Multimedia Tools and Applications (2021) 80:24069–24110
https://doi.org/10.1007/s11042-021-10839-7

A chaotic framework and its application in image encryption

Mousomi Roy[1] · Shouvik Chakraborty[1] · Kalyani Mali[1]

Received: 5 May 2020 / Revised: 8 December 2020 / Accepted: 10 March 2021 /
Published online: 30 March 2021

Abstract
A novel image encryption framework is proposed in this article. A new chaotic map and a pseudorandom bit generator are proposed. Apart from this, a novel image encryption system is designed based on the proposed map and the proposed pseudorandom bit generator. These three are the major contributions of this work that makes a complete cryptosystem. The proposed new chaotic map is proposed which will be known as the 'RCM map' and its chaotic property is studied based on Devaney's theory. The proposed pseudorandom bit generator is tested using the NIST test suite. The proposed method is simple to implement and does not involve any highly complex operations. Moreover, the proposed method is completely lossless, and therefore cent percent of data can be recovered from the encrypted image. The decryption process is also simple to implement i.e. just reverse of the encryption procedure. A scrambling algorithm is also proposed to further enhance the security of the overall system. The simulation, detailed analysis, and comparative studies of the proposed overall image encryption framework will help to understand the strengths and weaknesses of it. The experimental results are very promising and show the prospects of chaos theory and its usage in the field of data security.

Keywords Chaos theory · Chaotic maps · Cryptography · Pixel scrambling · Cryptanalysis · Pseudorandom bit generator

✉ Shouvik Chakraborty
shouvikchakraborty51@gmail.com

Mousomi Roy
iammouroy@gmail.com

Kalyani Mali
kalyanimali1992@gmail.com

[1] Department of Computer Science & Engineering, University of Kalyani, Kalyani, India

1 Introduction

The theory of chaos is an important and interesting field of study for a long time. Various applications of chaotic systems can be observed in different domains like physics, mathematics, computer science, etc. [4, 5, 10, 35]. The research in the field of chaos is evolving since the seventieth century and gradually progressing and its advantages are exploited by various domains. The field of data security is no exception and is continuously trying to exploit the advantages of chaos theory in various ways. In recent years, the field of image security is a very attractive topic of interest and becomes a hotspot in the study of data security. A huge number of images are transmitted every second over various networks. The advent of various social media platforms brings a sudden growth in the transmission of images and other multimedia content over the internet. Images and other multimedia data may contain various sensitive and personal information that needs to be preserved and communicated confidentially [45]. Data can be preserved in both online and offline modes. Online storages are available nowadays at a very cheap rate which increases its popularity and many people can afford them [8, 9]. Therefore, in another sense, the advancements and growth in science and technology increase the chance of data leakage from various sources. Therefore, data security is an active and prominent challenge and is to be defeated. This is the main reason behind the continuous effort of the researchers who are engaged to solve this problem, to secure the data communication process, and to make the data safe at the storage locations. It is necessary to protect privacy and confidential data because sometimes, unintentional data leakage can be very costly and can reveal various precious information about a person or an organization. So, data confidentiality and integrity must be maintained to ensure reliable and secure communication.

Steganography is considered as one of the most important topics that are to be discussed in the context of the secured data communication. Typically, image-based steganography approaches conceal an image into another image or in more than one image. The image or the set of images in which an actual confidential file is made hidden is typically not a secret file. Sometimes, steganography can be associated with the encryption process to make the overall system stronger. The encrypted digital image is kept inside of another image that can be shared publicly. Steganography is in active use for many centuries and it covers various techniques that provide a protective cover or a safeguard for the original messages. Two payload distribution strategies are developed for the steganographic purposes in [34]. These two approaches can effectively distribute the original content into multiple images and these approaches are based on texture-based features. Both approaches can be combined applied for image steganographic purposes. Experimental results prove that the performance of this approach can outperform some of the standard approaches. A convolutional neural network-based operation-chain detection mechanism is proposed in [33]. In this work, a novel framework is proposed to detect various tampering that has been performed on an image. This work is helpful in forensic investigations and can detect two image operations without knowing anything about the operations beforehand. This work proves to be efficient in detecting various operations automatically and also capable to detect the order to some extent. A comprehensive detail about steganography and its recent advancements can be found in [1].

Various methods and frameworks are available in the literature that can be used to secure images and videos [11, 12, 38, 44, 46, 49, 63]. Several traditional methods and their variants like, DES [13], AES [16], IDEA [32] etc. and other modern methods like chaotic system based techniques [11, 51, 63, 75], DNA computing based security methods [14, 19, 49, 56] and many more advanced methods can be found in literature. Chaotic systems are frequently used

in various applications including cryptography. A large number of methods are available in the literature that exploits different properties of chaotic systems like ergodicity, sensitivity to the initial conditions, pseudorandom behavior, mixing features, etc. [17]. Some chaotic properties and their mapping in the cryptography are given in Table 1. Some of the recent developments in the chaotic cryptosystems are discussed here. A chaos-based image encryption method is presented in [2] where a larger keyspace can be obtained with a single round of encryption. The correlation among the pixels is removed with the help of the chaotic sequences. This algorithm is tested by performing various experiments and proves the strength of various attacks. Different properties make this method suitable for various real-life applications. An integrated chaotic system based image encryption system is proposed in [30] where a complex chaotic map is generated and some of the existing problems are overcome. The efficiency of the chaotic map is proved using an image encryption system which is proved to have a large keyspace and robust against various attacks. A discrete chaotic map called 2D-TFCDM is proposed in [36]. This map is based on the discrete fractional calculus. Chaotic properties are numerically analyzed. Elliptic curves and the chaos are applied for the image encryption purpose. Chaotic map and the bitplane decomposition method are applied simultaneously in [41]. A one-dimensional chaotic map is used for the diffusion process and the beta map is used to scramble the bit planes. The key space is large enough and the execution time of this method is also low. A piecewise linear chaotic map-based image encryption method is proposed in [60]. A couple of binary sequences are generated using the bitplane decomposition method and then the diffusion procedure is applied in such a way so that the sequences become sensitive to a small change in the actual image. The piecewise linear chaotic map is used to control the confusion process. This algorithm is tested using many standard validation parameters and found to be robust against various types of attacks. A symmetric key image encryption system is developed in [6] which is based on the mixed chaotic map. A one-dimensional chaotic map is mixed up with a distinctive chaotic map to use in the image encryption process. Various experiments prove that the proposed method is highly resilient against various types of attacks and highly complex to provide better security. A multi-image encryption method based on piecewise linear chaotic map is proposed in [69]. This method can encrypt more than one image simultaneously. The proposed algorithm outperforms some of the established methods in terms of various standard parameters. A color image encryption method is proposed in [25]. This method is based on the well-known logistic map and the double random-phase encoding. The logistic map is used for the diffusion purpose and the double random-phase encoding system is used to combine all scrambled images into one encrypted image. Different experiments prove the efficiency of this method. An image encryption system is proposed in [67] which is based on the lifting scheme and chaotic maps. This method overcomes some security problems which are associated with the permutation-substitution models. At first, the input image divided into high and low-frequency components, and then chaos theory is used to

Table 1 Mapping of some chaotic properties and their corresponding cryptographic properties

Chaotic systems	Cryptography
Set of real numbers	Finite collection of integers
Secret key/set of keys	Values of seeds and controlling parameters
Confusion	Ergodicity
Diffusion	Sensitivity to the initial conditions

disturb these components. After that, the lifting scheme is used for the image encryption purpose. Experiments show the superiority of this method compared to some other methods. An image encryption method based on a one-dimensional sine powered chaotic system is proposed in [39]. A one-dimensional sine powered chaotic system is used to enhance security by performing the sequence addition. This method is tested and compared with some other methods and its performance is found to be satisfactory. A novel image encryption strategy is proposed in [43] based on chaos theory. In this work, the expand-shrink operation is incorporated in the chaotic environment for confusion and diffusion purposes. The confusion and the diffusion mechanism are applied at the pixel level. The actual image is expanded depending on the biplanes. The Hilbert scan approach is adopted to implement the confusion and diffusion approach. The experimental outcomes show that this approach performs well compared to some of the existing approaches. An another novel image encryption approach is proposed in [18]. This approach involves fractional Fourier transform and DNA sequence operation along with the chaotic environment. A chaotic Lorenz map is used to generate the random phase masks. This approach is proved to be efficient enough and proved to be resilient against different types of attacks. Experimental results show that this approach is reliable enough for real-life digital image encryptions. A chaos-based satellite image encryption system is proposed in [7]. This approach incorporates Fridrich's scheme to encrypt multispectral images. The experimental outcome show that this approach can achieve a good level of security with lesser hardware requirements and can get a throughput of120mbit/s. Some of the recent chaotic environment based image encryption approaches are discussed in detail in [22, 29, 40]. A data security approach is designed in [28] for the cloud environment that is based on hierarchal identity. This approach is useful to protect the cloud data from unauthorized persons and also helps in securing the cloud data from getting tampered with. This approach ensures the security of the cloud data storage and also takes care of the delivery of the data to legitimate users. A novel image encryption mechanism is proposed in [71] to provide security to the railway cloud services. This approach is based on the combination of the S-box coupled map lattice and chaotic environment. This approach overcomes some of the drawbacks of some of the previous approaches and experimental results prove the efficiency of this combined approach. A secured data communication and storage framework is proposed in [74]. This proposes a novel attribute-based image encryption method to secure the contents of the cloud as well as helping to maintain data integrity throughout the communication process. Experimental results provide proof of the effectiveness and efficiency of the proposed approach. A data security and encryption scheme is designed in [62] that is specifically designed to provide security to the data in the DaaS or database as a service cloud model. This work uses the DSP re-encryption method to design the new encryption framework besides developing an efficient access control mechanism. Experiments prove the efficiency and correctness of this approach. Elliptic-curve cryptography-based authentication mechanism is proposed in [52]. This approach is primarily designed for IoT based networks. Promela model and SPIN tool are used to validate the security and authentication approach.

In this article, a new chaotic map is proposed (which will be known as the 'RCM map' and in the rest of the article, the proposed map is referred to with this name) along with a pseudorandom bit generation method which is based on the proposed chaotic map. The proposed chaotic map and the pseudorandom bit generator is used to construct an image encryption method. The proposed new image encryption method is robust, resilient against different types of attacks, and useful for both grayscale and color images. This approach is completely independent of any external image and the core part of the proposed image

encryption method is designed using the proposed RCM chaotic map and the pseudorandom bit generator. The proposed algorithm involves a dimension transformation phase that generates a color encrypted image if the input image is in grayscale mode. If the input image has more than one channel (e.g. color images) then multiple encrypted images will be generated. The number of encrypted images is equivalent to the number of channels present in the encrypted image. The correlation of the pixels is disturbed using a new scrambling algorithm which is proposed in this work, however, the proposed scrambling method is flexible enough and can be easily modified and any permutation of the chaotic sequence can be used for a certain channel (please refer Section 4 for detailed description). The decryption method is completely lossless, easy to implement, and can be easily executed by performing the exactly reverse operations of the encryption method. The efficiency and the effectiveness of the proposed image encryption method are established via simulation and different experiments in both visual and quantitative manner.

This article contributes to the existing literature in three different ways. First of all, a new chaotic map called RCM is proposed in this work. The second one is, A pseudorandom bit generator is proposed that is based on the proposed RCM map. And the last one is, a novel image encryption system is designed based on the proposed RCM map and the proposed pseudorandom bit generator. These three are the major contributions of this work that makes a complete cryptosystem. Each individual contribution is analyzed separately and their advantages are depicted. For example, the proposed RCM map is analyzed in Section 2. Similarly, the proposed pseudorandom bit generator is analyzed in Section 3. The proposed encryption scheme is also analyzed and compared in Section 5. Therefore, the superiority of the proposed approach is established individually for three different contributions. The large keyspace makes the proposed approach resilient against exhaustive search-based attacks. Moreover, the experimental results show that the proposed approach can withstand different possible attacks that make it secured and acceptable for different real-life applications. Theoretical and experimental analysis build the foundation of the practical applicability of the proposed cryptosystem.

1.1 Motivation

No method can be claimed as a cent percent secured against various attacks. In most of the works, standard chaotic maps like logistics, tent, etc. are used for encryption purposes. Some traditional approaches like DES, AES are suitable for independent and identically distributed data. Typically, the distribution of multimedia data is not independent and identically distributed. Hence, the traditional approaches are not always suitable for multimedia data [5]. Although the strength of these approaches is already proved on different types of data but, the non-independent and non-identical nature of the multimedia data can often cause some serious problems [5]. It is well-known that AES should not be used in a block-wise fashion, but, the effect of AES in ECB mode on a digital image is not satisfactory at all and can be visualized in [4].

With the ever-increasing need for image communications, it is required to design sophisticated image encryption schemes to make the image communication system efficient. It is always challenging to design Chaotic systems that possess some properties like ergodicity, sensitivity to the initial conditions, pseudorandom behavior, mixing features, etc. that are lucrative from the perspective of the cryptosystem because these features can significantly increase the security of the overall encryption mechanism. Therefore, the main motivation of this proposed work is to design a new resilient and reliable cryptosystem for the images

because many traditional data security approaches are not suitable. Apart from this, an effort is paid to design a novel chaotic map and a pseudorandom bit generator that can support the proposed image encryption system. To enhance the security of the proposed approach image encryption system, a scrambling algorithm is also proposed and incorporated in the image encryption system. So, the proposed image encryption system is beneficial for real-life image communications. The benefits and the performance of the different components of the proposed framework are tested and discussed elaboratively in respective sections.

The remainder of this article is organized as follows: Section 2 describes the proposed RCM chaotic map. Section 3 illustrates the proposed pseudorandom bit generation method. Section 4 describes the proposed image encryption method which is based on the proposed RCM map and the proposed pseudorandom bit generation method. Section 5 shows the results of the simulation and a detailed performance analysis along with the security analysis of the proposed image encryption method can be found in Section 6. Section 7 concludes the article.

2 The proposed new chaotic map

The proposed chaotic map is defined in Eq. 1. The proposed map will be known as the 'RCM' chaotic map and in the remaining article, this map will be referred to by this name.

$$s_i = \psi \sin\left(e^{-s_{i-1}} \times \left(1 - s_{i-1}^3\right)\right) \tag{1}$$

Here, $s_0 \in [0, 1]$ is the initial value or the seed and $\psi \in [1, 4]$ is the control parameter or the bifurcation parameter. The proof of the chaotic nature of the above equation can be done using the definition given by the Devaney [54] and in the similar way as given in [68]. The definition of Devaney is given in definition 1 and the definition of the topological mixing map is given in the definition 2 [20].

Definition 1: Assume S is a set (metric space) and $f: S \rightarrow S$ is the continuous transformation of the metric space S. $f$can be called chaotic if it satisfies the following criteria:

i. f should be sensitive and have a high dependency on the initial conditions i.e. a small change in the initial condition results in a huge change in the output. Let us assume a constant $\alpha > 0$ which is known as the sensitivity constant. Now, for every $\widehat{s} \in S$and for every open interval I about $\widehat{s}$, there is some $\widehat{i} \in I$ and $p > 0$ such that, $\left| f^p(\widehat{s}) - f^p\left(\widehat{i}\right) \right| > \alpha$.
ii. f should be topologically transitive in nature. A dynamical system (S, f) can be called the topological transitive if for every non-empty pair $(x, y) \in S$, there must exist a non-negative integer a such that $f^a(x) \cap y \neq \phi$.
iii. Periodic points of f should be dense in S. Mathematically, every point that belongs to the attractor should be arbitrarily close to some particular point that belongs to a periodic orbit. Theoretically, if someone chose a point and a distance value $\sigma > 0$, there must be a periodic orbit, irrespective of the small value of σ, from the chosen point.

Definition 2: A continuous map $f: S \rightarrow S$ can be called as the topologically mixing map if for every non-empty subset $(u, v) \in S$, there must exist a non-negative integer K such that $f^k(u) \cap v \neq \phi$ where $k > K$.

Proposition 1: If a map is a topologically mixing map then it must be a topologically transitive map.

Proof. Expansion maps of S^1 are inherently topologically mixing maps.

Proposition 2: If an orbit is dense then it implies the transitivity property.

Proof. Every open subinterval can be visited by a dense orbit.

Proposition 3: If the space has more than one points then, every topologically mixing map is dependent on and sensitive to the initial conditions.

Proof. Assume that $f: S \rightarrow S$is a topologically mixing map and $|S| > 1$. Now consider two separate points $\widehat{s}_1, \widehat{s}_2 \in S$ and a set $\omega = \frac{1}{4} d(\widehat{s}_1, \widehat{s}_2) > 0$. If $k \gg K$ then, for every object $O(\widehat{s}, \varepsilon) \subseteq S$, $f^k(O(\widehat{s}, \varepsilon)) \cap O(\widehat{s}_1, \omega) \neq \phi$ and similarly $f^k(O(\widehat{s}, \varepsilon)) \cap O(\widehat{s}_2, \omega) \neq \phi$. Therefore, there exists $\widehat{t}_1, \widehat{t}_2 \in O(\widehat{s}, \varepsilon)$ and $f^k(\widehat{t}_i) \in O(\widehat{s}_i, \omega)$. Therefore, the following inequality can be written: $d\left(f^k(\widehat{t}_1), f^k(\widehat{t}_2)\right) \geq d(\widehat{s}_1, \widehat{s}_2) - d\left(\widehat{s}_1, f^k(\widehat{t}_1)\right) - d\left(\widehat{s}_2, f^k(\widehat{t}_2)\right) > 4\omega - \omega - \omega = 2\omega$. So, either $d\left(f^k(\widehat{t}_1), f^k(\widehat{s})\right) > \omega$ or $d\left(f^k(\widehat{t}_2), f^k(\widehat{s})\right) > \omega$.

2.1 Analysis of the proposed new chaotic map

In this section, the dynamics of the proposed chaotic map along with some other properties are discussed. The response of the chaotic map for 5000 iterations and the bifurcation diagram is given in Figs. 1 and 2 respectively.

In Fig. 1, the response value is plotted on the y-axis and the number of iterations is plotted on the x-axis. From Fig. 1, it can be observed that the response values are plotted for 5000

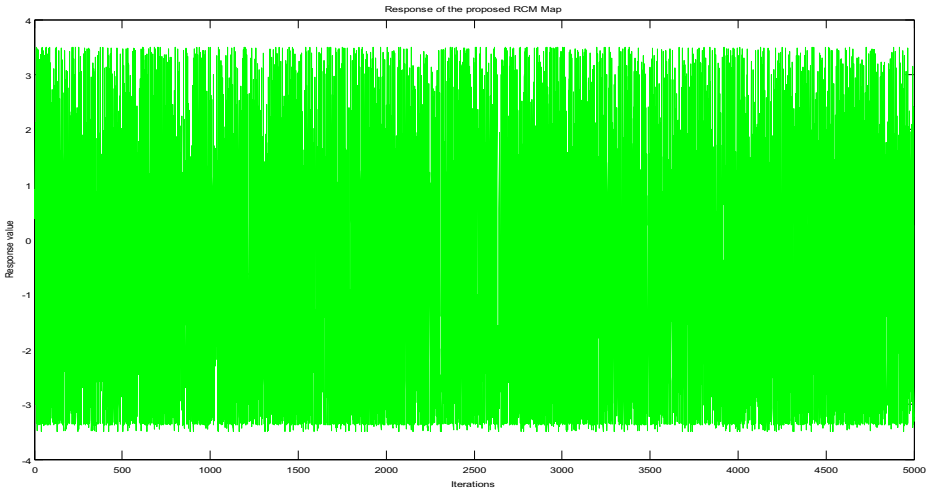


Fig. 1 Response of the proposed RCM chaotic map for 5000 iterations

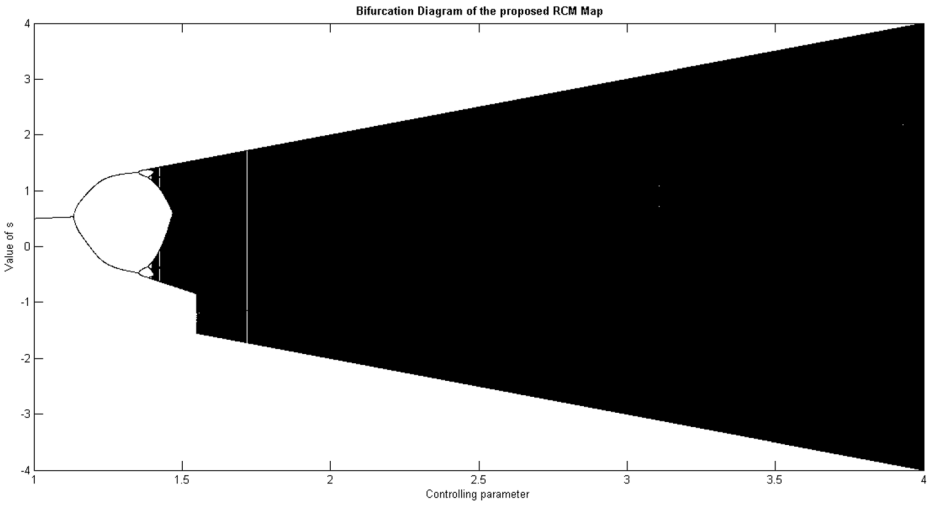


Fig. 2 Bifurcation diagram of the proposed RCM map

iterations and the range of the response values in the y axis is from −4 to +4. This figure helps to understand the fluctuations and the randomness of the proposed RCM chaotic map.

In Fig. 2, the value of the state parameter s is plotted on the y-axis and the value of the controlling parameter or the bifurcation parameter is plotted in the x-axis.

2.2 Lyapunov exponent

Lyapunov exponent or the Lyapunov characteristic exponent is a property of the dynamical systems. This parameter explains the divergence rate of the adjacent trajectories [50]. This property is helpful to understand the chaotic behavior of a chaotic map. The larger value of this parameter shows the more chaotic behavior of the corresponding chaotic map. The Lyapunov exponent λ can be calculated using Eq. 2.

$$\lambda = \lim_{N\to+\infty} \frac{1}{S} \sum_{p=1}^{S} \log\left|\frac{dx_{p+1}}{dx_p}\right| \tag{2}$$

The Lyapunov exponent of the proposed chaotic map is given in Fig. 3. A comparative study is presented in Table 2 where the Lyapunov exponent of the proposed chaotic map is compared with some other chaotic maps. From this table, it is clear that the value of the Lyapunov exponent for the proposed RCM map is higher than the other chaotic maps including the well-known logistic map.

In Fig. 3, the value of the Lyapunov exponent or the Lyapunov characteristic exponent is plotted on the y-axis and the value of the control parameter or the bifurcation parameter is plotted on the x-axis. Figure 3 helps to visualize the Lyapunov exponent.

2.3 System complexity analysis

Approximate entropy is one of the important parameters that are useful to understand the complexity of the system. It is helpful for quantitative analysis of the system complexity [42].

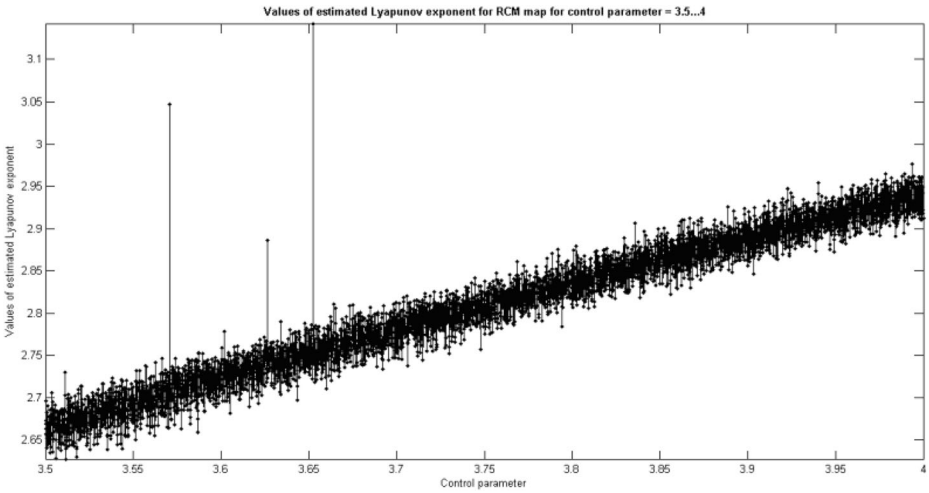


Fig. 3 Lyapunov exponents for proposed RCM map

Larger approximate entropy value indicates higher complexity of the system. Let us assume that D is the number of data points $\{d(i)\}$ taken from vector sequences $v(1)$ to $v(D-m+1)$ and it is defined in Eq. 3.

$$v(i) = [d(i), \ldots d(i+m-1)] \tag{3}$$

Here, m represents the dimension of the vector.

The distance between two vectors $v(i)$ and $v(j)$ $dist(v(i), v(j))$ can be calculated using Eq. 4.

$$dist(v(i), v(j)) = \max_{t=0\sim m-1} |d(i+t) - d(j+t)| \tag{4}$$

Now, let us assume a threshold value th, $(th > 0)$, η_i^m can be calculated using Eq. 5.

$$\eta_i^m(th) = \frac{The \quad count \quad of \quad dist(v(i), v(j))}{(M-m+1)} \tag{5}$$

From Eq. 5, the value of the η_i^m can be obtained which can be further used to compute the value of $\Phi^m(th)$. This value can be computed using Eq. 6.

$$\Phi^m(th) = \frac{1}{D-m+1} \sum_{i=1}^{D-m+1} \log_e \eta_i^m(th) \tag{6}$$

Table 2 Comparison of the Lyapunov exponents

Chaotic Map	Value of the Lyapunov exponent
Logistic (for controlling parameter=4)	0.6826
$x_{i+1} = 2x_i^2 - 1$	0.6876
Cross chaotic map [68]	1.5592
Proposed RCM map (for controlling parameter=3.6525)	3.1417
Proposed RCM map (for controlling parameter=4.0)	2.9122

The approximate entropy AE can be obtained using Eq. 7.

$$AE(m, th, D) = \Phi^{m}(th) - \Phi^{m+1}(th) \tag{7}$$

A comparative study is presented in Table 3 where the approximate entropy of the proposed chaotic map is compared with some of the chaotic maps. From this table, it is clear that the value of the approximate entropy for the proposed RCM map is higher than the other chaotic maps including the well-known logistic map.

The autocorrelation of the proposed RCM map is given in Fig. 4. The orbits of the proposed chaotic maps can be observed in Fig. 5.

3 The proposed new pseudorandom bit generator

The proposed chaotic map is used to generate a pseudorandom bit sequence and it is described in this section. First of all, two chaotic sequences of equal length n are generated using the proposed chaotic map with two different seed values using Eqs. 8 and 9. Here s_0 and t_0 are the initial seed values and ψ and ψ' are the controlling or the bifurcation parameters of the system. The seed values that is s_0 and $t_0$should not be same i.e. $s_0 \neq t_0$ and (s_0, $t_0 \in [0, 1]$).

In Fig. 4, the autocorrelation values are plotted on the y-axis corresponding to the time values that are plotted on the x-axis. This plot helps in visualizing the autocorrelation of the proposed RCM map.

Figure 5 depicts the orbits of the proposed RCM map i.e. the plot of the different states. It can be shown that Fig. 5a, 5b visually illustrate the state movements s(i) vs. s(i + 1), and s(i) vs. s(i + 3) respectively.

$$s_i = \psi \sin\left(e^{-s_{i-1}} \times \left(1 - s_{i-1}^3\right)\right) \tag{8}$$

$$t_i = \psi' \sin\left(e^{-t_{i-1}} \times \left(1 - t_{i-1}^3\right)\right) \tag{9}$$

In this specific experiment the seed values are considered as $s_0 = 0.5$ and $t_0 = 0.8$. Experiments can also be performed by taking any other seed values provided $s_0 \neq t_0$ condition is satisfied. One thing should be noted that the system parameter or the controlling parameter should be the same for both equations i.e. $\psi = \psi'$. It is necessary to make both the map surjective in a specific interval. Moreover, the value of the controlling parameter should be large enough, preferably near 4.0. The basic reason behind this concept is to obtain a significantly large interval for the initial seed values (i.e. s_0 and t_0).

Elements of each sequence must be between 0 and 1. Now, each value is converted into the IEEE 754 double-precision binary representation. Therefore, for each member of a particular

Table 3 Comparison of the approximate entropy

Chaotic Map	Value of the approximate entropy
Logistic (for controlling parameter=4)	0.718837
$x_{i+1} = 2x_i^2 - 1$	0.696589
Cross chaotic map [68]	1.069873
Proposed RCM map	1.09839

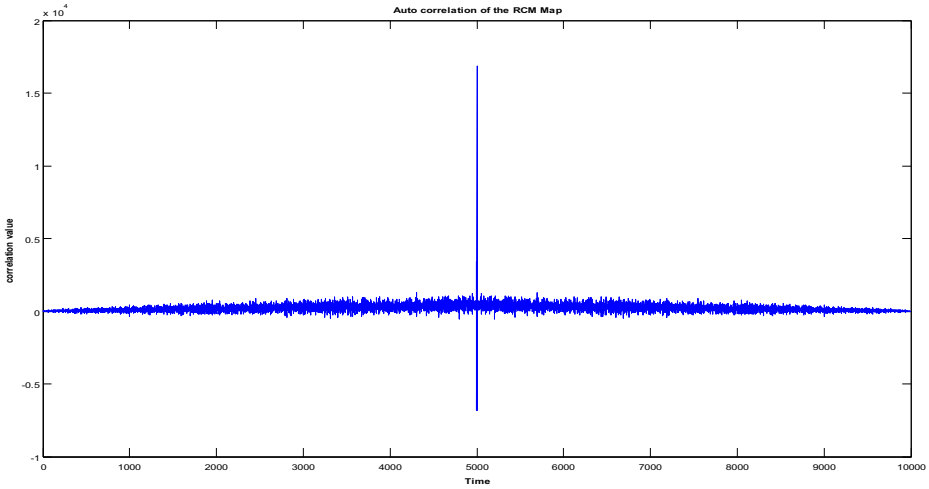


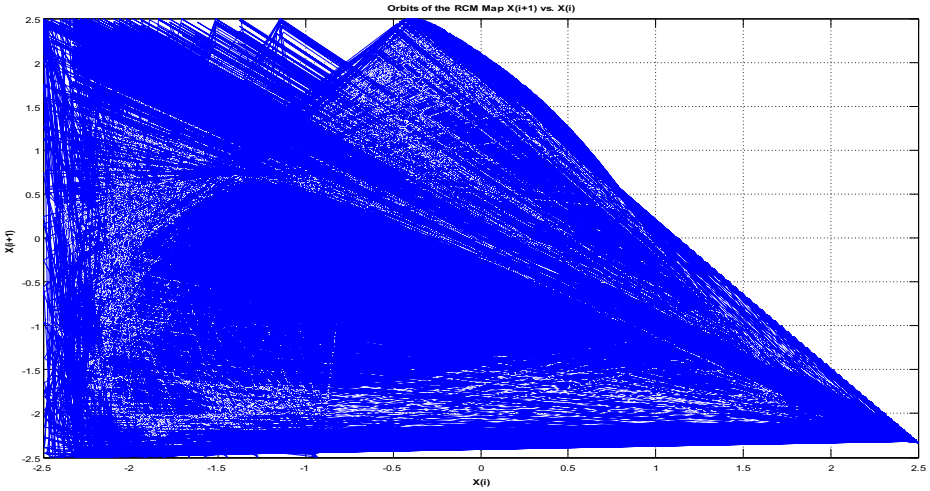
Fig. 4 Auto correlation of the proposed RCM map

sequence, there are corresponding 64 bits are generated [21] as shown in Fig. 6 where, the first bit or the MSB is the sign bit, next 11 bits are exponent and rest of the bits i.e. last 52 bits are mantissa. Now, these 64 bits are divided into 8 groups with 8 bits each.

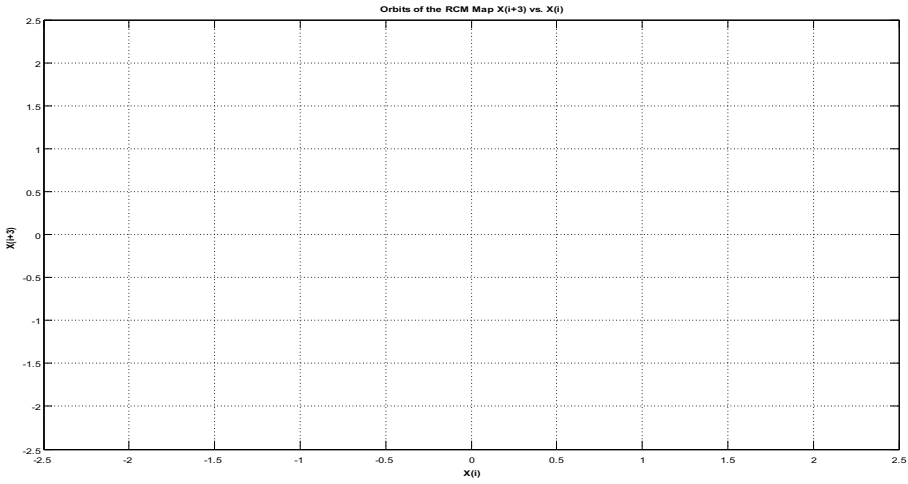
Now for each group, 8 bits are represented by a single bit. To get a single bit representative GR_b for the group, the following method is proposed. At first, the number of ones and number of zeros is counted to perform a majority voting i.e. if the number of ones is greater than the number of zeros then that particular group will be represented by 1 otherwise if the number of zeros is greater than the number of ones then that particular group will be represented by 0. For example, if a group is consisting of the following 8 bits i.e., then this group will be represented by 0 because of the majority of the number of zeros. Now, if a particular group contains an equal number of ones and zeros then, for that group, the representative bit $GR_b$is computed using Eq. 10 where GR_i represents the i^{th} bit of a group. For example, if a group is consisting of the following 8 bits i.e. 10110001the representative bit GR_b for this group will be 0. Now, by following the above procedures, 64 bits are reduced to 8 bits.

$$GR_b = remainder\left(\left|\sum_{i=1}^{4} GR_{2i} - \sum_{i=0}^{3} GR_{2i+1}\right|, 2\right) \tag{10}$$

The major problem which is associated with the aforementioned method is that there is a possibility to get a chain of the same bits to represent multiple groups. In the worst case, all representative 8 bits can be 0 or 1. To eliminate this possibility, one method is proposed that takes care of the consecutive three same bits i.e. the proposed methods eliminate the possibility of being similar consecutive three bits. Now to understand this method, let us assume three consecutive bits b_{-2}, b_{-1} and b. These three bits can have 8 possibilities but the third bit i.e. b is going to be determined on the basis of the previous two bits. It can be easily understood from Fig. 7a and if these three bits are going to be the same then, Y is the bit which is used to replace the third bit i.e. b. Figure 7b is the elaborated version of Fig. 7a that shows all possible 8 combinations and the required value of Y. From Fig. 7, it is clear that if b_{-2} and b_{-1} become same then, there is no



(a)



(b)

Fig. 5 Orbits of the proposed RCM map (**a**) s(i) vs. s(i + 1), (**b**) s(i) vs. s(i + 3)

option except to place the complementary bit of b_{-2} and b_{-1} at the third position i.e. b. Otherwise, the value of b can be kept as it is. Now, to achieve this, Fig. 7b is used to simplify the truth table using the Karnaugh map [27]. The simplification process can be visualized in Fig. 8. From this simplification, the logical expression for Ycan be obtained and it is given in Eq. 11. Here, · and + represents the standard Boolean AND and OR

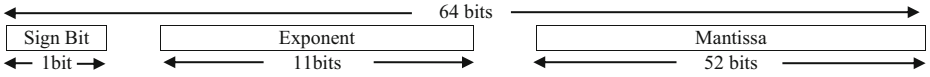


Fig. 6 IEEE 754 double precision floating point number representation format

b_{-2}	b_{-1}	Y
0	0	1
0	1	b
1	0	b
1	1	0

(a)

b_{-2}	b_{-1}	b	Y
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

(b)

Fig. 7 Possible combinations of the consecutive three-bit sequence **a** dependency of the third bit on the previous two bits, **b** elaborated table that shows the possible output value for all combinations of the consecutive three bits so that, no consecutive three bits can have the same value

operators respectively and $\overline{x}$ represents the complement of x (i.e. the Boolean NOT operation).

$$\begin{aligned} Y &= \overline{b}_{-2} \cdot \overline{b}_{-1} + \overline{b}_{-2} \cdot b + \overline{b}_{-1} \cdot b \\ &= \overline{b}_{-2} \cdot \left(\overline{b}_{-1} + b\right) + \overline{b}_{-1} \cdot b \end{aligned} \tag{11}$$

Now, each element of both the sequences can be represented by 8 bits. In each sequence of length n, there are $n * 8$ bits are present. Therefore, if a pseudorandom bit sequence of length n is to be generated then, the mapping ratio i.e. the number of bits which is to be mapped into a single bit in the pseudorandom bit sequence will be $mapRatio = \frac{number\ \ of\ \ bits\ \ in\ a\ sequence}{n}$ which is nothing but 8 in this case. Now, each sequence is divided into k number of groups with 16 elements in each group (because here, $2 * mapRatio = 16$). Now, perform XOR operation between the first 8 bits of the first sequence and the last 8 bits of the second sequence. Similarly, perform XOR operation between the first 8 bits of the second sequence and the last 8 bits of the first sequence. It is explained in Fig. 9 where, b_i^1 and b_i^2 are the i^{th} bit of the obtained groups from the first and second sequence respectively.

After this operation, two-bit sequences of length 8 bits can be obtained. Now, to convert each of them into a single bit, just perform an XOR operation with the consecutive bits as given in Eq. 12. Here, rb^k is the representative bit of the k^{th} sequence and x_j^k is the j^{th} bit of the k^{th} sequence. m represents the total number of bits present and for this experiment this value is 8.

$b_{-2} \setminus b_{-1} \cdot b$	00	01	11	10
0	1	1	1	0
1	0	1	0	0

Fig. 8 Karnaugh map simplification of the truth table which is given in Fig. 7b

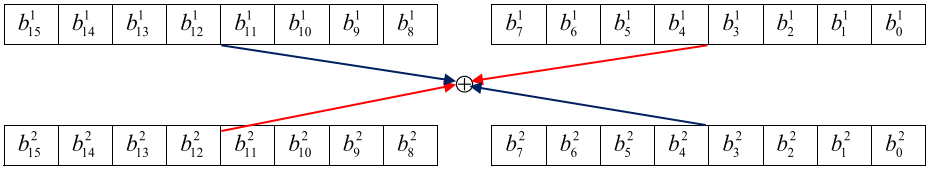


Fig. 9 Illustration of the XOR operation

$$rb^k = \left(\left(\left(\left(\left(x_{m-1}^k \oplus x_{m-2}^k\right) \oplus x_{m-3}^k\right) \oplus x_{m-4}^k\right) \oplus \ldots\ldots\ldots \oplus x_1^k\right) \oplus x_0^k\right) \tag{12}$$

The above procedure generates a pseudorandom bit sequence of length n. Now, to test the proposed pseudorandom bit generator, the well-known National Institute of Standards and Technology (NIST) statistical test suit is used [47]. As per the recommendation given in [48] 15 subtests are performed with the pseudorandom bit sequences of the length 1,000,000. The decisions are at the 1% level i.e. if the calculated $P-value < 0.01$ the sequence can be considered as non-random otherwise random. The result of the tests is given in Table 4. From the obtained results, it is clear that the proposed pseudorandom bit generator passes all the tests and therefore the proposed method is suitable enough for cryptographic applications.

4 The proposed image encryption method

In this section, one image encryption method is proposed which is based on the proposed RCM map and the proposed pseudorandom bit generator. The proposed method is tested on different types of images including grayscale, biomedical, biometric, color, and some other standard images. The proposed encryption algorithm is efficient enough to encrypt different types of images and the proposed method has no dependency on any extra image. The efficiency of the proposed method is illustrated in Section 6 by both visual and quantitative analysis. The encryption process begins with the transformation of the pixel dimension. Let us assume that an image I of size $M \times N$ is being encrypted and a pseudorandom bit sequence $prbs$ of length $M \times N \times 8$ is generated using the proposed pseudorandom bit generator and with the initial parameters (s_0, t_0, ψ_0). At first, every pixel of the image is converted into 8 bits binary representation. Now take the binary representation of two consecutive pixels $I(i,j)$ and $I(i,j+1)$where $1 \le i \le M$, $1 \le j \le N$ and reverse each of them individually. Now, divide each sequence into two halves where each of them consists of a nibble. Find the positions of the ones in the first half of the first sequence and the positions of the zeros in the second half of the first sequence considering LSB as the 0^{th} position. Again, find the positions of the ones in the second half of the second sequence and the positions of the zeros in the first half of the second sequence considering LSB as the 0^{th} position. The searching for both cases should begin from the LSB. The searched indexes are simply added by multiplying with the decimal positional weights. Therefore, in this method, a nibble can generate a maximum of a four-digit decimal number $dVal$ using Eq. 13 where n is the count of either 0 or 1 as per the above description and c_k is the k^{th} counting value from LSB.

Table 4 NIST test results for the proposed pseudorandom bit generator

Serial No.	Name of the test	P value	Result	Remarks
1	Frequency / Monobit Test	0.18622	Passed	
2	Frequency Test within a Block	0.16421	Passed	
3	Runs Test	0.039147	Passed	
4	Longest Run of Ones	0.99321	Passed	
5	Binary Matrix Rank Test	0.32697	Passed	
6	Discrete Fourier Transform (Spectral) Test	0.99793	Passed	
7	Non-overlapping Template Matching Test	0.92368	Passed	
8	Overlapping Template Matching Test	0.83319	Passed	
9	Maurer's "Universal Statistical" Test	0.63783	Passed	
10	Linear Complexity Test	0.64964	Passed	
11a	Serial Test	0.7591	Passed	P value 1
11b	Serial Test	0.78648	Passed	P value 2
12	Approximate Entropy Test	0.99379	Passed	
13a	Cumulative Sums (Cusum) Test	0.34477	Passed	Forward
13b	Cumulative Sums (Cusum) Test	0.49393	Passed	Reverse
14	Random Excursions Test	0.49049 0.99081 0.21415 0.68653 0.20455 0.29468 0.018924 0.53404	Passed	For eight states (i.e. -4 to +4 excluding 0), eight *P* values are generated.
15	Random Excursions Variant Test	0.22578 0.16852 0.15663 0.10785 0.12295 0.16238 0.39785 0.987 0.69282 0.67211 0.81959 0.72384 0.55035 0.5598 0.81832 0.77815 0.75407 0.93455	Passed	For eighteen states (i.e. -9 to +9 excluding 0), eighteen *P* values are generated.

$$dVal = \sum_{k=1}^{n} c_k \cdot 10^{k-1} \tag{13}$$

Now take the first 16 bits from the pseudorandom bit sequence and divide them into four blocks each consisting a nibble. Find the positions of the zeros in the first half of the first nibble and the positions of the ones in the second nibble. Again, find the positions of the ones in the third nibble and the positions of the zeros in the fourth nibble considering LSB as the 0^{th} position for each nibble. The searched indexes for every nibble are simply added separately by multiplying with the decimal positional weights using Eq. 13. The corresponding decimal value for every nibble of the pseudorandom bit sequence is to be added with the obtained decimal value of the corresponding nibbles of the pixels. Now every digit of the obtained sum is converted into binary. One important point that can be observed from this discussion is the obtained sum can be a maximum of 8642 (i.e. 4321*2). So, a maximum of 12 bits is sufficient to store the binary form of each digit sequentially. The 12 bits are divided in such a way so that the first digit from the left i.e. Most Significant Digit (MSD) gets 4 bits, the next two digits get 3 bits each and the last digit i.e. Least Significant Digit (LSD) gets 2 bits. The bit reservation pattern is shown in Fig. 10.

In this figure, the MSD indicates the first four bits i.e. (bit_{12}, bit_{11}, bit_{10}, bit_9), MSD-1 indicates the next three bits i.e. (bit_8, bit_7, bit_6), MSD-2 indicates the next three bits i.e. (bit_5, bit_4, bit_3), and LSD denotes the last three bits MSD-2 indicates the last two bits i.e. (bit_2, bit_1).

In this way, four decimal values are generated from two pixels which in turn generate 48 bits (i.e. 4*12 bits). Now, these 48 bits and 16 bits of the chaotic sequence are taken to perform the XOR operation. Chaotic 16 bits are replicated to make it 48 bits equivalent where the 16 bits of the middle are reversed. The obtained 48 bits are divided into 6 groups with 8 bits each. Each group is now converted into its decimal equivalent. So, we have 6 decimal values where each decimal value ranges from 0 to 255. Two sets are formed $\langle DecVal_1, DecVal_3, DecVal_5\rangle$ and $\langle DecVal_2, DecVal_4, DecVal_6\rangle$ where $DecVal_i \in \{0, 1, 2...255\}$ represents the corresponding decimal value of the i^{th} binary group. These sets represent a new pixel. Each members of the set are representing the values of three channels i.e. $\langle red, green, blue\rangle$.

So, the input image is transformed from two dimensions to three dimensions. The discussed method is very simple to implement and cost-effective because it involves some basic operations only. In this context, Fig. 11 can be helpful to understand the proposed method for dimension transformation. One important point can be observed here, a pixel of a grayscale image is transformed into a pixel that consists of three-color channels. It is worth mentioning that the proposed procedure is completely reversible. The process can be reversed and the original pixel can be regenerated by following the exactly reverse procedure of the proposed method. Therefore, the proposed transformation incurs zero loss, and a hundred percent of data can be retrieved. This transformation process is dependent on the pseudorandom bit sequence which is generated using the proposed chaotic map and the proposed pseudorandom bit generator. The process will continue until all pixels of the input image is processed accordingly. The proposed transformation method can also be applied to color images. In that case, three channels can be processed separately using the same method and three different color

12 bits

MSD				MSD-1			MSD-2			LSD	
bit_{12}	bit_{11}	bit_{10}	bit_9	bit_8	bit_7	bit_6	bit_5	bit_4	bit_3	bit_2	bit_1

Fig. 10 Bit reservation pattern

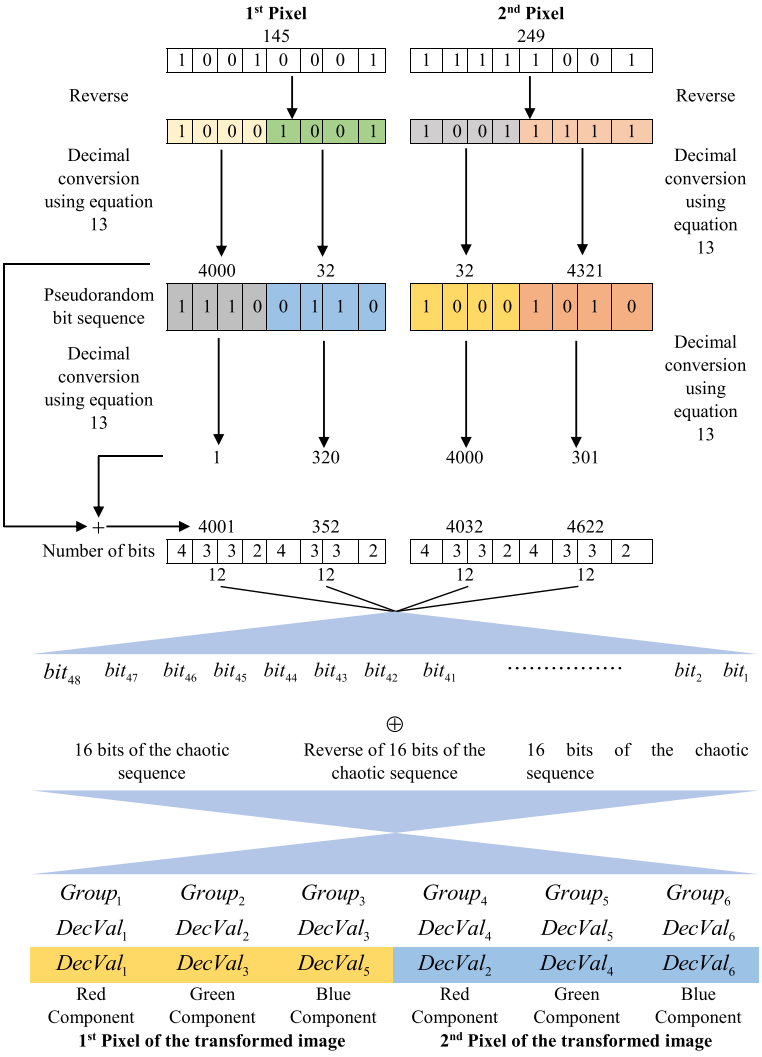


Fig. 11 Diagram to illustrate the proposed dimension transformation technique of a pixel

images can be obtained. If the total number of pixels in the input image is odd then the last pixel will be alone and cannot find a pixel to form a pair. But to execute this algorithm, simply take the last pixel and execute all the steps and form the set at the last stage as $\langle DecVal_1, DecVal_2, DecVal_3 \rangle$. At the time of decryption, the last pixel can be processed accordingly.

The obtained image will go through a scrambling process. The proposed pixel scrambling process is discussed next. The scrambling algorithm can efficiently shuffle the positions of the pixels. The proposed scrambling algorithm is also completely reversible i.e. the actual arrangements of the pixels can be retrieved from the scrambled image hence, there is no provision of data loss. Algorithm 1 describes the proposed scrambling method. The proposed scrambling algorithm works on every channel separately and each channel incurs a significant shuffling of the pixel positions which in turn modifies the whole image and disturbs the

correlation among the pixels. If the color image is considered for encryption purposes then, all three transformed images are to be processed separately. The proposed scrambling algorithm is very useful to enhance the security of the encrypted image and makes the proposed encryption system resilient against differential attacks.

Algorithm 1. Scrambling algorithm

Input: Transformed image $TI(i,j,k)$ whose size is $L = M \times N \times 3$ where the size of the actual image is $M \times N$ and the number of channels in the transformed image is 3.

1. Choose a seed value and a value for the control parameter and use this value pair $\left(s_0', \hat{\psi}\right)$ to generate a new chaotic sequence $cSeq$ of length L using the proposed RCM map.
2. Convert the one-dimensional chaotic sequence $cSeq$ into a three-dimensional matrix $\hat{M}$ of size $M \times N \times 3$ as $\hat{M}(i,j,k) = cSeq_{(i-1)\cdot N + j + (k-1)\cdot L/8}$.
3. Now create another 3-dimensional matrix $\hat{M}'$ of size $M \times N \times 3$ to store a modified version of $\hat{M}$. $\hat{M}$ is modified in the following way.
   a. For the first and the third channel of $\hat{M}$, sort every column and for the second channel, sort every row.
   b. The first, third and all other odd numbered columns of the first and the third channel of $\hat{M}$ is to be sorted in ascending order and the second, fourth and all other even numbered columns of the first and the third channel of $\hat{M}$ is to be sorted in descending order.
   c. The same sorting scheme is to be chosen for the second channel of $\hat{M}$ but in this case it is to be applied for the rows. To be more precise, all even numbered rows are to be sorted in descending order and all odd numbered rows are to be sorted in ascending order.
   d. The sorted array is to be stored in $\hat{M}'$.
4. Now, every column of the first and third channel and every row of the second channel of $\hat{M}'$ is nothing but the permutations of the corresponding columns and rows in $\hat{M}$ respectively. Construct a three-dimensional image $TI'(i',j',k')$ of size $L = M \times N \times 3$ from $TI(i,j,k)$ in such a way so that, $TI'(i',j',k') = TI(i,j,k)$ where $\hat{M}'(i',j',k') = \hat{M}(i,j,k)$.

Output: Scrambled image $TI'(i',j',k')$ whose size is $L = M \times N \times 3$ where the size of the image is $M \times N$ and the number of channels is 3.

Now choose another two seed values and a value for the control parameter and use the set $\left(s_0'', t_0'', \psi''\right)$ to generate new pseudorandom bit sequence $prbs'$ of length $Len = M \times N \times 3 \times 8$ and generate three dimensional matrix $Mat(p,q,r) = prbs'_{(p-1)\cdot N + q + (r-1)\cdot Len/64}$ where the size of each channel is $M \times N$ and each pixel consist of 8 bits. Now, every pixel (i',j') of the k^{th} channel of TI' is converted into 8 bit binary equivalent and XORed with the corresponding pixel (p,q) in the r^{th} channel of $Mat$where $i' = p, j' = q, r = k$and store the resultant image in an another matrix Mat'. The obtained image Mat'can be again scrambled using the algorithm 1. A value Itr is to be chosen that determines the number of iterations for which these steps are to be

repeated. Figure 12 illustrates the proposed image encryption method in detail. For multiple iterations, there is no need to choose different seed values all the time. Instead of that, the last value of every chaotic sequence can be saved for the next iteration and can be treated as the new seed in the next iteration.

Some of the advantages of the proposed image encryption method is given as follows:

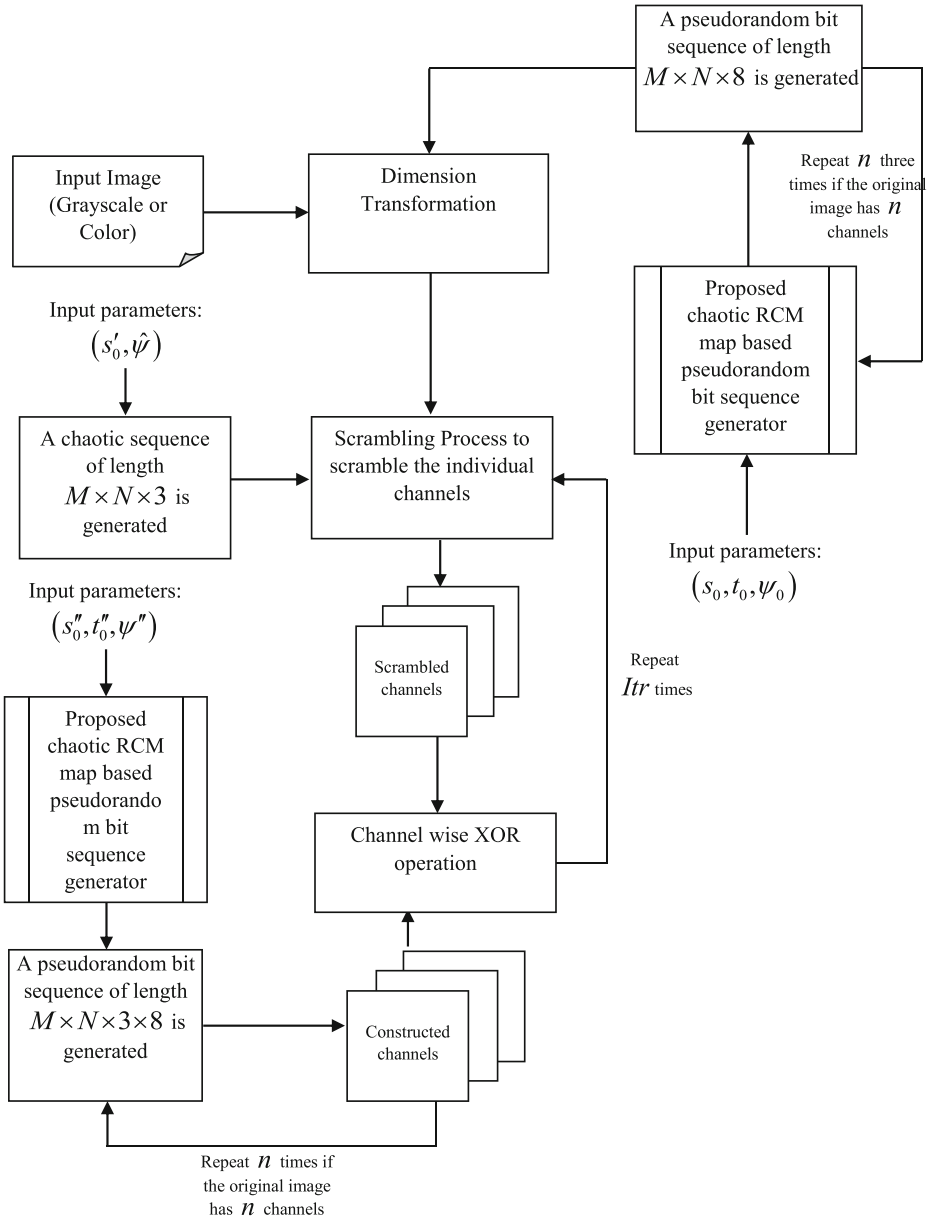


Fig. 12 Flow diagram of the proposed image encryption method

1. The proposed image encryption algorithm has no dependency on any additional image. The proposed method is efficient enough to encrypt different types of images using the proposed chaotic map and the pseudorandom bit generator.
2. The proposed encryption method is completely based on the proposed RCM chaotic map and the proposed pseudorandom bit generator. The efficiency of the proposed pseudorandom bit generator is already discussed earlier. The chaotic sequence as well as the pseudorandom bit sequence can be changed by varying the input parameters of the chaotic map. Therefore, it is very difficult to guess the pseudorandom bit sequence and the initial parameters of the chaotic map. These properties make the proposed encryption system safe and resilient against various types of attacks.
3. The proposed scrambling method can be easily modified. For example, the rows and columns may not be sorted instead that, any other permutations can be used.
4. The keyspace of the proposed method is sufficiently large that can prevent brute force attacks.
5. As discussed earlier, the proposed image encryption method is completely lossless in nature, and therefore, 100% of information can be recovered from the encrypted image.
6. The decryption process is very simple. The reverse operations are to be performed accordingly.
7. In the case of a grayscale image, the proposed image encryption method generates a color encrypted image which increases the confusion.
8. In case of a color image, the proposed image encryption method will generate three color encrypted images. So, at the time of decryption, all three encrypted images are necessary to get back the actual image.

5 Results of the simulation

This section presents the results which are obtained by applying the proposed image encryption method on different types of images. From this section, an idea about the proposed method can be obtained and a detailed analysis of the proposed image encryption system is given in the next section. The obtained results after applying the proposed image encryption algorithm are given in Fig. 13. As discussed earlier, the proposed method will generate a color encrypted image when the input image is in grayscale format. For the color images, the proposed encryption method will generate three different color encrypted images. At the time of decryption, all three images are necessary. From the given results, it is clear that the proposed image encryption method encrypts an image in such a way so that no one can understand or even guess the original image by interpreting the encrypted image(s). The encrypted images are given in Fig. 13b. Figure 13c shows the decrypted images and it can be clearly observed by the visual inspection that the decrypted images in Fig. 13c are quite similar to the corresponding original images under consideration, which are displayed in Fig. 13a. The lossless nature of the proposed image encryption method is analyzed and proved in the next section.

All experiments are performed in a computer that is equipped with an Intel i3 processor with 1.8GHz clock speed, 4 gigabytes of RAM, 500 GB hard disk, and Microsoft Windows 7 operating system. All simulations and experiments are performed in the MatLab R2014a environment.

The results of research work can be validated with the help of the obtained results by the similar work performed by various researchers. In this work, the proposed approach is

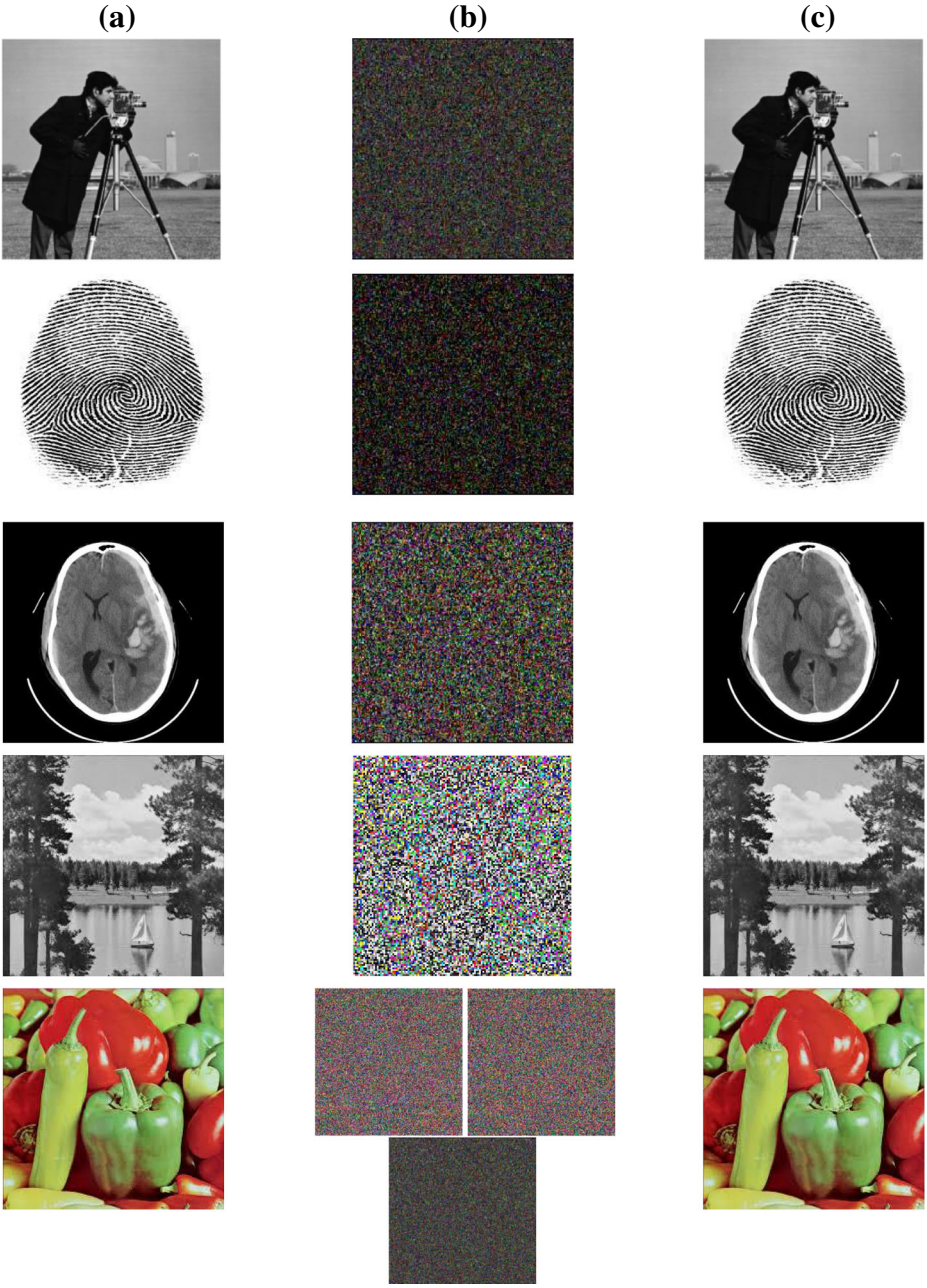


Fig. 13 Results of the propose image encryption **a** Actual Images (From top to bottom: Cameraman, Fingerprint (biometric image), CT Scan (biomedical image), Lake, Peeper (Color Image), Baboon (color image), watch (color image), and tulips (color image); **b** Encrypted Images; **c** Decrypted Images

compared with various standard image encryption procedures. The comparative analysis of the proposed approach is useful to establish the quality and efficiency of the proposed work. Moreover, the comparative analysis of the proposed work is helpful to validate the proposed

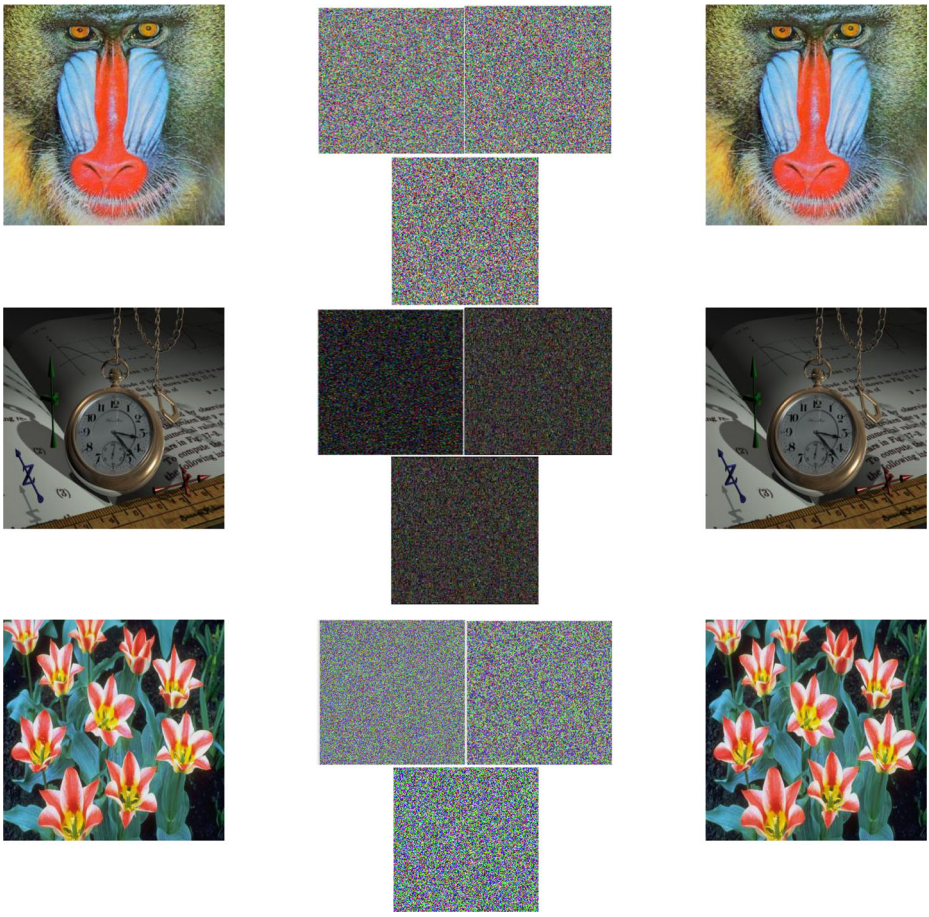


Fig. 13 (continued)

work from the context of the other established works. The obtained experimental results are promising and proven to be better enough compared to other approaches. Both qualitative and quantitative analysis helps to investigate the performance of different components with greater details. The lossless property of the proposed RCM map-based image encryption system is also proven by using both qualitative and quantitative manner. The NIST test results for the proposed pseudorandom bit generator is indicating the effectiveness of the method. Similarly, the detailed analysis of the proposed RCM map is depicting the applicability of this map in different domains.

The proposed image encryption method involves a parameter *Itr* which is used to determine the number of iterations is to be performed (please refer the Fig. 12). This *Itr*parameter has a major influence on the final quality of the encrypted images and the impact of this parameter is visually demonstrated in Fig. 14. The *Itr*is a very important parameter to be known to generate the original images from the decrypted image. If someone knows the other security keys except the value of *Itr* then also, the correct image is not possible to reconstruct. This feature is demonstrated in Fig. 15. So, the value of the *Itr*can be considered as a key.

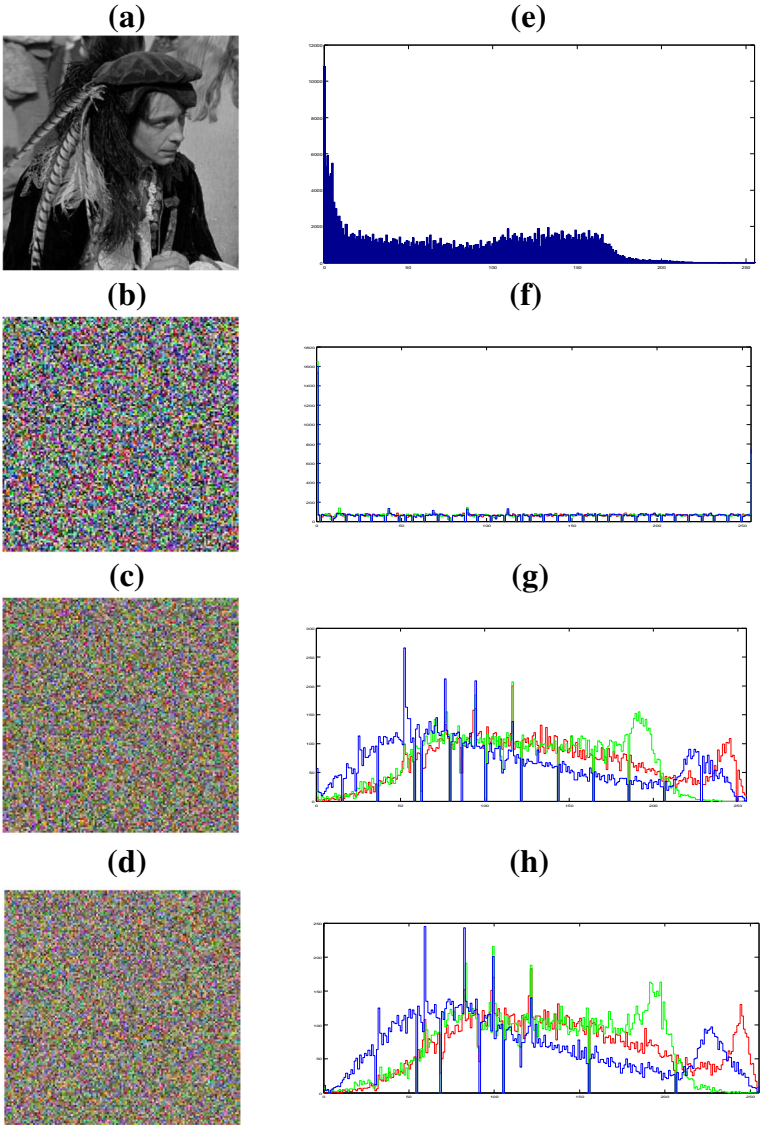


Fig. 14 The impact of the parameter *Itr* on the encryption **a** Original image; (b)-(d) The output of the proposed encryption algorithm after the **b** first, **c** second, **d** third iterations respectively; **e** histogram of the original image; (f)-(h) histograms of the encrypted output which is obtained after the **f** first, **g** second and **h** third iterations respectively

6 Performance and security analysis

On most occasions, visual investigations are may not be sufficient to test the quality of an image encryption system. In this section, various security aspects and performance of the proposed cryptosystem is analyzed in detail. Several relevant parameters like directional correlation coefficients, histogram analysis, strength against differential attacks, efficiency,

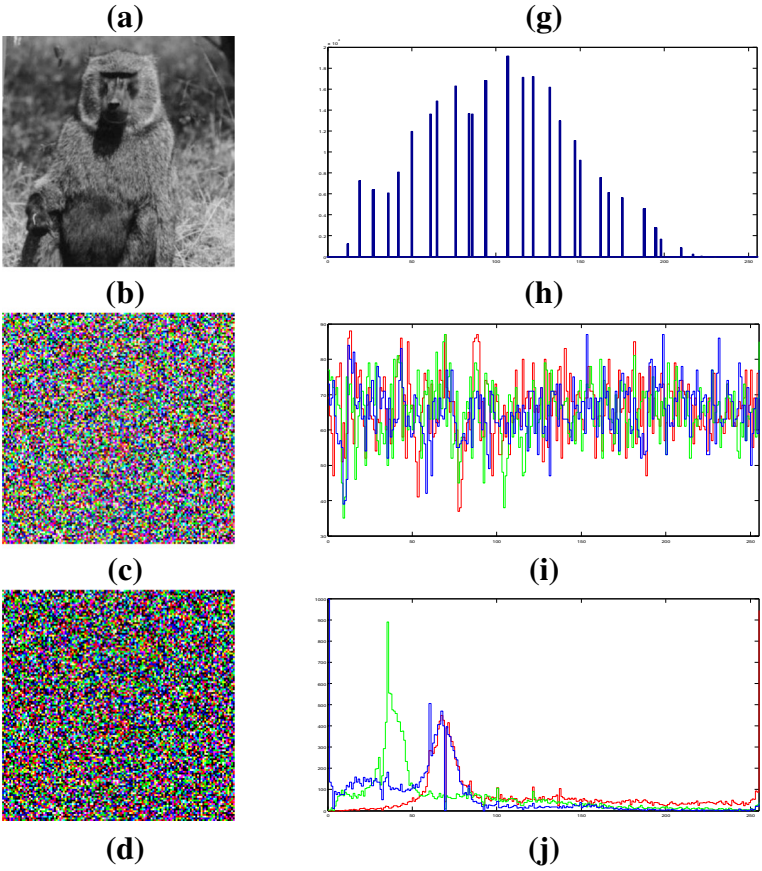


Fig. 15 The impact of the iterations on the decryption process (**a**) Original image; (g) histogram of the original image; (**b**) encrypted image; (h) histogram of the encrypted image; (c)-(f) The output of the decryption process after the (**c**) first, (**d**) second, (**e**) third and (**f**) fourth iterations respectively; (i)-(l) histograms of the decrypted output which is obtained after the (i) first, (**j**) second, (**k**) third and (**l**) fourth iterations respectively

etc. are evaluated and analyzed. Moreover, the keyspace and the sensitivity of the keys are also discussed.

6.1 Key space and strength against brute force attacks

The keyspace of a cryptographic system is a very important parameter from the security perspective. It is defined as the count of all possible combinations of a key or set of keys that are applied in various stages of an image cryptosystem. If the range of values or the set of possible values for the keys is known then it is possible to discover the original key or the set of keys by testing all possible combinations. This type of attack is the naïve approach by an intruder to break a cryptosystem and known as a brute-force attack.

It can be easily understood from the above discussion that, small keyspace is not at all desirable, and small keyspace is always vulnerable against brute force attacks which makes the overall cryptosystem weaker. It is necessary to design a cryptosystem with sufficiently large key space so that the encryption algorithm can withstand the brute force attacks and other

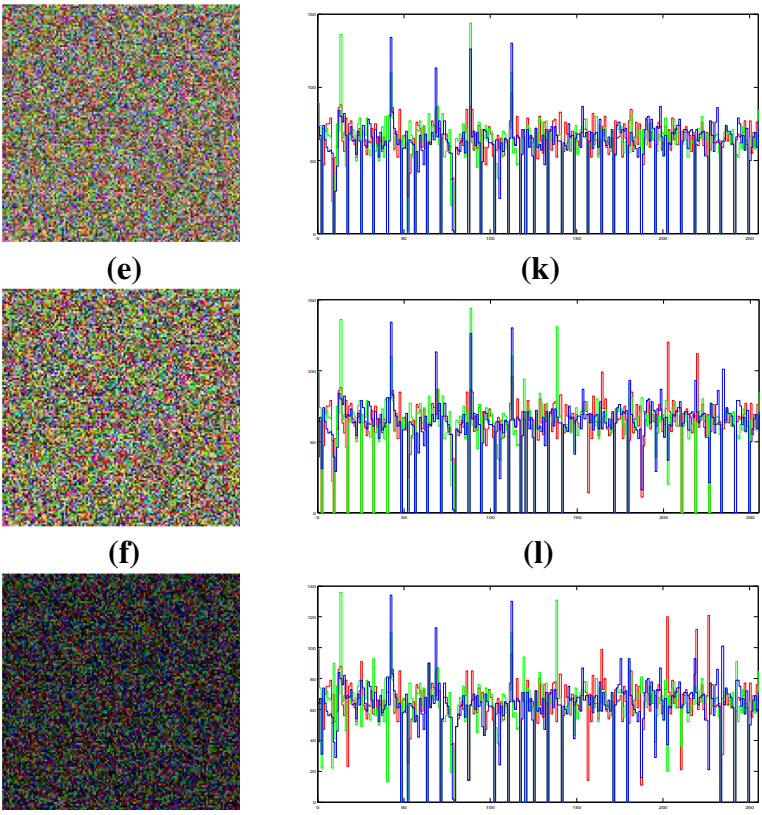


Fig. 15 (continued)

exhaustive search-based attacks. It is difficult to search a large key space exhaustively because modern-day computers also not very efficient to search a large key space and therefore it is hard for the intruders to guess or retrieve the actual key or the set of keys from the ocean of the possible keys.

The key space of the proposed image encryption system is composed of the following segments:

1. The input parameters (s_0, t_0, ψ_0) to generate a chaotic sequence which is required for the dimension transformation phase.
2. The input parameters $\left(s_0^{'}, \widehat{\psi}\right)$ for the scrambling algorithm.
3. The input parameters $\left(s_0^{''}, t_0^{''}, \psi^{''}\right)$ for the channel wise XOR operation.
4. The number of iterations i.e. *Itr*.

To determine the key space of the proposed method, these four segments should be taken into account. For the sake of explanation, consider a gray scale image of size $M \times N$. The input parameters (s_0, t_0, ψ_0) are required to perform the dimension transformation where s_0 and t_0 are the seeds of the chaotic maps and can take any values in the range (0, 1) i.e. $s_0, t_0 \in (0, 1)$. From the theoretical point of view, these two parameters can be assigned infinite number of values.

But for the sake of analysis, let us consider the precision up to two decimal points then the range of these two parameters are $0.01 \le s_0 \le 0.99$and $0.01 \le t_0 \le 0.99$. $\psi_0$is the controlling parameter or the bifurcation parameter of the proposed RCM map and can take any value between 1 to 4? So, this parameter can also take infinite number of values. Therefore, the analysis of the key space is possible under certain assumptions. Suppose, an attacker tries to generate the pseudorandom bit sequence without involving the chaotic maps then, for the dimension transformation phase, there are $P_1 = 2^{M \times N \times 8}$ number of possibilities which are needs to be investigated. The input parameters $\left(s_0^{'}, \widehat{\psi}\right)$ are required to perform the scrambling operation. Scrambling operation shuffles the position of the pixels. This operation can also be performed without involving the chaotic maps. A scrambling algorithm can modify the pixel positions in $P_2 = M! \times N! \times 3!$ ways. Now, the input parameters $\left(s_0^{''}, t_0^{''}, \psi^{''}\right)$ are required to perform the channel wise XOR operation. These input parameters are required to generate a chaotic pseudorandom bit sequence of length $M \times N \times 3 \times 8$ which is in turn used to generate the synthetic channels. This operation can also be performed without involving the chaotic maps in $P_3 = M! \times N! \times 3! \times 2^8$ ways. *Itr* is an another important parameter for the proposed method. As discussed earlier, without knowing the exact value of *Itr*, it is impossible to decrypt an encrypted image.

Therefore, the key space P for the proposed image cryptosystem can be expressed as $P = Itr \times P_1 \times P_2 \times P_3$ i.e. $P = Itr \times 2^{M \times N \times 8} \times M! \times N! \times 3! \times M! \times N! \times 3! \times 2^8 = Itr \times 2^{(M \times N \times 8)+8} \times (M! \times N! \times 3!)^2$. To explain it further and to get an essence of the actual key space for a real image, let us consider an grayscale image of size 128×128 is to be encrypted by using the proposed image encryption method. Assume that the value of the *Itr* is 5. Then the total possible key space for the proposed image encryption system which needs to be explored to perform a brute force attack is $P = 5 \times 2^{(128 \times 128 \times 8)+8} \times (128! \times 128! \times 3!)^2 \approx 4.0902 \times 10^{40323}$, which is significantly large and makes the proposed image encryption system resilient against exhaustive search-based attacks.

6.2 Key sensitivity analysis

A good cryptosystem should have high sensitivity to the key or the set of keys. It is one of the fundamental requirements of any image cryptosystem to ensure the security of the encrypted image. The actual image should not get revealed due to a tiny change in the key. Therefore, it is necessary to study the sensitivity of the keys for both encryption and the decryption process. As discussed earlier, the initial parameters of the chaotic systems are the keys of the proposed system along with the value of the *Itr*. The effect of the *Itr* is already discussed earlier. Fig. 16 shows the effect of small change in the parameter(s_0, t_0, ψ_0) which are required for the dimension transformation phase. Figure 17 demonstrates the impact of a tiny change in the parameter(s_0, t_0, ψ_0) on the decryption process.

Figure 16a shows the actual image. Figure 16b shows the encrypted image with the key values $s_0 = 0.5$, $t_0 = 0.8$, $\psi_0 = 3.5$. This combination of the key values is used for the demonstration purposes in this work. Figure 16c shows the encrypted image with the key values $s_0 = 0.6$, $t_0 = 0.7$, $\psi_0 = 3.5$. So, the s_0 and t_0 experienced slight modification but the controlling parameter i.e. ψ_0 kept unchanged. The encrypted image in Fig. 16c is significantly different from Fig. 16b and their difference can be observed from Fig. 16d. The sensitivity of the keys in the decryption process is illustrated in Fig. 17. Figure 17a is the decrypted image and it is

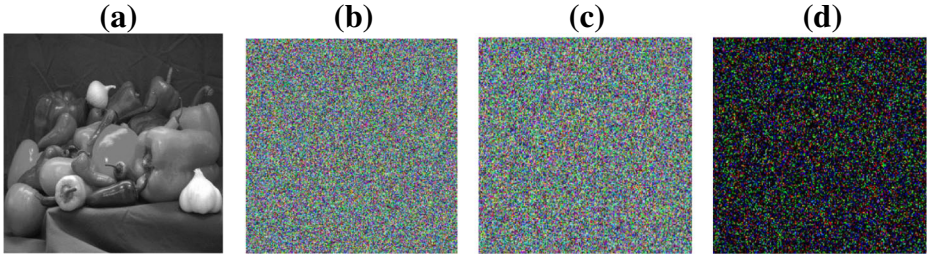


Fig. 16 The impact of the small change in the key for the dimension transformation phase for encryption (**a**) Actual image (peppers.png), (**b**) Encrypted image with $s_0 = 0.5$, $t_0 = 0.8$, $\psi_0 = 3.5$; (**c**) Encrypted image with $s_0 = 0.6$, $t_0 = 0.7$, $\psi_0 = 3.5$, (**d**) difference between (b) and (c)

completely the same as the actual image because the proposed image encryption method is completely lossless in nature. Figure 17b is the encrypted image with the key values $s_0 = 0.5$, $t_0 = 0.8$, $\psi_0 = 3.5$. The decryption method takes the encrypted image and tries to find out the actual image with a slightly different set of key values $s_0 = 0.4$, $t_0 = 0.7$, $\psi_0 = 3.5$ and the result is given in Fig. 17c. It can be easily observed that the decrypted image in Fig. 17c is significantly different and the difference can be observed in Fig. 17d.

One important point about the chaotic system that can be observed from the above discussion is that the changes in the encrypted or the decrypted images are obtained by slightly changing the seed values only. The system parameter ψ remains unchanged during the experiments. Therefore, a small change in the initial parameters of the chaotic map can bring a significant change in both encrypted and decrypted images which are significantly different from the actual encrypted and decrypted images respectively. As discussed earlier, the effect of the *Itr* parameter on encryption and the decryption process can be observed from Figs. 14 and 15 respectively.

6.3 Analysis of the histogram

The intensity distribution of an image can be understood from the analysis of the histogram. In general, meaningful images do not have a uniform intensity distribution. It is desirable to have a uniform distribution in the encrypted image to resist various statistical attacks. A comparative study of the histograms is presented in this work where the proposed method is compared with some of the standard methods [11, 72, 73, 75] in the literature to test the effectiveness of the

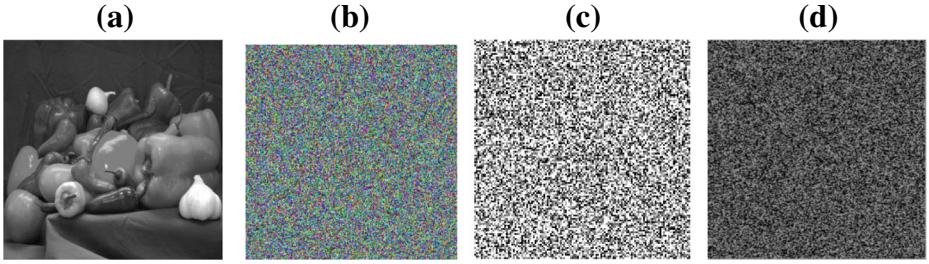


Fig. 17 The impact of the small change in the key for the dimension transformation phase for decryption (**a**) Decrypted Image (Same as Actual image peppers.png), (**b**) Encrypted image with$s_0 = 0.5$, $t_0 = 0.8$, $\psi_0 = 3.5$, (c) Decrypted image with$s_0 = 0.6$, $t_0 = 0.7$, $\psi_0 = 3.5$, (d) difference between (a) and (c)

proposed method and the obtained results are given in Fig. 18. The popular Lena image is considered for comparison purposes which are shown in Fig. 18a along with its histogram. Figure 18b to f are the results of the encryption procedure along with their corresponding histograms. The result of the histogram analysis is given in Fig. 18f. It can be observed that the histogram of the encrypted image has three channels in the proposed method because of the dimension transformation phase. From the histogram, it can be observed that all three channels have almost uniform intensity distribution in the encrypted image. This analysis and comparison prove that the proposed image encryption method is resilient against different statistical attacks.

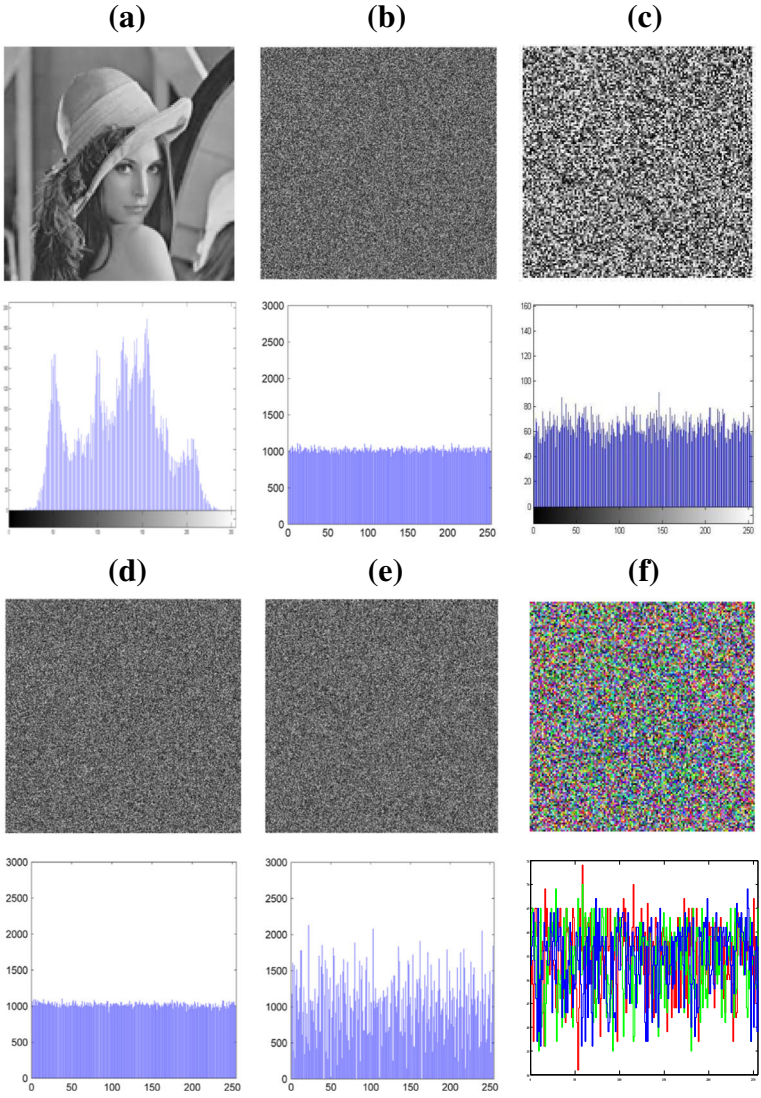


Fig. 18 **a** Actual Lena image and its histogram; (b)-(f) encrypted images and their corresponding histograms which are obtained using **b** Zhu's Method [75], **c** Chakraborty's Method [11] **d** Zhou's Method [72] **e** Zhou's Method [73] **f** Proposed Method

6.4 Analysis of the correlation coefficients

Typically, a meaningful image is constructed with highly correlated pixels. It is one of the fundamental requirements for any image encryption method to break such a high correlation. It is necessary to prevent unintentional data leakage. Therefore, the study of the correlation is very important from the security perspective. To analyze the correlation of various pixels, 2500 randomly chosen pairs of the adjacent pixels are taken into consideration and these pixels are considered in the horizontal, vertical, and diagonal directions for all three planes separately. Intensity values of these pair of pixels are plotted in a two-dimensional graph which is shown in Fig. 19. All three directions are considered and the corresponding intensity values of the pair of pixels are plotted. If two pixels are highly correlated then the diagonal line will be highly dense [23]. It can be easily observed from Fig. 19 that most of the pixel values are plotted near the diagonal line for the original image which signifies the high correlation whereas the pixel values for the encrypted images are plotted throughout the possible range of the intensity values which indicates a lesser correlation.

Figure 19 can only be used for visual inspection purposes. But as discussed earlier, a visual inspection may not always reveal the actual scene because it can vary from observer to observer. Therefore, a quantitative analysis is performed using Eq. 14.

$$CorCoef(m,n) = COV(m,n)/\sqrt{D(m)}\sqrt{D(n)} \tag{14}$$

Here, (m,n) represents the intensity values of a pair of adjacent pixels. $COV(m,n)$ can be computed using Eq. 15 and $D(x)$ can be computed using Eq. 16.

$$COV(m,n) = \frac{1}{Count_{pairs}} \sum_{i=1}^{Count_{pairs}} ((m_i - E(m))(n_i - E(n))) \tag{15}$$

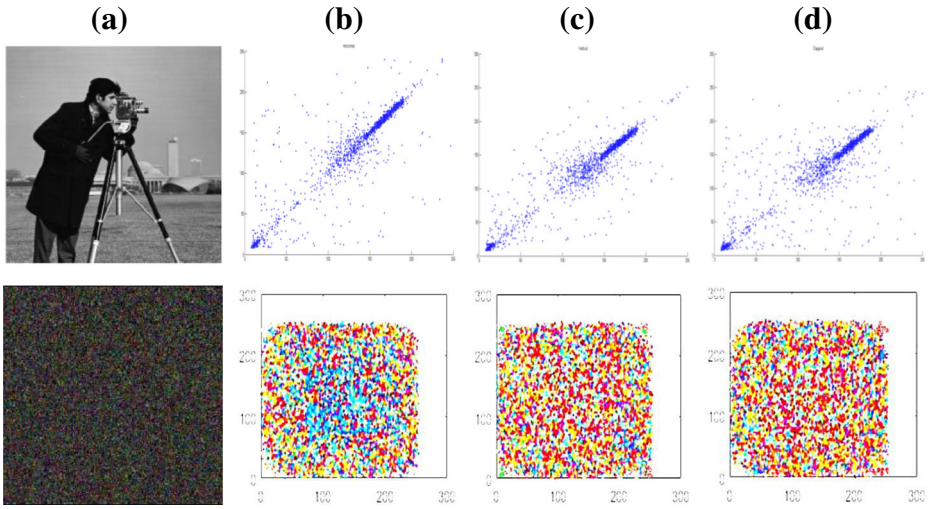


Fig. 19 Obtained correlations in various directions using the proposed image encryption algorithm. The top and bottom rows are showing the correlations of the (**a**) Original Cameraman image and the corresponding encrypted image and correlation of (**b**) Horizontal, (**c**) Vertical, (**d**) Diagonal directions, respectively

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

In Eqs. 15, and 16, the total number of randomly chosen pairs are represented by the $Count_{pairs}$. The value of $E(y)$ can be computed using Eq. 17.

$$E(y) = \frac{1}{Count_{pairs}} \sum_{j=1}^{Count_{pairs}} z_j \tag{17}$$

The *CorCoef* can take any value from the range $[-1, 1]$. The absolute value of the *CorCoef* is important here and if it is close to 1 then it indicates a high correlation among the pixels [66]. Therefore, a good encryption mechanism must generate a correlation value close to 0. Figure 19 demonstrates the correlation coefficient and shows the effect of the proposed image encryption method on the cameraman standard image. The quantitative analysis is performed using Eq. 14 and numerical results are reported in Table 5. It can be observed from Table 5 that, the values of the correlation coefficients for the encrypted images are nearly zero that proves the efficiency of the proposed image encryption method.

6.5 Strength against differential attacks

The differential attack is a variant of the chosen-plaintext attacks. A tiny change is performed on the plain image and then an intruder studies the original and the encrypted images and tries to find out the relation between the original and the encrypted images to get some hint about the encryption process as well as about the keys. This kind of attack can be prevented if a small change in the actual image produces a huge deviation in the encrypted image. The proposed image encryption method is tested against the differential attacks using the Lena image and compared with some standard algorithms and the results are reported in this subsection. The actual image of Lena is encrypted two times using the same set of keys but with a difference in one bit. Four algorithms are involved in this experiment. These are DecomCrypt [72], Zhu's Method [75], Zhou's method [73] and the proposed image encryption method. A small change

Table 5 Correlation Coefficients of various images and corresponding encrypted images using the proposed image encryption algorithm in different directions

Image	Original Image			Encrypted Image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Cameraman	0.9592	0.9335	0.9087	0.0005	0.0034	−0.0067
Liftingbody	0.9557	0.9532	0.9181	0.0021	−0.0029	−0.0041
Fingerprint	0.6794	0.8457	0.5575	0.0063	−0.0054	0.0019
CT Scan	0.8695	0.7852	0.9758	−0.0071	−0.0027	0.0009
Tree	0.9387	0.9275	0.8872	0.0009	0.0033	−0.0015
Pepper	0.9515	0.9580	0.9181	0.0037	−0.0049	0.0041
Lena	0.9508	0.8930	0.8538	0.0042	−0.0002	−0.0023
Cameraman	0.9592	0.9335	0.9087	0.0021	−0.0019	−0.0043

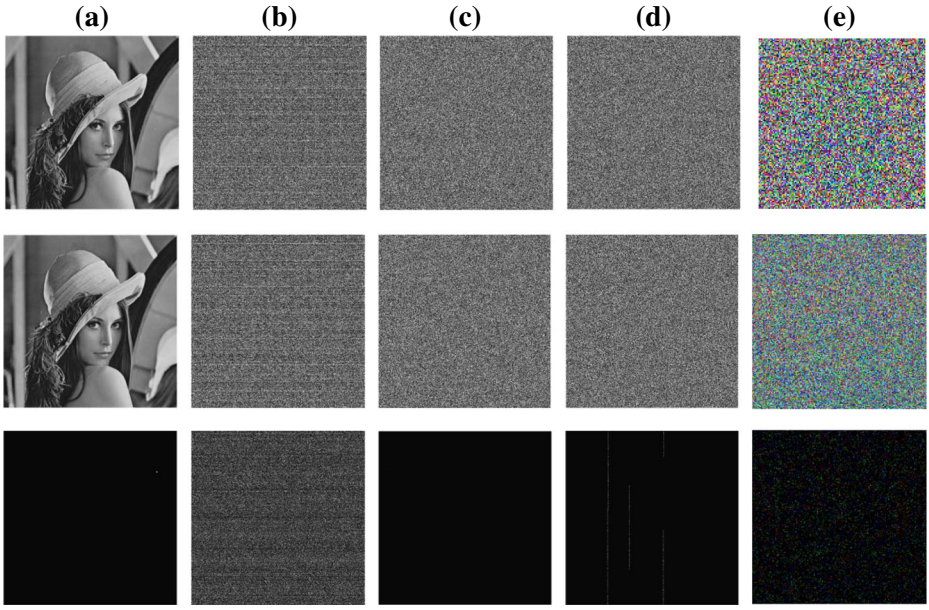


Fig. 20 Illustration of the differential attacks: (**a**) Original Lena images with a single-pixel variation and the difference between them; (b)-(e) obtained encrypted images and the difference between them after applying (**b**) DecomCrypt [72], (**c**) Zhou's algorithm [73], (**d**) Zhu's algorithm [75], (**e**) Proposed image encryption algorithm

in the actual image does not have any significant effect on the encrypted images for the Zhu's Method [75] and Zhou's method [73]. However, a small change produces a good amount of deviation in the encrypted images which are obtained using DecomCrypt [72] and the proposed image encryption system. It can be easily observed in Fig. 20. As discussed earlier, visual verification is not enough always. Therefore, two popular parameters are used to analyze the impact of a small change in the actual image on the encrypted image. The number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are the two parameters that are considered in this work. NPCR can be computed using Eq. 18 and UACI can be computed using Eq. 19.

$$NPCR = \frac{\sum_{i=1}^{\dim_1}\sum_{j=1}^{\dim_2} Difr(i,j)}{\dim_1 \times \dim_2} \times 100\% \tag{18}$$

$$UACI = \frac{1}{\dim_1 \times \dim_2}\sum_{i=1}^{\dim_1}\sum_{j=1}^{\dim_2}\frac{|IMG_1(i,j) - IMG_2(i,j)|}{255} \tag{19}$$

In Eq. 18 and 19, $\dim_1$ and $\dim_2$ are the dimensions of the images $IMG_1$and IMG_2. These two images are the encrypted images corresponding to the original images and these images are slightly different. $Difr(i,j)$is an array with dimension $\dim_1 \times \dim_2$consist of only binary elements. It stores the count of the different pixels in $IMG_1$and IMG_2. $Difr(i,j)$is defined in Eq. 20.

$$Difr(i,j) = \begin{cases} 1 & if\ IMG_1(i,j) = IMG_2(i,j) \\ 0 & Otherwise \end{cases} \tag{20}$$

Ten images are chosen randomly from this web repository [15] to analyze the strength of the proposed method against the differential attacks. The proposed method is compared with four standard algorithms and the comparative results are presented in Table 6. The image ids which are given in the first column of Table 6 corresponds to the image ids which are given in the specified web repository. It can be easily observed that the proposed image encryption method achieves 97.384% NPCR and 33.235% of UACI on an average over the ten test images. The obtained results are satisfactory compared to some other standard algorithms. This analysis proves that the proposed image encryption method is resilient against differential attacks. The effect of the parameter *Itr* in the proposed method on NPCR and UACI can be observed in Figs. 21 and 22 respectively (two separate figures are used for better understanding).

From Table 6, it can be observed that the proposed approach achieves the NPCR value 0.8963 to 0.9993 with the average NPCR value 0.97384. Although, the ideal value of NPCR is 96.6094% [57] still, the proposed approach achieves significant overall NPCR score of 97.384% which is very close to the ideal value. The performance of the encryption approaches is not same for different images and therefore, three state-of-the-art approaches are compared to establish the effectiveness of the proposed approach.

6.6 Analysis of the time complexity

The time complexity of the proposed image encryption algorithm is analyzed in this subsection. For the sake of this analysis, let us assume a grayscale image of size $M \times N$. The first operation i.e. the dimension transformation requires a pseudorandom bit sequence of length $M \times N \times 8$. The pseudorandom bit sequence can be generated using the proposed RCM map in two phases. In the first phase, the same chaotic map is used twice with different seed values to generate chaotic sequences, and then the proposed pseudorandom bit generation method is used to generate the pseudorandom bit sequence. The proposed pseudorandom bit generation method can be implemented in polynomial time because it is directly and linearly related to the number of elements to be generated. So, a pseudorandom bit sequence of length n can be generated using the proposed method in $O(n)$ time. The dimension transformation phase requires an $O(M \times N)$time.

The scrambling algorithm changes the position of the pixels in a three-dimensional matrix and produces a scrambled image. The operations which are associated with the scrambling process can be easily performed in $O(M \times N \times 3)$ times because positions of each pixel in a channel can be modified in constant time and the required chaotic sequence can be generated in $O(M \times N \times 3)$ time. The last phase i.e. the channel wise XOR operation can also be implemented in $O(M \times N \times 3)$ time considering XOR operation takes a constant amount of time. Therefore, the proposed image encryption method can be implemented in polynomial time. The required time is completely dependent on the size and type of the input image i.e. the required time will increase in case of a color image to treat three channels separately. Now, if the scrambling procedure and the channel wise XOR method is repeated for *Itr* number of times then the overall time complexity of the proposed image encryption procedure will be $O(itr \times M \times N \times 3)$ (because the function and the number of steps does not change and can be assumed as constant).

Table 6 Comparison of the computed NPCR and UACI values

Image Id	NPCR				UACI			
	DecomCrypt [72]	Zhou's algorithm [73]	Zhu's algorithm [75]	Proposed method	DecomCrypt [72]	Zhou's algorithm [73]	Zhu's algorithm [75]	Proposed method
1	0.9959	0.00000382	0.0048	0.9971	0.3454	0.000000314	0.0016	0.3348
2	0.9959	0.00000372	0.0012	0.9957	0.3342	0.000002244	0.0004	0.3968
3	0.9962	0.00000379	0.0024	0.9986	0.3363	0.000000254	0.0008	0.3427
7	0.9962	0.00000374	0.0004	0.9993	0.3341	0.000001586	0.0001	0.3298
12	0.7531	0.00000369	0.0059	0.8963	0.2661	0.000000793	0.0020	0.2719
14	0.9374	0.00000382	0.0053	0.9102	0.2864	0.000002872	0.0018	0.2347
15	0.9963	0.00000380	0.0010	0.9817	0.3456	0.000005595	0.0004	0.3748
20	0.9961	0.00000377	0.0000	0.9949	0.3699	0.000003471	0.0000	0.2968
25	0.9963	0.00000382	0.0070	0.9897	0.3348	0.000005984	0.0023	0.3638
35	0.9960	0.00000376	0.0042	0.9749	0.3358	0.000003560	0.0014	0.37741
Average	0.96594	0.00000377	0.00322	0.97384	0.32886	0.00000267	0.00108	0.33235

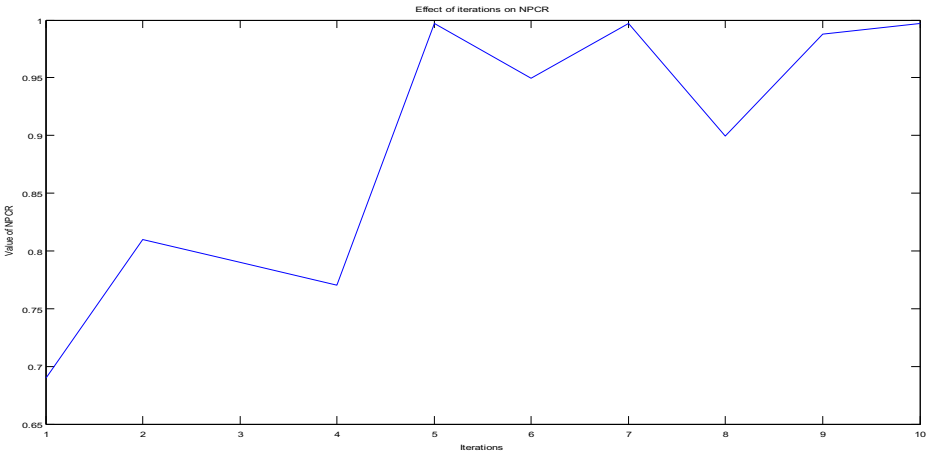


Fig. 21 Effect of *Itr* on the value of NPCR (Image with id 1 in Table 6 is used for this experiment)

6.7 Analysis of the information entropy

The information entropy is one of the important parameters which is helpful in evaluating an image encryption method. The information entropy can be computed using Eq. 21.

$$InfEntr(d) = \sum_{i=0}^{2^{len}-1} P(d_i)\log\frac{1}{P(d_i)} \tag{21}$$

Here, $InfEntr(d)$ denotes the information entropy of a message source d. len represents the length of the bit sequence of a symbol $d_i \in d$ and the $P(d_i)$ represents the probability of occurrence for a specific symbol d_i.

For a strong, robust, and reliable cryptographic system, the desired value of the information entropy is close to 8 [61]. Table 7 shows the values of information entropy after applying the proposed image encryption system. A comparative study of the information entropy is

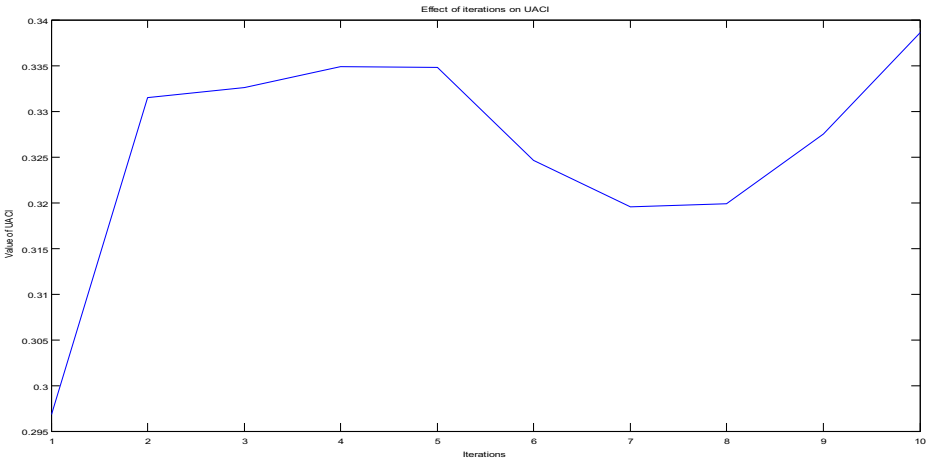


Fig. 22 Effect of *Itr* on the value of UACI (Image with id 1 in Table 6 is used for this experiment)

Table 7 Obtained values of the information entropy using the proposed image encryption system

Image	Cameraman	Liftingbody	Fingerprint	CT Scan	Tree	Pepper	Lena
Information Entropy	7.8475996	7.89667845	7.78588896	7.996863	7.669863	7.968336	7.989965

presented in Table 8 using the Lena image where the proposed method is compared with 7 standard methods of the literature. It can be easily observed that the proposed image encryption method produces satisfactory results and outperforms some of the standard methods.

6.8 Quantitative analysis of the average change in distance

The confusion characteristics of an encryption scheme can be well-understood by finding the average change in distance. The change in the average distance for a pixel (k, l) in an image of size $d_1 \times d_2$ is denoted as $\Phi_{avg}^{d_1,d_2}$ and defined in Eq. 22 [26]. In this equation, $d_E(i,j)$ represents the simple Euclidean distance between two points i and j. Equation 23 mathematically expresses the average change in the whole image. In this equation, the permuted pixel corresponding to the original pixel (k, l), is denoted using (k, l).

$$\Phi_{avg}^{d_1,d_2} = \frac{1}{4}\begin{bmatrix} d_E((l-1,k),(l-1,k)) + d_E((l+1,k),(l+1,k)) + \\ d_E((l,k-1),(l,k-1)) + d_E((l,k+1),(l,k+1)) \end{bmatrix} \tag{22}$$

$$\Phi_{avg} = \frac{1}{(d_1-2)\cdot(d_2-2)} \sum_{i=1}^{d_1-2} \sum_{j=1}^{d_2-1} \Phi_{avg}^{d_1,d_2} \tag{23}$$

Higher value of the average change in the distance denotes greater confusion.

6.9 Quantitative analysis of the change in graylevel intensity values

The change in the graylevel intensity values in the cipher image is measured to quantitatively analyze the quality of cipher image. Typically, the deviation of the graylevel intensity values in the encrypted image from the original image is measured using the approach proposed in [3, 37]. Equation 24 can be used to quantitatively analyze the cipher image using this criterion.

$$Q = \frac{\sum_{k=0}^{N-1} \left|\varphi_k(O_{img}) - \varphi_k(E_{img})\right|}{N} \tag{24}$$

In Eq. 24, the count of the graylevels is represented by N and the original image and its corresponding cipher images are denoted using O_{img} and E_{img} respectively. The number of the

Table 8 Comparison of the proposed image encryption method with some other standard methods in terms of information entropy (lena image is considered for the comparison)

Method	[61]	[24]	[58]	[59] (upto 8 rounds)	[55]	[70]	[65]	Proposed Method (upto 5 iterations)
Information Entropy	7.9993	7.9965	7.9909	7.9972	7.9951	7.9992	7.9991	7.999107

k^{th} graylevel intensity present is denoted with $\varphi_k(\cdot)$. Equation 25 helps to mathematically express the relative error [37].

$$Error_{avg}^{rel} = \frac{1}{d_1 \times d_2} \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} \frac{\left|O_{img}(i,j) - E_{img}(i,j)\right|}{\left|O_{img}(i,j)\right|} \tag{25}$$

6.10 Analysis of the degree of scrambling

Equation 26 can be used to compute the degree of scrambling that investigates the relatively closed pixels. This parameter can be computed using the approach developed in [64]. The range of this parameter can be 0 to 1 i.e. $DoS \in [0, 1]$) can be evaluated using the method proposed in.

$$DoS = \frac{\sum_{i=0}^{d_1-2} \sum_{j=0}^{d_2-2} \Psi_{ij}}{(\mathrm{N}-1)^2 \times (d_1-2) \times (d_2-2)} \tag{26}$$

In this equation, the term Ψ_{ij} is mathematically expressed in Eq. 27.

$$\Psi_{ij} = \lambda_1(i,j) + \lambda_2(i,j) + \lambda_3(i,j) + \lambda_4(i,j) \tag{27}$$

In Eq. 27, four functions i.e. $\lambda_q(i,j)$, $q = 1, \ldots, 4$ are mathematically defined in Eq. 28.

$$\begin{cases} \lambda_1(i,j) = \left|\left\{O_{img}(i-1,j) - E_{img}(i,j)\right\}^2 - \left\{E_{img}(i-1,j) - O_{img}(i,j)\right\}^2\right| \\ \lambda_2(i,j) = \left|\left\{O_{img}(i+1,j) - E_{img}(i,j)\right\}^2 - \left\{E_{img}(i+1,j) - O_{img}(i,j)\right\}^2\right| \\ \lambda_3(i,j) = \left|\left\{O_{img}(i,j-1) - E_{img}(i,j)\right\}^2 - \left\{E_{img}(i,j-1) - O_{img}(i,j)\right\}^2\right| \\ \lambda_4(i,j) = \left|\left\{O_{img}(i,j+1) - E_{img}(i,j)\right\}^2 - \left\{E_{img}(i,j+1) - O_{img}(i,j)\right\}^2\right| \end{cases} \tag{28}$$

In implementing these concepts, specifically for the Eqs. 23 and 26, 2 is subtracted from the actual dimension d_1 and d_2 to avoid the zero padding. Some images are selected from this web repository [39] to test the performance of the proposed system using the three evaluation parameters i.e. average change in distance, change in graylevel intensity values, degree of scrambling and the quantitative results are reported in Table 9. From Table 9, it can be observed that the proposed approach performs well and produces satisfactory results.

6.11 Analysis of the SSIM index

The structural similarity index is first proposed in [53]. Let us assume that, two images *IMG* and *IMG'* are two images from which, two windows ω_1 and ω_2 are extracted respectively. The value of the *SSIM* can be computed using Eq. 29 where, μ and σ denote the average and variance respectively and α_1 and α_2 are the two constants.

$$SSIM(\omega_1, \omega_2) = \frac{\left(2 \cdot \mu_{\omega_1} \cdot \mu_{\omega_2} + \alpha_1\right) \cdot \left(2 \cdot \sigma_{\omega_1\omega_2} + \alpha_2\right)}{\left(\mu_{\omega_1}^2 + \mu_{\omega_2}^2 + \alpha_1\right) \cdot \left(\sigma_{\omega_1}^2 + \sigma_{\omega_2}^2 + \alpha_2\right)} \tag{29}$$

The quantitative results obtained using the proposed approach on some of the selected images from this repository [39] are reported in Table 10.

Table 9 Quantitative results of average change in distance, change in graylevel intensity values, degree of scrambling

Image Id	Φ_{avg}	Q	DoS
1	145.3986615	0.142783874	0.408515749
2	186.3444784	0.243977051	0.339508547
3	171.0842967	0.231705946	0.706886953
7	137.0005695	0.172004683	0.226702528
12	171.2334979	0.155781579	0.850013996
14	159.6367482	0.193191149	0.74321016
15	147.8932886	0.141339761	0.66354039
20	129.6709985	0.115940559	0.563610112
25	165.3399391	0.208176778	0.812204582
35	179.6680505	0.30524544	0.373622424
Average	159.3270529	0.191014682	0.568781544

6.12 Analysis of the cyclic length of the proposed RCM map

Typically, the cycle length of continuously-realized and ergodic chaotic systems can be infinite. It can be hold for almost every orbit that begins with any seed or initial condition. In case of discrete realization with finite-precision can cause some short-length cycles [31]. In this subsection, the cycle length is analyzed with different seed values and with different values of the controlling parameter.

Here, the first experiment is performed by varying the seed values. The value of the controlling parameter ψ is made fixed at 3.5. The value of the initial seed is started with 0.01 and runs upto 0.99. It is observed that the maximum cyclic length obtained is 3,445,575 and it is obtained when the seed value is 0.96. The fluctuations in the cycle lengths can be visualized from Fig. 23.

In this figure, the seed values are plotted in the x-axis and the cyclic lengths are plotted in the y-axis. It is worth noting that for the seed value 0.96 the cyclic length becomes maximum. It should also be noted that for some seeds the cyclic length is very low, and hence those combinations may not be used direct. But this experiment is performed for only one value of the controlling parameter. In the second experiment, the effect of changing the value of the controlling parameter can be observed. The value of the initial seed is made fixed at 0.5 and the value of ψ varied ranging from 2.5 to 3.99. The maximum cyclic length obtained is 2,527,205 and this value is obtained for $\psi = 3.54$. Fluctuations in the cyclic length can be visualized from

Table 10 Obtained SSIM values

Image Id	$SSIM$
1	−0.1126
2	−0.03626
3	−0.33369
7	−0.096328
12	0.326965
14	−0.396523
15	−0.33011106
20	−0.2110396
25	−0.11120365
35	−0.4086932

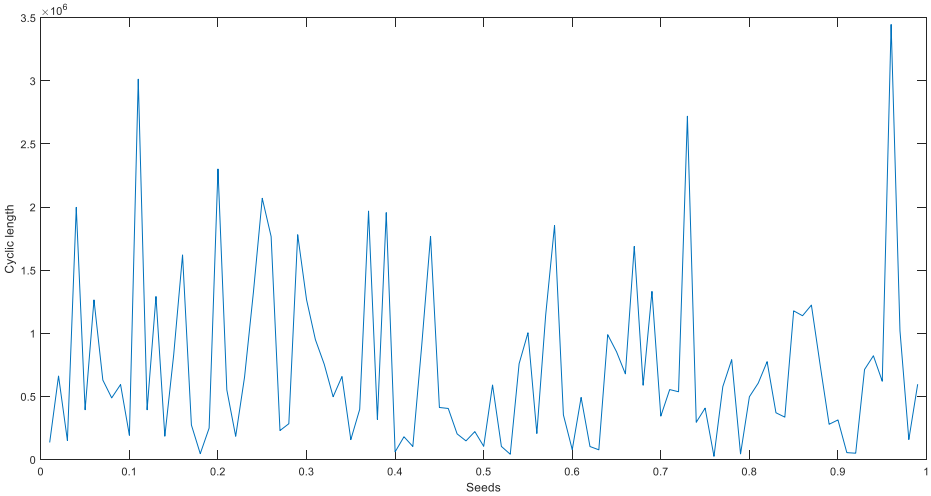


Fig. 23 Fluctuations in cyclic lengths when $\psi = 3.5$

Fig. 24. In this figure, the different values of ψ are plotted in the x-axis and corresponding of cyclic lengths are plotted in y-axis. It is worth noting that for the cyclic length becomes maximum when $\psi = 3.54$.

7 Conclusion

This article proposed a novel chaotic map called RCM and a new method to produce pseudorandom bit sequences. The proposed chaotic map and the pseudorandom bit generator is applied in an image cryptosystem. The proposed RCM map and the pseudorandom bit

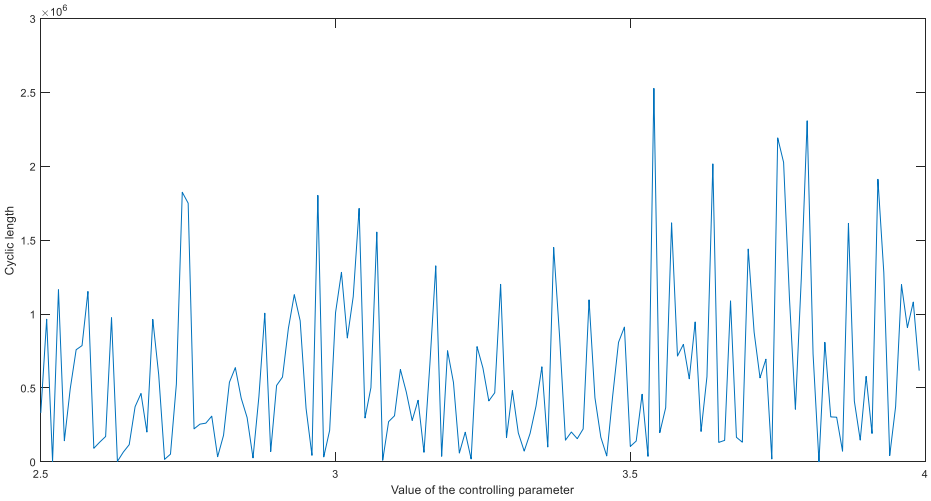


Fig. 24 Fluctuations in cyclic lengths when seed value = 0.5

generator is tested by various standard testing procedures to prove the strength and usefulness of it for various practical and real-life applications. The results which are produced by the proposed cryptosystem are tested and validated using both visual and quantitative methods which proves the effectiveness of the proposed method. The proposed image encryption method has no dependency on any external image in any phase of the whole process. The proposed method involves a significantly large keyspace and can easily withstand any exhaustive search-based attacks and statistical attacks. The scrambling method is flexible enough and can be easily modified by changing the rule of permutation. The proposed image encryption method is completely lossless and therefore, a cent percent of data can be recovered from the encrypted image. Simulation of the proposed method shows some aspiring results and encourages further experiments. This image encryption system is completely dependent on the proposed RCM map and proposed pseudorandom bit generation method and hence, highly sensitive to the initial conditions. Moreover, the i.e. number of iterations is another important parameter that serves as an additional layer of security. The proposed image encryption method is applied to various types of images and both visual and quantitative results speak itself about the strength and efficiency of the proposed approach. Therefore, the proposed image encryption system along with the proposed RCM map and the pseudorandom bit generator can be applied to secure real-life digital communications and can be further extended for various other types of data. The proposed image encryption system, the proposed RCM chaotic map, and the pseudorandom bit generator is found to be effective in securing digital images. However, in this work, only a single dimension is explored i.e. the application in the domain of image encryption. But the proposed approach can be applied in different other domains. For example, the proposed RCM map can be applied in the domain of non-linear dynamics, image segmentation, optimization problems, different industrial applications, neural networks, etc. Similarly, audio, video, text, and different other types of data can be encrypted with the proposed image encryption system with little or no modification. The proposed approach can further be extended by combining the metaheuristics with the proposed system. Moreover, the proposed scrambling approach can also be modified further the proposed system is flexible enough to adopt any new scrambling approach. Hence, there are lots of research directions on this topic is open that can be supported by this work.

References

1. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography
2. Ahmad J, Hwang SO (2016) A secure image encryption scheme based on chaotic maps and affine transformation. Multimed Tools Appl 75:13951–13976. https://doi.org/10.1007/s11042-015-2973-y
3. Ahmed HEH, Hamdy MK, Osama SFA (2006) Encryption quality analysis of the RC5 block cipher algorithm for digital images. Opt Eng 45:107003. https://doi.org/10.1117/1.2358991
4. Alatas B (2010) Chaotic harmony search algorithms. Appl Math Comput 216:2687–2699. https://doi.org/10.1016/j.amc.2010.03.114
5. Azar AT, Vaidyanathan S (2015) Chaos modeling and control systems design. Stud Comput Intell 581. https://doi.org/10.1007/978-3-319-13132-0
6. Behnia S, Akhshani A, Mahmodi H, Akhavan A (2008) A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons Fractals 35:408–419. https://doi.org/10.1016/j.chaos.2006.05.011
7. Bensikaddour EH, Bentoutou Y, Taleb N (2020) Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher. J King Saud Univ - Comput Inf Sci 32.1:50–56. https://doi.org/10.1016/j.jksuci.2018.05.002

8. Chakraborty S (2020) An advanced approach to detect edges of digital images for image segmentation. In: Chakraborty S, Mali K (eds) Applications of advanced machine intelligence in computer vision and object recognition: emerging research and opportunities. IGI GLobal
9. Chakraborty S, Mali K (2020) SuFMoFPA: a superpixel and meta-heuristic based fuzzy image segmentation approach to explicate COVID-19 radiological images. Expert Syst Appl 114142. https://doi.org/10.1016/j.eswa.2020.114142
10. Chakraborty, Shouvik, et al (2017) Image based skin disease detection using hybrid neural network coupled bag-of-features. In: 2017 IEEE 8th annual ubiquitous computing, Electronics and Mobile Communication Conference (UEMCON). IEEE, pp. 242–246
11. Chakraborty, Shouvik, et al. (2016) A novel lossless image encryption method using DNA substitution and chaotic logistic map. Int J Secur its Appl 10.2:205–216. https://doi.org/10.14257/ijsia.2016.10.2.19
12. Cheng H (2000) Partial encryption of compressed images and videos. IEEE Trans Signal Process 48:2439–2451. https://doi.org/10.1109/78.852023
13. Computer Security Division N FIPS (n.d.) 46–3, Data Encryption Standard (DES) (withdrawn May 19, 2005)
14. Cui G, Qin L, Wang Y, Zhang X (2008) An encryption scheme using DNA technology. In: 2008 3rd international conference on bio-inspired computing: theories and applications. IEEE, pp 37–42
15. CVG - UGR - Image database (n.d.). http://decsai.ugr.es/cvg/dbimagenes/g512.php. Accessed 15 Aug 2019
16. Daemen J, Rijmen RV (1999) The Rijndael block cipher: AES proposal. First candidate conference (AeS1)
17. Ephin M, Joy JA, Vasanthi NA (2013) Survey of Chaos based image encryption and decryption techniques
18. Farah, MA Ben, et al. (2020) A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt Laser Technol 121:105777. https://doi.org/10.1016/j.optlastec.2019.105777
19. Gehani A, LaBean T, Reif J (2003) DNA-based cryptography. Aspects of molecular computing. Springer, Berlin, Heidelberg, pp 167–188
20. Guo J (2014) Analysis of chaotic systems
21. Havaldar S, Gurumurthy KS (2017) Design of vedic IEEE 754 floating point multiplier. In: 2016 IEEE international conference on recent trends in electronics, information and communication technology, RTEICT 2016 - proceedings. Institute of Electrical and Electronics Engineers Inc., pp 1131–1135
22. Hosny KM (2020) Multimedia security using chaotic maps: principles and methodologies. Springer International Publishing, Cham
23. Hua Z, Zhou Y, Huang H (2019) Cosine-transform-based chaotic system for image encryption. Inf Sci (Ny) 480:403–419. https://doi.org/10.1016/J.INS.2018.12.048
24. Hua, Zhongyun, et al. (2015) 2D sine logistic modulation map for image encryption. Inf Sci (Ny) 297:80–94. https://doi.org/10.1016/J.INS.2014.11.018
25. Huang H, Yang S (2017) Colour image encryption based on logistic mapping and double random-phase encoding. IET Image Process 11:211–216. https://doi.org/10.1049/iet-ipr.2016.0552
26. Jolfaei A, Mirghadri A (2010) A new approach to measure quality of image encryption. Int J Comput Netw Secur 2(8):38–44
27. Karnaugh M (1953) The map method for synthesis of combinational logic circuits. Trans Am Inst Electr Eng Part I Commun Electron 72:(5)593–599. https://doi.org/10.1109/tce.1953.6371932
28. Kaushik S, Gandhi C (2019) Ensure hierarchal identity based data security in cloud environment. Int J Cloud Appl Comput 9:21–36. https://doi.org/10.4018/ijcac.2019100102
29. Kumar M, Saxena A, Vuppala SS (2020) A survey on chaos based image encryption techniques. In: Studies in Computational Intelligence. Springer, pp. 1–26
30. Lan R, He J, Wang S, Gu T, Luo X (2018) Integrated chaotic systems for image encryption. Signal Process 147:133–145. https://doi.org/10.1016/j.sigpro.2018.01.026
31. Lasota A, Mackey MC (1994) Chaos, fractals, and noise. Springer New York, New York, NY
32. Leong MP, Cheung OYH, Tsoi KH, Leong PHW A (n.d.) bit-serial implementation of the international data encryption algorithm IDEA. In: Proceedings 2000 IEEE Symposium on Field-Programmable Custom Computing Machines (Cat. No.PR00871). IEEE Comput. Soc, pp 122–131
33. Liao X, Li K, Zhu X, Liu KJR (2020) Robust detection of image operator chain with two-stream convolutional neural network. IEEE J Sel Top Signal Process 14:955–968. https://doi.org/10.1109/JSTSP.2020.3002391
34. Liao X, Yin J, Chen M, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features. IEEE trans dependable Secur Comput 1–1. https://doi.org/10.1109/tdsc.2020.3004708
35. Liu H, Abraham A, Clerc M (2007) Chaotic dynamic characteristics in swarm intelligence. Appl Soft Comput J 7:1019–1026. https://doi.org/10.1016/j.asoc.2006.10.006

36. Liu Z, Xia T (2018) Novel two dimensional fractional-order discrete chaotic map and its application to image encryption. Appl Comput Informatics 14:177–185. https://doi.org/10.1016/j.aci.2017.07.002
37. Luo RC, Chung LY, Lien CH (2002) A novel symmetric cryptography based on the hybrid haar wavelets encoder and chaotic masking scheme. IEEE Trans Ind Electron 49:933–944. https://doi.org/10.1109/TIE.2002.801252
38. Mali K, Chakraborty S, Seal A, Roy M (2015) An efficient image cryptographic algorithm based on frequency domain using Haar wavelet transform. Int J Secur Its Appl 9:279–288. https://doi.org/10.14257/ijsia.2015.9.12.26
39. Mansouri A, Wang X (2020) A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf Sci (Ny) 520:46–62. https://doi.org/10.1016/j.ins.2020.02.008
40. Mihailescu MI, Nita SL (2021) Chaos-based cryptography. In: Pro cryptography and cryptanalysis. Apress, Berkeley, CA, pp 359–378
41. Patro KAK, Acharya B, Nath V (2019) Various dimensional colour image encryption based on non-overlapping block-level diffusion operation. Microsyst Technol 1–12. https://doi.org/10.1007/s00542-019-04676-w
42. Pincus S (1995) Approximate entropy (ApEn) as a complexity measure. Chaos 5:110–117. https://doi.org/10.1063/1.166092
43. Rashmi P, Supriya MC, Kiran (2020) Colour image encryption using expand-shrink operation in Chaos encryption algorithm. IOP Conf Ser Mater Sci Eng 925:012027. https://doi.org/10.1088/1757-899x/925/1/012027
44. Roy M, Chakraborty S, Mali K, et al (2019) A dual layer image encryption using polymerase chain reaction amplification and dna encryption. In: 2019 International conference on Opto-electronics and applied optics, Optronix 2019. Institute of Electrical and Electronics Engineers Inc
45. Roy M, Chakraborty S, Mali K, et al (2020) Data security techniques based on DNA encryption. In: Advances in Intelligent Systems and Computing. Springer, pp. 239–249
46. Roy M, Chakraborty S, Mali K, et al (2019) Biomedical image security using matrix manipulation and DNA encryption. In: Advances in Intelligent Systems and Computing. Springer, Singapore pp. 49–60
47. Rukhin A, Soto J, Nechvatal J (2010) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Nist Spec Publ
48. Rukhin A, Soto J, Nechvatal J, et al (2010) SP800-22:A statistical test suite for random and pseudorandom number generators for cryptographic applications
49. Seal A, Chakraborty S, Mali K (2017) A new and resilient image encryption technique based on pixel manipulation, value transformation and visual transformation utilizing single–level haar wavelet transform
50. Skokos C (2010) The lyapunov characteristic exponents and their computation. Lect Notes Phys 790:63–135. https://doi.org/10.1007/978-3-642-04458-8_2
51. Sun F, Lu Z, Liu S (2010) A new cryptosystem based on spatial chaotic system. Opt Commun 283.10:2066–2073. https://doi.org/10.1016/j.optcom.2010.01.028
52. Tewari A, Gupta BB (2019) A novel ECC-based lightweight authentication protocol for internet of things devices. Int J High Perform Comput Netw 15:106. https://doi.org/10.1504/ijhpcn.2019.103548
53. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13:600–612. https://doi.org/10.1109/TIP.2003.819861
54. Wang X, Huang Y (2013) Devaney chaos revisited. Topol Appl 160.3:455–460. https://doi.org/10.1016/j.topol.2012.12.002
55. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18. https://doi.org/10.1016/J.OPTLASENG.2014.08.005
56. Wang X, Zhang Q (2009) DNA computing-based cryptography. In: 2009 fourth international on conference on bio-inspired computing. IEEE, pp 1–3
57. Wu Y, Noonan J, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1.2:31–38
58. Wu X, Wang D, Kurths J, Kan H (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf Sci (Ny) 349–350:137–153. https://doi.org/10.1016/J.INS.2016.02.041
59. Wu Y, Zhou Y, Noonan JP, Agaian S (2014) Design of image cipher using latin squares. Inf Sci (Ny) 264:317–339. https://doi.org/10.1016/J.INS.2013.11.027
60. Xu L, Gou X, Li Z, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52. https://doi.org/10.1016/j.optlaseng.2016.10.012
61. Xu M, Tian Z (2019) A novel image cipher based on 3D bit matrix and latin cubes. Inf Sci (Ny) 478:1–14. https://doi.org/10.1016/J.INS.2018.11.010
62. Yang J, Wang L, Baek J (2018) A privacy preserving and fine-grained access control scheme in DaaS based on efficient DSP re-encryption. Int J High Perform Comput Netw 11:231–241. https://doi.org/10.1504/IJHPCN.2018.091894

63. Ye R (2011) A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt Commun 284.22:5290–5298. https://doi.org/10.1016/j.optcom.2011.07.070
64. Yu XY, Zhang J, Ren HE, Li S, Zhang XD (2006) A new measurement method of Iimage encryption. J Phys Conf Ser 48:408–411. https://doi.org/10.1088/1742-6596/48/1/077
65. Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39–49. https://doi.org/10.1016/J.OPTLASENG.2017.04.009
66. Zhang Y (2018) The unified image encryption algorithm based on chaos and cubic S-box. Inf Sci (Ny) 450: 361–377. https://doi.org/10.1016/J.INS.2018.03.055
67. Zhang Y (2020) The fast image encryption algorithm based on lifting scheme and chaos. Inf Sci (Ny) 520: 177–194. https://doi.org/10.1016/j.ins.2020.02.012
68. Zhang M, Tong X (2014) A new chaotic map based image encryption schemes for several image formats. J Syst Softw 98:140–154. https://doi.org/10.1016/j.jss.2014.08.066
69. Zhang X, Wang X (2017) Multiple-image encryption algorithm based on mixed image element and chaos. Comput Electr Eng 62:401–413. https://doi.org/10.1016/j.compeleceng.2016.12.025
70. Zhang W, Yu H, Zhao Y, Zhu Z (2016) Image encryption based on three-dimensional bit matrix permutation. Signal Process 118:36–50. https://doi.org/10.1016/J.SIGPRO.2015.06.008
71. Zheng, Qiming, et al. (2017) A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service. IEEE Access 6:711–722. https://doi.org/10.1109/ACCESS.2017.2775038
72. Zhou Y, Cao W, Philip Chen CL (2014) Image encryption using binary bitplane. Signal Process 100:197–207. https://doi.org/10.1016/J.SIGPRO.2014.01.020
73. Zhou Y, Panetta K, Agaian S, Chen CLP (2013) (n, k, p)-gray code for image systems. IEEE Trans Cybern 43:515–529. https://doi.org/10.1109/TSMCB.2012.2210706
74. Zhu S, Han Y (2018) Secure data outsourcing scheme in cloud computing with attribute-based encryption. In: International Journal of High Performance Computing and Networking. Inderscience Enterprises Ltd., pp. 128–136
75. Zhu Z, Zhang W, Wong K, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci (Ny) 181:1171–1186. https://doi.org/10.1016/J.INS.2010.11.009