Research Journal of Applied Sciences, Engineering and Technology 5(3): 898-904, 2013
ISSN: 2040-7459; E-ISSN: 2040-7467

Submitted: June 19, 2012 Accepted: July 18, 2012 Published: January 21, 2013

Study on One Modified Chaotic System Based on Logistic Map

[1]Hua Xue, [1]Shubin Wang and [2]Xiandong Meng
[1]Department of Physics and Electronic Science, Binzhou University, Binzhou, 256603, China
[2]Department of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China

Abstract: This study puts a new chaotic system based on logistic. It can avoid several problems in original logistic equation, such as limited parameter range, complex computing and complication of the real circle. The result of the simulation shows its advancement. It is chaotic in boundless range, which can enhance the security of the encrypted system. Less resource is used by the modified equation, which can cut down the complexity of the encrypted system. Its simplicity can improve the computing-speed too. To a certain extent, the new equation can solve the existing problem of the original logistic map and it may help to build a better encrypted system in engineer.

Keywords: Discrete chaos, logistic, single-dimensional

INTRODUCTION

Chaos is a complicated nonlinear system and it has characters which similar to that of noise (Sun *et al*., 2008). Its dynamic behavior is decided by a certain formula, so it is an assured nonlinear system too in a sense. As we know, initial value sensitivity (Lau and Tse, 2003) and the randomicity are the most important characters of chaos systems. The properties of the chaos systems meet the need of cryptology and it has been widely applied in encryption.

Because discrete chaotic system is easy to control and has low complexity, comparing with the continuous chaotic system, it is of high efficiency. As an example of the discrete chaotic systems, Logistic Map has been widely used in many domain, it can be shown by the conference (Xia and Wang, 2009; Zhai and Guo, 2010). Its key space is small, which is also the most important shortcoming of it. In order to find a discrete chaotic system with larger key space, a new discrete chaotic system, which is proposed in reference (Kohda and Tsuneda, 1997), is investigated in this paper. It can be seen that the new chaotic system has better property than the Logistic Map through some analysis.

ANALYSIS FOR LOGISTIC MAP

Logistic Map is the most important discrete chaotic system and the equation of it is described in formula (Zhang and Wang, 2003) 1 as below:

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (1)$$

where, the parameter λ is set to be λ = 3.88 and the initial value is given as $x_1 = 0.3215$.

Then the iterant of it can be shown in Fig. 1 as below:

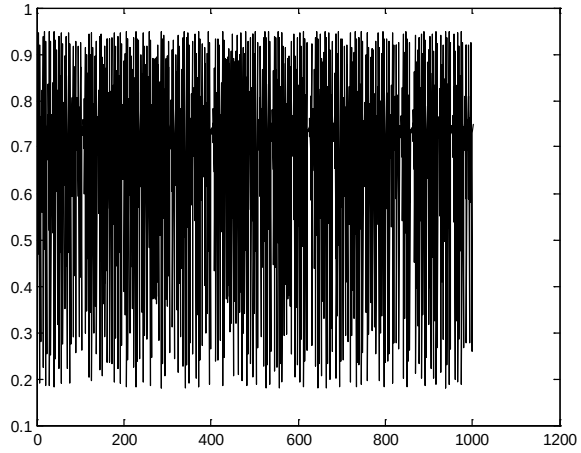

Fig. 1: Time domain waveform for logistic

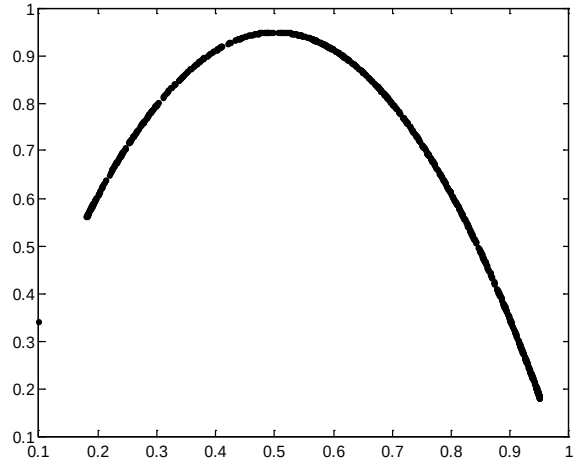

Fig. 2: Phase diagram of logistic map

Corresponding Author: Hua Xue, Department of Physics and Electronic Science, Binzhou University, Binzhou, 256603, China

The x-label is n, which is the number of the iterant. The y-label is the value of the iterant. It can be seen that the iterant of the formula 1 appear to be pseudorandom. Because it is sensitive to the initial value, the chaotic sequence of the system can be used as encryption key in cryptology.

The x-label of the Fig. 2 is x_n and the y-label is x_{n+1}. And it can be seen that the map from x_n to x_{n+1} is not onto mapping. It means that if using the chaotic sequence as encryption key, the security of the encrypted system is not very well.

Where the parameter λ is the x-label, whose range is [0, 4], and the y-label is the value of x_n.

The following conclusions can be achieved from the Fig. 1, 2 and 3:

- The Logistic Map has very good randomicity and the iterant of the map appear to be the noise. These properties make it easy to apply the chaos system in encryption.
- It can be seen from the bifurcation of the Logistic Map that only when the parameter λ is close to 4, it is chaotic. The chaotic sequence generated from the map with this parameter value can be used in encryption system and it will have good performance.

Even if we have got the above advantage of Logistic Map, but there are still some limitations too. They can be concluded as below:

- The range of parameter λ is limited. It can be concluded that if the parameter λ is set to be the other values, the Logistic Map is not chaotic and then the security of the encrypted system, using Logistic Map as key, has to decrease badly.
- The value of all the iterant is in the pale of (0, 1). The range of the values of the iterant implies that the range of the chaotic key is limited too. And it means that the security of the encrypted system is not very well in a sense.

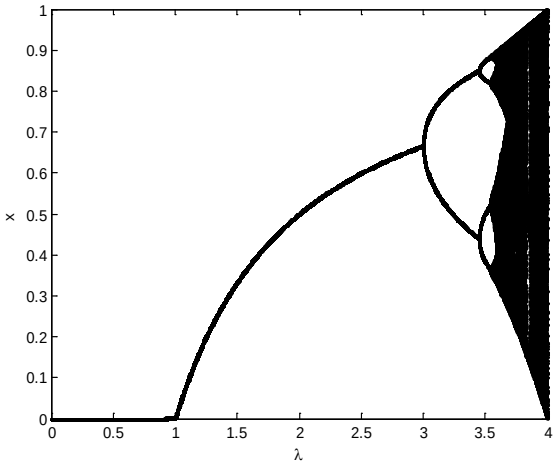

Fig. 3: The bifurcation diagram of the logistic map

As to the above defects in application, the Logistic Map cannot be widely used in encryption system. In order to overcome these defects of Logistic Map, a better chaos system with larger key range and iterant value range is put forward in the next chapter.

ANALYSIS OF A NEW CHAOTIC SYSTEM

A new discrete chaotic system is proposed in reference (Sun and Wang, 2011). It is always to be chaotic and has larger key range. The new chaotic system is shown in formula 2 as below:

$$x_{n+1} = ax_n - x_n^2/\mu \quad (2)$$

where, the parameter a is set to be a = 4 and the value of parameter μ can be set to any non-zero value with no limitation.

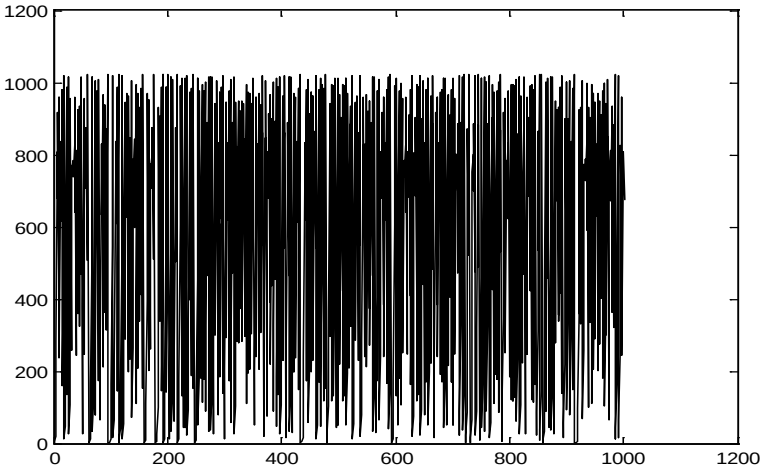

Fig. 4: Time domain waveform for new chaotic system when μ = 256

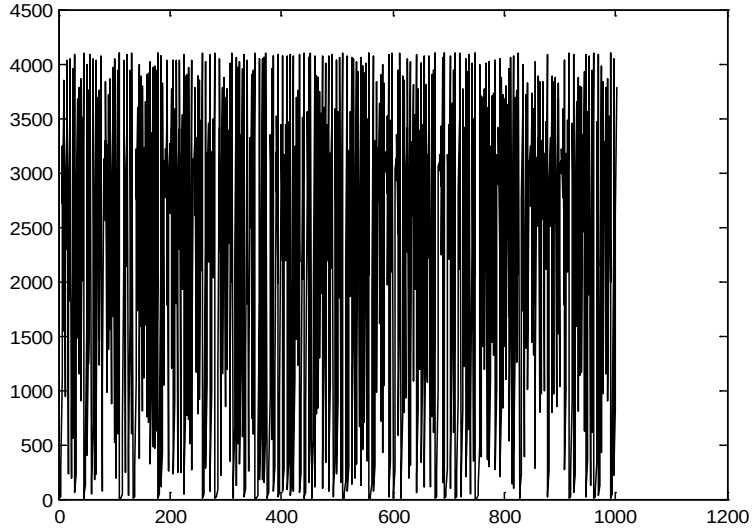

Fig. 5: Time domain waveform for new chaotic system when μ = 1000

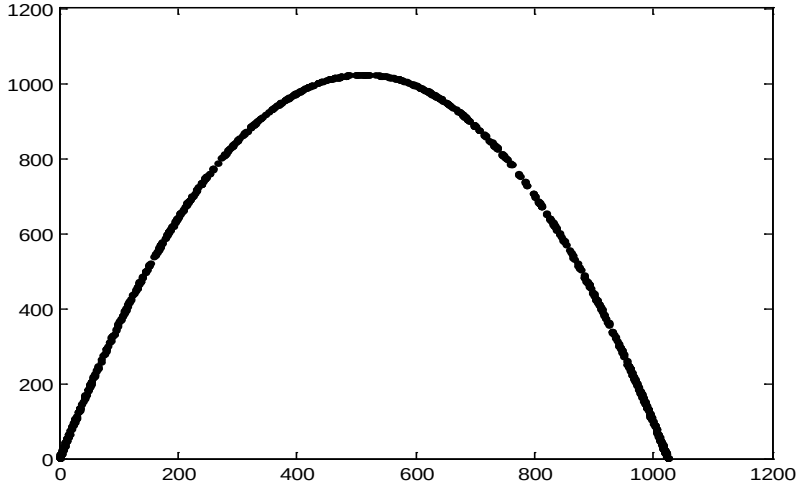

Fig. 6: The attractor of new chaotic system when μ = 256

Analysis of the time domain: As it said before, no matter what the value of the parameter μ is, the new chaotic system keeps chaotic if the parameter is set to be a = 4.

In Fig. 4 and 5, the values of parameter μ of the new chaotic system are separately set to be μ = 256 and μ = 1000, with same initial value x_1 = 1. It can be seen that when the values of the parameter μ of the formula 2 are different from each other, both the different iterant appear to be pseudorandom. Comparing with the Logistic Map, the new chaotic system has larger iterant value range and the range is (0.4 μ). It also means that the key range of the encryption system is wider and the encryption system using the new chaotic system is more secure than that using Logistic Map.

Analysis of the attractor: The value of the parameter μ of the formula 2 is set to be μ = 1000 and then the phase diagram can be shown as below in Fig. 6. The x-label is x_n and the y-label is x_{n+1}.

It can be seen from Fig. 7 that the map from x_n to x_{n+1} is an onto-mapping. It means that the chaotic sequence generated from the new chaotic system distributes in the full range and the randomcity is better than the Logistic Map.

Analysis of bifurcation diagram: The bifurcation diagram of the new chaotic system is shown in Fig. 8 and 9, which have different range for parameter μ in formula 2. The x-label is the value of parameter μ and the y-label is the values of the iterant of formula 2. As it is shown in the figures that the value of μ changes from 1 to 256 in Fig. 8 and changes from 1 to 1000 in Fig. 9.

It can be easily concluded from the Fig 8 and 9 that if the parameter a is set to be a = 4, the new chaotic

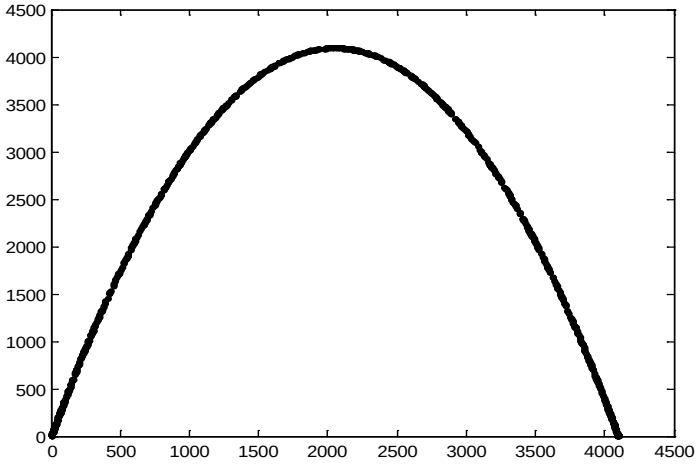

Fig. 7: The attractor of new chaotic system when μ = 1000

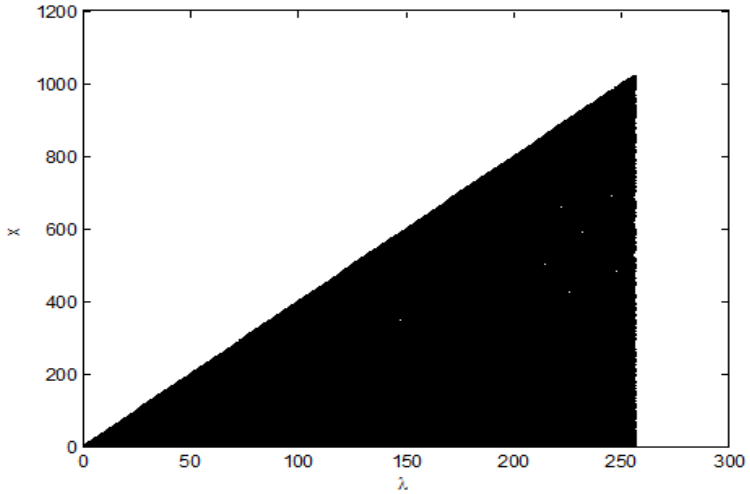

Fig. 8: The parameter μ changes from 1 to 256

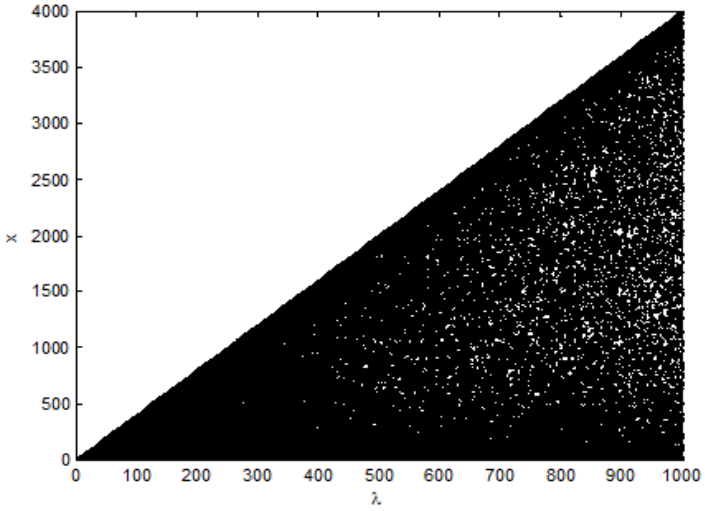

Fig. 9: The parameter μ changes from 1 to 100

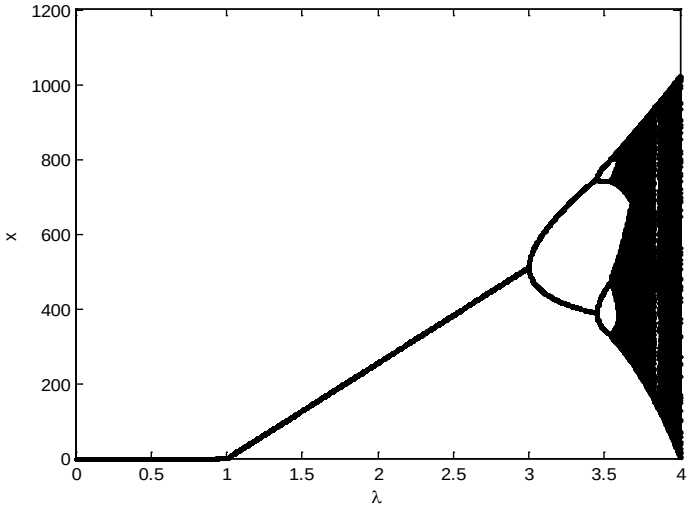

Fig. 10: The parameter μ = 256

system keeps chaotic no matter what the value of the parameter μ is.

If the parameter μ is set to be μ = 256 and the parameter a changes from 0 to 4, the bifurcation diagram is shown in Fig. 10.

It can be seen that the Fig. 10 is similar to the Fig. 3, which is the bifurcation diagram for Logistic Map, but the y-label of the two diagrams are different from each other. The range of iterant of the new chaotic system is much larger than that of Logistic Map. We can conclude that the parameter a in formula 2 decides whether the system is chaotic or not and the parameter μ decides the range of the chaotic iterant.

ANALYSIS OF CHAOTIC SEQUENCE OF THE TWO SYSTEMS

It can be concluded through the above analysis that the new chaotic system has better performance than Logistic Map. The security of the encryption system using the new chaotic map is better than that using Logistic Map. But there is no any chaotic sequence analysis about the new system before and it cannot be certain that the sequence of the new system is better than that of the Logistic Map. Some experiments on chaotic sequence generated from the both chaotic systems are done to make it clearly that which one is better than the other.

Frequency distribution of the chaotic sequences: The frequency of the 0 and 1 of the chaotic sequence is a important standard to test the performance of the sequence. If the number of 0 is close to the number of 1, it means that the sequence has good randomicity.

The procedure of the frequency distribution of the chaotic sequence can be described as below:

Table 1: The frequency of 1 and 0 of the sequence of logistic map

Initial value	Num of 0	Num of 1
0.1	48055	51945
0.2	46234	53766
0.3	48089	51911
0.7	48049	51951

Table 2: The frequency of 1 and 0 of the new chaotic system

Initial value	Num of 0	Num of 1
1	50034	49966
50	50015	49985
100	50035	49965
200	50040	49960

- Choose suitable bit of the iterant to generate the chaotic sequence.
- Computer the system for certain times to get a certain long chaotic sequence.
- Count the number of 0 and 1 of the chaotic sequence and compare the numbers with each other.

The length of both the sequences generated from the two systems is 100000 and the last bit of the iterant is chosen to constitute the sequences.

It can be seen from the table 1 and 2 that the chaotic sequence generated from the new system has better performance and it means that the randomicity of the sequence of the new system is better than that of Logistic Map.

Analysis of the autocorrelation of the chaotic sequences: If the length of a binary sequence is N, then autocorrelation coefficient of it can be described as formula (Kocarev, 1995) (3):

$$f(m) = \frac{\sum_{i=1}^{N-m} b_i b_{i+m}}{N} \quad (3)$$

Where the parameter m is the step length and it is m which decide the value of the autocorrelation coefficient. The less the autocorrelation coefficient changes when the parameter m changes, the better the sequence is Zhao and Liao (2009). And the result of the autocorrelation analysis for both the chaotic sequences generated from Logistic Map and new system is shown as below in Table 3. The result of the autocorrelation analysis shows that the chaotic sequence from the new system is better than that of the sequence from Logistic Map.

Analysis of sensitivity to the initial condition: The procedure of analysis for the sensitivity to the initial condition can be described as following steps:

- Get a certain long chaotic sequence and record the position of 0 and 1
- Make a little change on the initial condition for a chaos system
- Count the number of the 0 and 1 whose position changes

The formula to get the change rate is given as below in formula 4:

$$T = \frac{n'}{n} \tag{4}$$

where,

n' : The number of 0 and 1 whose position changes
n : The total length of the binary sequence

And the test result of sensitivity to initial condition for Logistic Map and the new chaos system is shown by Table 4 and 5.

It can be seen that when the initial condition changed by 0.001, the change rate of the chaotic binary sequence of Logistic Map is 0.23. And when the initial condition changed by 1, the change rate of the chaotic sequence of the new system is 0.25. What the table can express is that the sensitivity of the initial condition for the new chaos system is better than that of the Logistic Map.

Table 3: The results of autocorrelation analysis

M	N	Logistic	New system
0	10000	0.463	0.500
200	10000	0.210	0.240
300	10000	0.202	0.236
400	10000	0.203	0.239

Table 4: Change rate for sequence of logistic map

Initial	Changed	Change rate
0.222	0.223	0.229
0.333	0.332	0.226
0.444	0.445	0.228

Table 5: Change rate for sequence of the new system

Initial	Changed	Change rate
2000	2001	0.245
3300	3301	0.254
6000	6001	0.250

Analysis of lyapunov exponent: It can be concluded from Fig. 9 that the new chaos system keeps chaotic when the parameter a is set to bea = 4. But we need find another way to make sure of it. The Lyapunov exponent is a common method to prove that whether the chaos system is chaotic or not when its parameter changes. The Lyapunov exponent for discrete chaos system can be described in formula 5 as below:

$$lyp = \frac{1}{n}\sum_{i=1}^{n} \ln \left| \frac{df}{dx} \right|_{x=x_i} \tag{5}$$

where, the parameter n is the length of the sequence and f is the chaos map. If lyp>0, it means that the chaos system is currently chaotic with the certain condition. And if lyp≤0, the chaos system is not chaotic under

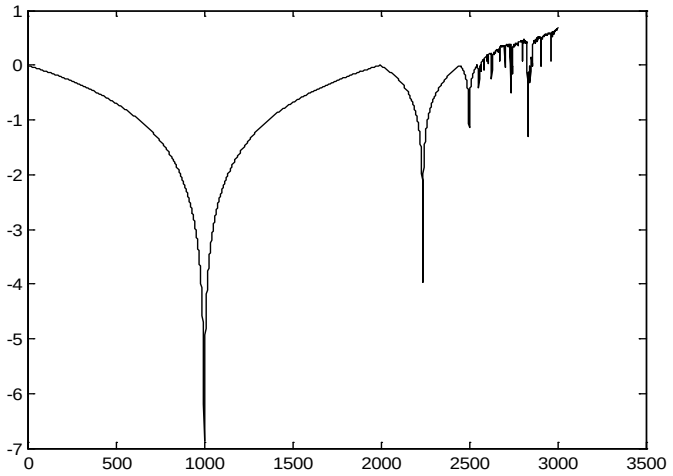

Fig. 11: Lyapunov exponent for logistic map

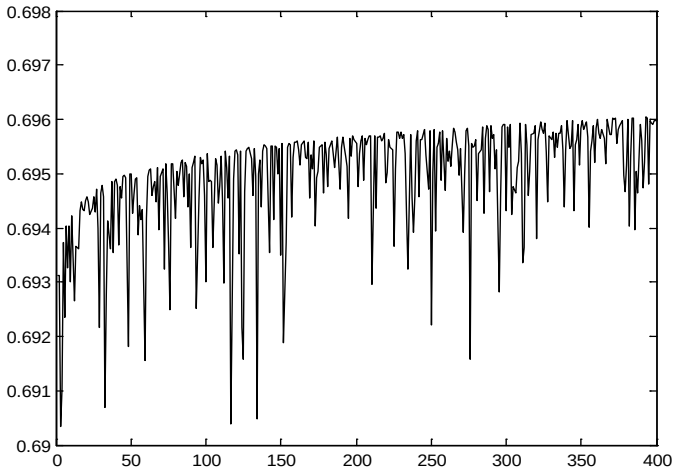

Fig. 12: Lyapunov exponent for new chaos system

current condition (Jiang, 2002; Kocarev, 1995; Zhang and Fan, 2007; Wu and Chen, 2008; Zhao and Liao, 2009).

The Lyapunov exponent for Logistic Map and the new chaos system is computed in MATLAB and the diagram can be shown in Fig 11 and 12.

In Fig. 11 and 12, the x-label is the value of parameter λ or μ and the y-label is the value of lyp.

It can be seen that only when the value of the parameter λ is close to 4, the Logistic Map is chaotic. And no matter what the parameter μ is, the new chaos system keeps chaotic.

CONCLUSION

In order to improve the sequence performance of Logistic Map, a new chaos system proposed in reference (Sun and Wang, 2011), which has larger key space and iterant range and the result prove that the new chaos system has better performance. The comparison is done to prove that the sequence of the new chaos system has better performance than that of Logistic Map. It can be concluded that the new chaos system is better than Logistic Map and it can improve the security of the encryption system.

REFERENCES

Jiang, Z.H.P., 2002. A note on chaotic secure communication systems. EEE Circ. Syst. I., 49(01): 92-96.

Kocarev, L., 1995. General approach for chaotic synchronization with application to communication. Phys. Rev. Lett., 74(05): 5028-5034.

Kohda, T. and A. Tsuneda, 1997. Statistics of chaotic binary sequences. IEEE T. Inform. Theory, 6(03): 104-112.

Lau, F.C.M. and C.K. Tse, 2003. Chaos-Based Digital Communication System. Springer-Verlag, Berlin.

Sun, Y. and G.Y. Wang, 2011. An image encryption scheme based on modified logistic map. The 4th International Workshop on Chaos-Fractals Theories and Applications, 4: 300-304.

Sun, F.Y., S.T. Liu and Q.L. Zh, 2008. A novel image encryption scheme based on spatial chaos map. Chaos. Solitons Fractals, 38(3): 631-640.

Wu, W. and Z.Q. Chen, 2008. Logcal bifureation analysis of a four-dimensional hyperchaotic system. Chin Phy., 17(07): 2402-2432.

Xia, H.X. and M. Wang, 2009. Economic loss for water contaminations in East Lake based on logistic model. International Conference on Environmental Science and Information Application Technology, 10: 287-290.

Zhai, S.J. and J.N. Guo, 2010. The application of e-commerce logistic system based on gridding management: Second ETP/IITA world congress in applied computing. Comput. Sci. Comput. Eng., 14: 491-493.

Zhang, H. and X.F. Wang, 2003. A new image encryption algorithm based on chaos system. Proceeding of IEEE International Conference on Robots, Intelligent Systems and Signal Processing, Changsha, China, pp: 778-782.

Zhang, X.F. and J.L. Fan, 2007. Extended logistic chaotic sequence and its performance analysis. Tsinghua Sci. Technol ., 12(07): 156-161.

Zhao, L. and X.F. Liao, 2009. Design and implemention of chaotic email encryption soft ware. J. Comput. Eng. Appl., 45(6): 101-105.