Neural Computing and Applications (2022) 34:4295–4319
https://doi.org/10.1007/s00521-021-06552-z

ORIGINAL ARTICLE

2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm

Abdurrahim Toktas[1] · Uğur Erkan[2]

Received: 17 March 2021 / Accepted: 14 September 2021 / Published online: 1 November 2021

Abstract

In this study, a novel 2D fully chaotic map (FULLMAP) derived through a multi-objective optimization strategy with artificial bee colony (ABC) algorithm is introduced for image encryption procedures (IMEPs). First, a model for FULLMAP with eighth decision variables was empirically constituted, and then, the variables were optimally determined using ABC for minimizing a quadruple-objective function composed of Lyapunov exponent (LE), entropy, 0–1 test and correlation coefficient. FULLMAP manifests superior performance in diverse measurements such as bifurcation, 3D phase space, LE, 0–1 test, permutation entropy (PE) and sample entropy (SE). The encryption performance of FULLMAP through an IMEP was verified with respect to various cryptanalyses compared with many reported studies, as well. The main advantage of FULLMAP rather than the optimization-based IMEP studies reported elsewhere is that it need not any optimization in the encryption procedures, and hence, it is faster than the reported procedures. On the other hand, those studies use ciphertext images through IMEPs in every cycle of the optimization. For this reason, they might have long processing time. As a result, the proposed IMEP with FULLMAP demonstrates better cryptanalyses for the most of the compared results.

Keywords Image encryption · 2D chaotic map · Metaheuristic algorithm · Multi-objective optimization · Artificial bee colony

1 Introduction

Data storing and transferring have been received increasingly interest in recent years [1–3]. While the data are being transferred through a wide area network (WAN), it is exposed to potential cyberthreats like network attacks, denial-of-service, man-in-the-middle and phishing [4]. That is why, the data must be encrypted via reliable and secure data encryption procedures for assuring the information security during the data transferring [5, 6]. The well-known procedures are data encryption standard (DES), triple-DES (3DES), international data encryption algorithm (IDEA) and an advanced encryption standard (AES), whereas they might be inefficient with regard to the security since current data have high amount and correlation among them [7, 8].

Image cryptosystems generally depend on the spatial and/or frequency domains. Cryptosystems in the spatial domain are deoxyribonucleic acid (DNA) coding, chaos, cellular automata and compressed sensing, and those in the frequency domains are Fourier and wavelet transforms [9, 10]. Chaotic map-based image encryption procedures (IMEPs) are mostly utilized techniques owing to providing high dynamization, complexity, sensitivity to initial conditions and system parameters. Thanks to these properties, chaotic maps have been also utilized in different engineering problems [11–16]. Chaotic map-based IMEPs are generally operated through two stages: permutation and diffusion. The positions of image's pixels are shuffled in the permutation, and the pixel's values are manipulated in the diffusion. They are committed by inputting sequences

✉ Uğur Erkan
ugurerkan@kmu.edu.tr

[1] Department of Electrical and Electronics Engineering, Faculty of Engineering, Karamanoglu Mehmetbey University, 70200 Karaman, Turkey

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

generated by a chaotic map. The chaotic maps are governed with an initial value and a control parameter obtained by a key. Therefore, the chaotic maps have a crucial role in operation of an IMEP.

Several IMEPs that have been recently reported are elaborately surveyed with respect to the employed chaotic map and cryptanalyses in Sect. 6. It is observed that suggested IMEPs have their own strong and weak sides and are robust for particular cryptanalyses. Chaotic maps such as logistic [17–22], sine/cosine [17, 23–26], Henon [25, 27], Chebyshev [26], Lorenz [28, 29], Yolo [30] and cellular automata [31] and their variants and combinations are mostly utilized with different dimensions. The performance of IMEPs is usually evaluated through various precise cryptanalyses such as key-space, key sensitivity, entropy, histogram, correlation, differential attack, noise attack and cropping attack [32]. As comparison, the key-space analyses are the lowest [23, 29, 33]. The mean entropy values are better [34], moderate [17, 25, 28, 31, 35–38] and worse [18, 20–22, 26, 29, 30, 33, 39]. The mean correlation coefficient for horizontal, vertical and diagonal directions seems lower [18, 19, 35] moderate [20, 22–27, 29–31, 34, 36–40] and higher [17, 21, 28, 33, 41]. Pixels changing rate (NPCR) can be sorted as the best [17, 18, 24–26, 35–40], medium [20–23, 28–31, 34] and weakest [19, 33]. The unified average changing intensity (UACI) is robust [18, 23, 24, 34, 40], intermediate [17, 25, 26, 28, 30, 35, 36, 38, 39] and poor [19, 21, 31, 33, 37]. Against the cropping attack, they are better [35], moderate [18, 23, 26, 38, 39] and poorer [24, 25, 30, 37, 40]. Noise attack is well [18, 38, 40], fair [24–26, 30, 37, 39] and worse [23]. According to the encryption processing time, they can be considered as the fast [24, 26, 30, 31, 36–38], intermediate [23, 40] and slow [21, 22, 29, 39]. It is deduced that as some of them are better in some particular cryptanalyses, the others are poor, and vice versa, i.e., they do not prove security at entire cryptanalyses.

Metaheuristic algorithms especially the nature-inspired optimization have been successfully utilized in single or multi-objective engineering problems [42–48]. They have been widely implemented to IMEPs with single [19–22, 27, 41, 49] or multi-objective [18, 29, 33, 34] strategies in order to enhance the security of the cryptosystems, as well. The optimization-based IMEPs are also elaborately reviewed in Sect. 6 which comprises the related studies. The multi-objective studies attempted to combine different objectives [18, 29]. There have been several studies using the nature-inspired optimization algorithms that are ant colony algorithm (ACO), particle swarm optimization (PSO) [18, 50], genetic algorithm (GA) [33], differential evolution (DE) [21, 51], whale optimization algorithm (WOA) [22], artificial bee colony (ABC), butterfly optimization algorithm (BOA) [52] and steepest descent optimization (SDO) [27]. The optimization algorithms have been generally used to optimize decision variables such as keys [18–20, 33, 41, 49], initial parameters of the chaotic maps [22, 29, 34], ciphertext image [27] and chaotic sequence optimization [21] for minimizing or maximizing different objective functions. The mostly utilized objective functions are entropy [18, 20–22, 29, 33, 34], correlation coefficient [19, 20, 29, 33], peak signal-to-noise ratio (PSNR) [49], NPCR [29, 34], UACI [29, 34] and energy [41]. While those studies surveyed, it is inferred that the optimization is able to enhance the encryption performance, and the main issue is yet that how the optimization can be implemented without increasing the encryption processing time. It is worth noting that those objective functions are evaluated on the ciphertext images. The main disadvantage of those studies is that the optimization algorithms were directly implemented to IMEP, i.e., the objective functions were dependent on the ciphertext images that must be computed through the entire image encryption operations. Because the objective values are achieved for the ciphertext images in every cycles of the optimization, they likely suffer from long encryption processing time and complexity, making IMEP inapplicable to the realistic systems. A fully chaotic map, which is optimized using a proper optimization algorithm for effective multiple objective functions, would be promising for an outperforming IMEP with regard to all cryptanalyses.

In this study, a novel 2D fully chaotic map (FULLMAP) constructed with the help of a multi-objective optimization using ABC algorithm is proposed for IMEP. An effective model for FULLMAP with eight decision variables was empirically constituted among various essayed chaotic map model. The decision variables of FULLMAP were optimally sought out for minimizing a versatile weighted multi-objective function involving Lyapunov exponent (LE), entropy, 0–1 test and correlation coefficient. The block diagram of FULLMAP-based IMEP with is depicted

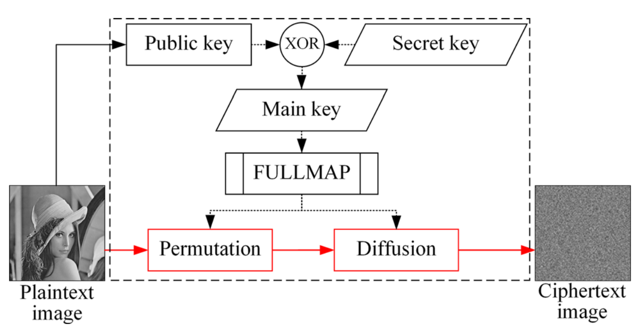


Fig. 1 The flowchart of the proposed FULLMAP-based IMEP

in Fig. 1. In order to clearly manifest the superiority of the proposed FULLMAP, an IMEP with only two operations: permutation and diffusion, is proposed. A main key is firstly got from public and secret keys. The control parameter and initial value of FULLMAP are then obtained using the main key so as to generate the chaotic sequences. Since ABC is merely implemented to constructing FULLMAP not to the ciphertext image as done in the literature, FULLMAP works independently from the encryption process. Hence, the proposed IMEP with FULLMAP operates faster than the state of the arts in which optimization is used. The cryptanalyses demonstrate that the proposed IMEP outperforms the reported results thanks to the optimized dynamic performance of FULLMAP. Furthermore, the contributions of our study can be briefly stated as follows:

- A method, in which a quadruple-objective optimization with ABC was implemented to achieve a fully hyperchaotic map, is proposed for IMEP.
- A fully chaotic map so-called FULLMAP whose chaotic performance was demonstrated through distinct measurements is optimally constructed using the proposed method.
- The encryption performance of FULLMAP was verified with IMEP with respect to various cryptanalyses in detail.
- The reported studies with and without optimization were surveyed to point out the capability of FULLMAP.

2 Construction of FULLMAP using ABC with multi-objective strategy

In this section, the principle of ABC algorithm and the handled objective functions for FULLMAP are explained. The model considered for FULLMAP with eight decision variables and implementation of ABC to optimize FULLMAP is addressed. Finally, the optimally determined variables and whole FULLMAP are presented.

2.1 ABC algorithm

ABC was modeled by imitating the foraging behavior of natural bees [53]. Once ABC was emerged, ABC and its variants have been implemented to numerous engineering problems due to its effective properties [54–58]. It is supposed that three groups of bees, namely employed, onlooker and scout bees, compose the artificial bee colony. They operate through three phases with the same name of the groups. The three phases are iteratively operated up to the predefined maximum number of cycles (MNC). The colony is equally divided into two groups of the employed bees and onlooker bees. The pseudocode of ABC is given in Algorithm 1.

2.1.1 Initialization phase

All employed bees work as scout bees and randomly discover the initial nectar sources, which stand for candidate solutions x_{ij} (decision variables), using the following operator (Line 2).

$$x_{ij} = x_{min} + rand(0,1) \times (x_{max} - x_{min}) \tag{1}$$

where $i = 1, 2, \ldots, NP$ is number of population (NP) and $j = 1, 2, \ldots, D$ is the dimension of decision vector. x_{min} and x_{max} are the minimum and maximum bounds of the search space.

2.1.2 Employed bees phase

The employed bees are then assigned to consume specific nectar sources, implying that they produce new solutions m_{ij} in the vicinity of the previous solutions as follows (Line 5):

$$m_{ij} = x_{ij} + \phi_{ij} \times \left(x_{ij} - x_{kj}\right) \tag{2}$$

where $(k \neq i) \in \{1, 2, \ldots, NP\}$ is random index different from i and $j \in \{1, 2, \ldots, D\}$. $\phi_{ij} \in [-1, 1]$ is a random number. The quality of the new nectar sources is then evaluated, i.e., the fitness values of all modified solutions are computed as given below (Line 6)

$$fit_i = \begin{cases} \dfrac{1}{1 + of_i(x)} & if\ \ of_i(x) \geq 0 \\ 1 + abs(of_i(x)) & if\ \ of_i(x) < 0 \end{cases} \tag{3}$$

where $of_i(x)$ is the objective value for each solution. The solutions are replaced with the corresponding better solutions of m_{ij} (Line 7). The worthiness of the solutions is then computed depending on the fitness values using the following operator (Line 8).

$$P_i = \frac{fit_i}{\sum_{i=1}^{NP/2} fit_i} \tag{4}$$

2.1.3 Onlooker bees phase

The employed bees share their information regarding the quality of nectar source by dancing in the hive. The onlooker bees probabilistically chose the nectar sources in accordance with this information, i.e., they decide the solutions depending on the worthiness of the solutions by means of the roulette wheel selection (Line 10). The onlooker bees then start to consume the selected nectar sources, meaning that it produces new solutions m_{ij} in the surrounding of the selected solutions using the operator in Eq. (2) (Line 11). The quality of the new nectar sources is then evaluated by computing the fitness values of the modified solutions using Eq. (3) (Line 12). The better solutions m_{ij} are taken place of the former reciprocal solutions (Line 13). Meanwhile, if an employed bee exhausts a nectar source, it then become a scout bee and is appointed for a completely new nectar source (Line 14). It means that if a solution cannot be improved after a predetermined number of essays called "limit", a new solution is generated using Eq. (1) (Line 16). The best solution achieved at the end of a cycle is recorded (Line 18). Finally, if the cycles reach to the MNC, ABC is stopped for the best solution (Line 19).

2.2.1 LE

The LE whose equation is given below is a logarithmic measure for the mean expansion rate per iteration of the distance between two infinitesimal close trajectories [59].

$$\mathrm{LE} = \lim_{n\to\infty} \sum_{i=1}^{n-1} ln\left|f'(v_i)\right| \tag{6}$$

where $f(v_i) = v_{i+1}$ is the chaotic map and n is the number of iterations for a specific value of the control parameter. The LE can be employed to evaluate a chaotic map's performance regarding the system's predictability and sensitivity to the control parameter and initial value. The LE must be as high as possible for a large range of the control parameter that shows better chaotic characteristic. Therefore, the correlation and entropy of the ciphertext image can be increased by elevating the LE of a map.

Algorithm 1: The pseudocode of ABC algorithm

```
ABC (MNC, limit, NP)
1   //Initialization phase
2   Generate randomly the initial population x_ij
3   for i = 1 to MNC
4       //Employed Bees
5       Produce new solutions m_ij in the vicinity of the previous solutions
6       Evaluate fitness fit_i of the solutions
7       Select greedy between x_i and v_i according to fitness values
8       Compute the worthiness P_i for the solutions
9       //Onlooker Bees
10      Select solutions depending on P_i
11      Produce the new solutions m_ij around the selected x_ij
12      Evaluate fitness fit_i of the solutions
13      Select greedy between x_i and m_i according to fitness values
14      if trial ≥ limit
15          //Scout Bees
16          Generate a new solution
17      end if
18      Record the best solution obtained so far
19  end
```

2.2 The considered four objective functions for the optimization of FULLMAP

Chaotic maps are frequently employed in IMEPs to generate a diverse sequence in accordance with the control parameter and initial value. The pixels of image to be encrypted are hereby scrambled and manipulated through the generated sequence by chaotic maps. In order to explain the objective functions for the chaotic map, the following 1D conventional logistic map is given.

$$v_{i+1} = uv_i(1 - v_i),\ \ v_i \in (0, 1) \tag{5}$$

where $u \in [0, 4]$ is the control parameter (growing rate) and v_i is the initial value. We need appropriate objectives evaluating chaotic performance of the map in the optimization process.

2.2.2 Entropy

The other potent approach that can be considered for the optimization is the entropy of the sequence of the chaotic map. The entropy for the evaluation is applied as follows:

$$Y = floor(256v_i) \tag{7}$$

$$H(Y) = \sum_{i=0}^{255} p(y_i) log_2 \frac{1}{p(y_i)} \tag{8}$$

where y is the information source of which probability is $p(y_i)$. Equation (7) was used to extend range of $v_i \in [0, 1]$ to $Y \in \{0, 1, 2, \ldots, 255\}$. For better chaotic performance of a map, the entropy of sequence should be maximized up to 8 which the maximum value entropy that it can take.

2.2.3 The 0–1 test

The 0–1 test was developed for measuring the growth rates of trajectory of a chaotic dynamical system [60]. It simply detects the occurrence of non-regular stationary responses of any sequence of a dynamical system with respect to the 2D Euclidean group. Assume that the input of the test is a 1D time series $\phi(n)$ used to drive the 2D system [24].

$$p(n+1) = p(n) + \phi(n)cos(cn) \tag{9}$$

$$q(n+1) = q(n) + \phi(n)sin(cn) \tag{10}$$

where $c \in (0, 2\pi)$ is fixed. Define the time-averaged mean square displacement

$$M(n) = \lim_{N=\infty} \frac{1}{N} \sum_{j=1}^{N} \left([p(j+n) - p(j)]^2 + [q(j+n) - q(j)]^2 \right),\ n = 1, 2, \ldots \tag{11}$$

and its growth rate

$$K = \lim_{n=\infty} \frac{\log M(n)}{\log n} \tag{12}$$

It takes either the value $K \approx 0$ signifying non-chaotic system or the value $K \approx 1$ referring fully chaotic system.

2.2.4 The correlation coefficient

Correlation coefficient of a ciphertext image is a crucial for evaluation of an IMEP. It can be also used to evaluate the chaotic performance of a map. In order to directly utilize the correlation coefficient as an objective function, a test image matrix 512×512 with totally zero entity is considered as a black image, and it is encrypted through the operations of IMEP which is outlined in Sect. 4.2. Then the correlation coefficients of the ciphertext in three directions horizontal, vertical and diagonal are calculated as follows:

$$r_{xy} = \frac{E[x - E(x)][y - E(y)]}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N} \left[(x_i - E(x)\right]^2$. x_i and y_i are the pixel's values of i-th pair of the adjacent pixels, and N is the number of the pixel samples that randomly selected from the ciphertext image.

The chaotic map will be optimized by maximizing LE, H and K, and minimizing r_{xy}. Therefore, it would be optimized entirely by taking into account diverse evaluation approaches.

2.3 The model of FULLMAP and implementation of ABC

The main aim of the study is to achieve a fully chaotic map through the multi-objective optimization. It is observed from the literature reviewed elaborately in Sect. 6, and the suggested chaotic maps were built on the well-known mathematical concept such as trigonometry (sine, cosine), iterative polynomial or series, e.g., logistic [17–22], sine/cosine [17, 23–26], Chebyshev [26], Lorentz [28, 29], Henon [25, 27], etc. They were conformed for chaotic map to generate complex sequences. None of them was subjected to an optimization process for determining any coefficient or mathematical operations. Therefore, we have attempted to optimally form a hyperchaotic map and its coefficients according to effective objective functions, i.e., to constitute a fully optimized chaotic map, FULLMAP. To this end, it was started to optimize simple map models that inspired by the existing chaotic maps in which a few decision variables were inserted to be optimized. While the models of chaotic maps were being essayed, the decision variables were being optimized for minimizing the weighted multi-objective objective function. The decided model for FULLMAP in which eight decision variables were embedded, giving the lowest objective value, was conceived with the best in trial given below:

$$v_{i+1} = mod((\alpha_1 + \alpha_2 uv_i)(exp(\alpha_3) + \alpha_4 w_i), 1) \tag{14}$$
$$w_{i+1} = mod((\alpha_5 + \alpha_6 uw_i)(exp(\alpha_7) + \alpha_8 v_{i+1}), 1)$$

The model involves eight unknown coefficients $\alpha_j,\ j \in [1, 8]$, regarding as the decision variables in the optimization. A flowchart related to the implementation of ABC to the derive FULLMAP is depicted Fig. 2. In accordance with the flowchart, the decision variables were then optimally determined for improving the following four objectives including LE, H, K and r_{xy}.

$$of_l = \left\{ of_1 = \overline{LE}, of_2 = \overline{H}, of_3 = \overline{K}, of_4 = \overline{r_{xy}} \right\},\ l = 1, 2, \ldots, 4 \tag{15}$$

where $\overline{LE}$, $\overline{H}$ and $\overline{K}$ are, respectively, the mean of LE, H and K, and $\overline{r_{xy}}$ is the mean of correlation coefficient for the three directions. The four objective functions compose a single minimizing weighted objective function as given below:

$$OF = w_1 \frac{1}{of_1} + w_2(8 - of_2) + w_3(1 - of_3) + w_4 of_4 \tag{16}$$

where w_i, $j = 1, 2, .., 4$ are the weighting factors taken as unity (1) in this study. Meanwhile, different weighting factors were also tried during the optimization process. The best results were achieved with the proposed strategy. The three objective functions were treated to be minimized by

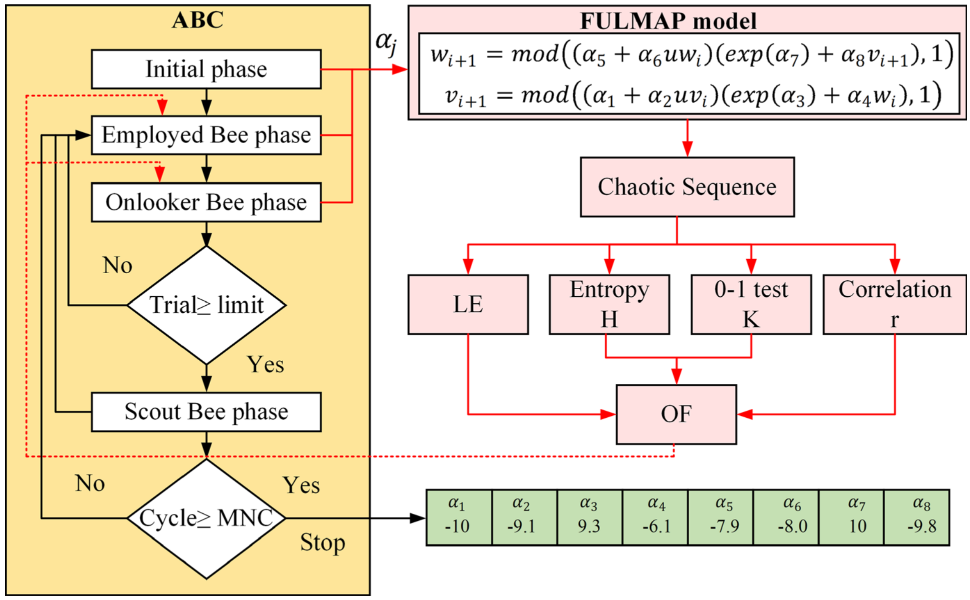


Fig. 2 A flowchart regarding the implementation of ABC to derive FULLMAP

taking $1/of_1$, $8 - of_2$ and $1 - of_3$, where 8 and 1 are, respectively, the maximum values of the entropy and 0–1 test that they can get. In initial phase, candidate decision variables α_j were randomly generated as NP = 30 using Eq. (1) between x_{max} and x_{min} that are set as 10 and -10 in this study, respectively. According to these variables, their fitness values were computed using Eq. (3) based on the weighted objective function as follows:

$$fit_i = \frac{1}{1 + OF_i(x)} \tag{17}$$

fit_i is the fitness value of every candidate decision variable. In employed bee phase, the population of decision variable were in turn modified using Eq. (2), and their fitness values were evaluated with Eq. (3). Then, some variables were randomly selected based on the worthiness of them utilizing Eq. (4). In onlooker bee phase, the selected ones were also modified using Eq. (2). Afterward, a greedy selection is performed for the better ones. If trial reached to limit = 20, scout bee phase took place where a totally new decision variable was generated using Eq. (1). The best decision variable that had been achieved so far is recorded. Thereafter, if the number of cycles was equal to the MNC = 500, ABC was stopped and the best decision variable was given as outcome.

The convergence tendency of the optimization cycles is plotted in Fig. 3. After approximately 200 cycles, the optimization converges to the final objective value of 0.1425. In the optimization, decision variables embedded in FULLMAP were rounded to the nearest tenth for the sake of simplicity. The resultant FULLMAP in which the optimized variables are substituted is given below:

$$v_{i+1} = mod((-10 - 9.1uv_i)(exp(9.3) - 6.1w_i), 1) \tag{18}$$

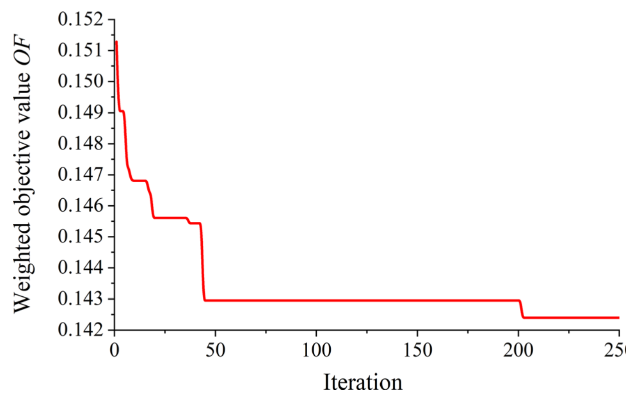


Fig. 3 The convergence tendency of the optimization of FULLMAP using ABC

$$w_{i+1} = mod((-7.9 - 8.0uw_i)(exp(10) - 9.8v_{i+1}), 1)$$

where u is the control parameter, and v_i and w_i are the initial values of FULLMAP.

3 The measurement and verification of FULLMAP

The spatial dynamic distribution of FULLMAP was examined from the perspective of bifurcation in Fig. 4 as compared with that of the conventional logistic map Eq. (5). The bifurcation shows the diversity and ergodicity a chaotic map versus according to the control parameter. The scatters in the graph are called bifurcation point. It is desired that a fully chaotic map can generate sudden points across the control parameters without any space. As the

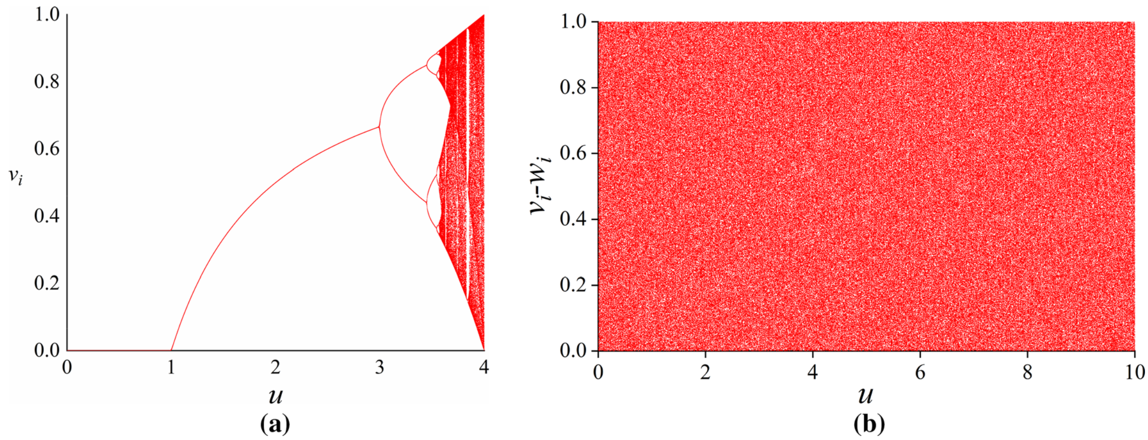


Fig. 4 Bifurcation diagrams: **a** Logistic map, **b** FULLMAP

logistic map generates only for $u \in [3.57, 4)$, FULLMAP does for all u (displayed up to 10).

3D phase space chaotic trajectories able to display the dynamic behavior of a chaotic map in multi-dimensional phase space are revealed in Fig. 5 for FULLMAP as well as compared with three different chaotic maps reported elsewhere [24, 36, 38]. A fully dynamic system is expected to occupy whole phase spaces without any aggregation and repetitive paths. It is evident that FULLMAP not only uniformly but also totally occupies all over the space rather than the others [24, 36, 38] which cluster on various curling paths. Such scattered trajectory implies that one could not anticipate the subsequent steps.

The chaotic performance of FULLMAP was measured regarding the LE, 0–1 test, sample entropy (SE) and permutation entropy (PE) in Fig. 6. Note that the SE and PE [61, 62] are independent metrics, which did not use as objective functions in the optimization. They are also compared with extent state-of-the-art results [17, 23, 24, 26, 36, 38, 59] to validate the chaotic performance. In Fig. 6a, their LE is illustrated. Given that the LE of a map must be positive for having chaotic capability, and a chaotic map is appreciated as better as how LE is high and stable. The LE of the conventional logistic map is positive and less than one only for $u \in [3.57, 4)$. Even the fact that the best of the reported LEs is about positive 5 [23, 26], the LE of FULLMAP outstands among the reported ones since it is 13 positively. The 0–1 tests of them are revealed in Fig. 6b, assessing the growth rates of trajectory. Hence, the 0–1 test can determine non-dynamic region of a system by giving zero result. It is clearly seen that the 0–1 test of FULLMAP seems the best with almost 1 among the reported ones. In Fig. 6c, the SE of the dynamic systems is given, which is able to measure the complexity of a dynamic system. It can be used to degrade the similarity of the sequence generated by a chaotic map. Suppose that $\{v_1, v_2, v_3, v_4, \ldots, v_N\}$ is a sequence, $v_m(i) = \{v_i, v_{i+1}, \ldots, v_{i+m+1}\}$ is a template vector, m is the dimension and r is the acceptance tolerance. Hence, the SE can be defined as

$$SE(m, r, N) = -log\frac{A}{B} \quad (19)$$

where A and B, respectively, represent the number of vectors for $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$, and $d[X_m(i), X_m(j)]$ is the Chebyshev distance between $X_m(i)$ and $X_m(j)$. The complexity of a sequence is evaluated as how SE is high as better. The SE variation of FULLMAP is illustrated in Fig. 6c including comparison with the literature. FULLMAP evidently shows higher complexity with about 2.2 than the state of the arts. PE is also a precise measurement of the complexity of a dynamic system [62]. The higher the PE, the more complex the sequence of a chaotic map. The PE of FULLMAP which is computed for embedding dimension 2 and time delay 1 is comparatively plotted in Fig. 6d. Given that the PE can get a maximum value of 1 for these parameters. The PE of FULLMAP is the highest with value of 1 within the others. Eventually, FULLMAP has the best results for all considered measurements thanks to the optimal chaotic map properties.

4 The proposed IMEP with FULLMAP

In this section, obtaining the initial values v, w and control parameters u of FULLMAP is outlined in Algorithm 2. They are obtained from the main key to produce chaotic sequences via FULLMAP. Then, the generation of sequence via FULLMAP is expressed in Algorithm 3. The chaotic sequences are employed in IMEP operated through permutation and diffusion in Algorithm 4.

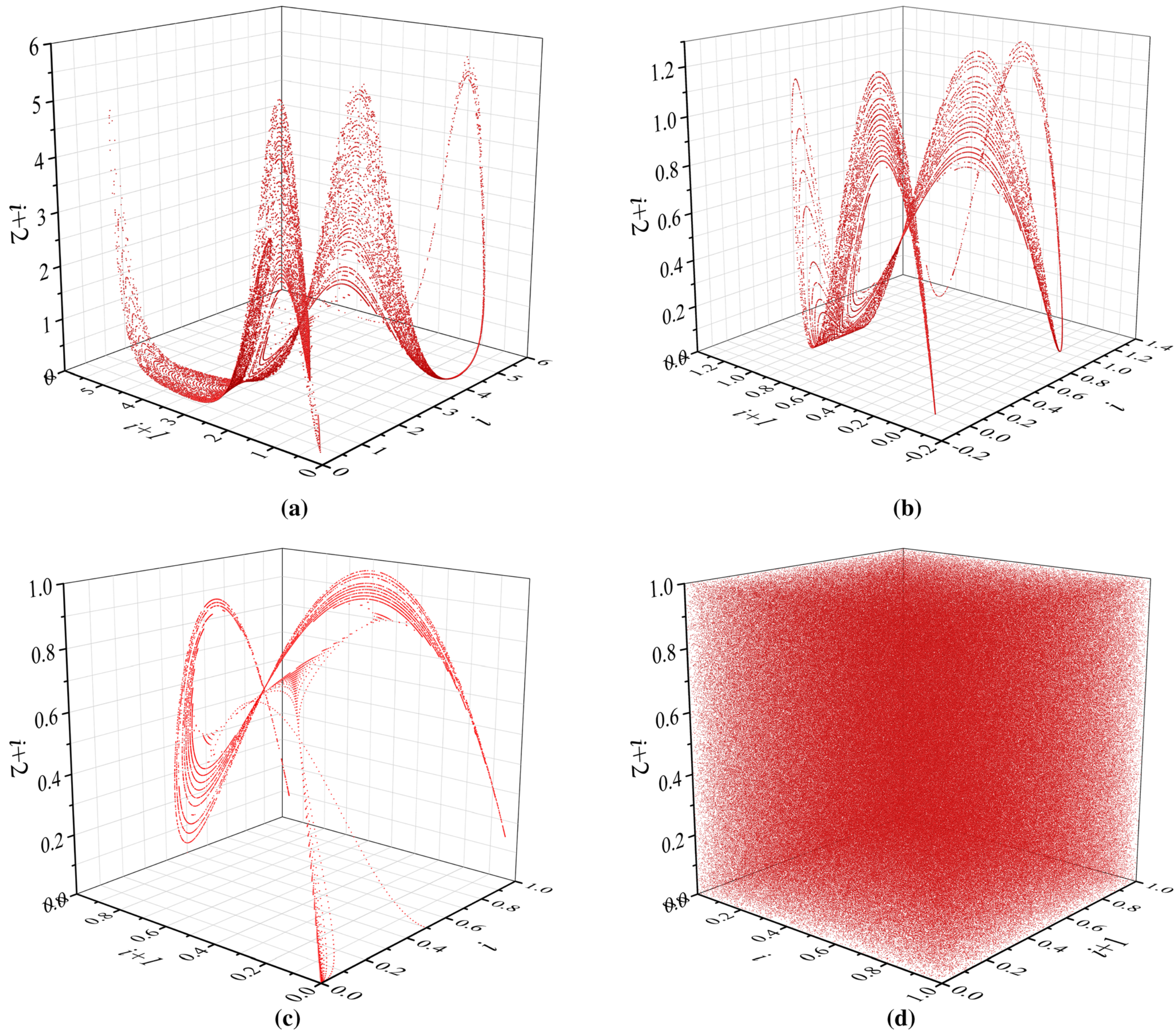


Fig. 5 3D chaotic trajectory: **a** [24], **b** [36], **c** [38], **d** FULLMAP

4.1 The initial values and control parameters obtaining from the keys

Obtaining the initial values and control parameters is clarified in Algorithm 2, and accordingly, its flowchart is illustrated step by step in Fig. 7 through an example for the Lena image. In IMEP, first the public key B was acquired from the plaintext image using SHA-512/MD5 hash value (Line 1). The plaintext image was imported to form vector A with size of $m \times n$. The public key is produced by calculating three vectors: total row, total column and total diagonal vectors of the plaintext image. Total row vector size of m is the sum of the pixel values of all rows. Total column vector size of n is the sum of the pixel values of all columns. Total column vector size of $m + n - 1$ is the sum of all diagonal pixel values. The public key matrix B is generated through the combination of SHA-512 and MD5 hash from these three vectors. Then, a secret key C is constructed (Line 2) and a main key D is got by XOR operation between the public and secret keys (Line 3). Afterward, the main key was divided into four submatrices and the columns of each submatrix in self were subjected to a series of transaction $\mathrm{mod}(\mathrm{sum}(E, 2), 2)$ (Line 5). The outcome of each submatrix 8×1 was combined to form E matrix size of 8×8 (Line 6). The binary matrix F was converted to a decimal matrix F (Line 7). $h_i = \frac{\mathrm{mod}(f_{1i} * sum(F), 256)}{256}$ were computed for the initial values (Line 9), and they were got from $v_1 = h_1$, $v_2 = h_3$, $w_1 = h_2$ and $w_2 = h_4$ as $V = [\,v_1 \quad v_2\,]$ and $W = [\,w_1 \quad w_2\,]$ (Line 11). A

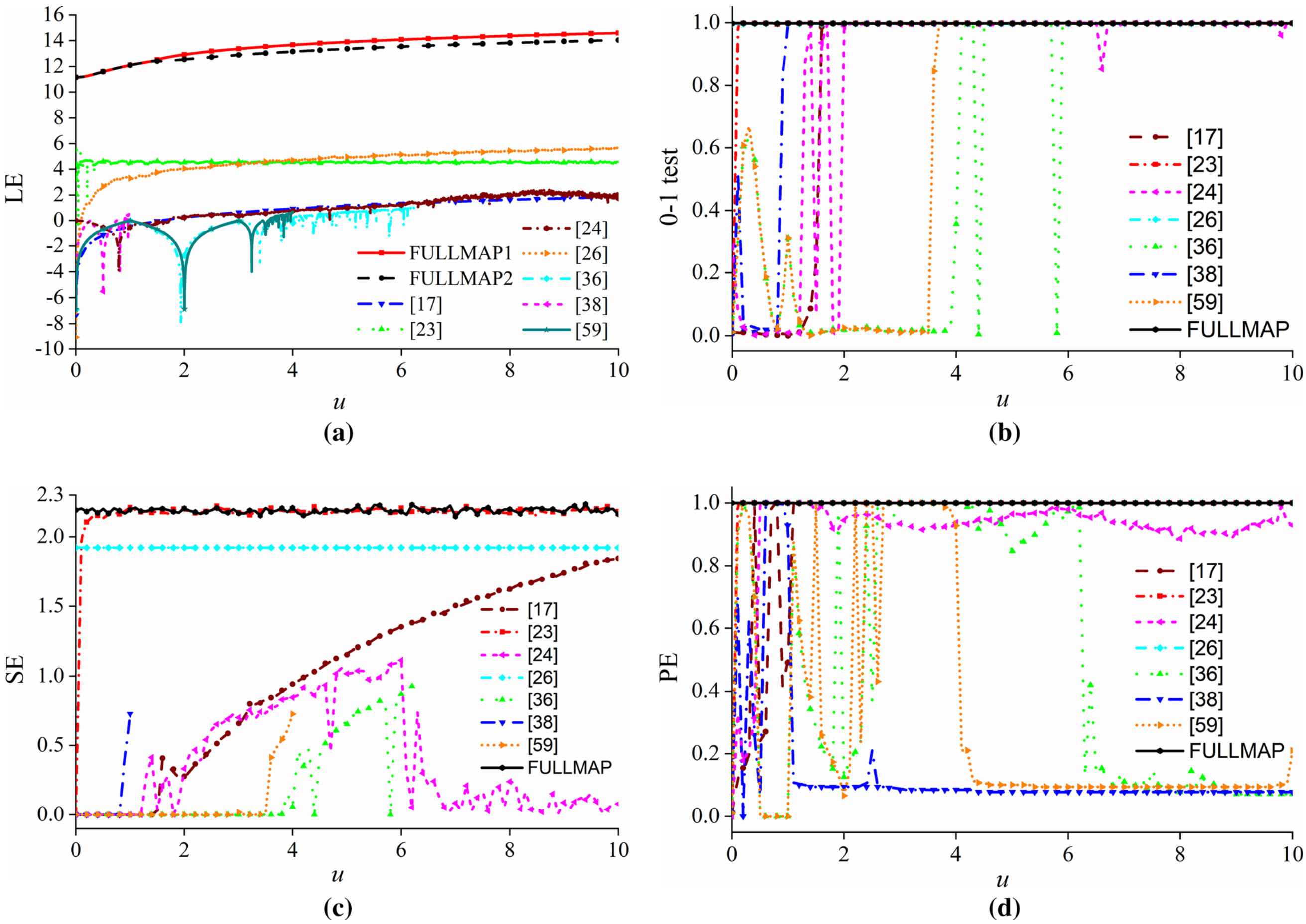


Fig. 6 The measurements of FULLMAP and comparison with the literature: **a** LE, **b** the 0–1 test, **c** SE, **d** PE

G matrix was computed from F matrix as $G = \mathrm{mod}((sum(F(5:6))\ \ sum(F(7:8))) * sum(F)), 256)$ (Line 12). Eventually, the control parameters $U = [u_1 \quad u_2]$ were achieved by dealing $u_1 = \frac{g_{1,1}}{256} + \mathrm{mod}(g_{1,1}, 10)$ and $u_2 = \frac{g_{1,2}}{256} + \mathrm{mod}(g_{1,2}, 10)$ (Line 13).

Algorithm 2: The initial values and control parameters obtaining from the main key

Start-Point-Calculator (A)

1 Compute a public key $B := [b_{1p}]_{1\times512}$ by SHA-512/MD5 hash value from the plaintext image
2 Construct a secret key $C := [d_{1p}]_{1\times512}$ being a binary row matrix
3 $D = B$ XOR C
4 Reshape D to 8×8×8 in shape
5 $E = \mathrm{mod}(\mathrm{sum}(D, 2), 2)$
6 Reshape E to 8×8 in shape
7 $F = [128\ 64\ 32\ 16\ 8\ 4\ 2\ 1] * E$
8 **for** $i = 1$ to 4
9 $$h_i = \frac{\mathrm{mod}(f_{1i} * \mathrm{sum}(F), 256)}{256}$$
10 **end**
11 $v_1 = h_1;\ v_2 = h_3; w_1 = h_2; w_2 = h_4;$
12 $G = \mathrm{mod}\left(\left(\mathrm{sum}(F(5{:}6))\ \mathrm{sum}(F(7{:}8))\right) * \mathrm{sum}(F)\right), 256)$
13 $u_1 = \frac{g_{11}}{256} + \mathrm{mod}(g_{11}, 10); u_2 = \frac{g_{12}}{256} + \mathrm{mod}(g_{12}, 10)$

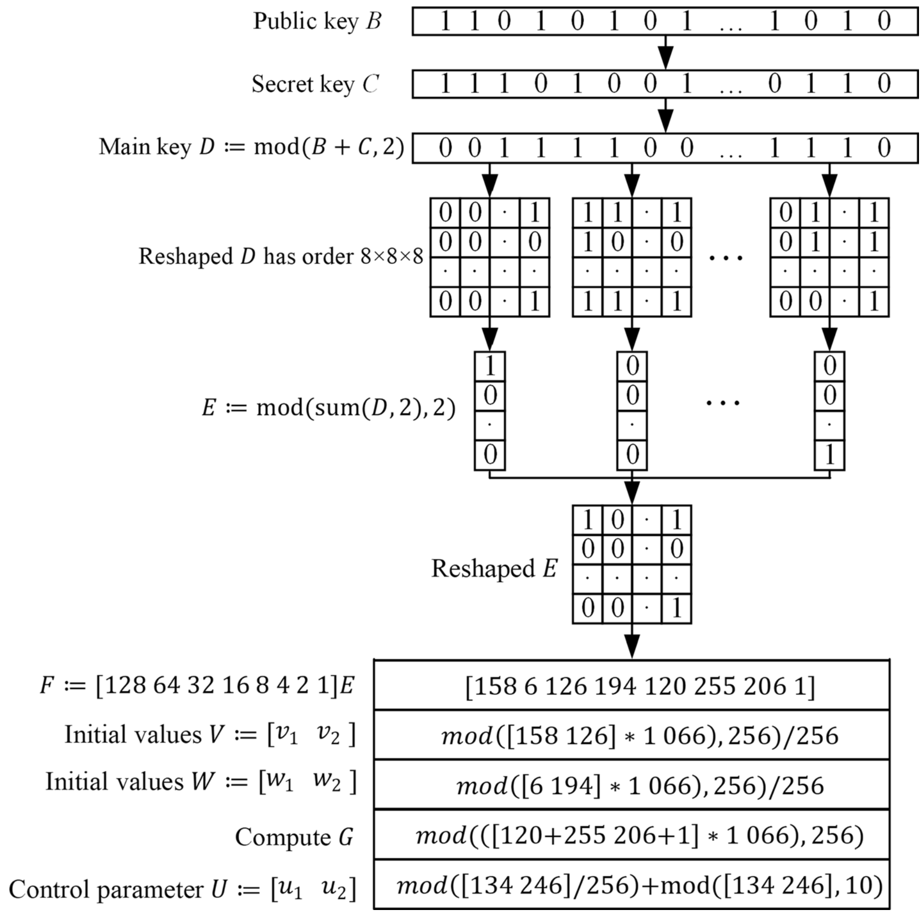
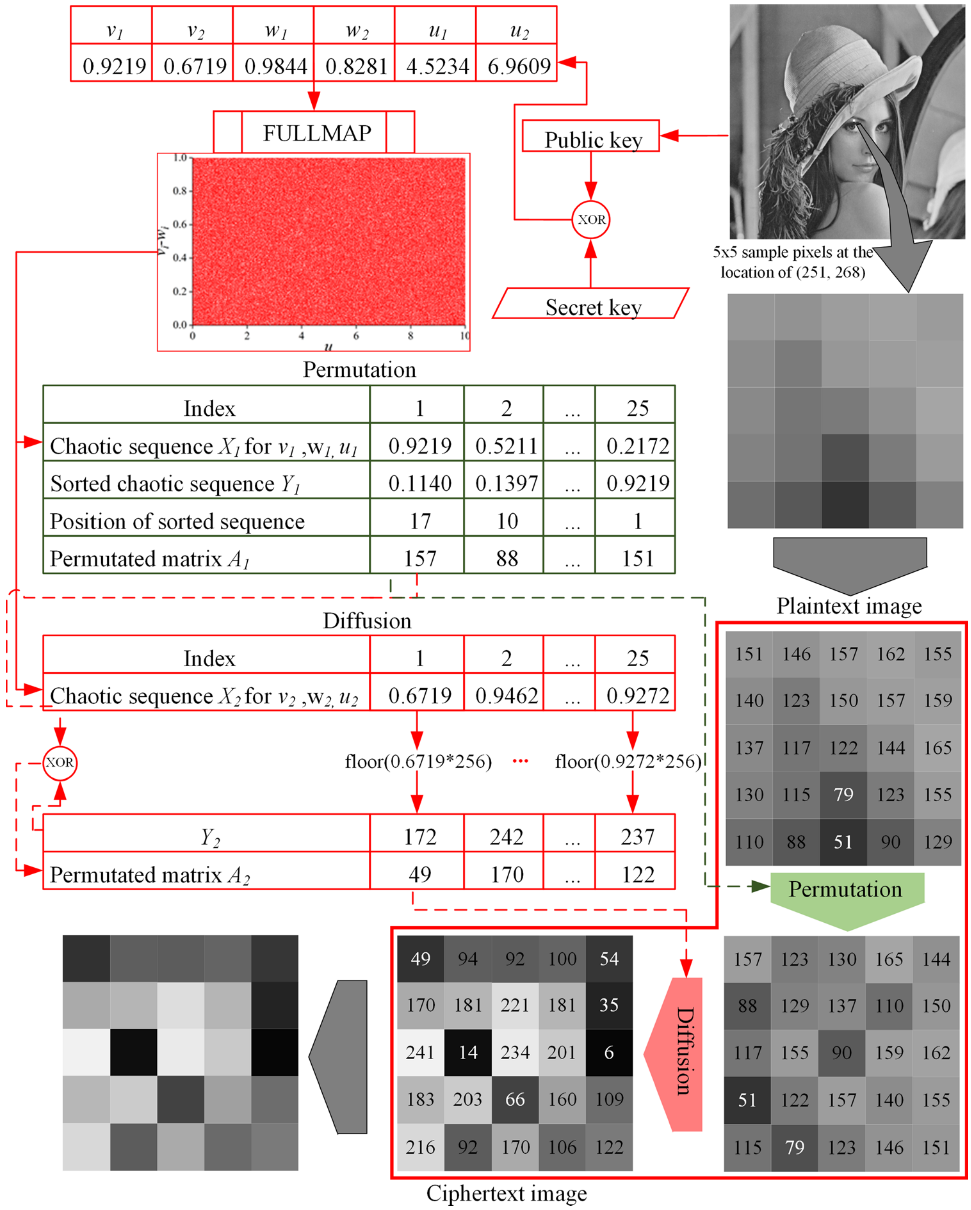


Fig. 7 Obtaining the initial values and control parameters

4.2 The encryption operations of IMEP

The generation of chaotic sequences via 2D FULLMAP using the initial values and control parameters is explained in Algorithm 3, where y_{i+1} and z_{i+1} stand for the 2D FULLMAP given in Eq. (18). They are intertwined to generate a chaotic sequence X in Algorithm 3: Line 5–7. IMEP across permutation and diffusion is elucidated step by step in Algorithm 4, and it is illustrated in Fig. 8 for an example of 5 × 5 pixel sample of the Lena image. The pixels were scrambled positionally and manipulated in pixel's values across the two operations, permutation and diffusion, governed by FULLMAP. First, a public key B from the plaintext image and a secret key C were acquired, and a main key D was got from the two keys. Then, in Algorithm 4: Lines 1 and 7, the initial value V and W and control parameter U achieved by Algorithm 2 were used as input to FULLMAP for generation of the chaotic sequences X_1 and X_2. In permutation, the chaotic sequence matrix X_1 was sorted in ascending order to form matrix Y_1 (Algorithm 4: Line 2). Afterward, the positions of the pixels were shuffled in accordance with the position of the sorted sequence, and thus, the permutated matrix A_1 arises (Algorithm 4: Line 3–6). In diffusion, a row matrix Y_2 was obtained to use in the diffusion operation (Algorithm 4: Line 8). The permutated matrix A_1 was then incurred an XOR operation with the matrix Y_2 in order for diffusing the pixel values (Algorithm 4: Line 9). Finally, the diffused matrix A_2 was accomplished as the ciphertext image (Algorithm 4: Line 10).

Fig. 8 The overview of the proposed IMEP with FULLMAP step-by-step for an illustrative example



Algorithm 3: The generation of chaotic sequence via 2D FULLMAP

2D-FULLMAP (y_1, z_1, u)

$j = 1$
for $i = 1$ to $\frac{mn}{2} + 1$
  $y_{i+1} = \mathrm{mod}\left((-10 - 9.1uy_i)(e^{9.3} - 6.1z_i), 1\right)$
  $z_{i+1} = \mathrm{mod}\left((-7.9 - 8.0uz_i)(e^{10} - 9.8y_{i+1}), 1\right)$
  $x_j = y_{i+1}$
  $x_{j+1} = z_{i+1}$
  $j = j + 2$
end
$X = [x_{ij}]_{1\times mn}$

Algorithm 4: Encryption operations of IMEP with FULLMAP

Image-Encryption (A, v_1, w_1, u_1)

$X_1 = $ 2D-FULLMAP (v_1, w_1, u_1) // $X_1 \coloneqq [x_{1r}^1]_{1\times mn}$ is the first chaotic sequence
$[Y_1\ P] = \mathrm{sort}(X_1)$ // $Y_1 \coloneqq [y_{1r}^1]_{1\times mn}$ is sorted X_1 in ascending order and $P \coloneqq [p_{1r}]_{1\times mn}$ is indices matrix of entries of Y_1 according to X_1
for $i = 1$ to mn
  $k = p_{1i}$
  $a_{1i}^1 = a_{1k}$
end
$X_2 = $ 2D-FULLMAP (v_2, w_2, u_2) // $X_2 \coloneqq [x_{1r}^2]_{1\times mn}$ is the second chaotic sequence
$Y_2 = \mathrm{floor}(256X_2)$ // $Y_2 \coloneqq [y_{1r}^2]_{1\times mn}$
$A_2 = A_1 \oplus Y_2$ //$A_2 \coloneqq [a_{1r}^2]_{1\times mn}$ is the diffused sequence obtain by XOR operation
Reshape to A_2 to $m\times n$ in shape //$A_2 \coloneqq [a_{ij}^2]_{m\times n}$ is the diffused matrix

Table 1 The numerical differences among ciphertext images with one-bit changed keys (Key 1 is the original)

Fig	One-bit changed keys	Difference with Fig. 9b (%)
9c	Key 2	99.6219
9d	Key 3	99.6131
9e	Key 4	99.6017
9f	Key 5	99.6074
Mean		99.6115

5 The comparative cryptanalyses

An IMEP is aimed at enhancing the resistant against potential cyberthreats through network attaches, namely denial-of-service, man-in-the-middle and phishing. Therefore, the security of an IMEP should be evaluated by simulating those cyberthreats [32]. The most reliable cryptanalyses are key-space, key sensitivity, entropy, histogram, correlation, differential attack, noise attack and cropping attack. These were performed on the well-known images with size 512 × 512. The encryption results were carried out via MATLAB R2020b running on a workstation with I(R) Xeon(R) CPU E5-1620 v4 @ 3.5 GHz, and 64 GB RAM. The results of the proposed IMEP with FULLMAP were also compared with some available state of the art [17, 18, 25, 26, 30, 35–37, 63–67].

5.1 Key-space

Brute force is the well-known cyberattack depending on prediction of the key by attempting numerous passwords. A ciphertext with a short key is indefensible to such attack in a short time. On the other hand, a longer key would resist for a long time and it would be impossible to predict the key if it has the proper length. Key-space analysis tests the proof ability to the brute-force attacks. Key-space analysis considers a key is secure; in case, it is longer than 2^{100} [68]. In our IMEP, a SHA 512-bit-length key was used, and thus, it is six floating numbers with 10^{15} precision, which is used as the initial values and control parameters of the FULLMAP. The key-space analysis is therefore $10^{15\times 6} = 10^{90} \cong 2^{298}$ that is much higher than the reference 2^{100}.

5.2 Key sensitivity

An IMEP must be sensitive to the key. It means that a minor change in the key should cause a major alteration in the ciphertext image for a secure IMEP. In order to analysis the key sensitivity, five secret keys which are one original key and its four different one-bit changed versions were utilized. The ciphertext images that are encrypted with these keys are shown in Fig. 9. At the same time, their differential images pixel by pixel are illustrated in Fig. 9(g), (h), (i), and (j). In this way, the number of pixels having the same pixel's values can be observed. The same pixel would seem black color due to zero difference. From the differential images, consequently, any black region is not seen.

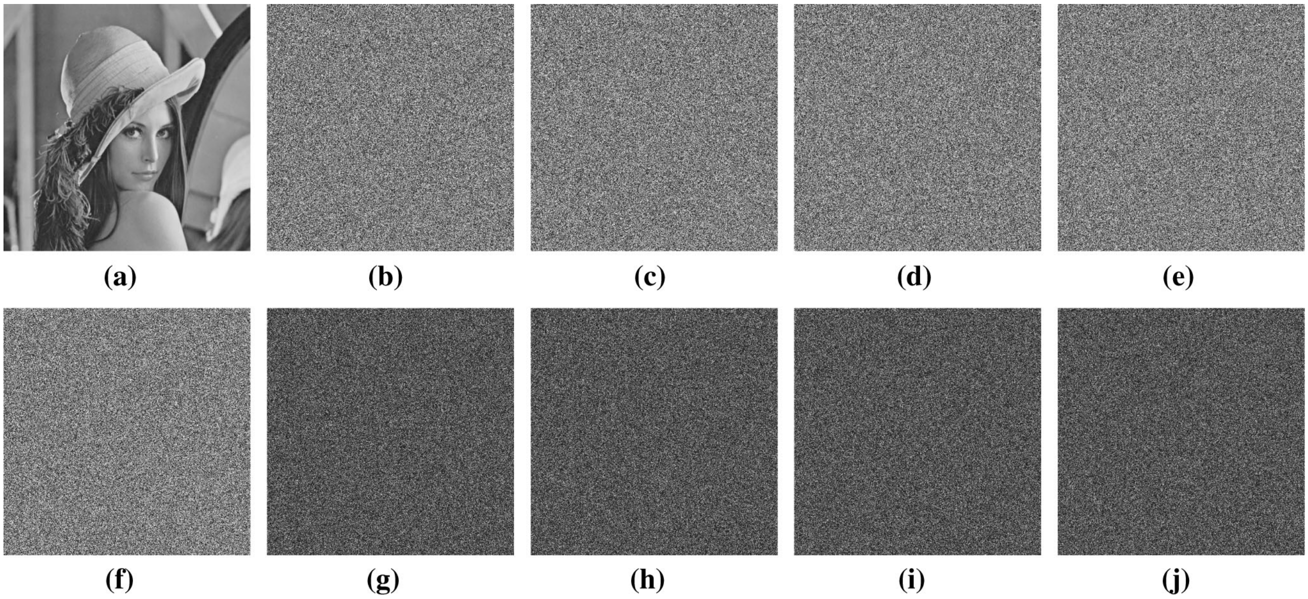


Fig. 9 Images for key sensitivity analysis: (**a**) Plaintext, (**b**) Ciphertext-Key 1, (**c**) Ciphertext-Key 2, (**d**), Ciphertext-Key 3 (**e**) Ciphertext-Key 4, (**f**) Ciphertext-Key 5; differential images: (**g**) Between (**b**) and (**c**), (**h**) Between (**b**) and (**d**), (**i**) Between (**b**) and (**b**), (**j**) Between (**b**) and (**f**)

Table 1 includes numerical results related to the distinctive level of the differential images to assess the key sensitivity. The distinctive levels were achieved as 99.6102%, 99.6257%, 99.6074% and 99.6028%, respectively, for Key 2, 3, 4 and 5, and mean of these levels as 99.6115%. It is evident that the proposed IMEP is very

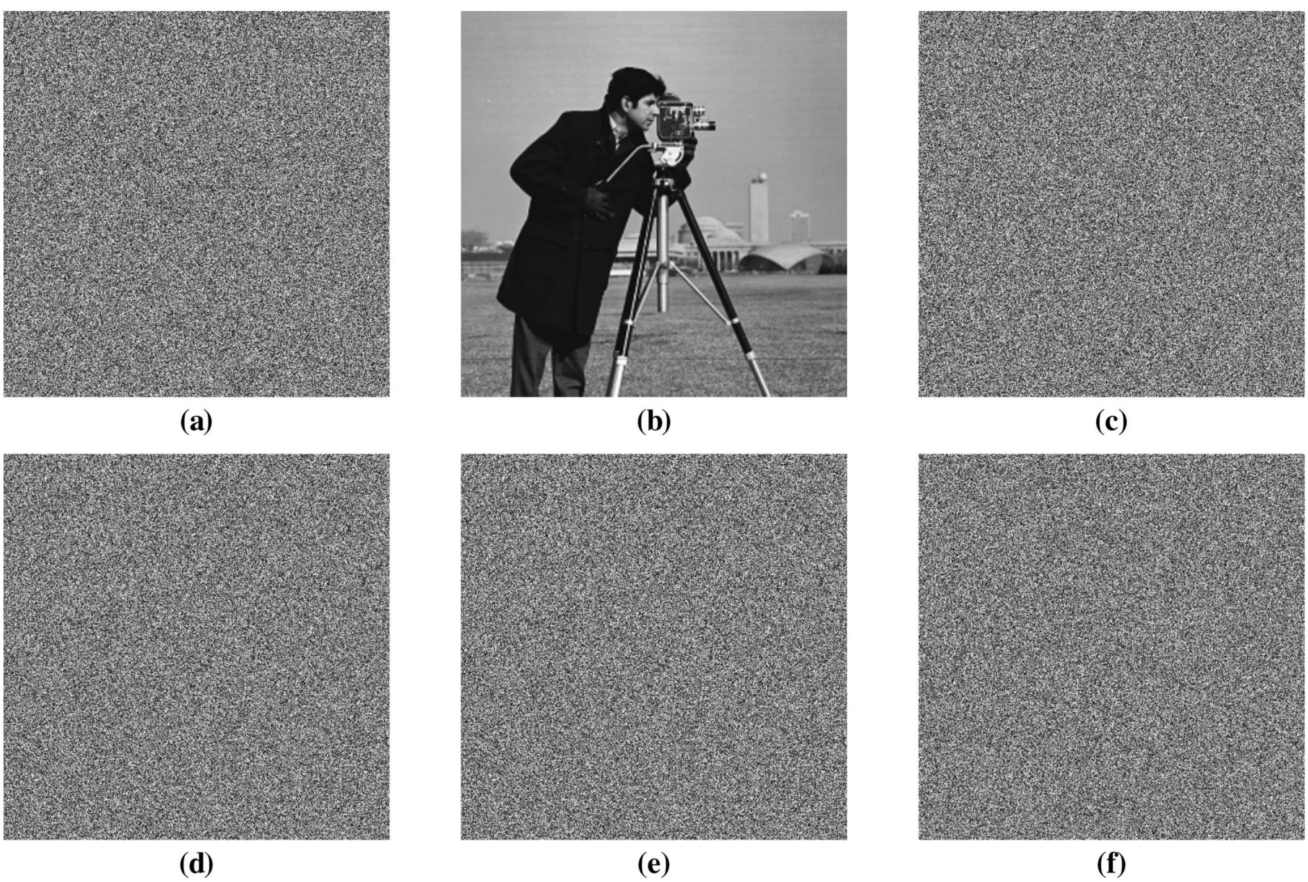


Fig. 10 Images for key sensitivity: (**a**) Ciphertext-Key 1 (original); decipher images: (**b**) Key 1, (**c**) Key 2, (**d**) Key 3, (**e**) Key 4, (**f**) Key 5

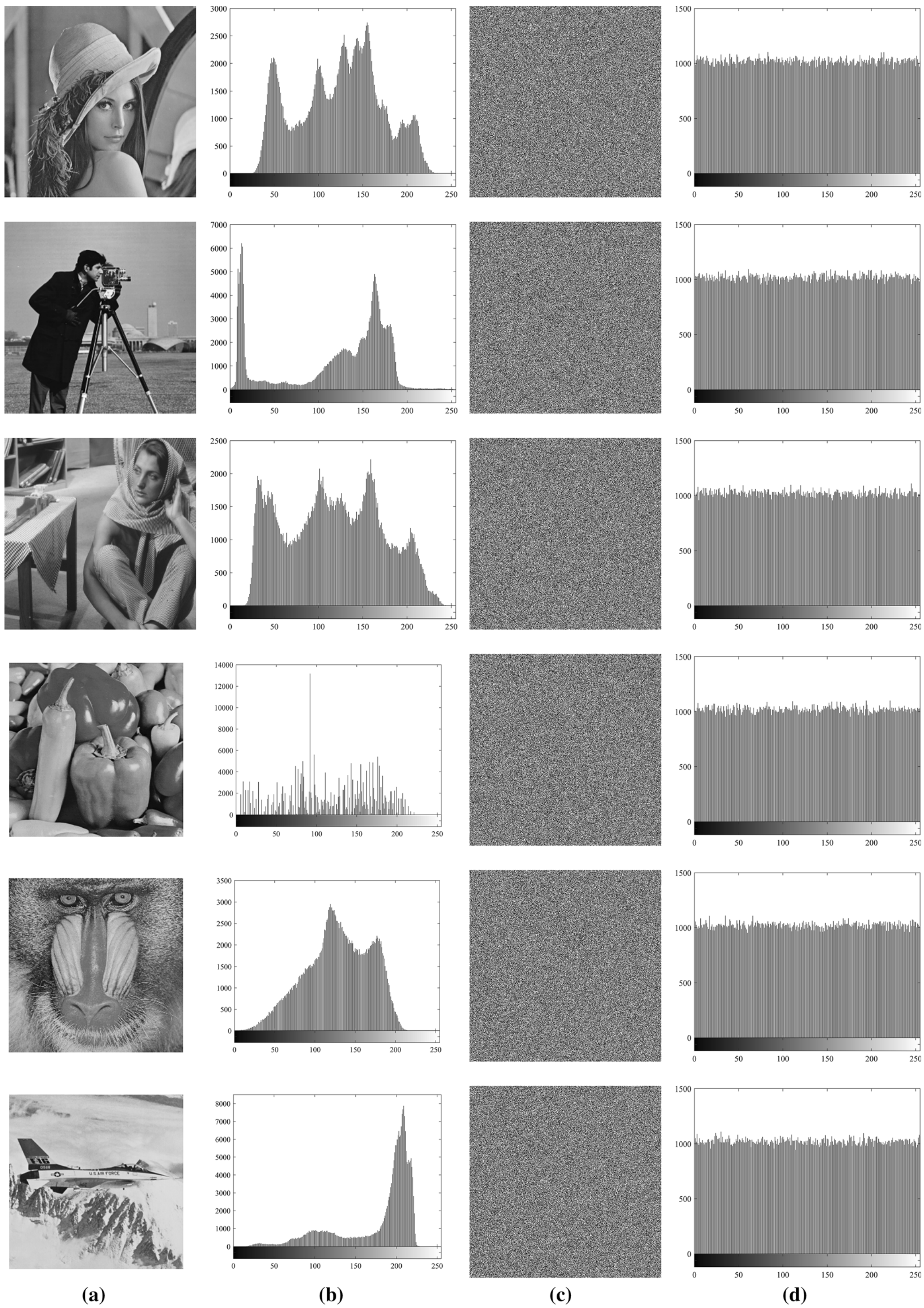


Fig. 11 Images and their histogram: **a** Plaintext, **b** Histogram of the plaintext images, **c** Ciphertext, **d** Histograms of ciphertext images

sensitive to the key thanks to the fully diversity of FULLMAP.

Moreover, it is desired to investigate whether the decrypted ciphertext images with the one-bit changed keys involve any information from the plaintext image or not. Therefore, the deciphered images with the original and one-bit changed keys are shown comparatively in Fig. 10. The ciphertext image with the original key is accurately decrypted as is expected, while the other decipher images are very complicated and far from the original plaintext image. This means that even if one-bit of the key is changed, the ciphertext image is completely altered.

Table 2 Variance and χ^2 test results of the test images

Test	Image	Lena	Cameraman	Peppers	Baboon	Barbara	Airplane
var	Plaintext	6,333,788.75	1,674,120.58	2,196,605.10	845,463.33	3,821,955.00	2,832,714.39
	Ciphertext	945.86	971.29	959.39	955.19	968.24	956.95
χ^2	Plaintext	158,344.71	418,530.14	549,151.27	211,365.83	95,548.87	708,178.59
	Ciphertext	236.66	241.87	238.90	237.86	245.38	238.30

Table 3 Entropies of the plaintext and ciphertext images by the proposed IMEP with the FULLMAP

Image	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
Plaintext image	7.4455	7.0479	7.6321	6.7624	7.2925	6.7135
Ciphertext image	7.9995	7.9995	7.9995	7.9995	7.9995	7.9995

Table 4 The entropies of the ciphertext images and the comparison with the literature

Ciphertext image	Ref. [35]	Ref. [17]	Ref. [36]	Ref. [37]	Ref. [25]	Ref. [26]	Ref. [30]	FULLMAP
Lena	7.9994	7.9993	7.9993	7.9975	7.9994	7.9970	7.9982	7.9995
Cameraman	7.9970	–	–	–	7.9993	7.9973	–	7.9995
Barbara	–	7.9992	–	7.9985	–	–	7.9981	7.9995
Peppers	–	–	7.9994	–	7.9993	7.9969	–	7.9995

5.3 Histogram

Histogram is able to represent a graphical representation of the pixel's values versus that of sequence. Thence, the uniformity of image pixels and the manipulation performance of FULLMAP can be thus examined. The manipulation performance is evaluated as high as how histogram is uniform. The histograms of the test images Lena, Cameraman, Barbara, Peppers, Baboon and Airplane and the related ciphertext images are observed in Fig. 11. As can be seen that the proposed IMEP with FULLMAP uniformly modifies the pixel's value. Because the histograms are sufficiently monotone. It implies that the IMEP is resistant to the statistical attacks and one cannot deduce any information from the ciphertext images.

In order to further examine the distribution of the pixels' values, variance and χ^2 tests of the histogram can be computed. For a grayscale image, variance and χ^2 tests are computed as given below:

$$var(\boldsymbol{X}) = \frac{1}{n^2}\sum_{i=0}^{n}\sum_{j=1}^{n}\frac{1}{2}(x_i - x_j)^2 \tag{20}$$

$$\chi^2 = \sum_{i=0}^{255}\frac{(n_i - n/256)^2}{n/256} \tag{21}$$

where n_i is the repetition frequency of the pixel's value i and n is the number of total pixels. $n/256$ is the expected repetition frequency of every pixel's value. $X = \{x_1, x_2, \ldots, x_{256}\}$ is the vector including the histogram's pixel's values. x_i and x_j are the numbers of pixels whose gray values are equal to i and j, respectively. For high uniformity, the variance is expected to be lower as much as possible. On the other hand, $\chi^2(0.05; 255)$ should be lower than 293.25 for verifying the significant level 0.05 of χ^2 test [69]. The results regarding the variance and χ^2 test are tabulated in Table 2 for the test images in Fig. 11. The proposed IMEP with FULLMAP is hence corroborated through the results for all the test images.

Table 5 Correlation coefficients of the test ciphertext images

Direction	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
Horizontal	16×10^{-6}	-78×10^{-6}	-79×10^{-6}	-21×10^{-6}	-44×10^{-6}	56×10^{-6}
Vertical	-67×10^{-6}	37×10^{-6}	-51×10^{-6}	-13×10^{-5}	57×10^{-6}	22×10^{-5}
Diagonal	-15×10^{-7}	98×10^{-6}	-73×10^{-7}	28×10^{-6}	10×10^{-5}	-72×10^{-7}

Table 6 The correlation coefficients of the ciphertext images and the comparison with the literature

Ciphertext image	Dir	Ref. [35]	Ref. [17]	Ref. [36]	Ref. [37]	Ref. [25]	Ref. [26]	Ref. [30]	FULLMAP
Lena	H	73×10^{-5}	13×10^{-3}	10×10^{-4}	27×10^{-4}	32×10^{-4}	22×10^{-4}	14×10^{-4}	16×10^{-6}
	V	44×10^{-5}	17×10^{-3}	-15×10^{-4}	13×10^{-4}	16×10^{-4}	13×10^{-4}	14×10^{-4}	-67×10^{-6}
	D	36×10^{-5}	67×10^{-5}	26×10^{-4}	11×10^{-4}	23×10^{-4}	8×10^{-4}	12×10^{-4}	-15×10^{-7}
Cameraman	H	93×10^{-4}	–	–	–	14×10^{-4}	39×10^{-4}	–	-78×10^{-6}
	V	10×10^{-5}	–	–	–	2×10^{-4}	7×10^{-4}	–	37×10^{-6}
	D	31×10^{-4}	–	–	–	35×10^{-4}	86×10^{-4}	–	98×10^{-6}
Barbara	H	–	-70×10^{-4}	–	-13×10^{-4}	–	–	12×10^{-4}	-79×10^{-6}
	V	–	-79×10^{-4}	–	43×10^{-4}	–	–	27×10^{-4}	-51×10^{-6}
	D	–	-22×10^{-3}	–	10×10^{-4}	–	–	-10×10^{-4}	-73×10^{-7}
Peppers	H	–	–	7×10^{-5}	–	6×10^{-4}	1×10^{-4}	–	-21×10^{-6}
	V	–	–	43×10^{-4}	–	38×10^{-4}	-26×10^{-4}	–	-13×10^{-5}
	D	–	–	-18×10^{-4}	–	10×10^{-4}	-23×10^{-4}	–	-28×10^{-6}

Dir: Direction, H: Horizontal, V: Vertical, D: Diagonal

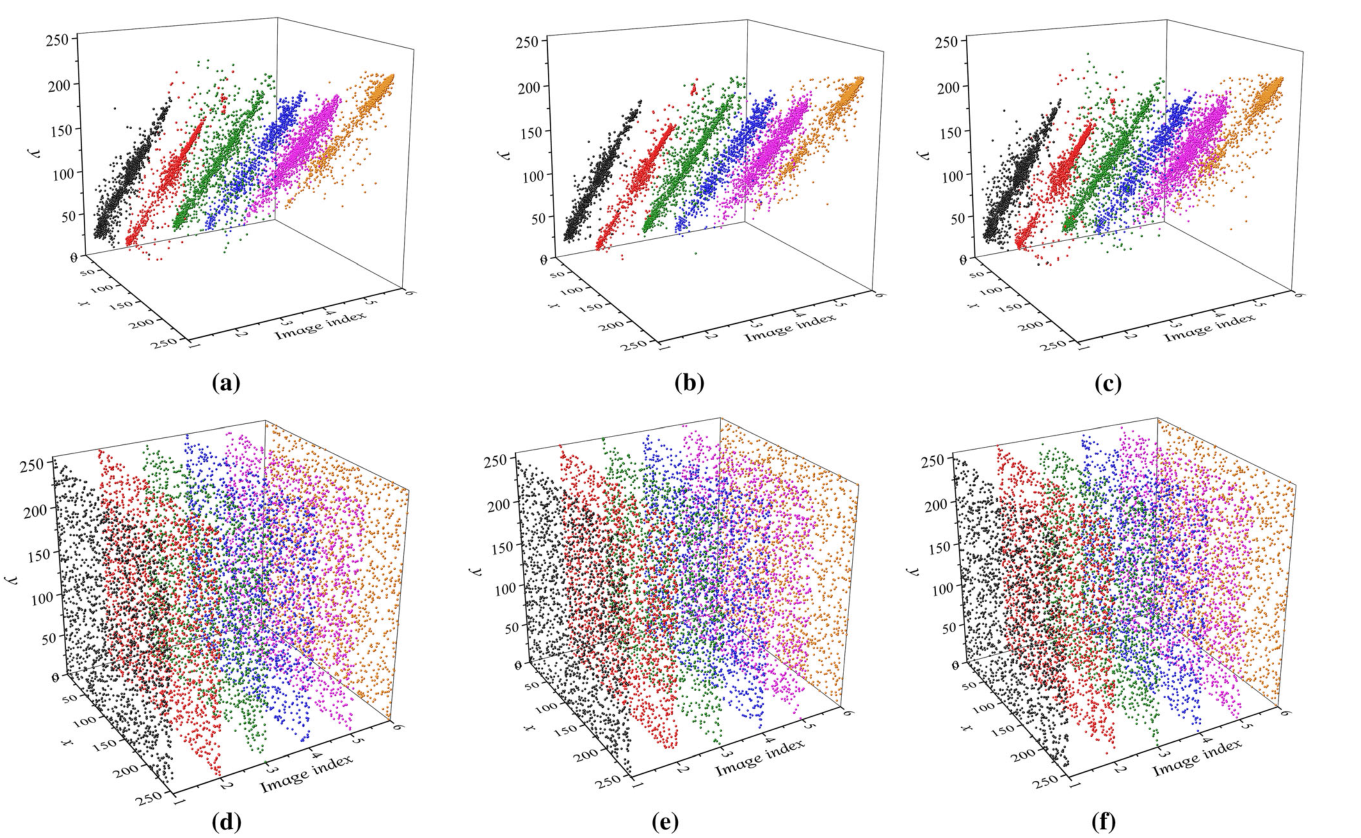


Fig. 12 The correlation distribution of the test images for the three directions: **a** Plaintext image-Horizontal, **b** Plaintext image-Vertical, **c** Plaintext image-Diagonal, **d** Ciphertext image-Horizontal, **e** Ciphertext image-Vertical, **f** Ciphertext image-Diagonal *(Image index of Lena:1, Cameraman: 2, Barbara: 3, Peppers: 4, Baboon: 5, Airplane: 6)*

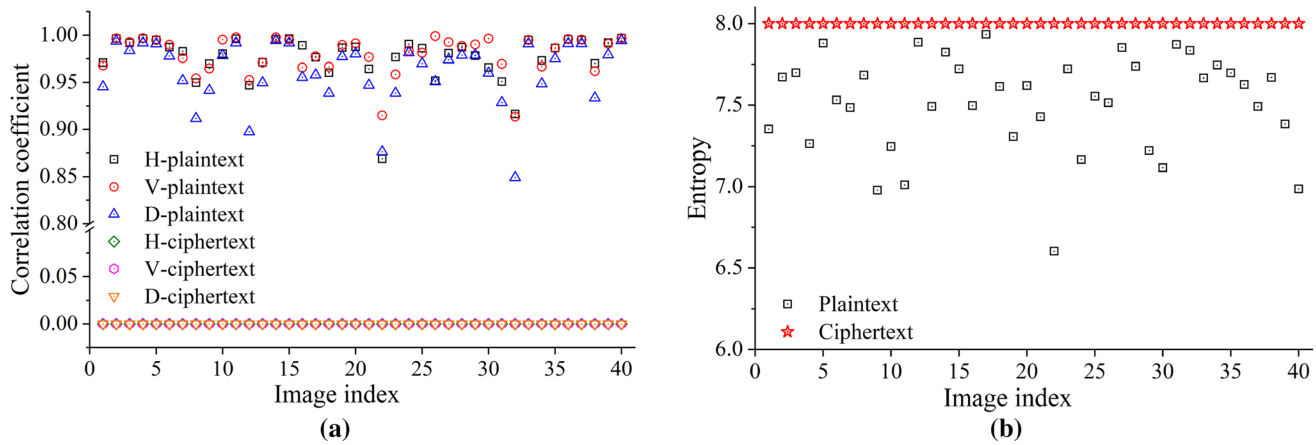


Fig. 13 Cryptanalyses for the plaintext and ciphertext 40#text-images [70] **a** Correlation coefficients, **b** Entropy

5.4 Entropy

Entropy is mostly exploited to evaluate the uncertainty and disorderliness of an image [4]. Recall that entropy in Eq. (8) was even used as one of the objective functions for optimization of FULLMAP. The entropy of an image is appreciated how it is close to 8 which is the maximum value. The entropy of the test images encrypted using the proposed IMEP with FULLMAP is given in Table 3, and the results are compared in Table 4 with the available ones in the literature [17, 25, 26, 30, 35–37]. From Table 3, all entropies are very close to 8. From Table 4, furthermore, the images encrypted using the proposed IMEP with FULLMAP have the closest entropy with 7.9995 among the other IMEPs reported elsewhere [17, 25, 26, 30, 35–37]. Therefore, the proposed IMEP with FULLMAP provides the most assured images against cyberattacks.

5.5 Correlation coefficient

Correlation analysis depends on the evaluation of the correlation coefficients of the adjacent pixels in three directions: horizontal, vertical and diagonal. It is expected that an IMEP securely reduces the correlation coefficient of a ciphertext image. Remember that the correlation coefficient given in Eq. (13) was also used as one of the objective functions for optimization of FULLMAP. The correlation coefficients of the encrypted test images using the proposed IMEP are given in Table 5, and also, they are compared with the available ones in the literature in Table 6 [17, 25, 26, 30, 35–37]. As can be seen from Table 5, the proposed IMEP with FULLMAP minimizes the correlation coefficients as close as to zero. Moreover, it surpasses IMEPs in the literature in view of the correlation coefficients given in Table 6.

The 3D correlation distributions of the plaintext and ciphertext images are shown in Fig. 12 in the three directions. The test images are indexed as Lena: 1, Cameraman: 2, Barbara: 3, Peppers: 4, Baboon: 5, Airplane: 6. Generally speaking, the correlation distributions of an image with mono-color pixels would be a point. Besides those of an image with totally correlated pixels are on $y = x$ line, and an image with completely uncorrelated pixel must be uniformly distributed, i.e., the correlation distribution of a ciphertext image. Therefore, it is intended by an IMEP maximally distributes the points so as to decrease the correlation. As can be seen from Fig. 12a–c that the correlation distributions of the plaintext images mostly intensify on $y = x$ line, while those of respective ciphertext images uniformly distribute and occupy all over the phase.

In order to further examine the proof of FULLMAP-based IMEP, an image database including 600 $\times$ 600 pixels 40#text-images with various features is employed for computation of correlation coefficient and entropy [70]. The computed results for the 40#text-images are scattered in Fig. 13. As the mean of correlation coefficients of plaintext 40#text-images is 0.9723, that of ciphertext 40#text-images is diminished to 4.92 $\times$ 10^{-7}. On the other side, while the average entropy of the plaintext 40#text-images is 7.5154, that of ciphertext 40#text-images is 7.9996. Therefore, IMEP with FULLMAP shows stable encryption performance not only for a limited number of images but also a large number of images.

5.6 Differential attack

Differential attack attempts to resolve the key and discover IMEP by investigating the differences. Differential analysis puts to proof IMEP against the cyberattacks by analyzing the difference between the plaintext and ciphertext images where a few bits in the plaintext image are changed. In this way, encryption capability of an IMEP can be evaluated

Table 7 The NPCR and UACI results for the test images encrypted via the proposed IMEP

Test	Lena	Cameraman	Barbara	Peppers	Baboon	Airplane
NPCR	99.6095	99.6085	99.6085	99.6087	99.6077	99.6098
UACI	33.4625	33.4692	33.4560	33.4679	33.4565	33.4611

Table 8 The NPCR and UACI results and the comparison

Image	Test	Ref. [35]	Ref. [17]	Ref. [36]	Ref. [37]	Ref. [25]	Ref. [26]	Ref. [30]	FULLMAP
Lena	NPCR	99.6078	99.5800	99.6000	99.6912	99.6000	99.6093	99.6621	99.6095
	UACI	33.4268	33.4300	33.4700	33.5098	33.5000	33.45969	33.5278	33.4625
Cameraman	NPCR	99.6323	–	–	–	99.6000	99.6068	–	99.6085
	UACI	33.4096	–	–	–	33.5500	33.4461	–	33.4692
Barbara	NPCR	–	99.6100	–	99.6912	–	–	99.7501	99.6085
	UACI	–	33.4300	–	33.5098	–	–	33.5102	33.4560
Peppers	NPCR	–	–	0.9960	–	99.6100	99.6057	–	99.6087
	UACI	–	–	33.4600	–	33.5200	33.50204	–	33.4679

whether it is sensitive to a bit change in the plaintext image or not. Differential attack analysis is apprised with the following NPCR and UACI.

$$D(i,j) = \begin{cases} 0, & if\ C^1(i,j) = C^2(i,j) \\ 1, & if\ C^1(i,j) \neq C^2(i,j) \end{cases} \quad (22)$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{mxn} x100\% \quad (23)$$

$$UACI = \frac{1}{mxn}\left[\sum\nolimits_{i,j} \frac{\left|C^1(i,j) - C^2(i,j)\right|}{255}\right] x100\% \quad (24)$$

where m and n refer to the height and width of a test image. C^1 and C^2 are the ciphertext images for unchanged and one-bit changed plaintext image, respectively. For a one-bit changed grayscale image, the ideal target of NPCR and UACI is 99.6094% and 33.4635%, respectively [71]. The NPCR and UACI of the test images encrypted via the proposed FULLMAP-based IMEP are given in Table 7, and compared with those of Lena, Cameraman, Barbara and Peppers reported elsewhere in Table 8. It is clearly seen that that the results of the proposed IMEP with FULLMAP are the closest to the ideal targets.

5.7 Cropping attack

Cropping attack analysis puts to proof an IMEP for losing or abusing some parts of the ciphertext images. Cropping attack analysis herewith evaluates the robustness of an IMEP. Therefore, a reliable and robust IMEP is able to decrypt a cropped image with the minimum corruption. The corruption shows itself as corrosion in some pixels of the decipher image. Hence, the lower the corrosion, the more robust the IMEP. For analyzing the proposed IMEP, the ciphertext image of the Barbara images cropped with the ratios 1/16, 1/16 (middle), 1/4, 1/2 and their decipher images are disclosed in Fig. 14. Moreover, the 1/16 cropped image is compared with the reported one in the literature in Fig. 15. From the illustrated results, the proposed IMEP with FULLMAP maximally decrypts the cropped images with the least corrosion.

Moreover, the decipher images with cropping attack by the proposed IMEP with FULLMAP are numerically assessed in terms of PSNR given in Eq. (25) that is able to measure the image quality by comparing to the plaintext images [72]. Therefore, the higher the PSNR, the lower the corruption. The PSNR scores of the decipher images via the proposed FULLMAP-based IMEP are listed in Table 9, and those of the Lena are compared with the reported results in Table 10 [18, 35, 65]. Thanks to the higher PSNR, the cropping attack performance of the proposed IMEP with FULLMAP is corroborated as well as the illustrative results.

$$PSNR = 10\log\left(\frac{255^2}{MSE}\right) \quad (25)$$

where MSE stands for the mean-squared error and calculated as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(e_{ij} - f_{ij}\right)^2 \quad (26)$$

where $E = [e_{ij}]$ is the plaintext image and $F = [f_{ij}]$ is the decipher image with cropping.

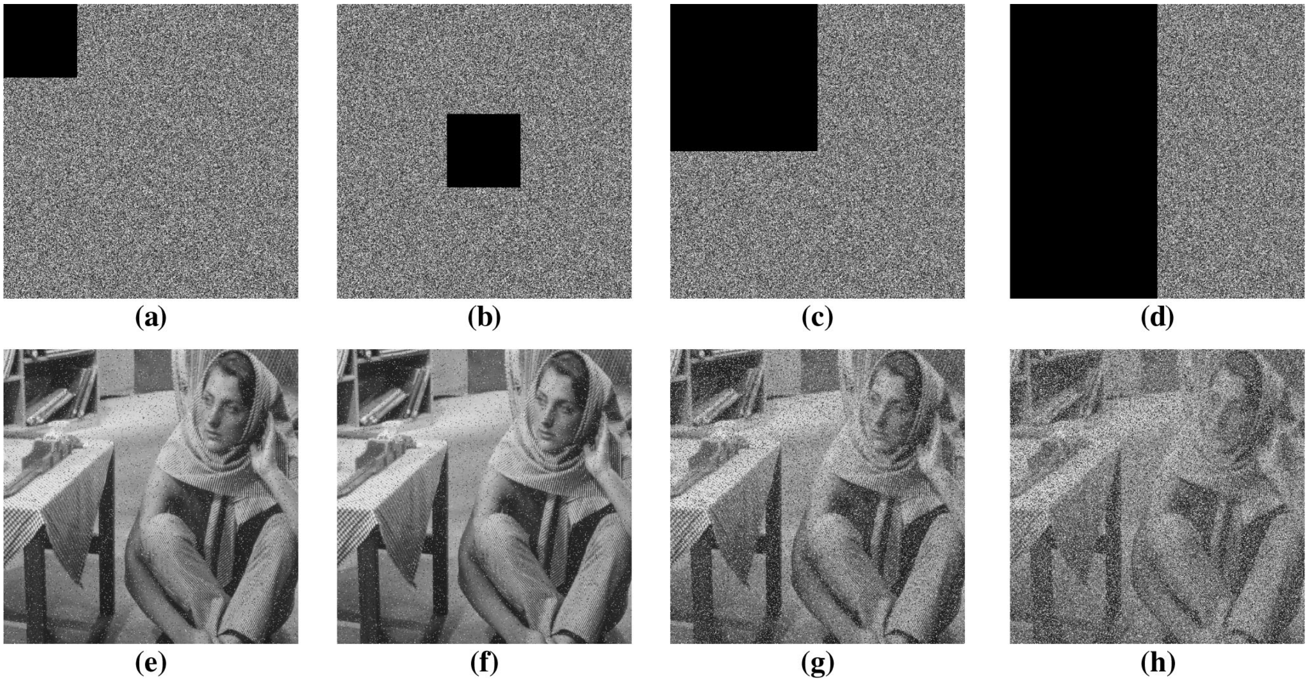


Fig. 14 Cropping attack analysis for the proposed IMEP with FULLMAP; ciphertext images cropped with ratios **a** 1/16, **b** 1/16 (middle), **c** 1/4, **d** 1/2; decipher images with ratios: **e** 1/16, **f** 1/16 (middle), **g** 1/4, **h** 1/2

Table 9 The PSNR scores for the ciphertext test images via the proposed IMEP with FULLMAP

Cropping ratio	Lena	Cameraman	Barbara	Pepper	Baboon	Airplane
1/16	21.38	20.60	20.97	21.12	21.77	20.21
1/4	15.27	14.95	15.05	15.01	15.62	14.19
1/2	12.25	11.85	12.02	12.25	12.65	11.10

5.8 Noise attack

Noise attack analysis examines an IMEP for adding some noise to the ciphertext images. It is herewith utilized to appreciate the reconstruction performances of an IMEP. Hence, recovering capability of an IMEP can be analyzed by inserting the SPN to the ciphertext image. Salt and pepper noise (SPN) is mostly exploited to prove an IMEP counter the noise attacks. The decipher images with adding different SPN densities 0.001, 0.005, 0.01, 0.1 are illustrated in Fig. 16, and they are corroborated through the PSNR scores measured as 39.88, 32.24, 29.05 18.97 for the decipher images with SPN densities 0.001, 0.005, 0.01, 0.1, respectively. In order to clearly see the added SPN, it is illustrated with red color. Eventually, the proposed FULLMAP-based IMEP recovers the images with the minimum degradation even if they are with high SPN.

5.9 Encryption Processing time and computational complexity

Along with the cryptanalyses aforementioned, the processing time of an IMEP is important evaluation for an applicable IMEP to the real-time systems. The processing time of the proposed IMEP with FULLMAP is 0.2050s. On the other side, the operating duration of an algorithm can be even apprised through the computational complexity using big O notation. From this point of view, the computational complexity of the proposed IMEP is $O\ (m \times n)$, where m and n stand for the row and column size of the image, respectively. Hence, it can be implemented to the real applications due to the fast-processing time and low computational complexity.

Fig. 15 The comparative cropping attack analysis for image cropped with 1/16 ratio: **a** [26], **b** [35], **c** [63], **d** [64], **e** [18], **f** [65], **g** [66], **h** [67], **i** The proposed FULLMAP

6 The related studies and the comparison among each other

Existing IMEPs that have been recently reported are elaborately surveyed in Table 11 together with our study with respect to employed chaotic map and cryptanalysis results. The available data in the reported studies are recorded in the table, and the others are necessarily remarked non-available (N/A). Notably, the studies indicated with asterisk* stand for those in which the optimization algorithms employed. Those are even reviewed with regard to the employed optimization algorithms and other parameters in Table 12.

It is observed from Table 11 that the IMEPs are based on various chaotic maps such as logistic, sine, cosine, Henon, Chebyshev, Lorenz, Henon and their variants and combinations. They were frequently evaluated with respect to different cryptoanalyses: key-space, entropy, correlation

Table 10 The PSNR scores and comparison with the literature

Image	Cropping ratio	Ref. [35]	Ref. [18]	Ref. [65]	FULLMAP
Lena	1/16	17.58	16.66	20.78	21.38
	1/4	15.03	10.64	14.96	15.27
	1/2	12.13	10.66	12.08	12.25

coefficient, differential attack over NPCR and UACI, cropping attack, noise attack and processing time. Those IMEPs are tried to be relatively classified into three levels:

Cryptoanalysis	Worst	Moderate	Best
Key-space	[23, 29, 33]	[26, 35, 38, 49]	[17, 18, 40, 20, 21, 24, 25, 27, 34, 36, 39]
Entropy	[18, 20–22, 26, 29, 30, 33, 39]	[17, 25, 28, 31, 35–38]	[34]
Mean correlation	[17, 21, 28, 33, 41]	[20, 22, 34, 36–40, 23–27, 29–31]	[18, 19, 35]
NPCR	[19, 33]	[20–23, 28–31, 34]	[17, 18, 40, 24–26, 35–39]
UACI	[19, 21, 31, 33, 37]	[17, 25, 26, 28, 30, 35, 36, 38, 39]	[18, 23, 24, 34, 40]
Cropping attack	[24, 25, 30, 37, 40]	[18, 23, 26, 38, 39]	[35]
Noise attack	[18, 38, 40]	[24–26, 30, 37, 39]	[23]
Processing time	[21, 22, 29, 39]	[23, 40]	[24, 26, 30, 31, 36–38]

Therefore, the proposed EIS with FULLMAP comes to the fore on account of key-space, entropy, correlation, NPCR, UACI, processing time of 2^{298}, 7.9995, 0.000061,

Table 11 A detailed survey in terms of the employed chaotic map and cryptanalysis results

Ref	Year	Chaotic map	Key-space	Entropy (mean)	Corr. (mean)	Differential attack (%)		Crop. attack	Noise Attack	Processing time (s)
						NPCR	UACI			
[23]	2018	Sine–sine	2^{128}	N/A	0.006300	99.6330	33.4716	▄	▖	0.5042
[35]	2021	4D memristive	2^{146}	7.9993	0.000511	99.6078	33.4268	▙	N/A	N/A
[17]	2019	2D logistic-adjusted sine	2^{338}	7.9993	0.013197	99.6042	33.4328	N/A	N/A	N/A
[36]	2019	A modified chaotic	2^{212}	7.9993	0.001710	99.6040	33.4340	N/A	N/A	0.0700
[37]	2019	Polynomial	N/A	7.9993	0.002003	99.6191	33.6751	▖	▄	0.2810
[38]	2018	Three integrated cascade	2^{186}	7.9993	0.003217	99.6040	33.4740	▄	▙	0.4442
[25]	2018	2D Henon–sine	2^{371}	7.9993	0.002417	99.6080	33.5470	▖	▄	N/A
[28]	2020	Lorenz	N/A	7.9991	0.051500	99.5676	33.4352	N/A	N/A	N/A
[31]	2019	Cellular automata	N/A	7.9992	0.002033	99.5180	33.2630	N/A	N/A	0.2240
[26]	2020	2D sine and Chebyshev	2^{158}	7.9972	0.001719	99.6090	33.4523	▄	▄	0.0605
[30]	2021	Yolo	N/A	7.9981	0.001523	99.7061	33.5190	▖	▄	0.2760
[39]	2019	Four-wing hyperchaotic	2^{700}	7.9971	0.008957	99.6000	33.4800	▄	▄	1.2800
[24]	2020	Sine	2^{412}	N/A	0.001827	99.6127	33.4691	▖	▄	0.0239
[40]	2019	Cosine transform	2^{256}	N/A	0.001410	99.6244	33.4548	▖	▙	0.9730
[33]*	2020	Coupled lattice	2^{128}	7.9519	0.046700	99.4547	31.3549	N/A	N/A	N/A
[29]*	2020	4D Lorenz system	2^{111}	7.9976	0.003720	99.6340	33.4330	N/A	N/A	14.8750
[34]*	2021	A 5D chaotic	2^{338}	7.9996	0.005973	99.6475	33.4700	N/A	N/A	N/A
[20]*	2019	Intertwining logistic	2^{338}	7.9987	0.003250	99.6535	33.5497	N/A	N/A	N/A
[21]*	2020	Intertwining logistic	2^{256}	7.9985	0.016467	99.6400	32.9500	N/A	N/A	600.00
[22]*	2021	Piecewise linear chaotic and 2D logistic	N/A	7.9723	0.001790	99.6746	33.4753	N/A	N/A	89.155
[18]*	2021	Logistic	2^{385}	7.9974	0.000113	99.6169	33.4658	▄	▙	1.1247
[19]*	2018	Logistic	N/A	N/A	0.000100	99.4547	31.3549	N/A	N/A	N/A
[27]*	2017	Henon	2^{381}	N/A	0.006133	N/A	N/A	N/A	N/A	N/A
[41]*	2012	N/A	N/A	N/A	0.084940	N/A	N/A	N/A	N/A	N/A
[49]*	2015	Coupled nonlinear	2^{168}	N/A	N/A	N/A	N/A	N/A	N/A	N/A
This study		FULLMAP	2^{298}	7.9995	0.000061	99.6087	33.4622	▙	▙	0.2050

*The studies stand for those in which the optimization algorithms are employed

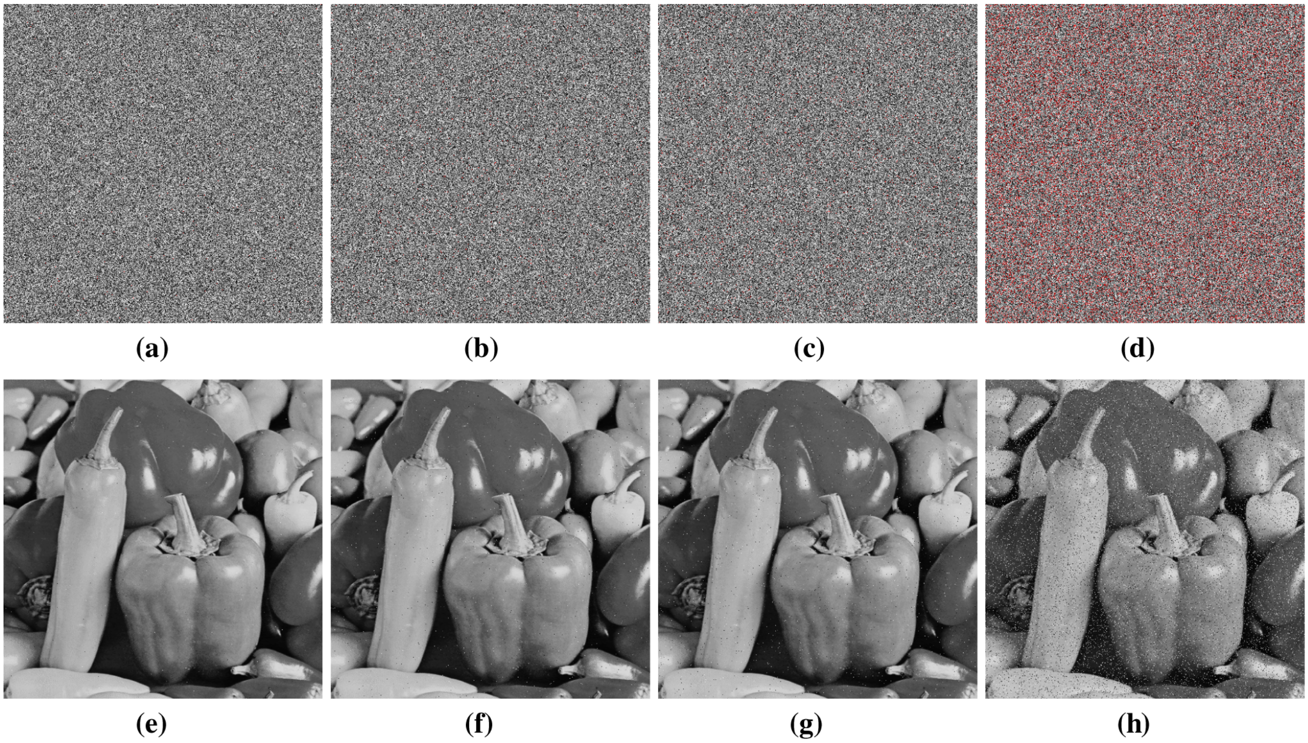


Fig. 16 Ciphertext images with adding different SPN densities: **a** 0.001, **b** 0.005, **c** 0.01, **d** 0.1; the related decipher images with SPN densities: **e** 0.001, **f** 0.005, **g** 0.01, **h** 0.1 (The added SPN pixels are shown with red color)

Table 12 A review on the metaheuristic optimization-based IMEPs

Ref	Year	Type of chaotic map	Optimization algorithm	Multi/Single	Objective function	Decision variable
[33]	2020	Coupled lattice	GA	Multi	Entropy and correlation of the ciphertext image	Key
[29]	2020	4D chaotic map based on Lorenz system	Pareto evolutionary algorithm-II	Multi	Weighted objective function of the ciphertext image: correlation coefficient, entropy, NPCR, UACI	Initial parameter of the map
[34]	2021	A 5D chaotic	Dual local search	Multi	UACI, entropy, NPCR of the ciphertext image	Initial parameter of the map
[20]	2019	Intertwining logistic	Memetic DE	Single	Entropy and correlation of the ciphertext image	Key
[21]	2020	Intertwining logistic	DE	Single	Entropy of the ciphertext image	A sequence for DNA operation
[22]	2021	Piecewise linear chaotic and 2D logistic	WOA	Single	Entropy of the ciphertext image	Initial parameter of the map
[18]	2021	Logistic	PSO	Multi	Weighted objective function for the ciphertext image: entropy and correlation coefficient	Key
[19]	2018	Logistic	PSO	Single	Correlation of the ciphertext image	Key
[27]	2017	Henon	SDO	Single	Complex object function based on CCD plane for the ciphertext image	Image
[41]	2012	N/A	ACO	Single	Energy of the ciphertext image	Key
[49]	2015	Coupled nonlinear	Hybrid of PSO and GA	Single	PSNR of the ciphertext image	Key
This study		FULLMAP	ABC	Multi	Weighted objective function of the chaotic map: LE, entropy, 0–1 test and correlation coefficient	Coefficients of the map

99.6087, 33.4622 and 0.2050 (s), respectively, as well as cropping and noise attacks among those reported elsewhere.

From Table 12, it is seen that the optimization algorithms such as ACO, PSO, GA, DE, SDO and WOA were frequently implemented to IMEPs. Decision variables might be the most critical parameters sought via the optimization algorithms. It appears that the keys and the initial parameters of the maps were often explored as the decision variables. Although various chaotic maps were utilized, entropy, correlation coefficient, PSNR, NPCR, UACI and their combinations were exploited as single or multiple objective strategies, in general. It is worth noting that these objective functions were handled on the ciphertext image obtained at the end of the entire operations of IMEP, i.e., the objective functions must be computed on the ciphertext images. In order to compute the objective functions in every cycle of the optimization algorithm, the plaintext image must be incurred throughout the operations of IMEP to obtain the ciphertext image. This makes those IMEPs inapplicable to the real-time systems due to the high complexity and encryption processing time. On the other hand, the proposed FULLMAP is derived by optimally finding out the decision variables using ABC with multi-objective strategy. The multi-objective function is directly applied to FULLMAP so as to optimize it. The plaintext image is thus encrypted through the proposed permutation and diffusion operations conducted by the FULLMAP. In other words, the main advantage of the proposed method is that ABC is directly applied to FULLMAP, not the ciphertext images.

7 Conclusion

A new 2D FULLMAP for IMEP, which is constructed using a multi-objective optimization strategy via ABC, is proposed in this work. The eight decision variables of FULLMAP model are found out through the four objective functions including the entropy, LE, 0–1 test, correlation coefficient. FULLMAP is appreciated with respect to many reliable measurements regarding bifurcation, 3D phase space, LE, 0–1 test, PE and SE. IMEP with FULLMAP is undergone various cryptanalyses, and the visual and numerical results are compared with those of various reported studies with and without optimization. The prominent cryptanalyses such as key-space, mean entropy, mean correlation, NPCR, UACI and processing time are 2^{298}, 7.9995, 0.000061, 99.6087, 33.4622 and 0.2050 (s), respectively. These copping and noise attacks are also remarkable. They are elaborately reviewed and compared among each other in order to prove superiority of the proposed FULLMAP-based IMEP. It is evident that the proposed IMEP is prominent among the state of the arts thanks to the efficiently optimized hyperchaotic properties of FULLMAP with quadruple-objective optimization. The proposed IMEP does not utilize ABC in the image encryption process rather than the other studies in which optimization is employed, even the fact that FULLMAP is constructed by the multi-objective optimization. Therefore, the proposed IMEP with FULLMAP efficiently encrypts the images with higher security and speed thanks to the optimized dynamic performance of the FULLMAP.

Declarations

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

References

1. Xuejing K, Zihui G (2020) A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Process Image Commun 80:1–11. https://doi.org/10.1016/j.image.2019.115670
2. Alawida M, Samsudin A, Sen TJ, Alkhawaldeh RS (2019) A new hybrid digital chaotic system with applications in image encryption. Signal Process 160:45–58. https://doi.org/10.1016/j.sigpro.2019.02.016
3. Bao L, Yi S, Zhou Y (2017) Combination of Sharing Matrix and Image Encryption for Lossless (k, n)-Secret Image Sharing. IEEE Trans Image Process 26:5618–5631. https://doi.org/10.1109/TIP.2017.2738561
4. Zhang F, Kodituwakku HADE, Hines JW, Coble J (2019) Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Trans Ind Informatics 15:4362–4369. https://doi.org/10.1109/TII.2019.2891261
5. Chen J, Chen L, Zhou Y (2020) Cryptanalysis of a DNA-based image encryption scheme. Inf Sci (Ny) 520:130–141. https://doi.org/10.1016/j.ins.2020.02.024
6. Liu Y, Qin Z, Liao X, Wu J (2020) Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. Nonlinear Dyn 100:2917–2931. https://doi.org/10.1007/s11071-020-05654-y
7. Hua Z, Zhu Z, Yi S et al (2021) Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inf Sci (Ny) 546:1063–1083. https://doi.org/10.1016/j.ins.2020.09.032
8. Talhaoui MZ, Wang X (2020) A new fractional one dimensional chaotic map and its application in high-speed image encryption. Inf Sci (Ny). https://doi.org/10.1016/j.ins.2020.10.048
9. Wen W, Wei K, Zhang Y et al (2020) Colour light field image encryption based on DNA sequences and chaotic systems. Nonlinear Dyn 99:1587–1600. https://doi.org/10.1007/s11071-019-05378-8
10. Zheng P, Huang J (2018) Efficient Encrypted Images Filtering and Transform Coding with Walsh-Hadamard Transform and Parallelization. IEEE Trans Image Process 27:2541–2556. https://doi.org/10.1109/TIP.2018.2802199
11. Ćalasan M, Abdel Aleem SHE, Bulatović M et al (2021) Design of controllers for automatic frequency control of different

interconnection structures composing of hybrid generator units using the chaotic optimization approach. Int J Electr Power Energy Syst 129:106879. https://doi.org/10.1016/j.ijepes.2021.106879
12. Pierezan J, dos Santos CL, Cocco Mariani V et al (2021) Chaotic coyote algorithm applied to truss optimization problems. Comput Struct 242:106353. https://doi.org/10.1016/j.compstruc.2020.106353
13. Yousri D, Allam D, Eteiba MB (2019) Chaotic whale optimizer variants for parameters estimation of the chaotic behavior in Permanent Magnet Synchronous Motor. Appl Soft Comput J 74:479–503. https://doi.org/10.1016/j.asoc.2018.10.032
14. Coelho LDS, Mariani VC, Guerra FA et al (2014) Multiobjective optimization of transformer design using a chaotic evolutionary approach. IEEE Trans Magn 50:669–672. https://doi.org/10.1109/TMAG.2013.2285704
15. Okamoto T, Hirata H (2013) Global optimization using a multipoint type quasi-chaotic optimization method. Appl Soft Comput J 13:1247–1264. https://doi.org/10.1016/j.asoc.2012.10.025
16. dos Coelho L, S, Mariani VC, (2009) A novel chaotic particle swarm optimization approach using Hénon map and implicit filtering local search for economic load dispatch. Chaos, Solitons Fractals 39:510–518. https://doi.org/10.1016/j.chaos.2007.01.093
17. Chai X, Gan Z, Yuan K et al (2019) A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput Appl 31:219–237. https://doi.org/10.1007/s00521-017-2993-9
18. 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
19. Ahmad M, Alam MZ, Umayya Z et al (2018) An image encryption approach using particle swarm optimization and chaotic map. Int J Inf Technol 10:247–255. https://doi.org/10.1007/s41870-018-0099-y
20. Kaur M, Kumar V, Li L (2019) Color image encryption approach based on memetic differential evolution. Neural Comput Appl 31:7975–7987. https://doi.org/10.1007/s00521-018-3642-7
21. Dua M, Wesanekar A, Gupta V et al (2020) Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. J Ambient Intell Humaniz Comput 11:3771–3786. https://doi.org/10.1007/s12652-019-01580-z
22. Saravanan S, Sivabalakrishnan M (2021) A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. Soft Comput 48:1–24. https://doi.org/10.1007/s00500-020-05528-w
23. Wang H, Xiao D, Chen X, Huang H (2018) Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Process 144:444–452. https://doi.org/10.1016/j.sigpro.2017.11.005
24. Mansouri A, Wang X (2020) A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf Sci (Ny) 520:46–62. https://doi.org/10.1016/j.ins.2020.02.008
25. Wu J, Liao X, Yang B (2018) Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process 153:11–23. https://doi.org/10.1016/j.sigpro.2018.06.008
26. Chen C, Sun K, He S (2020) An improved image encryption algorithm with finite computing precision. Signal Process 168:1–10. https://doi.org/10.1016/j.sigpro.2019.107340
27. Su Y, Tang C, Chen X et al (2017) Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. Opt Lasers Eng 88:20–27. https://doi.org/10.1016/j.optlaseng.2016.07.012
28. Farah MAB, Guesmi R, Kachouri A, Samet M (2020) A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt Laser Technol 121:105777. https://doi.org/10.1016/j.optlastec.2019.105777
29. Kaur M, Singh D, Uppal RS (2020) Parallel strength Pareto evolutionary algorithm-II based image encryption. IET Image Process 14:1015–1026. https://doi.org/10.1049/iet-ipr.2019.0587
30. Asgari-Chenaghlu M, Feizi-Derakhshi MR, Nikzad-Khasmakhi N et al (2021) Cy: Chaotic yolo for user intended image encryption and sharing in social media. Inf Sci (Ny) 542:212–227. https://doi.org/10.1016/j.ins.2020.07.007
31. Enayatifar R, Guimarães FG, Siarry P (2019) Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Opt Lasers Eng 115:131–140. https://doi.org/10.1016/j.optlaseng.2018.11.017
32. Chai X, Bi J, Gan Z et al (2020) Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Process 176:107684. https://doi.org/10.1016/j.sigpro.2020.107684
33. Suri S, Vijay R (2020) A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA. Neural Comput Appl 32:11859–11873. https://doi.org/10.1007/s00521-019-04668-x
34. Kaur M, Singh D (2020) Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption. Multidimens Syst Signal Process 32:281–301. https://doi.org/10.1007/s11045-020-00739-8
35. Yang Y, Wang L, Duan S, Luo L (2021) Dynamical analysis and image encryption application of a novel memristive hyperchaotic system. Opt Laser Technol 133:106553. https://doi.org/10.1016/j.optlastec.2020.106553
36. Hanis S, Amutha R (2019) A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure. Nonlinear Dyn 95:421–432. https://doi.org/10.1007/s11071-018-4573-7
37. Asgari-Chenaghlu M, Balafar MA, Feizi-Derakhshi MR (2019) A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Process 157:1–13. https://doi.org/10.1016/j.sigpro.2018.11.010
38. Lan R, He J, Wang S et al (2018) Integrated chaotic systems for image encryption. Signal Process 147:133–145. https://doi.org/10.1016/j.sigpro.2018.01.026
39. Chai X, Fu X, Gan Z et al (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process 155:44–62. https://doi.org/10.1016/j.sigpro.2018.09.029
40. 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
41. Sreelaja NK, Vijayalakshmi Pai GA (2012) Stream cipher for binary image encryption using Ant Colony Optimization based key generation. Appl Soft Comput J 12:2879–2895. https://doi.org/10.1016/j.asoc.2012.04.002
42. Carbas S, Toktas A, Ustun D (2021) Nature-Inspired Metaheuristic Algorithms for Engineering Optimization Applications. Springer Singapore
43. Li G, Liu L, Feng X (2019) Accelerating GPU Computing at Runtime with Binary Optimization. In: CGO 2019 - Proceedings of the 2019 IEEE/ACM International Symposium on Code Generation and Optimization. Institute of Electrical and Electronics Engineers Inc., pp 276–277
44. Premkumar M, Jangir P, Sowmya R (2021) MOGBO: A new Multiobjective Gradient-Based Optimizer for real-world structural optimization problems. Knowledge-Based Syst 218:106856. https://doi.org/10.1016/j.knosys.2021.106856
45. Moreno SR, Pierezan J, dos Coelho L, S, Mariani VC, (2021) Multi-objective lightning search algorithm applied to wind farm layout optimization. Energy 216:119214. https://doi.org/10.1016/j.energy.2020.119214

46. Vasconcelos Segundo EH, de, Mariani VC, Coelho L dos S, (2019) Metaheuristic inspired on owls behavior applied to heat exchangers design. Therm Sci Eng Prog 14:100431. https://doi.org/10.1016/j.tsep.2019.100431
47. Rubio-Largo Á, Vega-Rodríguez MA, González-Álvarez DL (2016) Hybrid multiobjective artificial bee colony for multiple sequence alignment. Appl Soft Comput J 41:157–168. https://doi.org/10.1016/j.asoc.2015.12.034
48. Zhou X, Liu Y, Li B, Sun G (2015) Multiobjective biogeography based optimization algorithm with decomposition for community detection in dynamic networks. Phys A Stat Mech its Appl 436:430–442. https://doi.org/10.1016/j.physa.2015.05.069
49. Sajasi S, Eftekhari Moghadam AM (2015) An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method. Appl Soft Comput J 30:375–389. https://doi.org/10.1016/j.asoc.2015.01.032
50. Alkebsi K, Du W (2020) A Fast Multi-Objective Particle Swarm Optimization Algorithm Based on a New Archive Updating Mechanism. IEEE Access 8:124734–124754. https://doi.org/10.1109/ACCESS.2020.3007846
51. Demertzis K, Iliadis L (2017) Adaptive elitist differential evolution extreme learning machines on big data: Intelligent recognition of invasive species. In: Advances in Intelligent Systems and Computing. Springer Verlag, pp 333–345
52. Arora S, Singh S (2016) Butterfly algorithm with Lèvy Flights for global optimization. In: Proceedings of 2015 International Conference on Signal Processing, Computing and Control, ISPCC 2015. Institute of Electrical and Electronics Engineers Inc., pp 220–224
53. 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
54. 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
55. Toktas A, Ustun D, Tekbas M (2020) Global optimisation scheme based on triple-objective ABC algorithm for designing fully optimised multi-layer radar absorbing material. IET Microwaves, Antennas Propag 14:800–811. https://doi.org/10.1049/iet-map.2019.0868
56. 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
57. Akdagli A, Toktas A (2010) A novel expression in calculating resonant frequency of H-shaped compact microstrip antennas obtained by using artificial bee colony algorithm. J Electromagn Waves Appl 24:2049–2061. https://doi.org/10.1163/156939310793675989
58. 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
59. May RM (1976) Simple mathematical models with very complicated dynamics. Nature 261:459–467. https://doi.org/10.1038/261459a0
60. Gottwald GA, Melbourne I (2016) The 0–1 test for chaos: A review. In: Lecture Notes in Physics. Springer Verlag, pp 221–247
61. 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
62. Bandt C, Pompe B (2002) Permutation Entropy: A Natural Complexity Measure for Time Series. Phys Rev Lett 88:4. https://doi.org/10.1103/PhysRevLett.88.174102
63. Yang F, Mou J, Liu J et al (2020) Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. Signal Process 169:1–16. https://doi.org/10.1016/j.sigpro.2019.107373
64. Wu Y, Zhang L, Qian T et al (2021) Content-adaptive image encryption with partial unwinding decomposition. Signal Process 181:107911. https://doi.org/10.1016/j.sigpro.2020.107911
65. Luo Y, Lin J, Liu J et al (2019) A robust image encryption algorithm based on Chua's circuit and compressive sensing. Signal Process 161:227–247. https://doi.org/10.1016/j.sigpro.2019.03.022
66. Chai X, Zheng X, Gan Z et al (2018) An image encryption algorithm based on chaotic system and compressive sensing. Signal Process 148:124–144. https://doi.org/10.1016/j.sigpro.2018.02.007
67. Wang X, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci (Ny) 539:195–214. https://doi.org/10.1016/j.ins.2020.06.030
68. 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
69. 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
70. Asuni N, Giachetti A (2014) TESTIMAGES: a large-scale archive for testing visual devices and basic image processing algorithms. In: Giachetti A (ed) STAG: Smart Tools & Apps for Graphics (2014). The Eurographics Association
71. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals Multidiscip Journals Sci Technol J Sel Areas Telecommun 31–38
72. Enginoğlu S, Erkan U, Memiş S (2019) Pixel similarity-based adaptive Riesz mean filter for salt-and-pepper noise removal. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-08110-1