Proceedings of EPNACS 2011 within ECCS'11
Emergent Properties in Natural and Artificial Complex Systems
Vienna, Austria - September 15, 2011

NEW ALTERNATE LOZI FUNCTION FOR RANDOM NUMBER GENERATION

Andrea Espinel, Ina Taralova and René Lozi *†

Abstract. An improved Lozi function with alternate coefficients has been proposed. The modifications in the model allow to remove the holes in the attractor which are not desirable, but appeared in the previous Lozi function; in this way, an everywhere dense attractor can be obtained. Moreover, the strong sensitivity to the type of binarisation (conversion of real values to 0 and 1) has been demonstrated; this conversion to binary numbers is instrumental to apply the NIST tests for randomness. The results have been validated and compared via NIST tests, for the different methods of quantization. Finally, is has been verified that the random properties of the output signal have been improved thanks to the following strategies : under-sampling of the output signal, and the system order increasing.

Keywords. Nonlinear dynamical system, Lozi function, NIST test, discrete-time map, dense chaotic attractor, pseudo random number generator

1 Introduction

The accelerated development of modern data transaction applications such as telecommunications requires encoding techniques with higher standards of security. Classically, these encoding sequences are obtained using Pseudo Random Number Generators (PRNG). As an efficient alternative, the chaotic-based generators are used to achieve even higher demanding encryption standards. Indeed, the chaotic systems exhibit a plethora of properties which make them suitable to meet the above requirements. The advantage to use chaotic systems lies in their extreme sensitivity to small parameter and initial conditions variations: in this way, as many different chaotic carriers as wanted can be generated.

However, the appropriate selection of a chaotic map that satisfies cryptographic applications requirements is a huge problem. It has to be emphasized that all chaotic maps are not applicable, because the chaotic generator - which is deterministic - has to satisfy at the same time the criteria for closeness to random signals. Therefore many practical problems arise, from the choice of the chaotic generator and its parameters, to the chaotic properties verification after the quantisation. Ideally, for cryptographic applications and higher security, an everywhere dense chaotic attractor is required, so all chaotic signal samples shall appear with the same probability (indeed, if there are holes in the chaotic attractor, the values of the state vector corresponding to the holes will never take place). Lozi had demonstrated that highly efficient discrete-time chaotic generators can be obtained from quite simple models such as the piece-wise linear ones, under some conditions [3]. To evaluate the random properties of these generators, a set of statistical based test known as NIST test developed by the National Institute of Standards and Technology have been used. A first coupled chaotic map confined to the 2D torus has already been proposed as a PRNG in [1], which random characteristics have been validated using the NIST tests. Nevertheless, since the state variables were not equidistributed, it has been demonstrated that the chaotic attractor exhibited holes delimited by the discontinuity lines and their forward iterates [1]. Therefore, there have been regions in the state space which the system orbits never visited, thus deteriorating the randomness.

2 System Definition

To improve the latter results, in this paper we deal with the new Lozi system with alternate coupled maps, confined to the p-dimensional torus $T^p = [-1, 1]^p$ by the map $M_p : T^p \Rightarrow T^p$

$$\begin{aligned} x^1_{n+1} &= 1 - 2\left|x^1_n\right| + k^1 \times x^2_n \\ M_p : x^2_{n+1} &= 1 - 2\left|x^2_n\right| + k^2 \times x^3_n \\ &\vdots \\ x^p_{n+1} &= 1 - 2\left|x^p_n\right| + k^p \times x^1_n \end{aligned} \tag{1}$$

where the parameters $k^i = (-1)^{i+1}$. A previous model with non alternate coefficients has been proposed in [1], with $k^i = 1$. The state variables are contained on the

*Andrea Espinel and Ina Taralova are with IRCCyN, UMR CNRS 6597, Ecole Centrale de Nantes, France. E-mails: andrea.espinel-rojas, ina.taralova@irccyn.ec-nantes.fr

†René Lozi is with Laboratoire J.A. Dieudonné, UMR CNRS 6621, Universit de Nice Sophia-Antipolis, France. E-mail:lozi@unice.fr

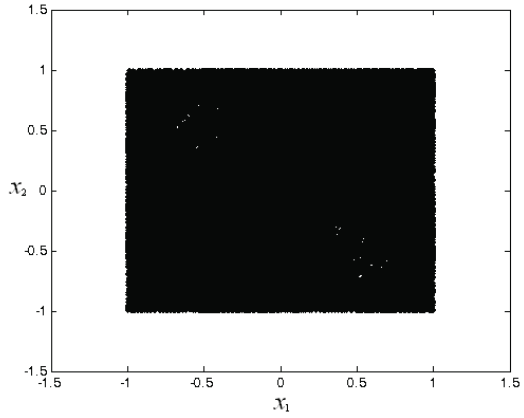

Figure 1: Map M_2 (1) on the torus $T^2 = [-1, 1]^2$

torus:

$$\begin{aligned} &if\ x_{n+1}^j = 1 - 2\left|x_n^j\right| + k^j \times x_n^{j+1} < -1 \\ &\qquad add\ 2 \\ &if\ x_{n+1}^j = 1 - 2\left|x_n^j\right| + k^j \times x_n^{j+1} < -1 \\ &\qquad substract\ 2 \end{aligned} \tag{2}$$

where $|x_n|$ denotes the absolute value of x_n. The alternate sign modification proposed in this paper eliminates the holes from the previous model (with only positive signs), and therefore the resulting basin of attraction is everywhere dense, which is very satisfactory for the RNG applications, see Figure 1. (The transient of 10.000 points has been cut off).

3 Results and Discussion

The random properties validation of a 4- dimensional system has been carried out. Additionally, the chaotic carrier output needs to be quantized and binarised (0 and 1) in order to be validated as being random using NIST tests [5]. First, the tests validate by default a sequence as being random (called the null hypothesis H0), and the idea is to show that there is no enough evidence to reject this proposition. For our application, different methods of binarisation(converting real signals to binary ones) have been implemented and compared:

A first 1-bit binarisation has been applied to the system (1) output:

$$\begin{aligned} &if\ y_n \geq 0 && b = 1 \\ &else && b = 0 \end{aligned} \tag{3}$$

The results for the 4-dimentional system have shown to be highly sensitive to the type of binarisation. Standart single (32 bits) and double (64 bits) precision types of binarisation as the IEEE754 form [6] have been compared. Therefore, after testing different methods, a 32-bit binarisation has been chosen as being the most suitable solution: Since the system is confined to the p-dimensional torus $T^p = [-1, 1]^p$, 31 bits are assigned to represent the decimal part, and 1 bit to the sign.

To illustrate the results, the NIST test for the four dimensional Lozi system M_4 (1) with parameters $\left[k^1, k^3\right] = 1$, $\left[k^2, k^4\right] = -1$ are shown in Table 1. For comparison, the same conditions as in [1] have been chosen:

Length of the original sequence: 10^8 bits
Length of *bit string*: 1M
Quantity of *bit strings*: 100

The output of the system has been arbitrary chosen as being: $y = x_4$.

P-VALUE	PROPORTION	STATISTICAL TEST
0.419021	100/100	Frequency
0.213309	100/100	BlockFrequency
0.978072	99/100	CumulativeSums
0.964295	99/100	CumulativeSums
0.075719	100/100	Runs
0.867692	99/100	LongestRun
0.494392	99/100	Rank
0.334538	99/100	FFT
0.213309	99/100	NonOverlappingTemplate
0.616305	99/100	OverlappingTemplate
0.779188	100/100	Universal
0.474986	99/100	ApproximateEntropy
0.452799	68/69	RandomExcursions
0.063482	69/69	RandomExcursionsVariant
0.437274	98/100	Serial
0.739918	99/100	LinearComplexity

Table 1: NIST test for the 4^{th} order Lozi function (1)

Furthermore, as the results show their independence from the initial conditions, every *bit string* in this first test is the resulting sequence of a different randomly chosen initial condition. The criterion for a successful test is that the p-value has to be superior to the significance level (0.01 for this case). This quantifier evaluates the uniformity of the zeros and the ones distribution in the sequence. For the present model (1), all tests have been successful thus the sequence can be accepted as being random. Thus, the results demonstrate that the new system has better statistical performances than the initial system without alternate coefficients presented in [1].

Finally, to improve the random properties of the signal, two possible strategies are suggested: undersampling of the output signal, or increasing the system order.

Different under-samplings have been tested from which the "1 out of 10" showed to be particularly successful. The "1 out of 10" under-sampling strategy results are shown in Table 2.

For the second method, the random properties validation of a 10-dimensional system has been carried out and the results are shown in Table 3. The conditions for the NIST test are identical to the NIST test for the

4-dimentional Lozi system. In addition, the initial condition has been randomly chosen:

$$x_0 = [-0.3365, 0.9501, 0.8913, -0.7764, 0.0185, 0.4447, 0.7919, -0.9218, -0.9355, 0.0579]$$

The output of the system has been arbitrary chosen as being: $y = x_{10}$.

P-VALUE	PROPORTION	STATISTICAL TEST
0.911413	99/100	Frequency
0.759756	97/100	BlockFrequency
0.897763	100/100	CumulativeSums
0.955835	99/100	CumulativeSums
0.122325	99/100	Runs
0.474986	99/100	LongestRun
0.911413	97/100	Rank
0.366918	99/100	FFT
0.419021	97/100	NonOverlappingTemplate
0.334538	99/100	OverlappingTemplate
0.935716	100/100	Universal
0.816537	98/100	ApproximateEntropy
0.128379	63/63	RandomExcursions
0.654467	61/63	RandomExcursionsVariant
0.554420	98/100	Serial
0.678686	99/100	LinearComplexity

Table 2: NIST test for the 4^{th} order system (1), "1 out of 10" under-sampling

P-VALUE	PROPORTION	STATISTICAL TEST
0.213309	100/100	Frequency
0.108791	98/100	BlockFrequency
0.075719	100/100	CumulativeSums
0.719747	100/100	CumulativeSums
0.719747	100/100	Runs
0.108791	100/100	LongestRun
0.816537	98/100	Rank
0.946308	98/100	FFT
0.115387	99/100	NonOverlappingTemplate
0.798139	98/100	OverlappingTemplate
0.058984	100/100	Universal
0.616305	98/100	ApproximateEntropy
0.054199	60/60	RandomExcursions
0.232760	59/60	RandomExcursionsVariant
0.437274	99/100	Serial
0.401199	100/100	LinearComplexity

Table 3: NIST test for the 10^{th} order Lozi function (1)

The improvement of random properties of both strategies has been corroborated by the experimental results.

4 Conclusion

A new new alternate Lozi function confined to the torus has been proposed as a pseudo random number generator. Unlike the previous model, here the chaotic attractor is everywhere dense and there are no holes inside, in this way all output values are supposed to appear with the same probalility. Therefore, the new alternate Lozi function proposed in this paper has proved to be more efficient than the first one (without alternation of the coefficients). Moreover, the fourth order system has been analyzed and all the NIST tests for randomness have been successfull for the representative test sequences. Finally, a higher order system and an under-sampling of the output signal has been added and the results have shown to be very satisfactory.

By consequence, the proposed PRNG could be used for encryption and many other applications wherever a random number generator is required.

References

[1] A. Espinel, I. Taralova, R. Lozi, "Dynamical and Statistical Analysis of a New Lozi Function for Random Numbers Generation," *PHYSCON 2011*, León, Spain, 5 − 8 September, 2011.

[2] R. Lozi, "Random properties of ring-coupled tent maps on the torus", submitted to *Discrete and continuous Dynamical Systems Series-B*.

[3] R. Lozi, "New enhanced chaotic number generators", *Indian Journal of Industrial and Applied Mathematics*, vol.1, pp. 1-23, 2008.

[4] S. Hénaff, I. Taralova, R. Lozi, "Statistical and spectral analysis of a new weakly coupled maps system", *Indian Journal of Industrial and Applied Mathemaics*, vol 2. N2, pp. 1-18 (to appear).

[5] A. Rukhin, et al, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST (2001)*, http://csrc.nist.gov/rng/.

[6] W. Kahan, "IEEE Standard 754 for Binary Floating Point Arithmetic, *Lecture Notes on the Status of IEEE 754*, Elect. Eng. & Computer Science University of California, Berkeley CA 94720-1776, May 1996.