Multimedia Tools and Applications (2022) 81:20483–20508
https://doi.org/10.1007/s11042-022-12071-3

Image cryptosystem based on plain image correlation rate and selective chaotic maps

Ahmad Pourjabbar Kari[1] · Ahmad Habibizad Navin[2] · Amir Massoud Bidgoli[1] · Mirkamal Mirnia[3]

Received: 15 November 2020 / Revised: 24 August 2021 / Accepted: 4 January 2022 /
Published online: 11 March 2022

Abstract

In this paper, a new image encryption algorithm is introduced for encrypting grayscale digital images of any size. To improve the encryption evaluation parameters, we suggested that the value of the plain image correlation coefficient be effective in the cryptographic process, so plain images with different properties and correlation coefficient rates are encrypted in different ways. According to the average absolute value of correlation coefficient of plain image, Logistic or Tent maps is selected to generate chaotic sequences to expand plain image matrix. As the first step of the diffusion phase, the plain image matrix is developed with larger size by proper selected chaotic sequences, and simultaneously a chaotic matrix with the same size is generated by chaotic Sine map sequences. In confusion phase, the modified Lorenz map changes pixel locations of new developed matrix by means of certain equations. Then bitwise XOR is applied between developed matrix include plain image and Sine map chaotic matrix, as second step of diffusion phase. Finally, encrypted image is generated after applying exchange operations on the content of pixels, as third step of diffusion phase. Experimental results and comparisons with some of the existing methods, show that the proposed image cryptosystem is able to resist common cryptanalytic attacks and can be used as a secure method for encrypting digital images.

Keywords Image encryption · Chaotic maps · Differential attack · Correlation · Diffusion · Confusion

1 Introduction

Image encryption is an unavoidable part of the image processing and information security. Image encryption is used to ensure the security of image data [33]. Common cryptographic

✉ Amir Massoud Bidgoli
am_bidgoli@iau–tnb.ac.ir

Extended author information available on the last page of the article

methods such as advanced encryption standard (AES) and data encryption standard (DES) are used in image encryption, but these traditional image encryption algorithms are less efficient in image encryption, especially when a large number of images are to be encrypted and image data must be sent in real time [69, 70]. Furthermore, since the image data volume is large and the data correlation among adjacent pixels and data redundancy is high [41], researchers have been encouraged to develop new methods for image encryption [4, 16] based on well-known theories and purposes.

As another secure communication mechanism, steganography has proven to be one of the practical ways of securing data [3]. In steganography, the main message is hidden in a cover media. In other words, steganography is a technical art on how to hide messages into other media as the steganographic cover or container [13, 30].

Existing steganography methods can successfully embed secret information into the carrier media (steganographic cover) without introducing distortion into the appearance of the carrier media [30]. Steganographic cover contains secret images in which can only be extracted by the recipient [13]. Digital pictures, videos, text documents and other digital files can be used as a container or carrier as long as they contain some redundant data [22].

The difference between cryptography and steganography is that in cryptography the goal is to hide the contents of the message, but in steganography the goal is to hide any sign of the message. In cases where the exchange of encrypted information is difficult, the existence of connection must be hidden. Cryptography and steganography can be used separately or simultaneously for data security. For higher security, one message can be encrypted first and then hidden inside another message, which will increase processing overhead and memory space.

The requirements for steganographic systems are summarized in 5 groups as follows [22]:

1- Message requirements (Maximum message size, Message modification, Multiple message);
2- Container requirements (Type of container, Supported file formats, Container selection type);
3- Stegocontainer requirements (Imperceptibility, Fidelity, Stegocontainer size, Embedding efficiency, False positive rate, Extraction method);
4- Algorithm requirements (Capacity, Speed, Embedding domain);
5- Security requirements (Resistance against steganalysis, Robustness, Resistance against attacks, Type of secret keys).

In Ref. [12] a hybrid grasshopper optimizer has been proposed to reduce the size of the feature set in the steganalysis process. This paper results from the stagnancy of local minima and slow convergence rate by the grasshopper algorithm in optimization problems. Therefore, the grasshopper optimization performance is improved with chaotic maps to make it chaotic grasshopper optimization. Then, the chaotic grasshopper optimization is combined with adaptive particle swarm optimization to make it chaotic particle-swarm grasshopper optimization algorithm. Next, authors use the proposed optimizer with entropy to find the best feature subset of the original subtractive pixel adjacency model and spatial rich model feature set.

Although, the encryption systems consist of a pair of linear (permutation) and nonlinear (diffusion) conversion, have effective security levels; high computation cost limits the performance of whole encryption system [55].

Introducing chaos in the field of cryptography helps to design better and more efficient encryption methods [58]. Chaos-based cryptosystems are suitable for image encryption owing to the inherent properties of chaotic systems. Unpredictability, ergodicity, and initial value sensitivity are significant properties of chaotic systems [1, 73]. Common chaotic maps such as Lorenz, Sine, Tent, and Logistic maps have simple structures and are easy to be implemented [32], but they have the defects of limited chaotic ranges [7] and vulnerability [5, 54].

To withstand possible attacks, a high-security nonlinear optical cryptography with phase-truncated Fourier transform (PTFT) was used in [48], in which phase and amplitude truncation operations are used to overcome the weakness of linearity in double random phase encoding (DRPE).

Ref. [68] proposed a new chaotic and hash-based image encryption algorithm (SHA-256), which uses confusion and diffusion methods to encrypt images. In [8] authors introduced a new image encryption algorithm based on pixel position displacement and random key flow. In [56], an image encryption algorithm combining DNA sequencing with chaotic mapping is proposed. Also, the proposed scheme employed an image processing algorithm based on discrete wavelet transform and multiple chaos. In [75] Arnold deformation is used to encrypt highly secure images.

The nonlinear multi-image encryption has attracted a lot of attention due to its higher encryption efficiency. Based on the phase truncation in the Fourier range, a multi-image encoding method has been proposed to eliminate linearity and obtain a white noise-like image in [72]. Based on the classical confusion and diffusion structure, an image encryption algorithm based on two-dimensional logic-sine pair mapping is proposed in [57]. In [76], a bit-level image encryption algorithm is constructed using a piecewise linear chaotic map.

To suppress the the dynamic degradation of digital chaos, a new model was introduced in [62]. In this model, the difference between two chaotic maps of the same type but with different initial values are employed, and the state feedback function is used to improve the performance of the digital chaotic map. Furthermore, a new key selection method, in what part of information of the image would be selected by using a chaotic map to generate a special value. In Ref. [17], a cryptosystem was presented based on a novel chaotic map and compressive sensing. In this paper, the sparse coefficient matrix is acquired by discrete wavelet transform of the original image, and the SHA-512 hash value of the original image are regarded as the initial values of two novel one dimensional chaotic maps.

An image cryptography method based on lifting wavelet transform, Latin square and wide range Beta chaotic map, was introduced in [43]. The proposed method is composed of different procedures. After the creation of the Latin square S-box, the wide range Beta map is used to generate the random key. The obtained key is applied in the encryption stage. In Ref. [44] three main contributions were proposed. An image encryption framework, a new chaotic map and a pseudorandom bit generator, and as the third contribution, a novel image encryption system was introduced based on the proposed map and the proposed pseudorandom bit generator. The proposed new chaotic map is designed which will be known as the 'RCM map' and its chaotic property is studied based on Devaney's theory. A scrambling algorithm was also proposed to further enhance the security of the overall system.

Ref [6], introduces a new algorithm for colour image encryption. The scheme is based on a new 3-dimensional discrete time chaos system which performs the diffusion and confusion processes. The novelty of the proposed work is the new 3-D map defined by five nonlinear terms and three control parameters to ensure better chaotic properties. Moreover, the proposed new map is used to perform 3-stage encryption algorithm which achieves better performance while preserving the traditional confusion-diffusion structure. An image encryption scheme based on a 2-dimensional chaotic Henon map has been proposed in Ref. [42]. The confusion phase is implemented by several iterations using chaotic map approach. In the subsequent stage, Edge Maps generated by edge detection filters and binary bit plane decomposition is applied to perform further confusion using a bit-xor operation to get a cipher image.

In [2], an image encryption scheme based on chaotic maps and algebraic structure has been introduced. The proposed cryptosystem is based on Lorenz chaotic system and primitive irreducible polynomial substitution box. For first step, 16 different S-boxes based on projective general linear group and 16 primitive irreducible polynomials of Galois field of order 256 has been proposed. For second step, S-boxes are utilized with combination of chaotic map in image encryption scheme. In Ref. [39], an image encryption scheme is proposed based on two dimension improved Logistic coupling map. In order to confirm the application of the proposed scheme to image encryptions, authors proposed a new image encryption algorithm which is simple in structure and combines bit level permutation, and pixel level diffusion and confirm the performance through experiments.

An image segmentation encryption scheme based on hyper chaotic system has been proposed in [15]. The authors decompose the scrambled sequence into three sequences of different lengths. Then, the initial values of the chaotic system are updated by these three sequences and using the updated initial value iterates the chaotic system and generates the key sequence. Authors in Ref. [35] proposed a new Sine powered chaotic maps generator. The proposed system uses one-dimensional chaotic maps as seed maps to produce new chaotic maps and also, a novel block-based image encryption scheme is proposed. The proposed scheme pre-processes the original image using pixels addition and blocks generation. Using the generated chaotic sequences, the columns and pixels between the generated blocks are shuffled and execute bit-level values manipulation.

An image cryptosystem based on two-dimensional hyperchaotic map, with two positive Lyapunov exponents and a phase distribution region has been proposed in [46]. Furthermore, authors introduced a novel randomized hyperchaotic image encryption algorithm based on the proposed two-dimensional hyperchaotic map. The proposed scheme is implemented in such a way that first adds randomization to the plain image, and uses the SHA-256 value of the randomized image with the key for extracting required parameters.

In Ref. [34], a heterogeneous chaotic generator has been proposed. The implementation of this scheme is done by using neural network. The heterogeneity of the generator is obtained by alternating two different chaotic maps; Logistic and piece-wise Linear chaotic map, in the neural network layers. In the paper, authors also proposed a new encryption algorithm using chaotic generator as input for its cryptographic operations including: pixel position permutation, DNA based substitution and DNA based bit permutation which was also introduced in this paper to enhance the statistical properties of the encrypted images. A novel image encryption algorithm based on the Once Forward Long Short Term Memory Structure (OF-LSTMS) and the Two-Dimensional Coupled Map Lattice (2DCML) fractional order chaotic system has been proposed in [23]. In this scheme, the original image is divided into several image blocks. According to the chaotic sequences generated by the 2DCML fractional-order chaotic system, the parameters of the input gate, output gate and memory unit of the OF-LSTMS are initialized, and the pixel positions are changed at the same time of changing the pixel values, achieving the synchronization of permutation and diffusion operations, which greatly improves the efficiency of image encryption and reduces the time consumption.

The most important limitations of reviewed papers are the processing time for encryption and decryption in high-dimensional chaotic maps, the complexity of implementation, and the vulnerability of one-dimensional chaotic maps to variety of attacks.

High Dimension (HD) maps have more complex structures and better chaotic behaviors. This makes their chaotic orbits more unpredictable [20]. However, HD chaotic maps have the drawback of high computation cost and implementation difficulty [27]. Therefore, it is necessary to design a new chaotic system to overcome mentioned problems. Since chaotic encryption algorithms have the advantages of high speed and low cost, the development and analysis of these image encryption schemes has become popular in the field of classical computing [38]. To ensure the security of image data in the process of sending and storing, some encryption algorithms based on chaos theory are proposed and applied to image encryption [64]. In this paper, an image encryption scheme based on a new hybrid chaotic system is presented. This system consists of modified Lorenz map to confusion process, and diffusion process is implemented by nonlinear combinations of three Logistic map, Tent map, and Sine map, XOR, and exchange operations. The performance analysis is performed on key spaces, key sensitivity, the capability of resisting statistical attacks, noise and cropping attacks, differential attacks and quality evaluation metrics of decrypted image. The goal of proposed method is to improve cryptography evaluating parameters.

The structure of this paper is organized as follows: Section 2 presents the basic definitions of four common chaotic maps. The proposed method is discussed in section 3. Section 4 exhibits the effectiveness of the proposed technique, security analysis, and extensive performance evaluation of the proposed cipher algorithm are analyzed in detail within this section. Section 5 presents speed analysis and finally conclusion is given in section 6.

2 Preliminaries

This section summarizes the four maps used in this article namely Lorenz map, Sine map, Tent map and Logistic map.

2.1 Lorenz chaotic map

Equation (1) shows the mapping equation of the Lorenz two-dimensional discrete chaotic system. When the parameters i∊ [0.9, 1] and j∊ [0.9, 1], the mapping is in the chaotic range [51]. For image encryption, when we use a Lorenz two-dimensional discrete chaotic system, parameters can be selected in this parameter range, which is difficult to break [51].

$$\begin{cases} a_{n+1} = \left[(1+ij)a_n - ja_nb_n\right] \\ b_{n+1} = \left[(1-j)a_n + j(a_n)^2\right] \end{cases} \tag{1}$$

In this paper we use modified Lorenz map to confuse the pixel coordinates according to Eq. (2), and this equation is employed to convert plain image coordinates to new coordinates.

$$\begin{cases} x_{n+1} = \mathrm{floor}\left(mod\left(\left|\left[(1+ij)x_n - jx_ny_n\right] \times 10^{14}\right|, Q\right)\right) \\ y_{n+1} = \mathrm{floor}\left(mod\left(\left|\left[(1-j)x_n + j(x_n)^2\right] \times 10^{14}\right|, Q\right)\right) \end{cases} \tag{2}$$

(x_n, y_n) is the location of pixels in the Q × Q plain image matrix, so that (x_n, y_n), $(x_{n+1}, y_{n+1}) \in \{0,1,2,\ldots, Q\text{-}1\}$, and (x_{n+1}, y_{n+1}) is the transformed position after applying Lorenz map. Also, mod Q and floor operations are used to bring x, y in unit Q × Q matrix. This chaotic map is employed to confuse the pixel locations, which i, j are two secret keys.

2.2 Sine map

Sine map is one of the most widely used one-dimensional chaotic map and has a simple dynamic structure, but it can create complex and chaotic sequences with amplitudes [0, 1]. The definition of Sine map is:

$$x_{n+1} = S(x) = u_s \sin(\pi x_n) \tag{3}$$

Where u_s is a parameter and according to the bifurcation diagram [28, 40], $u_s \in [0.87, 1]$ and s_0 is the initial value for x_n, $(x_0 = s_0)$.

2.3 Tent map

Tent mapping is a one-dimensional chaotic map that is used in many applications [28, 40]. The diagram of this map is similar to a tent, which is why it is known by this name. The definition of a tent map is as follows:

$$x_{n+1} = T(x) = \{\, 2u_t x_n \qquad\qquad x_n \tag{4}$$

Where u_t is a parameter and according to the bifurcation diagram $u_t \in [0.5, 1]$ and t_0 is the initial value for x_n, $(x_0 = t_0)$ [17, 62].

2.4 Logistic map

Logistic map is obtained using sine map, so it has some similar properties [28, 40]. In order for this mapping to be in the range [0, 1], the Logistic map is mathematically defined as follows

$$x_{n+1} = L(x) = 4u_l\, x_n(1 - x_n) \tag{5}$$

Where u_l is a parameter and according to the bifurcation diagram $u_l \in [0.9, 1]$ and l_0 is initial value for x_n, $(x_0 = l_0)$ [17, 62].

3 The proposed scheme

The proposed scheme is shown in Fig. 1. This method is designed for gray scale images of different sizes, but can also be used for color images and consists of two fundamental steps: chaotic confusion and diffusion. The confusion step is implemented to change the coordinates of the pixels, using the modified Lorentz mapping according to Eq. (2).

Diffusion phase is ruled by means of plain image matrix expansion, XOR, and exchange operations, aiming to elevate the sensitivity to plain image and accelerate the diffusion mechanism of the whole cipher algorithm. The original image, which is the input image of the proposed cryptographic system, is called the plain image. In

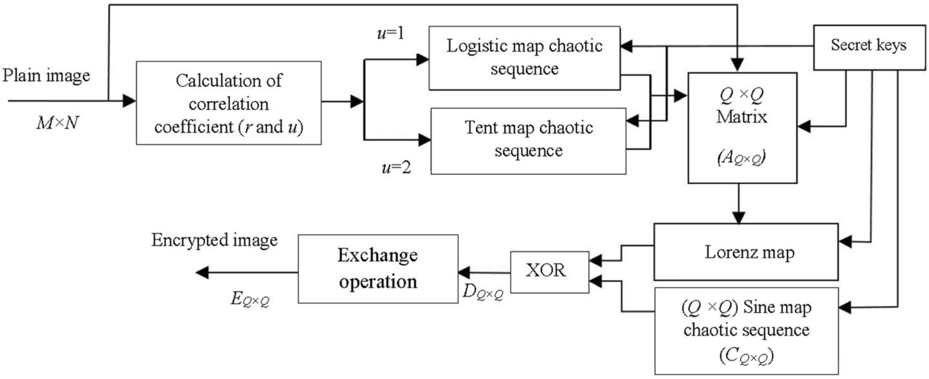

Plain image
$M \times N$
Calculation of correlation coefficient (r and u)
u=1
u=2
Logistic map chaotic sequence
Tent map chaotic sequence
Secret keys
$Q \times Q$ Matrix ($A_{Q\times Q}$)
Lorenz map
($Q \times Q$) Sine map chaotic sequence ($C_{Q\times Q}$)
XOR
$D_{Q\times Q}$
Exchange operation
Encrypted image
$E_{Q\times Q}$

Fig. 1 Proposed scheme based on plain image correlation rate and using chaotic maps, XOR and exchange operations

this paper, 2000 pixels of the plain image are randomly selected and the average absolute value of the correlation coefficients of horizontally, vertically and diagonally adjacent pixels with randomly selected pixels, is calculated using relationships (9) to (11), and thus the correlation rate of the plain image is calculated (r). We know that the absolute value of r is an integer number between 0 and 1, if r was between 0 and 0.8, then a Logistic chaotic mapping is selected to develop the input image matrix with larger size. If r was between 0.8 and 1, then Tent's chaotic mapping is chosen to develop the original image matrix. The detailed description of the encryption algorithm is given in 6 steps as follows:

Step 1: Let I be M × N gray scale plain image. In this step, the average absolute value of correlation coefficient (r) for 2000 randomly horizontaly, verticaly, and diagonal

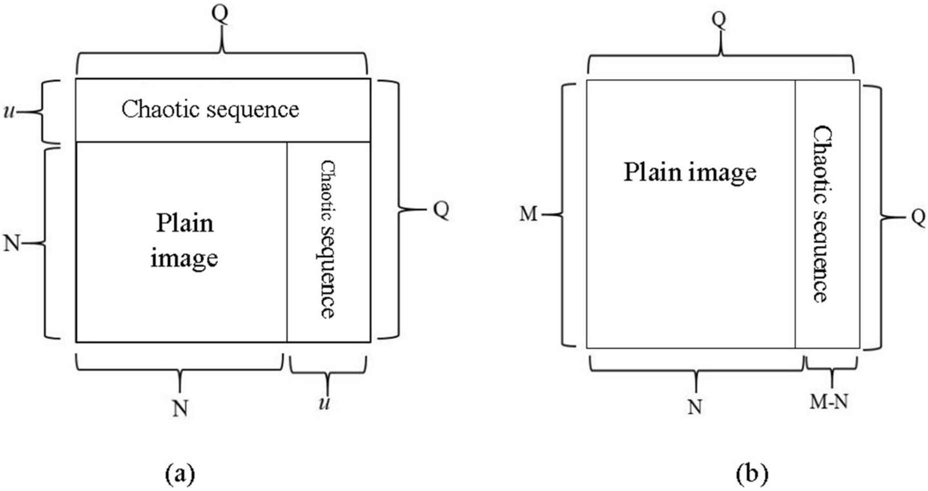


Fig. 2 **a** Extended matrix $A_{Q\times Q}$ for N × N plain image. **b** Extended matrix $A_{Q\times Q}$ for M × N plain image (M > N)

adjacent pairs of pixels in plain image is calculated. If $0 \le r \le 0.8$ let $u = 1$ and if $0.8 < r \le 1$ let $u = 2$.

Step 2: Suppose the maximum value of M, N is equal to Q, we expand original image I from M × N to square Q × Q matrix (Fig. 2b). If the original image is N × N according to the Fig. 2a, N + u number of rows and columns is added for expanding original matrix from N × N to Q × Q, (u obtained from step 1).

Step 3: According to the features of bifurcation diagram of Logistic and Tent map, if u = 1 Logistic map is selected, and if u = 2, Tent map is selected to generate chaotic sequences. The generated sequences by using Eqs. (4) and (5), are replaced by the empty components of the expanded matrix after being placed in the [0, 255] range from left to right, and up to down (Matrix $A_{Q \times Q}$ is generated). Chaotic sequences generated in the [0, 1] interval (Y_i), are converted to integer sequences (P_i) in the [0, 255] interval by using Eq. (6).

$$P_i = [(10^v \times Y_i)] \, mod \; 256. \tag{6}$$

The developed matrix $A_{Q \times Q}$ contains the original image data and the data from the chaotic sequence, v is the number of floating point of generated chaotic sequences and Y_i are chaotic components with a range of [0, 1], and i ϵ {1, 2, 3, ..., number of added components ([(u×Q) + u × (Q-u)] or [Q×(M-N)]}.

Step 4: Modified Lorenz map (Eq. (2)) is applied k times on the coordinates of $A_{Q \times Q}$ for scrambling the location of pixels by means of confusion. This generates matrix $B_{Q \times Q}$, and k is one of the other secret keys.

Step 5: Bitwise XOR applies on scrambled $B_{Q \times Q}$ matrix and binary Q × Q matrix ($C_{Q \times Q}$) generated by sine map with a range of [0, 255] by using Eqs. (3), (6). This step generates $D_{Q \times Q,}$ and is calculated according to Eq. (7).

$$D_{Q\times Q} = B_{Q\times Q} \oplus C_{Q\times Q}. \tag{7}$$

Step 6: Matrix $D_{Q \times Q}$ is changed to matrix $E_{Q \times Q}$ by exchanging the values of u and u + 1 positions in every 8 bit binary numbers, the value of u is obtained from step 1. $E_{Q \times Q}$ is the final encrypted image.

The decryption procedure is the same as that of the encryption one described above, unless it must be performed in the reverse order.

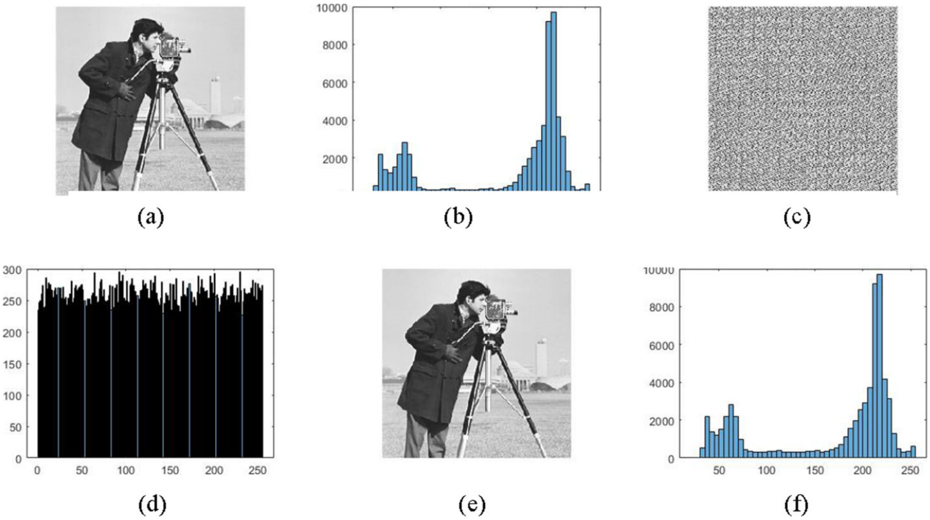
To clearance the workflow of data in Fig. 1, we summarize the proposed scheme as follows:

In Fig. 1, random pixels of the plain image with size M × N are selected and the absolute value of the average correlation coefficient between these random pixels and their adjacent pixels, is calculated. In this paper, we place the original M × N matrix completely inside a larger square matrix with larger dimensions Q × Q ($A_{Q \times Q}$) and fill the empty components with Logistic or Tent chaotic sequences as shown in Fig. 2. We define new variable u, and according to the step 1, if u = 1, in this case the sequences generated by Logistic map are used to fill the empty components of the developed matrix $A_{Q \times Q}$. And if u = 2, in this case the sequences generated by Tent's chaotic map are filled in empty components od developed matrix after normalization by Eq. (6) and using the initial values. These initial values are secret keys. After forming the matrix $A_{Q \times Q}$, the coordinates of this matrix are disturbed by modified Lorenz's two-dimensional map. Now we form another new matrix with dimensions Q × Q called $C_{Q \times Q}$ and its components are filled with sequences generated by chaotic Sine map according to the initial values which are the secret keys. Then the bitwise XOR operation is applied between the disrupted $A_{Q \times Q}$ and $C_{Q \times Q}$ and the $D_{Q \times Q}$ matrix is obtained. Finally, in all pixels of the $D_{Q \times Q}$ matrix, the contents of the bits u and u + 1 are swapped together to obtain the final matrix $E_{Q \times Q}$, which contains the encrypted image.

4 Security analysis

4.1 Histogram analysis

Histogram is an important tool for analyzing the original image and the encrypted image. The image histogram shows how the grayscale level of image pixels are distributed [9, 18]. One of the main goals of the image encryption method is to turn the non-uniform histogram of the original image into a uniform histogram after encryption. The horizontal axis of the image histogram represents the gray levels from 0 to 255 and the vertical axis represents the number of pixels with a specified gray level. Here are some standard gray scale images in Figs. 3, 4 and 5 as examples. The results show that the histogram of the encrypted images just in one round, has a uniform distribution compared to the original images which are unevenly distributed. These results show that the proposed algorithm has a good performance in breaking the correlation of image pixels and achieving a satisfactory image encoding performance. As shown in the histograms of the original image and the encrypted image, it is clear that the proposed method can withstand statistical attack [21, 22].



(a) (b) (c)

(d) (e) (f)

Fig. 3 **a** is "256×256 Camera man" plain image, **b** is plain image histogram, **c** is encrypted image in 1 round, **d** is encrypted image uniform histogram. **e** is decrypted image, **f** is decryped image histogram

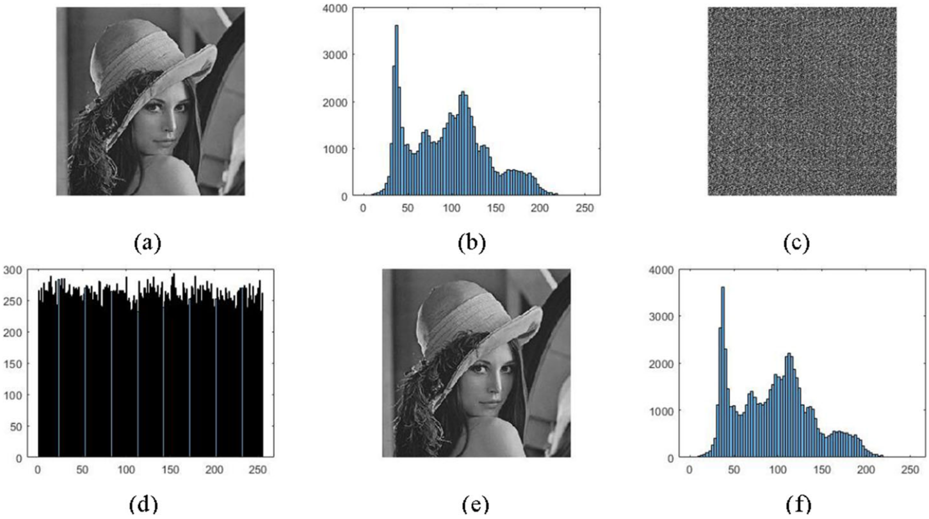


Fig. 4 **a** is standard “256 × 256 Lena” plain image, **b** is plain image histogram, **c** is encrypted image in 1 round, **d** is encrypted image uniform histogram. **e** is decrypted image, **f** is decryped image histogram

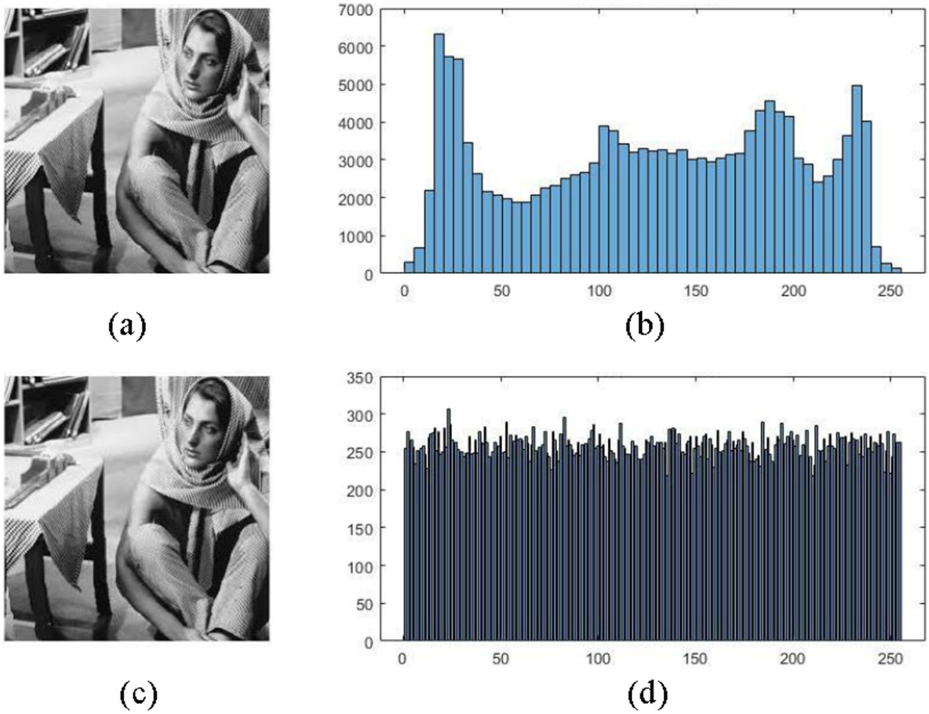


Fig. 5 **a** is “256 × 256 Female” plain image, **b** is plain image histogram, **c** is decrypted image, and **d** is encrypted image histogram with uniform histogram

4.2 Information entropy analysis

The histogram uniformity and the randomness of the gray scale of the encrypted image can be measured by the entropy of the information [2, 21, 47, 74]. When the probability function follows a uniform probability distribution, the information entropy for an image with a 256 level gray is 8. The XOR operation can randomly change the pixel values and then evenly distribute the pixel distribution of the highly encoded image. The data of a two-dimensional gray scale image M × N can be placed in an M × N matrix, so that the value of each component is an 8-bit number that is a decimal number between 0 and 255. The number 0 indicates black and the number 255 indicates white, and the rest of the gray levels are between 1 and 254. In general, each pixel in an image is adjacent to the other 8 pixels horizontally, vertically and diagonally. For example, if there is a large, completely white area in an image, then the adjacent pixels in this area all have a value of 255, and therefore there is a high correlation between adjacent pixels in this area and according to relationships (9) to (11), the correlation coefficient in this area is 1. In this case, if an attacker accesses the value of a pixel, he can easily guess the values of adjacent pixels. In contrast, if in an image the adjacent pixels have completely different levels of gray, then the average correlation coefficient in this image is low and its value is close to 0. Therefore, one of the important goals in designing an effective cryptographic system is to have a low and close to zero correlation between adjacent pixels in the encrypted image to reduce the likelihood of an attacker guessing the values of adjacent pixels. In this case, the entropy of the information will be close to 8. The data entropy of encrypted images by proposed scheme is over 7.9 which is very close to 8. The result shows that the probability of information leakage is very low and the pixel of the image encryption is highly random. Therefore, the proposed image encryption scheme can withstand statistical attack [24, 50, 52].

The plain image information entropy I is defined as Eq. (8). The ideal information entropy for an 8-bit gray scale image is 8, in which the image does not show any useful information to attackers. Equation (8) shows that the uniform distribution of the algorithm leads to a better entropy. Figures 3, 4, and 5 show that the histograms of standard encrypted images are uniform, so the proposed method has a good information entropy index.

$$H(s) = \sum_{i=0}^{255} P(s_i) \mathrm{Log}_2 \frac{1}{P(s_i)} \tag{8}$$

Where s_i denotes the gray-level and $P(s_i)$ is the probability of the occurrence s_i. Shannon entropy of different statndard images encrypted by the proposed scheme, is listed in Table 1 and it shows that the Shannon entropy of the proposed encrypted images is all close to 8. Table 2 shows comparison of the entropy value between proposed scheme and some other

Table 1 Information entropy test results for standard images

Test images	Image size	Cipher images entropy
Camera man	256×256	7.998962
Lena	256×256	7.998725
Baboon	256×256	7.999611
Female	256×256	7.999527
Airplane	256×256	7.998667

Table 2 Comparison of the entropy value between proposed scheme and other methods

Encryption scheme	Image	Size	Cipher images entropy
Proposed	Lena	512×512	7.999893
Ref. [40]	Lena	512×512	7.999918
Ref. [4]	Lena	512×512	7.999338
Ref. [8]	Lena	512×512	7.999319
Ref. [64]	Lena	512×512	7.999324
Ref. [67]	Lena	512×512	7.999301
Ref. [53]	Lena	512×512	7.999286
Proposed	Lena	256×256	7.998725
Ref. [40]	Lena	256×256	7.999834
Ref. [4]	Lena	256×256	7.996951
Ref. [34]	Lena	256×256	7.997600
Ref. [49]	Lena	256×256	7.997000
Ref. [29]	Lena	256×256	7.997200
Ref. [63]	Lena	256×256	7.997300
Proposed	Baboon	512×512	7.999921
Ref. [40]	Baboon	512×512	7.999896
Ref. [4]	Baboon	512×512	7.999350
Ref. [67]	Baboon	512×512	7.999263
Ref. [66]	Baboon	512×512	7.999300
Ref. [10]	Baboon	512×512	7.999345
Ref. [37]	Baboon	512×512	7.999300

methods. The information entropy results show that, proposed scheme is an effective method to change the values and positions of an input image, so the pixel values and positions in an image will get well-disturbed after encryption, therefore the diffusion and confusion of encrypted image is significantly enhanced.

4.3 Correlation analysis

One feature of plain image data is that the correlation coefficients of adjacent pixels are often high, while an efficient encryption algorithm must significantly reduce the correlation coefficients of the neighboring pixels in encrypted image. We select 2000 adjacent horizontal (vertical and diagonal) pixels in plain image and experimental cryptography to analyze their correlation coefficients according to Eq. (12). An efficient encryption algorithm should reduce the correlation between adjacent pixels in the encrypted image as much as possible to zero [11, 29, 65]. Table 3 shows the results obtained from the correlation coefficient values of the standard test images, and Table 4 illustrates the comparison of propsed scheme correlations with some recent image encryption schemes. From the results of the obtained correlation coefficient, it is obvious that high relationships between adjacent pixels of plain images (correlation coefficient close to 1) are effectively reduced in encrypted images (correlation coefficient close to 0).

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

Table 3 Correlation test results for 256 × 256 standard images

Test Image	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9711	0.9853	0.9853	0.0042	0.0051	0.0055
Camera man	0.9163	0.9732	0.9042	0.0073	0.0042	−0.008
Baboon	0.6111	0.6589	0.5211	0.0088	−0.0069	0.0036
Female	0.9812	0.9370	0.9420	0.0081	0.0086	0.0069

$$D(x) = \frac{1}{N}\sum_{i=1}^{i=N}\left[x_i - E(x_i)\right]^2 \tag{10}$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x_i)\right]\left[y_i - E(y_i)\right] \tag{11}$$

$$R_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}}, \tag{12}$$

where x and y are two adjacent pixels in the horizontal, vertical, and diagonal directions.

4.4 Resistance to differential attacks

The number of pixels changing rate (NPCR) and the unified average change intensity (UACI) are two common indicators for evaluating the sensitivity of image encryption algorithms. A powerful attacker may be able to find a significant relationship between the original image and the encrypted image [19, 71]. In order to ensure the effectiveness and resistance to differential attacks, the standard Lena image is encrypted by the proposed method (T_1). The six modified images are then obtained by changing only the least significant bit (LSB) of randomly matched pixels in the selected location (x, y), namely Lena (x, y). These modified images are shown

Table 4 Comparison of correlations with some recent image encryption schemes

Reference	Image	Correlation		
		Horizontal	Vertical	Diagonal
Proposed	Lena	0.0042	0.0051	0.0055
Ref. [40]	Lena	0.0054	0.0049	0.0042
Ref. [34]	Lena	0.00046	0.0011	0.0031
Ref. [44]	Lena	0.0090	0.0084	−0.0093
Proposed	Baboon	0.0088	−0.0069	0.0036
Ref. [23]	Baboon	0.001272	0.003794	0.000041
Ref. [37]	Baboon	−0.0038	0.0007	0.0003
Ref. [42]	Baboon	0.0092	0.0089	0.0075

Table 5 NPCR and UACI tests results for cipher Lena standard image

Test Image	NPCR (%)	UACI (%)
Lena (15,35)	99.5981	33.4651
Lena (60,65)	99.6625	33.4765
Lena (110,80)	99.8524	33.4436
Lena (145,120)	99.6628	33.4519
Lena (180,160)	99.7819	33.4910
Lena (230, 220)	99.6235	33.4715

with Lena (15,35), Lena (60,65), Lena (110,80), Lena (145,120), Lena (180,160), Lena (230, 220). Equations (13), (14) and (15) are used to calculate the NPCR and UACI values. These values are shown in Table 5.

$$\mathrm{NPCR} = \frac{\sum_{i,j} C(i,j)}{W \times H} \times 100\% \tag{13}$$

$$\begin{cases} C(i,j) = 0 \ \text{ if } \ T_1(i,j) = T_2(i,j) \\ C(i,j) = 1 \ \text{ if } \ T_1(i,j) \neq T_2(i,j) \end{cases} \tag{14}$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{\mid T_1(i,j) - T_2(i,j) \mid}{255}\right] \times 100\% \tag{15}$$

Where T_1 represents the encoded image obtained from the original plain image, while T_2 represents the plain image encryption after 1 bit modification on plain image, and W × H is the image size. NPCR and UACI are calculated after a random change of one pixel in the original image. NPCR and UACI for different plain images are listed in the Tables 5 and 6. According to the Eq. (13), the ideal value for NPCR is 100%, which indicates that 100% of the pixels are different in the encypted image. For gray images, the average value for UACI is 33.33%, because if we consider on average all the components of T_1 equal to 10,101,010, which is equivalent to 170 decimal, for maximum difference we expect all components of T_2 to be equal to 01010101, which is equivalent to 85 decimal. Therefore, |170–85| is equal to 85, and according to Eq. (15), if we sum W × H components with the value of 85, we will finally reach (85/255) × 100 = 33.33%.

It is clear that any pixel that changes in the original image, will result in significantly different encrypted images. The results show the effective performance of the proposed encryption algorithm to differential attacks.

Table 6 NPCR and UACI tests results for cipher standard 256 × 256 grayscale images

Test Image	NPCR (%)	UACI (%)
Lena	99.7015	33.3962
Baboon	99.6125	33.4784
Female	99.6478	33.4025
Airplane	99.6568	33.5324

Table 7 Comparison of the NPCR and UACI values between our proposed approach and the other methods

Method	Image	Size	NPCR (%)	UACI (%)
Proposed	Lena	512×512	99.6501	33.6012
Ref. [40]	Lena	512×512	99.6461	33.6252
Ref. [64]	Lena	512×512	99.6200	33.4100
Ref. [67]	Lena	512×512	99.6052	33.4111
Ref. [53]	Lena	512×512	99.6215	33.4654
Proposed	Lena	256×256	99.7015	33.4962
Ref. [40]	Lena	256×256	99.7298	33.4810
Ref. [4]	Lena	256×256	99.5941	33.5052
Ref. [34]	Lena	256×256	99.6155	28.5670
Ref. [29]	Lena	256×256	99.6100	33.4600
Ref. [63]	Lena	256×256	99.6100	33.5300
Proposed	Baboon	512×512	99.6255	33.4015
Ref. [40]	Baboon	512×512	99.6234	33.4156
Ref. [23]	Baboon	512×512	99.5979	33.5494
Ref. [67]	Baboon	512×512	99.3504	33.4520
Ref. [45]	Baboon	512×512	99.6048	33.4554
Ref. [10]	Baboon	512×512	99.6101	33.4354
Proposed	Baboon	256×256	99.6125	33.4784
Ref. [40]	Baboon	256×256	99.6215	33.4572
Ref. [4]	Baboon	256×256	99.6017	33.6287
Ref. [38]	Baboon	256×256	99.6124	33.4891

Table 7 shows the obtained results of experimental values for different standard cipher images attained under the application of certain existing methods including ours. These results indicates that our method is highly sensitive to plain image bit modification, therefore render differential attacks void.

4.5 Security key space

In order to resist against a variety of attacks, an effective encryption scheme must have a key space larger than 2^{100} [40]. In our scheme, the secret keys are as follows: the parameters M, N, k, r (M, N are the image size parameters for M × N image, k is Lorenz map iteration, and r is the correlation coefficient of plain image), and the initial values (u_s, s_0), (u_t, t_0), (u_l, l_0) of Sine map, Tent map, and Logistic map respectively. Also, i and j the two parameters related to Lorenz map are other secret keys. If the length of every key is set to 14 decimals, the key space is 10^{168} which is more greater

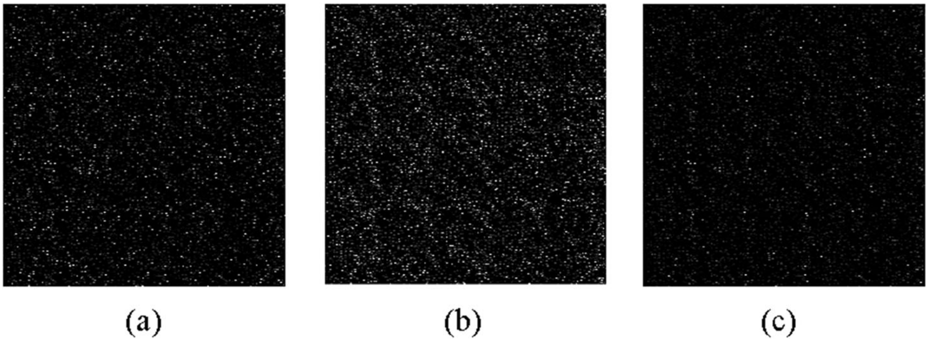


Fig. 6 Decryption of standard "Lena" with incorrect keys: **a** $K_{e1} + 10^{-14}$, **b** $K_{e2} + 10^{-14}$, **c** $K_{e3} + 10^{-14}$

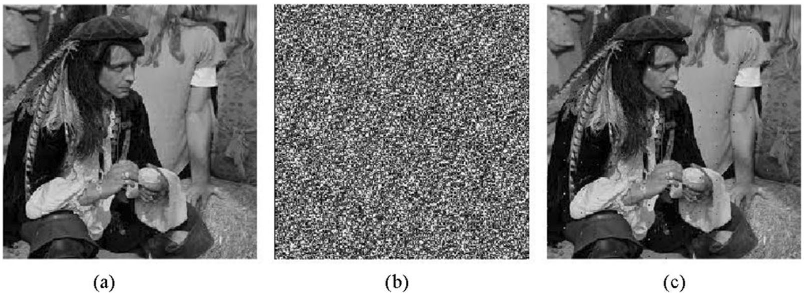


Fig. 7 Standard plain image (**a**), encrypted image in 1 round damaged by 5% Salt and Pepper noise (**b**), decryption of damaged cipher image (c)

than 2^{100}. Thus, the proposed algorithm can provide a high level security in key space. As a disadvantage, the number of secret keys is high and increases the key management overhead.

4.6 Key sensitivity analysis

In a good encryption scheme, if an attacker did not have the original secret key, but had a key very close to the secret key, he should not be able to decrypt the original image. The resistance of the cryptographic design to minor changes in the secret key is indicated by the sensitivity of the secret key. Key sensitivity analysis is usually used to test the ability of resisting inimical deciphering, which detects the variation of encryption results when a slight change (like 10^{-14}) caused in the encryption keys [59, 61]. In the other words, the cryptosystem should produce completely different encrypted image when slightly different secret keys are used to encrypt the image. Also, the cryptosystem should be unable to decrypt cipher text even for the slight

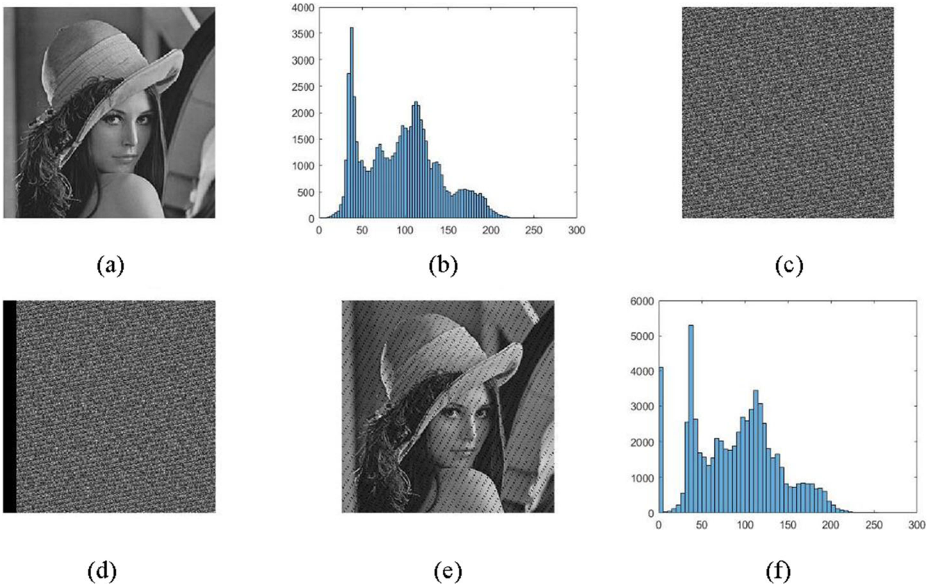
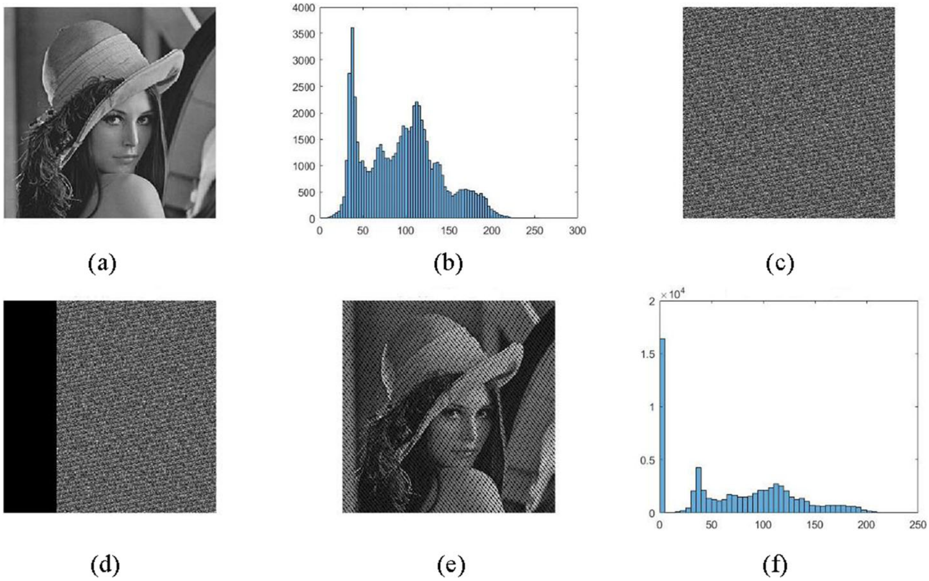


Fig. 8 **a** Standard test image, **b** histogram of plain image, **c** encrypted image with 1 iteration, **d** $\frac{1}{16}$ damaged of encrypted image, **e** decryption of damaged image, **f** histogram of damaged image decryption



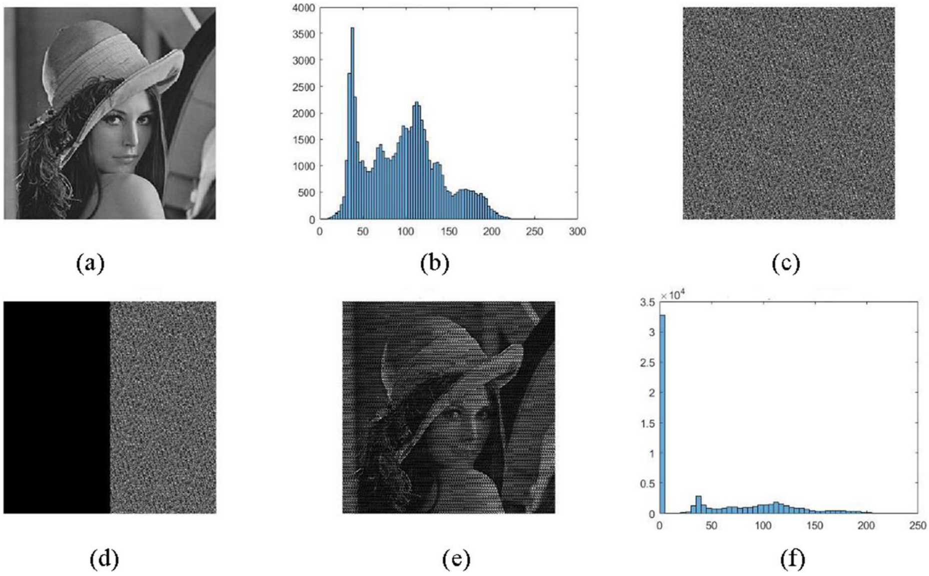
(a) (b) (c)

(d) (e) (f)

Fig. 9 **a** Lena standard test image, **b** histogram of test image, **c** encrypted image with 1 iteration, **d** 25% damaged of encrypted image, **e** decryption of damaged image, **f** histogram of damaged image decryption

difference in the encryption and decryption keys. In addition, the difference between failure reconstruction images is distinct.

The key sensitivity simulation results are shown in Fig. 6. K_{e1}, K_{e2}, K_{e3} are three encryption keys. The corresponding decrypted results with incorrect decryption keys $K_{e1} + 10^{-14}$, $K_{e2} + 10^{-14}$, and $K_{e3} + 10^{-14}$ for standard "Lena" image, are shown in Fig. 6.These results show that



(a) (b) (c)

(d) (e) (f)

Fig. 10 **a** Standard test image, **b** histogram of plain image, **c** encrypted image with 1 iteration, **d** 50% damaged of encrypted image, **e** decryption of damaged image, **f** histogram of damaged image decryption

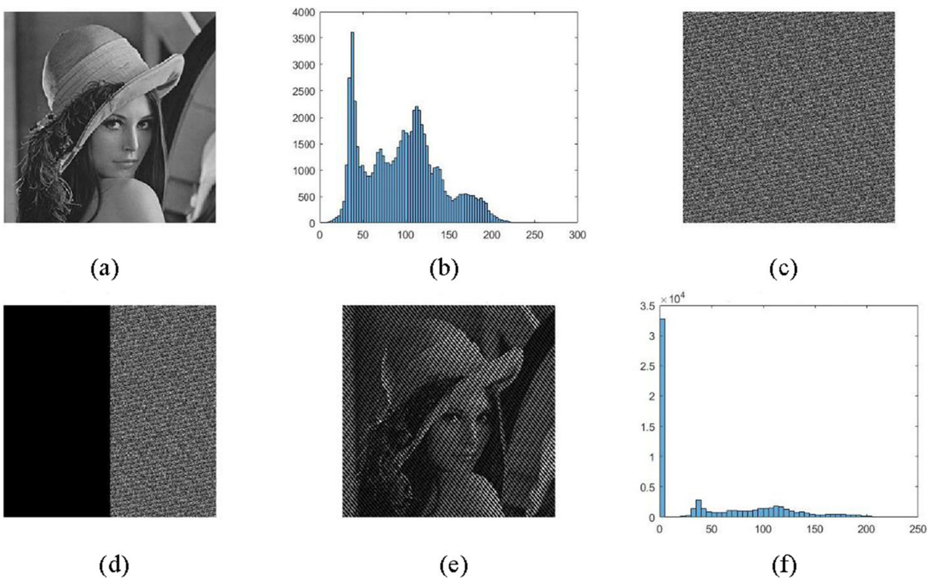


Fig. 11 **a** Standard test image, **b** histogram of plain image, **c** encrypted image with 10 iteration, **d** 50% damaged of encrypted image, **e** decryption of damaged image, **f** histogram of damaged image decryption

a tiny difference makes great changes between decrypted images. Therefore, we can conclude that proposed method has a high sensitivity to security keys in both encryption and decryption process. Additionally, only a tiny difference of 10^{-14} can result in significant changes in encryption/decryption results, which means the proposed algorithm has a large key space to defend the inimical deciphering.

4.7 Cropping and noise attack

A good cryptosystem should be robust enough to resist different types of noise and cropping attacks. The analysis of cropping attack aims to check the robustness of the encryption algorithm against cutting of cipher image [25, 26]. To check the robustness of the proposed scheme, we perform some experiments on the noise attack and the data loss.

To evaluate the resistance of proposed scheme against noise attack, encryption image of standard grayscale image is attacked by a 5% ‘salt & pepper’ noise (Fig. 7). Then the corresponding decrypted image is given in Fig. 7c. To evaluate the resistance of the proposed method against cropping and data loss attacks, grayscale plain images in Figs. 8, 9, 10 and 11,

Table 8 Encryption evaluating parameters for $\frac{1}{16}$ cropping attack and different iterations

Cropping value	Iteration	PSNR	SDR	SSIM	SNR
$\frac{1}{16}$	1	24.0106	15.6896	0.5849	16.3416
	20	24.1373	15.5957	0.5863	16.4727
	30	23.7981	15.6140	0.5887	16.1335
	40	24.1370	15.6008	0.5880	16.4724
	50	24.2885	15.5479	0.7251	16.6239

Table 9 Encryption evaluating parameters for 25% cropping attack and different iterations

Cropping value	Iteration	PSNR	SDR	SSIM	SNR
$\frac{1}{4}$	1	18.2136	9.6689	0.2779	10.5490
	20	18.0507	9.6987	0.2726	10.3861
	30	17.9894	9.6757	0.2675	10.3248
	40	17.8779	9.5486	0.2649	10.2133
	50	18.0965	9.8712	0.2731	10.4319

encrypt by proposed algorithm, then encrypted image is attacked by a data cut of different sizes. The results show that decipher images of cropped cipher images are still recognized visually, therefore proposed scheme is robust against cropping and noise attacks.

4.8 The structural similarity (SSIM) index

The structural similarity (SSIM) index is a method for measuring the similarity between two images. In this research, we use SSIM index between plain image and decrypted image after cropping attack. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close [13]. These dependencies carry important information about the structure of the objects in the visual scene. The resultant SSIM index is a decimal value between −1 and 1, and value 1 is only reachable in the case of two identical sets of data. SSIM is defined as Eq. (16).

$$\mathrm{SSIM}(x,y)=\frac{\left(2\mu_x\mu_y+C_1\right)\left(2\sigma_{xy}+C_2\right)}{\left(\mu_x^2+\mu_y^2+C_1\right)\left(\sigma_x^2+\sigma_y^2+C_2\right)} \tag{16}$$

μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, $\sigma_{xy}$is the covariance of x and y, $C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$, L the dynamic range of the pixel values, $k_1 = 0.01$ and $k_2 = 0.03$.

4.9 Peak signal to noise ratio (PSNR)

Peak signal to noise ratio is a measure of the impact of noise on original data. Higher value of PSNR is good, because it shows that the cropping attack has low effect on the decrypted image [13]. In this article we use PSNR between original plain image and decrypted image after cropping attack to evaluate the efficiency of proposed method against cropping attack. PSNR is calculated by Eq. (17).

Table 10 Evaluating parameters for different iterations and 50% cropping attack

Cropping value	Iteration	PSNR	SDR	SSIM	SNR
$\frac{1}{2}$	1	15.1202	6.6872	0.1455	7.4556
	20	15.1702	6.6666	0.1501	7.5056
	30	15.1848	6.5908	0.1498	7.5202
	40	15.2729	6.6583	0.1521	7.6083
	50	15.0750	6.7451	0.1450	7.4104

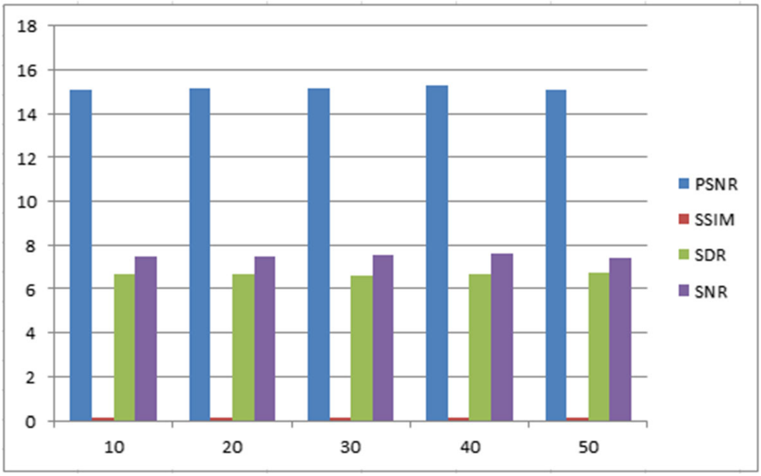


Fig. 12 PSNR, SSIM, SDR, and SNR evaluating parameters for $\frac{1}{2}$ cropping attack

$$\mathrm{PSNR} = 10\log 10\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right)^2 \ (\mathrm{db}) \tag{17}$$

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[\mathrm{I}(x,y) - \mathrm{I}'(x,y)\right]^2 \tag{18}$$

I is plain image and I′ is decrypted image after cropping attack, and MSE is Mean Square Error. If I and I′ were exactly the same, then the value of PSNR value will be infinite.

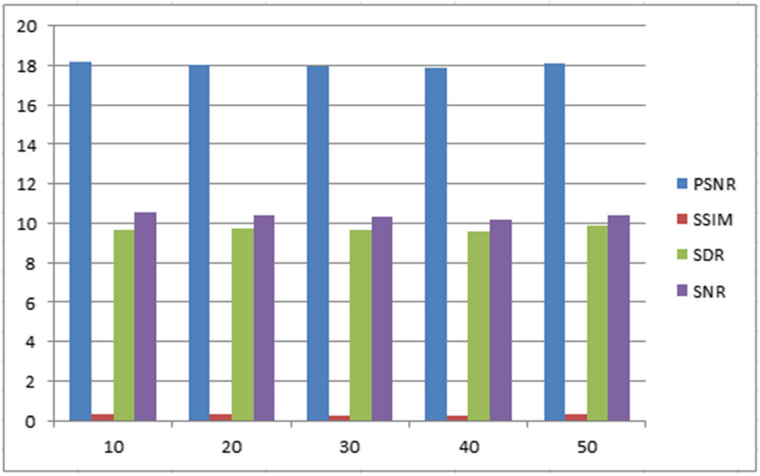


Fig. 13 PSNR, SSIM, SDR, and SNR evaluating parameters for $\frac{1}{4}$ cropping attack

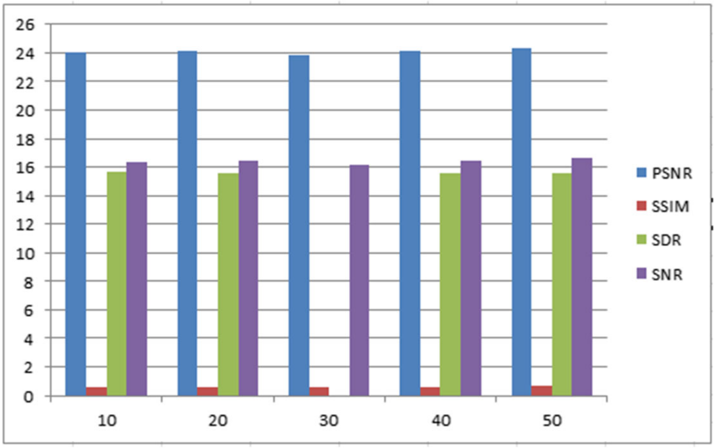


Fig. 14 PSNR, SSIM, SDR, and SNR evaluating parameters for $\frac{1}{16}$ cropping attack

4.10 Signal to distortion ratio (SDR)

To evaluate the quality of the decrypted image after cropping attack, we use an other parameter: the Signal to Distortion Ratio (SDR) between the plain image and the decrypted image after cropping attack. Higher value of SDR is good [13], because it indicates that the cropping attack has low effect on the decrypted image. The SDR in db (decibel) is calculated as Eq. (19).

$$SDR = 10\log_{10}\frac{\sum_{x,y} I(x,y)^2}{\sum_{x,y}\left(I(x,y) - I'(x,y)\right)^2} \quad (db) \tag{19}$$

I is plain image, and I′ is decrypted image after cropping attack. If I=I′, then SDR will be infinite.

Figure 8 and Table 8, demonstrate the result of histograms and evaluating parameters for different iterations and $\frac{1}{16}$ cropping attack.

Figure 9 and Table 9 show the results of histograms and evaluating parameters for different iterations and 25% cropping attack.

Figures 10, 11, and Table 10 illustrate the results of histograms and evaluating parameters for different iterations and 50% cropping attack.

Table 11 Comparision of average PSNR for different cropping attacks, in some references and proposed method

Reference	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{1}{2}$
55	20.7788	14.7340	11.4238
59	21.3236	14.8143	11.5291
60	20.2322	14.3316	11.3735
61	20.7460	14.7595	11.7448
62	20.1132	14.0453	11.0923
Proposed	**24.2885**	**18.2136**	15.2729

Table 12 The running time performance test (ms)

Image Size	Ref. [73]	Ref. [50]	Ref. [4]	Ref. [14]	Ref. [36]	Ref. [31]	Ref. [40]	Proposed
256×256	178	109	48	7641	189	569	92	81
512×512	663	390	139	34,768	758	2251	109	94
1024×1024	3142	1482	481	151,709	3096	8986	351	293

Implementation results show that, higher value of cropping attacks, causes lower evaluating parameters, and in some iterations, some parameters have better values. In Table 10 it is clear that the value of PSNR in 40 th iteration is better.

Figures 12, 13, and 14 show the PSNR, SSIM, SDR, and SNR evaluating parameters for different value of cropping attacks. The horizontal axis is the number of iterations.

Table 11 shows the comparision of PSNR for different cropping attacks in some references and maximum values of proposed method.

5 Speed analysis

In order to illustrate the speed performance, simulation results are given in this section. The experiment is conducted via MATLAB R2016b in a computer with 64 bit Windows 10 operating system, Intel(R) Core(TM) i7–6700 CPU @ 3.60GHz and 8GB RAM. All 26 images in the USC SIPI image database (http://sipi.usc.edu/database), are chosen as test images.

Execution-time is also an important factor with respect to security level. The duration of the proposed cipher algorithm in 1 round is evaluated and compared with some schemes under grayscale images of different sizes.

Table 12 shows the average encryption time of various methods. This comparision shows that speed of proposed scheme is proper considering that the proposed method is based on hybrid chaotic maps that possesses more complexity chaotic structures.

6 Conclusions

In this paper, a new image encryption method was introduced for different kind of grayscale image sizes. In the proposed method, images with different correlation coefficients are encrypted by different methods, and also the value of the correlation coefficient of the input plain image is involved in the whole encryption process. The confusion phase is governed by modified Lorenz map and the diffusion operation is controlled by extension of plain image matrix, XOR, and exchange operations. The uses of chaotic maps and XOR operation provide a dual layer of security. The key space of the encryption scheme is large enough to resist brute-force attacks, but as a disadvantage, the number of secret keys is high and increases the key management overhead. Also, the encrypted image has a uniform histogram, so the entropy value is close to the maximum value. Comparisons of the proposed method with some of the existing methods show that, this method has a proper processing time and has reasonable resistance to differential attacks, noise attacks and cropping attacks, so it can be used as a secure method for image encryption. Compared to our previous work in [40], and according to

Table 12, processing time has been reduced due to the use of the new structure, and the key space has also been increased from 10^{112} to 10^{168}.

References

1. Abbas NAM (2016) Image encryption based on independent component analysis and Arnold's cat map. Egypt Inform J 17:139–146
2. Al-Maadeed TA, Hussain I, Anees A et al (2021) A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. Multimed Tools Appl 80:24801–24822. https://doi.org/10.1007/s11042-021-10695-5
3. Al-Othmani AZ, Manaf AA, Zeki AM (2012) A survey on steganography techniques in real time audio signals and evaluation. IJCSI International Journal of Computer Science Issues 9(1, No 1):30–37, ISSN (Online): 1694–0814, License CC BY-NC-ND 4.0
4. Amina S, Mohamed FK (2017) An efficient and secure chaotic cipher algorithm for image content preservation. Signal Process. https://doi.org/10.1016/j.cnsns.2017.12.017
5. Bakhshandeh A, Eslami Z (2013) An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt Lasesr Eng 51(6):665–673
6. Bouteghrine B, Tanougast C, Sadoudi S (2021) Novel image encryption algorithm based on new 3-d chaos map. Multimed Tools Appl 80:25583–25605. https://doi.org/10.1007/s11042-021-10773-8
7. Chapaneri S, Chapaneri R, Sarode T (2014) Evaluation of chaotic map lattice systems for image encryption. Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on IEEE, pp 59–64
8. Chen J-x, Zhu Z-l, Fu C et al (2015) A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simul 20(3):846–860
9. Chen J-x, Zhu Z-l, Fu C et al (2015) An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. Commun Nonlinear Sci Numer Simul 23(1):294–310
10. Chen J-x, Zhu Z-l, Fu C et al (2015) An efficient image encryption scheme using gray code based permutation approach. Opt Lasers Eng 67:191–204
11. Cheng G, Wang C, Chen H (2019) A novel color image encryption algorithm based on hyper chaotic system and permutation-diffusion architecture. Int J Bifurcat Chaos 29(09):1950115
12. Chhikara S, Kumar R (2021) Image steganalysis with entropy hybridized with chaotic grasshopper optimizer. Multimed Tools Appl 80:31865–31885. https://doi.org/10.1007/s11042-021-11118-1
13. Darwis D, Junaidi A, Shofiana DA, Wamiliana (2021) A new digital image steganography based on center embedded pixel positioning. Cybern Inf Technol 21(2) Sofia. Print ISSN: 1311-9702; online ISSN: 1314-4081. https://doi.org/10.2478/cait-2021-0021
14. Del Rey AM, Sánchez GR, De La Villa Cuenca A (2015) A protocol to encrypt digital images using chaotic maps and memory cellular automata. Log J IGPL 23(3):485–494
15. Deng J, Zhou M, Wang C, Wang S, Xu C (2021) Image segmentation encryption algorithm with chaotic sequence generation participated by cipher and multi-feedback loops. Multimed Tools Appl 80:13821–13840. https://doi.org/10.1007/s11042-020-10429-z
16. Dhall S, Pal SK, Sharma K (2017) Cryptanalysis of image encryption based on a new 1D chaotic system. Signal Process. https://doi.org/10.1016/j.sigpro.2017.12.021
17. Dou Y, Li M (2021) An image encryption algorithm based on a novel 1D chaotic map and compressive sensing. Multimed Tools Appl 80:24437–24454
18. El Assad S, Farajallah M (2016) A new chaos-based image encryption system. Signal Process Image Commun 41:144–157
19. François M, Grosges T, Barchiesi D et al (2012, 1910) Image encryption algorithm based on a chaotic iterative process. Appl Math 3(12)
20. Fu C, Meng W-h, Zhan Y-f et al (2013) An efficient and secure medical image protection scheme based on chaotic maps. Comput Biol Med 43(8):1000–1010
21. Gong L, Qiu K, Deng C, Zhou N (2019) An image compression and encryption algorithm based on chaotic system and compressive sensing. Opt Laser Technol 115:257–267
22. Gribermans D, Jersovs A, Rusakovs P (2016) Development of requirements specification for steganographic systems. Appl Comput Syst 20:40–48. https://doi.org/10.1515/acss-2016-0014
23. He Y, Zhang Y-Q, He X, Wang X-Y (2021) A new image encryption algorithm based on the OF-LSTMS and chaotic sequences. Sci Rep 11:6398. https://doi.org/10.1038/s41598-021-85377-1

24. Hu T, Liu Y, Gong L-H, Guo S-F, Yuan H-M (2017) Chaotic image cryptosystem using DNA deletion and DNA insertion, 2017. Signal Process 134:234–243
25. Huang X, Ye G (2018) An image encryption algorithm based on hyper-chaos and DNA sequence. Multimed Tools Appl 72:57–70
26. Huang Z-J, Cheng S, Gong L-H, Zhou N-R (2019) Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Opt Lasers Eng 124:105821
27. Khanzadi H, Eshghi M, Borujeni SE (2014) Image encryption using random bit sequence based on chaotic maps. Arab J Sci Eng 39(2):1039–1047
28. Lan R, He J, Wang S, Tianlong G, Luo X (2018) Integrated chaotic systems for image encrypion. Signal Process. https://doi.org/10.1016/j.sigpro.2018.01.026
29. Li Y, Wang C, Chen H (2017) A hyper-chaos-based image encryption algorithm using pixellevel permutation and bit-level permutation. Opt Lasers Eng 90:238–246
30. Li Q, Wang X, Ma B, Wang X, Wang C, Xia Z, Shi Y (2021) Image steganography based on style transfer and quaternion exponent moments. Appl Soft Comput 110:107618. https://doi.org/10.1016/j.asoc.2021.107618
31. Liao X, Lai S, Zhou Q (2010) A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 90(9):2714–2722
32. Liu H, Wang X (2013) Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. J Syst Softw 86(3):826–834
33. Liu Y, Zhang LY, Wang J, Zhang Y, Wong K-w (2016) Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure. Nonlinear Dynamics 84(4):2241–2250
34. Maddodi G, Awad A, Awad D, Awad M, Lee B (2018) A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding. Multimed Tools Appl 77:24701–24725. https://doi.org/10.1007/s11042-018-5669-2
35. Mansouri A, Wang X (2021) A novel block-based image encryption scheme using a new sine powered chaotic map generator. Multimed Tools Appl 80:21955–21978. https://doi.org/10.1007/s11042-021-10757-8
36. Mohamed FK (2014) A parallel block-based encryption schema for digital images using reversible cellular automata. Eng Sci Technol Int J 17(2):85–94
37. Munir N, Khan M, Jamal SS, Hazzazi MM, Hussain I (2021) Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map. Mathematics and Computers in Simulation 190:826–836. https://doi.org/10.1016/j.matcom.2021.06.008
38. Norouzi B, Seyedzadeh SM, Mirzakuchaki S et al (2015) A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimed Tools Appl 74(3):781–811
39. Pak C, Kim J, Pang R, Song O, Kim H, Yun I, Kim J (2021) A new color image encryption using 2D improved logistic coupling map. Multimed Tools Appl 80:25367–25387
40. Pourjabbar Kari A, Habibizad Navin A, Bidgoli AM, Mirnia M (2020) A new image encryption scheme based on hybrid chaotic maps. Multimed Tools Appl 80:2753–2772. https://doi.org/10.1007/s11042-020-09648-1
41. Ran J, Liu YM, Wang CF, Wang ZW (2008) Complexity analysis of two-dimensional discrete Lorenz chaotic system. J Zunyi Normal Univ, vol. 20, no. 4, pp. 81_82, and 99
42. Rathore V, Pal AK (2021) An image encryption scheme in bit plane content using Henon map based generated edge map. Multimed Tools Appl 80:22275–22300. https://doi.org/10.1007/s11042-021-10719-0
43. Rim Z, Ridha E, Mourad Z (2021) An improved partial image encryption scheme based on lifting wavelet transform, wide range Beta chaotic map and Latin square. Multimed Tools Appl 80:15173–15191. https://doi.org/10.1007/s11042-020-10263-3
44. Roy M, Chakraborty S, Mali K (2021) A chaotic framework and its application in image encryption. Multimed Tools Appl 80:24069–24110. https://doi.org/10.1007/s11042-021-10839-7
45. Shahriyar T, Fathi MH, Sekhavat YA (2017, 2017) An image encryption scheme based on elliptic curve Pseudo random and advanced encryption system. Signal Process. https://doi.org/10.1016/j.sigpro.2017.06.010
46. Shakiba A (2021) A novel 2D cascade modulation couple hyperchaotic mapping for randomized image encryption. Multimed Tools Appl 80:17983–18006. https://doi.org/10.1007/s11042-021-10584-x
47. Shannon CE (2001) A mathematical theory of communication. ACM SIGMOBILE Mob Comput Commun Rev 5(1):3–55
48. Sha-ShaYu N-RZ, Gong L-H, Nieb Z (2020) Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Opt Lasers Eng 124:105816
49. Song C-Y, Qiao Y-L, Zhang X-Z (2013) An image encryption scheme based on new spatiotemporal chaos. Optik 124(18):3329–3334
50. Souyah A, Faraoun, Mohamed K (2016) An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dyn 86(1):639–653

51. Li T , Du B , Liang X (2020) Image encryption algorithm based on logistic and two-dimensional Lorenz, IEEE Access, Special Section on emerging approaches to cyber security, Digital Object Identifier https://doi.org/10.1109/ACCESS.2020.2966264
52. Wang X, Guo K (2014) A new image alternate encryption algorithm based on chaotic map. Nonlinear Dyn 76(4):1943–1950
53. Wang X, Xu D (2014) A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn 75(1–2):345–353
54. Wang X, Zhang H-l (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun 342:51–60
55. Wang H, Xiao D, Chen X, Huang H (2017) Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Process. https://doi.org/10.1016/j.sigpro.2017.11.005
56. Wang XY, Zhang YQ, Bao XM (2019) A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 73:53–61
57. Wu Y, Yang G, Jin H et al (2012) Image encryption using the two-dimensional logistic-Sine chaotic map. J Electron Imaging 21(1):013014-1–013014-15
58. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process. https://doi.org/10.1016/j.sigpro.2017.04.006
59. Wu J, Liao X, Yang B (2017) Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. Signal Process. https://doi.org/10.1016/j.sigpro.2017.06.014
60. Wu X, Zhu B, Hu Y, Ran Y (2017) A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps. IEEE Access. https://doi.org/10.1109/ACCESS.2017.2692043
61. Wu X, Kan H, Kurths J (2019) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl Soft Comput 37:24–39
62. Xiang H, Liu L (2021) A novel image encryption algorithm based on improved key selection and digital chaotic map. Multimed Tools Appl 80:22135–22162. https://doi.org/10.1007/s11042-021-10807-1
63. Xu L, Gou X, Li Z et al (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52
64. Yavuz E, Yazici R, Kasapbaşi MC et al (2015) A chaos-based image encryption algorithm with simple logical functions. Comput Electric Eng
65. Yu F , Li L , Tang Q , Cai S , Song Y, Xu Q (2019) A survey on true random number generators based on chaos, discrete dynamics in nature and society 2019, Article ID 2545123, 10 pages
66. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
67. Zhang X, Zhao Z (2014) Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dyn 75(1–2):319–330
68. Zhang W, Wong K-w, Yu H et al (2013) A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci Numer Simul 18(3):584–600
69. Zhang Y, Xiao D, Wen W, Nan H (2014) Cryptanalysis of image scrambling based on chaotic sequences and vigen'ere cipher. Nonlinear Dynamics 78(1):235–240
70. Zhang LY, Liu Y, Wang C, Zhou J, Zhang Y, Chen G (2018) Improved known-plaintext attack to permutation-only multimedia ciphers. Inf Sci 430:228–239
71. Zhang Q, Guo L, Wei X (2020) A novel image fusion encryption algorithm based on DNA sequence operation and hyper chaotic system. Optik-Int J Light Electron Opt 124:2593–3002
72. Zhi-Jing H, Cheng S, Li-Hua G, Nan-Run Z (2020) Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Opt Lasers Eng 124:105821
73. Zhou Y, Bao L, Chen CLP (2014) A new 1D chaotic system for image encryption. Signal Process 97:172–182
74. Zhou NR, Hua TX, Gong LH, Pei DJ, Liao QH (2015) Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf Process 14(4):1193–1213
75. Zhou N, Yan X, Liang H, Tao X, Li G (2018) Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system, Quantum Inf Process 17(12):article id. 338, 36 pp
76. Zhu Z-l, Zhang W, Wong K-w et al (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181(6):1171–1186

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Ahmad Pourjabbar Kari[1] **· Ahmad Habibizad Navin**[2] **· Amir Massoud Bidgoli**[1] **· Mirkamal Mirnia**[3]

Ahmad Pourjabbar Kari
a.pourjabar@gmail.com

Ahmad Habibizad Navin
a.habibizad@srbiau.ac.ir

Mirkamal Mirnia
mirnia-kam@tabrizu.ac.ir

[1] Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran

[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

[3] Department of Mathematics and Computer Sciences, University of Tabriz, Tabriz, Iran