Nonlinear Dyn (2012) 70:1589–1592
DOI 10.1007/s11071-012-0558-0

ORIGINAL PAPER

A new pseudo-random number generator based on CML and chaotic iteration

Xing-yuan Wang · Xue Qin

Received: 19 April 2012 / Accepted: 25 July 2012 / Published online: 21 August 2012

Abstract In this paper, we propose a new algorithm of generating pseudorandom number generator (PRNG), which we call (couple map lattice based on discrete chaotic iteration (CMLDCI)) that combine the couple map lattice (CML) and chaotic iteration. And we can prove that this method can be written in a form of chaos map, which is under the sense of Devaney chaos. In addition, we test the new algorithm in NIST 800-22 statistical test suits and we use it in image encryption.

Keywords CML · Chaotic iteration · NIST 800-22 · PRNG

1 Introduction

Since the couple map lattice (CML) has been proposed [1], it has been considered to be a powerful tool in many theoretical and practical fields, such as chemical, population, convection, fluid flow, biology, and computer networks [2–4]. Meanwhile, the conception of chaotic iteration has been discussed for a long time by different scientists such as Robert [5] and Chazan [6] in different methods. However, their focuses were both on the conditions of convergence; more wide range of chaotic iteration has not been discussed. The breakthrough happened in the literature of [7]; the author proved a very useful theorem that as long as the function f is under the transitivity condition, the chaotic iteration can be written in a chaotic map under the sense of Devaney chaos. We use this theorem to help us design a new pseudorandom number generator (PRNG). So that in this term, this new PRNG is chaotic in a sense of Devaney.

On the other hand, PRNG is widely utilized in the industry, as simulation, sampling, numerical analysis, computer programming, decision making, recreation, cryptographic protocols, and cryptosystems, etc. [8–14]. It is hard to obtain the truly random numbers, alternatively, people use PRNG in practical work. So generally, people use seeds and determinant processes to generate sequences which has good randomness and that is PRNG.

In this paper, we are trying to combine those two technologies of CML and chaotic iteration to get a new PRNG. And we can prove that this new algorithm can be reformed into a form of chaotic map under sense of Devaney chaos. And we do several experiments as NIST 800-22 statistical test suit [15], draw the autocorrelation and histogram figures, and we use the new algorithm in the image encryption. The results we obtained are pretty good and demonstrate that this new PRNG is suitable for practice.

X.-y. Wang (✉) · X. Qin
Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
e-mail: wangxy@dlut.edu.cn

X. Qin
e-mail: qintxx@gmail.com

2 Basic definition

We know that chaotic iteration is such a map [7]:

$$x^0 \in \mathbf{B}^N \quad \forall n \in \mathrm{N}^+ \quad \forall i \in \{1; N\}$$
$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ f(x^{n-1})_{s^n} & \text{if } S^n = i \end{cases} \tag{1}$$

B donates $\{0, 1\}$. $\{1; N\}$ donates $\{1, 2, \ldots, N\}$. S^n donatse the nth element of a sequence S, which elements all belong to $\{1; N\}$. And f is a chosen function. In the literature [7], as long as f satisfies the transitivity condition, this chaotic iteration is chaotic under Devaney's chaotic definition.

And as we know, one of the simplest CML is in the form

$$x_j^{n+1} = (\alpha)\big[f_j\big(x_j^n\big)\big] + (1-\alpha)\big[f_{j-1}\big(x_{j-1}^n\big)\big], \quad j \in \{1; M\} \tag{2}$$

Here, we choose $\alpha = 0.5$. M is the number of raw.

If $f : \chi \mapsto \chi$, then (χ, d) is a metric space.

Definition 1 f is said to be topologically transitive if, for any pair of open sets $U, V \subset \chi$, there exists $k > 0$ such that $f^k(U) \cap V \neq \phi$.

Definition 2 (χ, f) is said to be regular if the set periodic points is dense in χ.

Definition 3 f has sensitive dependence on initial conditions if there exist $\delta > 0$ such that, for any $x \in \chi$ and any neighborhood V of x, there exist $y \in V$ and $n \geq 0$ such that $|f^n(x) - f^n(y)| > 0$.

Now the definition of Devaney chaotic topological system is [16]:

Definition 4 $f : \chi \mapsto \chi$ is said to be chaotic on χ if (χ, f) is regular, topologically transitive, and has sensitive dependence on initial conditions.

3 New PRNG

The new PRNG we proposed is similar to CML where its definition is below:

$$\big(S_j^{n+1}, E_j^{n+1}\big) = G_j\big(S_j^n, E_j^n, E_{j-1}^n\big), \tag{3}$$

$$G : [1; N] \times \mathbf{B}^N \times \mathbf{B}^N \mapsto [1; N] \times \mathbf{B}^N \quad j \in \{1; M\},$$
$$G_j\big(S_j^n, E_j^n, E_{j-1}^n\big) = \big(\sigma\big(S_j^n\big), F_j\big(\sigma\big(S_j^n\big), E_j^n, E_{j-1}^n\big)\big), \tag{4}$$
$$F : [1; N] \times \mathbf{B}^N \times \mathbf{B}^N \mapsto \mathbf{B}^N \quad \forall i \in \{1; N\},$$

$$F_j\big(\sigma\big(S_j^n\big), E_j^n, E_{j-1}^n\big) = \big(\big(E_j^n\big)_{\cdot}^{i} \delta\big(\sigma\big(S_j^n\big), i\big) + f_j\big(E_j^n, E_{j-1}^n\big)_{\cdot}^{i} \neg\delta\big(\sigma\big(S_j^n\big), i\big)\big), \tag{5}$$

$$\sigma : [1; N] \mapsto [1; N], \quad \sigma\big(S^n\big) = S^{n+1}, \tag{6}$$

$$\delta(k, h) = \begin{cases} 0, & \text{if } k = h, \\ 1, & \text{if } k \neq h, \end{cases} \tag{7}$$

$$f : (\mathbf{B}^N, \mathbf{B}^N) \mapsto \mathbf{B}^N \quad f_j\big(E_j^n, E_{j-1}^n\big) = \neg\big(E_j^n \oplus E_{j-1}^n\big), \tag{8}$$

$$S_j^n = g_j\big(x_j^0, r_j\big) \tag{9}$$

Define the new distance as

$$d\big((S, E); \big(S', E'\big)\big) = d_e\big(E, E'\big) + d_s\big(S, S'\big), \quad (S, E), \big(S', E'\big) \in \chi$$

and

$$d_e\big(E, E'\big) = \sum_{k=1}^{N} \delta\big(E^k, E'^k\big),$$
$$d_s = \big(S, S'\big) = \frac{9}{N} \sum_{k=1}^{\infty} \frac{|S^k - S'^k|}{10^k}$$

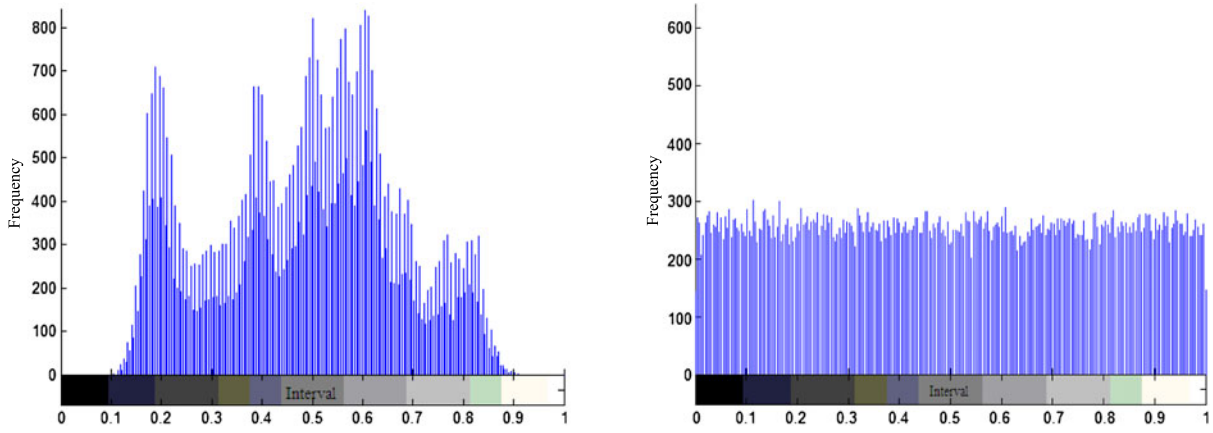
$\big(S_j^n, E_j^n\big)$ donate the jth row nth time note, which $S_j^n \in [1; N]$, $E_j^n \in \mathrm{B}^N$, $\mathrm{B} = \{0, 1\}$. S^n donates the nth term of a sequence S, which elements belong to $[1; N]$. S is called a *strategy*. $(E_j^n)^i$ donates the ith element of the

(a) The original image (b) The encrypted image

Fig. 1 Result of the encrypted Lena image

Table 1 Result of NIST 800-22 test suits

Test	p-value	Conclusion
Frequency Test	0.852683	random
Frequency Test within a Block	0.383347	random
Runs Test	0.310984	random
Test for the Longest Run of Ones in a Block	0.137473	random
Binary Matrix Rank Test	0.699313	random
Discrete Fourier Transform Test	0.129620	random
Maurer's "Universal Statistical" Test	0.484733	random
Linear Complexity Test	0.474938	random
Non-overlapping Template Matching Test	0.103441	random
Overlapping Template Matching Test	0.743101	random
Approximate Entropy Test	0.249343	random
Serial Test	0.081106	random
Cumulative Sums Test	0.099462	random
Random Excursions Test	0.642632	random
Random Excursions Variant Test	0.301426	random



(a) The original image (b) The encrypted image

Fig. 2 The histogram figure of the original and encrypted image

jth row nth time number sequence, which elements belong to B^N. g^k donate $\underbrace{g \circ g \cdots g}_{k \text{ time}}$.

Here, by the proof of literature [7], it is easy to find that the function f is under the condition of transitivity.

Theorem 1 *$f_j(E_j^n, E_{j-1}^n) = \overline{E_j^n \oplus E_{j-1}^n}$ is under the transitivity condition.*

We call our new method a couple map lattice based on discrete chaotic iteration (CMLDCI). And to more details of CMLDCI, we use the simple boundary rule: $\left(S_1^{n+1}, E_1^{n+1}\right) = G_1\left(S_1^n, E_1^n, E_M^n\right)$

4 Experiment

To specify, we choose

$N = 8, \quad M = 5, \quad x_j = [0.1; 0.5] \quad \forall j \in M,$

$\{0.1; 0.5\} = \{0.1, 0.2, 0.3, 0.4, 0.5\},$

$$E_j^1 = \{10010011, 01000110, 11010010, 10011100, 00100101\},$$

$$g_j\left(x_j^n\right) = r_j x_j^{n-1}\left(1 - x_j^{n-1}\right),$$

$$r_j = [3.91; 3.92; 3.93; 3.94; 3.95]$$

We test it in the NIST 800-22 statistical test suits and we get the result in Table 1. In the NIST 800-22 tests, if $p\text{-}value \geq 0.01$, then the PRNG passes this test, and the larger *p-value* is the larger randomness PRNG has. And we use the generated pseudorandom number (PRN) to encrypt the Lena image. Here, we use each 8-bit state of each note in our algorithm to form the 8-bit integer of the image. We obtained the original and encrypted image in Fig. 1(a) and Fig. 1(b), respectively. And we get the histogram figure of the original and encrypted image in Fig. 2(a) and Fig. 2(b), respectively.

5 Conclusion and future work

In this paper, we propose a new PRNG combining the technology of CML and chaotic iteration and we prove it can be transformed into a chaotic map under the sense of Devaney. We do NIST 800-22 test suits on it. We use it in an image encryption. And we draw the histogram of the original and encrypted Lena map. In the future, we hope to prove the algorithm that can also be in a form of the Li–York chaotic map and use it in a parallel condition.

Acknowledgements This research is supported by the National Natural Science Foundation of China (Nos: 61173183, 60973152, and 60573172), the Superior University Doctor Subject Special Scientific Research Foundation of China (No: 20070141014), the National Natural Science Foundation of Liaoning province (No: 20082165), and the Fundamental Research Funds for the Central Universities (No: DUT12JB06).

References

1. Kaneko, K.: Period-doubling of kink–antikink patterns, quasiperiodicity in anti-ferro-like structures and spatial intermittency in coupled logistic lattice. Prog. Theor. Phys. **72**(3), 480–486 (1984)
2. Cocho, G., Martınez-Mekler, G.: On a coupled maplattice formulation of the evolution of genetic sequences. Physica D **51**(1–3), 119–130 (1991)
3. Guirao, J., Lampart, M.: Chaos of a coupled lattice system related with the Belusov–Zhabotinskii reaction. J. Math. Chem. **48**(1), 159–164 (2010)
4. Succi, S.: Applying the lattice Boltzmann equation to multiscale fluid problems. Comput. Sci. Eng. **3**(6), 26–37 (2001)
5. Robert, F.: Discrete Iterations A Metric Study. Springer Series in Computational Mathematics, vol. 6. Springer, Berlin (1986)
6. Chazan, D., Miranker, W.: Chaotic relaxation. Linear Algebra Appl. **2**(2), 199–222 (1969)
7. Bahi, J., Guyeux, C.: Hash functions using chaotic iterations. J. Algorithms Comput. Technol. **4**(2):167–182 (2010)
8. Knuth, D.E.: The Art of Computer Programming. Seminumerical Algorithms, 3rd edn., vol. 2, Chap. 3. Addison-Wesley, Reading (1998)
9. Jakimoski, G., Kocarev, L.: Block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. I, Regul. Pap. **48**(2), 163–169 (2002)
10. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
11. Wang, B., Wu, Q., Hu, Y.: A knapsack-based probabilistic encryption scheme. Inf. Sci. **177**(19), 3981–3994 (2007)
12. Cao, F., Cao, G.: A secure identity-based proxy multisignature scheme. Inf. Sci. **179**(3), 292–302 (2009)
13. Xiao, D., Liao, X., Deng, S.: A novel key agreement protocol based on chaotic maps. Inf. Sci. **177**(4), 1136–1142 (2007)
14. Xiao, D., Liao, X., Deng, S.: Using time-stamp to improve the security of a chaotic maps-based key agreement protocol. Inf. Sci. **178**(6), 1598–1602 (2008)
15. NIST: A statistical test suite for random and pseudorandom number generators for cryptographic applications. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (2010)
16. Devaney, R.: An Introduction to Chaotic Dynamical Systems, 2nd edn. Addison-Wesley, Redwood City (1989)