Implementation of Chaos Neural Network which Generates Multi-Subseries with Different Periods

Hitoaki YOSHIDA, Mitsuaki SASAKI and Takeshi MURAKAMI

Faculty of Education, Iwate University, Japan

hitoaki@iwate-u.ac.jp

Abstract. A chaos neural network (B-6nn) which generates three independent subseries has been implemented. The sub-series afford different chaos orbits, respectively. The results of NIST SP800-22 tests also have been fine, if pseudo-random numbers are extracted from the lower-24-bit of an output in B-6nn. The whole period of outputs of B-6nn has been estimated ca. 1.58×10^{22}. Compared with the whole period of the conventional chaos neural network (C-4nn) which consists of 4 neurons 10^{16}-10^{18}, the whole period of B-6nn has been considerably improved. The method will be applied to multi-subseries more than three subseries in future work.

Key words. chaos, neural network, multi-subseries, pseudo random number

1. Introduction

We have studied on the chaos neural network (CNN) that consists of conventional artificial neurons and generates chaotic outputs [1]. We also have applied the CNN to a stream cipher [2-5], and have commercialized the CNN cipher.

In this work, we have designed a novel CNN (**Fig. 1**) which generates chaos multi-subseries.

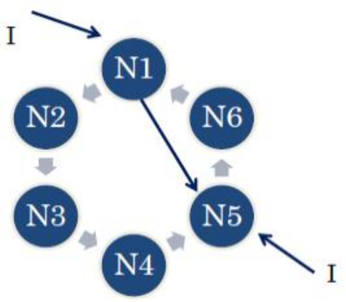

Fig. 1. CNN having bicyclic structure (B-6nn). *I* is an external input.

2. Results and Discussion

The output of B-6nn is separated 3 independent subseries (SS); α, β, γ series with time *t* (Eq.1-3).

$$\alpha(k) = \{x(t) \mid t = 3k,\ k = 0, 1, 2...\} \quad (1)$$

$$\beta(k) = \{x(t) \mid t = 3k+1,\ k = 0, 1, 2...\} \quad (2)$$

$$\gamma(k) = \{x(t) \mid t = 3k+2,\ k = 0, 1, 2...\} \quad (3)$$

We have tried to design the B-6nn so that each subseries have different periods by following 3 methods. Then a whole period of CNN is expected to extend greatly.

Method 1: To use different initial values.

Method 2: To determine parameters as Lyapunov exponents (λ) of subseries are different.

Method 3: To use a different slope of sigmoid function (S) for each subseries.

The experiments have been performed by the method based on ref. [4]. The time series has been analyzed by chaos time series analysis, fractal analysis and statistical tests for cryptographic applications (NIST SP800-22). Time series of B-6nn is embedded in 6-dimensional phase space. Poincare sections of the strange attractor in 4-dimentional phase space are shown in **Fig.2-3**. The time series has also plus Lyapunov exponents, which is characteristic of chaos time series. Results are shown in **Table 1-3**.

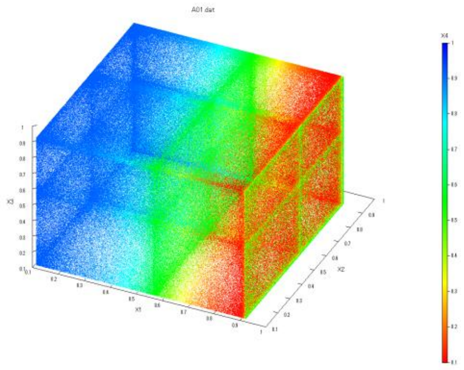

Fig. 2. Poincare sections of the strange attractor in 4-dimentional phase space (*x*1, *x*2, *x*3, *x*4).

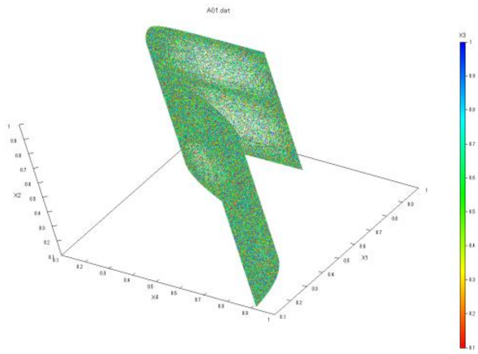

Fig. 3. Poincare sections of the strange attractor in 4-dimentional phase space (*x*4, *x*1, *x*2, *x*3).

Table 1. Results of **Method 2** for Each SS.

SS	Period (p)	q a)	λ b)
α	34242899	144296792	0.160
β	34242899	145196798	0.241
γ	47300630	17760110	0.155

a) The transition time (q) is roughly estimated in error by less than $\pm 10^6$.
b) A Lyapunov exponent.

Table 2. Results of **Method 3** for Each SS.

SS	p	q
α	145556010	10824240
β	190084691	107145918
γ	143951514	103919052

Table 3. Part of NIST Test Results (**Method 3**).

SS	FR	RU	OT	LC
α	0.0	0.0	0.0	0.3
β	0.0	0.0	1.2	0.1
γ	0.0	0.0	0.1	0.1

3. Conclusion

The results of **Method 1** and **2** are negative. Only **Method 3** has successfully generated three sub-series which have different periods. The slope of sigmoid functions are S_α = 1.600, S_β = 1.590 and S_γ = 1.585, respectively.

The results of NIST tests also have been fine, if pseudo-random numbers are extracted from the lower-24-bit of an output in B-6nn. The period of outputs of B-6nn has been estimated ca. 1.58×10^{22}. Compared with the period of conventional C-4nn 10^{16}-10^{18}, the period of B-6nn has been considerably improved.

The method will be applied to multi-subseries more than three subseries in future work.

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] S. Kawamura, H. Yoshida and M. Miura, "Minimum Constituents of Chaos Neural Network Composed of Conventional Neurons," Journal of IEICE (A), J84-A, pp.586–594, 2001.
[3] H. Yoshida, 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] Hitoaki Yoshida, Takeshi Murakami, Zhongda Liu, "High-Speed and Highly Secure Pseudo-Random Number Generator based on Chaos Neural Network," Frontiers in Artificial Intelligence and Applications, IOS Press, Vol.276, pp.224-237, 2015.
[5] 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, pp.13-18, 2012.