A new perturbation method to the Tent map and its application*

Wang Xing-Yuan(王兴元)† and Wang Lin-Lin(王林林)‡

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, *China*

(Received 23 November 2010; revised manuscript received 30 December 2010)

Disturbance imposed on the chaotic systems is an effective way to maintain its chaotic good encryption features. This paper proposes a new perturbation method to the Tent map. First it divides the Tent map domain into 2^N parts evenly and selects a particular part from them, then proliferates the Tent map mapping trajectory of this particular part, which can disturb the entire system disturbance. The mathematical analysis and simulated experimental results prove that the disturbed Tent map has uniform invariant distribution and can produce good cryptographic properties of pseudo-random sequence. These facts avoid the phenomenon of short-period caused by the computer's finite precision and reducing the sequence's dependence on the disturbance signal, such that effectively compensate for the digital chaotic system dynamics degradation.

Keywords: perturbation, Tent, degradation, chaotic

PACS: 05.45.Jn, 05.45.Xt **DOI:** 10.1088/1674-1056/20/5/050509

1. Introduction

Recently, with the continuous development of chaos theory, various encryption algorithms based on chaotic system are continually coming to the fore,[1−7] they are largely based on the chaotic system trajectory of the pseudo-randomness, as well as the sensitivity of the initial value, ergodicity and mixing property.[8,9]

In the classical chaos theory, chaotic systems are defined in a continuous domain, while computer and other digital system are discrete digital system, so in the process of the digital chaotic system, the computer's finite precision leads to the degradation behaviour of chaotic systems (short-cycle effects, low linear complexity and unbalanced distribution function etc.). Thus, in the finite precision environment, to maintain the good encryption features of chaotic systems is the core of chaotic encryption applications.

In order to overcome the degradation of chaotic dynamics in the computer systems, recently there have been many solutions, which can be divided into the following two types: (i) to increase the dimension of chaotic systems[10−14] or use compound chaotic systems;[15−17] (ii) to disturb the iteration process of the chaotic system using another low-dimensional chaotic system.[9] While the first kind of methods only slow down the speed of chaotic system degradation (with the gradually increasing number of iterations, the phenomenon of short-period of the chaotic system still appears), which are not real fundamental solutions to the chaotic system's degradation. The second method, perturbing the chaotic system gradually in the iterative process, can reduce the error and prevent the chaotic system's degradation, but the cycle of the final chaotic sequence will be affected by low-dimensional chaotic map which is used to disturb the iteration process. In this respect, we design a new disturbance method to the Tent map, theoretical analyses, mathematical proofs and computer simulation experiments confirm that the disturbed Tent map can produce good cryptographic properties of pseudo-random sequence, hence avoids the phenomenon of short-period caused by the computer's finite precision and reduces the sequence's dependence on the disturbance signal, thus effectively compensates for the digital chaotic system dynamics degradation.

The rest of this paper is organized as follows. Section 2 analyses the Tent map and designs the perturbation method. While mathematical proofs are provided in Section 3. Section 4 contains the simulation experiments and results of analysis. Finally, Section 5 concludes the paper.

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60573172 and 60973152), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20070141014), and the Natural Science Foundation of Liaoning Province of China (Grant No. 20082165).

†Corresponding author. E-mail: wangxy@dlut.edu.cn

‡Corresponding author. E-mail: wangdoublelin@126.com

© 2011 Chinese Physical Society and IOP Publishing Ltd

2. Design of the perturbation method

2.1. Analysis of Tent map

Tent map is a classical one-dimensional chaotic system, its definition is

$$x_{n+1} = g(x_n) = \begin{cases} \dfrac{x_n}{a}, & 0 \le x_n < a, \\ \dfrac{1-x_n}{1-a}, & a \le x_n \le 1, \end{cases} \tag{1}$$

where a is the system parameter. The chaotic map is defined in the interval $[0, 1]$, which has the same invariant distribution function: $\rho(x_n) = 1$, its Lyapunov exponent can be obtained by the following formula:

$$\lambda = \lim_{n\to\infty} \frac{1}{N} \sum_{i=1}^{N} \ln \left| \frac{\mathrm{d}g(x_n)}{\mathrm{d}x_n} \right|. \tag{2}$$

So we can obtain

$$\lambda = a \ln\left(\frac{1}{a}\right) + (1-a) \ln\left(\frac{1}{1-a}\right),$$

because $0 < a < 1$, so

$$\frac{1}{a} > 1, \quad \left(\frac{1}{1-a}\right) > 1$$
$$\Rightarrow \ln\left(\frac{1}{a}\right) > 0, \quad \ln\left(\frac{1}{1-a}\right) > 0,$$

that is $\lambda > 0$. Therefore, the Tent map is chaotic and its output signals have random, ergodicity and mixing property.

2.2. Description of the perturbation method

Without loss of generality, we can extend Eq. (1) to the following equation:

$$x_{n+1} = g(x_n) = \begin{cases} g_1(x_n), & 0 \le x_n < 1/2^N, \\ g_2(x_n), & 1/2^N \le x_n < 2/2^N, \\ \vdots & \vdots \\ g_{2^N}(x_n), & (2^N-1)/2^N \le x_n \le 1. \end{cases} \tag{3}$$

The interval [0, 1] is divided into 2^N equal length inter-cells:

$$I_1 = \left[0, \frac{1}{2^N}\right), \quad I_2 = \left[\frac{1}{2^N}, \frac{2}{2^N}\right), \ldots,$$
$$I_{2^N} = \left[\frac{2^N-1}{2^N}, 1\right].$$

Select an inter-cell I_r from 2^N equal length inter-cells and set the variable diffusion coefficient $e \in [0, 1]$. The interval I_r is divided into two parts: I_{r1} and I_{r2} according to the ratio of $(1-e) : e$. In each iteration of the Tent map, if the system variable x_n does not fall into the interval I_r, then x_n is unchanged; if the system variable x_n falls into the interval I_r, so the proliferation of system variables will be carried out according to Fig. 1, spread the interval I_{r1} to those intervals located on the left side of the interval I_{r1}, similarly, spread the interval I_{r2} to those intervals located on the right side of the interval I_{r2},

$$x'_n = \begin{cases} \dfrac{r-1}{1-e}\left(x_n - \dfrac{r-1}{2^N}\right), & x_n \in I_{r1}, \\ \dfrac{2^N-r}{e}\left(x_n - \dfrac{r-1}{2^N} - \dfrac{1-e}{2^N}\right) + \dfrac{r}{2^N}, & x_n \in I_{r2}. \end{cases} \tag{4}$$

Therefore, after the disturbance the Tent map becomes the following map:

$$x_{n+1} = f(x_n) = \begin{cases} g(x_n), & x_n \notin I_r, \\ g\left(\dfrac{r-1}{1-e}\left(x_n - \dfrac{r-1}{2^N}\right)\right), & x_n \in I_{r1}, \\ g\left(\dfrac{2^N-r}{e}\left(x_n - \dfrac{r-1}{2^N} - \dfrac{1-e}{2^N}\right) + \dfrac{r}{2^N}\right), & x_n \in I_{r2}. \end{cases} \tag{5}$$

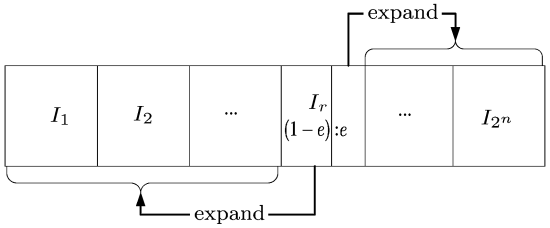


Fig. 1. Disturbance spread figure.

3. Mathematical analysis and proof

Theorem 1 The function (5) has the following properties: (a) $x_{n+1} = f(x_n)$ is a chaotic iteration function; (b) the function $f(x_n)$ has the same invariant distribution function: $\rho(x_n) = 1$.

Proof (i) By Eq. (2) we can obtain the Lyapunov exponent of function $f(x_n)$:

$$\lambda = \lim_{n\to\infty} \frac{1}{2^N} \sum_{i=1}^{2^N} \ln |f'(x_n)|.$$

Because of $1 < \ln |f'(x_n)| \leq 2^N$, we can obtain

$$0 < \lambda = \lim_{n\to\infty} \frac{1}{2^N} \sum_{i=1}^{2^N} \ln |f'(x_n)| \leq \ln 2^N = N \ln 2.$$

Therefore, $x_{n+1} = f(x_n)$ is a chaotic iteration function, so (a) is proved.

(ii) To prove (b), we only need to prove the probability $P\{x_n | f(x_n) < y\} = y$,

$$\begin{aligned}
& P\{x_n | f(x_n) < y\} \\
=\ & P\{x_n | f(x_n) < y, x_n \in I_r\} \\
& + P\{x_n | f(x_n) < y, x_n \notin I_r\} \\
=\ & P\{x_n | f(x_n) < y, x_n \in I_{r1}\} \\
& + P\{x_n | f(x_n) < y, x_n \in I_{r2}\} \\
& + \sum_{i=1}^{r-1} P\{x_n | f(x_n) < y, x_n \in I_i\} \\
& + \sum_{i=r+1}^{2^N} P\{x_n | f(x_n) < y, x_n \in I_i\} \\
=\ & P\{x_n | f(x_n) < y, x_n \in I_{r1}\} \\
& + P\{x_n | f(x_n) < y, x_n \in I_{r2}\} \\
& + \sum_{i=1}^{r-1} \frac{1}{2^N} y + \sum_{i=r+1}^{2^N} \frac{1}{2^N} y \\
=\ & \frac{1-e}{2^N} y + \frac{e}{2^N} y + \frac{2^N - 1}{2^N} y = y \Rightarrow \rho(x_n) = 1.
\end{aligned}$$

So (b) is proved to be correct.

Theorem 2 The inverse of function $f(x_n)$, denoted $f^{-1}(x_n)$, is a measure-preserving transformation in the Lebesgue sense.

Proof Suppose $I = [x_0, x_0 + \Delta x] \subset [0, 1]$, in order to prove that $f^{-1}(x_n)$ is a measure-preserving transformation, we only need to prove the equation: $\mu(f^{-1}(I)) = \Delta x$, where $\mu(f^{-1}(I))$ denotes the measure of the function $f^{-1}(x_n)$.

Assume that the length of the function $f^{-1}(I)$ corresponding to the interval $\left[0, \frac{r-1}{2^N}\right)$ is Δx_1, the length of the function $f^{-1}(I)$ corresponding to the interval $\left[\frac{r}{2^N}, 1\right]$ is Δx_2 and Δx_3 is the length of the function $f^{-1}(I)$ corresponding to the interval $\left[\frac{r-1}{2^N}, \frac{r}{2^N}\right)$. Therefore, we obtain the following equations:

$$\frac{\Delta x_1}{(r-1)/2^N} = \Delta x, \quad \frac{\Delta x_2}{(2^N - r)/2^N} = \Delta x.$$

The Δx_{31} denotes the length of the function $f^{-1}(I)$ corresponding to parts of the interval I_{r1} which is transformed into the interval $[0, \frac{r-1}{2^N})$, Δx_{32} denotes the length of the function $f^{-1}(I)$ corresponding to parts of the interval I_{r2} which is transformed into the interval $[\frac{r}{2^N}, 1]$, so we obtain the following two equations:

$$\frac{\left(\dfrac{r-1}{(1-e)/2^N}\right)\Delta x_{31}}{(r-1)/2^N} = \Delta x,$$

$$\frac{\left(\dfrac{(2^N - r)/2^N}{e/2^N}\right)\Delta x_{32}}{(r-1)/2^N} = \Delta x,$$

therefore we obtain

$$\begin{aligned}
\mu(f^{-1}(I)) &= \Delta x_1 + \Delta x_2 + \Delta x_3 \\
&= \Delta x_1 + \Delta x_2 + \Delta x_{31} + \Delta x_{32} \\
&= \frac{r-1}{2^N}\Delta x + \frac{2^N - r}{2^N}\Delta x \\
&\quad + \frac{1-e}{2^N}\Delta x + \frac{e}{2^N}\Delta x \\
&= \Delta x.
\end{aligned}$$

Thus, $f^{-1}(x_n)$ is a measure-preserving transformation in the Lebesgue sense.

First, we define an operator

$$M_j(x) = \left\lfloor 2^j \times x \right\rfloor \bmod 2, \quad x \in [0, 1], \quad j \in N. \quad (6)$$

The pseudo-random sequence, generated by the chaotic map $f(x_n)$, is transformed into a binary bit stream $\{b_i\}$ by Eq. (6),

$$b_i = M_j(x_i) = \left\lfloor 2^j \times x_i \right\rfloor \bmod 2.$$

Theorem 3 All bits in the binary bit stream $\{b_i\}$ are independent and identically distributed, that is

$$\forall (a_1, a_2, \ldots, a_n) \in F_2^n \quad (F_2^n = \underbrace{F_2 \times F_2 \times \cdots \times F_2}_{n}),$$

$$p(b_1 = a_1, b_2 = a_2, \cdots, b_n = a_n) = 2^{-n}.$$

Proof Without loss of generality, we only want to prove that when $j = 1$ by using mathematical induction:

(i) $n = 1$:$p(b_1 = 0) = p\{x_1 : M_1(x_1) = 0\} = p\{x_1 : x_1 \in [0, 0.5)\} = p\{x_1 : f^{-1}(x_1) \in [0, 0.5)\}$.

It is known from Theorem 2 that $f^{-1}(x_n)$ is a measure-preserving transformation in the Lebesgue sense, so we obtain

$$\begin{aligned} &p\{x_1 : f^{-1}(x_1) \in [0, 0.5)\} = 0.5 \\ \Rightarrow\ &p\{x_1 : M_1(x_1) = 0\} = p\{x_1 : M_1(x_1) = 1\} = 0.5, \end{aligned}$$

therefore the equation $p(b_1 = a_1) = 0.5 = 2^{-1}$ is true when $n = 1$.

(ii) $n = 2$: Without loss of generality, we assume the interval $I_r \subset [0.5, 1]$. In order to prove the equation $p(b_1 = a_1, b_2 = a_2) = 2^{-2}$, we first prove this situation: $p(b_1 = 0, b_2 = 1) = 2^{-2}$.

$$\begin{aligned} &p(b_1 = 0, b_2 = 1) \\ &= p\{x_1, x_1 : M_1(x_1) = 0, M_1(x_2) = 1\} \\ &= p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in [0.5, 1]\} \\ &= p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in I_r\} \\ &\quad + p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in [0.5, 1] \backslash I_r\}, \end{aligned} \tag{7}$$

and

$$\begin{aligned} &p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in I_r\} \\ &= p\left\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in \left[\frac{r-1}{2^N}, \frac{r-1}{2^N} + \frac{1-e}{2^N}\right]\right\} \\ &\quad + p\left\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in \left[\frac{r-1}{2^N} + \frac{1-e}{2^N}, \frac{r}{2^N}\right)\right\} \\ &= \frac{1-e}{2^N} \times \frac{\frac{1}{2} \times p\left\{x_2 : x_2 \in \left[0, \frac{r-1}{2^N}\right)\right\}}{p\left\{x_2 : x_2 \in \left[0, \frac{r-1}{2^N}\right)\right\}} + \frac{e}{2^n} \times \frac{\frac{1}{2} \times p\left\{x_2 : x_2 \in \left[\frac{r-1}{2^N}, 1\right]\right\}}{p\left\{x_2 : x_2 \in \left[\frac{r-1}{2^N}, 1\right]\right\}} \\ &= \frac{1-e}{2^N} \times \frac{1}{2} + \frac{e}{2^N} \times \frac{1}{2} = \frac{1}{2^{N+1}}, \end{aligned} \tag{8}$$

$$p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in [0.5, 1] \backslash I_r\} = \frac{1}{2} \times p\{x_2 : x_2 \in [0.5, 1] \backslash I_r\} = \frac{1}{2} \times \left(\frac{1}{2} - \frac{1}{2^N}\right). \tag{9}$$

With Eqs. (7), (8) and (9), we can obtain

$$\begin{aligned} &p(b_1 = 0, b_2 = 1) \\ &= p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in I_r\} \\ &\quad + p\{x_1, x_2 : x_1 \in [0, 0.5), x_2 \in [0.5, 1] \backslash I_r\} \\ &= \frac{1}{2^{N+1}} + \frac{1}{2} \times \left(\frac{1}{2} - \frac{1}{2^n}\right) = \frac{1}{4} = 2^{-2}. \end{aligned}$$

Similarly, we can obtain the following three equations:

$$\begin{aligned} p(b_1 = 0, b_2 = 0) &= 2^{-2}, \\ p(b_1 = 1, b_2 = 0) &= 2^{-2}, \\ p(b_1 = 1, b_2 = 1) &= 2^{-2}. \end{aligned}$$

So, the equation $p(b_1 = a_1, b_2 = a_2) = 2^{-2}$ has been proved, we can demonstrate the equation $p(b_i = a_i, b_{i+1} = a_{i+1}) = 2^{-2}$ for each $\forall i$ by the same way.

(iii) We assume the equation $p(b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k) = 2^{-k}$ is true when $n = k$, so when $n = k + 1$:

$$\begin{aligned} &p(b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k, b_{k+1} = a_{k+1}) \\ &= p(b_{k+1} = a_{k+1} | b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k) \\ &\quad \times p(b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k) \\ &= p(b_{k+1} = a_{k+1} | b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k) \times 2^{-k}. \end{aligned}$$

Because $b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k$ are independent, for as much as

$$\begin{aligned} &p(b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k, b_{k+1} = a_{k+1}) \\ &\quad = p(b_{k+1} = a_{k+1} | b_k = a_k) \times 2^{-k} \\ &\quad = \frac{1/4}{1/2} \times 2^{-k} = 2^{-(k+1)}. \end{aligned}$$

Therefore, $p(b_1 = a_1, b_2 = a_2, \cdots, b_k = a_k, b_{k+1} = a_{k+1}) = 2^{-(k+1)}$ is also proved. In the end, the Theorem 3 has been proved.

We can obtain the following conclusions from the above proof. The Tent map still has the following properties after the disturbance: (i) it is a chaotic iteration function; (ii) it has the same invariant distribution function $\rho(x_n) = 1$; (iii) all bits in the binary bit stream, produced by the Tent map iteration, are independent and identically distributed.

4. Analysis of simulation experiment

To estimate the performance of the proposed disturbance and illustrate its virtue, we carry out a series

of experimentals under the experiment environment: CPU: AMD Athlon 1.80 GHz; Memory: 1 GB; OS: Windows 7; Software: Matlab7.0.

4.1. Analysis of the Tent map trajectory

We do all the following experiments by using the form of the Tent map defined by the equation (1). Without loss of generality, take $a = 0.18$, that is,

$$x_{n+1} = g(x_n) = \begin{cases} \dfrac{x_n}{0.18}, & 0 \le x_n < 0.18, \\ \dfrac{1 - x_n}{0.82}, & 0.18 \le x_n \le 1. \end{cases} \tag{10}$$

The definition interval in Eq. (10) is divided into

$$I_1 = [0, 0.25), \quad I_2 = [0.25, 0.5), \\ I_3 = [0.5, 0.75), \quad I_4 = [0.75, 1], \tag{11}$$

without loss of generality, select the interval $I_2 = [0.25, 0.5)$ to disturb the Tent map, the interval I_2 is divided into two parts according to the ratio of $(1 - e) : e$, which are spread to other intervals respectively. The locus diagram is shown in Fig. 2.

Figure 2(a) is the image which is the trajectory diagram of the Tent map (1) with the initial value $x_0 = 0.24$, the iteration value has been 0 after a few iterations, which affects the generation of the digital chaotic sequence. Iterated 2000 times for the Tent map (10) with the initial value $x_0 = 0.24$, Fig. 2(b) is the trajectory diagram of the former 200 iterations and Fig. 2(c) is the trajectory diagram of the last 200 iterations. From the figure we can clearly see that the iterative trajectory of the Tent map (10) has maintained a good randomness which resists the defects of short-cycle phenomenon.

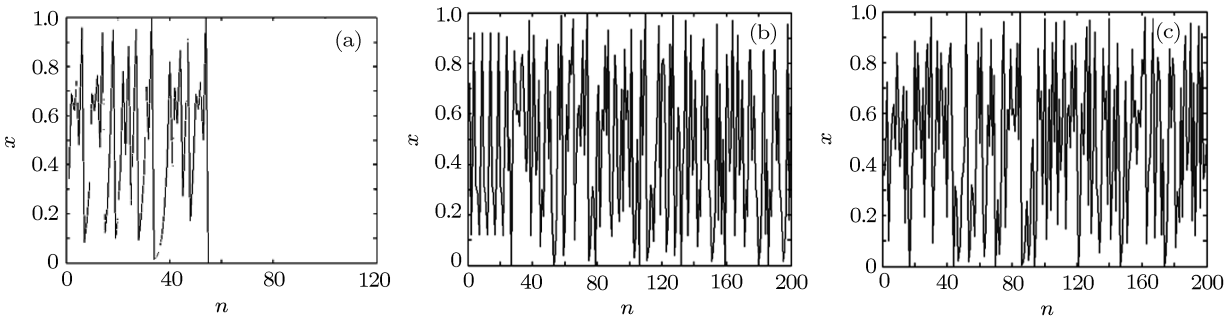


Fig. 2. Trajectory diagrams. (a) Tent map (1), $a = 0.5$; (b) Tent map (10), the former 200 iterations; (c) Tent map (10), the last 200 iterations.

4.2. Sensitivity test

1) The impact of the initial value on the chaotic sequence

Iterating the Tent map (10) on the initial value $x_0 = 0.24$ and $x_0 = 0.2400001$ respectively, we obtain two chaotic sequences which are completely different, as shown in Fig. 3. This shows that the Tent map (10) still maintains the high sensitivity of the initial value, so the chaotic sequence, produced by the Tent map (10), can be better used in information encryption.

2) The impact of the initial value on the 0–1 sequence

We select the initial value x_0 from 0 to 1 with step being equal to 0.0001, repeat the above experiment 10001 times and calculate the ratio of 0 in the 0–1 sequence for each time, the experimental data are shown in Fig. 4.

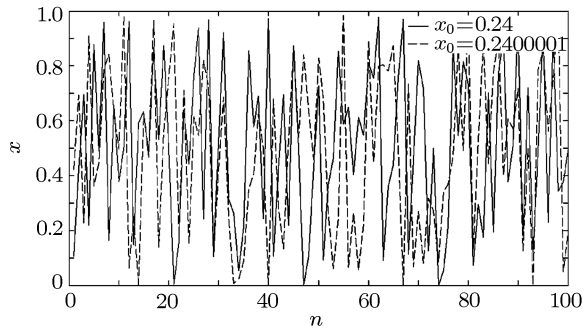


Fig. 3. The impact of the initial value on the chaotic sequence.

From the figure we can see that the ratio of 0 in the 0–1 sequence, always about 0.5, does not change with the change of the initial value, so the Tent map (10) is stable.

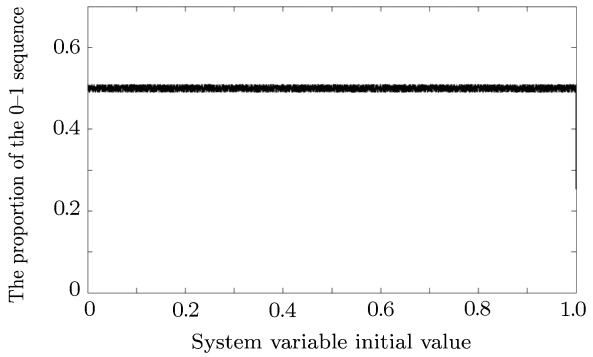


Fig. 4. The ratio of 0 in the 0–1 sequence.

4.3. Self-correlation and cross-correlation test

Self-correlation is used to describe the correlation between any two different values in one signal. Cross-correlation describes the correlation between the two values at a certain time which belong to two different signals.[18] They can be evaluated by the following formula:

$$R(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N-1} (b_i - b_{\text{mean}})(b_{i+m} - b_{\text{mean}}),$$

$$c(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N-1} (b_i - b_{\text{mean}})(b'_{i+m} - b'_{\text{mean}}),$$

where

$$b_{\text{mean}} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N-1} b_i,$$

$\{b_i\}$ and $\{b'_i\}$ are the 0–1 sequences which are produced by the Tent map (10) with different initial values.

Selecting the initial values $x_{01} = 0.57$, $x_{02} = 0.5700001$ respectively and the number of iterations $N = 10000$, we obtain two 0–1 sequences: $\{b_i\}$ and $\{b'_i\}$. Figure 5(a) is the self-correlation function image of the sequence $\{b_i\}$, Fig. 5(b) is the image of the cross-correlation function which denotes the correlation between the sequences $\{b_i\}$ and $\{b'_i\}$. From the above figures we can see that $R(m) \in [-0.05, 0.05]$ and $c(m) \in [-0.1, 0.1]$, therefore, the sequences generated by the Tent map (10) have good encryption features.

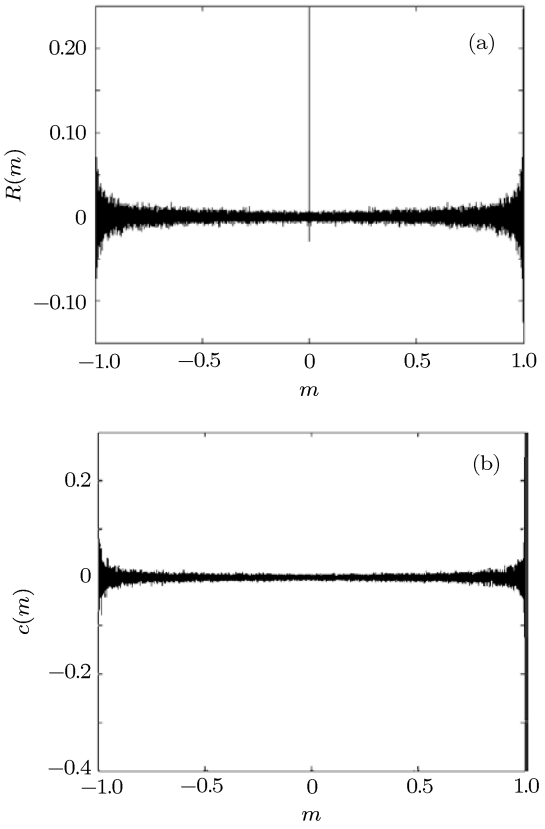


Fig. 5. Self/Cross-correlation function image. (a) Sequence $\{b_i\}$, (b) sequences $\{b_i\}$ and $\{b'_i\}$.

4.4. The SP 800-22 test

The national institute of standards and technology (NIST) special publication (SP) 800-22[19] tests are used for testing the sequence's randomness in this paper. The NIST Test Suite is a statistical package consisting of 16 tests which were developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random or pseudo-random number generators. These tests focus on a variety of different types of non-randomness which can could exist in a sequence. In this test, we test the cipher sequence, produced by the Tent map (10), whose length is 10^5 bits. The test results of testing sequence's randomness are shown in Table 1. We can conclude from Table 1 that the sequence produced by the Tent map (10) in this paper is stochastic.

Table 1. The SP 800-22 test results of sequence produced by the disturbed Tent map.

Statistical test	P-value	Conclusion
Frequency test ($n = 100$)	0.356147	random
Frequency test within a block ($n = 100$, $M = 10$)	0.459092	random
Runs test ($n = 100$, $\tau = 0.02$)	0.459092	random
Test for the longest run of ones in a block ($n = 128$)	0.704934	random
Binary matrix rank test ($n = 100000$, $M = Q = 32$)	0.731617	random
Discrete Fourier transform test ($n = 128$)	0.690421	random
Non-overlapping template matching test ($n = 2^{20}$, $B = 000000001$)	0.330470	random
Overlapping template matching test ($n = 1000000$, $B = 111111111$)	0.870238	random
Maurer's "Universal statistical" test ($n = 1048576$, $L = 7$, $Q = 1280$)	0.912352	random
Lempel–Ziv compression test ($n = 1000100$)	0.421743	random
Linear complexity test ($n = 1000,000$, $M = 1000$)	0.702401	random
Serial test ($m = 2$, $n = 1000000$)	0.991039	random
Approximate entropy test ($m = 2$, $n = 100$)	0.894901	random
Cumulative sums test ($n = 100$, mode=0 (forward))	0.460193	random
Random excursions test ($n = 1000000$)	0.949201	random
Random excursions variant test ($n = 1000000$)	0.251072	random

4.5. Application in image encryption

Experiment of the Lena image encryption has been done by using the sequence which is produced by the Tent map (10). The plain-image with the size 256×256 is shown in Fig. 6(a) and the corresponding histogram of the plain-image is shown in Fig. 6(b). Figure 6(c) is its encrypted image with the encryption key $x_0 = 0.24$ which is the initial value of the Tent map (10), and the corresponding histogram is shown in Fig. 6(d).

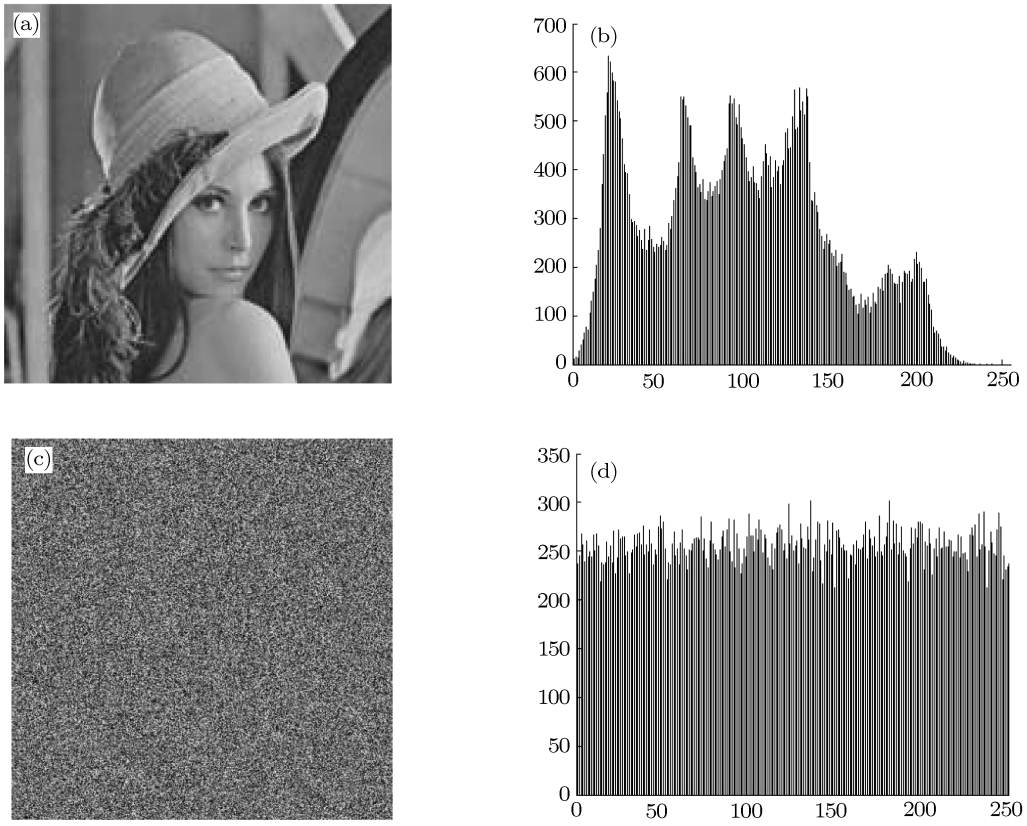


Fig. 6. Lena image encryption experimental result. (a) Original Lena, (b) corresponding histogram of image (a), (c) encrypted Lena, (d) corresponding histogram of image (c).

From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. This is because the image pixels are distributed uniformly using the sequence which is produced by the Tent map (10).

5. Conclusion

In this paper we design a new disturbance method to the Tent map. This novel disturbance method can avoid the phenomenon of short-period caused by the computer's finite precision, reduce the sequence's dependence on the disturbance signal and effectively compensate for the digital chaotic system dynamics degradation. Theoretical analyses, mathematical proofs and computer simulation experiments confirm that the disturbed Tent map can produce good cryptographic properties of pseudo-random sequence, which has a higher application potential in the confidential communications and information security.

References

[1] Gao H J, Zhang Y S, Liang S Y and Li D Q 2006 *Choas, Solitons and Fractals* **29** 393

[2] Zhang H G, Ma D Z and Wang Z S 2010 *Acta Phys. Sin.* **59** 147 (in Chinese)

[3] Xiang T, Liao X F, Tang G P, Chen Y A and Wong K W 2006 *Phys. Lett.* A **349** 109

[4] Kohda T and Tsuneda A 1997 *IEEE Trans. Inf. Theory* **43** 104

[5] Wang K, Pei W J, Hou X B, Hong S and He Z Y 2009 *Phys. Lett.* A **373** 653

[6] Wang X Y and Wang X J 2008 *Int. J. Mod. Phys.* C **19** 813

[7] Zhang H G 2007 *Acta Phys. Sin.* **56** 3796 (in Chinese)

[8] Chen G and Lai D 1998 *Int. J. Bifurcat. Chaos* **8** 1585

[9] Wang Y, Liao X, Xiang T, Wong K T and Yang D 2007 *Phys. Lett.* A **363** 277

[10] Pareek N K, Patidar V and Sud K K 2003 *Phys. Lett.* A **309** 75

[11] Emura T 2006 *Phys. Lett.* A **349** 306

[12] Wong K W 2003 *Phys. Lett.* A **307** 292

[13] Chen G R, Mao Y B and Chui C K 2004 *Choas, Solitonas and Fractals* **21** 749

[14] Zhang H G, Ma T D, Fu J and Tong S C 2009 *Chin. Phys.* B **18** 3751

[15] Wong W K, Lee L P and Wong K W 2001 *Comput. Phys. Commun.* **138** 234

[16] Zhang H G, Fu J, Ma T D and Tong S C 2009 *Chin. Phys.* B **18** 969

[17] Zhao Y, Zhang H G and Zheng C D 2008 *Chin. Phys.* B **17** 529

[18] Lü L and Li G 2008 *Acta Phys. Sin.* **57** 7517 (in Chinese)

[19] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J and Vo S 2001 *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* NIST Special Publication 800-22