A perturbation method to the tent map based on Lyapunov exponent and its application*

Cao Lv-Chen(曹绿晨)[a], Luo Yu-Ling(罗玉玲)[a]†, Qiu Sen-Hui(丘森辉)[a], and Liu Jun-Xiu(刘俊秀)[b]

[a] Guangxi Key Laboratory of Multi-source Information Mining & Security, Faculty of Electronic Engineering, Guangxi Normal University, Guilin 541004, China

[b] School of Computing and Intelligent Systems, University of Ulster, Derry, Northern Ireland BT48 7JL, UK

(Received 25 March 2015; revised manuscript received 28 April 2015; published online 20 August 2015)

Perturbation imposed on a chaos system is an effective way to maintain its chaotic features. A novel parameter perturbation method for the tent map based on the Lyapunov exponent is proposed in this paper. The pseudo-random sequence generated by the tent map is sent to another chaos function — the Chebyshev map for the post processing. If the output value of the Chebyshev map falls into a certain range, it will be sent back to replace the parameter of the tent map. As a result, the parameter of the tent map keeps changing dynamically. The statistical analysis and experimental results prove that the disturbed tent map has a highly random distribution and achieves good cryptographic properties of a pseudo-random sequence. As a result, it weakens the phenomenon of strong correlation caused by the finite precision and effectively compensates for the digital chaos system dynamics degradation.

Keywords: perturbation, tent map, Lyapunov exponent, finite precision

PACS: 05.45.–a, 05.45.Pq **DOI:** 10.1088/1674-1056/24/10/100501

1. Introduction

Chaos has aroused a research interest in various fields of cryptography due to its inherent random-like behaviours. In the last 20 years, a large number of cryptographic algorithms based on chaos have been proposed[1–3] and digital chaos systems have been employed in most of these cryptosystems. However, when chaos is realized in computers or digital circuits, a chaos system often suffers dynamical degradation, which refers to the short cycle length, non-ergodicity, low linear-complexity and strong correlation.[4] These features exist extensively in all chaos systems when they are digitally implemented, e.g. the logistic map is chosen to show the dynamical degradation phenomenon under the limitation precision of 0.01. The logistic map is presented as

$$x_{n+1} = \alpha \cdot x_n \cdot (1 - x_n), \tag{1}$$

where α is the control parameter and when $\alpha \in [3.57, 4]$, the logistic map is in the chaotic state, n is the time index, and x_n denotes the status value for the initial value after $n-1$ iterations. The parameter α is 4. Using numerical simulation, we obtain three representative sequences whose initial values are 0.02, 0.65 and 0.03. As shown in Fig. 1, an infinite loop occurs after several iterations when the sequence value becomes 0.97, 0.42 or 0.12. Such a dynamical degradation phenomenon can result in the performance attenuation of digital chaos based processing, e.g. the chaos based cryptosystems become vulnerable to attack.[5,6] Therefore, preventing the side-effects caused by the dynamical degradation is always a challenge to the chaos based cryptosystems.

Five remedy methods are commonly used for preventing the dynamical degradation of digital chaos systems. (i) Using high finite precision,[7] which can slow down the speed of degradation with gradually increasing the number of iterations, but the degradation still exists; it is not really a fundamental solution for chaos systems' degradation. (ii) Cascading multiple chaos systems.[8] This method can

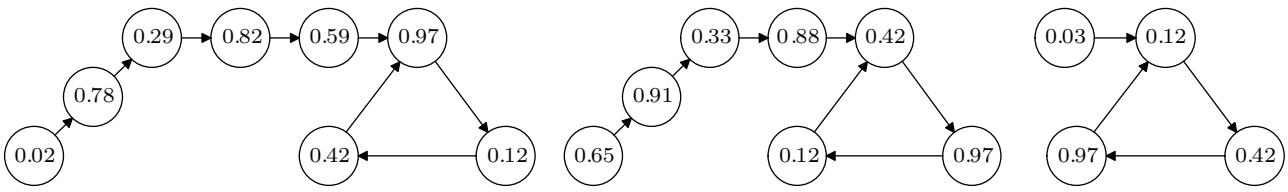


Fig. 1. Degradation phenomenon of logistic map when the precision is 0.01.

*Project supported by the Guangxi Provincial Natural Science Foundation, China (Grant No. 2014GXNSFBA118271), the Research Project of Guangxi University, China (Grant No. ZD2014022), the Fund from Guangxi Provincial Key Laboratory of Multi-source Information Mining & Security, China (Grant No. MIMS14-04), the Fund from the Guangxi Provincial Key Laboratory of Wireless Wideband Communication & Signal Processing, China (Grant No. GXKL0614205), the Education Development Foundation and the Doctoral Research Foundation of Guangxi Normal University, the State Scholarship Fund of China Scholarship Council (Grant No. [2014]3012), and the Innovation Project of Guangxi Graduate Education, China (Grant No. YCSZ2015102).

†Corresponding author. E-mail: yuling0616@gxnu.edu.cn

© 2015 Chinese Physical Society and IOP Publishing Ltd

effectively prolong the cycle of orbit but often leads to a worse distribution. (iii) Switching multiple chaos systems, which can also weaken the degradation and extend the length of the chaotic sequence.[9,10] But in this scheme the length of chaotic sequence is just a superposition of each chaotic sequence, therefore, the degradation phenomenon is still not alleviated. In addition, it is difficult to design a proper switch rule to preserve the properties of the system. (iv) Coupling different chaos systems, which is another method to reduce the degradation. As for this method, a proper chaos should be selected to avoid that the loss of system complexity exceeds the gain of performance improvements, otherwise it would lose the practicability. For example, a unidirectional coupling based hybrid method uses the three-dimensional (3D) Lorenz system to couple a one-dimensional (1D) logistic map.[11] Although the dynamical property of the logistic map is promoted, the complexity of the system is increased greatly. Using a continuous system to couple a discrete system is difficult in practical work because the Lorenz system costs more resources than the discrete-time chaos when they are implemented on the hardware.[12,13] The computing speed will be pulled down as the continuous system requires a longtime period for computation. (v) Pseudo randomly perturbing the chaos system,[14] which can greatly improve the dynamical properties of digital chaos systems and has been proved to be better than the aforementioned methods.[15] Although the perturbation sources are also generated on digital devices in the existing perturbation algorithms, a good performance can be obtained as long as the proper perturbation method is confirmed. Furthermore, this method does not need any large scale system which makes it easy to implement. The perturbation objects include system parameter and sequence value, and the perturbation degree and interval can be managed so that there will be significant influence on the performance of the result. In this paper, a new parameter perturbation method for the tent map based on the Lyapunov exponent and Chebyshev map is proposed. The main contributions of this paper include that i) a novel perturbation principle and method for the Tent map are proposed and ii) the performance evaluation results and a case study are also given. The rest of the paper is organized as follows. In Section 2, the performance of the Tent map and Chebyshev map is analyzed and a perturbation method is proposed. Performance analysis results and a case study are given in Section 3. Finally, some conclusions are drawn Section 4.

2. Perturbation method

Firstly, the analysis of the tent map and Chebyshev map are given in this section as they are both employed in the proposed perturbation method. The nonlinear tent map is a classical piecewise chaos system. It is defined as

$$X_{n+1} = \begin{cases} x_n/\alpha, & 0 \le x_n < a, \\ (1-x_n)/(1-\alpha), & \alpha \le x_n \le 1, \end{cases} \tag{2}$$

where a is the control parameter. When $\alpha \neq 0.5$ and α belong to most parts of interval (0, 1), the system presents good pseudo-randomness. The output of the tent map is in the interval of (0, 1), which has the same invariant density distribution: $\rho(x_n) = 1$. The Lyapunov exponent of the tent map is shown as follows:

$$\lambda = a \cdot \ln\left(\frac{1}{a}\right) + (1-a) \cdot \ln\frac{1}{1-a}. \tag{3}$$

It can be seen that the Lyapunov exponent only depends on parameter a. From the research outcome of Ref. [16], it is known that a system is in a chaotic state when the Lyapunov exponent is positive, and the chaotic state keeps a high level when the Lyapunov exponent is high. Figure 2 is the Lyapunov exponent (LE) of tent map versus system parameter α. The Lyapunov exponent is positive in the whole domain of a. When $a = 0.5$, the tent map has the biggest Lyapunov exponent (i.e. ~ 0.7), and when it is in the interval of (0.2, 0.8), the Lyapunov exponent is kept in a relatively high level (i.e., ~ 0.5).

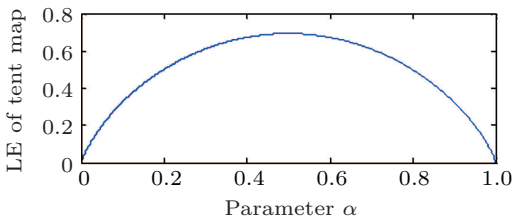


Fig. 2. (color online) Lyapunov exponent (LE) of tent map versus parameter a.

The Chebyshev map is another chaos system which is based on the trigonometric function. It is defined by

$$y_{n+1} = \cos(\beta \cdot \cos^{-1} y_n), \tag{4}$$

where β is the system parameter. When $\beta \ge 2$, the Chebyshev map has good chaotic properties with mixture and ergodicity, and its Lyapunov exponent is positively correlated to the parameter β.[1] Let $\{y_i\}$ be the chaotic sequence generated by Eq. (4), the statistical property of the chaotic sequence can be achieved by the following steps: Firstly, the probability density of a chaotic sequence generated from the Chebyshev map can be generated as shown below.

$$\rho(y) = \begin{cases} \dfrac{1}{\pi\sqrt{1-y^2}}, & -1 \le y \le 1, \\ 0, & \text{otherwise;} \end{cases} \tag{5}$$

Secondly, the mean of $\{y_i\}$ can be obtained on the basis of the following equation:

$$\bar{y} = \lim_{N\to+\infty} \frac{1}{N} \sum_{i=0}^{N-1} y_i = \int_{-1}^{1} y\rho(y)\,\mathrm{d}y = 0. \tag{6}$$

Equation (6) can be used to express the statistical property of the chaotic sequence. It indicates that the chaotic sequence generated by the Chebyshev map has good distribution characteristics as the mean of $\{y_i\}$ is 0. This feature is appropriate to use in the random number generating. In addition, the sequence value of the Chebyshev map ranges from -1 to 1, which is broader than that of the tent map.

According to the properties of the tent map and Chebyshev map, a novel special perturbation method is proposed in this paper. It is shown in Fig. 3 where the tent map is the original pseudo-random number generator, and its iteration values are sent to the Chebyshev map for the post processing.

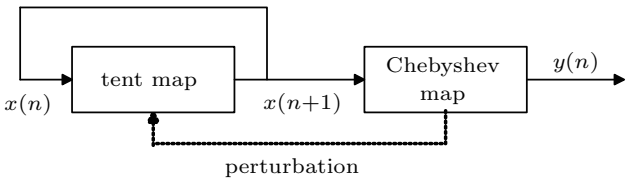


Fig. 3. Perturbation method.

Specifically, figure 4 shows the flow chart of the proposed system, where a 1D matrix $-P_\text{tent}(1,i)$ is used to store the changing parameters of the tent map, $x(1,i)$ is the sequence value of the tent map, $y(1,i)$ is the final output of the proposed system. Assigned to the system are an initial value and an initial parameter, which are denoted by $x(1,1)$ and $P_\text{tent}(1,1)$ respectively. As shown in Fig. 3, there are mainly two blocks in the proposed system. The first block is a tent map, and the other block is the post processing – parameter perturbation and transfer. All the chaotic values generated from the tent map are iterated once again through the Chebyshev for the post processing, that is, $y(1,i) = \cos(\beta \cdot \cos^{-1}(x(l,i+l)))$. The corresponding status values generated by the Chebyshev map are the final output. Suppose that δ is one of the final outputs, if δ falls into a range of (0.2, 0.5) or (0.5, 0.8), it will not only be used as the output value of the chaotic sequence but also sent back to the tent map to replace the original parameter a, then δ will be the parameter of the tent map in the next iteration. Otherwise, the parameter of the tent map in the last iteration is preserved for the next iteration. Therefore, the parameter of the tent map is always changed as long as the final output of the Chebyshev falls into an appropriate range.

Figure 5 shows the changing parameters of the tent map in the first 1000 iterations. It can be seen that the parameter changes hugely and continuously after several iterations. The changing parameters of the tent map destroy the original chaos orbit, which greatly prohibits the short circle phenomenon from occurring. Moreover, the post processing reduces the correlation among the status values. Figure 6 is the frequency distribution of the chaotic sequence generated by the proposed system. The chaotic sequence has a 'U'-shaped invariant density function, which is uniform except for two endpoints of -1 and 1. For a fixed length sequence, the probability distributed in each sub interval will be reduced as the scope of the output values extends to $(-1, 1)$. In this way, the proposed perturbation method can enhance the resistance to frequency attack.

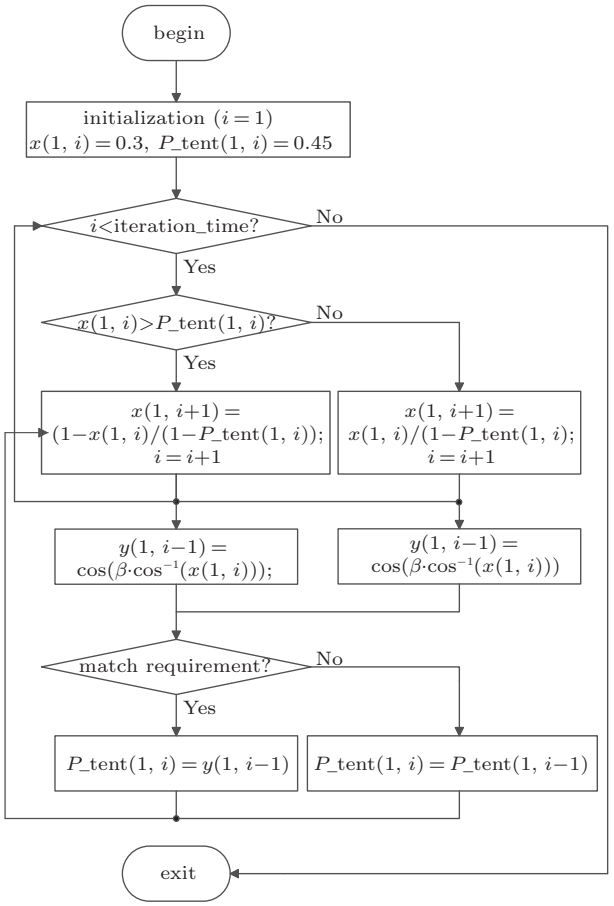


Fig. 4. Flow chart of the proposed system.

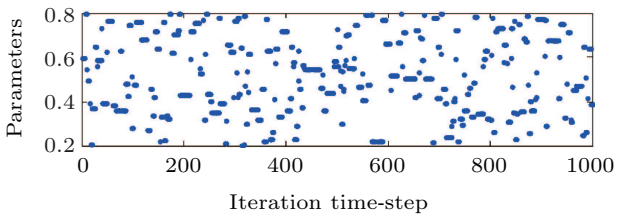


Fig. 5. (color online) Changing parameter of the tent map.

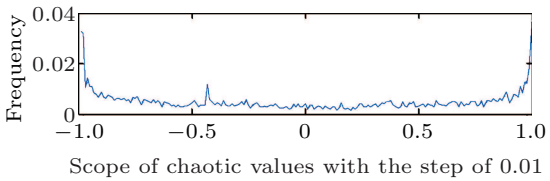


Fig. 6. (color online) Frequency distribution of output sequence of the proposed perturbation system where the step is 0.01.

3. Performance analysis and application

3.1. Autocorrelation

Autocorrelation is used to describe the correlation between any two different values in one number sequence. The normalized autocorrelation function of an arbitrary ideal random sequence $\{y_i\}$ is

$$\begin{aligned} AC(m) &= \lim_{N\to+\infty}\frac{1}{N}\sum_{i=0}^{N-1}(y_i-\bar{y})(y_{i+m}-\bar{y}) \\ &= \int_{-1}^{1} y f^m(y)\rho(y)\,\mathrm{d}y-\bar{y}^2 \\ &= \begin{cases} \mathrm{PSD}, & m=0, \\ 0.5, & m\neq 0, \end{cases} \end{aligned} \tag{7}$$

where $\rho(y)$ is defined by Eq. (5) and the PSD represents the power spectral density. In addition, according to Golomb's postulate for a pseudo-random sequence, an ideal chaotic sequence should have an important characteristic: its autocorrelation should be a delta function.[17,18]

Figure 7 shows the autocorrelations of the sequences generated by different chaos systems. The three figures in each column from left to right are the distributions of the tent map,

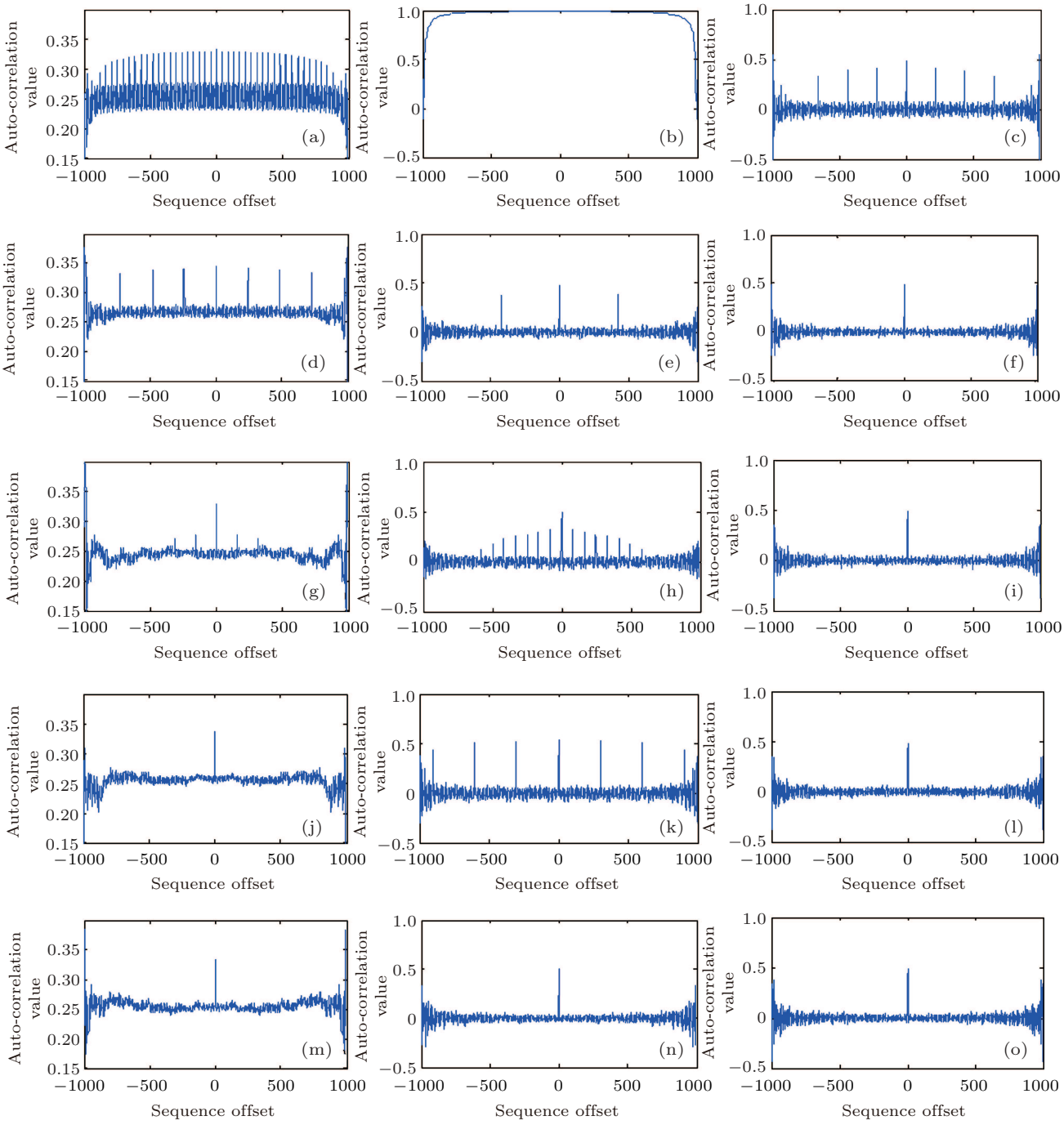


Fig. 7. (color online) $AC(m)$s under the precisions ranging from 10^{-4} to 10^{-8}: tent map (a), (d), (g), (j), (m); Chebyshev map (b), (e), (h), (k), (n); and the proposed system (c), (f), (i), (l), (o).

Chebyshev map and the proposed perturbation system, respectively. The precisions adopted by all the five rows are different ranging from 10^{-4} to 10^{-8}. The three sequences have the same length of 1000, and the same initial value of 0.3. In addition, for the Chebyshev map and the proposed perturbation system, the parameter β is 6. According to Eq. (7) and the Golomb's postulate, it is easy to see that the autocorrelation of the proposed system has achieved an ideal state when the computation precision is 10^{-5}, i.e. the shape of autocorrelation is similar to a delta function. The autocorrelation of the tent map has no burrs until the computation precision runs up to 10^{-7}. In addition, the $AC(m)$ of the tent map does not achieve 0 when $m \neq 0$, which indicates that the chaotic sequence has a strong correlation. For the Chebyshev map, its $AC(m)$ achieves an ideal state until the computation precision is 10^{-8} as shown in Fig. 7(n). The 'threshold accuracy' is defined as the time when the $AC(m)$ of a sequence reaches the ideal state under the lowest computation precision. Figure 7 illustrates the $AC(m)$s of the Tent map, Chebyshev map and the proposed system under precisions ranging from 10^{-4} to 10^{-8}. It is clear to see that the threshold accuracy of the proposed system is 10^{-5}, the threshold accuracy of the Chebyshev map is 10^{-8} and the threshold accuracy of the Tent map is higher than 10^{-8}. Therefore, the proposed system has a lower threshold accuracy than the tent map and Chebyshev map, i.e. it has the better chaotic feature.

3.2. Chaos attractor

The shape converged by all the values of one chaotic sequence in the spatiotemporal domain is defined as the chaos attractor. Most of the chaos attractors always have some geometric shapes and the complexity of the attractors can reflect the confusion degree of the chaos system. Figure 8 presents the chaos attractors of the tent map, Chebyshev map and the proposed perturbation system. The three different attractors all consist of the chaotic sequences each with a length of 1000. As shown in Fig. 8 the tent map has a piecewise linear attractor, and the Chebyshev map has a cosine function attractor. Any orbit of the two systems can traverse the whole interval of their mapped values. Compared with the two simple maps, the proposed perturbation system has a better ergodicity as the shape of attractor is destroyed. It makes the generated sequence appear "random" to the intruder. Thus the obvious correlation of neighbourhood is destroyed which enhances the security of the digital chaos system.

3.3. Approximate entropy

The approximate entropy is used to measure the complexity of the discrete time sequence. If the approximate entropy is too big, it will indicate that the sequence has a good complexity and stability. The test experiment is carried out by the following seven steps.

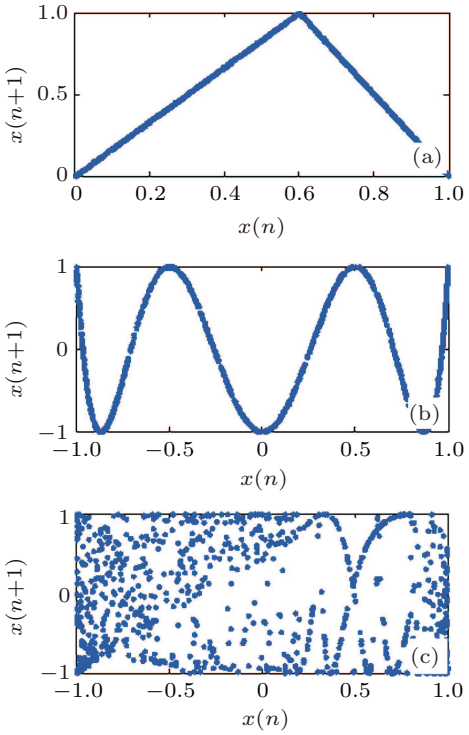


Fig. 8. (color online) Chaos attractors of (a) tent map, (b) Chebyshev map, and (c) the proposed system.

Step 1 A 1D discrete-time sequence with a length of N is given as $\{u(i),\ i = 1,\ldots,N\}$, then rebuild it into an m-dimensional vector: $X_i = \{u(i), u(i+1),\ldots,u(i+m-1)\}$, in which $i = 1,2,\ldots,n, n = N-m+1$.

Step 2 Compute the distance between any two vectors X_i and $X_j (j = 1,2,\ldots,N-m+1, j \neq i)$. The maximum absolute value of the corresponding elements between any two different vectors is defined as the distance that is described as

$$d_{ij} = \max|u(i+j) - u(j+k)|, k = 0,1,\ldots,m-1. \quad (8)$$

Step 3 Give a threshold value γ, normally in the interval of (0.2, 0.3). Count the number of d_{ij} which is less than $\gamma \times (SD)$, where SD is the standard value of the vector. Then the number is multiplied by $1/(N-m)$. The resulting number is denoted as $C_i^m(\gamma)$ i.e.,

$$C_i^m(\gamma) = \frac{1}{N-m}|\text{numberof}[d[X(i),X(j)] < \gamma]|, \quad i = 1 \sim N-m+1. \quad (9)$$

Step 4 Transform $C_i^m(\gamma)$ into a logarithmic form and obtain the corresponding average value which is denoted by $\emptyset^m(\gamma)$:

$$\emptyset^m(\gamma) = \frac{1}{N-m+1}\sum_{i=1}^{N-m+1} \ln C_i^m(\gamma). \quad (10)$$

Step 5 m is added by one, repeat the four steps above. $C_i^m(\gamma)$ and $\emptyset^m(\gamma)$ are obtained.

Step 6 The $\emptyset^{m+1}(\gamma)$ and $\emptyset^m(\gamma)$ are employed to compute the approximate entropy:

$$ApEn = \sum_{N\to\infty}[\emptyset^m(\gamma) - \emptyset^{m+1}(\gamma)]. \quad (11)$$

In this paper, the length of N is set to be 1000. Figure 9 shows the approximate entropies of the tent map, Chebyshev map and the proposed system. The x axis is the data precision P, e.g. the data precision is 10^{-10} if $p = 10$. It can be seen that the approximate entropy of the proposed perturbation system (i.e. $\sim$1.8) is greater than those of the tent map (i.e. $\sim$0.55) and Chebyshev map (i.e. $\sim$1.5), which means that the parameter perturbation can not only greatly enhance the complexity of the tent map but also make it more complicated than that of the Chebyshev map. Moreover, the approximate entropy of the proposed perturbation system is almost invariable with computation precision, i.e. the approximate entropy is still high even if the data precision is low (e.g. $P = 5$). Therefore, the proposed method is robust to computation precision, i.e. the expected chaotic sequence can be obtained even with a low precision; therefore the computing cost can be reduced (especially for the embedded system implementation).

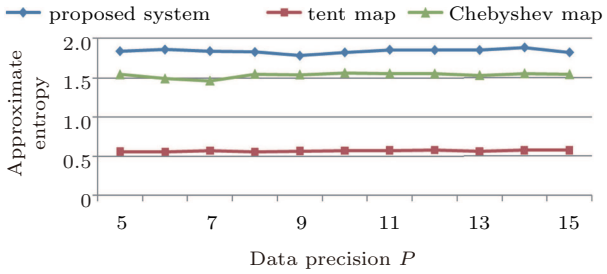


Fig. 9. (color online) Approximate entropies of the tent map, Chebyshev map, and the proposed system.

3.4. Sensitivity of initial value

If the system parameter is fixed, when the initial value has a small change, the extent of change of the sequence value can reflect the system sensitivity to the initial value. In this experiment, the system parameter is fixed to be $a = 0.6$, the initial value is $x_0 = 0.3$ and the change of initial value is 0.0000000001 (i.e., 10^{-10}). Figure 10 shows the output values of the original system and the modified system with a tiny change for the initial value. It can be seen that the output values of these two systems are completely different, e.g. after $\sim$20 times iterations, they begin to separate from each other. This shows that the proposed system maintains a high sensitivity to the initial value.

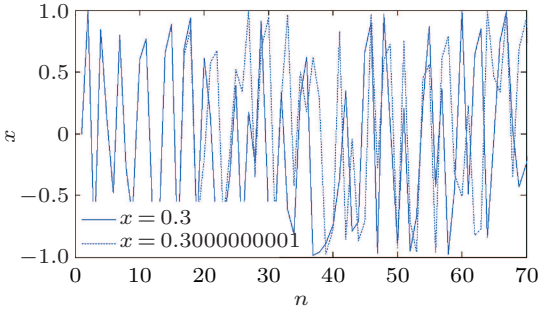


Fig. 10. (color online) Two sequences for different initial values.

3.5. SP 800-22 test

The SP 800-22 is a statistical test consisting of 15 tests. It was developed to test the randomness of arbitrarily long binary sequences produced by cryptographic random or pseudorandom number generators.[19,20] These tests focus on different types of non-randomness that could exist in a sequence. Each test is applied to the same sequence of n bits and gives a P-value, i.e. the probabilistic measure of the randomness of the sequence under test. If the significance level α is chosen to be 0.01 (common value of α in cryptography is about 0.01), then about 1% of the sequences are expected to be nonrandom.[6] A sequence passes a statistical test whenever the P-value$\geq \alpha$; otherwise it fails. In this experiment, the length of a bit-sequence produced by the proposed system is 10^7 bits, which is longer than values obtained by the approaches of Refs. [6] and [20], i.e., 10^5 and 10^6, respectively. The results of testing a sequence's P-values are shown in Table 1. It can be seen that the proposed system passes all the tests and the produced sequence has a good pseudo-randomness.

Table 1. SP 800-22 test results of the sequence produced by the proposed system.

Statistical tests	P-value	Conclusion
Frequency test	0.505022	pass
Block Frequency test ($m = 128$)	0.767020	pass
Cusum test mode 1 (forward)	0.593280	pass
Cusum test mode 2 (reverse)	0.628146	pass
Rank test	0.474332	pass
Long runs of ones test	0.276103	pass
Rank test	0.625811	pass
Spectral DFT test	0.690954	pass
Non-overlapping Templates test ($m = 9$, $B = 000000001$)	0.994654	pass
Overlapping templates test ($m = 9$)	0.148362	pass
Universal test	0.209906	pass
Approximate entropy test ($m = 10$)	0.632718	pass
Random excursions test ($x = +1$)	0.688189	pass
Random excursions variant test ($x = -1$)	0.358356	pass
Linear complexity test ($M = 500$)	0.244460	pass
Serial test ($m = 16$)	0.886045	pass

4. Applications in the image encryption

An image encryption experiment is designed by using the proposed perturbation system, where the generated chaotic sequence is employed to encrypt the image. Suppose that the size of the plain image is $\boldsymbol{M} \times \boldsymbol{N}$, the encryption algorithm is defined as follows.

Step 1 Iterate the proposed system $(\boldsymbol{M} \times \boldsymbol{N} - 1)$ times, the corresponding chaotic sequence is

$$\boldsymbol{S}_i = \{S_1, S_2, S_3, S_4, \ldots, S_{\boldsymbol{M}\times\boldsymbol{N}}\}$$

within a precision of 10^{-15} where $S_i \in (-1, 1)$.

Step 2 Transform the sequence S_i as follows:

$$\boldsymbol{S}_i = \text{uint8}((\text{abs}(\boldsymbol{S}_i) \times 10^{15} \text{mod} 256))$$

$$i = 1,2,3,\ldots,\boldsymbol{M}\times\boldsymbol{N}, \tag{12}$$

where the 'abs' operation means taking the absolute value, while 'mod' is the module operation. The 'uint8' is compulsory conversion. The real numbers are transformed into the integers with the format of 8-bit unsigned binary. After the transform, the numbers in $\boldsymbol{S}_i$ can be used to encrypt the plain image.

Step 3 Using the improved numbers in $\boldsymbol{S}_i$ to execute the bit-xor operation with all the pixels one by one from left to right, top to bottom.

Using this encryption algorithm, the plain image can be encrypted very well. A standard Lena image is used to evaluate the performance of the proposed encryption algorithm. The original Lena image with a size of 256×256 is shown in Fig. 11(a) and the corresponding histogram is shown in Fig. 11(b). Figure 11(c) is the encrypted image with the encryption key $x_0 = 0.3$ (i.e. the initial value of the proposed perturbation system), and its histogram is shown in Fig. 11(d). From these figures, it can be seen that the histogram of the encrypted image is fairly uniform and is significantly different from the original image as the image pixels of the encrypted image are distributed uniformly.

In addition, an experiment is carried out to test the entropy and the correlation between two adjacent pixels in vertical, horizontal, and diagonal directions of the cipher image. Table 2 shows the corresponding performance tests and comparisons. The same image of Lena by using the approaches of Refs. [1], [3], [21], and [22] are encrypted by their corresponding algorithms for 1, 2, 2, and 3 rounds, respectively. However, this method only needs one round of bit-xor encryption through the proposed system. But the cipher image achieves a good performance in correlation coefficient and entropy tests as well. In addition, from the results shown in Table 2, we can see that the time consumption of this case is the smallest in all the approaches. Therefore, the proposed system can be used in cryptography.

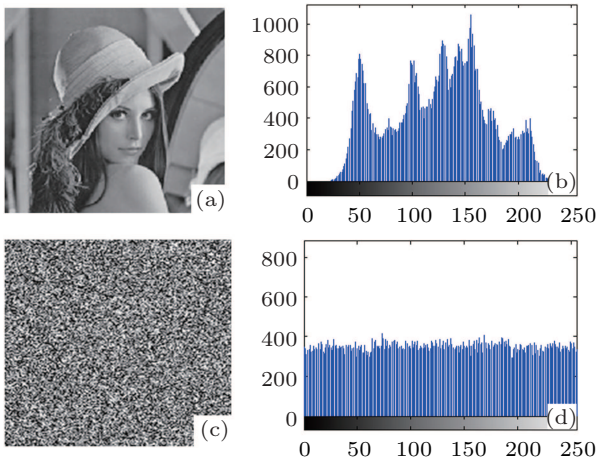


Fig. 11. (color online) Image encryption results: ((a) and (b)) Lena image and histogram, ((c) and (d)) encrypted image and histogram.

Table 2. Comparisons of cipher image among different approaches.

Approaches	Correlation coefficients at			Entropy	Speed/s	Rounds of encryption
	Horizontal	Vertical	Diagonal			
Ref. [1]	0.0008	0.0022	0.0065	7.9826	0.1130	1
Ref. [3]	0.0020	0.0062	0.0066	7.9992	N/A	2
Ref. [21]	0.0081	0.0085	0.0262	7.9989	2.1630	2
Ref. [22]	~ 0.0404	~ 0.0404	~ 0.0404	7.9975	4.9390	3
This work	0.0029	0.0059	-0.0038	7.9975	0.0798	1

5. Conclusions

In this paper, a novel parameter perturbation method for the tent map is proposed. Based on the Lyapunov exponent and Chebyshev map, the chaotic properties of the proposed system are hugely improved compared with those from the tent map and the Chebyshev map. This perturbation method can weaken the phenomenon of strong correlation caused by the finite precision, reduce the sequence's dependence on the perturbation signal and effectively compensate for the dynamics degradation of the digital chaos system. The theoretical analysis, performance tests and experimental results show that the proposed method can produce a pseudo-random sequence with good cryptographic properties, which has a good application potential in the fields of confidential communication.

References

[1] Luo Y L, Du M H and Liu J X 2015 *Commun. Nonliner Sci. Numer. Simul.* **20** 447
[2] Yuen C, Lui O and Wong K 2012 *Int. Symp., Circuits Syst.*, May 20–23, 2012, Seoul, Korea
[3] Lima J and Novaes L 2014 *Signal Processing* **94** 521
[4] Li S J, Chen G R and Mou X Q 2005 *Int. J. Bifur. Chaos* **15** 3119
[5] Bergamo P, DArco P, De Santis A and Kocarev L 2005 *IEEE Trans. Circuits Syst.* **52** 1382
[6] Wang X Y and Wang L L 2011 *Chin. Phys. B* **20** 050509
[7] Wang S H, Liu W R, Lu H P, Kuang J Y and Hu G 2004 *Int. J. Mod. Phys. B* **18** 2617
[8] Heidari-Bateni G and McGillem C D 1994 *IEEE Trans. Commun.* **42** 1524
[9] Azzaz M, Tanougast C, Sadoudi S, Fellah R and Dandache A 2013 *Commun. Nonliner Sci. Numer. Simul.* **18** 1792

[10] Tong X J 2013 *Commun. Nonliner Sci. Numer. Simul.* **18** 1725
[11] Hu H P, Deng Y S and Liu L F 2014 *Commun. Nonliner Sci. Numer. Simul.* **19** 1970
[12] Dabal P and Pelka R 2012 *19th Int. Conf. Mix. Des. Integr. Circuits Syst.*, May 24, 2012, Warsaw, Poland, p. 260
[13] Chung H and Miri A 2012 11*th Inernational Conf. Inf. Sci. Signal Process. Their Appl.*, October 21–25, 2012, Beijing, China, p. 460
[14] Liu S B, Sun J, Xu Z Q and Liu J S 2009 *Chin. Phys. B* **18** 5219
[15] Persohn K J and Povinelli R J 2012 *Chaos, Solitons and Fractals* **45** 238
[16] Liu N S 2011 *Commun. Nonliner Sci. Numer. Simul.* **16** 761
[17] Luo Y L and Du M H 2013 *Chin. Phys. B* **22** 080503
[18] Hu H P, Xu Y and Zhu Z Q 2008 *Chaos, Solitons and Fractals* **38** 439
[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
[20] Dabal P and Pelka R 2011 *IEEE* 14*th International Symposium on Design and Diagnostics of Electronic Circuits & Systems.* April, 13–15, 2011, Cottbus, German
[21] Wang X Y and Wang Q 2014 *Chin. Phys. B* **23** 030503
[22] Wang X Y, Zhao J F and Liu H J 2012 *Opt. Commun.* **285** 562