Multimedia Tools and Applications (2021) 80:22135–22162
https://doi.org/10.1007/s11042-021-10807-1

A novel image encryption algorithm based on improved key selection and digital chaotic map

Hongyue Xiang[1] · Lingfeng Liu[1]

Received: 5 September 2020 / Revised: 4 December 2020 / Accepted: 10 March 2021 /
Published online: 23 March 2021

Abstract
Chaotic systems are widely used in various fields, but under the finite precision device, chaotic systems would fall into a cycle and subsequently the performance degrade. Thus, the suppression method of the dynamic degradation of digital chaos is receiving increasing attention. This paper proposes a new improvement model to suppress the dynamical degradation under finite computing accuracy equipment. By using the difference between two maps of the same type but with different initial values, and the state feedback function to improve the performance of the digital chaotic map and extend the time before the chaotic map enters the cycle. Take the 1D Logistic map and x-dimensional of Baker map as examples to prove the effectiveness of the improvement model. Then we proposed a new key selection method, in what part of information of the image would be selected by using a chaotic map to generate a special value. The special value would be used as part of the key. Based this method, a new image encryption algorithm was proposed. The information entropy of the image encrypted by our encryption algorithm is 7.9972, the NPCR and UACI are 0.996095 and 0.334635, respectively, what both are very close to ideal values. The experimental simulation results show that the image encryption scheme exhibits good performances and high security and effectively resists various attacks.

Keywords Chaotic dynamical degradation · Image encryption · Image seed · Feedback

1 Introduction

In the era of rapidly increasing information, people are paying increasing attention to the privacy and security of information. The senders and the receivers of the information transmission do not want the information to be accessed by unauthorized third parties; thus, two most obvious solutions are provided to protect information privacy: encryption [3, 16, 26, 31,

✉ Lingfeng Liu
vatanoilcy@163.com

[1] School of Software, Nanchang University, Nanchang 330031, China

38–40] and steganography [1, 2]. Encrypting information transforms the information to a noise-like data which is observable but difficult to recover for the attackers. The main problem of encryption is that the result is a noise-like data, telling the attackers almost directly that there is important information here. The steganography technology conceals the existence of secret information by hiding in mundane communication that does not attract unwelcome snooping. In the digital steganography, the secret information is hidden in an ordinary carrier without changing the appearance of the carrier, resulting in other people cannot find which carrier the secret information is hidden in. That is to say, it should be impossible to tell whether a secret message has been added to a carrier by senses or by computer analysis. The general problems of steganography that need to be addressed are: the quality of the steganography, message detectability, payload capacity, and the robustness of the steganography against distortion attacks [2]. In this paper, we consider about the information encryption.

Information is widely divided into text, image, and video information. Among them, the image information is widely used and intuitive and vivid. Chaotic systems are widely used in the field of cryptography because of their inherent ergodicity, randomness, and extreme sensitivity to initial values, which are highly consistent with the requirements of cryptographic systems, especially in image encryption. Various image encryption algorithms are based on chaotic maps, such as the encryption algorithm that combines chaos with DNA coding [22, 32], cellular automata [25, 30], and wavelet transform [5, 7] and the chaotic encryption algorithm [26, 38–40]. However, in practical applications, chaotic systems running on devices with finite precision would eventually enter a cycle after multiple iterations due to the effects of truncation and rounding errors, which subsequentially affect the security of encryption algorithms. This is usually called as dynamical degradation of digital chaotic map. The suppression of the dynamic degradation of chaotic systems therefore received extensive attention.

So far, there are many cryptographers proposed different solutions to inhibit such dynamic degradation, which can be divided into the following categories. (1) Using higher precision equipment [12, 31]. This method is the fastest, simplest, and most direct among the proposed approaches. However, even without considering the cost, the precision of the equipment cannot be improved indefinitely. In addition, this method has inherent limitations that cannot be resolved in short term. (2) Disturbing the map [17, 18, 21, 36]. The parameters or state variables of maps can be disturbed to prolong the period and increase the randomness of the generated chaotic sequence. The disturbance source can be selected as a fixed constant, a variable, or a chaotic map. The choice of disturbance source and object is based on the cost constraint and desired effect. However, the effect of the improvement is limited. (3) Switching/Cascading multiple maps [9, 19, 23]. This method mainly relies on the superiority of the switch or cascading strategy. However, this method does not consider the internal influence that multiple different mappings may cause; and (4) Feedback mechanism [8, 11, 15, 34]. This method uses the state function to control the state variables of the digital chaotic map, which destroys the original state space. However, without the assistance of other methods, this method cannot significantly improve the performance of the digital chaotic map.

The above-mentioned methods have their own advantages and disadvantages. The improvement method proposed in this study is based on the third and fourth methods. We combined two different initial values into the same map to generate two different sequences. Subsequently, we used a nonlinear function to control the difference between the two sequences using state feedback, which enhanced the randomness and complexity of the generated chaotic sequence and suppressed the dynamic degradation of the digital chaotic map.

1D chaotic maps are widely used because of their simple structure, easy implementation, and low cost. We used this kind of maps in the experiment to confirm the effectiveness of the proposed method. The improved methods based on 1D maps could be divided as follows: (1) directly modifying the existing 1D chaotic map to generate a new chaotic sequence; (2) generating a new chaotic sequence using the sum or difference of the output sequences of two 1D sequence chaotic sequences; (3) combining two 1D chaotic maps into a 2D chaotic map; (4) taking the sequence of the 1D chaotic map as the initial values of another 1D chaotic map; and (5) switching among multiple 1D chaotic maps based on the parameters. This paper, we adopted the second improvement method. By bringing two different initial values into the 1D chaotic map, the difference of the sequence would be used as the intermediate output sequence, and then a feedback function would be used to control the intermediate output sequence to obtain the final sequence. 1D Logistic map and x-dimensional of 2D Baker maps are taken as examples. The experimental results show that this method suppressed the dynamic degradation of digital chaotic maps effectively under the condition of limited precision, and the improved maps display good performance.

The remarkable advantages of the improved method are elaborated as follows. (1) The improvement model is universal to all digital chaotic maps. When the map is one dimensional, directly adopt this model. And if the map is high dimensional, apply the model to each dimensional of the HD chaotic map. (2) No additional interference sources are introduced, the map is improved by introducing two different initial values into the same map, and a nonlinear function is used for state feedback control without excessive cost input. (3) The improved map exhibits a good effect and competitiveness with other improved schemes.

A good image encryption algorithm must be able to resist the known/selected plaintext attack. To strengthen the connection between the plaintext and encryption system, most image encryption algorithms calculate the sum of the pixel values of the plaintext image and subsequently update the initial value of the chaotic map using the calculated one [26, 35, 38]. However, this approach is not secure because the attackers can use images with the same sum of pixel values to attack the encryption system. Thus, we also designed a novel key selection method. In the method, a part information of a plain-text image would be selected by a sequence generated by 1D traditional Logistic map. Then use this information to calculate the special value p. Based on the special value, a new encryption algorithm was designed, the p value is used throughout the entire encryption algorithm, such as in updating the initial value of the chaotic map, determining the size of the rectangle for the image preprocess, and calculating the parameter in the row and column permutations. This value is also used to update the initial value of the chaotic map.

The significant advantages of the p value are summarized as follows. (1) On the basis of the sequence generated by the chaotic map, some pixels in the image are randomly selected, and the degree of randomness is high. (2) Using the p value is more secure than just using the pixel sum of the image. (3) For the same image, subtle differences in keys can result in different p values. Hence, cracking the algorithm, without clearly knowing the key is difficult for an unauthorized third party, thereby enhancing the security of the algorithm.

The remainder of this paper is organized as follows. Section 2 introduces the proposed improved model and lists the comparison results of various aspects of the 1D logistic map and x-dimensional of 2D baker map before and after improvements. In Section 3, we proposed a new image encryption scheme that uses part of images as seeds to generate a special value. The performances of the novel image encryption algorithm are discussed in Section 4. The conclusions are provided in Section 5.

2 Proposed model and improved map

This section introduces an improved model to suppress the dynamic degradation of digital chaos. The digital logistic map is used to prove the effectiveness of this method.

2.1 Improvement model

This model is mainly composed of the difference between two maps with the same type but different initial values, x_0, y_0. The tangent function is used to control the state of digital chaotic map to enhance the randomness and inhibit the degradation of the chaotic dynamics. The mathematical equation is expressed as

$$x(i+1) = F_{chaos}(u, x_i) \tag{1}$$

$$y(i+1) = F_{chaos}(u, y_i) \tag{2}$$

$$z(i+1) = \frac{|\lceil x(i+1) \times 2^n \rceil - y(i+1) \times 2^n|}{2^n} + k \times \tan(PI \times z(i)) \bmod 1 \tag{3}$$

where $F_{chaos}(\cdot)$ represents any one chaotic map, z is the final chaotic sequence generated by the model. And the initial value of sequence z is equal to x_0, which means $z_0 = x_0$. The tangent function was used to be a feedback function, then the final chaotic sequence z could be obtained by mixing the function values and difference between the maps. The function $\lceil x \rceil$ means the largest integer not greater than $(x+1)$, and PI = 3.1415926, n is the current computing precision of the equipment, u is the system parameter of the chaotic map, which ranges within [3.6,4), and k is a positive real number, whose value is selected based on the experiment. The concept of this model is universal to all 1D digital chaotic maps or anyone dimension of a HD (higher-dimensional) chaotic map, with minor form modifications. It is also possible to improve each dimension of the HD chaotic map to form a new HD chaotic map.

To better illustrate the effectiveness of this model, we used the 1D Logistic map and x-dimension of 2D Baker map as examples, respectively.

2.2 Improved logistic map

The traditional Logistic map is defined as

$$x(i+1) = F_{chaos}(u, x_i) = ux(i)(1-x(i)) \tag{4}$$

Where $x(i) \in (0, 1)$ is the state variable after i iterations, and $u \in (3.6, 4)$ is the system parameter. And the modified Logistic map after applying the proposed approach is then defined as

$$\begin{cases} x(i+1) = ux(i)(1-x(i)) \\ y(i+1) = uy(i)(1-y(i)) \\ z(i+1) = \dfrac{|\lceil x(i+1) \times 2^n \rceil - y(i+1) \times 2^n|}{2^n} + k \times \tan(PI \times z(i)) \bmod 1 \end{cases} \tag{5}$$

where k value is selected according to the experimental result, there set $k = e^2$.

The parameters are set as follows: $n = 15$, $u = 3.99$, the initial values are $x_0 = z_0 = 0.3312$, and $y_0 = 0.5845$. If no additional instructions are given, leave these settings unchanged. Several properties of the improved and original 1D Logistic maps are analyzed to evaluate the improvement effect, including the trajectory and phase space, autocorrelation function, sensitivity to initial value, approximate entropy (ApEn), permutation entropy (PE), and iteration steps before entering the period.

2.2.1 Trajectory and phase diagrams

The trajectory of the theoretical chaotic maps does not enter the period, regardless of the number of iterations, and such maps have satisfactory ergodicity in the phase space. However, the result of running on finite precision equipment is not satisfactory. The value remains the same if no special emphasis is present. Figure 1(a) and (b) show the trajectories of the original and improved Logistic maps, respectively. The figures show that the original Logistic map iterates less than 200 times before entering a period. The sequence generated by the improved chaotic map did not enter a cycle despite iterating more than 5000 times. These results indicate that the improvement method does effectively delay the entry of the map into the cycle. Figure 2(a) and (b) show that the phase diagrams of the original and improved maps, respectively. The phase diagram of the original map is a fixed upside-down U with an extremely low density that does not traverse the entire diagram space, whereas that of the improved one has no fixed shape and is much denser than the original. In conclusion, the improved map has better performance, higher security and better randomness than the original one. In addition, the dynamical degradation in the former is inhibited.

2.2.2 Autocorrelation analysis

Auto-correlation functions describe the correlation between any two values in a sequence. The autocorrelation of an ideal chaotic map rapidly decays along with the interval in one sequence. Thus, the diagram of the autocorrelation function is similar to that of the δ function. The comparison results when the computing precision $n = 16$ are showed in Fig. 3. Figure 3(a) displays the auto correlation function of the original map, which decreases with the increase or decrease in the interval and suddenly increases in particular intervals. Figure 3(b) shows the autocorrelation function of the improved map. When the current interval is not zero, the value of the curve is stable and close to zero. The correlation sharply increases when the interval

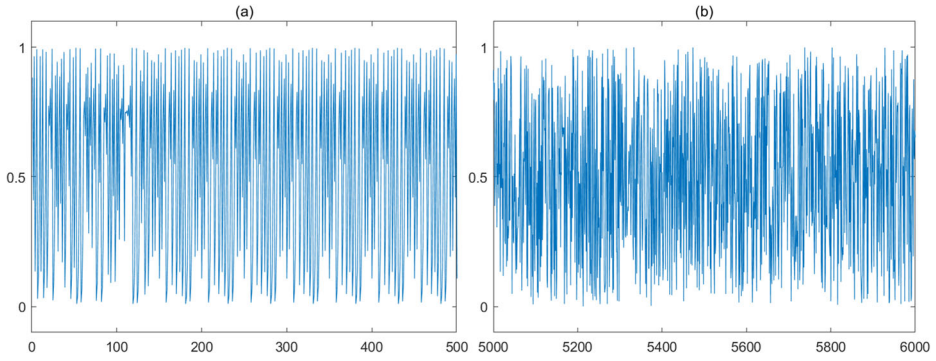

Fig. 1 Trajectories of the (**a**) original and (**b**) improved Logistic maps

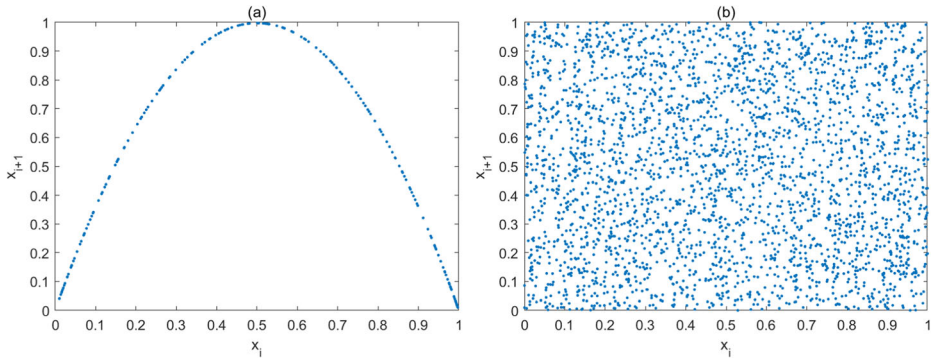

Fig. 2 Phase diagrams of the (**a**) original and (**b**) improved Logistic maps

value is zero. The shape of the curve is identical to that of the δ function, which indicates that the improved chaotic map is close to the ideal one.

2.2.3 Period analysis

One of the main manifestations of the dynamic degradation of digital chaotic systems is the entrance of the sequences to a cycle after a certain number of iterations. In this section, we focused on period length and the number of iterations before entering the cycle. Compare the change of period length and iteration steps of 1D Logistic map before and after improvement under different precisions to verify whether the improved map is better than the original one, thus proving the effectiveness of the improvement method. We take the same parameters under different accuracy conditions, generate sequences with length of 500,000, and calculate the num of iteration times before entering the cycle and their period length. The results are showed in the Table 1. These results only come from one experiment under a certain parameter and initial value, rather than the average result brought by many experiments, which cannot represent the overall trend of the whole map. From the table, the effectiveness of the improved method was illustrated.

2.2.4 Sensitivity to initial conditions

A good chaotic map is extremely sensitive to subtle changes in initial conditions. The initial conditions include initial values and system parameters. Any small change in these values or

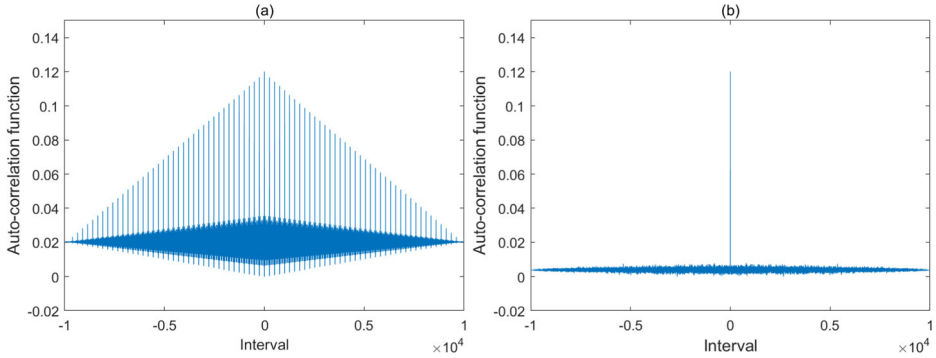

Fig. 3 Autocorrelation function of the (**a**) original and (**b**) improved Logistic maps

parameters will result in a huge difference in the generated sequence. By applying minor modifications to the initial values and parameters, we generated two sequences and compared their trajectories to verify that the improved chaotic map has a good performance and extreme sensitivity to the initial conditions. Figure 4 shows the experimental results under a precision of 2^{-15}. The blue lines in Fig. 4(a)–(d) represent the trajectory of the improved chaotic mapping within 50 iterations under certain conditions; Fig. 4(a)–(d) show the comparison of the sequence curve after the slight modification of u, x and y, and the sequence curve before the parameter change. The results show that even a slight alteration can cause a complete change in the sequences.

2.2.5 Complexity analysis

ApEn and PE are scalars that are commonly used when evaluating the complexity of a chaotic map. ApEn measures the probability of the new pattern generated in the sequences using growing embedding dimensions [28]; the larger the probability, the more complex the sequence. PE [4], compares the sizes of several consecutive values in the sequence and adds the different order types. Shannon's entropy is then used to measure the uncertainty of these orders. The PE of an ideal random sequence should be close to 1. Set the initial values are $x_0 = z_0 = 0.4312$, and $y_0 = 0.5845$, and the test result diagrams shown in Figs. 5 and 6 are used for the analysis. From the figures, it's obvious that the ApEn and PE values of the improved map are greater than those of the original one. And the ApEn value of the improved map after stabilization is much higher than that of the original map. The PE value of the improved map closer to ideal value 1.

Table 1 Period length and step length before entering the cycle (Logistic map)

Precision	Period length		Step length	
	Original map	Improved map	Original map	Improved map
2^{-4}	3	9	2	3
2^{-5}	5	10	1	15
2^{-6}	11	33	1	8
2^{-7}	6	24	4	16
2^{-8}	10	40	3	24
2^{-9}	3	54	2	10
2^{-10}	30	30	16	399
2^{-11}	29	261	9	244
2^{-12}	4	80	4	157
2^{-13}	35	700	28	444
2^{-14}	37	222	41	1148
2^{-15}	50	2550	137	456
2^{-16}	253	4048	90	10,262
2^{-17}	178	2314	117	2753
2^{-18}	392	15,288	87	1899
2^{-19}	83	2988	416	3307
2^{-20}	989	10,879	688	11,253
2^{-21}	399	6384	1595	10,209
2^{-22}	1021	–	508	–
2^{-23}	3715	–	944	–
2^{-24}	100	–	985	–
2^{-25}	1362	–	547	–

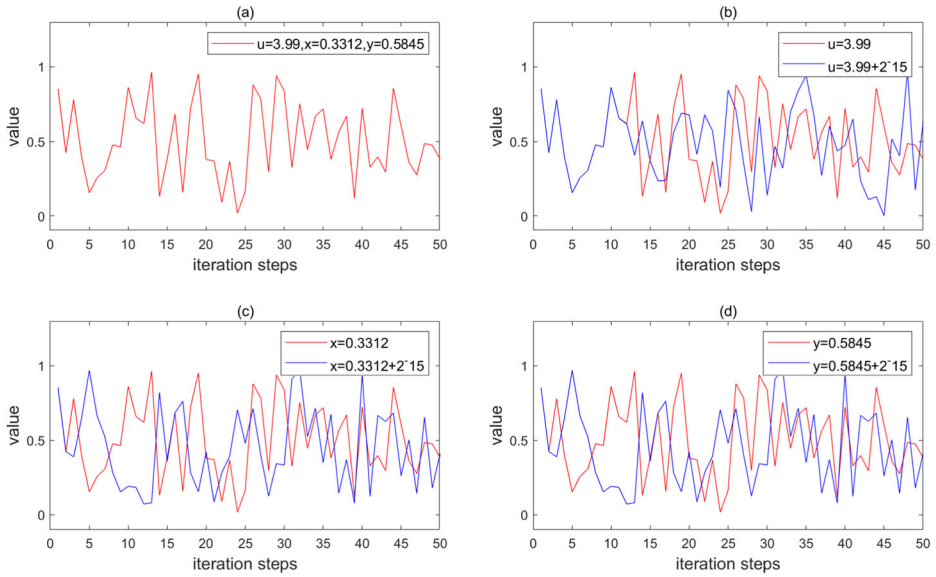

Fig. 4 Sensitivity analysis of the initial condition (**a**) curve at $u = 3.99$, $x = 0.3312$, $y = 0.5845$; (**b**) curves at $u = 3.99$ and $u = 3.99 + 2^{-15}$; (**c**) curves at $x = 0.3312$ and $x = 0.3312 + 2^{-15}$; (**d**) curves at $y = 0.5845$ and $y = 0.5845 + 2^{-15}$

2.3 Improved baker map

As one of the common 2D digital chaotic maps, Baker map is expressed as follows:

$$(x_{i+1}, y_{i+1}) = \begin{cases} \left(\frac{x_i}{p}, py_i\right), & 0 < x_i \leq p \\ \left(\frac{x_i - p}{1-p}, (1-p)y_i + p\right), & p < x_i \leq 1 \end{cases} \tag{6}$$

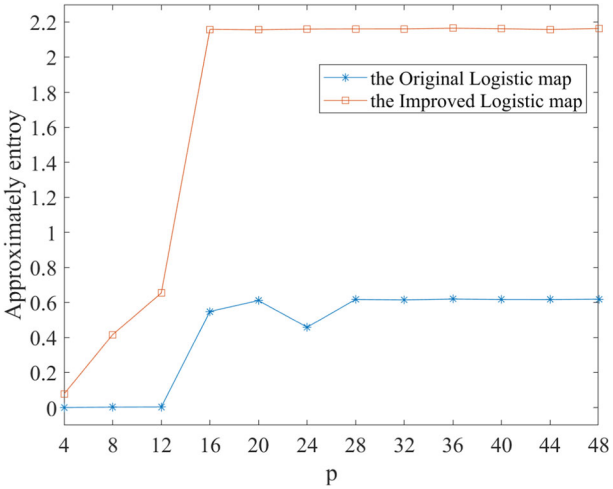

Fig. 5 Approximate Entropy analysis under different precisions

Where $p \in (0, 1)$ is the system parameter. We selected x-dimensional of Baker chaotic map as example to prove the effectiveness of the improvement method and the generality in all 1D maps or one dimension of a HD map. The x-dimensional of Baker chaotic map could be described as:

$$x_{i+1} = \begin{cases} \frac{x_i}{p}, & 0 < x_i \leq p \\ \frac{x_i - p}{1-p}, & p < x_i \leq 1 \end{cases} \tag{7}$$

Thus, the modified x-dimensional of Baker map would be expressed as.

$$\begin{aligned} x(i+1) &= \begin{cases} \frac{x(i)}{a}, & 0 < x(i) \leq a \\ \frac{x(i)-a}{1-a}, & a < x(i) \leq 1 \end{cases} \\ y(i+1) &= \begin{cases} \frac{y(i)}{a}, & 0 < y(i) \leq a \\ \frac{y(i)-a}{1-a}, & a < y(i) \leq 1 \end{cases} \\ z(i+1) &= \frac{|\lceil x(i+1) \times 2^n \rceil - y(i+1) \times 2^n|}{2^n} + k \times \tan(PI \times z(i)) \mod 1 \end{aligned} \tag{8}$$

where $a \in (0, 1)$ is the system parameter, and PI = 3.1415926, and set $k = 6$. The same experimental methods as in Section 2.2 is used to compare the classical and modified x-dimensional of Baker map. The parameters are set as follows: $n = 12$, $a = 0.6$, the initial values are $x_0 = z_0 = 0.3312$, and $y_0 = 0.5845$. If no additional instructions are given, leave these settings unchanged. In this experiment, we only analyze the x-dimensional of Baker map.

Figure 7 (a) and (b) showed the trajectories of the classical and modified map. From the figure, it's clear that the improvement method does extend the time for the generated sequence to enter the cycle. The phase diagram analysis is showed in Fig. 8 (a) and (b). In this experiment, we plot by using x_i and x_{i+1} to depict the attractor complexities. As shown in Fig. 8 (a) and (b), the modified map has more complicated attractor than its classical

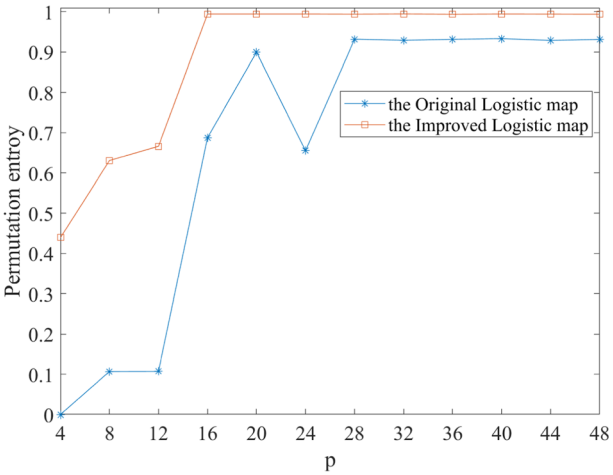

Fig. 6 PE analysis under different precisions

counterpart. After the improvement, the phase diagram points of the map are discretized and the density is higher. These results fully demonstrate the effectiveness of our improved method.

Next, we calculate the num of iteration times before entering the cycle and their period length. Set $x_0 = z_0 = 0.4312$. The results are showed in the Table 2. From the table, we can conclude that the improvement method does extend the period length and the iteration times before entering a cycle. What's more, when the accuracy exceeds 2^{-12}, the x-dimension of the improved Baker map cannot measure the period. Again, the results of this experiment are derived from the experimental data under a certain parameter condition, which can only represent a certain situation. And the results could only be used to prove that the improved method is effective and the improved map has a longer cycle and iteration times than that before the improvement.

The ApEn and the PE analysis for two maps are plotted as Figs. 9 and 10, respectively. From the two figures, it's clear that under the same computing precision the ApEn and PE values of improved x-dimensional of Baker map are much larger than the original ones. And the PE value of improved map are closer to ideal value, 1. These proved that the capability of the proposed approach in enhancing the complexity of the classical x-dimensional of Baker map on a finite precision machine. As Fig. 11 showed, the improved map remains the sensitivity to initial conditions. Under the computing precision of 2^{-12}, the initial condition is only 2^{-12} apart, resulting in a complete separation of the two curves.

All the above results not only prove the effectiveness of the improved method, but also prove its universality to digital chaotic maps. And then we designed a new encryption algorithm based on the improved digital logistic map and a new key selection method.

3 New cryptosystem based on the improved digital logistic map

We proposed a new image encryption algorithm with partial plaintext images as the seed information based on the improved map. This algorithm is applicable to grayscale and colored images. For the convenience of description, the encryption of the grayscale image is considered as an example here. If it is a colored image, it only needs to be divided into three channels. After encrypting each channel, the final colored ciphertext image can be obtained through the XOR operation.

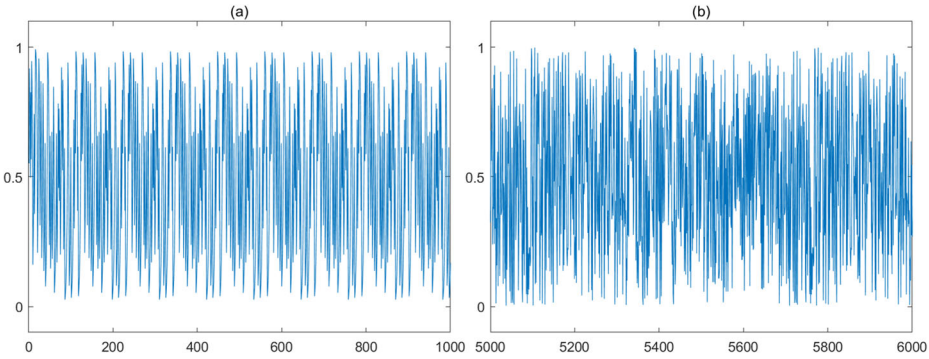

Fig. 7 Trajectories of the (**a**) original and (**b**) improved x-dimensional of Baker maps

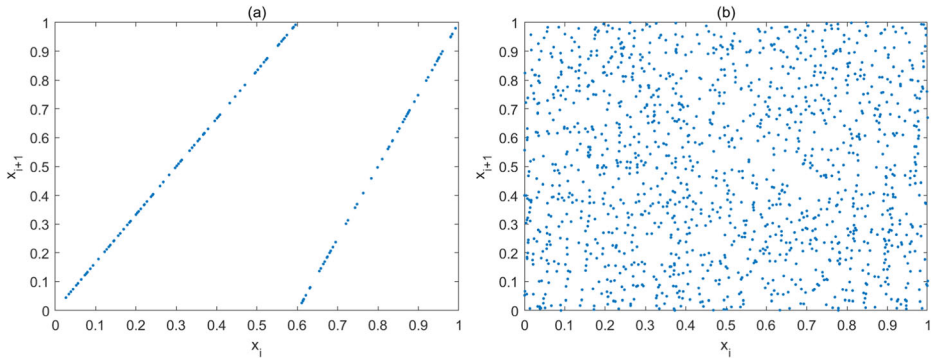

Fig. 8 Phase diagram analysis of the (**a**) original and (**b**) improved *x*-dimensional of Baker maps

3.1 Secret key structure and the key selection method

As shown in Fig. 12, the secret key of the proposed cryptosystem comprises four parts, namely, system parameter $u \in (3.6,4)$, initial values x and $y \in (0,1)$, and the special value of the image $p \in (0,1)$. The special value, p, is derived from plaintext image, which strengthens the correlation between cipher text system and plaintext image. Moreover, this method is more effective than simply calculating the average pixel value of the plaintext image. Only by calculating the average pixel value of the plaintext image to enhance the ability to resist plaintext attacks is not secure. Because it could be attacked by different images of the same pixel sum, thus cracking the encryption algorithm. However, our method relies on chaotic map to randomly select some pixels of the image, and even a slight difference in the secret key will result in different points being selected from the plaintext image. So only if you have the correct key and special value can you get a plaintext image correctly.

Next, the steps to generate the special value p are described in detail. Assume the plain image is represented by P and its size is set as $M \times N$.

First, the original 1D Logistic map is used to generate two sequences of length a, $\{px_i\}$ and $\{py_i\}$, where $i = 1,2,3, \ldots, a$. $a = round(min\ (M, N)/5)$, function $min(M, N)$ represents the smaller value between M and N, and $round(\cdot)$ means round to get an integer. The initial values are $px(0) = x$ and $py(0) = y$.

Table 2 Period length and step length before entering the cycle (*x*-dimensional of Baker map)

Precision	Period length		Step length	
	Original map	Improved map	Original map	Improved map
2^{-4}	1	8	2	3
2^{-5}	25	25	1	10
2^{-6}	14	14	2	27
2^{-7}	8	16	2	52
2^{-8}	20	40	5	21
2^{-9}	249	249	1	63
2^{-10}	35	210	50	53
2^{-11}	78	702	10	86
2^{-12}	112	336	52	613
2^{-13}	2903	–	1	–
2^{-14}	123	–	1	–

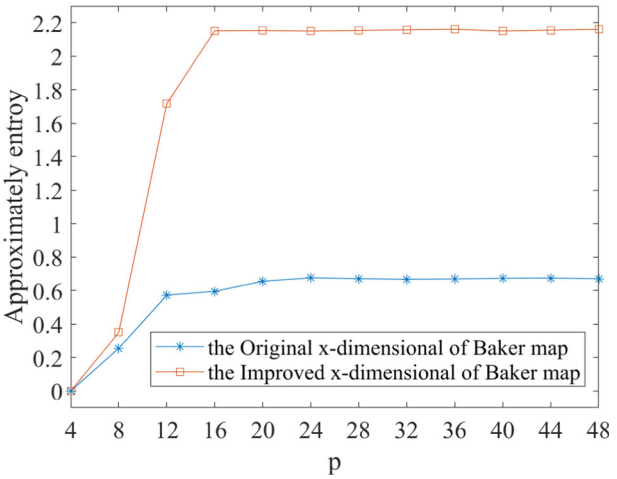

Fig. 9 Approximate Entropy analysis of the (**a**) original and (**b**) improved *x*-dimensional of Baker maps

$$\begin{aligned} px(i+1) &= u \times px(i) \times (1-px(i)) \\ py(i+1) &= u \times py(i) \times (1-py(i)) \end{aligned} \tag{9}$$

Second, the two sequences $\{px_i\}$ and $\{py_i\}$ are converted into integer sequences $\{pX_i\}$ and $\{pY_i\}$, respectively. Where n represents the current computing precision.

$$\begin{aligned} pX_i &= ceil(px(i+1) \times 2^n) \mod M \\ pY_i &= ceil(py(i+1) \times 2^n) \mod N \end{aligned} \tag{10}$$

Third, the two integer sequences are processed to form a sequence $\{Z\} = \{(pX_1, pY_1), (pX_2, pY_2), \ldots, (pX_i, pY_i), \ldots, (pX_a, pY_a)\}$. The corresponding points in image P of each pair of values in this sequence (coordinates) are obtained and the total value SUM is obtained through summation.

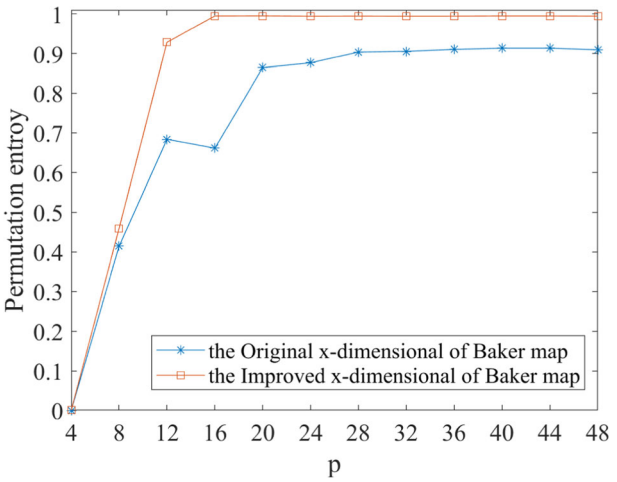

Fig. 10 Permutation Entropy analysis of the (**a**) original and (**b**) improved *x*-dimensional of Baker maps

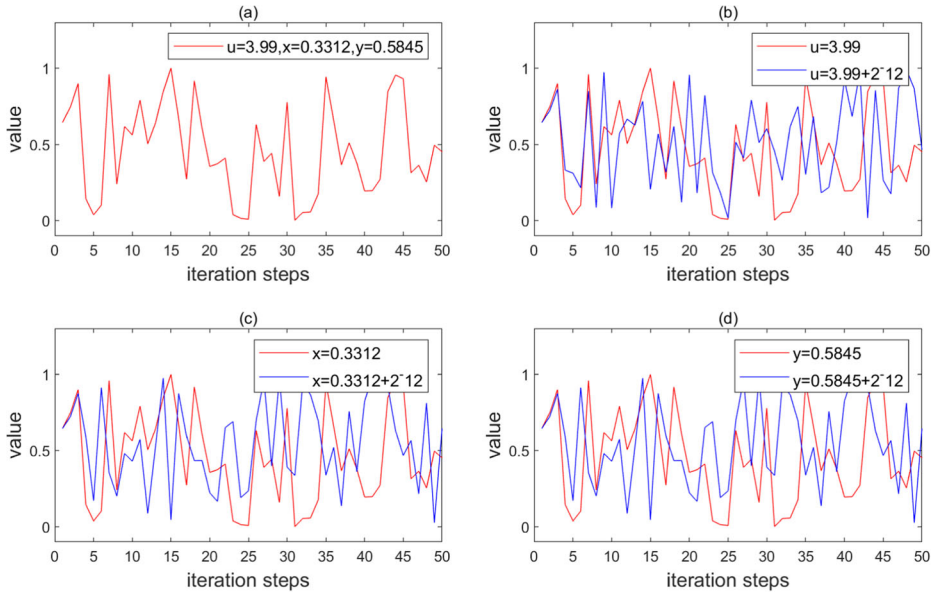

Fig. 11 Sensitivity analysis of the initial condition (**a**) curve at $u = 3.99$, $x = 0.3312$, $y = 0.5845$; (**b**) curves at $u = 3.99$ and $u = 3.99 + 2^{-12}$; (**c**) curves at $x = 0.3312$ and $x = 0.3312 + 2^{-12}$; (**d**) curves at $y = 0.5845$ and $y = 0.5845 + 2^{-12}$

$$SUM = P(pX_1, pY_1) + P(pX_2, pY_2) + \ldots + P(pX_a, pY_a) \tag{11}$$

Fourth, the value of sequence $\{z_i | \, i = 1, 2, \ldots, a\}$ is calculated. Before this calculation, the value of SUM is used to obtain the *dire* value, which was used to select corresponding computational equation.

$$\begin{aligned} dire &= SUM \bmod 3 \quad + \quad 1 \\ z(i) &= \begin{cases} P(pX_i, pY_i) \quad \oplus \quad P(pX_i + 1, pY_i), & if \;\; dire = 1 \\ P(pX_i, pY_i) \quad \oplus \quad P(pX_i, pY_i + 1), & if \;\; dire = 2 \\ P(pX_i, pY_i) \quad \oplus \quad P(pX_i + 1, pY_i + 1), & if \;\; dire = 3 \end{cases} \end{aligned} \tag{12}$$

Finally, the special value p of the image P is obtained as

$$p = \frac{\sum_{i=1}^{a} z(i)}{a} \bmod 1 \tag{13}$$

where sum(•) represents the cumulative sum of this sequence. The above expression is the calculation for the p value, which is then used as a part of the secret key.

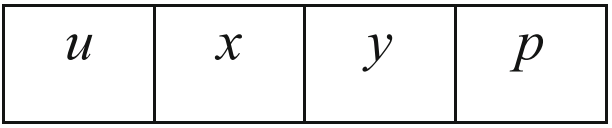

Fig. 12 Secret key structure of the image

3.2 Image encryption and decryption algorithms

P is a plain grayscale image with a size of M × N. The reasons for using grayscale images have already been discussed in a previous section and will not be repeated here. For the plain image P, we first calculated the p value using the method described in Section 3.1. Subsequently, we started the encryption algorithm step and used the grayscale Lena image as an example.

Step 1: Preprocessed plain-text image P. Using the p value, a rectangle with a size of $L1 \times L2$ is selected from the plaintext image for processing. Obtain $L1, L2$ value by using p value, the equation could be described as follow:

$$L1 = \begin{cases} round(p \times M), & 0 < p < 0.5 \\ round((1-p) \times M), & 0.5 < p < 1 \end{cases} L2 = round(p \times N) \tag{14}$$

In the rectangle, each element in the ith row is XORed with the corresponding element in the $(i + L1)$th row, and the preprocessed image is obtained. Put it in mathematical form as follow:

$$P(i,j) = P(i,j) \oplus P(i + L1, j) \quad 1 \leq i < L1, 1 \leq j < L2 \tag{15}$$

The rectangle can be taken from anywhere in the image, but for simplicity, the rectangle is extracted from the upper left corner. Finally, the preprocessed image A would be obtained. For example, the images before and after the preprocessing are shown in Figs. 13 (a) and (b).

Step 2: The p value is also used to update the initial value x and y.

$$\begin{aligned} x &= (x + p) \bmod 1 \\ y &= (y + p) \bmod 1 \end{aligned} \tag{16}$$

The initial conditions u, the updated value x and y are introduced to the improved chaotic map to generate a chaotic sequence $\{s\} = \{s_1, s_2, s_3, \ldots, s_{M \times N}\}$. Obtain sorted sequence $\{s_{order}\}$ by ranking the sequence from smallest to largest, keeping the index the same.

Fig. 13 Images (**a**) before and (**b**) after preprocessing

The processed image A is scanned from top to bottom and from left to right to obtain a 1D sequence $\{A\}$. And then the index order $\{r_1, r_2, \ldots, r_{M\times N}\}$ of sequence $\{s_{order}\}$ is used to scramble the sequence $\{A\}$, which was described as follow:

$$\{s_{order}\} = \{s_{r1}, s_{r2}, s_{r3}, \ldots, s_{rM\times N}\} \tag{17}$$

$$\{A_{order}\} = \{A_{r1}, A_{r2}, A_{r3}, \ldots, A_{rM*N}\} \tag{18}$$

Step 3: The sorted sequence $\{A_{order}\}$ is transformed from top to bottom and left to right into a 2D matrix A_{order}.

Step 4: Sequence $\{s\}$ is also used to calculate the parameters as

$$D_{rx}(i) = round\left(s(i)*p*10^6\right) \bmod 255 + 1, 1\le i\le M \tag{19}$$

$$D_r(i) = round\left(s(i)*p*10^6\right) \bmod N, 1\le i\le M \tag{20}$$

$$D_{cy}(j) = round\left(s(M+j)*p*10^6\right) \bmod 255 + 1, 1\le j\le N \tag{21}$$

$$D_c(j) = round\left(s(M+j)*p*10^6\right) \bmod M, 1\le j\le N \tag{22}$$

Where $D_{rx}(i) \in [1, 255]$, $D_r(i) \in [0, N-1]$ are used for row substitution and row shift, respectively, and then $D_{cy}(j) \in [1, 255]$, $D_c(j) \in [0, M-1]$ are used to perform column substitution and column shift, respectively.

Step5: Perform row substitution and row shift with $D_{rx}(i)$ and $D_r(i)$. XOR operation is conducted on the ith row pixels A_{order}(i,:) and the encrypted row pixels are determined as

$$B(i,:) = A_{order}(i,:) \oplus D_{rx}(i), 1\le i\le M \tag{23}$$

Subsequently, D_r is used to perform the circular shift, which represents the number of steps moved. If the number is odd, the ith encrypted B(i,:) is shifted toward the left; otherwise, the shift is directed toward the right.

Step 6: For $i = i + 1$, step 5 would be repeated in a loop until $i > M$; matrix B represents the image after the row permutation.

Step7: Perform column substitution and column shift with $D_{cy}(j)$, $D_c(j)$. XOR operation is conducted on jth column pixels B(:, j), and the encrypted column pixels are determined as

$$C(:,j) = B(:,j) \oplus D_{cy}(j) \tag{24}$$

$D_c(j)$ is used to perform the circular shift. If the number is odd, circular the j-th encrypted C(:, j) is shifted upward; otherwise it is shifted downward.

Step 8: For $j = j + 1$, step 7 would be performed in a loop until $j > N$.
Step 9: The encrypted image C is obtained after the row and column permutation. We transformed the sequence {s} to the 2D matrix S. Then, XOR operation is conducted and the final encrypted image E is obtained as

$$E = S \oplus C \tag{25}$$

The flow chart of the entire encryption process is illustrated in Fig. 14.

The decryption process is the reverse of the encryption process. The value of p is passed to the recipient as part of the secret keys. The flowchart of the decryption process is shown in the Fig. 15.

3.3 Simulation results

In order to illustrate the universality and practicability of this encryption algorithm, we used 10 different images for experiments. However, due to space limitation, we only show the results of three images here. The precision is set to as 15 and the initial conditions are established as follows: $u = 3.99$, $x = 0.3312$, and $y = 0.5845$. The p value of each figures is calculated respectively and the encryption steps are subsequently performed to encrypt the plaintext images. Figure 16 shows the simulation results.

From Fig. 16, it's obvious that the encrypted image no longer provides information on the plain image, and the correct decrypted image is the same as the plain image.

4 Performance analysis and comparison

4.1 Key space

The size of the key space of the encryption algorithm directly affects the ability of the algorithm to resist brute force attacks. Under similar conditions, the larger the key space, the stronger the ability of the encryption algorithm to resist brute force attacks and the more secure the algorithm will be. The keys in the proposed method are divided into four parts (u, x, y, p), where $u \in (3.6, 4)$, x, y, $p \in (0, 1)$. In general, the key space of a secure encryption algorithm should be larger than 2^{128}. The proposed key space is $0.4 \times 10^{15} \times (1 \times 10^{15})^3 = 0.4 \times 10^{60} \approx 0.4 \times 2^{189.7} >> 2^{128}$, with an accuracy of 15. This space is larger than those obtained in previous studies (i.e., 10^{56} [13], 10^{45} [33], 10^{57} [14], and 10^{53} [37]). In conclusion, the proposed algorithm can effectively resist brute force attacks.

4.2 Histogram analysis

The histogram shows the distribution of the pixel intensity values of the images. The image with an uneven distribution of histogram can be easily cracked by statistical attacks. A good encryption algorithm has an encrypted image that does not show any information and a uniformly distributed histogram. In addition, the histogram of the decrypted image should be consistent with that of the original image. The experiment results are showed as Figs. 17, 18 and 19. The results show that the histogram distribution of the original image is extremely

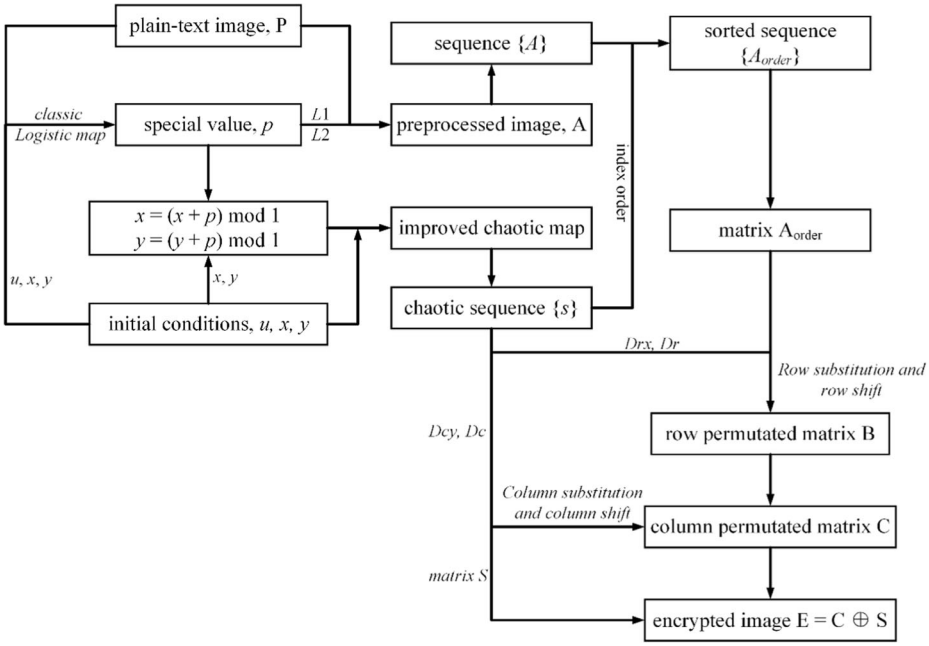

Fig. 14 Flowchart of the encryption process

uneven, thereby exposing the information distribution of the image. Conversely, the histogram distribution of the ciphertext image is uniformly distributed, which cannot be easily cracked by statistical attacks. The histogram of the decrypted image is consistent with that of the original image. As previously established, the proposed algorithm satisfies the requirements of a good encryption algorithm.

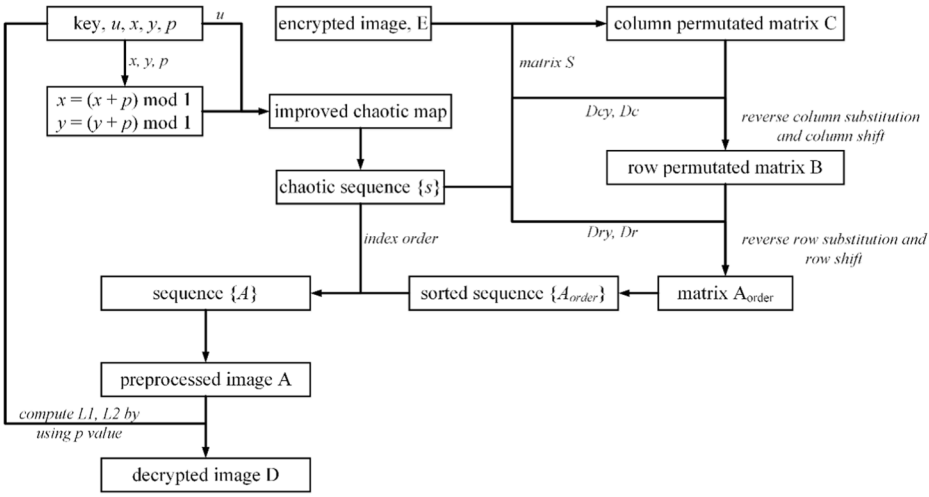

Fig. 15 Flowchart of the decryption process

Fig. 16 (**a**) plain-text image (**b**) encrypted image (**c**) decrypted image of Lena image; (**d**) plain-text image (**e**) encrypted image (**f**) decrypted image of Rice image; (**g**) plain-text image (**h**) encrypted image (**i**) decrypted image of Cameraman image

4.3 Correlation analysis

The most challenging aspect of image encryption is the strong correlation between adjacent pixels. If this problem is not solved, the security of the encryption algorithm will be greatly reduced. The correlation of two adjacent pixels is defined as

$$\rho_{xy} = \frac{\sum_{i=1}^{G}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{G}(x_i - E(x))^2 \sum_{i=1}^{G}(y_i - E(y))^2}} \tag{26}$$

where x and y are two adjacent pixel points, G is the sample counts, $E(x) = \frac{1}{N}\sum_{i=1}^{G} x_i$, and $E(y) = \frac{1}{N}\sum_{i=1}^{G} y_i$. A total of 10,000 pairs of adjacent pixels were taken from the horizontal, vertical, and diagonal directions of the images before and after encryption, and the correlation among them was calculated. The correlation between the adjacent pixels of the Lean image is

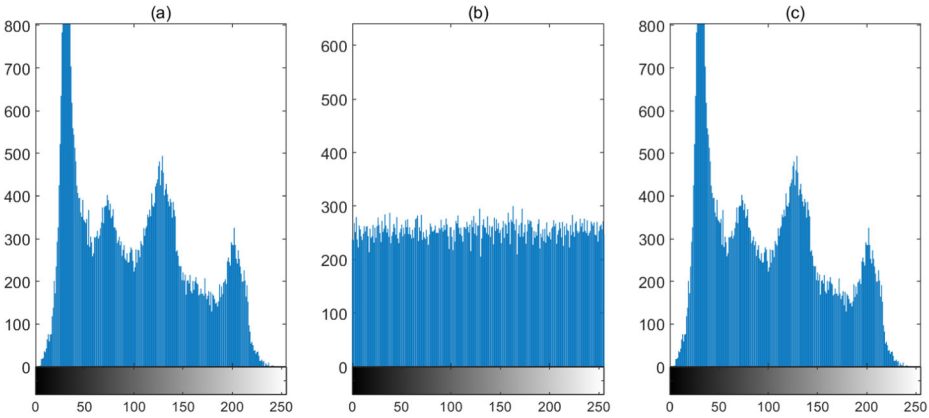

Fig. 17 Histogram diagrams of the (**a**) plain, (**b**) encrypted, and (**c**) decrypted Lena images

strong in any of the three directions (Fig. 20(a)- (c)). However, Fig. 20(d)- (f) show that the correlation between the adjacent pixels of the ciphertext image broken and exhibits a discrete distribution. The experimental results of other two example images (Rice image and Cameraman image) are the same. However, due to the space limitation of the paper, we only show the adjacent pixel distribution of the encrypted image here (Figs. 21 and 22).

Table 3 presents the comparison of the correlation coefficients of the proposed encryption algorithm with those of other algorithms. The comparison results show that the proposed algorithm is competitive.

4.4 Key sensitivity

Key sensitivity is the degree of the changes in the result when the key is slightly changed during the encryption process. A small change in the keys can result in a completely different encrypted image. The satisfactory image encryption algorithm should demonstrate outstanding key sensitivity. To investigate the key sensitivity of the proposed algorithm, we slightly modified u, x, and y and then calculated the mean square error (MSE) between the ciphertext image generated by the modified key and the original ciphertext image.

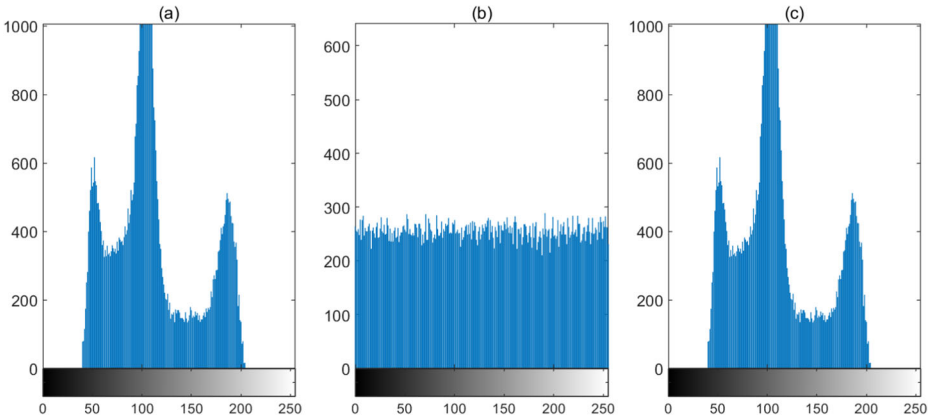

Fig. 18 Histogram diagrams of the (**a**) plain (**b**) encrypted and (**c**) decrypted Rice images

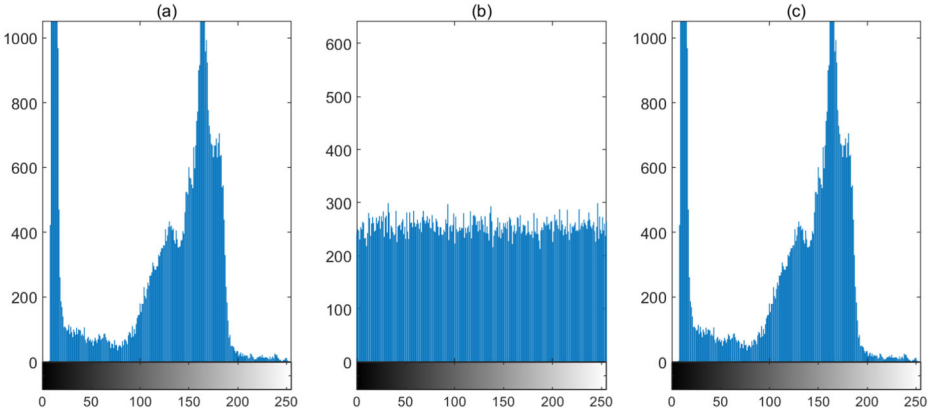

Fig. 19 Histogram diagrams of the (**a**) plain (**b**) encrypted and (**c**) decrypted Cameraman images

$$MSE = \frac{1}{R}\sum_{i=1}^{R}(y_i - x_i)^2 \tag{27}$$

where R = M × N. The ciphertext image generated by the modified key is compared with each element of the original ciphertext image. The calculated MSE value of Lena image is shown in Fig. 23. Except for the difference value of 0, in other cases, the MSE value of the changed and original ciphertext images is extremely large regardless if the change is applied to u, x, or y. The results of other two sample images show the same trend, which are not shown here due to space limitations. This finding implies that the proposed encryption algorithm is extremely sensitive to the key.

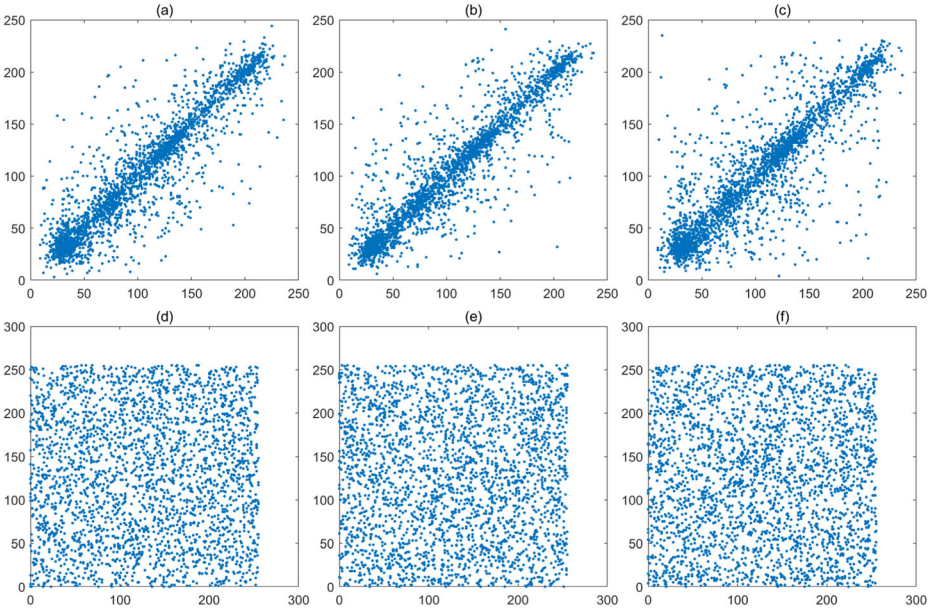

Fig. 20 Distribution of the adjacent pixels: (**a**) horizontal (**b**) vertical (**c**) diagonal directions of the plain Lena image and (**d**) horizontal (**e**) vertical (**f**) diagonal directions of the encrypted Lena image

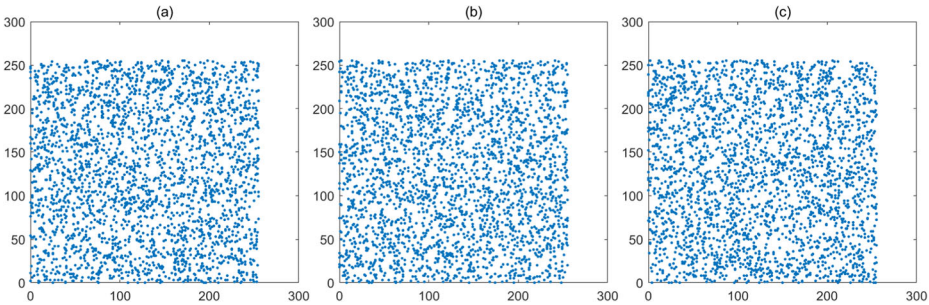

Fig. 21 Distribution of the adjacent pixels: (**a**) horizontal (**b**) vertical (**c**) diagonal directions of the encrypted Rice image

4.5 Information entropy analysis

Information entropy is used to measure the randomness of information. The greater the information randomness, the greater the entropy and the more information is needed for clarification. The maximum information entropy for a 256 × 256 grayscale image is 8.

$$H(u) = \sum_{i=1}^{W} p(u_i) \log \frac{1}{p(u_i)} \tag{28}$$

where u represents a message source, W is the total number of symbols, and $p(u_i)$ is the probability of symbol u_i [10]. The results of the different algorithms are listed in Table 4. The results reveal that the information entropy of the proposed method is extremely close to the ideal value 8, compared with other methods, which indicates that the proposed algorithm is competitive.

4.6 Analysis of the resistance to differential attacks

A differential attack is an effective and the most common mode of attack. In general, the values of the number of pixel change rate (NPCR) and unified average changed intensity (UACI) are used to evaluate the ability of an encryption algorithm to resist differential attacks. The calculation formula of NPCR and UACI are expressed as

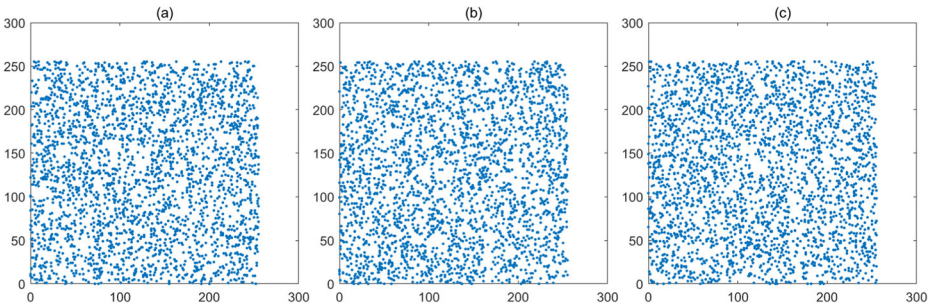

Fig. 22 Distribution of the adjacent pixels: (**a**) horizontal (**b**) vertical (**c**) diagonal directions of the encrypted Cameraman image

Table 3 Correlation coefficients of different algorithms

Algorithm	Horizontal	Vertical	Diagonal
Lena image	0.9281	0.9456	0.8947
Our method (2^{-16})	0.0013	−0.0041	−0.0044
Ref. [37]	−0.0032	0.0141	0.0058
Ref. [27]	0.0064	0.0004	−0.0095
Ref. [24]	−0.0069	0.0070	−0.0014
Rice image	0.9236	0.9369	0.8890
Encrypted rice image	0.0019	0.0008	−0.0014
Cameraman image	0.9333	0.9565	0.9059
Encrypted cameraman image	0.0004	0.0012	−0.0004

$$NPCR(C1,C2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|sign(C1(i,j) - C2(i,j))|}{MN} \tag{29}$$

$$UACI(C1,C2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{MNF} \tag{30}$$

where M and N are the length and width of the image, respectively, C1 and C2 represent two different images with the same size, F is the largest allowed pixel value in the images, and $sign(\cdot)$ is the symbol function. If $C1(i,\ j) = C2(i,\ j)$, then $|sign(\cdot)| = 0$; otherwise, $|sign(\cdot)| = 1$. In addition, $M = N = 256$ and $F = 255$. The ideal values of NPCR and UACI are 0.9961 and 0.3346, respectively. In this experiment, the difference between the two images is only one pixel, and the value of this pixel only differs by 1.

Table 5 presents the NPCR and UACI values of different algorithms for the sample image. The values of the proposed method are close to the ideal ones. Therefore, the proposed algorithm is competitive compared with the other ones.

4.7 Robustness analysis against data-loss and noise attacks

The encrypted image must be transmitted to the receiver. The image information is extremely vulnerable to various attacks or influences during the transmission process, which results in partial loss of data or overlaying of noise on the image. An ideal encryption algorithm can decrypt the ciphertext image to the correct image when former is affected. The decrypted image may not be perfect, but it must have the ability to see the general information of the

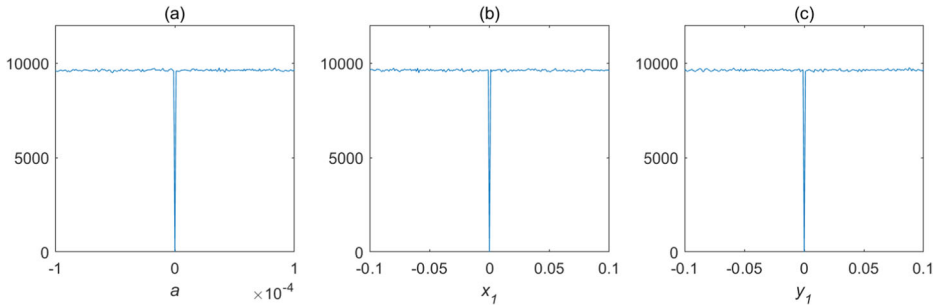

Fig. 23 MSE of (**a**) u, (**b**) x, and (**c**) y

Table 4 Information entropy of different algorithms

Algorithms	Information Entropy
Lena image	7.5635
our method (2^{-16})	7.9972
Ref. [32]	7.9892
Ref. [25]	7.9972
Ref. [13]	7.9971
Rice image	7.0115
Encrypted Rice image	7.9976
Cameraman image	7.0097
Encrypted cameraman image	7.9973

original image. The test results of data-loss attack are shown in Figs. 24 and 25. The ciphertext images can be correctly decrypted despite the different levels of data loss attacks. And Figs. 26 and 27 shows the three images experimental results under different kinds of noise attacks. Most parts of the original image can be seen despite the slight flaws, which proves the ability of the proposed encryption algorithm to resist robust attacks.

4.8 Speed analysis

A good encryption algorithm must not only have good performance, but also have a fast enough encryption speed to be practical. There some studies claim that traditional encryption is faster than chaotic encryption for images, such as [29]. Thus, we take the speed analysis here. The encryption speeds of different schemes are shown in Table 6. These results indicate that our algorithm is competitive for practical use.

5 Conclusion

In this study, a novel improvement model is proposed to suppress the dynamical degradation of digital chaotic map and a new image encryption scheme is designed. Two chaotic maps with the same type but different initial values are used as the difference, and a nonlinear function is used as feedback function to affect the previously obtained difference, then degradation of the chaotic dynamics was suppressed. A 1D Logistic map and x-dimensional of 2D Baker map are taken as examples to improve the effectiveness of the proposed improvement model. What's more, a new key selection method is proposed. In the method, part information of plain-text image would be selected by the sequence generated by a chaotic map, which resulting in the randomness of the selection of the part information. The special value p would be obtained by

Table 5 NPCR and UACI values of different algorithms

Algorithms	NPCR	UACI
ideal values	0.9961	0.3346
Our method (2^{-16})	0.996094	0.334635
Ref. [22]	0.9976	0.3912
Ref. [13]	0.9962	0.3347
Ref. [27]	0.9961	0.3350

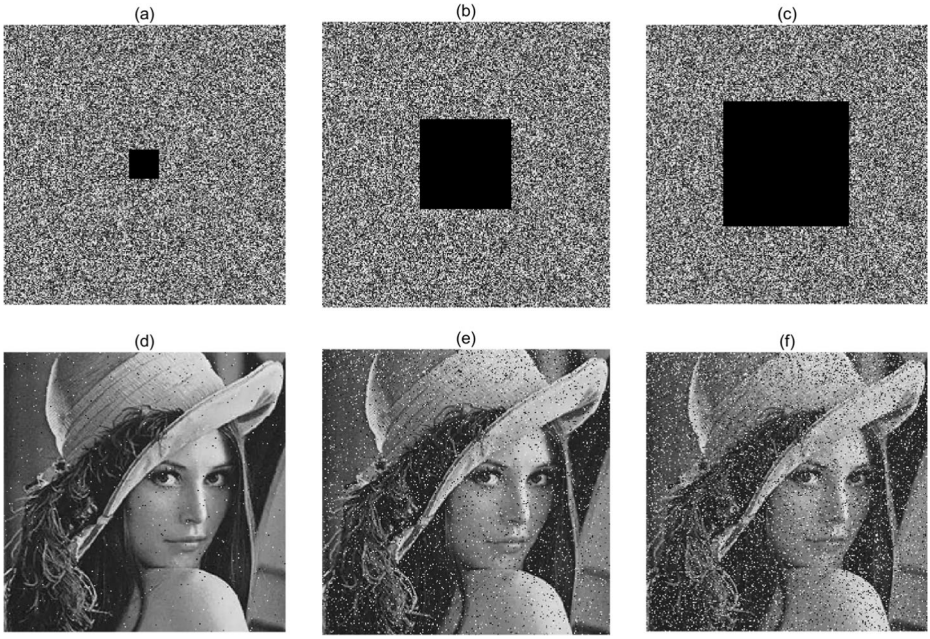

Fig. 24 Robustness against occlusion attacks: encrypted Lena image with (**a**) 0.01 data loss, (**b**) 0.1 data loss, and (**c**) 0.2 data loss; decrypted Lena image with (**d**) 0.01 data loss, (**e**) 0.1 data loss, and (f) 0.2 data loss

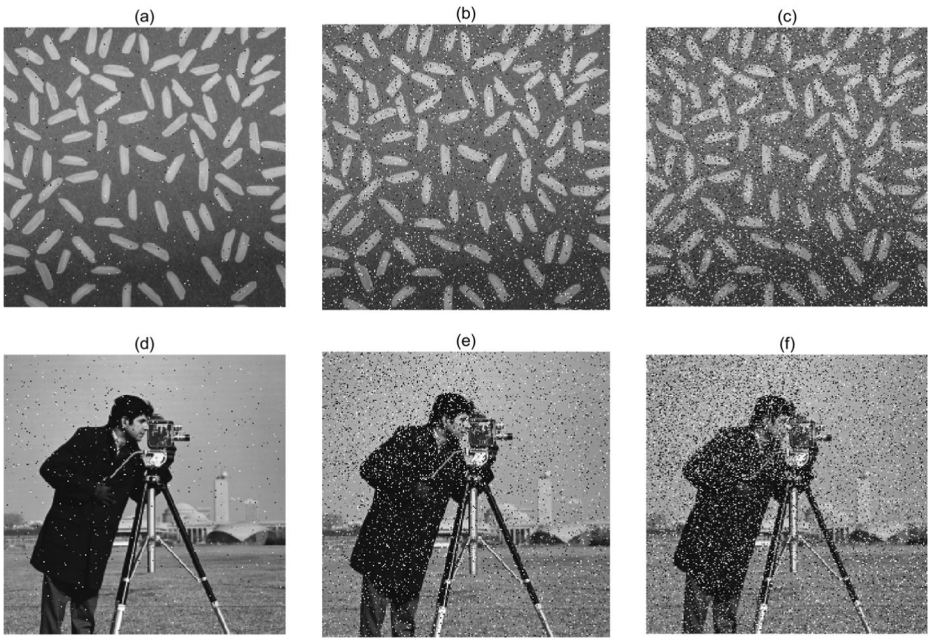

Fig. 25 Robustness against occlusion attacks: decrypted Rice image with (**a**) 0.01 data loss, (**b**) 0.1 data loss, and (**c**) 0.2 data loss; decrypted Cameraman image with (**d**) 0.01 data loss, (**e**) 0.1 data loss, and (**f**) 0.2 data loss

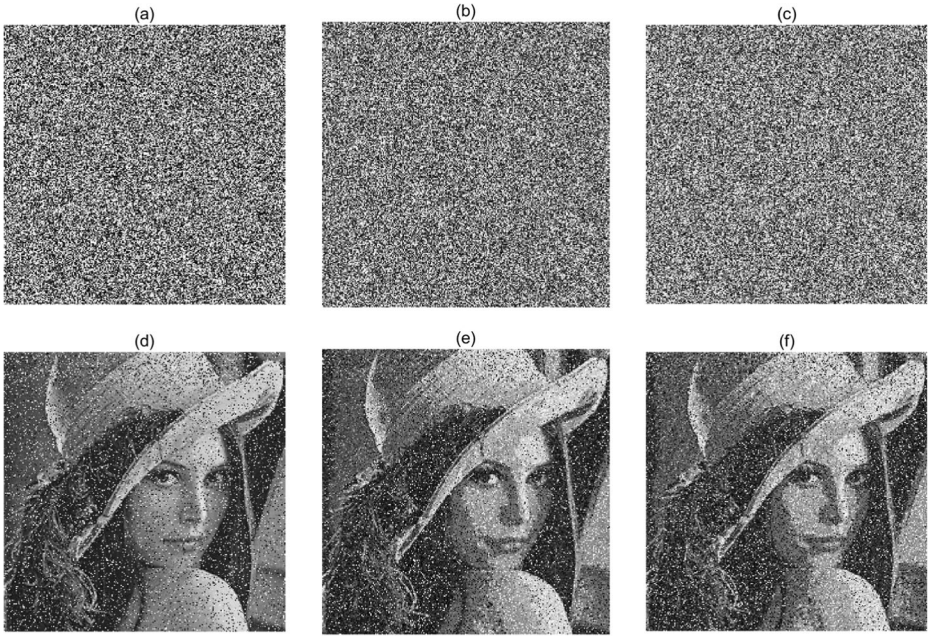

Fig. 26 Robustness against noise attacks: encrypted Lena image with (**a**) 0.2 salt and pepper noise, (**b**) 0.02 speckle noise, and (**c**) 0.02 Gaussian noise; decrypted Lena image with (**d**) 0.2 salt and pepper noise, (**e**) 0.02 speckle noise, and (**f**) 0.02 Gaussian noise

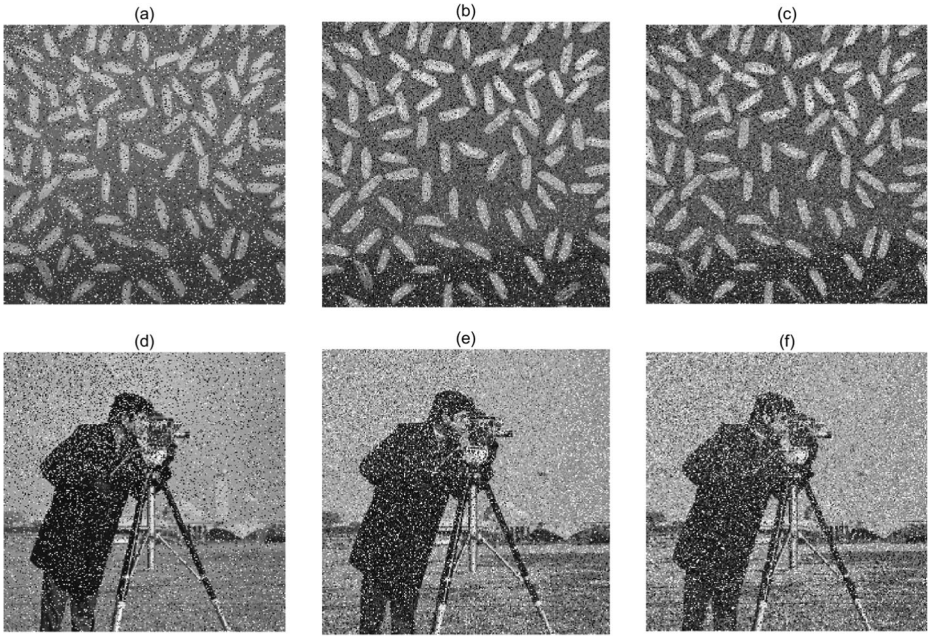

Fig. 27 Robustness against noise attacks: decrypted Rice image with (**a**) 0.2 salt and pepper noise, (**b**) 0.02 speckle noise, and (**c**) 0.02 Gaussian noise; decrypted Cameraman image with (**d**) 0.2 salt and pepper noise, (**e**) 0.02 speckle noise, and (**f**) 0.02 Gaussian noise

Table 6 Speed analysis of different algorithms

Algorithm	Speed (s)
Our method	0.10105
Ref. [18]	0.363
Ref. [6]	1.120248
DES (Ref. [20])	0.598
AES (Ref. [20])	0.113

using the selected pixels. A slight change in the key will result in different selected pixels, resulting in different special values. Then based on this selection method, a new image encryption was proposed. The p value was used to update the initial value of the encryption algorithm. What's more, the p value is applied throughout the entire encryption algorithm, which increase the correlation between plain-text image and encryption algorithm, resulting in high resistance to plain-text attacks. For the same image, determining the correct p value is difficult if the key is unknown. Consequently, cracking the encryption algorithm is challenging, which signifies that the security of the algorithm is improved. The effectiveness of the model and encryption algorithm is verified by comparing the sequences produced by the improved and original maps and testing the ciphertext image generated by the encryption algorithm. All results show that the improved model and the proposed encryption algorithm exhibit good performance in all aspects, as well as certain competitiveness compared with other algorithms, especially when the precision is low. In future, it may be considered to introduce neural network to perturb the improved model so as to greatly improve the effect of suppressing the dynamical degradation of digital chaotic map or introducing the Hopfield chaotic neural network to generate the self-diffusion chaotic matrix so as to increase the security of image encryption algorithm.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61862042); Innovation Special Fund Designated for Graduate Students of Jiangxi Province (YC2019-S101).

References

1. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography [D]. University of Buckingham
2. Adbulla AA, Sellahewa H, Jassim SA (2014) Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping [C]. Security Standardisation Research, SSR 8893:151–166
3. Anand A, Raj A, Kohli R, Bibhu V (2016) Proposed symmetric key cryptography algorithm for data security. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 159–162.
4. Bandt C, Pompe B (2002) Permutation entropy: a natural complexity measure for time series [J]. Phys Rev Lett 88(17):174102
5. Beiazi A, El-Latif AAA, Diaconu AV, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms [J]. Opt Lasers Eng 88:37–50
6. Ben Farah MA, Guesmi R, Kachouri A et al (2020) A new design of cryptosystem based on S-box and chaotic permutation [J]. Multimed Tools Appl 79(27–28):19129–19150
7. Ben ZH, Min LS, Min G, et al. (2016) Chaotic image encryption & image sharing algorithm research based on wavelet transform and CRT [C].2016 13th International Computer Conference on Wavelet Active Media

Technology and Information Processing (ICCWAMTIP), International Computer Conference on Wavelet Active Media Technology and Information Processing: 28–32
8. Bocheng L, Hongyue X, Lingfeng L (2020) Reducing the dynamical degradation of digital chaotic maps with time-delay linear feedback and parameter perturbation [J]. Math Probl Eng 2020(2):1–12
9. Chen Chen, Sun Kehui, He Shaobo. An improved image encryption algorithm with finite computing Precision [J]. Signal Process, 2019, 168, 107340.
10. ChengQing L, Lin DD, BingBing F et al (2018) Cryptanalysis of a chaotic image encryption algorithm based on information entropy [J]. IEEE Access 6:75834–75842
11. Chyun-Chau F, Wang M-C (2011) A combined input-state feedback linearization scheme and independent component analysis filter for the control of chaotic systems with significant measurement noise [J]. J Vib Control 17(2):215–221
12. Flores-Vergara A, Inzunza-Gonzalez E, Garcia-Guerrero EE et al (2019) Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors [J]. Entropy 21(3): 268
13. Guodong Y, Pan C, Xiaoling H et al (2018) An efficient pixel-level chaotic image encryption algorithm [J]. Nonlinear Dyn 94(1):745–756
14. Ismail SM, Said LA, Radwan AG, Madian AH, Abu-Elyazeed MF (2018) Generalized double-humped logistic map-based medical image encryption [J]. J Adv Res 10:85–98
15. Khlebodarova TM, Kogai VV, Fadeev SI, Likhosvai VA (2017) Chaos and hyperchaos in simple gene network with negative feedback and time delays [J]. J Bioinforma Comput Biol 15(2):1650042
16. Kohli R, Kumar M (2013) FPGA implementation of cryptographic algorithms using multi-encryption technique [J]. Computer Science
17. Lingfeng L, Suoxia M (2017) Delay-introducing method to improve the dynamical degradation of a digital chaotic map [J]. Inf Sci 396:1–13
18. Lingfeng L, Lin J, Suoxia M et al (2017) A double perturbation method for reducing dynamical degradation of the digital baker map [J]. Int J Bifurcation Chaos 27(7):14750103
19. Lingfeng L, Bocheng L, Hu H et al (2018) Reducing the dynamical degradation by bi-coupling digital chaotic maps [J]. Int J Bifurcation Chaos 28(5):1850059
20. Lingfeng L, Shidi H, Lin J et al (2018) Image block encryption algorithm based on chaotic maps [J]. IET Signal Process 12(1):22–30
21. Lv-Chen C, Luo Y-L, Sen-Hui Q, Jun-Xiu L (2015) A perturbation method to the tent map based on Lyapunov exponent and its application [J]. Chinese Physics B 24(10):100501
22. Mondal B, Mandal T (2017) A light weight secure image encryption scheme based on chaos & DNA computing [N]. J King Saud Univ – Comput Inform Sci 29(4):499–504
23. Nagaraj N, Shastry MC, Vaidya PG (2008) Increasing average period lengths by switching of robust chaos maps infinite precision [J]. European Phys J Special Topics 165:73–83
24. Nan J, Dong X, Hu H et al (2019) Quantum image encryption based on Henon mapping [J]. Int J Theor Phys 58(3):979–991
25. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata [J]. Opt Lasers Eng 90:225–237
26. Parvaz R, Zarebnia M (2018) A combination chaotic system and application in color image encryption [J]. Opt Laser Technol 101:30–41
27. Pator KAK, Acharya B, Nath V (2019) A secure multi-stage one-round bit-plane permutation operation based chaotic image encryption [J]. Microsyst Technol Micro Nanosyst -Inf Storage Process Syst 25(6): 2331–2338
28. Pincus S (1995) Approximate entropy (APEN) as a complexity measure [J]. Chaos 5(1):110–117
29. Preishuber M, Hutter T, Katzenbeisser S, Uhl A (2018) Depreciating motivation and empirical security analysis of Chaos-based image and video encryption [J]. IEEE Trans Inform Foren Secur 13(9):2137–2150
30. Souyah A, Faraoun KM (2016) Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata [J]. Nonlinear Dyn 84(2):715–732
31. Wheeler DD, Matthews RAJ (1991) Supercomputer investigations of a chaotic encryption algorithm [J]. Cryptologia 15(2):140–152
32. Wu XJ, Wang KS, Wang X, Kan H, Kurths J (2018) Color image DNA encryption using NCA map-based CML and one-time keys [J]. Signal Process 148:272–287
33. Xiaojun T, Wang Z, Miao Z et al (2015) An image encryption algorithm based on the perturbed high-dimensional chaotic map [J]. Nonlinear Dyn 80(3):1493–1508
34. Xiao-Jun T, Miao Z, Wang Z, Yang L (2014) A image encryption scheme based on dynamical perturbation and linear feedback shift register [J]. Nonlinear Dyn 78(3):2277–2291
35. Yueping L, Wang C, Hua C (2017) A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation [J]. Opt Lasers Eng 90:238–246

36. Yunqi L, Luo Y, Shuxiang S et al (2017) Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation [J]. Int J Bifurcation Chaos 27(3):1750033
37. Zenggang X, Wu Y, Conghuan Y et al (2019) Color image chaos encryption algorithm combining CRC and nine palace map [J]. Multimed Tools Appl 78(22):31035–31055
38. Zhongyun H, Yicong Z, Chi-man P et al (2015) 2D sine logistic modulation map for image encryption [J]. Inf Sci 297:80–94
39. Zhongyun H, Fan J, Xu B et al (2018) 2D logistic-sine-coupling map for image encryption [J]. Signal Process 149:148–161
40. Zhongyun H, Yicong Z, Hejiao H (2019) Cosine-transform-based chaotic system for image encryption [J]. Inf Sci 480:403–419