A Spatiotemporal Chaotic System Based on Pseudo-Random Coupled Map Lattices and Elementary Cellular Automata

Youheng Dong (✉ Dyh_231@bupt.edu.cn)
Beijing University of Posts and Telecommunications https://orcid.org/0000-0002-5658-096X
Zhao Geng
Beijing Electronics Science and Technology Institute

Research Article

Keywords: Spatiotemporal chaotic system, Elementary cellular automata, Coupled map lattices, Pseudo-random coupling, Crypto-system

Posted Date: March 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-218822/v1

A spatiotemporal chaotic system based on pseudo-random coupled map lattices and elementary cellular automata

Dong You-Heng

School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China

Tel.: +86-18810399628

E-mail: Dyh_231@bupt.edu.cn

Zhao Geng

Beijing Institute of Electronic Science and technology, Beijing 100070, China

E-mail: zg@besti.edu.cn

Article Note This research is supported by the National Natural Science Foundation of China (Nos: 61772047, and 6164021).

Declarations No conflict of interest exists in the submission of this manuscript, and the manuscript is approved by all authors for publication. I would like to declare on behalf of my co-authors that the work described was original research that has not been published previously, and not under consideration for publication elsewhere, in whole or in part. All the authors listed have approved the manuscript that is enclosed.

Abstract The coupled map lattices (CML) is a spatiotemporal chaotic system with complex dynamic behavior. In this paper, we propose a spatiotemporal chaotic system with a novel pseudo-random coupling method based on the elementary cellular automata (ECA), and add different perturbations to lattices in each iteration according to ECA. We investigate the spatiotemporal dynamic properties and chaotic behaviors of the proposed system such as bifurcation diagrams, Kolmogorov-Sinai entropy density, and universality. Moreover, the correlation between any two lattices is discussed. Theory analysis and simulation test indicate that the new system has better performance in complexity, ergodic and unpredictability than conventional CML systems such as adjacent CML and mixed linear-nonlinear CML. Furthermore, the correlation coefficient between any two lattices in proposed system is significantly lower than other systems, and another advantage of the proposed system is utilizing the output of ECA to perturb the chaotic system which can effectively alleviate the dynamical degradation in digital system. The excellent performance of proposed system demonstrates that it has great potential for crypto-system.

Keywords *Spatiotemporal chaotic system; Elementary cellular automata; Coupled map lattices; Pseudo-random coupling; Crypto-system*

CML: Coupled Map Lattices;

ECA: Elementary Cellular Automata;

PRCML: Pseudo-random Coupled Map Lattices;

LE: Lyapunov exponent;

NIST: National Institute of Standards and Technology;

MLNCML: Mixed Linear-nonlinear Coupled Map Lattices;

LDCML: Logistic-dynamic Mixed Linear-nonlinear Coupled Map Lattices.

1 Introduction

In the past decades, the chaotic system has become a research hotspot in nonlinear systems. Since the chaotic system which is a deterministic system possesses many particular dynamical properties such as ergodicity, unpredictability, pseudo-randomness and initial sensitivity, etc. [1-6], it has been utilized in many fields, including mathematics [7-8], biology [9-10], physics [11-12], cryptology [3-5, 13-14], and even social science [15-16]. Nevertheless, dynamical degradation will occur when the chaotic system operates in digital computers with finite computing precision [17]. Due to the inherent drawback that digital chaos systems have, quite a few schemes have been proposed to alleviate the dynamical degradation: using higher precision digital system [18], cascading multiple chaotic systems [19-20], randomly perturbing the chaotic systems [21]. According to the theoretical analysis in literature [17], the best of the above-mentioned scheme is randomly perturbing the system. And the most effective perturbation-based solution is perturbing the output of iteration in the chaotic system, hence it attracts much more attention than other solutions [22-24]. In literature [25-27], the authors use the delay-introducing method as a novel solution to improve the dynamical degradation. It's essentially perturbing the control parameter. In other words, comparing with perturbing the output of iteration the effect of this approach is limited.

The above-mentioned schemes for alleviating dynamical degradation are low-dimensional chaos systems. Unfortunately, they are vulnerable to attacks based on the phase space reconstruction for crypto-system [28]. In recent years, as the international research on chaotic systems goes further, high-dimensional chaotic systems have attracted more attention, especially the spatiotemporal chaotic systems [3-5, 13-14] which not only can efficiently alleviate the dynamical degradation but also possess a larger Lyapunov exponent (LE) and more complex dynamical performance[3]. Since the coupled map lattices (CML) [29-30] as an enlightening technique was proposed in 1985 [31], lots of spatiotemporal chaotic systems based on CML are investigated. According to coupling methods, the spatiotemporal chaotic systems can be classified into three categories [4]: spatial adjacent coupling, spatial random coupling, spatial nonlinear coupling. Although the first category is the most popular scheme that regards the output of adjacent lattices as interference to the current lattice [3, 14, 32-33], the periodic windows still exist in its bifurcation diagrams which signify that the ergodicity of the system is broken, and the correlation between the output sequences of different lattices is very high that obviously increases the security risk to crypto-system[13]. The spatial random coupling efficiently reduces the above-mentioned correlation, but it has a fatal flaw for a crypto-system that the sequences generated by such system can't be reproduced [5]. It means that the spatiotemporal chaotic system based on the spatial random coupling just suits for a pseudo-random numbers generator rather than a crypto-system. As for the spatial nonlinear coupling, it takes into account the complexity and reproducibility of the spatiotemporal chaotic systems. Zhang et al. [4-5] developed a nonlinear coupling based on the Arnold cat map [34], and found that the systems they proposed possess new chaotic features which are superior to the conventional CML. It was subsequently employed in image encryption [1-2]. They demonstrated the effectiveness, feasibility and security of the CML based on nonlinear coupling for crypto-system. However, the randomness of the sequences generated by the system was not tested by the NIST SP800-22 suite [35] which is used as an important standard for judging whether the sequences possess random performance. Moreover, according to the analysis in literature [36-38], Arnold cat map has the characteristic of periodicity that brings potential flaws for the system.

To remedy the aforementioned problems, a novel pseudo-random CML (PRCML) system with perturbation is proposed in this article, which not only has the advantages of above-mentioned schemes but also significantly reduces the correlation between the sequences generated by any two different lattices. Moreover, the sequences generated by the proposed spatiotemporal chaotic system have passed the NIST test that proves the outstanding randomness of our scheme. The main contributions of this paper are as follows:

Without loss of generality, the logistic map is used as the iterative function of each lattice. And rather than employing the adjacent lattices for coupling as a conventional CML, the PRCML's choice of lattices for coupling is innovatively dependent on the iterative result of the ECA which can be chaotic or complex [39-41]. Thus, the dynamical degradation is effectively mitigated. Moreover, because of the chaotic character of ECA, the periodicity as Arnold cat map is avoided.

The iterative result of the ECA is employed for disturbing the PRCML which leads to the following advantages: Firstly, the periodic windows in bifurcation diagram fade out obviously. Secondly, dynamical degradation is further alleviated according to literature [17]. Thirdly, owing to the different pseudo-random perturbation for each lattice, the correlation between any two lattices is significantly reduced. Above all, the perturbation based on the ECA improves the ergodicity, unpredictability and complexity of the PRCML which is more suitable for crypto-system.

The remaining part of this paper is organized as follows. In Sect. 2, the preliminary knowledge about CML and ECA is introduced, and the PRCML with perturbation is presented in Sect. 3. Then, simulation results and performance analyses are reported in Sect. 4. Finally, the conclusion is drawn in Sect. 5.

2 Preliminaries

2.1 Coupled map lattices system

Coupled map lattices system is a spatiotemporal chaotic system that can alleviate the dynamical degradation and enhance the complexity of digital chaotic system. In the CML system, the current lattice is determined by the two adjacent coupling lattices, which is defined as Eq. (1):

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

where n (n = 0, 1, 2, …) is the number of iterations and ε ($0 \leq \varepsilon \leq 1$) is the coupling coefficient which represents the strength of coupling. i (i = 1, 2, …, L) is the index of current lattice, and L is the total number of lattices in the system in which Lth lattice is regarded as the left adjacent lattice of the 1-th. In generally, $f(x)$ is the logistic map as follows:

$$f(x) = \mu x(1-x), x \in (0,1) \tag{2}$$

where μ ($0 < \mu \leq 4$) is the control parameter. When μ is in interval [3.6, 4], the system is chaotic.

2.2 Elementary cellular automata

The Cellular automata (CA) was proposed by Stanislaw M. Ulam and John von Neumann in 1948 [42], which was initially utilized for simulating the self-reproduction of bio-systems. And it was also a simplified mathematical model of complex phenomena in nature.

The CA is made up of the cell, cell-space, neighbor and rule that can be defined as follows:

$$CA = (A^N, \Sigma, f, E), \tag{3}$$

where A^N represents cell-space, and N is the dimension of cell space. $\sum$ is the set of cell states. f is local transition rule. E denotes the boundary condition of CA.

As for the elementary CA (ECA), it's a special one-dimension CA in which the number of cell states is 2. And the set of cell states $\sum$ can be represented as {0, 1}. The radius of cellular automata is 1 which means that the neighbors of current cell are the adjacent two cells. And the boundary condition of ECA is cyclic boundary condition which is shown as Fig. 1.

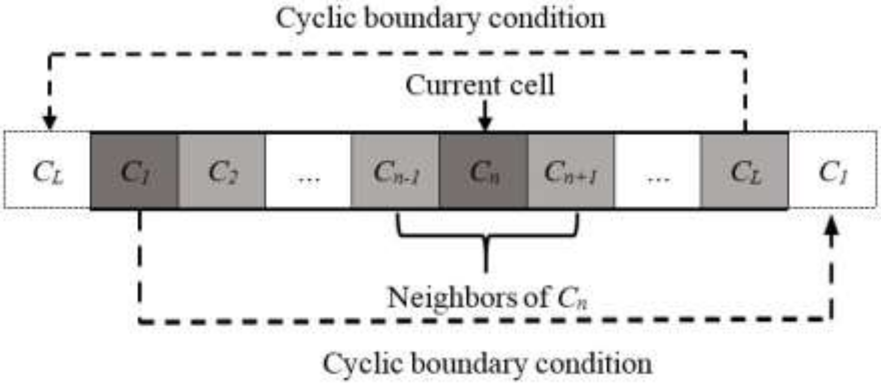


Fig. 1 Organization form of ECA

In Fig. 1, L is the total number of cells. C_{n-1} and C_{n+1} are neighbors of C_n (n = 1, 2, …, L). And according to the cyclic boundary condition, C_L is the left neighbor of C_1, and C_1 is the right neighbor of C_L. In the ECA, the next state of a cell is absolutely determined by the current states of itself and its two neighbors that is expressed as Eq. (4).

$$S_i^{t+1} = f(S_{i-1}^t, S_i^t, S_{i+1}^t), \tag{4}$$

in which S_i^t is the current state of i-th cell which can be represented as "0" or "1", t is the number of iterations, and i is the index of cells. f is the local transition rule that is essentially a mapping from the set {000, 001, 010, 011, …, 111} to the set {0, 1}, and it is easy to know that there are 256 ECAs. For instance, the local transition rule of ECA *No.* 105 is shown in Table 1.

Table 1 The local transition rule of ECA *No.* 105

$S_{i-1}^t, S_i^t, S_{i+1}^t$	111	110	101	100	011	010	001	000
S_i^{t+1}	0	1	1	0	1	0	0	1

The dynamical behaviors of the ECA with different local transition rules are substantially dissimilar. According to the research on the classification of CA [39, 41], the ECA can be classified into four categories: fixed, cyclic, chaotic, complex. In this paper, the chaotic ECA is employed for assisting in building PRCML. *No.* 105 belongs to the chaotic ECAs. Set the initial status value of ECA *No.* 105 to a random binary number which is 100 bits, *L*=100, *t*=100, then the iterative result of ECA *No.* 105 is shown as Fig. 2, in which the black(white) lattice represents the cell with the status value "1" ("0"). It is obvious that the iterative result is pseudo-random, aperiodic, etc.

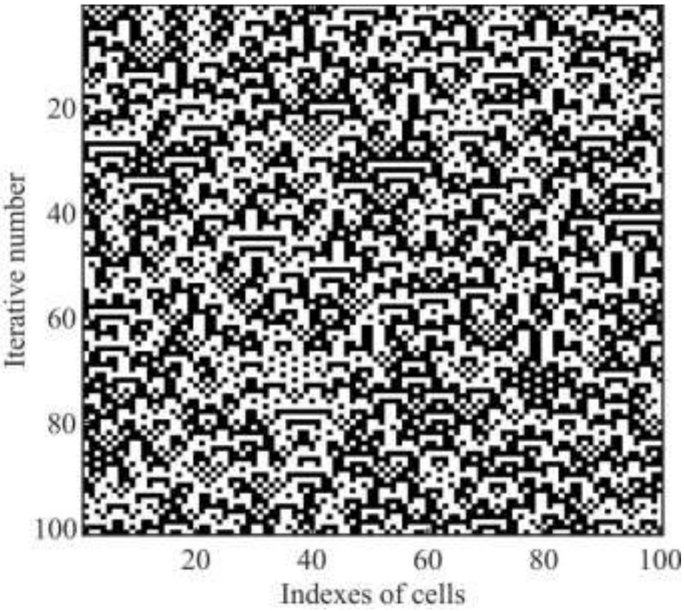


Fig. 2 Iterative result of ECA *No.*105

3 The proposed pseudo-random CML system with perturbation

The proposed system coupled by pseudo-random links as follows:

$$x_{n+1}(i) = \left\{ (1-\varepsilon) f[x_n(i)] + \frac{\varepsilon}{2}\{ f[x_n(a)] + f[x_n(b)] \} + 0.5 \times p(S^n) \times \delta(s_i^n) \right\} \bmod 1, \quad (5)$$

where $f(x)$ represents the logistic map as Eq. (2). ε is the coupling coefficient. i (i = 1, 2, …, L) denotes the index of the current lattice, and L is the total number of lattices, L = 100 in proposed system. n (n = 0, 1, 2, …) is the number of iterations. a and b are the indexes of lattices for coupling, which are defined by the ECA as follows:

$$[a, b] = search(S^n, i), \quad (6)$$

in which S^n is the iterative result of the ECA as Eq. (4), n is the number of iterations in Eq. (5). And the total number of cells is 100 in the proposed system. i is the index of current lattices in Eq. (5). $search(S^n, i)$ is a function for finding two cells, the status value of which must be "1", and they are the nearest two of the i-th cell in S^n. The return values of $search(S^n, i)$ are the indexes of above two cells. For example, the process of this function is shown as Fig. 3.

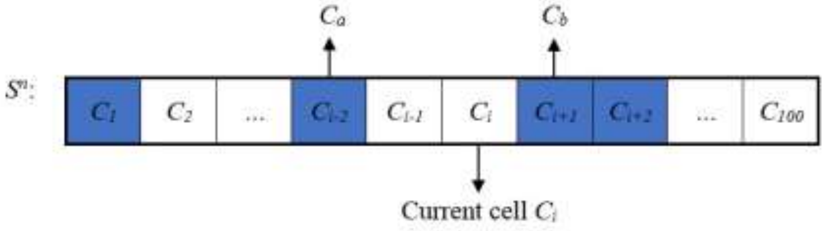


Fig. 3 The function $search(S_n, i)$

In Fig. 3, the blue(white) lattice represents the cell with the status value "1" ("0"), and according to the function *search*, it can be acquired that $a = i - 2$, $b = i + 1$.

As for $p(S^n)$ in Eq. (5), it is the function to calculate the perturbation. S^n can be regarded as a binary number $S^n = b_1 b_2 b_3 \dots b_{100}$, and b_i denotes the status value of C_i. The middle 32 bits of S^n are employed for perturbing the proposed system. $p(S^n)$ is calculated as

$$p(S^n) = \frac{bin2dec[S^n(b_{35}b_{36}\mathrm{L}\ b_{66})]}{2^{32}-1}, \quad (7)$$

where *bin2dec*(•) is a function that converts a binary number to a decimal number. Apparently, $p(S^n)$ is in interval [0, 1]. $\delta(s_i^n)$ is a function to determine the sign of perturbation, in which s_i^n is the status value of C_i in S^n. $\delta(s_i^n)$ is acquired by follows:

$$\delta(s_i^n)=\begin{cases} 1, & s_i^n=1 \\ -1, & s_i^n=0 \end{cases}, \tag{8}$$

and the operation *x mod* 1 is to preserve the fractional part of *x*, which ensures that the result of Eq. (5) is always in the interval (0, 1).

4 The dynamic properties of PRCML system

For comparison analysis, the control parameters and initial value of PRCML system are set as follows: $\mu \in (3, 4]$, $\varepsilon \in (0, 1]$. The initial value of logistic map $x_0(1)$ is set to 0.05, and this map is iterated for 99 times to initialize each lattice $x_0(1)$, $x_0(2)$, …, $x_0(100)$. A random number of 100 bits is employed for initializing the S_i^0 (i = 1, 2, …, 100). In this article, S^0 is set to:

$$S^0 = 2CED\_3DF5\_0D18\_E315\_7C54\_4F69\_D0, \tag{9}$$

where S0 is represented as a hexadecimal number. And No. 105 is selected as the local transition rule of the ECA, which insures that the ECA is chaotic, aperiodic and pseudo-random.

The CML system, the mixed linear-nonlinear CML (MLNCML) system and the Logistic-dynamic mixed linear-nonlinear CML (LDCML) system [13] are chosen to compare with the proposed system. The initial values of them are set as former, and η=0.8 in the MLNCML and LDCML.

4.1 Kolmogorov-Sinai entropy

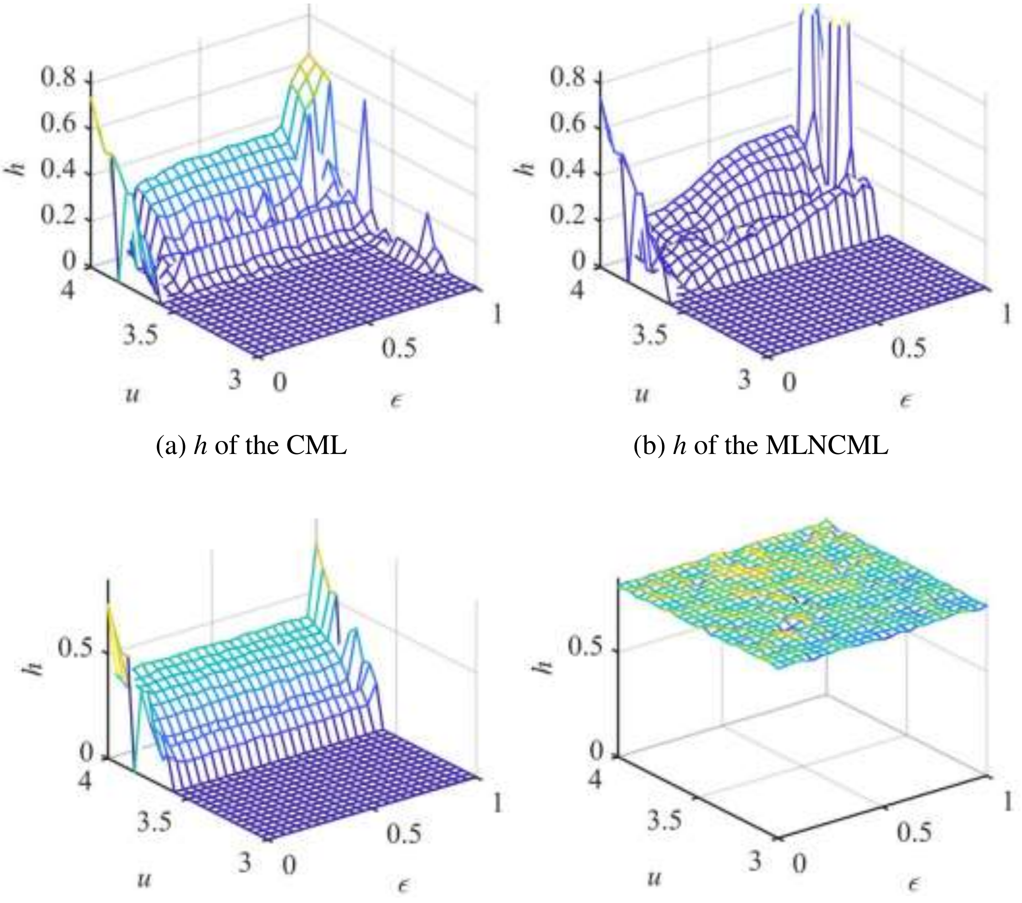
The Lyapunov exponent (LE) is an important indicator to evaluate the average exponential divergence rate of adjacent orbits in the phase space [14], which is defined as:

$$\lambda = \lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{dF(x)}{dx}\right|_{x=x_i}, \tag{10}$$

where $F(x)$ is the mathematical expression of dynamical system. A chaotic system must possess at least one positive LE, and the larger λ is, the more chaotic and complex the system is. Without loss of generality, the LEs are calculated by the wolf method [43] as many researchers do [1-3, 14]. The Kolmogorov-Sinai entropy density is the average of the positive LEs of all lattices [14], which can evaluate the entire multi-dimensional chaotic behavior. It can be described as follows:

$$h = \frac{\sum_{i=1}^{L} \lambda^{+}(i)}{L}, \tag{11}$$

where h denotes the Kolmogorov-Sinai entropy density, $\lambda^{+}(i)$ is the positive LE and L indicates the number of lattices. The positive h implies that the system is in chaos. And the larger the value is, the stronger the chaos of the system is. The results of PRCML system and other systems under different control parameters are show in Fig. 4.



(a) h of the CML

(b) h of the MLNCML

(c) h of the LDCML

(d) h of the PRCML

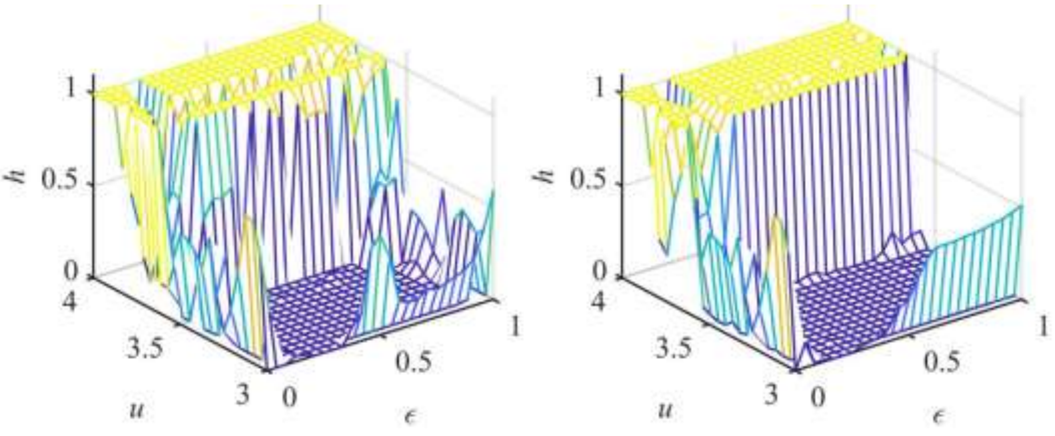
Fig. 4 The Kolmogorov-Sinai entropy density

Generally speaking, it's obvious that the Kolmogorov-Sinai entropy densities of CML, MLNCML and LDCML systems are below 0.5 under the most control parameters according to Fig. 4(a)-(c). Correspondingly, the PRCML system's reaches 0.8 in Fig. 4(d), which is markedly higher than any of the above systems. It's verified that the chaotic characteristic of PRCML system is much better. Specifically speaking, as shown in Fig. 4(a)-(c), only when μ >3.6 can the former three systems be in chaos, and the chaotic property is sensitive to the control parameter μ because that the Kolmogorov-Sinai entropy densities increase as μ rises. Furthermore, h is lower around $\varepsilon = 0.2$ in Fig. 4(a)-(b), which indicates that the chaos of CML and MLNCML system is weak when coupling coefficient is around 0.2, and the LDCML system effectively overcomes this drawback as shown in Fig. 4(c). Fortunately, the PRCML system not only avoids above weakness but also has the higher Kolmogorov-Sinai entropy density in entire interval $\mu \in (3, 4]$ and $\varepsilon \in (0, 1]$. It means that the range of control parameters which lead to chaotic behavior is wider than former three systems.

The Kolmogorov-Sinai entropy universality is another important indicator to evaluate the chaotic behavior in spatial level, which is defined as follow:

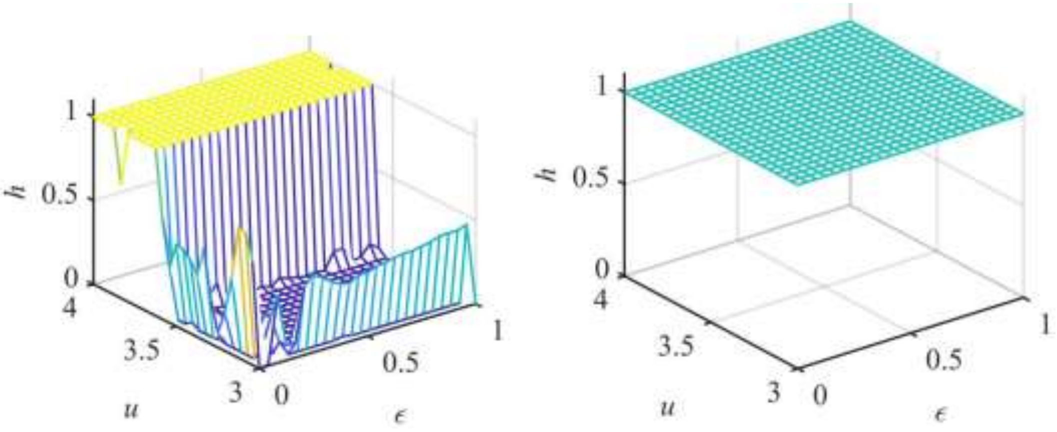
$$hu = \frac{L^{+}}{L}, \tag{12}$$

in which L^{+} is the number of lattices with positive LEs in the spatiotemporal chaotic system, and L denotes the total number of lattices. Apparently, hu indicates the percentage of lattices which is in chaos. The Kolmogorov-Sinai entropy universality of above-mentioned systems is illustrated in Fig. 5.



(a) *hu* of the CML

(b) *hu* of the MLNCML



(c) *hu* of the LDCML

(d) *hu* of the PRCML

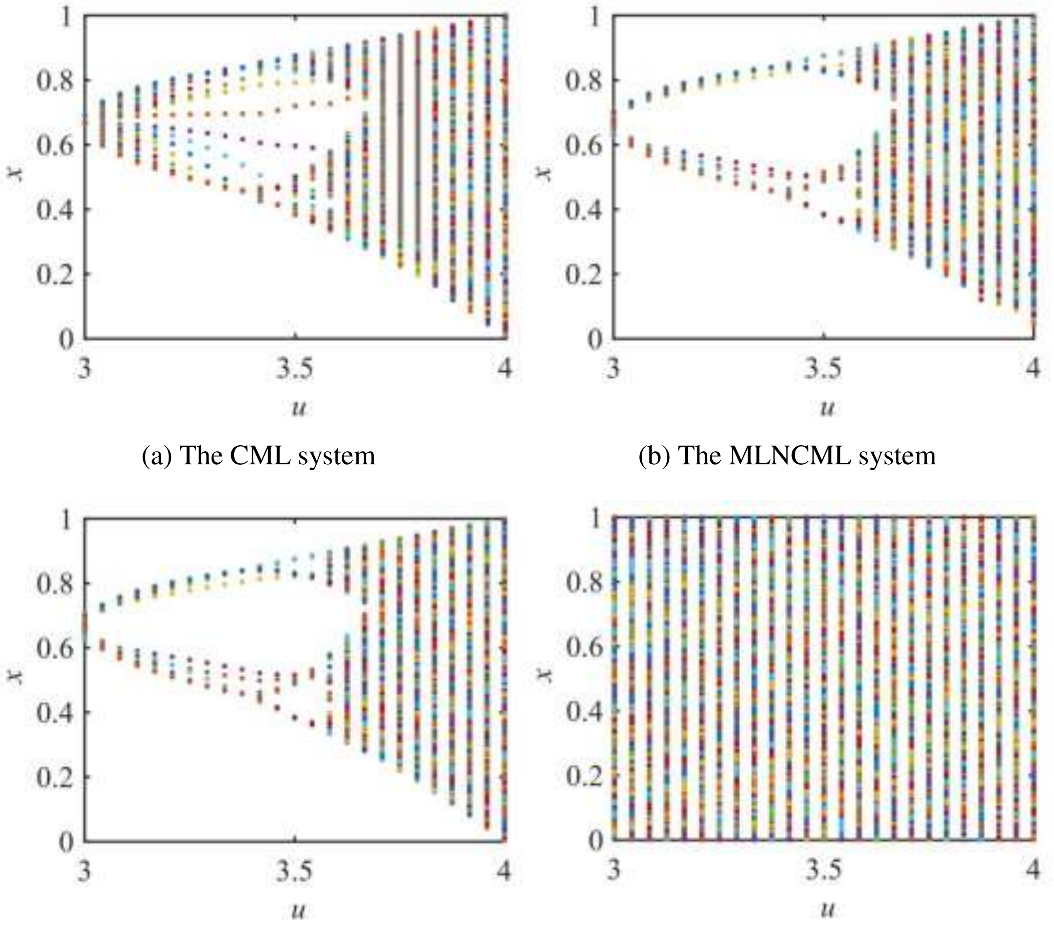
Fig. 5 The Kolmogorov-Sinai entropy universality

Corresponding to the Kolmogorov-Sinai entropy density, the percentage of chaotic lattices reaches 100% only in μ >3.6 according to Fig. 5(a)-(c), and a low percentage of lattices is in chaos around $\varepsilon = 0.2$ in Fig 5.(a)-(b). In other words, the number of parameter pairs (ε , μ) which lead to extensive chaotic behavior is limited in the CML and MLNCML systems. Although the weak chaos around $\varepsilon =$ 0.2 is improved in LDCML, lots of lattices is not in chaos when μ < 3.6. Fortunately, the situation has been greatly improved in the PRCML system as shown in Fig. 5(d), from which it's easy to know that all lattices are chaotic in entire interval $\mu \in (3, 4]$, $\varepsilon \in (0, 1]$.

In conclusion, the PRCML system possesses stronger chaotic property, and it contains more parameter pairs which lead to chaos. That is, the proposed system provides wider secret key space in parameter (ε , μ) than others so that it is more suitable for building a crypto-system.

4.2 Bifurcation diagram

The befurcation diagram evaluates the periodicity and ergodicity of the systems. For comparison analysis, we assign ε =0.625 and select the lattice No.50 as the example. The bifurcation diagrams of above-mentioned systems are shown in Fig. 6.



(a) The CML system

(b) The MLNCML system

(c)The LDCML system

(d) The PRCML system

Fig. 6 The bifurcation diagram

According to Fig. 6(a)-(c), the CML, MLNCML and LDCML systems all have periodic windows when μ <3.6, and the aperiodicity of CML system is even better than the latter two systems. Furthermore, it’s obvious that although the system is in chaos when μ >3.6, the iterative results traverse the entire interval [0,1] only when μ =4. By contrast, as shown in Fig. 6(d), the periodic windows have almost disappeared in the PRCML system, and the ergodicity of it is also better than the former three systems because the iterative results can traverse the entire interval in $\mu \in (3, 4]$.

For describing the PRCML system at large, we extend the parameter μ to the interval [0, 4], and the bifurcation diagram is shown as follow:

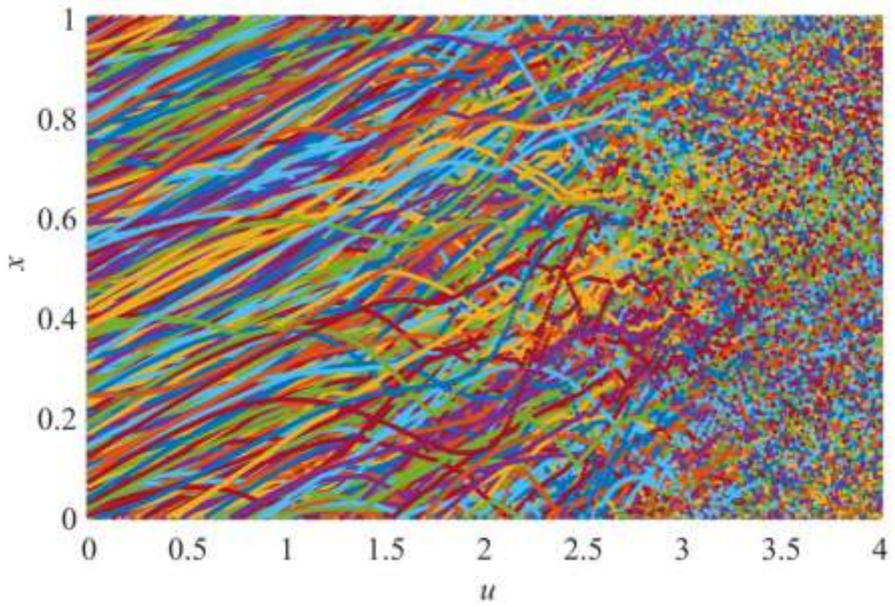
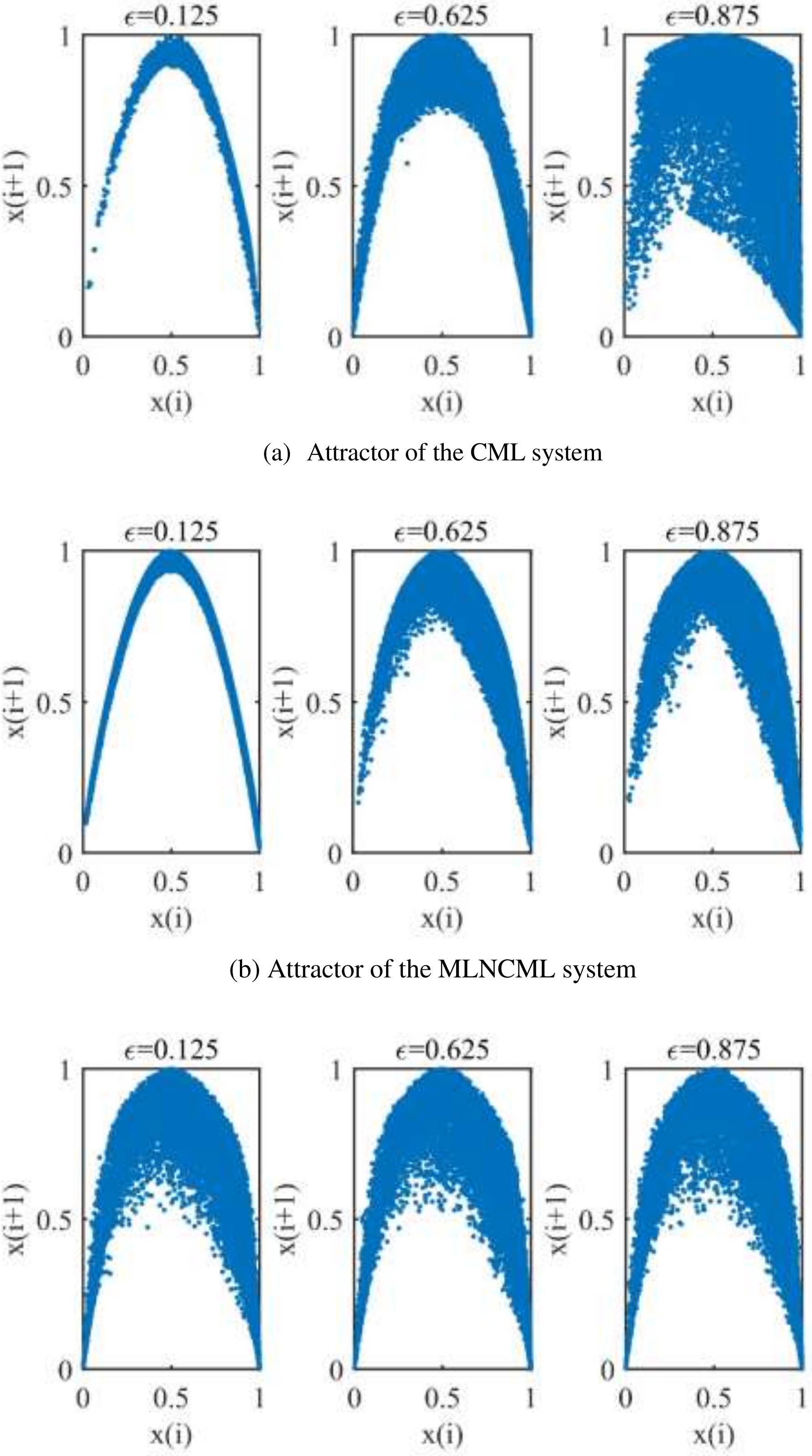


Fig. 7 The bifurcation diagram of PRCML system

As shown in Fig. 7, the diagram can be divide into three parts by $\mu = 1$ and $\mu = 2.5$. Approximately parallel orbits can be recognized in part one $0<\mu < 1$, and the aperiodicity and ergodicity of systems are provided by the ECA. With the increasing of μ, the bifurcations and overlap between orbits begin to occur as shown in interval $\mu \in (1, 2.5)$. There are two reasons for this situation: On the one hand, the influence of ECA always exists, which leads to the chaos. On the other hand, the period doubling bifurcation of coupled map lattices occurs in this interval. When μ>2.5, the identifiable orbits have disappeared, and because the ECA and coupled map lattices is both in chaos the PRCML system is thoroughly chaotic and turbulent.

4.3 Phase space and time-domain analysis

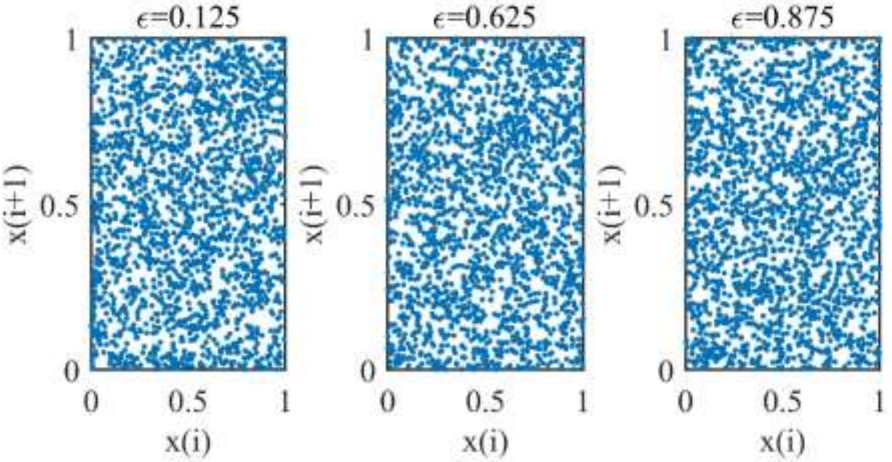
The uniformity is an important property of a chaotic system when it is employed in crypto-system. The phase space and time-domain analysis are utilized for evaluating the uniformity of the spatiotemporal chaotic system. We assign μ=4. The chaotic attractors of CML, MLNCML, LDCML and PRCML systems in phase space are listed as follows.



(a) Attractor of the CML system

(b) Attractor of the MLNCML system

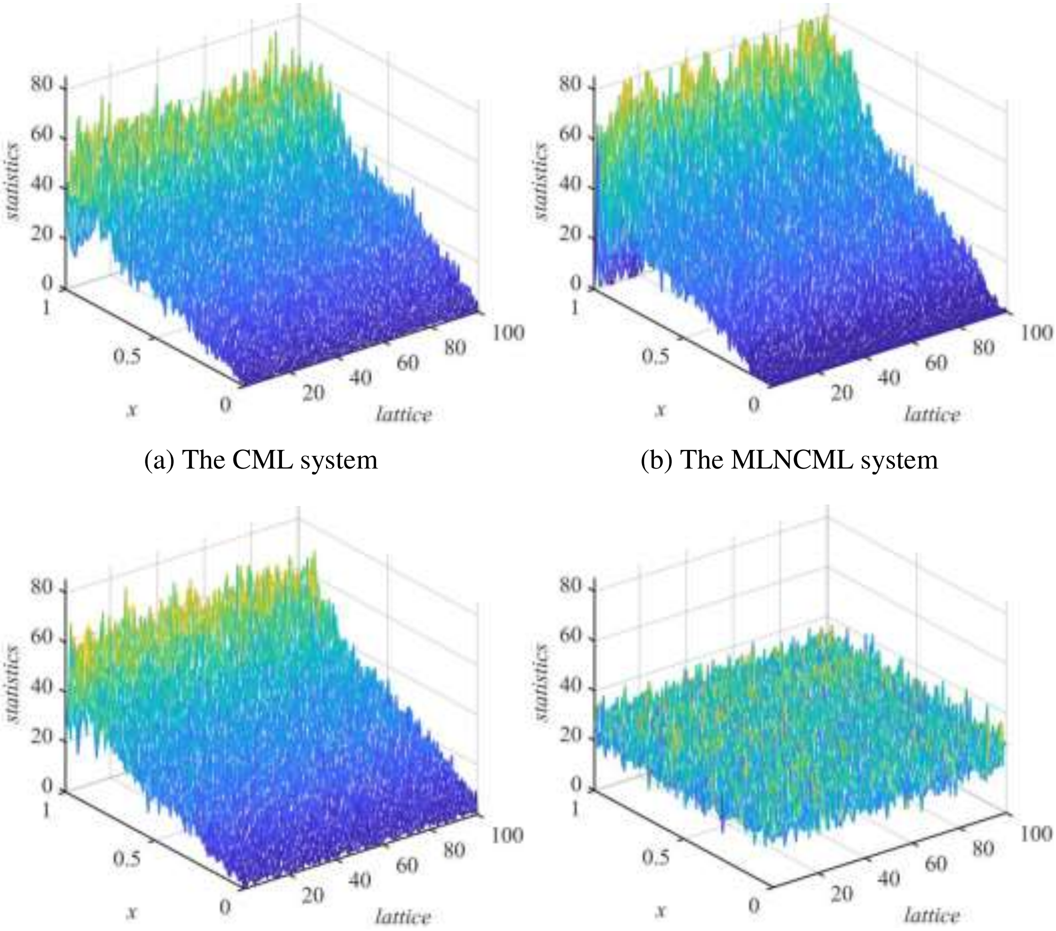
(c) Attractor of the LDCML system



(d) Attractor of the PRCML system

Fig. 8 Phase space analysis

As shown in Fig. 8(a)-(b), with the increasing of coupling coefficient ε, the point in phase space gradually disperses. However, the shape of attractor can still be identified, and it's vulnerable to attack by phase-space reconstruction in crpyto-system. The LDCML system is insensitive to the coupling coefficient, but it also possesses the above weakness as shown in Fig 8.(c). In contrast, according to Fig. 8(d), the points of PRCML system are almost uniform in phase space no matter how much the coupling coefficient is, and the phase-space reconstruction is ineffective to proposed system. Furthermore, we assign the number of iterations n=5000, ε=0.625， μ=4. And the interval [0,1] is divided into 200 segments equally. Then the number of iterative results in each segment is counted. The statistics of iterative results of every lattice in time-domain are illustrated in Fig. 9. It's obvious that the iterative results of CML, MLNCML and LDCML systems are mainly concentrated in interval [0.8, 1] as shown in Fig. 9(a)-(c). On the contrary, the iterative results of PRCML system uniformly distribute on entire interval [0, 1]. So the uniformity of proposed system is better than the former three systems.



(a) The CML system

(b) The MLNCML system

(c)The LDCML system

(d) The PRCML system

Fig. 9 The time-domain analysis

4.4 Correlation analysis

Because of the coupling in conventional spatiotemporal chaotic system, the correlation between the outputs of lattices is very high. However, the sequences generated by a same crypto-system should be uncorrelated between each other. Otherwise, the enemy can easily deduce the output of current lattice according to the outputs of other lattices. In other words, there is a serious security problem in conventional CML system when it is utilized in crypto-system. In this article, Pearson correlation coefficient of each two lattices is employed for correlation analysis, which is defined as follow:

$$r_{ij} = \frac{\operatorname{cov}(x_i, x_j)}{\sqrt{D(x_i)}\sqrt{D(x_j)}}, (i \neq j) \tag{13}$$

$$x_i = x_i - E(x_i), x_j = x_j - E(x_j), \tag{14}$$

$$E(x_i) = \frac{1}{T}\sum_{t=1}^{T} x_i^t, \tag{15}$$

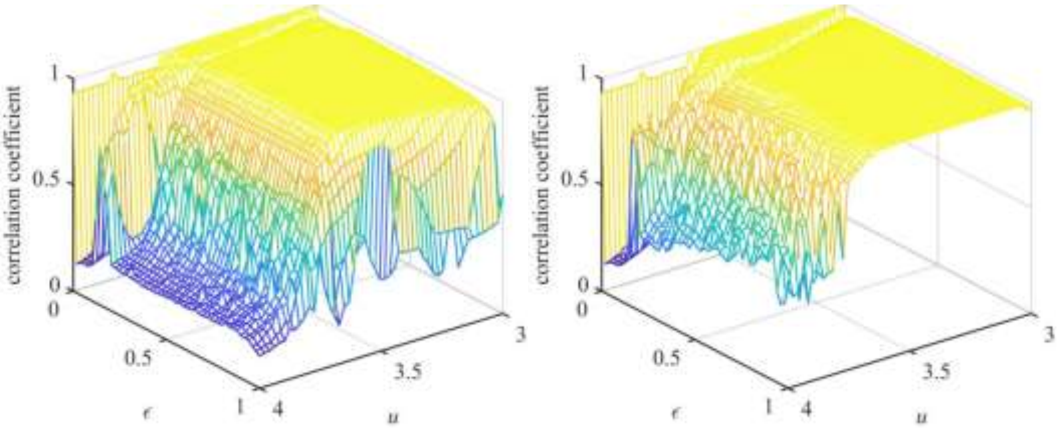
$$D(x_i) = \frac{1}{T}\sum_{t=1}^{T} (x_i^t - E(x_i))^2, \tag{16}$$

$$\mathrm{cov}(x_i, x_j) = \frac{1}{T}\sum_{t=1}^{T} (x_i^t - E(x_i))(x_j^t - E(x_j)), \tag{17}$$

Where *i*, *j* are the indexes of lattices, and *T* is the total number of iterations or the length of the sequence which is set to 500. x_i denotes the sequence generated by *i*-th lattice. E(x_i) and D(x_i) are the expectation and the variance of x_i, respectively. And due to the sequence is in interval [0, 1], positive direct component always exists in the sequences. For comparison analysis and making the difference between the correlation coefficients of sequences generated by different systems more obvious, the positive direct component of sequence should be subtracted as Eq. (14). Then the average *R*(*e*, *u*) of the r_{ij} when $\varepsilon=e$， $\mu=u$ is acquired as follow:

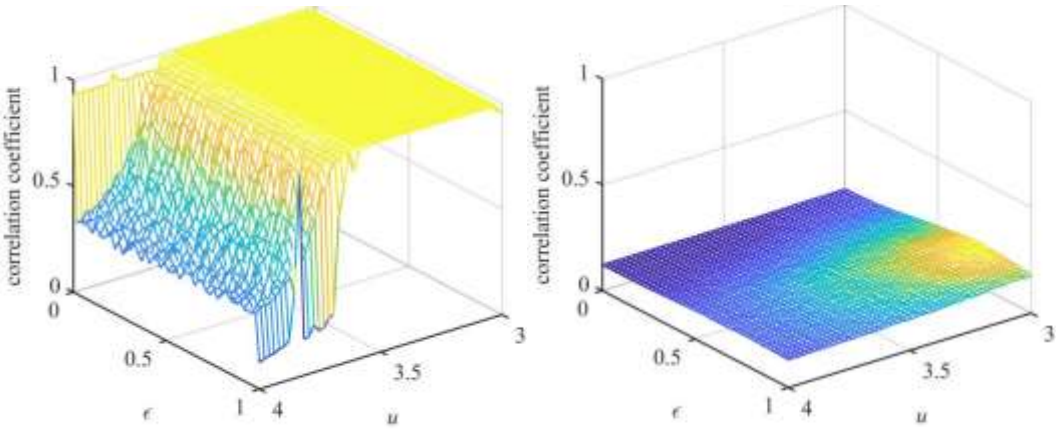
$$R(e,u) = mean(r_{ij}), i \neq j, \varepsilon = e, \mu = u, \tag{18}$$

where $e \in [0,1]$ ，$u \in [3,4]$, and the *R*(*e*, *u*) of different systems are shown in Fig. 10.



(a) The CML system

(b) The MLNCML system



(c)The LDCML system

(d) The PRCML system

Fig. 10 The correlation analysis

As shown in Fig. 10(a)-(c), the correlation coefficients decline only when μ>3.5. And under most pairs of parameters, the averages of correlation coefficients are greater than 0.2. Moreover, almost half of $R(e, u)$s are around 1, which means that the sequences generated by different lattices in CML, MLNCML or LDCML system are closely related to each other. By contrast, all of averages of correlation coefficients in Fig. 10(d) are less than 0.21. And it indicates that the sequences generated by different lattices in the PRCML system are independent of each other.

4.5 The NIST test

The NIST SP800-22 suite proposed by National Institute of Standards and Technology is the most common statistical test tool, which is employed for evaluating the randomness and unpredictability of the sequences. There are 15 sub-tests in this suite as listed in Table 2, and all of them can be utilized to estimate the randomness of the sequence. For these tests, each *P-value* is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. If a *P-value* for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A *P-value* of zero indicates that the sequence appears to be completely non-random[36]. In this paper, the significance level α is set to 0.01. If *P-value*≥ α, the sequence apears to be random, which means that the sequence would be considered to be random with a confidence of 99%. Otherwise, the sequence is non-random with a confidence of 99%. For example, we assign *μ*=4, *ε*=0.25, then select the sequence *X*(*x*(10001), *x*(10002), …, *x*(41250)) generated by lattice No. 60 for the test, which have been converted to 32bit unsigned number as follow:

$$y(t) = x(t) \times (2^{32} - 1), \tag{19}$$

where Y(y(10001), y(10002), …, y(41250)) is the sequence for the test, the length of which is 106 bits. The test results are listed in Table 2.

Table 2 Test results of NIST 800-22:

No.	Sub-tests	*P-value*	Result
1	Frequency	0.487682	Pass
2	Block frequency	0.034696	Pass
3	Runs	0.771448	Pass
4	Longest runs of ones	0.980655	Pass
5	Rank	0.732141	Pass
6	FFT	0.317188	Pass
7	Non-overlapping template matching(average)	0.470642	Pass
8	Overlapping template matching(all ones)	0.995805	Pass
9	Universal statistical	0.270091	Pass
10	Linear complexity	0.742281	Pass
11	Serial 1	0.692208	Pass
	Serial 2	0.341663	Pass
12	Approximate entropy	0.196619	Pass
13	Cumulative sums (forward)	0.771929	Pass
	Cumulative sums (reverse)	0.557029	Pass
14	Random excursions		
	x=-4	0.612169	Pass
	x=-3	0.72621	Pass
	x=-2	0.92413	Pass
	x=-1	0.158412	Pass
	x=1	0.395969	Pass
	x=2	0.078504	Pass
	x=3	0.755938	Pass
	x=4	0.778582	Pass
15	Random excursions variant		
	x=-9	0.975605	Pass

	x=-8	0.800813	Pass
	x=-7	0.902589	Pass
	x=-6	0.746598	Pass
	x=-5	0.552756	Pass
	x=-4	0.738695	Pass
	x=-3	0.832539	Pass
	x=-2	0.8699	Pass
	x=-1	0.974854	Pass
	x=1	0.249939	Pass
	x=2	0.334788	Pass
	x=3	0.756469	Pass
	x=4	0.79784	Pass
	x=5	0.833561	Pass
	x=6	0.84925	Pass
	x=7	0.674758	Pass
	x=8	0.648563	Pass
	x=9	0.571585	Pass

Base on Table 2, we can get that the sequence generated by lattice No. 60 in PRCML system passes the 15 sub-tests of NIST SP800-22 suite. Moreover, the sequences generated by lattice No. 10, 64, 95, etc. also pass the NIST test, and it indicates that the sequence generated by some lattices in the PRCML system possesses good randomness and unpredictability. For comparison analysis, we assign μ=4, ε=0.25, and the sequence generated by each lattice of CML, MLNCML and LDCML system is tested after operation of Eq. (19). It's necessary to note that all subsequent tests depend on the passing of frequency test, which is employed for testing the above sequences. The results of the frequency test are listed in Table 3.

Table 3 Test results of frequency test

System	Total number of lattices	Pass rate/%	Pass rate of all sub-tests/%
CML	100	0	—
MLNCML	100	0	—
LDCML	100	0	—
PRCML	100	100	42

According to literature [44], because of the non-uniformity of conventional chaotic systems such as CML, MLNCML and LDCML system, the sequence generated by them can not be utilized for crypto-system directly. The bit-extracting algorithm and some nonlinear functions are usually used in the chaotic crypto system for acquiring better uniformity, randomness and complexity. Fortunately, without the above methods, the PRCML system still possesses good dynamical properties, which is fully confirmed by that the sequences generated by itself can pass the NIST test.

5 Conclusion

By utilizing ECA to build the spatiotemporal chaotic system, a novel PRCML system is proposed in this paper. And it possesses two special features: firstly, the coupling of the proposed system is pseudo-random and dynamic, even so, the PRCML system can be reproduced. Secondly, the perturbation for the system is generated by ECA, which is essentially the discrete dynamical system. Therefore, the degeneration of digital chaotic system does not exist in the ECA, when it is in chaos. Furthermore, the analysis results of Kolmogorov-Sinai entropy, bifurcation diagram indicate that the PRCML system owns more complex dynamic behavior, better ergodicity and aperiodicity than other conventional spatiotemporal chaotic systems. Besides, the phase space, time-domain analysis, correlation analysis and NIST test demonstrate that the uniformity, randomness and unpredictability of sequences generated by the PRCML system are outstanding. In summary, these excellent properties of the proposed system are able to contribute more secret keys and larger secret key space for crypto-systems. Thus, the PRCML system is more suitable for building a crypto-system.

Acknowledgement

This research is supported by the National Natural Science Foundation of China (Nos: 61772047, and 6164021).

References

[1] Y. He, Y. Zhang, X. Wang, A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system, Neural Computing and Applications, 32 (2020) 247-260.

[2] Y. Zhang, Y. He, P. Li, X. Wang, A new color image encryption scheme based on 2DNLCML system and genetic operations, OPT LASER ENG, 128 (2020) 106040.

[3] Z. Liu, Y. Wang, Y. Zhao, L.Y. Zhang, A stream cipher algorithm based on 2D coupled map lattice and partitioned cellular automata, NONLINEAR DYNAM, 101 (2020) 1383-1396.

[4] Y. Zhang, X. Wang, L. Liu, Y. He, J. Liu, Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices, COMMUN NONLINEAR SCI, 52 (2017) 52-61.

[5] Y. Zhang, Y. He, X. Wang, Spatiotemporal chaos in mixed linear–nonlinear two-dimensional coupled logistic map lattice, Physica A: Statistical Mechanics and its Applications, 490 (2018) 148-160.

[6] M.A. Balootaki, H. Rahmani, H. Moeinkhah, A. Mohammadzadeh, On the Synchronization and Stabilization of fractional-order chaotic systems: Recent advances and future perspectives, Physica A: Statistical Mechanics and its Applications, 551 (2020) 124203.

[7] A. Saha, Dynamics of the generalized KP-MEW-Burgers equation with external periodic perturbation, COMPUT MATH APPL, 73 (2017) 1879-1885.

[8] J.F. Gomez-Aguilar, Chaos and multiple attractors in a fractal-fractional Shinriki's oscillator model, PHYSICA A, 539 (2020).

[9] M. Fahimi, K. Nouri, L. Torkzadeh, Chaos in a stochastic cancer model, Physica A: Statistical Mechanics and its Applications, 545 (2020) 123810.

[10] N.N. Moghadam, F. Nazarimehr, S. Jafari, J.C. Sprott, Studying the performance of critical slowing down indicators in a biological system with a period-doubling route to chaos, PHYSICA A, 544 (2020).

[11] S. Moshfegh, A. Ashouri, S. Mandavifar, J. Vahedi, Integrable-chaos crossover in the spin-1/2 XXZ chain with cluster interaction, PHYSICA A, 516 (2019) 502-508.

[12] Q. Wang, Signatures of quantum chaos in the dynamics of bipartite fluctuations, Physica A: Statistical Mechanics and its Applications, 554 (2020) 124321.

[13] X. Wang, H. Zhao, L. Feng, X. Ye, H. Zhang, High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices, OPT LASER ENG, 122 (2019) 225-238.

[14] X. Wang, N. Guan, H. Zhao, S. Wang, Y. Zhang, A new image encryption scheme based on coupling map lattices with mixed multi-chaos, SCI REP-UK, 10 (2020).

[15] D. Ghosh, S. Chakraborty, S. Samanta, Study of translational effect in Tagore's Gitanjali using Chaos based Multifractal analysis technique, PHYSICA A, 523 (2019) 1343-1354.

[16] H. Yu, X. Li, On the chaos analysis and prediction of aircraft accidents based on multi-timescales, Physica A: Statistical Mechanics and its Applications, 534 (2019) 120828.

[17] S.J. Li, G.R. Chen, X.Q. Mou, On the dynamical degradation of digital piecewise linear chaotic maps, INT J BIFURCAT CHAOS, 15 (2005) 3119-3151.

[18] A. Flores-Vergara, E.E. Garcia-Guerrero, E. Inzunza-Gonzalez, O.R. Lopez-Bonilla, E. Rodriguez-Orozco, J.R. Cardenas-Valdez, E. Tlelo-Cuautle, Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic, NONLINEAR DYNAM, 96 (2019) 497-516.

[19] C. Chen, K. Sun, S. He, An improved image encryption algorithm with finite computing precision, SIGNAL PROCESS, 168 (2020) 107340.

[20] A.A. Abd El-Latif, B. Abd-El-Atty, M. Amin, A.M. Iliyasu, Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications, SCI REP-UK, 10 (2020).

[21] L. Liu, J. Lin, S. Miao, B. Liu, A Double Perturbation Method for Reducing Dynamical Degradation of the Digital Baker Map, INT J BIFURCAT CHAOS, 27 (2017) 1750103.

[22] J. Zheng, H. Hu, X. Xia, Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos, NONLINEAR DYNAM, 94 (2018) 1535-1546.

[23] R. Wang, H.G. Ma, X.Y. Li, X.F. Zhu, A Novel Encryption Method, Chinese Control Conference, IEEE, NEW YORK, 2016. pp. 5185-5189.

[24] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, J. Harkin, Counteracting Dynamical Degradation of Digital Chaotic Chebyshev Map via Perturbation, INT J BIFURCAT CHAOS, 27 (2017) 1750033.

[25] J. Tang, Z. Yu, L. Liu, A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption, MULTIMED TOOLS APPL, 78 (2019) 24765-24788.

[26] X. Lv, X. Liao, B. Yang, A novel pseudo-random number generator from coupled map lattice with time-varying delay, NONLINEAR DYNAM, 94 (2018) 325-341.

[27] L. Liu, S. Miao, Delay-introducing method to improve the dynamical degradation of a digital chaotic map, INFORM SCIENCES, 396 (2017) 1-13.

[28] A. Zhang, Z. Xu, Chaotic time series prediction using phase space reconstruction based conceptor network, COGN NEURODYNAMICS, 14 (2020) 849-857.

[29] K. Kaneko, Chaos focus issue on coupled map lattices, CHAOS, 2 (1992) 279-408.

[30] K. Kaneko, Pattern dynamics in spatiotemporal chaos, Physica D Nonlinear Phenomena, 34 (1992) 1-41.

[31] K. Kaneko, Spatiotemporal Intermittency in Coupled Map Lattices, Progress of Theoretical Physics, 74 (1985) 1033-1044.

[32] W. Xingyuan, F. Le, W. Shibing, C. Zhang, Z. Yingqian, Spatiotemporal Chaos in Coupled Logistic Map Lattice With Dynamic Coupling Coefficient and its Application in Image Encryption, IEEE ACCESS, 6 (2018) 39705-39724.

[33] X. Wang, Y. Wang, X. Zhu, C. Luo, A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level, OPT LASER ENG, 125 (2020) 105851.

[34] G.R. Chen, Y.B. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, CHAOS SOLITON FRACT, 21 (2004) 749-761.

[35] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22, Gaithersburg, MD, US, 800 (2001) 163.

[36] X. Wang, X. Zhu, Y. Zhang, An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map, IEEE ACCESS, 6 (2018) 23733-23746.

[37] G. Jian-Sheng, J. Chen-Hui, An attack with known image to an image cryptosystem based on general cat map, Journal of China Institute of Communications, (2005).

[38] Y.Q. Zhang, X.Y. Wang, Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation, NONLINEAR DYNAM, 77 (2014) 687-698.

[39] Wolfram, Stephen, Cellular automata as models of complexity, NATURE, 311 (1998) 419-424.

[40] S. Wolfram, A.J. Mallinckrodt, Cellular Automata and Complexity, Computers in Physics, 9 (1995).

[41] Christopher, G., Langton, Self-reproduction in cellular automata, Physica D Nonlinear Phenomena, (1984).

[42] J. Neumann, A.W. Burks, Theory of self-reproducing automata, University of Illinois press Urbana1966.

[43] A. Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, Determining Lyapunov exponents from a time series, Physica D: Nonlinear Phenomena, 16 (1985) 285-317.

[44] A.V. Tutueva, E.G. Nepomuceno, A.I. Karimov, V.S. Andreev, D.N. Butusov, Adaptive chaotic maps and their application to pseudo-random numbers generation, Chaos, Solitons & Fractals, 133 (2020) 109615.

Figure

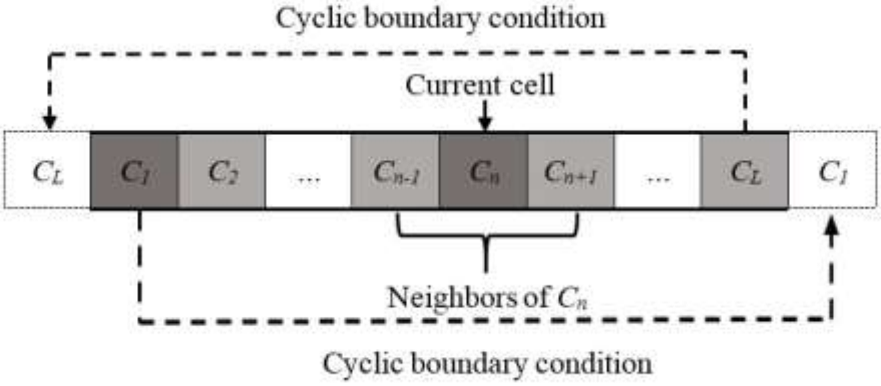


Fig. 1 Organization form of ECA

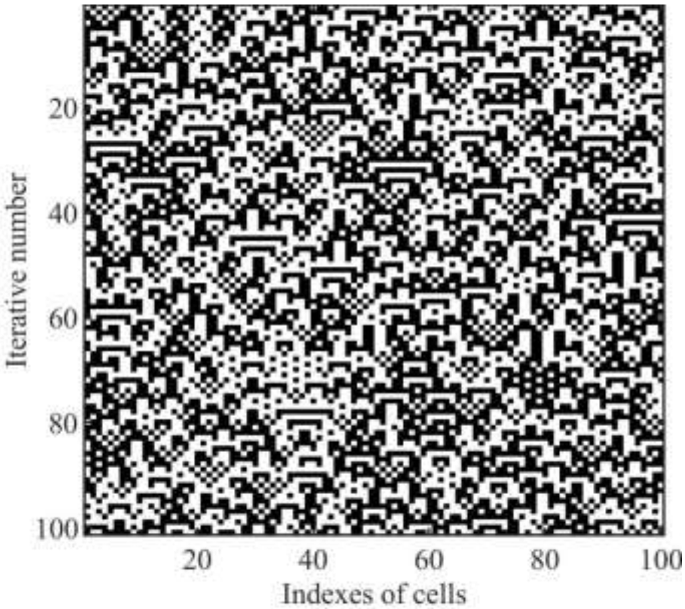


Fig. 2 Iterative result of ECA *No.*105

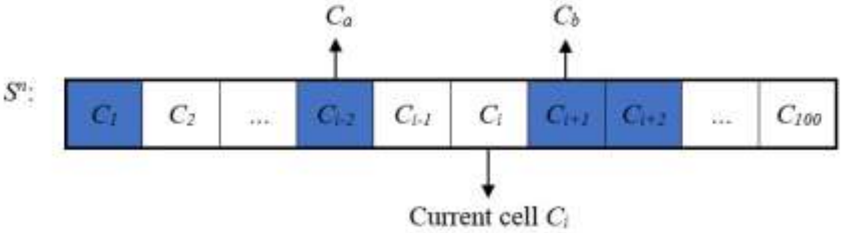
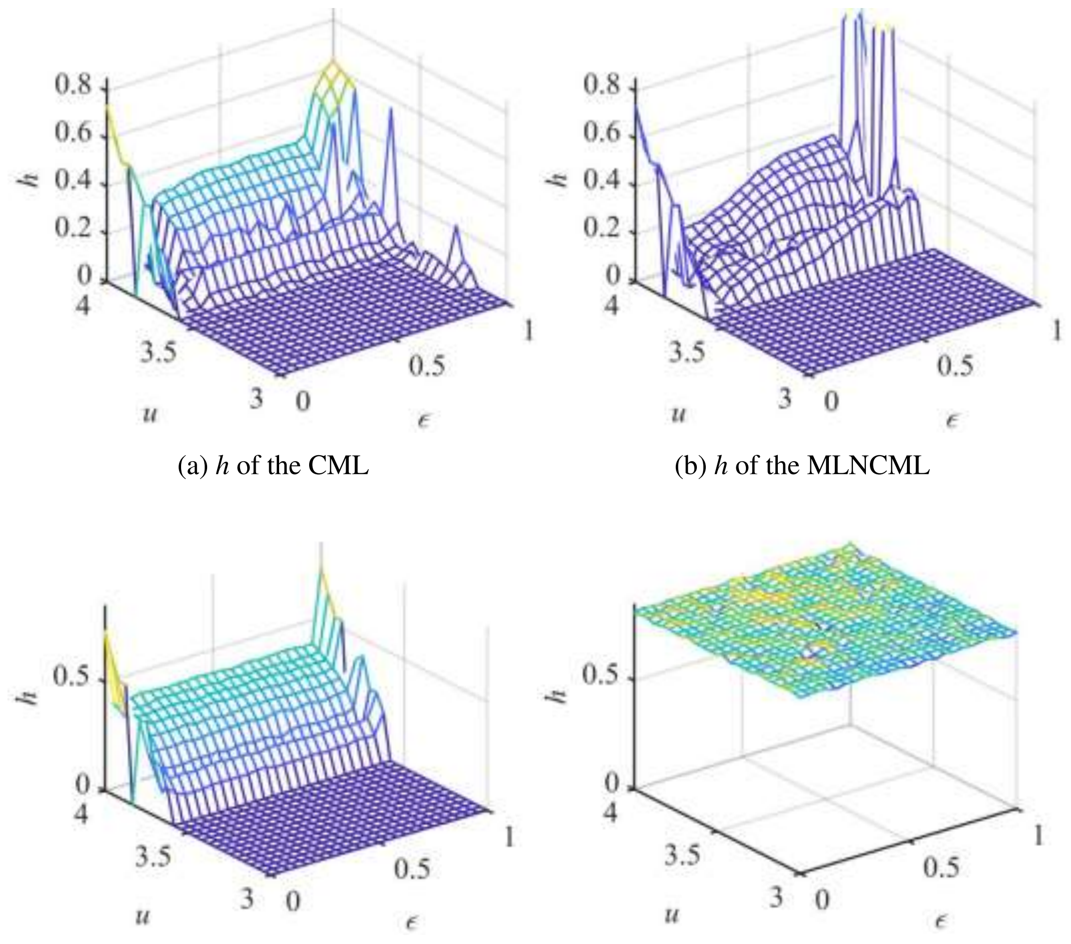


Fig. 3 The function *search*(S_n, *i*)



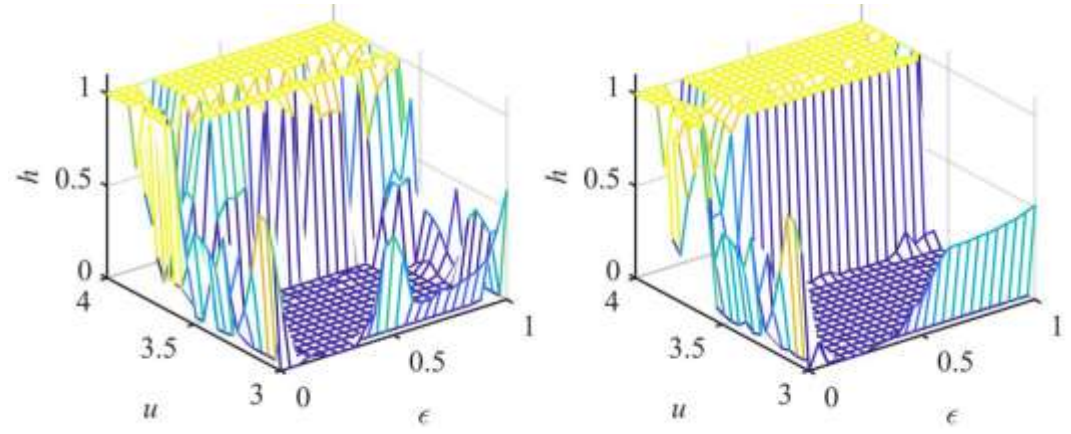
(a) *h* of the CML

(b) *h* of the MLNCML

(c) *h* of the LDCML

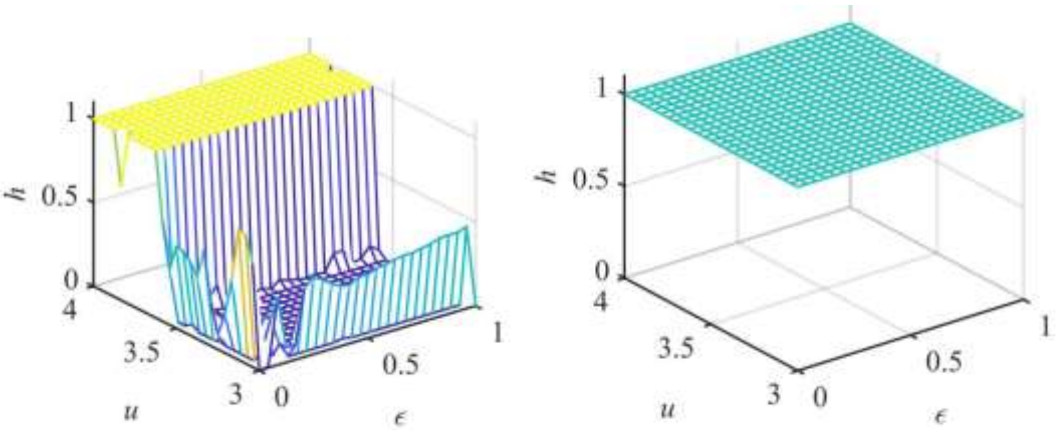
(d) *h* of the PRCML

Fig. 4 The Kolmogorov-Sinai entropy density



(a) *hu* of the CML

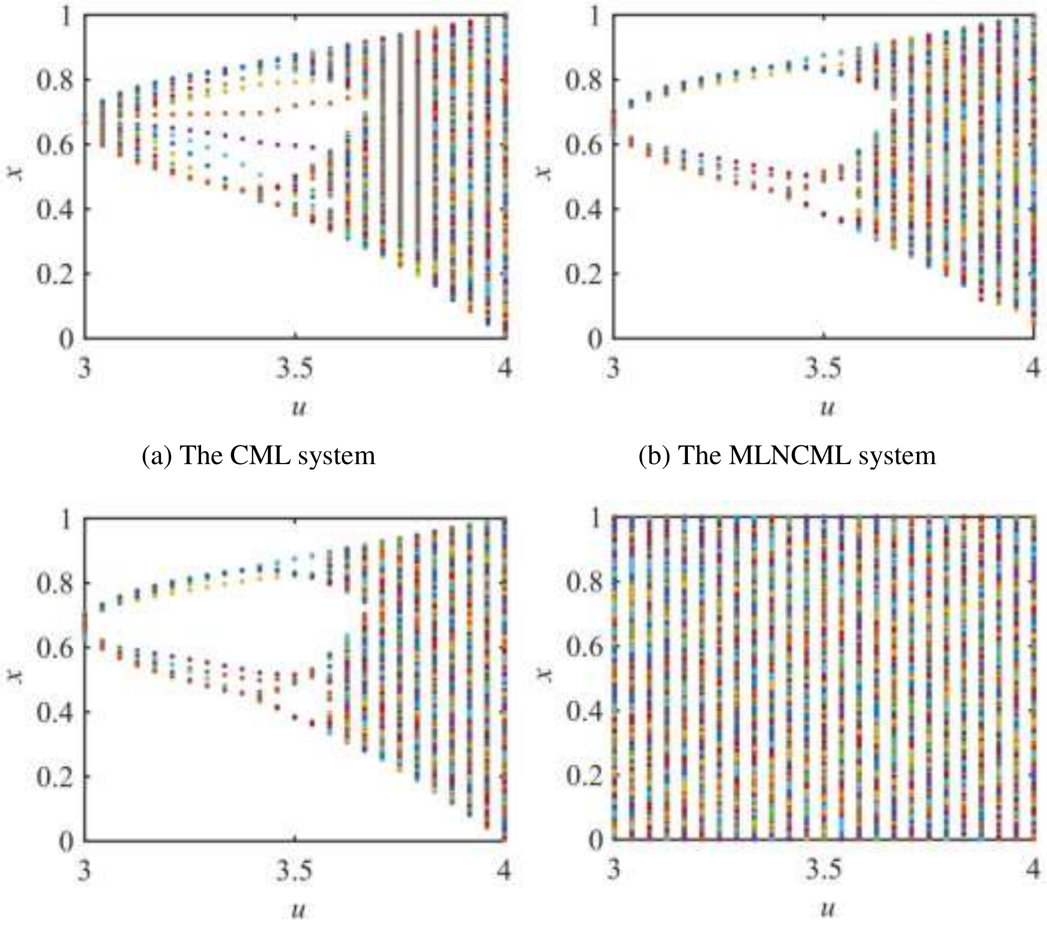
(b) *hu* of the MLNCML



(c) *hu* of the LDCML

(d) *hu* of the PRCML

Fig. 5 The Kolmogorov-Sinai entropy universality



(a) The CML system

(b) The MLNCML system

(c)The LDCML system

(d) The PRCML system

Fig. 6 The bifurcation diagram

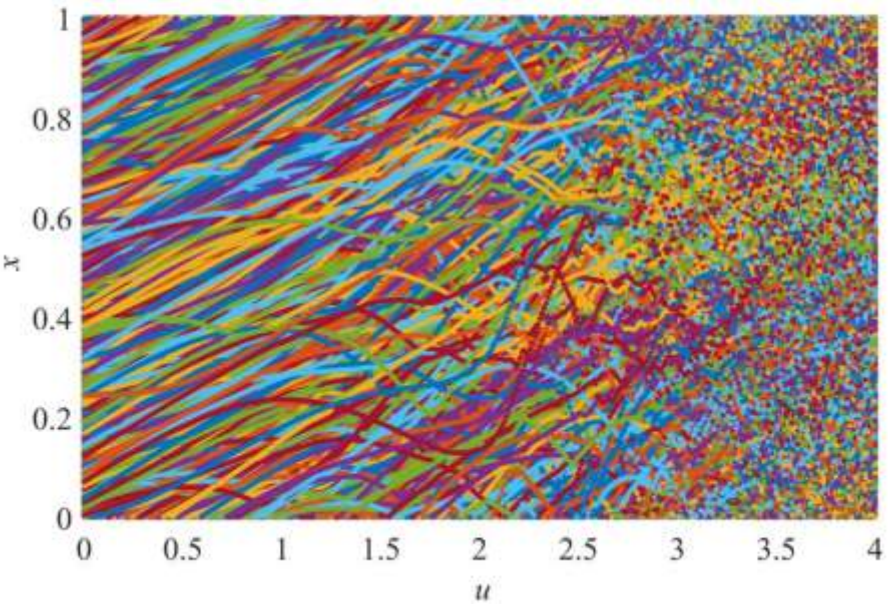
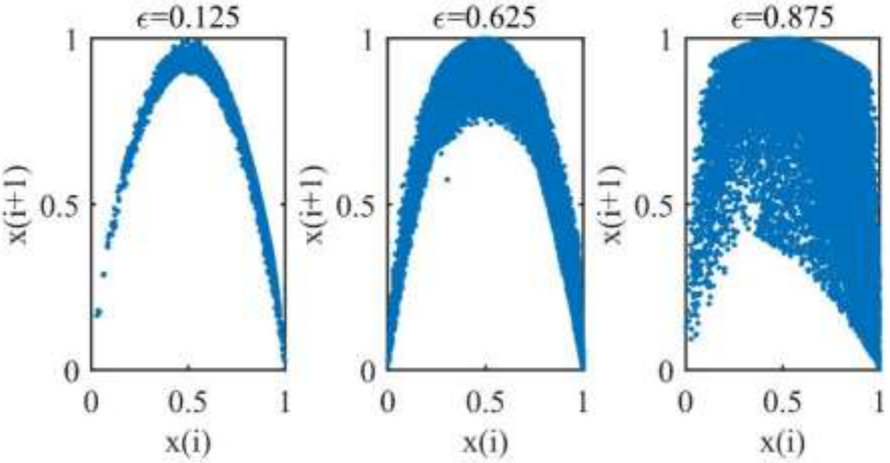
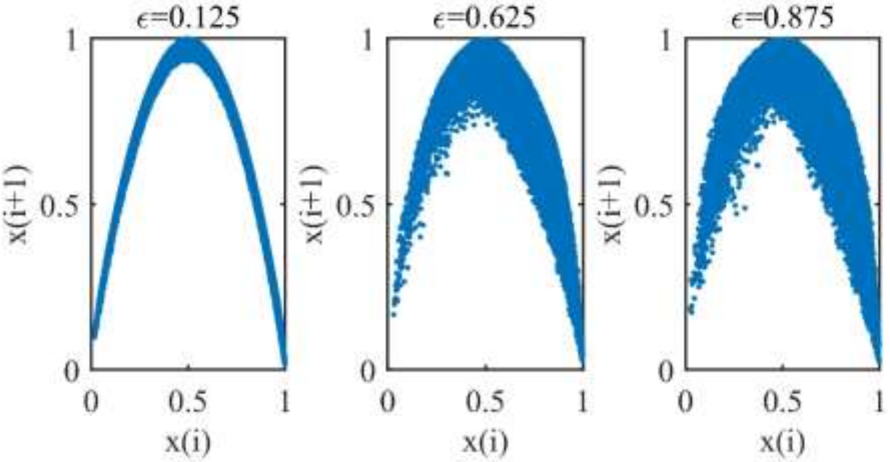


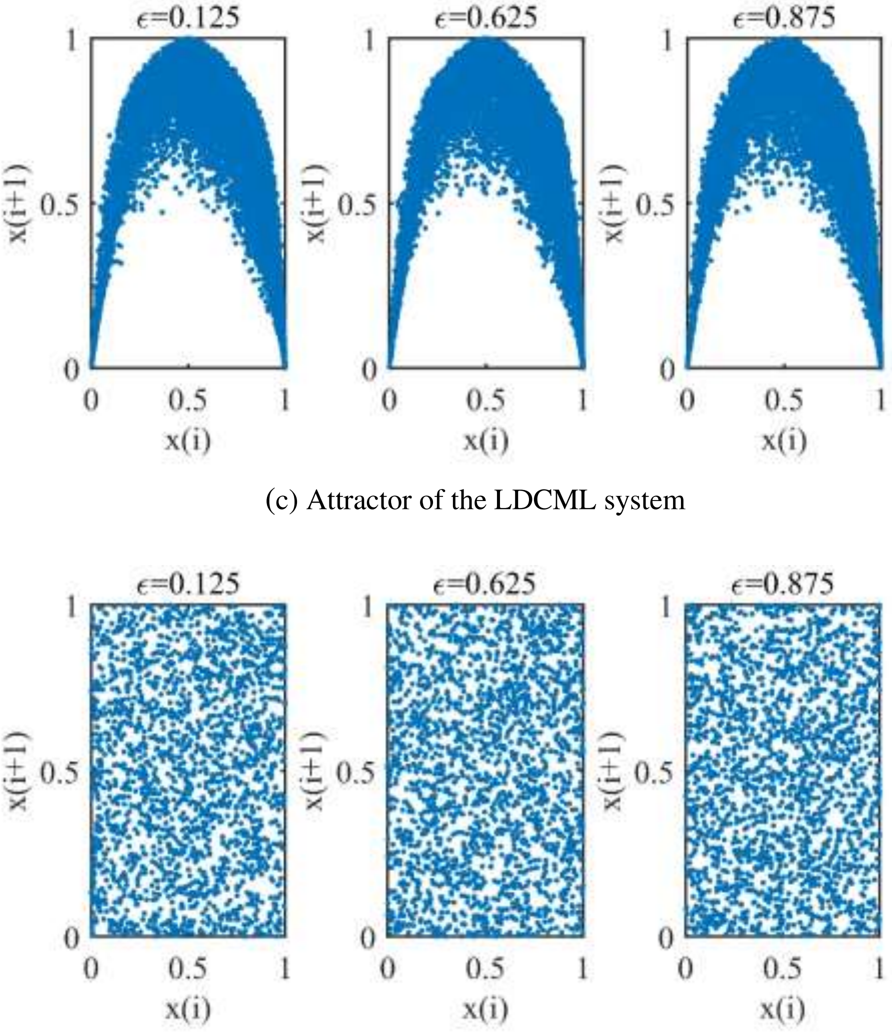
Fig. 7 The bifurcation diagram of PRCML system



(b) Attractor of the CML system



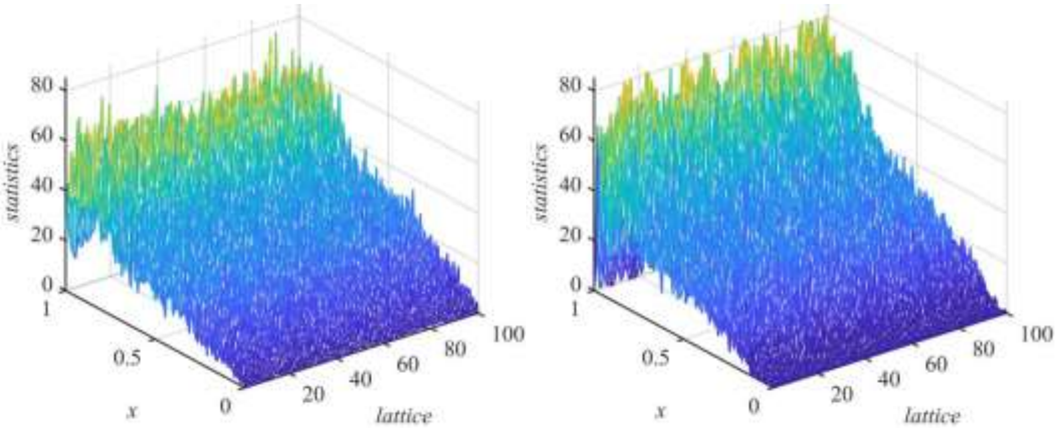
(b) Attractor of the MLNCML system



(c) Attractor of the LDCML system

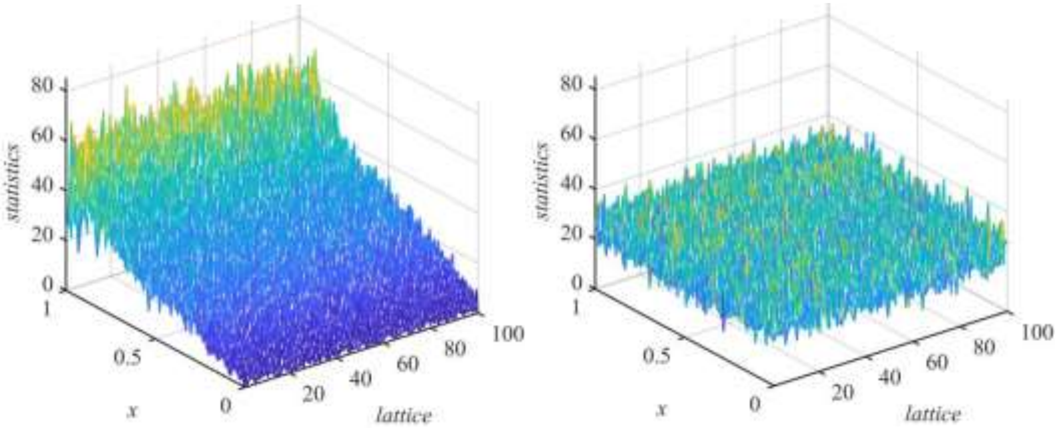
(d) Attractor of the PRCML system

Fig. 8 Phase space analysis



(a) The CML system

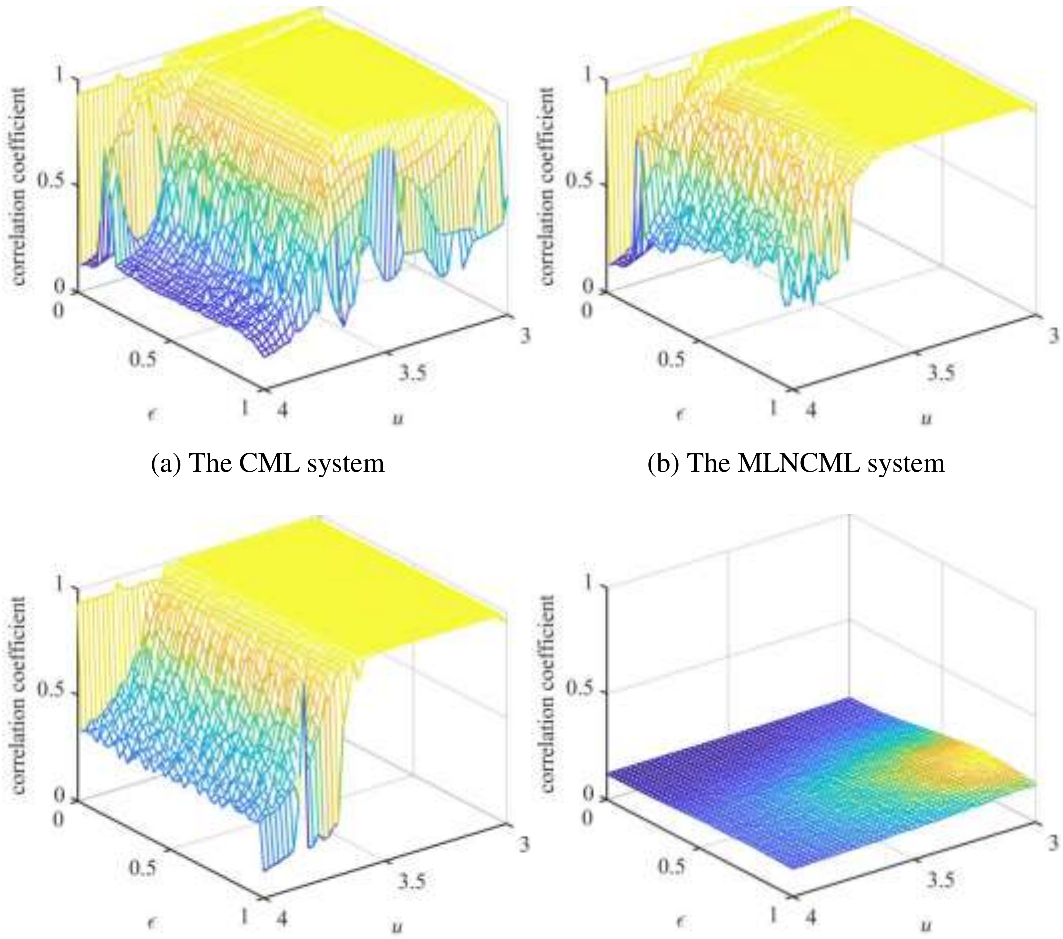
(b) The MLNCML system



(c)The LDCML system

(d) The PRCML system

Fig. 9 The time-domain analysis



(a) The CML system

(b) The MLNCML system

(c)The LDCML system

(d) The PRCML system

Fig. 10 The correlation analysis

Table

Table 1 The local transition rule of ECA *No.* 105

$S_{i-1}^t, S_i^t, S_{i+1}^t$	111	110	101	100	011	010	001	000
S_i^{t+1}	0	1	1	0	1	0	0	1

Table 2 Test results of NIST 800-22:

No.	Sub-tests	*P-value*	Result
1	Frequency	0.487682	Pass
2	Block frequency	0.034696	Pass
3	Runs	0.771448	Pass
4	Longest runs of ones	0.980655	Pass
5	Rank	0.732141	Pass
6	FFT	0.317188	Pass
7	Non-overlapping template matching(average)	0.470642	Pass
8	Overlapping template matching(all ones)	0.995805	Pass
9	Universal statistical	0.270091	Pass
10	Linear complexity	0.742281	Pass
11	Serial 1	0.692208	Pass
	Serial 2	0.341663	Pass
12	Approximate entropy	0.196619	Pass
13	Cumulative sums (forward)	0.771929	Pass
	Cumulative sums (reverse)	0.557029	Pass
14	Random excursions		
	x=-4	0.612169	Pass
	x=-3	0.72621	Pass
	x=-2	0.92413	Pass
	x=-1	0.158412	Pass
	x=1	0.395969	Pass
	x=2	0.078504	Pass
	x=3	0.755938	Pass
	x=4	0.778582	Pass
15	Random excursions variant		
	x=-9	0.975605	Pass
	x=-8	0.800813	Pass

	x=-7	0.902589	Pass
	x=-6	0.746598	Pass
	x=-5	0.552756	Pass
	x=-4	0.738695	Pass
	x=-3	0.832539	Pass
	x=-2	0.8699	Pass
	x=-1	0.974854	Pass
	x=1	0.249939	Pass
	x=2	0.334788	Pass
	x=3	0.756469	Pass
	x=4	0.79784	Pass
	x=5	0.833561	Pass
	x=6	0.84925	Pass
	x=7	0.674758	Pass
	x=8	0.648563	Pass
	x=9	0.571585	Pass

Table 3 Test results of frequency test

System	Total number of lattices	Pass rate/%	Pass rate of all sub-tests/%
CML	100	0	—
MLNCML	100	0	—
LDCML	100	0	—
PRCML	100	100	42

Figures

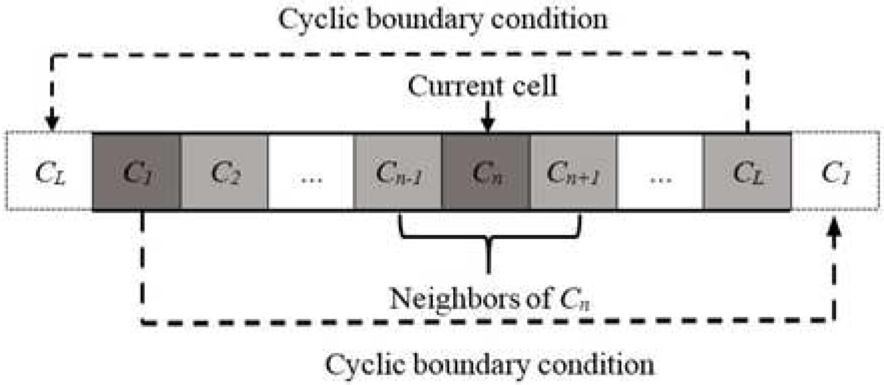


Figure 1

Organization form of ECA

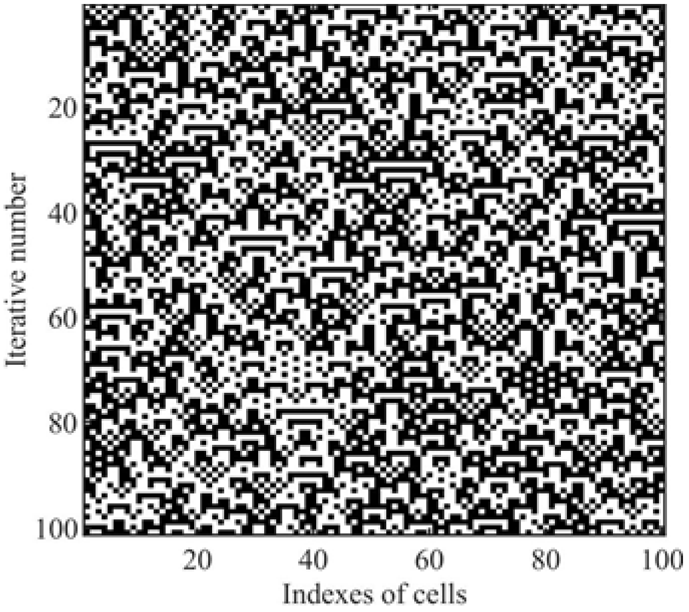


Figure 2

Iterative result of ECA No.105

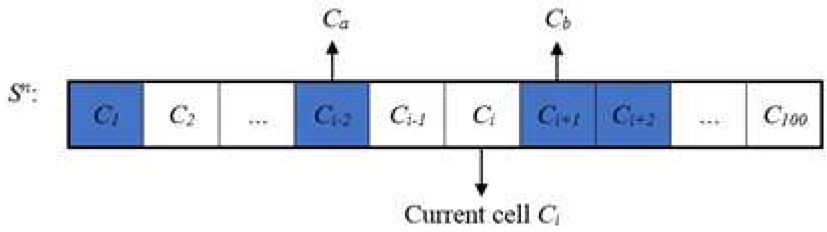
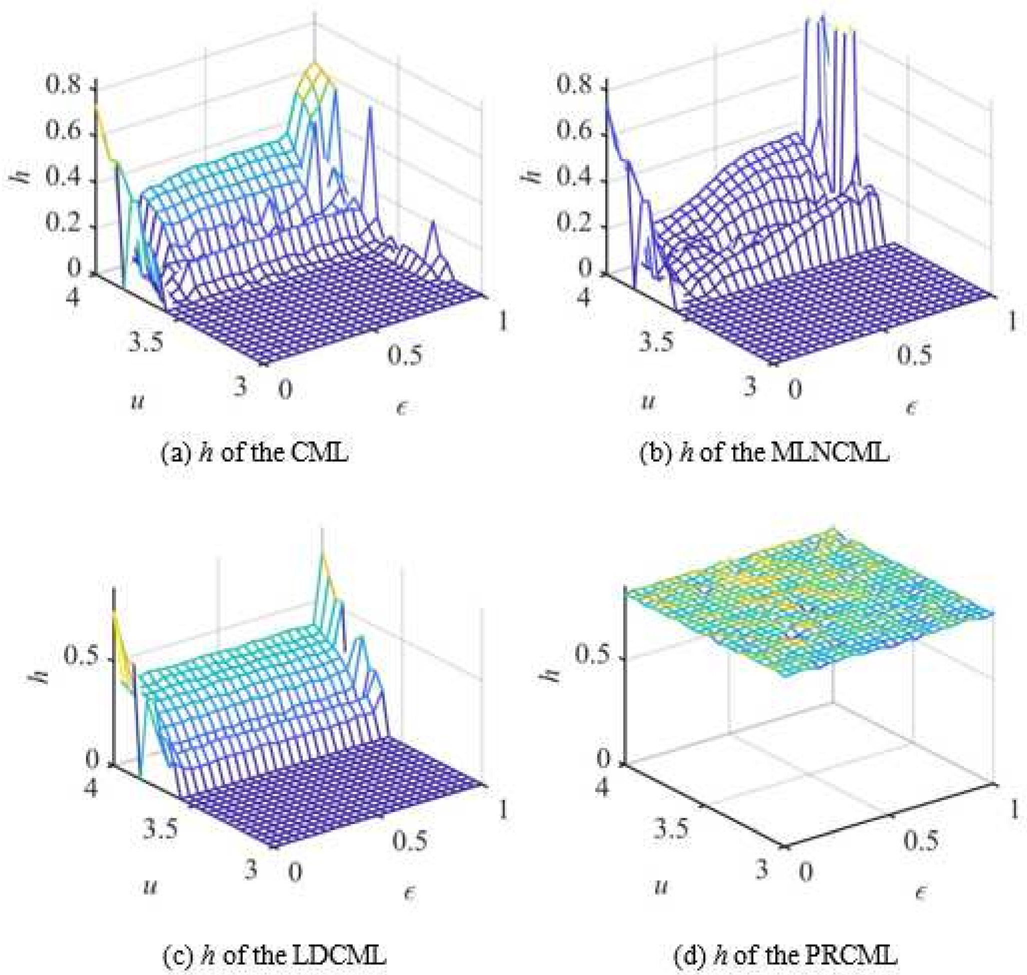


Figure 3

The function search(Sn, i)



(a) *h* of the CML

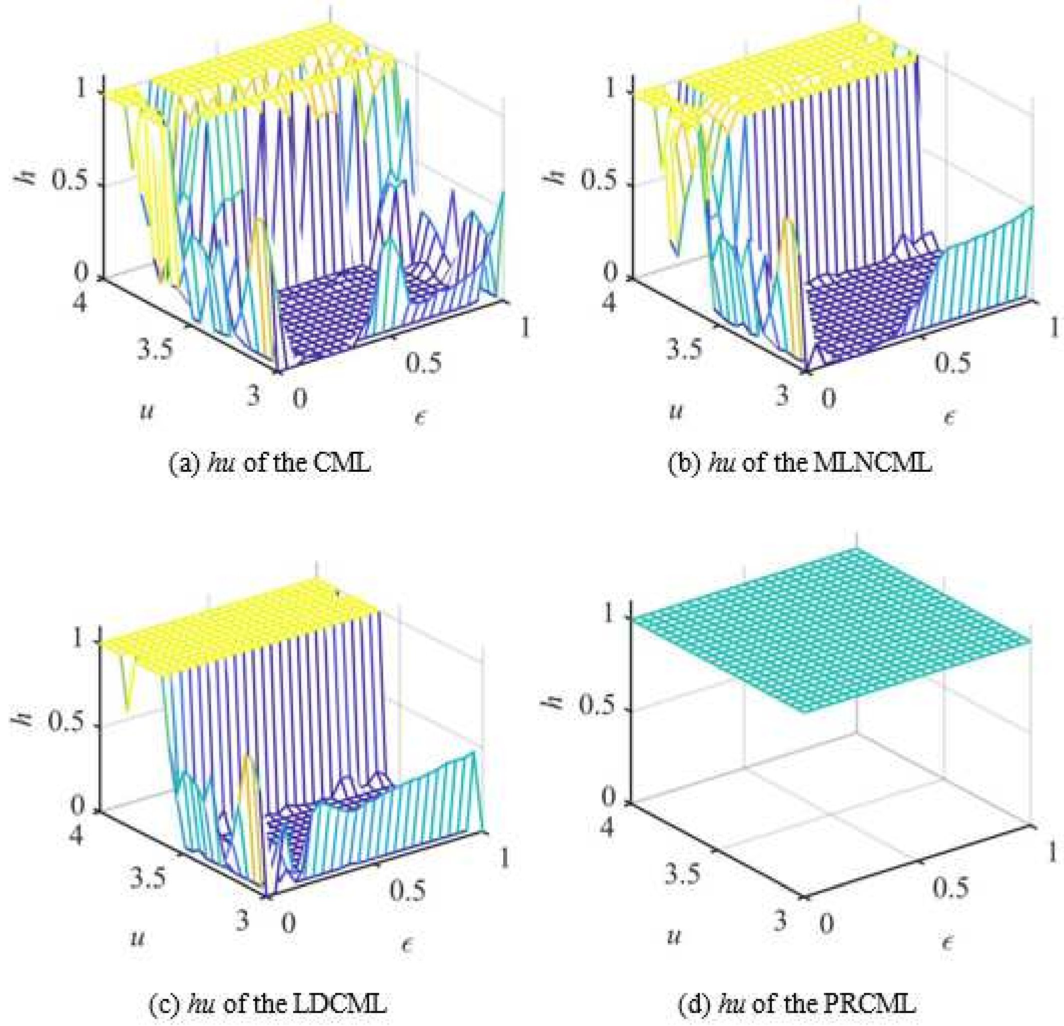
(b) *h* of the MLNCML

(c) *h* of the LDCML

(d) *h* of the PRCML

Figure 4

The Kolmogorov-Sinai entropy density



(a) *hu* of the CML

(b) *hu* of the MLNCML

(c) *hu* of the LDCML

(d) *hu* of the PRCML

Figure 5

The Kolmogorov-Sinai entropy universality

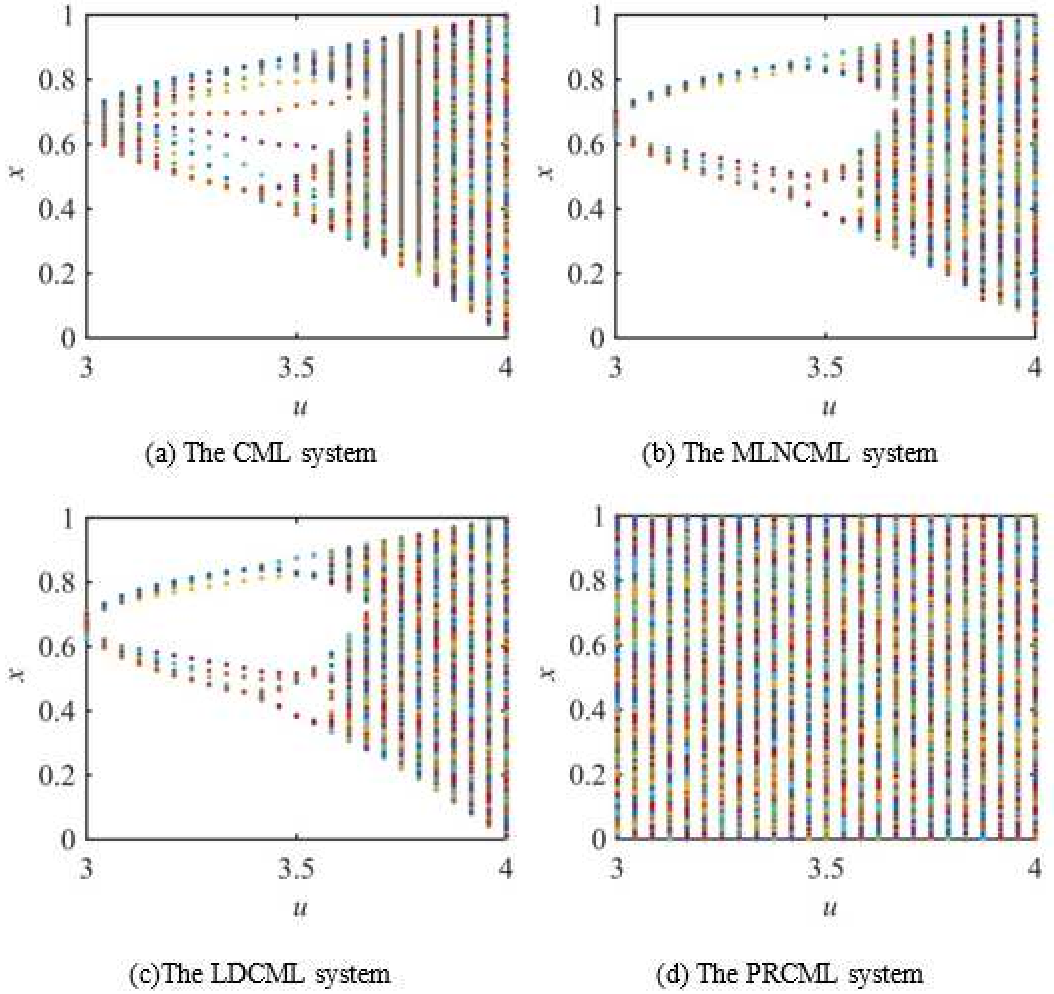


Figure 6

The bifurcation diagram

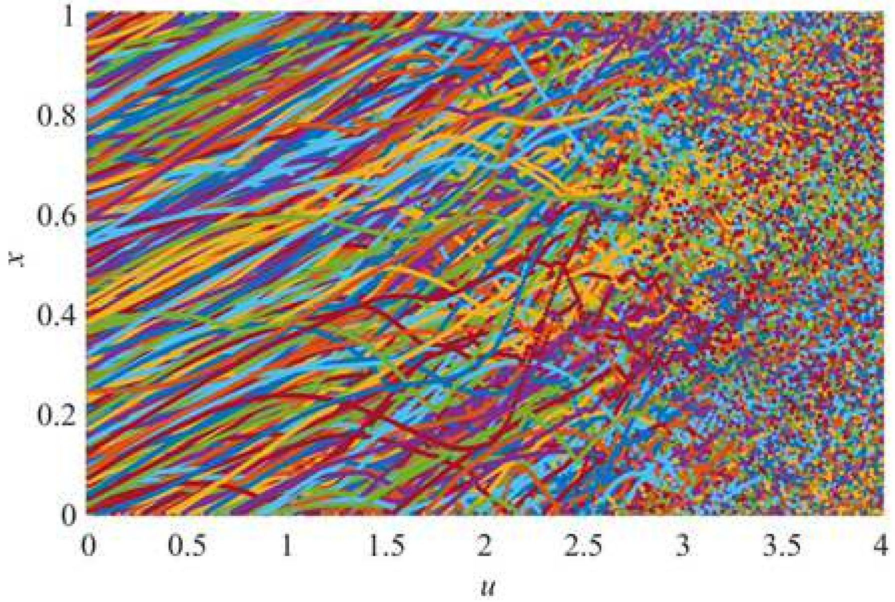
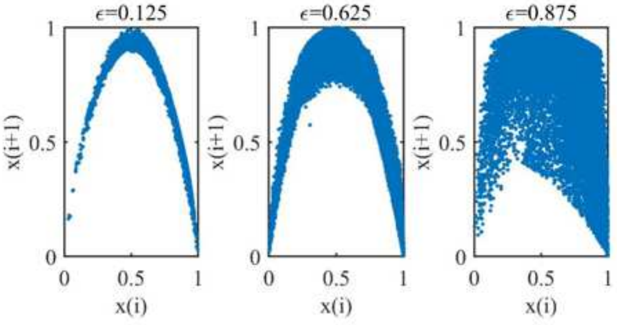
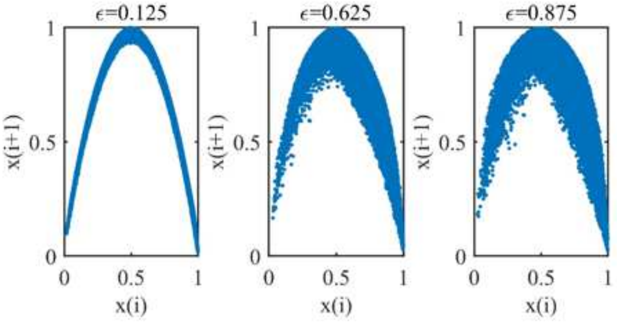


Figure 7

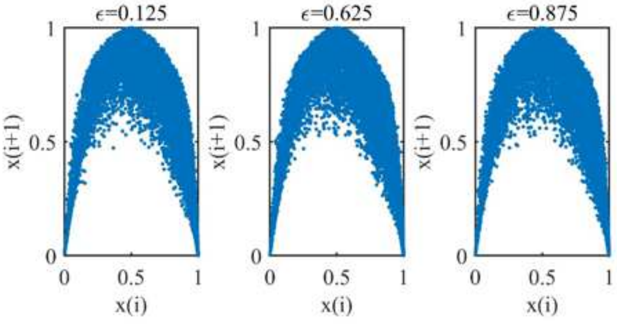
The bifurcation diagram of PRCML system



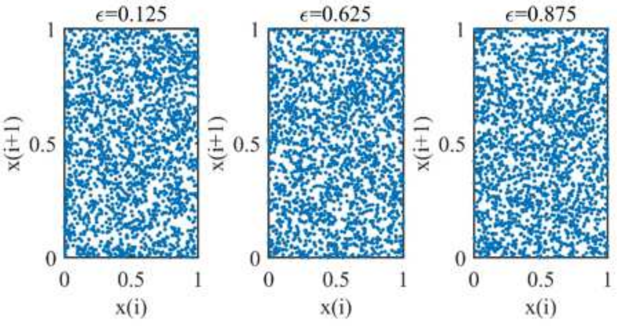
(a) Attractor of the CML system



(b) Attractor of the MLNCML system



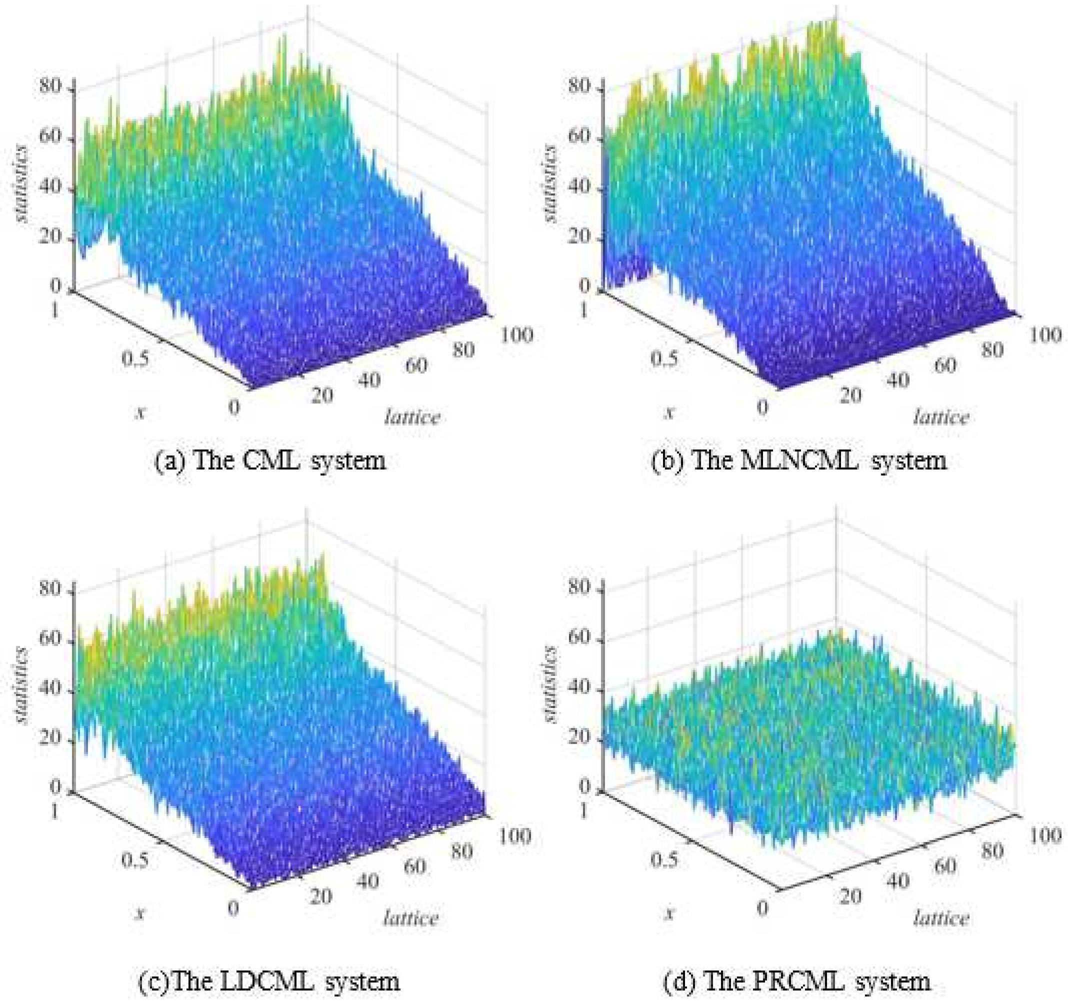
(c) Attractor of the LDCML system



(d) Attractor of the PRCML system

Figure 8

Phase space analysis



(a) The CML system

(b) The MLNCML system

(c)The LDCML system

(d) The PRCML system

Figure 9

The time-domain analysis

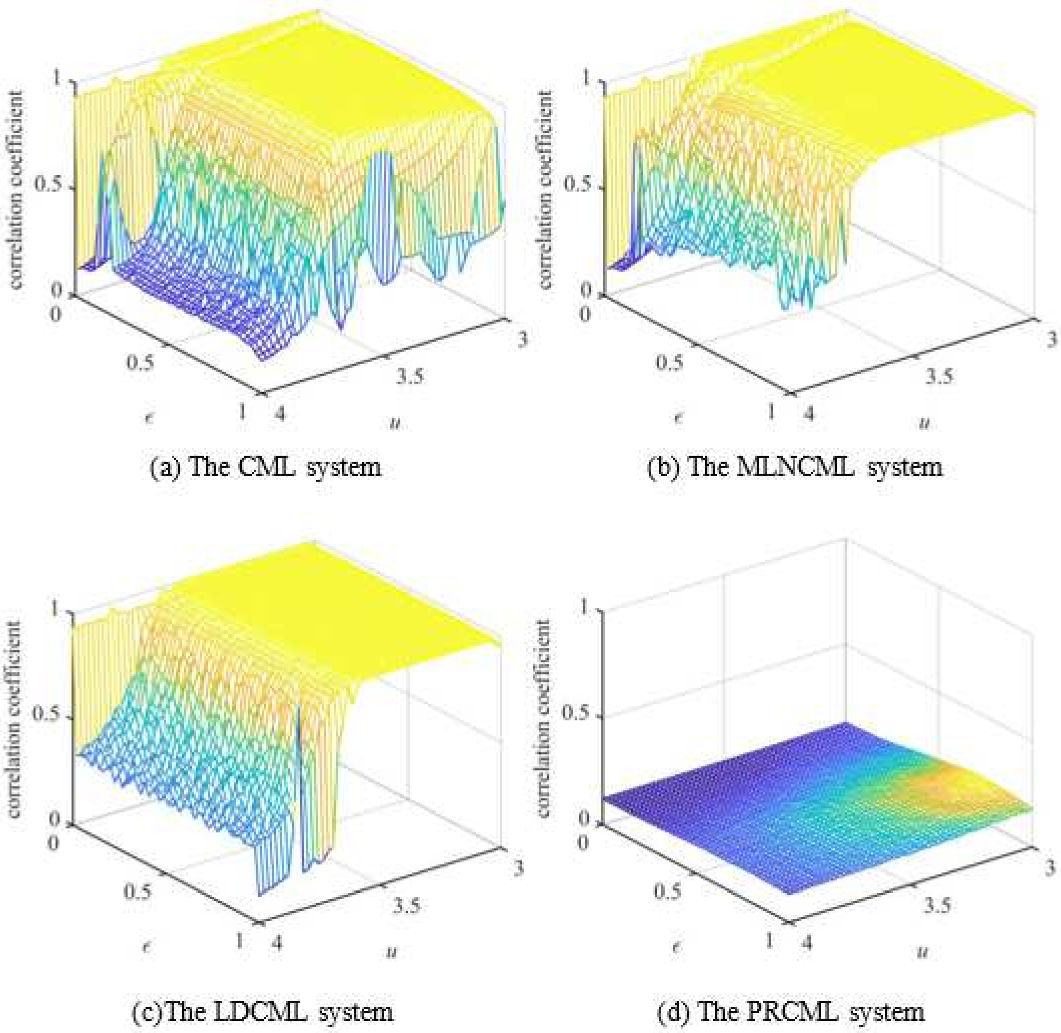


Figure 10

The correlation analysis