Study on Properties of Periodic Chaos and Controlling Method of Islands in Chaos Neural Network Outputs

Hitoaki YOSHIDA, Mitsuaki SASAKI, Takeshi MURAKAMI and Satoshi KAWAMURA

Faculty of Education, Iwate University, Japan

hitoaki@iwate-u.ac.jp

Abstract. The properties of periodic chaos from CNN outputs changing the number of islands have been studied in detail. As the result of NIST SP800-22 tests the pseudo-random number from periodic chaos should not be used for security system. The correlation coefficient between subseries is normally negligible (< 0.01), because the 2 subseries are independent. Periodic chaos, however, has only 2 modes, (i) two subseries simultaneously visit the same island (plus correlation), (ii) both series singly visit the other island (negative correlation). In this system only plus correlation is observed. Therefore periodic chaos can be numerically detected by correlation coefficient, so that periodic chaos is removed easily for a security system.

Key words. periodic chaos, chaos neural network, pseudo random number

1. Introduction

A simple Java program which is made by a university class has been slightly modified as a chaos simulator. The modified program can allow the student to simulate chaos time series, visually and instinctively. It can become an effective GUI probe for the complex system which has sensitive dependence on initial conditions. The results are tested and confirmed with the high-speed computer in the computer center of Iwate University.

We have studied on the chaos neural network (CNN) that consists of conventional artificial neurons and generates chaotic outputs [1].

In this study, we have investigated properties of periodic chaos from CNN and controlling method of the number of islands (N_i). The effect of periodic chaos to randomness of the generated pseudo-random number series has been studied in B-6nn.

2. Results and Discussion

The experiments have been performed by the method based on ref. [3]. The result of simulation is shown in **Table 1** and the attractor of periodic chaos is shown in **Fig.1**. The time series has been analyzed by chaos time series analysis, fractal analysis and NIST SP800-22 tests for cryptographic applications. [4] The results of analysis are shown in **Table 2-3**.

Table 1. Number of Islands and Range of Input.

Number of Islands	Range of Input Value
2	3.495 ~ 3.508
4	3.468 ~ 3.478
4	3.448 ~ 3.450
8	3.4388 ~ 3.4400
16	3.4373 ~ 3.4388
32 <	3.4368 ~ 3.4372

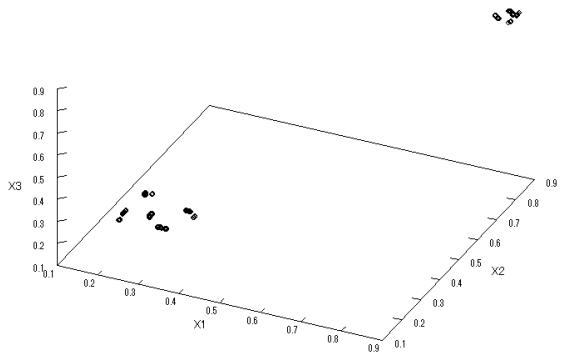

Fig.1. 3D-Attractor Based on Three Subseries (α, β, γ) of Periodic Chaos (N_i = 32, I = 3.437).

Table 2. Selected Results of Analysis on α Series of Periodic Chaos.

N_i	I	p [a]	q [b]	OT [c]	UN [c]	RE [c]	RV [c]	LC [c]
2	3.5020	16393460	73671074	0.80%	0.50%	0.38%	0.06%	0.50%
4	3.4730	115895678	74913014	0.10%	0.60%	0.48%	0.15%	0.10%
4	3.4490	41033918	39624368	0.90%	3.80%	0.31%	0.08%	0.20%
8	3.4394	97611218	36152720	0.50%	0.20%	0.49%	0.12%	0.10%
16	3.4385	49573346	1226186	3.70%	0.20%	0.40%	0.14%	0.10%

a) The period of CNN. b) The transition time (q) is roughly estimated in error by less than $\pm 10^6$. c) The averaged ratio of failed tests (%) in NIST SP800-22 tests. OT: over-lapping template matching test, UN: Maurer's "universal statistical" test, RE: random excursions test, RV: random excursions variant test, LC: linear complexity test.

The latest version NIST SP800-22 test suite (sts-2.1.2) is used which corrects problems of OT test and so on. Maurer's "universal statistical" test (UN) has been improved according to Coron's approximation.

The orbit of periodic chaos always visits 2^n islands with regularity. [2] The results of the NIST tests for periodic chaos are also shown in **Table 2**; the part of the OT tests and the UN tests are considerably worse. Periodic chaos is known to be also ergodic but not mixing. The ergodic property can be evaluated through the NIST tests, because UN test is designed to be able to detect any one of the very general class of statistical defects that can be modeled by an ergodic stationary source. There is no contradiction on ergodicity of chaotic maps. The cause of the worse results of OT and UN test, however, is now under investigation.

The pseudo-random number from periodic chaos should not be used for security system. The correlation coefficient between two subseries is shown in **Table 3**, where the series means whole bits not lower 24 bits. The correlation coefficient between subseries is normally negligible (< 0.01), because the 2 subseries is independent. Periodic chaos, however, has only 2 modes, (i) two subseries simultaneously visit the same island (plus correlation), (ii) both series singly visit the other island (negative correlation). In this system only plus correlation is observed. Therefore periodic chaos can be numerically detected by correlation coefficient, so that periodic chaos is removed easily for a security system.

3. Conclusion

The number of islands in periodic chaos from CNN outputs has been controlled well. The properties of periodic chaos changing the number of islands have been studied in detail. In future work, the authors will investigate the relationship among periodic chaos and ergodicity or mixing character.

Table 3. Correlation Coefficient between Two Subseries.

N_i	Correlation coefficient		
	α–β	β–γ	α–γ
2	0.941	0.943	0.944
2	0.845	0.842	0.854
4	0.897	0.896	0.992
8	0.902	0.902	0.999
16	0.902	0.902	0.999
32	0.902	0.902	0.999

Acknowledgements

The calculations in this study have performed with the SGI UV-100 in Iwate University Super-Computing and Information Sciences Center (ISIC). Special thanks to the staff members of ISIC.

References

[1] H. Yoshida, K. Yoneki, Y. Tsunekawa and M. Miura, "Chaos Neural Network," Proceedings of Papers, ISPACS'96, vol. l of 3, 16.1.1-5, 1996.

[2] J. M. T. Thompson, H. B. Stewart, "Nonlinear dynamics and chaos: geometrical methods for engineers and scientists," Wiley, 1986.

[3] H. Yoshida, A, T. Murakami, T. Inao and S. Kawamura, "Origin of Randomness on Chaos Neural Network," Trends in Applied Knowledge- Based Systems and Data Science, LNAI 9799, Springer, pp.587-598, 2016.

[4] H. Yoshida, T. Murakami, and S. Kawamura, "Study on Testing for Randomness of Pseudo-Random Number Sequence with NIST SP800-22 rev. la," Technical Reports of IEICE, 110 (2012), 13-18.