Observers design for a new weakly coupled map function

Sebastien Hénaff, Ina Taralova, René Lozi

Observers design for a new weakly coupled map function

Sébastien Hénaff*, Ina Taralova*, and René Lozi**

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

***Abstract*—In some engineering applications, such as chaotic encryption, chaotic maps have to exhibit required statistical and spectral properties close to those of random signals. However, most of the papers dealing with synchronization and observer synthesis consider maps exhibiting poor statistical and spectral properties. Moreover, most of the time these properties, however essential for the chaotic encryption, are simply neglected. Unlike these papers, in our work we present the analysis of a new ultra 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 random signals (NIST). Two different observers have been designed. The convergence rate has been discussed in the case of 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 map.**

I. Introduction

CHAOS has recently received a growing interest in various fields of science and engineering, and in particular, in secure communications. Pecora and Carroll were the first who synchronised chaotic systems [1]. Several chaotic cryptographic schemes have been proposed since [2], [3] and can be classified in three main categories : chaotic masking, chaotic modulation and chaotic shift keying.

In the cryptographic application, the chaotic generator must exhibit appropriate features close to those of the pseudo-random generators. These adapted properties have been studied more precisely in [4], [5], [6].

Further researchers have then looked for finding appropriate systems testing different architectures : traditional chaotic maps (for example, the logistic map, the Hénon map [7], the generalised Hénon map) piece-wise linear map, cascaded map [8] or coupled map lattice. In order to evaluate the features of the system, 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) tests.

It appears that most of the maps classically used for chaotic encryption do not pass successfully these tests, and don't exhibit the required features. However, most of the papers dealing with synchronisation and observer synthesis consider precisely these kinds of maps, highly inefficient in the context of chaotic encryption.

Unlike these models, Lozi [10] introduced in 2008 a new ultra weakly coupled maps system to generate pseudo-random signals which exhibits very good statistical properties. To use this system for secure communication, it must exhibit good spectral features and have to be observable. So the aim of this paper is to identify and to design an observer for the weakly coupled map system.

This paper is organised as follow : after briefly presenting the system under investigation, sections three and four present the issues on parameter identifiability and system observability. Sections five and six propose and compare two different observers. Finally, a concluding section ends the paper.

II. System definition

The N-th order function F can be written as :

$$X(n+1) = F(X(n))$$

with $X(n) = (x_1(n), x_2(n), \ldots, x_N(n))$

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

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 tent function applied to every the components 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 the tent function :

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

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 :

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

where A_n is :

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

The rest of the paper only consider the second order system.

III. Identifiability

The purpose of this section is to determine if the coder can generate two identical outputs 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 presented study concerns the second order system without the scaling. Let consider two second order systems systems governed by the same law :

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

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

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 $\Lambda(x_i(n+j)) = 1 + s_{ij}$.

$$s_{ij} = \begin{cases} -2 & \text{if } x_i(n+j) > 0 \\ 2 & \text{else} \end{cases}$$

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

$$\begin{cases} \hat{y}(n) &=& y(n) \\ \hat{y}(n+1) &=& y(n+1) \end{cases}$$
$$\Rightarrow (\hat{\epsilon}_1 - \epsilon_1)\Lambda(x_1(n)) = \hat{\epsilon}_1\Lambda(\hat{x}_2(n)) - \epsilon_1\Lambda(x_2(n))$$

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

Both x_1 and x_2 appear in the last. But $\{x_1; x_2\}$ is the state of the chaotic system, which has the property to visit the whole state space $[-1;1]^2$. In other words, to a given parameter 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 then the independent variables $\Lambda(x_1(n))$ et $\Lambda(x_2(n))$. In this case, one obtains the following system of equations :

$$\begin{cases} (\hat{\epsilon}_1 - \epsilon_1)(1-\epsilon_1)s_{11} - \hat{\epsilon}_1\hat{\epsilon}_2\hat{s}_{21} + \epsilon_1\epsilon_2 s_{21} \\ \quad -(\hat{\epsilon}_1 - \epsilon_1)(1-\hat{\epsilon}_2)\hat{s}_{21} = 0 \\ \epsilon_1[-(\hat{\epsilon}_1 - \epsilon_1)s_{11} - (1-\epsilon_2)s_{21} + (1-\hat{\epsilon}_2)\hat{s}_{21}] = 0 \end{cases}$$

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 :

$$\begin{cases} (\hat{\epsilon}_1 - \epsilon_1)(1-\epsilon_1)s_{11} - \hat{\epsilon}_1\hat{\epsilon}_2\hat{s}_{21} + \epsilon_1\epsilon_2 s_{21} \\ \quad -(\hat{\epsilon}_1 - \epsilon_1)(1-\hat{\epsilon}_2)\hat{s}_{21} = 0 \\ -(\hat{\epsilon}_1 - \epsilon_1)s_{11} - (1-\epsilon_2)s_{21} + (1-\hat{\epsilon}_2)\hat{s}_{21} = 0 \end{cases}$$

The resolution leads to the following result:

$$\forall (s_{11}, s_{21}, \hat{s}_{21}) \in \{-2;2\}^3,$$
$$\begin{cases} s_{21} = \hat{s}_{21} & \Rightarrow & \{\hat{\epsilon}_1, \hat{\epsilon}_2\} = \{\epsilon_1, \epsilon_2\} \\ s_{11} = s_{21} = -\hat{s}_{21} & \Rightarrow & \epsilon_1 = 0 \text{ et } \hat{\epsilon}_2 + \epsilon_2 - \hat{\epsilon}_1 = 0 \\ -s_{11} = s_{21} = -\hat{s}_{21} & \Rightarrow & \epsilon_1 = 0 \text{ et } \hat{\epsilon}_2 + \epsilon_2 + \hat{\epsilon}_1 = 0 \end{cases}$$

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

$$\begin{cases} \hat{y}(n) &=& y(n) \\ \hat{y}(n+1) &=& y(n+1) \\ \hat{y}(n+2) &=& y(n+2) \\ \epsilon_1 &\neq& 0 \end{cases} \Rightarrow \{\hat{\epsilon}_1, \hat{\epsilon}_2\} = \{\epsilon_1, \epsilon_2\}$$

Finally, there are no redundant parameters and the whole set of parameter combinations can be used as a set of encryption keys of the coder, there are no parameters different from the one used for the encryption which could allow to decrypt the message.

IV. Observability

An affine system can be written as :

$$\begin{cases} x(n+1) = F(x(n)) = A.x(n) + B \\ y(n) = Cx(n) \end{cases}$$

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

$$O = \begin{pmatrix} C \\ CA \end{pmatrix}$$

Here, the system is piece-wise affine, therefore the observability matrix shall be different according to the region to which belong the system state. 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 $\epsilon_1 > 0$. Therefore, the system is observable.

V. 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 :

$$\begin{cases} x(n+1) = F(x(n)) = A.x(n) + B \\ y(n) = Cx(n) \end{cases}$$

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

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 $x(n)$ in 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 second order, $(A+KC)^2 = 0$ therefore if the system states x and its estimate $\hat{x}$ belong to the same region of the state space twice consecutively, then the estimate shall synchronise with the original system.

Zero eigenvalues lead to the following solutions for the gain :

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

The zero eigenvalues assure the convergence in two iterations of the affine system if the system states remain in the same region of definition. Then 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,

$$e(n+2) = (A+KC)^2 e(n) = 0$$

In reality, 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 three iterations are necessary before the trajectories converge. When the system falls consecutively into two different configurations, the equation which governs the error becomes :

$$e(n+2) = (A_1 + K_1C)(A_2 + K_2C)e(n)$$

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 the two triangularised matrices. It comes :

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

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 exemple, since the matrices D_1 and D_2 have zero eigenvalues, if $P_1 = P_2$,

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

Finally, considering that the two systems are in the same domains of definition, they have one chance out of two to synchronise.

Now, if one considers that the transition evolution of the two systems is independent in the domain of definition until they synchronise, they have statistically one chance out of sixteen to fall twice consecutively in the same domains of definition, which decreases the probability to synchronise at a given instant to 1/32.

Finally, two synchronisation strategies are possible : the classical one considers that the master system starts from any initial condition and follows the same law during the synchronisation. In this case, the slave system will synchronise - in average - after 32 iterations and it is governed by the equation :

$$\hat{x}(n+1) = F(\hat{x}(n)) + B + K(C\hat{x}(n) - y(n))$$

On the other hand, one can consider that the observer consists of several systems following different laws, each following its own law whatever the value of its state at the next iterates. A system can then be governed by the law :

$$S1 : \hat{x}(n+1) = \hat{A}_1\hat{x}(n) + B + K_1(C\hat{x}(n) - y(n))$$

where A_1 et K_1 are derived from the definition of the systems related to the desired domain of definition, $\hat{x}(n) \in [-1;0]^2$ for instance. The observer systems have to cover the whole set of possible combinations of the state evolutions which allow to synchronise, i.e. four observers for a second order system. The advantage to use these systems lies in the fact that the probability that one of the forth systems synchronises with the original systems rises up to 1/2. Once synchronised, a classical observer can allow to follow the trajectory of the states of the original system.

If the classical use of a second order system leads to a synchronisation in 32 iterations in average, when the system order is increased, the synchronisation time increases exponentialy. The simultaneous use of several observers allows to divide the time for synchronisation by 16 for a second order system. The drawback is that several observer systems have to run simultaneously.

VI. Another observer

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 :

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

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 greater order systems.

VII. Conclusion

Most of the papers devoted to observer synthesis considered maps with poor statistical and spectral properties. We present here the synthesis of efficient observers for the system of weakly coupled map which satisfied all statistical (NIST) and spectral analysis tests. Two different observers have been designed. The convergence rate has been discussed in the case of 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 map. The design and analysis of higher order map observers is currently under investigation.

References

[1] T. L. Caroll and L. M. Pecora, *Synchronising chaotic circuits*. IEEE Trans. Circuits Syst., **Volume 38** (1991), Pages 453-456.

[2] L. Kocarev, J. Makraduli and P. Amato, *Public-key encryption based on Chebyshev polynomials*. Circuits, Systems, and Signal Processing **Volume 24, Number 5** (2005), Pages 497-517.

[3] P. Fei, Q. Shui-Sheng and L. Min, *A secure digital signature algorithm based on elliptic curve and chaotic mappings*. Circuits, Systems, and Signal Processing **Volume 24, Number 5** (2005), Pages 585-597.

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

[5] M. Götz, K. Kelber and W. Schwarz, *Discrete-time chaotic encryption systems - Part I. Statistical design approach*. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions, **Volume 44, Issue 10** (1997), Pages 963-970.

[6] 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 pseudorandom numbers for cryptographic applications*, NIST Special Publication **Volume 366** (2001)

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

[8] W. P. Tang and H. K. Kwan, *Chaotic communications using nonlinear transform pairs*. IEE ISCAS, (2004), Pages 740-743.

[9] 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)

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