Multimedia Tools and Applications (2022) 81:8179–8198
https://doi.org/10.1007/s11042-022-11917-0

Adaptive image encryption based on twin chaotic maps

Munazah Lyle[1] · Parsa Sarosh[1] · Shabir A. Parah[1]

Received: 11 July 2021 / Revised: 26 October 2021 / Accepted: 3 January 2022 /
Published online: 1 February 2022

Abstract
The information stored or shared via the internet is growing massively and includes images primarily. The images are vulnerable to attacks when transferred over the internet as they contain confidential information about a person. We propose an adaptive image encryption scheme for the security of images based on twin chaotic maps; Quadratic map and 2-dimensional chaotic Henon map. In the proposed encryption scheme, the Pseudo-Random Number (PRN) sequence for shuffling the pixels has been generated from the Henon map. The PRN sequence for the diffusion process has been produced from the classical Quadratic map. The significant contribution of the presented work is that both the chaotic sequences (for confusion and diffusion) are plain image dependent, making the encryption scheme adaptive and hence highly resilient to brute force attack. Image quality analysis, histogram analysis, correlation coefficient analysis, entropy analysis, key sensitivity analysis, and differential attack analysis have been carried out on eight natural images of size 512 × 512 to validate the performance of the proposed encryption scheme. The proposed encryption algorithm has correlation coefficient values that are very close to zero, entropy value of 7.9993 (average), Net Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) values of 99.62% (average) and 33.3% (average) respectively. The histogram of the encrypted images is flat, meaning no information can be deduced about the plain image. The comparison of the proposed encryption technique with other recent encryption schemes validates the performance of the proposed cryptosystem. The computational time taken to encrypt Lena image of size 512 × 512 using the proposed encryption scheme is 0.25 s.

Keywords Image encryption · Privacy · Security · Quadratic map · Henon map · Brute force attack

✉ Shabir A. Parah
shabireltr@gmail.com

[1] Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

1 Introduction

The growing use of mobile devices and digital technology has led to the generation of massive amounts of multimedia data that are primarily images [27]. The openness of networks and advanced computer processors has made the images vulnerable to attacks. By September 2021, there have been 97 security breaches that have affected 91,127,815 million records. The major breach among these is the Facebook data breach, where the data of 533 million individuals was hacked. In 2021, the average cost of data breaches is nearly USD 4.24 million and is the highest in 17 years. Thus, the protection of images transmitted over low-security channels has become very important [43]. Therefore, image encryption has become a hot research topic among researchers for medical imaging, military communications, etc., since these applications contain very sensitive data [9]. The images can be protected against unauthorized access by ensuring confidentiality. Confidentiality can be realized using encryption in which images are transformed into a form intelligible only to the one who possesses the key. This encrypted data is known as cipher data or encrypted data. The process by which the original data or image is recovered is known as decryption. The traditional encryption schemes such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adelman (RSA) are used in image encryption [8, 21, 41]. The size of images is usually huge, the redundancy and correlation between adjacent pixels are also very high [42]. The huge amount of image data hassles the encoding and decoding operations. While encrypting an image, the file format should not be affected. If the image data is considered ordinary data for encryption, it becomes difficult to perform file format conversion. Therefore, for image encryption, the file header and control information should not be encrypted. Because of the reasons mentioned above, it becomes cumbersome to apply algorithms that have been devised for textual data to encrypt images. Furthermore, the algorithms developed for text data are usually very slow, which prevents their use in real-time applications. This has led to the need to develop such encryption algorithms suitable for images, with chaos-based systems being the ideal ones. The randomness property of chaotic systems makes them suitable for image encryption.

The first stream cipher was devised by Matthews [29] in 1989 by employing a Logistic map. Since then, chaos-based systems have found significant application in exploring encryption algorithms for images as they provide more advantages than traditional encryption systems. The properties of chaos, such as extreme sensitivity to initial conditions, non-periodicity to motion trajectories, unpredictability, and nonlinearity, make them suitable for image encryption. Chaos-based image encryption schemes have become a crucial branch of cryptosystems [19]. Chaos-based encryption techniques are comprised of two phases: confusion and diffusion. In the confusion phase, the correlation between adjacent pixels is broken by changing the position of pixels. The image becomes unrecognizable, and the key dependency problem gets solved. The image can still be recovered by an attacker. So, it is not secure to have only the permutation stage. In the diffusion phase, the value of every pixel of the image is changed. The pixel values are changed in sequence by the PRN sequence generated from chaotic maps. This confusion-diffusion round is repeated several times to achieve security of satisfactory level [12].

Various image encryption schemes based on chaos have been proposed to protect the images transmitted and stored. Tian et al. [35] present an image encryption scheme based on deoxyribonucleic acid (DNA) employing coupled map lattices based upon Piecewise Linear chaotic map (PWLCM). The pseudo-random sequences are produced from the PWCLM. The control parameters and initial conditions have been obtained from the external keys and the hash value of the plain image. Li et al. [26] propose an image encryption scheme based on chaos. It

employs the imitating jigsaw method, which consists of shifting and revolving operations. The control sequences for shifting have been obtained from the hyperchaotic Lorenz system. The initial conditions for the hyperchaotic sequences have been obtained from the original image and external keys. Yan et al. [38] focus on the solution of the unrigorous scrambling and single diffusion method problems faced in the encryption of images. The authors devise a new method employing the arithmetic sequence scrambling method, 1-D Logistic map, and DNA encoding. Ferdush et al. [11] propose a lightweight image encryption method that is based on two chaotic maps which are Arnold and Logistic maps. The lightweight encryption schemes are superior to other methods as they need less memory and less time. Also, the power or energy required is less. Abdelfatah et al. [1] propose an encryption scheme based on four different chaotic maps for the encryption of multimedia. Authors have employed the Logistic, Lorenz, and Chebyshev chaotic maps in parallel and serial combinations.

Li et al. [25] propose an image encryption scheme based on a 2-D Logistic map and a 2-D Lorenz map. The scrambling of the image pixels is performed using two chaotic sequences obtained from the 2-D Logistic map. The XOR operation performs diffusion between the scrambled image sequence and the chaotic sequence obtained from the 2-D Lorenz map. Gopalakrishnan and Ramakrishnan [14] propose an image encryption scheme based on the hyperchaos, Lorenz, and Chens' systems. The permutation of the plain image is done using a 2-D hyperchaos map. The shuffled image is diffused using Lorenz's and Chen's systems. Afterward, a circular shift is given to the keystream used in the permutation to get the diffusion keystream. The keystream for the diffusion process is generated using multiple hyperchaotic maps depending on the plain image. Mishra and Saharan [30] propose an image encryption scheme based on the Henon map. The PRN sequence for shuffling is obtained from the Henon map, which uses a 128 bit externally supplied secret key. The encrypted image is obtained by XOR operation between the shuffled image and the cipher image obtained from the Henon map. Arab et al. [4] propose a chaos-based image encryption scheme in which the Arnold chaos sequence has been used as an encryption key, and a modified AES algorithm has been used for encryption. Ramasamy et al. [33] propose an image encryption scheme based on block scrambling and modified Zigzag Transformation. The key has been generated from an enhanced logistic – tent map.

Khan and Ahmad [22] propose a selective encryption scheme for next-generation multimedia networks. In this scheme, the plaintext image is divided into non-overlapping blocks. The random numbers are generated from a skew tent map. Two random sequences are generated from the Tangent-Delay Ellipse Reflecting Cavity Map System (TD- ERCS) chaotic map and permute the image. Khan et al. [23] propose a partial encryption scheme based on Discrete Wavelet Transform (DWT). DWT has been used to compress the plaintext image. Two pseudo-random sequences generated from PWLCM and Nonlinear Chaotic Algorithm are used to shuffle the image column-wise and row-wise, respectively. Another pseudo-random sequence is derived from the Intertwining Logistic map and XORed with the permuted image sequence. Kulsoom et al. [24] propose an encryption scheme for gray images based on chaotic maps and DNA complementary rules. In this scheme, the image is, first of all, shuffled using a sequence generated from the PWLCM. Afterward, the idea is decomposed into the most significant bits (MSB) and the least significant bits (LSB). Another sequence generated from the logistic map is XORed with MSB and LSB parts separately, and then these two parts are combined to get the cipher image. Darwish [10] propose selective image encryption and compression scheme. In this scheme, a 3-D cat map has been used to reduce the correlation between the adjacent pixels.

Chai et al. [7] propose a medical image encryption technique based on chaotic systems and Latin square. Plain image and Latin square have been used to shuffle the pixels of the image. The image is diffused using 4-dimensional memristive chaotic system. SHA 256 hash value of the plain image is computed and used as the initial condition of the memristive chaotic map. Tang et al. [34] propose an image encryption technique based on double spiral scans, Henon chaotic map, and Lu chaotic map. They have used double spiral scans for scrambling the image pixels. The starting point for the spiral scan is selected randomly with the help of the Henon chaotic map. The Lu chaotic map key is derived from image content, and a secret matrix of the size of the input image is generated. Lastly, an XOR operation is performed between the generated secret image matrix and the shuffled image matrix. Alsmirat et al. [2] present a fingerprint recognition system to address the problem of the loss of information of an individual faced with the use of digital cameras for fingerprint recognition. AlZu'bi et al. [3] present a 3-D model for the segmentation of 3-D medical images. This model is a modified version of the 2-D fuzzy C-means algorithm. The authors use images that have been obtained from various medical scanners like PET, CT, MRI as the input to the system. The contribution of the authors is towards the attainment of segmented 3-D volume in a very short computation time. Yu et al. [40] present an image encryption scheme based on the quaternion fresnel transform, two-dimensional logistic-adjusted sine map, and computer-generated hologram. First of all, quaternion algebra is used to represent the four original images that are processed holistically using Quaternion fresnel transform (QFST). Fresnel transform is used to encode the input complex amplitude with two virtual independent random phase masks. Wang et al. [36] present a visual saliency model. This model integrates direction, intensity, and color saliency maps to generate the overall saliency map.

Developing efficient, less complex, and fast image encryption algorithms for real-time applications is still a research problem. The existing encryption schemes suffer from some drawbacks, which are as follows:

- Some schemes have a small key-space which makes them prone to brute force attacks.
- Most of the existing schemes have not provided computational time analysis. Those that have provided it take more time to encrypt images, rendering them useless for real-time applications.
- Some of the state-of-the-art schemes have not provided the noise attack analysis.
- Most of the existing schemes are not adaptive, which leads to guessing the key and weakens the encryption scheme.

This work is motivated to develop self-adaptive image encryption algorithms with low computational complexity. The proposed image encryption scheme is less complex, adaptive, fast, robust to noise attacks, and has better security. The main contributions of the proposed encryption schemes are as follows:

- The proposed encryption scheme has low complexity because of less complex chaotic maps used for encryption and still has better performance than other chaos-based image encryption schemes.
- The proposed scheme has real-time application as the time to encrypt a 512×512 image is only 0.25 s.
- It is adaptive as the initial values of the chaotic maps have been made dependent on the plain image.

- The proposed scheme has a large keyspace and is robust to noise attacks.
- The histogram of the encrypted images is completely flat for both natural and medical images, preventing information leakage.

The organization of the rest of the paper is as follows. Section 2 explains the preliminaries, which include the Quadratic map and the Henon map. Section 3 describes the proposed cryptosystem in detail. Section 4 explains the experimental results and the comparison with other recent methods of the proposed encryption method. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Henon map

The Henon map is a discrete-time dynamical system [20] stated in Eqs. (1) and (2).

$$x_{n+1} = 1 - a \times {x_n}^2 + y_n \tag{1}$$

$$y_n = b \times x_n \tag{2}$$

Where a and b are the control parameters defined as a = 1.4 and b = 0.3 and x (1) and y (1) are the initial conditions. The Henon map is sensitive to the initial values and has good pseudo-randomness.

2.2 Quadratic map

The Quadratic map is a chaotic map [32] that can be stated in Eq. (3).

$$q_{n+1} = s - {q_n}^2 \tag{3}$$

The Quadratic map is nonlinear. Since the chaotic map's behavior is determined by its equation, it is deterministic. Changing the initial value q (1) slightly changes the map's behavior drastically. The chaotic behavior can be seen when $s \in [1.5, 2]$, and the periodic behavior can be seen when $s \in [0.74, 1.5]$.

3 Encryption algorithm

The key generation process and the encryption steps have been discussed in Sections 3.1 and 3.2, respectively and the encryption process is shown in Algorithm 1.

3.1 Key values generation

Step 1. Convert 2-D image (I) into a 1-D vector, i.e., K = I (:) and obtain the value of Q as shown in Eq. (4). Then calculate the sum of the image sequence pixels and take its modulus with the integer value 512, the modulus returns a remainder 'Q' after division in accordance with Eq. (4). The value of Q is used to generate the initial

value of the Henon map. The value of Q changes with every image and is dependent on the sum of the pixels of the plain image. This makes the encryption process adaptive.

$$Q = mod(sum(K), 512)\Big) \tag{4}$$

Step 2. Generate initial values of the Henon map from Eqs. (5) and (6).

$$x(1) = u \tag{5}$$

$$y(1) = Q \times 10^{-3} + v \tag{6}$$

The values of u and v have been chosen arbitrarily in the range of 0 to 1 to generate chaotic PRN sequences. Here, u = 0.192467976789447, and v = 0.112348694444999. Generate values of x(1) and y (1) from Eqs. (5) and (6) and values of a = 1.4, b = 0.3. After substituting initial values obtained from Eqs. (5) and (6) and values of a and b in Eqs. (1) and (2) iterate Eqs. (1) and (2) 512 × 512 times to generate Henon map PRN sequence (y) of length 512 × 512. The Henon map PRN sequence is used to obtain the shuffled image.

Step 3. Convert the PRN sequence (y) generated from the Henon map into image intensity range i.e. 0 to 255 using Eq. (7).

$$k1 = uint8\Big(mod\big(y \times 10^6, 256\big)\Big) \tag{7}$$

Step 4. Generate the initial value of the Quadratic map PRN sequence using Eq. (8).

$$q(1) = \frac{w + mod(Q, 0.512)}{6} \tag{8}$$

Where w = 0.757891552279999, which has been chosen arbitrarily. Substitute the value of Eq. (8) and s = 1.989891119999994 in Eq. (3) and iterate 512 × 512 times to generate the Quadratic map PRN sequence (q) of length 512 × 512.

Step 5. Convert values of sequence q into image intensity range using Eq. (9).

$$k2 = uint8\big(mod\big(q \times 10^6\big), 256\big) \tag{9}$$

Algorithm 1: Encryption Algorithm

Input: Image (I) of size (512,512), k1, k2

```
Start
Read image I of size (512 x 512).
Convert 2-D image matrix (I) into a 1- D sequence (K).
    [~, k3] = sort(k1)
     b = K
for j = 1 to M × N
    b = K(k3(j))
end
    D = XOR (b, k2')
    C = reshape(D, 512,512)
Stop
```

Output: Cipher image (D) of size (512,512)

3.2 Encryption steps

Step 1. Read a grayscale image I of size (512, 512).

Step 2. Convert 2-dimensional image matrix (I) into 1-dimensional image sequence i.e., K = I (:).

Step 3. Shuffle pixels of the image sequence (K) with the Henon map PRN sequence k1 to obtain shuffled image sequence (b). The sort function returns a sequence k3 in accordance with Eq. (10) that is the index of the sequence k1 (Henon map PRN sequence) in ascending order of the value of k1.

$$[\sim, \mathrm{k}3] = \mathrm{sort}(\mathrm{k}1) \tag{10}$$

The 1-D image sequence K is scrambled using the Eq. (11) to get the scrambled sequence b.

$$\mathrm{b} = \mathrm{K}(\mathrm{k}3(\mathrm{j})) \tag{11}$$

Here, $1 \leq j \leq 512$, $1 \leq j \leq 512$.

Step 4. The diffusion operation is performed by XOR operation between shuffled image and the Quadratic map PRN sequence (k2) using Eq. (12).

$$D = bit\ xor\ \left(b, k2^{'}\right) \tag{12}$$

Step 5. Reshape sequence D into 512 × 512 matrix to get 2-D image matrix C that is the encrypted image. This step completes the encryption process.

3.3 Decryption steps

For decryption, the same keys need to be available at the receiving end as the sender in addition to the key Q. The key generation process for decryption is the same as that of the encryption process. However, key Q needs to be sent to the receiver in addition to the other keys ("u", "v", "s", "w", "a", and "b"). The decryption process is the reverse of the encryption process. This is shown in Algorithm 2.

Algorithm 2: Decryption algorithm

Input: Cipher Image (D) of size (512,512), k1, k2

```
Start
Read cipher image (D) of size 512 x 512.
C1= XOR (D, k2')
    [~, k3] = sort(k1)
     b = C1
 for j = 1 to 512 × 512
    b = C1(k3(j))
 end
    I = reshape(b, 512,512)
Stop
```

Output: Plain image(I) of size (512,512)

4 Experimental results

The experimental results have been provided in this section. The test images used to validate the proposed algorithm are shown in Fig. 1. Several experiments were carried on the test images to validate the proposed encryption scheme. The experiments have been carried on MATLAB 2015a, a 64-bit Windows 10 Operating system with an intel core i5 processor, 4 GB RAM, and 2 GHz clock speed. To validate the proposed encryption scheme, Peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), NPCR, UACI, and Entropy have been used.

Moreover, the key sensitivity test and correlation coefficients analysis has also been performed. The computational time taken by the proposed encryption scheme has been given in this section. The experiments have been carried on the test images of size 512 × 512. Figure 2(a) shows the original images, Fig. 2(b) shows the encrypted images, and Fig. 2(c) shows the decrypted images.

4.1 Analysis of the encrypted image quality

PSNR and SSIM have been used to measure the encrypted image quality [16]. Here, the original image is the reference. Table 1 shows the comparative analysis of the PSNR and SSIM results for the images encrypted with the proposed scheme. The encryption algorithm is said to have a good performance if the PSNR and SSIM values are less than 10 and close to zero, respectively. The smaller the PSNR value, the greater is the difference between the original and the encrypted images. From Table 1, it is evident that the PSNR values are less than 10 dB and SSIM values are close to zero, which implies that the encrypted images have very low quality. Thus, predicting the original image from the encrypted image is difficult.

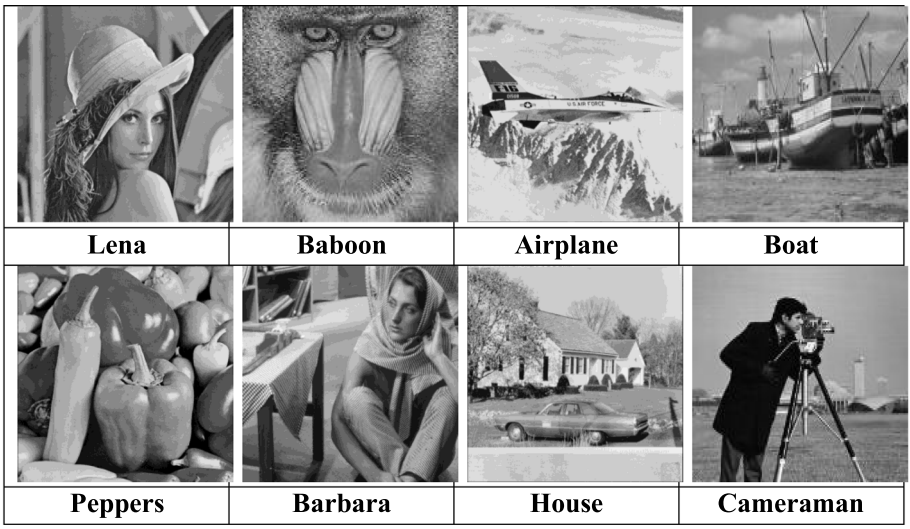

Fig. 1 Test images

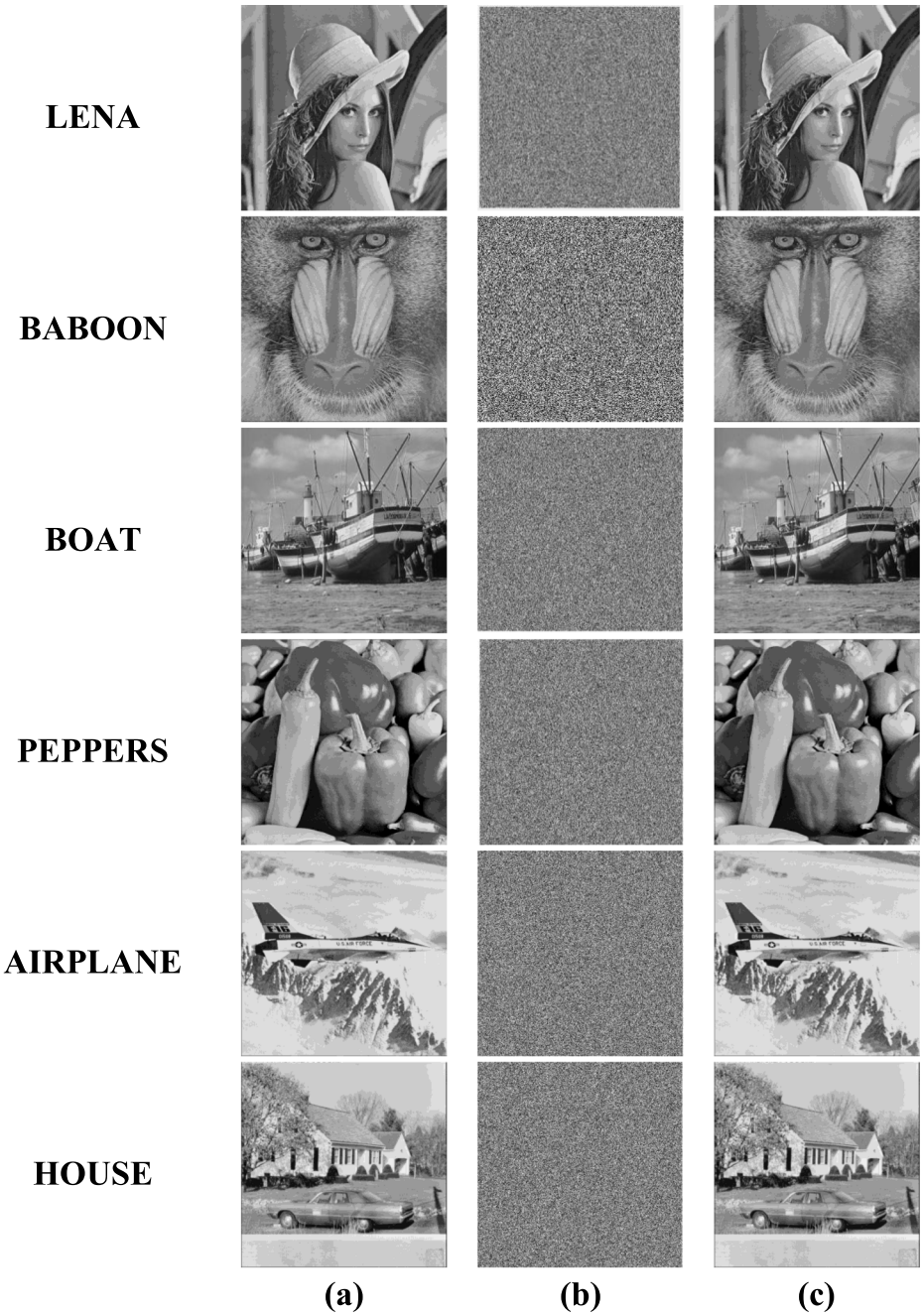

Fig. 2 (**a**) Original image, (**b**) encrypted image, (**c**) decrypted image

Table 1 PSNR and SSIM values of the encrypted image

Image	PSNR (dB)	[39]	SSIM
Lena (512×512)	9.21	9.239	0.0102
Baboon	9.82	9.520	0.0130
Boat	9.30	–	0.0098
Barbara	8.81	–	0.0095
Peppers	8.85	8.880	0.0087
House	8.65	–	0.0102
Boat	9.30	–	0.0098
Airplane	8.64	–	0.0101

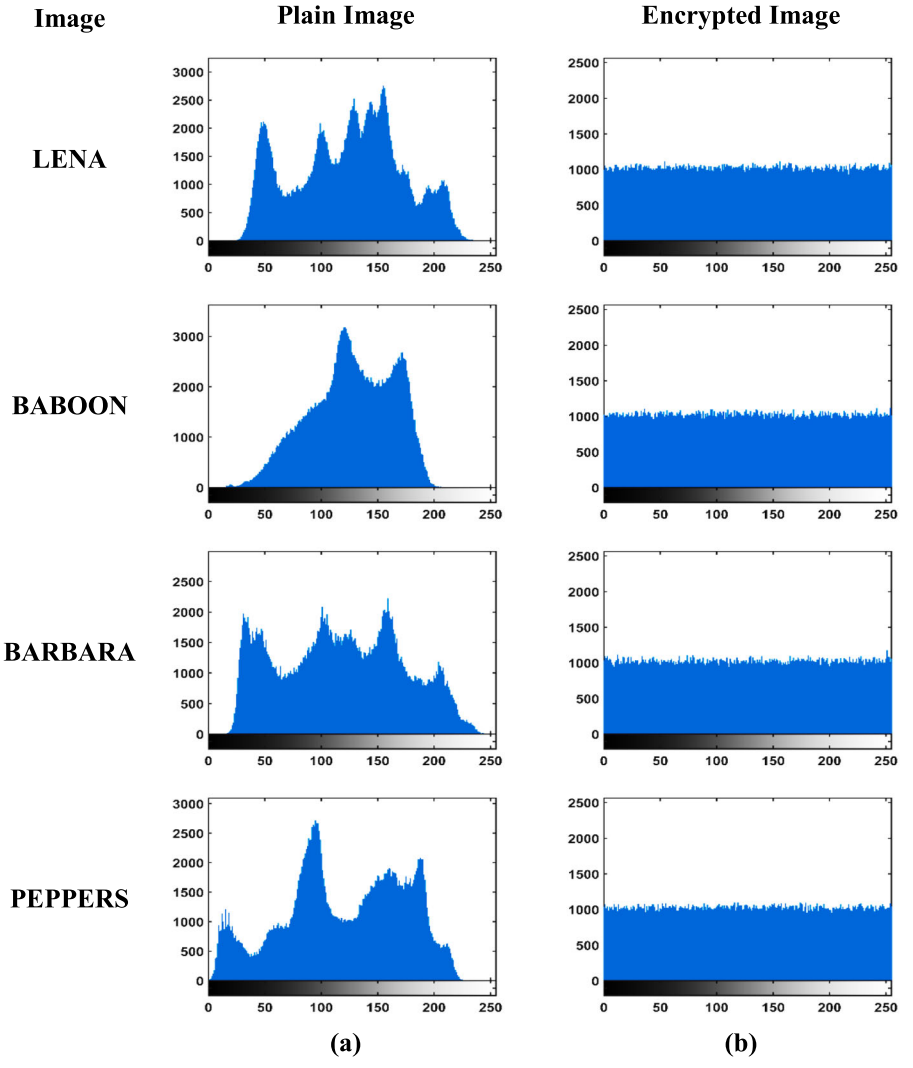

Fig. 3 (**a**) Histogram of plain image (**b**) histogram of the encrypted image

4.2 Statistical analysis

The statistical analysis includes entropy analysis, histogram analysis, and correlation coefficient analysis.

i Histogram Analysis

The histogram illustrates the pixel value distribution in an image. For a good encryption scheme, the histogram of the cipher image should be flat and should be different from that of the original image so that no information about the plain image is leaked. The x-axis gives the value of the pixel, and the y-axis gives the sum of all the pixel values. Figure 3(a) shows the histogram of the plain images and Fig. 3(b) shows the histogram of encrypted images. From Fig. 3, it can be seen that the histograms of the encrypted images are flat, uniform, and different from that of plain images. This means there is no leakage of information and thus is secure against statistical attacks.

ii Correlation Coefficient Analysis

The degree of correlation among adjoining pixels is given by the correlation coefficient. The value of the correlation coefficient should be low for a good encryption scheme. A positive correlation coefficient means that when one value increases or decreases, another also increases or decreases, a negative correlation coefficient indicates that as one value increases, another value decreases. When the correlation coefficient is zero, it implies that there is no correlation among the adjacent pixels. The correlation coefficient is stated in Eq. (13).

$$r = \frac{S\sum I_1\overline{I_1}\ (\sum I_1)\left(\sum \overline{I_1}\right)}{S\left(\sum {I_1}^2\right) + \left(\sum I_1\right)^2 \sqrt{N\left(\overline{{I_1}^2}\right) + \left(\sum \overline{I_1}\right)^2}} \tag{13}$$

where S is the size of the image and $\overline{I_1}$ and I_1 are the adjacent pixels of the image and the gray levels of the original image, respectively. From Table 2, it can be seen that the correlation between adjacent pixels of the images has been greatly reduced after encryption using the proposed scheme and is nearly equal to zero. Table 3 shows the correlation coefficient comparison of the proposed scheme for images of size 512 × 512 with recent schemes. It can be seen from the table that the values of correlation coefficients in horizontal, vertical, and

Table 2 Correlation coefficients of adjacent pixels

Image	Cipher image		
	Vertical	Diagonal	Horizontal
Lena	−0.0015	−4.6225e-04	−0.0023
Baboon	−0.0013	−5.3112e-04	0.0014
Boat	−0.0046	−8.8442e-05	3.8583e-04
Barbara	−0.0015	0.0027	0.0011
Peppers	−9.1885e-04	0.0019	−9.4816e-04
House	4.6688e-04	−0.0013	0.0041
Airplane	0.0035	−0.0013	−1.4613e-04
Cameraman	−0.0024	3.1390e-04	−0.0031

Table 3 Comparative analysis of Correlation coefficients for encrypted Lena image

Scheme	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Proposed scheme	−0.0015	−4.6225e-04	−0.0023
[31]	0.0008	0.0004	0.002
[18]	0.0250	0.0116	0.0025
[17]	0.0019	0.0690	0.0200
[15]	0.0015	−0.0090	−0.0120
[25]	−7.42e-04	0.0019	−0.043
[5]	−0.0091	−0.0198	−0.0062

diagonal directions are better than all other recent schemes. The work presented in [25, 31] has better horizontal direction results, but our values of correlation coefficients of the vertical and diagonal directions are much better. This implies our scheme is overall better than these two references also. Thus, it concludes that the proposed scheme has much better performance. Figure 4(a) shows the correlation plot of the plain Lena image and Fig. 4(b) shows the correlation plot of the encrypted Lena image.

iii Entropy attack analysis

Entropy is used to measure the quality of the encryption algorithm. It illustrates the distribution of gray levels in an image. It is difficult for invaders to predict a plain image from a cipher image with high entropy value. Equation (14) states the Entropy.

$$H(U) = \sum_{i=0}^{255} p\Big((u_i)\log_2\ p(u_i) \tag{14}$$

where $p(u_i)$ gives the frequency of the element (u_i). The ideal value of Entropy for a grayscale image is 8. Table 4 shows the comparative entropy analysis of different images using the proposed encryption scheme. The proposed encryption scheme is good because the value of Entropy for all encrypted images is very close to the ideal value 8. The entropy values of the proposed encryption scheme are comparable with the schemes presented in [13, 31] and better

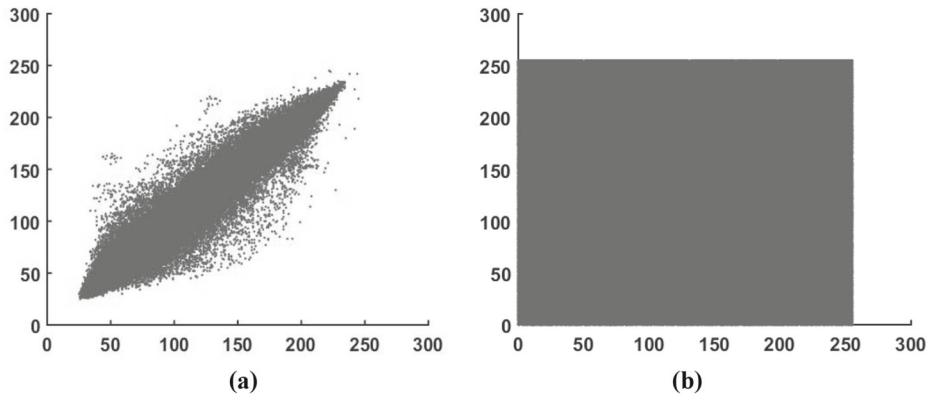

Fig. 4 (a) Correlation coefficient plots

than the schemes presented in [6, 17, 18]. This implies that the proposed encryption scheme can resist entropy attacks and is better than other state-of-the-art schemes.

4.3 Keyspace analysis

The total keyspace includes secret keys P, u, v, w, s, a, and b. The keys u, v, s, and w, have a precision of 15 bits. So, the total keyspace will be $(10^{15})^4 = 10^{60}$ which is greater than 10^{40}, which is the minimum keyspace for a good encryption scheme. This implies the proposed scheme has better performance in terms of keyspace as well.

4.4 Key sensitivity test

A good cryptosystem should be very sensitive to the changes in preliminary conditions. A small change in initial values should result in a huge change in the decrypted image. To validate the key sensitivity analysis, the encrypted image is decrypted with the incorrect key w = 0.757891552279989 instead of the correct key w = 0.757891552279999. The key differs in just one decimal place and still results in a completely noisy image. This implies that the keys are very sensitive. Figure 5 shows the key sensitivity test. Figure 5(a) shows the original image, Fig. 5(b) shows the encrypted image, Fig. 5(c) shows the decrypted image with the wrong key, and Fig. 5(d) shows the decrypted image with the correct key. From Fig. 5(c), it can be seen that the decrypted image is entirely different from the original image. The correct value of key "w" will recover the original image. Other secret keys are also sensitive to the change in keys.

4.5 Differential attack analysis

In differential cryptanalysis, one of the plaintext image (P1) pixels is modified to obtain another image, say (P2), by an attacker. Then both the plaintext images are encrypted using the same secret keys to obtain two encrypted images (C1) and (C2). The attacker then observes the relationship between the plain and encrypted images to guess the keys. A good image cryptosystem should resist the differential attack, which implies that the cipher image obtained by changing one pixel of the plain image should be completely different from the original encrypted image [37].

NPCR and UACI are calculated as shown in Eqs. (15) and (16).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{15}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|I_1(i,j) - I_2(i,j)|}{255}\right] \times 100\% \tag{16}$$

Where,

$$D(i,j) = \begin{cases} 1 \ if \ I_1(i,j) \neq I_2(i,j), \\ 0 \ otherwise \end{cases}$$

Table 4 Entropy comparative analysis

Image	Proposed	[31]	[6]	[18]	[17]	[13]	[15]
Lena	7.9993	7.9993	7.9995	7.9976	7.9993	7.9996	7.9939
Baboon	7.9993	7.9993	7.9974	7.9974	7.9992	7.999	7.9866
Boat	7.9994	7.9993	–	–	7.9992	7.9993	–
Barbara	7.9992	7.9994	7.9991	–	–	–	–
Peppers	7.9994	7.9998	7.9889	7.9971	7.9992	7.9996	7.9894
Airplane	7.9992	–	–	7.9971	7.9993	7.9993	–
House	7.9993	–	–	–	–	–	–
Cameraman	7.9994	–	–	–	–	–	–

I_1represents the encrypted image, and I_2 represents the encrypted image changed by one pixel, and the height and width of the images are denoted by W and H, respectively. The ability to resist diffusion attacks can be measured using NPCR and UACI.

Table 5 shows the comparative analysis of NPCR, and Table 6 shows the comparative analysis of UACI for natural images of size 512 × 512. Tables 5 and 6 show that the NPCR values are higher than the ideal value of 99.6%, and the UACI values are greater than the ideal value of 33.3%, making the proposed encryption scheme secure. The scheme [31] has NPCR values higher than our proposed encryption scheme, but the UACI values of this scheme are less than the ideal value of 33%, and the UACI values for all our encrypted images are greater than 33%. This implies proposed encryption scheme is better than [31] also. The NPCR values of the proposed encryption are better than the schemes [6, 13, 15, 17, 18, 28]. This establishes that the scheme can withstand differential attacks and is better than the state-of-the-art schemes.

4.6 Robustness analysis

We check the robustness of the proposed encryption scheme by attacking the encrypted image with noise and data loss. The encryption scheme is said to have good performance if it can resist noise and data loss. We attack the encrypted Lena image by adding Gaussian noise and salt and pepper noise to it. Also, we check the robustness by polluting the baboon image with data loss. The proposed encryption scheme can efficiently restore the original image from the attacked encrypted image after decryption. Slight data is lost after the image is decrypted after data loss, but the image is still recognizable, and other information is not lost.

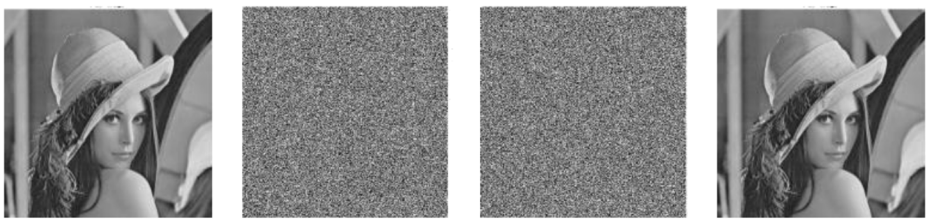

Fig. 5 Key sensitivity test: **a**) original image, **b**) encrypted image, **c**) decrypted image with the wrong key, **d**) decrypted image with the correct key

Table 5 NPCR test results for natural images

Image	Proposed	[31]	[6]	[28]	[18]	[17]	[13]	[15]
Lena (512×512)	99.6201	99.68	99.21	–	99.59	99.61	99.60	99.61
Baboon	99.6040	99.69	99.22	99.62	99.59	99.60	99.61	99.61
Boat	99.6231	99.70	–	–	99.60	99.61	–	–
Barbara	99.6262	99.97	99.22	–	–	–	–	–
Peppers	99.6143	99.69	99.21	99.60	99.61	99.58	99.60	99.60
House	99.6193	–	–	99.60	–	–	–	–
Cameraman	99.6025	–	–	99.58	–	–	–	–
Airplane	99.6170	99.66	99.61	–	99.61	99.60	–	–

4.6.1 Noise attack and data loss analysis

During transmission, noise may get added to the images. This noise can either be salt and pepper or gaussian noise. Also, some of the information may be get lost while the information is being transmitted through a public channel. So, a good encryption algorithm should be able to resist them, which means we should be able to recover the plain image from the noisy encrypted image.

The proposed algorithm has been tested against noise for the Lena image. Gaussian noise with variances of 0.01 and 0.1 is added to the encrypted images and then decrypted with the correct keys. Furthermore, the robustness of the proposed algorithm against salt and pepper noise with variances of 0.05 and 0.1 has been checked by measuring the values of PSNR and Mean Square Error (MSE). Assume X and Y denote the plain and decrypted images after the noise has been incorporated into the encrypted image. Equations (17) and (18) have been used to measure MSE and PSNR, respectively. Table 7 shows the noise attack analysis.

$$MSE = \frac{1}{M \times N} \sum_{i}^{M} \sum_{j}^{N} \left(X_{ij} - Y_{ij}\right)^2 \tag{17}$$

$$PSNR = 10 \times \log_{10} \frac{I^2}{MSE} \tag{18}$$

From the PSNR values calculated and shown in Table 7, it can be seen that the plain images and decrypted images are almost similar despite the noise that may have been added in the

Table 6 UACI comparison of the proposed encryption scheme

Image	Proposed	[31]	[6]	[28]	[18]	[17]	[13]	[15]
Lena (512×512)	33.4302	37.56	33.59	–	33.48	33.43	33.47	33.45
Baboon	33.4435	32.27	32.87	33.38	33.52	33.47	33.46	33.50
Boat	33.4523	31.89	–	–	33.47	33.46	–	–
Barbara	33.4859	34.60	31.60	–	–	–	–	–
Peppers	33.4407	30.80	33.67	33.51	33.55	33.40	33.46	3.41
House	33.3536	–	–	33.38	–	–	–	–
Cameraman	33.4209	–	–	33.45	–	–	–	–
Airplane	33.4916	32.78	32.53	–	33.43	33.45	–	–

Table 7 Noise attack analysis

Noise	MSE (proposed)	MSE [5]	PSNR (dB) (proposed)	PSNR (dB) [5]
Gaussian noise with variance=0.01 and mean=0	1967.6	2321	15.19	14.5
Gaussian noise with variance=0.1 and mean=0	4642.0	5201.2	11.46	11
Salt and pepper noise with density=0.05	383.6	437.9	22.29	21.7
Salt and pepper noise with density 0.1	780.9	893.1	19.20	18.6

channel. Figure 6 shows the results. Figure 6(a) shows the encrypted Lena image after adding Gaussian noise of variance 0.01, Fig. 6(b) shows the encrypted Lena image after adding Gaussian noise of variance 0.1, Fig. 6(c) shows the encrypted Lena image with variance 0.05, Fig. 6(d) shows the encrypted Lena image after adding variance of 0.1 and Fig. 6(e,f,g,h) show the respective decrypted images. Figure 7 shows the decryption results of data loss. Figure 7(a) shows the 1/16 cropping image and its decrypted image, Fig. 7(b) shows the 1/8 cropping image and its decrypted image, Fig. 7(c) shows the 1/4 cropping image and its decrypted image, and Fig. 7(d) shows the 1/2 cropping image and its decrypted image. Despite a part of the image being lost after the cropping attack, the images are still recognizable, and most information can be deduced from them. Table 8 shows the PSNR measurement results of decrypted images after data loss. It can be seen from the table that the PSNR values of our scheme are better than the other recent works. The data loss is shown on the baboon image.

4.7 Computational time analysis

To measure the execution time of the proposed scheme, several experiments have been carried on the Lena image of size 512 × 512. The system used to carry out these experiments is Intel core i5 CPU (2 GHz) and 4 GB of RAM and windows 10 pro (64-bit version) using MATLAB

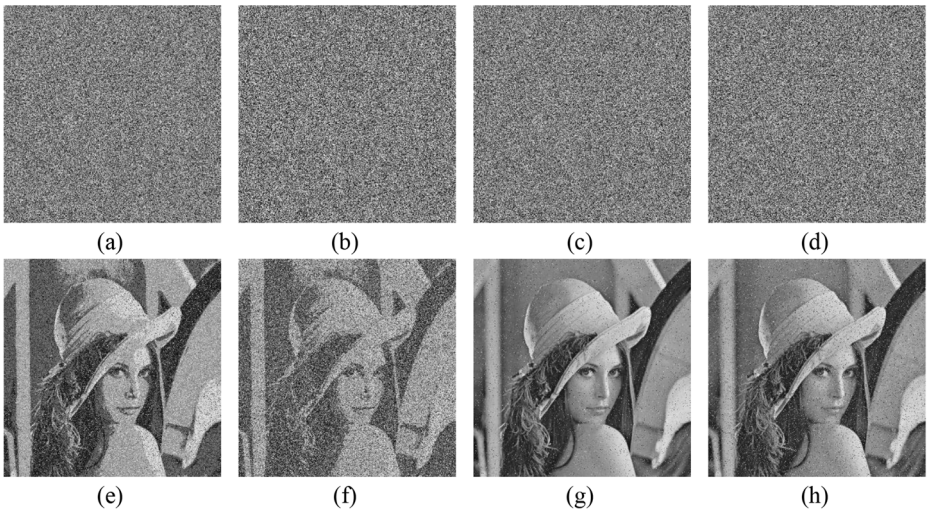

Fig. 6 (**a**, **b**, **c**, **d**) Encrypted images after adding Gaussian and salt and pepper noise, (**e**, **f**, **g**, **h**) images decrypted images after using correct secret keys

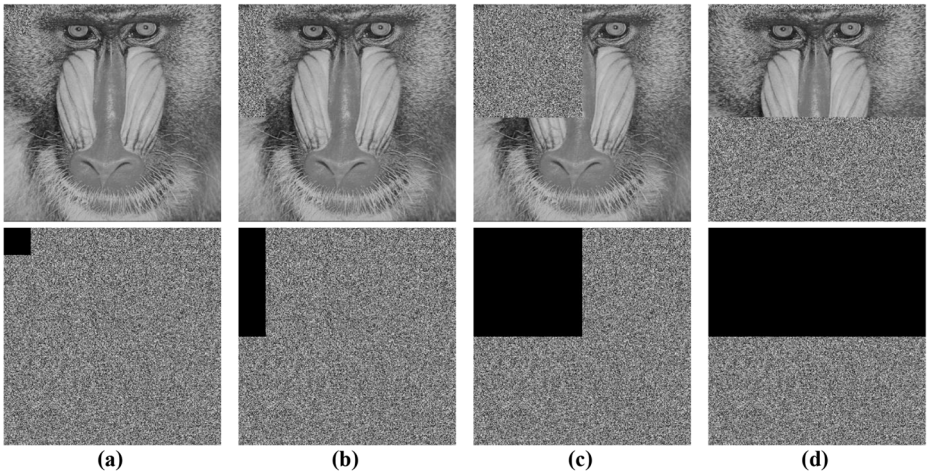

Fig. 7 Decryption results of data loss (**a**) 1/16 cropping image and its decrypted image, (**b**) 1/8 cropping image and its decrypted image, (**c**) 1/4 cropping image and its decrypted image, and (**d**) 1/2 cropping image and its decrypted image

Table 8 PSNR result of the decrypted image after data loss

Algorithm	Cipher image polluted by data loss of			
	1/16	1/8	1/4	1/2
Proposed	27.78	21.54	15.62	12.93
[13]	21.54	18.21	15.37	12.73
[15]	–	18.20	15.22	12.23

R2015b programming language. Table 9 shows the comparative analysis of computational time. From the comparative analysis of the proposed scheme with other state-of-the-art schemes, it is evident that it has a very small encryption time compared to other recent works (Fig. 8).

5 Conclusion

A new adaptive image encryption scheme based on simple chaotic maps has been proposed in this paper. The PRN sequences have been obtained from the Henon map and Quadratic map. The encryption time has been reduced because the shuffling and diffusion process is carried on pixels directly rather than bits. The proposed encryption scheme uses less complex chaotic maps. The experimental results carried on natural images prove the robustness and security

Table 9 Computational time analysis for proposed encryption scheme

Image	Proposed	[31]	[15]	[25]	[44]
Lena	0.25	3.007	1.43	0.46	1.708

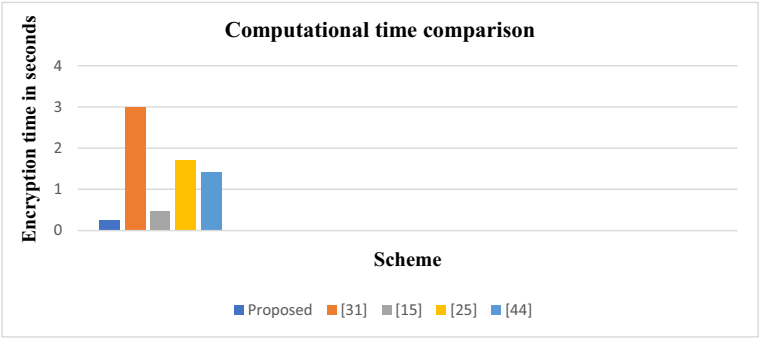

Fig. 8 Computational time comparison

level provided. The experiments show that the encryption scheme can resist statistical attacks and entropy attacks. Also, the correlation coefficients in all three directions, i.e., vertical, diagonal, and horizontal, are close to zero. The proposed encryption scheme is a one-round encryption scheme. The comparisons of the proposed scheme with other recent techniques prove the efficiency of the scheme. The computational time analysis shows that it takes only 0.25 s to encrypt an image of size 512 × 512. The possible applications of the proposed algorithm are in Internet of things (IoT) scenarios and real-time applications because of its fast speed and less computational complexity.

Acknowledgments The authors would like to thank the Department of Science and Technology (DST) New Delhi, Government of India for providing financial support under the DST Inspire Fellowship Scheme.

Declarations

Conflict of interest The authors of this paper do not have any conflict of interest.

References

1. Abdelfatah RI, Nasr ME, Alsharqawy MA (2020) Encryption for multimedia based on chaotic map: several scenarios. Multimed Tools Appl 79:19717–19738
2. Alsmirat MA, Al-Alem F, Al-Ayyoub M (2019) Impact of digital fingerprint image quality on the fingerprint recognition accuracy. Multimed Tools Appl 78:3649–3688
3. AlZu'bi S, Shehab MA, Al-Ayyoub M, Jararweh Y, Gupta B (2020) Parallel implementation for 3D medical volume fuzzy segmentation. Pattern Recogn Lett 130:312–318
4. Arab M, Rostami MJ, Ghavami B (2019) An image encryption method based on chaos system and AES algorithm. J Supercomput 75:6663–6682
5. Askar S, Karawia A, Khedhairi A, Ammar FS (2019) An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. Entropy 21(1):44
6. Bhaskar M, Behera P, Sugata G (2021) A secure image encryption scheme based on a novel 2D sine–cosinecross-chaotic(SC3) map. J Real-Time Image Proc 18:1–18
7. Chai X, Zhang J, Gan Z (2019) Medical image encryption algorithm based on Latin square and memristive chaotic system. Multimed Tools Appl 78:35419–35453
8. Chatterjee A, Dhanotia J, Bhatia V, Rana S, Prakash S (2017) Optical image encryption using fringe projection profilometry, Fourier fringe analysis, and RSA algorithm. In Proc. 14th IEEE India Council Int. Conf. (INDICON), pp 1–5
9. Chenghai L, Fangzheng Z, Liu C, Lei L, Zhang J (2019) A Hyperchaotic Color Image Encryption Algorithm and Security Analysis, *Security and Communication Networks*, vol. 2019, Article ID 8132547, 8 pages. https://doi.org/10.1155/2019/8132547

10. Darwish SM (2019) A modified image selective encryption-compression technique based on 3D chaotic maps and arithmetic coding. Multimed Tools Appl 78:19229–19252
11. Ferdush J, Begum M, Shorif Uddin M (2021) Chaotic lightweight cryptosystem for image encryption. Adv Multimed 2021:Article ID 5527295, 16 pages
12. Gayathri V (2016) A survey on security and efficiency issues in chaotic image encryption. Int J Inf Comput Secur 8(4):347–381
13. Ge B, Chen X, Chen G, Shen Z (2021) Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation. IEEE Access 9:137635–137654
14. Gopalakrishnan T, Ramakrishnan S (2019) Image encryption using a hyperchaotic map for permutation and diffusion by multiple hyper-chaotic maps. Wirel Pers Commun 109(1):437–454
15. Gupta MD, Chauhan RK (2021) Secure image encryption scheme using 4D-hyperchaotic systems based reconfigurable pseudo-random number generator and S-box. Integration 81:137–159
16. Hore A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. In: 2010 20th International Conference on Pattern Recognition, IEEE, pp 2366–2369
17. Hosny KM, Kamal ST, Darwish MM, Papakostas GA (2021) New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix. Electronics 10:1066. https://doi.org/10.3390/electronics10091066
18. Hua Z, Zhou Y, Huang H (2019) Cosine-transform-based chaotic system for image encryption. Inf Sci 480:403–419
19. Huang I, Wang S, Xiang J, Sun Y (2020) Chaotic color image encryption scheme using deoxyribonucleic acid (DNA) coding calculations and arithmetic over the Galois field. Math Probl Eng 2020:1–22
20. Idrees B, Zafa S, Rashid T (2020) Image encryption algorithm using S-box and dynamic Hénon bit-level permutation. Multimed Tools Appl 79:6135–6162
21. Islam N, Shahid Z, Puech W (2016) Denoising and error correction in noisy AES-encrypted images using statistical measures. Signal Process Image Commun 41:15–27
22. Khan JS, Ahmad J (2019) Chaos-based efficient selective image encryption. Multidim Syst Sign Process 30:943–961
23. Khan M, Ahmad J, Javaid Q, Saqib NA (2016) An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps, and substitution box. J Mod Opt 64:1–10
24. Kulsoom A, Xiao D, Rehman A (2016) An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. Multimed Tools Appl 75:1–23
25. Li T, Du B, Liang X (2020) Image encryption algorithm based on logistic and two-dimensional Lorenz. IEEE Access 8:13792–13805
26. Li Z, Peng C, Tan W, Li L (2021) An effective chaos-based image encryption scheme using imitating Jigsaw method. Complexity 2021:Article ID 8824915, 18 pages. https://doi.org/10.1155/2021/8824915
27. Lin CY, Wu JL (2020) Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintexts related permutation and diffusion. Entropy 22(5):589
28. Liu D, Zhang W, Yu H (2018) An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion. Signal Process 151. https://doi.org/10.1016/j.sigpro.2018.05.008
29. Matthews R (1989) On the derivation of a 'chaotic' encryption algorithm. Cryptologia 13(1):29–42
30. Mishra K, Saharan R (2019) A fast image encryption technique using Henon chaotic map. Proceedings of ICACIE 2017, vol. 1
31. Mondal B, Singh S (2019) A secure image encryption scheme based on cellular automata and chaotic skew tent map. J Inf Secur Appl 45:117–130
32. Ramadan N, Hossam E, Said E, Fathi E (2016) Chaos-based image encryption using an improved quadratic chaotic map. Am J Signal Proc 6(1):1–13
33. Ramasamy P, Ranganathan V, Kadry S, Damasevicius R, Blazauskas T (2019) An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—tent map. Entropy 21:656
34. Tang Z, Yang Y, Xu S, Yu C, Zhang X (2019) Image encryption with double spiral scans and chaotic maps. Secur Commun Netw 2019:1–15
35. Tian J, Lu Y, Zuo X (2021) A novel image encryption algorithm using PWLCM map-based CML chaotic system and dynamic DNA encryption. Multimed Tools Appl 80:32841–32861
36. Wang H, Li Z, Li Y, Gupta B, Choi C (2020) Visual saliency guided complex image retrieval. Pattern Recogn Lett 130:64–72
37. Wu Y, Noonan JP, Agaian S (2011) Npcr and uaci randomness tests for image encryption. Cyber J Multidiscip J Sci Technol J Sel Areas Telecommun (JSAT) 1(2):31–38
38. Yan X, Wang X, Xian Y (2021) Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. Multimed Tools Appl 80:10949–10983

39. Yasser I, Khalifa F, Mohamed A, Samrah AS (2020) A New Image Encryption Scheme based on Hybrid Chaotic Maps", *Complexity*, vol. 2020, Article ID 9597619, 23 pages, 2020. https://doi.org/10.1155/2020/9597619
40. Yu C, Li J, Li X (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos, and computer-generated hologram. Multimed Tools Appl 77:4585–4608
41. Zhan P, Xie X (2018) Implementation of DES and AES algorithms and their efficiency in image encryption. Netw Secure Technol Appl 9:41–42
42. Zhang X, Feng H, Ying N (2017) Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding. Comput Intell Neurosci 2017:1–11
43. Zhu S, Zhu C (2020) Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. Entropy (Basel) 22(7):772
44. Zhu S, Wang G, Zhu C (2019) A secure and fast image encryption scheme based on double chaotic S-boxes. Entropy 21(8):790