Multimedia Tools and Applications (2019) 78:26203–26222
https://doi.org/10.1007/s11042-019-07818-4

A novel chaotic image encryption technique based on multiple discrete dynamical maps

Majid Khan [1,2] · Fawad Masood [1,3]

Received: 18 September 2018 / Revised: 15 April 2019 / Accepted: 21 May 2019 /
Published online: 6 June 2019

Abstract
The propagation of information over insecure communication system is one of the most important aspect of digitally advance era. The electronic information is travels in form of binary bits. The secrecy of these digital contents is one of the most important issue of existing world. In this article, we have utilized multiple chaotic iterative maps in order to propose a novel image encryption technique. The suggested encryption added confusion as well as diffusion in offered scheme which is one of the most fundamental aspect of encryption technique. We have tested our anticipated scheme against different performances analysis and compared it with already existing results. The designed scheme is capable of providing an excellent privacy to digital images.

Keywords Image encryption · Confusion · Diffusion · Multiple chaotic maps

1 Introduction

In recent era of science and technology digital information become a basic currency to nations. The ultimate goal of the digital communication is to transmit information with ease within no time. The faith of the nation's precisely depends on its secret information. The privacy of digital information is one of the unavoidable issues of the digitally advanced fifth generation communications. The digital information are nowadays places in the form of bits in different national and multinational organizations databanks. The digital contents are now in the form of images, audio and video files. The digital information is accessed and available largely on different social and web links. In order

✉ Majid Khan
mk.cfd1@gmail.com

[1] Cyber and Information Security Lab (CISL), Institute of Space Technology, Islamabad, Pakistan

[2] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan

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

to secure the secret information different data security techniques were designed which includes classical and modern encryption schemes. The classical encryption schemes either utilized substitution or permutation [20–22, 24, 25, 35]. This means that idea of confusion and diffusion proposed by Claude Shannon, were used separately before 1949. Nowadays, modern encryption mechanisms particularly private encryption schemes use both confusion, diffusion and number of rounds in a combined fashion. The most famous block ciphers which were based on idea of confusion and diffusion were international data encryption algorithm (IDEA), data encryption standard (DES) and advanced encryption standard (AES) and their different variants [23, 26]. Designing of new encryption methodology is one of the prominent area of research in information security. Several adaptations were proposed in standard encryption schemes in order to deploy them in different environments. Moreover, numerous encryption algorithms were designed in order to secure the digital information. The encryption algorithms which are in fashion nowadays are chaos based cryptosystems. The fundamental characteristics of chaos are quite related with cryptography which make it possible to equally utilize chaos in encryption of digital information. The sensitivity of chaotic parameters and initial state dependency are the famous characteristics of chaos which were utilized in order to ensure the confusion and diffusion characteristics in designed encryption scheme [2–5, 11, 15, 31, 36, 38, 39, 42–45].

Chaotic dynamical systems, which are the building blocks of any chaotic encryption. These systems can be characterized into discrete and continuous chaotic systems [7, 8, 10, 14, 33]. Discrete chaotic systems utilize an arrangement of different chaotic iterative maps, while the continuous chaotic frameworks are can be represented by differential equations. The development of chaos theory in the field of information security from last one decade is quite promising. The idea of confusion and diffusion developed by Shannon in 1949 can be achieved by utilizing different chaotic systems. There are fundamentally two domains of digital image namely spatial and frequency. Several image encryption techniques based on chaotic systems were developed based on spatial and frequency domains. In spatial domains, most significant and least significant bits are two basic components. The nonlinear chaotic systems were operated either on most significant and least significant bits or as a whole n-bits of a pixel. Another important classification in spatial domain chaotic image encryption is selective image encryption techniques which reduces the computational in processing of digital image enciphering in real time encryption. The second most important class of chaotic image encryption techniques is frequency based design mechanisms. These schemes fundamentally used different frequency filters in order to encrypt the digital contents. Numerous transforms such as discrete cosine and sine transform, fast Fourier transform and wavelets transform were used to encrypt images along with chaotic dynamical systems [1, 6, 9, 12, 13, 16–19, 26–30, 32, 34, 37, 41]. Our scheme is based on discrete chaotic dynamical systems namely Henon map, circle map and duffing map. The principle aim of article is to utilize multiple chaotic maps in order to achieve strong confusion and diffusion with minimum rounds. The decrease in number of round surely minimize the computational cost which of the important aspects of modern cryptosystems.

The rest of the paper is prepared as follows. In Section 2, we have discussed some relationships between chaos and cryptography. In Section 3, we have presented the proposed encryption algorithm. The performance analyses are placed in Section 4. Finally, we have ended our article with conclusion in Section 5.

2 Chaos and cryptography

Chaos is branch of mathematics which deals with the study of behavior of dynamical systems. These systems are highly sensitive to initial conditions and chaotic parameters. Some well-known properties of chaos comprise topology mixing, strange attractor, ergodicity, randomness and dependence on its initial conditions [7, 8, 10, 14, 33]. These properties attract to make strong cryptosystem algorithm for security against advertisers. Chaotic systems show high randomness in its output and exhibit unique properties. Without the knowledge of its parameters, chaotic system become not deterministic. This property show that it is suitable for designing good cryptographic algorithms. For good chaotic output, we must know initial condition of supposed map. If we know initial conditions of the map, then it became deterministic for us. These chaotic properties can be utilized for different cryptosystem though substitution can be borne out very meticulously. The important property of sensitive to initial conditions ascertain ease in the implementation of cryptosystem and provide hurdle in the path for malicious person. For encounter cryptanalysis, we have proposed nonlinear system with property of confusion and diffusion. Basic flow diagram for the chaotic encryption is given in Fig. 1.

2.1 Basic features of chaotic systems

Chaos was witnessed in various natural systems for instance biology, ecology, physics, electronics, meteorology economics, computer science and engineering. These cases show, as stated before, show particular assets that form them unpredictable along with complex system. The chaos theory contracts with systems that exhibit a special kind of dynamical behavior in time. Usually chaos occurs in a nonlinear deterministic dynamical systems (NLDS). It is clear that chaos occurs when there is a continuous and rough-looking persistent change to the mathematician criteria. There is a set of characteristics that observed the professional in chaotic systems. The mathematical criteria for chaos are defined. The most relevant are [21]:

- **Dynamic instability**

This criterion is also denoted as butterfly effect, it is the feature of sensitivity to initial conditions, where two subjectively closed initial conditions changes with significantly divergent and different trajectories.

- **Topological mixing**

Topological mixing instinctively described as mixing colored dyes, it means that the system will change during time so that any known area of states is always overlaps or converted with any other known area.

Fig. 1 Basic schematic system model for image encryption

- **Aperiodicity**

The system in the orbit never replicate itself with the passage of time or non-periodic in nature.

- **Dense periodic orbits**

Dense periodic orbits mean that the system follows some dynamics that can subjectively nearly approach every probable asymptotic state.

- **Ergodicity**

Statistical measurement of variable that give analogous output irrespective of performance over space or time. The dynamics show same statistics properties when immediately observed over space and time.

- **Self-similarity**

The progression of system, in space or time, show similarity at dissimilar measurement. This property makes unique system that look like auto-repetitive (repetition) at different measurement.

The connects between chaos and cryptography can be seen in Table 1 [21].

3 Proposed image encryption algorithm

In this section, we have presented our proposed encryption algorithm. We have used two properties of chaos that are confusion and diffusion while designing secure encryption scheme. Our proposed scheme utilized multiple one dimensional and two dimensional chaotic iterative maps in order to achieve the confusion and diffusion capabilities.

3.1 Maps for proposed cryptosystem

In this subsection, we have discussed the chaotic iterative maps which will be helpful for the construction of our image encryption technique.

Table 1 Connection between chaos and cryptography

Chaotic Properties	Cryptographic Properties	Explanation
Ergodicity and mixing property	Confusion	Output of the system look identical to input
Sensitivity to control parameters and initial conditions	Diffusion	A negligible difference or change in the input produces a very different output.
Deterministic	Deterministic pseudo randomness	Deterministic technique that outcomes to pseudo randomness
Complexity	Algorithmic Complexity	Algorithm that outcomes to immensely complex outputs

3.1.1 Henon chaotic map

Two-dimensional discrete time dynamical map having good chaotic behavior. This map take points (x_n, y_n) and maps to a new point. Mathematically it can expressed as follows [21]:

$$x_{n+1} = 1 - ax_n + y_n, \tag{1}$$

$$y_{n+1} = bx_n, \tag{2}$$

where x_0 and y_0 are initial conditions of the map. This system performs chaos when setting parameters to $x_0 = 1.61001$, $y_0 = 2.9996$, $a = 1.7085$, $b = 0.32032$.

3.1.2 Rand block function

Rand block is use to generate blocks of image to randomize values of internal cell. This command help us in better permutation during image encryption.

3.1.3 Circle chaotic map

Circle map is one dimensional map and exhibit very good chaotic behavior when apply to any data. The mathematical form can be expressed as:

$$\theta_{n+1} = \mathrm{mod}\left(\theta_n + \Omega - \frac{K}{2\pi}\sin(2\pi(\theta_n)), 1\right), \tag{3}$$

where $\theta_0 = 0.4$, $\Omega = 0.5$ and θ_{n+1} is computed as mod 1 and K is constant. This map has basically two important parameters Ω and K, where Ω can be frequency that is being applied externally and K is spring constant.

3.1.4 Duffing chaotic map

The duffing map is two dimensional discrete time dynamical system that exhibit chaotic behavior. It take points (x_n, y_n) and give its output. Duffing map equation can be expressed in Eqs. (4)–(5) respectively:

$$x_{n+1} = y_n, \tag{4}$$

$$y_{n+1} = -bx_n + ay_n - y_n^3, \tag{5}$$

where $x_0 = -1.5$, $y_0 = 1.5$, $a = 2.738$, $b = 0.1534$.

Steps involved in image encryption stage

1. Read an image of size $256 \times 256 \times 3$ and transform into three channels (R, G, B).
2. In first phase (R, G, B) channels are divided into blocks of 32×32 cells, each cell having size of 8×8.

3. In second phase pixels are shuffled within blocks using two dimensional Henon chaotic map for each channel.
4. In third phase blocks are permuted of each respective channel.
5. In fourth phase pixels are distorted using one dimensional circle map.
6. Finally for better confusion, again bitwise *XOR* for each channel respectively using two dimensional discrete time duffing map.

Steps involved in image decryption stage

1. In first phase two dimensional duffing chaotic map is bitwise *XOR* for each channel with the output of step 5 in encryption stage.
2. In second phase reverse process bitwise *XOR* for each channel with circle map to get back random blocks of each channel.
3. In third phase inverse randblock is use to get uniform blocks with shuffled pixels as done in encryption stage step 3.
4. In fourth phase inverse Henon chaotic map is treated with the output of third phase to get unshuffled pixels.
5. In fifth phase output of fourth phase is retreated with inverse of first phase in encryption stage.
6. Finally image is treated with cat command to get back into decrypted plain image (Fig. 2).

4 Security analysis

Security analysis play an important role in reliability of encryption algorithms. The weakness of encryption algorithm make is possible for unauthorized person to examine secret information and try to use of different combination to get plaintext. We have examined our suggested encryption scheme against different statistical analysis that includes histogram analysis, mean square error (MSE), correlation coefficient test, peak signal to noise ratio (PSNR), entropy, plaintext sensitivity analysis.

4.1 Histogram analysis

Histogram is the way to represent pixel occurrences in digital images. In order to deceive the eavesdropper, the encryption algorithm must have a strong converge towards uniformity after successful application of enciphering scheme. Uniformity is one of the aspect of encrypted images to hide the actual content of digital images. We took standard Lena image of size $256 \times 256 \times 3$ and divided into three respective channels (RGB). The histograms of each channel at plain level comprises sharp peaks whereas histograms of cipher images are distributed equally over the entire region with no sharp peaks (see Figs. 3, 4, 5, 6, 7 and 8). The investigation of histograms of encrypted images clearly reveals that projected algorithm does not provide any clue to passive and active eavesdropper to get any secret information easily due to uniformity of histograms.

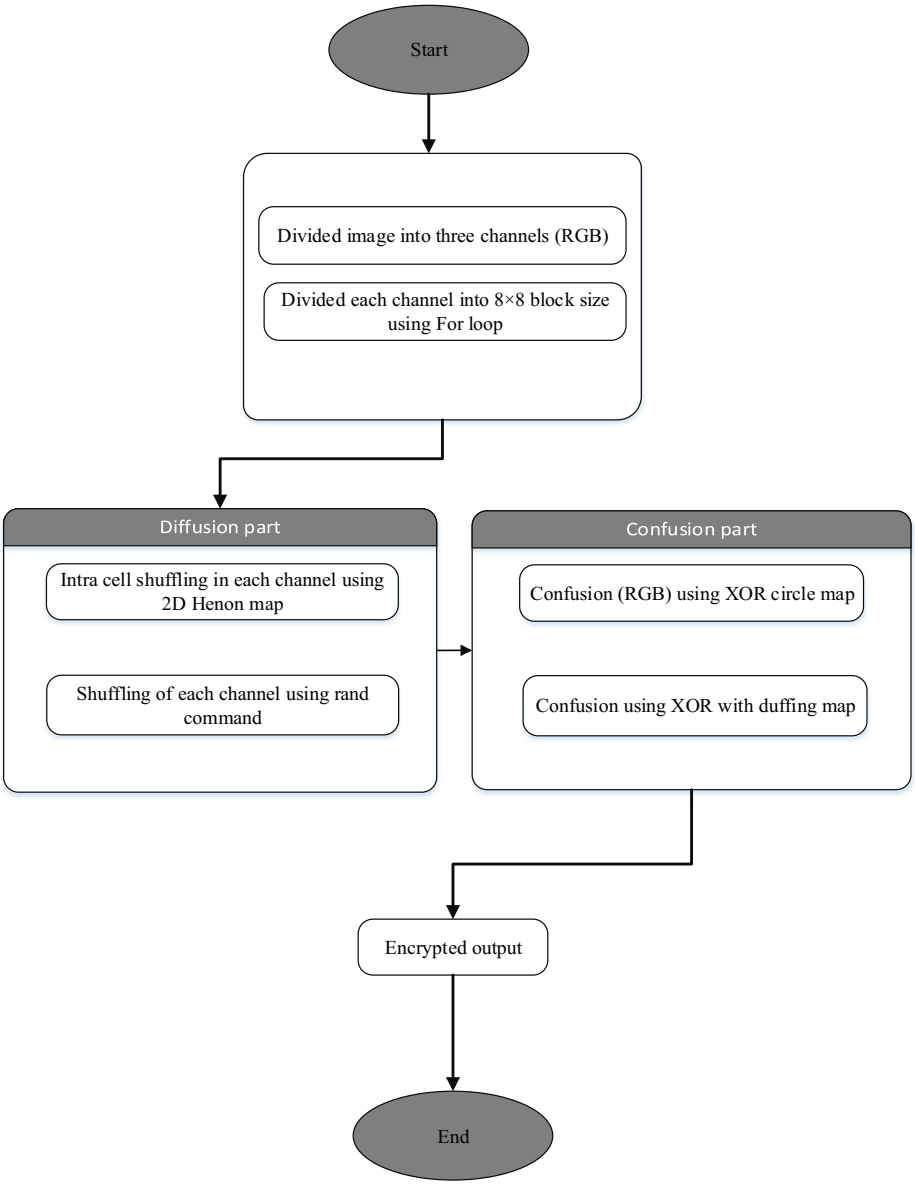

Fig. 2 Flow diagram for proposed encryption

4.2 Correlation

In this segment, we have analyzed correlation between adjacent pixels which means similarity between pixels of image in three different directions i.e. vertical, horizontal and diagonal. The value of correlation coefficient (CC) lies within the interval [−1,1]. For totally uncorrelated image the value of CC quite closed to zero, whereas −1 corresponds to negative correlation and 1 belong to positive correlation. For cryptographically secure encryption algorithms CC remains closed to zero. We have added tables for three cases to

Fig. 3 **a** Lena image red channel; **b** Lena image green channel; **c** Lena image blue channel

examined the relation of adjacent pixels in three different directions i.e. vertically, horizontally and diagonally (see Figs. 9, 10, 11, 12, 13, 14, 15 and 16, Tables 2, 3 and 4). The mathematically expressions for correlation coefficient are given by:

$$\gamma_{XY} = \frac{\delta_{XY}}{\sqrt{\delta_X^2 \delta_Y^2}}, \tag{6}$$

where δ_{XY} is known as covariance of random variables X and Y, μ_X and μ_Y are expected values of random variables and δ_X^2 and δ_Y^2 are variances respectively given below:

$$\delta_{XY} = \sum_{j=1}^{N} \frac{\left(X_j - \mu_j\right)\left(Y_j - \mu_Y\right)}{N}, \delta_X^2 = \sum_{j=1}^{N} \frac{\left(X_j - E(X)^2\right)}{N}, \delta_Y^2 = \sum_{j=1}^{N} \frac{\left(Y_j - E(Y)^2\right)}{N}. \tag{7}$$

The linear relationship can be observed among the pixels of plain image (see Figs. 9, 11, 13, 15) and corresponding numerical value of CC is closed to unity (see Tables 2, 3 and 4). The application of our proposed image encryption scheme make it possible to break the neighboring relation among pixels. The value of CC reduces to zero which shows the strength of our anticipated technique (see Figs. 10, 12, 14, 16 and Tables 2, 3 and 4).

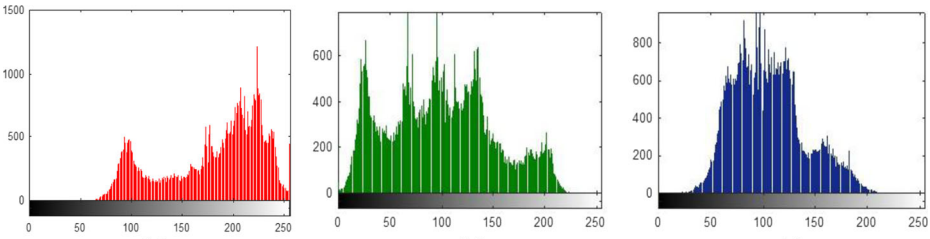

Fig. 4 **a** Lena red channel histogram; **b** Lena green channel histogram; **c** Lena blue channel histogram

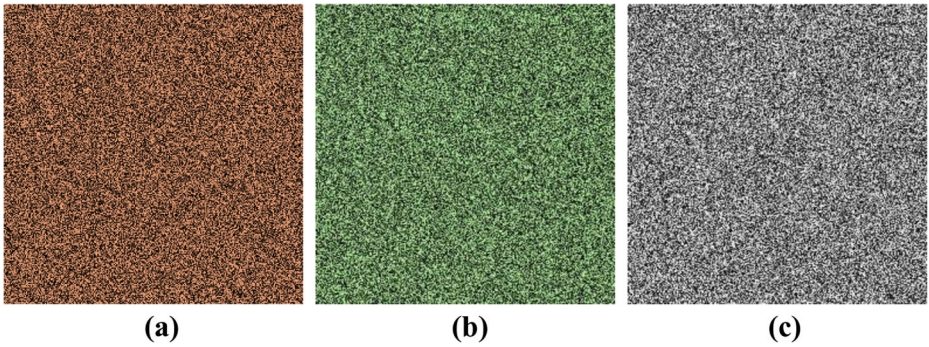

Fig. 5 **a** Encrypted red channel after circle map; **b** Encrypted green channel after circle map; **c** Encrypted blue channel after circle map

4.3 Mean square error

For authenticity we evaluated mean square error (MSE) for Lena plain and encrypted image which showed reliability of the proposed algorithm. (MSE) can be calculated as in Eq. (8):

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(A_{(i,j)} - Q_{(i,j)} \right), \tag{8}$$

where $A_{i,j}$ and $Q_{i,j}$ show pixels are positioned at i^{th} row and j^{th} column, $M \times N$ is the overall extent (size) of image of original and enciphered image respectively, MSE value must be large enough to provide robust security against different cryptographic attakcs (see Tables 5 and 6).

4.4 Peak signal to noise ratio

Peak signal to noise ratio (PSNR) can be used to assess the quality of encryption technique. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image [31]. The mathematical expression for PSNR is given in Eq. (9):

$$PSNR = 10 \log_2 \frac{I^2_{\max}}{MSE}, \tag{9}$$

where $I_{\max}$is maximum value of image, for better security the value for PSNR should be low enough to comply with good security (see Tables 5 and 6).

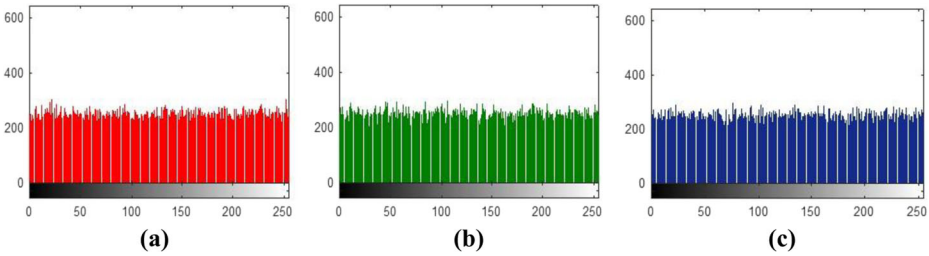

Fig. 6 **a** Encrypted red channel histogram after circle map; **b** Encrypted green channel histogram after circle map; **c** Encrypted blue channel histogram after circle map

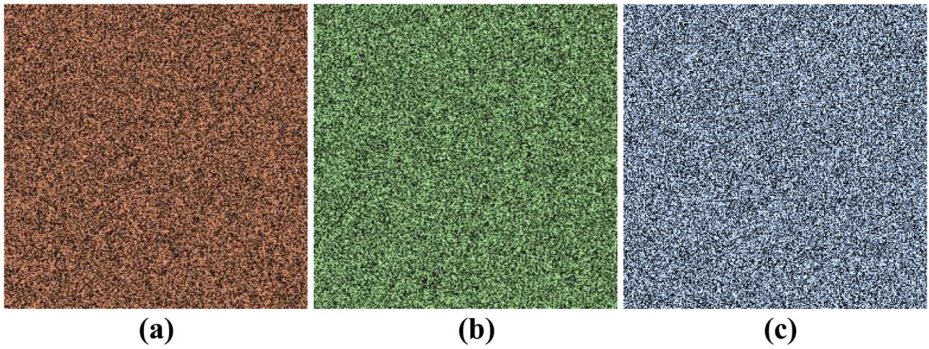

Fig. 7 **a** Red encrypted channel after circle and duffing map; **b** Green channel encrypted after circle and duffing map; **c** Blue encrypted channel after circle and duffing map

4.5 Entropy

Entropy analysis is measurable quantity which measure randomness in the information content of the test image. The entropy can be represented by the following expression:

$$H = -\sum_{J=0}^{N-1} p(x_j) \log_b p(x_j), \tag{10}$$

where $p(x_j)$ represent occurrence of probability of symbol x_j. The theoretical value of entropy is 8 for 8-bit image and practical values through our offered scheme is *7.999*, which is quite close to ideal value [23, 26, 31, 39, 42] (see Tables 7, 8, 9 and 10). This reveals that, our suggested encryption scheme based on multiple chaotic iterative maps is considerably increases the randomness among the pixel's distribution of original image. The histogram of encrypted image is uniform and contain no similarity of plain image which makes it impossible for eavesdropper to extract any information.

4.6 Mean absolute error

Mean absolute error (MAE) is criterion (model) to inspect pursuance of resisting against differential aggression. We calculated mean absolute error (MAE) between original and encrypted images. MAE value must be large enough to ensure the robustness of crypto-system. We evaluated our proposed scheme for the size of $256 \times 256 \times 3$ test images. Let

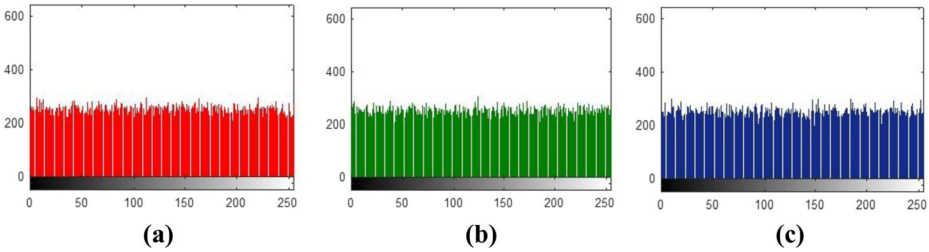

Fig. 8 **a** Encrypted red channel histogram after circle and duffing map; **b** Encrypted green channel histogram after circle and duffing map; **c** Encrypted blue channel histogram after circle and duffing

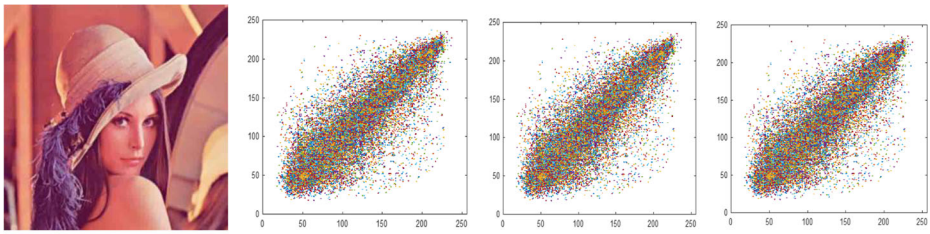

Fig. 9 **a** Plain image; **b** Horizontal correlation of plain image; **c** Diagonal correlation of plain image; **d** Vertical correlation of plain image

$E_{i,j}$ and $F_{i,j}$ be two grey level pixels at i^{th} row and j^{th} column of an image extent (size) $M \times N$ for both plain and enciphered image then Eq. (11) for two respectively images can be written as:

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{J=0}^{N-1} \left| \left(E_{(i,j)} - F_{(i,j)} \right) \right|. \tag{11}$$

Table 11 show for both plain and cipher image grey level pixels at $E_{(i,j)}$and $F_{(i,j)}$ respectively.

The MAE values of our offered chaos based algorithm is high as compared to other outcomes available in literature [23]. The clearly reveals that our anticipated algorithm is one of the best candidate for chaos based image encryption schemes.

4.7 Differential attacks analysis

Differential attack analysis is fundamentally fall into the chosen-plaintext attacks category [23]. The capability of battling against differential attacks is measured by comparing the differences between two ciphers images i-e., minor change in plain image results completely change in cipher image. Thus, much difference between encrypted forms is expected in order to keep high security. Number of pixels changing rate (NPCR) and unified average change intensity (UACI) become two widely used security analyses in the image encryption community for differential attacks. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired cipher images [40].

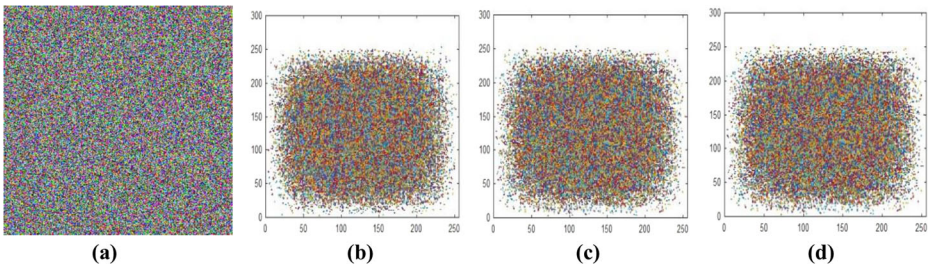

Fig. 10 **a** Encrypted image; **b** Horizontal correlation of encrypted image; **c** Diagonal correlation of encrypted image; **d** Vertical correlation of encrypted image

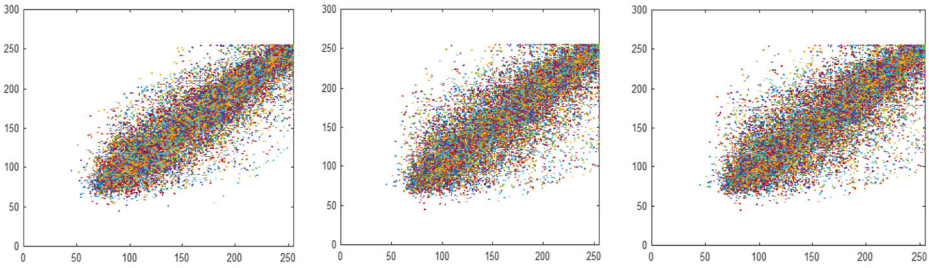

Fig. 11 **a** Red channel horizontal correlation of plain image; **b** Red channel diagonal correlation of plain image; **c** Red channel vertical correlation of plain image

4.7.1 Number of pixels changing rate

Number of pixels changing rate (NPCR) actually finds rate of change of pixels' location amid plain and encrypted image. Here we take two encrypted images for NPCR test and had difference of only pixel, we represented cipher image with $E_{1(i,j)}$and $E_{2(i,j)}$ whose analogous plain image have only pixel difference. An array $V_{(i,j)}$ can be calculated using $E_{1(i,j)}$and $E_{2(i,j)}$ respectively though NPCR can be evaluated as in Eq. (12):

$$NPCR = \frac{\left(\sum_{i,j} V_{i,j}\right)}{W \times H} \times 100, \tag{12}$$

where $V_{i,j}$ in above equation can be construe as:

$$V_{i,j} = \begin{cases} 0 & E_{1(i,j)} = E_{2(i,j)} \\ 1 & E_{1(i,j)} \neq E_{2(i,j)} \end{cases}$$

4.7.2 Unified average change intensity

The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image and expression for UACI is given below:

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{\left[E_{1(i,j)} - E_{2(i,j)}\right]}{255}. \tag{13}$$

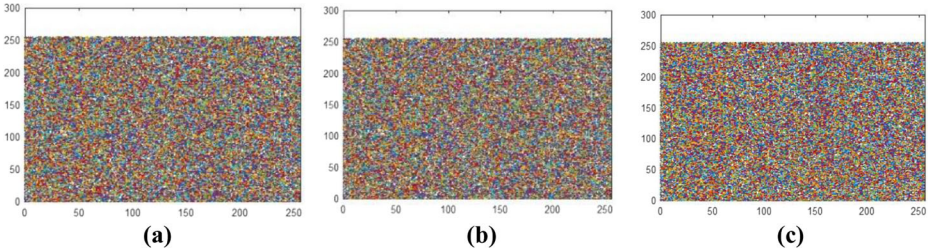

Fig. 12 **a** Red channel horizontal correlation of encrypted image; **b** Red channel diagonal correlation of encrypted image; **c** Red channel vertical correlation of encrypted image

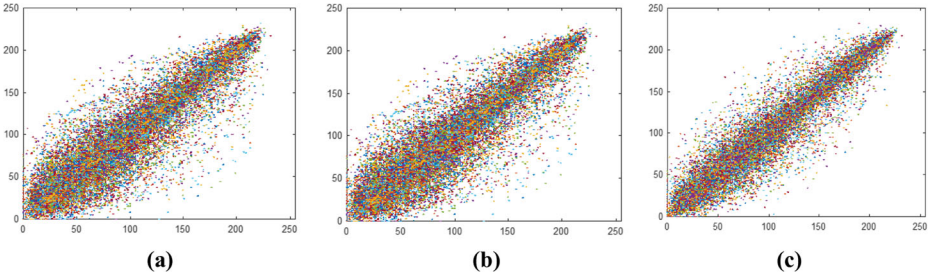

Fig. 13 **a** Green channel horizontal correlation of plain image; **b** Green channel diagonal correlation of plain image; **c** Green channel vertical correlation of plain image

We have tested Lena image of size 256 × 256 × 3 as a test image for our proposed algorithm. We examined that larger unified average changing rate means our encryption algorithms is quite excellent and mark i.e. encryption performance increases. We showed input image one-pixel difference between two source images, the change that is made were almost 0.01% at input side of images for respected ciphered images. Results are tabulated in Tables 12 and 13.

It is clear from Table 13 that the value of NPCR is greater 99.60% and that of UACI is greater than 33.35% which means that slight variation in a particular pixel of the original image consequences in a major modification of all the pixels of the encrypted image.

4.8 NIST analysis

NIST abbreviated as National Institute of Standards and Technology issued special publication (SP 800–22) of statistical tests *i. e.* random and pseudo random numbers for cryptography. This is one the most substantial observation and inspection. This test is basically applying on binary sequences main reason is that the encrypted (cipher) image at the output can be estimated as binary data stream file. The tests result of the cipher image Lena is given in Table 14.

The consequences of data entropy examination for the total arrangement of test pictures are recorded and compared in Tables 6, 7 and 8. These outcomes show that the proposed scheme gets ciphertext images whose entropy scores substantially nearer to the entropy upper bound than those encoded by different procedures. The more like zero the correlation coefficient is the weaker connection between the pixel succession and its adjoining pixel arrangement. Since the adjoining pixel succession is evidently removed from the horizontal, vertical and diagonal directions.

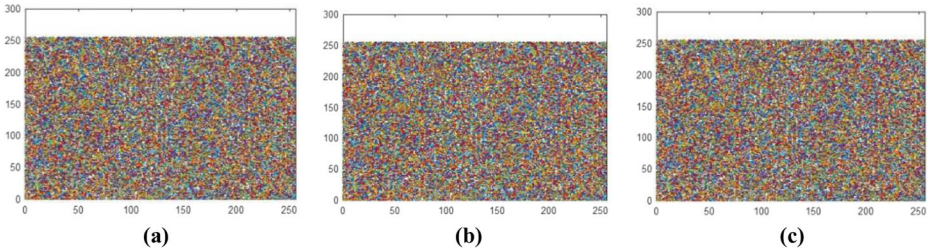

Fig. 14 **a** Green channel horizontal correlation of encrypted image; **b** Green channel diagonal correlation of encrypted image; **c** Green channel vertical correlation of encrypted image

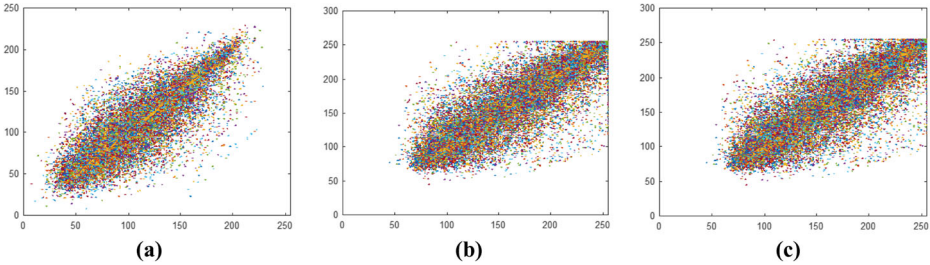

Fig. 15 **a** Blue channel horizontal correlation of plain image; **b** Blue channel diagonal correlation of plain image; **c** Blue channel vertical correlation of plain image

Figures 9, 10, 11, 12, 13, 14, 15 and 16, demonstrates the adjacent pixel correlation plots of the arbitrarily chosen 10,000 sets of nearby pixels along the horizontal, vertical and diagonal orders. The pixel distributions are stick towards the main diagonal which shows that the pixels of the original image are linearly correlated. But in case of encrypted images, the pixel's linear relation is break with the application of proposed encryption scheme and consequently, we have scattered pixels' distribution.

The adjacent pixel correlation results for different images are placed in Tables 2 and 3 and compassion of suggested techniques with already existing are available in Table 4. The results of the numerical values of correlation coefficient suggested that our proposed scheme is capable of adding confusion and removing pixels neighboring relation. The suggested technique dissociates nearby pixels in the plaintext picture after the encryption procedure. It beats the recorded encryption schemes [24, 35].

Tables 12 and 13 shows the values of NPCR (>99%) and UACI (≈33%) for each digital color image component for three commonly diverse standard images. By investigating obtained results clearly reflects that the estimated values of NPCR and UACI are very close to the theoretical values, which justify the validity of theoretical values. Therefore, the suggested enciphering technique is resistant against differential attacks.

The NIST suit is tested for the proposed image encryption technique. The NIST suit fundamentally consist of number of randomness tests used to examine the degree of randomness in any digital content for instance text, image, audio and video files. The results of NIST suit for our offered encryption scheme suggest that our scheme combat against different cryptographic attacks. The true values for each component in NIST suit must be greater than 0.01 in order to pass each tests. The results of NIST for encrypted digital image of Lena is calculated in Table 14. The closed investigation of Table 14, we can simply draw a conclusion that our proposed scheme clearly satisfies each tests of randomness.

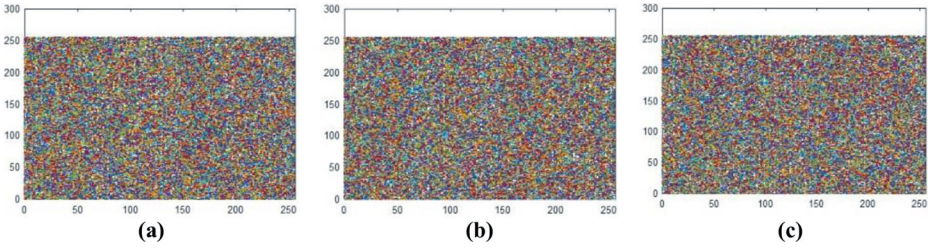

Fig. 16 **a** Blue channel horizontal correlation of encrypted image **b** Blue channel diagonal correlation of encrypted image **c** Blue channel vertical correlation of encrypted image

Table 2 Correlation coefficient of various plain and encrypted images

Image	Plain image			Encrypted image		
	Correlation coefficient			Correlation coefficient		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.9518	0.9293	0.9769	0.0054	0.0054	0.0016
Baboon	0.8727	0.7938	0.8914	0.0011	−0.0001	0.0003
Peppers	0.9465	0.9108	0.9394	0.0008	0.0013	0.0011

Table 3 Correlation coefficient of red, green and blue channels for various images

Channel	CC	Lena		Baboon		Ref. [44]
		Plain	Cipher	Plain	Cipher	
R	HC	0.9556	0.0017	0.9483	−0.0007	−0.00201
	DC	0.9339	0.0049	0.9103	−0.0077	0.00293
	VC	0.9786	−0.0004	0.9347	0.0023	−0.00164
G	HC	0.9571	0.0011	0.9068	0.0057	−0.00149
	DC	0.9372	−0.0002	0.8394	−0.0002	−0.00221
	VC	0.9795	0.0076	0.8861	0.0043	0.00349
B	HC	0.9187	−0.0030	0.9465	0.0056	0.00055
	DC	0.8837	0.0049	0.9108	−0.0040	0.00037
	VC	0.9590	0.0050	0.9394	0.0002	−0.00092

Table 4 Comparison of correlation coefficient different direction

Direction	Horizontal	Diagonal	Vertical
Original Image	0.9518	0.9293	0.9769
Proposed	0.0054	0.0054	0.0016
Ref. [36]	0.0681	0.0128	0.0049
Ref. [15]	0.2157	0.0008	0.0011
Ref. [11]	0.0072	0.0026	0.0010
Ref. [45]	0.0214	0.0054	0.0072
Ref. [43]	0.0820	0.0042	0.0003

Table 5 MSE and PSNR values of red, green and blue channels for various images

Images	Channels	Size	Projected Techniques	
			MSE	PSNR
Lena	Red	256 × 256	10,801.21	7.7930
	Green	256 × 256	10,856.16	7.7739
	Blue	256 × 256	10,951.82	7.7363
Baboon	Red	256 × 256	10,934.26	7.7432
	Green	256 × 256	10,935.44	7.7427
	Blue	256 × 256	10,921.30	7.7482
Peppers	Red	512 × 512	10,887.08	7.7618
	Green	512 × 512	10,922.29	7.7478
	Blue	512 × 512	10,883.17	7.7635

Table 6 Comparison of average MSE and PSNR values with existing values of various images

Images	Size	Projected Technique		Ref. [40]		Ref. [23]	
		Avg. MSE	Avg. PSNR	MSE	PSNR	MSE	PSNR
Lena	256 × 256	10,869.73	7.7677	4859.03	11.30	10,351	9.5513
Baboon	256 × 256	10,930.33	7.7447	6399.05	10.10	8053	9.3214
Pepper	512 × 512	10,897.50	7.7577	7274.44	9.55	9050	8.9455

Table 7 Entropy values of red, green and blue channels for various images

Images	Channels	Size	Entropy values
Lena	Red	256 × 256	7.9973
	Green	256 × 256	7.9972
	Blue	256 × 256	7.9975
Baboon	Red	256 × 256	7.9972
	Green	256 × 256	7.9970
	Blue	256 × 256	7.9977
Pepper	Red	512 × 512	7.9993
	Green	512 × 512	7.9992
	Blue	512 × 512	7.9993

Table 8 Comparison of Entropy value for red, green and blue channels of Lena image

Algorithms	Channels Entropy values		
	Red	Green	Blue
Proposed Algorithm	7.9973	7.9972	7.9975
Ref. [31]	7.9791	7.9802	7.9827
Ref. [39]	7.9893	7.9898	7.9894

Table 9 Entropy values for various test images

Image name	Size	Projected Technique Evaluated value
Lena	256 × 256	7.9990
Baboon	256 × 256	7.9991
Peppers	512 × 512	7.9998

Table 10 Comparison of proposed entropy value with existing values

Algorithm	Size	Projected Technique Entropy
Proposed	256 × 256	7.9990
Sun's algorithm [42]	256 × 256	7.9965
Baptista's algorithm [42]	256 × 256	7.9260
Wong's algorithm [42]	256 × 256	7.9690
Xiang's algorithm [42]	256 × 256	7.9950

Table 11 MAE test analysis for Lena, Baboon and Pepper images

Image name	Size	Projected Technique MAE	Ref. [23] MAE
Lena	256 × 256	87	77.35
Baboon	256 × 256	92	73.91
Pepper	512 × 512	92	–

Table 12 Channel wise NPCR and UACI test analysis

Image name	Size	Test Type	Red channel	Green channel	Blue channel
Lena	256 × 256	NPCR	99.58	99.56	99.64
	256 × 256	UACI	33.27	33.36	33.50
Baboon	256 × 256	NPCR	99.62	99.60	99.60
	256 × 256	UACI	33.47	33.48	33.45
Pepper	512 × 512	NPCR	99.60	99.60	99.61
	512 × 512	UACI	33.39	33.46	33.40

Table 13 Comparison of NPCR and UACI values

Images name	Size	Tests	Combined layers	Ref. [37]
Lena	256 × 256	NPCR	99.60	99.60
	256 × 256	UACI	33.37	33.55
Baboon	256 × 256	NPCR	99.61	99.60
	256 × 256	UACI	33.51	33.41

Table 14 NIST test analysis for different layers of encrypted Lena image

Test Name	Red	Green	Blue	Remarks
Frequency	0.54795	0.087705	0.94957	Success
Block Frequency	0.65797	0.61164	0.93047	Success
Run (m = 10,000)	0.25729	0.047794	0.61293	Success
Long runs of ones	0.7127	0.71270	0.7127	Success
Rank	0.29191	0.291910	0.1600	Success
Spectral DFT	0.88464	0.66336	0.29191	Success
No overlapping	0.8011	0.71242	0.9994	Success
Overlapping	0.76598	0.81656	0.85988	Success
Universal	0.98681	0.99321	0.99282	Success
Serial	7.9952e-05	2.3066e-08	0.81968	Success
Serial	9.8805e-06	6.6784e-05	0.66153	Success
Approx. Entropy	0.71663	0.035714	0.82344	Success
Cumulative sum forward	0.2243	0.039901	0.24268	Success
Cumulative sum reverse	0.94313	0.096191	0.98587	Success

5 Conclusion

In this paper we have introduced an encryption algorithm based on multiple chaotic maps with minimum rounds of encryption. The multiple chaotic map added confusion and diffusion capability projected encryption scheme. The suggested scheme is further tested against different encryption quality measures in order to gauge the strength of encryption technique. The results of performance suggested that the proposed scheme show better resistance against different attacks. The method can be extended to other multimedia contents such as audio and video files. All of the cryptographic strengths characteristics indicated that our suggested technique is appropriate for digital image encryption.

Acknowledgments The authors of this article are highly thankful to Vice Chancellor Dr. Syed Willayat Hussain, Dean Iqbal Rasool Memon and Director Cyber and Information Security Lab Dr. Muhammad Amin, Institute of Space Technology, Islamabad Pakistan, for providing decent atmosphere for research and development.

Compliance with ethical standards

Conflict of interest There is no any conflict of interest between the authors regarding the publication of this articles.

References

1. Abokhdair NO, Manaf ABA, Zamani M, (2010) Integration of chaotic map and confusion technique for color medical image encryption. In: 6th International Conference on Digital Content, Multimedia Technology and its Applications, pp 20–23. IEEE
2. Ahmad M (2011) Cryptanalysis of chaos based secure satellite iImagery cryptosystem. In: Aluru S. et al. (eds) Contemporary Computing. IC3 2011. Communications in Computer and Information Science, vol 168. Springer, Berlin, Heidelberg
3. Ahmad M, Ahmad T (2012) A framework to protect patient digital medical imagery for secure telediagnosis. Procedia Engineering 38:1055–1066
4. Ahmad M, Ahmad T (2014) Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys. International Journal of Communication Networks and Distributed Systems 12(1):113–128
5. Ahmad M, Chugh H, Goel A, Singla P (2013) A chaos based method for efficient cryptographic S-box design. In: Thampi S.M., Atrey P.K., Fan CI., Perez G.M. (eds) Security in Computing and Communications. SSCC 2013. Communications in Computer and Information Science, vol 377. Springer, Berlin, Heidelberg
6. Alsmirat MA, Al-Alem F, Al-Ayyoub M, Jararweh Y, Gupta B (2018) Impact of digital fingerprint image quality on the fingerprint recognition accuracy. Multimed Tools Appl 78 (2019): 3649–3688
7. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos 16(08):2129–2151
8. Amigo JM, Kocarev L, Szczepanski J (2007) Theory and practice of chaotic cryptography. Phys Lett A 366(3):211–216
9. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimed Tools Appl 76(18): 18451–18472
10. Baptista MS (1998) Cryptography with chaos. Phys Lett A 240(1–2):50–54
11. Enayatifar R, Abdullah AH, Isnin IF (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Lasers Eng 56:83–93

12. Gupta BB (ed) (2018) Computer and Cyber Security. New York: Auerbach Publications. https://doi.org/10.1201/9780429424878
13. Gupta, B., Agrawal, D.P. and Yamaguchi, S. eds., 2016. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global. https://doi.org/10.4018/978-1-5225-0105-3
14. Hénon M (1976) A two-dimensional mapping with a strange attractor. Commun. Math. Phys., 50, 69–77
15. Huang CK, Nien HH (2009) Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 282(11):2123–2127
16. Huh JH (2018) PLC-integrated sensing Technology in Mountain Regions for drone landing sites: focusing on software technology. Sensors 18(8):2693
17. Huh JH, Seo K (2018) Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. J Supercomput 75 (6) (2019): 3123–3139
18. Ismail IA, Amin M, Diab H (2010) A digital image encryption algorithm based a composition of two chaotic logistic maps. IJ Network Security 11(1):1–10
19. Jolfaei A, Mirghadri A (2010) An applied imagery encryption algorithm based on shuffling and baker's map. In: Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10), Florida, USA, pp 279–285
20. Khan M (2015) A novel image encryption scheme based on multiple chaotic S-boxes. Nonlinear Dynamics 82(1–2):527–533
21. Khan M, Asghar Z (2018) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation. Neural Comput & Applic 29(4):993–999
22. Khan M, Shah T (2014) A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dynamics 76(1):377–382
23. Khan M, Shah T (2015) An efficient chaotic image encryption scheme. Neural Comput & Applic 26(5): 1137–1148
24. Khan M, Shah T, Gondal MA (2013) An efficient technique for the construction of substitution box with chaotic partial differential equation. Nonlinear Dynamics 73(3):1795–1801
25. Khan M, Shah T, Batool SI (2016) Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Comput & Applic 27(3):677–685
26. Khan M, Shah T, Batool SI (2017) A new approach for image encryption and watermarking based on substitution box over the classes of chain rings. Multimed Tools Appl 76(22):24027–24062
27. Li J, Yu C, Gupta BB, Ren X (2018) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Multimed Tools Appl 77(4):4545–4561
28. Liao X, Yin J (2018) Two Embedding Strategies for Payload Distribution in Multiple Images Steganography. In: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp 1982–1986. IEEE
29. Liao X, Yin J, Guo S, Li X, Sangaiah AK (2018) Medical JPEG image steganography based on preserving inter-block dependencies. Comput Electr Eng. 67 (2018): 320-329
30. Liao X, Guo S, Yin J, Wang H, Li X, Sangaiah AK (2018) New cubic reference table based image steganography. Multimed Tools Appl 77 (8): 10033–10050
31. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16–17):3895–3903
32. Mastan JMK, Sathishkumar GA, Bagan KB (2011, July) A color image encryption technique based on a substitution-permutation network. In International conference on Advances in Computing and Communications 524-533, Springer, Berlin, Heidelberg
33. Matthews R (1989) On the derivation of a "chaotic" encryption algorithm. Cryptologia 13(1):29–42
34. Patidar V, Pareek NK, Purohit G, Sud KK (2011) A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Opt Commun 284(19):4331–4339
35. Rafiq A, Khan M (2018) Construction of new S-boxes based on triangle groups and its applications in copyright protection. Multimed Tools Appl:1–18. https://doi.org/10.1007/s11042-018-6953-x
36. Rhouma R, Meherzi S, Belghith S (2009) OCML-based colour image encryption. Chaos, Solitons Fractals 40(1):309–318
37. Seyedzadeh SM, Norouzi B, Mosavi MR, Mirzakuchaki S (2015) A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dynamics 81(1–2):511–529
38. Sharma PK, Ahmad M, Khan PM (2014) Cryptanalysis of image encryption algorithm based on pixel shuffling and chaotic S-box transformation. In International Symposium on Security in Computing and Communication 173-181, Springer, Berlin, Heidelberg
39. Wu X, Li Y, Kurths J (2015) A new color image encryption scheme using CML and a fractional-order chaotic system. PLoS One 10(3):e0119660
40. Younas I, Khan M (2018) A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. Entropy 20(12):913

41. Yu C, Li J, Li X, Ren X, Gupta BB (2018) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimed Tools Appl 77(4):4585–4608
42. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284(12):2775–2780
43. Zhang L, Liao X, Wang X (2005) An image encryption approach based on chaotic maps. Chaos, Solitons Fractals 24(3):759–765
44. Zhang W, Wong KW, Yu H, Zhu ZL (2013) A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci Numer Simul 18(3):584–600
45. Zhen P, Zhao G, Min L, Jin X (2016) Chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl 75(11):6303–6319