electronics

MDPI

Article

Single-Objective Particle Swarm Optimization-Based Chaotic Image Encryption Scheme

Jingya Wang [1], Xianhua Song [1,*] and Ahmed A. Abd El-Latif [2,3]

[1] School of Science, Harbin University of Science and Technology, Harbin 150080, China
[2] EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3] Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
* Correspondence: songxianhua@hrbust.edu.cn

Abstract: High security has always been the ultimate goal of image encryption, and the closer the ciphertext image is to the true random number, the higher the security. Aiming at popular chaotic image encryption methods, particle swarm optimization (PSO) is studied to select the parameters and initial values of chaotic systems so that the chaotic sequence has higher entropy. Different from the other PSO-based image encryption methods, the proposed method takes the parameters and initial values of the chaotic system as particles instead of encrypted images, which makes it have lower complexity and therefore easier to be applied in real-time scenarios. To validate the optimization framework, this paper designs a new image encryption scheme. The algorithm mainly includes key selection, chaotic sequence preprocessing, block scrambling, expansion, confusion, and diffusion. The key is selected by PSO and brought into the chaotic map, and the generated chaotic sequence is preprocessed. Based on block theory, a new intrablock and interblock scrambling method is designed, which is combined with image expansion to encrypt the image. Subsequently, the confusion and diffusion framework is used as the last step of the encryption process, including row confusion diffusion and column confusion diffusion, which makes security go a step further. Several experimental tests manifest that the scenario has good encryption performance and higher security compared with some popular image encryption methods.

Keywords: image encryption; particle swarm optimization; logistic map

check for updates

Citation: Wang, J.; Song, X.; El-Latif, A.A.A. Single-Objective Particle Swarm Optimization-Based Chaotic Image Encryption Scheme. *Electronics* **2022**, *11*, 2628. https://doi.org/10.3390/electronics11162628

Academic Editor: Stefanos Kollias

Received: 31 July 2022
Accepted: 17 August 2022
Published: 22 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Over the years, with the improvement of science and technology and the rapid increase in Internet usage, a great quantity of data has been produced, and data dissemination has increased significantly on various networks. It can be clearly observed that multimedia data, especially digital images, have been increasing sharply. However, the authenticity, integrity and security of these massive amounts of data have become important challenges for users and institutions that process these data. Techniques such as steganography and image encryption are feasible methods to solve the security problem of digital image transmission [1–3]. Among all the technical means to provide image security, the encryption scheme is a traditional, efficient, and practical method.

A large number of pixels and the high correlation in the image require efficient encryption algorithms in addition to preliminary technologies such as AES, RSA and DES [4–6]. Consequently, various encryption scenarios based on diverse methods have been created, mainly including quantum methods [7,8], cellular automata methods [9,10], image compressed sensing methods [11,12], DNA sequence methods [13–15], and chaotic system methods [16,17].

The properties of chaos theory, such as pseudorandomness and sensitivity to the initial value [18–20], are consistent with the requirements of cryptography. The initial value sensitivity of the chaotic map corresponds to the key sensitivity required by cryptography. The mixing properties and topology of chaos are consistent with the diffusion and scrambling characteristics in the encryption process. Chaos signals are very suitable for designing image encryption schemes. Many scholars apply chaos theory to the design of encryption and decryption algorithms [21–25]. Therefore, the field has come a long way since chaotic signals were used for image encryption in the last century.

When using chaotic systems for encryption, both one and high-dimensional chaotic systems are available. 1D chaotic maps, such as logistic, sine and tent maps, have simple chaotic orbits and relatively few parameters [26,27]. Zhou et al. [28] created a model capable of generating multiple 1D chaotic maps and enforced secure image encryption. Kumar et al. [29] utilized a 1D logistic map for encryption and used pseudorandom numbers in the encryption process to improve the anti-attack ability. Many scholars have proposed high-dimensional chaotic systems. Hua et al. [30] proposed a 2D chaotic model, which enhanced the nonlinearity and randomness of 2D chaotic sequences. Wang et al. [31] created a 2D-SCLMS system with a larger chaotic range for image encryption. Luo et al. [32] created a novel encryption scenario based on logistic and Baker maps. In addition, various chaotic systems, such as 2D sine logistic modulation map, nonadjacent coupled map lattices, reverse 2-dimensional chaotic map, and Chen system, have been used for the image encryption domain [33–37].

A general chaotic image encryption algorithm usually consists of two main parts: diffusion and confusion. Fridrich proposed a framework of confusion and diffusion for encryption on the basis of chaos theory in 1998 [38]. Under this framework, many image encryption algorithms have been proposed [39,40]. Certainly, to better scramble images, block theory is often used in image encryption methods. Murugan et al. [41] created a chaotic encryption scenario based on confusion and diffusion of chaotic map blocks. Wang et al. [42] used block theory and divided it into two sections: interblock scramble and intrablock scramble. Image expansion is also a process of encryption, which can add random numbers to the image, making the image more resistant to selective plaintext attacks. Zhao et al. [37] also expanded the plaintext image under the framework of confusion and diffusion and achieved good encryption effect.

An optimization-based encryption scenario is also emerging, which optimizes the information attributes of the cipher image by choosing a suitable fitness function to obtain an optimized encryption effect. With the optimization scheme, the correlation coefficient or information entropy (IE) of the ciphertext image approaches the standard number, thereby greatly reducing the amount of useful information embodied in the encrypted image. To achieve the optimal encryption effect, some optimization algorithms, such as PSO, are usually applied to image encryption scenarios. Sabarinath et al. [43] studied an image encryption scenario using an improved PSO algorithm. The method involves Arnold transformation and then uses a key generated from an improved PSO to disrupt the pixel locations in each block of the encrypted image. Musheer et al. [44] created an encryption scenario based on PSO and a logistic map. The optimization objective is to minimize the correlation coefficient of the encrypted image; therefore, the optimal ciphertext image is searched. Wang et al. [45] studied the image encryption scheme based on multi-objective PSO and applied DNA coding and 1D logistic map. The objective function of PSO is the correlation coefficient and information entropy. For the above PSO algorithm for image encryption, named cipher image-based PSO (CIPSO), the statistical characteristics of the ciphertext image are used as the optimization objective to acquire the final ciphertext image in which many rounds of encryption are performed. However, because the PSO is used in every cipher image, encryption algorithms are inevitably iterated many times which makes the algorithm unsuitable for real-time requirements, especially under large data image encryption conditions.

Different from the above CIPSO image encryption ideas, a novel framework is proposed to use the population-based particle swarm optimization algorithm in the paper. Because the chaotic performances of chaotic systems only depend on their initial values and systematic parameters, if we acquire the optimized parameters and initial values for one chaotic map, it can be applied to chaotic encryption for any image. In addition, to decrease the complexity of applying the PSO algorithm, in the proposed framework, for the logistic chaotic system, only the information entropy of the sequences generated by the chaotic map is taken as the variable of the optimal objective function. The encryption steps in this paper include chaotic sequence preprocessing, expansion, block scrambling, confusion and diffusion. Our proposed encryption algorithm does not require multiple encryption processes, so it is faster than the CIPSO methods. This allows the chaotic system to have better properties in encrypting images and producing encryption results.

The innovations of the paper are as follows: (1) The optimization framework solves the dependence of chaotic systems on initial values and parameters. The framework can be applied in any chaotic system except the 2D logistic chaotic system. (2) A novel encryption method is proposed, especially the intra block scrambling process, which is a novel scrambling method.

This paper also has certain shortcomings. For example, the correlation between the encryption scheme and the plaintext image is not close, and it cannot achieve a good ability to resist differential attacks. This requires us to strengthen the algorithm's ability to resist differential attacks in future research.

The contents of the remaining sections are arranged as follows. Section 2 introduces the related work used in the encryption process, including the chaotic system, image scrambling methods and image expansion method. Section 3 designs the PSO scheme and the process of finding the optimized solution. Section 4 demonstrates the novel encryption scenario. Section 5 describes the corresponding decryption process. Section 6 presents the simulation results and security analysis of the encryption scenario, which can prove the usability of the newly proposed algorithm. Section 7 gives the discussion results of the paper. Section 8 is the conclusion.

2. Related Work

In this section, we briefly introduce the chaotic map and related encryption methods that will be used in the new encryption scheme.

2.1. Chaotic Map

A 2D logistic map [42] is utilized as an example to show the PSO-based optimized framework, iteratively generate chaotic sequences, and encrypt the image. Its expression is

$$\begin{cases} x_{n+1} = \mu_1(x_n - x_n^2) + \lambda_1 y_n^2 \\ y_{n+1} = \mu_2(y_n - y_n^2) + \lambda_2(x_n^2 + x_n y_n) \end{cases} \tag{1}$$

In Equation (1), $x_n, y_n \in (0, 1)$, the four system parameters are μ_1, μ_2, λ_1, λ_2 respectively. When $\mu_1 \in$ (2.75, 3.4], $\mu_2 \in$ (2.75, 3.45], $\lambda_1 \in$ (0.15, 0.21] and $\lambda_2 \in$ (0.13, 0.15], the map is in chaos, and the chaotic sequences are conducive to image encryption to achieve better results.

2.2. Block Scrambling

This paper applies block theory to scramble images, which aims to make the lower correlation between adjacent pixels and strong robustness resist statistical attacks. This consists of two portions. Specifically, intrablock scrambling traverses the pixel matrix in squares to reduce the correlation between pixels; interblock scrambling performs block exchange according to the chaotic sequence. To improve performance, the number of image blocks designed is 16.

2.2.1. Interblock Scrambling

Sixteen subblocks of equal size are divided by the image in the experiment. One of the chaotic sequences determines the interblock scrambling method. Then, the chaotic sequence is converted to a positive integer sequence, and interblock scrambling is applied to the image blocks according to the rules of ordering. An example of a 3 × 3 matrix is presented in Figure 1.

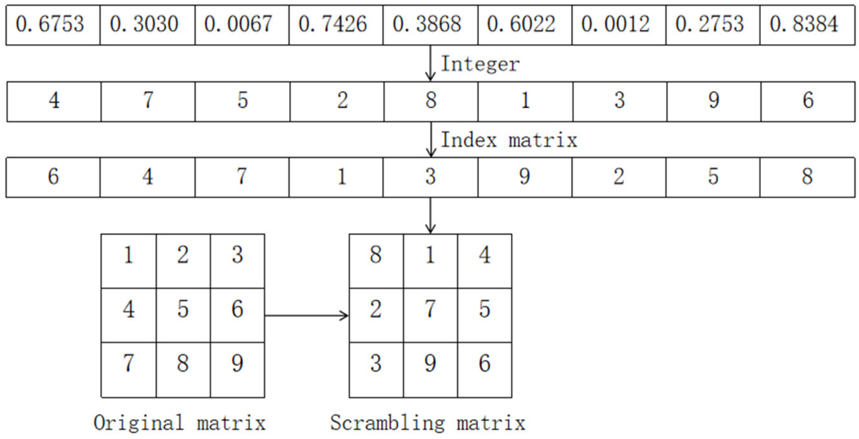


Figure 1. Interblock scrambling.

2.2.2. Intrablock Scrambling

Intrablock scrambling realizes the messing of pixels in each block. This scrambling method traverses each pixel from the inside to the outside by drawing a square. First, the pixel values are extracted starting in the middle of the image subblock, and after one round of drawing, the number of rows and columns are reduced by one. Then, a new round of square drawing is started until the end of each pixel value of the traversal subblock. Each obtained pixel value is sequentially stored in a 1D sequence and finally converted into a 2D pixel block matrix of the same size as the subblock. For example, this paper uses a 4 × 4 matrix to explain the method in Figure 2.

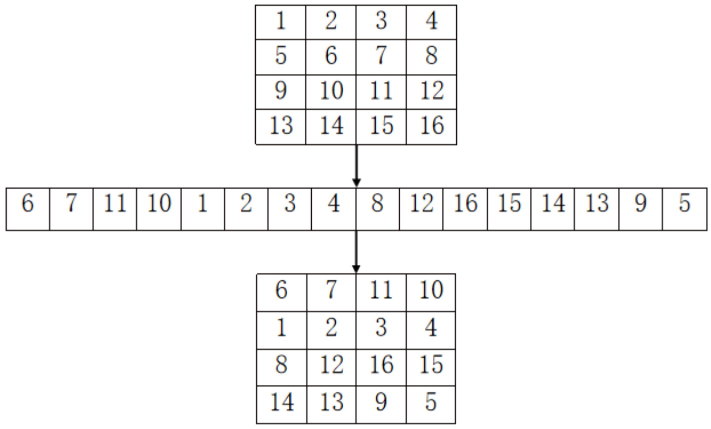


Figure 2. Intrablock scrambling.

2.3. Image Expansion

Image expansion adds random numbers to the image matrix to ensure that different ciphertext images can be obtained by encrypting the image twice under the same key value, which increases the algorithm's resistance to selective plaintext attacks. Specifically, this is explained as follows:

(1) Generate two random matrices R_0 and R_1, where the sizes of R_0 and R_1 are $4 \times (N + 4)$ and $M \times 4$, respectively.

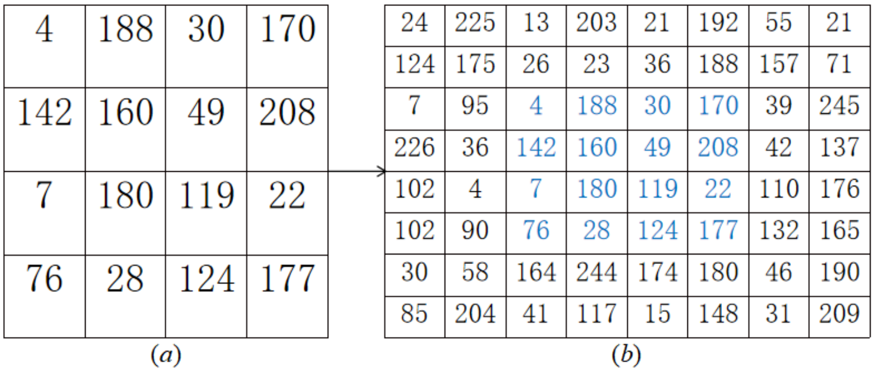
(2) Add the first two columns of R_1 to the leftmost side of the original image and add the last two columns of R_1 to the rightmost part of the original image.

(3) The first two lines of R_0 are added to the top line of the changed image, and the last two lines of R_0 are added to the bottom line of the changed image.

Therefore, the image expansion is completed, and the expanded image size is $(M + 4) \times (N + 4)$. Take the matrix 4 × 4 as an example in Figure 3.

$$R_0 = \begin{pmatrix} 24 & 225 & 13 & 203 & 21 & 192 & 55 & 21 \\ 124 & 175 & 26 & 23 & 36 & 188 & 157 & 71 \\ 30 & 58 & 164 & 244 & 174 & 180 & 46 & 190 \\ 85 & 204 & 41 & 117 & 15 & 148 & 31 & 209 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 7 & 226 & 102 & 102 \\ 95 & 36 & 4 & 90 \\ 39 & 42 & 110 & 132 \\ 245 & 137 & 176 & 165 \end{pmatrix}^T$$



4	188	30	170
142	160	49	208
7	180	119	22
76	28	124	177

(*a*)

24	225	13	203	21	192	55	21
124	175	26	23	36	188	157	71
7	95	4	188	30	170	39	245
226	36	142	160	49	208	42	137
102	4	7	180	119	22	110	176
102	90	76	28	124	177	132	165
30	58	164	244	174	180	46	190
85	204	41	117	15	148	31	209

(*b*)

Figure 3. Image dilation. (**a**) The primitive image matrix; (**b**) The extended image matrix.

3. PSO-Based Parameter Selection for the Chaotic Map

3.1. PSO

PSO was created by Eberhart and Kennedy in 1995 [46,47]. PSO is a population-based optimization technique that is an optimization algorithm for population intelligence in the field of computer intelligence [48]. Suppose a flock of birds forage randomly in a large field. How then to explain, no birds know where the food is in the field, but they only know the distance from the food. One of the most effective ways to find food is to hang out with the birds that are closest to the food site. PSO has the advantages of intuitive process, simplicity and easy realization. It is applied in many fields, for example, function optimization, signal processing, neural networks and so on. The specific operation of the algorithm is described.

The PSO algorithm first needs to initialize a group of particles $R = \{x_1, x_2, \ldots, x_N\}$ in the feasible solution space s, where the number of particles is assumed to be N and the objective function f is established. Each particle corresponds to an objective function $f(x_i)$ and iterates by updating the velocity $v_i(t)$ and position $x_i(t)$ of the particle. During the iteration, the individual extremum Pbest and the group extremum Gbest of the particle are recorded to find the particle that can make the objective function $f(x)$ reach the best.

Particles have only two attributes: velocity $v_i(t)$ and position $x_i(t)$. $v_i(t)$ represents the speed of movement and $x_i(t)$ represents the direction of movement. The expressions for the update iteration of particle velocity $v_i(t)$ and position $x_i(t)$ are

$$\begin{gathered} v_i(t+1) = \omega v_i(t) + c_1 r_1 (Pbest_i(t) - x_i(t)) + c_2 r_2 (Gbest_i(t) - x_i(t)) \\ x_i(t+1) = x_i(t) + v_i(t+1) \end{gathered} \tag{2}$$

where ω is the inertia weight. r_1, $r_2 \in [0, 1]$ are random vectors. c_1 and c_2 are constants. Normally, there are certain restrictions on the velocity and position used for iterative updates, such as velocity and position within the interval $[V_{\min}, V_{\max}]$, $[X_{\min}, X_{\max}]$, respectively.

3.2. The Newly Proposed Parameter Selection of the Chaotic Map Algorithm

The PSO scheme is used to find the optimized parameter values of the 2D logistic map. Therefore, we must determine the optimization objective of PSO algorithm.

IE is an efficient quota to appraise the randomness of sequences, which is expected to produce a better image encryption effect when the chaotic sequence used in image encryption has a higher IE. Therefore, IE is an appropriate objective function for optimization problems. The optimization scheme is introduced in detail below.

The gray value of the image is generally an integer between [0, 255], and the chaotic sequences are used for image confusion and diffusion after preprocessing. To finally make the pixels of the obtained cipher image still in the range of [0, 255], the chaotic sequences $\{x_n\}$, $\{y_n\}$ generated by Equation (1) are transformed into sequences of integers in the interval [0, 255] according to Equation (3).

$$\begin{aligned} x_n^1 &= floor(x_n \times 255) \\ y_n^1 &= floor(y_n \times 255) \end{aligned} \tag{3}$$

Entropy is a quantification method of the average amount of information possessed by the information source, which can be used to assess the degree of disorder of the map. For the information source, the expression is Equation (4).

$$H(s) = -\sum_{i=0}^{M} p(s_i) \log_2 p(s_i) \tag{4}$$

where M is the number of signals. Herein, $M = 255$. $s_i \in s$, p is the probability. The IE of a true random source is 8 [49].

The 2D logistic map generates two sequences, each of which has its corresponding entropy, in this case two objective functions. To facilitate the calculation, a simple method is introduced to establish an overall objective function $f(x)$ [50], which is represented as

$$f(x) = \alpha f_1(x) + \beta f_2(x) \tag{5}$$

where α and β are constants that represent the weights of the two subobjective functions $f_1(x)$ and $f_2(x)$. The two subobjective functions in this paper are equally important for the overall objective function, namely, $\alpha = \beta = 0.5$.

The specific expression of the overall objective function is shown in Equation (6).

$$f(x) = \alpha_1 [\sum_{i=0}^{M} p_1(s_i) \log_2 \frac{1}{p_1(s_i)}] + \alpha_2 [\sum_{i=0}^{M} p_2(s_i) \log_2 \frac{1}{p_2(s_i)}] \tag{6}$$

where α_1 and α_2 are constants representing the weights of the two parts. $\alpha_1 = \alpha_2 = 0.5$.

In the PSO algorithm, the initial particle population and the initial velocity are chosen randomly. Because the 2D logistic map has two initial values x_0 and y_0 and four initial parameters μ_1, μ_2, λ_1, and λ_2, the dimensionality of each particle is six dimensions, among $x_0 \in (0, 1)$, $y_0 \in (0, 1)$, $\mu_1 \in (2.75, 3.4]$, $\mu_2 \in (2.75, 3.45]$, $\lambda_1 \in (0.15, 0.21]$ and $\lambda_2 \in (0.13, 0.15]$. The velocity and position of each particle are iterated, and the particle corresponding to the overall objective function generated is the optimized initial values and parameters sought. The initial particle swarm and initial velocity are randomly selected, so the optimized initial values and parameters generated by the PSO algorithm are different each time in Algorithm 1.

Algorithm 1 PSO framework

```
Input: 2D Logistic map, initial values $x_0$, $y_0$, initial parameters $\mu_1$, $\mu_2$, $\lambda_1$, $\lambda_2$, initial dimensions, number of particles, velocity, position, and iterations $t$, and maximum iterations $T$.
Output: optimized particle
1: for each iteration
2:     for each particle
3:         for each dimension
4:             Iterative 2D Logistic map according to Equation (1)
5:             Calculate the entropy of the sequence $\{x_n\}$ according to Equations (3) and (4)
6:             Calculate the entropy of the sequence $\{y_n\}$ according to Equations (3) and (4)
7:             Calculate the overall objective function $f(x)$ according to Equation (6)
8:                 if $f(x)$ > Gbest_val
9:                 The particle corresponding to the overall objective function is the current optimized particle
10:                end
11:                 if $t < T$
12:                     Update the speed $v_i$ according to Equation (2)
13:                     Update the position $x_i$ according to Equation (2)
14:                 if $x_i$ exceeds the value range of the chaotic system
15:                         $x_i = x_{i-1}$
16:                 end
17:                end
18:                Repeat steps 4 through 17 until the iteration is complete
19:                The global optimum is the optimized particle
20:            end
21:        end
22: end
```

Note: The process of particle swarm iteration (steps 14–16) limits the range of particles, i.e., the range of motion of particles cannot exceed the parameter range required by the chaotic map.

4. Image Encryption

The image encryption process mainly includes key selection, chaotic sequence preprocessing, block scrambling, expansion, confusion and diffusion. The detailed explanation is: PSO is utilized to select the optimized key for encryption. Chaotic sequence preprocessing makes the sequence more random. Block scrambling is divided into intra block and inter block scrambling, which reduces the correlation and provides better protection against statistical attacks. The expansion step adds random numbers to the original image so that each encryption obtains a different ciphertext image, which can better resist selective plaintext attacks. Confusion and diffusion complicate the relationship between ciphertext and keys, making it difficult for an adversary to decrypt from a ciphertext image, which further enhances the resistance of the scenario. The encryption flowchart drawn according to the above description is shown in Figure 4.

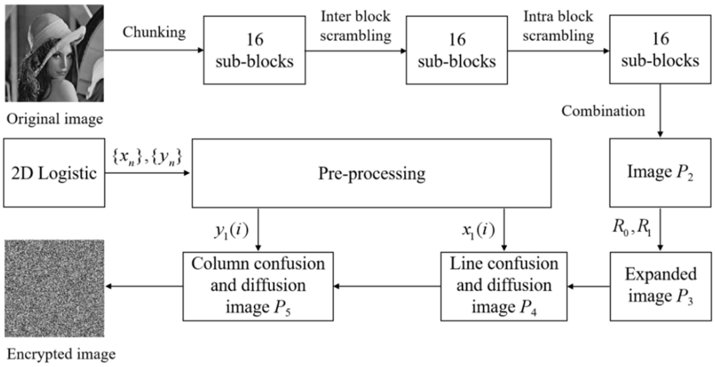


Figure 4. Image encryption framework.

4.1. Key Selection

The optimized values x_0, y_0, μ_1, μ_2, λ_1 and λ_2 generated by the PSO algorithm are used as the keys for the 2D logistic map. To avoid transient effects, the first two hundred points are discarded, and Equation (1) is used to generate two chaotic sequences $\{x_n\}$, $\{y_n\}$, which are of length MN.

4.2. Chaotic Sequence Preprocessing

The two chaotic sequences $\{x_n\}$, $\{y_n\}$ are preprocessed according to Equation (7).

$$\begin{array}{c} x_1(i) = 10^q \cdot x_n(i) - round(10^q \cdot x_n(i)) + 0.5 \\ y_1(i) = 10^q \cdot y_n(i) - round(10^q \cdot y_n(i)) + 0.5 \end{array} \tag{7}$$

where $x_1(i)$ and $y_1(i)$ are chaotic sequences $\{x_n\}$, $\{y_n\}$ preprocessed sequences, where q = 8.

4.3. Image Scrambling

(1) The 16 subblocks $B(i)$, i = 1,2, ... ,16 of the same size are divided by the original image P_1, and the last 16 numbers of the sequence $x(i)$ are taken to compose a sequence $D(i)$. Then, it is transformed into an integer sequence $S(i)$. The obtained integer sequence $S(i)$ is sorted, and interblock scrambling is achieved according to Equation (8).

$$\begin{array}{c} S(i) = floor(mod(D(i) \times 10^{14}, 16)) + 1 \\ [s, l] = sort(S) \\ B1 = B(l) \end{array} \tag{8}$$

(2) Sequences t_1 and t_2 are composed of 8 sequence values in the middle of sequences $x(i)$ and $y(i)$, respectively, and the new sequence t is formed according to Equation (9). Each subblock is disordered t_i times by the intrablock scrambling introduced in Section 2.2.2 to form the new disordered 16 sub-blocks.

$$\begin{cases} t(2(i-1)+1) = floor(\mathrm{mod}(t1 \times 10^{14}, 3)) + 4 \\ t(2i) = floor(\mathrm{mod}(t2 \times 10^{14}, 3)) + 4 \end{cases} \tag{9}$$

(3) The 16 subblocks are merged to form image P_2.

4.4. Image Expansion

Two random matrices R_0 and R_1 are generated, where the sizes of R_0 and R_1 are 4 × (N + 4) and M × 4, respectively. Expand image P_2 according to the method shown in Section 2.3 to form an expanded image P_3.

4.5. Confusion and Diffusion

4.5.1. Confusion and Diffusion of Row

First, calculate the new row index $r(i)$ = $ceil$ ($x_1(i)$ × (M + 4)) using $x_1(i)$, and then compare row i with row indexes $r(i)$.

$$\begin{array}{c} if\ r(i) < i, then \\ r(i) = i \end{array} \tag{10}$$

Second, the parameter k_{11}, k_{12} is calculated using $x_1(i)$.

$$\begin{array}{c} k_{11}(i) = mod(floor(x_1(i) \times 10^8), 256) \\ k_{12}(i) = mod(floor(x_1(i) \times 10^9), 256) \end{array} \tag{11}$$

Third, perform a bitwise XOR operation on the expansion image P_3 with parameter k_{11}, k_{12}.

$$\begin{gathered} if\ i = r(i), then \\ P_{30}(i,:) = P_3(i,:) \oplus k_{11}(i) \\ if\ i \neq\ r(i), then \\ P_{30}(i,:) = P_3(i,:) \oplus k_{11}(i) \\ P_{30}(r(i),:) = P_3(r(i),:) \oplus k_{12}(i) \end{gathered} \tag{12}$$

Fourth, swap the i-th and $r(i)$-th row of P_{30} to obtain P_{31}.

$$\begin{gathered} temp = P_{30}(i,:) \\ P_{30}(i,:) = P_{30}(r(i),:) \\ P_{30}(r(i),:) = temp \\ P_{31} = P_{30} \end{gathered} \tag{13}$$

Fifth, the first and last columns of P_{31} are calculated to obtain P_4.

$$P_4(i,1) = \mathrm{mod}(P_{31}(i,1) + P_{31}(i, N+4), 256) \tag{14}$$

Sixth, the other columns of P_{31} and P_4 are calculated.

$$P_4(i,j) = \mathrm{mod}(P_{31}(i,j) + P_4(i,j-1), 256) \tag{15}$$

4.5.2. Confusion and Diffusion of the Column

The confusion and diffusion of columns are similar to the rows', except that sequence $y_1(i)$ is used instead of sequence $x_1(i)$. The specific calculation procedure is presented in Algorithm 2.

Algorithm 2 Column confusion and diffusion

```
Input: Image $P_4$ and preprocessed chaotic sequence $y_1(i)$
Output: Image $P_5$
for $j$ = 1 to $N$ + 4
    $q(j) = ceil((N+4) \cdot y_1(j));$
    $k_{21}(j) = \mathrm{mod}(floor(10^8 \times y_1(j)), 2^8);$
    $k_{22}(j) = \mathrm{mod}(floor(10^9 \times y_1(j)), 2^8);$
    if $q(j) < j$ then
        $q(j) = j;$
    end if
    if $q(j) = j$ then
        $P_4(:,j) = k_{21}(j) \oplus P_4(:,j);$
    else if
        $P_4(:,j) = k_{21}(j) \oplus P_4(:,j);$
        $P_4(:,q(j)) = k_{22}(j) \oplus P_4(:,q(j));$
    end if
    $temp = P_4(:,j);$
    $P_4(:,j) = P_4(:,q(j));$
    $P_4(:,q(j)) = temp;$
    $P_{41} = P_4;$
    for $i$ = 1 to $M$ + 4
        $P_5(1,j) = \mathrm{mod}(P_{41}(1,j) + P_{41}(M+4,j), 2^8);$
        $P_5(i,j) = \mathrm{mod}(P_5(i-1,j) + P_{41}(i,j), 2^8);$
    end for
end for
```

5. Image Decryption

Decryption is the process of decrypting the ciphertext image according to the reverse step of the encryption process. From the encryption algorithm in Section 4, we get that the decryption steps are the inverse of confusion and diffusion, expansion, and block scrambling. The decryption key is the encryption key, so the decrypted image can be obtained correctly. The decryption flowchart corresponding to the encryption flowchart is shown in Figure 5.

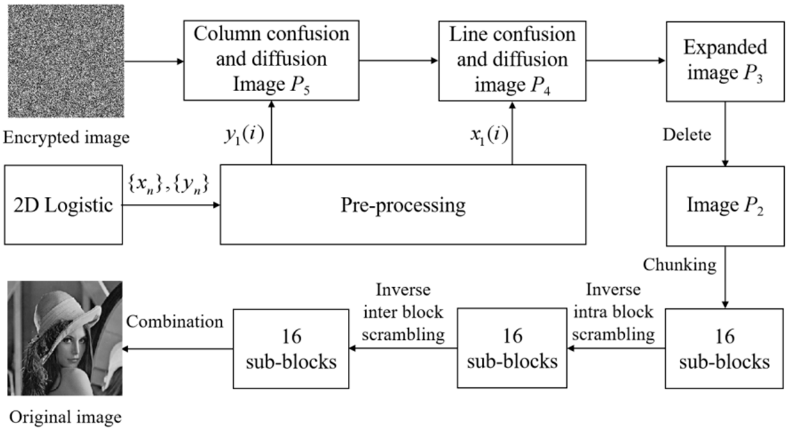


Figure 5. Image decryption framework.

Step 1: The two optimized initial values x_0 and y_0 and four optimized system parameters μ_1, μ_2, λ_1 and λ_2 generated by the PSO algorithm are used as the security keys of the 2D logistic map, and the sequence $\{x_n\}$, $\{y_n\}$ is generated by iterative Equation (1).

Step 2: The random sequence $\{x_n\}$, $\{y_n\}$ generated by the 2D logistic map can obtain the preprocessed sequences $x_1(i)$ and $y_1(i)$ according to Equation (7). Image P_4 is acquired by executing the reverse operation of confusion and diffusion of the column on encrypted image P_5 according to sequence $y_1(i)$.

Step 3: Image P_3 is acquired by executing the reverse operation of confusion and diffusion of the row on image P_4 according to sequence $x_1(i)$.

Step 4: Delete the first two lines and the last two lines of image P_3 in turn and then delete the first two columns and the last two columns to obtain image P_2.

Step 5: Image P_2 is partitioned into 16 subblocks of the same size. The sequence t is calculated according to Equation (9), and the inverse of the block-internal scrambling is executed for each subblock.

Step 6: According to the sequence $S(i)$, the inverse of the interblock operation is performed on each subblock, and then the 16 subblocks are combined to obtain the plain image P_1.

6. Simulation Results and Performance Analysis

This part gives the simulation experiments and the performance analysis of the scheme. Grayscale images of different sizes are chosen, mainly "Lena" (L, 256 × 256), "Cameraman" (C, 256 × 256), "7.1.02" (512 × 512) and "Boat" (B, 512 × 512). The number of PSO iterations t is 50, and the particle swarm is 50.

6.1. Experimental Environment

In order to simulate the encryption scheme and verify the performance of the algorithm, all experiments are conducted on a PC with AMD Ryzen 2.00 GHz CPU, 8 G RAM, and 1 TB hard disk with Window 10 Ultimate system. This experiment is operated by MATLAB R2020a software.

6.2. Simulation Results

To verify the effect of encryption, the simulation experiments are presented in Figure 6. It presents the plain, ciphertext and corresponding decrypted images of "Lena", "Cameraman", "7.1.02" and "Boat" respectively. All the ciphertext images resemble noise images, and no information can be obtained, which demonstrates that the encryption achieves good results, and all the encrypted images can achieve correct decryption.

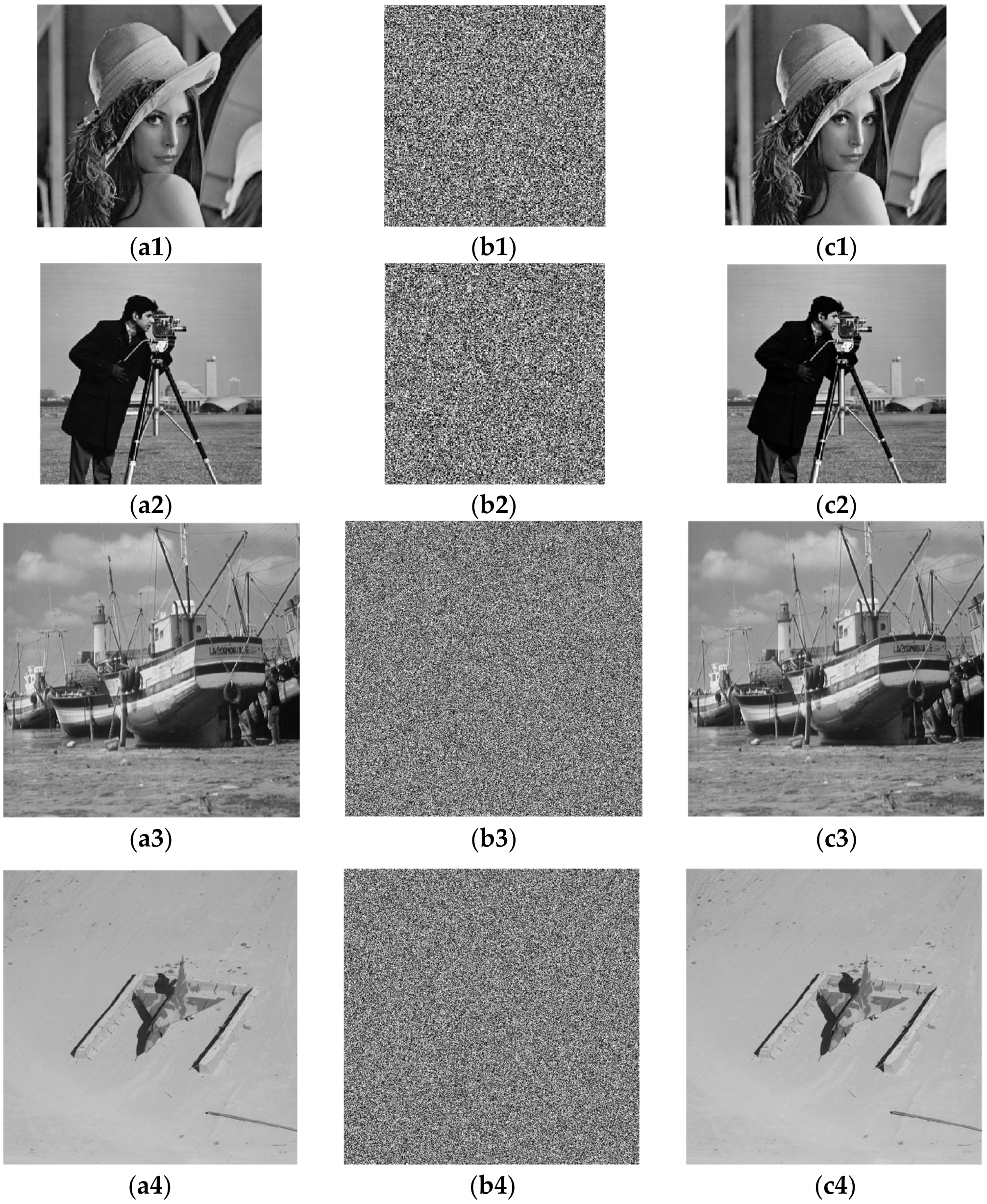


Figure 6. Experimental simulation. (**a1**–**a4**) Plaintext images; (**b1**–**b4**) Ciphertext images; (**c1**–**c4**) Decrypted images.

6.3. Running Time

To demonstrate the utility of the scenario, the running time is presented in Table 1. The running time is acceptable, which demonstrates that the scheme is practical.

Table 1. Encryption runtime (Unit: s).

Image	**Lena**	**Cameraman**	**Boat**	**7.1.02**
Time	0.430096	0.377874	1.219809	1.412237

6.4. Key Space Analysis

The PSO algorithm generates optimized initial values x_0 and y_0 and parameters μ_1, μ_2, λ_1 and λ_2. Therefore, x_0, y_0, μ_1, μ_2, λ_1, and λ_2 are both keys. It is presumed that the calculation accuracy is 10^{-14}, and the total key space $10^{14\times 6} = 10^{84} \gg 2^{100}$; that is, it is sufficiently large, which offers strong resistance to violent attacks.

6.5. Key Sensitivity Analysis

The more sensitive the scheme is to the key value, the better and more secure the algorithm is. Figure 7 takes the "Lena" as an example for illustration. When any key changes by 10^{-14}, the decrypted image resembles noise, which demonstrates that the scheme is key sensitive.

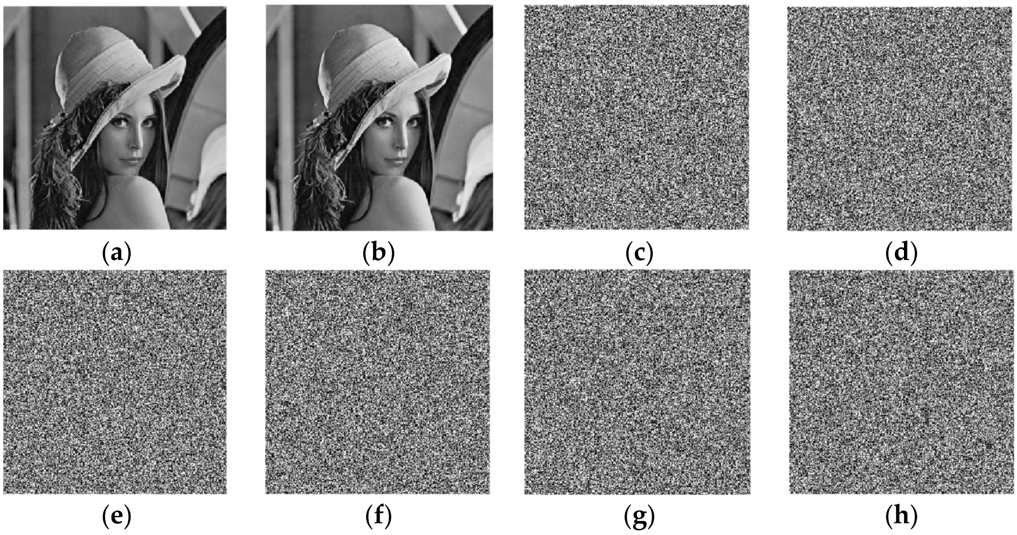


Figure 7. Key sensitivity analysis. (**a**) Plain Lena; (**b**) Decrypted image; (**c**) x_0 changes to $x_0 + 10^{-14}$; (**d**) y_0 changes to $y_0 + 10^{-14}$; (**e**) μ_1 changes to $\mu_1 + 10^{-14}$; (**f**) μ_2 changes to $\mu_2 + 10^{-14}$; (**g**) λ_1 changes to $\lambda_1 + 10^{-14}$; (**h**) λ_2 changes to $\lambda_2 + 10^{-14}$.

To test the sensitivity of the scheme to the key, the unified average change intensity (UACI) and the number of pixel change rate (NPCR) are adopted [51], and their expressions are

$$\begin{aligned} UACI &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255} \\ NPCR &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|Sign(C_1(i,j)-C_2(i,j))| \end{aligned} \tag{16}$$

where C_1 and C_2 are two different ciphertext images.

When the NPCR > NPCR^*_α, the NPCR passes the test. When the UACI is between [UACI^{*-}_α, UACI^{*+}_α], the UACI passes the test [52]. NPCR and UACI statistical tests on key sensitivity are shown in Tables 2 and 3.

Table 2. The NPCR statistical test on key sensitivity.

Image	NPCR	Theoretical NPCR Critical Value		
512 × 512		$N^*_{0.001}$ = 99.5717%	$N^*_{0.01}$ = 99.5810%	$N^*_{0.05}$ = 99.5893%
		0.001-level	0.01-level	0.05-level
L	99.6109%	Pass	Pass	Pass
C	99.6095%	Pass	Pass	Pass
B	99.6139%	Pass	Pass	Pass
7.1.02	99.5955%	Pass	Pass	Pass

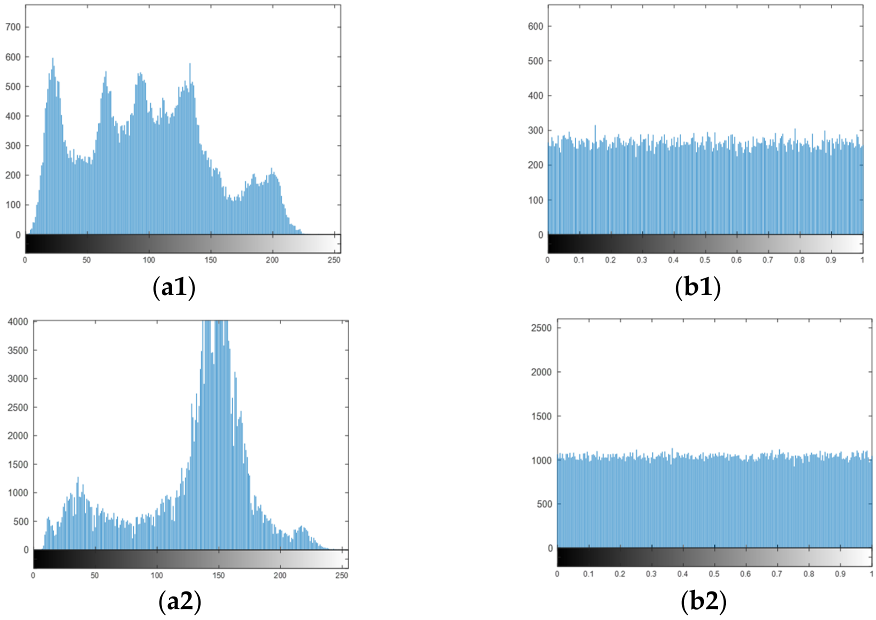
Table 3. The UACI statistical test on key sensitivity.

Image	UACI	Theoretical UACI Critical Value		
512 × 512		$N^{*-}_{0.001}$ = 33.3115%	$N^{*-}_{0.01}$ = 33.3445%	$N^{*-}_{0.05}$ = 33.3730%
		$N^{*+}_{0.001}$ = 33.6156%	$N^{*+}_{0.01}$ = 33.5826%	$N^{*+}_{0.05}$ = 33.5541%
		0.001-level	0.01-level	0.05-level
L	33.5384%	Pass	Pass	Pass
C	33.4358%	Pass	Pass	Pass
B	33.4196%	Pass	Pass	Pass
7.1.02	33.4063%	Pass	Pass	Pass

6.6. Statistical Attack Analysis

6.6.1. Histogram Analysis

The histogram indicates the pixel value distribution [53]. The more uniform the histogram of the ciphertext image, the less image information is displayed. Figure 8 presents the histogram of the original and cipher images of "Lena" and "Boat". The histograms of the ciphertext images are similarly uniformly distributed, indicating that the scenario is very good.



(**a1**) (**b1**)

(**a2**) (**b2**)

Figure 8. Histogram analysis. (**a1**,**a2**) Plain image histograms; (**b1**,**b2**) encrypted image histograms.

6.6.2. Chi-Square Analysis

Chi-square is a quantitative indicator that can be utilized to appraise the ability of an algorithm to resist statistical attacks. Its expression is

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \tag{17}$$

where v_i is the frequency occupied by i. v_0 = $MN/256$. The chi-square value of all test images is enumerated in Table 4. The chi-square of the original image is larger, while the chi-square of the encrypted image is lower than 293.2478 [54], which indicates that the scheme can resist statistical attacks.

Table 4. Chi-square.

Image		Lena	Cameraman	Boat	7.1.02
Chi-square	Ciphertext image	206.7957	203.6677	216.3745	238.2732
	Plaintext image	30,665.7	110,973.3	383,969.7	5,401,084.9

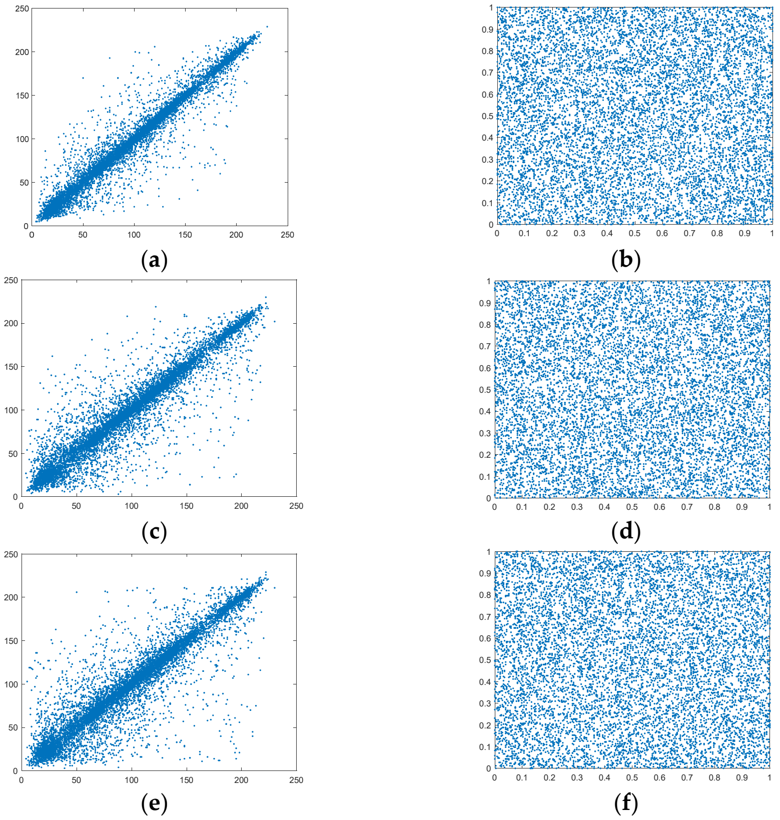
6.6.3. Correlation Analysis

The correlation between adjacent pixels of the ciphertext image is smaller, and the more resistant it is to statistical analysis attacks. The correlation coefficients [55] are calculated by Equation (18).

$$\begin{gathered}\rho_{xy}=\frac{\frac{1}{N}\sum\limits_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{D(x)D(y)}}\\ E(x)=\frac{1}{N}\sum\limits_{i=1}^{N}x_i\\ D(x)=\frac{1}{N}\sum\limits_{i=1}^{N}(x_i-E(x))^2\end{gathered}\tag{18}$$

where x and y express the adjacent pixel values of the image and ρ_{xy} represents the correlation coefficient.

In this paper, we select 10,000 pairs of adjacent pixels in the horizontal (H), vertical (V) and diagonal (D) directions for the original and encrypted images of "Lena". The plaintext image is close to the diagonal direction in all three directions, while the points in all directions of the ciphertext image are randomly distributed throughout the data range in Figure 9, which demonstrates that the scheme greatly reduces the original image correlation.



(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 9. Correlation analysis. (**a**) The horizontal direction of the plaintext; (**b**) The horizontal direction of the ciphertext; (**c**) The vertical direction of the plaintext; (**d**) The vertical direction of the ciphertext; (**e**) The diagonal direction of the plaintext; (**f**) The diagonal direction of the ciphertext.

The correlation coefficients of all original images are close to 1, while the encrypted images are close to 0 in Table 5, indicating that the scheme is good and can effectively resist statistical attacks.

Table 5. Correlation coefficient.

Image	Direction	Original Image	Encryption Image		
			Ref. [33]	Ref. [37]	Ours
Lena	H	0.9777	0.00043	0.0052	0.0017
	V	0.9593	0.0048	−0.00011	0.00092
	D	0.9502	−0.0040	−0.0022	0.0011
Cameraman	H	0.9591	0.0010	0.0014	0.00047
	V	0.9572	−0.0048	0.0027	−0.0055
	D	0.9392	0.0080	−0.0004	−0.00004
Boat	H	0.9719	0.0013	0.00032	−0.00011
	V	0.9437	0.00014	0.0016	0.0021
	D	0.9250	0.0044	−0.0025	−0.0041
7.1.02	H	0.9743	−0.0044	−0.0031	0.0015
	V	0.9785	−0.0011	0.0022	0.00026
	D	0.9661	0.0012	0.0038	−0.0027

6.6.4. Information Entropy

The IE expresses the degree of random distribution of an image and is often called Shannon entropy, which is expressed as Equation (4). A higher IE indicates a more random image pixel distribution. The IE of the test image is presented in Table 6. The IE of the ciphertext images of the new scenario is closer to 8 and outperforms the values of other algorithms, which demonstrates that the scenario is better.

Table 6. Information entropy.

Image	Ref. [33]	Ref. [37]	Ours
L	7.9975	7.9977	7.9978
C	7.9976	7.9972	7.9978
B	7.9973	7.9994	7.9994
7.1.02	7.9993	7.9992	7.9994

6.6.5. Local Information Entropy (LIE)

LIE can represent the randomness of local images. To accurately evaluate the randomness of the local image in the ciphertext image, the LIE is used.

$$\overline{LH_{k,T_B}}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{19}$$

In Equation (19), k is randomly selected for the number of subimages after image segmentation. T_B randomly selects the number of pixels in the subimage. S expresses the encrypted image. $H(S_i)$ expresses the IE of S_i. Specifically, we choose $k = 30$ and $T_B = 1936$. When the confidence interval is 0.001, the LIE belongs to the interval (7.901901305, 7.903037329) [56]. We take these four images as examples in Table 7. Four images passed the test, which explains why the randomness of the local image is good.

Table 7. LIE.

Image	Value	Outcome
L	7.902669871	Pass
C	7.902592647	Pass
B	7.902378187	Pass
7.1.02	7.902937793	Pass

6.7. Cropping Attack

To evaluate the anti-interference capability of the encryption scenario under a cropping attack. Cropping attacks of different strengths are used on the encrypted images. A cropping attack is performed by setting a portion of the pixel block value of the encrypted image to 0 and decrypting it. The decrypted images under different cropping strengths are shown in Figure 10. The new encryption scenario can recover the encrypted image to a certain extent from clipping attacks, which demonstrates that the scenario is robust and resistant to cropping attacks.

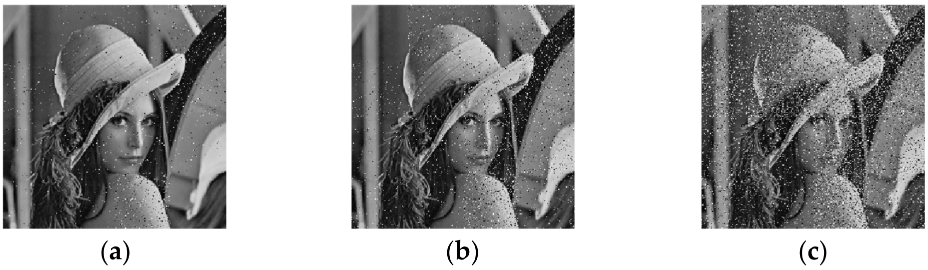


Figure 10. Cropping attack. Data loss with (**a**) 30 × 30; (**b**) 50 × 50; (**c**) 100 × 100.

6.8. Noise Attack

Images are affected by various noises during transmission over the Internet, which have an impact on decrypted images. To qualitatively test the resistance in noisy environments, we add different strengths of salt and pepper noise (SPN) to the encrypted images. The noise strength is set to 0.005, 0.01 and 0.05 in order. The results of the noise resistance test of the encryption algorithm are presented in Figure 11. Some content of the original image can still be seen from the decrypted image after adding different strengths of noise to the ciphertext image. This indicates that the new scenario can resist noise attacks of a certain strength. Thus, the scenario is secure and resistant to noise attacks.

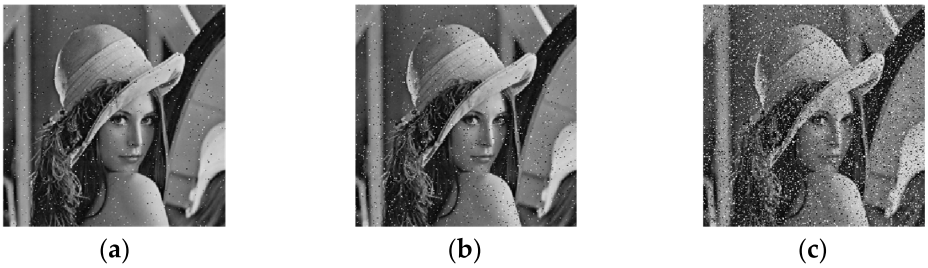


Figure 11. Noise attack. Noise strength (**a**) 0.005; (**b**) 0.01; (**c**) 0.05.

6.9. The Influence of the PSO Algorithm on Image Encryption

The objective function of PSO is composed of the information entropy of two chaotic sequences. To better explain the impact of the optimized initial values and parameters obtained by PSO on image encryption, we stochastically choose two different sets of initial values and parameters, denoted as value 1 and value 2. Different indicators of "Lena" are compared in Table 8. The indicators under the optimized initial values and parameters are better than others. This shows that a chaotic map is conducive to image encryption to achieve better results under the optimized initial values and parameters acquired by the PSO algorithm.

Table 8. Comparison of different initial values.

Index		Value 1	Value 2	Optimized Values
Information entropy		7.9972	7.9974	7.9978
Chi-square		261.8054	243.1583	206.7957
Correlation coefficient	H	−0.0036	0.0099	0.0017
	V	0.0080	−0.0018	0.00092
	D	−0.0096	0.0043	0.0011

7. Discussion

The chaotic image encryption scheme based on PSO algorithm proposed in this paper can resist various attacks, in addition to demonstrating security and timeliness. However, it also has certain limitations. Since the optimized initial value and parameters of the chaotic map are generated by the PSO algorithm, the key has no correlation with the plaintext image, so that the encryption result will not change greatly due to the change of the pixels in the plaintext image. This requires us to improve the relevance of the algorithm to plaintext images in future research.

8. Conclusions

The PSO framework is proposed to seek the optimized initial values and optimized parameters of chaotic systems and is then used for encryption by a special chaotic map. The objective function of PSO is composed of the IE of the chaotic sequences. The optimized initial values and parameters can make the chaotic sequences more similar to the random sequence, which is beneficial to the encryption to achieve better results. In the process of encryption, the methods of scrambling, expansion, confusion and diffusion are used in this paper. In the scrambling process, different block scrambling methods are adopted in this paper, which immensely decreases the correlation of the ciphertext image and improves the ability of the image to resist statistical attack analysis. For the confusion and diffusion framework, this paper adopts operations on rows and columns, respectively, which further improves the resistance of the scenario. The simulation analysis of the new scenario shows that the scheme achieves good results in image encryption, especially the maximum IE is 7.9994, which is closer to 8 compared with other scenarios. In addition, the scenario also has the ability to resist various attacks, and the key sensitivity is extremely high. The UACI and NPCR of the sensitivity test are only slightly different from the standard value. All tests demonstrate that the security of the new scenario has been significantly improved.

In the future, we intend to further explore the optimization scenario of image encryption to achieve a better encryption effect. In addition, we should further study the encryption scheme of images so that encryption may see a greater breakthrough in terms of security and practicability.

Author Contributions: Conceptualization, J.W.; methodology, J.W. and X.S.; software, J.W.; formal analysis, J.W. and A.A.A.E.-L.; investigation, J.W. and A.A.A.E.-L.; data curation, X.S.; writing—original draft preparation, J.W. and X.S.; writing—review and editing, A.A.A.E.-L.; visualization, X.S. and A.A.A.E.-L.; supervision, X.S.; project administration, X.S. and A.A.A.E.-L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Natural Science Foundation of Heilongjiang Province, China (QC2017075) and the National Natural Science Foundation of China (61501148). Ahmed A. Abd El-Latif thanks the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Hassan, F.S.; Gutub, A. Improving data hiding within colour images using hue component of HSV colour space. *CAAI Trans. Intell. Technol.* **2021**, *7*, 56–68. [CrossRef]
2. Sonar, R.; Swain, G. Steganography based on quotient value differencing and pixel value correlation. *CAAI Trans. Intell. Technol.* **2021**, *6*, 504–519. [CrossRef]
3. Kumar, A.; Abhishek, K.; Shah, K.; Namasudra, S.; Kadry, S. A novel elliptic curve cryptography-based system for smart grid communication. *Int. J. Web Grid. Serv.* **2021**, *17*, 321–342. [CrossRef]
4. Abd El-Latif, A.A.; Li, L.; Wang, N.; Han, Q.; Niu, X. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **2013**, *93*, 2986–3000. [CrossRef]
5. Xiao, D.; Liao, X.; Wong, K.W. An efficient entire chaos-based scheme for deniable authentication. *Chaos Soliton Fract.* **2005**, *23*, 1327–1331. [CrossRef]
6. Das, S.; Namasudra, S. A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Comput. Electr. Eng.* **2022**, *101*, 107991. [CrossRef]
7. Zhou, R.-G.; Wu, Q.; Zhang, M.-Q.; Shen, C.-Y. Quantum image encryption and decryption algorithms based on quantum image geometric transformations. *Int. J. Theor. Phys.* **2013**, *52*, 1802–1817. [CrossRef]
8. Akhshani, A.; Akhavan, A.; Lim, S.-C.; Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 4653–4661. [CrossRef]
9. Jin, J. An image encryption based on elementary cellular automata. *Opt. Lasers Eng.* **2012**, *50*, 1836–1843. [CrossRef]
10. Enayatifar, R.; Sadaei, H.J.; Abdullah, A.H.; Lee, M.; Isnin, I.F. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Opt. Lasers Eng.* **2015**, *71*, 33–41. [CrossRef]
11. Zhou, N.; Li, H.; Wang, D.; Pan, S.; Zhou, Z. Image compression and encryption scheme based on 2D compressive sensing and fractional mellin transform. *Opt. Commun.* **2015**, *343*, 10–21. [CrossRef]
12. Hu, G.; Xiao, D.; Wang, Y.; Xiang, T. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *J. Vis. Commun. Image Represent.* **2017**, *44*, 116–127. [CrossRef]
13. Zhang, Q.; Guo, L.; Wei, X. Image encryption using DNA addition combining with chaotic maps. *Math. Comput. Model.* **2010**, *52*, 2028–2035. [CrossRef]
14. Jain, A.; Rajpal, N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools Appl.* **2016**, *75*, 5455–5472. [CrossRef]
15. Pavithran, P.; Mathew, S.; Namasudra, S.; Singh, A. Enhancing randomness of the ciphertext generated by DNA-based cryptosystem and finite state machine. *Clust. Comput.* **2022**, 1–17. [CrossRef]
16. Chai, X.; Chen, Y.; Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **2017**, *88*, 197–213. [CrossRef]
17. Kaur, M.; Kumar, V.J.E.L. Efficient image encryption method based on improved lorenz chaotic system. *Electron. Lett.* **2018**, *54*, 562–564. [CrossRef]
18. Zhu, C.X.; Sun, K.H. Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms. *Acta Phys Sin.* **2012**, *61*, 120503–120521.
19. Teh, J.S.; Alawida, M.; Sii, Y.C. Implementation and practical problems of chaos-based cryptography revisited. *J. Inf. Secur. Appl.* **2020**, *50*, 102421. [CrossRef]
20. Wang, X.; Gao, S. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Inf. Sci.* **2020**, *507*, 16–36. [CrossRef]
21. Wong, K.-W.; Kwok, B.S.-H.; Law, W.-S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2008**, *372*, 2645–2652. [CrossRef]
22. Tang, Y.; Wang, Z.; Fang, J.-A. Image encryption using chaotic coupled map lattices with time-varying delays. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 2456–2468. [CrossRef]
23. Kanso, A.; Ghebleh, M. A novel image encryption algorithm based on a 3D chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 2943–2959. [CrossRef]
24. Ye, G.; Huang, X. A novel block chaotic encryption scheme for remote sensing image. *Multimedia Tools Appl.* **2016**, *75*, 11433–11446. [CrossRef]
25. Xie, E.Y.; Li, C.; Yu, S.; Lü, J. On the cryptanalysis of fridrich's chaotic image encryption scheme. *Signal Process.* **2017**, *132*, 150–154. [CrossRef]
26. Singh, N.; Sinha, A. Optical image encryption using Hartley transform and logistic map. *Opt. Commun.* **2009**, *282*, 1104–1109. [CrossRef]
27. Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. *Nonlinear Dyn.* **2017**, *87*, 127–133. [CrossRef]
28. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2013**, *97*, 172–182. [CrossRef]
29. Kumar, M.; Gupta, P. A new medical image encryption algorithm based on the 1D logistic map associated with pseudo-random numbers. *Multimedia Tools Appl.* **2021**, *80*, 18941–18967. [CrossRef]
30. Hua, Z.; Jin, F.; Xu, B.; Huang, H. 2D logistic-Sine-coupling map for image encryption. *Signal Process.* **2018**, *149*, 148–161. [CrossRef]

31. Wang, J.; Song, X.; Wang, H.; Abd El-Latif, A.A. Applicable image security based on new hyperchaotic system. *Symmetry Basel* **2021**, *13*, 2290. [CrossRef]
32. Luo, Y.; Yu, J.; Lai, W.; Liu, L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimed. Tools Appl.* **2019**, *78*, 22023–22043. [CrossRef]
33. Hua, Z.; Zhou, Y.; Pun, C.-M.; Chen, C.P. 2D sine logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
34. Natiq, H.; Al-Saidi, N.M.G.; Said, M.R.M.; Kilicman, A. A new hyperchaotic map and its application for image encryption. *Eur. Phys. J. Plus* **2018**, *133*, 1–14. [CrossRef]
35. Zhang, Y.-Q.; Wang, X.-Y. A new image encryption algorithm based on non-adjacent coupled map lattices. *Appl. Soft Comput.* **2015**, *26*, 10–20. [CrossRef]
36. Boriga, R.; Dăscălescu, A.C.; Priescu, I. A new hyperchaotic map and its application in an image encryption scheme. *Signal Process. Image Commun.* **2014**, *29*, 887–901. [CrossRef]
37. Zhao, C.-F.; Ren, H.-P. Image encryption based on hyper-chaotic multi-attractors. *Nonlinear Dyn.* **2020**, *100*, 679–698. [CrossRef]
38. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
39. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F.; Altameem, A.; Lee, M. Image encryption using a synchronous permutation-diffusion technique. *Opt. Lasers Eng.* **2017**, *90*, 146–154. [CrossRef]
40. Essaid, M.; Akharraz, I.; Saaidi, A.; Mouhib, A. A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. *Procedia Comput. Sci.* **2018**, *127*, 539–548. [CrossRef]
41. Murugan, B.; Nanjappa Gounder, A.G. Image encryption scheme based on block-based confusion and multiple levels of diffusion. *IET Comput. Vis.* **2016**, *10*, 593–602. [CrossRef]
42. Wang, X.; Guan, N. Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata. *Opt. Laser Technol.* **2020**, *132*, 106501. [CrossRef]
43. Sabarinath, R.; Jegadeesan, S.; Venkatalakshmi, K. Image encryption using modified particle swarm optimization. *IJRCCT* **2014**, *3*, 241–246.
44. 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.* **2018**, *10*, 247–255. [CrossRef]
45. Wang, X.; Li, Y. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Opt. Lasers Eng.* **2021**, *137*, 106393. [CrossRef]
46. Eberhart, R.; Kennedy, J. A new optimizer using particle swarm theory. In *MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, 4–6 October 1995*; IEEE: New York, NY, USA, 1995; pp. 39–43.
47. Chakraborty, R.; Verma, G.; Namasudra, S. IFODPSO-based multi-level image segmentation scheme aided with masi entropy. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 7793–7811. [CrossRef]
48. Madheswari, K.; Venkateswaran, N. Swarm intelligence based optimisation in thermal image fusion using dual tree discrete wavelet transform. *Quant. Infrared Thermogr. J.* **2017**, *14*, 24–43. [CrossRef]
49. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
50. Kanmani, M.; Narsimhan, V. An image contrast enhancement algorithm for grayscale images using particle swarm optimization. *Multimed. Tools Appl.* **2018**, *77*, 23371–23387. [CrossRef]
51. Xian, Y.; Wang, X.; Yan, X.; Li, Q.; Wang, X. Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion. *Opt. Lasers Eng.* **2020**, *134*, 106202. [CrossRef]
52. Wang, J.; Song, X.; El-Latif, A.A.A. Efficient entropic security with joint compression and encryption approach based on compressed sensing with multiple chaotic systems. *Entropy Switz* **2022**, *24*, 885. [CrossRef]
53. Gutub, A. Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing. *CAAI Trans. Intell. Technol.* **2022**, 1–13. [CrossRef]
54. Huang, W.; Jiang, D.; An, Y.; Liu, L.; Wang, X. A novel double-image encryption algorithm based on rossler hyperchaotic system and compressive sensing. *IEEE Access* **2021**, *9*, 41704–41716. [CrossRef]
55. Ding, L.; Ding, Q. A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos. *Electron. Switz* **2020**, *9*, 1280. [CrossRef]
56. Shengtao, G.; Tao, W.; Shida, W.; Xuncai, Z.; Ying, N. A novel image encryption algorithm based on chaotic sequences and cross-diffusion of bits. *IEEE Photon. J.* **2020**, *13*, 1–15. [CrossRef]