A Novel of Cryptography Digital Images with the Wavelet Help of Multidimensional Chaotic Mapping

Mohammad Misagh Javaherian[1]
1*Department of Computer, Lahijan branch, Islamic Azad University, Lahijan, Iran.
Misagh.java@yahoo.com
Mansour EsmaeilPour[2]
2*Department of Computer, Hamedan branch, Islamic Azad University, Hamedan, Iran.
Abbas Karimi[3]
3*Department of Computer, Arak branch, Islamic Azad University, Arak, Iran.
Faraneh Zarafshan[4]
4*Department of Computer, Arak branch, Islamic Azad University, Arak Iran.

Abstract

Today, security is one of the most important issues in countering the intrusion of illegal intruders on the privacy of individuals and valuable information of organizations. One of the most powerful tools in securing information and communication is cryptography. Regular or clutter-based encryption algorithms have many advantages over conventional encryption algorithms. Conventional encryption algorithms have many problems such as speed, high security, high cost and low security. In this dissertation, a new algorithm for Image encryption using chaotic mapping to protect the exchange of digital images has been proposed in an efficient and secure way. In this dissertation, the proposed design was measured by tests and comparisons, and according to the results obtained in tests and research, the mean values for the square error coefficients and the average accuracy of the work were 33.6248 and 99.6472%, respectively. In addition, the preconditions for quality security and execution performed by scrambled squared values (9.005955) and entropy (7.999275) have been proven..

Keywords*: Wavelet, Security, Cryptography, Multidimensional chaos mapping*

1. Introduction

Encryption is the confusion of information in a way that is incomprehensible to anyone. Encryption technology deprives unauthorized persons of the ability to view, read and interpret messages sent. Cryptography can also be implemented and used for various applications. These applications include political, military, commercial and ....

Turbulence is a phenomenon that occurs in definable nonlinear systems. This phenomenon has a high sensitivity to initial conditions as well as quasi-random behavior. The development of an encryption system can provide integrity, availability, and privacy for multimedia data. Chaos with the definable features of the system while its quasi-random behavior has been considered by many researchers to do this.

Among the cryptographic methods, chaotic-based cryptographic algorithms have good features such as speed, computing power and computational overhead, which are very important for image and video encryption. In this regard, there are different methods and algorithms. Image pixel permutation and replacement operation. These two steps are repeated until the coded image is generated.

The main problem in designing an encryption method is to quickly disrupt the location of the pixels and change their level. In cryptographic algorithms based on permutation, the pixels of the image are moved but their values do not change. In the playback phase, the values of the pixels are changed so that a slight change in one pixel is propagated to as many pixels as possible. The two stages of permutation and playback are two repetitive and separate stages, both of which require scanning the image to obtain pixel values. In this proposal, we intend to propose a fast image encryption algorithm that will improve the encryption speed and provide a digital image encryption algorithm, and we will measure this by using a series of tests and comparisons on a number of images and their implementation.

There are various algorithms to prevent unauthorized access to images and to hide them. Image data with its special features such as bulk, large additions and high pixel correlation and high compression, makes the implementation of encryption methods Text with classical algorithms such as DES, IDEA, AES on images is very hard and slow and do not have the necessary performance in this area, the second problem that exists in algorithms is their key length, which is due to the amount of encrypted data.

2. The Proposed Chaotic Systems

To improve the quality of cryptography and execution, which will be described below, we recommend the use of a new and pristine irregular system. Our system is a multidimensional, nonlinear, discrete-time technique that provides dynamic perturbation behavior. Depending on the probabilities, they can achieve more general and general explorations in a faster and shorter period of time. It can be assured that the proposed map has excellent irregularity in terms of uniform distribution conditions and has a relatively large parametric space that can be suitable for image encryption. (The diagram of this map is shown in Figure 1 (b).

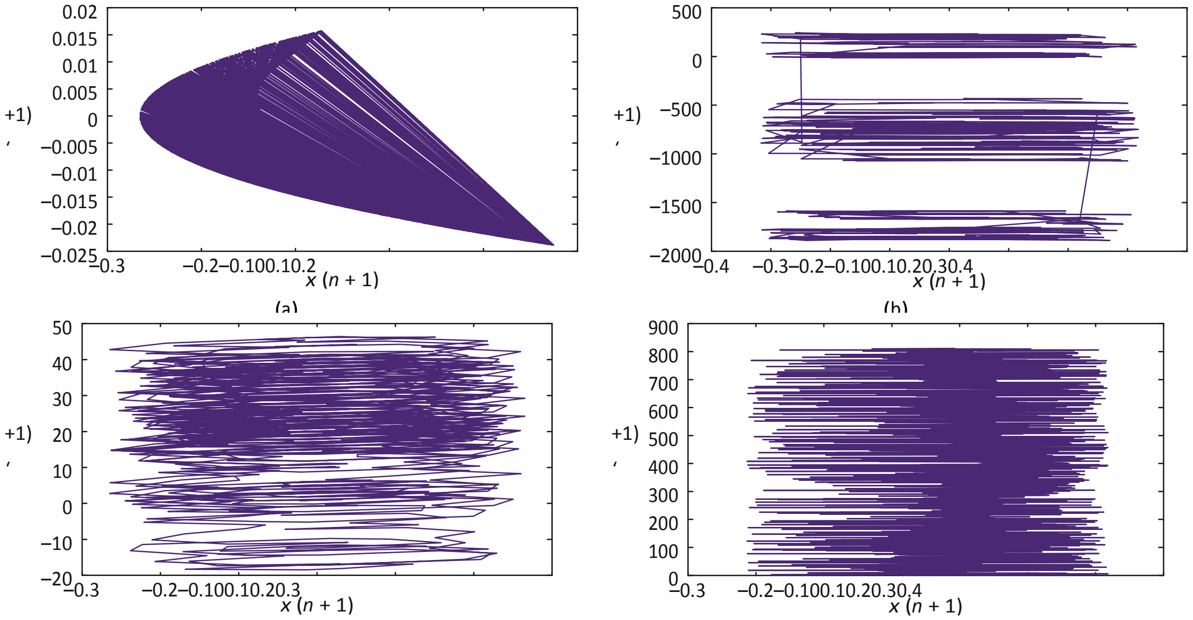

Figure 1 Numerical simulation of a 2D phase diagram on page (x, y) of the modern financial model defined by (a) Equation (1)

An example of the proposed algorithm code snippets:

```
//Chaoticproposedalgorithm
Begin
(1) Itcouldbeasystemofadiscretetimethatmapspoint        $(x-n,y-n)$.
(2) Definetheinitialvalueofmaximumnumberofiterations     t Max,upperboundary,andlowerbound,populationsize     n,numberof
dimensionsdimanddefinethefitnessfunction.
(3) Randomlyinitializethepositionsofmap.
(4) Beginiteration   (n).
(5) Selectoneofthefourproposedfinancedynamicalmodels.
(6) Endfor
End
```

ALGORITHM1: Proposedchaoticpseudocode.

The third proposed irregularity map in our pipelines is a dimensional irregularity map that includes a generation of a transmitted image so that the pixel position itself changes in a unique image in some new positions using Taking care of the following conditions will include:

$$\begin{cases} y_{n+1} = y_n - r.\tan x_n, \\ x_{n+1} = \sin x_n + \sin y_{n+1}. \end{cases}$$

Where n is the number or number of iterations using this map, the irregularity time, the state variables x and y are the same as the simulated time series, and r also represents the irregularity parameter. The diagram of this map can be seen in Figure 1 (c).

Finally, the fourth proposed irregularity map is obtained using the iterative function expressed by the following equations: (4):

$$\begin{cases} y_{1+n} = y_n + a\,.\,r\cos x_n, \\ x_{1+n} = \cos x_n + \sin y_{n+1}, \end{cases}$$

Where the turbulent time series determining the distance xn, yn ε [0,1] are generated, a and r correspond to the control of external parameters, and n is the number of recreated foci. The diagram of this map will be obtained in Figure 1 (d).

The proposed characteristics of modern financial models are obtained using MATLAB for financial parameters, for example, the initial values of the state are x (0) = 0.02 and y (0) = 0.02. The dynamics of the turbulent map are shown by the circuit. The turbulent map circuit is characterized by a discontinuous or intermittent and non-planar motion. The proposed irregular map structures are shown. As can be easily seen from the figure, each turbulent system has its own extraordinary signature - which can be a special feature of the absorber. The equilibrium that focuses on the other parts of the proposed turbulent system is obtained by understanding the following pseudocode in Algorithm 1.

3-3 -Assessing the disordered behavior or disorder of the proposed maps.

The performance of chaos can be evaluated using various techniques such as Lyapunov, bifurcation and trajectory. A quick overview of those methods is provided below. The evaluation of turbulent behavior for the proposed maps based on their branching diagrams, performance diagrams or iteration functions, and Lyapunov representative is described in more detail in the next section. Liaponov's representative shows the most salient features of a chaotic framework and can, in general, establish the public execution of chaotic maps. He used it as a quantitative scale for sensitive reliance on initial conditions. For a discrete system xn + 1 = f (xn) and for a circuit starting with x0, the Lyapunov representation can be described as follows.

$$\lambda(x_0) = \lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{i=1}^{\infty} \ln|f\prime(xi)|,$$

Where 'f is a function of capacity f. If λ is negative, this framework is not attractive. Being in a position beyond the chance of being zero for λ, this means that the relevant framework is impartially and uniformly in a perfectly consistent state. If the value of λ is definite or definite, the progression is very unpleasant for the initial condition and will therefore be in a state of disorder. Furthermore, it is not unexpected that Lyapunov Maximum Power (MLE) would not be invoked, given the fact that it was decided to think of adaptation for a riotous framework. (The larger the MLE, the more turbulent the guide, and the number or quantity of cycles to achieve the required level of dissemination or clutter of information and data will become an important factor, and this is an amazing and superior guide. On the other hand, the bifurcation diagram is normally seen as the mental progression from normal to chaotic behavior by changing the control parameter. Is used as a component of control parameter estimates.) Does the chart or diagram make us know the relevant parts of the framework and show that the bifurcation and substrate problem can rely on the estimates of the control parameters of the r parameter (16). The rotational asset scheme and the iteration of the connection between the quantities of N cycles are done and the quadrilateral state disorganizes the various estimates and the parameters remain at a certain initial value such as X0 (17). The parameter r can be divided into three domains and recreated using MATLAB was analyzed.

4-3 -Analysis of the proposed turbulent maps.

The quadratic map is the basic premise of a chaotic framework. This may provide a well-known and more widely used one-dimensional (1D) irregular logistics map illustrated with scientific repetition.

$$x_{n+1} = rx_n(1 - x_n),$$

Where r is the noisy parameter and n is the quantitative value of the repeats. The arrangement of the second-order guide is chaotic or disorderly, especially given the fact that it is a non-linear factor. This is a definite phenomenon because it has conditions that determine the behavior of the framework. Likewise, a slight difference in your core value can immediately trigger a completely unique guide behavior. From Figure 2 it can be seen that only for 3.57≤r≤4. The logistics map generally has a positive LE and scattered validity or appropriateness As shown, the logistics logistics guide has negative signs, e.g. It is a situation when -r-4 is assumed to be 3.57≤r and the smallest value is LE = 0.6923. Will be seen as focused.

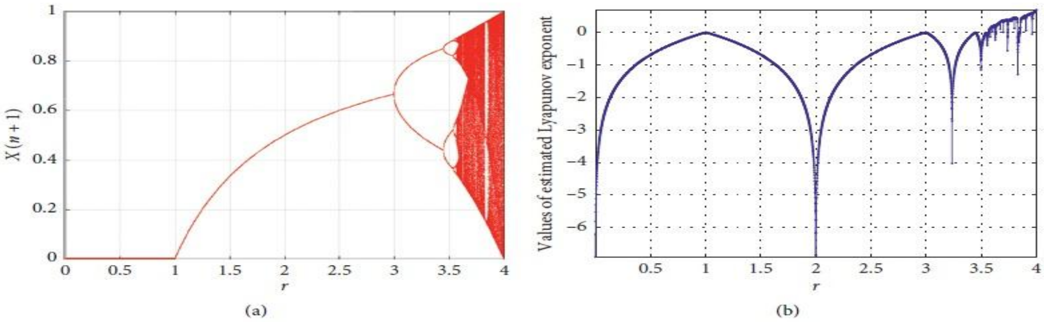

Figure 2 Logistics map: (a) branch diagram and (b) Lyaponov representative.

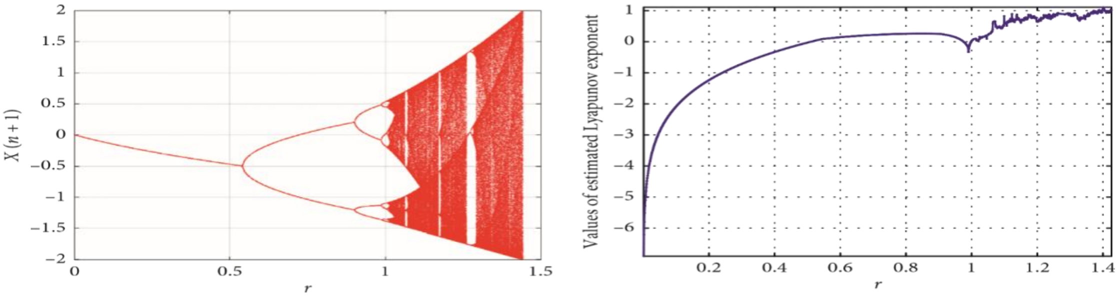

Figure 3 Branch diagram (a) and Lyapunov representative (b) for the first proposed map

1-4-3 -Analysis of the first proposed turbulent map.

The branching diagram of the first proposed turbulence map is presented in Figure 3 (a). This diagram has three areas: (i) the assembly area, which is assumed to be rε [0.55,1.0], and the place of confusion in rε [1.0,1.4]. Where the disorder behavior occurs Figure 3 (b) shows Lyapunov type of the proposed turbulent master map. It is clear that when rE (0.055) is assumed, all Lyapunov representatives will be less than or equal to zero.

When [rE (0.0.55) is assumed, Lyapunov's representatives or components are positive and therefore noisy. The maximum Lyapunov value from the initial turbulence map is 1.225. The repeatability and routing tests are shown in Figure 4. After a few stresses without any perturbation behavior, when rε [0.55, 1.0] is assumed, as shown in Figures 4 (b) and 4 (e), the framework shows that it has an alternating behavior. [1.0,1.4], becomes a turbulent system as shown in Figures 4 (c) and 4 (f).

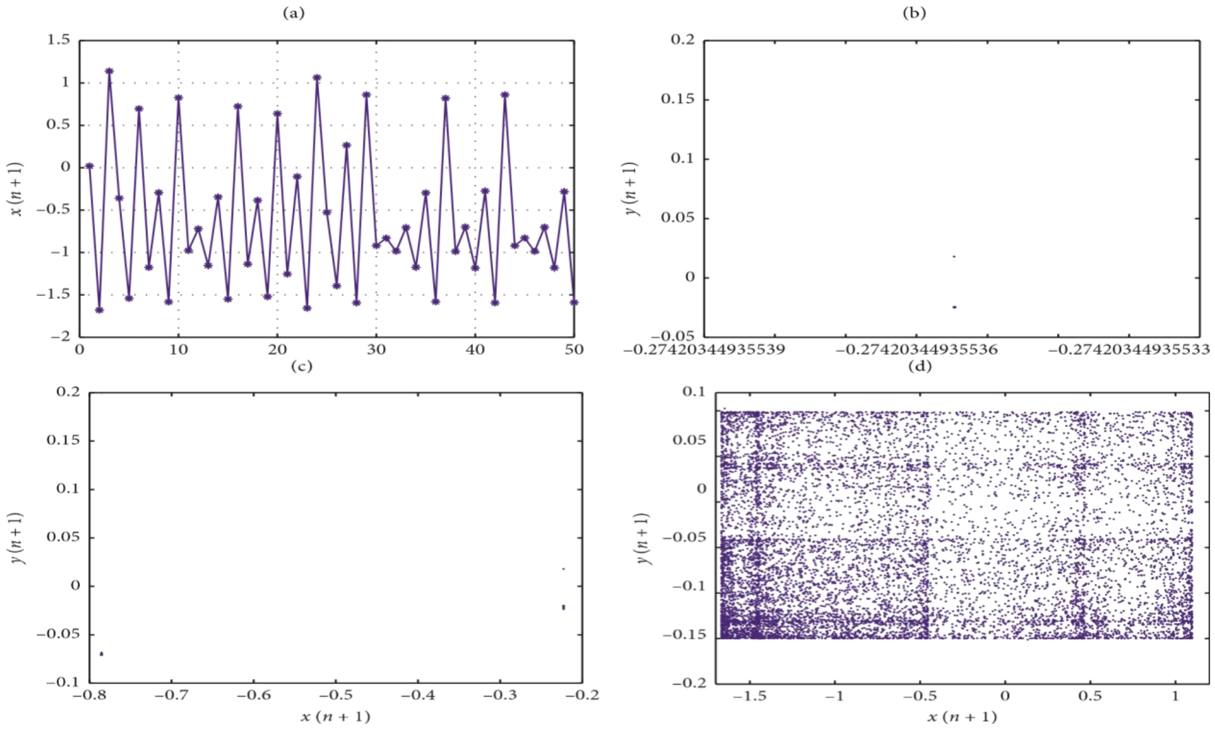

Figure 4 Repeat analysis and path of the first proposed turbulent map

2-4-3.- Analysis of the second proposed turbulent map

The behavior of the second proposed map is introduced through Figure 5. As shown in the branching scheme shown in Figure 5 (a), the guide clearly shows an irregular behavior in rε (500). (0.2%) is around r = 2.0 and its branching point is [4,5]. In Figure 5 (b), for all estimates of r, regardless of [5, ∞], the representative or component Lyaponov has a positive value.

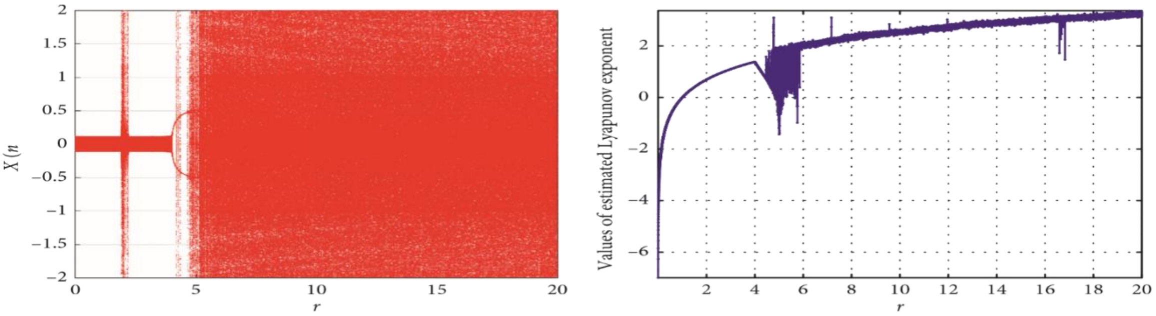

Figure 5 (e) Branch diagram (a) and Lyapunov representative (b) for the second proposed map

Along these lines, the proposed map shows a turbulent behavior in the rest of the range. (The MLE of the proposed map is 3.317. (The iteration and trajectory analysis for the second map proposed in Figure 6 is presented.) The bifurcation site in r is E (4,5) .As shown in Figures 6 (a) and 6 (d), the value determined after several cycles without any turbulent guidance reaches approximately the same result. [4,5], as shown in Figures 6 (c) and 6f), this system is shown as an occasional behavior. When [5, ∞ is present, as shown in Figures 6 (c) and 6 (f), it becomes a chaotic system.

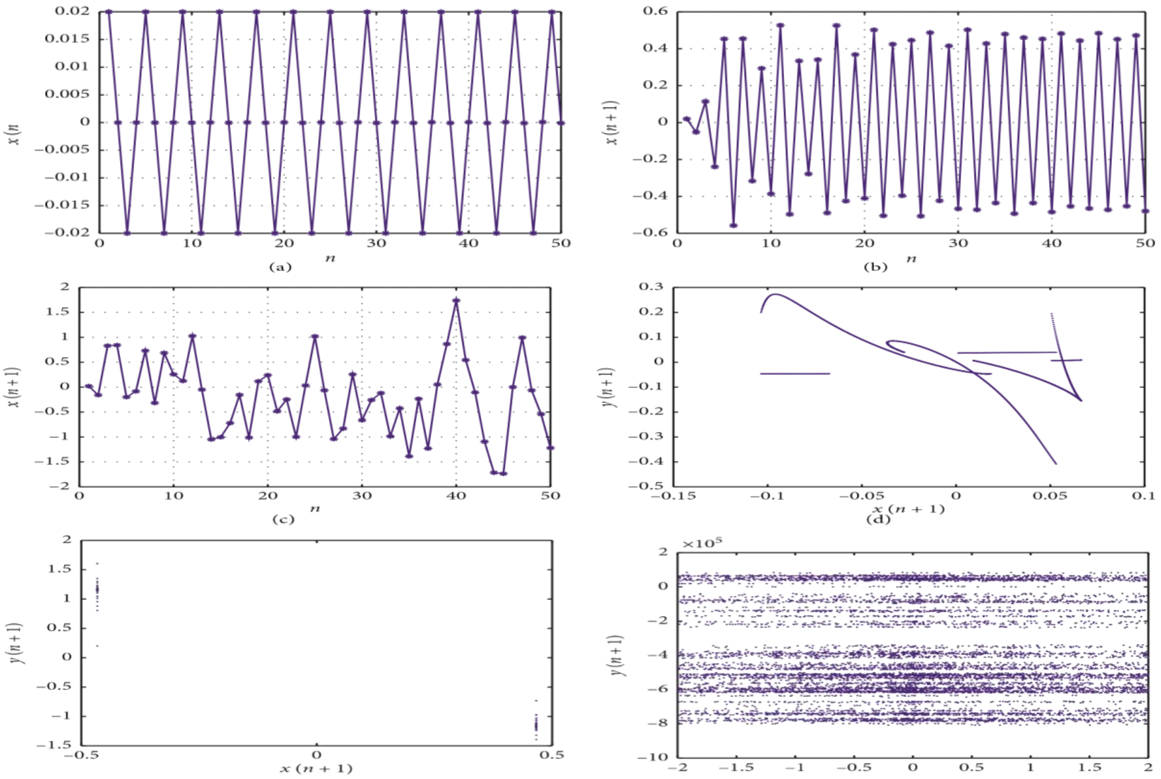

Figure 6 Repeat analysis and path of the proposed chaotic second map

3-4-3.- Analysis of the proposed map of the third chaos

Figures 7 a) and 7 (b) show two branches of Lyapunov components. As can be easily seen, the convergence regions are infinitely wide at r∈ [0.04.0], r∈ [6.8,7.8] and The likes of it fall. Usually the branching regions are infinitely large at r∈ [4.0,5.7], r∈ [7.9,8.2] and so on. Chaotic regions exist in the assumptions r∈ [6.0,6.5], r∈ [8.5,13.0], rE (14.5,19), etc., except for small assembly points and bifurcation, where turbulent behavior Falls are seen. Figure 7-b, Lyapunov's representative, conveys a positive motivation in all r estimates. Hence the proposed chaos may show a disordered behavior in the rest of the range. The MLE value in the third case is 4.499.

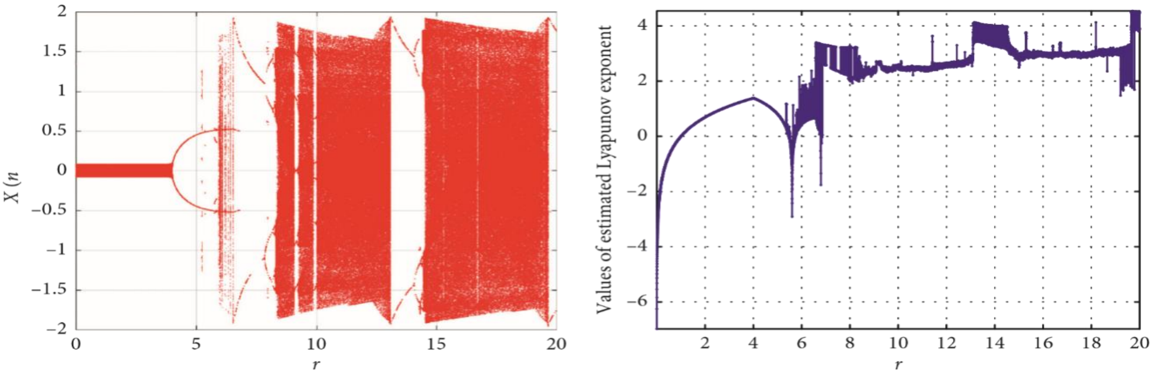

Figure 7 Branch diagram (a) and Lyapunov representative (b) for the third proposed map

Analysis and routing emphasis for the third guide in Figure 8. introduced. After emphasizing several times without any disorganized behavior, we will reach the same result. As shown in Figures 8 (b) and 8a), the framework is shown to have an intermittent and uniform behavior. When the assumptions [4.0.5.7], r∈ [7.9,8.2], and so on.], R∈ [8.5,13.0], r∈ [14.5,19], are discussed within the framework of a mediator treatment shown towards framework in accordance with the above-mentioned assumptions led to a never-ending point and become a chaotic system Be as shown in Figures 8 (c) and 8 (f).

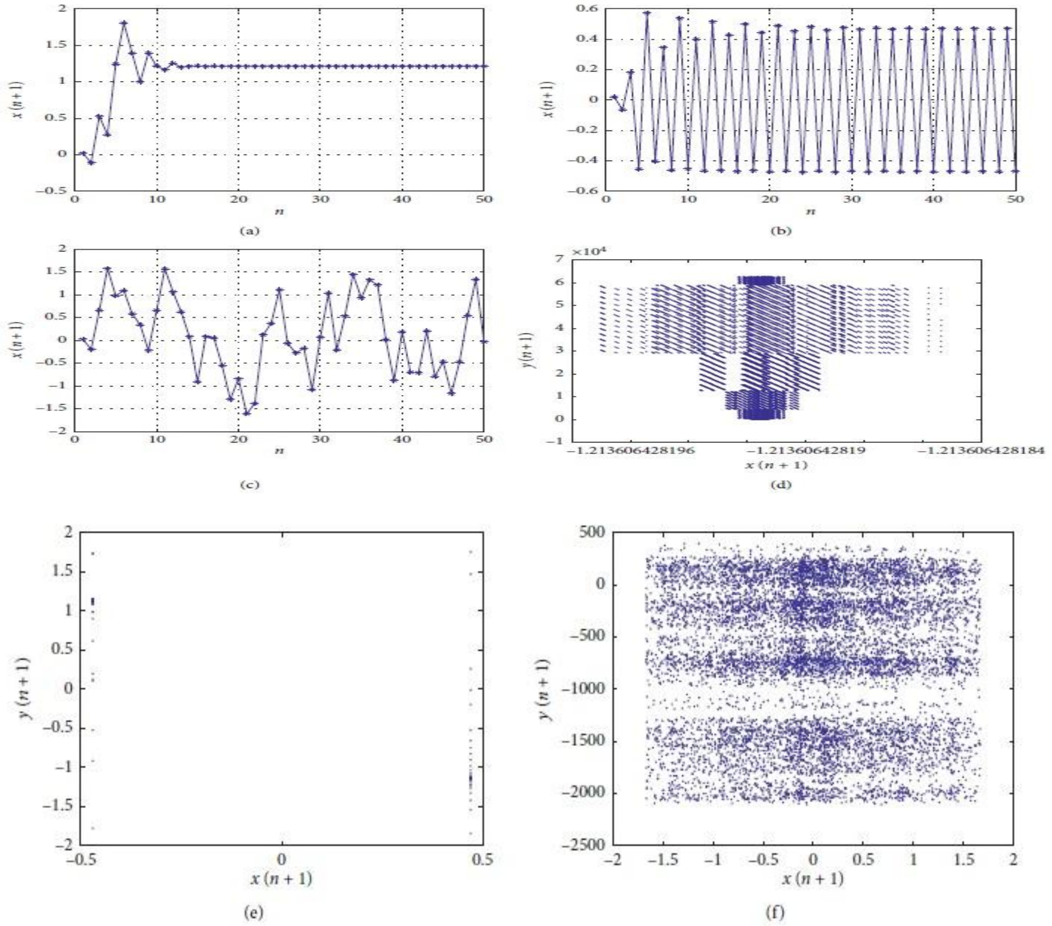

Figure 8 Replication and analysis of the proposed proposed map path 3

5-4-3.- Analysis of the proposed map of the fourth chaos

In Longlast, the disordered behavior of the fourth guide is shown in Figures 9 and 10. (The branching diagram in Figure 9 (a) shows the hybrid, bifurcated, and chaotic regions and the flexibility can be seen. (External branching regions [4.4, 4.5]], r∈ [8.55, 8, 7] Etc. for the ability to play a mediating role (and the assembly regions of atr∈ [4.2, 4.3], r∈ [8.4,8,8.5], etc. contribute to the inexhaustibility of the variable. 8.8,12.5] etc. is boundless, where wrong behavior occurs.In Figure 9 (b), Liaponov's representative has a positive motivation with the assumptions df atr∈ [4,5,8,4], r∈ [8,8,12.5], Etc. are considered to be inexhaustible and consequently the fourth noisy map proposed shows the amazing behavior in these periods. (MLE The proposed map is set at a scale of 3.091.) Iteration and routing test for the fourth map The proposed perturbation is presented in Figure 10. The assumptions Whenr∈ [4.2,4.3], r∈ [8.4,8,8.5], etc. contribute to the greater breadth as shown in Figures 10 (a) and 10.

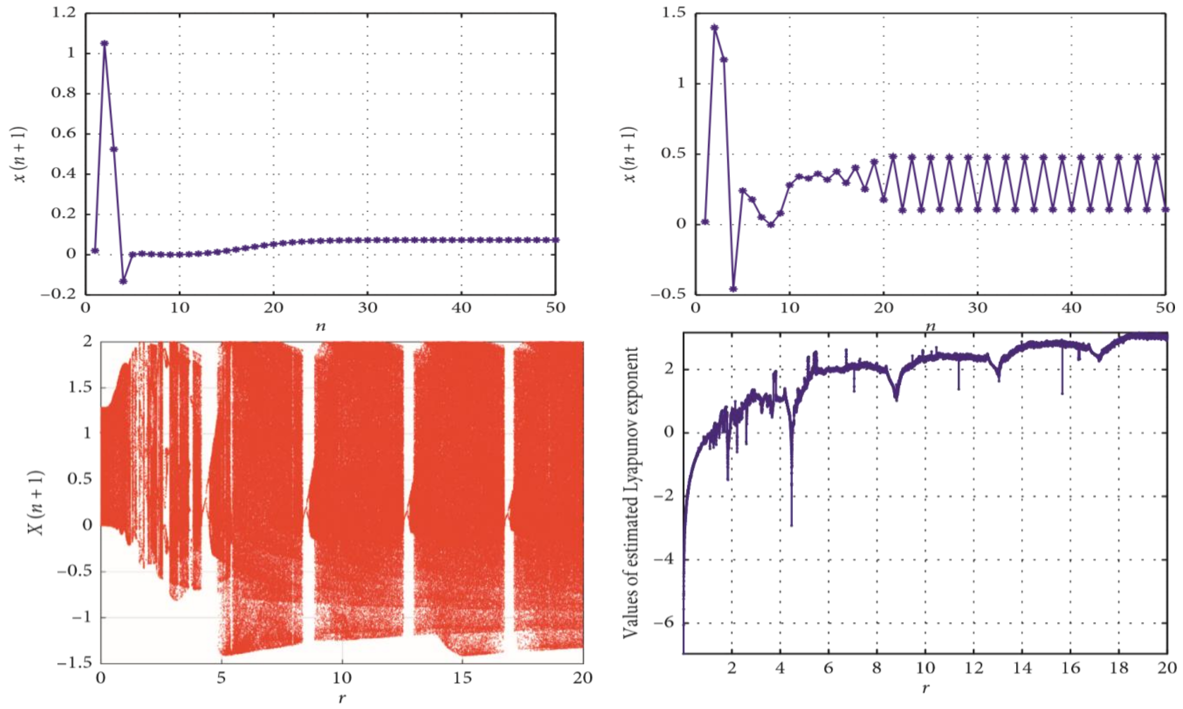

Figure 9 (Branch diagram (a) and Lyapunov representative (b) for the fourth proposed map

(b), here certain qualities with the same results are seen after the repetitions with irregular behavior. In addition, after repetition with unpleasant behaviors, we reach a similar result. As shown in Figures 10 (b) and 10 (e), the system without delay when [4.4.4.5], r∈ [8.55,8.7], etc. is shown, the system as a behavior Occasionally shows itself. The assumptions r∈ [4,5,8,4], r∈ [8.8,12.5] etc. are infinitely transformed into the acoustic system as shown in Figures 10 (c) and 10.

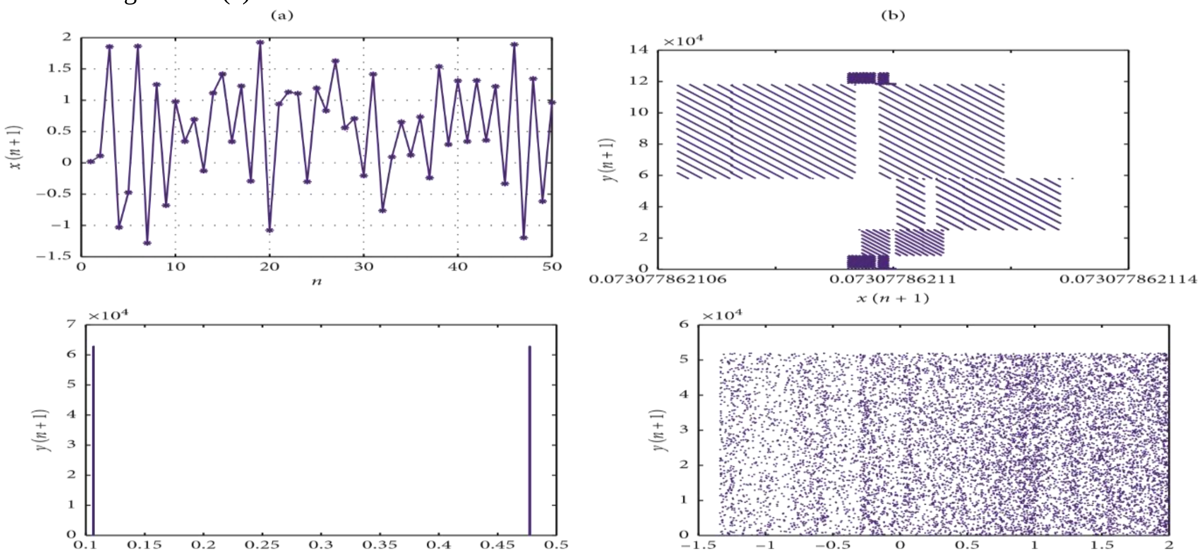

Figure 10 Repetition and path analysis of the proposed fourth turbulent map

(Story 1 is a summary of the study of classical and proposed turbulent maps. This represents an improvement in the turbulent parameters of the MLE.3 domain. The proposed encryption system As shown in Exchanges (1) to (4), the proposed turbulent capacities are used. (These capacities together guarantee the complexity and propagation method for encryption. To increase security and reduce encryption time, the algorithm is also supported by logical operations (encryption structures and decryption methods are shown in Figure 11).

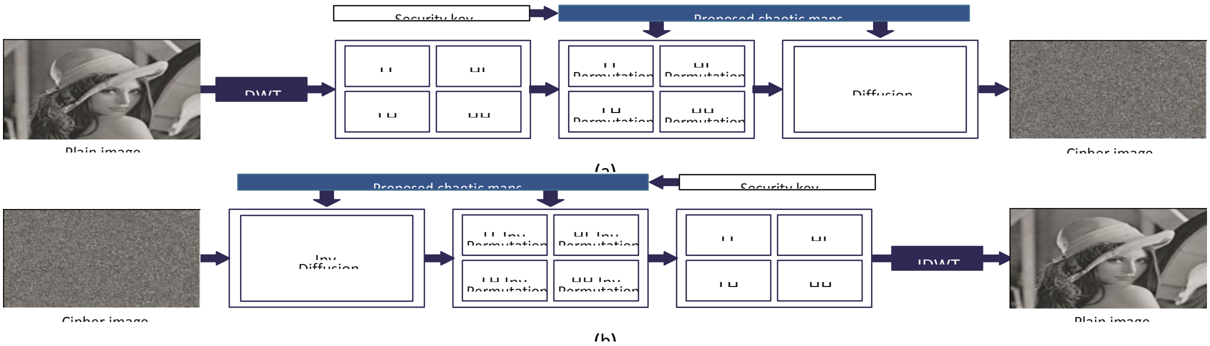

Figure 11 Schematic illustration

e DWT is based on the operation of filtering the top and bottom points of the bus in the analysis of the inner bands below the image. To parse a level, it presents animation as four subdivisions of work nds; The first sub-band represents the low-low approximation (LL) image and other details of the display in the low-low horizontal (HL), low-high vertical (LH) and very high diagonal (HH) directions. (The four proposed maps are used to reposition the four sub-band pixels.) DiscreteWavelet Transform (IDWT) enables complete image reconstruction. The following section contains details of encryption and decryption algorithms. Primary and control parameters (key modes) are extracted from the secret key and the proposed maps are used to generate disturbed consequences.

5-3.Encryption process

(The proposed image encoding for chaotic structure is shown in Figure 11 (a). Wavelet, permutation, and diffusion) steps arer0510152021.510.50–0.5–1–1.5–2X (n + 1) (a) -) - T - DfiD {lues0of0estim ted0By punov0exponentxTD) qD qT q) qx Dfiqfir (b) Figure 5:Staging and Diffusion Tasks To use noisy modes and simple image information to change pixel positions and replace pixel credits separately, create an amazing cryptographic image.

6-3.Discrete wavelet transform

The publishing step in the proposed encryption scheme is done by the specified key with a simple image calculation that uses only the public scattering activity and the key relies on the main key and the main image (in the diffusion method our method depends on the proposed turbulent maps. We will talk about the encryption method exactly, because decryption is the opposite method (the subtleties of the encryption method can be summarized by algorithm 2.3.2.

7-3 Decryption process

The activity decryption method is the opposite of the encryption method. A matrix representation of the decoding structure is shown in Figure 11 (b). Using similar ciphers, a noisy record can be created for grouping the irregular vectors created in the coding process. It consists of three basic steps: reverse diffusion, reverse configuration, and IDWT. We obtain the combined alternative vector and reassemble it into four-step subgroups (LLP, LHP, HIP, and HHP. We get the original P. (The decoding method is described in detail in Algorithm 3.4. Performance Criteria (Quantitative performance of the proposed methods compared to traditional techniques can be measured using different criteria.) These include 1) statistical parameters, (2) differential parameters And 3) efficiency parameters are 4] statistical parameters. A good password should be highly resistant to any measurable examination. To confirm the security of any encryption method, the following statistical tests should be performed.

8-3.Histogram analysis

An image histogram depicts the image transformer by plotting the number of pixels on each level of the gray scale. (Plain text redundancy and irregular vectors created in the encryption process). (The decoding calculation also consists of three basic steps: reverse diffusion, reverse confusion, and first, we convert the encrypted image to C insizeM × N. At that moment t, we generate a reverse diffuser vector. In addition, we obtain the combined alternative vector and combine it into four-phase subgroups (LLP, LHP, HIP, and HHP), and finally, the default phase subband (LL, LH, HI). And HH) are recorded using the wrong recording order and the original image of P is obtained using IDWT (the decoding method is detailed in Algorithm 3.4. Performance Criteria) Quantitative performance of the proposed methods compared to traditional techniques Power can be measured using different criteria. These include (1 statistical parameters, 2 differential parameters, and 3) efficiency parameters [4] are statistical parameters.A good code should have high resistance to any measurable test The following statistical tests should be performed to confirm the security of any encryption method

Histogram Analysis An image histogram depicts the pixel links of an image by plotting the number of pixels at each level of the gray scale. (And the redundancy of plain text must be hidden in the distribution of the encrypted text, and this logical division must be uniform). From the following image, irregular vectors created in the encryption process are obtained.

$$P_n = \frac{\text{number of pixels with intensity } n}{\text{total number of pixels}}, \quad n = 0, 1, \ldots, L-1,$$

(The decoding calculation also includes three basic steps: reverse diffusion, reverse confusion, and IDWT. First, we convert the encrypted image to C insizeM × N. In that step, we generate a reverse image distributor. In addition, we obtain the combined alternative vector and reassemble it into four-phase subgroups (LLP, LHP, HIP, and HHP), and finally the last inverse phase default band (LL, LH, HI and HH) Using the wrong recording arrangement and using the original IDWT P (the decoding method is given in detail in Algorithm 3.4. Performance Criteria) The quantitative performance of the proposed techniques compared to traditional techniques can be Measured using various criteria. (Including the latter (i) statistical parameters, (ii) differential parameters, and (iii) performance parameters. Details of these criteria are provided below.

4.1. Statistical parameters. Any measurable test To confirm the security of any encryption method, the following statistical tests must be performed

. Histogram analysis. The image histogram depicts the pixels of the image by plotting the number of pixels in each level of the gray scale. (Plain text redundancy should be hidden in the encrypted text distribution, and logically this segmentation should be uniform).

DWT is known for its versatile image in many video / video applications. (The basic thinking of DWT for a two-dimensional image is shown below. By changing the pyramid of an organized pyramid wave, the original image will be confronted with several different digits. Produces subgroups LL, LH, HL and HH.

To obtain the following large-scale scale wavelet coefficients, the LL subband is further dissected and is essentially the subpoint that is being investigated. This method can be restored several times. The OI is the pixel value of the original image, and the DI pixel is the value of the decoded image. Evaluation is the degree of randomness. (Message source entropy can be calculated as.

$$R = \frac{\sum_m \sum_n \left(\mathrm{OI}_{mn} - \overline{\mathrm{OI}}\right)\left(\mathrm{DI}_{mn} - \overline{\mathrm{DI}}\right)}{\sqrt{\left(\sum_m \sum_n \left(\mathrm{OI}_{mn} - \overline{\mathrm{OI}}\right)^2\right)\left(\sum_m \sum_n \left(\mathrm{DI}_{mn} - \overline{\mathrm{DI}}\right)^2\right)}},$$

Where does not show the number of bits for each symbol and p (meters) probability symbolmi.4.2. Differential parameters and encrypted image should be sensitive to minor changes in plain image. An attacker can change many features in a simple image to make changes to an encrypted one. Attacks lose their effectiveness and become useless.

```
Input: plain image P
Output: cipher image C
Begin //Permutation Process
  Step 1: examine the plain image P in size $M \times N$. P can be a gray-scale or RGB image.
  Step 2: decompose the image into four level sub-bands (LL, LH, HL, and HH) by the selected DWT.
  Step 3: choose a two-dimensional chaotic system and generalize it by introducing the initial values ($x_0$, $y_0$, $a$, $b$, $r$) , these initial values as secret keys.
  Step 4: generate the chaotic sequences using the proposed chaotic maps and set the appropriate values of the secret keys. Can use the 1st proposed chaotic map.
  Step 5: change the chaotic sequence, with the same method, into a consistently dispersed grouping by altering the initial values and parameters.
  Step 6: iterate the chaotic sequence for LL sub-band for scrambling $LL_P$ row by row and column by column (starting from the first row and the first column)
  Step 7: like step 3, compute the next quantized chaotic pair using the 2nd, 3rd, and 4th proposed chaotic maps to scramble the next sub-bands of LH, HL, and HH, respectively, and reiterate this step total times. (When the last row or the last column has been scrambled, switch to the first row or the first column over again.)
  Step 8: combine the chaotic vectors ($LL_P$, $LH_P$, $HI_P$, and $HH_P$) into one vector with $S_k$ in size $M$
  $\times N$. Step 9: make the new vector of mistook pixels for $S_P$ in size $M \times N$ as $S_P$ $S_K$(index).
  //Diffusion Process
    Step 10: adjust and change the vector $S_P$ realizing that every component of level gray ranges in [0, 255] utilizing the accompanying condition: $S_P(i)$  mod(round($10^{12} S_P(i)$), 256), where $1 \leq i \leq M \times N$
    Step 11: create the diffused vector with $S_D$ in size $M \times N$ as follows: $S_D$ $S_P \oplus S_K$, where $\oplus$ denotes the exclusive OR operation bit by bit
        Step 12: create the final matrix with cipher image C as follows: C  reshape($S_D$, $M$, $N$)
```

Algorithm 2: Proposed encryptionprocess.

```
Input:cipherimageC
Output:plainimageP
Begin
  Step1:producethedeshuffledvectorasfollows:    $S_P$   $S_D \oplus S_K$,where  $\oplus$denotestheexclusiveORoperationbitbybit
  Step2:producethepermutatedeachvectorasfollows:    $S_P$   $S_K$ (index)
  Step3:obtainthepermutationsub-bands($LL_P$,$LH_P$,$HI_P$,and$HH_P$)
  Step4:oppositestageandreshapevectorcomponentsutilizingthechaoticindexsequencetogetsub-bands(LL,LH,HI,andHH)
  Step5:useIDWTrecoverstoobtaintheoriginalimage
End
```

ALGORITHM3: Proposeddecryptionprocess.

9-3 Mean squares error

(Mean Error Squares (MSE)) This dissertation is used to measure the difference between simple encrypted images and square errors. (The high value of MSE is due to the large difference between plain and encrypted images. This can be represented as Equation (10):

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i)\log_2(p(m_i)),$$

$$\mathrm{MSE} = \frac{1}{M_x N_x f} \sum_{K=1}^{f} \sum_{i=1}^{M} \sum_{j=1}^{N} (P(i,j) - C(i,j)]^2,$$

Where there are no columns, it shows the wrong number of rows and the number of image frames. (Parameters P (i, j) and C (i, j) reference are converted to plain pixels and encrypted images, respectively. For a 30 dB MSE≥, there is a difference of 4.2.2. The mean square error is normalized. Another popular performance measure for MSE is the Normalized Mean Square Error (NMSE), which is equal to the MSE divided by the maximum MSE in Equation (11) [30].

$$\mathrm{NMSE} = \frac{\mathrm{MSE}}{(\max \mathrm{MSE})}.$$

10-3 Maximum signal to noise ratio

And Maximum Noise Rate (PSNR) measures the correspondence between the decoded images at the source [31]. For an image with size M × N, it can be evaluated as follows:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{Max}_{01}^{2}}{\mathrm{MSE}}\right)\mathrm{dB},$$

Where Max01 shows the maximum possible pixel value for the original image. For a good encryption algorithm, thePSNR should be as small as possible between the plain and the encrypted image. The number of pixels in the rate varies. PixelsChange Rate (NPCR) digits are used to measure the percentage of different pixel numbers between the original and decoded images and are evaluated under the following conditions:

$$\mathrm{NPCR} = \left[\frac{1}{M \times N \times f}\sum_{K=1}^{f}\sum_{i=1}^{M}\sum_{j=1}^{N} D_i(i,j)\right] \times 100\%,$$

$$D_i(i,j) = \begin{cases} 0, & \text{if } \mathrm{OI}(i,j) = \mathrm{DI}(i,j), \\ 1, & \text{if } \mathrm{OI}(i,j) \neq \mathrm{DI}(i,j). \end{cases}$$

Evaluate the amount of pixel change in the encoded image after modifying it in a pixel of an original image; Despite the higher value for NPCR, more efficient performance [32] (practical value of 1-NPCR should be approximately 0.99.

11-3. Intensity of unified average variable:

Measures the average difference between plain and decoded images. This can be calculated using the following equation)

$$\mathrm{UACI} = \left[\frac{1}{M \times N \times f}\sum_{K=1}^{f}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{\mathrm{OI}(i,j) - \mathrm{DI}(i,j)}{2^{l} - 1}\right] \times 100\%,$$

Where the number of columns is denoted by N, the number of wrong rows, fis the number of image frames, the encrypted hidden image, the OI of the original image, and then the number of bits per pixel of the original image.

12-3 Performance parameters

High performance and speed are also essential for a successful encryption, between simple images and encryption. Specifically, for real-time Internet applications. In general, much encryption speed depends on CPU / MPU, RAM size, operating system, programming language and compiler option. Therefore, there is no need to compare the image encryption speed of two cryptographers using two different devices.

(The most commonly used parameter for performance analysis) s is a time slip (s) that speaks to the overall encoding calculation time as well as the decoding time / s prepared for the initial tests. Experimental results Most cryptographic algorithms are tested using very poor examination. (Analysis is used to find the distance between the encrypted image and the original image.

Tests and results

All our tests were performed using a 7-core Windows i5-2400 with 4GB of RAM, 160GB of HDD and the same version of the MATLAB programming environment. Our device was mostly connected to the web. The experiments are connected more than once, so the elapsed time represents the average simulation time for each test. (Implementation of the proposed algorithm is tested using MATLAB R2017a, in which the experimental arrangement of the main tests is tested) Images. With the multi-map circuit key, the proposed maps of each shape are formed. (The most important direct method for selecting an irregular degree is the image encoded by the sense of sight. On the other hand, the randomness of the encrypted images can be quantified by the connection coefficient. Using the proposed maps, the parameters must be adjusted accordingly. To agree with step 1 in algorithm 2. Based on the experimental approach, the histogram for the selected sample images is shown in Figure 14.

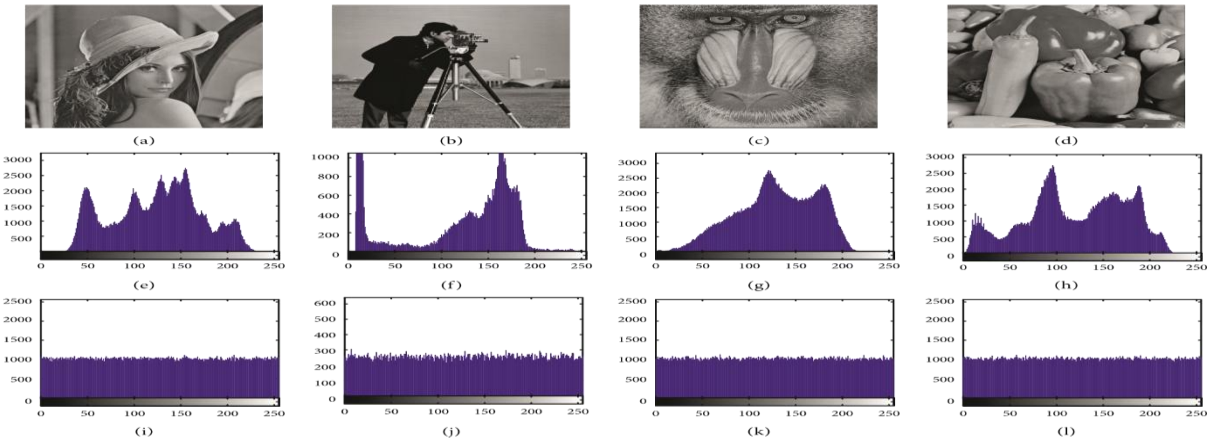

Figure 14 Simulation results of sample experimental images

As shown in Figure 14 (i) –14 (l), the graphs of the encrypted images are uniform and have no clue as to the use of any actual attack. After that, it is difficult for attackers to actually test because there is no valuable data in the encrypted images. Key space analysis (Total space is the total number of different keys that can be used in the encryption process. (The proposed calculation consists of two correction proposals: permutation and propagation). In the alternative method, we use four proposed maps. With autonomousfactorsx0, y0, a, bandr for four subbands.

In the propagation process, the proposed pressure fist map has dependent variables x0andr. We have a wholenumbercandc compatibility in the key specified by the plain content algorithm

[1, 255]. (We have the key space {x0, y0, a, b, r.. Since x0, y0, a, the numbers are twice the accuracy of the band, the absolute number of different qualities forx0, y0, a, bandrismore is more than 1014 In this way, the key space will be larger than 1014 × 1014 × 1014 × 1014 × 1014 × 255. (The key space is sensitive to resist the attack of a brutal force.

4-2- Key Sensitivity Analysis

In addition to histogram analysis, we have used another important feature of decryption cryptography, which is key sensitivity during decryption, that any slight change in the key will lead to a variety of results. Even if only one parameter has changed, the encrypted data cannot be decrypted. In addition, the information cannot be decrypted by knowing all the keys, because encryption does not occur in the correct order.

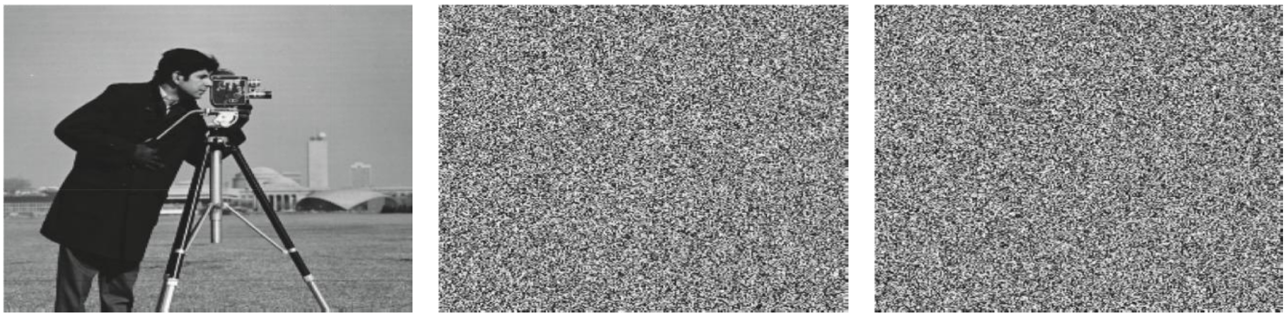

Figure 15 Key sensitivity of the encrypted process

Figure 15 shows the encrypted image of the proposed approach when using special keys.

Figure 15 (a) shows the main image of the cameraman. Figures 15 (b) and 15 (c) show encrypted images using various decoded keys, and there is no pattern or shadow in the corresponding decoded image using off-key keys.

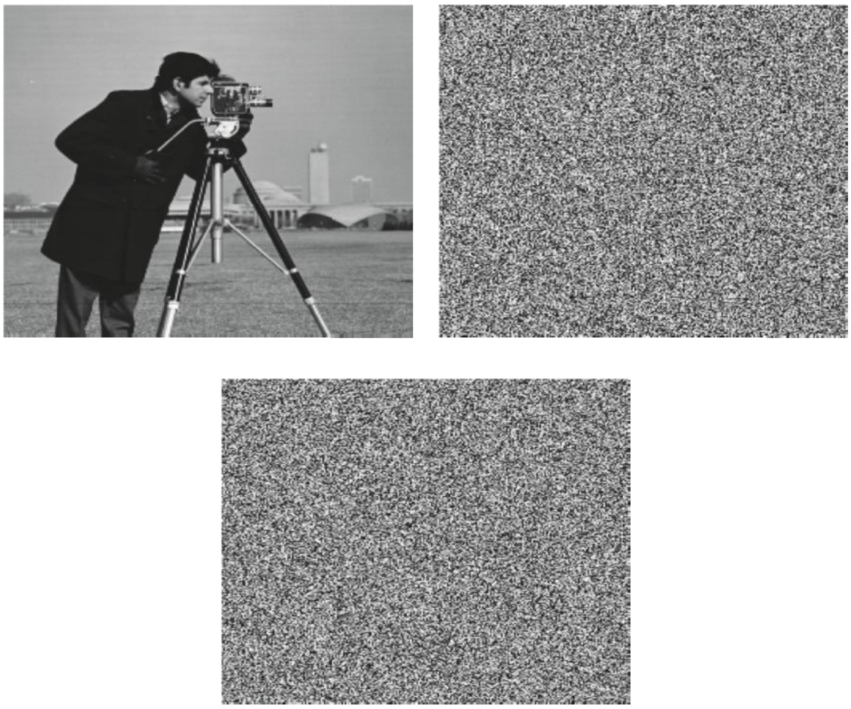

Figure 16 Key Sensitivity Decoding Process

Figure 16 shows the decoded image, here Figure 16 (a) shows the decoded image using the same encryption keys. Figures 16 (b) and 16 (c) show illegal decryption images when using the error keys. (The results show that not all encrypted images are known.) This means that the original image cannot be recovered without using the right key. A slight change in the key will result in an error in the decryption results.

3-4 - Test results

After reviewing the results in MATLAB software, the security performance of the proposed algorithm is better than the results mentioned. In order to test the algorithm's capacity to withstand attack, noise attack may be a common video attack strategy, often during transfer preparation. Encrypted image happens. Two pa parameters, namely NPCR and UACI, were used to analyze the attack. (The algorithm must be very sensitive to the plain image, which means that there is a large difference in the cryptographic image due to the small change in the plain image).

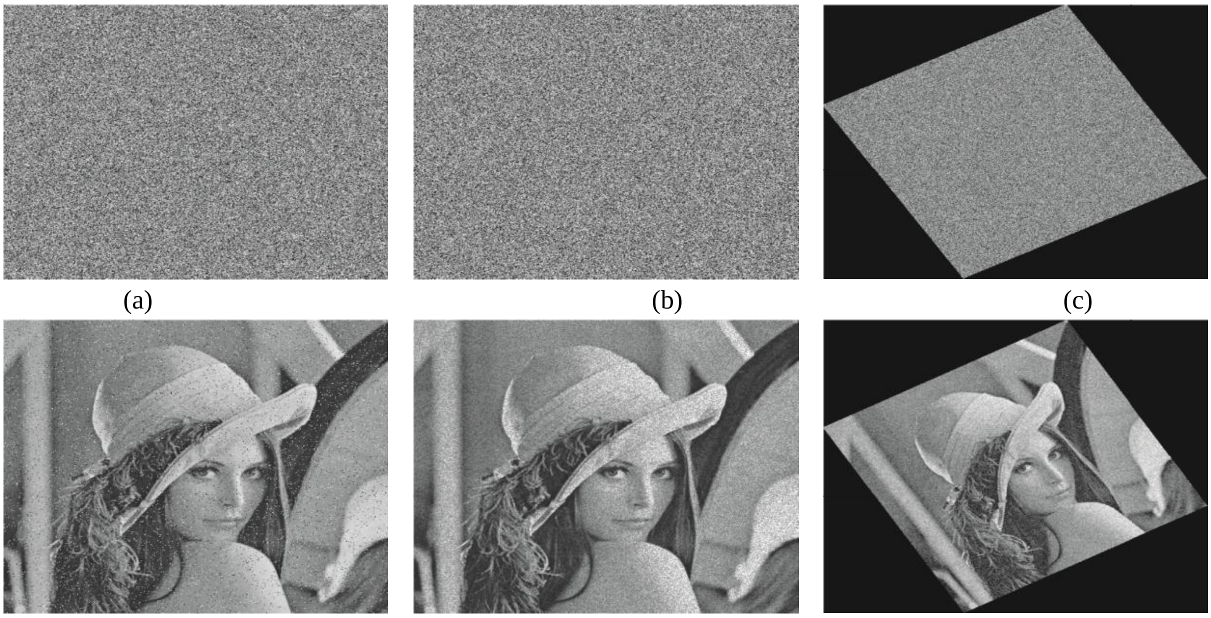
(a) (b) (c)
(d) (e) (f)

Figure 17 Shows the attack and its effects on the image

The proposed design can withstand various attacks (sound attack and rotation attack). This may be a common form of cryptographic analysis, and a secure encryption scheme should have a high capacity to withstand these attacks.

For an image encoding scheme, up to the number of pixels of the modified speed and the intensity of the interconnected variable can measure the capacity to withstand differential attack. (Results can be seen in Tables 3 and 4).

Image name	Proposed method	Wu et al. [11]	Ben Slimane et al. [13]	Wang et al. [35]	Luo and Ge [36]	Amina and Mohamed [37]	Alawida et al. [38]
Lena	99.6641	99.6002	99.6271	99.59	99.6137	99.6452	99.620
Cameraman	99.6523	99.6082	NA	99.59	99.6131	NA	NA
Baboon	99.6438	99.5903	99.6145	99.56	99.6111	99.6154	99.601
Peppers	99.6287	99.6112	NA	99.61	99.6137	99.6315	99.617

Table 3: Comparison of the proposed model with other proposed models with NPCR

Image name	Proposed method	Wu et al. [11]	Ben Slimane et al. [13]	Wang et al. [35]	Luo and Ge [36]	Amina and Mohamed [37]	Alawida et al. [38]
Lena	33.6124	33.5079	33.5589	33.48	33.4594	33.6152	33.505
Cameraman	33.6425	33.5574	NA	33.53	33.4615	NA	NA
Baboon	33.6430	33.5281	33.4277	33.58	33.4629	33.4354	33.424
Peppers	33.6012	33.5265	NA	33.41	33.3948	33.5073	33.391

Table 4: Comparison of the proposed model with other proposed models with UACI

As can be seen, the NPCR is over 99 U while the UACI is over 33. (These results prove that the sensitivity of the proposed calculation to changing the miniature made to plain image, decoded images will be completely different, even if there is only one bit change between two simple images in our test, quadratic image results and average UACI value And the NPCR separately are 33.6248 99 and 99.6472 ٻ, respectively. Using a test sample of the design is important.

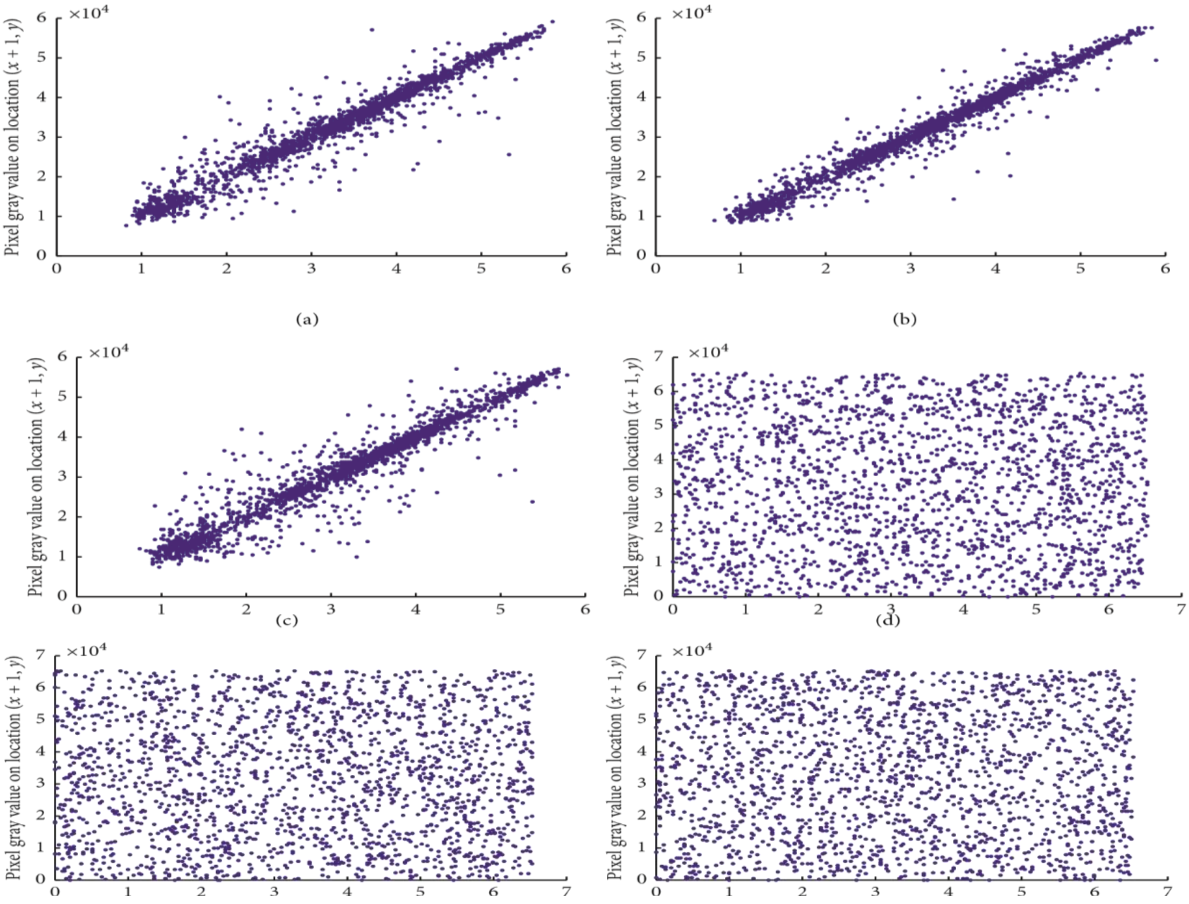

Figure 18 Adjacent pixel correlation test for Lena

Guaranteed image: (These tests include the DIEHARD andNIST measurable test suite (SP800). The DIEHARD test is significant in that it is the most significant and troublesome test suite in all respects. In the range of achievements is 0.01 <Pisteem <0.99. NIST is a measurable set that includes many experiments (these experiments are generally randomly generated from the encrypted image to pseudo-random number generators. Tables 6 and 7 NIST consequences And shows DIEHARD; the results show that the encrypted images have passed all the evaluations, which shows that they are behaving completely randomly.Conclusions A set of new turbulent maps based on wavelet and dual performance in an effort to improve the quality and implementation of encryption is presented. In this way, the projected pipeline was able to prevent many cryptographic methods of analysis and cryptographic attacks. (472 and 33.6248, separately). (Dynamic analysis and sample entropy algorithms showed that the proposed map with high sensitivity and high complexity is quite versatile. (We, chaotic image encryption can be considered a suitable tool for applications such as wireless communication). Several research centers that can be followed after this review. (The selection of key categories can be random.) Encrypt attached to the same image.) For a multimedia security algorithm can be used based on a chaotic computing system.

Resources

[1]E. Yavuz, R. Yazıcı, M. C. Kasapbas¸ı, and E. Yamaç, "A chaosbased image encryption algorithm with simple logical functions," Computers & Electrical Engineering, vol. 54, pp. 471–483, 2016.
[2] Y. Zhang, "(e unified image encryption algorithm based on chaos and cubic S-box," Information Sciences, vol. 450, pp. 361–377, 2018.
[3] X. L. Aqeel-ur-Rehman, X. Liao, and M. A. R. Hahsmi, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," Optik- International Journal for Light and Electron Optics, vol. 153, pp. 117–134, 2018.

[4] C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," Optik- International Journal for Light and Electron Optics, vol. 124, no. 18, pp. 3329–3334, 2013.
[5] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaosbased fast image encryption algorithm," Applied Soft Computing,vol. 11, no. 1, pp. 514–522, 2011.
[6] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," Optics & Laser Technology, vol. 101, pp. 30–41, 2018.
[7] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D H´enon-Sine map and DNA approach," Signal Processing,vol. 153, pp. 11–23, 2018.
[8] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "An efficient nested chaotic image encryption algorithm based on DNA sequence," International Journal of Modern Physics C,vol. 29, no. 7, Article ID 1850058, 2018.
[9] N. Ben Slimane, K. Bouallegue, and M. Machhout, "Designing a multi-scroll chaotic system by operating logistic map with fractal process," Nonlinear Dynamics, vol. 88, no. 3, pp. 1655–1675, 2017.
[10] S. Su, Y. Su, and M. Xu, "Comparisons of firefly algorithm with chaotic maps," Computer Modelling & New Technologies, vol. 18, no. 12, pp. 326–332, 2014.
[11] S. Al, S. Najim, and E. Hato, "A speech encryption based on chaotic maps," International Journal of Computer Applications, vol. 93, no. 4, pp. 19–28, 2014.
[12] A. S. Menon and K. S. Sarila, "Image encryption based on chaotic algorithms: an overview," International Journal of Science, Engineering and TechnologyResearch, vol. 2, no. 6,pp. 1328–1332, 2013.
[13] C. Li, G. Luo, and C. Li, "An image encryption scheme based on the three-dimensional chaotic logistic map," IJ Network Security, vol. 21, no. 1, pp. 22–29, 2019.
[14] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," Optics and Lasers in Engineering,vol. 96, pp. 39–49, 2017.
[15] L. Wang and H. Cheng, "Pseudo-random number generatorbased on logistic chaotic system," Entropy, vol.21, no. 10, p. 960, 2019.
[16] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and
M. R. Mosavi, "A novel image encryption based on hash
function with only two-round diffusion process," Multimedia Systems, vol. 20, no. 1, pp. 45–64, 2014.
[17] X. Wang, S. Wang, N. Wei, and Y. Zhang, "A novel chaotic image encryption scheme based on hash function and cyclic shift," IETE Technical Review, vol. 36, no. 1, pp. 39–48, 2019.
[18] H. Luo and B. Ge, "Image encryption based on Henon chaotic system with nonlinear term," Multimedia Tools and Applications, vol. 78, no. 24, pp. 34323–34352, 2019.
[19] M. Ausloos and M. Dirickx, Eds., *e Logistic Map and the
Route to Chaos: From the Beginnings to Modern Applications, Springer, Berlin, Germany, 2006.
[20] M. Ahmad, M. N. Doja, and M. M. S. Beg, "A new chaotic map based secure and efficient pseudo-random bit sequence
generation," International Symposium on Security in Computing and Communication, Springer, Berlin, Germany, 2018.
[21] B. Toufik and N. Mokhtar, "(e wavelet transform for image
processing applications," Advances in Wavelet *eory and *eir Applications in Engineering, Physics and Technology, vol. 17, pp. 395–422, 2012.
[22] E. A. Albahrani and T. Karam Alshekly, "New chaotic substation and permutation method for image encryption," International Journal of Applied Information Systems, vol. 12, no. 4, pp. 34–39, 2017.
[23] G. Hanchinamani and L. Kulakarni, "Image encryption based
on 2-D zaslavskii chaotic map and pseudo Hadmard transform," International Journal of Hybrid Information Technology, vol. 7, no. 4, pp. 185–200, 2014.
[24]. Yang, K. W. Wong, X. Liao, W. Zhang, P. (2010) A fast image encryption and authentication scheme based on chaotic map, Elsevier, Commun Nonlinear Sci Number Simulat, pp. 3507-3517.
[25]. Ye R. (2011) A novel chaos-based image encryption scheme with an efficient permutation–diffusion mechanism.Opt Commun, (284), pp. 5290–8.
[26].Yong, W., Kwok-Wo, W., Xiaofeng, L., and Guanrong C. (2011) A new chaos-based fast image encryption algorithm. Elsevier, Applied Soft Computing, (11), pp. 514-522.
[27].Yoon, J.W., and Kim, H. (2010) An image encryption scheme with a pseudorandom permutation based on chaotic maps. Elsevier, Commun Nonlinear Sci Numer Simulat , (15), pp. 3998–4006
[28] Zhang Q,Guo L,Wei X.)2010) Image encryption using DNA addition combining with chaotic maps.Math Comput Model, (52), pp.2028–35.
[29] Zhang G, Liu Q. (2011) A novel image encryption method based on total shuffling scheme. Opt Commun, (284), pp.2775–80.

[30]. MaoY, Chen G, Lian S. (2004) A novel fast image encryptions cheme based on3D chaotic bakermaps.Int J Bifurcat Chaos, (14), pp. 3613–24.

[31]. Mohamed, M.A., Zaki, F.W., and El-mohandes, A.M. (2013) Enhanced Diffusion Encryption for Transmission over Mobile WiMax Networks. International Journal of computer Science, 10(2), pp.1694-0784.

[32]. Nanrun, Z.,Yixian, W., Lihua, G., Xiubo, C., and YixianYang. (2012) Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Elsevier, Optics & Laser Technology, (44) pp. 2270-2281.

[33]. Narendra, K. P., Vinod, P., and Krishan, K.Sud. (2013) Diffusion–substitution based gray image encryption scheme. Elsevier, Digital Signal Processing, (23), pp. 894–901.

[34]. Osama, M., Abu, Z., Nawal, A., Nigm, E. M., and Osama, S. F. (2013) A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security. International Journal of Computer Applications, 61(5), pp.0975- 8887.

[35]. Pareek N,Patidar V,Sud K. (2003) Discrete chaotic cryptography using external key.Phys Lett A, (309), pp. 75–82.

[36]. Payal, M., and Rajender, S. C. (2013) A New And Secure Chaos Based Multimedia Encryption Scheme. International Journal of Engineering Research and Applications, 3(4), pp.2063-2068.

[37]. Raja Kumar, R., Sampath, Dr.A., and Indumathi, Dr.P. (2011) Enhancement and Analysis of Chaotic Image Encryption Algorithms. Computer Science & Information Technology, (02), pp.143–153.

[38]. Ramesh Kumar, y., Singh, Dr. B. K., Sinha, S.K., and Pandey, K. K. (2013) A New Approach of Colour Image Encryption Based on Henon like Chaotic Map. Journal of Information Engineering and Applications, 3(6).

[39]. Sharma, M., and Kowar, M. K. (2010) Image Encryption Techniques UsingChaotic Schemes: a Review. International Journal of EngineeringScience and Technology, 2(6), pp. 2359-2363.

[40]. Shen J, Jin X, Zhou C.A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. Lect Notes Comput Sci, (3768), pp. 270–80.

[41]. Shubo Liu, Jing Sun, Zhengquan Xu. (2009) An improved image encryption algorithm based on chaotic system, J. Comput, (4), pp. 1091–1100.

[42]. SunF,Liu S,Li Z,Lu Z. (2008) A novel image encryption scheme based on spatial chaos map.Chaos Solitons Fractals, (38), pp. 631–40.

[43]. Xing-Yuan, C. Feng, W. Tian. (2010) A new compound mode of confusion and diffusion for block encryption of image.