



# A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map

Bhaskar Mondal<sup>1</sup> · Pratap Kumar Behera<sup>2</sup> · Sugata Gangopadhyay<sup>2</sup>

Received: 7 August 2019 / Accepted: 23 December 2019 / Published online: 9 January 2020  
© Springer-Verlag GmbH Germany, part of Springer Nature 2020

## Abstract

In this paper, we propose a new 2D sine–cosine cross-chaotic (SC3) map to design an image encryption scheme with high confusion and diffusion capability. We evaluate the maximum Lyapunov exponent (MLE) of the proposed SC3 map to measure its degree of sensitivity to initial conditions and perform bifurcation analysis to find the chaotic region. The proposed chaotic map generates two pseudo-random sequence  $R_1$  and  $R_2$ , which are used in confusion (permutation) and diffusion phase, respectively. The confusion layer is designed by shuffling the image pixels, and the diffusion layer is designed by bitwise XOR operation. The strength of the proposed image encryption scheme is evaluated against resistance to the statistical attack (information entropy, correlation coefficient, and histogram analysis), differential attack (NPCR and UACI), and sensitivity to the secret key. The experimental results of both security and performance analysis show that the proposed image encryption scheme is secure enough to resist all the existing cryptanalytic attack and efficient in terms of encryption time.

**Keywords** Confusion and diffusion · Sine–cosine cross-chaotic map · Lyapunov exponent · Differential attack

## 1 Introduction

With the rapid increase in the number of smart devices, Internet of Things (IoT) devices, and lightweight mobile applications, a huge amount of multimedia data (images) are being generated and transmitted over the insecure public channel and stored in a trusted cloud server. The user's data communicated over an insecure channel is vulnerable and must be protected from the existing cryptanalytic attack. The traditional block cipher such as AES [1] and DES [2], lightweight block cipher such as PRESENT, GIFT and stream cipher such as grain [3] are not efficient enough in a constrained environment due to low computational and storage capability.

To improve the performance of an image encryption scheme without compromising the security level, chaos-based cryptosystem [4–7] is a suitable choice for fast and secure transmission of multimedia data. In fact, chaos-based cryptosystems are based on the confusion and diffusion principle as proposed by Claude Shannon [8]. Confusion principle hides the relationship between key and ciphertext, whereas diffusion principle hides the relationship between plaintext and ciphertext as complex as possible. The inherent characteristics of any chaos-based cryptosystems are unpredictability and sensitivity to initial conditions, which are based on confusion and diffusion principle respectively. The existing chaotic map is of two types, i.e., 1D chaotic map [9–11] and multidimensional chaotic map [12–14]. In 1D chaotic map, only one variable and few parameters are involved to generate the pseudo-random sequence. The initial parameters are easily estimated due to small key space and less complex structure of 1D chaotic maps. So, it is not secure enough for image encryption. On the other hand, multidimensional chaotic map involves multiple initial variables, which makes it more secure than 1D chaotic map, but takes more computational time.

In this paper, we design a chaotic map called 2D sine–cosine cross-chaotic (SC3) map, which generates two different pseudo-random sequences concurrently  $R_1$  and

✉ Pratap Kumar Behera  
pbehera@cs.iitr.ac.in

Bhaskar Mondal  
bhaskarmondal.cs@gmail.com

Sugata Gangopadhyay  
sugatfma@iitr.ac.in

<sup>1</sup> Xavier School of Computer Science and Engineering, Xavier University Bhubaneswar, Orissa, India

<sup>2</sup> Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee, India

$R_2$  for confusion (permutation) and diffusion layer, respectively. The pseudo-random sequence  $R_1$  is used to permute the image pixels to reduce the high correlation between adjacent pixels within the plain image. The pseudo-random sequence  $R_2$  is used to modify the pixel values of the permuted image by doing bitwise XOR operation. Based on the security requirements, the encryption process can be iterated for multiple rounds to make it more secure according to the type of environment (hardware/software).

## 2 Our contribution

The contribution of our research work is twofold: first one is from chaotic point of view, and second one is security analysis. The performance of our proposed 2D SC3 map is evaluated by the phase diagram, bifurcation analysis, and randomness testing. The security analysis is performed on image encryption using permutation and diffusion structure.

The proposed chaotic map has achieved a much wider range of chaotic behavior. The proposed 2D SC3 map has chaotic behavior when  $\alpha \in [0.49, 1]$ , and  $\beta \in [0.79, 1]$  and maximum Lyapunov exponent value  $\lambda_1$  and  $\lambda_2$  is 2.6239 and 2.6189, respectively. A higher value of LE increases its degree of unpredictability and sensitivity to initial condition. We compare our proposed chaotic map with 2D LASM [15] in terms of LE, and chaotic range. The proposed chaotic map has a higher LE value and a much wider chaotic range than 2D LASM. The NIST statistical testing results shows that the proposed chaotic map passed all the tests, which signifies the chaotic map is truly random as recommended by NIST [16].

To measure the confusion and diffusion capability of our proposed chaotic map, we design an image encryption algorithm using permutation and diffusion structure. The control parameters ( $\alpha, \beta$ ) are chosen within their corresponding chaotic range along with initial parameter ( $x_0, y_0$ ) as a secret key. The initial seed or secret key is used to generate the pseudo-random sequence to permute the image pixel followed by the bit diffusion process with XOR operation. The security analysis of the image encryption algorithm resistance to statistical attack, differential attack, and sensitivity to the secret key shows that the proposed chaotic map has high confusion and diffusion capability to attain desired security level.

## 3 Related work

In this section, we will discuss about the recently proposed chaotic map used in the image encryption scheme for both grayscale and color images. The main idea of designing any chaos-based image encryption scheme is to resist both statistical attack and cryptanalytic attack [17]. So, it is important

to analyze cryptographic strength of the proposed chaotic map. The chaotic behavior of any chaotic map denotes the confusion and diffusion capability of the proposed scheme. First, we describe the properties used to evaluate the confusion and diffusion capability of any chaotic map and later we discuss the underlying architecture used for image encryption. The Lyapunov exponent is a quantitative measurement to check sensitivity to the initial conditions [18] of any chaotic map. To achieve the high confusion and diffusion capability, the pseudo-random sequence with chaotic behavior is not enough. The underlying architecture also plays an important role for security of the image encryption to resist both statistical and cryptanalytic attack. Basically, there are three widely known architectures for designing an image cryptosystem, such as permutation (confusion) only, diffusion only, and both permutation–diffusion structure [19]. In permutation only method, the image pixels are shuffled to reduce the high correlation among adjacent pixels. Since only pixel values are shuffled, the distribution of pixel values remains unchanged in cipher image and becomes non-uniform, which makes the cipher vulnerable against statistical attack. A study on some popular image scrambling techniques is presented in [20]. In diffusion only structure, the pixel values are modified using bit permutation or Xor operation, which results a uniform distribution of the pixel values in an encrypted image. But in diffusion structure, high correlation among adjacent pixels is not fully reduced, which leads to the correlation attack. In permutation–diffusion structure [21], the plain image is permuted first, and then the diffusion operation is performed by modifying the pixel values.

Almost all chaos-based image encryption schemes follow permutation–diffusion structure by 1D chaotic map [9], multidimensional (2D/3D) chaotic map, multiple 1D chaotic map [12, 15, 22, 23], chaotic map with DNA computing [14, 24, 25], chaotic map with cellular automata [21, 22], or chaos-based S-Box [6, 10, 26, 27]. The main goal is to design an image encryption scheme with computational complexity without compromising the security level, specially for constrained environment and lightweight mobile application.

The 1D chaotic map has a simple structure and generating only one pseudo-random sequence. It is easy to implement and takes less computational effort, but it is vulnerable to the cryptanalytic attack due to its simple structure. Zhu et al. [28] proposed a symmetric image encryption scheme based on a 1D logistic map for diffusion operation and Arnold cat map for bit-level permutation. The computational complexity is very high in this scheme. Belazi et al. [29] propose a novel image encryption scheme which is based on 1D chaotic map and S-Boxes using the substitution–permutation network. The author used a new chaotic map for diffusion using XOR operation and then performed the substitution

operation using S-Boxes. The diffusion is done using the logistic map, and finally permutation is performed with a permutation function. This cryptosystem has a more complex structure, and time complexity is quite higher. Wang et al. [25] apply the logistic map for color image encryption using pixel-level permutation as a combination of row scrambling and column scrambling followed by the diffusion. The author generates two different pseudo-random sequences with length  $3M \times N$  and  $3M \times N$  for row and column scrambling, respectively, for RGB components.

Wu et al. [23] propose a robust color image encryption scheme using three different improved 1D chaotic maps and DNA computing such as logistic tent system, logistic sine system, and tent sine system. The security level is quite high in comparison to other image encryption schemes. The computational complexity is more, as it uses three different maps and it involves encoding and decoding process of DNA computing, which is not suitable for a lightweight application. Cao et al. [30] design an image encryption scheme based on 2D LICM hyperchaotic map using bit permutation approach for both confusion and diffusion layer. Since the bit permutation is a time-consuming approach, so this encryption scheme was also not efficient for a constrained environment. Hua et al. [15] use 2D logistic-adjusted sine map to design image cryptosystem with bit manipulation confusion and diffusion. This encryption scheme adds a random number to the surrounding pixel intensities of the plain image in every round to enhance the security level. Mondal et al. [21] propose an image encryption scheme based on cellular automata and chaotic skew tent map. The author used the skew tent map to generate the initial vector for cellular automata. The plain image then permuted using pseudo-random sequence followed by the diffusion process. Ping et al. [22] designed image cipher using life-like cellular automata and chaotic map with the permutation–substitution network. The cellular automata-based image cipher using chaotic map suffers from drawbacks such as having no explicit classification of CA rules, small rule space and low diffusion capability.

Fu et al. [31] propose an image encryption scheme with improved spatial bit-level permutation strategy using the 3D cat map. The bit-level permutation has both confusion and diffusion capability. The author generates the keystream using a function of secret key and plain image to enhance the security against chosen plaintext attack. Ping et al. [32] design an image encryption scheme with simultaneous permutation–substitution structure using discrete henon map. The plain image is scanned only once and the image pixels are shuffled with pixel positions generated by 2D discrete henon map and followed by two-point diffusion simultaneously using the keystream as a function of plain image. The proposed scheme increases the efficiency of image encryption with simultaneous confusion and diffusion operation. Kandar et al. [33] design image encryption

using the sequence generated by the cyclic group for both confusion and diffusion process. The author applied both row permutation and column permutation in confusion phase, bit-level permutation and bit-level transformation in diffusion phase using the pseudo-random sequence generated by the cyclic group. Liu et al. [6] propose a color image encryption scheme using chaos-based bijective S-Box. The chaotic map used in this paper generates three different pseudo-random sequences for both confusion and diffusion. The confusion process is substituted by bijective S-Box and diffusion process done using bitwise XOR operation. Zhan et al. [34] proposed a scalable coding scheme, which performs encryption using modulo-256 addition followed by an encoding scheme. In this scheme, encoded bit streams are made of quantized subimage and remainders of Hadamard coefficients. Qin et al. [35] proposed a scheme for image encryption with compression techniques. The plain image is masked with modulo-256 addition followed by a block permutation. This scheme achieves better rate-distortion performance. Panwar et al. [36] propose an image encryption using DNA sequence and multiple 1D chaotic map. In this paper, the author analyzes how the original encryption scheme found to be low sensitivity by slight modification of plain image which leads to diffusion process becoming insecure. The author improves the existing techniques to resist these shortcomings. The same author [37] also improve the image encryption by combination of 1D chaotic map.

## 4 Preliminaries

A chaotic map is an evolution function which is a deterministic, and nonlinear dynamic system. It generates a pseudo-random sequence having both confusion and diffusion capability, so that it can be secured enough when applied for image encryption. The chaotic map can be defined as follows:

$$x_{n+1} = f(x_n), \quad (1)$$

where  $n = 0, 1, 2, \dots$ , and so on. It determines the value of the next state based on the present state. The dynamics of the systems depends upon the composition of the  $n$ th iteration of the evolution function, i.e.,  $f^n(x_0)$ . The most important properties of any chaotic map is its chaotic behavior, i.e., sensitive to initial condition, wider chaotic range. The sensitivity to an initial condition properties is important for image encryption. To design an evolution function, initial parameters are not enough, it requires some control parameter to become more chaotic. But the 1D chaotic map is vulnerable to cryptanalytic attack and not secure for image encryption. So the chaotic map is dependent on multiple initial values as well as multiple control parameters to increase the security

level and this type of chaotic map is called multidimensional chaotic map, which can be generalized as Eq. 2:

$$\begin{cases} x_{i+1} = f_1(y_i; \alpha_i) \\ y_{i+1} = f_2(x_i; \alpha_i). \end{cases} \quad (2)$$

In the above equation,  $f_1$  and  $f_2$  are both inter-dependent to generate two different pseudo-random sequences and this type of chaotic map is called cross-chaotic map. In this paper, we propose a sine–cosine cross-chaotic map which demonstrates all properties of chaotic behavior. The map is used to generate two pseudo-random sequence.

### 5 Proposed 2D sine–cosine cross-chaotic (SC3) map

In this section, the mathematical definition of our proposed chaotic map is presented and then evaluated whether the proposed system exhibits chaotic behavior. The 2D SC3 map is defined in Eq. 3.

$$\begin{cases} x_{i+1} = \sin\left(\frac{\alpha}{y_i}\right)^{\frac{3}{2}} \\ y_{i+1} = \cos\left(\beta \cos^{-1}x_i\right), \end{cases} \quad (3)$$

where  $x_0, y_0$  are two initial parameters,  $(x_0, y_0) \in [0, 1]$  and  $\alpha, \beta$  are two control parameters, where  $(\alpha, \beta) \in [0, 1]$ .

#### 5.1 Bifurcation analysis and phase diagram

The performance of the chaotic map is measured by the phase diagram, bifurcation analysis, and Lyapunov exponent.

The phase diagram represents the distribution of attractors or output pairs  $(x_{i+1}, y_{i+1})$  in a 2D phase plane. The attractors of our proposed 2D SC3 map is shown in Fig. 1 with initial values  $(x_0, y_0) = (0.5, 0.6)$ . The figure denotes the distribution of data covers a much larger region, which signifies the proposed map covers the entire region. It is not clustered to a particular region, which tells the randomness and uniform distribution of the pseudo-random sequence to achieve the high diffusion capability. The phase diagram suggests it is more chaotic, and good ergodicity.

Bifurcation occurs when there is a changes in its topological structure with respect to change in control or bifurcation parameter, i.e., distribution of output values with respect to its control parameters. The bifurcation diagram are shown in Figs. 2 and 3 with respect to varying of  $\alpha$  and  $\beta$ , respectively. Figure 2a, b represents the bifurcation diagram of  $X$  and  $Y$  sequence, respectively, when  $\alpha$  varies from 0 to 1 and  $\beta = 0.85$  with step value of 0.001. The solid line represents the fixed point and periodic window, whereas the dotted line represents the chaotic region. The obtained results show that

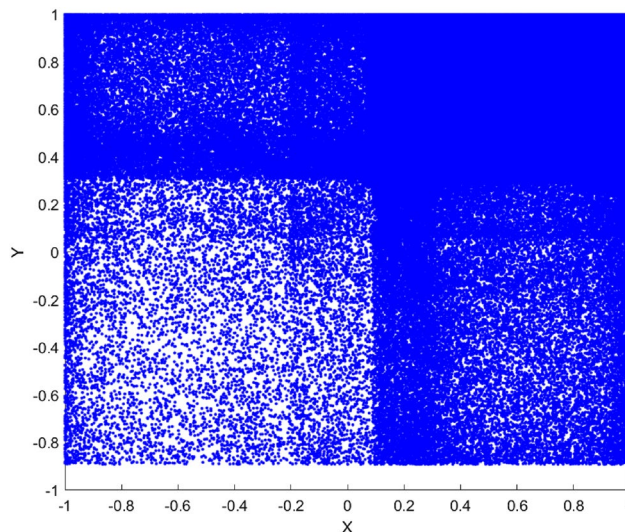


Fig. 1 Phase diagram of proposed chaotic map

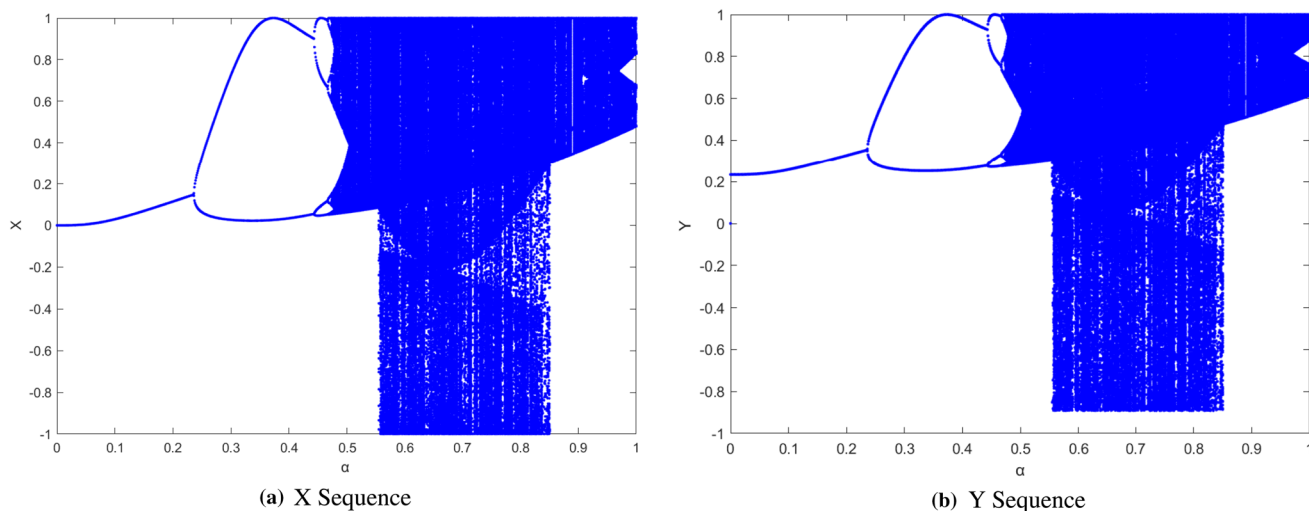
the proposed map has chaotic behavior when control parameter  $\alpha \in [0.49, 1]$ . Figure 3a, b shows the bifurcation diagram of  $X$  and  $Y$  sequence, respectively, when  $\beta$  varies from 0 to 1 and  $\alpha = 0.90$ . The figure signifies that the system attains the chaotic behavior when  $\beta \in [0.79, 1]$ . The wide chaotic range of the control parameter suggests that it has large key space which improves the security of the cipher against an exhaustive search attack.

#### 5.2 Maximum Lyapunov exponent

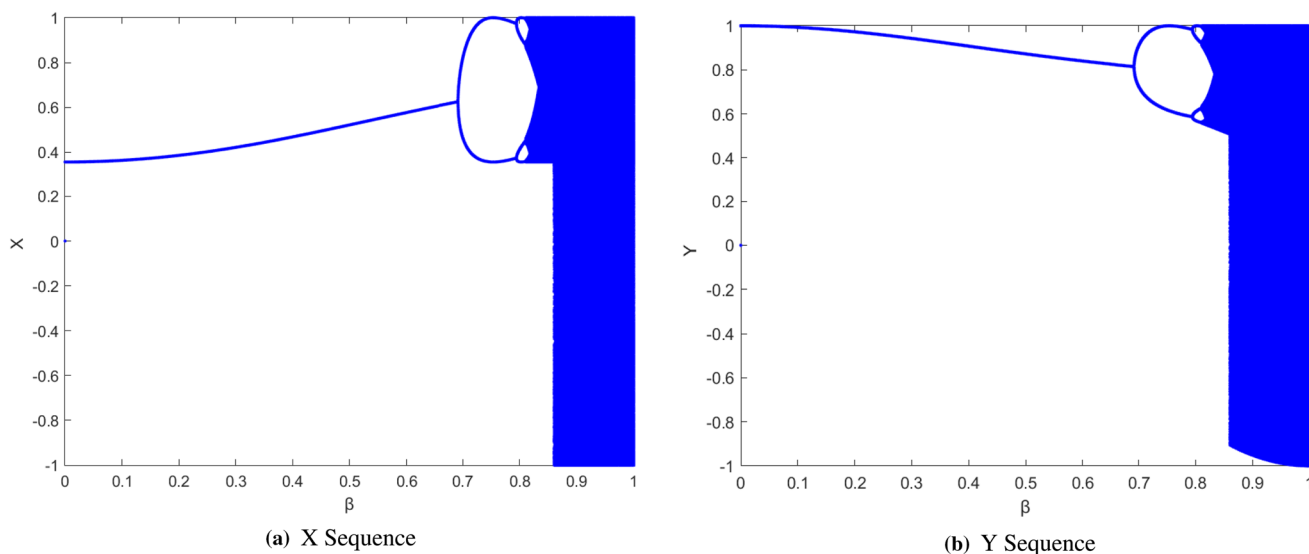
The chaotic behavior of a dynamical system is defined by its sensitiveness to initial conditions and unpredictability. The Lyapunov exponent is a quantitative measurement to determine the dynamic system’s chaotic behavior [38]. Lyapunov exponent measures the degree of divergence between any two nearby trajectories of a dynamic system which is the stretching of an orbit. If the orbit is stable, then the maximum Lyapunov exponent is less than zero and stretching is minimal. The positive value of maximum Lyapunov exponent shows exponential stretching of an orbit. Technically, if we take two initial points which are very close together say  $x_0, y_0(x_0 + \delta_0)$  and iterate the evolution function  $n$  times to get the  $x_n$  and  $y_n$ . The difference between two sequence  $y_n - x_n$  should grow exponentially and is mathematically defined in Eq. 4:

$$|\delta_n| \sim |\delta_0|e^{\lambda n}. \quad (4)$$

The constant  $\lambda$  is called Lyapunov exponent. If the Lyapunov exponent (LE)  $\lambda$  is positive, then the system is chaotic and if it is negative or zero then the systems exhibits non-chaotic



**Fig. 2** Bifurcation diagram ( $\alpha = \text{vary}, \beta = 0.85$ )



**Fig. 3** Bifurcation diagram ( $\beta = \text{vary}, \alpha = 0.90$ )

behavior. Every chaotic system has at least one positive Lyapunov exponent to achieve the chaotic behavior.

$$\lambda(x_0) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|. \tag{5}$$

A multidimensional chaotic map has more than one LE and if all the LEs are positive, then the dynamic systems possess hyperchaotic behavior. The hyperchaotic behavior is good for image encryption and it is very difficult for attacker to predict the secret key.

In this paper, we calculate the Lyapunov exponent by keeping  $\alpha$  vary,  $\beta$  fixed and  $\beta$  vary,  $\alpha$  fixed as shown in Figs. 4 and 5, respectively. Since our proposed chaotic

map is 2D, it has two Lyapunov exponents ( $\lambda_1$  and  $\lambda_2$ ). Figure 4 shows the Lyapunov exponent values  $\lambda_1$  and  $\lambda_2$  with respect to change in control parameters, i.e.,  $\alpha$  varies from 0 to 1 and  $\beta = 0.85$ . We observe that both  $\lambda_1$  and  $\lambda_2$  are positive when  $\alpha \in [0.49, 1]$ . The maximum Lyapunov exponent value of  $\lambda_1$  and  $\lambda_2$  is 2.3218 and 2.2938, respectively. Similarly, Fig. 5 shows the Lyapunov exponent values  $\lambda_1$  and  $\lambda_2$  with respect to change in control parameters, i.e.,  $\beta$  varies from 0 to 1 and  $\alpha = 0.90$ . Both  $\lambda_1$  and  $\lambda_2$  are positive, when  $\beta \in [0.79, 1]$ . The maximum Lyapunov exponent value of  $\lambda_1$  and  $\lambda_2$  is 2.6239 and 2.6189, respectively. The higher value of LE denotes the system is more difficult to be predicted. The computation of maximum Lyapunov exponent is performed with different combinations of  $\alpha$

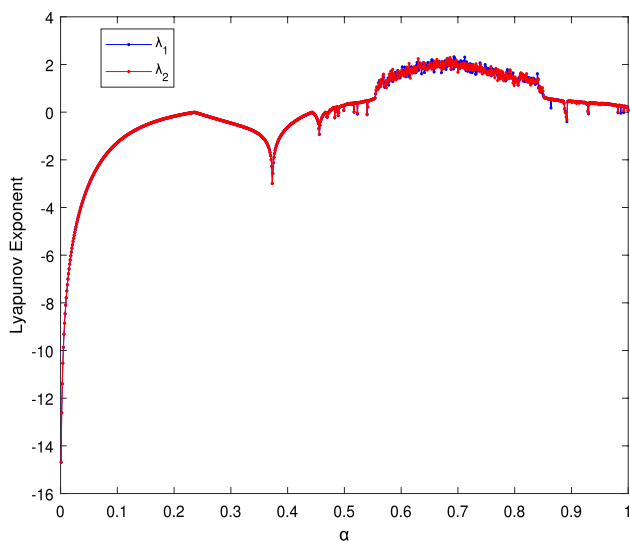


Fig. 4 Lyapunov exponent ( $\alpha = \text{vary } \beta = 0.85$ )

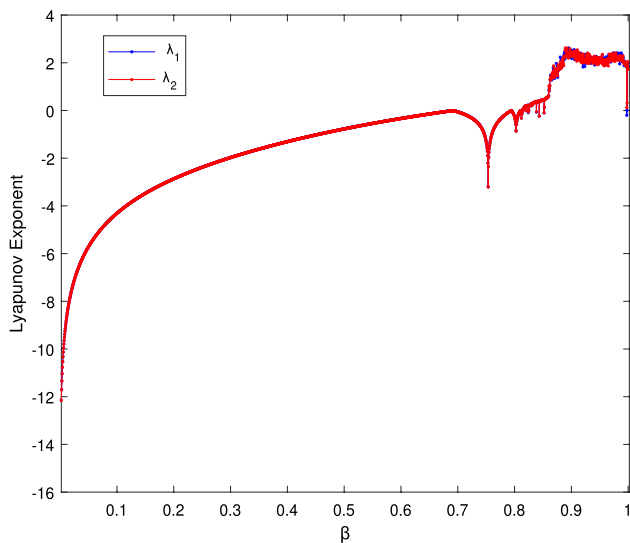


Fig. 5 Lyapunov exponent ( $\beta = \text{vary } \alpha = 0.90$ )

Table 1 Lyapunov exponent value of the proposed map

$(\alpha, \beta)$	LE ( $\lambda_1$ )	LE ( $\lambda_2$ )
(0.85, 0.90)	1.9577	2.1899
(0.88, 0.95)	2.2718	2.3670
(0.70, 0.90)	2.7632	2.4306
(0.75, 0.85)	1.8427	1.6771

and  $\beta$  as shown in Table 1. We compared our results with the results obtained by the chaotic map [29] as shown in Table 2, and it shows that the proposed chaotic map has higher Lyapunov exponent.

Table 2 Lyapunov exponent value of the existing chaotic map [29]

(IC, PC)	LE
(0.3, 8)	1.38632
(0.4, 7.6)	1.09744
(0.6, 6.258)	0.996836
(0.5, 6)	0.968348

### 5.3 NIST statistical test

The pseudo-random sequence generated by the chaotic map must satisfy the randomness property for cryptographic application. The pseudo-random sequence generated for image encryption should be unpredictable even if the initial and control parameters are known to the attacker. For cryptographic application, the sequence must be truly random or it must be indistinguishable from a random sequence in a polynomial time algorithm. Randomness in a given sequence is defined as the distribution of data in different patterns of sequence which is difficult to be predicted by the attacker. The NIST published a test battery to evaluate the randomness criteria of any binary sequence by detecting the deviation of a given binary sequence from a randomness property. There are sixteen different test criteria present in NIST test suite [39] to check the randomness property of either random or pseudo-random generator. We calculate the  $p$  value of our sequence generated by the proposed chaotic map. To evaluate any randomness testing, the  $p$  value is compared with the significance level  $\alpha$ . If the resulting  $p$  value is larger than the significance level  $\alpha$ , then the test is random and considered as passed. As recommended by NIST,  $\alpha$  is commonly set to 0.01 for cryptographic application.

In our experiment, we perform NIST statistical test on 100 different sequence of length  $(10)^k$ , where  $k$  varies from 3 to 5 for all the test suite except binary matrix rank and Maurer’s universal statistical test. For binary matrix rank test and Maurer’s universal statistical test, the minimum length of the bit string sequence must be 38912 bits and 387840 bits, respectively, as per NIST recommendation [16, 39]. The pseudo-random sequence generated by our proposed chaotic map passed all the NIST statistical tests and the test result is shown in Table 3.

### 5.4 Discussion

In this section, we evaluate the performance of our proposed chaotic map in terms of phase diagram, bifurcation analysis, and Lyapunov exponent. The phase diagram of proposed 2D SC3 map covers whole data range in a 2D phase plane and has much larger distribution. The output pairs  $(x_{i+1}, y_{i+1})$  become more dense as it approaches 1. We compare our phase diagram with 2D logistic map, 2D SLMM, Henon map, and 2D LASM. The comparison results shows that

**Table 3** NIST statistical test results

Statistical test	X		Y	
	p value	Result	p value	Result
Frequency test (monobit)	0.12904130	Passed	0.22949314	Passed
Frequency test within a block	0.55073783	Passed	0.58415244	Passed
Run test	0.95712949	Passed	0.063684666	Passed
Longest run of ones in a block	0.28376140	Passed	0.38592092	Passed
Binary matrix rank test	0.06175534	Passed	0.12975621	Passed
Discrete Fourier transform (spectral) test	0.14679308	Passed	0.24573870	Passed
Non-overlapping template matching test	0.02864036	Passed	0.98727193	Passed
Maurer’s universal statistical test	0.59803015	Passed	0.59803015	Passed
Linear complexity test	0.91968885	Passed	0.67666207	Passed
Serial test-1	0.84711484	Passed	0.84711484	Passed
Serial test-1	0.70556119	Passed	0.57042515	Passed
Approximate entropy test	0.99920661	Passed	0.9992917	Passed
Cumulative sums (forward) test	0.22768839	Passed	0.1754094	Passed
Cummulative sums (reverse) test	0.18747258	Passed	0.34770916	Passed
Random excursions test (state = - 1)	0.17868683	Passed	0.29880578	Passed
Random excursions variant test (state= - 1)	0.26355247	Passed	0.84451926	Passed

the output trajectory of 2D logistic map, Henon map, and 2D SLMM chaotic map clustered to a particular region, whereas the phase diagram of proposed 2D SC3 map covers entire region in 2D phase plane. The bifurcation analysis of 2D LASM has chaotic behavior when  $\mu \in [0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93] \cup 1$ , i.e., which seems to cover less range as compared to proposed 2D SC3 map. The proposed map has chaotic behavior when  $\alpha \in [0.49, 1]$ , and  $\beta \in [0.79, 1]$ . The proposed map covers a much wider region than 2D LASM. The maximum Lyapunov exponent values  $\lambda_1$  and  $\lambda_2$  are 2.6239 and 2.6189, respectively, which is much higher than the Lyapunov exponent value of 2D LASM ( $\lambda < 1.5$ ). We also compared our Lyapunov exponent results with the chaotic map mentioned in the Table 2. The maximum value of LE has achieved by the chaotic map [29] is 1.38632, which is much lesser than our proposed chaotic map.

We perform NIST statistical testing on the pseudo-random sequence generated by the proposed chaotic map to check the randomness property. The proposed chaotic map passed 14 test out of 16 statistical testing as shown in Table 3.

### 6 Proposed cryptosystem based on SC3 map

In this section, we apply our proposed 2D SC3 map to design the cryptosystem for image encryption to resist the brute force attack, statistical attack, and differential attack. But in permutation followed by bit-level diffusion structure, the encryption algorithm both shuffles the

image pixels and substitutes with different values which can resist all types of attack like statistical attack, differential attack, and correlation attack. The architecture of our proposed cryptosystem is shown in Fig. 6. The architecture takes the plain image as input and transformed to cipher image by applying pixel shuffling and bitwise XOR using pseudo-random sequences  $R_1$  and  $R_2$ , respectively. The pseudo-random sequences  $R_1$  and  $R_2$  were generated as a function of the shared secret key using the proposed 2D SC3 map. The initial parameters  $(x_0, y_0)$  and control parameters  $(\alpha, \beta)$  combined together  $(x_0, y_0, \alpha, \beta)$  and  $(x'_0, y'_0, \alpha', \beta')$  to form the secret key  $K_1$  and  $K_2$  for both confusion and diffusion layer, respectively. The encryption and decryption process is described in algorithm 1 and algorithm 2, respectively.

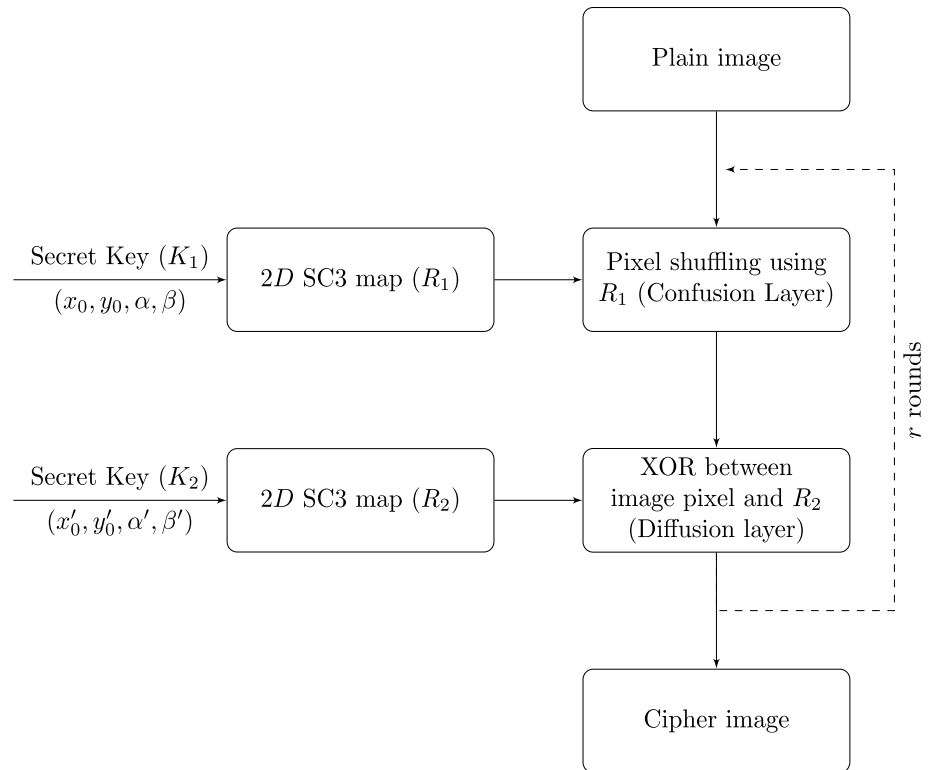
**Algorithm 1:** Key setup and Encryption process

```

1 Read the 2D plain image P of size W × H and convert into 1D vector P = {p1, p2, ..., pN},
  where N = W × H;
2 Generate the control parameters α, β ∈ [0, 1] and obtain initial parameters x0, y0 ∈ [0, 1];
3 Secret key K1 = (x0, y0, α, β) and K2 = (x'0, y'0, α', β');
4 for i ← 1 to N do
5   | x_{i+1} = sin(α/y_i)^(3/2);
6   | t1 = (x_{i+1} × 10^15) mod W × H;
7   | Insert t1 into R1;
8   | y_{i+1} = cos(β acos x_i);
9   | t2 = (y_{i+1} × 10^15) mod 256;
10  | Insert t2 into R2;
11 end
12 for j ← 1 to N do
13  | I ← swap(P[j], P[R1[j]]);
14 end
15 for k ← 1 to N do
16  | C[k] ← XOR(I[k], R2[k]);
17 end
18 Reshape the sequence C into size of W × H cipher image;

```

**Fig. 6** Architecture of proposed image cryptosystem



## 6.1 Confusion based on pixel scrambling

The confusion principle states that the relationship between cipher image, and secret key should be as complex as possible and sensitive to the secret key. The changes of single bit in secret key must affect the cipher image in a pseudo-random way. The pixel shuffling phase permutes the plain image using the pseudo-random sequence  $R_1$  to reduce the correlation between the adjacent pixel.

### Algorithm 2: Decryption process

```

1 Obtain the secret key  $K_1(x_0, y_0, \alpha, \beta)$  and  $K_2(x'_0, y'_0, \alpha', \beta')$ ;
2 Read the cipher image  $C$  of size  $W \times H$  and decompose into 1D vector of size  $N (W \times H)$ ;
3 for  $i \leftarrow 1$  to  $N$  do
4    $x_{i+1} = \sin\left(\frac{\alpha}{y_i}\right)^{\frac{2}{3}}$ ;
5    $t_1 = (x_{i+1} \times 10^{15}) \bmod W \times H$ ;
6   Insert  $t_1$  into  $R_1$ ;
7    $y_{i+1} = \cos(\beta \cos x_i)$ ;
8    $t_2 = (y_{i+1} \times 10^{15}) \bmod 256$ ;
9   Insert  $t_2$  into  $R_2$ ;
10 end
11 for  $j \leftarrow 1$  to  $N$  do
12    $I[j] \leftarrow \text{XOR}(C[j], R_2[j])$ ;
13 end
14 for  $k \leftarrow 1$  to  $N$  do
15    $P \leftarrow \text{swap}(I[k], I[R_1[k]])$ ;
16 end
17 Reshape the sequence  $P$  into size of  $W \times H$  plain image;
  
```

## 6.2 Diffusion using bit manipulation

The diffusion principle hides the relationship between the plain image and cipher image by making it as complex as possible to resist the differential attack. The diffusion phase not only hides the relationship between plain image and cipher image, it also maintains the uniform distribution of pixel values of the cipher image. That means, as the pixel values of plain images are highly clustered within a particular interval, the attacker can mount the statistical attack by computing the variance of the histogram. The good diffusion methods transform the plain image into cipher image with uniform distribution of pixel values which is difficult for the statistical attack. The diffusion phase suggests that the cipher image is highly sensitive to the change in plain image pixel values, i.e., one pixel change in plain image must be changed into cipher image by at least 50%. This is called avalanche effect. In this paper, the pixel values are manipulated using bitwise XOR operation with the pseudo-random sequence  $R_2$  generated by the 2D SC3 map.



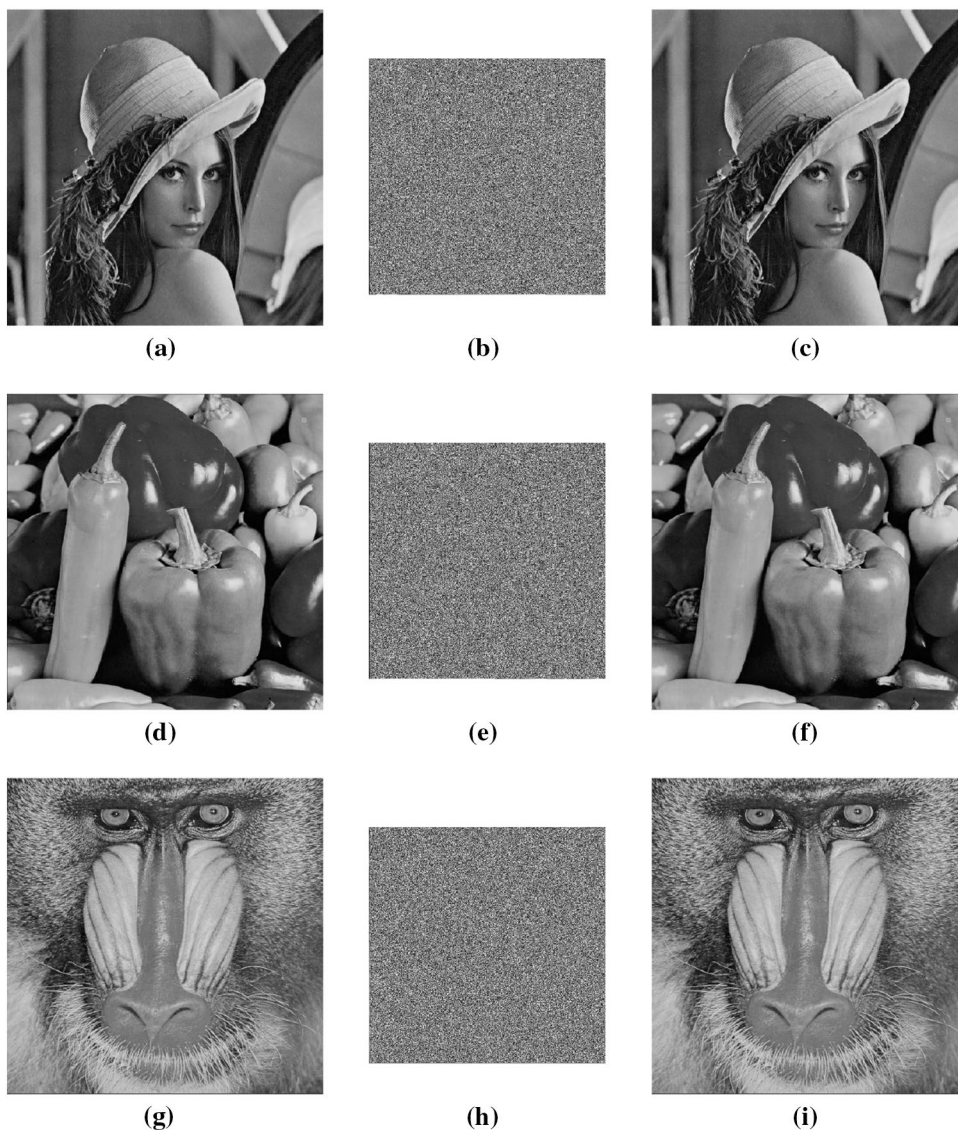
### 7 Experimental details

We evaluate both the security aspect and performance of proposed encryption scheme by experimenting in MATLAB (R2018b) on the standard image “Lena”, “Baboon”, “Peppers”, “Nike logo”, “Airplane”, and “Barbara” of size  $512 \times 512$ . The two secret keys ( $K_1$  and  $K_2$ ) used for generating the pseudo-random sequence  $R_1$  and  $R_2$  for confusion and diffusion layer, respectively. The initial parameters  $(x_0, y_0)$ , and the control parameters  $(\alpha, \beta)$  are considered as secret key  $K_1$ , where  $x_0, y_0, x'_0, y'_0 \in [0,1]$ , and  $\alpha, \beta, \alpha', \beta' \in [0,1]$ . The two secret keys in our experiment are  $K_1 = (x_0, y_0, \alpha, \beta)$  and  $K_2 = (x'_0, y'_0, \alpha', \beta')$ , where  $x_0 = 0.5217649304251095$ ,  $y_0 = 0.6392750215680951$ ,  $\alpha = 0.5672104389217190$ ,  $\beta = 0.8502175864356750$ , and

$$x'_0 = 0.7356439802176543, \quad y'_0 = 0.8530267952419067, \\ \alpha' = 0.5678093425186743, \quad \beta' = 0.9256810743901653.$$

The experiments are conducted on the system having windows 10 operating system, 4GB RAM, Intel i5 Generation 3. We evaluate our encryption scheme against resistance to statistical attack, resistance to differential attack, key space analysis to resist brute force attack, and key sensitivity analysis. The computational complexity of our proposed encryption scheme is less than existing image encryption scheme and encryption/decryption time is quite faster. The standard test images, encrypted images, and decrypted images of Lena, Peppers, and Baboon are shown in Fig. 7a–i, respectively. The cipher images are completely noisy one and unrecognizable. So, the attacker finds it difficult to discover any hidden information to recover either secret key or plain image.

**Fig. 7** **a** Plain image Lena; **b** encrypted image Lena; **c** decrypted image Lena; **d** plain image Peppers; **e** encrypted image Peppers; **f** decrypted image Peppers; **g** plain image Baboon; **h** encrypted image Baboon; **i** decrypted image Baboon



## 8 Security and performance analysis

This section presents the experimental results of six gray-scale images of key space analysis, key sensitivity analysis, statistical analysis, differential cryptanalysis and encryption quality of proposed image encryption scheme.

### 8.1 Key space analysis

To resist the brute force attack or exhaustive search, the total key search space should be huge. In this paper, the proposed 2D SC3 map-based image encryption scheme have four parameters  $(x_0, y_0, \alpha, \beta)$  to generate the secret key. In our experiment, the computational precision is allowed up to  $10^{-16}$ , so the total key space is  $10^{64} \approx 2^{213}$ . Table 4 provides the comparison results of the total search space of the secret

**Table 4** Comparison results of total key space of proposed and existing scheme

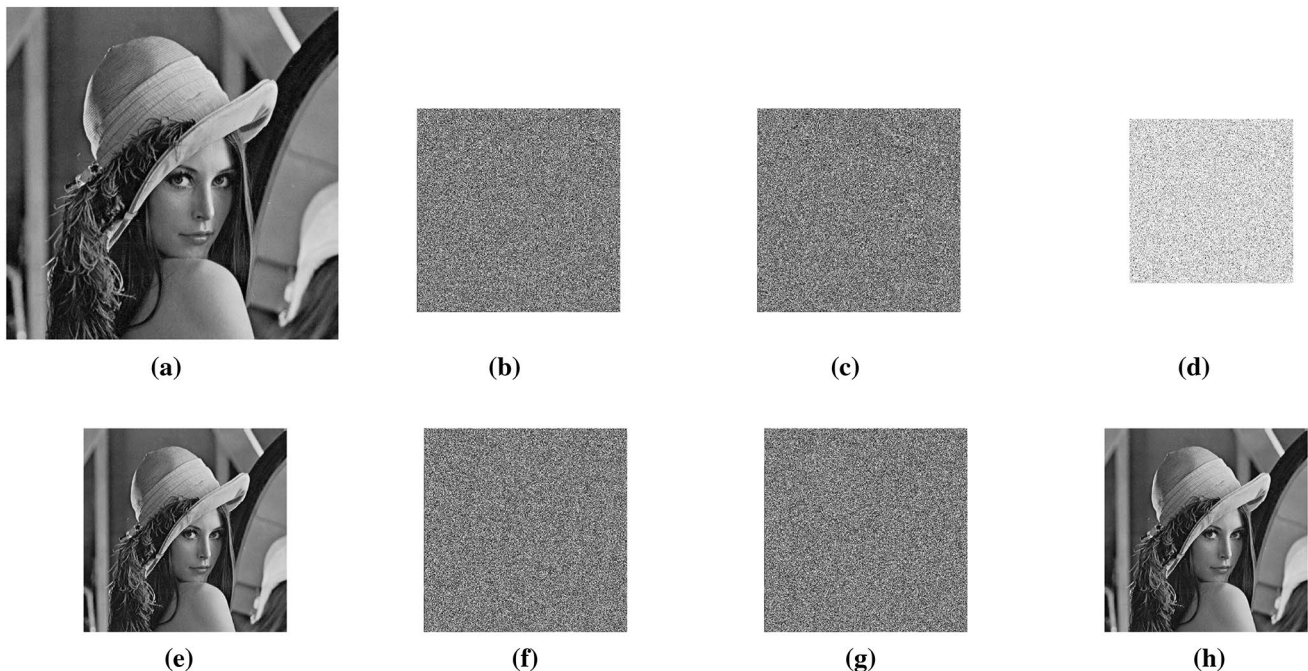
Algorithm	Key space
Proposed	$10^{64} \approx 2^{213}$
Ref. [40]	$10^{60} \approx 2^{199}$
Ref. [21]	$2^{256}$
Ref. [15]	$2^{232}$
Ref. [41]	$2^{100}$
Ref. [29]	$2^{624}$

key of our proposed encryption scheme and the existing encryption scheme. Our proposed image scheme has larger key space to resist the brute force attack.

### 8.2 Key sensitivity analysis

The key sensitivity analysis suggests minor changes in key bits would have a significant impact on the cipher image that means resulting in a complete different encrypted image. A good image encryption algorithm must be sensitive to the secret key and it can be possible when the chaotic map used in the encryption scheme is highly sensitive to initial conditions. We analyze our proposed encryption scheme to evaluate the sensitivity to the secret key by modifying only one parameter and keeping other parameters unchanged.

The secret key of our proposed cryptosystem has four parameters  $(x_0, y_0, \alpha, \beta)$ . Two different set of keys  $(K_1, K_2)$  are used for both confusion and diffusion, respectively. We modify the  $x_0$  value of  $K_1$ , i.e.,  $x_{\text{mod}} = x_0 + (10^{-k})$  where  $k \in [10, 16]$ . The secret key  $K_1$  and  $K'_1 = (x_{\text{mod}}, y_0, \alpha, \beta)$  is used to encrypt the Lena image in Fig. 8a. Figure 8b, c represent the cipher image obtained by  $K_1$  and  $K'_1$ , respectively. Figure 8d is the pixel-by-pixel difference between (b) and (c). To get the plain image, the receiver must decrypt with the correct key. Figure 8e, f represents the decrypted image of the Fig. 8b using correct ( $K_1$ ) and wrong key ( $K'_1$ ), respectively. Similarly, Fig. 8g, h is the decrypted image of



**Fig. 8** **a** Plain image Lena; **b** encrypted image of Lena using  $K_1$ ; **c** encrypted image of Lena using  $K'_1$ ; **d** the pixel-by-pixel difference between **b** and **c**; **e** decrypted image from **b** using  $K_1$ ; **f** decrypted

image from **b** using  $K'_1$ ; **g** decrypted image from **c** using  $K_1$ ; **h** decrypted image from **c** using  $K'_1$

Fig. 8c using wrong key ( $K_1$ ) and correct key ( $K'_1$ ), respectively. Figure 8f, g is completely unrecognizable since it uses the wrong keys. This proves that the slight changes in key bits would make a significant impact on the encryption and decryption mechanism. The experimental results shows that the proposed image cryptosystem is highly sensitive to the secret key.

### 8.3 Resistance to statistical attack

#### 8.3.1 Histogram analysis

Histogram represents the distribution of the pixel values [0, 255] of the image. The secure image cryptosystem should achieve uniform distribution of the pixel values of the encrypted image which makes the attacker very difficult to

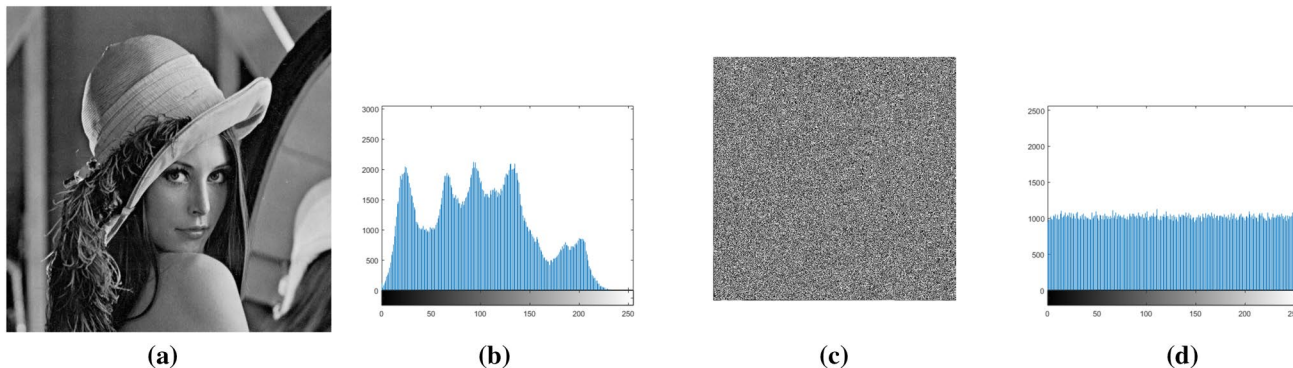


Fig. 9 a Plain image Lena; b histogram of plain image Lena; c Cipher image Lena; d histogram of cipher image Lena

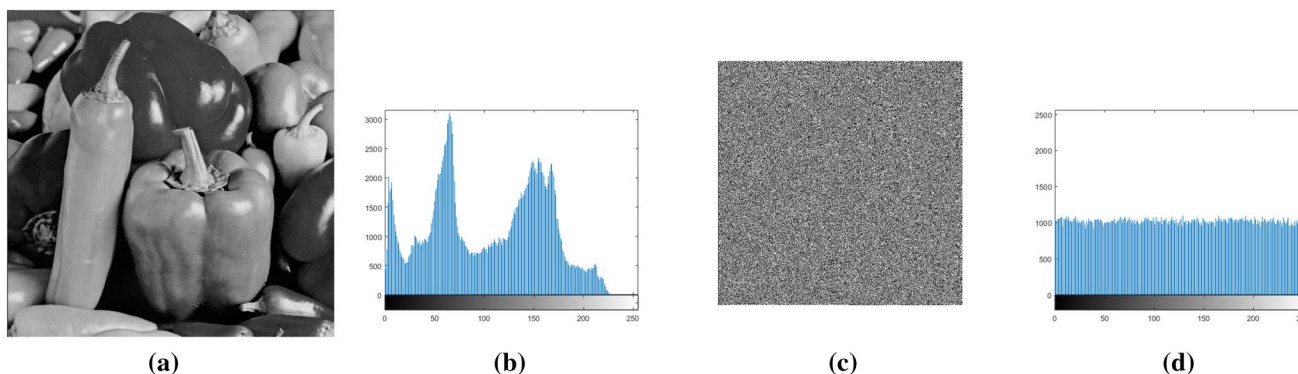


Fig. 10 a Plain image Peppers; b histogram of plain image Peppers; c Cipher image Peppers; d histogram of cipher image Peppers

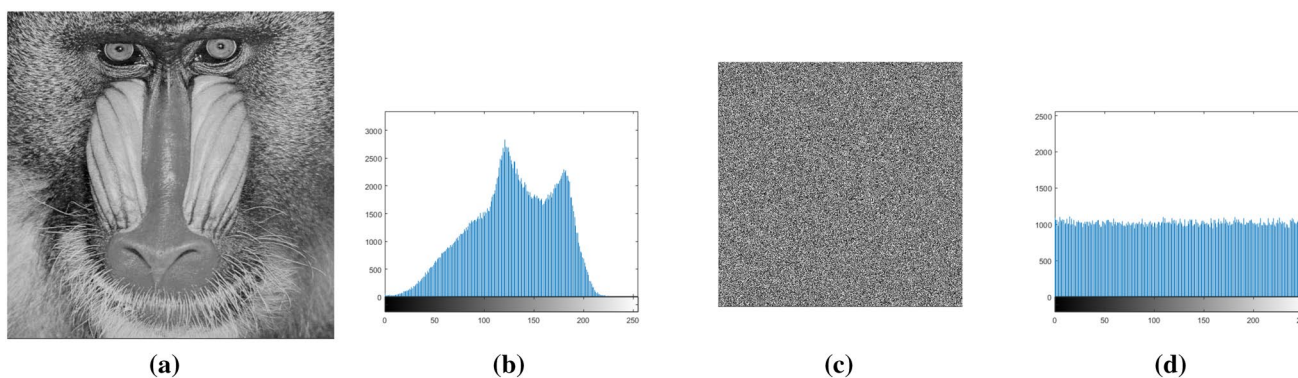
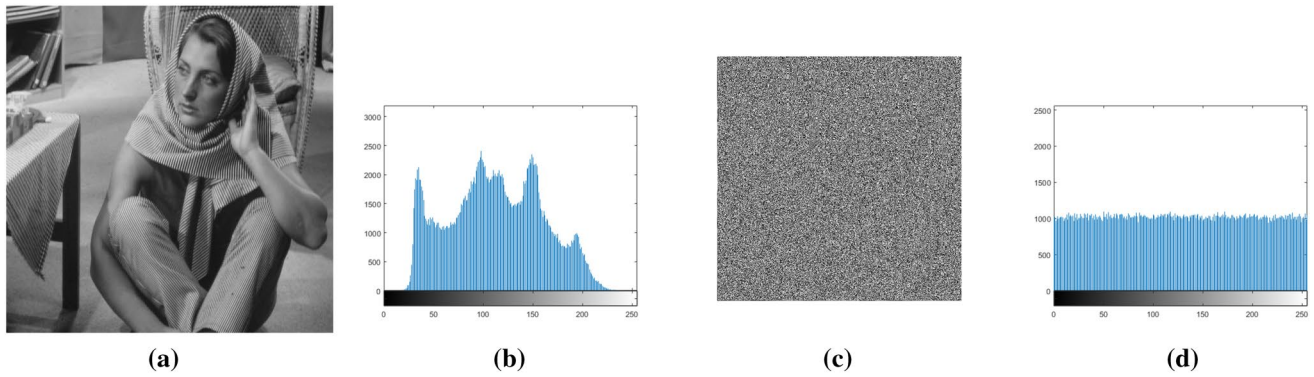
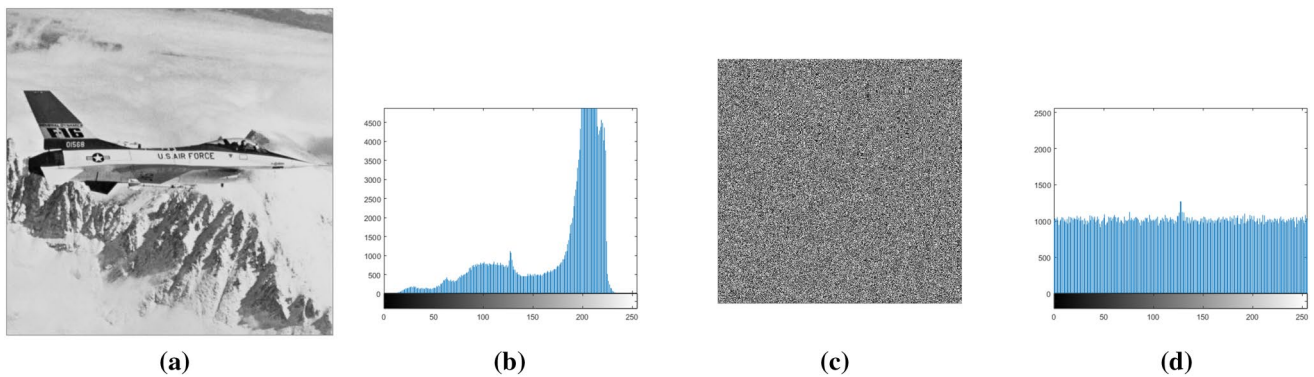


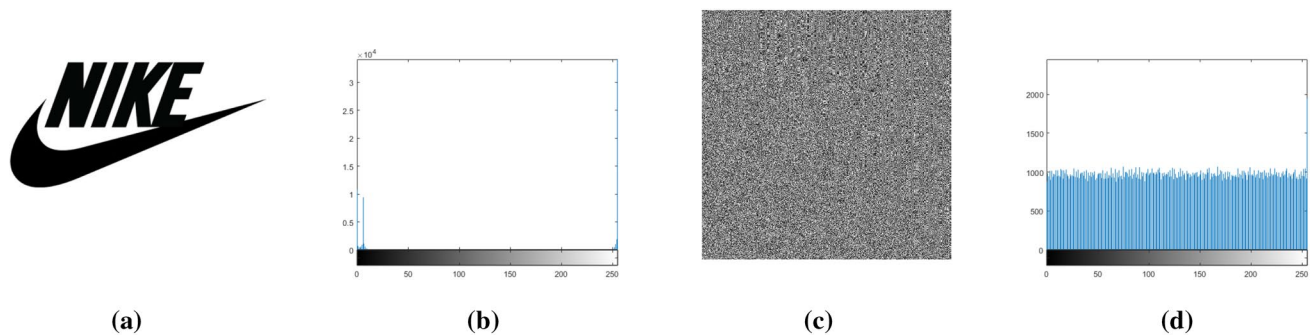
Fig. 11 a Plain image Baboon; b histogram of plain image Baboon; c Cipher image Baboon; d histogram of cipher image Baboon



**Fig. 12** **a** Plain image Barbara; **b** histogram of plain image Barbara; **c** Cipher image Barbara; **d** histogram of cipher image Barbara



**Fig. 13** **a** Plain image Airplane; **b** histogram of plain image Airplane; **c** Cipher image Airplane; **d** histogram of cipher image Airplane



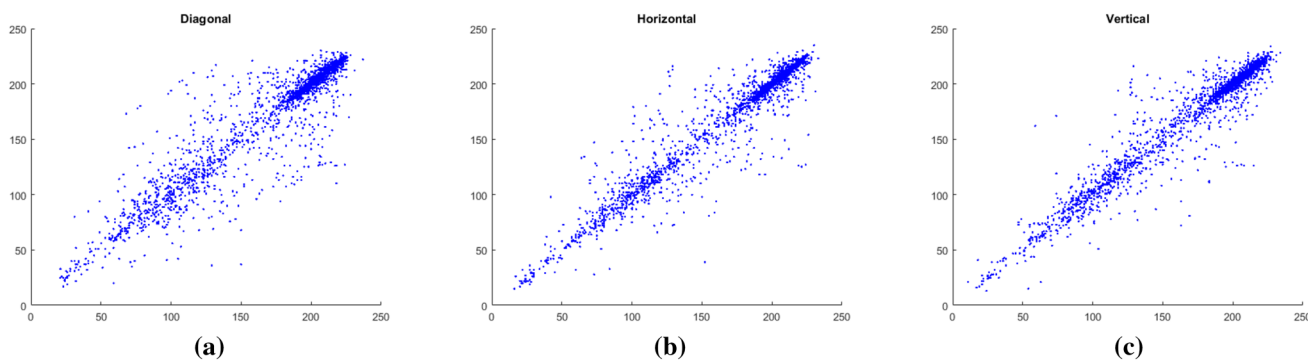
**Fig. 14** **a** Plain image Nike; **b** histogram of plain image Nike; **c** Cipher image Nike; **d** histogram of cipher image Nike

introduce the statistical attack. Basically, the distribution of pixel values is not uniform and clustered within a particular interval and the image encryption scheme having high diffusion capability encrypts the plain image by modifying the pixel values to achieve uniform distribution. If the cipher image is not uniform, then the attacker can perform statistical analysis to recover the plain image. Figures 9, 10, 11, 12, 13 and 14 shows the histogram of both plain image and cipher image of six grayscale images and the experimental

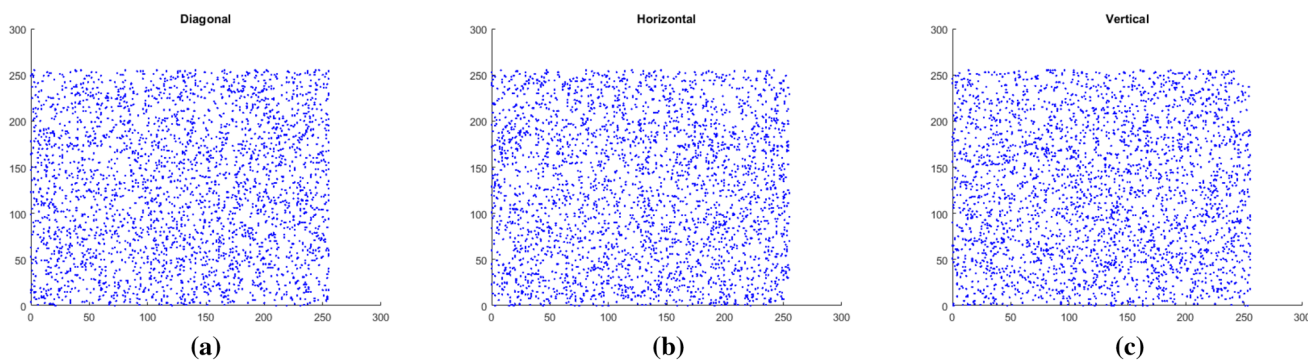
results shows that histogram of all cipher images has uniform distribution of the pixel values.

### 8.3.2 Correlation analysis of adjacent pixels

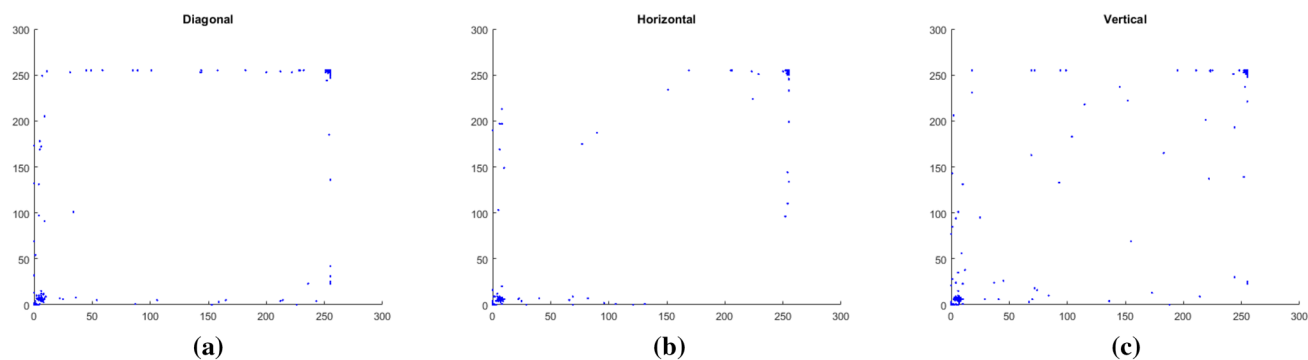
In digital image, the adjacent pixels in plain image are highly correlated which is vulnerable to the correlation coefficient attack. Thus, a secure image encryption algorithm should break this correlation to resist correlation coefficient attack.



**Fig. 15** **a** Diagonal correlation coefficient of plain Airplane image; **b** horizontal correlation coefficient of plain Airplane image; **c** vertical correlation coefficient of plain Airplane image



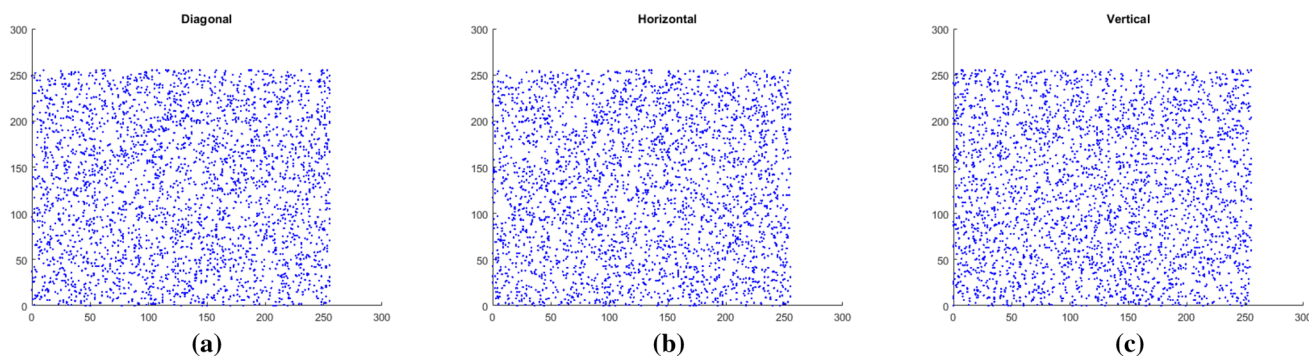
**Fig. 16** **a** Diagonal correlation coefficient of cipher Airplane image; **b** horizontal correlation coefficient of cipher Airplane image; **c** vertical correlation coefficient of cipher Airplane image



**Fig. 17** **a** Diagonal correlation coefficient of plain Nike image; **b** horizontal correlation coefficient of plain Nike image; **c** vertical correlation coefficient of plain Nike image

To evaluate the correlation coefficient of both plain image and cipher image, we choose 3000 random pairs of adjacent pixels in horizontal, vertical, and diagonal direction. Mathematically, the correlation coefficient is computed as defined in Eq. 6. Figures 15 and 16 denote the correlation coefficient of the Airplane image and Airplane cipher image, respectively. Figures 17 and 18 denote the correlation coefficient of NIKI plane image and cipher image, respectively. The cipher image is distributed in

a much larger region among the pixel values, whereas the correlation coefficient of plane image is clustered into a particular region. The experimental results of correlation coefficient are presented in Table 5. Further, a comparison of correlation coefficient of the proposed scheme with the existing scheme is presented in Table 6 using the Lena image. The comparison shows that the proposed scheme is performing comparatively better.



**Fig. 18** **a** Diagonal correlation coefficient of cipher Nike image; **b** horizontal correlation coefficient of cipher Nike image; **c** vertical correlation coefficient of cipher Nike image

**Table 5** Correlation coefficient of adjacent pixels of original and encrypted image

Image	Horizontal		Vertical		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Lena	0.9669	0.0008	0.9818	0.0004	0.9521	0.0020
Peppers	0.9822	0.0046	0.9856	0.0039	0.9697	− 0.0018
Baboon	0.9717	0.0047	0.8943	− 0.0001	0.9275	− 0.0011
Airplane	0.9669	0.0016	0.9666	− 0.0015	0.9395	− 0.0003
Nike	0.9833	0.0090	0.9836	0.0013	0.9596	− 0.0006
Barbara	0.9584	− 0.0001	0.9581	0.0022	0.9412	0.0010

**Table 6** Comparison of Lena image

Direction	Proposed	Ref. [36]	Ref. [29]	Ref. [15]	Ref. [41]
Horizontal	0.0008	− 0.0007	− 0.0048	0.0015	− 0.0008
Vertical	0.0004	− 0.0003	− 0.0112	0.0043	− 0.0025
Diagonal	0.0020	− 0.0007	− 0.0045	0.0023	0.0010

$$C_{xy} = \frac{\text{Cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{6}$$

where  $x$  and  $y$  are the gray values of two adjacent pixels.

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

$$D(y) = \frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2$$

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

$$E(y) = \frac{1}{N} \sum_{i=1}^N y_i$$

$$\text{Cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)).$$

### 8.3.3 Information entropy analysis

Information entropy suggest the average number of bits required to represent the entire message. In image encryption, information entropy is used to measure the uncertainty or randomness or the distribution of the gray scale values of the cipher image. The higher the information entropy, more the uniform distribution of the gray scale values which becomes more difficult for the attacker to mount the statistical attack. For any random source generating the message consisting of total  $2^N$  symbols, the entropy should be  $H(\text{msg}) = N$ . In any grayscale image, the pixel values occurs within  $[0, 255]$  and total 8 bit required to represent the entire image. If the information entropy of cipher image attains 8 bit or very close to it, then the cryptosystem is more secure against statistical attack. Mathematically, Shannon’s entropy is defined as in Eq. 7:

$$H(\text{msg}) = - \sum_{i=0}^{2^N-1} P(\text{msg}_i) \log_2 P(\text{msg}_i), \tag{7}$$

where  $\text{msg}_i$  denotes  $i$ th position grayscale value and  $P(\text{msg}_i)$  denotes the probability of value  $\text{msg}_i$  present in the cipher image. The cipher image whose entropy is more close to 8 and is considered more secure. We have computed the

**Table 7** Information entropy results

Image	Original image	Encrypted image
Lena	7.6112	7.9995
Peppers	7.1842	7.9889
Baboon	7.7319	7.9974
Airplane	6.7631	7.9989
Nike	1.0027	7.4856
Barbara	7.4681	7.9991

**Table 8** Comparison of information entropy

Image	Proposed	Ref. [36]	Ref. [29]	Ref. [15]	Ref. [41]
Lena	7.9995	7.9997	7.9963	–	–

information entropy of our plain images and cipher images and present the results in Table 7. From Table 7, we observed that the entropy of all cipher image is close to 8 which makes statistical attack more difficult. The comparison results are shown in Table 8.

### 8.4 Resistance to differential attack

The differential cryptanalysis is a chosen plaintext attack. That means, the attacker chooses a plain image ( $P_1$ ) and modifies one pixel to get a different image ( $P_2$ ). Both the images  $P_1$  and  $P_2$  are encrypted using the same secret key to get the cipher image  $C_1$  and  $C_2$ . The attacker tries to find the output differences by observing both the pairs to discover the relationship between plain image and cipher image, which leads to recovery of the key bits. The image cryptosystem having good diffusion capability is highly sensitive to changes in pixel values, i.e., one pixel change in the plain image influences the cipher image completely which becomes more difficult for the attacker to find the relationship between plain image and cipher image. The quantitative measurement to evaluate the diffusion capability of the image cryptosystem resistance to differential attack is number of pixel change rate (NPCR) and unified average changing intensity (UACI). Mathematically,

$$NPCR = \frac{\sum_{i,j} D(i, j)}{WH} \times 100\%, \tag{8}$$

where  $W$  and  $H$  is width and height of the plain image and  $D(i, j)$  denotes whether the pixel values of both the encrypted image  $C_1$  and  $C_2$  are same or not.

$$D(i, j) = \begin{cases} 1 & \text{if } C_1(i, j) \neq C_2(i, j) \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

**Table 9** Results of average NPCR and UACI values of different plain images

Plain image	NPCR (%)	UACI (%)
Lena	99.2157	33.5904
Peppers	99.2130	32.6708
Baboon	99.2252	32.8760
Airplane	99.6128	32.5345
Nike	99.2272	33.5607
Barbara	99.2245	31.6783

**Table 10** Comparison of NPCR and UACI results of Lena image

Algorithm	NPCR (%)	UACI (%)
Proposed	99.21	33.59
Ref. [36]	99.6193	33.4286
Ref. [29]	99.6228	37.7041
Ref. [15]	99.60	33.46
Ref. [41]	99.60	33.50

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%. \tag{10}$$

In our experiment, 200 random pixels are selected from the plain image and changed the pixel values to generate the new image. Then we encrypt both the images using the same secret key to generate the cipher image  $C_1$  and  $C_2$ . We compute the minimum, maximum and average values of NPCR and UACI and the result is shown in Table 9. The average value of NPCR and UACI is very close to  $NPCR_{\text{expected}}$  (99.61%) and  $UACI_{\text{expected}}$  (33.46 %). The comparison of NPCR and UACI results is shown in Table 10.

### 8.5 Encryption quality

The proposed image encryption scheme achieves lossless encryption when the plain image and decrypted image are completely identical. Both images will be identical when the mean square error (MSE) will be zero. Mean square error is used to evaluate the peak signal-to-noise ratio (PSNR), a quantitative measurement to find the similarity between the plain image and decrypted image. When the  $PSNR \geq 30$  db, the image is not able to differentiate. Mathematically, PSNR is defined as Eq. 11, while MSE is defined as Eq. 12:

$$PSNR = 20 \log_{10} \left( \frac{255}{\sqrt{MSE}} \right) \tag{11}$$

$$MSE = \frac{\sum_{i=1}^W \sum_{j=1}^H (P'(i,j) - P(i,j))^2}{WH}, \tag{12}$$

where  $W$  and  $H$  denote the width and height of the plain image, respectively, and  $P$  and  $P'$  represent the plain image and decrypted image, respectively. The lesser the values of MSE, the higher the value of PSNR, and more similarity between the plain image and decrypted image. The proposed image encryption scheme achieves lossless encryption.

### 8.5.1 Irregular deviation

The irregular deviation is a quantitative measure of the statistical distribution of the deviation between plain image and cipher images to the uniform distribution. Mathematically, irregular deviation [29] can be defined as:

$$I_D = \sum_{i=0}^{N-1} H_{D_i}, \tag{13}$$

where  $H_{D_i} = |h_i - A_H|$ ,  $h_i$  is the amplitude of histogram at index  $i$  and  $A_H$  is the average sum of histogram values of deviation matrix i.e.,  $\frac{1}{256} \sum_{i=0}^{N-1} h_i$ . The amplitude of histogram at index  $i$  is the absolute difference between plain image and cipher image pixel values. The lower value of the irregular deviation denoting the encryption quality becomes high. Table 11 presents the obtained results of our proposed cryptosystem and our results are in acceptable range.

### 8.6 Speed and computational complexity

Apart from security analysis of the image encryption scheme, performance analysis is also an important aspect to evaluate the encryption/decryption time and time complexity of the algorithm. To evaluate the encryption speed of our proposed algorithm, the experiment is carried out in the system having configuration of windows 10 operating system, 4GB RAM, Intel i5 Generation 3 in MATLAB (R2018b). The encryption time taken by our proposed algorithm is shown in Table 12 of our standard image data set.

**Table 11** Irregular deviation of the proposed image cryptosystem

Plain image	Irregular deviation	Uniform deviation
Lena	319850	262144
Peppers	309204	262144
Baboon	258548	262144
Airplane	158040	262144
Nike	552677	250000
Barbara	293348	262144

**Table 12** Encryption time/decryption time (in s) of the proposed algorithm

Plain image	Encryption/decryption time (s)
Lena	0.139008
Peppers	0.139435
Baboon	0.139999
Airplane	0.137665
Nike	0.196549
Barbara	0.140332

Since the encryption and decryption time of the image cryptosystem vary according to the type of environment (hardware/software) and the system configuration, so it is not the right way to compare with the existing algorithm. So we analyze our proposed image cryptosystem based on the time complexity related to all the steps involved in encryption/decryption process. There are different steps involved generating the pseudo-random sequence, confusion phase, and diffusion phase. Since our chaotic map is 2D map, so it generates two pseudo-random sequences and the time complexity becomes  $\Theta(2 \times W \times H)$ . In confusion phase, computational cost includes shuffling of the pixels  $W \times H$  times using the sequence  $R_1$ , so the time complexity becomes  $\Theta(W \times H)$ . In diffusion phase, it involves the bitwise Xor operation with pixel values. Since each pixel value is represented in 8 bits, the time complexity becomes  $\Theta(8 \times W \times H)$ . The comparison result of computational complexity is shown in Table 13.

## 9 Conclusion

In this paper, a novel 2D sine–cosine cross-chaotic map is proposed. In proposed chaotic map, two pseudo-random sequences  $R_1$ , and  $R_2$  are generated for confusion and diffusion process, respectively. The proposed scheme has a wide range of chaotic behavior, uniformity, much larger attractor distribution in 2D phase plane, and higher Lyapunov exponent value. So, the proposed chaotic map is more suitable for image encryption. We apply our proposed chaotic map

**Table 13** Encryption time/decryption time (in s) of the proposed algorithm

Algorithm	Computational complexity
Proposed	$\mathcal{O}(8 \times W \times H)$
Ref. [36]	$\mathcal{O}(24 \times W \times H)$
Ref. [23]	$\mathcal{O}(24 \times W \times H)$
Ref. [29]	$\mathcal{O}(W \times H)$



in image encryption using permutation–bit diffusion structure to measure the confusion and diffusion capability. The security analysis of the encryption scheme shows that the algorithm is secure enough to resist statistical attack, differential attack, and key sensitivity analysis. The proposed chaotic map has a large key space of  $2^{213}$ , i.e., large search space to resist brute force attack.

**Acknowledgements** The authors thank the editor and all anonymous reviewers for their comments and suggestions which improved both the technical and editorial quality of the paper.

## Compliance with ethical standards

**Conflict of interest** The authors declared that they have no conflicts of interest to this work.

## References

- Daemen, J., Rijmen, V.: The Design of Rijndael: AES-the Advanced Encryption Standard. Springer Science & Business Media, New York (2013)
- Coppersmith, D.: The data encryption standard (des) and its strength against attacks. *IBM J. Res. Dev.* **38**(3), 243–250 (1994)
- Hell, M., Johansson, T., Meier, W.: Grain: a stream cipher for constrained environments. *IJWMC* **2**(1), 86–93 (2007)
- Kocarev, L.: Chaos-based cryptography: a brief overview. *IEEE Circuits Syst. Mag.* **1**(3), 6–21 (2001)
- Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **16**(08), 2129–2151 (2006)
- Liu, H., Kadir, A., Niu, Y.: Chaos-based color image block encryption scheme using s-box. *AEU Int. J. Electron. Commun.* **68**(7), 676–686 (2014)
- Wang, M., Wang, X., Zhang, Y., Zhou, S., Zhao, T., Yao, N.: A novel chaotic system and its application in a color image cryptosystem. *Opt. Lasers Eng.* **121**, 479–494 (2019)
- Shannon, C.E.: Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**(4), 656–715 (1949)
- Zhou, Y., Bao, L., Chen, C.P.: A new 1d chaotic system for image encryption. *Signal Process.* **97**, 172–182 (2014)
- Hussain, I., Shah, T., Gondal, M.A.: Application of s-box and chaotic map for image encryption. *Math. Comput. Model.* **57**(9–10), 2576–2579 (2013)
- Ye, G.: Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognit. Lett.* **31**(5), 347–354 (2010)
- Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos Solitons Fractals* **21**(3), 749–761 (2004)
- Diab, H.: An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. *IEEE Access* **6**, 42227–42244 (2018)
- Diab, H., El-semari, A.M.: Secure image cryptosystem with unique key streams via hyper-chaotic system. *Signal Process.* **142**, 53–68 (2018)
- Hua, Z., Zhou, Y.: Image encryption using 2D logistic-adjusted-sine map. *Inf. Sci.* **339**, 237–253 (2016)
- Marton, K., Suci, A.: On the interpretation of results from the NIST statistical test suite. *Sci. Technol.* **18**(1), 18–32 (2015)
- Li, S., Zheng, X.: Cryptanalysis of a chaotic image encryption method. In: 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat.No. 02CH37353), vol. 2, pp. II–II. IEEE (2002)
- Rosenstein, M.T., Collins, J.J., De Luca, C.J.: A practical method for calculating largest Lyapunov exponents from small data sets. *Phys. D Nonlinear Phenomena* **65**(1–2), 117–134 (1993)
- Mondal, B., Kumar, P., Singh, S.: A chaotic permutation and diffusion based image encryption algorithm for secure communications. *Multimed. Tools Appl.* **77**(23), 31177–31198 (2018)
- Mondal, B., Mandal, T.: A novel chaos based secure image encryption algorithm. *Int. J. Appl. Eng. Res.* **11**(5), 3120–3127 (2016)
- Mondal, B., Singh, S., Kumar, P.: A secure image encryption scheme based on cellular automata and chaotic skew tent map. *J. Inf. Secur. Appl.* **45**, 117–130 (2019)
- Ping, P., Wu, J., Mao, Y., Xu, F., Fan, J.: Design of image cipher using life-like cellular automata and chaotic map. *Signal Process.* **150**, 233–247 (2018)
- Wu, X., Kan, H., Kurths, J.: A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps. *Appl. Soft Comput.* **37**, 24–39 (2015)
- Bhaskar Mondal, T.M.: A light weight secure image encryption scheme based on chaos & dna computing. *J. King Saud Univ. Comput. Inf. Sci.* **26**, 499–504 (2016)
- Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. *Signal Process.* **92**(4), 1101–1108 (2012)
- Çavuşoğlu, U., Kaçar, S., Pehlivan, I., Zengin, A.: Secure image encryption algorithm design using a novel chaos based s-box. *Chaos Solitons Fractals* **95**, 92–101 (2017)
- Silva-Garcia, V., Flores-Carapia, R., Renteria-Marquez, C., Luna-Benoso, B., Aldape-Perez, M.: Substitution box generation using chaos: an image encryption application. *Appl. Math. Comput.* **332**, 123–135 (2018)
- Zhu, Z., Zhang, W., Wong, K.W., Yu, H.: A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **181**(6), 1171–1186 (2011)
- Belazi, A., El-Latif, A.A.A., Belghith, S.: A novel image encryption scheme based on substitution–permutation network and chaos. *Signal Process.* **128**, 155–170 (2016)
- Cao, C., Sun, K., Liu, W.: A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. *Signal Process.* **143**, 122–133 (2018)
- Fu, C., Huang, J.B., Wang, N.N., Hou, Q.B., Lei, W.M.: A symmetric chaos based image cipher with an improved bit-level permutation strategy. *Entropy* **16**(2), 770–788 (2014)
- Ping, P., Xu, F., Mao, Y., Wang, Z.: Designing permutation-substitution image encryption networks with henon map. *Neurocomputing* **283**, 53–63 (2018)
- Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B.C.: Image encryption using sequence generated by cyclic group. *J. Inf. Secur. Appl.* **44**, 117–129 (2019)
- Zhang, X., Feng, G., Ren, Y., Qian, Z.: Scalable coding of encrypted images. *IEEE Trans. Image Process.* **21**(6), 3108–14 (2012)
- Qin, C., Zhou, Q., Cao, F., Dong, J., Zhang, X.: Flexible lossy compression for selective encrypted image with image inpainting. In: IEEE Transactions on Circuits and Systems for Video Technology (2018)
- Panwar, K., Purwar, R.K., Jain, A.: Cryptanalysis and improvement of a color image encryption scheme based on DNA sequences and multiple 1D chaotic maps. *Int. J. Bifurc. Chaos* **29**(08), 1950103 (2019)
- Panwar, K., Purwar, R.K., Jain, A.: Cryptanalysis and improvement of an image encryption scheme using combination of one-dimensional chaotic maps. *J. Electron. Imaging* **27**(5), 053037 (2018)

38. Al-Shameri, W.F.: Dynamical properties of the Hénon mapping. *Int. J. Math. Anal.* **6**(49), 2419–30 (2012)
39. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E.: *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Booz-Allen and Hamilton Inc, Mclean (2001)
40. Chen, J., Zhu, Z.L., Zhang, L.B., Zhang, Y., Yang, B.Q.: Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. *Signal Process.* **1**(142), 340–53 (2018)
41. Ping, P., Fan, J., Mao, Y., Xu, F., Gao, J.: A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access* **6**, 67581–67593 (2018)

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Bhaskar Mondal** received his M.Tech degree in Computer Science and Engineering from Kalyani Government Engineering college west Bengal in 2010. He completed his Ph.D. from the National Institute of

Technology Jamshedpur in 2018. Currently he is an Assistant professor in Xavier University. His research interest includes chaotic map, image processing, and designing lightweight image cryptosystem.

**Pratap Kumar Behera** received his M.Tech degree in Information Security from the National Institute of Technology Rourkela, India in 2015. He is currently doing Ph.D. in Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee, India. His research area includes cryptology, information security, and secure image encryption.

**Sugata Gangopadhyay** received his Master of Science in Mathematics degree in the year 1993 from the Indian Institute of Technology Kharagpur. He completed Ph.D. from the Indian Institute of Technology Kharagpur in 1998. Currently, he is a Professor at Indian Institute of Technology Roorkee. His research interests are in symmetric cryptology.