Complex & Intelligent Systems (2021) 7:2751–2764
https://doi.org/10.1007/s40747-021-00460-4

ORIGINAL ARTICLE

An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial

Majid Khan[1] · Ammar S. Alanazi[2] · Lal Said Khan[3] · Iqtadar Hussain[4]

Received: 3 April 2021 / Accepted: 3 July 2021 / Published online: 13 July 2021

Abstract

The security of digital content during transmission and storage through insecure communication links and databases is a challenging issue in today's world. In this article, an encryption scheme based on fractal Tromino and Chebyshev polynomial-based generated chaotic matrix is presented. The scheme fulfills the most fundamental aspect of encryption that is diffusion and confusion. For confusion highly non-linear, pre-defined S-boxes are used. The proposed scheme has been tested using state-of-the-art key performance indicators including differential analysis, statistical analysis. Information entropy analysis, mean square error, and NIST-based randomness analysis. The encrypted images have the highest practically achievable entropy of 7.999 and the time analysis shows that the proposed system is suitable for real-time implementation. The rest of the results indicates that the proposed cryptosystem possesses high immunity toward various attacks. The security analysis compared with the existing scheme shows the strength of the suggested scheme.

Keywords Chebyshev polynomials · Fractal Tromino · Image encryption

Introduction

In this modern era of technology, the transmission and storage of multimedia content grow rapidly. The security and privacy of these contents have been an unavoidable subject of research for the last few decades. One of the main issues in this era of fifth-generation communication is the privacy of digital content [1]. In different databases, the information is stored, and travel in the form of bits, this information includes digital images, audio, video, etc., and available to different users through the Internet. The databases can be accessed by an unauthorized user and the information can be stolen and misused if the databases are secure enough that the intruder cannot access this database, then will monitor the traffic, and can steal information during communication from the database to the authorized user. The information needs security during storage as well as the transmission phase, so that if the intruder gets that information, it will have no use for her. The science of securing information is called cryptography. Cryptography is traditionally referred to as the science of secrecy, although the concept of cryptography is more closely related to it today. Encryption is the act of converting "unhidden" plain text to "hidden" to guard it against data intruders. There is another aspect of this phase where the hided text desires to be decrypted to be understood at the other end. In our everyday lives, the use of cryptography is everywhere. We use it, for instance, to easily submit passwords through large networks for online transactions. Bank servers and email clients also use encryption to preserve their passwords. The authentication of all communicated information in our IoT-related world is encrypted and authenticated by cryptography. Cryptography can be categorized as symmetric and asymmetric key cryptography. In symmetric-key cryptography, the keys for encryption and decryption are the same. The encryption comprises of diffusion and confusion. Guidelines for a reasonable level of safety and the utmost adequate characteristics of a cryptosystem are presented in [2]. The recommended guidelines report three foremost concerns: implementation, key management,

✉ Majid Khan
mk.cfd1@gmail.com

1 Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan

2 King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia

3 Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

4 Department of Mathematics, Statistics and Physics, Qatar University, 2713 Doha, Qatar

and security analysis. A comprehensive revision of various cryptosystems design techniques and development in meta-heuristic-based image encryption is presented in [3]; the numerous attacks and evaluation of results allied to cryptosystem have also been presented. Most of the researchers [4, 5] utilize chaos base generated sequences for the diffusion process, and due to extraordinary sensitivity to initial conditions, the use of chaos is widespread in cryptography [6–8]. Particle swarm optimization, based confusion, and chaotic map-based diffusion are presented in [9]. Fractals accompanied with chaotic maps have been also widely used in cryptography [10]. A lot of work has been done in the field of cryptography [11] discrete and continuous chaotic maps are utilized by the work presented in [12]. To add more diffusion in the cryptosystem fractals and multiple chaotic maps are utilized in [13]. For the deployment of the encryption scheme in different environments, several alterations have been done in the design of cryptosystems [14–16]. Chebyshev polynomial-based chaos has been utilized for image encryption [17]. Various transform like discrete cosine transform [18] and wavelet transform have also been utilized for image encryption [19, 20]. The encryption system can be broadly classified as classic and modern cryptosystems, in classic cryptosystems, the process of diffusion or confusion is done, one at a time while in modern cryptosystems, both confusion and diffusion are performed. Only confusion can be easily broken [21]. The work presented in [22] uses only confusion and can be easily decrypted the procedure in [21]. It is shown [21] that encryption by solitary S-box, which is the essential part of AES and DES, is not sufficient. A privacy-preserving data aggregation scheme with a flexibility property that uses ElGamal is presented in [23]. A secure and efficient mutual authentication protocol for smart grid under grid is proposed in [24].

In this article, we have utilized Chebyshev polynomial and fractal Tromino accompanied by pre-defined highly nonlinear S-boxes to encrypt the secret images. Reducing computational complexity without affecting the security strength of a cryptosystem is important for real-time implementation. AES has excellent security, but when it came to implementation on images, it takes more time. Due to their uttermost simplicity in implementation and less computational complexity, the computed time for encryption makes this scheme suitable for real-time implementation. The reason for less time is the use of pre-defined S-boxes and less computational complexity of Chebyshev polynomial and fractal Tromino. The security analysis is performed and tabulated which reveals the strength of the cryptosystem to different cryptographic attacks. The remaining of the manuscript is arranged as the discussion of the different basics concepts and procedure are described in section two of the article, the step includes in the encryption process, and the explanation and flow diagram of the proposed cryptosystem is discussed in section three of the paper and to validate the strength and immunity to various attacks, the security analysis is computed and displayed in section four of the article, and finally, conclusion is drawn in Sect. 5 of the paper.

Preliminaries

This segment is dedicated to the discussion of basics utilized in the proposed cryptosystem.

Generation of fractal Tromino

The fractal Tromino is generated using the succeeding steps.

Step 1: A matrix R of dimension M × 3 N is created where M × N × 3 is the dimension of the plain image.

Step 2: two random keys k_1 and k_2 are created; each key has a length of 8-bits.

Step 3: The values of the Matrix generated in step 1 are updated using the following rule in Eq. (1):

$$R(i,j) = \begin{cases} \text{mod}(j,f) & \text{if mod } (i, k_2 \times c) < k_1 \times c \\ \text{mod}(i,f) & \text{if mod } (j, k_2 \times c) > k_1 \times c \\ \text{mod}(c-i,c) & \text{otherwisw} \end{cases}, \tag{1}$$

where c can be computed using relation in Eq. (2)

$$c = \sqrt{(255-m) \times m}. \tag{2}$$

The value of c is rounded to the nearest digit, where m in Eq. (2) is the mean of the matrix generated in step 1.

Step 4: The matrix updated as in step 3 is reshaped $M \times N \times 3$. This is desired fractal Tromino. The generated fractal is shown in Fig. 1, and part b displays the image after XORing with the fractal.

Chebyshev polynomial-based chaotic matrix generator

Chebyshev polynomial (CP) is a sequence of cosine-related polynomials. In this section based on CP, random sequences are created by utilizing [25] the two relations in Eq. (3)

$$\begin{aligned} p(k+1) &= T_n(p_k) = \cos(x \times \arccos(w_k)), \\ q(l+1) &= T_m(q_l) = \cos(y \times \arccos(q_l)), \end{aligned} \tag{3}$$

where the governing bounds for CP are $(p_k, q_l) \in [-1, 1]$ and $(l, k) \in [2, \infty]$. The following describes the rest of the algorithm.

Step 1: The starting values $p(0)q(0)$ and parameters (x, y) are initiated as a key.

Step 2: Eq. (3) is iterated $M \times N$ times, where $M \times N$ is the size of each layer of the plain image, and by doing

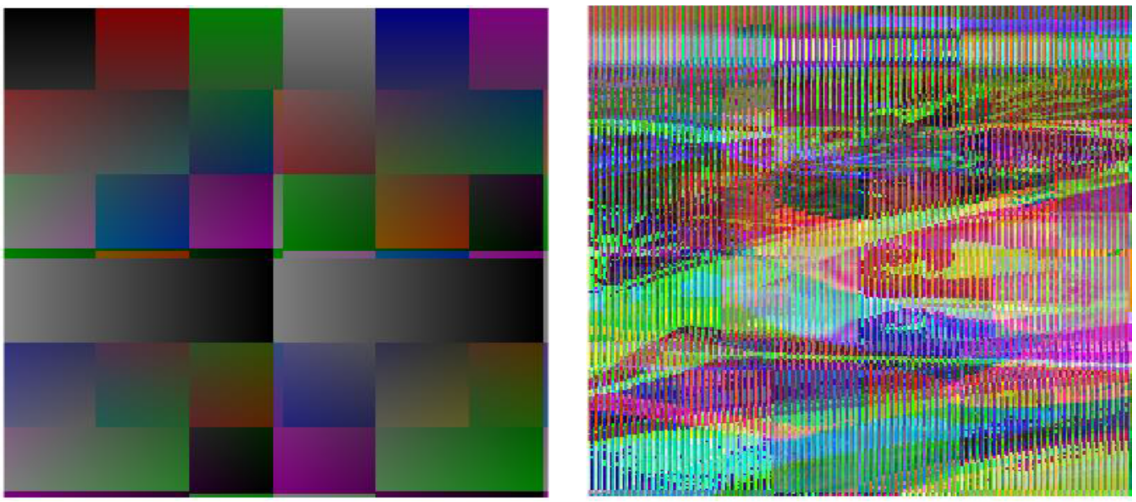

Fig. 1 **a** Generated fractal Tromino and **b** after XORing RGB Plain image with fractal

this, we have obtained two matrices containing the decimal fractional entries; these values are processed using Eq. (4)

$$p(k) = \mathrm{mod}(floor(abs(p(n) \times 10^{14})), r),$$
$$q(l) = \mathrm{mod}(floor(abs(q(m) \times 10^{14})), r), \quad (4)$$

where $r = 256$.

Step 3: These two matrices are XORed and a third matrix is obtained.

The chaotic matrix is converted into a row vector in and the first 200 iterations output are plotted, as shown in Fig. 2.

Substitution using S-boxes

In cryptography, an S-box is a core element of the symmetric-key system that accomplishes the substitution. To unclear the relationship, in the block cipher between the key and the ciphertext, S-boxes are utilized. The process of substitution is shown in Fig. 3. In our case, we have utilized the highly non-linear S-boxes generated by [26]. The pixel of the plain image is taken; after converting into binary, it is divided into MSBs and LSBs, again converted into decimal; the MSB converted decimal indicates column index of S-box and the other indicates the row of the S-box, and the intersected element is a substitute of the pixel in the ciphered image.

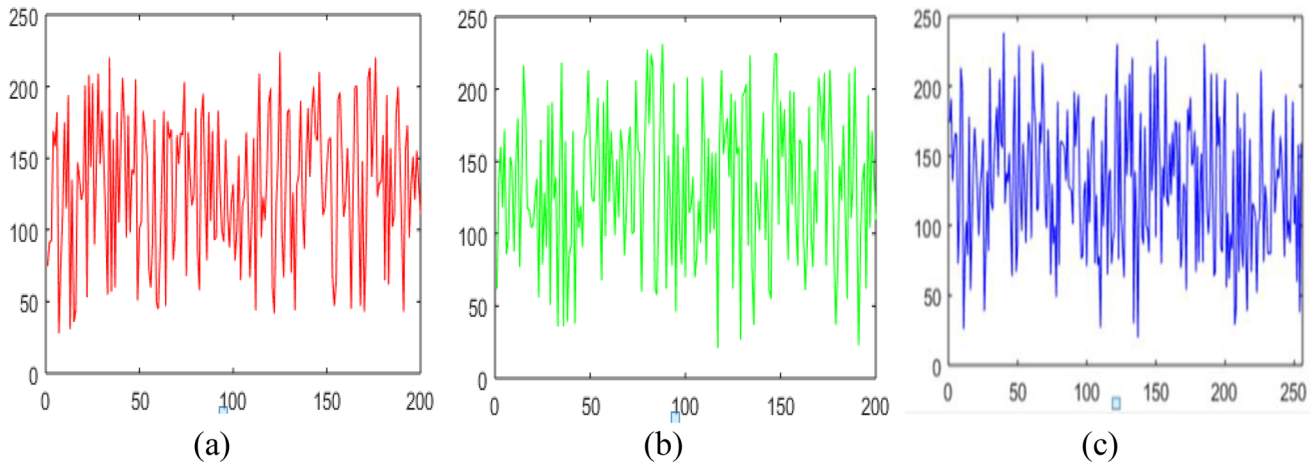

Fig. 2 First 200 iterations of the Chaotic Matrices generated using CPs

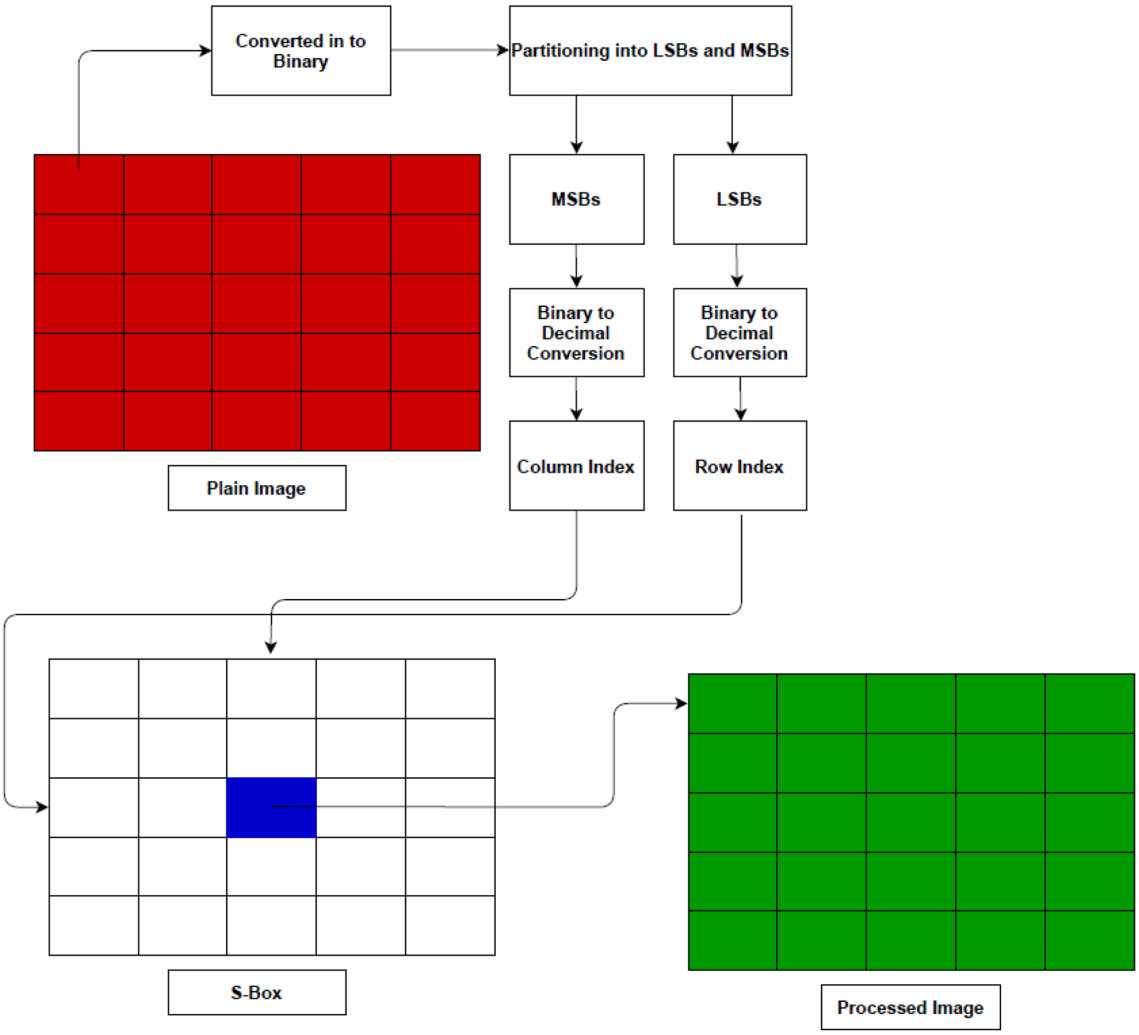

Fig. 3 The process of confusion addition through substitution

Proposed encryption scheme

The proposed encryption scheme can be implemented using the following steps. The procedure is depicted in Fig. 4.

Step 1: The secret color RGB image that needs to be enciphered is loaded and split into respective channels.

Step 2: Two keys K_1 and K_2 are initiated and L-shaped fractal Tromino is generated using the procedure in Sect. 2.1 of the article.

Step 3: The 3-fractal Tromino is XORed with the respective layers of the image.

Step 4: The parameters for CPs are initiated and chaotic matrices are generated using the procedure discussed in Sect. 2.2 of the article.

Step 5: The chaotic matrices obtained in step 4 are XORed with outcomes of step 3.

Step 6: The processed image layers obtained in step 5 are further passed through the process of substitution using the procedure discussed in Sect. 2.3 of the article.

Step 7: The three split layers of the image obtained in step 1 are encrypted till step 6; now the three layers are combined to achieve the concluding encrypted RGB image.

The procedure of encryption is presented in Fig. 4. The process of decryption is carried out using the reverse approach, but instead, in the substitution phase using the S-boxes, first, the inverse S-boxes are computed, and the process of substitution is carried out using the inverse S-boxes following the same procedure for substitution as discussed in Sect. 2.3. To estimate the effectiveness of the proposed encryption against various thread security analysis is carried out and discussed in the upcoming section of the paper.

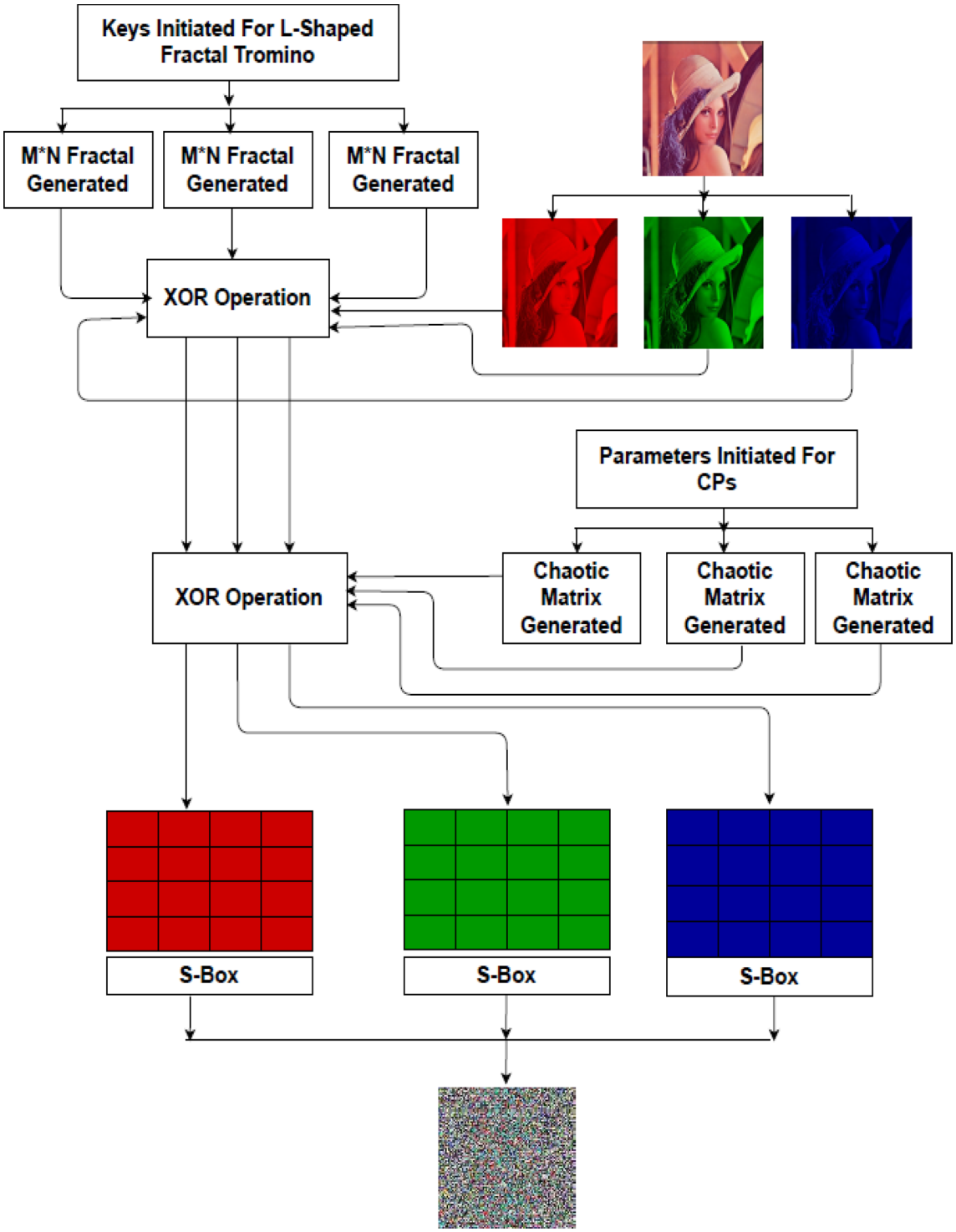

Fig. 4 Proposed encryption scheme

Security analysis

To evaluate the strength of the cryptosystem in contradiction of various cryptographic threads, the security analysis of the system is essential. Here, we have encrypted Lena, baboon, airplane, girl, and pepper images, and the following analysis was carried out to validate the strength of the proposed system. The size of the images utilized is $256 \times 256 \times 3$.

Differential analysis

To evaluate the immunity of the proposed cryptosystem to resist differential attacks, differential analysis is carried out. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are employed in the examination against differential attacks (DA). In DA, the intruder faintly changes the original image and encrypt that image then compares the originally encrypted and the modified encrypted images and tries to find information regarding the cryptosystem. The NPCR and UACI analysis are as described.

NPCR

In computing NPCR, one-pixel change in the plain image is done and comparing the modified encrypted and original image without modification is encrypted through the same encryption scheme and the percentage change in terms of pixel change rate is studied; for a good cryptosystem, the value of NPCR needs to high. The NPCR can be computed using the relation in Eq. (5)

$$NPCR = \frac{\sum_{a,b} D(a,b)}{M \times N}, \tag{5}$$

where

$$D(a,b) = \begin{cases} 0 \ if \ O(a,b) = O^{'}(a,b) \\ 1 \ if \ O(a,b) \neq O^{'}(a,b) \end{cases}, \tag{6}$$

where $M \times N$ is the dimension of images and O symbolizes the original image, O is the encrypted image after the one-pixel change. The NPCR value for a good cryptosystem needs to be near 100. The NPCR is computed and displayed in Table. 1. The results of NPCR show strong immunity toward differential attacks.

UACI

After one-pixel alteration in the plain image, the average alteration in intensity among the original image encrypted and the modified image encrypted is studied in UACI. It can be computed using Eq. (7)

$$UACI = \frac{\sum_{a,b} O(a,b) - O^{'}(a,b)}{255 \times M \times N}. \tag{7}$$

The values of UACI are computed for various images and tabulated as in Table 1. The computed value of NPCR is closest to the theoretically achievable value of 100 in each case, and comparison with the recently proposed encryption scheme is presented in Table 2. The graphs are shown in Fig. 5 from NPCR and UACI measurements we are confidently claiming that our proposed cryptosystem is secure against differential analysis.

Table 1 NPCR and UACI for (256×256×3) images, having a first alteration

Image	NPCR	UACI
Lena	**99.6393**	33.47
Peppers	99.610	33.46
Airplane	99.629	33.46
Baboon	99.6093	33.46

Statistical analysis

The statistical analysis can also be utilized in the cryptanalysis of an Encryption scheme. To confirm the robustness of encryption against statistical attacks, histograms, and correlation among adjacent pixels are utilized, to withstand the statistical analysis, the encrypted must have a uniform histogram and zero correlation among the adjacent pixels.

Histogram analysis

A graph displaying the occurrence of something is known as a histogram. Typically, the histogram has bars that reflect the frequency of data that occurs in the data collection as a whole. The histogram has two axes, the x-axis and the y-axis. The x-axis includes an occurrence whose frequency has to count. The y-axis has a frequency. Various bar heights indicate the different frequency of data occurrence. Figure 6, displays the histograms of both plaintext and ciphertext. It can be seen from Fig. 6 that the non-uniform histogram having more frequent pixels in the range 200–50 refers to Fig. 6a, i.e., some pixel's frequency is less as compared to the rest. While the histogram of the encrypted image has an equal count of occurrence of every pixel and the distribution is uniform. When the histogram of an image is uniform, it does not convey any beneficial statistics to the intruders. Keeping in view the histograms in Figs. 6 and 7, we are confidently claiming that the Proposed encryption scheme retains great immunity against attacks that utilize histogram examination.

Table 2 Comparison of NPCR and UACI for (256×256×3) Lena with existing techniques

Algorithm	NPCR	UACI
Ref. [27]	99.63	33.46
Ref. [28]	99.57	33.45
Ref. [29]	99.62	33.44
Ref. [30]	99.62	33.50
Proposed	99.64	33.47

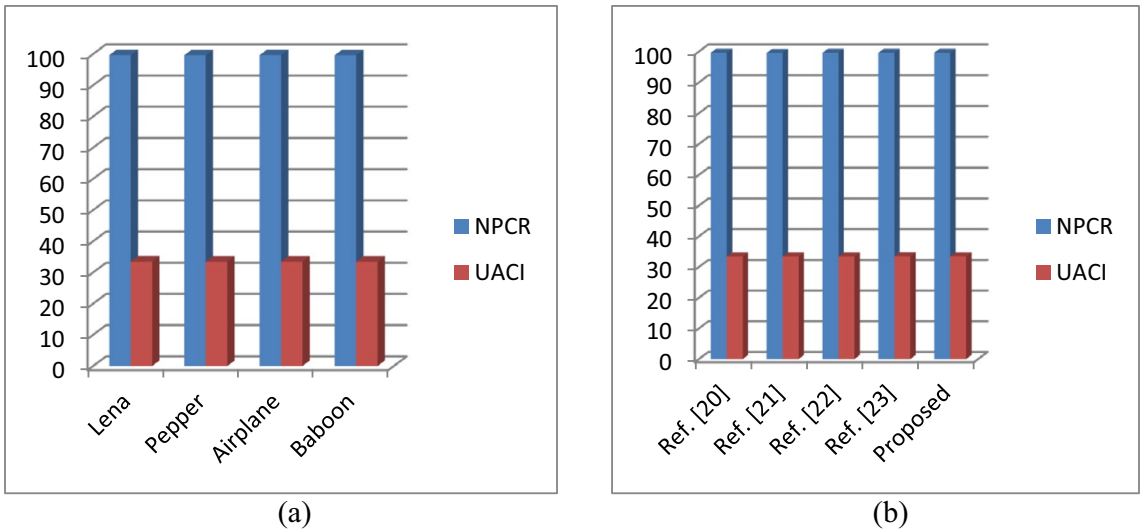

Fig. 5 Graph of NPCR and UACI for (256×256×3) images: **a** NPCR and UACI for Test images. **b** Comparison with recently suggested encryption systems

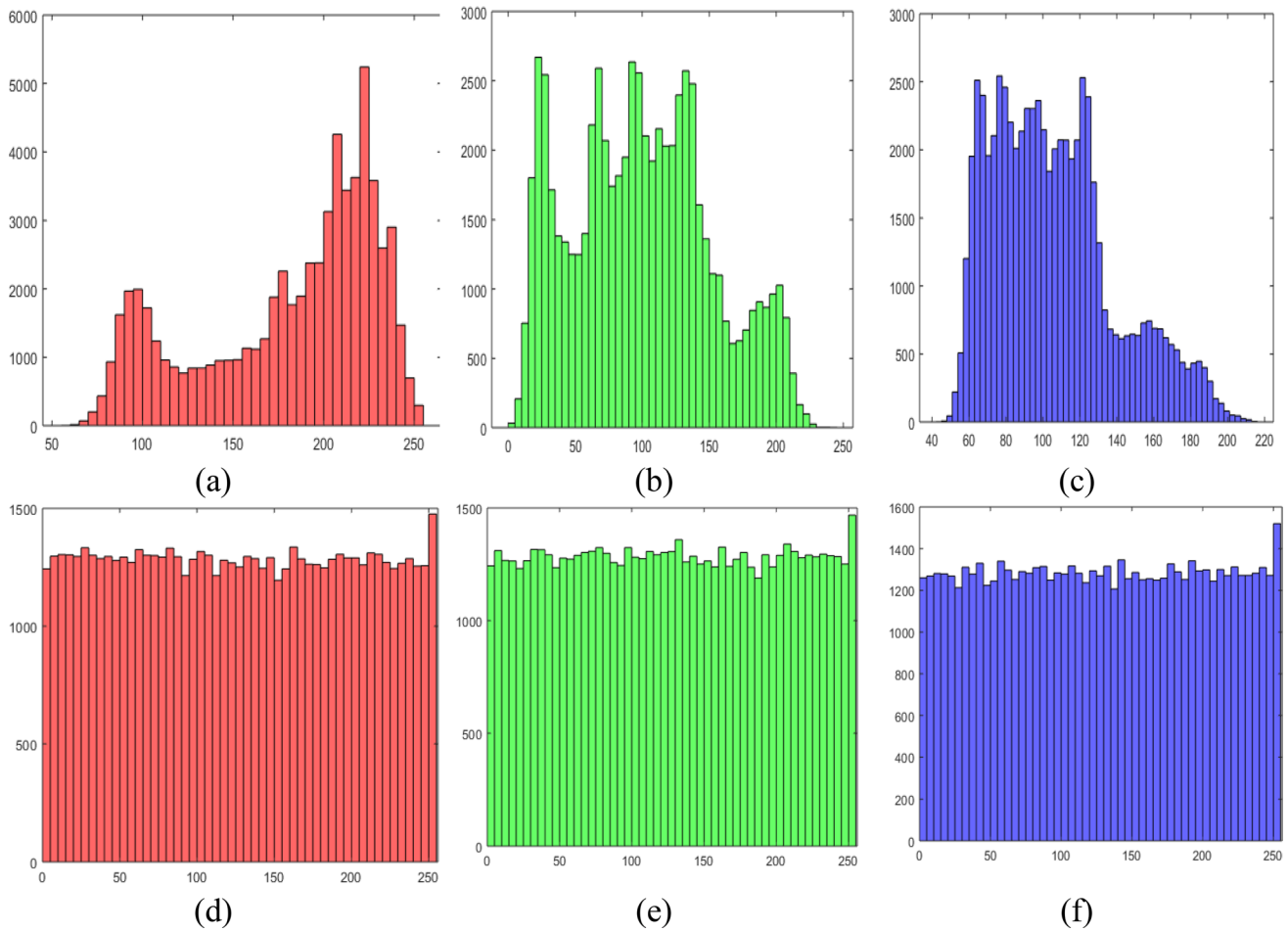

Fig. 6 Histogram analysis of plain and ciphered image layers. **a**–**c** Histogram of Red, Green, and Blue channels of plain image. **d**–**f** Histograms of encrypted red, green, and blue layers

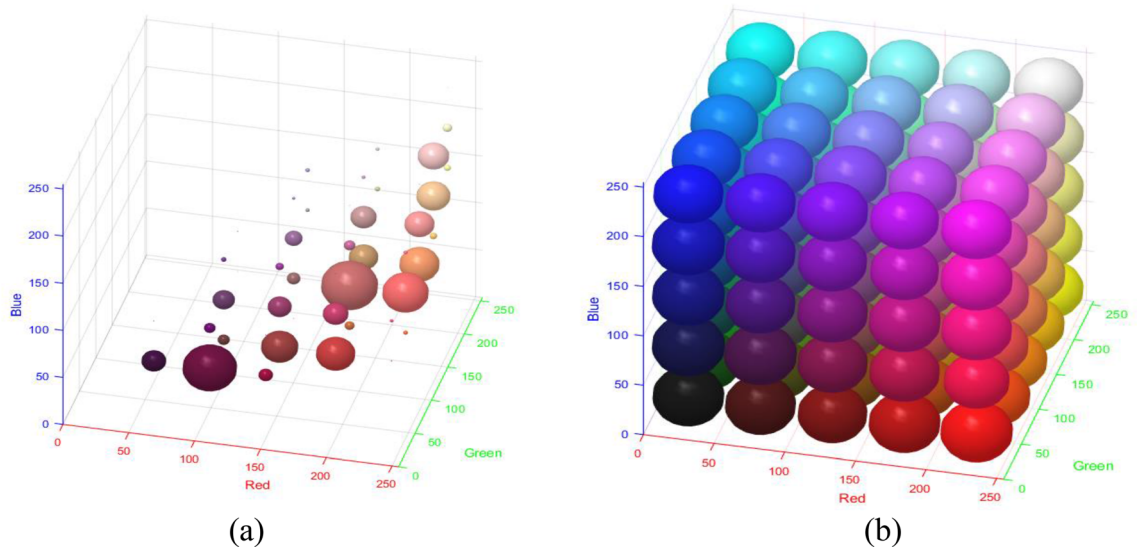

Fig. 7 Three-dimensional histograms of **a** original image and **b** ciphered image

Correlation coefficient (CC)

The degree of association is calculated by the correlation coefficient (CC). The Pearson correlation coefficient is often named CC after its originator and is a linear association metric. On a scale that ranges from + 1 to 0 to − 1, the CC is computed. Either + 1 or − 1 reveals the full relationship between the two variables. In the case of images if the contiguous pixels are similar, the CC is near to unity; total lack of correlation is characterized by 0. The pixels in plain images are highly correlated and its CC is near to unity, as shown in Table. 3. The encrypted image pixels must not possess a high correlation to withstand statistical attacks. The CC for each layer of plain and encrypted images are computed using the relation given in Eq. (8) and displayed in Table 3

$$r_{k,l} = \frac{A(k,l)}{\sqrt{B(k)}\sqrt{B(l)}}, \tag{8}$$

where

$$A(k,l) = \frac{\sum_{a=1}^{C}((k_a - E(k)(l_a - E(l)))}{C}, \tag{9}$$

$$B(k) = \frac{1}{C}\sum_{a=1}^{C}(k_a - E(k))^2, \tag{10}$$

$$B(l) = \frac{1}{C}\sum_{a=1}^{C}(l_a - E(l))^2, \tag{11}$$

Table 3 Correlation coefficient in three directions of plain and cipher 256×256 single layer

Image	Direction	Original			Encrypted		
		R	*G*	*B*	*R*	*G*	*B*
Lena	Vertically	**0.95721**	**0.94315**	**0.9284**	0.002078611	0.005484	0.0034543
	Horizontally	0.93388	0.91923	0.9006	0.006132242	− 0.00534	− 0.000105
	Diagonally	0.97888	0.97134	0.9559	0.001245919	− 0.00077	− 0.000690
peppers	Vertically	0.96457	0.96983	0.9570	− 0.00142832	− 0.00575	− 0.000111
	Horizontally	0.93694	0.94657	0.9262	− 0.00163305	0.001661	− 0.003471
	Diagonally	0.96796	0.97500	0.9636	− 0.00088374	0.001106	− 0.001517
airplane	Vertically	0.93893	0.96983	0.9503	0.000509314	0.000773	− 0.000805
	Horizontally	0.87379	0.94657	0.8800	0.000836903	0.005760	− 0.011994
	Diagonally	0.92385	0.97500	0.9088	− 0.00083985	0.001232	0.0008292
Baboon	Vertically	0.94744	0.87278	0.9215	0.010287103	0.003698	− 0.004251
	Horizontally	0.90339	0.79245	0.8762	0.001722889	0.007302	− 0.003072
	Diagonally	0.92076	0.83804	0.9138	0.006384370	0.005746	− 0.001145

where *A(k,l)* is the covariance between pixel a and b, C is the number of pairs (*a,b*), and *B(k)*, and *B(l)* represent the standard deviation of *k* and *l*. The linear relation is observed in Fig. 8 of the plain image pixels in all directions. While in the case of encrypted image, the pixels are distributed all over the plane.

Information entropy analysis (IE)

Randomness in information can be quantified using information entropy (IE). For an image that contains 256 levels of shades have an ideal value of IE 8. The purpose of encryption is to increase the randomness in the distribution of the pixels. The developed the value of the IE the higher will be the randomness in pixels distribution of an image and the harder it will be for an intruder to get any valuable information from the encrypted image. IE can be computed using the relation in Eq. (13)

$$IE = -\sum_{a=0}^{N-1} p(k_a) \log_b p(k_a), \tag{13}$$

where $p(k_a)$ denotes the probability distribution for the event k_a. The computed value of IE for each layer of plain and its

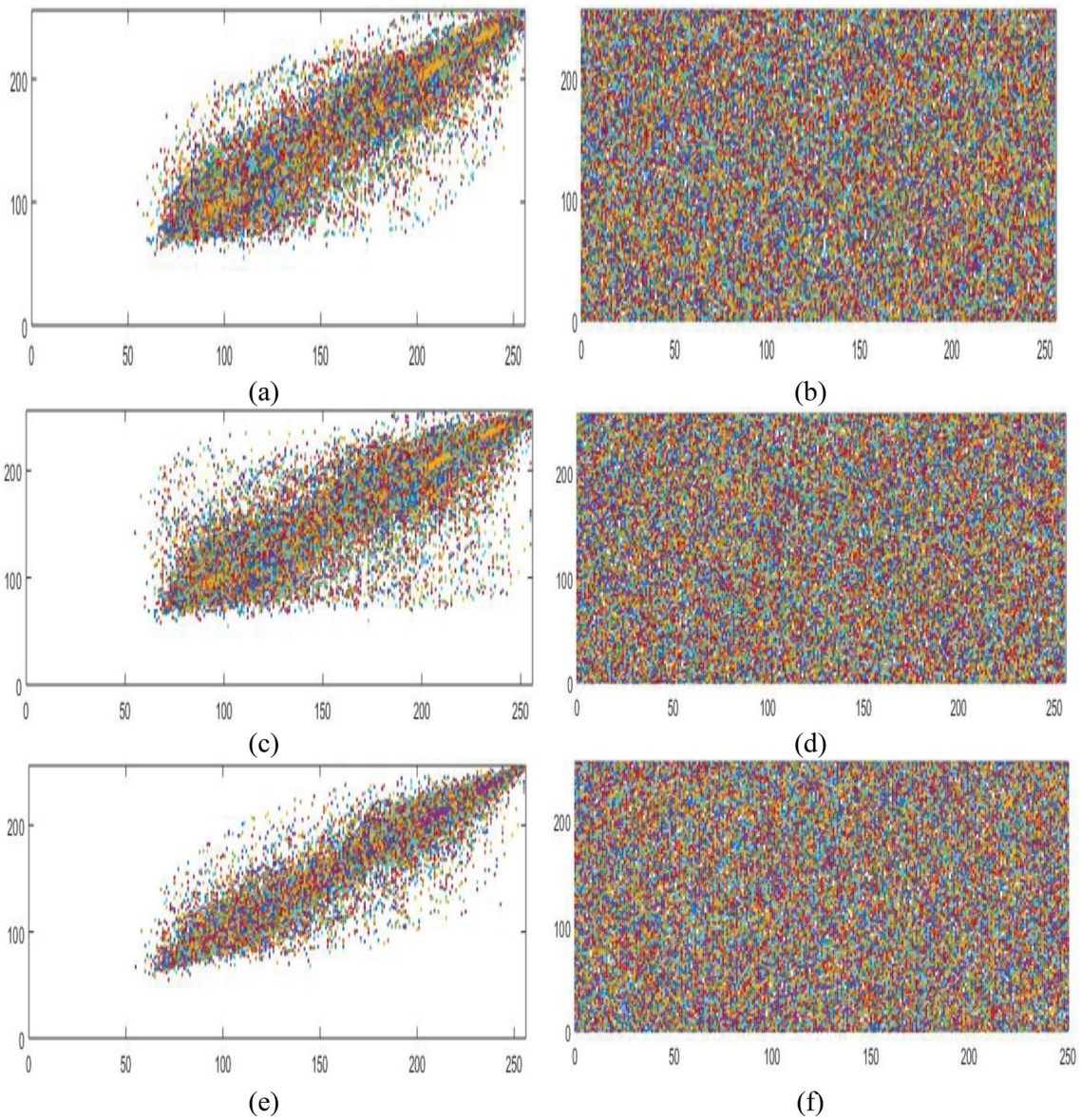

Fig. 8 Pixels scattering of original image and encrypted image. **a** Vertical pixel scattering of plain image. **b** Vertical pixel scattering of ciphered image. **c** Horizontal pixel scattering of plain image. **d** Horizontal pixel scattering of ciphered image. **e** Diagonal pixel scattering of plain image. **f** Diagonal pixel scattering of ciphered image

Table 4 Information entropy for plain and cipher image 256×256, RGB image

Image	Original RGB image			Encrypted RGB image		
	R	G	B	R	G	B
Lena	**7.733005**	**7.7330**	**7.733**	7.9973718	7.9973081	7.997047
Peppers	7.7037542	7.7037	7.7037	7.9970918	7.9974736	7.997031
Airplane	6.6787253	6.6787	6.6787	7.9977183	7.9973816	7.997317
Baboon	7.6785228	7.6785	7.6785	7.9974720	7.9974369	7.997042

Table 5 Information entropy for cipher image 256×256, RGB image

Image	Encrypted RGB image
Lena	7.999
Peppers	7.999
Airplane	7.999
Baboon	7.999

Table 6 Comparison of entropy for cipher image 256×256×3, RGB images with the recently proposed algorithm

Algorithm	Entropy
Ref. [31]	7.9993
Ref. [32]	7.9975
Ref. [27]	7.9970
Ref. [30]	7.9980
Ref. [33]	7.9994
Ref. [29]	7.999
Ref. [28]	7.997
Ref. [27]	7.997
Ref. [9]	7.999
Proposed	7.9999

equivalent ciphered image is displayed in Table 4. It can be perceived that the value of entropy is near to the superlative value of 8 in the case of encrypted layer images which shows the strength of the proposed cryptosystem.

Mean square error analysis (MSE)

Pixel-by-pixel squared difference examination of the plain and ciphered image is done in MSE analysis. The high value of MSE is the necessity of a worthy encryption structure (Tables 5, 6). The MSE can be computed by utilizing the relation in Eq. (14)

$$MSE = \frac{1}{M \times N} \sum_{a=1}^{M} \sum_{b=1}^{N} ((O(a,b) - P(a,b))^2, \tag{14}$$

where M×N is the dimension of images and O symbolizes the plain image and P symbolizes the processed ciphered image. The measurement of MSE is computed from different images and displayed in Table 7.

Table 8 MSE measurement for each layer of 256×256 test images

Image	MSE *RGB*	PSNR *RGB*
Lena	4701.667	11.40
Peppers	5321.16	10.870
Airplane	7176.624	9.571601
Baboon	3893.889	12.226

Peak signal-to-noise ratio (PSNR)

PSNR, is computed by utilizing MSE as depicted in Eq. (15) as the MSE is in the denominator so when it divides by the high value of MSE will result in a small PSNR. For a good encryption scheme, the lower value of PSNR is preferred. The PSNR can be computed using the relation in Eq. (15)

$$PSNR = \frac{(2^m - 1)^2}{MSE}, \tag{15}$$

Table 7 MSE measurement for each layer of 256×256 test images

Image	MSE			PSNR		
	R	*G*	*B*	*R*	*G*	*B*
Lena	10,697	8968	7041.695	7.83786	8.60359	9.6540309
Peppers	8016.2	11,082.22	11,148.89	9.09109	7.684535	7.658485
Airplane	9815.9	11,159.11	10,303.23	8.21149	7.654505	8.001066
Baboon	8296.07	7329.53	9037.369	8.9420	9.4800	8.5703832

Table 9 Comparison of average MSE measurement of Lena 256×256 test image with existing techniques

Algorithm	Average MSE
Reference [28]	936.2
Reference [34]	1035
Reference [35]	4859
Proposed	4701

Table 10 Time analysis of the proposed encryption system

Image	Time for encryption
Lena	2.090
Pepper	1.813
Boat	1.702
Airplane	2.081
Girl	2.170
Baboon	1.730

where m denotes the bits per pixel, and PSNR is often dignified in dBs. The measurement of PSNR is computed for every layer of the encrypted and plain image and tabulated in Table 7 and Table 8. Table 9 shows the comparison of the MSE for the proposed system with the recently proposed systems.

Throughput analysis for encryption procedure

The throughput of the cryptosystem is the proportion of the total size of the image to be encrypted to the total time taken by the encryption process for the image to encrypt. For real-time communication, throughput of a system is considered one of the most key performance indicators for an encryption scheme, the high the throughput the better the system. The throughput can be computed using the relation in Eq. (16)

$$\text{Throughput} = \frac{\text{Size of plaintext}}{\text{Time for encryption}}. \tag{16}$$

The memory occupied by the file to be enciphered is 500kBs, and the duration taken for encryption is 2.0050104. The throughput computed is 249.37527 kbs.

Time analysis

Time analysis of the proposed encryption scheme is carried out using MATLAB 2018 b on a PC Intel(R), Core(TM) i3-7700 CPU @ 3.60 GHz, 8 GB RAM with Windows 8. The computed time is tabulated in Table 10. The time analysis shows that the proposed encryption system is suitable for practical implementation.

NIST-based Randomness analysis

A non-regulatory and physical science laboratory National of Standard and Technology (NIST) issued a special edition of randomness test named NIST randomness analysis [36], which utilizes for the randomness in data. The detail of the tests is presented in [36], and the test is said to be certified if the value of the outcomes is less than unity. The subject test is accomplished, and the outcomes are displayed in Table 11. All the random tests are certified by the encryption scheme, it can be perceived from the results that the ciphered image achieves high randomness, which is the desired characteristic of a good encryption system.

Heat map analysis

The part of an image that grabs more attention is indicated warm-to-cool color spectrum in a heat map. The heat map for a plain image is computed. The heat map tells where the most important content of this image lies. In Fig. 9a, the most important content of image Lena lies in the range, colored as 200–256 in the scroll map. In the encrypted image, this content should be spread all over the encrypted image referred to Fig. 9b; in the encrypted image, the color is spread, and there are no contiguous pixels of the same color. The heat map in the encrypted image does not make any sense and does not convey any useful info regarding the most important content of the image as the most important information is distributed in an encrypted image. Part c of Fig. 9 signifies the distribution of the pixels of the most important content of image Lena. The part d of Fig. 9 shows the scattering of pixels of the most important content of the Lena image.

Conclusion

In this article, utilizing L-shaped fractal Tromino, three fractals are generated followed by the generation of CPs based chaotic matrices for the encryption process. To obscure the relation of key and ciphertext substitution is performed using highly non-linear S-boxes. The security analysis is performed and tabulated. The performance comparison with the recently proposed encryption schemes is performed. The security analysis reveals that the suggested encryption system possesses strong invulnerability against various threads.

Table 11 Test findings for the proposed Cryptosystem from NIST SP 800–22 experiments

Test	*pvalue* for every layer of enciphering image			
	R	G	B	Qualified
Frequency	0.87437	0.29669	0.2059	√
Block frequency	0.56641	0.017958	0.7964	√
Cumulative sums forward	0.23771	0.18834	0.3668	√
Overlapping test	0.81656	0.81567	0.85068	√
Long runs of ones	0.7127	0.7127	0.7127	√
Approximate entropy	0.41237	0.7305	0.60243	√
Spectral DFT	0.66336	0.11048	0.46816	√
Non-overlapping	0.98974	0.9994	0.999234	√
Rank	0.29191	0.29191	0.29191	√
Universal	0.88966	0.998947	0.9952	√
Serial 1	0.70874	0.15777	0.47387	√
Serial 2	0.43474	0.699054	0.71857	√
Runs (M = 10,000)	0.75213	0.16927	0.91937	√
Cumulative sums reverse	0.67591	0.9199	0.23463	√
Random excursions $X = -4$	0.46772	0.13903	0.17807	√
$X = -3$	0.73043	0.4557	0.21555	√
$X = -2$	0.84811	0.4582	0.02374	√
$X = -1$	0.8959	0.1088	0.37508	√
$X = 1$	0.7469	0.7127	0.64443	√
$X = 2$	0.6597	0.9007	0.56942	√
$X = 3$	0.40953	0.966	0.96843	√
$X = 4$	0.51222	0.9727	0.09684	√
Random excursions variant $X = -9$	0.68064	0.67442	0.8226	√
$X = -8$	0.58388	0.65472	0.2183	√
$X = -7$	0.5563	0.63095	0.17037	√
$X = -6$	0.70116	0.60151	0.1467	√
$X = -5$	0.81366	0.5637	0.17208	√
$X = -4$	0.95737	0.58538	0.2521	√
$X = -3$	0.84952	0.79625	0.2040	√
$X = -2$	0.87028	0.50499	0.09369	√
$X = -1$	0.67137	0.38648	0.06454	√
$X = 1$	0.67137	0.99978	0.08581	√
$X = 2$	0.46243	0.61708	0.6962	√
$X = 3$	0.2823	0.19671	0.96404	√
$X = 4$	0.069159	0.51269	0.83404	√
$X = 5$	0.0054144	0.92334	0.8185	√
$X = 6$	0.00929	0.999872	0.36229	√
$X = 7$	0.01347	0.7887	0.2584	√
$X = 8$	0.02357	0.94058	0.3084	√
$X = 9$	0.1069	0.72629	0.2674	√

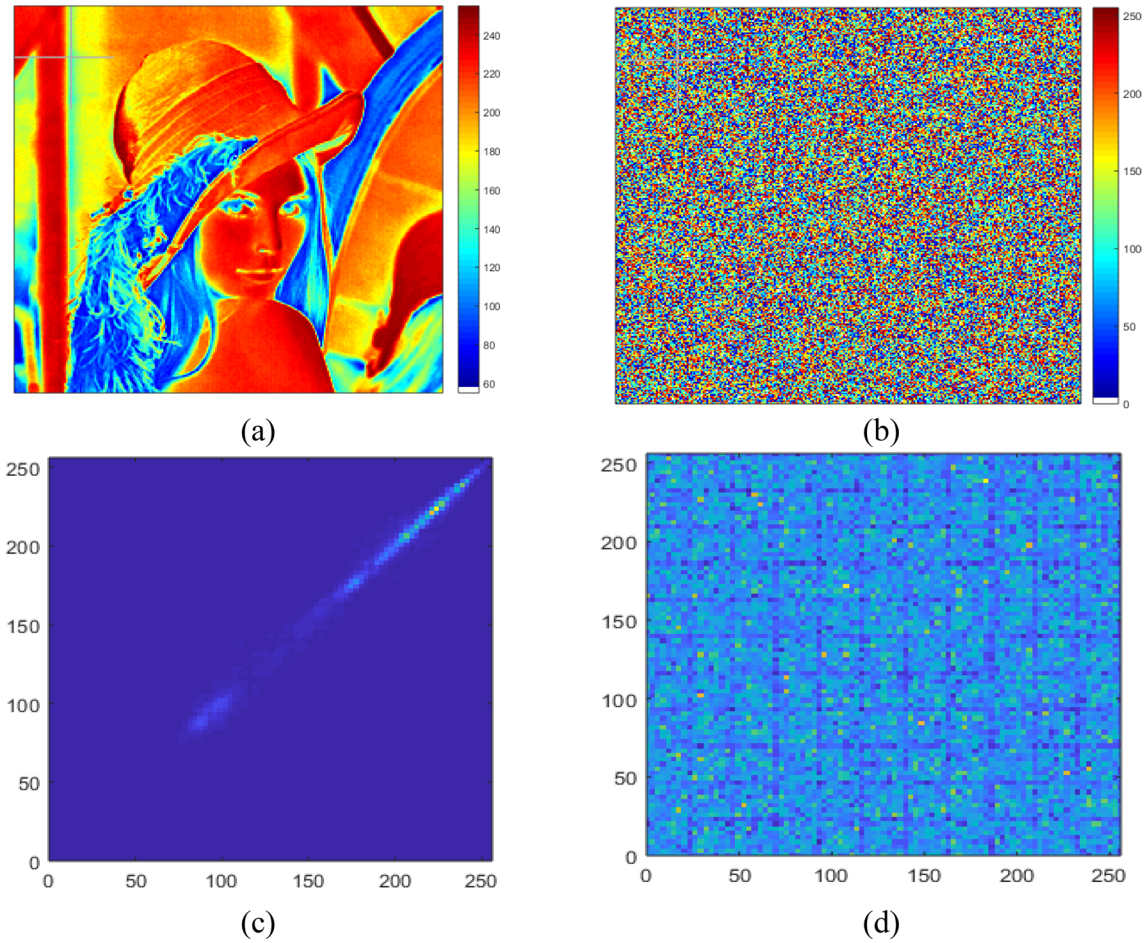

Fig. 9 Heat map analysis. **a** Plain Image. **b** Ciphered Image. **c** Pixels distribution

Declarations

Conflict of interest The authors have not any conflict of interest regarding the publication of this article.

References

1. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 27:15–43
2. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based. Int J Bifurcat Chaos 16(8):2129–2151
3. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 43:15–27
4. Özkaynak F (2020) On the effect of chaotic system in performance characteristics of chaos based s-box designs. Physica A Stat Mech Appl 550
5. Farah MAB, Farah A, Farah T (2020) An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn 99:3041–3064
6. Khan M, Masood F (2019) A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl 358:26203–26222
7. Zhang Q, Guo L, Wei X (2013) A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Opt Int J Light Electron Opt 124(18):3596–3600
8. Arshad U, Khan M, Shaukat S, Amin M, Shah T (2020) An efficient image privacy scheme based on nonlinear chaotic system

and linear canonical transformation. Physica A: Stat Mech Appl 546
9. Said L, Hazzazi MM, Khan M, Jamal SS (2021) A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. Chin J Phys
10. Masood F, Ahmad J, Shah SA, Jamal SS, Hussain I (2020) A novel hybrid secure image encryption based on Julia Set of fractals and 3D Lorenz Chaotic map. Entropy 22:274
11. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 15–43:27
12. Younas I, Khan M (2018) A new efficient digital image encryption based on inverse left almost semi group and Lorenz Chaotic system. Entrpy 20(12):913
13. Khan M, Masood F, Alghafis A (2020) Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. Neural Comput Appl 32:11837–11857
14. Khade PN, Narnaware M (2012) 3D chaotic functions for image encryption. IJCSI Int J Comput Sci 9(3):323–328
15. Chong F, Jun-jie C, Hao Z, Wei-hong M, Yong-feng Z, Ya-wen Y (2012) A chaos-based digital image encryption scheme with an improved diffusion strategy. Opt Express 20(3):2363–2378
16. Zhang LY, Hu X, Liu Y, Wong K-W A chaotic image encryption scheme owning temp-value feedback. Cornell University Journal.
17. Geisel T, Fairén V (1984) Statistical properties of chaos in Chebyshev maps. Phys Lett A 105(6):263–266
18. Yepdia LMH, Tiedeu A, Lachiri Z (2020) Multiple-image fusion encryption (MIFE) using discrete cosine transformation (DCT) and pseudo random number generators. Multimed Inf Retrieval
19. Jamal SS, Shah T, Farwa S, Khan MU (2019) A new technique of frequency domain watermarking based on a local ring. Wireless Netw 25(4):1491–1503
20. Waqas UA, Khan M, Batool SI (2020) A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images. Multimed Tools Appl 79:6891–6914
21. Munir N, Khan M, Shah T, Hussian I (2021) "Cryptanalysis of nonlinear confusion component based encryption algorithm. Integr VLSI J 79:41–47
22. Wang X, Wang Q (2014) A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. NonLinear Dyn 75:567–576
23. J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan and Y. Liu, "FPDP:Flexible Privacy-preserving Data Publishing Scheme for Smart Agriculture," *IEEE SENSORS JOURNAL,* 2020.
24. W. Wang, . H. Huang, L. Zhang and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-to-Peer Networking and Applications,* 2020.
25. B. Stoyanov and K. Kordov, "Novel Image Encryption Scheme Based on Chebyshev Polynomial and Duffing Map," *The Scientific world Journal: Recent Advances in Information Security,* 2014.
26. Ali KM, Khan M (2019) A new construction of confusion component of block ciphers. Multimed Tools Appl 78:32585–32604
27. Khan S, Han L, Lu HI, Butt KK, Bachira G, Khan NU (2019) A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI. IEEE Access 7:81333–81350
28. Alghafis A, Firdousi F, Khan M, Batool SI, Amin M (2020) An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing. Math Comput Simul 177:441–466
29. He Y, Zhang YQ, Wang XY (2020) A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system. Neural Comput Appl 32:247–260
30. Norouzi B, Mirzakuchaki S (2017) An image encryption algorithem based on DNA sequence operations and cellular neural network. Multimed Tools Appl 76:13681–13701
31. He Y, Zhang YQ, Wang XY (2020) A new image encryption algorithem based on two dimensional spatiotemporal chaotic system. Neural Comput Appl 32:247–260
32. Alghafis A, Firdousi F, Khan M, Batool SI, Amin M (2020) An efficient image encryption sheme based on chaotic and Deoxyribonucleic acid sequencing. Math Comput Simul 177:441–466
33. Gan Z, Chai X, Zhang M, Lu Y (2018) A double color image encryption scheme based on three dimensional Brownian motion. Multimed Tool Appl 77:27919–27953
34. Khan M, Shah T (2015) An efficient chaotic image encryption scheme. Neural Comput Appl 26:1137–1148
35. Younas I, Khan M (2018) New efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system. Entropy 20(12):913
36. Rukhin A, JuanSoto J, Nechvata J. A statistical test suite for random and pseudorandom number generators for cryptographic applications.