A Spatiotemporal Chaotic Sequence Based on Coupled Chaotic Tent Map Lattices System With Uniform Distribution

Jian-dong Liu
Information Engineering College
Beijing Institute of Petrochemical Technology
Beijing, China
Liujiandong@bipt.edu.cn

Kai Yang
Information Engineering College
Beijing Institute of Petrochemical Technology
Beijing, China
Yangkai0212@bipt.edu.cn

***Abstract*—A coupled chaotic map lattices system with uniform distribution (CML-UD) consisting of tent maps, which generates spatiotemporal chaos, is presented based on the security from the point view of cryptography. The system inherited the coupled diffusion and parallel iteration mechanism of coupled map lattices (CML). Through the dual non-linear effect of the rolled-out and folded-over of local lattices tent map and modular algorithms, CML-UD allows the system to enter into an ergodic state, and to rapidly generate uniform distributed multi-dimensional pseudo-random sequences concurrently. The experimental results show that, the spatiotemporal chaos sequences generated by the system has the same differential distribution character with the real random sequence of which each element has equal appearance rate, and it effectively restrains the short-period phenomenon which is easy to occur in digital chaotic system. In addition, it had many special properties such as zero correlation in total field, uniform invariable distribution and the maximum Lyapunov exponent is much bigger and steady. All of the properties suggest that the CML-UD possesses the potential application in encryption.**

***Index Terms*—cryptography, chaos, coupled map lattices, tent map, uniform distribution**

I. INTRODUCTION

An important difference between chaotic system and conventional cryptographic algorithm rests on real number field defined by chaotic system. Under the condition of limited precision, the dynamics feature of digital chaotic system is seriously degraded compared with its corresponding continuous system [1]. In order to apply the chaotic encryption algorithm in practice, it is necessary to examine the security issue of the digital chaotic system with a cryptology view, to design a safe chaotic system which fully meets the requirements of cryptology.

In some typical chaotic systems which are under existing researches, a class of piecewise linear mapping represented by tent map is featured with uniform distribution [2-4], but its initial low bit rate has no big influence to the output signal because there is a strong correlation between the consecutive values of the truncate chaotic sequences generated by this type of low dimensional chaotic system. This feature also could be utilized to conduct a divide-and-conquer attack on Chaos cryptography [5]. Furthermore, they also have some security flaws such as small key space and short output sequence period under some initial values.

Coupled Tent Map Lattices (CML) is a typical example of High-dimensional spatiotemporal chaos system [6], and it is realized through the tent map coupling, which could greatly enhance the complexity of a chaotic system, so as to enhance the security of the system [7]. Unfortunately, the CML has no longer had the feature of uniform distribution of tent map [8]. Furthermore, it also could not fully meet the design requirements of cryptographic algorithm.

The chaotic system given by the literature [9] well meets the security requirements of cryptography application, but its output is not featured with uniform distribution. The literature [10] gives a sequence uniformization method, which, no doubt, increases the computational load. In addition, this system requires complicated trigonometric calculations, so it may face difficulty for its hardware implementations.

In this paper, A coupled chaotic map lattices system with uniform distribution (CML-UD) consisting of tent maps is presented based on the security from the point view of cryptography. The system inherited the coupled diffusion

doi:10.4304/jcp.6.2.190-199

and parallel iteration mechanism of coupled map lattices(CML). Through the dual non-linear effect of the rolled-out and folded-over of local lattices tent map and modular algorithms, CML-UD allows the system to enter into an ergodic state, and to rapidly generate uniform distributed multi-dimensional pseudo-random sequences concurrently. The experimental results show that, the time sequences generated by the system has the same differential distribution character with the real random sequence of which each element has equal appearance rate, and it effectively restrains the short-period phenomenon which is easy to occur in digital chaotic system. In addition, it had many special properties such as zero correlation in total field, uniform invariable distribution and the maximum Lyapunov exponent is much bigger and steady.

II. ANALYSIS ON THE FEATURES OF TENT MAP

Tent maps is defined as:

$$F_\alpha : x_i = \begin{cases} \dfrac{x_{i-1}}{\alpha}, & 0 \le x_{i-1} < \alpha, \\ \dfrac{1-x_{i-1}}{1-\alpha}, & \alpha \le x_{i-1} \le 1. \end{cases} \quad (1)$$

As its function is featured by uniform distribution[2], the tent maps almost have the same distribution density with different control parameters, this feature is propitious to meet the balance need of cryptographic system. But, the time sequences generated by the tent map have two problems as follow:

1) The tent map is defined in real number field, when realized by computers, its precision is limited, the problem of short-cycle period will be exist, and, the property of chaotic will degenerate seriously. For example, when α=0.5, after few iterations, the results of iterate will always be 0 [11].

2) Because of the piecewise linear property of the tent map, the consecutive points of chaotic sequence have strong relativity with each other. To reflect these restrictions, the absolute value of the difference between two adjacent iterative sequence states is defined as d_1. Namely, $d_1=|x_{n+1}-x_n|$, d_1 is the first order difference, similarly, $d_k=|x_{n+k}-x_n|$, called d_k as k^{th} order difference [11].

The differential absolute value of real random sequence, of which each element has equal appearance rate, has linear decreasing distribution. However, because of the certain and strong restriction between the adjacent states of the chaotic sequence generated by tent map, the distribution of difference *p(d)* show a notable phase step (Fig. 1) when the difference of iterations *k* is less. When *k*≥*30*, *p(d)* tends to be linear decreasing and correspond with theoretical distribution. The phase step feature of the difference distribution will divulge important information of the system. As the experimental result shows in Fig. 2, the position of first order difference where the phase step take place linear changes with the parameter α, so that, it is easy to estimate the approximate value of the parameter α. of Eq.1 from the difference distribution.

III. ANALYSIS ON THE FEATURES OF CML

Model of CML is [6]:

$$x_{n+1}(i) = (1-\varepsilon) f(x_n(i)) + \frac{\varepsilon}{2}[f(x_n(i-1)) + f(x_n(i+1))] \quad . (2)$$

Among which, n is discrete-time step; i=1, 2,…, L is discrete lattice coordinate, L is system size; ε is coupling coefficient, and conform to $0<\varepsilon<1$; Non-linear function f is tent map(Eq. (1)). Boundary conditions are realized by $x_n(0)=x_n(L)$, $x_n(L+1)=x_n(1)$, and initial condition is the random number within[0,1].

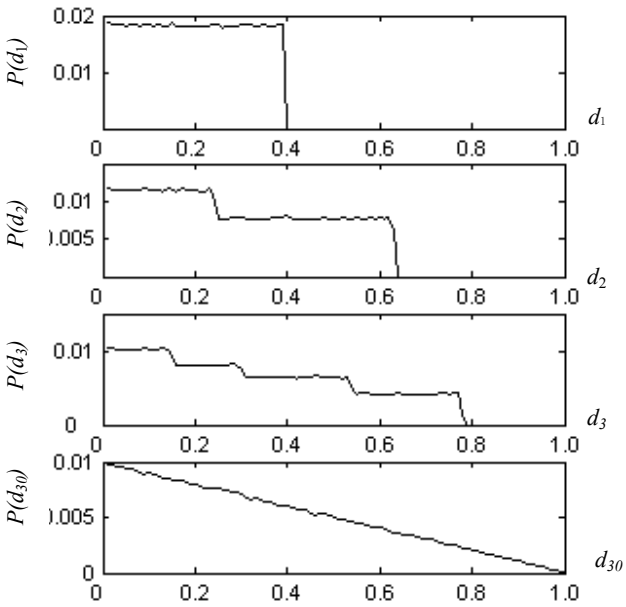


Figure 1. difference distribution of tent map(α=0.61), (a), (b),(c) and (d) is the 1st, 2nd, 3rd, 30th order difference distribution

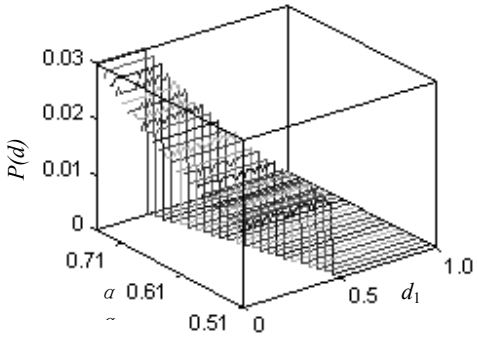


Figure 2. Influence of parameter α to the 1st order difference distribution of tent map (parameter α ranges from 0.51 to 0.71, with step length of 0.01)

CML has spatial-temporal chaotic behaviour, with a couple of positive Lyapunov exponents. It is chaotic both in time and space directions, and its dynamic behaviours are very rich and complicated. To a certain extent, it could eliminate the influence of limited precision of computer. However, CML is still not perfect from the angle of cryptography.

1) The coupling between lattices for CML exerts a diffusion function, and it could diffuse the changes of a single lattice, to influence all of other lattices. However, the coupling effect between lattices exerts great influence to the distribution properties of time sequence. The original uniform distribution of single tent map, after coupled according to the Eq. (1), is damaged. Fig. 3 illustrates the distribution of chaotic sequence generated by CML, given couple coefficient ε is 0.2.

When CML is in chaotic state, the system reaches an invariant distribution state. This distribution is affected by the parameters of $L,\varepsilon,$ and α. Given L=8, α=0.61, and when ε takes different values, a corresponding invariant distribution probability curve is worked out. From Fig.4, we can see, lattices probability distribution is related to the value of coupling coefficient ε, and its distribution of probability density is extremely uneven.

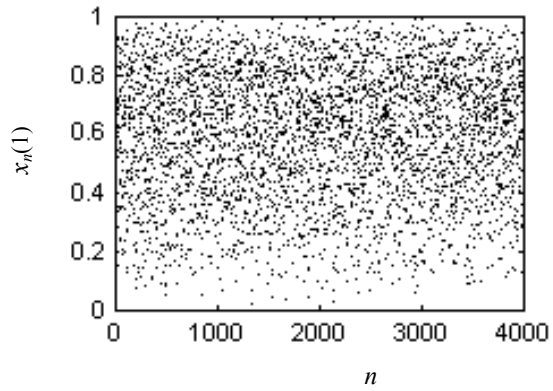


Figure 3. Distribution of Sequence Generated by CML (ε=0.2,α=0.61)

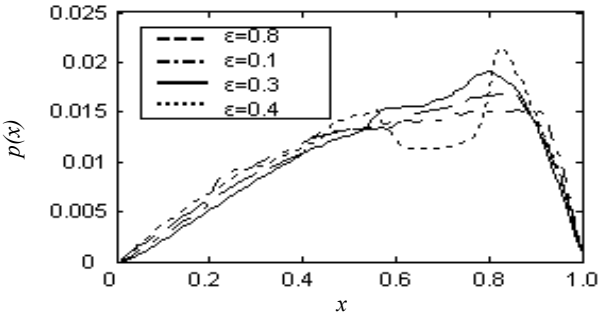


Figure 4. Distribution of Probability Density of Lattice State of CML

2) The consecutive points of time sequence generated by CML still have strong restrictions with each other. Fig.5 shows the experimental result of difference distribution in time direction. From the experiment it can be seen, the first order difference and second order difference show a notable step jump. When $k\geq 7$, distribution of d_k tends to be stable, but its distribution has large difference with theoretical distribution. The reason is that the time sequence generated by the CML does not have the feature of uniform distribution. In addition, change of coupling coefficient ε also has great influence on the differential distribution(Fig. 6).

IV. Improvement and Analysis on the Coupled Chaotic Tent Map Lattices

A. CML-UD

Coupled chaotic tent map lattices model (Eq. (2)) is improved. The diffusion coefficient ε is removed, and constant term k_i is added. The following system model (CML-UD) is achieved through modular algorithms to limit its lattice values within [0, 1].

$$x_{n+1}(i)=f(x_n(i))+f(x_n(i-1))+f(x_n(i+1))+k_i \ (mod\ 1) \qquad (3)$$

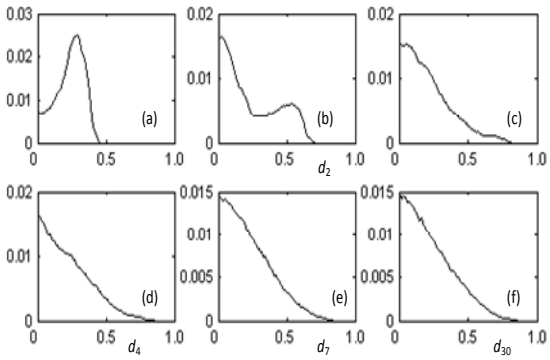


Figure 5. CML difference distribution (L=8, α=0.61, ε=0.6) (a),(b),(c),(d),(e) and(f)is the 1st , 2nd ,3rd, 4th, 7th 30th order difference distribution respectively; the longitudinal coordinate is the probability distribution density p(d)

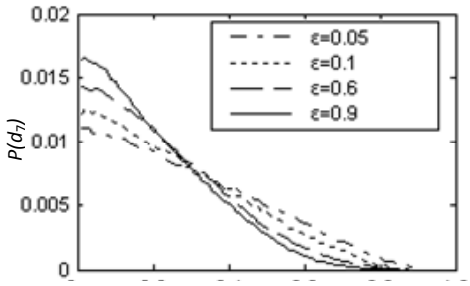


Figure 6. Influence of coupling coefficient ε to the 7th order difference distribution(L=8, α=0.61)

In the Eq.(3), meanings of n, i, and L are same as those in the Eq. (1). Here, $L \geq 4$. Non-linear function f is still tnt map F_α. Initial condition is random number within [0, 1], and k_i is constant term, and given $k_i=\sin(i)$, i is radian. CML-UD model (Eq. (3)) has excellent cryptography property.

B. Uniform distribution property of CML-UD

Fig. 7 illustrates the distribution of time sequence generated by CML-UD. Given $L=8$, when α takes different values, corresponding invariant distribution probability curve is worked out. It is illustrated in the Fig. 8. The experimental results show that, the time sequence generated by the CML-UD model has an ideal uniform distribution property.

Since structure of lattices of CML-UD is symmetric, each lattice has the same statistical characters. Randomly select a group of initial values, and given $\alpha=0.61$, taking any lattice for analysis, and equally divide the value set [0, 1] into 10^4 sections. When significant level reaches 5%, conduct the χ^2 uniform distribution examination on the number of each sections. When iteration $N=10^5$, the examined value is:

$$\chi^2 = \sum_{i=1}^{10000} \frac{(n_i - N/10000)^2}{N/10000} = 10110.6$$

When $N=10^6$, examined value $\chi^2=9930.3$

When $N=10^7$, examined value $\chi^2=9923.2$

When significant level reaches 5%, and by looking up the table， $u_{0.95}=1.645$, the result can be approximately calculated [12]:

$$x_{1-a}^2(n) = x_{0.95}^2(10000-1) \approx 10233.5$$

It can be seen from the analysis, CML-UD can pass through the uniform distribution hypothesis testing under the significant level of 5%.

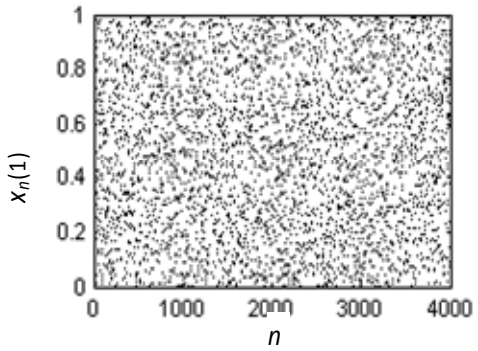


Figure 7. Time Sequence Distribution Generated by CML-UD (L=8, α=0.61)

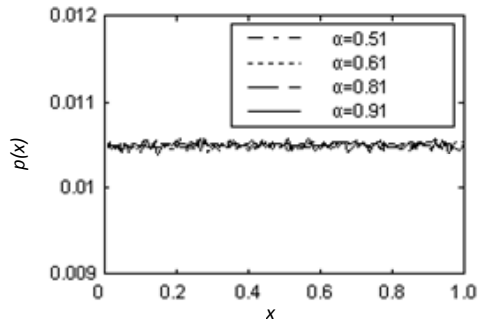


Figure 8. Distribution of Probability Density of Lattice State of CML-UD

C. Difference distribution property of CML-UD

The time sequence generated by CML-UD has the same differential distribution property with the real random sequence of which each element has equal appearance rate. When $k \geq 1$, differential distribution tends to have a linear decline. Fig.9 illustrates an experiment result of the first order different distribution of the time sequence generated by CML-UD, when α takes different values. From the characteristics of the difference of sequence, it is impossible to distinguish the sequence generated by CML-UD from the real random sequence of which each element has equal appearance rate. It is not feasible in calculation to draw up the system structure and parameter information that it produces from a time sequence generated by CML-UD.

D. Periodic problem under limited precision

Realization of computerized limited precision of the chaotic system is bound to generate periodic orbit. In order to overcome short-cycle behaviour, a perturbation method is put forward [13]. This method increases the complexity of the system, and the generated sequence period depends on the period of the perturbation. In CML (Eq. (2)), average periods and average transient time realized by computer increase along with the increase of coupling lattices L, but there are still some short periodic orbits. Therefore, CML still could not eliminate the short period problem caused by limited precision. CML-UD (Eq. (3)) allows the system to enter into an ergodic state through dual non-linear effect of the stretching and folded-over of local lattices tent map and

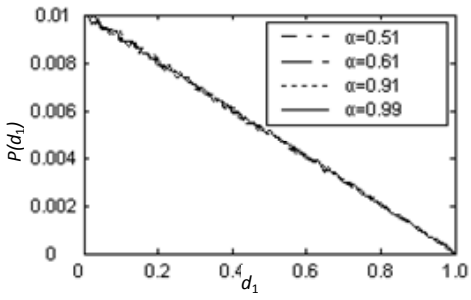


Figure 9. First Order Difference Distribution of CML-UD (L=8)

modular algorithms, to further increase the period of the system. For analysis the diffusion coefficient is removed in Eq. (3), and the modular algorithms effect is added. Firstly, the constant term is removed from the Eq. (3), we can get:

$$x_{n+1}(i)=f(x_n(i))+f(x_n(i\text{-}1))+f(x_n(i+1)) \pmod 1 \qquad (4)$$

Fig.10 gives the phase space trajectory, when tent map, Eq. (1), and Eq. (4) take calculation precisions of 2^{-4} and 2^{-7} respectively, and iterations n=4000 (calculation precision 2^{-h}, namely, after each iteration, truncation is made for double precision lattice variables, only to the binary decimal h^{th} digits after the decimal point). When calculating, Eq. (2) and (4) take same initial value. It can be seen that, for tent map, when the calculation precision is 2^{-4}, phase space orbit becomes a fixed point; when the calculation precision is 2^{-7}, mapping shows a simple and repeated vibrating in finite points; state trajectory of CML becomes complicated, but it is still restricted within a limited area; Removal of constant term from CML-UD (Eq. (4)) leads to that the track points are distributed into the entire phase space, which indicates that constraint information of the system is no longer available from time sequence, and the degree of chaos of the system has increased.

In Eq. (4), except for initial values, each lattice is symmetrical in structure. After adding a constant term (Eq. (3)), this structural symmetry could be broken. This technology has be widely applied (e.g. MD5, SHA-1, etc) in the structure of cryptographic Hash Functions [15]. After being added with constant term, the confusion property of the system is enhanced, and it allows the minimum period of the sequence generated by the system to be further increased. Tab. Ⅰ gives the calculated minimum period and average period of two models, given calculation precision $10^{-h_{10}}$ (h_{10}=2, 3), with randomly selected 100 groups of initial values, and under different number of lattices and different precisions. From Tab.1 it can be seen, in CML, when h_{10}=2，L takes the values between 4 and 7, namely, finite iterations converge to the fixed points, compared with CML, periodicity of the generated time sequence of CML-UD is improved notably under limited precision.

E. Lyapunov exponent

Maximum Lyapunov exponent is a quantified exponent to represent average exponent divergence rate of the adjacent orbits of phase space, and it describes the amplification of small deviation of orbits, and it is able to quantify the divergence of adjacent orbits. The larger the Lyapunov exponent value, the stronger the divergence is, and thus the higher the chaotic degree of the system will be. From an angle of cryptographic algorithm design, we always hope to have a larger Maximum Lyapunov exponent for a chaotic map.

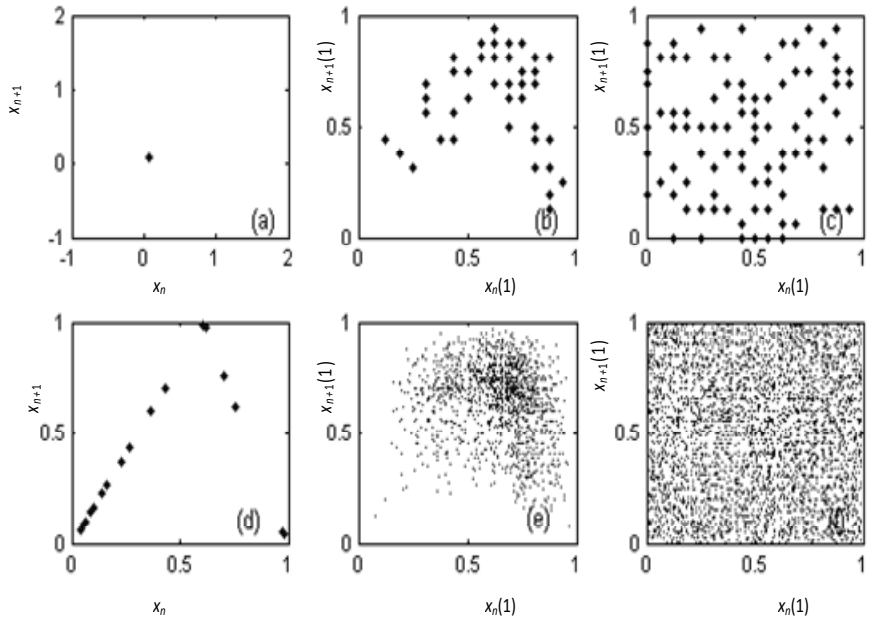


Figure 10. Phase Space Orbit of Sequence
(a) tent map(α=0.61,h=4)；(b) CML(α=0.61,ε=0.9,L=8,h=4)；(c) CML-UD (constant term removed,α=0.61,L=8,h=4)); (d) tent map(α=0.61,h=7); (e) CML(α=0.61,ε=0.9,L=8, h=7)；(f) CML-UD (constant term removed,α=0.61,L=8,h=7)

TABLE I.

MINIMUM PERIOD AND AVERAGE PERIOD OF TWO MODELS FROM 100 EXPERIMENTS UNDER DIFFERENT NUMBER OF LATTICES AND PRECISIONS

Name	h_{10}	*L*	*minimum period*	*average period*
CML	2	4	1	2
	2	5	1	32
	2	6	1	6
	2	7	1	789
	3	4	72	442
	3	5	175	1945
ICML	2	4	231	1645
	2	5	1657	3590
	2	6	1839	5325
	3	4	358511	493217

By adopting the method of literature [16], Eq. (5) could be used to calculate the maximum Lyapunov exponent of the coupled chaotic tent map lattices system, which is expressed by λ_{max}, namely,

$$\lambda_{\max} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log \frac{\| \boldsymbol{dx_n} \|}{\| \boldsymbol{dx_{n-1}} \|} \qquad (5)$$

In Eq. (5), $\| dx_n \| = \sqrt{\sum_{i=1}^{L} [dx_n(i)]^2}$.

For comparison convenience, the maximum Lyapunov exponent of CML (Eq. (2)) and CML-UD(Eq. (3)) has been calculated. The applied method is to randomly select a group of initial values. Given $dx_0=10^{-8}$, and 1000 steps of transients are removed to calculate follow up 3000 steps. The maximum Lyapunov exponents of system at the time when dimensionality *L* of the system and variable parameter α changes independently are calculated respectively. The result of the calculation is illustrated in the Fig. 11.

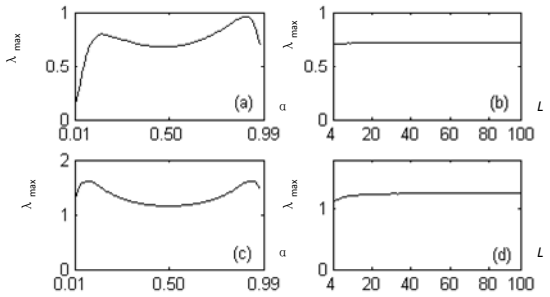


Figure 11. Maximum Lyapunov exponent
(a) CML, parameter α ranges from 0.01to 0.99, with step length of 0.01(coupling coefficient ε=0.01, *L*=8); (b) CML, system size *L* rangs from 4 to 100, step length 1 (coupling coefficient ε=0.01, α=0.61); (c) CML-UD, parameter α ranges from 0.01 to 0.99, step length 0.01(*L*=8); (d) CML-UD, system size *L* ranges from 4 to 100, step length 1(α=0.61)

According to the calculation result, we find that the change of the model size *L* only has small influence on the maximum Lyapunov exponent of two models. In CML, the change of parameter α has great influence on maximum Lyapunov exponent, while in CML-UD, the influence of parameter α to the maximum Lyapunov exponent obviously becomes smaller, and the value of the maximum Lyapunov exponent is very large, which indicates that CML-UD is a spatial-temporal chaotic system with a relatively stable large and positive Lyapunov exponent.

F. Correlation Property

Normalized auto-correlation function of the time sequence generated by coupled tent map lattices system is defined as:

$$C_{ii}(\tau) = \hat{C}ii(\tau) / \hat{C}ii(0)$$

$$\hat{C}_{ii}(\tau) = \frac{1}{N} \sum_{n=1}^{N} [x_n(i) - \bar{x}(i)][x_{n+|\tau|}(i) - \bar{x}(i)]$$

Cross-correlation function is defined as:

$$C_{ij}(\tau) = \hat{C}_{ij}(\tau) / \sqrt{\hat{C}_{ii}(0)\hat{C}_{jj}(0)}$$

$$\hat{C}_{ij}(\tau) = \frac{1}{N} \sum_{n=1}^{N} [x_n(i) - \bar{x}(i)][x_{n+|\tau|}(j) - \bar{x}(j)]$$

Among which, $|\tau| \in [0,N]$, *N* is the length of sequence , $\bar{x}(i)$ is the average value of sequence $x_n(i)$, *i* represents spatial lattice, *n* represents the steps of iterations.

Given *N*=999, parameter α ranges from 0.51 to 0.99, step length 0.01, correlation function of time sequence generated by CML and CML-UD is calculated. The result is illustrated in Fig. 12 and Fig. 13. Experiment results show that, for CML, when α>0.90，correlation is poor，when $|\tau|$ tends to zero, value of correlation is high. It indicates that the sequence of synchronous adjacent lattices has strong correlation; the auto-correlation function of CML-UD model is similar to δ function, and the cross-correlation between adjacent lattices tends to zero. It is a zero correlation in total field.

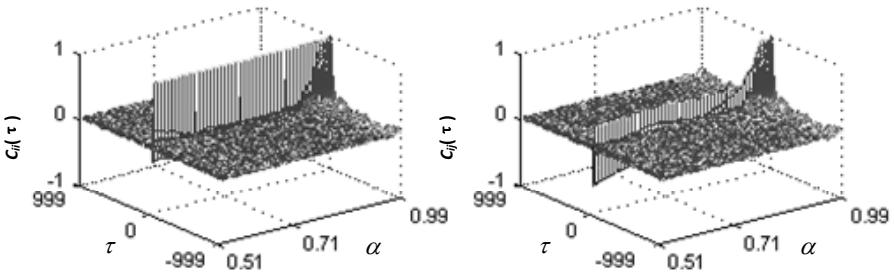


Figure 12. Correlation Function of CML (a) auto-correlation function; (b) cross-correlation function between adjacent lattices

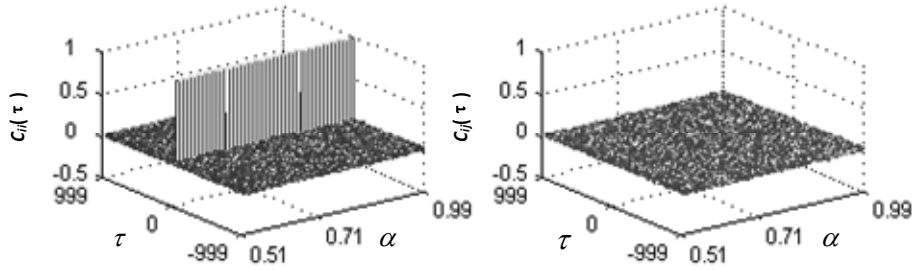


Figure 13. Correlation Function of CML-UD (a) auto-correlation function; (b) cross-correlation function between adjacent lattices

G. Balance

After N times iterations, the CML system, of which the system length is L, will parallelly generate L sequences $\{x_n(i)\}$, $i=1, 2, ..., L$, $x_n(i) \in [0,1)$, with the length of the sequences is N. On the basis of standard IEEE 75-1985, the mantissa of double precision which is binary should be 52-bits, that is:

$$x_n(i)= b_1^i \times 2^{-1}+ b_2^i \times 2^{-2}+\cdots \boldsymbol{b}_{52}^{\boldsymbol{i}} \times 2^{-52}$$

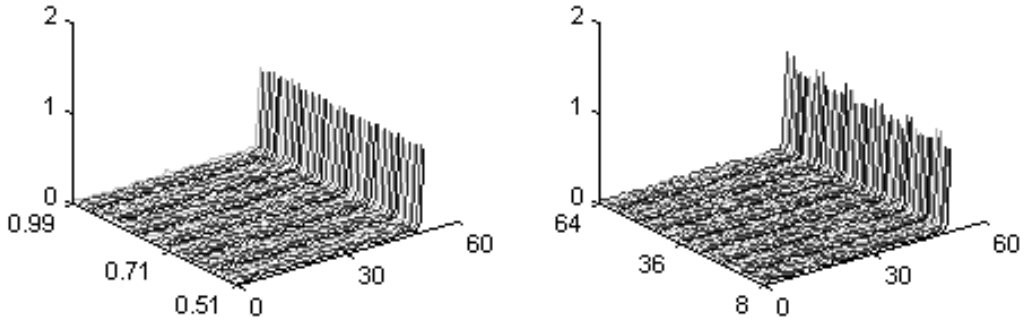
So that, it can generate a bit sequence $\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}\}$, j=1, 2, …, 52.

If the bit sequence $\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}\}$ has a uniform distribution property, namely, $P\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}=0\}= P\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}=1\}$, the bit sequence $\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}\}$ will have ideal balance property. N_1 and N_0 are the number of '1' and '0' of the sequence respectively, N is the length of the sequence, the degree of balance of the bit sequence is defined as:

$$E=\frac{|\boldsymbol{N}_1-\boldsymbol{N}_0|}{\boldsymbol{N}}$$

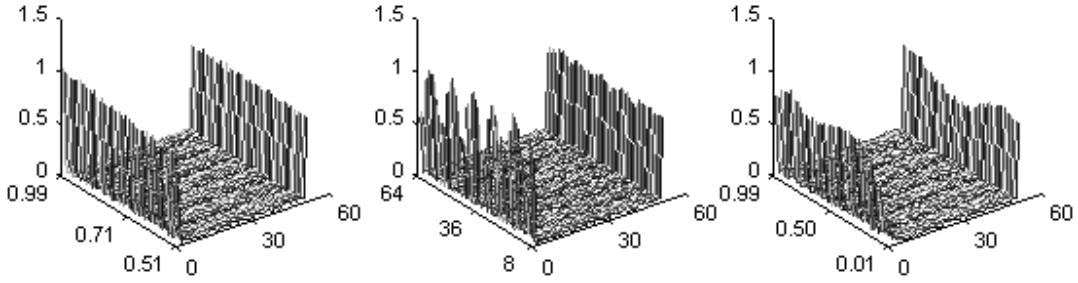
The smaller the E is, the better the balance will be.

Give N=999, the degree of the bit sequence generated by CML and CML-UD is calculated. The result of the calculation is illustrated in Fig. 14 and Fig. 15. In Fig. 14 (a), parameter α ranges from 0.51to 0.99, step length is 0.01, coordinate of lattice point i=8. In Fig. 14 (b), i ranges from 8 to 64, step length is 1, α=0.61. In Fig. 15 (a), α ranges from 0.51 to 0.99, step length is 0.01, coupling coefficient ε=0.9, coordinate of lattice point i=8. In Fig. 15 (b), i ranges from 8 to 64, step length is 1, coupling coefficient ε=0.9, α=0.61. In Fig. 15 (c), coupling coefficient ε ranges from 0.01 to 0.99, step length is 0.02, i=8, α=0.61. From the result of the experiment we can see, in the case of CML-UD, the balance of bit sequence $\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}\}$ is better when j=1, 2, …, 51, and it becomes worse when j=52, well, in the case of CML, the balance of bit sequence $\{\boldsymbol{b}_{\boldsymbol{j}}^{\boldsymbol{i}}\}$ is better when j=5, 6,…., 51, and it is worse when j=1, 2, 3, 4 and 52. Both of the balance of the last 1-bit are bad in two kinds of models, and it is caused by the carry mechanism of real number of computer calculation. For comparison, the first 4 (when j=1, 2, 3, 4) sequences have more differences with each other which are generated by CML and CML-UD respectively.



（a）α：0.51:0.01:0.99 *i*=8 （b）*i*：8:1:64 α=0.61

Figure 14. Balance of CML-UD bit sequence.



（a）α：0.51:0.01:0.99 ε=0.9 *i*=8 （b）*i*：8:1:64 α=0.61ε=0.9 （c）ε：0.01:0.02:0.99 α=0.61 *i*=8

Figure 15. Balance of CML bit sequence

H. Run-length property

The phenomenon that a number of same bits (0 or 1) present continuously is called run, and the number of 1 or 0 in a run is run-length. For a random two-value sequence, both of the number of 1 runs and the 0 runs are 50% in total, the appearing probability of a run with the run length i is 2^{-i}.

Tab. Ⅱ gives the mean value of the run-length distribution proportion of the bit sequence generated by two models. In the experiment, given the sequence length 2048 bits, the system size L=8, the coupling coefficient ε=0.9, the parameter α=0.61. The result shows that, in the sequences generated by the CML model, 1st, 2nd, 3rd and 52nd bit sequences are different from the theoretical value, the others are close to it, while, in the case of CML-UD, all sequences are close to the theoretical value except the 52nd bit sequence.

V. ANALYSIS ON SENSITIVITY OF INITIAL VALUE

To reflect the initial value sensitivity of the CML-UD, we select 100 groups of initial vectors $\boldsymbol{X}_0=[x_0(1),x_0(2),\ldots x_0(L)]$ for determination. δ is defined as the variation of $x_0(1)$. After n times of iteration, the initial vector $\boldsymbol{X}_0=[x_0(1),x_0(2),\ldots x_0(\mathrm{L})]$ generate the lattice vector $\boldsymbol{X}_n=[x_n(1),x_n(2),\ldots x_n(L)]$, and, the lattice vector $\hat{\boldsymbol{X}}_n=[\hat{x}_n(1),\hat{x}_n(2),\ldots,\hat{x}_n(L)]$ is generated by the initial vector $\hat{\boldsymbol{X}}_0=[x_0(1)+\delta,x_0(2),\ldots x_0(\mathrm{L})]$. Given L=8, select 50 bits in the front of mantissa from every components of $\boldsymbol{X}_n$ and $\hat{\boldsymbol{X}}_n$ to generate a 400 bits sequence $\boldsymbol{B}$ and $\hat{\boldsymbol{B}}$ respectively. $\overline{B}$ is defined as the mean value of the changed bits between B and $\hat{\boldsymbol{B}}$ corresponding to δ. If the value of $\overline{B}$ is close to 200, we consider that the system is high sensitive to δ after n times of iteration. The experiment result of δ- $\overline{B}$ relationship is illustrated in the Fig. 16, because of the symmetry of the model, we will get the same result with different initial value components.

Fig. 16 gives the experiment result of CML model and CML-UD model respectively. In order that corresponding to $\delta_{(x0(1))}$ the sensitivity of the model can reach the 10^{-16} order of magnitude (according to the standard IEEE-754, it is the highest sensitivity we can reach in the condition of double precision), The CML model needs 80 times of iteration, while the CML-UD needs 30. With the minish of the iteration times r, the sensitivity of the key will decline obviously, but, in the case of CML-UD, the diffusion speed of initial value variation is much higher, it shows that the initial value sensitivity of CML-UD model is better than that of CML model obviously.

TABLE II.
MEAN VALUE OF THE RUN-LENGTH DISTRIBUTION PROPORTION

Name of sequence	*type*	*proportion*				
		1 run-length	2 run-length	3 run-length	4 run-length	5 run-length
CML-PRNS	1-bit	0.8081	0.1798	0.0106	0.0014	0.0000
	2-bit	0.6146	0.1692	0.1147	0.0421	0.0266
	3-bit	0.5117	0.2265	0.1376	0.0551	0.0285
	4-bit	0.4985	0.2582	0.1208	0.0572	0.0323
	5-bit	0.5054	0.2418	0.1282	0.0654	0.0309
	51-bit	0.5055	0.2474	0.1201	0.0633	0.0300
	52-bit	0.2808	0.2221	0.1451	0.1045	0.0658
CML-UD-PRNS	1-bit	0.4988	0.2503	0.1274	0.0601	0.0326
	2-bit	0.4946	0.2543	0.1253	0.0636	0.0309
	5-bit	0.4989	0.2506	0.1248	0.0642	0.0316
	51-bit	0.4976	0.2473	0.1285	0.0637	0.0314
	52-bit	0.2767	0.2069	0.1447	0.1059	0.0730
theoretical value		0.5000	0.2500	0.1250	0.0625	0.0312

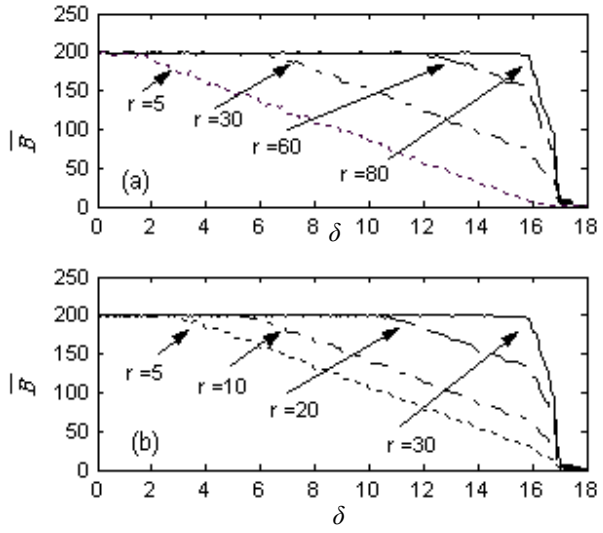


Figure 16. δ- $\overline{B}$ relationship, the horizontal coordinate is the negative log of the initial value variation, the longitudinal coordinate is the $\overline{B}$ value, r is the times of iteration. (a) result of CML model, r is 5, 30, 60, 80. (b) result of CML-UD, r is 5, 10, 20, 30

VI. CONCLUSION

Security of encryption algorithms rests with its weakest index. That is so called "Cask Effect". In some typical chaotic system under research, their system performance indexes have great changes along with the change of parameter, even there are some poor performance indexes. Therefore, in practice, it is very difficult to avoid the existence of some weak keys. CML-UD overcomes these problems. In addition to have a large maximum Lyapunov exponent, it is also very stable when the parameters change, and the correlation of its sequence is almost not affected by the change of parameters. These properties greatly improve the security of the system in the cryptography application. CML-UD is featured with uniform distribution, easy to calculate, high computation efficiency, which makes it suitable of the design for sequential cipher and Hash function.

REFERENCES

[1] Shujun Li, Xuanqin Mou, et al. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Computer Physics Communications, 2003, 153:52-58.

[2] YI X. Hash function based on chaotic tent maps[J].IEEE transactions on circuits and systems-α:Express briefs,2005,52 (6):354-357.

[3] S.Behnia, A.Akhshani, S.Ahadpour, H.Mahmodi, A.Akhavan. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Physics Letters A 2007, 366:391-396.

[4] Di Xiao, Xiaofeng Liao, Shajiang Deng. One-way Hash function construction based on the chaotic map with changeable- parameter. Chaos, Solitons and Fractals, 2005,24:65-71.

[5] Jin Chen-Hui, Yang Yang. A Divide-and-Conquer Attack on Self-Synchronous Chaotic Ciphers[J]. Acta Electronica Sinica, 2006, 34(7): 1337-1341 (in Chinese).

[6] Yang W M. Spatiotemporal Chaos and coupled Map Lattice. Shanghai: Shanghai Scientific and Technological Education Publishing House, 1994 (in Chinese).

[7] Li P, Li Z, Halang W A, Chen G R. Analysis of a multiple-output pseudo-random-bit generator based on a spatiotemporal chaotic system[J]. International Journal of bifurcation and chaos, 2006, 16 (10): 2949-2963.

[8] Liu Jian-Dong, Fu Xiu-li. Spatiotemporal Chaotic One-Way Hash Function construction based on Coupled Tent Maps[J]. Journal on communications, 2007, 28 (6): 30-38 (in Chinese).

[9] Sheng L Y, Sun K H, Li C B. Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties, *Acta Phys. Sin.* 2004,53 (9)**:** 2871-2877 (in Chinese).

[10] Sheng L Y, Xiao Y Y, A universal algorithm for transforming chaotic sequences into uniform pseudo-random sequences, *Acta Phys. Sin.* 2008, 57 (7)**:** 4007-4013 (in Chinese).

[11] Wang Yong. Research on Chaos Based Encryption Algorithm and Hash Function Construction[D], Chongqing: Chongqing University, 2007 (in Chinese).

[15] National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS 180-2, August 2002.

[16] Lai Jianwen, Zhou shiping, Li Guohui, Xu Deming, a method for computing lyapunov exponents spectra without reorthogonalization, Acta Phys. Sin, 2000, 49 (12): 2328-2333

[12] Qin Honglei, LinXiaobai. A chaotic search method for global optimization on tent map, Electric machines and control, 2004, 8 (1): 67-70.

[13] Zhou Hong, Ling Xie-Ting, Realizing finite precision chaotic systems via perturbation of m-Sequences[J]. ACTA Electronica Sinica. 1997, 25 (7): 95-97.

[14] Shihong Wang, Weirong Liu, Gang Hu, Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. International journal of modern physics B, 2004, 19: 2617-2622.

LIU Jian-Dong , born in 1966 , He has been professor of Beijing Institute of Petro-chemical Technology since 2008. His main research interests are chaos cryptography and information hiding.