Cryptographic Properties Analysis of Piecewise Logistic Map

Yong Wang[1, 2], Zhaolong Liu[1], Peng Lei[1]

[1]College of Computer Science and Technology, ChongqingUniversity of Posts and Telecommunications, Chongqing 400065, China
[2]College of Economy and Management, ChongqingUniversity of Posts and Telecommunications, Chongqing 400065, China

Abstract- The method for constructing piecewise logistic chaotic map is proposed. The bifurcation diagram, Lyapunov exponent, density distribution and ergodicity of the piecewise logistic map is given by numeric analysis. Simulation results show that the maximum Lyapunov exponent of the piecewise logistic map become larger with the increase of the segments. The ergodicity and bifurcation of the piecewise logistic map become better when more partitions are divided. Although the piecewise logistic map still has no uniform density probability, it can be made up when iterating the piecewise logistic map with variable control parameters. Therefore, the piecewise logistic maps has better cryptographic properties than the logistic map, which is more suitable to be applied to designing chaotic encryption algorithms.

Keywords: Piecewise logistic map; Cryptographic properties; Lyapunov exponent; Ergodicity; Density probability

1. Introduction

Recently, the chaotic maps has been widely applied to data security and secure communications [1-3]. The logistic map shown as below is one of popular chaotic system used to design encryption algorithms[4-6].

$$x_{n+1}=\mu x_n(1- x_n \qquad (1)$$

where x_n is the current state value and $\mu\in[3.57,4]$ is the control parameter.

However, the logistic map has inherent problems from the view of cryptography, such as uneven density distribution and existence of weak keys[7]. In this paper, the extend form of logistic map, i.e. the piecewise logistic map is researched. Some cryptographic properties of this chaotic map are described by numeric analysis. The simulation results show that the piecewise logistic map has better cryptographic performance than the logistic map.

This rest of this paper is organized as follows. Section 2 discusses the piecewise logistic map and its cryptographic properties. In Section 3, the piecewise logistic map with variable control parameter is presented, which has better uniform density probability. Finally, conclusions are drawn in Section 4.

2. The Piecewise Logistic Map

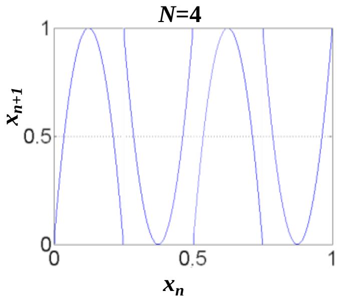

Fig. 1 The piecewise logistic map with N = 4

The presented piecewise logistic map is defined as below:

$$x_{j+1}=\begin{cases} N^2\mu x_j(\frac{1}{N}-x_j), & 0<x_j<\frac{1}{N} \\ 1-N^2\mu x_j(\frac{1}{N}-x_j), & \frac{1}{N}<x_j<\frac{2}{N} \\ \cdots & \\ N^2\mu(x_j\text{-}\frac{i-1}{N})\ (\frac{i}{N}-x_j), & \frac{i-1}{N}<x_j<\frac{i}{N} \\ 1-N^2\mu(x_j\text{-}\frac{i-1}{N})\ (\frac{i}{N}-x_j), & \frac{i}{N}<x_j<\frac{i+1}{N} \\ \cdots & \\ N^2\mu(x_j\text{-}\frac{N-2}{N})\ (\frac{N-1}{N}-x_j), & \frac{N-2}{N}<x_j<\frac{N-1}{N} \\ 1-N^2\mu(x_j\text{-}\frac{N-2}{N})\ (\frac{N-1}{N}-x_j), & \frac{N-1}{N}<x_j<1 \end{cases} \qquad (3)$$

where $x_j \in (0,1)$ is the state value of the piecewise logistic map, $\mu\in(0,4)$ is the control parameter and N is the partition number of the piecewise logistic map. The piecewise logistic map with N = 4 is illustrated in Fig.1.

2.1 Lyapunov Exponent

For dynamical systems, the Lyapunov exponent characterizes the velocity of evolution between two near trajectories. For function $x_{n+1}= f(x_n)$, its Lyapunov exponent λ is calculated as follows [4]:

$$\lambda=\lim_{x\to\infty}\frac{1}{n}\sum_{i=1}^{n-1}\ln\left|\frac{df}{dx}\right|_{x=x_i} \qquad (2)$$

In Fig.2, the Lyapunov exponents of the piecewise logistic map are plotted with respect to the system parameter μ for different N Meanwhile, the Lyapunov exponents of the logistic map is shown in Fig.3.

Based on Figs. 2 and 3, it can be concluded that:(i) Compared with the logistic map, the piecewise logistic map has greater Lyapunov exponent when the control parameter μ is fixed to the same values. (ii) With the increase of partition number of the piecewise logistic map, the interval of control parameter μ corresponding to positive Lyapunov exponent become wider. (iii) The maximum Lyapunov exponent of the piecewise logistic map is increased with the increase of segments. It means that the orbit of the piecewise logistic map become more unstable and its sequence is more complex.

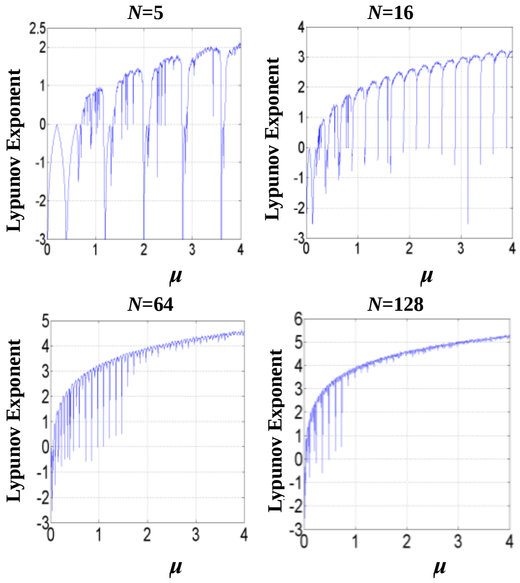

Fig. 2 Lyapunov exponents of the piecewise logistic map

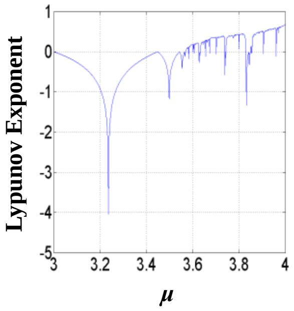

Fig. 3 Lyapunov exponents of the logistic chaotic map

2.2. Bifurcation Diagram

The bifurcation diagrams of the piecewise logistic map with different segmentations N are obtained by numeric calculation and shown in Fig. 4. Similarly, the bifurcation diagram of logistic map is shown in Fig. 5. From Figs. 4 and 5, we can see that: (i) The piecewise logistic map enters the full chaotic state when the control parameter μ is about 2, while μ must be 4 for the logistic map. (ii) The logistic map start to enter chaotic state when μ is greater than 3.57. For the piecewise logistic map, μ is much smaller than 3.57 when it entering chaotic state.

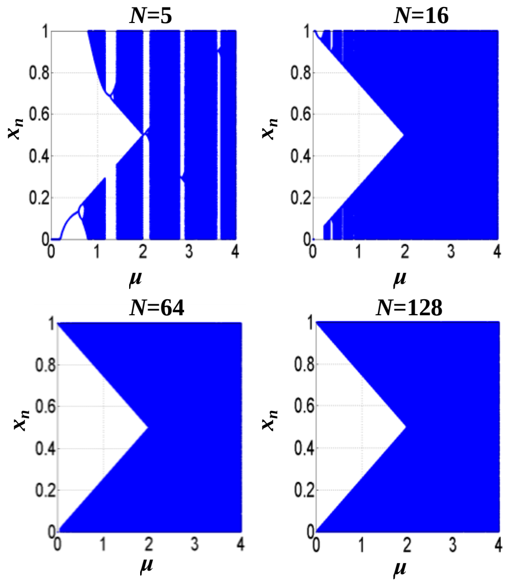

Fig. 4 Bifurcation diagram of the piecewise logistic map

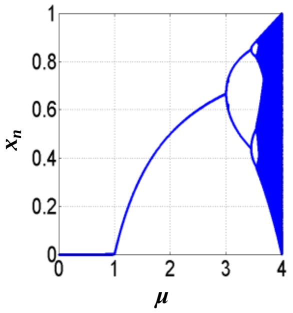

Fig. 5 Bifurcation diagram of the logistic map

2.3.Ergodicity

The piecewise logistic map and the logistic map are iterated when μ is fixed to different values. Then, the distributions of the chaotic state values are obtained and shown Figs. 6 and 7, respectively.

It can be seen from Figs 6 and 7 that the ergodicity of the piecewise logistic map is better than that of the logistic map. Moreover, the ergodictiy of the piecewise logistic map become better when increasing *N*.

2.4.Density Probability

The interval [0, 1] is divided into 1000 subintervals. Then, we iterate the piecewise logistic map with *N* = 64 for 40,000 times and

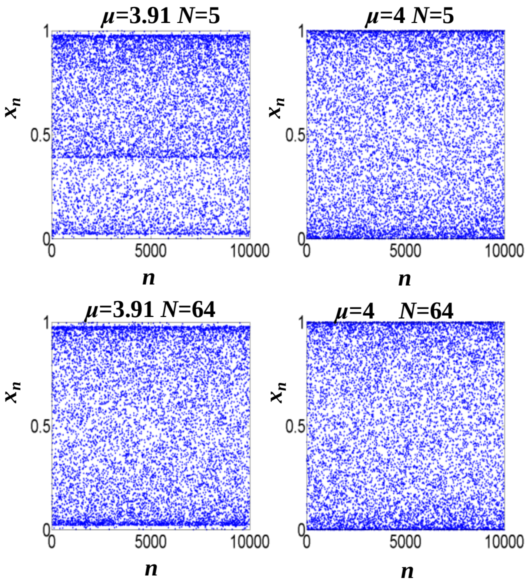

Fig.6 The distribution of state value of piecewise logistic map

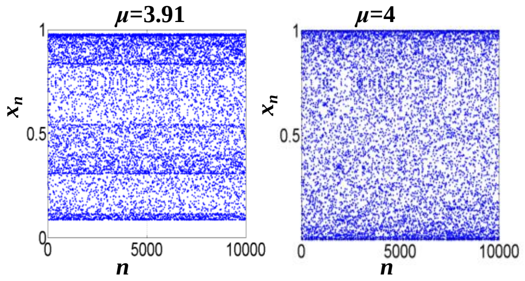

Fig. 7 The distribution of state value of the logistic map

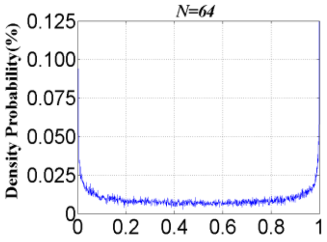

Fig. 8 Densityprobability distribution of the piecewise logistic map

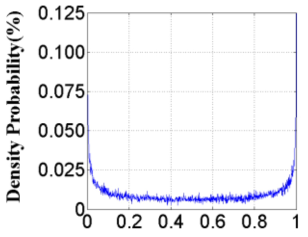

Fig. 9 Densityprobability distribution of the logistic map calculate the probability of the state values appearing in each subintervals. The density probability distribution is shown in Fig. 8, which is similar to that of the logistic map shown in Fig. 9. Furthermore, the same result will obtained when change the value of *N*.

3. The piecewise logistic map with variable μ

The density distribution of the piecewise logistic map is not uniform, which means that the sequences generated by this chaotic map probably has no enough good random properties. To solve this problem, we present the piecewise logistic map with $N = 64$ and suggest that the control parameter μ is changed from 0.1 to 3.9 with step 0.01 when each iteration is completed. If μ is greater than 3.9, reset $\mu = 0.1$.

With the same method in Section 2.4, the density probability distribution of the piecewise logistic map with variable μ is got and shown in Fig.10. According to Figs. 8 and 10, the piecewise logistic map with variable μ has much more uniform density probability distribution than the origin one. Thus, it is more suitable to be used for designing encryption schemes.

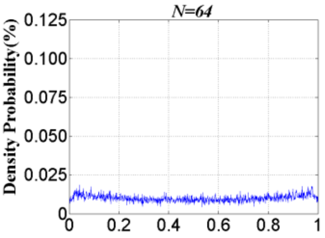

Fig. 10 Density probability distribution of the piecewise logistic map

4 Conclusions

In this paper, the piecewise logistic map is researched. Some properties related to cryptography are shown. Compared to the logistic map, the piecewise logistic map has larger Lyapunov exponent, better bifurcation and ergodicity. To achieving the more uniform densityprobability distribution, the piecewise logistic map with variable control parameters is proposed, which is more suitable to design chaos-base encryption scheme.

Acknowledgements

The work described in this paper was supported by grants from the National Natural Science Foundation of China (No. 61003256), the Natural Science Foundation of CQ CSTC (No. cstc2013jcyjA40017), the Foundation of Chongqing Education Committee (No. KJ120506). the Natural Science Foundation of CQUPT(No. A2011-20)

References

[1] K.-W. Wong, Q. Lin,J. Chen, “Simultaneous arithmetic coding and encryption using chaotic maps”*IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, pp.146-150, 2010.

[2] Wang. XY, Guo. K, “A new image alternate encryption algorithm based on chaotic map”*NONLINEAR DYNAMICS*, vol.76,pp.1943-1950, 2014.

[3] Behnia S, Akhshani A, Akhavan A, Mahmodi H,” Applications of tripled chaotic maps in cryptography”,*Chaos Solitons Fractals*, vol.40,pp. 1505-519,2009.

[4] QC Zhang, R L Tian,W a Halang,” Homoclinic and heteroclinic orbits in a modified Lorenz systerm”, *Information Sciences*, vol. 165, pp.235-245, 2004.

[5] G. Situ,J. Zhang,”Double random-phase encoding in the Fresnel domain ”*Opt. Lett*,vol. 29, pp.1584–1586,2004.

[6]Mandal MK,Banik GD, ChattopadhyayD,” An image encryption process based on Chaotic logistic map”*IETE TECHNICAL REVIEW*,vol.441, pp.441-452, 2009.

[7] Zhang X F, Fan J L,”Piecewise Logistic Chaotic Map and Its Performance Analysis” *Acta Electronica Sinica*,vol.37, pp.720-725, 2009 (in Chinese).