668
Sailboat	99.6933	33.4196	NA	NA	99.7845	33.1865
House	99.6948	33.6581	99.5285	33.4262	99.9012	33.2823
Lake	99.6959	33.3849	99.6138	33.4548	99.7975	33.1234
Tree	NA	NA	NA	NA	99.7728	33.1293

TABLE VI. THE SUGGESTED KEYSPACE VERSUS CURRENT METHODS

	Ref [21]	***Ref [11]***	***Ref [15]***	***Suggested work***
Key Space	2^{190}	2^{240}	2^{392}	2^{512}

TABLE VII. THE PERFORMANCE RESULT OF INFORMATION ENTROPY WITH DIFFERENT ENCRYPTED IMAGES

		Information	**Entropy**	
Images	**Ref [11]**	**Ref [16]**	**Ref [17]**	**Proposed**
Baboon	7.960851	7.9973	7.999328	7.999786
Girl	7.967375	N/A	N/A	7.969568
Lake	N/A	7.9971	7.99938	7.998599
Lena	7.955365	7.9980	7.999302	7.999878
Peppers	7.962092	7.9976	7.999342	7.999659
Sailboat	7.992138	7.9971	N/A	7.998637
Splash	7.942957	7.9977	7.999262	7.999479
Tiffany	7.976750	7.9973	7.999262	7.999385

TABLE VIII. THE PERFORMANCE RESULT OF INFORMATION ENTROPY WITH DIFFERENT ENCRYPTED IMAGES

Images	***Plain and Cipher Image***	***Plain and Recovered Image***
Baboon	0.0763	0.947
Elaine	0.0549	0.959
F16	0.0823	0.935
Girl	0.0401	0.967
House	0.0794	0.958
Jelly Bean	0.0399	0.948
Lake	0.0554	0.978
Lena	0.0481	0.943
Peppers	0.0219	0.954
Sailboat	0.0156	0.951
Splash	0.0983	0.919
Tiffany	0.0971	0.938
Tree	0.0821	0.936

F. Structure Similarity Index Measure

This test uses to measure the resemblances between two images. The SSIM is computed to determine the resemblance between original and encrypted images. The test results return a value between 1 and -1. Two images are said to be distinct from each other if the value of SSIM is equal to -1 else indistinct, otherwise, the images were similar. “Fig. 12” and “Fig. 13” display the image side-dependent variation of SSIM values achieved by the proposed encryption system.

The overall conduct for SIPI dataset explained clearly in previous two figures. That shows the occurrences of SSIM values for all images very close to -1 are very much promising and these results another prove about the goodness of the proposed method. The multiple categories of image flaws are analyzed using SSIM.

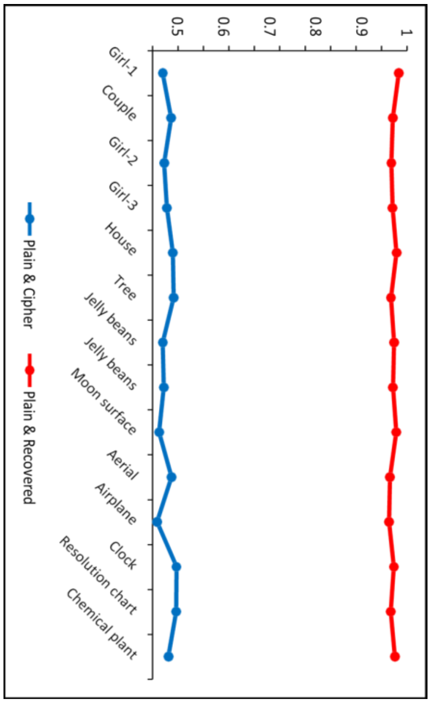


Fig. 10. Demonstrates Q values between original and cipher images based on image size (256 X 256).

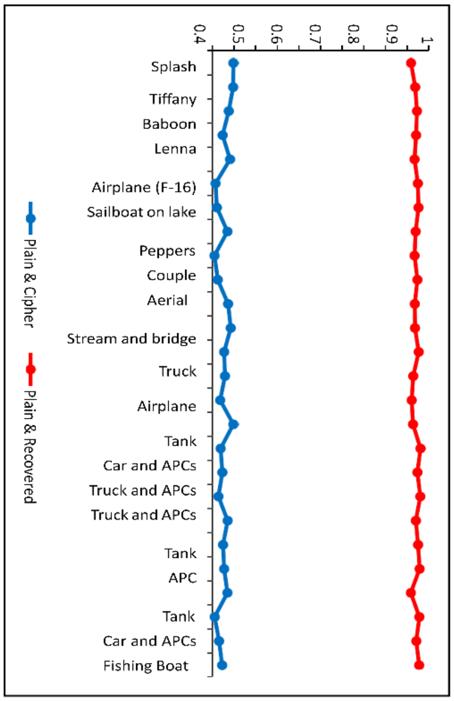


Fig. 11. Demonstrates Q values between original and cipher images based on image size (512x512).

SSIM is applicable to numerous techniques, including image/video coding, biomedical image processing, watermarking, and image encryption. This measure is used to evaluate the change in pixel intensity, cross-correlation, and variance between images.

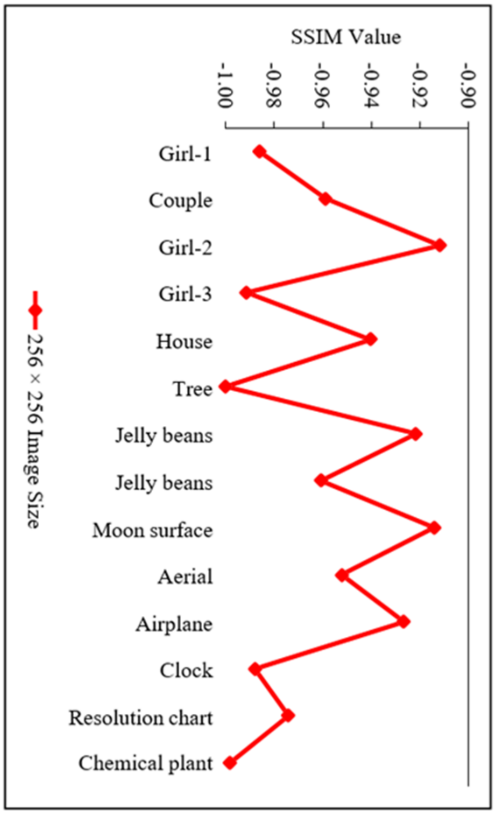


Fig. 12. Demonstrates the result of SSIM based on the size image (256x256).

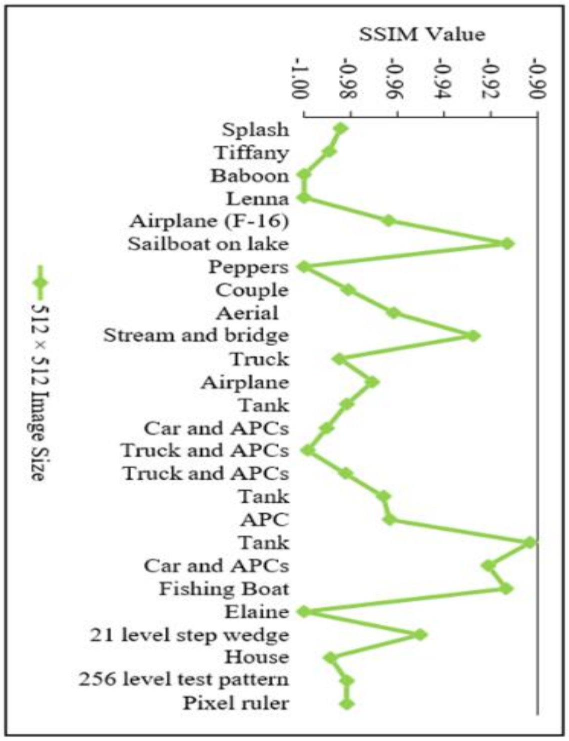


Fig. 13. Demonstrates the result of SSIM based on the size image (512x512).

The data set used for experiments is listed in Tables IX and X below, with their detailed specifications.

TABLE IX. THE EXPERIMENT RESULTS USING THE 256X256 IMAGES SIZE

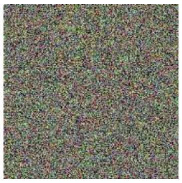
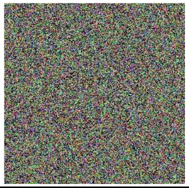
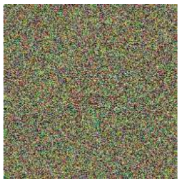
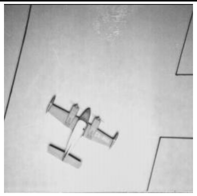
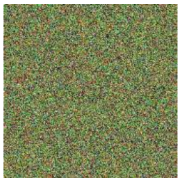
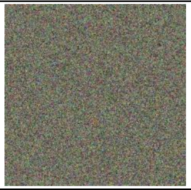
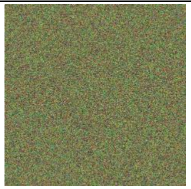
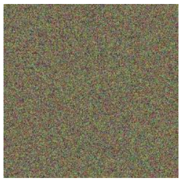
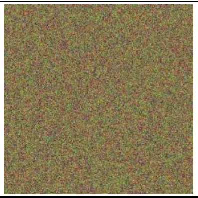
Image Name	Color	Plain Image	Cipher Image
Girl	Color		
Couple	Color		
House	Color		
Airplane	Gray		

TABLE X. THE EXPERIMENT RESULTS USING THE 512X512 IMAGES SIZE

Image Name	Color	Plain Image	Cipher Image
Splash	Color		
Tiffany	Color		
Truck	Gray		
Tank	Gray		

G. MSE and PSNR

Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR), which are based on the difference between the plain image and its corresponding encrypted image, were used to measure the effectiveness of the proposed method. Both plain and encrypted photos were used in the MSE and PSNR computations. Table XI displays the evaluation findings for MSE and PSNR.

TABLE XI. THE RESULT OF PROPOSED WORK BASED ON MSE AND PSNR

Method	MSE	PSNR
Ref [17]	9629	8.33
Ref [16]	9775	8.31
Proposed work	**9876**	**8.22**

Based on future work and the limitation of the proposed method, the image encryption is still an interesting and challenging area of research. The focus is to reach the optimality. Present work opened new avenues and many future research directions as mentioned below.

1) The main problem in image encryption is in the process of key generation. To resolve this issue, current research used different chaotic maps as a generator for the encryption keys. However, adding the new chaotic maps will enhance the generation of an encryption key. This can add more difficulty to the generated keys against attackers and improve the extra robustness of the image encryption system.

2) The swapping process between image pixels needs more time, especially when applied to the large image size. Further research is required for a fast swapping process such as the use of parallel processing technique, which may be a very useful technique for reducing the execution time.

3) A new method must be developed for hiding the initial encryption key inside the encrypted image for easy transfer among different parties, rather than sending them together one at a time.

4) Evaluation of the encryption system is very important to decide its optimality. More accurate evaluation techniques need to be developed that can give an exact measure of an encryption system.

In short, it is believed that the present study successfully resolved some significant issues related to the image encryption field and contributed to future development. The newly proposed image encryption algorithms with enhanced robustness against several known attacks may constitute a basis for highly secured and safe image transfer over open internet channels.

VI. CONCLUSION

Based on Shannon's theory [18], the ideal encryption method should have two processes confusion and diffusion, such a method has not yet been realized. The proposed work demonstrates that an ideal cryptographic secrecy method can be attained with the proposed confusion and diffusion method in addition to other processes in the proposed work. The histogram and information entropy for the encrypted image is optimal when the suggested structure is implemented. In addition, the remainder of the image's statistical characteristics, such as the correlation between differential attack and SSIM, are significantly improved. The suggested MLM with other chaotic methods improves key security by increasing keyspace and key size while preserving key sensitivity. Shortly, the proposed study successfully resolved some significant issues related to the image encryption field and contributed to future development.

REFERENCES

[1] Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." Entropy 23, no. 3 (2021): 341.

[2] Taha, Mustafa Sabah, Mohd Shafry Mohd Rahem, Mohammed Mahdi Hashim, and Hiyam N. Khalid. "High payload image steganography scheme with minimum distortion based on distinction grade value method." Multimedia Tools and Applications 81, no. 18 (2022): 25913-25946.

[3] Taha, Mustafa Sabah, Mohammed Hashim Mahdi, Hiyam N. Khalid, Azana Hafizah Mohd Aman, and Zainab Senan Attarbashi. "A Steganography Embedding Method Based on P single/P double and Huffman Coding." In 2021 3rd International Cyber Resilience Conference (CRC), pp. 1-6. IEEE, 2021.

[4] Man, Zhenlong, Jinqing Li, Xiaoqiang Di, Yaohui Sheng, and Zefei Liu. "Double image encryption algorithm based on neural network and chaos." Chaos, Solitons & Fractals 152 (2021): 111318.

[5] Hua, Zhongyun, Yicong Zhou, and Hejiao Huang. "Cosine-transform-based chaotic system for image encryption." Information Sciences 480 (2019): 403-419.

[6] Hashim, Mohammed Mahdi, Marwah M. Kareem, Waleed Khalid Al-Azzawi, Abdullah A. Nahi, Mustafa Sabah Taha, and Adnan Hussien Ali. "Based Complex Key Cryptography: New Secure Image Transmission Method utilizing Confusion and Diffusion." In 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), pp. 59-65. IEEE, 2022.

[7] Alawida, Moatsum, Je Sen Teh, and Azman Samsudin. "An image encryption scheme based on hybridizing digital chaos and finite state machine." Signal Processing 164 (2019): 249-266.

[8] Hashim, Mohammed Mahdi, Ahmed Kamal Mohsin, and Mohd Shafry Mohd Rahim. "All-encompassing review of biometric information protection in fingerprints based steganography." In Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control, pp. 1-8. 2019.

[9] Hashim, Mohammed Mahdi, Ali A. Mahmood, and Mohammed Q. Mohammed. "A pixel contrast based medical image steganography to ensure and secure patient data." International Journal of Nonlinear Analysis and Applications 12, no. Special Issue (2021): 1885-1904.

[10] Hosny, Khalid M., Sara T. Kamal, and Mohamed M. Darwish. "A color image encryption technique using block scrambling and chaos." Multimedia Tools and Applications (2022): 1-21.

[11] Li, Chunmeng, and Xiaozhong Yang. "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos." Optik 260 (2022): 169042.

[12] Saad, Mohammed Ayad, Hayder Jasim Alhamdane, S. A. H. Ali, Mohammed Mahdi Hashim, and Bassam Hasan. "Total energy consumption analysis in wireless mobile ad hoc network with varying mobile nodes." Indonesian Journal of Electrical Engineering and Computer Science 14, no. 2 (2019).

[13] Taha, Mustafa Sabah, Abbas Abd-Alhussein Haddad, Nabeel Abdulrazaq Yaseen Alrashdi, Mohammed Hashim Mahdi, Hiyam N. Khalid, and Qasim Jaber Yousif. "An Advance Vehicle Tracking System Based on Arduino Electronic Shields and Web Maps Browser." In 2021 International Conference on Advanced Computer Applications (ACA), pp. 238-243. IEEE, 2021.

[14] Alexan, Wassim, Marwa Elkandoz, Maggie Mashaly, Eman Azab, and Amr Aboshousha. "Color Image Encryption Through Chaos and KAA Map." IEEE Access 11 (2023): 11541-11554.

[15] Kareem, Marwah M., Sameer Abdul-Sattar Lafta, Raed Khalid Ibrahim, Adnan Hussein Ali, Mohammed Mahdi Hashim, and Yasir Adnan Hussein. "Exploring Attitudes Concerning The Applying Of Mobile Learning In Technical Education With Responsibility And Generativity." In 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), pp. 39-45. IEEE, 2022.

[16] Chen, Xin, Qianxue Wang, Linfeng Fan, and Simin Yu. "A Novel Chaotic Image Encryption Scheme Armed with Global Dynamic Selection." Entropy 25, no. 3 (2023): 476.

[17] Zhu, Hegui, Jiangxia Ge, Wentao Qi, Xiangde Zhang, and Xiaoxiong Lu. "Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system." Mathematics and Computers in Simulation 198 (2022): 188-210.

[18] Kumar, Sarvesh, Prabhat Kumar Srivastava, Gaurav Kumar Srivastava, Prateek Singhal, Dinesh Singh, and Dinesh Goyal. "Chaos based image encryption security in cloud computing." Journal of Discrete Mathematical Sciences and Cryptography 25, no. 4 (2022): 1041-1051.

[19] Kumar, Atul, and Mohit Dua. "A GRU and chaos-based novel image encryption approach for transport images." Multimedia Tools and Applications (2022): 1-28.

[20] Idoko, J.B., Abiyev, R. (2023). Introduction to Machine Learning and IoT. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_1.

[21] Idoko, J.B., Simsek, E. (2023). Face Mask Recognition System-Based Convolutional Neural Network. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_3.

[22] Idoko, J.B., Sadeq, M.J. (2023). Fuzzy Inference System Based-AI for Diagnosis of Esophageal Cancer. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_4.

[23] Bush, I.J., Abiyev, R. (2023). Skin Detection System Based Fuzzy Neural Networks for Skin Identification. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_5.

[24] Idoko, J.B., Mohammed, M., Mohammed, A.U. (2023). Machine Learning Based Cardless ATM Using Voice Recognition Techniques. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_6.

[25] Idoko, J.B. (2023). Automated Classification of Cardiac Arrhythmias. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_7.

[26] Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham.

[27] Idoko, B., Idoko, J.B. (2023). IoT Security Based Vulnerability Assessment of E-learning Systems. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_15.

[28] Gofwen, M.M., Idoko, B., Idoko, J.B. (2023). Application of Zero-Trust Networks in e-Health Internet of Things (IoT) Deployments. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_14.

[29] Idoko, J.B., Ahmed, B.A. (2023). Implementation of Semantic Web Service and Integration of e-Government Based Linked Data. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_13.

[30] Idoko, J.B., Ogolo, D.T. (2023). A Semantic Portal to Improve Search on Rivers State's Independent National Electoral Commission. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_12.

[31] Idoko, J.B., Palmer, J. (2023). A Comprehensive Review of Virtual E-Learning System Challenges. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_11.

[32] Idoko, J.B. (2023). The Emerging Benefits of Gamification Techniques. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_10.

[33] Idoko, J.B. (2023). Implementation and Evaluation of a Mobile Smart School Management System—NEUKinderApp. In: Idoko, J.B., Abiyev, R. (eds) Machine Learning and the Internet of Things in Education. Studies in Computational Intelligence, vol 1115. Springer, Cham. https://doi.org/10.1007/978-3-031-42924-8_9.

[34] Kumar, Vijay, and Ashish Girdhar. "A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach." Multimedia Tools and Applications 80 (2021): 3749-3773.

[35] Ahmad, Nadeem, Zainul Abdin Jaffery, and Deependra Sharma. "Low bitrate image coding based on dual tree complex wavelet transform." In 2019 International Conference on Power Electronics, Control and Automation (ICPECA), pp. 1-6. IEEE, 2019.