Statistical and spectral analysis of a new weakly coupled maps system

Sebastien Hénaff, Ina Taralova, René Lozi

Statistical and spectral analysis of a new weakly coupled maps system

Sébastien Hénaff, Ina Taralova
IRCCyN, UMR CNRS 6597, École Centrale Nantes, 1 rue de la Noë, BP 92101,
F-44321 Nantes Cedex 3, France
René Lozi
Laboratoire J.A. Dieudonné, UMR CNRS 6621, Université de Nice Sophia-Antipolis,
F-06108 Nice Cedex 02, France

1 Introduction

Iteration equations, and in particular chaotic maps have attracted an enormous interest due to their capacity to model successfully a large number of systems in varied domains, such as biology, finance, physics, engineering etc. In the latter field, different applications can be mentioned, as switching control systems, walking robots, AC/DC and DC/DC converters, power electronics, digital filters [1] etc... In this plethora of applications, one field has recently yield a particular attention, due to the outstanding development of the telecommunications (wireless technology, Internet, e-banking...), namely the secure data transmission and storage. This phenomenon can be explained by the growing research interest for new and secure communication technologies, among which the chaos-based ones [2]. From the dynamical systems theory point of view, the problem is to design the most appropriate chaotic generator in the cryptographic network, and the richness of the inherent non-linear dynamics is thoroughly exploited. Indeed, the chaotic systems are deterministic ones; however, for some particular structures and tunings they can generate signals, whose spectral properties (spectrum, correlation and autocorrelation) are very close to those of random signals [3]. In addition, the chaotic signals used for encryption have to satisfy the statistical tests for closeness to random signals.

In order to evaluate the latter features, statistical tests developed for random number generators (RNG) are to be applied to the chaotic system, 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) [4] tests.

This evaluation is not sufficient to validate the use of a given chaotic map as generator. Further features are related to the cryptographic architecture. In the considered one, the secret message to transmit is mixed up with the chaotic dynamics. For example, let consider a chaotic system (f_1, f_2) used at parameter values α. The message to transmit m modifies the state values (x_1, x_2) by the expression:

$$\begin{cases} x_{1(n+1)} &= f_1(x_{1(n)}, x_{2(n)}, \alpha) \\ x_{2(n+1)} &= f_2(x_{1(n)}, x_{2(n)}, \alpha) + m(n) \\ y_{(n)} &= x_{1(n)} \end{cases}$$

In order to preserve the chaotic properties of the dynamics, we need an assumption on the magnitude of $m(n)$; we assume that $m(n) << x_{1(n)}, x_{2(n)}$. The cyphertext y is then transmitted

though an unsecured channel. At the reception, a decyphring block should identify the original message m thanks to the knowledge of the reconstructed states $(\hat{x}_1; \hat{x}_2)$ by the formula:

$$\hat{m}_{(n)} = \hat{x}_{2(n+1)} - f_2(\hat{x}_{1(n)}, \hat{x}_{2(n)}, \alpha)$$

It is worth noting that it is impossible to reconstruct the message if the parameters are unknown.

But before that operation, the knowledge of the values of the states is needed. This is done thanks to an observer. It permits to identify the states only thanks to the partial information y.

This paper presents the analysis of a new ultra weakly coupled maps system introduced by Lozi [5] and study its application to the cryptographic architecture. The paper is organized as follows: the considered system is firstly described in section 2, section 3 analyses its closeness to random generators though statistical as well as chaotic features, then the space of useful parameters for encryption is determined in section 4. An observer is finally elaborated for reconstructing the states of the system.

2 System under study

Lozi introduced in 2008 a new coupled map system in [5]. The particularity of this system consists in the fact that an operation, the chaotic sampling, is added after applying the traditional map and this increases pseudo-random features. The N^{th} order function F under consideration is defined as follow:

$$(x_1(n+1), x_2(n+1), \ldots, x_N(n+1)) = F(x_1(n), x_2(n), \ldots, x_N(n))$$

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \\ \vdots \\ x_N(n+1) \end{pmatrix} = \begin{pmatrix} 1-(N-1)\epsilon_1 & \epsilon_1 & \ldots & \epsilon_1 \\ \epsilon_2 & 1-(N-1)\epsilon_2 & \ldots & \epsilon_2 \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_N & \epsilon_N & \ldots & 1-(N-1)\epsilon_N \end{pmatrix} \begin{pmatrix} \Lambda(x_1(n)) \\ \Lambda(x_2(n)) \\ \vdots \\ \Lambda(x_N(n)) \end{pmatrix} \quad (1)$$

where 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 [5], the maps are weakly coupled choosing $\epsilon_1 = 10^{-14}$ et $\epsilon_i = i\epsilon_1$. In this paper, parameters are taken in a larger interval $\epsilon_i < 1/(N-1)$. This bound comes from the fact that the states should stay in the interval $[-1; 1]^N$.

Since $x_1(n+1) = (1-(N-1)\epsilon_1)\Lambda(x_1(n)) + \epsilon_1\Lambda(x_2(n)) + \ldots + \epsilon_1\Lambda(x_N(n))$, then we should choose parameters such that $(1-(N-1)\epsilon_1) > 0$. This is the written inequation above.

As the system is piece-wise affine, it is possible to rewrite it: let X be the state so that $X(n) = (x_1(n), x_2(n), \ldots, x_N(n))$

$$X(n+1) = F(X(n)) = A\ \Lambda(X(n))$$

where A is a NxN matrix defined by:

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

and Λ is the triangular function applied to each component of $X \in [-1;1]^N$:

$$\Lambda(X(n)) = \begin{pmatrix} \Lambda(x_1(n)) \\ \Lambda(x_2(n)) \\ \vdots \\ \Lambda(x_N(n)) \end{pmatrix}$$

Since the function is piece-wise linear, it can be rewritten under a matrix form, by rewriting Λ:

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

or using the generic form :

$$\Lambda(x) = sx + 1$$

with :

$$s = \begin{cases} 2 & \text{if } x < 0 \\ -2 & \text{else} \end{cases}$$

For the second order, the general system F is then governed by :

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \end{pmatrix} = A_n \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{2}$$

where A_n is :

$$A_n = \begin{pmatrix} (1-\epsilon_1)s_{10} & \epsilon_1 s_{20} \\ \epsilon_2 s_{10} & (1-\epsilon_2)s_{20} \end{pmatrix}$$

and

$$\forall (i,j) \in \mathbb{N}^2, s_{ij} = \begin{cases} 2 & \text{if } x_i(n+j) < 0 \\ -2 & \text{if } x_i(n+j) > 0 \end{cases}$$

A traditional system consider equations (1) and with traditional output signal $\bar{x}(n) = x_1(n)$. Here, a chaotic sampling and mixing is applied on the states $\{x_1; x_2; ...; x_N\}$: for the Nth-order system governed by equations (1), this sampling is defined by:

$$\bar{x}(q) = \begin{cases} x_1(n) & \text{if } x_N(n) \in [T_1, T_2] \\ x_2(n) & \text{if } x_N(n) \in [T_2, T_3] \\ & \vdots \\ x_{N-1}(n) & \text{if } x_N(n) \in [T_{N-1}, 1] \end{cases} \tag{3}$$

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 signal is chosen in such a way that for a second order system, $\bar{x}(q) = x_1(n(q))$.

This chaotic sampling increases the chaoticity of the system.

3 System Analysis

The final objective of the study consists in elaborating a chaotic encryption system. The weakly coupled map (1) has been proposed by Lozi as being a pseudo random generator in [6] that presents good statistical features, which do not consider any sampling. These statistical properties are

precisely determinant to discriminate and classify the chaotic generator by these performances. This section analyses the above features. First of all, a spectral analysis is performed, then sensitivity to initial conditions are measured though Lyapunov exponents before quantifying the distribution of the attractor and the one of the generated signal. The long term repetitiveness is then observed though the Hurst exponents. The statistical NIST tests are finally applied on several signals. For all tests, numerical results are compared to the ones obtained for other pseudo-random signals and random signals.

3.1 Signal

The spectrum X of a signal x is defined as :

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

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

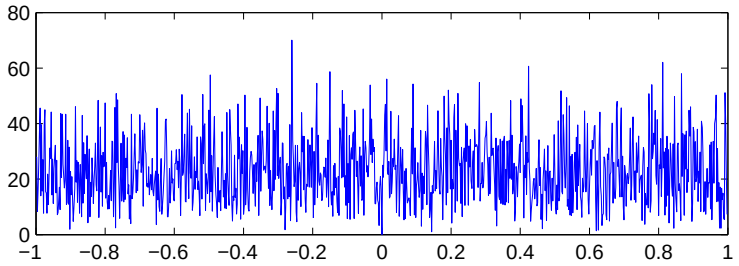

Figure 1: spectrum X_1

by the autocorrelation of the signal. The correlation of two real signals x and y is defined 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 :

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

The autocorrelation Γ_{x1} is plotted in figure 2. Ideally, it should be similar to the random signal one which is close to a dirac peak. The tests which have been carried out show that the system generates a wide-band signal before, and also after the sampling (3). The presented curve is these of the signal before the sampling. The ratio between the value of the highest peak and the second highest peak one is equal to 0.073.

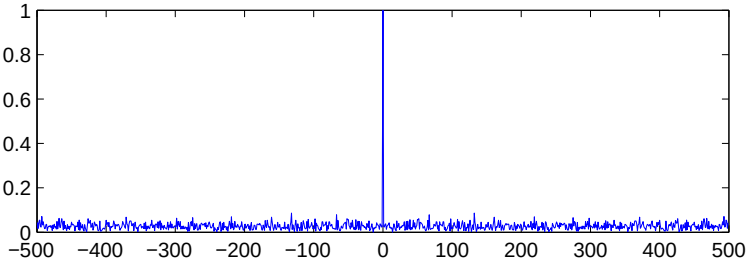

Figure 2: autocorrelation of x_1

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 previous definition can be applied to any classical system, without sampling such as the system F defined by equation (1). A special sampling is then applied (3) so that this definition has to be adapted to this special system. To do so, 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 (3) are kept.

One interesting feature of the system F is that the chaotic attractor is uniformly distributed in the space $[-1; 1]^N$. In particular, the signal x_N is uniformly distributed in the interval $[-1; 1]$, therefore, if $T_1 = 0.98$, the states are selected when $x_N \in [0.98; 1]$, what comes in average one point out of hundred iterates. 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 higher 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 values of H are one hundred times more than for system F.

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 (3) is considered, taking into account that in average one point out of 100 iterates is kept.

Note that in this table, all Lyapunov exponents are positive for all cases, which means that all dynamical trajectories will diverge in all directions.

Table 1: Lyapunov exponents value

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

3.3 Signal repartition analysis

This section quantifies the signal repartition to identify whether the generated signal exhibits a higher probability to belong to a particular set than an other. By observing the chaotic attractor in the phase plane in figure 3, the states of the system visit the whole space $[-1;1]$. To have more objective indication, and according to [5], a repartition measure is calculated by considering the error between this distribution and the ideal uniform distribution. The following two quantifiers have been used:

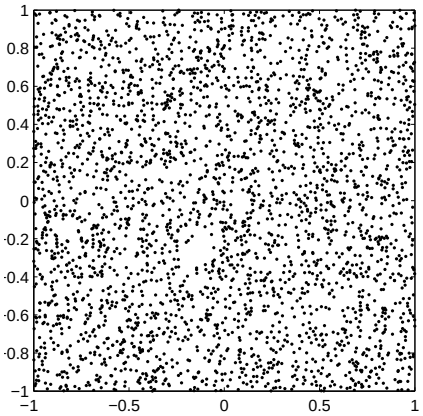

Figure 3: attractor in the phase plane $(x_1; x_2)$

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

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

A perfect generated signal would be characterised by a distribution as close as possible to the uniform one so the ideal distribution quantifiers Ec_1 and Ec_2 would be close to zero. The distribution is calculated in the phase plane $(y_{(n)}; y_{(n+1)}; ...; y_{(n+p)})$ where y is the output signal.

In this section, the dimension of the phase plane, here $p+1$, is called the " distribution dimension ". The quantifiers are used for the signal repartition analysis in several dimensions.

Table 2 compares the signal distributions for different dimensions. To have comparable results, a histogram with the same constant number of boxes has to be considered whatever the dimension of the phase space; 2^{19} points have been processed. For this kind of histogram, the results are identical whatever the dimension. A higher number of points is required in order to observe an error decrease, but the algorithm was too slow in this case, so this analysis has not been carried out.

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: $(x_{(n)},x_{(n+p_1)},x_{(n+p_2)})$, $p_2 \in [\![1;1000]\!]$, $p_1 \in [\![1;p_2[\![$ up to dimension 4. The results show that the error Ec_1 is between $1,1.10^{-3}$ and $1,2.10^{-3}$. Ec_2 is between $1,38.10^{-3}$ and $1,42.10^{-3}$. Finally, no significant deviation can be noticed, 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 figures of pi, and the third is a computer pseudo-random signal. 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 comparison in function of systems

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

The evolution of the figures of pi is known as being a perfect random signal with uniform distribution. From table 3, it comes that the generator under study (1) with the sampling (3) presents the same distributions as pi and the computer pseudo-random generator so the system has an uniform distribution.

3.4 Hurst exponents

The Hurst exponents [7] quantify long term repetitiveness of an evolving sequence. They are calculated by the expression :

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

The Hurst exponent H 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 related to this criterion. If the exponent is greater than 0.5, the signal is said to be persistent, and its points have a tendency to follow the previous one: for example, an increase is generally followed by an increase. 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 characteristics as figures of number π.

Table 4: Hurst exponents

signal	100 000 points
2nd order system	0.530
3rd order system	0.522
4th order system	0.528
pi	0.522
computer random signal	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) [4]. 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 example the spectrum distribution, the long term redundancy. The data appearing in table 5 represent the probability that the analysed 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 have been 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 (3) characterised by $T_1 = 0.99$. The system S_2 represents the forth order system, with parameters $\epsilon_1 = 10^{-9}$ and the sampling $T_1 = 0.9$. 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 "computer" and "Frey" are respectively generated by the pseudo-random generator of the computer and by the Frey system [8].

By comparing S_1 and S_2, the results show that the data series generated by the system (1) are improved when the sampling is more selective, which goes in the same sense that the Lyapunov exponents analysis. Further more it comes that S_2 and S_3 generate predictable signals for some criterion. On the other hand, the system S_1 exhibits properties comparable to the random generator of the computer and the Frey generator.

Table 5: NIST tests

	S_1	S_2	S_3	computer	Frey
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

4 Parameter analysis

All the previous statistical analyses have been carried out for 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 $[-1; 1]$. However, the statistical criterion (signal distribution, spectrum) as well as the ones from the dynamical systems theory (sensitivity to the initial conditions, parameter sensitivity) give additional conditions to define the acceptable parameter regions.

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 [5] but our purpose here is to study the same system for a large set of parameter values. In this case, the property of uniform distribution has to be satisfied. 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 4. When the parameter ϵ_1 becomes higher than 10^{-3}, the generated signal does not fulfil the whole interval $[-1; 1]$. That's why tests of validity of distribution uniformity have carried out in order to determine an exploitable parameter space.

The error distribution is the distance between the uniform distribution and this one as presented in [5]. It has been calculated for a large set of parameter combinations, a projection of these results is reported in figure 5. It can be noticed that the distribution error is mainly determined by the

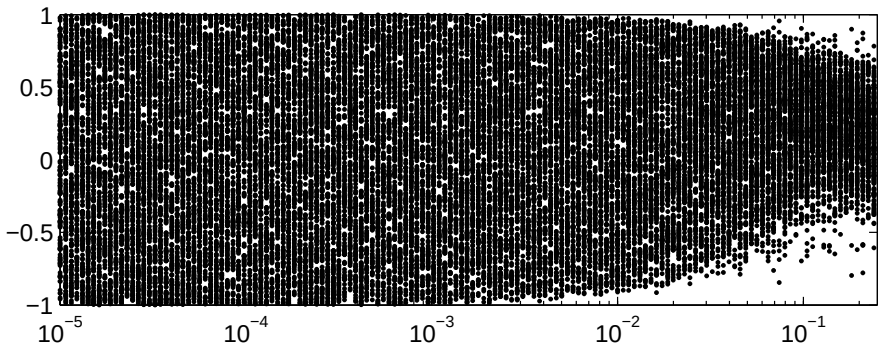

Figure 4: Signal evolution x_1 for $\epsilon_1 \in [10^{-5}; 0.25]$, $(\epsilon_2, \epsilon_3, \epsilon_4) = (10^{-3}, 10^{-4}, 10^{-5})$

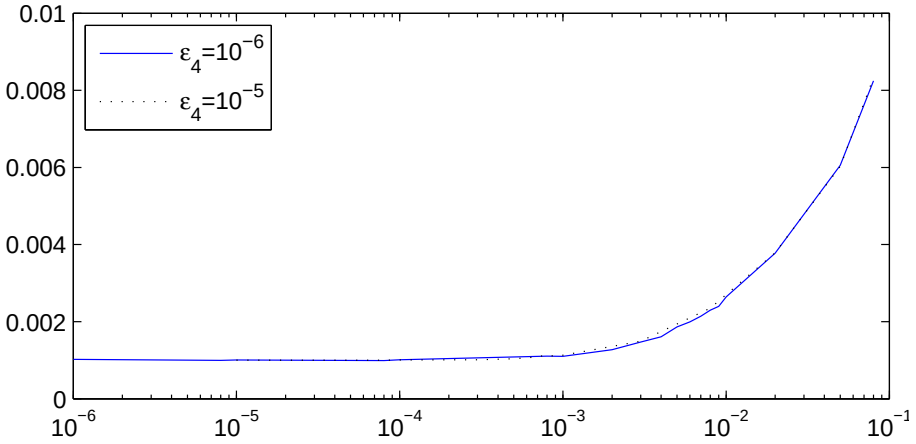

Figure 5: Distribution error evolution Ec_2 for $\epsilon_1 \in [10^{-6}; 10^{-1}]$, $\epsilon_2 = 4\epsilon_4$ and $\epsilon_3 = 2\epsilon_4$ for $\epsilon_4 = 10^{-6}$ and $\epsilon_4 = 10^{-5}$

biggest parameter. Indeed, ϵ_2, ϵ_3 and ϵ_4 don't have any influence on the distribution here when $\epsilon_1 > 10^{-4}$. Following the uniform distribution criterion, the system parameters have to be smaller than 10^{-3}.

4.2 Lyapunov exponents evolution and bifurcations

The analysis of the Lyapunov exponents evolution allows to identify, among others, the parameter regions exhibiting bifurcations. In order to identify them, the Lyapunov exponents have been calculated for a range of parameters. A sudden change of their values would indicate a bifurcation. The simulations results show that the Lyapunov exponents vary continuously, which excludes bifurcations in the selected parameter space, as shown in figure 6. The set of simulations is carried out in the parameter space $\epsilon_1 \in [0; 0.1]$ and $\epsilon_2 = 4.10^{-5}$, $\epsilon_3 = 2.10^{-5}$, $\epsilon_4 = 10^{-5}$ for the fourth order system. In this figure, the three exponents λ_2, λ_3 and λ_4 have the same constant value. The fact that all Lyapunov exponents are positive excludes that the states would converge to stable periodic points.

For all selected parameter combinations, if the attractor is dense in $[-1; 1]^N$ and if the Lyapunov exponents are all positive, then, no stable periodic points exist and the system would never converge to periodic points, which is the case here.

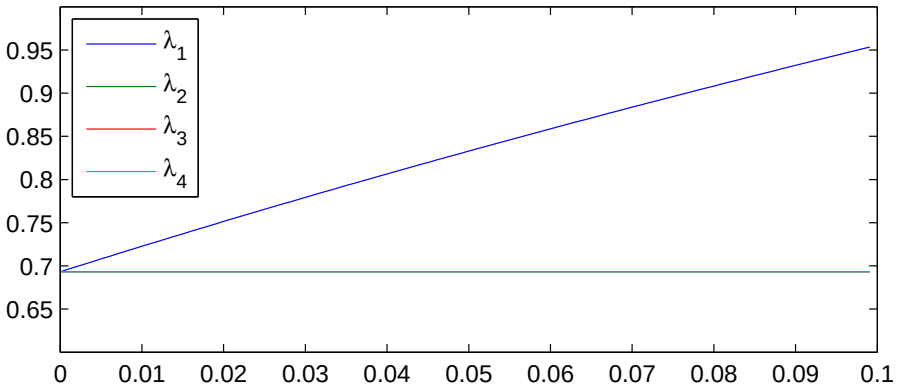

Figure 6: Lyapunov exponents evolution $\epsilon_1 \in [0; 0.1]$,$\epsilon_2 = 4.10^{-5}$, $\epsilon_3 = 2.10^{-5}$, $\epsilon_4 = 10^{-5}$

Finally, the system under study has good features to be used as pseudo-random number generator or for chaotic encryption. This section demonstrated that the system should not be exploited for parameter values greater than 10^{-3} because of the bad distribution. Considering the defined above space of acceptable parameter combination values, the next section focuses on states reconstruction using observers.

5 System observer

The previous section focused on determining whether the system presents good spectral properties and defining a range of acceptable parameter combinations. After validating the use of this system in the context of chaotic encryption, the decryption process has to reconstruct the states thanks to the knowledge of the output signal, and supposing different initial conditions for the coder and the decoder. This can be achieved by designing an observer, which is the aim of this section. If the observer converges in finite time (i.e. the error between the encoder and the decoder states evolution cancels in a finite number of iterations), the synchronization between the encoder and the decoder is guaranteed. To simplify the problem, this section considers the second order system without the chaotic sampling (or, equivalently, during the synchronization phase, the chaotic sampling is switched off). It can be argued that, once synchronized, the chaotic sampling shall be switched on for both systems (the encoder and the decoder). They will remain synchronized, since identical chaotic maps with identical chaotic sampling law may run in parallel at the encoder and the decoder, and the problem of the different initial conditions will be already solved by the observer.

5.1 Identifiability

The purpose of this section is to determine if the coder can generate two identical output signals from two different encryption keys. In terms of system theory, it means that the system generates two identical outputs for two different parameter combinations. If this is the case, the base of the varying parameters has to be modified, and the parameter redundancies removed. To do so, the two outputs have to be equalized and their impact on the parameters has to be investigated. The following study concerns the second order system without the sampling. Let consider two second order systems systems governed by the same law :

$$\left\{\begin{array}{rcl} x_1(n+1) &=& (1-\epsilon_1)\Lambda(x_1(n)) + \epsilon_1\Lambda(x_2(n)) \\ x_2(n+1) &=& (1-\epsilon_2)\Lambda(x_2(n)) + \epsilon_2\Lambda(x_1(n)) \\ y(n) &=& x_1(n) \end{array}\right.$$

$$\left\{\begin{array}{rcl} \hat{x}_1(n+1) &=& (1-\hat{\epsilon}_1)\Lambda(\hat{x}_1(n)) + \hat{\epsilon}_1\Lambda(\hat{x}_2(n)) \\ \hat{x}_2(n+1) &=& (1-\hat{\epsilon}_2)\Lambda(\hat{x}_2(n)) + \hat{\epsilon}_2\Lambda(\hat{x}_1(n)) \\ \hat{y}(n) &=& \hat{x}_1(n) \end{array}\right.$$

Considering the same outputs : $(\hat{y}(n))_n = (y(n))_n$, is it possible that the parameters would be different? The system is piece-wise linear, so let $s_{ij} \in \{-2; 2\}$ be defined by $\Lambda(x_i(n+j)) = 1 + s_{ij}$.

$$s_{ij} = \left\{\begin{array}{ll} -2 & \text{if } x_i(n+j) > 0 \\ 2 & \text{else} \end{array}\right.$$

$$\hat{y}(n) = y(n) \Rightarrow \hat{x}_1(n) = x_1(n)$$

$$\begin{array}{l} \left\{\begin{array}{rcl} \hat{y}(n) &=& y(n) \\ \hat{y}(n+1) &=& y(n+1) \end{array}\right. \\ \Rightarrow (\hat{\epsilon}_1 - \epsilon_1)\Lambda(x_1(n)) = \hat{\epsilon}_1\Lambda(\hat{x}_2(n)) - \epsilon_1\Lambda(x_2(n)) \end{array}$$

$$\begin{array}{l} \left\{\begin{array}{rcl} \hat{y}(n) &=& y(n) \\ \hat{y}(n+1) &=& y(n+1) \\ \hat{y}(n+2) &=& y(n+2) \end{array}\right. \\ \Rightarrow \begin{array}{c} [(\hat{\epsilon}_1 - \epsilon_1)(1-\epsilon_1)s_{11} - \hat{\epsilon}_1\hat{\epsilon}_2\hat{s}_{21} + \epsilon_1\epsilon_2 s_{21} - (\hat{\epsilon}_1 - \epsilon_1)(1-\hat{\epsilon_2})\hat{s}_{21}]\Lambda(x_1(n)) \\ = \epsilon_1[-(\hat{\epsilon}_1 - \epsilon_1)s_{11} - (1-\epsilon_2)s_{21} + (1-\hat{\epsilon}_2)\hat{s}_{21}]\Lambda(x_2(n)) \end{array} \end{array} \quad (4)$$

Both $\Lambda(x_1)$ and $\Lambda(x_2)$ appear in equation (4). $\{x_1; x_2\}$ represents the state of the chaotic system, which visits the whole space $[-1; 1]2$ since the attractor is uniformly distributed in this space. So, to a given particular combination $\{\epsilon_1, \epsilon_2, \hat{\epsilon}_1, \hat{\epsilon}_2, s_{10}, s_{20}, s_{11}, s_{21}, \hat{s}_{10}, \hat{s}_{20}, \hat{s}_{11}, \hat{s}_{21}\}$ can be associated an infinity of states $\{x_1; x_2\}$. One can consider both quantities $\Lambda(x_1(n))$ and $\Lambda(x_2(n))$ as independent. In this case, one obtains the following system of equations :

$$\left\{\begin{array}{l} (\hat{\epsilon}_1 - \epsilon_1)(1-\epsilon_1)s_{11} - \hat{\epsilon}_1\hat{\epsilon}_2\hat{s}_{21} + \epsilon_1\epsilon_2 s_{21} - (\hat{\epsilon}_1 - \epsilon_1)(1-\hat{\epsilon_2})\hat{s}_{21} = 0 \\ \epsilon_1[-(\hat{\epsilon}_1 - \epsilon_1)s_{11} - (1-\epsilon_2)s_{21} + (1-\hat{\epsilon}_2)\hat{s}_{21}] = 0 \end{array}\right.$$

One solution of the second equation is : $\epsilon_1 = 0$. ϵ_1 is one of the system parameters, and this solution corresponds to a decoupled system. Therefore, this particular case is to be excluded. One obtains then the new system of equations:

$$\left\{\begin{array}{l} (\hat{\epsilon}_1 - \epsilon_1)(1-\epsilon_1)s_{11} - \hat{\epsilon}_1\hat{\epsilon}_2\hat{s}_{21} + \epsilon_1\epsilon_2 s_{21} - (\hat{\epsilon}_1 - \epsilon_1)(1-\hat{\epsilon_2})\hat{s}_{21} = 0 \\ -(\hat{\epsilon}_1 - \epsilon_1)s_{11} - (1-\epsilon_2)s_{21} + (1-\hat{\epsilon}_2)\hat{s}_{21} = 0 \end{array}\right.$$

The resolution leads to the following result:

$$\forall (s_{11}, s_{21}, \hat{s}_{21}) \in \{-2; 2\}^3, \quad \left\{\begin{array}{rcl} s_{21} = \hat{s}_{21} &\Rightarrow& \{\hat{\epsilon}_1, \hat{\epsilon}_2\} = \{\epsilon_1, \epsilon_2\} \\ s_{11} = s_{21} = -\hat{s}_{21} &\Rightarrow& \epsilon_1 = 0 \text{ and } \hat{\epsilon}_2 + \epsilon_2 - \hat{\epsilon}_1 = 0 \\ -s_{11} = s_{21} = -\hat{s}_{21} &\Rightarrow& \epsilon_1 = 0 \text{ and } \hat{\epsilon}_2 + \epsilon_2 + \hat{\epsilon}_1 = 0 \end{array}\right.$$

Considering that the solution $\epsilon_1 = 0$ is impossible, then the following conclusion can be drawn:

$$\left\{\begin{array}{rcl} \hat{y}(n) &=& y(n) \\ \hat{y}(n+1) &=& y(n+1) \\ \hat{y}(n+2) &=& y(n+2) \\ \epsilon_1 &\neq& 0 \end{array}\right. \quad \Rightarrow \{\hat{\epsilon}_1, \hat{\epsilon}_2\} = \{\epsilon_1, \epsilon_2\} \quad (5)$$

Finally, the parameters of this system are identifiable and there are no redundant parameters. From a more applicative point of view, the whole set of parameter combinations can be used as a set of encryption keys of the coder, since no parameter combination -different from the one used for the encryption- could decode the message.

5.2 Observability

In the context of encryption issue, a message encoded though a chaotic generator should be reconstructed at the reception. This could be achieved if the only knowledge of the output signal allows to reconstruct the states; that is the definition of observability.

The considered system (1) is a piece-wise affine system, therefore, for each region of determination, the system is locally affine and it can the be written as :

$$\begin{cases} x_{(n+1)} = F(x_{(n)}) = A.x_{(n)} + B \\ y_{(n)} = Cx_{(n)} \end{cases} \tag{6}$$

A second order affine system is locally observable if its observability matrix is a full-rank one :

$$rg(O) = rg \begin{pmatrix} C \\ CA \end{pmatrix} = 2$$

Here, the observability matrix shall be different according to the region to which belong the system states. It is equal to :

$$O = \begin{pmatrix} 1 & 0 \\ 2(1-\epsilon_1)s_{10} & 2\epsilon_1 s_{10} \end{pmatrix}$$

which is full-rank since $\epsilon_1 > 0$ and $s_{10} \in \{-2; 2\}$. Therefore, the system (6) is observable.

5.3 Linear Luenberger Observer

The system is piece-wise affine. Considering it as such, the present section identifies a piece-wise linear observer. The second order system can be rewritten using the affine form on the four domains where it is defined :

$$\begin{cases} x_{(n+1)} = F(x_{(n)}) = A.x_{(n)} + B \\ y_{(n)} = Cx_{(n)} \end{cases}$$

$$\begin{cases} x_{(n+1)} = \begin{pmatrix} (1-\epsilon_1)s_{10} & \epsilon_1 s_{20} \\ \epsilon_2 s_{10} & (1-\epsilon_2)s_{20} \end{pmatrix} x_{(n)} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ y_{(n)} = \begin{pmatrix} 1 & 0 \end{pmatrix} x_{(n)} \end{cases}$$

where s_{10} and s_{20} defined the four regions:

$$\{s_{10}, s_{20}\} = \begin{cases} \{2, 2\} & \text{if } x_{(n)} \in [-1; 0]^2 \\ \{2, -2\} & \text{if } x_{(n)} \in [-1; 0] \times [0; 1] \\ \{-2, 2\} & \text{if } x_{(n)} \in [0; 1] \times [-1; 0] \\ \{-2, -2\} & \text{if } x_{(n)} \in [0; 1]^2 \end{cases}$$

The associated Luenberger system is :

$$\hat{x}_{(n+1)} = \hat{A}\hat{x}_{(n)} + B + K(C\hat{x}_{(n)} - y_{(n)})$$

K is a predefined gain such that the error $e_{(n)}$ tends to zero. Let consider $\hat{x}_{(n)}$ and $x_{(n)}$ belonging to the same region of definition. In this case, $\hat{A} = A$ and therefore,

$$e_{(n+1)} = (A + KC)e_{(n)}$$

One can identify the values of the gain K which cancel the eigenvalues of the matrix $(A + KC)$ as a function of the affine system model. In this case, since the matrix is of two dimension, $(A + KC)2 = 0$, if the system states x and its estimate $\hat{x}$ belong to the same region of the state space twice consecutively, the estimate shall synchronise with the original system in two iterations.

Zero eigenvalues lead to the following solutions for the gain :

$$K = \begin{cases} \begin{pmatrix} (\epsilon_1 + \epsilon_2 - 2) \\ \frac{2\epsilon_2 - \epsilon_2^2 - \epsilon_1\epsilon_2 - 1}{\epsilon_1} \end{pmatrix} & \text{if } \hat{x}_{(n)} \in [-1;0]^2 \\ \begin{pmatrix} (\epsilon_2 - \epsilon_1) \\ \frac{2\epsilon_2 - \epsilon_2^2 + \epsilon_1\epsilon_2 - 1}{\epsilon_1} \end{pmatrix} & \text{if } \hat{x}_{(n)} \in [0;1] \times [-1;0] \\ \begin{pmatrix} -(\epsilon_2 - \epsilon_1) \\ -\frac{2\epsilon_2 - \epsilon_2^2 + \epsilon_1\epsilon_2 - 1}{\epsilon_1} \end{pmatrix} & \text{if } \hat{x}_{(n)} \in [-1;0] \times [0;1] \\ \begin{pmatrix} -(\epsilon_1 + \epsilon_2 - 2) \\ -\frac{2\epsilon_2 - \epsilon_2^2 - \epsilon_1\epsilon_2 - 1}{\epsilon_1} \end{pmatrix} & \text{if } \hat{x}_{(n)} \in [0;1]^2 \end{cases}$$

The zero eigenvalues assure the convergence in two iterations of the affine system if the system states remain in the same region of definition. Otherwise the synchronisation may not take place for any states evolution. The error of the linear system evolves following the equation :

$$e_{(n+1)} = (A + KC)e_{(n)}$$

Since the matrix $(A + KC)$ is nilpotent, if the system remains in the same domain of definition,

$$e_{(n+1)} = (A + KC)^2 e_{(n)} = 0$$

In reality, since the states distribution is uniform (section 4.1), the system states have a probability of 1/4 to fall twice consecutively in the same domain of definition. Considering that both systems (the original one and the observer) start from the same region, then statistically, in average, three iterations would be necessary before the trajectories converge and both systems synchronise. When the system falls consecutively into two different regions, the equation which governs the error becomes:

$$e_{(n+1)} = (A_1 + K_1C)(A_2 + K_2C)e_{(n)}$$

Let P_1, P_2 be two transformation matrices which triangularise respectively the matrices $(A_1 + K_1C)$ and $(A_2 + K_2C)$, and let D_1, D_2 be both triangularised matrices. It comes:

$$e_{(n+1)} = P_1 D_1 P_1^{-1} P_2 D_2 P_2^{-1} e_{(n)}$$

As soon as $P_1 \neq P_2$, the error e does not cancel in two iterations. Now, the proper bases of the matrices $(A + KC)$ are the same for the domains of definition $\hat{x}_{(n)} \in [-1;0]^2$ and $\hat{x}_{(n)} \in [0;1]^2$. On the other hand, the bases are the same for the domains of definition $\hat{x}_{(n)} \in [0;1] \times [-1;0]$

and $\hat{x}_{(n)} \in [-1;0] \times [0;1]$. In the example, since the matrices D_1 and D_2 have zero eigenvalues, if $P_1 = P_2$,

$$e_{(n+2)} = P_1 D_1 D_2 P_2^{-1} e_{(n)} = 0$$

and the synchronisation is done in two iterates.

If $P_1 \neq P_2$, for example when $(x_{(n)}, x_{(n+1)}) \in ([-1;0] \times [0;1]) \times [0;1]^2$,

$$e_{(n+2)} = (A_1 + K_1' C)(A_2 + K_2' C) e_{(n)}$$

$e_{(n+2)} = 0$ if $(A_1 + K_1' C)(A_2 + K_2' C) = 0$, this equation leads to the particular solution:

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} -(2-\epsilon_1-\epsilon_2) \\ \frac{1-2\epsilon_2+\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ \frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([-1;0]^2) \times ([-1;0] \times [0;1])$$

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} 2-\epsilon_1-\epsilon_2 \\ \frac{1-2\epsilon_2+\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ \frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([0;1]^2) \times ([-1;0] \times [0;1])$$

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} -(2-\epsilon_1-\epsilon_2) \\ \frac{1-2\epsilon_2-\epsilon_1\epsilon_2-\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ -\frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([-1;0]^2) \times ([0;1] \times [-1;0])$$

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} 2-\epsilon_1-\epsilon_2 \\ \frac{1-2\epsilon_2+\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ -\frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([0;1]^2) \times ([0;1] \times [-1;0])$$

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} \epsilon_1-\epsilon_2 \\ \frac{1-2\epsilon_2-\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ \frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([-1;0] \times [0;1]) \times ([-1;0]^2)$$

$$\left\{ \begin{array}{l} K_1 = \begin{pmatrix} \epsilon_1-\epsilon_2 \\ \frac{1-2\epsilon_2-\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ -\frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{array} \right. \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([-1;0] \times [0;1]) \times ([0;1]^2)$$

$$\begin{cases} K_1 = \begin{pmatrix} -(\epsilon_1-\epsilon_2) \\ -\frac{1-2\epsilon_2-\epsilon_1\epsilon_2+\epsilon_2 2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ -\frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{cases} \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([0;1]\times[-1;0]) \times ([0;1]^2)$$

$$\begin{cases} K_1 = \begin{pmatrix} -(\epsilon_1-\epsilon_2) \\ -\frac{1-2\epsilon_2-\epsilon_1\epsilon_2+\epsilon_2^2}{\epsilon_1} \end{pmatrix} \\ K_2 = \begin{pmatrix} p \\ \frac{1-\epsilon_1-\epsilon_2+p(1-\epsilon_2)}{\epsilon_1} \end{pmatrix} \end{cases} \quad \text{if } (\hat{x}_{(n)}, \hat{x}_{(n+1)}) \in ([0;1]\times[-1;0]) \times ([-1;0]^2)$$

Finally, it is possible to synchronise in two iterates for all possible configurations by considering the observer composed of 16 parallel systems. Each system would then be governed by the law :

$$S_i : \begin{array}{l} \hat{x}_{(2k+1)} = \hat{A}_j \hat{x}_{(2k)} + B + K_1(C\hat{x}_{(2k)} - y_{(2k)}) \\ \hat{x}_{(2k+2)} = \hat{A}_{j'} \hat{x}_{(2k+1)} + B + K_2(C\hat{x}_{(2k+1)} - y_{(2k+1)}) \end{array}$$

5.4 Inverse lag observer

A second estimator, also known as numerical observer, can be designed based on the inverse lag. It allows to identify the current states by considering the inverse function. For the second order system, the autonomous system is :

$$\begin{cases} x_1(n+1) = (1-\epsilon_1)\Lambda(x_1(n)) + \epsilon_1\Lambda(x_2(n)) \\ x_2(n+1) = (1-\epsilon_2)\Lambda(x_2(n)) + \epsilon_2\Lambda(x_1(n)) \\ y(n) = x_1(n) \end{cases}$$

With two measurements at the output y, it is possible to reconstruct the signal :

$$\begin{cases} \hat{x}_1(n) = y(n) \\ \hat{x}_2(n+1) = \epsilon_2\Lambda(y(n)) + \frac{1-\epsilon_2}{\epsilon_1}(y(n+1) - (1-\epsilon_1)\Lambda(y(n))) \end{cases}$$

Finally, this reconstructor can identify the original state for all values, which is not the case of the first observer. Although, this method can be difficultly be applied to systems of higher order.

6 Conclusion

Most of the papers devoted to chaotic encryption have considered maps with poor statistical and spectral properties. Unlike these papers, we have investigated a new system of weakly coupled maps with an chaotic sampling which satisfied all statistical and spectral analysis tests for closeness to random signals. In addition, we have presented the synthesis of efficient observers for the system of weakly coupled map, and two different observers have been designed. The convergence rate has been discussed in the case of piece-wise affine maps, and the conditions to decrease the convergence rate by a factor of 16 have been presented, based on the locally linear behaviour of the weakly coupled maps. The design and analysis of higher order map observers are currently under investigation.

References

[1] D. Fournier-Prunaret, O. Feely, and I. Taralova-Roux. Lowpass sigma-delta modulation: an analysis by means of the critical lines tool. *Nonlinear Analysis*, 47(8):5343 – 5355, 2001.

[2] 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, june 2009.

[3] G. Álvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8):2129–2151, 2006.

[4] NIST. *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*. 2001.

[5] R. Lozi. New enhanced chaotic number generators. *Indian journal of industrial and applied mathematics*, 1(1):1–23, january 2008.

[6] R. Lozi. Giga-periodic orbits for weakly coupled tent and logistic discretized maps. In A.H. Siddiqi, I.S. Duff, and O. Christensen, editors, *Modern Mathematical Models, Methods and Algorithms for Real World Systems*, pages 80–124. International Conference on Industrial and Applied Mathematics, New Delhi, Anamaya Publishers, New Delhi, India, december 2004.

[7] H.E. Hurst. A suggested statistical model of some time series which occur in nature. *Nature*, 180(4584):494, september 1957.

[8] D.R. Frey. Chaotic digital encoding: an approach to secure communication. *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, 40(10):660–666, October 1993.