Multimedia Tools and Applications (2021) 80:2753–2772
https://doi.org/10.1007/s11042-020-09648-1

A new image encryption scheme based on hybrid chaotic maps

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

Received: 22 December 2019 / Revised: 25 July 2020 / Accepted: 18 August 2020 /
Published online: 16 September 2020

Abstract

In this paper, a novel grayscale image cryptosystem based on hybrid chaotic maps is proposed. The scheme employs both confusion phase to scramble the location of pixels and diffusion phase for changing the content of pixels in consecutive manner. In this scheme, Arnold's cat map is introduced to perform confusion operation and the principle of diffusion is achieved by using the proper selection of combined Sine map, Logistic map, and Tent map. Furthermore, exclusive OR (XOR), exchange, and transform operations are used to enhance the efficiency of diffusion phase. Accordingly, the use of chaotic maps and XOR operation provides a dual layer of security. Depending on the average absolute value of horizontal, vertical, and diagonal correlation coefficient of plain image as well as bifurcation properties of chaotic maps, one of the mentioned chaotic maps is selected for diffusion phase. First, original gray scale image matrix is extended to square matrix by adding the sequences generated with proper chaotic maps to implement the first step of diffusion phase. Then the Arnold's cat map changes pixels location of new extended matrix by means of certain equation as confusion phase. The encrypted image is generated after applying XOR, exchange and transform operations on the content of pixels as second step of diffusion phase. Thus the system is able to build several more complicated chaotic structures. In addition the encryption and decryption processing time directly depend on the value of correlation coefficient of original image. Plain images with less correlation coefficient have less encryption and decryption processing time, and vice versa. Compared with several existing methods, the proposed scheme has more better properties, including wider chaotic ranges and more complex chaotic behavior. Experimental results show that the proposed system has proper encryption and decryption processing time, unified average changing intensity (UACI), number of pixel change rate (NPCR), and extensive security analysis for kind of images.

✉ Ahmad Pourjabbar Kari
a.pourjabar@gmail.com

Extended author information available on the last page of the article

Keywords Cryptography · Chaotic maps · Arnold's cat map · Tent map · Logistic map · Sine map

1 Introduction

With the rapid development of computer networks, information leakage events occur in the process of network transmission and storage in an endless stream. This makes most network users aware of the threat from privacy leakage [12, 26]. Secured storage and transmission of the digital image is one of the prime concerns in multimedia communication [49, 55]. Cryptography, steganography, and watermarking are three ways to protect digital data from unauthorized access and illegal usage [17, 21, 50]. Among these, cryptography plays a significant role in providing highly secured transmission over insecure channel. The cryptographic algorithms are classified into stream ciphers and block ciphers. Stream ciphers uses a secret key generator to encrypt the digital data bit by bit, while block ciphers encrypts blocks of bits instead. Most commonly used stream ciphers are linear feedback shift registers (LFSR) based on stream cipher and RC4. Block ciphers include the well-known advanced encryption standard (AES), data encryption standard (DES), triple DES (TDES) [16, 39], and etc. These conventional encryption schemes are not suitable for image encryption since image data requires strong real time property in communications [22]. Moreover, these ciphers require higher processing time, more computational resources, and high power for real time image encryption [42]. Furthermore, some intrinsic features of image, such as big storage capacity, high data redundancy, and strong correlation among adjacent pixels, are different from other information [25, 46, 52]. Hence, researchers have presented many effective image cryptographic schemes [5, 36] based on different theories and purposes. Chaotic cryptography offers a series of properties whitch are suitable for image encryption. These properties have extreme sensitivity to initial conditions, also have non-periodicity, pseudo-randomness, ergodicity, reproduction, and can generate a large number of chaotic sequences quickly and accurately [44].

The chaotic maps that are used in image encryption schemes, can be divided into two categories: one dimensional (1D) and higher dimensional (HD) chaotic maps. 1D chaotic maps have simple structures and are easy to be implemented [2, 22], but they have the defects of limited chaotic ranges [28, 36] and vulnerability [43].

HD maps have more complex structures and better chaotic behaviors. This makes their chaotic orbits more unpredictable [14]. However HD chaotic maps have the limitations of high computation cost and implementation difficulty [37, 38]. In order to overcome these difficulties, numerous encryption algorithms based on optical transformation [6, 7, 25], DNA computing [29, 37, 48], cellular automata [30, 41], and others [11, 15, 20] have been proposed.

Recently a new image encryption scheme has been introduced based on the phase-truncated short-time fractional Fourier Transform and the hyper-chaotic system [31]. In this method the plain image is divided into four sub-images to be encoded separately.

Huang Zhi-Jing et al. proposed a method based on chaotic system and two-dimensional linear canonical transform [51]. The scheme has proper robustness against different attacks due to the elimination of linearity and the main keys associated with the plain images.

Lihua Gong et al. presented an image compression and encryption scheme based on chaotic system and compressive sensing [18]. The bitwise XOR operation and a pixel-scrambling method controlled by chaos map are employed to improve the efficiency of diffusion and confusion operations of the measurement results, respectively. The keys used in the chaotic systems are related to the plain image and generated by the SHA-256 algorithm.

To save more storage space than the existing quantum image representation models and encrypting an arbitrary number of images simultaneously, Zhou Nan run et al. presented a new scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system [54]. In this method a quantum representation model for multiple images and a novel quantum multi-image encryption scheme has been proposed by combining quantum 3D Arnold transform and quantum XOR operations with scaled Zhongtang chaotic system. Moreover, a quantum image encryption scheme based on generalized Arnold transform and double random-phase encoding was proposed by Zhou Nan run et al. [53]. In this scheme, by combining generalized Arnold transform with double random-phase encoding, a quantum image encryption algorithm has been introduced.

In order to reduce the processing time and enhance the efficiency of encryption and decryption for color images, Guangfeng Cheng et al. proposed a novel color image encryption scheme based on hyper chaotic system and permutation-diffusion architecture [10]. In this method, a block permutation is employed to enhance the efficiency, and a hyper chaotic system generates the key streams to diffuse the pixels. For better security three R, G, B color components are affected each other by different mixing schemes.

Studies have revealed that intrinsic properties of the chaotic maps are equivalent to the counterparts of cryptography [19, 36, 52]. Hence, hybrid chaotic systems are the perfect candidate for cryptography, which has been extensively used in image encryption. In this paper an image encryption scheme based on a new hybrid chaotic system is presented. 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 rest of the paper is organized as follows: Section 2 presents the basic definitions concerning Arnold's cat map and three other 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 section 5. Section 6 gives a conclusion to the paper, and finally in section 7 we introduce future work.

2 Preliminaries

This section briefly reviews four representative chaotic maps, namely Arnold's cat map, Sine map, Tent map, Logistic map, and their combinations respectively.

2.1 Arnolds' cat map

According to Arnold's transformation (Eq. (1)), an image is hit with the transformation that apparently randomizes the original organization of its pixels. However, enough iteration can generate the original image [1]. The number of considered iterations is known as the Arnold's period. The period depends on the image size, and parameters *a, b*.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \begin{bmatrix} \mathrm{x}_{\mathrm{n}+1} \\ \mathrm{y}_{\mathrm{n}+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ N) = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod\ N). \tag{1}$$

Where N is the size of $N \times N$ square image, a and b are positive integers and $det\ (A) = 1$. (x_n, y_n) is the position of samples in the $N \times N$ data such as image, so that $(x_n, y_n) \in \{0,1,2,\ldots,N\text{-}1\}$ and (x_{n+1}, y_{n+1}) is the transformed position after cat map.

Arnold's cat map, which bring chaotic movement, has two typical factors including tension (multiply matrix (A) in order to enlarge (x, y)) and fold (taking mod in order to bring x, y in unit matrix).

Table 1 the shows the Arnold's period for typical image sizes and different a, b parameters. In this paper for simplicity we choose $a = b$.

2.2 Sine map

Sine map, one of the mostly used 1D chaotic maps, has a simple dynamic structure, but it can generate complex chaotic sequences with a range of [0, 1]. The definition of Sine map is:

$$f_{n+1} = s \times \sin(\pi f_n), \tag{2}$$

where s is a parameter and according to the bifurcation diagram [22], $s \in [0.87, 1]$ and s_0 is the initial value for f_n.

2.3 Tent map

Tent map is another 1D chaotic map that is used in many applications. It is well known that its graph in bifurcation diagram looks like the curve of tent function. The definition of Tent map is presented as follows [22]:

$$g_{n+1} = \begin{cases} 2tg_n & g_n < 0.5 \\ 2t(1-g_n) & g_n \geq 0.5, \end{cases} \tag{3}$$

where t is a parameter and according to the bifurcation diagram $t \in [0.5, 1]$ and t_0 is the initial value for g_n.

Table 1 Arnold's period for typical image sizes and different a, b parameters

Image Size	a	b	Arnold's Period
128 × 128	1	1	96
128 × 128	2	2	64
128 × 128	3	3	96
128 × 128	4	4	128
256 × 256	1	1	192
256 × 256	2	2	128
256 × 256	3	3	192
256 × 256	4	4	256
512 × 512	1	1	384
512 × 512	2	2	256
512 × 512	3	3	384
512 × 512	4	4	512
1024 × 1024	1	1	768
1024 × 1024	2	2	512
1024 × 1024	3	3	768
1024 × 1024	4	4	1024

2.4 Logistic map

Logistic map is derived from Sine map, so they have some similar properties. In order to restrict the input value in a range of [0, 1], Logistic map is mathematically defined as follows [22]:

$$h_{n+1} = 4l\, h_n(1-h_n), \tag{4}$$

where l is a parameter and according to the bifurcation diagram $l \in [0.9, 1]$ and l_0 is initial value for h_n.

2.5 Hybrid chaotic maps

In this paper we use four hybrid chaotic systems; Logistic-Tent system (LT), Logistic-Sine system (LS), Sine-Tent system (ST) and Logistic-Tent-Sine system (LTS). Each of chaotic system is a nonlinear mixture of two or three different chaotic maps, i.e., Logistic map, Tent map and Sine map, which are supposed to be seed maps. These hybrid chaotic maps are based on the nonlinear combination of seed maps, which are described as follows:

$$\text{LT system}: x_{n+1} = \text{Logistic}\ (\text{Tent}\ (x_n)) \qquad \mathit{mod}\ 1. \tag{5}$$

$$\text{LS system}: x_{n+1} = \text{Logistic}\ (\text{Sine}\ (x_n)) \qquad \mathit{mod}\ 1. \tag{6}$$

$$\text{ST system}: \ x_{n+1} = \text{Sine}\ (\text{Tent}\ (x_n)) \qquad \mathit{mod}\ 1. \tag{7}$$

$$\text{LTS system}: x_{n+1} = \text{Logistic}\ \Big(\text{Tent}\ \Big(\text{Sine}\ (x_n)\Big) \quad \mathit{mod}\ 1. \tag{8}$$

The *mod* operation here ensures the output is restricted to [0, 1]. The cascade operator is applied to seed maps, which improves complexity level of the chaotic structure. Simulations and analysis have clarified the excellent chaotic ness that characterize hybrid maps.

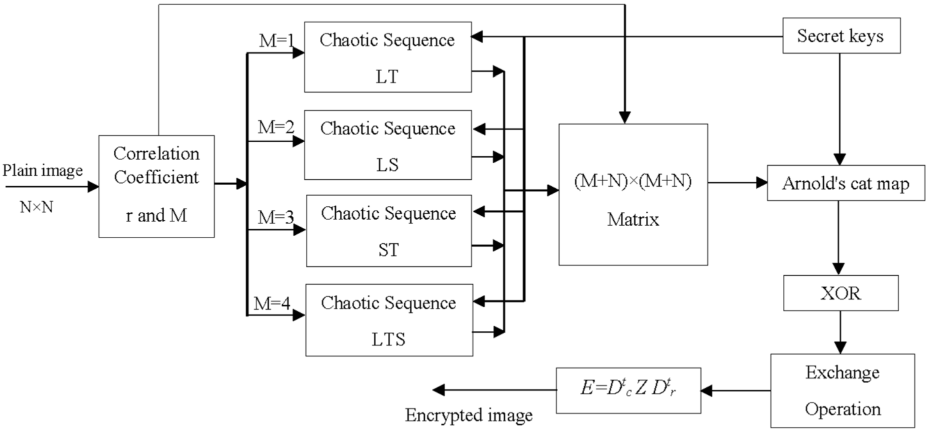

Fig. 1 Block diagram of the proposed encryption process

3 The proposed method

A new encryption scheme for efficient and secure image content preservation is presented in Fig. 1. This method is specialized for grayscale images with different sizes, and it consists of two iterative phases: chaotic confusion and pixel diffusion. An improved hybrid chaotic system is employed by both of these phases, where it's dynamical initial value and system parameter are produced by means of the external secret key, for the sake of generating one-time chaotic sequences, increasing the sensitivity to small changes of the plain image, and hence ensuring the immunity of the cryptosystem against known/chosen plain image attacks.

The diffusion phase is ruled by means of extension, *XOR*, transform, and exchange operations, aiming to elevate the sensitivity to plain image and accelerate the diffusion mechanism of the whole cipher algorithm. The confusion phase is governed by Arnold's cat map. The detailed description of the encryption algorithm is given in 9 steps as follow:

Step 1: Let I be $N \times N$ gray scale plain image. In this step, the average absolute value of correlation coefficient (r) for 3000 randomly horizontaly, verticaly, and diagonal adjacent pairs of pixels in plain image is calculated. If $0 < r \leq 0.7$ then let $M = 1$ and $r_1 = r$. If $0.7 < r \leq 0.8$ then let $M = 2$ and $r_2 = r$. If $0.8 < r \leq 0.9$ then let $M = 3$ and $r_3 = r$. If $0.9 < r < 1$ then let $M = 4$ and $r_4 = r$.

Step 2: Extend the original image I from $N \times N$ to $(M + N) \times (M + N)$ and denote it by R (Fig. 2); M is obtained from *step 1*. For simplicity, we assume that original image is square, otherwise we can add proper number of rows and columns to achieve square matrix (for example we can add $M + d$ rows and $M + e$ columns and fill them by binary chaotic integers between [0,255], where d and e are positive integers).

Step 3: According to the features of bifurcation diagram of Logistic, Tent and Sine map, one of the following combination of chaotic maps is applied to generate chaotic sequences:

For r_1 mode, apply LT system (combination of Logistic and Tent map).
For r_2 mode, apply LS system (combination of Logistic and Sine map).
For r_3 mode, apply ST system (combination of Tent and Sine map).

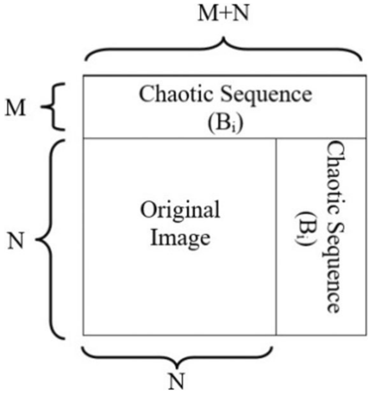

Fig. 2 Extended matrix

For r_4 mode, apply LTS system (combination of Logistic, Tent and Sine map).

Step 4: Fill $(M\times N)+M\times(M+N)$ components of extended matrix R by using the generated chaotic sequences by using Eqs. (5–8) from left to right and up to down according to *step 5*.

Step 5: Here we convert the chaotic sequence W_i generated by proposed hybrid chaotic maps (LT, LS, ST or LTS), with a range [0, 1] into an integer sequence $((M\times N)+M\times(M+N)$ components) with a range [0, 255] by using Eq. (9):

$$S_i=[(10^q\times W_i)]\ mod\ 256, \tag{9}$$

where q is the number of floating point of generated chaotic sequences. Then S_i is converted to a binary sequence B_i. New extended $(M+N)\times(M+N)$ matrix R, contains the plain image I and the extended components B_i.

Step 6: In this step, we apply Arnold's cat map k times for scrambling the location of pixels by means of confusion. To reduce the number of secret keys, we let $a=b=M$. k is one of the secret keys with respect to the Arnold's period by noting that $mod\ (M+N)$ will be used here.

Step 7: We use row and column XOR operations for diffusion; e.g. suppose we have 6 pixels:

Pixel No.1	Pixel No.2	Pixel No.3	Pixel No.4	Pixel No.5	Pixel No.6
11101010	10110100	01101101	11110010	11000101	11010101

We have:

a- (Pixel No.1) ← (Pixel No.1) ⊕ (Pixel No.2)
b- (Pixel No.2) ← (Pixel No.2) ⊕ (Pixel No.3)
c- (Pixel No.3) ← (Pixel No.3) ⊕ (Pixel No.4)
d- (Pixel No.4) ← (Pixel No.4) ⊕ (Pixel No.5)
e- (Pixel No.5) ← (Pixel No.5) ⊕ (Pixel No.6)

Therefore we will have:

Pixel No.1	Pixel No.2	Pixel No.3	Pixel No.4	Pixel No.5	Pixel No.6
01011110	11011001	10011111	00110111	00010000	11010101

Reverse operations are similar the scheme from e to a.

Step 8: Matrix R will be changed to matrix Z by exchanging the values of M and $M+4$ positions in every binary number for all $(M+N)\times(M+N)$ components.

Step 9: Let row Z_r and column Z_c are generated by the *step 8*, then we define new matrix D according to the following equations:

$$D_c(i,j) = \begin{cases} 0 & for(Z_r(j), j) \\ 1 & others \end{cases} \tag{10}$$

$$D_r(k,l) = \begin{cases} 0 & for(k, Z_c(k)) \\ 1 & others \end{cases} \tag{11}$$

Final encrypted output is generated as follows:

$$E = D_c^t \, Z \, D_r^t \tag{12}$$

In decryption process, the matrix Z will be recovered by the following way:

$$Z = \left(D_c^t\right)^{-1} E \left(D_r^t\right)^{-1} \tag{13}$$

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

3.1 Motivation

As first motivation, to reduce time complexity and more efficiency, we proposed that plain images with different features and correlations must encrypt in different ways.

Furthermore, seed maps such as Logistic, Tent and Sine maps have the limitations of chaotic performance, which will impair encryption effect and make the encrypted images easy to crack. Also, high dimension chaotic maps suffer from high computation cost and difficult implementation, so it is necessary to design a new chaotic system to enhance chaotic properties for an extensive range of system parameters. Hence, as second motivation, we proposed to employ hybrid chaotic systems.

3.2 Theoretical analysis of proposed scheme

To analyze the efficiency of our scheme theoretically, we use Lyapunov exponent (LE) to study the chaotic behavior of proposed method. It is known that a system with bigger positive LE values will have a good chaotic behavior. In this part we present a proof analysis of the chaotic behavior of LT structure (combination of Logistic and Tent maps). Other structures (LS, ST, LTS) proof analysis, are similar.

Suppose x_0, y_0 are two initial values and difference between them is too small. Also x_1, y_1 are the next iteration of x_0 and y_0. $L(x)$, $T(x)$ are Logistic and Tent maps respectively. We have:

$$|x_1 - y_1| = \left(\frac{|L(T(x_0)) - L(T(y_0))|}{|T(x_0) - T(y_0)|} \; \frac{|T(x_0) - T(y_0)|}{|x_0 - y_0|}\right.$$

If $x_0 \rightarrow y_0$ then $T(x_0) \rightarrow T(y_0)$ and we have:

$$\left| \frac{d(L)}{dx} \right|_{T(x_0)} \left| \approx \lim_{T(x_0) - T(y_0)} \frac{|L(T(x_0)) - L(T(y_0))|}{|T(x_0) - T(y_0)|}, \left| \frac{d(T)}{dx} \right|_{x_0} \right| \approx \lim_{x_0 - y_0} \frac{|T(x_0) - T(y_0)|}{|x_0 - y_0|}.$$

Now we have:

$$|x_1 - y_1| \approx \left(\left| \frac{d(L)}{dx} \right|_{T(x_0)} \left| \left| \frac{d(T)}{dx} \right|_{x_0} \right| \right) |x_0 - y_0|.$$

So we have the following result after n iteration:

$$|x_1 - y_1| \approx \left(\left| \prod_{i=0}^{n-1} \frac{d(L)}{dx} \right|_{T(x_i)} \left| \left| \prod_{i=0}^{n-1} \frac{d(T)}{dx} \right|_{x_i} \right| \right) |x_0 - y_0|.$$

Let $\Delta P(x)$ is the average chnage in each iteration from $|x_1 - y_1|$ to $|x_n - y_n|$ we have:

$$\Delta P(x) \approx \left(\left| \prod_{i=0}^{n-1} \frac{d(L)}{dx} \right|_{d(T(x_i))} \left| \left| \prod_{i=0}^{n-1} \frac{d(T)}{\mathrm{dx}} \right|_{x_i} \right| \right)^{\frac{1}{n}}.$$

According to the definition of Lyapunov exponent (LE), we can calculate LE of $P(x)$ as:

$$\lambda_{P(x)} = \ln(\Delta P(x)) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left(\left| \frac{d(L)}{dx} \right|_{d(T(x_i))} \left| \left| \frac{d(T)}{dx} \right|_{x_i} \right| \right) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left(\frac{d(L)}{dx} \right|_{d(T(x_i))} \Bigg)$$
$$+ \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left(\frac{d(T)}{dx} \right|_{x_i} \Bigg) = \lambda_{L(x)} + \lambda_{T(x)},$$

where $\lambda_{L(x)}$ and $\lambda_{T(x)}$ are Lyapunov exponent of $L(x)$ (Logistic map) and $T(x)$ (Tent map).

We know the larger value of a positive LE has better chaotic performance, so $\lambda_{L(x)}$ and $\lambda_{T(x)}$ must be positive numbers, and it is clear that $\lambda_{P(x)} \geq \lambda_{L(x)}$ and $\lambda_{P(x)} \geq \lambda_{T(x)}$. As a result, we proved the structure with combination of Logistic and Tent maps (LT system) has wide chaotic range rather than Logistic and Tent maps separately.

4 Security and performance analysis

In order to illustrate the performance clearly, 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.

4.1 Distribution of the cipher image

An image histogram displays that how pixels in an image are distributed by plotting the number of pixels [2]. Here taking a 512 × 512 standard gray scale image in Fig. 3 (boat.512 in http://sipi.usc.edu/database). The histogram of encrypted image is uniform-distributed compared with those of the original images that are unevenly distributed. These results indicate that the proposed algorithm performs well in breaking the correlations of image pixels and achieving satisfactory image encryption performance. Histograms of the other images and the corresponding ciphered images are shown in Fig. 4. As it was displayed, the histograms of the original image and the ciphered image, it does not provide any clues to the use of any statistical analysis attack on the encrypted image [28].

4.2 Shannon entropy analysis

Information entropy is the most significant measure of the strength of a cryptosystem. The information entropy of plain image I is defined as Eq. (14). The ideal information entropy of an 8 bit truly random image is 8, where the image would not show any useful information to attackers. Equation (14) implies that uniform distribution leads the algorithm to the better entropy.

$$H(s) = \sum_{i=0}^{255} P(s_i) Log_2 \frac{1}{P(s_i)} \tag{14}$$

where s_i denotes the gray-level and $P(s_i)$ is the probability of the occurrence s_i. Table 2 represents the entropy of sample standard gray level images. Results show that the entropy of all encrypted images are more than 7.99.

Figures 3, 4 and 5 show the Boat, Lena, Peppers, Baboon, Female, Airplane and Stream & bridge images. Shannon entropy of different images encrypted by the proposed scheme, is listed in Table 3 and it shows that the Shannon entropy of the proposed encrypted images is all close to 8.

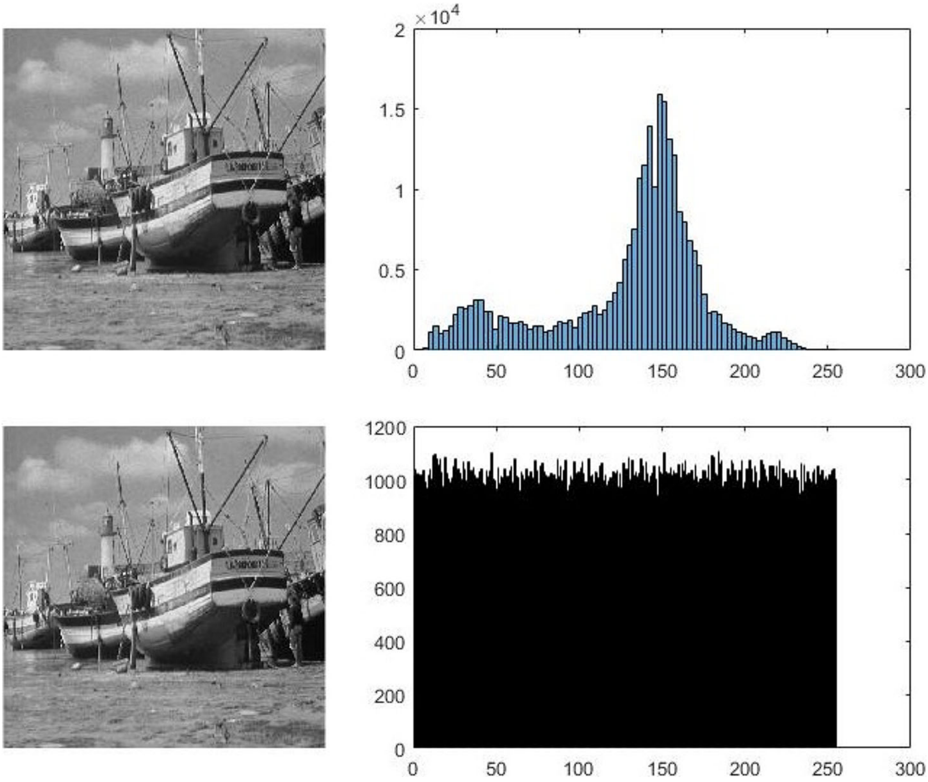

Fig. 3 The first row shows original 512 × 512 standard gray scale image and its histogram. The second row illustrate the decrypted image and encrypted histogram

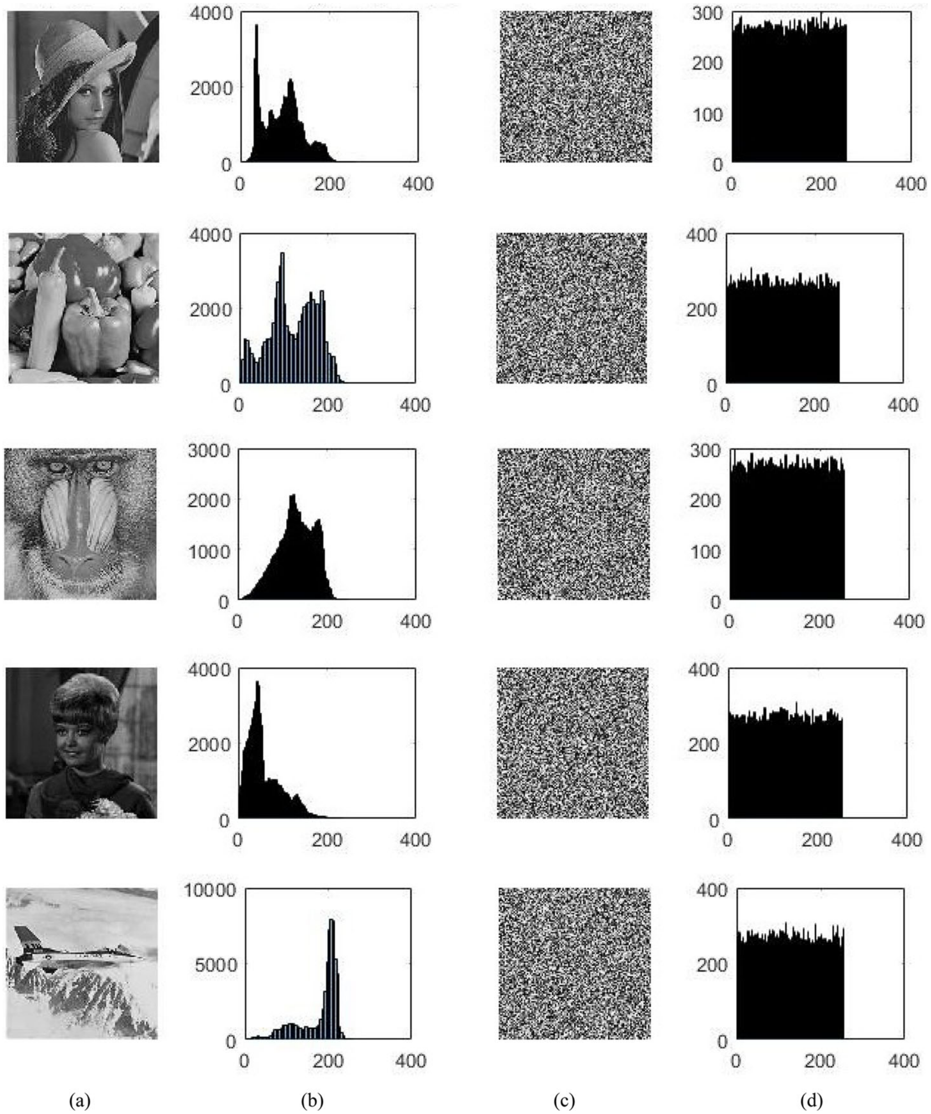

Fig. 4 Simulation results of different types of images. The first and second columns show original images and their histograms (a,b). The third and fourth columns illustrate the ciphered images and their histograms (c,d)

4.3 Correlation analysis

The adjacent pixels of plain image always have high correlation coefficients, while an effective encryption algorithm should significantly reduce the correlation coefficients of the cipher image. We select 3000 horizontal (vertical and diagonal) adjacent pixels in the test plain and cipher image randomly to analyze their correlation coefficients according to Eq. (18).

An efficient cipher algorithm should conceal such relations between adjacent pixels, and exhibit a good performance of balanced 0–1 ratio and zero correlation [4, 5]. Table 4 shows the

Table 2 Information entropy test results for standard images

Test images	Image size	Cipher images entropy
Boat	512 × 512	7.999978
Lena	256 × 256	7.999834
Peppers	256 × 256	7.999297
Baboon	256 × 256	7.999481
Female	256 × 256	7.998741
Airplane	256 × 256	7.998523
Stream and bridge	512 × 512	7.999821

obtained results of correlation coefficient values of the selected standard test images and their modified images. To find plain images with different correlations, in order to cover 4 proposed correlation modes ($r_1,...,r_4$), we employed modified standard images as shown in Table 4.

From the obtained correlation coefficient results, it is obvious that the high relations among plain images' neighboring pixels (correlation coefficient close to 1) effectively reduced in the corresponding cipher images' pixels (correlation coefficient close to 0), using the proposed cipher algorithm, reflecting the efficiency of this later to conceal the spatial redundancy within the cipher image's pixels.

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{15}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{i=N}[x_i-E(x_i)]^2 \tag{16}$$

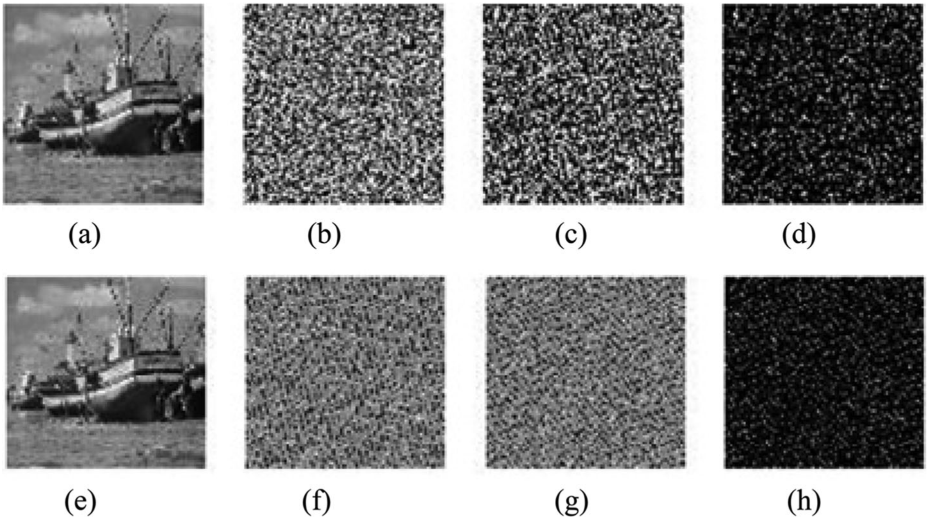

Fig. 5 Key sensitivity analysis. **a** Original image. **b** Encryption image E_1 with K_{e1}. **c** Encryption image E_2 with K_{e2}. **d** Difference between encryption images $|E_1\text{-}E_2|$. **e** Decryption image D_1 with correct secret key. **f** Decryption image D_2 from E_1 with $K_{e1} + 10^{-14}$. **g** Decryption image D_3 from E_2 with $K_{e2} + 10^{-14}$. **h** Difference between two decryption images |D2-D3|

Table 3 Comparison of the entropy value between proposed scheme and other methods

Encryption scheme	Image	Size	Cipher images entropy
Our method	Lena	512 × 512	7.999918
Ref. [2]	Lena	512 × 512	7.999338
Ref. [8]	Lena	512 × 512	7.999319
Ref. [43]	Lena	512 × 512	7.999324
Ref. [47]	Lena	512 × 512	7.999301
Ref. [35]	Lena	512 × 512	7.999286
Our method	Lena	256 × 256	7.999834
Ref. [2]	Lena	256 × 256	7.996951
Ref. [32]	Lena	256 × 256	7.997000
Ref. [23]	Lena	256 × 256	7.997200
Ref. [42]	Lena	256 × 256	7.997300
Our method	Peppers	512 × 512	7.999880
Ref. [2]	Peppers	512 × 512	7.999240
Ref. [9]	Peppers	512 × 512	7.999275
Our method	Peppers	256 × 256	7.999297
Ref. [2]	Peppers	256 × 256	7.996940
Ref. [32]	Peppers	256 × 256	7.997300
Ref. [42]	Peppers	256 × 256	7.997500
Our method	Baboon	512 × 512	7.999896
Ref. [2]	Baboon	512 × 512	7.999350
Ref. [47]	Baboon	512 × 512	7.999263
Ref. [9]	Baboon	512 × 512	7.999345

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x_i)][y_i - E(y_i)] \tag{17}$$

$$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}}, \tag{18}$$

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

Table 4 Correlation test results for 256 × 256 standard and modified images

Test Image	Original Image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Standard Lena	0.9712	0.9854	0.9852	0.0054	0.0049	0.0042
Standard Peppers	0.9174	0.9741	0.9047	0.0081	0.0031	−0.0077
Standard Boat	0.9709	0.9365	0.9403	0.0065	0.0082	0.0054
Modified Lena 1	0.8315	0.8257	0.8421	0.0051	0.0060	0.0061
Modified Peppers 1	0.8168	0.8469	0.8112	0.0078	−0.0045	0.0043
Modified Boat 1	0.8452	0.8625	0.8321	0.0054	0.0075	0.0038
Modified Lena 2	0.7568	0.7357	0.7621	0.0049	0.0065	−0.0022
Modified Peppers 2	0.7834	0.7796	0.7365	0.0068	0.0041	0.0071
Modified Boat 2	0.7213	0.7392	0.7426	−0.0034	0.0067	0.0044
Modified Lena 3	0.5810	0.6126	0.5339	0.0028	0.0057	0.0061
Modified Peppers 3	0.3664	0.4842	0.4155	0.0031	0.0048	0.0029
Modified Boat 3	0.2012	0.1988	0.2467	0.0019	0.0033	−0.0025

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

Test Image	*NPCR* (%)	*UACI* (%)
Lena (10,33)	99.6975	33.4788
Lena (55,60)	99.7491	33.4693
Lena (100,77)	99.7123	33.4515
Lena (130,115)	99.7422	33.4413
Lena (190,155)	99.7710	33.4891
Lena (250, 210)	99.7155	33.4801

4.4 Robustness against differential attacks

A powerful attacker may be able to find a meaningful relationship between the original image and the encrypted image [49]. For the sake of ensuring the effectiveness and robustness against differential attacks, the standard grayscale Lena image is enciphered by the proposed method (T_1). Then six modified images are attained by only changing the least significant bit (LSB) of the matching randomly chosen pixels at location (x,y), namely Lena (x,y).These modified images are denoted by Lena (10,33), Lena (55,60), Lena (100,77), Lena (130,115), Lena (190,155), Lena (250, 210). Equations (19), (20), and (21) are used to calculate *NPCR* and *UACI* values. These values are shown in Table 5.

$$NPCR = \frac{\sum_{i,j} C(i,j)}{W \times H} \times 100\% \tag{19}$$

$$\begin{cases} C(i,j) = 1 \ \text{if} \ T_1(i,j) \neq T_2(i,j) \\ C(i,j) = 0 \ \text{if} \ T_1(i,j) = T_2(i,j) \end{cases} \tag{20}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|T_1(i,j) - T_2(i,j)|}{255}\right] \times 100\% \tag{21}$$

where T_1 represents the obtained cipher image from the original plain image, whereas T_2 is obtained after 1 bit plain image's modification and $W \times H$ is the size of image. *NPCR* and *UACI* are computed after randomly altering one pixel in the original image. The *NPCR* and *UACI* of different original images are listed in Tables 5 and 6. Almost 99.7% pixels between the encrypted images are different and the score of the *UACI* between the encrypted images is

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

Test Image	*NPCR* (%)	*UACI* (%)
Lena	99.7298	33.4810
Peppers	99.6412	33.5102
Baboon	99.6236	33.4311
Female	99.6389	33.4132
Airplane	99.6311	33.5484
Boat	99.6215	33.4572
Stream and bridge	99.5621	33.5098

not less than 33.41%. In proposed scheme any pixel changed in the original image would result in significantly and substantially different encrypted images. The results clearly indicates the effective performance of the proposed encryption algorithm resisting the differential attacks.

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.

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

Method	Image	Size	*NPCR* (%)	*UACI* (%)
Our method	Lena	512 × 512	99.6461	33.6252
Ref. [2]	Lena	512 × 512	99.6452	33.6152
Ref. [8]	Lena	512 × 512	99.6200	33.4300
Ref. [13]	Lena	512 × 512	99.6070	33.4630
Ref. [43]	Lena	512 × 512	99.6200	33.4100
Ref. [47]	Lena	512 × 512	99.6052	33.4111
Ref. [35]	Lena	512 × 512	99.6215	33.4654
Our method	Lena	256 × 256	99.7298	33.4810
Ref. [2]	Lena	256 × 256	99.5941	33.5052
Ref. [28]	Lena	256 × 256	99.5894	33.4645
Ref. [32]	Lena	256 × 256	99.6550	33.5160
Ref. [23]	Lena	256 × 256	99.6100	33.4600
Ref. [42]	Lena	256 × 256	99.6100	33.5300
Our method	Peppers	512 × 512	99.7136	33.5413
Ref. [2]	Peppers	512 × 512	99.6315	33.5073
Ref. [8]	Peppers	512 × 512	99.6000	33.5400
Ref. [47]	Peppers	512 × 512	99.6052	33.4372
Ref. [35]	Peppers	512 × 512	99.6112	33.4612
Ref. [9]	Peppers	512 × 512	99.6391	33.5128
Our method	Peppers	256 × 256	99.6412	33.5102
Ref. [2]	Peppers	256 × 256	99.5849	33.4641
Ref. [42]	Peppers	256 × 256	99.6300	33.5800
Our method	Baboon	512 × 512	99.6234	33.4156
Ref. [34]	Baboon	512 × 512	99.6154	33.4354
Ref. [8]	Baboon	512 × 512	99.6100	33.3351
Ref. [47]	Baboon	512 × 512	99.3504	33.4520
Ref. [45]	Baboon	512 × 512	99.6048	33.4554
Ref. [9]	Baboon	512 × 512	99.6110	33.4354
Our method	Baboon	256 × 256	99.6236	33.4311
Ref. [2]	Baboon	256 × 256	99.6017	33.6287
Ref. [28]	Baboon	256 × 256	99.6124	33.4891
Our method	Boat	512 × 512	99.6194	33.5562
Ref. [2]	Boat	512 × 512	99.6284	33.5407
Ref. [3]	Boat	512 × 512	99.1025	33.1600
Ref. [13]	Boat	512 × 512	99.6154	33.4654
Our method	Boat	256 × 256	99.6215	33.4572
Ref. [2]	Boat	256 × 256	99.6139	33.4751
Ref. [32]	Boat	256 × 256	99.6250	33.4530

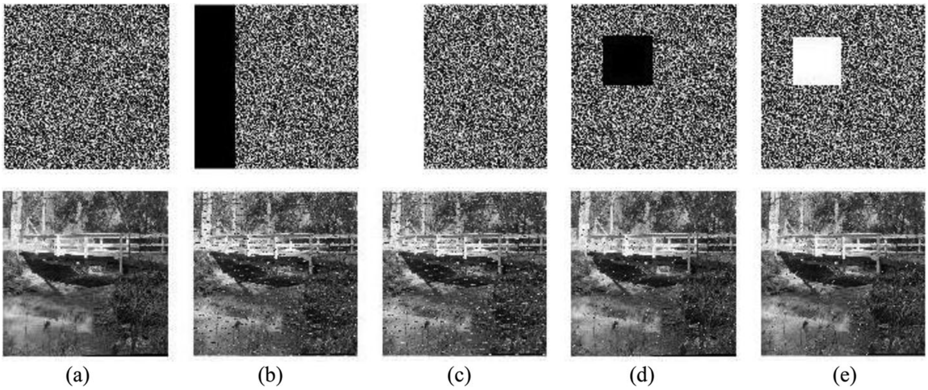

Fig. 6 The images on the first row are the original encrypted 'stream and bridge' 512 × 512 Gy scale image (**a**), and its damaged versions by 25% black cropping (**b**), 25% white cropping (**c**), 150 × 150 square black data loss (**d**), 150 × 150 square white data loss (**e**). Those images on the second row are decrypted results of corresponding encrypted images

4.5 Security key space

A good encryption scheme should have a key space more than 2^{100} to resist the brute force attack [48]. For the proposed scheme, the security key includes eight parts; (s_0, u_s), (l_0, u_l) and (t_0, u_t) are the initial values for Sine map, Logistic map and Tent map respectively in a range of [0, 1], also Arnold's cat map iteration (k) and finally M are positive integers. If the length of every sub key is set to 14 decimals, the key space of proposed method will be 10^{112} .

4.6 Key sensitivity analysis

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. Key sensitivity test is usually tested in the image encryption and decryption procedures as follows [2]:

1. The cryptosystem should produce completely different encrypted image when slightly different secret keys are used to encrypt the image.

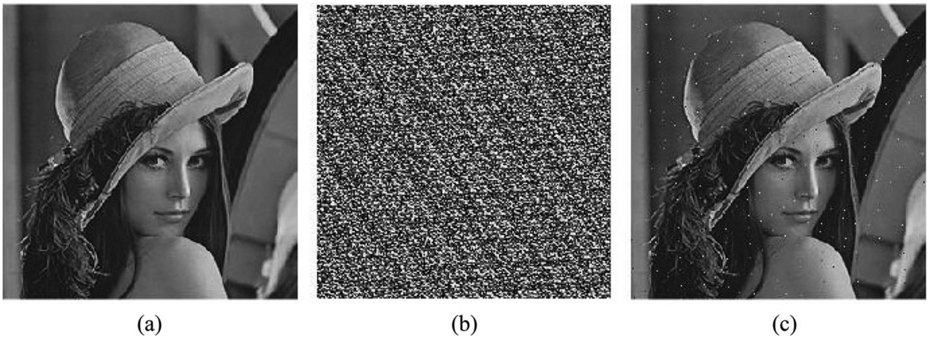

Fig. 7 Lena 512 × 512 standard plain image (**a**), damaged by 5% Salt and Pepper noise (**b**), decryption of damaged cipher image (**c**)

Table 8 The running time performance test (ms)

Image Size	Ref. [52]	Ref. [33]	Ref. [2]	Ref. [40]	Ref. [27]	Ref. [24]	Proposed
256 × 256	178	109	48	7641	189	569	92
512 × 512	663	390	139	34,768	758	2251	109
1024 × 1024	3142	1482	481	151,709	3096	8986	351

2. The cryptosystem should be unable to decrypt cipher text even for the slight 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. 5. K_{e1} and K_{e2} are two encryption keys with a tiny difference of 10^{-14}. The pixel-to-pixel difference can be acquired by calculating the absolute value of difference between the two encrypted images, which is shown in Fig. 5d. The corresponding decrypted results with incorrect decryption keys.

$K_{e1} + 10^{-14}$ and $K_{e2} + 10^{-14}$ are shown in Fig. 5f and g, whose pixel-to-pixel difference is obtained in Fig. 5h. This figure shows that 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 [41]. To check the robustness of the proposed scheme, we perform some experiments on the noise attack and the data loss. Grayscale image in Fig. 6, encrypted by proposed algorithm, then encrypted image is attacked by a data cut of different sizes.

To evaluate the resistance of proposed scheme against noise attack, encryption image of Lena 256 × 256 standard grayscale image is attacked by 5% 'salt & pepper' noise (Fig. 7). Then the corresponding decrypted image is given in Fig. 7c. The results show that decipher images of cropped cipher images are still recognized visually, therefore proposed scheme is robust against cropping and noise attacks.

5 Speed analysis

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 8 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 novel grayscale image cryptosystem based on chaotic maps is proposed. In contrast to the traditional chaos based cryptosystems, the proposed cryptosystem with successive confusion and diffusion procedures enhances the security level. The confusion phase is governed by Arnold's cat map and the diffusion operation is controlled by extension of plain image matrix, *XOR* operation, and exchange operation. The key space of the encryption scheme is large enough to resist brute-force attacks, and the scheme is extremely sensitive to keys. The encrypted image of the proposed scheme has a uniform histogram, a correlation coefficient which is close to zero, and an entropy which is close to the maximum entropy. All of these illustrate that the scheme can resist statistical attack substantially. The *UACI* scores are close to the ideal score, and the *NPCR* scores are proper for resisting differential attack. In addition the encryption and decryption processing time directly depend on the value of correlation coefficient of original image. Plain images with less correlation coefficient have less encryption and decryption processing time, and vice versa. The dynamical analysis and evaluation results show that the proposed scheme has wide chaotic regime for an extensive range of system parameters and offers good security, and can resist common attacks.

7 Future work

In the future work, we intend to introduce an intelligent scheme by using neuro-fuzzy methods to improve the encryption speed and efficiency. In this scheme, different images with different features will encrypt intelligently by proper encryption schemes, and make it more robust for reliable and practical cryptographic applications.

References

1. Abbas NAM (2016) Image encryption based on Independent Component Analysis and Arnold's Cat Map. Egypt Inform J 17:139–146
2. Souyah Amina, Mohamed FK (2017) An efficient and secure chaotic cipher algorithm for image content preservation, Signal processing, https://doi.org/10.1016/j.cnsns.2017.12.017, PII: S1007–5704(17)30439–2
3. Bakhshandeh A, Eslami Z (2013) An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt Lasers Eng 51(6):665–673
4. Borujeni SE, Eshghi M (2013) Chaotic image encryption system using phasemagnitude transformation and pixel substitution. Telecommun Syst 52(2):525–537
5. 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. p. 59–64
6. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons Fractals 21(3):749–761
7. 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
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 efficient image encryption scheme using gray code based permutation approach. Opt Lasers Eng 67:191–204
10. Cheng G, Wang C, Chen H (2019) A novel color image encryption algorithm based on hyper chaotic system and permutation-diffusion architecture. Int J Bifurcation Chaos 29(09):1950115
11. 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

12. Dhall S, Pal SK, Sharma K (2017) Cryptanalysis of image encryption based on a new 1D chaotic system, Signal processing, PII S0165–1684(17)30434–6, https://doi.org/10.1016/j.sigpro.2017.12.021
13. El Assad S, Farajallah M (2016) A new chaos-based image encryption system. Signal Process Image Commun 41:144–157
14. François M, Grosges T, Barchiesi D et al (2012) Image encryption algorithm based on a chaotic iterative process. Appl Math 3(12):1910
15. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 8(06): 1259–1284
16. Fu C, Chen J-j, Zou H et al (2012) A chaos-based digital image encryption scheme with an improved diffusion strategy. Opt Express 20(3):2363–2378
17. 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
18. 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
19. Hua Z, Zhou Y (2016) Image encryption using 2D Logistic-adjusted-Sine map. Inf Sci 339:237–253
20. Kanso A, Ghebleh M (2015) An efficient and robust image encryption scheme for medical applications. Commun Nonlinear Sci Numer Simul 24(1):98–116
21. 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
22. Lan R, He J, Wang S, Gu T, Luo X (2018) Integrated Chaotic Systems for Image Encryion, Signal processing, PII S0165–1684(18)30041–0, https://doi.org/10.1016/j.sigpro.2018.01.026
23. 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
24. Liao X, Lai S, Zhou Q (2010) A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 90(9):2714–2722
25. 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
26. 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
27. 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
28. 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
29. Pan SM, Wen RH, Zhou ZH, Zhou NR (2017) Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. Multimed Tools Appl 76:2933–2953
30. Shannon CE (2001) A mathematical theory of communication. ACM SIGMOBILE Mobile Comput Commun Rev 5(1):3–55
31. 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
32. Song C-Y, Qiao Y-L, Zhang X-Z (2013) An image encryption scheme based on new spatiotemporal chaos. Optik-Int J Light Electron Optics 124(18):3329–3334
33. Souyah A, Faraoun KM (2016) An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dynamics 86(1):639–653
34. Wang X, Guo K (2014) A new image alternate encryption algorithm based on chaotic map. Nonlinear Dynamics 76(4):1943–1950
35. Wang X, Xu D (2014) A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dynamics 75(1–2):345–353
36. Wang X, Zhang H-l (2015) A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt Commun 342:51–60
37. Wang Y, Wong K-W, Liao X et al (2011) A new chaos-based fast image encryption algorithm. Appl Soft Comput 11(1):514–522
38. Wang H, Xiao D, Chen X, Huang H (2017) Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map, Signal processing, PII: S0165–1684(17)30394–8, https://doi.org/10.1016/j.sigpro.2017.11.005
39. Wong K-W, Kwok BS-H, Yuen C-H (2009) An efficient diffusion approach for chaosbased image encryption. Chaos, Solitons Fractals 41(5):2652–2663
40. Wu Y, Yang G, Jin H et al (2012) Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 21(1):013014-1-013014-15

41. Wu J, Liao X, Yang B (2017) Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme, Signal processing, PII: S0165–1684(17)30134–2, https://doi.org/10.1016/j.sigpro.2017.04.006
42. 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
43. Yavuz E, Yazici R, Kasapbaşi MC et al (2015) A chaos-based image encryption algorithm with simple logical functions, Comput Electric Eng
44. 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, p. 10
45. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
46. Zhang Y-Q, Wang X-Y (2014) A symmetric image encryption algorithm based on mixed linear– nonlinear coupled map lattice. Inf Sci 273:329–351
47. Zhang X, Zhao Z (2014) Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dynamics 75(1–2):319–330
48. 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
49. 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
50. 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
51. 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
52. Zhou Y, Bao L, Chen CLP (2014) A new 1D chaotic system for image encryption. Signal Process 97:172–182
53. 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
54. 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.
55. 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 Habibizad Navin
a.habibizad@srbiau.ac.ir

Amir Massoud Bidgoli
Am_bidgoli@iau-tnb.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