Neural Computing and Applications (2023) 35:13207–13223
https://doi.org/10.1007/s00521-023-08434-y

ORIGINAL ARTICLE

Parameter optimization of chaotic system using Pareto-based triple objective artificial bee colony algorithm

Abdurrahim Toktas[1] · Uğur Erkan[2] · Deniz Ustun[3] · Xingyuan Wang[4]

Received: 24 August 2022 / Accepted: 20 February 2023 / Published online: 10 March 2023

Abstract

Chaotic map is a kind of discrete chaotic system. The existing chaotic maps suffer from optimal parameters in terms of chaos measurements. In this study, a novel approach of optimization of parametric chaotic map (PCM) using triple objective optimization is presented for the first time. A PCM with six parameters is first conceived and then optimized using Pareto-based triple objective artificial bee colony (PT-ABC) algorithm. Pareto optimality is employed to catch the trade-off among the objectives: Lyapunov exponent (LE), sample entropy (SE), and Kolmogorov entropy (KE). A global optimal design including the six parameters is selected for minimizing the reciprocal of the three objectives independently. The chaotic performance of PCM is verified through an evaluation with bifurcation diagram, attractor, LE, SE, KE, and correlation dimension. The results are also validated by comparison with those of which reported elsewhere. Furthermore, the applicability of PCM is examined over image encryption and the results are compared with existing chaos-based IEs. Therefore, the PCM manifests the best ergodicity and complexity thanks to its PT-ABC algorithm.

Keywords Chaotic system · Multi-objective optimization · Pareto optimization · Image encryption

1 Introduction

Nonlinear dynamical systems might look chaotic, unexpected, or paradoxical because they reflect changes in variables across time. For such dynamical systems, small changes in beginning circumstances might result in very different outcomes, making long-term prediction problematic in general. Chaotic systems are mathematical frameworks for characterizing chaotic behaviors in natural or unnatural phenomena. Chaotic map is a term used to describe a discrete chaotic system. Chaotic maps are deterministic iterated functions with discrete time as a parameter. Chaotic maps which are recursive functions show chaotic characteristics, such as ergodicity, complexity, and unpredictability [1]. They generate chaotic series that are sensitive to beginning circumstances and control factors. Even though chaotic maps are predictable, predicting long-term behavior is impossible. Secure communication [2], watermarking [3], data compression [4], data hiding [5], and multimedia encryption [6] are among areas where chaotic maps are useful. The performance of the chaos-depended applications is heavily related to the chaotic characteristics of the chaotic systems. The chaotic systems have to show excellent and continuous chaotic traits like ergodicity, erraticity, variety, complexity, aperiodicity, and susceptible to control factors and beginning circumstances for preventing the chaotic sequence from being anticipated [7, 8]. With the densely occurrence of security problems in cyber-physical systems, the research of protection methods against cyber-physical attacks has grown in importance [9, 10]. The defense mechanism detects data integrity threats sensitively, such as fake data injection attacks, denial-of-service attacks, and replay

✉ Uğur Erkan
ugurerkan@kmu.edu.tr

[1] Department of Artificial Intelligence and Data Engineering, Engineering Faculty, Ankara University, 06830 Gölbaşı, Ankara, Turkey

[2] Department of Computer Engineering, Faculty of Engineering, Karamanoglu Mehmetbey University, 70200 Karaman, Turkey

[3] Department of Computer Engineering, Engineering Faculty, Tarsus University, 33400 Tarsus, Mersin, Turkey

[4] School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang 330013, China

attacks, and provides safe transmission against eavesdropping attacks.

Traditional chaotic systems are generally based on logistic, sine, tent, Gauss, Lorentz, and Henon maps [11, 12]. Many studies have proven that various classical chaotic systems have performance problems in practical applications due to significant increases in computer capability and the advent of technology for identifying chaos. First, a wide range of technologies, notably artificial intelligence approaches, might be utilized to estimate the chaotic attitude of various chaotic systems [13, 14]. Second, the chaos in these systems is fragile. Frail chaos refers to chaotic dynamics that are insufficiently robust, meaning that small changes in system characteristics can cause chaos to vanish. Finally, due to the problem of dynamical deterioration, many classical chaotic systems have major security weaknesses. This is due to their simplistic structures and actions. As a result, bifurcation diagram, attractor, Lyapunov exponent (LE), sample entropy (SE), Kolmogorov entropy (KE), and correlation dimension (CD) should be used to evaluate a system's dynamic performance for assuring a chaotic system.

Several chaotic systems have been developed for various chaos-depended applications [15–17]. Chaotic systems were created employing seed maps from previously created chaotic systems in general, [7]. Combining [18], coupling [19], switching [20], cascading [21], or hybridizing [22] the existing chaotic systems resulted in system models. The most recent six existing 1D chaotic systems developed for image encryption (IE) are clarified in Table 1 [23–28]. In [23], a 1D logistic self-embedding (1DLSE) depending on logistic and sine map was designed. A 1D chaotic system was built using the fraction of cosine over sine (1-DFCS) in [24]. In [25], for IE, a chaotic system based on cosine-logarithmic function that exploits existing 1D chaotic maps having weak chaotic attitude to build new 1D hyperchaotic maps was proposed. A fractional 1D chaotic map was developed in [26]. A 1-D modular chaotic system based on the cubic map and the exponential function (1-DCE) is devised in [27]. A chaotic system combining logistic and sine map is invented in [28]. In our study, their chaotic performance was also compared to one another using a variety of chaos measurements. New chaotic systems have only been considered infrequently as potentially promising chaotic systems with improved performance [26, 27, 29, 30]. They have more complicated dynamics as compared to classical chaotic systems. However, because to a lack of parameter optimization, its chaotic efficiency may stay limited according to chaos measurements. Their parameters are determined empirically. Hence, their performance on real-time applications may be limited, as well. Consequently, a new chaotic system with optimal parameters may have the best chance of success with regard to the chaos measurements.

In the last few decades, metaheuristic optimization algorithms inspired by natural phenomena have produced astounding breakthroughs in optimal engineering designs [31]. They derive their accomplishments from nature's perfection. The strategies are based on controlled stochastic calculations that aim to iteratively improve candidate solutions. From them, artificial bee colony (ABC) algorithm was developed utilizing a honey bee's nectar seeking behavior as a model [32]. The ABC algorithm and its modifications have been used to solve a range of technical challenges [33–36]. In general, additional strategies, such as Pareto optimality, are incorporated to adapt the multi-objective capabilities [34–36]. Because of using Pareto strategy, it is able to refine optimum solutions in accordance with all objective functions and so identify a global optimum solution by considering the trade-offs among the objective functions. Pareto-based optimization can be implemented to parameter optimization of a chaotic system for determining optimum parameters.

Table 1 Existing chaotic systems

Ref#	Chaotic generator	Control parameter range
$[23]^{2021}$	$x_{i+1} = \alpha((1-\sin(\pi x_i)) + \lambda)(4\alpha x_i(1-x_i))(1-4\alpha x_i(1-x_i) \bmod 1$	$\sigma \in [5, +\infty)\, \lambda \in [0, +\infty)$
$[24]^{2021}$	$x_{i+1} = \frac{\cos((ax_i+1)^2+1)}{\sin((ax_i+1)^2+1)+2}$	$a \in [0, +\infty)$
$[25]^{2021}$	$x_{i+1} = \frac{\lvert\cos(2\alpha\beta\pi x_i(1-x_i))\rvert}{\log(3-4\beta x_i(1-x_i))}$	$\alpha \in [0, +\infty)\, \beta \in [0, 1]$
$[26]^{2021}$	$x_{i+1} = \begin{cases} \dfrac{1}{x_i^2+\alpha} - \beta x_i & \text{if } x_i \in \left[0, \dfrac{1}{\alpha}\right] \\ \dfrac{-1}{x_i^2+\alpha} - \beta x_i & \text{if } x_i \in [\dfrac{-1}{\alpha}, 0) \end{cases}$	$\alpha \in (0, 1]\, \beta \in (-0.5, 1+\alpha/2]$
$[27]^{2022}$	$x_{i+1} = re^{x_i^3} + (1-r)e^{x_i} \bmod 1$	$r \in [0, 1]$
$[28]^{2022}$	$x_{i+1} = (rx_i(1-x_i) + r\sin(\pi x_i)) \times 2^{12} \bmod 1$	$r \in (0, 4]$

Various parametric chaotic systems have been designed in the literature [37–43]. In [37–39], parameters of chaotic systems were empirically determined. In [40–43], the parameters of chaotic systems were optimized with the help of metaheuristic optimization algorithms such as ABC [42, 43], sparrow search [40] and differential evolution [41] algorithms. However, the parametric chaotic systems were attempted to optimize using weighting objective functions. The weights of objectives are adjusted for balancing the weighting factors. In this situation, one or more objective vectors can be more dominant than the others, i.e., while the dominant objective values improve, the others get worse. Therefore, they might not allow to find a precise global solution. Pareto optimality can balance the contributions of the objective functions and design trade-off chaotic system among the objective vectors.

In this study, a novel approach based on Pareto-based triple objective ABC (PT-ABC) algorithm is proposed for parameter optimization of chaotic systems for the first time. A new parametric chaotic map (PCM) is hereby designed, and then the parameters of the chaotic system are optimally determined through PT-ABC for improving the objectives of LE, SE and KE. A global optimal PCM which ensures the trade-off among the objectives is selected within the Pareto optimal set. After conceiving the chaotic system, the performance of the proposed PCM is evaluated and validated by a comparison through the chaos measurements with the recently reported chaotic systems in Table 1. The results demonstrate the PCM has the best chaotic performance with regard to LE, SE, KE, and CD. Lastly the applicability of PCM is tested on PCM-based IE (PCMbIE).

2 Pareto-based triple objective artificial bee colony

ABC was motivated to solve single-objective optimization problems by the collective foraging activities of wild honey bees. The Pareto optimality approach is an effective way to tailor a multi-objective procedure to ABC. According to Pareto strategy, the global solutions are the best fits for each objective among all accessible solutions in terms of all objectives.

2.1 Artificial bee colony

ABC algorithm was thrived by replicating the organizing and cooperative rummaging behavior of honey bee communities. It can be referred to [35] for the pseudocode of ABC. Employed bees, onlooker bees, and scout bees forage as three colonies. The stages of ABC are likewise known by the same colony name. Artificial bees in colonies look for high-quality nectar sources. ABC goes through these steps iteratively. The employed and onlooker bees are regarded two equal colonies in a colony with a number of bees equal to the number of population (NP). Each bee searches for a nectar supply, and place of each represents a potential solution. The suitability of candidate solutions corresponds to the attributes of nectar sources. At both the employed and onlooker bee processes, the number of NP/2 plausible solutions is explored independently. All employed bees begin their careers as scout bees, charged for discovering new food sources. They then look for nectar sources and educate the onlooker bees on the nectar sources' characteristics. Based on this knowledge, the onlooker bees return to region of the food resources indicated by the employed bees. The nectar source is abandoned and an entirely new nectar source is produced in its stead if a nectar source with higher-quality could not be found within a given number of attempts "limit".

2.2 Pareto optimality

Multi-objective optimizations are common in engineering design challenges. Objective functions are connected to each other because they are reliant on decision vectors (design variables). In other words, while modifying the decision vector may enhance one goal, it may degrade others. As a result, while determining optimal solutions for all objectives, the outcomes of all objective functions must be considered. Given that each objective function has a result for each decision vector. Dependent on one objective value, a decision vector may overrule the other vectors, but it may not be based on the other objective function values. As a consequence, a collection of decision vectors that dominate all other objective function should be explored over the whole goal space. The most successful strategy used in metaheuristic algorithms is Pareto optimality, whose pseudocode is shown in [35]. It enables the independent discovery of a diverse and uniform optimum solution set (non-dominated solutions), referred to as the Pareto front.

3 The objective functions for the optimization using PT-ABC

We need effective objective functions for assessing the chaotic performance of PCM throughout the optimization process.

3.1 Lyapunov exponent

Measuring whether a dynamic system is chaotic is an important issue. In this point, the LE is an effective tool for handle this issue. The LE of a dynamical system describes the ratio of separation of infinitesimal close orbits. A chaotic system is considered if LE is positive. Besides, as the LE increases, it means fast the phase plane paths diverge from one another. The LE for 1D chaotic system may be calculated as follows [44]:

$$\mathrm{LE} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln\left|f'(x_i)\right| \tag{1}$$

where n is the maximum iteration number. $f'(x_i)$ is the first derivation of the chaotic map x_{i+1} with respect to x_i.

3.2 Sample entropy

SE is a statistical measurement used to assess the self-similarity of time series in a dynamic system [45]. It measures the self-similarity produced by the dynamic system. The produced series is quite complicated, which explains why SE is so high. Let $X = \{x_1, x_2, \cdots, x_n\}$ be the pattern having size n and $x_m(i) = \{x_i, x_{i+1}, \ldots, x_{i+m+1}\}$ be the template vector of dimension. As a result, SE may be calculated as:

$$\mathrm{SE}(m, r, n) = -\log\frac{A}{B} \tag{2}$$

where $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$ are the Chebyshev distances between $X_m(i)$ and $X_m(j)$, respectively. r is the maximum tolerance, A and B are the number of vectors. In accordance with [45], m should be 2 or 3, and r can be set to be in the range of 0.1–0.25 times the time-series' standard deviation (std). However, they are generally adjusted as $m = 2$ and $r = 0.2 \times \mathrm{std}(X)$. Accordingly, we set the same in our study. While the SE is increased, the regularity decreases, and in this way, randomness of the dynamic system is also raised.

3.3 Kolmogorov entropy

The KE is an impactful chaos measurement, indicating the data needed to evaluate the next trajectory of a dynamic system given its current state [46, 47]. ε^D's phase space is divided into D-dimensional hypercubes. Accordingly, the Kolmogorov entropy defined as

$$K = \lim_{T\to\infty} \lim_{\epsilon\to 0^+} \lim_{N\to\infty} \frac{1}{NT} \sum_{n=0}^{N-1} (K_{n+1} - K_n) \tag{3}$$

where

$$K_n = -\sum_{i_0,\ldots,i_n} P_{i_0,\ldots,i_n} ln P_{i_0,\ldots,i_n}$$

The hypercubes are i_0 at $t = 0$, i_1 at $t = T$ and i_n at $t = nT$ in which $P_{i_0,\ldots,i_n}$ is the likelihood. Given the trajectories up to nT, $K_{n+1} - K_n$ is the data required to determine which hypercube the trajectory will be in at $(n+1)T$. If KE is zero, the nonlinear system is considered as regular to the action. When the KE is positive, the nonlinear system requires more information to compute the next trajectory. While the KE is increased, the needed information is also raised. Therefore, a nonlinear system that have a positive KE is considered as unpredictable.

4 The parametric chaotic map model and its optimization

The study's main goal is to use PT-ABC to create a chaotic system. According to the literature, the proposed chaotic systems are based on familiar scientific principles like trigonometry (sine, cosine), iterative polynomial or series. We attempt to build a globally optimized PCM by optimizing its parameters in terms of effective objective functions. To this aim, fundamental map models are conceived, which are influenced by classical chaotic maps and included a few decision parameters to be improved. The flowchart depicting the optimization of PCM through PT-ABC is shown in Fig. 1. In Step 1, the PCM model is constructed. The determined PCM model, which included six decision parameters, was designed with the best in trial as follows:

$$x_{i+1} = \left(e^{a_1} u x_i + a_2 u x_i^{a_3} + {a_4}^{a_5 x_i + a_6}\right) \mathrm{mod} 1 \tag{4}$$

The optimization model includes six unknown coefficients $a_j, j \in \mathbb{Z}[1, 6]$ that serves as decision parameters. In Step 2, the decision parameters were then ideally calculated in-line with the flowchart for enhancing the following three objectives of_j involving LE, SE, and KE.

$$of_k = \left\{ of_1 = \frac{1}{\overline{\mathrm{LE}}}, of_2 = \frac{1}{\overline{\mathrm{SE}}}, of_3 = \frac{1}{\overline{\mathrm{KE}}} \right\} \tag{5}$$

where $\overline{\mathrm{LE}}$, $\overline{\mathrm{SE}}$, and $\overline{\mathrm{KE}}$ are the averages of LE, SE, and KE, respectively. In optimization, minimizing problems are more practical and reasonable. That is why, the reciprocal of them is performed for converting the three objective functions to be minimizing. In Step 3, in the Initial phase of ABC, possible decision parameters a_j were randomly created as NP = 400 to be between 0 and 20. Note that these values are empirically determined after attempting different values. Their fitness values were calculated based on these parameters. The population of decision parameters was updated and their fitness values were tested in the Employed bee phase in Step 4. Then, in Step 5, several parameters were chosen at random based on their probability. The selected ones were also changed throughout the Onlooker bee phase. For the better ones, a greedy selection is made. In Step 6, if the trial reached limit = 20, the Scout

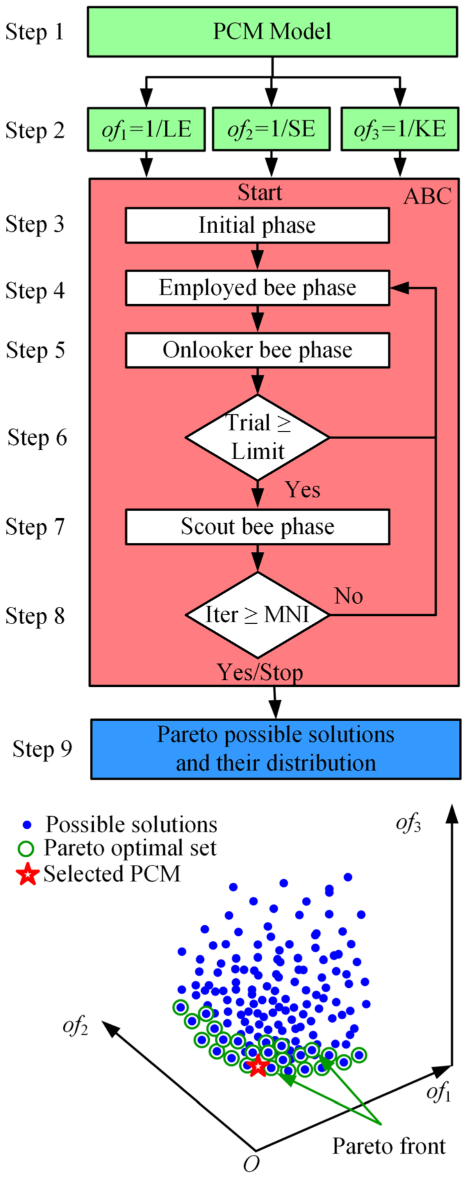

Fig. 1 Flowchart of PT-ABC

bee phase (Step 7) began, which generated a whole new decision parameter, similar to the Initial phase. In Step 8, ABC was then stopped if the maximum number of iterations (MNI) was equal to 1000. Because the results were settled beyond MNI = 1000. In Step 9, the Pareto optimum set is refined among the possible solutions. The final Pareto distribution is illustrated in Fig. 2. The global optimal PCM was selected within the Pareto optimal set as seen from the figure. The following equation is the generated PCM, in which the global optimal parameters have been substituted:

$$x_{i+1} = \left(e^{13.444} u x_i + 15.624 u x_i^{4.493} + 9.776^{2.792 x_i + 1.223}\right) \bmod 1 \tag{6}$$

where u is the control parameter and x_i is the initial values of PCM.

5 Chaotic behavior measurement of the parametric chaotic map

The chaotic impact of the PCM is assessed using chaos evaluation such as the bifurcation diagram and attractor, as well as the LE, SE, CD, and KE.

5.1 Bifurcation diagram and attractor

The bifurcation diagram identifies chaotic series components as a function of one parameter while keeping the others stationary [48]. The bifurcation displays the progression of each series element. The series' ergodicity may therefore be investigated visually. It is preferable to have the parts of the series spread out over the diagrams in a random way rather than settling on a line or point. The bifurcation diagrams are investigated in Fig. 3a as a function of the control parameters u. The figure shows no accumulation and the pieces are widely apart.

In addition to being a point representation, the attractor also shows their positioning relative to each other. From a chaotic series, it is hoped that the points evenly distribute across the phases and hence completely seat the spaces. Figure 3b shows a 2D attractor representing x_{i+1} in relation to x_i, and Fig. 3c shows a 3D attractor representing x_{i+2} versus x_{i+1} versus x_i. According to the statistics, the entrance points are evenly distributed over the phase, which may be ascribed to the PCM's greater chaoticity.

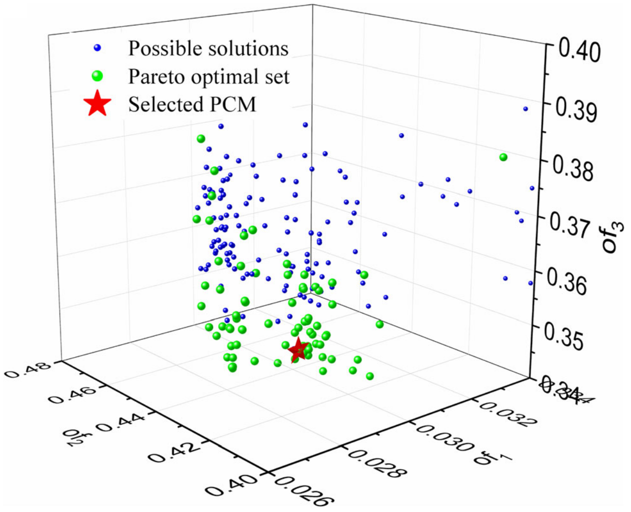

Fig. 2 The final Pareto distribution of solutions

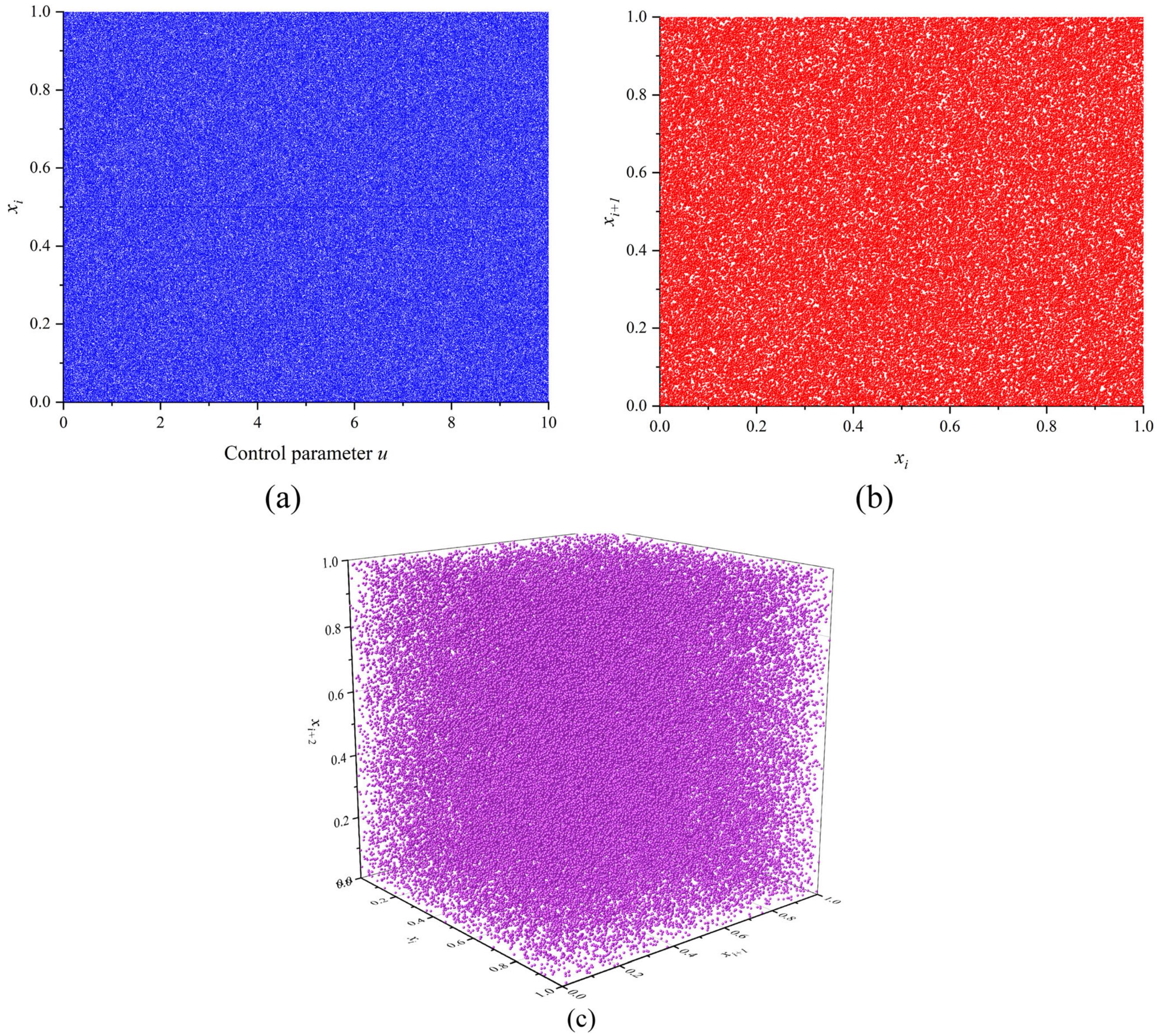

Fig. 3 a Bifurcation diagram, b 2D attractor, c 3D attractor

5.2 Lyapunov exponent

Figure 4 depicts the LE of PCM as a function of control parameters u. As the control parameter u fluctuates, LE becomes practically steady. Furthermore, in Fig. 4, LE is compared to the previously discovered chaotic systems, and their mean values are shown in Table 2. In the range $u \in [0, 10]$, the mean LE is 14.75. The next closest mean value is 10.28 [28]. The proposed chaotic system exhibits the most chaotic behavior.

5.3 Sample entropy

Figure 5 compares the SE findings to the previously published chaotic systems. Their mean values are shown in Table 2. The mean SE of the suggested PCM is 2.189, whereas the best of the others is 2.186 [28]. According to the results, the proposed PCM creates more complicated series than the previously reported maps.

5.4 Kolmogorov entropy

In Fig. 6, KE values belonging to the chaotic systems are scattered through a comparison. Table 2 also exhibits the

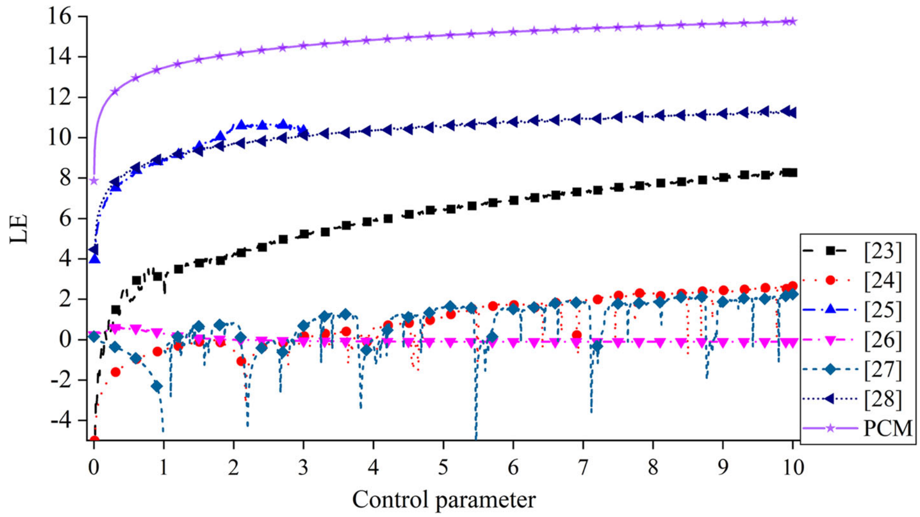

Fig. 4 Comparative LE results

mean KE in comparison. The proposed PCM's KE has the highest score of 2.584. Besides, the best of the others is 2.271 [23]. Therefore, the trajectory of PCM is unpredictable in the view of KE.

5.5 Correlation dimension

The CD is a form of fractal dimension that evaluates the dimensionality of occupied space in time series [49]. The CD may be used to separate deterministic chaotic systems from true chaotic ones. The CD has been used to examine time-series data in a variety of applications. For chaotic systems, the fractal dimension is equal to the phase-space dimension; however, for truly chaotic systems, the fractal dimension is smaller and usually not an integer. A time series is said to be chaotic if its CD is greater than zero. Besides, as the CD is increased, the spatial dimensionality of the sequence is promoted. The CD can be calculated using the formula below.

$$\mathrm{CD}(R) = \frac{2}{N(N-1)} \sum_{i=1}^{N} N_i(R) \tag{7}$$

where

$$N_i(R) = \sum_{i=1, i\neq k}^{N} 1(\|Y_i - Y_k\| < R)$$

$$R = \exp(\mathrm{linspace}(\log(r_{\min}), \log(r_{\max}), N))$$

where N stands for the number of points. R represents the radius of similarity. 1 is the indicator function. $r_{\min}$ and $r_{\max}$ are, respectively, the lowest and maximum radius. The CD is indicated by the slope of $\mathrm{CD}(R)$ versus R. Note that the score of CD is worthwhile because CD is not used in the optimization as an objective function. Figure 7 reveals the CD compared to the recently reported results. Moreover, the mean CD values are calculated in Table 2. From the CD results, the PCM surpasses the others because of its superior mean CD value of 1.942.

Table 2 Comparative mean chaos measurements

Ref.#	LE	SE	KE	CD
[23]	5.91	2.014	2.271	1.358
[24]	0.85	0.788	0.826	0.621
[25]	9.31	1.253	0.416	1.524
[26]	− 0.01	0.082	0.104	0.199
[27]	0.77	0.856	0.861	0.673
[28]	10.28	2.186	2.037	1.524
PCM	14.75	2.189	2.584	1.942

6 Experimental study

It is implemented to IE to examine the practical performance of the proposed PCM to chaos-based applications [41]. The robustness of PCM-based IE (PCMbIE) is then assessed by effective cryptanalysis such histogram, correlation, information entropy, cropping attack, and noise attack.

6.1 Key-space

It is expected from as secure IE, the key-space is large enough to survive brute-force attacks, which should be more than 2^{100} [50]. Two chaotic series are required in the IE's permutation and diffusion phases, each with a initial value and a variation parameter. As a result, the SHA 512-bit-length key is employed in the PCMbIE system, which has floating values with 10^{15} accuracy according to IEEE

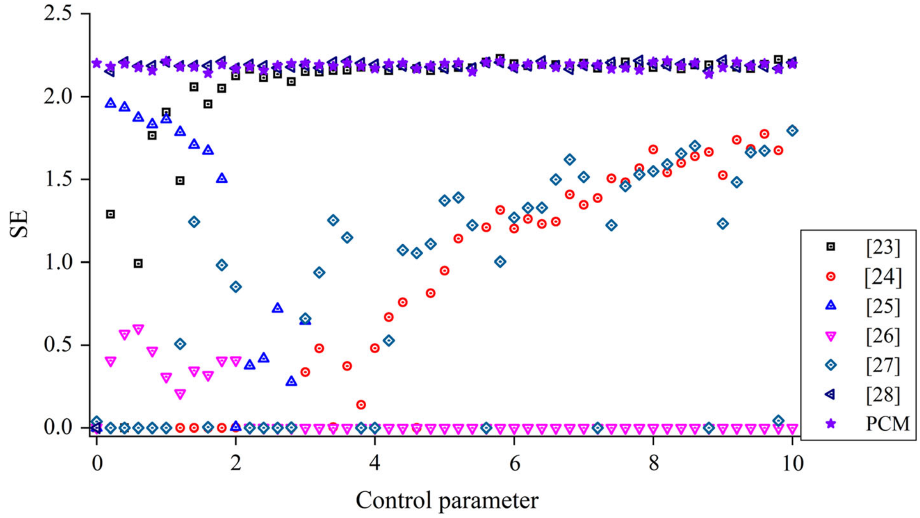

Fig. 5 Comparative SE measurement plot

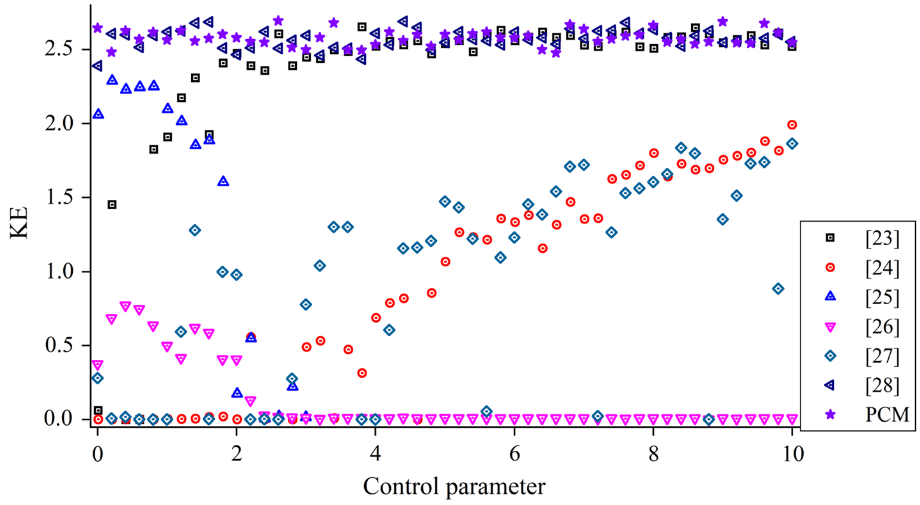

Fig. 6 Comparative KE measurement plot

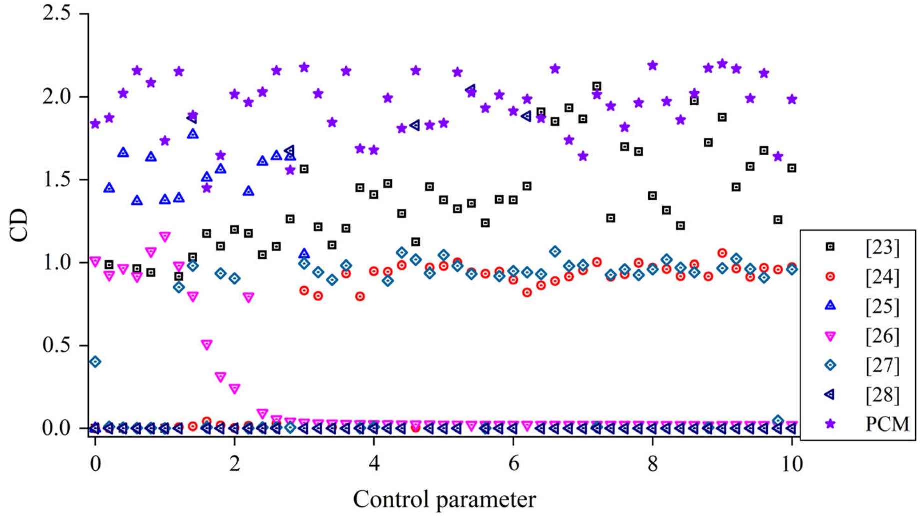

Fig. 7 Comparative CD measurement plot

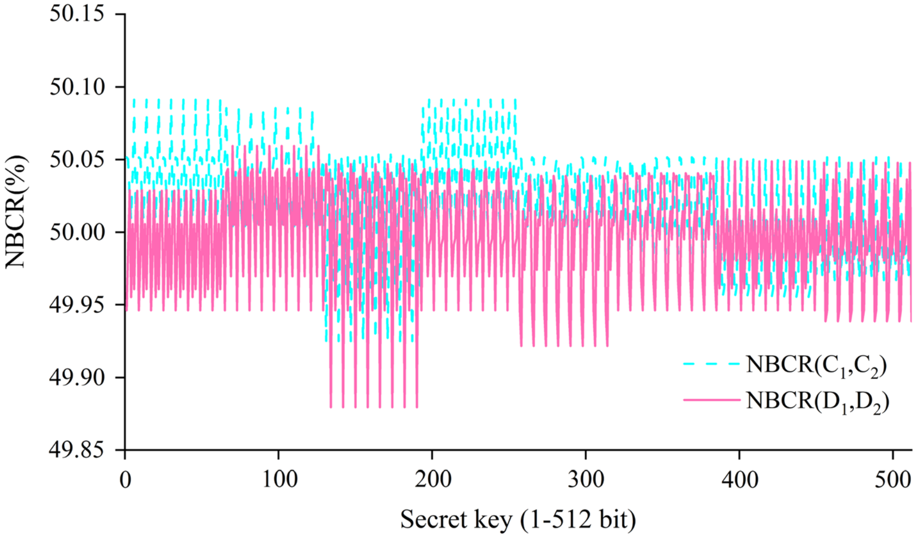

Fig. 8 The computed NBCR plot for the Lena image

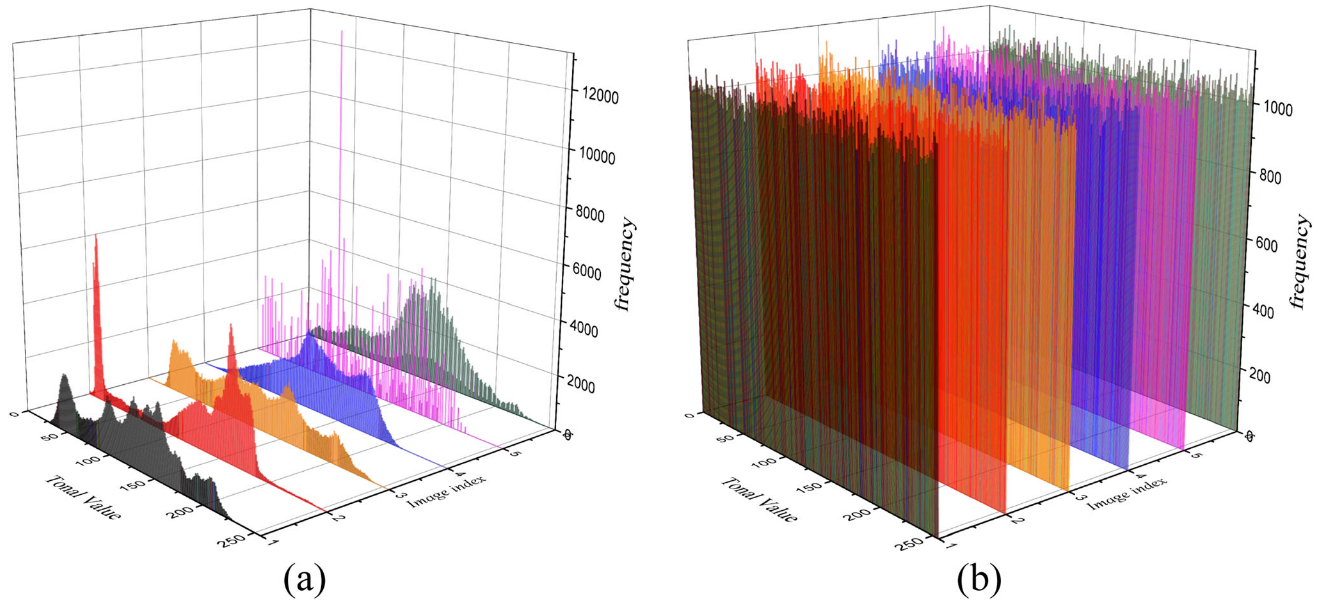

Fig. 9 Histograms analysis for images for **a** Plain, **b** Cipher (The image index is as follow: *1-Lena, 2-Cameraman, 3-Barbara, 4-Baboon, 5-Peppers, 6-Plane*)

standards. As a result, the key-space has a length of $10^{15\times4} = 10^{60} \cong 2^{200}$, which is securely more than 2^{100}.

6.2 Key sensitivity

The number of bit change rate (NBCR) [51] is a useful technique for analyzing key sensitivity. The following formula can be used to determine the difference pixels between encrypted and decrypted images.

$$\mathrm{Ham}(I_1, I_2) = \frac{1}{M \times N} \sum_{i=1}^{M\times N\times T_c} [I_1(i) \oplus I_2(i)] \times 100\% \qquad (8)$$

$$\mathrm{NBCR}(I_1, I_2) = \frac{\mathrm{Ham}(I_1, I_2)}{T_c} \qquad (9)$$

where the key length is denoted by T_c. $\mathrm{Ham}(I_1, I_2)$ is the Hamming distance, which indicates the difference in bits between two images of $M \times N$ size, I_1 and I_2. The greater the NBCR, the greater the difference between images I_1 and I_2. Figure 8 depicts the NBCR result for the Lena images in terms of one complete key's bit. The NBCR is calculated for each altered bit of the entire key from the first to the 512th bits. $\mathrm{NBCR}(C_1, C_2)$, respectively, compares the bits in the encrypted images C_1 and C_2 using the unchanged and one-bit changed keys. $\mathrm{NBCR}(D_1, D_2)$ calculates the difference in bits between deciphered images

D_1 and D_2 using the unchanged key and a one-bit changed key, respectively. The NBCR for the PCMbIE varies between 50.0191 and 49.9988% with standard deviation of 0.0339 and 0.0381, respectively.

6.3 Histogram

The histogram, which represents the occurrence frequency of pixel values, is a statistical cryptanalysis tool that is particularly useful for the assessing diffusion performance. An encrypted image's histogram should be as uniform as possible [52]. The histograms belonging to plaintext and ciphertext images are discovered in Fig. 9. It is clear that, just as plaintext images' histograms deploy in unison, ciphertext images' histograms disperse uniformly. In Table 3, the Var and χ^2 scores are listed. It should be less than 293.25 for the crucial value 0.05 [53] to pass the χ^2 (0.05; 255) test. Thanks to the proposed PCM, the PCMbIE gives guaranteed ciphered images.

6.4 Information entropy

The information entropy which is a useful statistical tool measures the grade of disorder and uncertainty in a images. Given that the distribution of pixel values in a raw image is inconsistent, a strong IE scheme should distribute the pixel or bit value consistently. To boost resistance against entropy-based attacks, the highest possible information entropy score for an 8-bit ciphered image is 8 [54]. Hence, while the entropy is increased, security of IE system enhances. Table 3 includes the information entropies of the plain and ciphered images that the PCMbIE manipulates the cipher image with the best average information entropy of 7.99944 as compared with the existing IE systems.

6.5 Correlation coefficient

It is well-known that the plain images inherently have a built-in correlation between their pixels. Correlation-based attacks break the encryption scheme by exploiting a statistical flaw. When it comes to IE it's critical to think about correlation susceptibility. Hence, a reliable IE system should lower the correlation coefficient among nearby pixels in directions of horizontal (H), vertical (V), and diagonal (D) [55]. 3D correlation scattering is illustrated in Fig. 10. Given that the correlation allocation of a image having one color pixels is a point. That of plaintext image which naturally includes related pixels are scattered on $y = x$ line. On the other hand, that of cipher image which must be completely uncorrelated pixels should be uniformly distributed on the graph. It is clear that the PCMbIE securely breaks the correlation between the pixels as given in Fig. 10d–f. Moreover, Table 3 tabulates the comparative correlation coefficients. The correlation is reduced to between 6.2×10^{-5} and 9.8×10^{-4} using the PCMbIE.

6.6 Cropping attack

Some ciphered image pixels may be hijacked or naturally lost during image transmission. During decryption, an IE is expected to restore image with the minimum amount of harm. The Lena image is used to test the IE system' ability to recover. The cropped images with ratios of 1/16, 1/4, and 1/2, as well as their deciphered ones, are shown in Fig. 11. Given that that when the cropping rate is increased, the decipher image's blurriness raises. Nevertheless, the recovered images are very distinct. Therefore, even if a large portion of the cipher image is cut off, the PCMbIE's restoring capacity is satisfactory. The peak signal-to-noise ratio (PSNR), that is a statistic rate of a signal's peak attainable strength to distortion strength, is

Table 3 The different cryptanalysis results

	Entropy for images		Correlation			Statistical test		Differential attack	
	Plaintext	Ciphertext	H	V	D	χ^2	*Var*	NPCR	UACI
Lena	7.44506	7.99951	1.3×10^{-4}	-8.6×10^{-4}	8.8×10^{-4}	250.72	1017.1	99.6080	33.4743
Cameraman	7.04795	7.99945	8.8×10^{-4}	8.1×10^{-4}	4.8×10^{-4}	243.91	1029.9	99.6090	334,648
Barbara	7.63211	7.99941	7.9×10^{-4}	9.8×10^{-4}	8.3×10^{-4}	231.22	989.8	99.6079	33.4270
Peppers	6.76242	7.99941	5.8×10^{-4}	7.1×10^{-4}	7.4×10^{-4}	242.16	1010.7	99.6066	33.4508
Baboon	7.29254	7.99942	6.2×10^{-5}	5.6×10^{-4}	6.2×10^{-5}	233.86	995.6	99.6086	33.4236
Jet-Plane	6.71351	7.99943	-7.2×10^{-4}	$- 3.5 \times 10^{-4}$	1.9×10^{-4}	240.28	1015.2	99.6100	33.4705

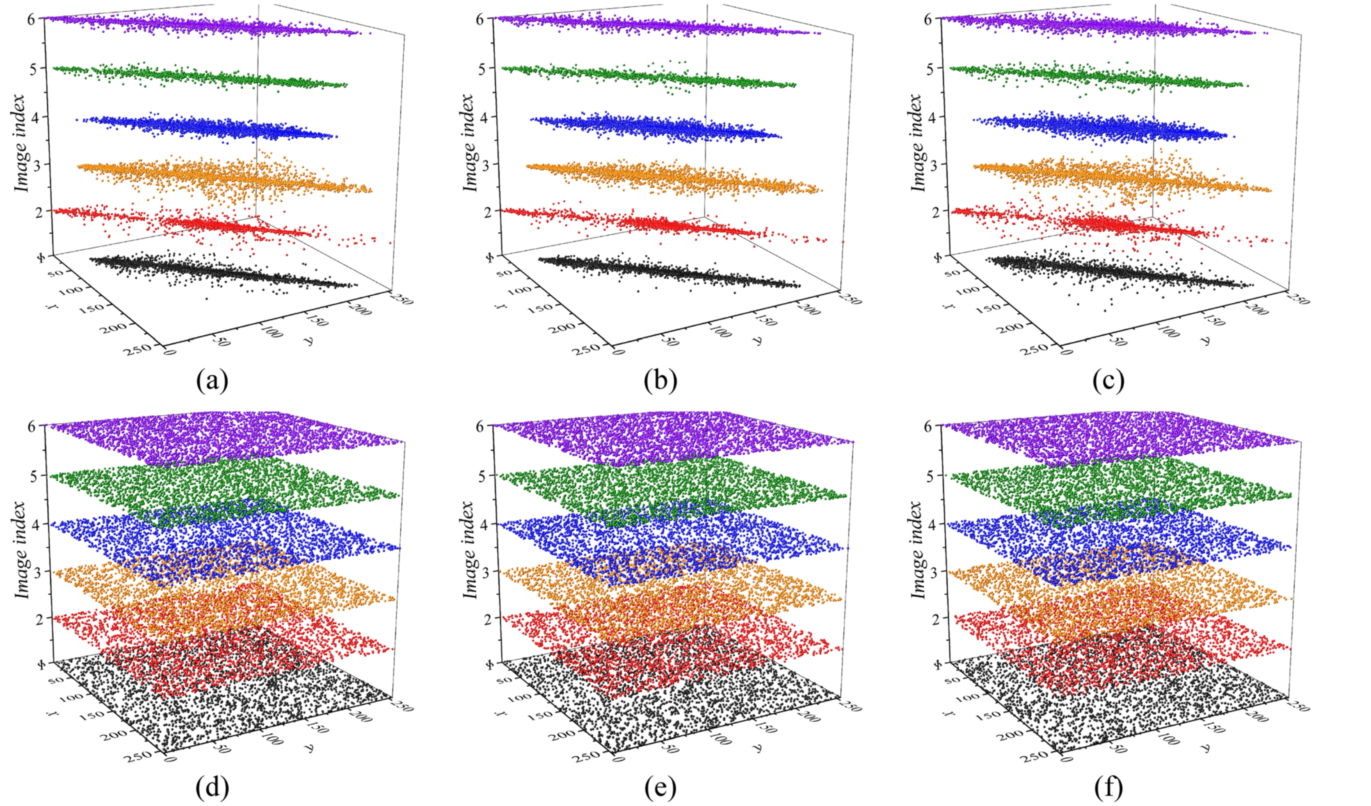

Fig. 10 The analyzed images for correlation distribution: **a** Plaintext (H), **b** Plaintext (V), **c** Plaintext (D), **d** Ciphertext (H), **e** Ciphertext (V), **f** Ciphertext (D) (The image index is as follow: *1-Lena, 2-Cameraman, 3-Barbara, 4-Baboon, 5-Peppers, 6-Plane*)

frequently used to assess degradation [56]. The image quality can be assessed as the increase in the PSNR. With cropping ratios of 1/16, 1/4, and /2, the PSNRs of the deciphered images are 21.41, 15.32, and 12.29, respectively.

6.7 Noise attack

Some pixels in an image might be intrinsically damaged or hijacked when it is transported. Salt and pepper noise (SPN) can be added to ciphered image to emulate the noise attack. To do this, the SPN is applied to the ciphertext Lena image with densities of 0.001, 0.01, and 0.1. Note that SPN is shown with red pixels. The lower the SPN density, the worse the decrypted image quality. Figure 12 displays the ciphered images with SPN, as well as their deciphered ones. SPN pixels that have been added are depicted in red color. The encrypted images with SPN intensities of 0.001, 0.01, and 0.1 had PSNR values of 40.99, 29.59, and 19.35, respectively. Furthermore, as shown in Fig. 12, the PCMbIE yields the images with the least amount of contamination.

6.8 Differential attack

To uncover an IE’s strategy, attackers may make tiny modifications to plaintext images in order to examine how the ciphered image changes, a technique known as differential attack. If the IE’s dispersal ability improves, it will be able to withstand this attack. Minor modification in the plain image must yield big alterations in the cipher image to withstand differential attacks and remove resembles between the plain and cipher images. To qualitatively assess an IE’s resilience to this attack, the number of pixels changing rate (NPCR) and unified average changing intensity (UACI) are utilized. The NPCR and UACI scores of the test images ciphered through PCMbIE are tabulated in Table 3. The desired NPCR and UACI scores for a 1-bit altered grayscale image are, respectively, 99.6094% and 33.4635% [57]. When scores of the NPCR and UACI tests are combined, as shown in Table 3, test results that are extremely near to the desired values are produced. Hence, a tiny change in the plaintext image, such as a 1-bit change, creates a significant variation in the ciphertext image.

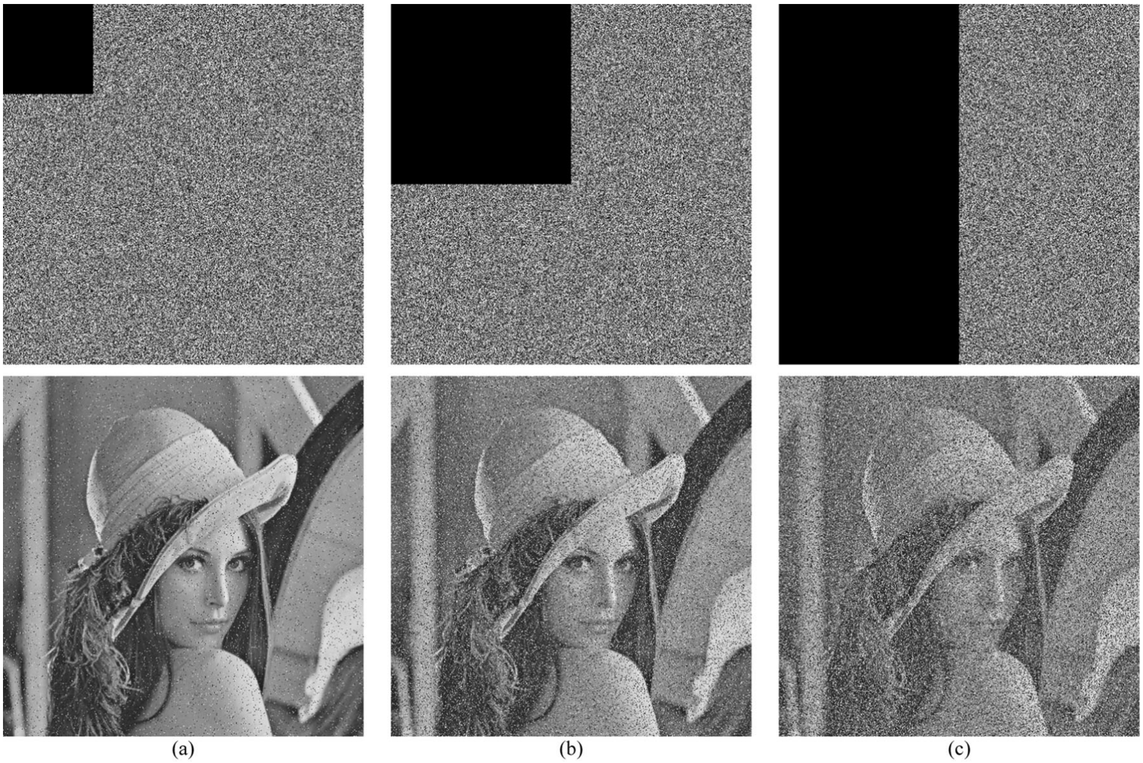

Fig. 11 Encrypted and decrypted images cropping with **a** 1/16 (PSNR: 21.41), **b** 1/4 (PSNR: 15.32), **c** 1/2 (PSNR: 12.29)

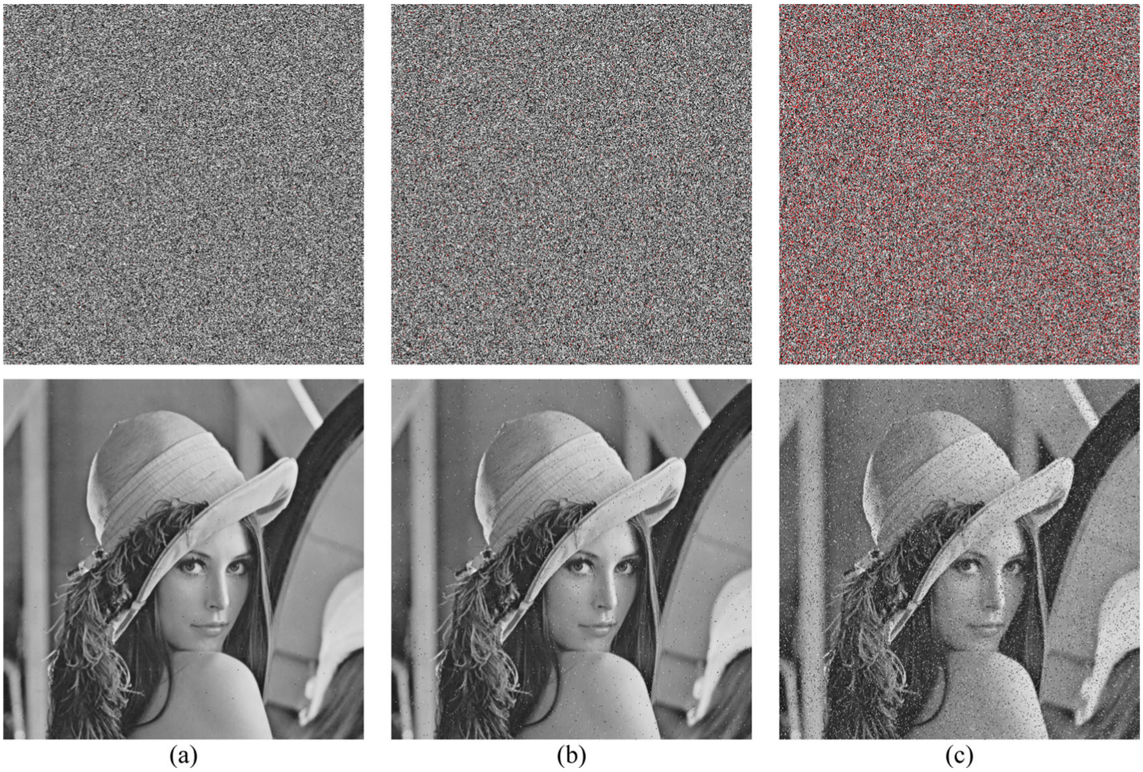

Fig. 12 Cipher and decipher images adding SPN intensity **a** 0.001 (PSNR: 40.99), **b** 0.01 (PSNR: 29.59), **c** 0.1 (PSNR: 19.35)

Table 4 Comparative results for Lena image with 512 × 512 pixels

References	Ciphertext entropy	Correlation (Mean)	NPCR	UACI	χ^2
[28]	7.9993	1.9×10^{-3}	99.6000	33.48	–
[58]	7.9993	8.1×10^{-3}	99.6051	33.5033	246.28
[59]	7.9993	9.5×10^{-3}	99.6053	33.4397	278.27
[60]	7.9993	2.4×10^{-3}	–	–	247.05
[24]	7.9993	2.4×10^{-3}	–	–	229.10
[61]	7.9993	1.2×10^{-3}	99.6200	33.5100	–
[62]	7.9994	2.5×10^{-3}	–	–	235.22
[63]	7.9970	4.9×10^{-3}	99.5900	33.4700	272.00
PCM	7.9995	6.2×10^{-4}	99.6080	33.4743	250.72

6.9 Performance comparison through IE results

In order to validate the performance of PCMbIE, it is compared with the-state-of-art IEs [24, 28, 58–63] for important numerical scores and visual results related to cropping and noise attacks. Table 4 shows the comparative results such as information entropy, correlation coefficient, NPCR, UACI, χ^2 for Lena image with 512 × 512 pixels. Therefore, the practical performance of PCM is verified through the comparison in which PCMbIE is evidently better than the others.

Figure 13 compares visual findings for cropping attack [24, 28, 58–61, 64] with the PCMbIE. The distinguishing outcome of the proposed PCMbIE appears to be more effective than the other algorithms tested. The allocation of the lost pixels in the decipher image should not aggregate after the cropping attack. From Fig. 13h, the proposd PCMbIE does not perform local gathering of faulty pixels in the image. The restored image contains a rich of information about the plain image.

Figure 14 depicts SPN comparing findings at 0.01 noise intensity to visually assess noise immunity. The suggested PCMbIE appears to be significantly more successful than previous algorithms for visually recovering the decipher image. Local aggregations of noise pixels exist in deciphered images in various IE systems. The PCMbIE decipher image contains no noise pixel aggregation. The decipher image has almost all of the information of the plaintext image.

As previously mentioned, chaotic systems have been used in applications of secure communication [2], watermarking [3], data compression [4], data hiding [5], and multimedia encryption [6]. The performance of the applications is heavily connected to the behavior of chaotic systems. Therefore, the main handicap of chaos-based applications is highly related to weak chaotic map of which the trajectory is able to predict, especially, the chaotic systems having periodic windows. Moreover, the chaotic maps depend on the initial values. Attaining the initial values can lead to reveal the behavior of the chaotic map and thus figure out the encryption algorithm. In order to prevent this, the chaotic maps should be evaluated through reliable chaos-based metrics such as LE, bifurcation, attractor, SE, KE and CD. It is difficult to figure out the chaotic maps with high complexity and randomness verified through these metrics. Note that the proposed PCM is extensively evaluated and eminently pass these metrics. The other limitation is about implementation to real-time systems such as industries. Because of the restricted accuracy of the computer in practical applications, resulting in the degradation effect of chaos to a certain extent. Therefore, there might be some potential risks in practical applications.

7 Conclusion

A new methodology based on parameter optimization of chaotic system through Pareto optimality is presented for the first time. Herewith, a novel chaotic system abbreviated as PCM was designed and optimized using PT-ABC algorithm. A six-parameter PCM was empirically contrived, and then its parameters were globally found out by providing the trade-off among the objectives LE, SE, and KE. The chaotic performance of PCM was evaluated through LE, SE, KE, and CD in comparison with the reported ones as well as bifurcation diagram and attractor. The PCM stands out among the compared existing chaotic systems thanks to the best mean values LE 14.75, SE 2.189, KE 2.584, and CD 1.942. Moreover, the PCM was tested by applying it to IE experiment, namely PCMbIE. The PCMbIE also demonstrates the best encryption performance as compared to the existing chaos-based IEs. The proposed PCM manifests the best complexity and pseudo-randomness due to its optimal structure. Therefore,

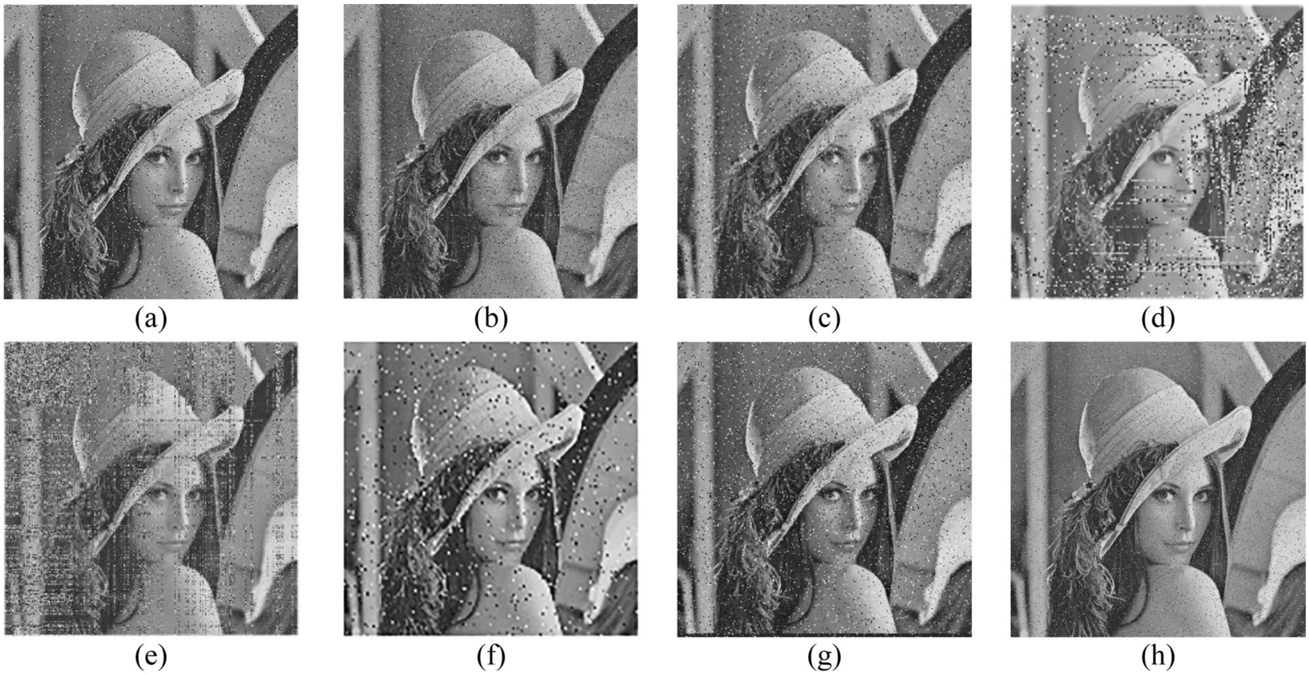

Fig. 13 The comparative visual cropping attack results for cropping ratio 1/16: **a** [58], **b** [59], **c** [60] (PSNR 19.81), **d** [24], **e** [64], **f** [61], **g** [28], **h** Proposed (PSNR: 21.41)

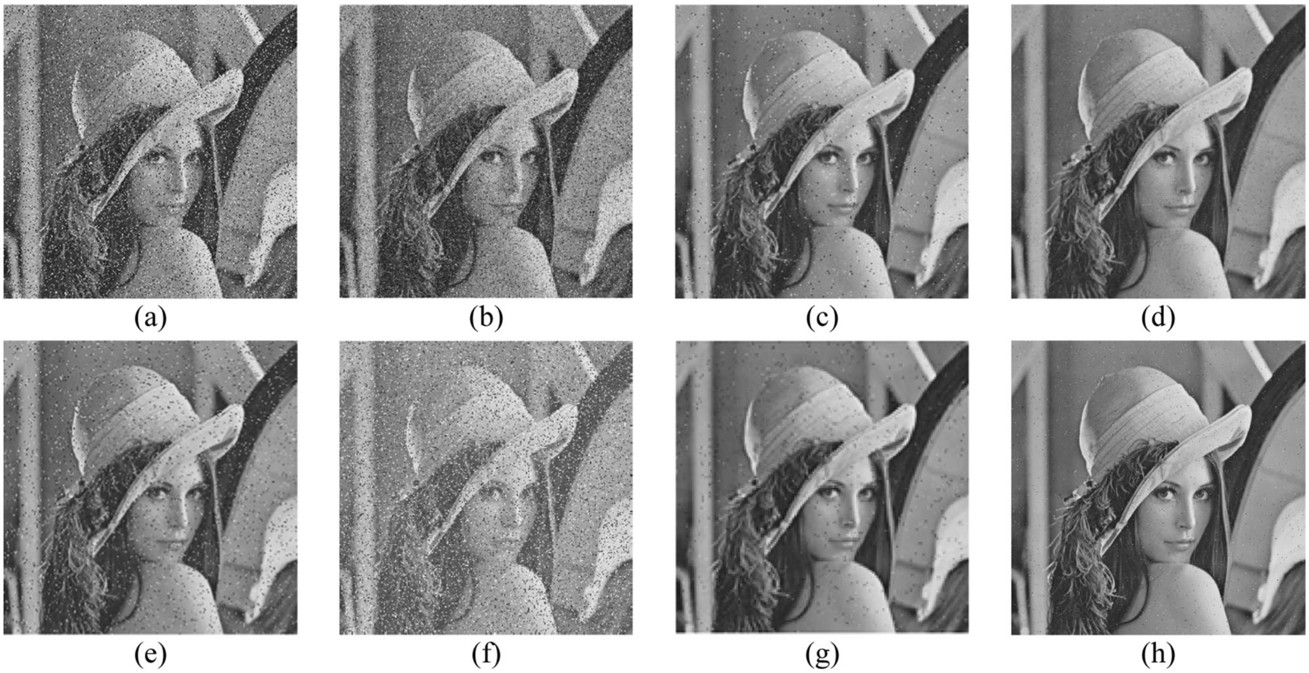

Fig. 14 The comparative visual noise attack results for SPN intensity 0.01: **a** [58], **b** [59], **c** [60] PSNR(24.97), **d** [23], **e** [63], **f** [65], **g** [66] (PSNR: 29.59)

the Pareto-based optimization is an effective approach for producing optimal chaotic system.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Gao S, Wu R, Wang X et al (2023) Asynchronous updating Boolean network encryption algorithm. IEEE Trans Circuits Syst Video Technol. https://doi.org/10.1109/TCSVT.2023.3237136
2. Lin CM, Pham DH, Huynh TT (2021) Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by TSK fuzzy brain emotional learning controllers. IEEE Trans Cybern. https://doi.org/10.1109/TCYB.2021.3134245
3. Li Q, Wang X, Ma B et al (2021) Concealed attack for robust watermarking based on generative model and perceptual loss. IEEE Trans Circuits Syst Video Technol. https://doi.org/10.1109/TCSVT.2021.3138795
4. Itier V, Puteaux P, Puech W (2020) Recompression of JPEG crypto-compressed images without a key. IEEE Trans Circuits Syst Video Technol 30:646–660. https://doi.org/10.1109/TCSVT.2019.2894520
5. Kaur R, Singh B (2021) A novel approach for data hiding based on combined application of discrete cosine transform and coupled chaotic map. Multimed Tools Appl 80:14665–14691. https://doi.org/10.1007/s11042-021-10528-5
6. Xian Y, Wang X, Teng L (2021) Double parameters fractal sorting matrix and its application in image encryption. IEEE Trans Circuits Syst Video Technol. https://doi.org/10.1109/TCSVT.2021.3108767
7. Kang X, Ming A, Tao R (2019) Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption. IEEE Trans Circuits Syst Video Technol 29:1595–1607. https://doi.org/10.1109/TCSVT.2018.2851983
8. Gao S, Wu R, Wang X et al (2023) A 3D model encryption scheme based on a cascaded chaotic system. Signal Process 202:108745. https://doi.org/10.1016/j.sigpro.2022.108745
9. Wu S, Jiang Y, Luo H et al (2022) An integrated data-driven scheme for the defense of typical cyber–physical attacks. Reliab Eng Syst Saf 220:108257. https://doi.org/10.1016/j.ress.2021.108257
10. Jiang Y, Wu S, Yang H et al (2022) Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. IEEE Trans Syst Man Cybern Syst 52:7799–7809. https://doi.org/10.1109/TSMC.2022.3164024
11. Zhang Y, Hua Z, Bao H et al (2022) An n-dimensional chaotic system generation method using parametric pascal matrix. IEEE Trans Ind Inform. https://doi.org/10.1109/TII.2022.3151984
12. Zheng W, Yan L, Gou C, Wang F-Y (2021) An ACP-based parallel approach for color image encryption using redundant blocks. IEEE Trans Cybern. https://doi.org/10.1109/TCYB.2021.3105568
13. Xu G, Li C, Wang Q (2019) Unified multi-scale method for fast leaf classification and retrieval using geometric information. IET Image Process 13:2328–2334. https://doi.org/10.1049/iet-ipr.2018.6551
14. Gao S, Wu R, Wang X et al (2023) EFR-CSTP: encryption for face recognition based on the chaos and semi-tensor product theory. Inf Sci (Ny) 621:766–781. https://doi.org/10.1016/j.ins.2022.11.121
15. Wang X, Zhang W, Guo W, Zhang J (2013) Secure chaotic system with application to chaotic ciphers. Inf Sci (Ny) 221:555–570. https://doi.org/10.1016/j.ins.2012.09.037
16. Babanli K, Ortaç Kabaoğlu R (2022) Fuzzy modeling of desired chaotic behavior in secure communication systems. Inf Sci (Ny) 594:217–232. https://doi.org/10.1016/j.ins.2022.02.020
17. Wang Y, Liu Z, Zhang LY et al (2021) From chaos to pseudorandomness: a case study on the 2-D coupled map lattice. IEEE Trans Cybern. https://doi.org/10.1109/TCYB.2021.3129808
18. Márquez-Martínez LA, Cuesta-García JR, Pena Ramirez J (2022) Boosting synchronization in chaotic systems: combining past and present interactions. Chaos, Solitons Fractals 155:111691. https://doi.org/10.1016/j.chaos.2021.111691
19. Wang X, Li Y (2021) Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Opt Lasers Eng 137:106393. https://doi.org/10.1016/j.optlaseng.2020.106393
20. Wu Y, Zhou Y, Bao L (2014) Discrete wheel-switching chaotic system and applications. IEEE Trans Circuits Syst I Regul Pap 61:3469–3477. https://doi.org/10.1109/TCSI.2014.2336512
21. Zhou Y, Hua Z, Pun C-M, Philip Chen CL (2015) Cascade chaotic system with applications. IEEE Trans Cybern 45:2001–2012. https://doi.org/10.1109/TCYB.2014.2363168
22. Zheng J, Hu H (2022) A highly secure stream cipher based on analog–digital hybrid chaotic system. Inf Sci (Ny) 587:226–246. https://doi.org/10.1016/j.ins.2021.12.030
23. Wang X, Guan N, Yang J (2021) Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map. Chaos, Solitons Fractals 150:111117. https://doi.org/10.1016/J.CHAOS.2021.111117
24. Midoun MA, Wang X, Talhaoui MZ (2021) A sensitive dynamic mutual encryption system based on a new 1D chaotic map. Opt Lasers Eng 139:106485
25. Mansouri A, Wang X (2021) A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. Inf Sci (Ny) 563:91–110. https://doi.org/10.1016/J.INS.2021.02.022
26. Talhaoui MZ, Wang X (2021) A new fractional one dimensional chaotic map and its application in high-speed image encryption. Inf Sci (Ny) 550:13–26. https://doi.org/10.1016/J.INS.2020.10.048
27. Yahi A, Bekkouche T, El Hossine DM, Diffellah N (2022) A color image encryption scheme based on 1D cubic map. Optik (Stuttg) 249:168290. https://doi.org/10.1016/J.IJLEO.2021.168290
28. Zhou W, Wang X, Wang M, Li D (2022) A new combination chaotic system and its application in a new bit-level image encryption scheme. Opt Lasers Eng 149:106782. https://doi.org/10.1016/J.OPTLASENG.2021.106782
29. Chan JCL, Lee TH, Tan CP (2022) Secure communication through a chaotic system and a sliding-mode observer. IEEE Trans Syst Man Cybern Syst 52:1869–1881. https://doi.org/10.1109/TSMC.2020.3034746
30. Han M, Zhong K, Qiu T, Han B (2019) Interval type-2 fuzzy neural networks for chaotic time series prediction: a concise overview. IEEE Trans Cybern 49:2720–2731. https://doi.org/10.1109/TCYB.2018.2834356

31. Carbas S, Toktas A, Ustun D (2021) Nature-inspired metaheuristic algorithms for engineering optimization applications. Springer, Singapore
32. Karaboga D, Basturk B (2007) A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. J Glob Optim 39:459–471. https://doi.org/10.1007/s10898-007-9149-x
33. Karaboga D, Gorkemli B, Ozturk C, Karaboga N (2014) A comprehensive survey: artificial bee colony (ABC) algorithm and applications. Artif Intell Rev 42:21–57. https://doi.org/10.1007/s10462-012-9328-0
34. Toktas A, Ustun D, Erdogan N (2020) Pioneer pareto artificial bee colony algorithm for three-dimensional objective space optimization of composite-based layered radar absorber. Appl Soft Comput 96:1–12. https://doi.org/10.1016/j.asoc.2020.106696
35. Toktas A (2021) Multi-objective design of multilayer microwave dielectric filters using artificial bee colony algorithm. In: Carbas S, Toktas A, Ustun D (eds) Nature-inspired metaheuristic algorithms for engineering optimization applications. Springer, Singapore
36. Toktas A, Ustun D (2020) Triple-objective optimization scheme using butterfly-integrated ABC algorithm for design of multilayer RAM. IEEE Trans Antennas Propag 68:5603–5612. https://doi.org/10.1109/TAP.2020.2981728
37. Hua Z, Chen Y, Bao H, Zhou Y (2022) Two-dimensional parametric polynomial chaotic system. IEEE Trans Syst Man Cybern Syst 52:4402–4414. https://doi.org/10.1109/TSMC.2021.3096967
38. Yuan CM, Feeny BF (1998) Parametric identification of chaotic systems. J Vib Control 4:405–426. https://doi.org/10.1177/107754639800400404
39. Capeáns R, Sabuco J, Sanjuán MAF (2016) Parametric partial control of chaotic systems. Nonlinear Dyn 86:869–876. https://doi.org/10.1007/s11071-016-2929-4
40. Xiong Q, Shen J, Tong B, Xiong Y (2022) Parameter identification for memristive chaotic system using modified sparrow search algorithm. Front Phys. https://doi.org/10.3389/fphy.2022.912606
41. Toktas A, Erkan U, Toktas F et al (2021) Chaotic map optimization for image encryption using triple objective differential evolution algorithm. IEEE Access 9:127814–127832. https://doi.org/10.1109/ACCESS.2021.3111691
42. Toktas A, Erkan Ustun UD (2021) An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm. Nonlinear Dyn 1052(105):1885–1909. https://doi.org/10.1007/S11071-021-06675-X
43. Toktas A, Erkan U (2022) 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. Neural Comput Appl 34:4295–4319. https://doi.org/10.1007/s00521-021-06552-z
44. Rosenstein MT, Collins JJ, De Luca CJ (1993) A practical method for calculating largest Lyapunov exponents from small data sets. Phys D Nonlinear Phenom 65:117–134. https://doi.org/10.1016/0167-2789(93)90009-P
45. Richman JS, Moorman JR (2000) Physiological time-series analysis using approximate and sample entropy. Am J Physiol—Hear Circ Physiol 278:2039–2049. https://doi.org/10.1152/ajpheart.2000.278.6.h2039
46. Grassberger P, Procaccia I (1983) Estimation of the Kolmogorov entropy from a chaotic signal. Phys Rev A 28:2591–2593. https://doi.org/10.1103/PhysRevA.28.2591
47. Gao L, Wang J, Chen L (2013) Event-related desynchronization and synchronization quantification in motor-related EEG by Kolmogorov entropy. J Neural Eng 10:36023. https://doi.org/10.1088/1741-2560/10/3/036023
48. 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
49. Theiler J (1987) Efficient algorithm for estimating the correlation dimension from a set of discrete points. Phys Rev A 36:4456–4462. https://doi.org/10.1103/PhysRevA.36.4456
50. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos 16:2129–2151. https://doi.org/10.1142/S0218127406015970
51. Castro JCH, Sierra JM, Seznec A et al (2005) The strict avalanche criterion randomness test. Math Comput Simul 68:1–7. https://doi.org/10.1016/J.MATCOM.2004.09.001
52. de NetoO JR, Lima JB, Panario D (2020) The design of a novel multiple-parameter fractional number-theoretic transform and its application to image encryption. IEEE Trans Circuits Syst Video Technol 30:2489–2502. https://doi.org/10.1109/TCSVT.2019.2925522
53. Zhang X, Zhao Z, Wang J (2014) Chaotic image encryption based on circular substitution box and key stream buffer. Signal Process Image Commun 29:902–913. https://doi.org/10.1016/j.image.2014.06.012
54. Zhu L, Jiang D, Ni J et al (2022) A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. Signal Process 195:108489. https://doi.org/10.1016/j.sigpro.2022.108489
55. Preishuber M, Hütter T, Katzenbeisser S, Uhl A (2018) Depreciating motivation and empirical security analysis of chaos-based image and video encryption. IEEE Trans Inf Forensics Secur 13:2137–2150. https://doi.org/10.1109/TIFS.2018.2812080
56. Erkan U, Toktas A, Toktas F, Alenezi F (2022) 2D eπ-map for image encryption. Inf Sci (Ny) 589:770–789. https://doi.org/10.1016/j.ins.2021.12.126
57. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber J Multidiscip J Sci Technol J Sel Areas Telecommun 1:31–38
58. Liang Q, Zhu C (2023) A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. Opt Laser Technol 160:109033. https://doi.org/10.1016/j.optlastec.2022.109033
59. Wang X, Li Y, Jin J (2020) A new one-dimensional chaotic system with applications in image encryption. Chaos, Solitons Fractals 139:110102. https://doi.org/10.1016/j.chaos.2020.110102
60. Wang X, Du X (2021) Pixel-level and bit-level image encryption method based on Logistic-Chebyshev dynamic coupled map lattices. Chaos, Solitons Fractals. https://doi.org/10.1016/j.chaos.2021.111629
61. Khalil N, Sarhan A, Alshewimy MAM (2021) An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. Opt Laser Technol 143:107326. https://doi.org/10.1016/J.OPTLASTEC.2021.107326
62. Wang X, Zhang M (2021) High-sensitivity synchronous image encryption based on improved one-dimensional compound sine map. IET Image Process 15:2247–2265. https://doi.org/10.1049/ipr2.12193
63. Wu W, Wang Q (2022) Cryptanalysis and improvement of an image encryption algorithm based on chaotic and latin square. Nonlinear Dyn. https://doi.org/10.1007/s11071-022-07990-7
64. Talhaoui MZ, Wang X, Talhaoui A (2021) A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. Vis Comput 37:1757–1768. https://doi.org/10.1007/s00371-020-01936-z

65. Lai Q, Zhang H, Kuate PDK et al (2022) Analysis and implementation of no-equilibrium chaotic system with application in image encryption. Appl Intell 52:11448–11471. https://doi.org/10.1007/s10489-021-03071-1

66. Folifack Signing VR, Gakam Tegue GA, Kountchou M et al (2022) A cryptosystem based on a chameleon chaotic system and dynamic DNA coding. Chaos, Solitons Fractals 155:111777. https://doi.org/10.1016/j.chaos.2021.111777

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