Chai et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:162
https://doi.org/10.1186/s13638-018-1167-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Periodic characteristics of the Josephus ring and its application in image scrambling

Zongqian Chai[1], Shili Liang[1*], Guorong Hu[2*], Ling Zhang[3], Yansheng Wu[1] and Chunlei Cao[1]

Abstract

This paper proposes a new image scrambling algorithm based on the periodic characteristics of the Josephus ring. The algorithm composes the pretreatment part of the entire image encryption system and scrambles the rows and columns of the plain image. The Josephus scrambling algorithm is adjustable by using three kinds of parameters: *step*, m_0, and *n*. Different values affect the size of the periodic value of the Josephus ring. In this paper, we focus on the method of determining the period of the Josephus cycle when the parameters are set and the Josephus rule space under arbitrary parameters. Because the Josephus ring is a mathematical problem, we analyze it using the group theory of modern algebra. After the Josephus scrambling, the plain image is encrypted. Because a CA is suitable for image encryption, the encryption part adopts a CA encryption algorithm using a one-dimensional, four-neighbor CA, which has chaotic behavior at the rules of 9d62 (hex). Finally, the number of pixels change rate, the unified averaged changed intensity test, and correlation detection are carried out on the experimental results. The results show that the use of the Josephus scrambling algorithm greatly improves the security of the entire encryption system.

Keywords: CA, Image scrambling, Josephus problem, Periodic characteristics

1 Introduction

The remarkable growth in computational power has made the use of digital images over open networks more popular than ever before. However, this widespread use and the growth of the amount of data are also a great challenge for the security design of image encryption algorithms, especially for such private images as medical images [1, 2]. Traditional encryption methods such as the Data Encryption Standard, the International Data Encryption Algorithm (DES) [3], and the Advanced Encryption Standard (AES) [4] are not suitable for image encryption; those methods including chaotic encryption method perform poorly due to their low efficiency [5]. Therefore, improving the security and efficiency of image encryption algorithms has become a key issue.

It is known that a cellular automaton (CA) can be used to encrypt images efficiently [6–11], and using an image scrambling algorithm can make the entire encryption system safer and more reliable [12–14]. In computer science and mathematics, the Josephus problem is a theoretical problem related to a certain counting-out game [15]. The scrambling algorithm becomes an important part of the entire encryption system if the particular periodic characteristics of the algorithm are based on a Josephus ring [16–18].

The proposed algorithm is a row and column scrambling method based on transformation sequences. A plain image's row and column configuration is called the original sequence, and new sequences are generated by particular times of a Josephus cycle. The following is a brief introduction to the Josephus ring and Josephus problem.

The Josephus ring is a classic problem in mathematics: A known number of individuals (designated 1, 2, 3, ..., *n*) sit around a round table. One by one, players call out numbers in increments of 1 beginning at the one whose serial number is m_0. The number *X* is the step number in the game, when someone's number is *X* they leave the table. The next player then counts from 1 again; this rule is repeated until only one player remains. The problem is to determine

* Correspondence: lsl@nenu.edu.cn; hugr@nenu.edu.cn
[1]School of Physics, Northeast Normal University, Changchun 130022, Jilin, China
[2]School of Mathematics and Statistics, Northeast Normal University, Changchun 130022, Jilin, China
Full list of author information is available at the end of the article

in advance what the serial number of the last player will be in a sequence of length n. Usually, we assign a number from 0 to $n-1$ as a solution to such a problem. For a digital image, the final column number is $f(n)+1$: it is also the original problem's solution:

$$\begin{aligned} f(1) &= 0 \\ f(n) &= [f(n-1)+step] \mod n \end{aligned} \tag{1}$$

2 Periodic characteristics of Josephus ring

2.1 Experimental methods

The Josephus problem has been solved by the recursion method, but the focus of this study is the periodic characteristics of the Josephus ring. We propose a new image scrambling algorithm with the following characteristics:

m_0 starting position	*step* interval step
n length of the original sequence	A_n original sequence

Josephus displacement: $a_{out} = f(m_0, step, A_n)$. This operation chooses an element from the original sequence as output, represented as a_{out}. In Eq. (2), A_n' is the state of the original sequence after a Josephus replacement operation and m' is the starting position for the next Josephus replacement:

$$\begin{aligned} a_{out} &= a_{m_0+(step-1)} \\ A_n' &= (a_1, a_2, \ldots a_{out-1}, a_{out+1}, \ldots a_{n-1}) \\ m' &= \text{out}+1 \end{aligned} \tag{2}$$

Josephus cycle: First, set the length of the original sequence as n. Then multiply n by the Josephus displacement in the original sequence and place each a_{out} in order. The new sequence B_n emerges:

$$B_n = (a_{out_1}, a_{out_2}, a_{out_3} \ldots a_{out_n}) \tag{3}$$

B_{n_j}: A new sequence generated by j times the Josephus cycle from the original sequence. It is commonly used in the sections of this paper that discuss the periodicity of the Josephus problem.

At first, the original sequence takes the Josephus replacement (F), and every replacement generates an element. Put each element in order until all the elements are out. This obtains a new sequence. This operation is called one Josephus cycle, denoted t. Then determine the period of the Josephus cycle when m_0 and *step* are given. Also, determine the change of t when $m_0 = 1$ and *step* = 1, 2, 3,. .. . Then, explore whether the change of t is periodic with the change of *step*. If so, call it the "period step," or the period of the Josephus rule, denoted as T. Finally, this paper discusses a scrambling algorithm based on a ring structure, for which the location of the starting point can be arbitrary. Here, for the sake of narration and argumentation, the starting point is $m_0 = 1$. When m_0 takes other values, its nature and the general rules described in the article do not change.

To facilitate the presentation, we define a new operation as a Josephus cycle, which can also be regarded as a kind of computation. Apparently, the Josephus cycle is composed of N times the Josephus displacement, so the Josephus ring in this problem contains only one regular operation: Josephus displacement f. Therefore, the problem belongs to the category of abstract algebra group theory: in group theory the analysis method is reasonable.

Meanwhile, to observe the periodic characteristics of the Josephus ring, we use natural numbers 1, 2, 3, ... to represent the original sequence; these numbers are only the element subscript number that shows the position information. They do not represent the

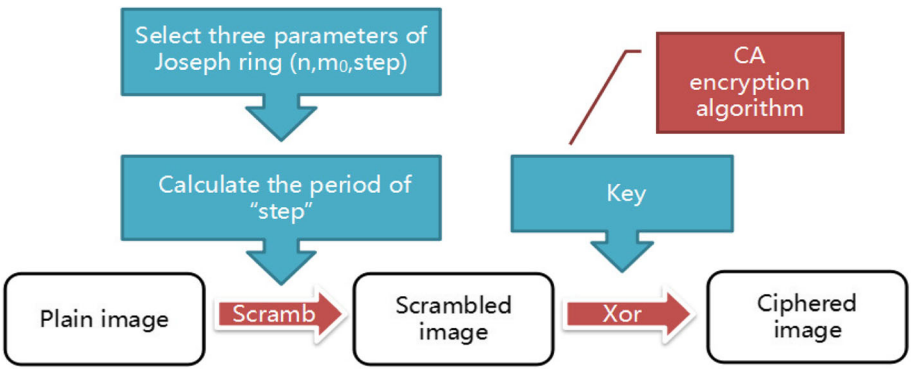

Fig. 1 Overall structure of the encryption algorithm

content of the element as do other new sequences transformed from the original sequence.

Figure 1 is a schematic diagram of the entire encryption system. As shown in the figure, the Josephus scrambling algorithm is a pretreatment element for entering the encryption algorithm system.

2.2 The period of the Josephus cycle

The period of the Josephus cycle is represented by t. To determine the period of each Josephus cycle, we need to multiply j by the Josephus cycle on the original sequence (A_n).

If the following equation is established:

$$A_n = B_{n_j} \tag{4}$$

then we have

$$t = j \tag{5}$$

The period of this Josephus cycle is the value of j.

Experiment 1: When $n = 4$, $m_0 = 1$, and $step = 2$, the Josephus cycle states are shown in Table 1.

For $A_n = B_{n_3}$, the period of the Josephus cycle is 3.

In Table 1, element 1 corresponds to element 2, element 2 corresponds to element 4, element 4 corresponds to element 1, and element 3 corresponds to itself.

So under these n, m_0, and $step$ values, n is countable: this Josephus cycle has two cycle sets,

{1,2,4} and {3}.

Experiment 2: When $n = 20$, $m_0 = 1$, and $step = 3$, each Josephus cycle state is shown in Table 2.

It can be found in Table 2 that $A_n = B_{n_{30}}$, so the period of this Josephus cycle is 30.

Table 2 shows that in the same way as experiment 1, this Josephus cycle has six cycle sets:

{1,3,9,10,14,17,8,5,15,7}, {2,6,18}, {4,12}, {19,13,11}, {20}, and {16}.

By observing many results with different n, m_0, and $step$ values, a calculation method for the Josephus cycle's period can be found. To use this method based on experiment 2 ($n = 20$, $m_0 = 1$, and $step = 3$):

Table 1 Josephus cycle states in experiment 1

New sequence generated by j times the Josephus cycle (B_{nj})	Original sequence (A_n)			
	1	2	3	4
B_{n1}	2	4	3	1
B_{n2}	4	1	3	2
B_{n3}	1	2	3	4
...	...	...	...	...
B_{nj}	...	...	...	...

{1,3,9,10,14,17,8,5,15,7}: total number of elements is 10; {2,6,18}: total number of elements is 3; {4,12}: total number of elements is 2; {19,13,11}: total number of elements is 3; {20}: total number of elements is 1; {16}: total number of elements is 1.

Record each different total number of elements in each cycle set: $A = \{10,3,2,1\}$. The minimum common multiple of the elements in the A set is calculated, that is, the period of the Josephus cycle under these parameter values.

The least common multiple of 10,3,2,1 is 30, so $t = 30$.

This period calculation method is consistent with some properties of the n-order symmetric group S_n and its r-cycles in abstract algebra [19], so this problem can be analyzed from the point of view of abstract algebra, especially the part of the symmetric group and its r-cycles.

This n degree symmetric group can be represented in r-cycles formed as 10-cycles {1,3,9,10,14,17,8,5,15,7}; 3-cycle, {2,6,18}; 2-cycle {4,12}; 3-cycle {19,13,11}; 1-cycle {20}; and 1-cycle {16}.

With the three parameters n, m_0, and $step$ determined, calculating the period of this Josephus cycle is equivalent to determining the order of one certain permutation group of this n-degree symmetric group, which is equal to the order of the product of all its disjoint r-cycles.

In experiment 2, all the r-cycles are disjoint. Obviously, each r-cycle's order equals r. Furthermore, the r-cycles of S_n have this property: the order of the product of disjoint r-cycles equals the minimum common multiple of each factor's order.

So in summary, the order of this certain permutation group equals the order of {1,3,9,10,14,17,8,5,15,7}{2,6,18}{4,12}{19,13,11}{20}{16}. Then, determining the lowest common multiple of all the factor's orders, the LCM of 10,3,2,3,1,1 is 30.

The results of this calculation coincide with the calculated results obtained by the observation, and the theorems and properties quoted in this analysis are well proved mathematically. Therefore, when the parameter values of n, m_0, and $step$ are fixed, the periodic problem of the Josephus cycle is effectively a problem of solving the order of a specific n permutation group of the certain n order symmetric group S_n.

2.3 The period of the Josephus rule

Josephus rule: For each of the original sequences, certain n, m_0, and $step$ values correspond to a certain period of the Josephus cycle. For simplicity, we use $J(n, m_0, step)$ to represent the Josephus rule. Figure 2 shows the structural levels among the Josephus displacement, the Josephus cycle, the Josephus rule, and the final scrambling algorithm.

Table 2 Each Josephus cycle state of experiment 2

j	Original sequence (A_n)																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	3	6	9	12	15	18	1	5	10	14	19	4	11	17	7	16	8	2	13	20
2	9	18	10	4	7	2	3	15	14	17	13	12	19	8	1	16	5	6	11	20
3	10	2	14	12	1	6	9	7	17	8	11	4	13	5	3	16	15	18	19	20
4	14	6	17	4	3	18	10	1	8	5	19	12	11	15	9	16	7	2	13	20
5	17	18	8	12	9	2	14	3	5	15	13	4	19	7	10	16	1	6	11	20
6	8	2	5	4	10	6	17	9	15	7	11	12	13	1	14	16	3	18	19	20
7	5	6	15	12	14	18	8	10	7	1	19	4	11	3	17	16	9	2	13	20
8	15	18	7	4	17	2	5	14	1	3	13	12	19	9	8	16	10	6	11	20
9	7	2	1	12	8	6	15	17	3	9	11	4	13	10	5	16	14	18	19	20
10	1	6	3	4	5	18	7	8	9	10	19	12	11	14	15	16	17	2	13	20
30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

2.3.1 Periodic analysis of the step parameter

We find that a change in *step* changes the Josephus cycle. Does this change also show periodicity? That is to say, whether there is a T to make Eq. (6):

$$J(n, m_0, step) = J(n, m_0, step + T) \tag{6}$$

To analyze the effect of the *step* value in the Josephus rule, keep parameter settings like m_0 unchanged (the value of m_0 can be any positive integer); for example, $m_0 = 1$, $step = 1, 2, 3,...$, and then observe changes in the Josephus cycle and the Josephus rule. We may pay more attention to the Josephus rule's periodic characteristics caused by *step*'s change.

After the parameters n, m_0, and *step* are determined, according Eq. (2), the subscripts of a_{out} (the value of *out*) are determined after it. Also, the launch of the new series B_{n_1} to B_{n_j} is determined, so we use B_{n_1} obtained by one Josephus cycle to represent all the states of that Josephus cycle. Because for B_{n_1} to B_{n_j}, they all correspond to the same Josephus rule.

Experiment 3: $m_0 = 1$, $n = 4$, and the original sequence is $A_n = (1, 2, 3, 4)$:

As the value of *step* increases from 1, B_{n_1} changes with it. According to Table 3, a different B_{n_1} means a different Josephus rule. Record the value of *step* when $J(n, m_0, step)$ is consistent with $J(n, m_0, 1)$, and then we obtain $T = step - 1$ (T is the period of *step*).

In experiment 3, when $step = 13$, B_{n_1} returns to the original state, as the first line shows ($step = 1$). That means the value of *step* has gone through a cycle, and it is easy to see that the period of *step*'s cycle is 12:

$$\begin{aligned} &J(n, m_0, 13) = J(n, m_0, 1) \\ &T = 12 \end{aligned} \tag{7}$$

Experiment 4: $m_0 = 1$, $n = 7$, and the original sequence is $A_n = (1, 2, 3, 4, 5, 6, 7)$ (Table 4).

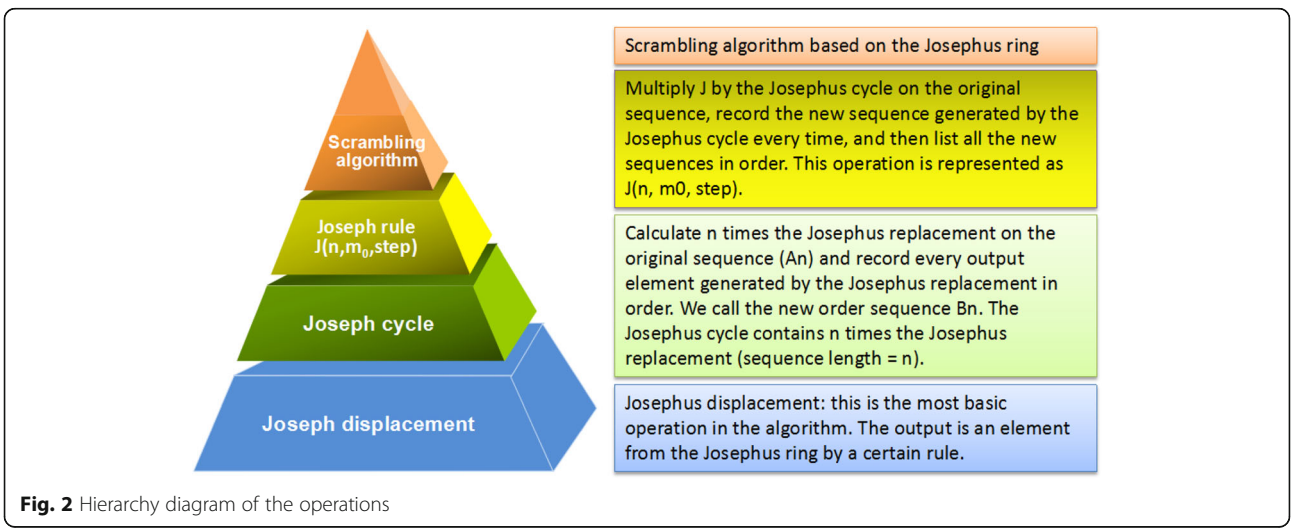

Fig. 2 Hierarchy diagram of the operations

Table 3 Josephus cycle state of each *step* value in experiment 3

Value of *step*	New sequence B_{n_1} generated after one Josephus cycle (t) from original sequence A_n				Period of Josephus cycle (t)
1	1	2	3	4	1
2	2	4	3	1	3
3	3	2	4	1	3
4	4	1	3	2	3
5	1	3	4	2	3
6	2	1	4	3	2
7	3	4	1	2	2
8	4	2	1	3	3
9	1	4	2	3	3
10	2	3	1	4	3
11	3	1	2	4	3
12	4	3	2	1	2
13	1	2	3	4	1
...	...	...	...	...	...

Experiments 3 and 4 show a change in the *step* value, which leads to a periodic change of B_{n_1}, representing the $J(n, m_0, step)$:

$$J(n, m_0, step) = J(n, m_0, step + T) \tag{8}$$

When we explore the general method of computing the value of T, we notice that there is some relation between that value and the sequence length n. Therefore, we set up a sequence of length N, redefine its *step*'s cycle T as T_n, and then do the following analysis:

The $T_4 = 12$ of experiment 3 and the $T_7 = 420$ of experiment 4 are solved by the programming method of cyclic traversal. The periods of the *step*'s cycle T_1 to approximately T_{11} and of $n = 1$ to approximately $n = 11$'s sequence are solved by the same method. The results are as follows:

$$\begin{aligned}
&n = 1 \quad 1! = 1 \quad T_1 = 1\\
&n = 2 \quad 2! = 2 \times 1 \quad T_2 = 2\\
&n = 3 \quad 3! = 3 \times 2 \times 1 \quad T_3 = 6\\
&n = 4 \quad 4! = 4 \times 3 \times 2 \times 1 \quad T_4 = 12\\
&n = 5 \quad 5! = 5 \times 4 \times 3 \times 2 \times 1 \quad T_5 = 60\\
&n = 6 \quad 6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_6 = 60\\
&n = 7 \quad 7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_7 = 420\\
&n = 8 \quad 8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_8 = 840\\
&n = 9 \quad 9! = 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_9 = 2520\\
&n = 10 \quad 10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_{10} = 2520\\
&n = 11 \quad 11! = 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \quad T_{11} = 27720
\end{aligned} \tag{9}$$

Table 4 Josephus cycle state of each *step* value in experiment 4

Value of *step*	New sequence B_{n_1} generated after one Josephus cycle (t) from the original sequence A_n							Period of Josephus cycle (t)
1	1	2	3	4	5	6	7	1
2	2	4	6	1	5	3	7	6
3	3	6	2	7	5	1	4	4
4	4	1	6	5	7	3	2	10
...	...	...	...	...	...	...	...	...
421	1	2	3	4	5	6	7	1

First, express each N's factorial in the form of $n! = n \times (n-1)!$ $(n \geq 1)$, and then change the form of every N from an integer to the product of several certain prime factors. The results are:

$$\begin{aligned}
&n = 1 \quad 1! = 1 \quad T_1 = 1\\
&n = 2 \quad 2! = 2 \times 1! \quad T_2 = 2\\
&n = 3 \quad 3! = 3 \times 2! \quad T_3 = 6\\
&n = 4 \quad 4! = 2^2 \times 3! \quad T_4 = 12\\
&n = 5 \quad 5! = 5 \times 4! \quad T_5 = 60\\
&n = 6 \quad 6! = 3 \times 2 \times 5! \quad T_6 = 60\\
&n = 7 \quad 7! = 7 \times 6! \quad T_7 = 420\\
&n = 8 \quad 8! = 2^3 \times 7! \quad T_8 = 840\\
&n = 9 \quad 9! = 3^2 \times 8! \quad T_9 = 2520\\
&n = 10 \quad 10! = 5 \times 2 \times 9! \quad T_{10} = 2520\\
&n = 11 \quad 11! = 11 \times 10! \quad T_{11} = 27720
\end{aligned} \tag{10}$$

Now observe the relation between T_n and T_{n-1}:

$$\begin{aligned}
&T_1 = 1 \qquad\qquad T_7 = T_6 \times 7\\
&T_2 = T_1 \times 2 \qquad T_8 = T_7 \times 2\\
&T_3 = T_2 \times 3 \qquad T_9 = T_8 \times 3\\
&T_4 = T_3 \times 2 \qquad T_{10} = T_9 \times 1\\
&T_5 = T_4 \times 5 \qquad T_{11} = T_{10} \times 11\\
&T_6 = T_5 \times 1
\end{aligned} \tag{11}$$

As shown in Eq. (6), n is the sequence length. First, we do the prime factor decomposition for n and obtain the

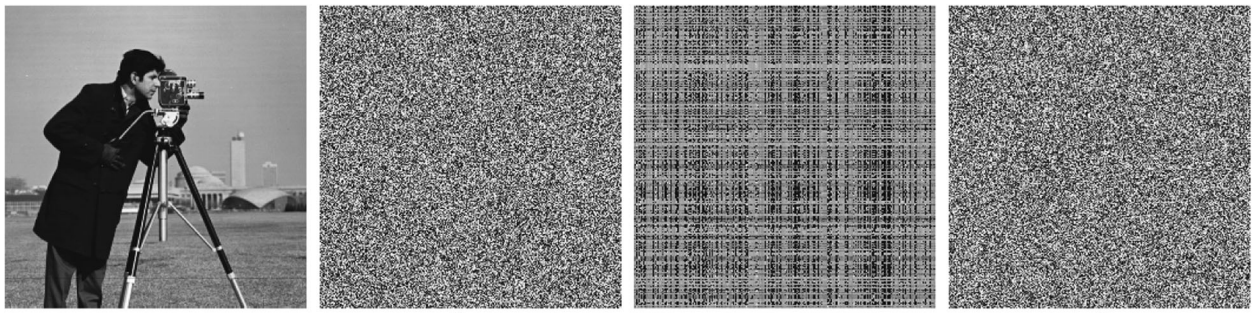

Fig. 3 **a** Plain image (cameraman). **b** Directly CA-encrypted image (cameraman). **c** Scrambled image (cameraman). **d** The cipher image after scrambling the plain image (cameraman)

prime factors x_i, keeping $x_i \le n$. In the equation, p is the number of different qualitative factors and a_i is the exponent of x_i:

$$n = \prod_{i=1}^{p} x_i^{a_i} \tag{12}$$

The following inference is made from the above experimental data:

When $p = 1$, that is to say, n can be represented only as the power of a certain prime number, there are

$$T_n = x_i T_{n-1} \tag{13}$$

When $p > 1$, that is, n can be expressed as the product of the power of several prime factors, there are

$$T_n = T_{n-1} \tag{14}$$

2.3.2 Formula generalization of step's period

In Section 3.1, we researched the period of *step* (T_n), and T_n was found to have a direct relation with the sequence's length. *Step* and m_0 are two parallel parameters of the Josephus cycle, so it could be asked whether T_n is also the period of m_0, or whether T_n is related only to the sequence's length.

It has been found that, for a sequence of length N, *step*'s periodic characteristic is also suitable for m_0. The research method is the same as what Section 3.1 shows. The difference is only that keeping the value of *step* unchanged, we increase m_0 from 1 to n.

Therefore, we get

$$J(n, m_0, step) = J(n, m_0 + T_n, step) \tag{15}$$

With the conclusion of Section 3.1, we can get the following relation:

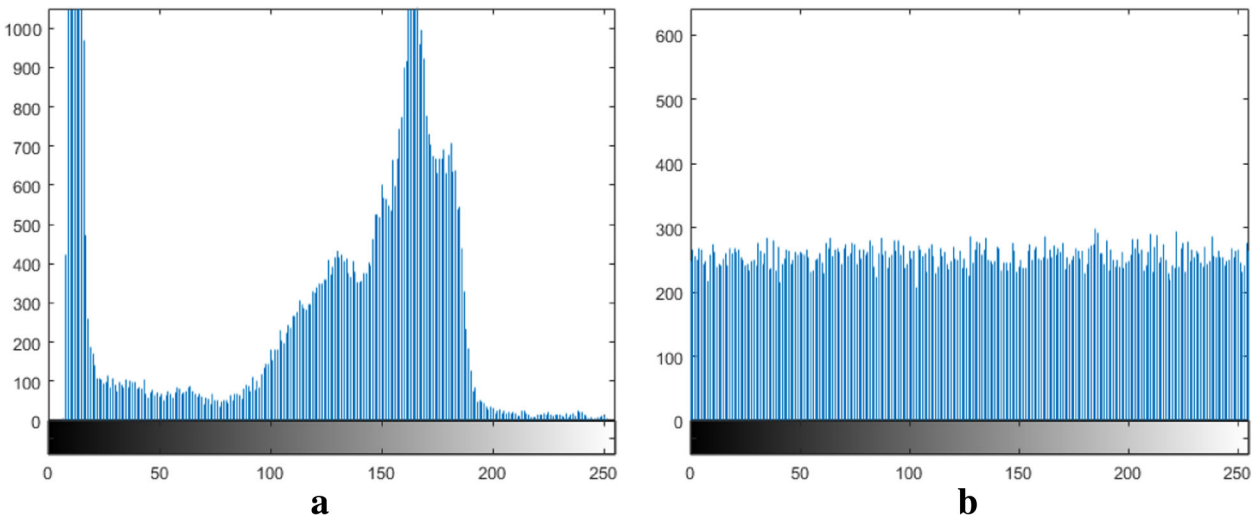

Fig. 4 **a** Gray histograms of Lena. **b** Gray histograms of cipher Lena image

Fig. 5 **a** Cameraman. **b** Lena. **c** Couple. **d** Boats. **e** Baboon. **f** Town. **g** Barb. **h** Peppers

$$J(n, m_0, step) = J(n, m_0 + T_n, step + T_n) \tag{16}$$

In conclusion, T_n is the period of both *step* and m_0, and it is related only to the sequence's length. Therefore, we propose that T_n is the period of the Josephus rule.

Table 5 NPCR and UACI *p* values

Item Test image	NPCR(%)	UACI (%)	p-value	Size
Cameraman	99.5620	31.1169	0.0261	256 × 256 × 1
Scrambled cameraman	99.6185	31.1317	0.0127	256 × 256 × 1
Lena	99.5788	33.8519	0.0452	256 × 256 × 1
Scrambled Lena	99.6093	34.0460	0.0440	256 × 256 × 1
Couple	99.6078	32.8495	0.0750	256 × 256 × 1
Scrambled couple	99.6643	33.0188	0.0279	256 × 256 × 1
Boat	99.5937	29.3294	0.0466	512 × 512 × 1
Scrambled boat	99.6154	29.3675	0.0218	512 × 512 × 1
Baboon	99.6063	27.7792	0.1011	512 × 512 × 1
Scrambled baboon	99.6234	27.8718	0.0366	512 × 512 × 1
Town	99.6055	29.1728	0.0770	512 × 512 × 1
Scrambled town	99.6174	29.2275	0.0478	512 × 512 × 1
Barbara	99.6189	28.8729	0.0832	512 × 512 × 1
Scrambled barbara	99.6310	28.8842	0.0470	512 × 512 × 1
Peppers	99.6143	30.9129	0.0658	512 × 512 × 1
Scrambled peppers	99.6325	30.9247	0.0412	512 × 512 × 1

2.3.3 Space of the Josephus rule

A different $J(n, m_0, step)$ means a different Josephus cycle: each Josephus cycle corresponds to a certain different Josephus rule. Now we discuss the question of how many different rules exist; the scrambling algorithm should have a very large space of rules. Because T_n is the period of both *step* and m_0 according to Section 3.2, we can easily find that the *space* of the Josephus rule is the square of T_n. So we get

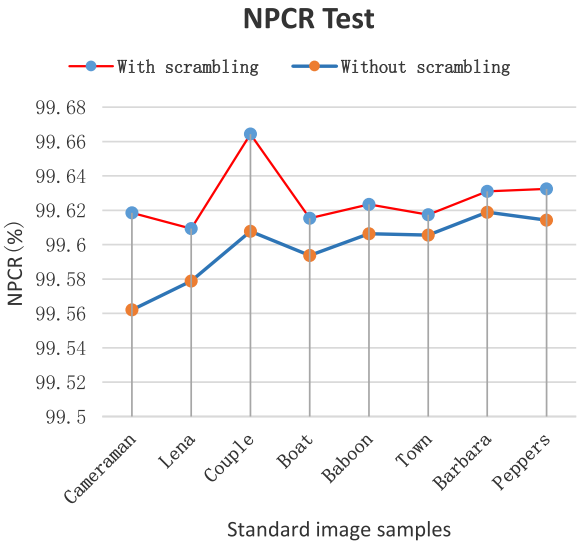

Fig. 6 NPCR test

Table 6 Confidence intervals

Samples	Mean of NPCR(%)	σ	*n*	CI
Scrambled images	99.6265	0.0172	8	[0.996265 ± 0.011918]

$$space = T_n^2 \tag{17}$$

3 Results and discussion

3.1 Number of pixels change rate and unified averaged changed intensity tests

Number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI) are two important parameters for judging the strength of an encryption algorithm [20]. The values of NPCR and UACI are computed using the following equations:

$$NPCR = \left(\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} D[i,j]\right) \times 100\% \tag{18}$$

$$UACI = \left(\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} \frac{|C_1[i,j] - C_2[i,j]|}{255}\right) \times 100\% \tag{19}$$

where N and M denote the image's width and height respectively. $C_1[i,j]$ is the obtained cipher image from the original plain image, whereas $C_2[i,j]$ is obtained after one bit of the plain image is modified. For each (i,j) position, if $C_1[i,j] = C_2[i,j]$, then $D[i,j] = 0$, else $D[i,j] = 1$.

We incorporated the Josephus scrambling algorithm into the encryption algorithm system, and then tested the Josephus scrambling algorithm's ability to enhance the effect of the partial X cell automaton encryption algorithm. We used the 256×256 cameraman as an example. In Fig. 3, the pictures from left to right are the plain image, the direct CA-encrypted image, the scrambled image, and the cipher image after scrambling. Figure 4 are gray histograms of above images. As we can see from Fig. 4, the cipher image's pixel distribution is more uniform than plain image, which proves this encryption system can protect the information of plain image.

Table 7 Correlation detection results for the cameraman picture

Correlation Samples	Vertical	Horizontal	Diagonal
Plain image	0.9565	0.9334	0.9564
Scrambled image	0.2663	0.1844	0.2720
Directly CA-encrypted images	-8.9832×10^{-4}	−0.0055	0.0036
Scrambled and encrypted images	2.4281×10^{-4}	0.0027	0.0031

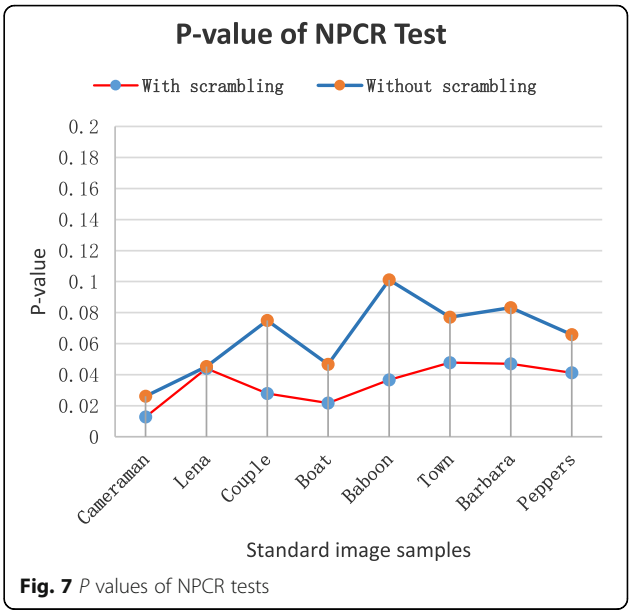

Fig. 7 *P* values of NPCR tests

To analyze the security of the entire encryption algorithm intuitively [21–25], we took 1×10^4 pixel points of each experimental image as samples. Next, we should demonstrate that using the scrambling algorithm can improve the security of the entire encryption algorithm.

Figure 5 shows several standard images used as experimental materials. To prove the hypothesis above, we did NPCR and UACI tests on pairs of plain images, comparing each encrypted image before scrambling, with the same encrypted image after scrambling. We called them the sample image pairs.

At the same time, we used the hypothesis testing method to calculate the p value of the NPCR test results. If the proposed algorithm was able to encrypt images that were indistinguishable from random images under the

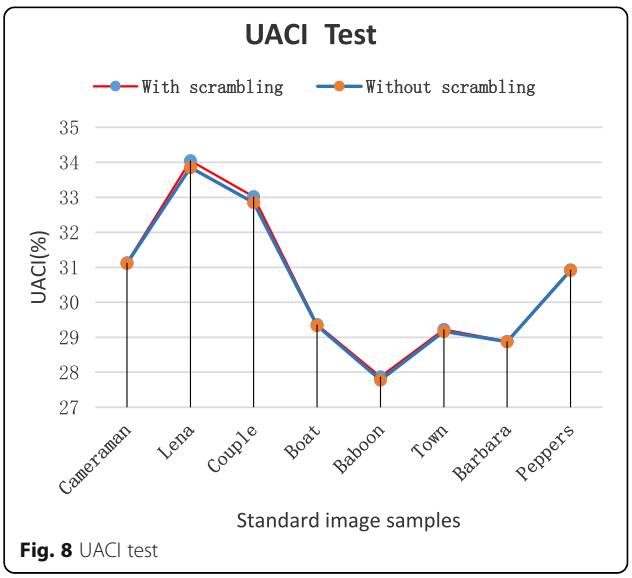

Fig. 8 UACI test

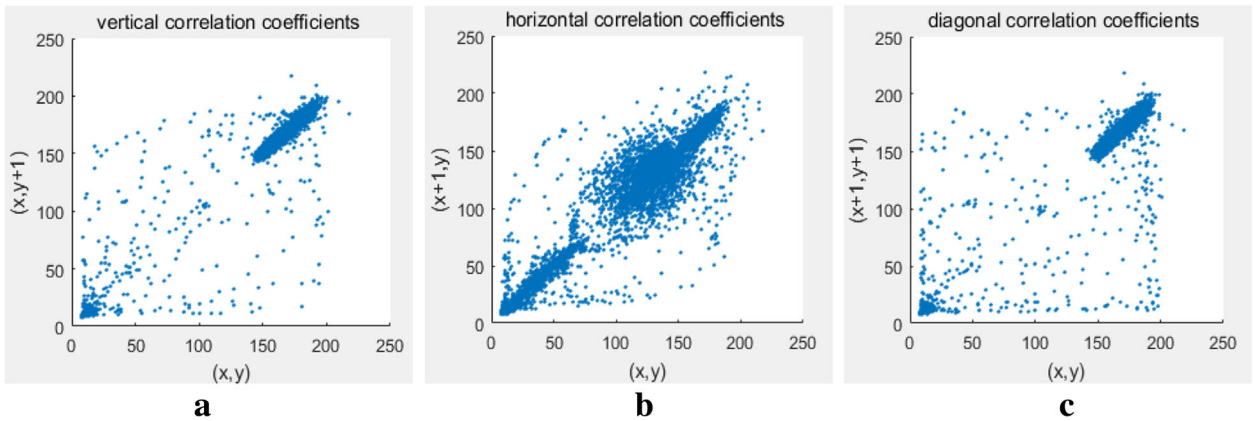

Fig. 9 **a** Vertical correlations of original images. **b** Horizontal correlations of original images. **c** Diagonal correlations of original images

NPCR and UACI measures, the p values simply represented the possibility that our tested images were indeed random-like. Take the significance level $\alpha = 0.05$, and then judge the randomness and credibility of the sample image pairs according to the sizes of the p value and α. When the p value is less than α, the sample image pair is strongly random-like, but when the p value is greater than or equal to α, the sample image pair has low randomness. Figure 6 shows the p value test results. Table 5 shows NPCR, UACI, and p value testing results of standard images. As shown in Fig. 7, in this encryption system, the NPCR value of the scrambled images is generally higher than that of the nonscrambled images. UACI results for both of the two series are similar: as Fig. 8 shows, the red line is just slightly higher than the blue line. It is a normal test result.

3.2 Confidence intervals

Due to the normal distribution of the cipher image samples, we get $X \sim N(\mu,\sigma^2)$, X is the average value of NPCR, under significance level $\alpha = 0.05$, and confidence degree is $1-\alpha = 0.95$.

Confidence intervals:

$$\left[\overline{X} \pm \frac{\sigma}{\sqrt{n}} \times Z_{\frac{\alpha}{2}}\right] \tag{20}$$

Look-up the normal distribution table with the confidence degree of 0.95, we get:

$$Z_{\frac{\alpha}{2}} = 1.96 \tag{21}$$

So confidence intervals is [0.984347,1.008183]. Details are displayed in the (Table 6).

3.3 Correlation detection

Correlation detection is a conventional detection method for encrypted images [26, 27]. It is also used to evaluate the performance of encryption or scrambling algorithms. Table 7 shows the details, and Figs. 9, 10, and 11 show the correlation detection results of the cameraman picture.

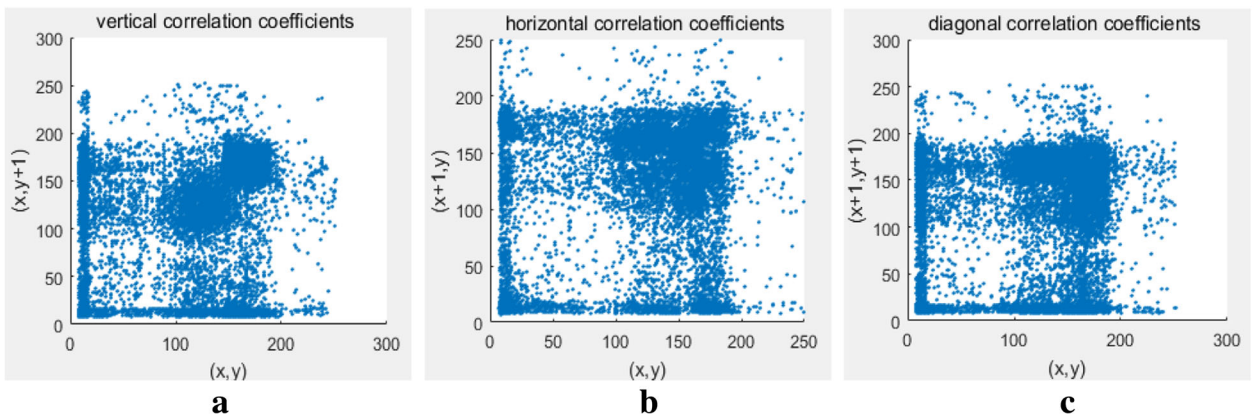

Fig. 10 **a** Vertical correlations of scrambled images. **b** Horizontal correlations of scrambled images. **c** Diagonal correlations of scrambled images

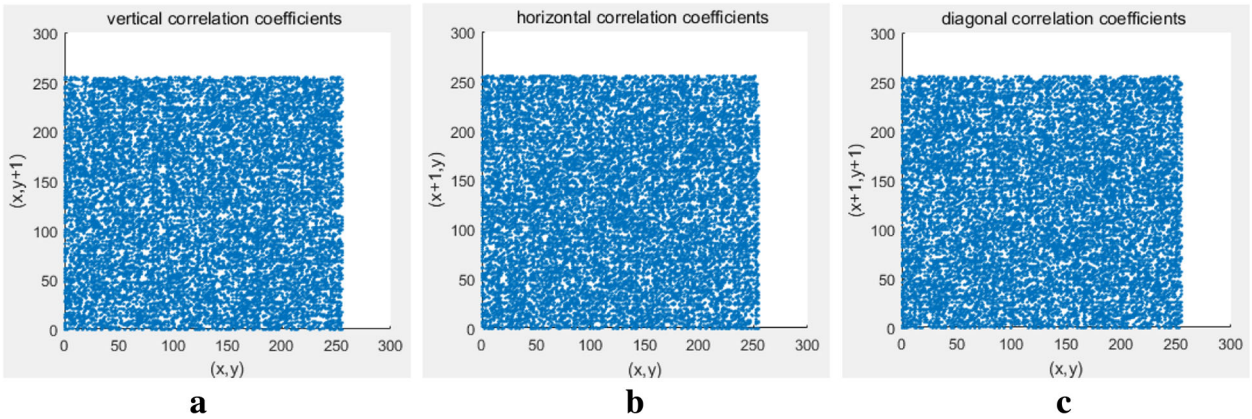

Fig. 11 **a** Vertical correlations of scrambled and encrypted images. **b** Horizontal correlations of scrambled and encrypted images. **c** Diagonal correlations of scrambled and encrypted images

4 Conclusions

In this study, starting from the classic Josephus problem we used the Josephus loop algorithm to generate scrambled sequences from the original sequences. These new sequences were then applied to the image scrambling of columns and rows. The scrambling operation is the preprocessing part of the entire encryption system, which has a great influence on the security of the encryption algorithm. Then we focused on the period of the Josephus cycle (t) and the period of the Josephus rule (T_n), both of which are the core of the Josephus scrambling algorithm and guarantee the reversibility and rule space complexity of that algorithm. Different selections of m_0 and *step* also have a direct impact. To obtain a general conclusion, we encrypted experimental group images with the Josephus scrambling treatment and a control group of images without it. Both image groups used the cameraman, Lena, and other standard images. Then we did NPCR and UACI tests and correlation detection for two sets of samples. The experimental data show that compared with the control group, the images encrypted with Josephus scrambling had better randomness and higher NPCR values; the lower p value also shows the reliability of the experimental results. Therefore, we found that the Josephus scrambling algorithm can improve the randomness of image enciphering and the reliability of an encryption system.

Abbreviations

AES: Advanced Encryption Standard; CA: Cellular automaton; CI: Confidence intervals; DES: Data Encryption Algorithm; LCM: Least common multiple; NPCR: Number of pixels change rate; UACI: Unified averaged changed intensity

Acknowledgements

Northeast Normal University and Changchun University of Science and Technology offer the experiment platform.

Funding

This work is supported by the following funding: Jilin Provincial Development and Reform Commission under Grant 2017c033–1 as well as the National defense research frontier exploration project of The Northeast Normal University.

Authors' contributions

ZQC conceived and designed the experiments and wrote this paper. SLL and LZ helped to perform the analysis with constructive discussions. GRH provides mathematical and statistical guidance for this paper. YSW and CLC contributed to the structuring and reviewing of the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]School of Physics, Northeast Normal University, Changchun 130022, Jilin, China. [2]School of Mathematics and Statistics, Northeast Normal University, Changchun 130022, Jilin, China. [3]College of Science, Changchun University of Science and Technology, Changchun 130022, China.

Received: 5 April 2018 Accepted: 30 May 2018
Published online: 25 June 2018

References

1. Z Hua, S Yi, Y Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **144**, 134–144 (2018).
2. A Kanso, M Ghebleh, An efficient and robust image encryption scheme for medical applications. Commun. Nonlinear Sci. Numer. Simul. **24**(1), 98–116 (2015).
3. Data encryption standard, National Bureau of Standards. Gaithersburg: Information Technology Laboratory, National Institute of Standards and Technology; 1999.
4. FIPS PUB 197: Avanced encryption standard, Announcing the Advanced Encryption Standard (AES). Gaithersburg: Information Technology Laboratory, National Institute of Standards and Technology; 2001.
5. M Yang, N Bourbakis, S Li, Data-image-video encryption. IEEE Potentials **23**(3), 28–34 (2004).
6. J Jun, in *Southeaston, 2009*. Image encryption method based on elementary cellular automata, vol 50 (IEEE, Southeastcon, 2009), pp. 345–349.
7. AA Abdo, S Lian, IA Ismail, M Amin, H Diab, A cryptosystem based on elementary cellular automata. Commun. Nonlinear Sci. Numer Simul. **18**, 136–147 (2013).

8. T Chen, M Zhang, W J, C Yuen, Y Tong, Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling. Opt. Laser Technol. **84**, 118–133 (2016).
9. Y Zhou, W Cao, CL Philip Chen, Image encryption using binary bitplane. Signal Process. **100**, 197–207 (2014).
10. A Bakhshandeh, Z Eslami, An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt. Lasers Eng. **51**, 665–673 (2013).
11. L Shi-li, C Zong-qian, Image encryption method based on partial X type cellular automaton. J. Jilin Univ. (Eng. Technol. Ed.) **47**, 1653–1660 (2017).
12. X Desheng, X Yueshan, Digital image scrambling based on Josephus traversing. Comput. Eng. Appl **10**, 44–46 (2005).
13. S Liu, C Guo, JT Sheridan, A review of optical image encryption techniques. Opt. Laser Technol. **57**, 327–342 (2014).
14. G Ye, Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recogn. Lett. **31**, 347–354 (2010).
15. P Van-Roy, S Haridi, *Concepts, techniques, and models of computer programming* (MIT Press, Cambridge, 2004).
16. G Yang, H Jin, N Bai, Image encryption using the chaotic Josephus matrix. Math. Probl. Eng. **2014**, 1–13 (2014) Article ID 632060.
17. X Wang, X Zhu, Y Zhang, An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access **99**, 1 (2018). https://doi.org/10.1109/ACCESS.2018.2805847.
18. B Xu, Z Hua, H Huang, in *International Symposium on Cyberspace Safety and Security*. A novel image encryption scheme using Josephus permutation and image filtering (Cyberspace Safety and Security, Xi'an, 2017), pp. 307–319. https://doi.org/10.1007/978-3-319-69471-9_23.
19. JJ Rotman, *Advanced modern algebra*, 2nd edn. (American Mathematical Society, Providence, 2010).
20. Y Wu. NPCR and UACI Randomness Tests for Image Encryption. Cyber J. J. Selected Areas Telecommun. (2011).
21. P Refregier, B Javidi, Optical image encryption based on input plane and Fourier plane random encoding. Opt. Let. **20**(7), 767-769 (1995).
22. Q Zhang, L Guo, X Wei, Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. **52**, 2028–2035 (2010).
23. Y Zhou, L Bao, CP Chen, A new 1D chaotic system for image encryption. Signal Process. **97**, 172–182 (2014).
24. S Amina, FK Mohamed, An efficient and secure chaotic cipher algorithm for image content preservation. Commun. Nonlinear Sci. Numer. Simul. **60**, 12–32 (2018).
25. MG Kechaidou, GC Sirakoulis, Game of life variations for image scrambling. J. Comput. Sci. **21**, 432–447 (2017).
26. H Liu, X Wang, Color image encryption based on one-time keys and robust chaotic maps. Comput. Math. Appl. **59**, 3320–3327 (2010).
27. L Xu, X Gou, Z Li, et al., A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt. Lasers Eng. **91**, 41–52 (2017).