DYNAMICAL ANALYSIS OF A NEW STATISTICALLY HIGHLY PERFORMANT DETERMINISTIC FUNCTION FOR CHAOTIC SIGNALS GENERATION

Sébastien Hénaff
Institut de Recherche en Communication
et Cybernétique de Nantes
IRCCyN, UMR CNRS 6 597
École Centrale Nantes
France
sebastien.henaff@irccyn.ec-nantes.fr

Ina Taralova
Institut de Recherche en Communication
et Cybernétique de Nantes
IRCCyN, UMR CNRS 6 597
École Centrale Nantes
France
ina.taralova@irccyn.ec-nantes.fr

René Lozi
Laboratoire J.A. Dieudonné,
UMR CNRS 6 621
Université de Nice Sophia-Antipolis
France
r.lozi@unice.fr

Abstract

Many engineering applications such as secure communications based on chaos require the use of highly performant chaotic generators in the sense that they should generate signals closed to random ones. This paper studies the dynamical and statistical properties of a new weakly coupled map system, which are evaluated for several statistical tests. It comes that the system satisfies all requirements for such an application. Furthermore, the chaotic sampling, applied on the states to select the output signal, improves considerably these properties.

Key words

chaos, discrete-time, pseudo-random generators.

1 Introduction

In some engineering applications, such as chaotic encryption, chaotic maps have to exhibit required spectral and statistical properties close to those of random signals [Alvarez and Li, 2006] [Noura et al, 2009]. In order to evaluate the latter features, statistical tests developed for random number generators (RNG) can also be applied to chaotic maps, in order to gather evidence that the map generates "good" chaotic signals, i.e. having a considerable degree of randomness. To address this particular problem, different statistical tests for the systematic evaluation of the randomness of cryptographic random number generators can be applied, among which the most popular NIST (National Institute of Standards and Technology) [Rukhin et al, 2008] tests. In this paper we present the analysis of a new ultra weakly coupled maps system introduced by Lozi in [Lozi, 2008]. This paper is organised as follows : section two presents the considered map. Section three studies its statistical properties and section four analyses its evolution with parameter variation. A conclusion ends this paper.

2 System under study

In [Lozi, 2008], a new coupled map system was introduced. The N^{th} order function F under consideration can be written as :

$$x(n+1) = F(x(n)) = A\,\Lambda(x(n)) \qquad (1)$$

with $x(n) = (x_1(n), x_2(n), \ldots, x_N(n))$
where A is a NxN matrix defined by:

$$A = A_a + A_b$$

$$A_a = \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \vdots \\ \epsilon_N \end{pmatrix} \begin{pmatrix} 1 \; 1 \ldots 1 \end{pmatrix}$$

$$A_b = (N-1) \begin{pmatrix} \epsilon_1 & 0 & \ldots & 0 \\ 0 & \epsilon_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \epsilon_N \end{pmatrix}$$

and Λ is the triangular function.

$$\Lambda(x) = \begin{cases} 2x+1 \text{ if } x < 0 \\ -2x+1 \text{ else} \end{cases}$$

As introduced by Lozi in [Lozi, 2008], the maps are weakly coupled choosing $\epsilon_1 = 10^{-14}$ et $\epsilon_i = i\epsilon_1$. The states evolve in the interval : $[-1;1]^N$. In the definition, the output signal $\bar{x}$ to be transmitted is constructed choosing a particular sampling of the states $\{x_1; x_2; ...; x_n\}$ of the system F :

$$\bar{x}(q) = \begin{cases} x_1(n) & \text{if} \quad x_N(n) \in [T_1, T_2] \\ x_2(n) & \text{if} \quad x_N(n) \in [T_2, T_3] \\ \vdots \\ x_{N-1}(n) \text{ if } x_N(n) \in [T_{N-1}, 1] \end{cases} \quad (2)$$

with $-1 < T_1 < T_2 < ... < T_{N-1}$. q denotes the index of the signal $\bar{x}$ and n is associated to the original map F. The notation $n(q)$ is used to represent the index of the original map. The index of the generated pseudo-random signal is chosen in such a way that for the second order, $\bar{x}(q) = x_1(n(q))$.

3 System Analysis

3.1 Signal

The spectrum X of a signal x is defined as :

$$X(k) = FT(x)(k)$$

The spectrum of the generated signal x_1 is represented in figure 1. It can be quantified by the autocorrelation

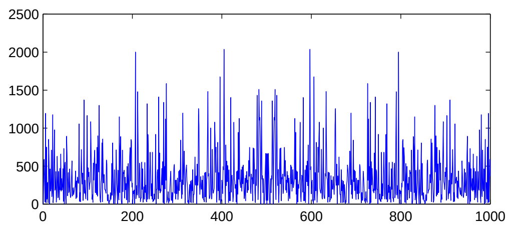

Figure 1. spectrum X_1

of the signal. The correlation of two real signals x and y is calculated by the following expression :

$$\Gamma_{xy}(\tau) = \sum_n x(n+\tau)y(n)$$

it is related to the spectra X and Y of the signals x and y by the relation :

$$\Gamma_{xy} = TF^{-1}(XY^*)$$

The autocorrelation Γ_x is plotted in figure 2. The autocorrelation of a pseudo-random signal is close to a Dirac peak. The tests which have been carried out show that the system generates a wide-band signal before, as well as after the chaotic sampling (2). The presented curves are those of the signal before the chaotic sampling.

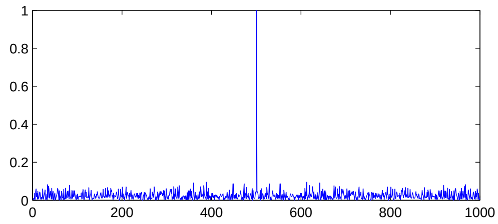

Figure 2. autocorrelation of x_1

3.2 Lyapunov Exponents

The Lyapunov Exponents (LE) quantify the sensitivity to the initial conditions using the average of the Jacobians matrix. If F' is the Jacobian matrix, then, the Lyapunov exponents are :

$$\lambda_i = \lim_{N \to \infty} \frac{1}{N} \ln |vp_i(F'(x_{(N)})F'(x_{(N-1)})...F'(x_{(1)}))|$$

where F is the investigated function, F' is the corresponding Jacobian, and x represents the system state. The signal x_N is uniformly distributed in the interval $[-1, 1]$, therefore we select in average one point out of hundred iterates if $T_1 = 0.98$. The LE of the global system have to be redefined. To do this, let consider the system H, defined in second order by :

$$H : (y_1(q+1), y_2(q+1)) = H(y_1(q), y_2(q))$$

The states $(y_1; y_2)$ are defined by : $y_1(q) = x_1(n(q))$ et $y_2(q) = x_2(n(q))$. In other words, only the states of F remaining after the sampling (2) are kept. The values used for the simulations are the following : considering the second order function, $T_1 = 0.98$, with the third order function, $(T_1, T_2) = (0.98, 0.99)$ and with the fourth order function , $(T_1, T_2, T_3) = (0.98, 0.987, 0.993)$. The results are the same whatever the initial conditions, since the chaotic attractor fills entirely the phase space. Table 1 compares the Lyapunov Exponent values for different system orders. This value does not vary with the system order, but is increased by a factor of one hundred when the global system with the chaotic sampling (2) is considered, taking into account that approximately one point out of 100 iterates is kept. The LE are defined as the speed of deviation of two trajectories initialised in the same vicinity. Therefore the LE of FoF should be twice bigger compared to the LE of F. Keeping in mind that the iterates of (1) are in average selected one out of hundred, then the LE of H are one hundred times more important as it appears in table 1.

3.3 Signal repartition analysis

According to [Lozi, 2008], the following quantifiers are used :

1) Ec_1 : Norm L_1 of the deviation between the signal distribution and the uniform distribution

Table 1. Calculation of the Lyapunov exponents

system order		2	3	4
system F	λ_1	0.693	0.693	0.693
	λ_2	0.693	0.693	0.693
	λ_3		0.693	0.693
	λ_4			0.693
system H	λ_1	69.3	69.3	69.3
	λ_2	69.3	69.3	69.3
	λ_3		69.3	69.3
	λ_4			69.3

2) Ec_2 : Deviation from the uniform distribution according to the norm L_2

The quantifiers are used for the signal repartition analysis in all dimensions. The table 2 compares the signal distributions for different system dimensions. In order to have comparable results, a histogram with a constant number of intervals has to be considered whatever the dimension of the phase space. For this kind of histogram, the results are identical whatever the dimension.

Table 2. system distribution vs distribution dimension

dimension	Ec_1	Ec_2
2	$1,1.10^{-3}$	$1,38.10^{-3}$
3	$1,1.10^{-3}$	$1,38.10^{-3}$
4	$1,2.10^{-3}$	$1,40.10^{-3}$
6	$1,1.10^{-3}$	$1,38.10^{-3}$
7	$1,2.10^{-3}$	$1,42.10^{-3}$

The second test compares the signal distributions in the phase space(x_n,x_{n+p}), $p \in [1;1000]$ and in dimension three : (x_n,x_{n+p},x_{n+2p}), $p \in [1;1000]$ up to dimension 4. The results show that the standard deviation is between 10.9 and 11.8, Ec_1 is between 1.710^{-5} and 1.810^{-5}. Ec_2 is between 1.3310^{-3} and 1.4410^{-3}. Finally, we don't notice a significant deviation, the distributions remaining homogeneous.

The third test in table 3 consists in comparing the results for different systems. The first signal is the signal under investigation, the second is the signal composed of the numbers of pi, and the third (rand) is a pseudo-random signal generated by the computer. The calculation of the histogram is adapted to the specificity of the signal pi : it is calculated over 10 intervals by dimension, which explains the differences between the obtained values and the previous ones, but also the differences between two dimensions.

Table 3. distribution comparaison in fonction of systems

dim.	signal	Ec_1	Ec_2
1	2nd order	$6,69.10^{-4}$	$7,73.10^{-4}$
	3rd order	$7,12.10^{-4}$	$8,47.10^{-4}$
	4th order	$8,37.10^{-4}$	$9,50.10^{-4}$
	pi	$6,01.10^{-4}$	$7,43.10^{-4}$
	rand	$8,75.10^{-4}$	$9,75.10^{-4}$
2	2nd order	$7,51.10^{-4}$	$9,38.10^{-4}$
	3rd order	$7,64.10^{-4}$	$9,68.10^{-4}$
	4th order	$7,99.10^{-4}$	$9,61.10^{-4}$
	pi	$7,70.10^{-4}$	$9,71.10^{-4}$
	rand	$7,70.10^{-4}$	$9,69.10^{-4}$
3	2nd order	$8,18.10^{-4}$	$1,03.10^{-3}$
	3rd order	$7,82.10^{-4}$	$9,92.10^{-4}$
	4th order	$7,81.10^{-4}$	$9,75.10^{-4}$
	pi	$7,90.10^{-4}$	$9,79.10^{-4}$
	rand	$8,11.10^{-4}$	$1,01.10^{-3}$

3.4 Hurst exponents

The Hurst exponents quantify the repetitivity (short) of a long time evolving sequence. They are calculated by the expression :

$$R/S(n) = \sum_{k=1}^{n}(s(k) - \overline{s})$$

The Hurst exponent is then defined as being the slope of the curve $\ln(R/S)/ln(n)$. An exponent equal to 0.5 indicates that the signal is random. If the exponent is $H > 0.5$, the signal is said to be persistent, and its points have a tendency to follow the previous one. If $H < 0.5$, the signal is anti-persistent, this is the opposite case. The Hurst exponents have been calculated for the three different systems as shown in table 4. Finally, the studied system presents the same caracteristics to pi.

Table 4. Hurst exponents

signal	100 000 points
2nd order	0.530
3rd order	0.522
4th order	0.528
pi	0.522
rand	0.510

3.5 Statistical Analysis

The National Institute of Standards and Technology (NIST) has developed a statistical test suite for the systematic evaluation of the randomness of cryptographic random number generators (RNG) [Rukhin et al, 2008]. These tests are statistical tests which allow to investigate the degree of randomness for binary sequences produced by random number generators (RNG). The presented tests are applied over 100 series of data of the system (2) composed of 1 000 000 points. The sequence validates the tests if each small series validates a list of elementary tests for exemple the spectrum distribution, the long term redundancy. The data appearing in table 5 represent the probability that the analyzed data are random so ideally, all probabilities are equal to one. Certain tests propose several different probabilities, and only the worst (i.e. the weakest) ones are reported.

In the notation of the table, the system S_1 represents the forth order system, with parameters $\epsilon_1 = 10^{-9}$ and a sampling interval $[0.99; 1]$ ($T_1 = 0.99$). The system S_2 represents the forth order system, with parameters $\epsilon_1 = 10^{-9}$ and the sampling interval $[0.9; 1]$ ($T_1 = 0.9$). The third system S_3 is a fourth order one with parameters $\epsilon_1 = 10^{-5}$ and a sampling $T_1 = 0.99$. The other parameters of the three previous systems are defined by $\epsilon_i = i\epsilon_1$ and the parameters T_2 et T_3 are defined in order to distribute them equitably in the space $[T_1; 1]$. Finally S_4 et S_5 are respectively generated by the function random of the computer and by the Frey system [Frey, 1993].

By comparing S_1 and S_2, the results show that the data series generated by the system (1) have been improved when the sampling is more selective, which goes in the same sense that the Lyapunov exponents analysis. On the other hand, the system exhibits properties comparable to the random generator of the computer and the system of Frey.

4 Parameter analysis

All the previous statistical analyses have been carried out for a particular parameter values. However, in order to be used in chaotic encryption, the system has to exhibit desirable properties for a large set of parameter values (which form the encryption key). This section aims at determining which is the set of acceptable parameter values. From the definition, the system (1) can be used only in the parameter space $\epsilon_k \in [0; \frac{1}{N}]$ where N is the order of the system in such a way that the system states remain in the space $[-1; 1]$ but the statistical criteria (signal distribution, spectrum) as well as the ones from the dynamical systems theory (sensitivity to the initial conditions, parameter sensitivity) have to bring additional conditions allowing to define the acceptable parameter regions.

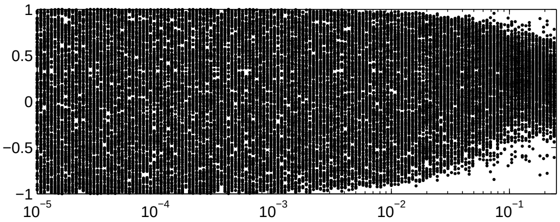

Figure 3. Signal evolution x_1 for $\epsilon_1 \in [10^{-5}; 0.25]$, $(\epsilon_2, \epsilon_3, \epsilon_4) = (10^{-3}, 10^{-4}, 10^{-5})$

4.1 Signal distribution

The uniform distribution of a pseudo-random signal is an elementary feature. The analysis of the signal distribution generated by (1) for small parameter values have already been studied in [Lozi, 2008] but our purpose here is to study the same system for a larger set of parameter values. In this case, the property of uniform distribution has to be satisfied on the whole domain where the function is defined. However, by varying the parameter combinations, the features have been deteriorated. The evolution of the signal values generated for increasing ϵ_1 values is represented in figure 3. When the parameter ϵ_1 becomes higher than 10^{-3}, the generated signal does not fulfill the whole interval $[-1; 1]$. That's why tests of validity of distribution uniformity are carried out in order to determine an exploitable parameter space.

The approach consists in applying the same tests as the ones presented in [Lozi, 2008] but for a larger set of parameter values. Following this criterion, the system parameters have to remain smaller than 10^{-3} so that the distribution of the points was uniform.

4.2 Lyapunov exponents evolution and bifurcations

The analysis of the Lyapunov exponents allows to identify, among others, the parameter regions exhibiting bifurcations. In order to identify them, the Lyapunov exponents have been calculated for a set of parameters. A sudden change of their values would indicate a bifurcation. The simulations show that the Lyapunov exponents vary continuously, which excludes bifurcations in the selected parameter space, as shown in figure 4. The set of simulations is carried out in the parameter space $\epsilon_1 \in [0; 0.1]$ and $\epsilon_2 = 2\epsilon_3 = 4\epsilon_4 = 4.10^{-5}$ for the third order system. In this figure, the three exponents λ_2, λ_3 and λ_4 have the same constant value.

5 Conclusion

This paper presented the dynamical and statistical analysis of a weakly coupled maps system introduced by Lozi. The model is a deterministic one, but exhibits spectral properties (spectrum, correlation and autocorrelation) close to those of random signals, and successfully passed all the statistical tests for closeness to ran-

Table 5. NIST tests

	S_1	S_2	S_3	S_4	S_5
Frequency	0.978072	0.474986	0.319084	0.867692	0.699313
BlockFrequency	0.055361	0.719747	0.122325	0.883171	0.455937
CumulativeSums	0.262249	0.275709	0.834308	0.275709	0.213309
Runs	0.334538	0.275709	0.334538	0.249284	0.946308
LongestRun	0.066882	0.455937	0.867692	0.798139	0.699313
Rank	0.971699	0.350485	0.911413	0.224821	0.779188
FFT	0.066882	0.002758	0.055361	0.013569	0.004301
OverlappingTemplate	0.213309	0.102526	0.867692	0.534146	0.534146
Universal	0.319084	0.000000	0.037566	0.350485	0.719747
ApproximateEntropy	0.419021	0.000000	0.236810	0.834308	0.137282
RandomExcursions	0.000600	0.006990	0.000001	0.000320	0.000045
RandomExcursionsVariant	0.058984	0.016717	0.006990	0.096578	0.054199
Serial	0.055361	0.000000	0.971699	0.798139	0.137282
LinearComplexity	0.911413	0.048716	0.554420	0.739918	0.678686

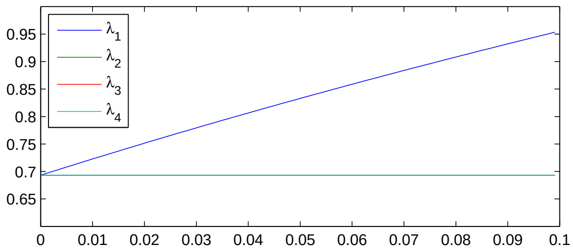

Figure 4. Lyapunov exponents evolution $\epsilon_1 \in [0;0.1]$,$\epsilon_2 = 2\epsilon_3 = 4\epsilon_4 = 4.10^{-5}$

dom signals (NIST). In addition, if a particular sampling is applied, the Lyapunov exponent is shown to increase. The analyses of the spectral properties, the statistical (NIST) tests, the signal repartition and the Hurst exponents show very satisfactory results. In addition, it can be deduced that the data series generated by the system (1) have been improved when the sampling is more selective, which goes in the same sense that the Lyapunov exponents analysis. Finally, it can be concluded that the proposed weakly coupled map system is highly performant and exhibits properties comparable to those of the random number generators.

References

G. Alvarez and S. Li, *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*. International Journal of Bifurcation and Chaos (IJBC), **Vol. 16** (2006), Pages 2129-2151.

H. Noura, S. Hénaff, I. Taralova and S. El Assad *Efficient cascaded 1-D and 2-D chaotic generators*. Second IFAC Conference on Analysis and Control of Chaotic Systems, (2009)

A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators and for Cryptographic Applications*, National Institute of Standards and Technology (NIST) Special Publication 800-22 revision 1, Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1, 131 pages (2008)

R. Lozi, *New enhanced chaotic number generators*. Indian journal of industrial and applied mathematics, **Vol. 1 No. 1** (2008), Pages 1-23.

D.R.Frey, *Chaotic digital encoding: an approach to secure communication*. IEEE Trans.Circuits Syst. II, **Vol. 40, Issue 10** (1993), Pages 660-666.