NEW ALTERNATE LOZI FUNCTION FOR RANDOM NUMBER GENERATION

Andrea Espinel Rojas, Ina Taralova, René Lozi

NEW ALTERNATE LOZI FUNCTION FOR RANDOM NUMBER GENERATION

Andrea Espinel, Ina Taralova
IRCCyN, UMR CNRS 6597
Ecole Centrale de Nantes
France
andrea.espinel-rojas, ina.taralova@irccyn.ec-nantes.fr

René Lozi
Laboratoire J.A. Dieudonné, UMR CNRS 6621
Université de Nice Sophia-Antipolis
France
lozi@unice.fr

Introduction

The accelerated development of modern data transactions 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. 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. 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. To evaluate the random properties of these generators the National Institute of Standards and Technology has developed a set of statistical-based test known as NIST tests. 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, the chaotic attractor exhibited holes delimited by the discontinuity lines and their forward iterates. Therefore, there have been values which the signal never took, and that impact deteriorates the randomness.

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 $M_p : T^p \Rightarrow T^p$

$$M_p:\ \begin{aligned} x_{n+1}^1 &= 1-2\left|x_n^1\right| + k^1 \times x_n^2 \\ x_{n+1}^2 &= 1-2\left|x_n^2\right| + k^2 \times x_n^3 \\ &\vdots \\ x_{n+1}^p &= 1-2\left|x_n^p\right| + k^p \times x_n^1 \end{aligned} \qquad (1)$$

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 torus:

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

$|x_n|$ denotes the absolute value of x_n.

The alternate sign modification 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 fig. 1. (The transient of 10.000 points has been cut off).

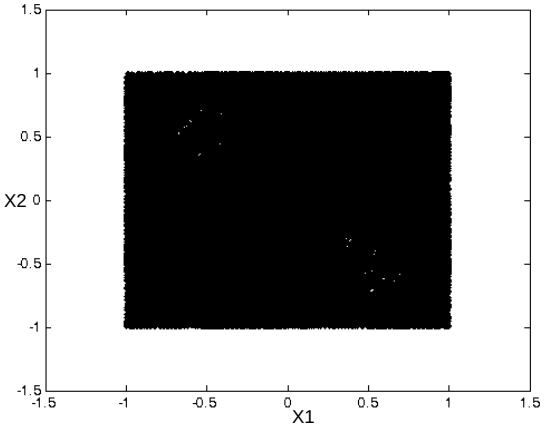

Figure 1. Map M_2 (1) on the torus $T^2 = [-1,1]^2$

Results and Discussion

The random properties validation of a 4-dimensional system has been carried out. Additionally, the chaotic carrier output needs to be quantised and binarised (0 and 1) in order to be

validated as being random using NIST tests. Therefore, 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:

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

The results for the 4-dimentional system showed to be highly sensitive to the type of binarisation. Therefore, after testing several different methods, a 32-bit binarisation has been chosen as being the most suitable solution. Because 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 $\lfloor k^1, k^3 \rfloor = 1, \lfloor k^2, k^4 \rfloor = -1$ are shown in Table 1. 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: $y = x_4$.

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.

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.

The criterion for a successful test is that the p-value has to be superior to the significance level (0.01 for this case). For the present model (1), all tests were 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: under-sampling of the output signal, or increasing the system order.

Different under-sampling 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 [1].

For the second method, the random properties validation of a 10-dimensional system has been carried out and the results are shown in Table. 2. The conditions for the NIST test are the same from 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
0.213309	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 2.

Random improvement of both strategies has been corroborated by the experimental results.

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

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