Nonlinear Dyn (2021) 105:1885–1909
https://doi.org/10.1007/s11071-021-06675-x

ORIGINAL PAPER

An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm

Abdurrahim Toktas · Uğur Erkan · Deniz Ustun

Received: 25 March 2021 / Accepted: 26 June 2021 / Published online: 7 July 2021

Abstract A novel optimal chaotic map (OCM) is proposed for image encryption scheme (IES). The OCM is constructed using a multi-objective optimization strategy through artificial bee colony (ABC) algorithm. An empirical model for the OCM with four unknown variables is first constituted, and then, these variables are optimally found out using ABC for minimizing the multi-objective function composed of the information entropy and Lyapunov exponent (LE) of the OCM. The OCM shows better chaotic attributes in the evaluation analyses using metrics such as bifurcation, 3D phase space, LE, permutation entropy (PE) and sample entropy (SE). The encrypting performance of the OCM is demonstrated on a straightforward IES and verified by various cryptanalyses that compared with many reported studies, as well. The main superiority of the OCM over the studies based on optimization is that it does not require any optimization in the encrypting operation; thus, OCM works standalone in the encryption. However, those reported studies use ciphertext images obtained through encrypting process in every cycle of optimization algorithm, resulting in long processing time. Therefore, the IES with OCS is faster than the others optimization-based IES. Furthermore, the proposed IES with the OCM manifests satisfactory outcomes for the compared results with the literature.

Keywords Image encryption · Chaotic map · Optimization algorithm · Multi-objective optimization · Artificial bee colony

A. Toktas (✉)
Department of Electrical and Electronics Engineering, Faculty of Engineering, Karamanoğlu Mehmetbey University, 70200 Karaman, Turkey
e-mail: atoktas@kmu.edu.tr

U. Erkan
Department of Computer Engineering, Faculty of Engineering, Karamanoğlu Mehmetbey University, 70200 Karaman, Turkey

D. Ustun
Department Computer Engineering, Faculty of Engineering, Tarsus University, 33400 Tarsus, Mersin, Turkey

1 Introduction

Nowadays, real-time messaging or data transferring has been attacking considerable interest [1–3]. When the data are transferred through a wide area network (WAN), it may fall into potential cyber threats such as network attacks, denial-of-service, man-in-the-middle and phishing [4, 5]. Therefore, the data must be encrypted via reliable data encrypting techniques for providing information security during the data transferring [6–8]. The well-known techniques are data encryption standard (DES), triple-DES (3DES), international data encryption algorithm (IDEA) and an advanced encryption standard (AES). However, they may be inconvenient for the image security since current multimedia data are high in correlation and big in amount [9, 10].

Image encryption schemes (IESs) are frequently operated in the spatial and/or frequency domains. IESs 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 [11, 12]. Owing to providing high dynamization, complexity, sensitivity to the initial conditions and system parameter, chaotic map-based IESs are mostly utilized approaches. The IESs based on chaotic maps and DNA are generally operated through two operations which are permutation and diffusion. In permutation, the positions of image's pixels are interchanged; and in diffusion, the tonal values of the image's pixels are manipulated. The permutation and diffusion operations are handled with sequences produced via a chaotic map. The chaotic maps are conducted with an initial value and control parameter achieved by a key. Therefore, the chaotic maps have a critical role in the operations of an IES. The performance of an IES is analyzed through various precise cryptanalyses such as key-space, key sensitivity, information entropy, histogram, correlation, differential attack, noisy attack and cropping attack [13]. Different cryptosystems based on various types of chaotic maps based on recursive polynomial [14] and series like logistic [15–17], sine/cosine [18–23] memristive [24], Henon [20, 25], Lorentz [26, 27], Yolo [28], Chebyshev [21] and cellular automata [29] with various dimensions and integration [30, 31] have been suggested in the literature. Those systems are surveyed in detail with regard to the cryptanalyses in Sect. 6 includes related studies. As they are surveyed, they are robust in particular cryptanalyses. In other words, they are not successful at whole cryptanalyses.

Nature-inspired evolutionary algorithms have been widely implemented to the engineering problems and cryptosystems [32]. The efficacy of the cryptosystems has been therewith improved with single [15, 17, 25, 33–35] or multi-objective strategies [16, 27, 36, 37]. There have been plenty kinds of the nature-inspired optimization algorithms. From them, ant colony algorithm (ACO) [34], particle swarm optimization (PSO) [16, 17, 35], genetic algorithm (GA) [35, 36], differential evolution (DE) [33], whale optimization algorithm (WOA) [15], artificial bee colony (ABC), butterfly optimization algorithm (BOA) and steepest descent optimization (SDO) [25] can be listed as the mostly utilized algorithms. In general, the optimization algorithms have been applied to optimally explorer keys used in the IES [16, 17, 34–36, 38] or initial/control parameters of the chaotic maps [15, 27, 37] for minimizing or maximizing various objective functions regarding information entropy [15, 16, 33, 36–38], energy [34], correlation coefficient[16, 27, 38], peak signal to noise ratio (PSNR) [35], pixels changing rate (NPCR) [27, 37], the unified average changing intensity (UACI) [27, 37]. The optimization-based IES is elaborately reviewed in Sect. 6 comprises the related studies. The main shortcoming of those studies is that the optimization algorithms were applied to throughout the cryptosystem, i.e., the objective functions were dependent on the ciphertext images that must be undergone the entire encrypting operations. Therefore, they suffer from long encryption processing time and complexity, making the IES is inapplicable to the realistic systems. An application of optimization to IES without depending encrypting operations, thus avoiding extent of the processing time could improve the security of the IES. Moreover, optimizing a chaotic map using a proper evolutionary optimization algorithm with multi-objective strategy for enhancing effective evaluations of map would be promising and outperforming in terms of all cryptanalyses.

Therefore, we propose a plain IES based on a novel optimal chaotic map (OCM) derived through a multi-objective optimization using ABC algorithm in this study. The sprinkled unknown variables of the OCM are optimally found out for minimizing a weighted multi-objective function involving information entropy and Lyapunov exponent (LE). The chaotic performance of OCM is appreciated through various visual and numerical metrics such as bifurcation, 3D trajectory, LE, permutation entropy (PE) and sample entropy (SE). The initial value and control parameter of the OCM are achieved from the main key so as to produce the chaotic sequences for the encrypting operations. In order to manifest the superiority of the proposed OCM, a plaintext image is encrypted through only two straightforward encrypting operations that are permutation and diffusion. The new contributions of our study can be summarized as follows:

- A methodology, where an evolutionary optimization algorithm so-called ABC with multi-objective strategy is implemented to build a chaotic map, is proposed.
- A novel chaotic map denoted OCM with satisfactory chaotic and randomization performance is optimally constructed through methodology.
- The performance of OCM is demonstrated upon various metrics, and an IES operated across benchmarking test images and corroborated in terms of plenty cryptanalyses.
- An elaborate review and comparison are carried out not only for the studies in which optimization algorithms employed, but also for those not used.

The cryptanalysis results demonstrate that the proposed IES outperforms the state of the art thanks to the optimized dynamic performance of the OCM. Since ABC is solely implemented to constructing the OCM not to the ciphertext image, the OCM performs as standalone in the optimization, i.e., it works independently from the encryption process. Thence, the proposed IES with the OCM operates faster than the state of the art in which optimization is used.

2 General view of the optimization procedure and IES

The block diagram of the proposed optimization procedure and IES with OCM is revealed in Fig. 1. First, a chaotic map model for the OCM is constituted empirically by inspiring the existing chaotic maps in which a few decision variables are inserted to be optimized. It is then attempted to optimally find out its variables with the guidance of effective objective functions. While the models of chaotic maps are tried to change, the decision variables are optimized for minimizing the weighted multi-objective objective function. Once the optimization cycles are completed, the OCM with final best decision variables is ready for IES. Afterward, a plaintext image is encrypted through the operations of permutation and diffusion. For this, a public key is produced from the plaintext image, and a secret key is formed. The initial value and control parameter of the OCM are achieved from the main key so as to produce the chaotic sequences for the encrypting operations. Eventually, the plaintext image is encrypted through the permutation and diffusion governed by the chaotic sequences.

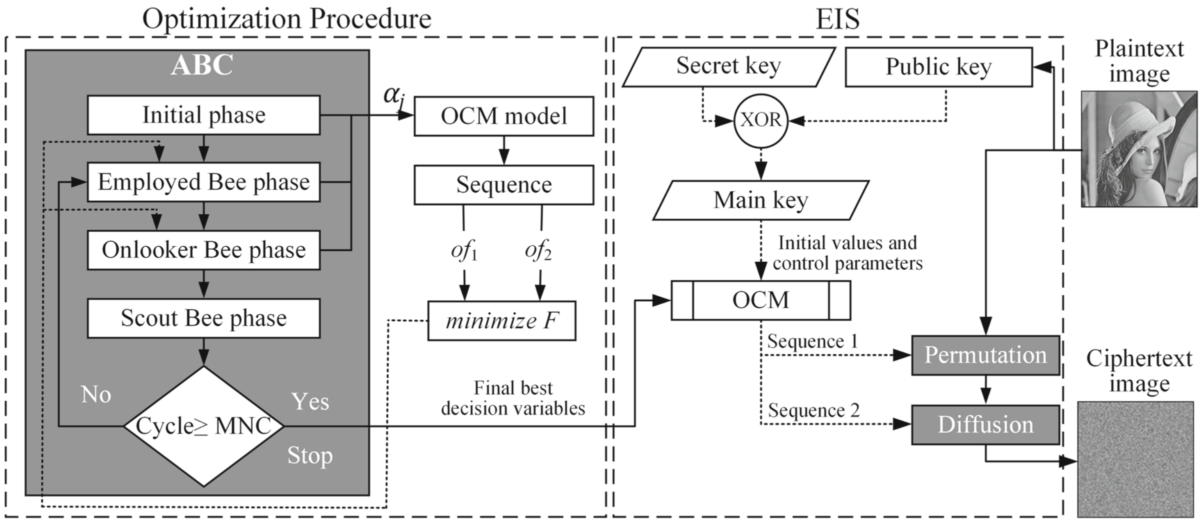


Fig. 1 The block diagram of the proposed optimization procedure and IES with the OCM

3 The optimization procedure for construction of the OCM using ABC

In this section, the working principles of ABC algorithm are firstly expressed, and then, the evaluation of chaotic maps for consideration of the objective functions is presented. Finally, the model that considered for the OCM model with the four unknown variables and implementation of ABC to the optimization of OCM is explained.

3.1 ABC algorithm

ABC was modeled by imitating the foraging behavior of natural bees [39]. Once ABC was emerged, ABC and its variants have been implemented to numerous engineering problems due to its effective properties [40–44]. It is supposed that three groups of bees, namely employed, onlooker and scout bees, compose the artificial bee colony. They work 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.

All employed bees work as scout bees in initialization phase and randomly discover the initial nectar sources, which stand for candidate solutions x_{ij} (decision variables), using the following operator (Step 1).

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

where $i = 1, 2, \ldots, \mathrm{NP}$ 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.

In the 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 (Step 2):

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

here, $(k \neq i) \in \{1, 2, \ldots, \mathrm{NP}\}$ 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. In other words, the fitness values of all modified solutions are computed as given below (Step 3)

Algorithm 1: The pseudocode of ABC algorithm

```
  //Initialization Phase
Step 1.  Generate randomly the initial population of solutions $x_{ij}$
Repeat
             //Employed Bees Phase
Step 2.      Produce new solutions $m_{ij}$ in the vicinity of the previous solutions
Step 3.      Evaluate fitness $fit_i$ of the solutions
Step 4.      Select greedy between $x_i$ and $v_i$ according to fitness values
Step 5.      Compute the probabilities $P_i$ for the solutions
             //Onlooker Bees Phase
Step 6.      Select solutions depending on $P_i$
Step 7.      Produce the new solutions $m_{ij}$ around the selected $x_{ij}$
Step 8.      Evaluate fitness $fit_i$ of the solutions
Step 9.      Select greedy between $x_i$ and $m_i$ according to fitness values
             //Scout Bees Phase
Step 10.     If a solution is not improved after a number of "limit", generate a new one
Step 11.     Record the best solution achieved so far
End Repeat
Step 12. If the cycles reach to MNC, stop the algorithm
```

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

where $of_i(x)$ is the objective value for each solution. The solutions are replaced with the corresponding better solutions of m_{ij} (Step 4). The probabilities of the solutions are then computed depending on the fitness values using the following operator (Step 5).

$$P_i = \frac{\text{fit}_i}{\sum_{i=1}^{\text{NP}/2} \text{fit}_i} \quad (4)$$

In onlooker bee phase, the employed bees share 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 probabilities of the solutions by means of the roulette wheel selection (Step 6). The onlooker bees then start to consume the selected nectar sources, implying that it produces new solutions m_{ij} in the surrounding of the selected solutions using the operator in Eq. (2) (Step 7). The quality of the new nectar sources is then evaluated by computing the fitness values of the modified solutions using Eq. (3) (Step 8). The better solutions m_{ij} are taken place of the former reciprocal solutions (Step 9).

Meanwhile, if an employed bee exhausts a nectar source, it then becomes a scout bee and is appointed for a completely new nectar source in scout bee phase. It means that if a solution that cannot be improved after a predetermined number of essays called "limit," a new solution is generated using Eq. (1) (Step 10). The best solution achieved at the end of a cycle is recorded (Step 11). Finally, if the cycles reach to the MNC, ABC is stopped for the best decision variables (Step 12).

3.2 The considered two objective functions for multi-objective optimization

Chaotic maps are generally employed in the IESs to produce a diverse sequence in accordance with the initial value and control parameter. The pixels of image to be encrypted are hereby scrambled and manipulated through the produced sequence by chaotic map. The following conventional logistic map is delivered in order to express the evaluation for chaotic maps.

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

where v_i is the initial value, and $u \in [0,4]$ is the control parameter (growing rate). We need appropriate evaluation that is able measure chaotic performance of the maps, which will be used as objective functions in the optimization process. LE whose equation given below is a well-known and effective measurement [45].

$$\text{LE} = \lim_{n\to\infty} \sum_{i=1}^{n-1} \ln|f'(v_i)| \quad (6)$$

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

The other impactful evaluation that can be considered for the optimization is the information entropy of the sequence of the chaotic map. The information entropy is modified as follows for objective function.

$$Y = floor(256v_i) \quad (7)$$

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

where Y is the sequence of the chaotic map v_i that adapted to be between 0 and 255. $p(y_i)$ is probability of this sequence. Therefore, increasing the information entropy of the sequence is also improving the information entropy of the ciphertext image. The chaotic map will be optimized by maximizing the two objective functions LE and H. While the divergence and thus permutation performance of the chaotic map is herewith improved by increasing the LE, the diffusion performance is enhanced by augmenting H.

3.3 Implementation of ABC to the optimization of OCM

In the constitution of the OCM, it is inspired by the existing maps in the literature (See Sect. 6). Thence, different chaotic map models are empirically essayed in the constitution. A chaotic map model including decision variables is considered to be optimized for improving the multiple objectives. The considered

OCM, which gives the best objective value, is given below:

$$v_{i+1} = mod((\exp(\alpha_1) + u^{\alpha_2})(\alpha_3 + \alpha_4 v_i), 1) \quad (9)$$

The model includes four unknown coefficients $\alpha_j, j \in [1, 4]$ regarding as the decision variables in the optimization process. The variables are optimally found out by maximizing the two objectives of of_1 and of_2 as follows:

$$of_1 = \overline{\mathrm{LE}} \quad (10)$$

$$of_2 = \bar{H} \quad (11)$$

where $\overline{\mathrm{LE}}$ and $\bar{H}$ are the mean of LE and H, respectively. The two objective functions compose a single minimizing objective function as given below:

$$F = w_1 \times \frac{1}{of_1} + w_2 \times (8 - of_2) \quad (12)$$

here, w_1 and w_2 are the weight factors chosen as 1 and 99, respectively. These two factors are determined as trade-off with the numerous trials. The two objective functions are converted to be minimized by taking $1/of_1$ and $8 - of_2$, where 8 is the maximum value of the information entropy that it can get. Therefore, the fitness function of ABC can be constituted as follows:

$$\mathrm{fit}_i = \frac{1}{1 + F_i(x)} \quad (13)$$

fit_i is the fitness value of each candidate solution.

The OCM is optimized to find out the unknown variables using ABC for minimizing the multi-objective function F in Eq. (12). In ABC, the NP, MCN and limit are taken as 40, 1000 and 20. $x_{\max}$ and $x_{\min}$ are set as 10 and 0.1. The convergence tendency of the optimization cycles is plotted in Fig. 2. After approximately 750 cycles, the optimization converges to the final objective value. In the optimization, it is aimed to find out the decision variables embedded in the OCM to be integer for the sake of simplicity. Therefore, the determined variables of the OCM are given in Table 1. The ultimate OCM where the variables are substituted is given below:

$$v_{i+1} = mod\left(\left(\exp(10) + u^2\right)(9 + 7v_i), 1\right) \quad (14)$$

here, v_i and u are the initial value and control parameter of OCM, respectively.

4 Metrics for the appreciation of OCM

Figure 3 demonstrates the dynamic and chaotic performance of the OCM. In Fig. 3a, the bifurcation diagram of the OCM is scattered for 10^3 iterations, which manifests the diversity and ergodicity of the OCM. For a high diverse system, the bifurcation points in the graph are expected that they should be so-sudden and adjacent for different the control parameters without any space. Figure 3b shows 3D phase space chaotic trajectory of the OCM to investigate its dynamical behavior. The chaotic trajectory demonstrates the dynamic behavior of a system in multi-dimensional phase space. A non-dynamic system shows periodic behaviors represent closed curves, whereas a dynamic behavior is expected to occupy the whole phase space instead of representing repetitive paths as parallel with the dynamic capability.

The chaotic and complexity performance of the OCM is investigated in terms of reliable metrics like LE, PE and SE in Fig. 4. They are compared with those reported in the literature [18, 19, 21, 22, 30, 31, 45] to validate the OCM's superior chaotic performance. The LE plots of the chaotic maps are given in Fig. 4a. For better chaotic capability, LE should be positively as high and stable as possible. Recall that the LE of the conventional logistic map is positive and less than one only for $u \in [3.57, 4)$. Even though the best of the reported LEs is about positive 5 [18, 21], the LE of the OCM is prominent among those reported as it is positive 12 and shows stable characteristic. In Fig. 4b, the PE variations of the chaotic maps are comparatively

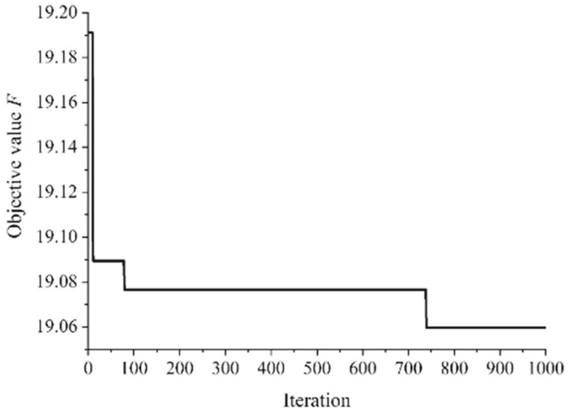
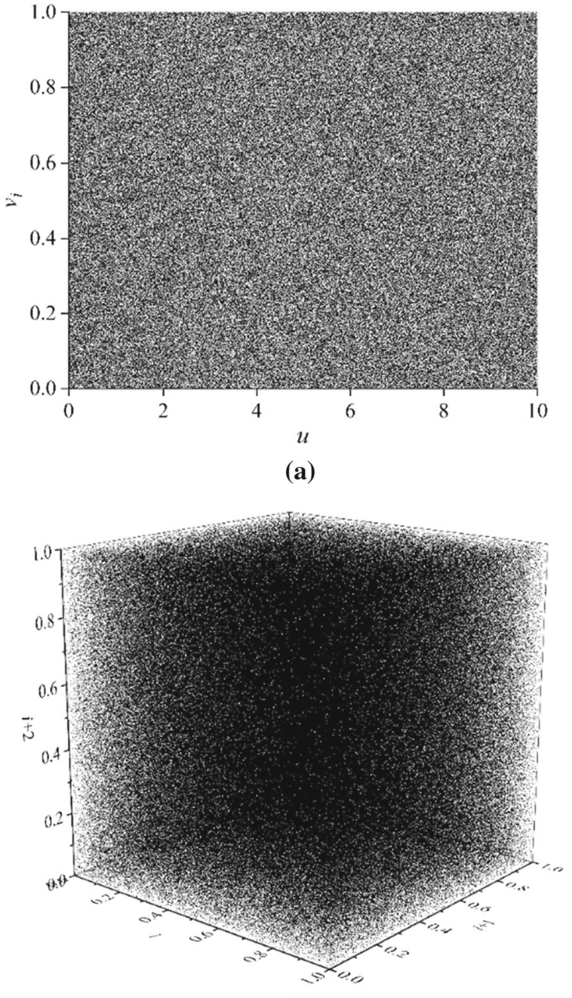


Fig. 2 The convergence tendency of the optimization of the OCM using ABC

Table 1 The optimally found coefficients of the OCM by ABC

α_j	α_1	α_2	α_3	α_4
Variable	10	2	9	7

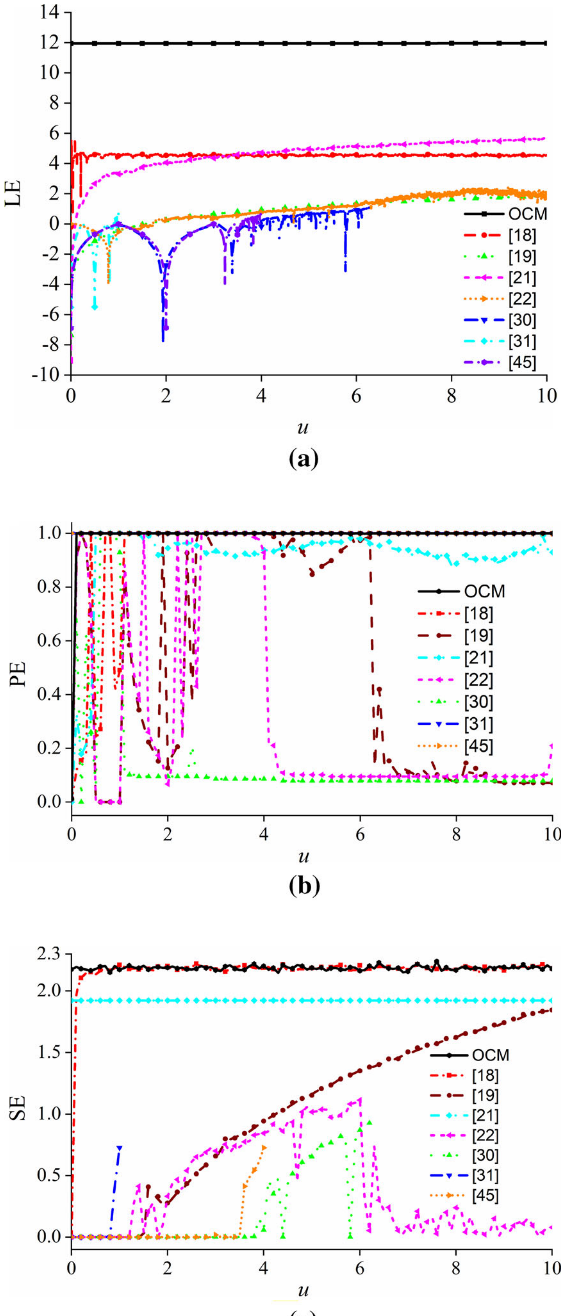


(a)

(b)

Fig. 3 Dynamic performance of the OCM: **a** bifurcation diagram for 10^3 iterations, **b** 3D chaotic trajectory for 10^6 iterations

presented. It is also a precise metric of the complexity of a dynamic system [46] that appreciated if how it is high. The PE of OCM is computed for embedding dimension 2 and time delay, and thus, it can be maximally 1. Therefore, the PE of OCM is the best with value of 1 among the others. In Fig. 4c, the SE of



(a)

(b)

(c)

Fig. 4 Appreciation of the OCM using metrics: **a** LE, **b** PE, **c** SE

the dynamic systems are given, which is able to measure the complexity of a dynamic system [23]. It can be used to degrade the similarity of the sequence generated by a chaotic map. The higher the SE, more complex the dynamic system. The OCM evidently shows higher complexity with about 2.2 than the state of the arts. Eventually, the OCM has the best results for all considered metrics thanks to the optimal chaotic map properties.

In order for verifying the randomness ability of the OCM, NIST SP800-22 test suit [47] consisting of 15 sub-tests is performed for both a sequence of OCM and a ciphertext image by the IES with OCM. The achieved probability P values are tabulated in Table 2. According to NIST, they are expected to be greater than 0.01 for passing the tests. It is clearly seen from the table, the OCM successfully passes all results not only for sequence but also ciphertext images thanks to its optimal complexity and randomness properties.

5 The proposed IES with OCM

In this section, first, the achievement of the initial value and control parameter will elaborate, and then, the encrypting operations of the IES will step-by-step introduced.

5.1 Achieving the initial value and control parameter

In the IES, first, the public key is generated from the plaintext image. Then, a main key is obtained by XOR operation between the public key and a secret key. The initial value v and control parameter u are achieved using the main key to produce chaotic sequences via the OCM. The chaotic sequences are employed in the permutation and diffusion operations. The achieving of the initial values and control parameters is defined in Algorithm 2 and illustrated in Fig. 5 over an example for the Lena image. In Step 1, the plaintext image is imported to form vector A with sized of $m \times n$. In Step 2, the public key is generated by calculating three vectors A_{01}, A_{02} and A_{03} that extracted from the plaintext image. Vector A_{01} size of m is the sum of the pixel values of all rows. Vector A_{02} size of n is the sum of the pixel values of all columns. Vector A_{03} size of $m + n - 1$ is the sum of all diagonal pixel values. Afterward, the public key matrix B is produced through the combination of SHA-512 and MD5 hash from these three vectors A_{01}, A_{02} and A_{03}. In Step 3, a secret key matrix C is constructed. In Step 4, the main key matrix D is obtained by XOR operation between the public and secret key. In Step 5, the main key is divided into four submatrices, and then, the columns of each submatrix in self are subjected a series of transaction $\text{mod}(\text{sum}(E, 2), 2)$. The outcome of each submatrix 8×1 is combined to form E matrix size of 8×4. In Step 6, the binary matrix F is converted to a decimal matrix F. Eventually, in Steps 7 and 8, the initial values $V := [v_1 \quad v_2]$ and control parameters $U := [u_1 \quad u_2]$ are, respectively, achieved by transactions $\frac{f_{1i}}{256}$ and $\frac{f_{1,i+4}}{256} + \text{mod}(f_{1,i+4}, 10)$.

Algorithm 2: Achieving of the initial value and control parameter

```
Step 1. Read an image matrix $A$
Step 2. Generate a public key $B \coloneqq [b_{1p}]_{1\times512}$ by SHA-512/MD5 hash value from the plaintext image
Step 3. Construct a secret key $C \coloneqq [c_{1p}]_{1\times512}$ that a binary row matrix
Step 4. Evaluate the main key $D \coloneqq B$ XOR $C$ and reshape $D$ to 8×16×4 in shape
Step 5. Compute $E \coloneqq \text{mod}(\text{sum}(D,2),2)$ and then reshape $E$ to 8×4 in shape where $\text{sum}(D,2)$ means the sum
        of the rows of each submatrix in shape 8×16 of $D$
Step 6. Figure out $F \coloneqq [128\ 64\ 32\ 16\ 8\ 4\ 2\ 1]E$
Step 7. Achieve the initial values $v_i \leftarrow \frac{f_{1i}}{256}, i \in \{1,2\}$
Step 8. Achieve the control parameters $u_i \leftarrow \frac{f_{1,i+2}}{256} + \text{mod}(f_{1,i+2}, 10), i \in \{1,2\}$
```

Table 2 The results of NIST SP 800-22 test

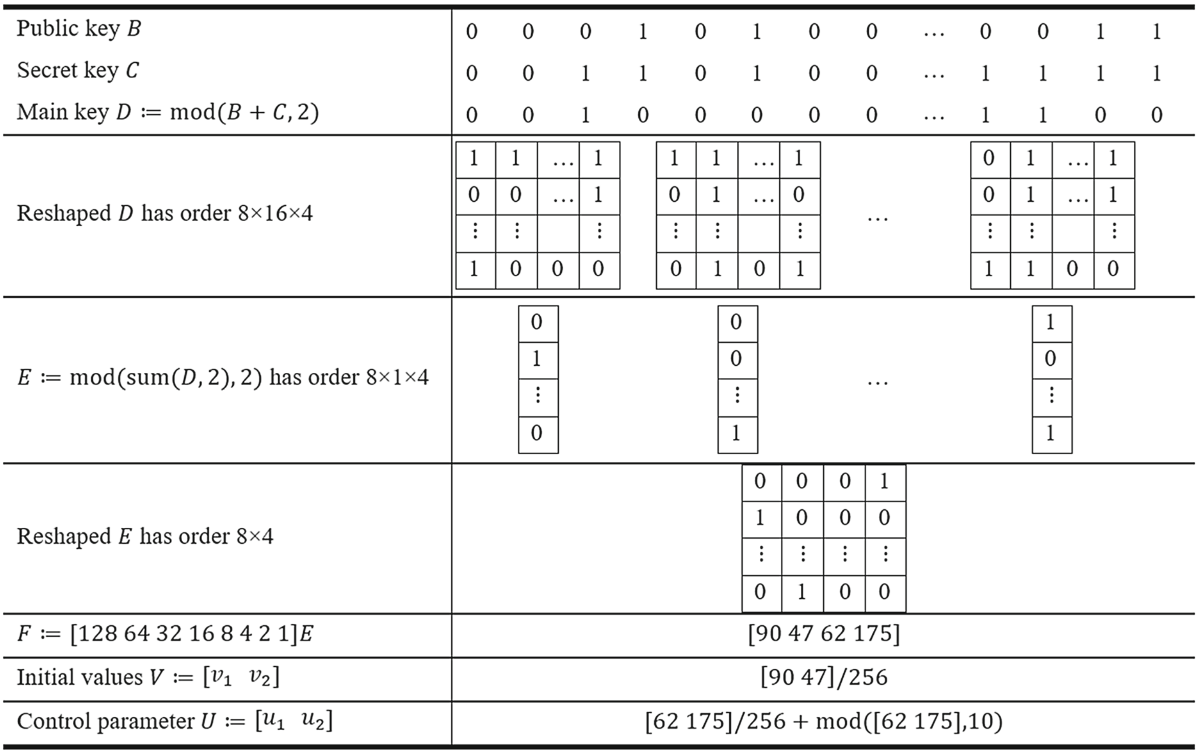
Statistical test	P value	
	Sequence of OCM	Ciphertext image of Lena
Frequency	0.894984	0.897432
Block frequency	0.837977	0.989848
Runs	0.922355	0.811463
Longest run	0.923137	0.854344
Rank	0.975543	0.821333
FFF	0.791282	0.755145
Nonoverlapping template (average)	0.443004	0.550344
Overlapping template	0.976047	0.969338
Universal	0.809425	0.911442
Serial	0.849237	0.948414
Approximate entropy	0.689774	0.992916
Cumulative sums (forward) test	0.832407	0.904994
Random excursions	0.896164	0.882079
Random excursions variant	0.879257	0.941958
Linear complexity	0.518899	0.913205

5.2 The operations of the IES

Algorithm 3 manages the proposed IES with the OCM through the permutation and diffusion operations for an illustrative example for 5 × 5 pixel sample of the Lena image in Fig. 6. The pixels are scrambled positionally and manipulated in tonal values across the two operations governed by the OCM. The initial values V and control parameters U have been achieved as stated above. In Step 1 and 4, they are used as input to the OCM for production of the chaotic sequences X_1 and X_2. In the permutation, Step 2, the chaotic sequence matrix X_1 is sorted in ascending order to form matrix Y_1. In Step 3, the positions of the pixels are shuffled in accordance with the position of the sorted sequence, and thus, the permutated matrix A_1 is revealed. In the diffusion, Step 5, a row matrix Y_2 is obtained to be utilized in the diffusion operation. In Step 6, the permutated matrix A_1 is incurred an XOR operation with the matrix Y_2 in order for diffusing the pixel values, and finally, the diffused matrix A_2 is accomplished as the ciphertext image.

Algorithm 3: Step by step the operations of the IES with the OCM

```
//Permutation
Step 1. Produce the first chaotic sequence $X_1 := [x^1_{1r}]_{1\times mn}$ by using the initial value $v_1$, the control parameter
        $u_1$via the OCM (see Eq. (3))
Step 2. Form $Y_1 := [y^1_{1r}]_{1\times mn}$ by sorting $X_1$ in ascending order
Step 3. Calculate a permutated matrix $A_1 := [a^1_{kl}]_{m\times n}$ defined by $a^1_{kl} := a_{ij}$ such that $x^1_{1,n(i-1)+j} = y^1_{1,n(k-1)+l}$
//Diffusion
Step 4. Produce the second chaotic sequence $X_2 := [x^2_{1r}]_{1\times mn}$ by using the initial value $v_2$, the control parameter
        $u_2$, and the OCM
Step 5. Constitute the row matrix $Y_2 := [y^2_{1r}]_{1\times mn}$ defined by $Y_2 := \text{floor}(256X_2)$ and then reshape $Y_2$ to $m\times n$ in
        shape
Step 6. Accomplish the diffused matrix $A_2 := [a^2_{kl}]_{m\times n}$ defined by $A_2 := A_1 \oplus Y_2$
```



Public key B	0 0 0 1 0 1 0 0 … 0 0 1 1
Secret key C	0 0 1 1 0 1 0 0 … 1 1 1 1
Main key $D \coloneqq \mathrm{mod}(B + C, 2)$	0 0 1 0 0 0 0 0 … 1 1 0 0
Reshaped D has order 8×16×4	$\begin{array}{\|c\|c\|c\|c\|}\hline 1 & 1 & \dots & 1 \\ \hline 0 & 0 & \dots & 1 \\ \hline \vdots & \vdots & & \vdots \\ \hline 1 & 0 & 0 & 0 \\ \hline \end{array}$ $\begin{array}{\|c\|c\|c\|c\|}\hline 1 & 1 & \dots & 1 \\ \hline 0 & 1 & \dots & 0 \\ \hline \vdots & \vdots & & \vdots \\ \hline 0 & 1 & 0 & 1 \\ \hline \end{array}$ … $\begin{array}{\|c\|c\|c\|c\|}\hline 0 & 1 & \dots & 1 \\ \hline 0 & 1 & \dots & 1 \\ \hline \vdots & \vdots & & \vdots \\ \hline 1 & 1 & 0 & 0 \\ \hline \end{array}$
$E \coloneqq \mathrm{mod}(\mathrm{sum}(D, 2), 2)$ has order 8×1×4	$\begin{array}{\|c\|}\hline 0 \\ \hline 1 \\ \hline \vdots \\ \hline 0 \\ \hline \end{array}$ $\begin{array}{\|c\|}\hline 0 \\ \hline 0 \\ \hline \vdots \\ \hline 1 \\ \hline \end{array}$ … $\begin{array}{\|c\|}\hline 1 \\ \hline 0 \\ \hline \vdots \\ \hline 1 \\ \hline \end{array}$
Reshaped E has order 8×4	$\begin{array}{\|c\|c\|c\|c\|}\hline 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline 0 & 1 & 0 & 0 \\ \hline \end{array}$
$F \coloneqq [128\ 64\ 32\ 16\ 8\ 4\ 2\ 1]E$	[90 47 62 175]
Initial values $V \coloneqq [v_1\ \ v_2]$	[90 47]/256
Control parameter $U \coloneqq [u_1\ \ u_2]$	[62 175]/256 + mod([62 175],10)

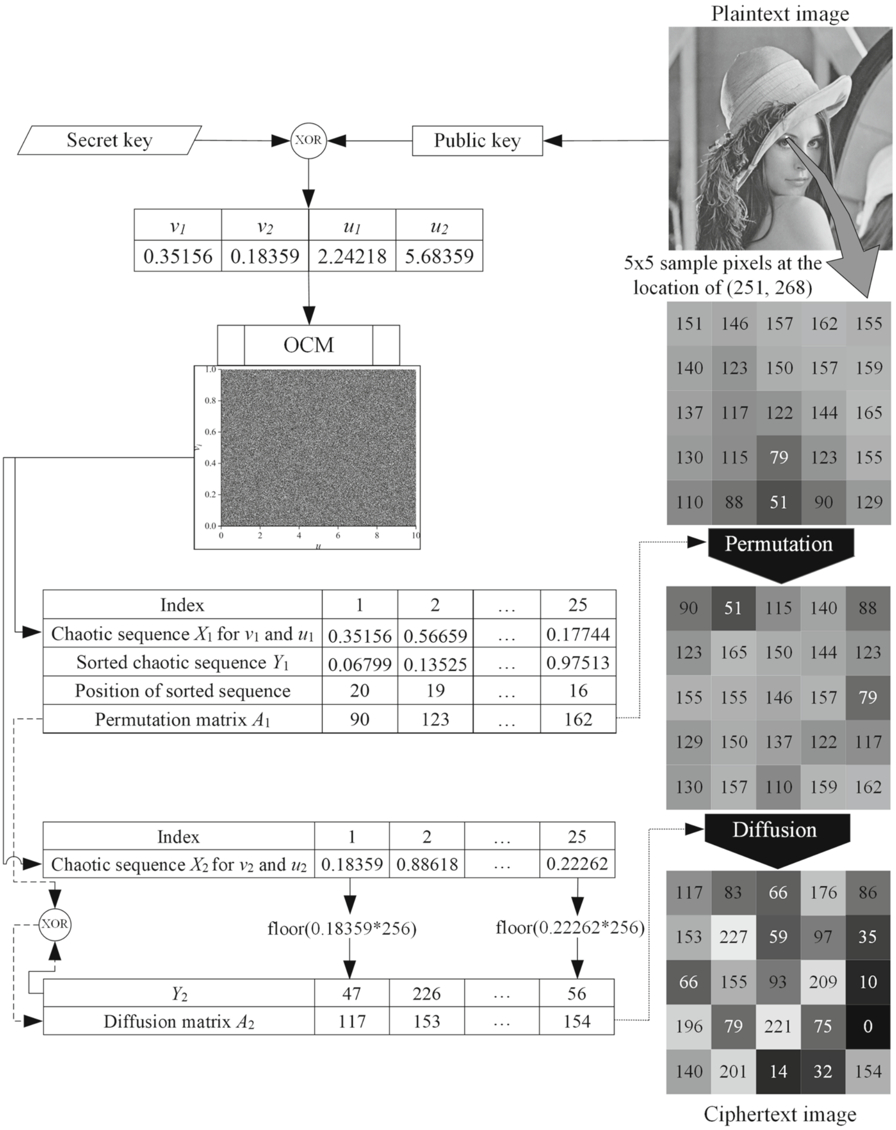
Fig. 5 The procedure for achieving the initial values and control parameters

6 Cryptanalyses and comparison

The security level of an IES should be evaluated by simulating some cyberattacks [13]. The well-known and reliable cryptanalysis is key-space, key sensitivity, information entropy, histogram, correlation, differential attack, noisy attack and cropping attack. These cryptanalyses are performed on a diverse image set with size 512 × 512. The IES is operated at MATLAB R2020b running on a workstation with I(R) Xeon(R) CPU E5-1620 v4 @ 3.5 GHz, and 64 GB RAM. The visual and numerical cryptanalyses are also compared with available the-state-of-the-art results [14, 16, 19–21, 24, 28, 30, 48–52].

6.1 Key-space analysis

There are various cyberattacks such as brute-force depend on predicting the key by attempting numerous passwords. A ciphertext with a short key is hence indefensible to such attack in a short time. On the other hands, 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 if it is longer than 2^{100} [53]. In our IES, a SHA 512-bit-length key is used, and thus, it is eight floating numbers with 10^{15} precision, which used as the initial values and control parameters of the OCM. The key-space analysis is therefore $10^{15\times4} = 10^{60} \cong 2^{199}$ that is higher than 2^{100}.



v_1	v_2	u_1	u_2
0.35156	0.18359	2.24218	5.68359

Index	1	2	…	25
Chaotic sequence X_1 for v_1 and u_1	0.35156	0.56659	…	0.17744
Sorted chaotic sequence Y_1	0.06799	0.13525	…	0.97513
Position of sorted sequence	20	19	…	16
Permutation matrix A_1	90	123	…	162

Index	1	2	…	25
Chaotic sequence X_2 for v_2 and u_2	0.18359	0.88618	…	0.22262

Y_2	47	226	…	56
Diffusion matrix A_2	117	153	…	154

151	146	157	162	155
140	123	150	157	159
137	117	122	144	165
130	115	79	123	155
110	88	51	90	129

90	51	115	140	88
123	165	150	144	123
155	155	146	157	79
129	150	137	122	117
130	157	110	159	162

117	83	66	176	86
153	227	59	97	35
66	155	93	209	10
196	79	221	75	0
140	201	14	32	154

Fig. 6 Step-by-step the proposed IES with the OCM through an illustrative example

6.2 Key sensitivity analysis

An IES must be sensitive to the key, meaning that a minor change in the key yields a major variation in the ciphertext image. In order to analysis the key sensitivity, five secret keys that are original key and its one-digit changed version are given in Table 3. The ciphertext images that are encrypted with those keys are shown in Fig. 6. Their differential images are illustrated to see the number of pixels having the same tonal values which would seem black color due to zero difference. From Fig. 7g–j, there does not seem any black region.

Table 4 includes numerical results related to the distinctive level of the differential images to assess the key sensitivity. The distinctive levels are achieved as 99.6028%, 99.5975%, 99.6257% and 99.6051%, respectively, for Key 2, 3, 4 and 5, and mean of these levels as 99.6164%. It is evident from the results that the proposed IES is very sensitive to the key thanks to the diversity performance of the OCM.

In the other visual analyses regarding the key sensitivity, it is aimed to investigate if the decrypted ciphertext images with the one-digit changed keys involve any information belonging to the plaintext image. The decipher image with the one-digit changed must be very different of the original plaintext image. The ciphertext images which are encrypted with the one-digit changed keys are decrypted and comparatively showed in Fig. 8. The ciphertext image with the original key is correctly decrypted as is excepted, while the other decipher images are very confusing and far from the original plaintext image.

6.3 Histogram analysis

Histogram is a graph that represents the repetition frequency of the pixel's tonal value. In this way, the uniformity of the image pixels can be examined, and herewith, the manipulation performance of the OCM can be appreciated. Therefore, the manipulation performance of IES is regarded high as uniform as the histogram is. The histograms of the plaintext images Lena, Cameraman, Baboon, Peppers, Airplane and Barbara and the related ciphertext images are observed in Fig. 9. As can be seen that the proposed IES with the OCM uniformly modifies the tonal value. It means that the IES is resistant to the statistical attacks, i.e., one cannot deduce any information from the ciphertext images.

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

$$var(\boldsymbol{X}) = \frac{1}{n^2}\sum_{i=0}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(x_i - x_j\right)^2 \tag{15}$$

$$\chi^2 = \sum_{i=0}^{255}\frac{\left(n_i - n/256\right)^2}{n/256} \tag{16}$$

here, n_i is the repetition frequency of the tonal value i and n is the number of total pixels. $n/256$ is the expected repetition frequency of every tonal value. $X = \{x_1, x_2, \ldots, x_{256}\}$ is the vector of the histogram's tonal 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 hands, $\chi^2(0.05; 255)$ should be lower than 293.25 for verifying the significant level 0.05 of χ^2 test [54]. The results regarding the variance and χ^2 tests are listed in Table 5 for the images under the histogram analysis in Fig. 9. The proposed IES with the OCM is hence corroborated with regard to the results for all the images under the analysis.

6.4 Information entropy analysis

Information entropy is mostly exploited to evaluate the uncertainty and disorderliness of an image [4]. Recall that the information entropy in Eq. (8) is even used as one of the objective functions of the OCM in the optimization. With the use of information entropy, the manipulation performance of a chaotic map can be assessed. The information entropy of an image is appreciated how it is close to 8 which is the maximum value. The information entropy of the under-test images encrypted using the proposed IES with the OCM is given in Table 6, and they are compared with the available results in the literature [14, 19–21, 24, 28, 30] in Table 7. It is evident from Table 6 that all entropies are very close to 8. Furthermore, the ciphertext images by proposed IES with the OCM have the closest information entropy with 7.9994 among the other IESs reported elsewhere [14, 19–21, 24, 28, 30]. Therefore, the proposed IES with the OCM provides the most assured images against cyberattacks.

6.5 Correlation analysis

This analysis uses the evaluation of the correlation between the adjacent pixels. It is expected that an IES securely reduces the correlation of a ciphertext image as much as possible. The correlation coefficient of an image is computed in the three directions: horizontal, vertical and diagonal as follows:

$$r_{xy} = \frac{E[x - E(x)][y - E(y)]}{\sqrt{D(x)\sqrt{D(y)}}} \tag{17}$$

here, the sub-equations are $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x)]^2$. x_i and y_i are the tonal values of ith pair of the adjacent pixels, and N stands for the number of the pixel samples. In our study, $N = 3600$ pixel samples are randomly selected from the ciphertext image.

The correlation coefficients of the encrypted under-test images using the proposed IES are given in Table 8, and also they are compared with the available results in the literature in Table 9 [14, 19–21, 24, 28, 30]. As can be seen from Table 8,

Table 3 A secret key and its one-digit changed versions

Key	SHA-512
Key 1 (original)	0011010000011010010100110111001100001001000000011101010100011110…01111
Key 2 (changed)	0100010000011010010100110111001100001001000000011101010100011110…01111
Key 3 (changed)	0101010000011010010100110111001100001001000000011101010100011110…01111
Key 4 (changed)	0110010000011010010100110111001100001001000000011101010100011110…01111
Key 5 (changed)	0111010000011010010100110111001100001001000000011101010100011110…01111

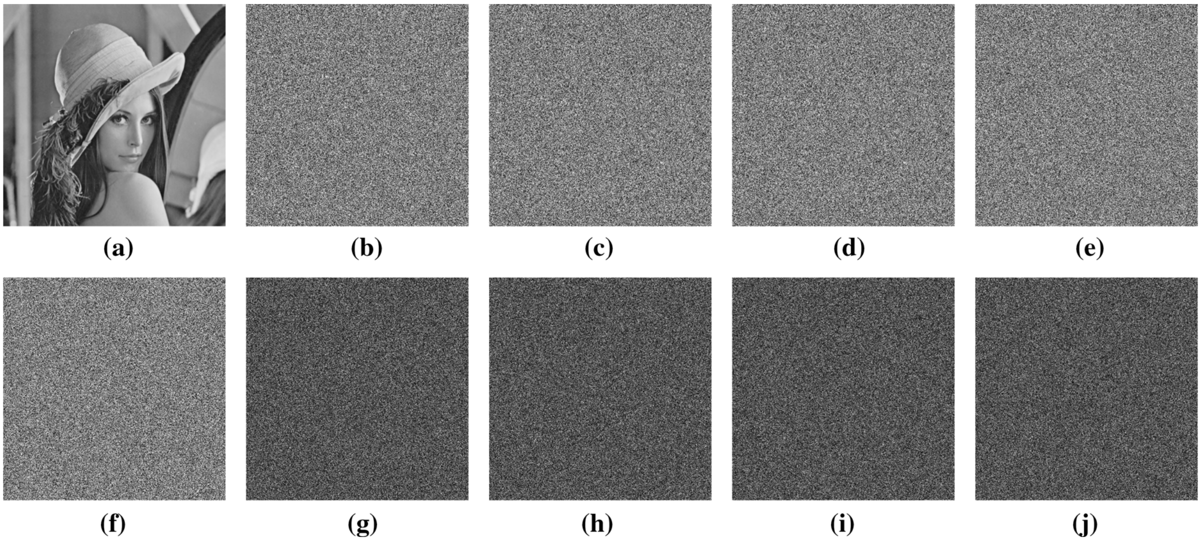


Fig. 7 Key sensitivity analysis for Lena image: **a** plaintext image; **b** ciphertext with key 1; **c** ciphertext with key 2; **d** ciphertext with key 3; **e** ciphertext with key 4; **f** ciphertext with key 5; **g** differential image between (**b**) and (**c**); **h** differential image between (**b**) and (**d**); **i** differential image between (**b**) and (**e**); **j** differential image between (**b**) and (**f**)

Table 4 The numerical differences among ciphertext images with one-digit changed keys

Figures	Encryption keys	Difference with 7b (%)
7c	Key 2	99.6028
7d	Key 3	99.5975
7e	Key 4	99.6257
7f	Key 5	99.6051
Mean		99.6078

the proposed IES with the OCM minimizes the correlation coefficients as close as to zero. Moreover, it surpasses the IESs in the literature in views of the correlation coefficients given in Table 9.

The correlation distribution of the Lena's plaintext and ciphertext images is shown in Fig. 10 in the three dimensions. Given that the correlation distribution of a mono-color image would be a point. Hence, the distribution of a totally correlated pixel would be on $y = x$ line. The correlation coefficients of Lena's plaintext image are 0.9369, 0.9552 and 0.9085 for the three directions of the horizontal, vertical and diagonal, respectively. The respective correlation distributions mostly intensify on $y = x$ line. Whereas that of the ciphertext image uniformly scatter due to very low correlation coefficients of -26×10^{-5}, -11×10^{-5} and -15×10^{-5} from Table 9.

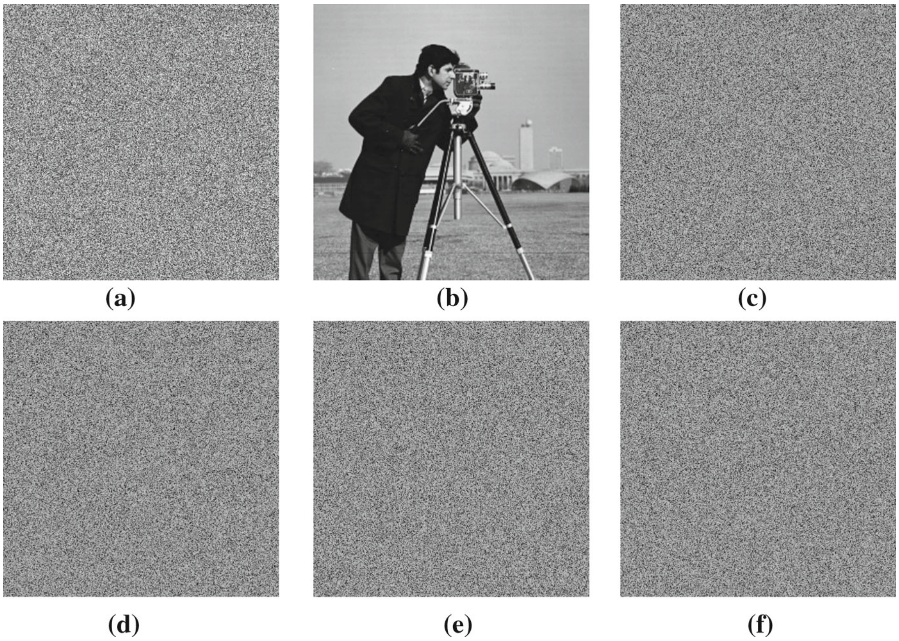


Fig. 8 Key sensitivity for Cameraman image: **a** ciphertext image with key 1 (original); **b** decipher image with key 1; **c** decipher image with key 2; **d** cipher image with key 3; **e** decipher image with key 4; **f** decipher image with key 5

6.6 Differential attack analysis

Differential attack attempts to resolve the key and discover the IES by investigating the differences. Differential analysis puts to proof the IES against the cyberattacks by analyzing the difference between the plaintext and ciphertext images of which a few bits in the plaintext image are changed. In this wise, both permutation and manipulation performances of an IES can be evaluated that whether it is sensitive to a bit change in the plaintext image. Differential attack analysis is apprised with the following NPCR and UACI.

$$D(i,j) = \begin{cases} 0, & \text{if } C^1(i,j) = C^2(i,j) \\ 1, & \text{if } C^1(i,j) \neq C^2(i,j) \end{cases} \tag{18}$$

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \tag{19}$$

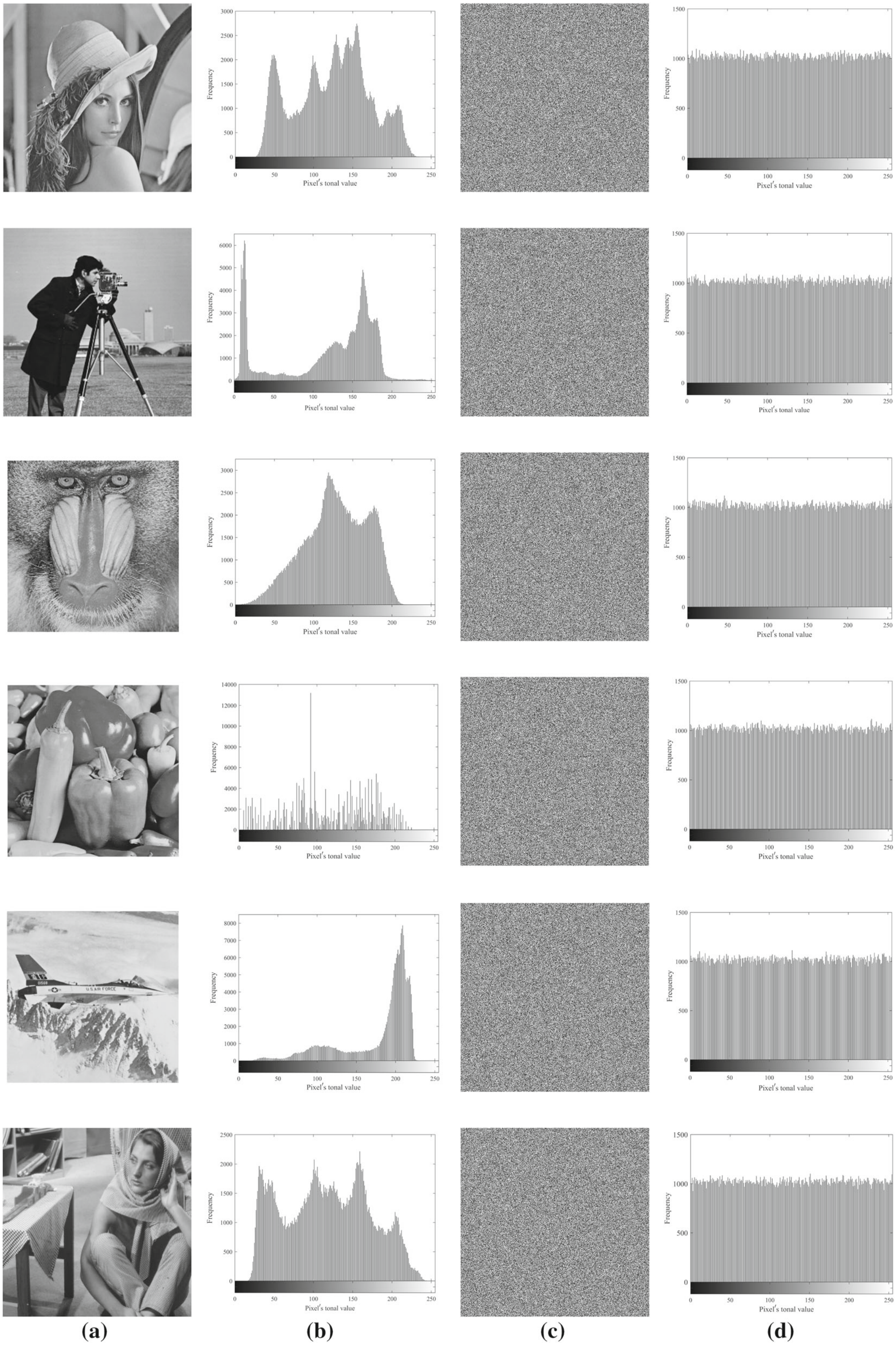
$$\text{UACI} = \frac{1}{m \times n}\left[\sum_{i,j} \frac{\left|C^1(i,j) - C^2(i,j)\right|}{255}\right] \times 100\% \tag{20}$$

here, m and n refer to the height and width of the image under-test. 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 [55]. The NPCR and UACI results of the under-test images encrypted via the proposed OCM-based IES are given in Table 10, and they are compared with those of reported elsewhere in Table 11. It is clearly seen that the results of the proposed IES with the OCM are the closest to the ideal targets.

6.7 Cropping attack analysis

Cropping attack analysis is able to prove an IES for losing or abusing some parts of the ciphertext images. Cropping attack analysis herewith evaluates the robustness of an IES in terms of both the permutation and manipulation performance. Therefore, a reliable and robust IES is able to decrypt a cropped image with the minimum corruption. For analyzing the proposed IES, the ciphertext image of the Peppers cropped with the ratios of 1/16, 1/16 (middle), 1/4, 1/2, and their decipher images are disclosed in Fig. 11. Moreover, the 1/16 cropped image is compared with the reported results in the literature in Fig. 12. From the visual results, the proposed OCM-based IES maximally decrypts the cropped images with the least corruption.

Moreover, the cipher images of the cropped Lena images the proposed IES are assessed in numerical in terms of PSNR given in Eq. (21) measuring the image


Frequency
Pixel's tonal value
0
50
100
150
200
250
500
1000
1500
2000
2500
3000
4000
5000
6000
7000
8000
10000
12000
14000
(a)
(b)
(c)
(d)

◀**Fig. 9** Histograms of the images under analysis: **a** the plaintext images, **b** histograms of the plaintext images, **c** the ciphertext images, **d** the histograms of ciphertext images

quality by comparing to the plaintext images [56]. Hence, the higher the PSNR, the lower the corruption. The PSNR scores of the decipher images via the proposed IES with the OCM are listed in Table 12, and those of the Lena are compared with the other results in Table 13 [24, 50]. Thanks to the higher PSNR, the cropping attack performance of the proposed IES is corroborated as well as the illustrated results in Fig. 12.

$$\mathrm{PSNR} := 10\log\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{21}$$

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

Table 5 Variance and χ^2 test results of the images under the histogram analysis

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	953.26	960.51	945.68	948.27	968.24	975.43
χ^2	Plaintext	158,344.71	418,530.14	549,151.27	211,365.83	95,548.87	708,178.59
	Ciphertext	239.66	232.85	231.69	238.65	235.31	233.57

Table 6 Entropies of the plaintext and ciphertext images by the proposed IES with OCM

Image	Lena	Cameraman	Baboon	Peppers	Barbara	Airplane
Plaintext image	7.4455	7.0479	7.2925	6.7624	7.6321	6.7135
Ciphertext image	7.9994	7.9994	7.9994	7.9994	7.9994	7.9994

Table 7 The entropies of the ciphertext images and the comparison with the literature

Ciphertext image	Ref. [24]	Ref. [19]	Ref. [30]	Ref. [14]	Ref. [20]	Ref. [21]	Ref. [28]	OCM
Lena	7.9994	7.9993	7.9993	7.9975	7.9994	7.9970	7.9982	7.9994
Cameraman	7.9970	–	–	–	7.9993	7.9973	–	7.9994
Peppers	–	–	7.9994	–	7.9993	7.9969	–	7.9994
Barbara	–	7.9992	–	7.9985	–	–	7.9981	7.9994

Table 8 Correlation coefficients of the under-test ciphertext images

Direction	Lena	Cameraman	Baboon	Peppers	Barbara	Airplane
Horizontal	26×10^{-5}	-17×10^{-5}	43×10^{-5}	-32×10^{-6}	26×10^{-5}	15×10^{-5}
Vertical	11×10^{-5}	05×10^{-5}	19×10^{-6}	16×10^{-5}	-21×10^{-6}	24×10^{-6}
Diagonal	15×10^{-5}	-20×10^{-5}	13×10^{-6}	-28×10^{-6}	-32×10^{-6}	34×10^{-6}

Table 9 The correlation coefficients of the ciphertext images and the comparison with the literature

Ciphertext image	Dir	Ref. [24]	Ref. [19]	Ref. [30]	Ref. [14]	Ref. [20]	Ref. [21]	Ref. [28]	OCM
Lena	H	73×10^{-5}	13×10^{-3}	10×10^{-4}	27×10^{-4}	32×10^{-4}	22×10^{-4}	14×10^{-4}	-26×10^{-5}
	V	44×10^{-5}	17×10^{-3}	-15×10^{-4}	13×10^{-4}	16×10^{-4}	13×10^{-4}	14×10^{-4}	11×10^{-5}
	D	36×10^{-5}	67×10^{-5}	26×10^{-4}	11×10^{-4}	23×10^{-4}	8×10^{-4}	12×10^{-4}	15×10^{-5}
Cameraman	H	93×10^{-4}	–	–	–	14×10^{-4}	39×10^{-4}	–	-17×10^{-5}
	V	10×10^{-5}	–	–	–	2×10^{-4}	7×10^{-4}	–	05×10^{-5}
	D	31×10^{-4}	–	–	–	35×10^{-4}	86×10^{-4}	–	-20×10^{-4}
Peppers	H	–	–	7×10^{-5}	–	6×10^{-4}	1×10^{-4}	–	-32×10^{-6}
	V	–	–	43×10^{-4}	–	38×10^{-4}	-26×10^{-4}	–	16×10^{-5}
	D	–	–	-18×10^{-4}	–	10×10^{-4}	$- 23 \times 10^{-4}$	–	$- 28 \times 10^{-6}$
Barbara	H	–	$- 70 \times 10^{-4}$	–	$- 13 \times 10^{-4}$	–	–	12×10^{-4}	26×10^{-5}
	V	–	$- 79 \times 10^{-4}$	–	43×10^{-4}	–	–	27×10^{-4}	$- 21 \times 10^{-6}$
	D	–	$- 22 \times 10^{-3}$	–	10×10^{-4}	–	–	$- 10 \times 10^{-4}$	$- 32 \times 10^{-6}$

Dir direction, *H* horizontal, *V* vertical, *D* diagonal

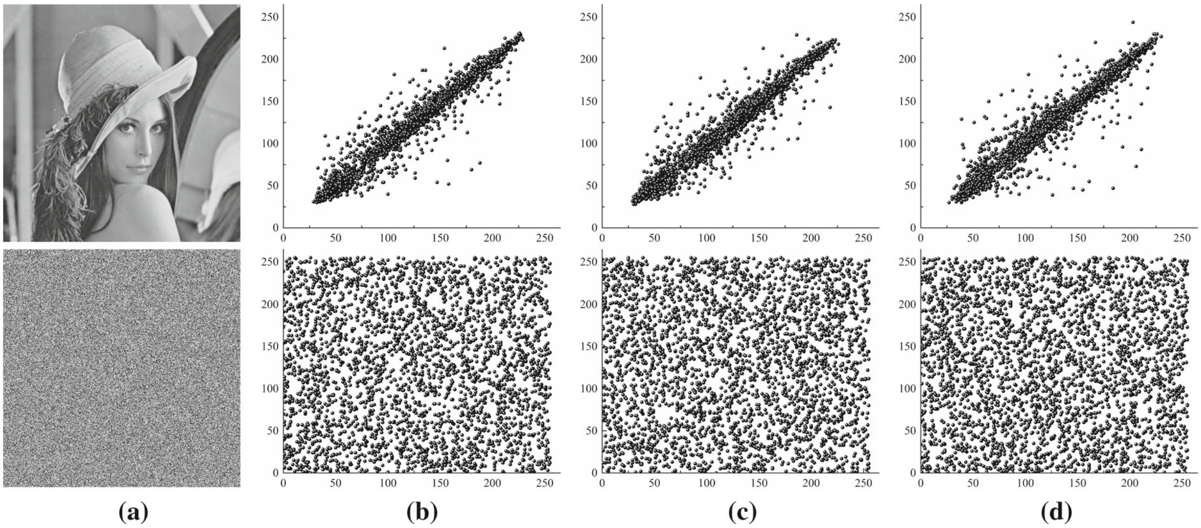


Fig. 10 The correlation distribution for the three directions: **a** the Lena's image, **b** horizontal, **c** vertical, **d** diagonal

Table 10 The NPCR and UACI results for the under-test images encrypted via the proposed IES

Direction	Lena	Cameraman	Baboon	Peppers	Barbara	Airplane
NPCR	99.6089	99.6086	99.6093	99.6089	99.6088	99.6094
UACI	33.4691	33.4585	33.4586	33.4689	33.4697	33.4595

Table 11 The NPCR and UACI results and the comparison

Image	Test	Ref. [24]	Ref. [19]	Ref. [30]	Ref. [14]	Ref. [20]	Ref. [21]	Ref. [28]	OCM
Lena	NPCR	99.6078	99.5800	99.6000	99.6912	99.6000	99.60934	99.6621	99.6089
	UACI	33.4268	33.4300	33.4700	33.5098	33.5000	33.45969	33.5278	33.4691
Cameraman	NPCR	99.6323		–	–	99.6000	99.60683	–	99.6086
	UACI	33.4096		–	–	33.5500	33.44610	–	33.4585
Peppers	NPCR	–	–	0.9960		99.6100	99.60576		99.6089
	UACI	–	–	33.4600		33.5200	33.50204		33.4689
Barbara	NPCR	–	99.6100	–	99.6912	–	–	99.7501	99.6088
	UACI	–	33.4300	–	33.5098	–	–	33.5102	33.4697

$$\mathrm{MSE} := \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(e_{ij} - f_{ij}\right)^2 \tag{22}$$

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

6.8 Noise attack analysis

Noise attack analysis examines an IES for adding some noise to the ciphertext images. It is herewith utilized to appreciate the permutation and manipulation performances of an IES. Salt and pepper noise (SPN) is mostly exploited to prove an IES counter the noise attacks. Hence, the recovering capability of an IES can be analyzed by inserting the SPN to the

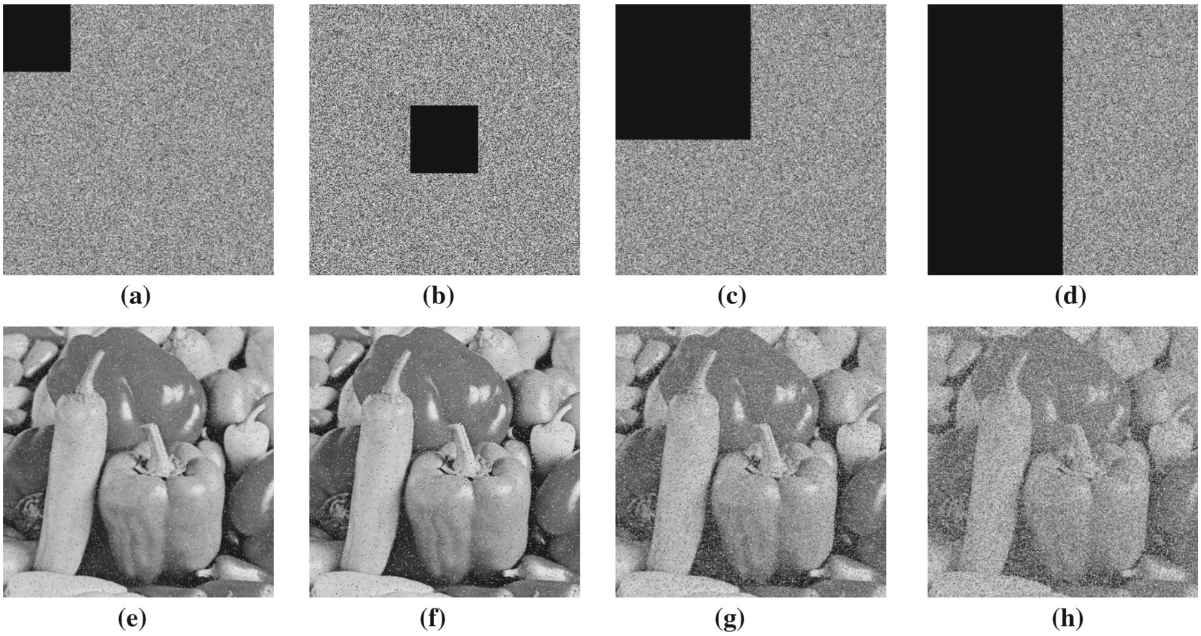


Fig. 11 Cropping attack analysis of the proposed IES for the Peppers image, ciphertext images cropped with ratios **a** 1/16, **b** 1/16(middle), **c** 1/4, **d** 1/2, and decipher images with ratios **e** 1/16, **f** 1/16(middle), **g** 1/4, h) 1/2

ciphertext image. The decipher images with adding different SPN densities of 0.001, 0.005, 0.01, 0.1 are illustrated in Fig. 13, and they are corroborated through the PSNR that measured as 39.23, 32.13, 29.16, 19.05 for the decipher images with SPN densities of 0.001, 0.005, 0.01, 0.1, respectively. Eventually, the proposed IES with the OCM recovers the images with the minimum corruption even if they are with high SPN.

6.9 Encryption processing time and computational complexity analyses

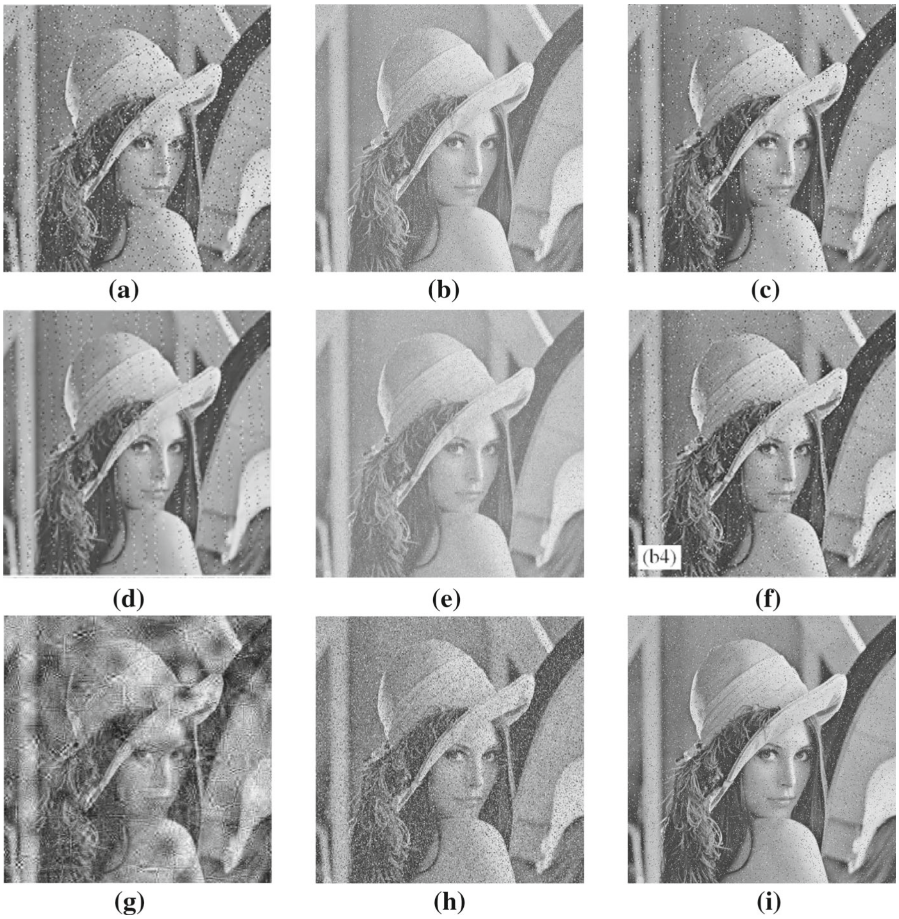
Along with the cryptanalyses performed above, the computational time of an IES is a crucial metric for an applicable IES. The processing time of the proposed IES with the OCM is 0.1748 (s). On the other hands, the operating duration of an algorithm can be even apprised through the computational complexity using big O notation. From this point of view, the computational complexity of the proposed IES is $O\ (m \times n)$ in which m and n indicate the row and column size, respectively. Hence, it can be implemented to a real application because of the fast-processing time and low computational complexity.

7 The related studies and comparison

The up-to-date IESs, which have been recently reported in the literature, are elaborately surveyed together with our study in view of the employed chaotic map and cryptanalysis in Table 14. In the table, the available data are used, and the others are compulsorily indicated as non-available (N/A). Note that the studies indicated with star* 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 15.

From Table 14, it is observed that suggested IESs have their own strengths and weaknesses and can be considered successful for particular cryptanalysis. Logistic, sine, cosine, Henon, Chebyshev, Lorenz, memristive and their variants and combinations are the most utilized chaotic maps. If the cryptanalyses results are roughly compared, key-space analyses in [18, 27, 36] can be regarded the lowest that in [26, 35, 38, 49] are medium, those in [17, 18, 20, 21, 24, 25, 27, 34, 36, 39, 40] are highest. The mean information entropy values can be evaluated better [37], moderate [14, 19, 20, 24, 26, 29–31] and worse [15, 16, 21, 27, 28, 33, 36, 38, 57]. As the mean

Fig. 12 The comparative cropping attack analysis for the decipher Lena image cropped with 1/16 ratio: **a** [21], **b** [24], **c** [48], **d** [49], **e** [16], **f** [50], **g** [51], **h** [52], **i** the proposed OCM



(a) (b) (c) (d) (e) (f) (g) (h) (i)

Table 12 The PSNR scores for the cipher under-test images via the proposed IES with the OCM

Cropping ratio	Lena	Cameraman	Baboon	Pepper	Barbara	Airplane
1/16	21.43	20.64	21.52	21.12	20.98	20.34
1/4	15.32	15.23	15.83	15.01	15.16	15.17
1/2	12.19	12.05	12.71	12.25	12.14	12.09

Table 13 The PSNR scores and comparison with the literature

Image	Cropping ratio	Ref. [24]	Ref. [16]	Ref. [50]	OCM
Lena	1/16	17.58	16.66	20.78	21.43
	1/4	15.03	10.64	14.96	15.32
	1/2	12.13	10.66	12.08	12.19

correlation results for horizontal, vertical and diagonal directions in [16, 17, 24] seem lower which are the best, those in [14, 15, 18, 20–23, 25, 27–31, 37, 38, 57] appear moderate and those in [19, 26, 33, 34, 36] are higher. The proof of the IESs with respect to NPCR in [14, 16, 19–24, 30, 31, 57], [15, 18, 26–29, 33, 37, 38]

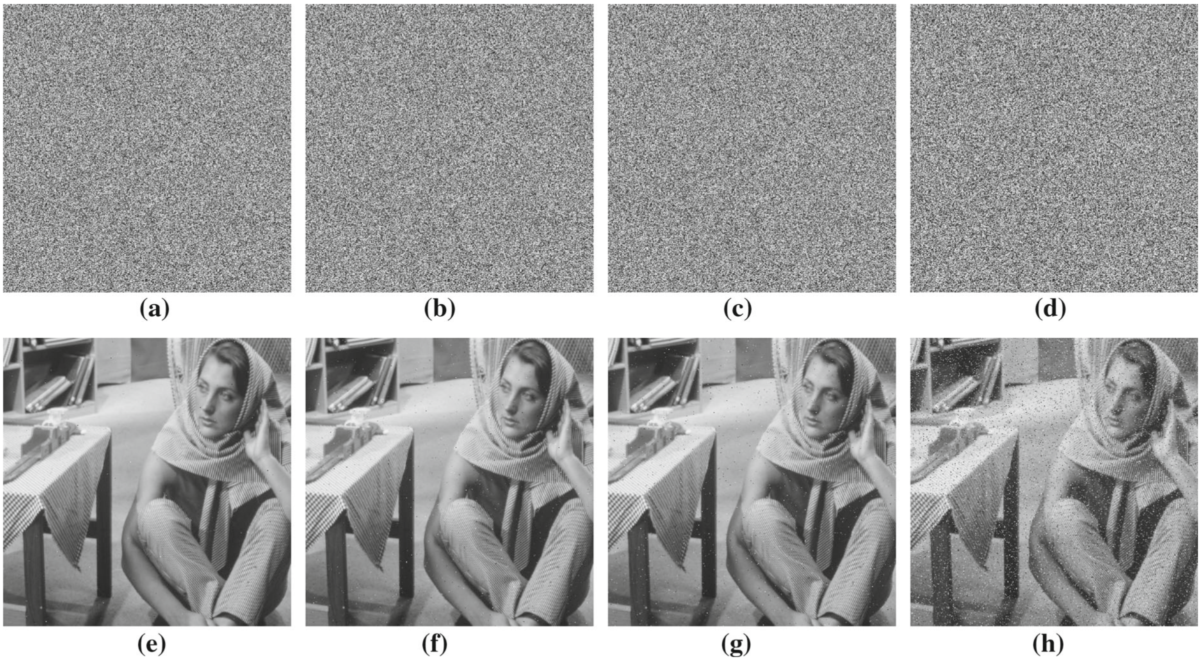


Fig. 13 Ciphertext images with inserting different SPN densities: **a** 0.001, **b** 0.005, **c** 0.01, **d** 0.1 and the related decipher images with SPN densities: **e** 0.001, **f** 0.005, **g** 0.01, **h** 0.1

and [17, 36] can be sorted from the strongest to the weakest. On the other sides, those in [16, 18, 22, 23, 37], [19–21, 24, 26, 28, 30, 31, 57] and [14, 17, 29, 33, 36] can be listed from the robust to the poorest in view of UACI. The IESs in [24], [16, 18, 21, 24, 31, 57] and [14, 20, 22, 23, 28], respectively, seem better, moderate and poorer counter the cropping attack, and those in [16, 23, 31], [14, 16, 20–23, 28, 31, 57] and [18] appear well, fair and worse across the noise attacks, respectively. Eventually, the IESs can be apprised as fast [14, 21, 22, 28–31], intermediate [18, 23] and slow [15, 27, 33, 57]. Therefore, the proposed EIS with the OCM comes to the fore on account of key-space, information entropy, correlation, NPCR, UACI, processing time of 2^{199}, 7.9994, 0.000210, 99.6090, 33.4640 and 0.1748 (s), respectively, as well as cropping and noise attacks among those reported elsewhere.

From Table 15, it is seen that the optimization algorithms such as ACO [34], PSO [16, 17, 35], GA [35, 36], DE [33], SDO [25] and WOA [15] were frequently implemented to the IESs. Decision variables might be the most critical parameters that searched through the optimization algorithms. It appears that the keys and the initial parameters of the maps are often applied as the decision variables. Although various chaotic maps were utilized; information entropy, correlation coefficient, PSNR, NPCR, UACI and their combinations are exploited as single or multiple objective functions, in general. It is worth noting that these objective functions are handled on the ciphertext image which obtained at the end of the entire operations of the IES, i.e., the objective functions must be computed on the ciphertext images. In order to compute the objective functions in every cycles of the optimization algorithm, the plaintext image must be incurred throughout the operations of IES to obtain the ciphertext image. This makes those IESs inapplicable to the real-time systems due to high processing time. On the other hands, the proposed OCM is derived by optimally finding out the unknown variables using ABC with multi-objective strategy involving the information entropy and LE. The multi-objective function is directly applied to the outcomes of the OCM. The plaintext image is thus encrypted through the proposed permutation and diffusion operations conducted by the OCM. In other words, ABC is directly applied to the OCM, not the ciphertext images.

Table 14 A thorough survey in terms of the employed chaotic map and cryptanalysis results

References	Year	Chaotic map	Key-space	Entropy (mean)	Corr (mean)	Differential attack (%)		Crop. attack	Noise attack	Encryption processing time (s)
						NPCR	UACI			
[18]	2018	Sine-sine	2^{128}	N/A	0.006300	99.6330	33.4716	▄	▖	0.5042
[24]	2021	4D memristive	2^{146}	7.9993	0.000511	99.6078	33.4268	▟	N/A	N/A
[19]	2019	2D logistic-adjusted-sine	2^{338}	7.9993	0.013197	99.6042	33.4328	N/A	N/A	N/A
[30]	2019	A modified chaotic	2^{212}	7.9993	0.001710	99.6040	33.4340	N/A	N/A	0.0700
[14]	2019	Polynomial	N/A	7.9993	0.002003	99.6191	33.6751	▖	▄	0.2810
[31]	2018	Three-integrated cascade	2^{186}	7.9993	0.003217	99.6040	33.4740	▄	▟	0.4442
[20]	2018	2D hénon-sine	2^{371}	7.9993	0.002417	99.6080	33.5470	▖	▄	N/A
[26]	2020	Lorenz	N/A	7.9991	0.051500	99.5676	33.4352	N/A	N/A	N/A
[29]	2019	Cellular automata	N/A	7.9992	0.002033	99.5180	33.2630	N/A	N/A	0.2240
[21]	2020	2D sine and Chebyshev	2^{158}	7.9972	0.001719	99.6090	33.4523	▄	▄	0.0605
[28]	2021	Yolo	N/A	7.9981	0.001523	99.7061	33.5190	▖	▄	0.2760
[57]	2019	Four-wing hyperchaotic	2^{700}	7.9971	0.008957	99.6000	33.4800	▄	▄	1.2800
[22]	2020	Sine	2^{412}	N/A	0.001827	99.6127	33.4691	▖	▄	0.0239
[23]	2019	Cosine-transform	2^{256}	N/A	0.001410	99.6244	33.4548	▖	▟	0.9730
[36]*	2020	Coupled lattice	2^{128}	7.9519	0.046700	99.4547	31.3549	N/A	N/A	N/A
[27]*	2020	4D Lorenz system	2^{111}	7.9976	0.003720	99.6340	33.4330	N/A	N/A	14.8750
[37]*	2021	A 5D chaotic	2^{338}	7.9996	0.005973	99.6475	33.4700	N/A	N/A	N/A
[38]*	2019	Intertwining logistic	2^{338}	7.9987	0.003250	99.6535	33.5497	N/A	N/A	N/A
[33]*	2020	Intertwining logistic	2^{256}	7.9985	0.016467	99.6400	32.9500	N/A	N/A	600.00
[15]*	2021	Piecewise linear chaotic and 2D logistic	N/A	7.9723	0.001790	99.6746	33.4753	N/A	N/A	89.155
[16]*	2021	Logistic	2^{385}	7.9974	0.000113	99.6169	33.4658	▄	▟	1.1247
[17]*	2018	Logistic		N/A	0.000100	99.4547	31.3549	N/A	N/A	N/A
[25]*	2017	Henon	2^{381}	N/A	0.006133	N/A	N/A	N/A	N/A	N/A
[34]*	2012	N/A	N/A	N/A	0.084940	N/A	N/A	N/A	N/A	N/A
[35]*	2015	Coupled nonlinear	2^{168}	N/A	N/A	N/A	N/A	N/A	N/A	N/A
This study		OCM	2^{199}	7.9994	0.000210	99.6090	33.4640	▟	▟	0.1748

*The studies stand for those in which the optimization algorithms employed. ▖: poor, ▄: moderate, ▟: better

8 Conclusion

A new OCM for IES with derived utilizing multi-objective optimization via ABC is proposed in this study. The unknown variables of the OCM model were found out through the multi-objective function including the information entropy and LE of the OCM. The standalone OCM was appreciated in terms of reliable metrics regarding bifurcation, 3D phase space, LE, PE and SE. The IES with the OCM was undergone various cryptanalyses, and the visual and numerical results were compared with those of many reported works with and without optimization. They were elaborately reviewed and compared among each other in order to demonstrate the superiority of the proposed OCM-based IES. It is evident that the proposed IES is prominent among the state of the arts thanks to the efficient chaotic performance of the OCM that

Table 15 A review on the evolutionary optimization-based IESs

Reference	Year	Type of chaotic map	Optimization algorithm	Multi/single	Objective function	Decision variable
[36]	2020	Coupled lattice	GA	Multi	Entropy and correlation of the ciphertext image	Key
[27]	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
[37]	2021	A 5D chaotic	Dual local search	Multi	UACI, entropy, NPCR of the ciphertext image	Initial parameter of the map
[38]	2019	Intertwining logistic	Memetic DE	Single	Entropy and correlation of the ciphertext image	Key
[33]	2020	Intertwining logistic	DE	Single	Entropy of the ciphertext image	A sequence for DNA operation
[15]	2021	Piecewise linear and 2D logistic	WOA	Single	Entropy of the ciphertext image	Initial parameter of the map
[16]	2021	Logistic	PSO	Multi	Weighted objective function for the ciphertext image: entropy and correlation coefficient	Key
[17]	2018	Logistic	PSO	Single	Correlation of the ciphertext image	Key
[25]	2017	Henon	SDO	Single	Complex object function based on CCD plane for the ciphertext image	Image
[34]	2012	N/A	ACO	Single	Energy of the ciphertext image	Key
[35]	2015	Coupled nonlinear	Hybrid of PSO and GA	Single	PSNR of the ciphertext image	Key
This study		OCM	ABC	Multi	Weighted objective function of the chaotic map: entropy and LE	Unknown coefficients of the map

optimized via multi-objective optimization with ABC. The IES does not utilize ABC in the image encrypting operations rather than the studies in which optimization is employed, though the OCM is achieved by the multi-objective optimization strategy. Therefore, the proposed IES with the OCM effectively encrypts the images with better security and speed thanks to the optimized chaotic performance of the OCM. On the other hands, in the comparison, the correlation coefficient is comparatively higher than few of the reported studies. For this reason, it is projected to construct a multi-dimensional chaotic map via multi-objective functions including also correlation coefficient through the proposed methodology.

Data availability statement The data made available with the article are used from public resources.

Declaration

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

References

1. Xuejing, K., Zihui, G.: A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Process. Image Commun. **80**, 1–11 (2020). https://doi.org/10.1016/j.image.2019.115670
2. Alawida, M., Samsudin, A., Teh, J. Sen., Alkhawaldeh, R.S.: A new hybrid digital chaotic system with applications in image encryption. Signal Process. **160**, 45–58 (2019). https://doi.org/10.1016/j.sigpro.2019.02.016
3. Bao, L., Yi, S., Zhou, Y.: Combination of sharing matrix and image encryption for lossless (k, n)-secret image sharing. IEEE Trans. Image Process. **26**, 5618–5631 (2017). https://doi.org/10.1109/TIP.2017.2738561

4. Zhang, F., Kodituwakku, H.A.D.E., Hines, J.W., Coble, J.: Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. IEEE Trans. Ind. Inform. **15**, 4362–4369 (2019). https://doi.org/10.1109/TII.2019.2891261
5. Sambas, A., Vaidyanathan, S., Tlelo-Cuautle, E., Abd-El-Atty, B., El-Latif, A.A.A., Guillen-Fernandez, O., Hidayat, Y., Gundara, G.: A 3-D multi-stable system with a peanut-shaped equilibrium curve: circuit design, FPGA realization, and an application to ımage encryption. IEEE Access. **8**, 137116–137132 (2020). https://doi.org/10.1109/ACCESS.2020.3011724
6. Chen, J., Chen, L., Zhou, Y.: Cryptanalysis of a DNA-based image encryption scheme. Inf. Sci. (NY) **520**, 130–141 (2020). https://doi.org/10.1016/j.ins.2020.02.024
7. Liu, Y., Qin, Z., Liao, X., Wu, J.: Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. Nonlinear Dyn. **100**, 2917–2931 (2020). https://doi.org/10.1007/s11071-020-05654-y
8. Vaidyanathan, S., Azar, A.T., Rajagopal, K., Sambas, A., Kacar, S., Cavusoglu, U.: A new hyperchaotic temperature fluctuations model, its circuit simulation, FPGA implementation and an application to image encryption. Int. J. Simul. Process Model. **13**, 281–296 (2018). https://doi.org/10.1504/IJSPM.2018.093113
9. Hua, Z., Zhu, Z., Yi, S., Zhang, Z., Huang, H.: Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inf. Sci. (NY) **546**, 1063–1083 (2021). https://doi.org/10.1016/j.ins.2020.09.032
10. Talhaoui, M.Z., Wang, X.: A new fractional one dimensional chaotic map and its application in high-speed image encryption. Inf. Sci. (NY) (2020). https://doi.org/10.1016/j.ins.2020.10.048
11. Wen, W., Wei, K., Zhang, Y., Fang, Y., Li, M.: Colour light field image encryption based on DNA sequences and chaotic systems. Nonlinear Dyn. **99**, 1587–1600 (2020). https://doi.org/10.1007/s11071-019-05378-8
12. Zheng, P., Huang, J.: Efficient encrypted images filtering and transform coding with Walsh–Hadamard transform and parallelization. IEEE Trans. Image Process. **27**, 2541–2556 (2018). https://doi.org/10.1109/TIP.2018.2802199
13. Chai, X., Bi, J., Gan, Z., Liu, X., Zhang, Y., Chen, Y.: Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Process. **176**, 107684 (2020). https://doi.org/10.1016/j.sigpro.2020.107684
14. Asgari-Chenaghlu, M., Balafar, M.A., Feizi-Derakhshi, M.R.: A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Process. **157**, 1–13 (2019). https://doi.org/10.1016/j.sigpro.2018.11.010
15. Saravanan, S., Sivabalakrishnan, M.: A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. Soft Comput. **48**, 1–24 (2021). https://doi.org/10.1007/s00500-020-05528-w
16. Wang, X., Li, Y.: Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Opt. Lasers Eng. **137**, 106393 (2021). https://doi.org/10.1016/j.optlaseng.2020.106393
17. Ahmad, M., Alam, M.Z., Umayya, Z., Khan, S., Ahmad, F.: An image encryption approach using particle swarm optimization and chaotic map. Int. J. Inf. Technol. **10**, 247–255 (2018). https://doi.org/10.1007/s41870-018-0099-y
18. Wang, H., Xiao, D., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Process. **144**, 444–452 (2018). https://doi.org/10.1016/j.sigpro.2017.11.005
19. Chai, X., Gan, Z., Yuan, K., Chen, Y., Liu, X.: A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput. Appl. **31**, 219–237 (2019). https://doi.org/10.1007/s00521-017-2993-9
20. Wu, J., Liao, X., Yang, B.: Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process. **153**, 11–23 (2018). https://doi.org/10.1016/j.sigpro.2018.06.008
21. Chen, C., Sun, K., He, S.: An improved image encryption algorithm with finite computing precision. Signal Process. **168**, 1–10 (2020). https://doi.org/10.1016/j.sigpro.2019.107340
22. Mansouri, A., Wang, X.: A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf. Sci. (NY) **520**, 46–62 (2020). https://doi.org/10.1016/j.ins.2020.02.008
23. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. (NY) **480**, 403–419 (2019). https://doi.org/10.1016/j.ins.2018.12.048
24. Yang, Y., Wang, L., Duan, S., Luo, L.: Dynamical analysis and image encryption application of a novel memristive hyperchaotic system. Opt. Laser Technol. **133**, 106553 (2021). https://doi.org/10.1016/j.optlastec.2020.106553
25. Su, Y., Tang, C., Chen, X., Li, B., Xu, W., Lei, Z.: Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. Opt. Lasers Eng. **88**, 20–27 (2017). https://doi.org/10.1016/j.optlaseng.2016.07.012
26. Farah, M.A.B., Guesmi, R., Kachouri, A., Samet, M.: A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt. Laser Technol. **121**, 105777 (2020). https://doi.org/10.1016/j.optlastec.2019.105777
27. Kaur, M., Singh, D., Uppal, R.S.: Parallel strength Pareto evolutionary algorithm-II based image encryption. IET Image Process. **14**, 1015–1026 (2020). https://doi.org/10.1049/iet-ipr.2019.0587
28. Asgari-Chenaghlu, M., Feizi-Derakhshi, M.R., Nikzad-Khasmakhi, N., Feizi-Derakhshi, A.R., Ramezani, M., Jahanbakhsh-Nagadeh, Z., Rahkar-Farshi, T., Zafarani-Moattar, E., Ranjbar-Khadivi, M., Balafar, M.A.: Cy: chaotic yolo for user intended image encryption and sharing in social media. Inf. Sci. (NY) **542**, 212–227 (2021). https://doi.org/10.1016/j.ins.2020.07.007
29. Enayatifar, R., Guimarães, F.G., Siarry, P.: Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Opt. Lasers Eng. **115**, 131–140 (2019). https://doi.org/10.1016/j.optlaseng.2018.11.017
30. Hanis, S., Amutha, R.: A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure. Nonlinear Dyn. **95**, 421–432 (2019). https://doi.org/10.1007/s11071-018-4573-7

31. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Process. **147**, 133–145 (2018). https://doi.org/10.1016/j.sigpro.2018.01.026
32. Carbas, S., Toktas, A., Ustun, D. (eds.): Nature-Inspired Metaheuristic Algorithms for Engineering Optimization Applications. Springer, Singapore (2021)
33. Dua, M., Wesanekar, A., Gupta, V., Bhola, M., Dua, S.: Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. J. Ambient Intell. Humaniz. Comput. **11**, 3771–3786 (2020). https://doi.org/10.1007/s12652-019-01580-z
34. Sreelaja, N.K., Vijayalakshmi Pai, G.A.: Stream cipher for binary image encryption using ant colony optimization based key generation. Appl. Soft Comput. J. **12**, 2879–2895 (2012). https://doi.org/10.1016/j.asoc.2012.04.002
35. Sajasi, S., Eftekhari Moghadam, A.M.: An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method. Appl. Soft Comput. J. **30**, 375–389 (2015). https://doi.org/10.1016/j.asoc.2015.01.032
36. Suri, S., Vijay, R.: A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA. Neural Comput. Appl. **32**, 11859–11873 (2020). https://doi.org/10.1007/s00521-019-04668-x
37. Kaur, M., Singh, D.: Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption. Multidimens. Syst. Signal Process. **32**, 281–301 (2020). https://doi.org/10.1007/s11045-020-00739-8
38. Kaur, M., Kumar, V., Li, L.: Color image encryption approach based on memetic differential evolution. Neural Comput. Appl. **31**, 7975–7987 (2019). https://doi.org/10.1007/s00521-018-3642-7
39. Karaboga, D., Basturk, B.: A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. J. Glob. Optim. **39**, 459–471 (2007). https://doi.org/10.1007/s10898-007-9149-x
40. Toktas, A., Ustun, D.: Triple-objective optimization scheme using butterfly-integrated ABC algorithm for design of multilayer RAM. IEEE Trans. Antennas Propag. **68**, 5603–5612 (2020). https://doi.org/10.1109/TAP.2020.2981728
41. Toktas, A., Ustun, D., Tekbas, M.: Global optimisation scheme based on triple-objective ABC algorithm for designing fully optimised multi-layer radar absorbing material. IET Microw. Antennas Propag. **14**, 800–811 (2020). https://doi.org/10.1049/iet-map.2019.0868
42. Toktas, A., Ustun, D., Erdogan, N.: Pioneer Pareto artificial bee colony algorithm for three-dimensional objective space optimization of composite-based layered radar absorber. Appl. Soft Comput. **96**, 1–12 (2020). https://doi.org/10.1016/j.asoc.2020.106696
43. Akdagli, A., Toktas, A.: 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 (2010). https://doi.org/10.1163/156939310793675989
44. Toktas, A.: 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 (2021)
45. May, R.M.: Simple mathematical models with very complicated dynamics. Nature **261**, 459–467 (1976). https://doi.org/10.1038/261459a0
46. Bandt, C., Pompe, B.: Permutation entropy: a natural complexity measure for time series. Phys. Rev. Lett. **88**, 4 (2002). https://doi.org/10.1103/PhysRevLett.88.174102
47. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications Lawrence E Bassham III Special Publication 800-22 Revision 1a
48. Yang, F., Mou, J., Liu, J., Ma, C., Yan, H.: Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. Signal Process. **169**, 1–16 (2020). https://doi.org/10.1016/j.sigpro.2019.107373
49. Wu, Y., Zhang, L., Qian, T., Liu, X., Xie, Q.: Content-adaptive image encryption with partial unwinding decomposition. Signal Process. **181**, 107911 (2021). https://doi.org/10.1016/j.sigpro.2020.107911
50. Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R., Cao, Y., Ding, X.: A robust image encryption algorithm based on Chua's circuit and compressive sensing. Signal Process. **161**, 227–247 (2019). https://doi.org/10.1016/j.sigpro.2019.03.022
51. Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y.: An image encryption algorithm based on chaotic system and compressive sensing. Signal Process. **148**, 124–144 (2018). https://doi.org/10.1016/j.sigpro.2018.02.007
52. Wang, X., Gao, S.: 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 (2020). https://doi.org/10.1016/j.ins.2020.06.030
53. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**, 2129–2151 (2006). https://doi.org/10.1142/S0218127406015970
54. Zhang, X., Zhao, Z., Wang, J.: Chaotic image encryption based on circular substitution box and key stream buffer. Signal Process. Image Commun. **29**, 902–913 (2014). https://doi.org/10.1016/j.image.2014.06.012
55. Wu, Y., Noonan, J.P., Agaian, S.: NPCR and UACI randomness tests for ımage encryption. Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. **1**, 31–38 (2011)
56. Enginoğlu, S., Erkan, U., Memiş, S.: Pixel similarity-based adaptive Riesz mean filter for salt-and-pepper noise removal. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-08110-1
57. Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y.: A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process. **155**, 44–62 (2019). https://doi.org/10.1016/j.sigpro.2018.09.029

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