ORIGINAL PAPER

An efficient pixel-level chaotic image encryption algorithm

Guodong Ye · Chen Pan · Xiaoling Huang ·
Qixiang Mei

Received: 7 August 2017 / Accepted: 25 May 2018 / Published online: 5 June 2018

Abstract In this paper, a new and efficient pixel-level image encryption algorithm is presented. In contrast to the traditional permutation–diffusion architecture, the proposed method enhances the connection between position shuffling for pixels and value changing for grayness. As a result, the separate attack becomes more difficult when attacking our structure of permutation–rewriting–diffusion (PRD). Before the diffusion operation, a rewriting function is applied to the permuted image in a simple way, which can be seen as a remedy for permutation's inability to change the frequency of pixels. Moreover, the keystream is designed dependent upon the plain-image. Therefore, the proposed method can disturb the chosen plain-image and known plain-image attacks. Experimental results together with security analysis also show good efficiency of the PRD mechanism. Compared to some bit-level-based image encryption algorithms, our method shows increased faster speed and satisfies the performance requirements of real-time communication.

Keywords PRD · Pixel-level · Chaotic map · Encryption algorithm · Security

G. Ye (✉)
Faculty of Mathematics and Computer Science,
Guangdong Ocean University, Zhanjiang 524088, China
e-mail: guodongye@hotmail.com

C. Pan · X. Huang · Q. Mei · G. Ye
College of Information Science and Electronic
Engineering, Zhejiang University, Hangzhou 310027, China

1 Introduction

Digital images, as a multimedia resource, have played an important role in the modern big data era. There are many application fields for them in our daily life, for example, the fields of medicine institution, aerospace, education, electronic commerce, military affairs and so on. To share image information, we can conveniently transmit it over the open network by computer or other mobile equipment. However, unauthorized cryptanalysis is a big threat to the communication of images [1,2]. More importantly, some images concern individual privacy or national strategy, for example, ECGs (Electrocardiographs) or satellite reconnaissance. Thus, the question of how to efficiently protect the security of a communicated image has attracted a large amount of attention from experts and scholars all over the world [3–5]. It is noted that images have inherent characteristics different to those found in text [6,7] such as high redundancy, bulk data capacity, and strong correlation. Consequently, traditional ciphers such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), and IDEA (International Data Encryption Algorithm) are not suitable for efficiently encrypting images [8,9].

Recently, image encryption schemes using chaos have shown their superior performance [10–12]. This may be attributable to properties of chaotic systems such as high sensitivity to initial conditions, non-periodicity, nonlinearity, and pseudo-randomness [13–15]. As early as 1998, Fridrich [16] proposed a sym-

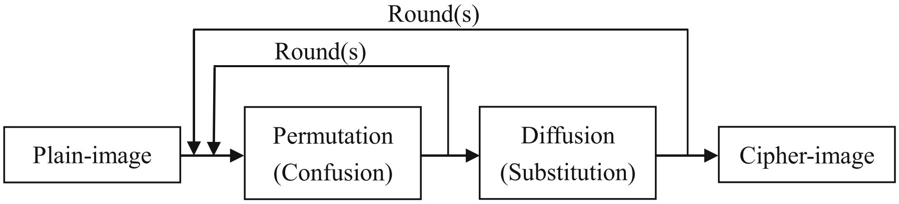


Fig. 1 Classical permutation–diffusion mechanism

metric encryption scheme for images using a two-dimensional chaotic map. Permutation–diffusion architecture was suggested to encrypt image content, where a permutation operation is performed to change the positions of pixels, while a diffusion to alter gray values. Figure 1 shows the classical permutation–diffusion mechanism, which has been widely studied and applied [17–19]. For example, a new color image encryption algorithm was proposed in [20] with a new revised one-dimensional chaotic map. Compared to the traditional one-dimensional chaotic map, the revised one-dimensional chaotic map exhibits better chaotic behavior. Firstly, the method [20] reshapes a color image of size $M \times N$ into an one-dimensional image matrix, P, with length $3MN$. It then produces a permutation position matrix, X', from chaotic sequence X to shuffle pixel positions for P and obtain a permuted image, P'. After that, a diffusion operation for P', using a diffusion matrix D' from X, is taken to achieve C. A rotating function is applied to C to get C'. Finally, the cipher-image is formed after reshaping C' into an R, G, and B color image. In [21], a new hyperchaotic system in four dimensions was designed for image encryption. First, image scrambling is applied to image blocks of size 256 × 256, in which index sequences S and T are generated from chaotic sequences to translate the row and column for each block. As for the operation of value substitution, the method changes the values based on the pseudo-random sequence $Rand$Image produced from a pseudo-random sequence generator. A new confusion scheme based on paired interpermuting planes [22] was implemented into an image encryption algorithm. It is noted that the algorithm [22] employs a ‘exchange and random access strategy’ to replace the traditional confusion operation. In the diffusion stage, the confused image is transformed into a one-dimensional array; then, a bitwise XOR operation is applied to get the cipher-image. One-time key was simulated in [23] to enhance the sensitivity, in which MD5 of the mouse-position from entropy was employed. To implement the double effects of diffusion, bit-level permutation [24] was designed in confusion stage. Being activated by deoxyribonucleic acid (DNA) coding, a new method encryption algorithm [25] has been proposed to confuse the pixels by transforming the nucleotide into its base pair for random times. By using a perceptron model within a neural network, a novel image encryption algorithm under perceptron model was suggested in [26].

There are also many other encryption algorithms [27–33] that have been proposed to protect image content. For example, a quantum realization of the generalized Arnold transform was designed for image encryption in [30]. To decrease the transmission burden, a new compression–encryption scheme was proposed [31] with the help of compressive sensing. Moreover, the fractional Mellin transform was introduced for compression–encryption scheme [32]. However, security problems still threaten the communication of digital image. Some algorithms were found to be insecure, for example, Parvin et al. [34] proposed an image encryption scheme in which a operation of two-stage permutation and one-stage substitution is adopted. After setting the secret keys, three pseudo-random keystreams are generated, i.e., K_1 for circular shift by row, K_2 for circular shift by column, and K_3 for substitution. However, the keystreams are produced with no relationship to the plain-image; thus, by chosen-plaintext attack [35], it was proven that the encryption scheme in [34] can be cracked. In [36], Brownian motion and PWLCM (piecewise linear chaotic map) are applied into image encryption algorithm. It uses Brownian motion to scramble the image; in particular, the sum of image pixels is used in the image permutation to update the initial keys u_0 and v_0 of the logistic map. PWLCM is then employed to generate the pseudo-random sequence D for the diffusion operation. However, the secret keys can be divulged by chosen-plaintext attacks [37]. As for the class of image encryption schemes based on the Chinese remainder theorem, for example [38], the equivalent secret key of CECRT (Compression–Encryption and Chinese Remainder Theorem) can be recovered easily due to properties of the CRT (Chinese Remainder Theorem) [39], and the keystream is only dependent on the secret keys. It has been proven that the attack complexity is $O(L)$ for a plaintext with length L. Moreover, most image encryption algorithms [40,41] commonly divide the encryption process into two separate processes, i.e., permutation and diffusion, and do not connect them into one entirety, so, separate attacks can also crack their algorithms [42,43]. Additionally, there are some image encryption schemes which attempt to avoid the permutation–diffusion structure, for example, one-round diffusion [44] or permutation-only [45] was employed. However, they have been pointed out to be insecure [45–47]. Some bit level based on image encryption algorithms have also been proposed, for example [48,49]. The novelty of these methods is that they can exchange bit positions and then alter simultaneously pixel values. However, they should spend more time on transforming between the decimal numbers and binary numbers.

Based on the analysis above, an efficient pixel-level-based chaotic image encryption algorithm is suggested in this paper to try to satisfy the secure communication requirements for images: (1) to solve the problems of permutation-only or diffusion-only methods, and the low security existing in Fridrich's scheme [43], a permutation–rewriting–diffusion (PRD) is designed. (2) To frustrate the known-plaintext and chosen-plaintext attacks, the keystreams used in stages of permutation and diffusion are dependent on the image. (3) To avoid the separate attack, a connection of permutation with diffusion is established to make them into a whole. It is noted that [42] in a substitution–diffusion-based chaotic image encryption algorithm, the two stages of confusion and diffusion are solely finished by substitution and the diffusion operations, respectively. Therefore, the two stages can be attacked separately [42] under this design. The rest of this paper is organized as follows. The PRD-based image encryption algorithm is introduced in Sect. 2. Then, experiments and security analysis are given in Sect. 3 in order to show the good efficiency of the proposed algorithm. Finally, some conclusions are drawn in Sect. 4.

2 PRD-based image encryption algorithm

2.1 Chaotic map

To avoid the small key space existing in one-dimensional chaotic maps, for example logistic map, two- or more-dimensional map is suggested to satisfy the requirement of the minimum key space of $2^{100} \approx 10^{30}$ [29]. In this paper, a TD-SLMM (two-dimensional sine logistic modulation map) [10] is employed to produce a chaotic sequence as pseudo-random outputs, which can be defined and seen as

$$\begin{cases} x_{i+1} = \alpha(\sin(\pi y_i) + \beta)x_i(1 - x_i), \\ y_{i+1} = \alpha(\sin(\pi x_{i+1}) + \beta)y_i(1 - y_i), \end{cases} \tag{1}$$

where $\alpha \in [0, 1]$ and $\beta \in [0, 3]$ are seen as open control parameters. The action of β is used to modulate the output and enhance the nonlinearity and randomness [10]. When β is set close to 3 with α close to 1, the TD-SLMM has hyperchaotic behavior with two positive Lyapunov exponent values. The performance of chaotic behavior for the TD-SLMM can be seen in [10]. Figure 2 shows the chaotic behavior by x-ordinary and y-ordinary. However, the degradation exists in each chaotic system (map); we can turn to the analysis method by [50] and it is out of our scope. As we know that it needs more time to solve differential equation in continual system, for example, Chen chaotic system, and Lorenz chaotic system, by mathematical method. So, we consider the chaotic map TD-SLMM in discrete case with two dimensions. Of course, for an extensive generality, the TD-SLMM can also be changed to other two-dimensional chaotic map.

2.2 The proposed algorithm

In the traditional Fridrich method, two operations are employed: permutation and diffusion. In the first place, permutation is used to exchange the position of pixels reducing the high correlation existing in two adjacent pixels. However, only the removal of pixels is carried out in this stage not changing of pixel values. That is to say, each pixel keeps the same value before and after permutation. As a result, the pixel distribution (or histogram) will also remain invariant. To enhance the security, diffusion is then employed after permutation to alter the pixel values for the permuted image. There-

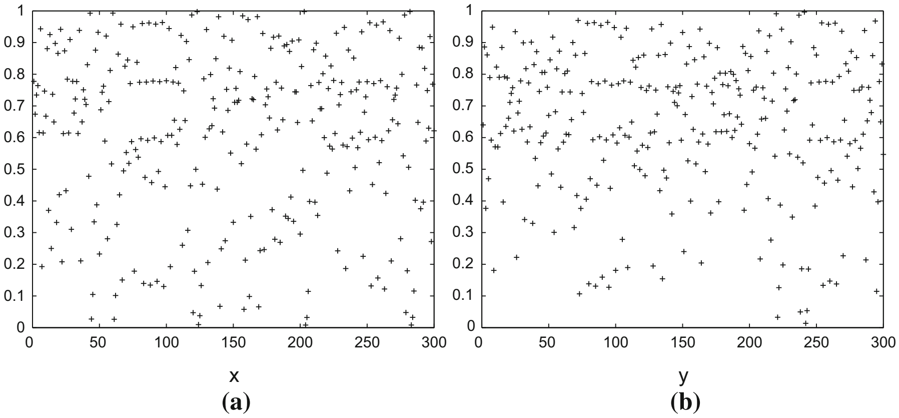


Fig. 2 Chaotic behavior: **a** x-ordinary, **b** y-ordinary

fore, the distribution of pixels will be different after diffusion compared to that of the plain-image. However, there is no connection between permutation and diffusion, so, separate attacks [42] may analyze the structure and reveal the original information. As a remedy, a new PRD-based image encryption algorithm is designed in this paper, the contributions of which are: (1) the connection of permutation and diffusion into a whole to solve the shortcomings of Fridrich's structure, and then frustrate the separate attack. (2) The use of a PRD-based algorithm to implement double diffusion effects to enhance the security of Fridrich's structure. (3) The design of a keystream dependent upon the plain-image in both permutation and diffusion operations to avoid known-plaintext and chosen-plaintext attacks.

Suppose that the plain-image of size $m \times n$ is P, and the corresponding cipher-image is C with the same size. Then, x_0 and y_0 are the initial conditions for permutation stage, while z_0 and w_0 are the initial conditions for diffusion. To ensure a high randomness, the control parameters are fixed at $\alpha = 0.9998$, $\beta = 2.9925$.

(1) Permutation-based encryption algorithm

The function of permutation is to shuffle the pixel position but not change the gray values. Let s be the statistical characteristics extracted from P, computed as

$$s = \sqrt{\sum P_{i,j}^2 + a}, \tag{2}$$

where $a \geq 1$ is a control parameter used to avoid black image attacks. We know that if the keystream is generated only from keys, with no relationship to the plain-image, then the designed algorithm will be insecure against known-plaintext and chosen-plaintext attacks. To ensure security, the keys x_0 and y_0 in the permutation stage are designed to be influenced by s as

$$\begin{cases} x_0' = x_0 + \frac{s+1}{256(mn+a)} \bmod 1, \\ y_0' = y_0 + \frac{s+2}{256(mn+a+1)} \bmod 1. \end{cases} \tag{3}$$

In this case, the keys x_0' and y_0' will be different after being updated with respect to different plain-images. Then, with the new values of x_0' and y_0' iterated into the TD-SLMM, sequence $\{x_0', y_0', x_1', y_1', \ldots\}$ is obtained after numerous rounds of iteration. To avoid the transient effect [6], the previous t iterated values should not be used, for example, t is set as 200 in this paper. That is to say, the random sequence is collected as $s = \{x_{t+1}', y_{t+1}', x_{t+2}', y_{t+2}', \ldots\}$. Suppose that the vector for row permutation is $h = \{x_{t+1}', x_{t+2}', \ldots, x_{t+m}'\}$, while $l = \{y_{t+1}', y_{t+2}', \ldots, y_{t+n}'\}$ is the vector for column permutation. Then, a circular permutation [7] for both rows and columns is carried out to obtain the permuted image R. Before permutation, vectors h and l should be processed to meet the size of the pre-encrypted image, where

$$\begin{cases} h \doteq \lceil h \times 10^{14} \rceil \bmod n, \\ l \doteq \lceil l \times 10^{14} \rceil \bmod m, \end{cases} \tag{4}$$

$\lceil x \rceil$ rounds the element x to the nearest integer toward minus infinity.

(2) Rewriting-based encryption algorithm

In the traditional Fridrich encryption scheme, only the exchange of pixel positions is considered before the diffusion operation. Moreover, there are two mutually independent stages: permutation and diffusion.

The effects of confusion and diffusion are implemented only by the permutation and diffusion operations, respectively. As a result, it has been found that the above two stages can be attacked separately [42]. To solve this problem, a rewriting operation of pixels in the permuted image is suggested between permutation and diffusion in the proposed algorithm.

Let the parameter λ equal $\lambda = \lceil (x_0 + y_0 + z_0 + w_0) \times 10^{14} \rceil \bmod 255 + 1$, which is dependent on the secret keys. The rewriting function for the permuted image is defined as

$$Q = R + \lambda E_{m \times n} \bmod 256, \tag{5}$$

where $E_{m\times n}$ represents an $m \times n$ matrix with ones as elements. Therefore, pixel distribution for Q will be different from that of R. The whole algorithm will then be blended together by parameter λ.

(3) Diffusion-based encryption algorithm

To enhance the security, the diffusion operation is required to make a histogram uniform in the cipher-image, especially a huge difference from that of the plain-image. More important, the primary objective is to achieve a tiny change in one pixel spreading over the entire image by pixel value modification. As a result, the avalanche effect can be carried out in this stage. For the keys z_0 and w_0, a preprocess for them is defined as

$$\begin{cases} z_0' = z_0 + \frac{x_0}{b} \bmod 1, \\ w_0' = w_0 + \frac{y_0}{d} \bmod 1, \end{cases} \tag{6}$$

where b and d are bigger prime numbers. Obviously, former values of x_0 and y_0 will influence the values of z_0 and w_0. Therefore, it can combine the permutation and diffusion operations into a whole. Then, by iterating the map TD-SLMM with z_0' and w_0', a random matrix M is obtained after numerous rounds of iteration. To meet the gray scale for a gray image, each element of M is processed by

$$M_{i,j} = \lceil M_{i,j} \times 10^{14} \rceil \bmod 256. \tag{7}$$

For the diffusion by rows, the operation can be seen as

$$\begin{cases} tp = \lceil (x_0 + y_0) \times 10^{14} + (\sum_{j=i+1}^{m} Q_{j,t}) \times i \rceil \bmod 256, \\ E_i = E_{i-1} + Q_i + (tp \times e_n + M_i) \bmod 256, i = 1, 2, \ldots, m, \end{cases} \tag{8}$$

where $t = \lceil (z_0 + w_0) \times 10^{14} \rceil \bmod n + 1$, e_n is a $1 \times n$ vector with ones as its elements, E_0 is a zeros vector, and $Q_{m+1,t} = 0$. Then, we obtain image E. Similarly, for the diffusion in the column direction, the operation can also be applied by exchanging $x_0 + y_0$, t and $z_0 + w_0$ in Eq. (8). However, to save the time consumption, only diffusion in the row, column or both directions be chosen randomly. Finally, the cipher-image C is achieved. Moreover, to satisfy a certain security level, more than one round of encryption is found necessary [42,51] for better performance.

2.3 Flowchart for encryption process

In this section, to clearly express the whole encryption process with a PRD structure, a flowchart is displayed in Fig. 3 with an algorithm to show the implement of our encryption method. The complexity for the whole algorithm is $O(n)$ for a message with length n, which belongs to complexity P.

Algorithm

```
Input: image $P$, keys $x_0$, $y_0$, $z_0$, $w_0$,
        control parameters $a$, $b$, $d$.
Output: image $C$.
  Set $E = zeros(m, n)$, $C = E$.
  Generate $s$ by Eq. (2).
  Do permutation operation according to $h$ and $l$.
  Do rewriting operation by Eq. (5) using λ.
  Produce $M$ using Eq. (7) after updating keys.
  Implement diffusion operation using Eq. (8) for row.
  Implement diffusion operation for column (optional).
  Obtain cipher-image $C$.
```

As for the decryption of a received cipher-image by using our PRD method, the encryption process can be done in the inverse direction due to the symmetric structure. The order for inverse is diffusion, rewriting, and permutation. Fortunately, an extra transmission is not needed in the proposed algorithm.

3 Experiments and security analysis

3.1 Experiments

To show the performance and demonstrate the efficiency of new method, simulated experiments are

Fig. 3 Flowchart

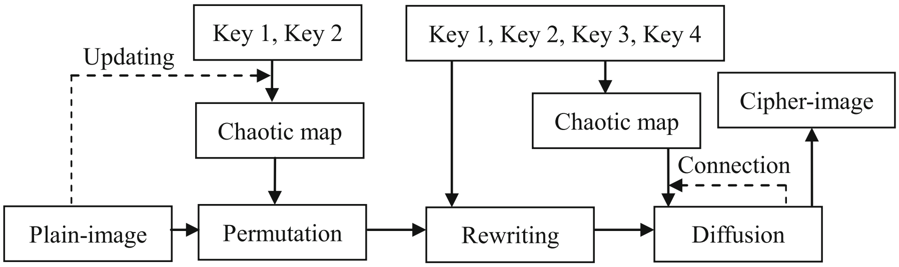
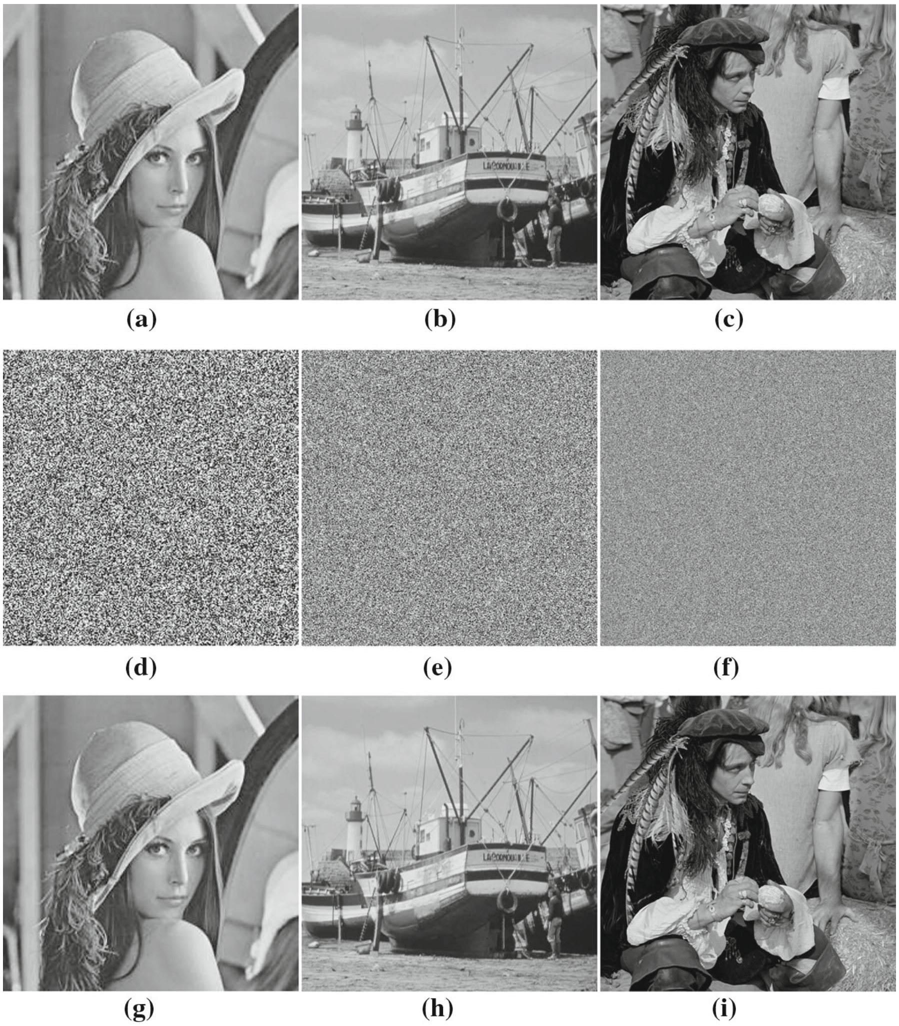


Fig. 4 Tests: Plain-images: **a** Lena, **b** boat, **c** man; Cipher-images: **d** Lena, **e** boat, **f** man; decryption results: **g** Lena, **h** boat, **i** man



undertaken in this section. The keys and parameters used in the proposed algorithm are $x_0 = 0.0056$, $y_0 = 0.3678$, $z_0 = 0.6229$, $w_0 = 0.7676$, $a = 11$, $b = 113$, and $d = 217$. To avoid the transient effect [13], previous 200 iterated values of the chaotic sequence are discarded. The test data, chosen at random, consist of a size 256 × 256 image Lena, a size 512 × 512 image of Boat, and a size 1024 × 1024 image Man. Figure 4a–c shows the plain-images of them, while Fig. 4d–f shows the corresponding cipher-images, respectively. So, no useful information can be found in the cipher-images produced by the proposed method. Using correct initial conditions, parameter values, and the keys, original images can be recovered seeing Fig. 4g–i.

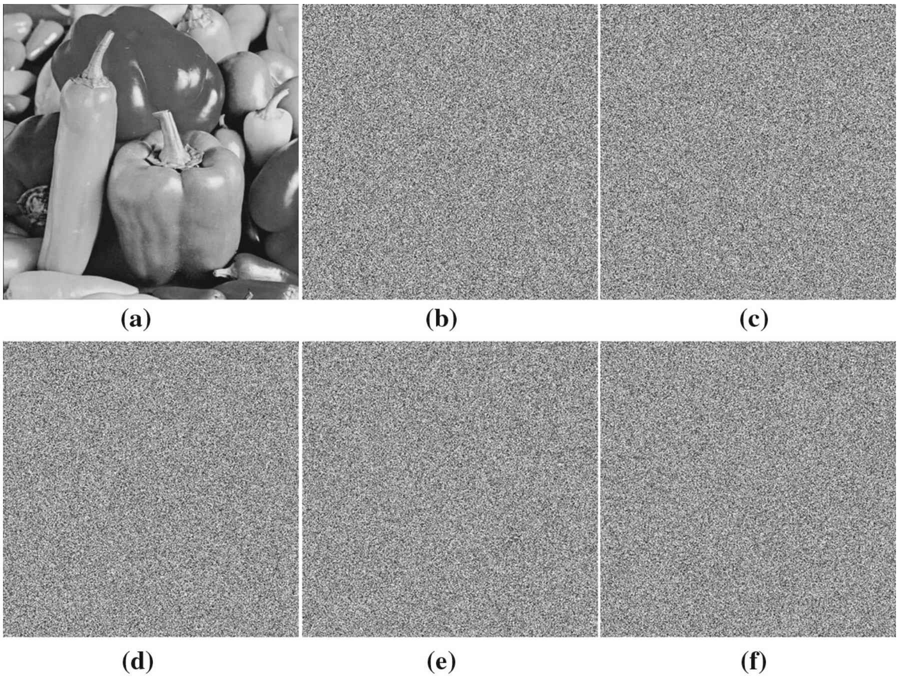


Fig. 5 Sensitivity tests: **a** plain-image, **b** cipher-image, **c** decryption with $x_0 + 10^{-14}$, **d** decryption with $y_0 + 10^{-14}$, **e** decryption with $z_0 + 10^{-14}$, **f** decryption with $w_0 + 10^{-14}$

3.2 Key space analysis and its sensitivity

A large key space is needed in a good encryption algorithm to resist brute-force attack, and the scheme should have high sensitivity to any key used. Keys are composed of x_0, y_0, z_0, and w_0, that is, the key space can reach as large as 10^{56} if the precision is set to 10^{-14}. Therefore, it is infeasible to make a brute-force attack. Moreover, to demonstrate high sensitivity, an image of Peppers, of size 512 × 512, was randomly chosen for testing. Figure 5a shows the plain-image, while Fig. 5b displays the corresponding cipher-image. But, original plain-image cannot be restored when a tiny change is made to the keys. Figure 5c–f shows incorrect decryption results by adding 10^{-14} to the keys x_0, y_0, z_0, and w_0, respectively. From them, the proposed algorithm can perform high key sensitivity.

3.3 Histogram analysis

By using our algorithm, Fig. 6a–d shows the results of histogram test for plain-images by Boat and Peppers. It is found that the cipher-images have fairly uniform distribution for gray values, significantly different from that of their respective plain-images, of which means that applying histogram attacks will be very difficult.

3.4 Chi-square analysis

For a message, Chi-square [53] analysis can also determine whether the distribution is uniform or not. The definition for Chi-square is seen as

$$\chi^2_{test} = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i}, \tag{9}$$

where $k = 256$ for a grayscale image, o_i and e_i represent the observed occurrence frequency and the expected occurrence frequency for each gray value, respectively. Table 1 gives the results for different images. All values produced by our method are smaller than the theoretical value 294, which implies that the gray distribution is in uniformity [53]. Therefore, our method passes the Chi-square test.

3.5 Know-plaintext and chosen-plaintext attacks

The encryption structure of PRD algorithm includes permutation, rewriting, and diffusion. The statistical property s, extracted from plain-image, is used to update the keys x_0 and y_0, that is, the keystream generated will be different with respect to different plain-images. In order to frustrate the separation attack and

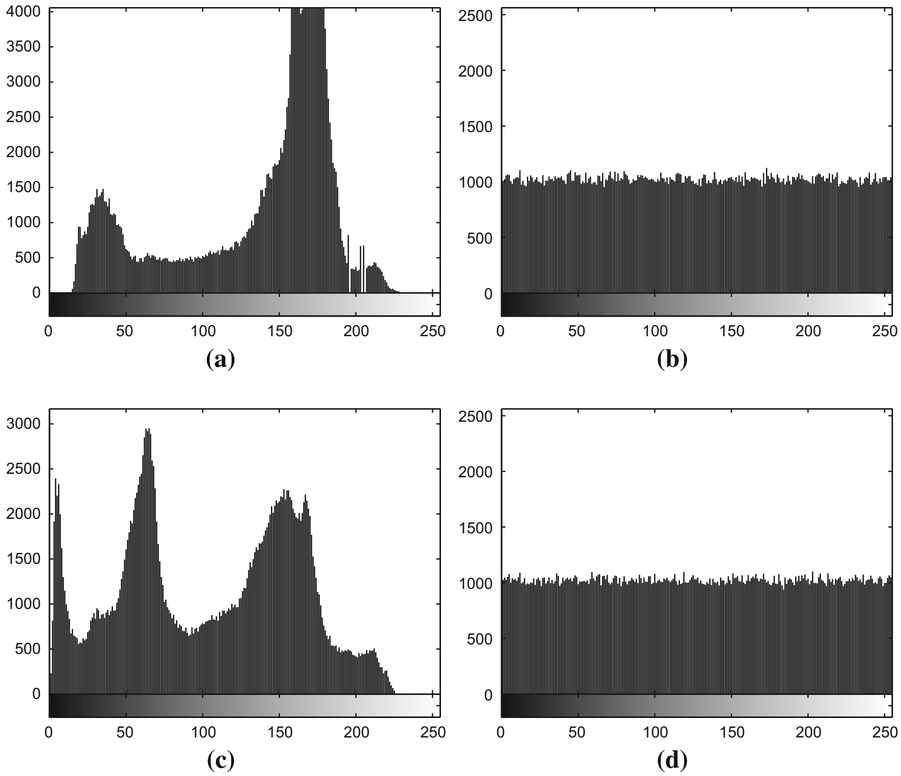


Fig. 6 Histogram tests: **a** plain-image of boat, **b** cipher-image of **a**, **c** plain-image of Peppers, **d** cipher-image of **c**

Table 1 Chi-square tests

Images	Lena	Boat	Peppers
$\chi^2_{256,0.05}$	294	294	294
χ^2_{test}	267	265	222
Pass or not	Pass	Pass	Pass

Table 2 Information entropy for different images

Images	Lena	Peppers	Boat
Plain-image	7.453238	7.571478	7.123758
Cipher-image	7.997067	7.999391	7.999273

avoid the shortcoming existing in the Fridrich structure, a simple rewriting operation is designed by connecting all the keys. Furthermore, in the diffusion stage, the function (8) is proposed to make the keystream $tp \times e_n + M_i$ dependent on the permuted image. As a result, both permutation and diffusion can enhance the security of our algorithm and resist known-plaintext and chosen-plaintext attacks.

3.6 Comparisons

(1) Information entropy

We usually employ information entropy to test the randomness for messages, which is given by

$$I(\varphi) = \sum_{i=1}^{2^{Lgh}-1} \phi(\varphi_i) \log_2 \frac{1}{\phi(\varphi_i)} \tag{10}$$

where Lgh is the length of the pixel value in form of bits, and φ denotes the test message with the probability of each φ_i written as $\phi(\varphi_i)$. After using our encryption algorithm, the results are listed in Table 2 for different images. Obviously, all values in encrypted images are approaching the theoretical value of 8. Moreover, some comparisons for different cipher-images are also given in Table 3. Therefore, the proposed encryption method demonstrates better performance.

(2) Plaintext sensitivity

To test whether a slight change in the same plain-image can produce a completely different cipher-

Table 3 Comparison of information entropy

Images	Ours	[10]	[54]	[57]
Peppers	7.999391	7.991481	7.991647	7.991587
Lena	7.997067	7.989462	7.989783	7.989442
Boat	7.999273	7.991556	7.991262	7.991436

Table 4 UACI and NPCR tests

Images	Boat	Peppers	Lena
UACI	33.398040	33.460146	33.473774
NPCR	99.603653	99.599838	99.620056

image, the UACI (unified averaged changed intensity) and NPCR (number of pixel changing rate) are used to measure the sensitivity of plain-images. They are defined by

$$\text{UACI} = \frac{1}{m \times n}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100, \tag{11}$$

$$\text{NPCR} = \frac{\sum_{ij} D(i,j)}{m \times n} \times 100\%, \tag{12}$$

where C_1 and C_2 denote the two cipher-images which have a one-bit change corresponding to same plain-image. $D(i, j) = 0$ if $C_1(i, j) = C_2(i, j)$, else, $D(i, j) = 1$. The ideal value for UACI is about 33.4635%, while the ideal value for NPCR is about 99.6094% [51,52]. Table 4 lists the results for the test images using our method. [The position is randomly chosen as (23, 15).] To demonstrate further the high sensitivity to the plaintext by using our method, two positions are changed at the same time but with the same pixel summation for the plain-image. [The positions are randomly chosen as (11, 131) and (236, 207).] Moreover, by using the proposed algorithm, other comparisons are shown in Tables 5 and 6 to prove the increased performance.

(3) Speed analysis

For real-time communication, time cost is an important factor to influence the use of an algorithm. To test the speed of our method, Table 7 shows the comparison with some references. Obviously, the proposed algorithm is an efficient way to communicate over the network.

3.7 Randomness test by TestU01

As for randomness test by TestU01, one usually applies SmallCrush, Crush, and BigCrush test batteries. Then, the test can be passed if the P-value is within the range [0.001, 0.9990]. In our process, we do the TestU01 for the randomness [58] with results (the number passed) listed in Table 8.

3.8 Chosen-plaintext attack

Commonly, attacks of ciphertext only, known plaintext, chosen plaintext and chosen ciphertext are taken to cryptanalyze a cryptosystem. Among these, if a cryptosystem can resist chosen ciphertext attack, then it can resist others [60]. In our method, the new algorithm is sensitive to both plain-image and keys. Any tiny change in them will lead to a different cipher-image. At the permutation stage, the keystream is dependent on the plain-image. Then, in diffusion stage, current row in cipher-image is related to current row in permuted image, former row in cipher-image, and remaining rows in permuted image. As a result, the proposed algorithm can resist the chosen-plaintext and ciphertext attacks [60].

Table 5 Comparison of UACI and NPCR by two bits change

	Our	[54]	Our	[54]	Our	[54]
Images	Lena	Lena	Boat	Boat	Peppers	Peppers
UACI	33.485855	0.345387	33.456980	0.325243	33.433757	0.148366
NPCR	99.604797	44.055176	99.601364	10.328674	99.601746	18.842316

Table 6 Other comparisons with [55,56]

	Our	[55]	[56]
Encryption process	PRD	PD	PPD
Keystream related to plain-image	Yes	No	No
Extra transmission	No	No	No
Plaintext sensitivity	Yes	Yes	Yes

Table 7 Speed analysis and comparison (unit: second)

Methods	Ours	[19]	[57]
256 × 256	0.059280	0.400089	0.379082
512 × 512	0.226201	1.232756	1.453929
1024 × 1024	0.836165	6.423496	5.762677

Table 8 Statistical test comparison

Battery	SmallCrush	Crush
Ours	6	56
Chebyshev map	0	5
Chen map	7	58
Ref. [59]	1	22

3.9 Discussion

As to the application of nonlinear dynamics in image encryption, some reviews were presented in [61]. According to the checklist steps [61], Table 9 gives a requirement analysis step-by-step. Therefore, one can check these checklist steps before completing an encryption algorithm based on chaos.

Table 9 Checklist requirement analysis

Checklist step	Requirement	Other notes
Checklist step 1	Satisfied	PRD structure
Checklist step 2	Satisfied	All functions in mathematical symbols
Checklist step 3	–	Encryption and decryption processes
Checklist step 4	Satisfied	Sect. 2.3
Checklist step 5	Satisfied	No extra transmission
Checklist step 6	Satisfied	Start from Sect. 3.2
Checklist step 7	Satisfied	PRD structure
Checklist step 8	Satisfied	Sect. 2.3
Checklist step 9	Satisfied	Sect. 2.3
Checklist step 10	Satisfied	Randomness produced by chaotic map
Checklist step 11	–	One can turn to designer of chaos
Checklist step 12	–	One can turn to hardware applicator

4 Conclusions

A new pixel-level image encryption algorithm using chaotic map has been proposed in this paper. The results of our analysis have shown that the cipher-image produced in our method does not leak any information contained in the plain-image. Information entropy, histogram, and Chi-square are analyzed to show uniform gray distribution. Then, both key sensitivity and plaintext sensitivity are analyzed to show the good performance of high sensitivity by using the proposed algorithm. The PRD structure has been designed as a remedy for the weakness to separation attacks found in traditional methods. Fortunately, in both stages of permutation and diffusion, keystreams are generated related to the image, allowing strong resistance against known-plaintext and chosen-plaintext attacks.

Acknowledgements The work described in this paper was supported by the National Natural Science Foundations of China (Nos. 61602124, 61702116), the Postdoctoral Science Foundation of China (No. 2017M611991), the Natural Science Foundations of Guangdong Province of China (Nos. 2016A030310333, 2015A030313614, 2015A030313620), the Science and Technology Planning Project of Guangdong Province of China (No. 2017A010101025), the Program for Scientific Research Start-up Funds of Guangdong Ocean University of China (No. R17037), the Special Funding Program for Excellent Young Scholars of Guangdong Ocean University of China (No. HDYQ2017006), and the Project of Enhancing School With Innovation of Guangdong Ocean University of China (GDOU2016050228).

References

1. Zhang, L.Y., Liu, Y.S., Pareschi, F., Zhang, Y.S., Wong, K.W., Rovatti, R., Setti, G.: On the security of a class of diffusion mechanisms for image encryption. IEEE Trans. Cybernetics **48**, 1163–1175 (2018)
2. Liu, H., Wan, H.B., Tse, C.K., Lü, J.H.: An encryption scheme based on synchronization of two-layered complex dynamical networks. IEEE Trans. Circuits-I **63**, 2010–2021 (2016)
3. Chou, H.G., Chuang, C.F., Wang, W.J., Lin, J.C.: A fuzzy-model-based chaotic synchronization and its implementa-

tion on a secure communication system. IEEE Trans. Inf. Foren. Sec. **8**, 2177–2185 (2013)

4. Bhatnagar, G., Wu, Q.M.J.: Chaos-based security solution for fingerprint data during communication and transmission. IEEE Trans. Instrum. Meas. **61**, 876–887 (2012)
5. Yang, Y.G., Tian, J., Lei, H., Zhou, Y.H., Shi, W.M.: Novel quantum image encryption using one-dimensional quantum cellular automata. Inf. Sci. **345**, 257–270 (2016)
6. Chai, X.L., Gan, Z.H., Yang, K., Chen, Y.R., Liu, X.X.: An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Process-Image **52**, 6–19 (2017)
7. Ye, G.D., Huang, X.L.: A feedback chaotic image encryption scheme based on both bit-level and pixel-level. J. Vib. Control **22**, 1171–1180 (2016)
8. Enayatifar, R., Abdullah, A.H., Isnin, I.F.: Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Laser. Eng. **56**, 83–93 (2014)
9. Wu, X.J., Kan, H.B., Kurths, J.: A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl. Soft Comput. **37**, 24–39 (2015)
10. Hua, Z.Y., Zhou, Y.C.: Image encryption using 2D logistic-adjusted-Sine map. Inf. Sci. **339**, 237–253 (2016)
11. Murillo-Escobara, M.A., Cruz-Hernándezb, C., Abundiz-Péreza, F., López-Gutiérreza, R.M., Acosta Del Campo, O.R.: A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process. **109**, 119–131 (2015)
12. Huang, X.L., Ye, G.D.: An efficient self-adaptive model for chaotic image encryption algorithm. Commun. Nonlinear SCI. **19**, 4094–4104 (2014)
13. Seyedzadeh, S.M., Norouzi, B., Mosavi, M.R., Mirzakuchaki, S.: A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dyn. **81**, 511–529 (2015)
14. Wu, Y., Hua, Z.Y., Zhou, Y.C.: n-dimensional discrete cat map generation using Laplace expansions. IEEE Trans. Cybern. **46**, 2622–2633 (2016)
15. Pareschi, F., Setti, G., Rovatti, R.: Implementation and testing of high-speed CMOS true random number generators based on chaotic systems. IEEE Trans. Circuits-I **57**, 3124–3137 (2010)
16. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcat. Chaos **8**, 1259–1284 (1998)
17. Ye, G.D., Huang, X.L.: Spatial image encryption algorithm based on chaotic map and pixel frequency. Sci. China Inf. Sci. **61**, 058104 (2018)
18. Huang, X.L., Ye, G.D.: An image encryption algorithm based on hyper-chaos and DNA sequence. Multimed. Tools Appl. **72**, 57–70 (2014)
19. Liu, H.J., Kadir, A.: Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process. **113**, 104–112 (2015)
20. Pak, C., Huang, L.L.: A new color image encryption using combination of the 1D chaotic map. Signal Process. **138**, 129–137 (2017)
21. Tong, X.J., Liu, Y., Zhang, M., Xu, H., Wang, Z.: An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps. Entropy **17**, 181–196 (2015)
22. Zhang, W., Yu, H., Zhu, Z.L.: Color image encryption based on paired interpermuting planes. Opt. Commun. **338**, 199–208 (2015)
23. Liu, H.J., Wang, X.Y.: Color image encryption based on one-time keys and robust chaotic maps. Comput. Math. Appl. **59**, 3320–3327 (2010)
24. Liu, H.J., Wang, X.Y.: Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun. **284**, 3895–3903 (2011)
25. Liu, H.J., Wang, X.Y., Kadir, A.: Image encryption using DNA complementary rule and chaotic maps. Appl. Soft Comput. **12**, 1457–1466 (2012)
26. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**, 615–621 (2010)
27. Xiao, D., Wang, L., Xiang, T., Wang, Y.: Multi-focus image fusion and robust encryption algorithm based on compressive sensing. Opt. Laser Technol. **91**, 212–225 (2017)
28. Zhang, L.Y., Wong, K.W., Zhang, Y.S., Zhou, J.T.: Bi-level protected compressive sampling. IEEE Trans. Multimedia **18**, 1720–1732 (2016)
29. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos **16**, 2129–2151 (2006)
30. Zhou, N.R., Hua, T.X., Gong, L.H., Pei, D.J., Liao, Q.H.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process. **14**, 1193–1213 (2015)
31. Zhou, N.R., Pan, S.M., Cheng, S., Zhou, Z.H.: Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt. Laser Technol. **82**, 121–133 (2016)
32. Zhou, N.R., Li, H.L., Wang, D., Pan, S.M., Zhou, Z.H.: Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt. Commun. **343**, 10–21 (2015)
33. Liu, Z.J., Guo, C., Tan, J.B., Liu, W., Wu, J.J., Wu, Q., Pan, L.Q., Liu, S.T.: Securing color image by using phase-only encoding in Fresnel domains. Opt. Lasers Eng. **68**, 87–92 (2015)
34. Parvin, Z., Seyedarabi, H., Shamsi, M.: A new secure and sensitive image encryption scheme based on new substitution with chaotic function. Multimed. Tools Appl. **75**, 10631–10648 (2016)
35. Norouzi, B., Mirzakuchaki, S.: Breaking an image encryption algorithm based on the new substitution stage with chaotic functions. Optik **127**, 5695–5701 (2016)
36. Wang, X.Y., Xu, D.H.: A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn. **75**, 345–353 (2014)
37. Zhu, C.X., Xu, S.Y., Hu, Y.P., Sun, K.H.: Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn. **79**, 1511–1518 (2015)
38. Zhy, H.G., Zhao, C., Zhang, X.D.: A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. Signal Process.-Image **28**, 670–680 (2013)
39. Li, C.Q., Liu, Y.S., Zhang, L.Y., Wong, K.W.: Cryptanalyzing a class of image encryption schemes based on Chi-

nese remainder theorem. Signal Process.-Image **29**, 914–920 (2014)

40. Diaconu, A.V.: Circular inter–intra pixels bit-level permutation and chaos-based image encryption. Inf. Sci. **355–356**, 314–327 (2016)
41. Belazi, A., Khan, M., El-Latif, A.A.A., Belghith, S.: Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption. Nonlinear Dyn. **87**, 337–361 (2017)
42. Kocarev, L., Galias, Z., Lian, S.G.: Intelligent Computing Based on Chaos, pp. 333–354. Springer, Berlin (2009)
43. Xie, E.Y., Li, C.Q., Yu, S.M., Lü, J.H.: On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process. **132**, 150–154 (2017)
44. Abanda, Y., Tiedeu, A.: Image encryption by chaos mixing. IET Image Process. **10**, 742–750 (2016)
45. Li, C.Q., Lin, D.D., Lü, J.H.: Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE MultiMedia **24**, 64–71 (2017)
46. Li, X.W., Xiao, D., Wang, Q.H.: Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. Opt. Lasers Eng. **100**, 200–207 (2018)
47. Zhang, Y.S., Xiao, D., Wen, W.Y., Li, M.: Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Nonlinear Dyn. **76**, 1645–1650 (2014)
48. Zhang, Y.Q., Wang, X.Y.: A new image encryption algorithm based on non-adjacent coupledmap lattices. Appl. Soft Comput. **26**, 10–20 (2015)
49. Zhang, Y.Q., Wang, X.Y.: A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf. Sci. **273**, 329–351 (2014)
50. Li, S.J., Chen, G.R., Mou, X.Q.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurcat. Chaos **15**, 3119 (2005)
51. Ghebleh, M., Kanso, A., Stevanovic, D.: A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation. Multimed. Tools Appl. **77**, 7305–7326 (2018)
52. Chen, J.X., Zhu, Z.L., Zhang, L.B., Zhang, Y.S., Yang, B.Q.: Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. Signal Process. **142**, 340–353 (2018)
53. Chen, J.X., Zhu, Z.L., Fu, C., Yu, H., Zhang, Y.S.: Reusing the permutation matrix dynamically for efficient image cryptographic algorithm. Signal Process. **111**, 294–307 (2015)
54. Wang, X.Y., Liu, C.M., Xu, D.H., Liu, C.X.: Image encryption scheme using chaos and simulated annealing algorithm. Nonlinear Dyn. **84**, 1417–1429 (2016)
55. Wang, X.Y., Liu, L.T., Zhang, Y.Q.: A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt. Lasers Eng. **66**, 10–18 (2015)
56. Wang, X.Y., Zhang, Y.Q., Bao, X.M.: A novel chaotic image encryption scheme using DNA sequence operations. Opt. Lasers Eng. **73**, 53–61 (2015)
57. Huang, X.L.: Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dyn. **67**, 2411–2417 (2012)
58. Liu, Y.Q., Luo, Y.L., Song, S.X., Cao, L.C., Liu, J.X., Harkin, J.: Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation. Int. J. Bifurcat. Chaos **27**, 1750033 (2017)
59. Addabbo, T., Member, S., Alioto, M., Fort, A., Pasini, A., Rocchi, S., Vignoli, V.: A class of maximum-period nonlinear congruential generators derived from the Rényi chaotic map. IEEE Trans. Circuits Syst.-I: Reg. Pap. **54**, 816–828 (2007)
60. Wang, X.Y., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. **92**, 1101–1108 (2012)
61. Özkaynak, F.: Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn. **92**, 305–313 (2018)