http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (20): 5487-5491, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5487.5491

Detection Complexity of Chaotic Sequence

[1]Xu Wei, [2]Ding Qun and [3]Zhang Xiaogang
[1]School of Computer Science and Technology, Heilongjiang University, Harbin, 150080, China
[2]School of Electronic Engineering, Heilongjiang University, Harbin, 150080, China
[3]Education Office of Heilongjiang Province, Harbin, 150001, China

Abstract: To generate digital chaotic sequence and apply that in hardware encryption system, this paper analyzes Chaos'complexity quantitative analysis methods and presents the approximate entropy as criterion of measuring the complexity of the chaotic sequences. Set tent and logistic two kinds of chaotic systems as examples, analysis and comparison their complexity.It is proved that the method can distinguish different complex chaos and chaotic sequences on the basis of short observed sequence for judging the criterion mentioned above. Researches show that the complexity of the Logistic map is better than Tent's. The results of the study provide the theoretical and experimental basis for the application of chaotic sequence in the information security communication.

Key words: Chaos, complexity, approximate entropy

INTRODUCTION

Chaos, as a classical complex phenomenon of nonlinear dynamic system, has attracted widespread attention for its broadband, noise-like and sensitive features for initial state. In recent years, with more research on chaos, chaos has replaced the traditional pseudo random sequence in the high density of the commercial and most spread spectrum communication system (Huang and Yin, 2009; Parlitz and Ergezinger, 1994). The encryption method of the password system based on chaos is simple, fast, easy to be realized. The relationship between cryptograph, plaintext and key is very complicated and close and any change of plaintext or key will cause great changes in cryptograph, which makes the encryption system has higher security.

The complexity of the sequence is not only a similarity degree of measurement between chaotic pseudo-random sequence and random sequence, bu also a complexity degree of measurement by using part of the sequence to recovery the whole. The bigger complexity of the sequence is, the smaller the possibility of recovery is. Therefore, the complexity of the sequence is an important index of quantify the performance of chaotic sequence. It is important to research the chaotic complexity.

The research of complexity have been attention by domestic and foreign scholars. Kolmogorov (1965)defined a measure entropy and used it to measure the disordered degree of system movement. And then Lempel and Ziv (1976) realized the measure entropy method by computer. Pincus (1991) proposed the definition of approximate entropy through measuring the complexity of time series and then Bandt and Pompe (2002) proposed permutation entropy for measuring time series. Xiao *et al*. (2004) proposed apply a symbolic dynamics approach for the complexity analysis of chaotic pseudo-random sequences. Next year Larrondo *et al*. (2005) proposed a intensive statistical complexity measure to quantify the performance of chaotic Pseudorandom number generators. Chen *et al*. (2011) proposed a new complexity metric to evaluate the unpredictability of the chaotic pseudorandom sequences based on the Fuzzy Entropy.

Kolmogorov-sinai entropy proposed by Kolmogrov can measure the complexity of chaotic system but it needs a lot of sample space and heavy computation. The approximate entropy is a method of quantize the complexity of time series based on edge probability distribution statistics.It can accurate calculation the complexity of the sequence but the result is influenced by select the different parameters. The symbolic dynamics approach can reduce the degree of dependence on the parameters but before we measure the complexity, we must get the size of symbol space of the initial sequences, which is very difficult for us to obtain the priori knowledge in practice. Permutation entropy is an appropriate complexity measure for chaotic time series, in particular in the presence of dynamical and observational noise, since the method is extremely fast, it seems preferable when there are huge data sets and no time for preprocessing and fine-tuning of parameters.

Because the calculate of approximate entropy is fast, accurate and easy to be realized, in addition the algorithm

Corresponding Author: Ding Qun, School of Electronic Engineering, Heilongjiang University, Harbin 150080, China

can calculation the sequence complexity through very short length of sample space.The article assesses randomness of Logistic mapping via approximate entropy to find the inner link between the parameters of Logistic mapping and complexity and then provides powerful basis for realization the chaotic encryption system by the hardware.

QUALITATIVE CHARACTERISTICS OF CHAOS

Chaos, as one of the nonlinear dynamic systems has the geometry and statistical features that deterministic movement usually do not have, such as local instability while overall stability, strange attractor, continuous power spectrum, positive Lyapunov index, fractal dimension, positive measure entropy and so on. To sum up, the chaos has the following three main qualitative characteristics (Zhao and Fang, 2003): Inherent randomness, Fractal dimension characteristics, Universality.

There is no strict mathematical definition of the chaotic complexity so far, therefore, when we research the chaotic complexity, the main type of complexity parameters we use are entropies, fractal dimensions, Lyapunov exponents and so on (Wang *et al*., 2006).

APEN ALGORITHM

Approximate entropy was proposed by Pincus in 1990.The techniques to determine changing system complexity from data were evaluated. The higher data series' complexity is, the more value of ApEn is. Convergence of a frequently used correlation dimension algorithm to a finite value does not necessarily imply an underlying deterministic model or chaos.

Given a positive integer N and nonnegative integer m, with m = N, a positive real number r and a time-series of data x: = x (1), x (2),... x (N), from measurements equally spaced in time, form a sequence of vectors X (1), X (2),..., X (N-m+1) in R^m, define by X (i) = [x (I), x (i+1), …. x (i+m-1)], next, define for each i, 1 = i = N-m+1, let the distance between two blocks X (I) and X (j) be defined by:

$$d[X(i),X(j)] = \max_{k=1,2,..,m} |x(i+k-1) - x(j+k-1)|$$

Then let:

$$C_i^m(r) = \frac{\text{No. of } j \le N\text{-}m\text{+}1 \text{ such that } d[X(i),X(j)] \le r}{(N\text{-}m\text{+}1)}$$

Now define:

$$F^m(r) = \frac{1}{N-m+1}\sum_{i=1}^{N-m+1}\log C_i^m(r)$$

And:

$$ApEn(m,r,N) = F^m(r) - F^{m+1}(r), m \ge 1$$

ApEn (m, r, N) measures the logarithmic frequency with which blocks of length m that are close together for blocks augmented by one position, with larger values of ApEn implying greater irregularity in x.

ANALYSIS THE COMPLEXITY OF CHAOTIC SEQUENCE

Generated chaotic sequence: The Logistic map is given by:

$$X_{n+1} = \mu X_n(1-X_n),\ 0 \le x \le 1,\ 0 < \mu \le 4 \qquad (1)$$

Figure 1 display the sequence diagram of Logistic map, where iterations and initial value respectively are 1024 and 0.3.

Figure 2 display the bifurcation diagram of Logistic map. Figure 3 display the Lyapunov exponent' trend of Logistic map with change of parameter μ.

Tent mapping is defined as follows:

$$Xn+1 = 1-|1-\mu xn| x \in [0, 1] \qquad (2)$$

Figure 4 display the sequence diagram of Tent map, bifurcation diagram of tent map on the interval [1, 2.4] in Matlab is shown in Fig. 5.

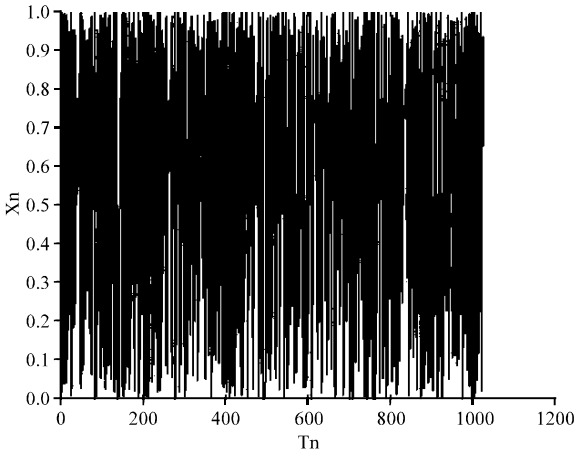

Fig. 1: Sequence diagram of Logistic map

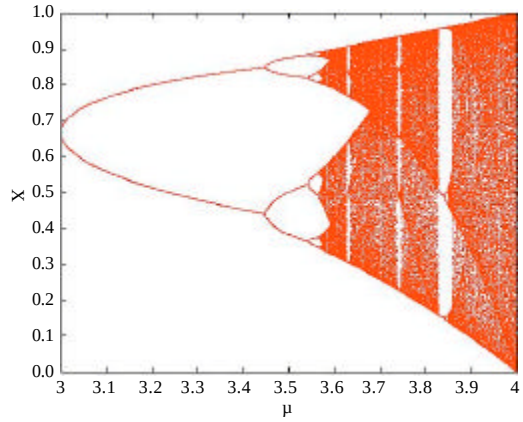

Fig. 2: Orbit diagram for the Logistic map

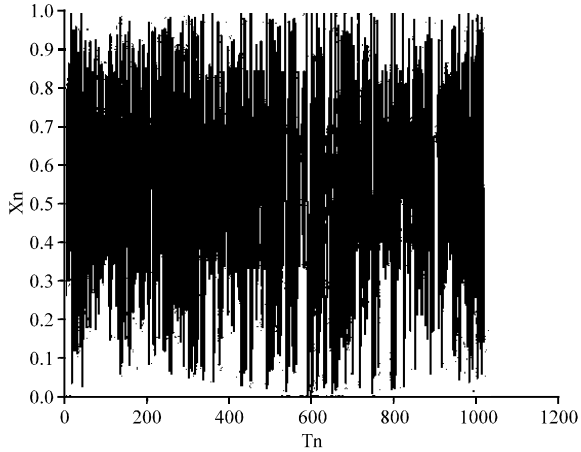

Fig. 4: Sequence diagram of Tent map

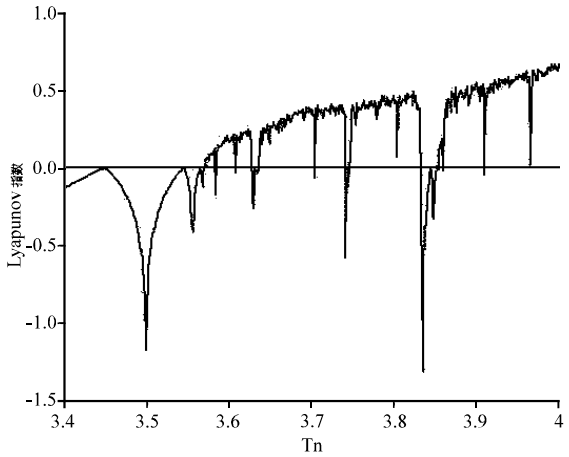

Fig. 3: Lyapunov exponent for the Logistic map as function of parameter μ

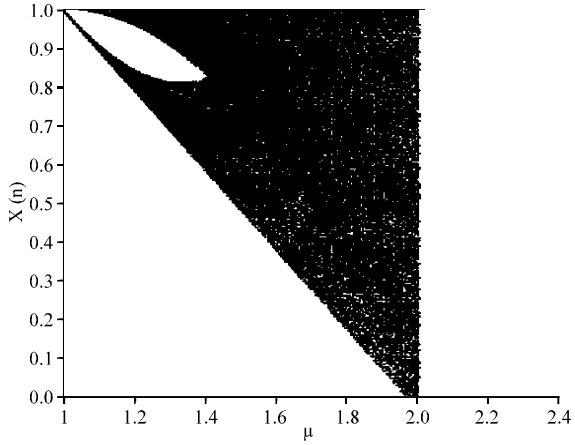

Fig. 5(a-b): Bifurcation diagram of tent map on the interval [1, 2.4]

For choice of m, r and N, we can suppress the dependence of ApEn on them, Pincus (1991) points out the value of ApEn is dependent on N the least, when m = 2, r = 0.1, 0.25 SD_x.

The parameter m is the dimension of distance vector. We demonstrate the utility of ApEn by applying this statistic to Logistic and Tent map, observing the dependence of ApEn on m. The simulation results we obtained for N = 2000 and N = 5000 as shown in Fig. 6 and 7 inrespectively. The results have shown that the value of ApEn when N = 5000 is better then N = 2000 in either case.The value of ApEn are near 0.69 when m = 2, while the Lyapunov exponent of Logistic is 0.69.The ApEn of Tent map is max when m = 2, we thus infer m = 2.

Generally, sample means and standard deviating converge to a limiting value much more quickly than

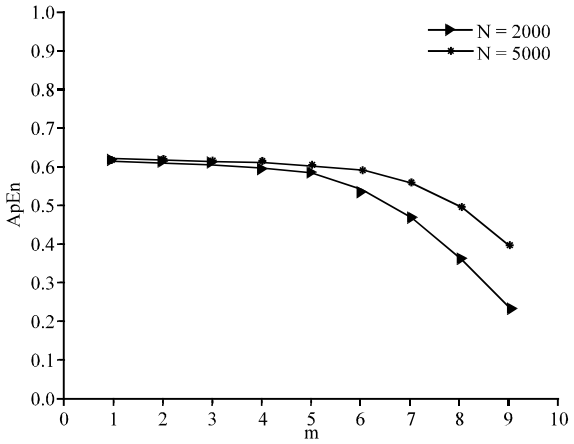

Fig. 6: ApEn of Logistic on m

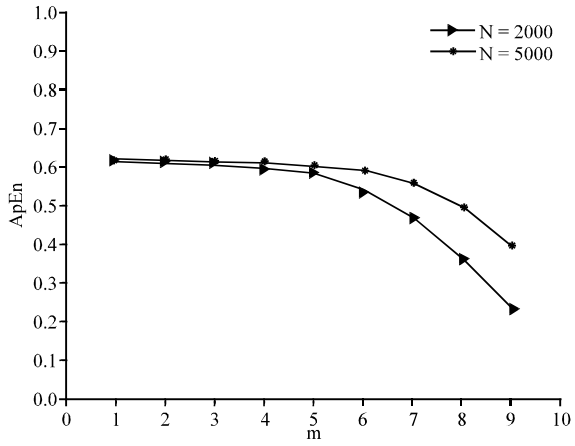

Fig. 7: ApEn of Tent on m

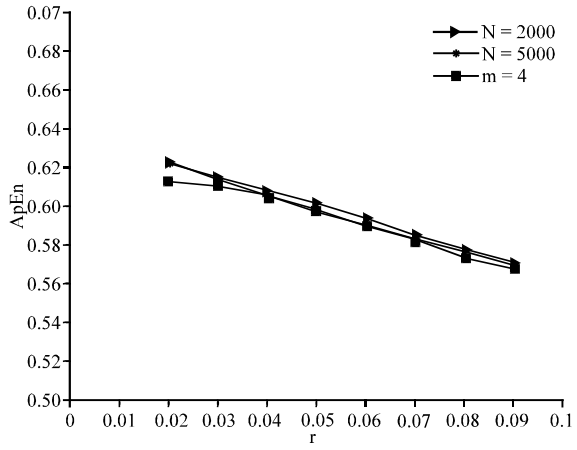

Fig. 9: ApEn of Tent map on r

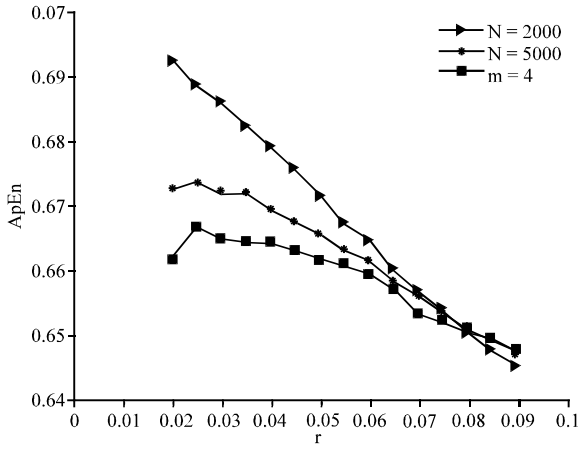

Fig. 8: ApEn of Logistic map on r

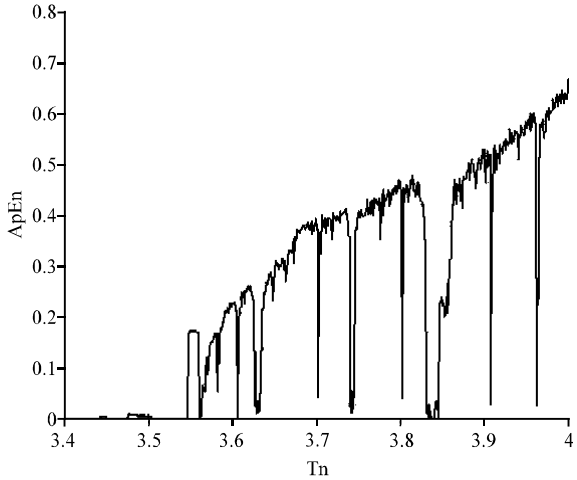

Fig. 10: ApEn of Logistic map on μ

ApEn does. Greater utility for ApEn arises when the means and standard deviations of evolving systems show little change with system evolution. The accuracy of complexity in the chaotic system is determined by parameter r which is a value of the distance. The value of r should be in the scope 0.1~0.25SD_x. We use ApEn algorithm to test the complexity of sequence produced by Logistic mapping and Tent mapping. Figure 8 and 9 are the simulation results we obtained for N = 5000, m = 2, 3, 4. As the results have shown, when r is smaller with m is increase, the value of ApEn is decrease. It demonstrated the m is connected with r and when r is increase all the curve for different m have the same trend, that is the value of r relate to ApEn. The results show that the value of ApEn is better when N = 5000 and m = 2, r<0.04, therefore we recommend r = 0.1 Sd_x.

Then we test the initial value whether impact on ApEn of sequence. The Table 1 and 2 have shown the ApEn of Logistic map and Tent map respectively for different initial values.

Table 1: ApEn of Logistic map

				ApEn = (2, r, N)		
Model type	SD_x	r	x	N = 300	N = 1000	N = 3000
Tent	0.219	0.022	0.1	0.5214	0.5582	0.5659
Tent	0.221	0.022	0.3	0.5294	0.5633	0.5644
Tent	0.220	0.022	0.6	0.5164	0.5526	0.5644
Tent	0.215	0.022	0.8	0.5349	0.5701	0.5580

From the tables we can see, the ApEn is better when N>1000. It demonstrated that the algorithm can calculation the sequence complexity through very short length of sample space. Notice that for both systems, the initial value has little impact on ApEn of sequence.

COMPLEXITY OF THE TWO KINDS OF MAPPING

According to the result, we choose parameters m = 2, r = 0.1 SD_x, N> 1000 and tested the ApEn of sequence produced by Logistic map and Tent map. The results as shown in Fig. 10 and 11.

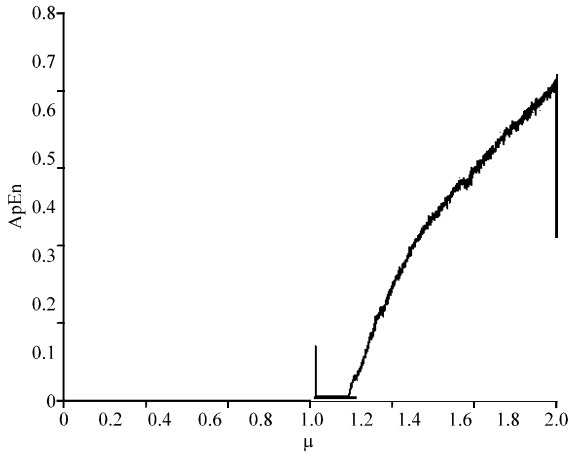

Fig. 11: ApEn of Tent map on μ

Table 2: ApEn of Tent map

				ApEn = (2, r, N)		
Model type	SD_x	r	x	N = 300	N = 1000	N = 3000
Logistic	0.247	0.025	0.1	0.426	0.447	0.445
Logistic	0.247	0.025	0.3	0.404	0.437	0.446
Logistic	0.247	0.025	0.6	0.436	0.455	0.453
Logistic	0.247	0.025	0.8	0.414	0.435	0.443

CONCLUSION

According to the result of figure 8, we can see μ of Logistic map is a basic linear relation with ApEn.Some of these ApEn are very small which corresponding the sequence complexity are very low e.g. μ = 3.837, 3.840, so when we choose the parameters, we should abandon these value. The sequence complexity reaches the maximum value of 0.684 when μ = 4, it is shown that our complexity behaves similar as Lyapunov exponents mentioned above.The figure 9 has shown the max ApEn of Tent map is 0.6104 when μ = 1.897. Application of approximate entropy algorithm test these two kinds of chaotic sequence complexity, we can judge the Logistic map produced by the complexity of the chaotic sequence is better than the Tent map. Tent chaotic mapping has good ergodicity and uniformity but the randomness is not ideal. The results of the study provide the theoretical and experimental basis for the application of chaotic sequence in the information security communication.

ACKNOWLEDGMENT

This study is supported by the National Natural Science Foundation of China (No. 61072072). Innovated Team Project of "Modern Sensing Technology" in colleges and universities of Heilongjiang Province (No. 2012TD007).

REFERENCES

Bandt, C. and B. Pompe, 2002. Permutation entropy: A natural complexity measure for time series. Phys. Rev. Lett., Vol. 88. 10.1103/PhysRevLett.88.174102

Chen, X.J., Z. Li and B.M. Bai, 2011. A new complexity metric of chaotic pseudorandom sequences based on fuzzy entropy. J. Electr. Inform. Technol., 33: 1198-1203.

Huang, L.L. and Q.T. Yin, 2009. Chaos synchronization secure communication system based on output control. J. Electr. Inform. Technol., 31: 2402-2405.

Kolmogorov, A.N., 1965. Three approaches to the quantitative definition ofinformation. Problems Inform. Transmission, 1: 1-7.

Larrondo, H.A., C.M. Gonzalez, M.T. Martin, A. Plastino and O.A. Rosso, 2005. Intensive statistical complexity measure of pseudorandom number generators. Physica A: Stat.l Mech. Appli., 356: 133-138.

Lempel, A. and J. Ziv, 1976. On the complexity of finite sequences. IEEE Trans. Inform. Theory, 22: 75-81.

Parlitz, U. and S. Ergezinger, 1994. Robust communication based on chaotic spreading sequences. Phys. Lett. A, 188: 146-150.

Pincus, S.M., 1991. Approximate entropy as a measure of system complexity. Proc. Natl. Acad. Sci., 88: 2297-2301.

Wang, Y.X., Y.F. Weng and D.L. Zheng, 2006. Study on the complexity analysis Methodology and application to Logisitic map. J. Beijing Technol. Bus. Univ., 24: 38-41.

Xiao, F.H., G.R. Yan and Y.H. Han, 2004. A symbolic dynamics approach for the complexity analysis of chaotic pseudorandom sequences. Acta Phys. Sin., 53: 2877-2880 Acta Phys. Sin., 53: 2877-2880.

Zhao, G. and J.Q. Fang, 2003. Modern information safety and advances in application research of chaos-based security communication. Prog. Phys., 23: 212-252.