Observers based synchronization and input recovery for a class of nonlinear chaotic models

Estelle Cherrier, Mohamed Boutayeb, José Ragot

Observers based synchronization and input recovery for a class of nonlinear chaotic models

Estelle Cherrier, Mohamed Boutayeb and José Ragot

***Abstract*— In this note, we propose a simple and efficient crypto-system based on a chaotic time delay model. It consists of two steps: the first one assures the transmitter/receiver synchronization while the second step focuses on the encryption/decryption procedure. The synchronization is performed through a non linear state observer design, driven by the transmitted signal. Both full order and reduced order state estimation techniques are established. One of the main results is that sufficient conditions for asymptotic convergence, to assure the synchronization, are derived in terms of Linear Matrix Inequalities (i.e. convex problem) easily and numerically tractable. Efficiency of the proposed approach is shown through the transmission of two encrypted messages : a sound wave and a digital picture. Finally, some security issues are discussed at the end of this note.**

***Index Terms*— Nonlinear observer, time-delayed chaotic system, synchronization, cryptosystem**

I. Introduction

THE field of synchronization of chaotic systems is quite recent, and has been opened by the work of Pecora and Carroll [1], [2]. They showed that two identical chaotic systems, starting with different initial conditions, may synchronize, provided that they are coupled according to the *drive-response principle*. Among the applications induced by this pioneering work, secure communication became a popular research topic. A conventional communication scheme is based on random carriers: an information signal is added to a random signal at the transmitter, and then it is recovered at the receiver. For this process to be performed, the receiver needs to know perfectly the random carrier to allow its subtraction from the transmitted signal, thus revealing the secret message. The operation is quite simple and, in the case of a pseudo-random generator, the receiver needs to know the initial conditions of the transmitter. The broadband spectrum of the random signal guarantees the security of the communication scheme, since the secret message is drowned into the noise-like carrier. The communication can rely on sinusoidal carriers, see [3] for a survey of the theory of conventional communications. Chaotic models can be used as noise-like carriers, and are extremely sensitive to initial conditions. Moreover, chaotic signals are not periodic, contrary to classical carriers (even if their period is very large): consequently, chaos-based communications can resist to attacks based on periodicity of signal carriers. Chaotic communication schemes rely on synchronization: the information signal is mixed at the transmitter, a chaotic signal is then generated and sent to the receiver, which enables synchronization. Once synchronization is achieved, the information signal is recovered by the receiver. An overview of the different chaotic synchronization schemes applied to digital and analog communications can be found in [4], [5], [6] and [7].

Many schemes have been designed to transmit a message in an efficient and secure way: the main difference lies in the method chosen to inject or hide the message at the transmitter, and then to recover it at the receiver. This variety of encoding methods can be seen as an additional advantage of chaotic encryption compared to classical encryption. The main chaotic message encoding methods are *chaotic masking*, *chaotic shift keying*, *chaotic modulation*, *chaotic cryptosystems*, relying on analog synchronization and *impulsive methods*, relying on impulsive synchronization. In *chaotic masking* [4], [8], [9] the information signal is added to the chaotic signal sent by the transmitter. If the amplitude of the message is small enough (compared with the amplitude of the chaotic signal), the receiver is able to synchronize with the transmitter: the reconstructed chaotic signal is then simply subtracted from the transmitted signal to obtain the information signal. In *chaotic shift keying* [10] usually the information signal is supposed to be binary. A switch between two parameter sets of the chaotic transmitter is realized, depending on the value (there are two possible) of the signal at each time. The receiver consists of two possible chaotic systems, and the decision is taken according to the synchronization error: at each time, the transmitted signal enables the synchronization of only one of the receivers. In *chaotic modulation* [11], also called *inverse system approach*, the information signal modulates some parameter(s) of the chaotic encoder. Once the synchronization is achieved at the receiver, the reconstructed chaotic signal is applied to the inverse encoder to recover the message. These processes are the first chaotic communication schemes that have been designed. Some attacks [12], [13] have shown that they suffer from a lack of security. Recently, *chaotic cryptosystems* have been proposed, see [14], [15], or [16] to mention just a few. The theory of impulsive differential equations has led to a new generation of chaotic synchronization

Manuscript received June 15, 2005; revised November 29, 2005. This paper was recommended by Associate Editor C. T. Lin.

E. Cherrier is with the Institut National Polytechnique de Lorraine (INPL), Centre de Recherche en Automatique de Nancy (CRAN), Vandoeuvre-les-Nancy Cedex 54516, France, and also with the Laboratoire des Sciences de l'Image de l'Informatique et de la Télédétection (LSIIT), Strasbourg, Illkirch Cedex 67412, France (e-mail: cherrier@eavr.u-strasbg.fr). J. Ragot is with the Institut National Polytechnique de Lorraine (INPL), Centre de Recherche en Automatique de Nancy (CRAN), Vandoeuvre-les- Nancy Cedex 54516, France. M. Boutayeb is with the Computer Sciences and Remote Sensing Laboratory [Laboratoire des Sciences de l'Image de l'Informatique et de la Télédétection (LSIIT)], University Louis Pasteur, Strasbourg, Illkirch Cedex 67412, France. Digital Object Identifier 10.1109/TCSI.2006.882817

schemes [7], called *impulsive methods*. Other methods have been proposed, combining two (or more) of these techniques, or using tools from other fields (identification, optics). [17] presents a communication scheme based on the detection of a parameter mismatch. A modulation technique is proposed in [18], where the receiver is designed as a nonlinear filter. In [19], the chaotic carrier is modulated with an appropriately chosen scalar signal. The properties of optical systems are exploited to design communication schemes, as in [20]. Some observer-based communication schemes are designed in [21], [22], [23], [24] , [25].

Regardless of the type of encryption used, when a new chaos-based communication scheme is designed, it is worth to analyze some security aspects. Besides, some attacks against new cryptosystems are developed in [26], [27], [28], [29]. [30] gives an overview of the cryptanalysis methods. It details the points that are rarely verified to guarantee the security of the previous chaotic communication schemes.

In this note, we propose a simple and efficient method to transmit a message in a secure way, which can be seen as a new *chaotic cryptosystem*, to use the previous terminology. For this purpose, two chaotic signals are sent by the transmitter. On the one hand, a first signal is aimed at synchronizing the receiver, which is designed following a nonlinear observer-based approach: the full-order and reduced-order observer cases are addressed for a class of time-delayed systems, and sufficient conditions for asymptotic convergence are derived in terms of Linear Matrix Inequalities (i.e. convex problem) easily and numerically tractable. On the other hand, a second signal is used to encrypt the message: the information signal is injected in the second chaotic signal to create a variable delay. Thus, this process performs a kind of phase modulation of the original chaotic signal. The recovery of the message is realized at the receiver. An estimation of the delay is enabled by the comparison between the transmitted delayed signal, and the estimation of the same signal without delay. The transmitter is a new chaotic system, chosen for its noise-like trajectories, for its mathematical properties, and for its great sensitivity to a particular parameter, that will be seen as a possible secret key.

The first part of this note details the new cryptosystem. Section II gives some details about the chaotic transmitter, the observer-based synchronization is addressed in Section III, and Section IV is devoted to the encryption-decryption method. The efficiency of our cryptosystem is then tested in section V through the encryption, the transmission (through the Internet) and the recovery of a sound signal and a picture. Section VI ends this paper with a study of some security aspects of the proposed cryptosystem.

II. The transmitter: a time-delayed chaotic system

The field of "anticontrol" of chaos is quite new. It consists in generating chaos in a non-chaotic system, or in enhancing the chaotic behavior of a chaotic system. [31] details the example of well-known systems which belong to the class of chaotic systems, such as the systems of Rössler, Lorenz, or Chua's circuit: their chaotic behavior becomes more complex if a time-delayed feedback is added in the third state component. In [32] the case of Chua's circuit is detailed, and the modified Chua's circuit designed in that paper was chosen as the chaotic transmitter in the synchronization schemes that we proposed in [33] and [34]. A particularity of Chua's circuit is that its nonlinear part is a piecewise-linear function, which may be not desirable from a mathematical point of view. In fact, this nonlinearity can be replaced by any scalar nonlinearity, provided that it is an odd function: for example in [35], the new nonlinearity is a polynomial of degree three. We have chosen to keep the structure of the chaotic transmitter of [33] to design a new chaotic system: its linear part is based on the structure of the dimensionless form of Chua's circuit, its nonlinear part is an hyperbolic tangent and a time-delayed feedback creates the chaos:

$$\dot{x}(t) = Ax(t) + F\left(x(t)\right) + H\left(x(t-\tau)\right) \tag{1}$$

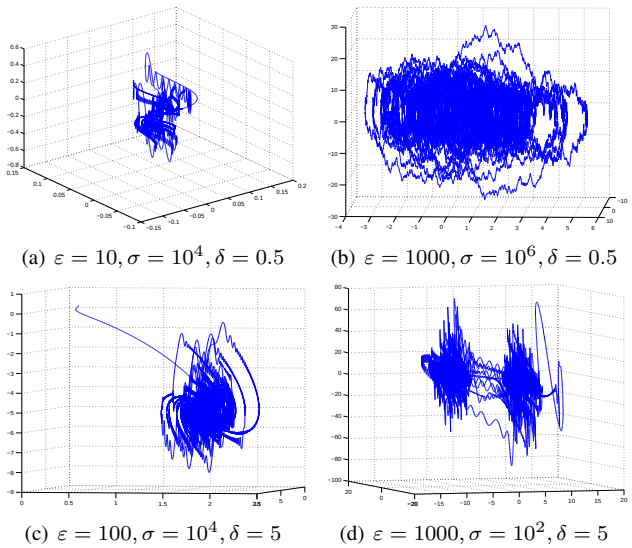
where

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{2}$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta \tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix} \tag{3}$$

$$H(x(t-\tau)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma x_1(t-\tau)) \end{pmatrix} \tag{4}$$

The presence of the delayed feedback $H(.)$ is necessary to observe a chaotic behavior: if ε equals zero, system (1) is not chaotic. We provide some representations of the chaotic behavior of this system on Fig. 1(a)-1(d), for the following fixed values of the parameters: $\alpha = 9$, $\beta = 14$, $\gamma = 5$, $\tau = 1$ (the values of ε, σ and δ are given under each figure). Farmer [36] has shown that the complexity of the chaotic attractor is strongly linked with the presence of the time-delay feedback. Therefore changes in the parameters values (particularly the parameters of $H(.)$) lead to various shapes and complicated chaotic attractors. However, the study of the chaos in system (1) deserves further investigations. In practice, computation of the Lyapunov exponents (see [37] for a complete definition) is the only available and tractable



(a) $\varepsilon = 10, \sigma = 10^4, \delta = 0.5$ (b) $\varepsilon = 1000, \sigma = 10^6, \delta = 0.5$

(c) $\varepsilon = 100, \sigma = 10^4, \delta = 5$ (d) $\varepsilon = 1000, \sigma = 10^2, \delta = 5$

Fig. 1. Attractors for different values of ε, σ, δ

tool to show that a system is chaotic (only a necessary one). The Lyapunov exponents of (1) can be computed using the method detailed in [36], since all the involved nonlinearities are smooth enough. For the lack of space, this question is not addressed here, and will be detailed in a future work.

Notations: Throughout this paper, the superscript T stands for matrix transposition. The matrix I_n stands for identity matrix of dimension n. We recall that a function $f(.)$ verifies the Lipschitz property if there exists a positive scalar k such that:

$$\|f(x) - f(y)\| \leq k\|x - y\| \ \forall \ x, y \tag{5}$$

k is called the Lipschitz constant of $f(.)$. (3) and (4) show that the nonlinear functions $F(.)$ and $H(.)$ satisfy the Lipschitz condition with constants $k_F = |\alpha\delta|$ and $k_H = |\varepsilon\sigma|$ respectively.

III. Observer-based synchronization: full-order and reduced-order observer designs

In this section we are interested in the design of a receiver which ensures synchronization with the transmitter (1), by the means of a transmitted signal. Two important methods are available: the *drive-response principle*, and the *observer-based synchronization*. The first one was developed by Pecora and Carroll in 1990 [1]. In this scheme, the transmitter is a chaotic system, and the receiver is a duplicate of a subsystem of the transmitter, while the driving signal sent by the transmitter is some of its state variables. Under some conditions detailed in [1] (the conditional Lyapunov exponents [37] of the response system driven by the transmitted signal must be all negative), they showed that synchronization occurs between the transmitter and the receiver, in spite of the extreme sensibility of chaotic systems to their initial conditions (indeed, the receiver has no information about the initial conditions of the transmitter). The only limitation of this concept remains the difficulty to find a "good" decomposition of the chaotic transmitter to obtain a drive signal and a receiver which synchronizes, since there is no systematic procedure available. The second method, detailed in [38], [39], is called *observer-based synchronization* since the problem of synchronization can benefit from the results of the estimation theory. If the transmitter is a chaotic system, and if the receiver is designed as an observer of the transmitter, the receiver actually synchronizes with the transmitter, provided that the receiver and the transmitted signal verify a detectability condition, with some additional conditions that will be detailed. We refer the reader to some observers based synchronization schemes [40], [41], [21], [23], [22] and to the references inside.
In this section, we develop two observer-based approaches, adapted from the results of [33], in which we detailed a full-order-observer-based synchronization, and of [34], in which we designed a reduced-order observer.

A. Full-order observer-based synchronization

In this section we propose a full-order observer-based approach to ensure synchronization with the transmitter (1). The receiver estimates the three states of the transmitter, by means of the following transmitted signal:

$$y_1(t) = Cx(t) \tag{6}$$

The chaotic behavior of system (1) depends on the values of ε and σ: the larger these parameters are, the more complex the chaos is (and the more secure the encryption is, see section VI). Consequently the Lipschitz constant of the function H defined by (4) is quite large (generally over 10^5), and we choose the matrix C of the form $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$:

$$y_1(t) = x_1(t) + \zeta x_2(t) \tag{7}$$

The dynamic model of the transmitter (1) can be rewritten as:

$$\left\{ \begin{array}{rcl} \dot{x}(t) & = & \tilde{A}x(t) + \tilde{B}y_1(t) + \tilde{F}(y_1(t), x_2(t)) \\ & & +\tilde{H}(y_1(t-\tau), x_2(t-\tau)) \\ y_1(t) & = & Cx(t) \end{array} \right. \tag{8}$$

where

$$\tilde{A} = \begin{pmatrix} 0 & \alpha(1+\zeta) & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{9}$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix} \tag{10}$$

$$\tilde{F}(y_1(t), x_2(t)) = \begin{pmatrix} \alpha\delta \tanh(y_1(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix} \tag{11}$$

$$\tilde{H}(y_1(t-\tau), x_2(t-\tau)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin\left(\sigma(y_1(t-\tau) - \zeta x_2(t-\tau))\right) \end{pmatrix} \tag{12}$$

The dynamic model of the full-order observer chosen as the receiver is the following:

$$\begin{array}{rcl} \dot{\hat{x}}(t) & = & \tilde{A}\hat{x}(t) + \tilde{B}y_1(t) + \tilde{F}(y_1(t), \hat{x}_2(t)) \\ & & +\tilde{H}(y_1(t-\tau), \hat{x}_2(t-\tau)) + K(y_1(t) - C\hat{x}(t)) \end{array} \tag{13}$$

where K is the observer gain, and will be determined in the following.
We define the synchronization error vector $e(t) = x(t) - \hat{x}(t)$, and its derivative is given by

$$\dot{e} = A_K e + \tilde{F} - \hat{\tilde{F}} + \tilde{H} - \hat{\tilde{H}} \tag{14}$$

with the notations

$$\begin{array}{l} A_K = \tilde{A} - KC, \\ \tilde{F} = \tilde{F}(y_1(t), x_2(t)), \quad \hat{\tilde{F}} = \tilde{F}(y_1(t), \hat{x}_2(t)), \\ \tilde{H} = \tilde{H}(y_1(t-\tau), x_2(t-\tau)), \quad \hat{\tilde{H}} = \tilde{H}(y_1(t-\tau), \hat{x}_2(t-\tau)) \end{array}$$

The following theorem provides sufficient conditions for the synchronization of the full-order observer (13) with the transmitter (8).

Theorem 1: If the following conditions are verified:

1) the pair $(\tilde{A}, C)$ is detectable;
2) there exist $k_1, k_2 > 0$, a matrix K and a symmetric, positive-definite matrix P (of appropriate dimensions) solution of the following LMI:

$$\zeta^2 k_H^2 - k_1 + 1 < 0 \tag{15}$$

$$\begin{pmatrix} A_K^T P + P A_K + k_1 I_3 & P \\ P & -\frac{1}{k_2} I_3 \end{pmatrix} < 0 \tag{16}$$

then (13) is an observer for the transmitter (8): $\hat{x}(t) \to x(t)$ when $t \to \infty$.

Proof: The transmitter is a time-delay system, so we consider a Lyapunov-Krasovskii functional

$$V = e^T P e + \xi \int_{-\tau}^{0} e(t+\theta)^T e(t+\theta) d\theta \tag{17}$$

where P is a symmetric, positive-definite matrix, and ξ is a positive scalar. It is easy to show that V is positive and upper bounded.
We compute the derivative of V along the trajectories of (14):

$$\begin{aligned} \dot{V} &= e^T \left(A_K^T P + P A_K\right) e + 2e^T P(\tilde{F} - \hat{\tilde{F}}) \\ &\quad + 2e^T P(\tilde{H} - \hat{\tilde{H}}) + \xi e^T e - \xi e_\tau^T e_\tau \end{aligned} \tag{18}$$

with $e_\tau(t) = e(t-\tau)$.
The application of the Young inequality leads to:

$$2e^T P(\tilde{F} - \hat{\tilde{F}}) \leq \zeta^2 k_F^2 e^T P P e + e^T e \tag{19}$$

where k_F denotes the Lipschitz constant of F.
The same reasoning applied to the function H gives the following upper bound:

$$2e^T P(\tilde{H} - \hat{\tilde{H}}) \leq e^T P P e + \zeta^2 k_H^2 e_\tau^T e_\tau \tag{20}$$

With (19) and (20), (18) can be rewritten as:

$$\begin{aligned} \dot{V} &\leq e^T \left(A_K^T P + P A_K + (1+\xi) I_3 + (1+\zeta^2 k_F^2) P^2\right) e \\ &\quad + (\zeta^2 k_H^2 - \xi) \|e_\tau\|^2 \end{aligned} \tag{21}$$

We set $k_1 = 1 + \xi$ and $k_2 = 1 + \zeta^2 k_F^2$.
If we set $\zeta^2 k_H^2 - \xi < 0$, then condition (15) holds, and (21) reduces to:

$$\dot{V} \leq e^T \left(A_K^T P + P A_K + k_1 I_3 + k_2 P^2\right) e \tag{22}$$

So the derivative of the Lyapunov-Krasovskii function V is negative-definite:

$$\dot{V} \leq -e^T W e \tag{23}$$

with

$$W = -(A_K^T P + P A_K + k_1 I_3 + k_2 P^2) > 0 \tag{24}$$

The inequality $W > 0$ is transformed into a convex problem, easily and numerically tractable. Indeed, thanks to the Schur complement, we obtain:

$$W > 0 \Leftrightarrow \begin{pmatrix} A_K^T P + P A_K + (1+\xi) I_3 & P \\ P & -\frac{1}{(1+\zeta^2 k_F^2)} I_3 \end{pmatrix} < 0 \tag{25}$$

This demonstrates the condition (16), and guarantees that e converges towards zero. ■
Thus the synchronization step is achieved.
The LMI (25) can be solved numerically. If we note $L = PK$ (which is equivalent to $K = P^{-1}L$ since P is invertible), we obtain:

$$A_K^T P + P A_K + (1+\xi) I_3 = \tilde{A}^T P + P \tilde{A} - C^T L^T - P L + (1+\xi) I_3 \tag{26}$$

where we recall that $A_K = \tilde{A} - KC$.
The right-hand side term is linear in P and L, and thus the LMI (25) can be easily solved by standard convex optimization algorithms.

Remark 2:
The detectability of the pair $(\tilde{A}, C)$ is guaranteed by the fact that the matrix W is negative-definite. Indeed, (25) implies (with $k_1 > 0$):

$$A_K^T P + P A_K < 0 \tag{27}$$

which means that the matrix A_K is stable.

Remark 3: In practice, to find a solution to the LMI (16), we set $\xi \leq 1$. Consequently, to satisfy (15), ζ is chosen such that $-1 \leq \zeta k_H \leq 1$.

B. Reduced-order observer-based synchronization

In a second step, it seems that it is not necessary to design a full-order observer to estimate the three chaotic states of the transmitter (8), since the transmitted signal y_1 contains some information about the trajectories of the states. So we propose another observer, of reduced order, to ensure synchronization with the transmitter. Before we give the dynamics of this reduced-order observer, we make some transformations on the dynamical model (8). We only consider the differential equations defining x_2 and x_3: let E be a matrix orthogonal to F (defined in (3)), such that $\begin{pmatrix} E \\ C \end{pmatrix}$ is of full column rank. From (8) we obtain the following singular equation:

$$E\dot{x}(t) = EAx(t) + EF(x(t)) + EH(x(t-\tau)) \tag{28}$$

With the following notations:

$$\begin{aligned} &\tilde{A} = EA \\ &\tilde{H}(x(t-\tau)) = EH(Ex(t-\tau), y_1(t-\tau)) \end{aligned} \tag{29}$$

if we replace x_1 by $y_1 - \zeta x_2$, according to (7), (28) becomes, using (8):

$$\begin{cases} E\dot{x}(t) = \tilde{A}x(t) + \tilde{H}(Ex(t-\tau), y_1(t-\tau)), \\ y_1(t) = Cx(t) \end{cases} \tag{30}$$

Since the matrix $\begin{pmatrix} E \\ C \end{pmatrix}$ is of full column rank, there exist two matrices (of appropriate dimensions) P and Q such that:

$$\begin{pmatrix} P & Q \end{pmatrix} \begin{pmatrix} E \\ C \end{pmatrix} = I_3 \tag{31}$$

Then:

$$\begin{pmatrix} P & Q \end{pmatrix} = \left(\begin{pmatrix} E \\ C \end{pmatrix}^T \begin{pmatrix} E \\ C \end{pmatrix} \right)^{-1} \begin{pmatrix} E \\ C \end{pmatrix}^T \tag{32}$$

We set

$$z = Tx = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \tag{33}$$

where T is chosen such that the components of z are two independent linear combinations of x_2 and x_3.
To ensure synchronization with the transmitter (8), we propose the following reduced-order observer:

$$\begin{cases} \dot{z}(t) = Nz(t) + Ky_1(t) + r(z(t), y_1(t), z(t-\tau), y_1(t-\tau)) \\ \hat{z}(t) = z(t) + TQy_1(t) \end{cases} \tag{34}$$

where N, K and the function $r(.)$ should be be determined so that $z(t) - \hat{z}(t)$ goes to zero.
The following theorem provides a sufficient condition for the synchronization of the reduced-order observer (34).

Theorem 4: If the following conditions are verified:

1) $$\text{rank} \begin{pmatrix} sE - \tilde{A} \\ C \end{pmatrix} = \dim x, \ \forall s \geq 0 \tag{35}$$

2) there exists a matrix N solution of the Sylvester equation:
$$NTPE - TP\tilde{A} + KC = 0 \tag{36}$$

3) the matrix $\begin{pmatrix} TPE \\ C \end{pmatrix}$ is non singular;

4) there exist two symmetric, positive-definite matrices W and U such that:

$$N^T U + UN = -W \tag{37}$$

and

$$W - \rho k_H I_2 > 0, \text{ with } \rho = 2\|UTP\| \tag{38}$$

then the function r can be defined by:

$$r(z(t), y_1(t), z(t-\tau), y_1(t-\tau)) = TP\tilde{H}(\hat{x}(t-\tau)) \tag{39}$$

with

$$\hat{x}(t) = \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} \begin{pmatrix} \hat{z}(t) \\ y_1(t) \end{pmatrix} \tag{40}$$

In this case, the reduced order-observer (34) is asymptotically convergent, and $\hat{x}(t)$ synchronizes with $x(t)$.

Proof: The reduced state estimation error vector is given by:

$$e = \hat{z} - z \tag{41}$$

(30), (31) and (34) yield:

$$e = (z + TQy_1) - z = TQCx = T(I_3 - PE)x = z - TPEx \tag{42}$$

By derivation of (42), the dynamics of the error is:

$$\begin{aligned} \dot{e} &= Nz + Ky_1 + r(z, y_1, z_\tau, y_{1\tau}) \\ &\quad -TP\left(\tilde{A}x + \tilde{H}(Ex_\tau, y_{1\tau})\right) \\ &= Ne + \left(NTPE + KC - TP\tilde{A}\right)x + r(z, y_1, z_\tau, y_{1\tau}) \\ &\quad -TP\tilde{H}(Ex_\tau, y_{1\tau}) \end{aligned} \tag{43}$$

By making use of the Sylvester equation (36) and the definition of r (39), (43) becomes:

$$\dot{e} = Ne + TP\left(\tilde{H}(\hat{x}_\tau) - \tilde{H}(x_\tau)\right) \tag{44}$$

The stability of the matrix N is guaranteed if we can find a symmetric, positive-definite matrix U and a positive-definite matrix W such that (37) holds.
Then the matrix U is used to design a Lyapunov function:

$$V = e^T U e \tag{45}$$

The derivative of V along the trajectories of (44) is given by:

$$\dot{V} = e^T(N^T U + UN)e + 2e^T UTP\left(\tilde{H}(\hat{x}_\tau) - \tilde{H}(x_\tau)\right) \tag{46}$$

We obtain the following upper bound for $\dot{V}$:

$$\dot{V} \leq -e^T We + 2k_H \|UTP\| e\|^2 \tag{47}$$

If (38) holds, then $\dot{V} \leq 0$, so the reduced-order observer (34) is asymptotically convergent.
To show that $\hat{x}$ converges towards x, we compute the difference (using (40)):

$$\begin{pmatrix} TPE \\ C \end{pmatrix}(\hat{x} - x) = \begin{pmatrix} \hat{z} - TPEx \\ y_1 - Cx \end{pmatrix} \tag{48}$$

Besides, using (42), we can write $\hat{z} \to TPEx$. Consequently

$$\begin{pmatrix} TPE \\ C \end{pmatrix}(\hat{x} - x) \to 0 \tag{49}$$

Since the matrix $\begin{pmatrix} TPE \\ C \end{pmatrix}$ is invertible by hypothesis 3) of Theorem 1, (49) is equivalent to $\hat{x} \to x$. ∎
Hereafter we provide a design procedure for N and K (see details in [34]) :

- choose a matrix R such that $\begin{pmatrix} R \\ C \end{pmatrix}$ is invertible
- compute

$$L_1 = \begin{pmatrix} R \\ C \end{pmatrix}^{-1} \begin{pmatrix} I_2 \\ 0 \end{pmatrix} \tag{50}$$

- compute S such that $N = RP\tilde{A}L_1 - SC\tilde{A}L_1$ and N is stable (i.e. all eigenvalues have negative real part) and then deduce N
- compute $T = R - SC$ and $F = TQ - S$
- compute

$$L_2 = \begin{pmatrix} R \\ C \end{pmatrix}^{-1} \begin{pmatrix} F \\ 1 \end{pmatrix} \tag{51}$$

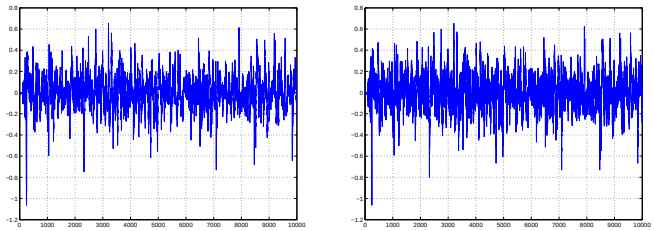
and then $M = NTL_2 - TP\tilde{A}L_2$, $K = NTQ - M$

IV. The encryption method

In this section we describe the encryption/decryption approach, based on the synchronization step detailed above. The aim is to send a chaotic signal, with a message "mixed" or "hidden" in it, in such a way that no one can suspect that information has been transmitted. Some attacks showed that some schemes are not secure enough [12], [13], [30], so we have designed a method for "injecting" the message which prevents it from altering the transmitted signal or its power spectral density.
Since the chaotic signal y_1 is only sent for synchronization purpose, we introduce a second chaotic signal independent of y_1 (see security issues in section VI). We underline that y_2 is sent independently of y_1, where the message is injected in the following manner:

$$y_2(t) = x_3(t - T_u u(t)) \tag{52}$$

The parameter T_u will be discussed later. (52) shows that the signal $y_2(t)$ is obtained from the chaotic signal $x_3(t)$, by a phase modulation. Therefore, y_2 is also a noise-like signal (see Fig. 2 with $u(t) = |sin(t)|$). Now we detail the



(a) Plot of $x_3(t)$ (b) Plot of $y_2(t)$

Fig. 2. Comparison of $x_3(t)$ and $y_2(t)$

encryption/decryption process. Since all the functions involved in the design of the transmitter (8) are sufficiently smooth, the Taylor-Lagrange formula can be applied to $x_3(t)$, y_2 being defined in (52), and we obtain the following first-order approximation:

$$x_3(t) - x_3(t - T_u u(t)) \simeq \dot{x}_3(t) T_u u(t) \tag{53}$$

In practice, the information signal is normalized, i.e. $u(t) \in [0, 1]$, that T_u must be less than T_e (the integration step) in order to apply the Taylor-Lagrange formula and by the way to ensure a good quality of signal reconstruction. Consequently, T_u plays a major role in the encryption procedure. Indeed, T_u introduces a flexibility in the choice of the integration step T_e which is chosen with respect to dynamics of the chaotic model.
Now we intend to give an estimation of $u(t)$, from (53). First, we remark that our encryption method relies on the fact that chaotic signals vary very fast, so they are never

constant. Otherwise, it would be impossible to recover the delay, since x_3 and y_2 would take the same value. That is why this encryption tool well fits to chaotic systems. So we may deduce $u(t)$ from (53) (provided that $\dot{x}_3(t) \neq 0$):

$$u(t) \simeq \frac{x_3(t) - y_2(t)}{T_u \dot{x}_3(t)} \tag{54}$$

Remark 5: If the case $\dot{x}_3(t) = 0$ happened, we would consider a second-order approximation, involving the second-order derivative of x_3 and therefore it is possible to express $u(t)$ as a function of $\ddot{x}_3(t)$.
Once the synchronization step is achieved at time t, it is possible to recover $u(t)$, by the use of (54) (we note $\hat{u}$ the recovered message):

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \tag{55}$$

where $\dot{\hat{x}}_3(t)$ is replaced as a function of $\hat{x}(t)$ and $y_1(t)$, given by the dynamic model of the receiver, (13) or (34).

The efficiency of our encryption-decryption method mainly relies on the efficiency of the synchronization, which can be done in a completely separated step: the receiver synchronizes with the transmitter as fast as possible thanks to y_1, and the estimated states are used to decrypt the message thanks to the signal y_2. This will be illustrated in the next section through Internet transmission of two messages, whereas some security issues will be discussed in section VI.

V. Simulations of the cryptosystem

To test the theoretical results obtained in the previous parts, we will study the synchronization and the encryption/decryption of two messages (a sound wave, and a picture), both drive signals y_1 and y_2 being transmitted through the Internet. The proposed approach concerns continuous-time systems. However simulations have been performed at a first step on a computer, in the goal to evaluate its performances.
We recall the dynamic model of the transmitter (8), and we precise the values of the parameters chosen in this section:

$$\left\{ \begin{array}{lcl} \dot{x}_1(t) &=& -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) &=& x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &=& -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_1(t-\tau)) \end{array} \right. \tag{56}$$

with $\alpha = 9$, $\beta = 14$, $\gamma = 5$, $\delta = 0.5$, $\varepsilon = 10$, $\sigma = 10^4$, $\tau = 1$.
The observation equation is:

$$y_1(t) = Cx(t) \tag{57}$$

with $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$, and $\zeta = \frac{1}{\varepsilon\sigma} = 10^{-5}$.

A. Synchronization

We first look at the performances of the full-order observer (13). The hypotheses of theorem 1 are verified, with $\xi = 1$, so $k_1 = 2$, $k_2 = 1.000000002025$, and:

$$K = \begin{pmatrix} 32.15612817030280 \\ 26.91023086940931 \\ -28.44982242054409 \end{pmatrix} \tag{58}$$

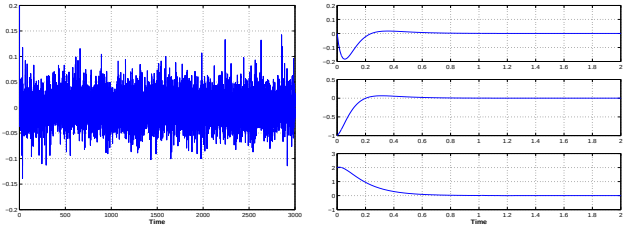
The initial conditions for the transmitter and the receiver are respectively:

$$x_0 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}^T \tag{59}$$

and

$$\hat{x}_0 = \begin{pmatrix} 1 & 2 & -1 \end{pmatrix}^T \tag{60}$$

The simulations are done with a time integration step $T_e = 0.01$. We show the synchronizing signal $y_1(t)$ sent by the transmitter in Fig. 3(a). The results of the synchronization



(a) The synchronizing signal y_1 (b) Plots of the synchronization errors

Fig. 3. Full-order observer-based synchronization

step are plotted in Fig. 3(b), which shows the three state reconstruction errors: the synchronization is achieved very fast, after two seconds.

Now we analyze the efficiency of the reduced-order observer (34) chosen as the receiver. To apply Theorem 4, we take the following matrices:

$$E = T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{61}$$

We obtain by using (32):

$$P = \begin{pmatrix} -\zeta & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{62}$$

$$Q = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T \tag{63}$$

The matrices involved in the reduced-order observer (34) are:

$$N = \begin{pmatrix} -1 & 1 \\ -\beta & -\gamma \end{pmatrix} \tag{64}$$

$$K = \begin{pmatrix} 1 & 0 \end{pmatrix}^T \tag{65}$$

Equation (37) is checked, with $W = I_2$ and

$$U = \begin{pmatrix} 1.05263157851685 & -0.03947368425496 \\ -0.03947368425496 & 0.09210526314901 \end{pmatrix} \tag{66}$$

Fig. 4 shows the efficiency of the reduced-order observer-based synchronization: it is quite similar to the efficiency of the full-order observer, synchronization is also achieved in about two seconds. However, since the number of states to estimate is reduced, the simulation time is reduced too.

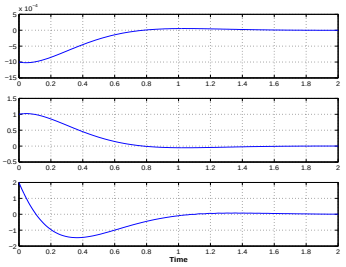


Fig. 4. Plots of the three synchronization errors for the reduced-order observer-based synchronization

The notion of key will be discussed later (see Section VI), however, we can mention that the parameter σ may be considered as a possible key for the proposed encryption method. In Sections V-A and V-B, the aim is to show the effectiveness of the proposed scheme between the transmitter and an authorized receiver, so the value of σ is perfectly known by the receiver.

B. Encryption and decryption

We test the efficiency of our encryption method on two types of messages: a sound message, and a digital picture.

1) Example 1 - a sound message:
the message u is generated from a sound signal, and is scaled to guarantee that $u(t) \in [0,1]\ \forall t > 0$. Fig. 5 shows its plot. This vector is used to define $y_2(t)$, from $x_3(t)$ (see Fig. 6(a)). The decryption step is performed using formula (55),

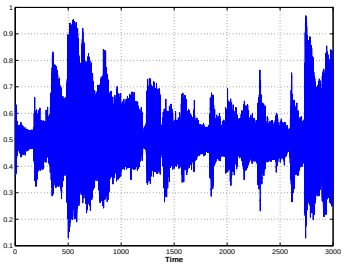
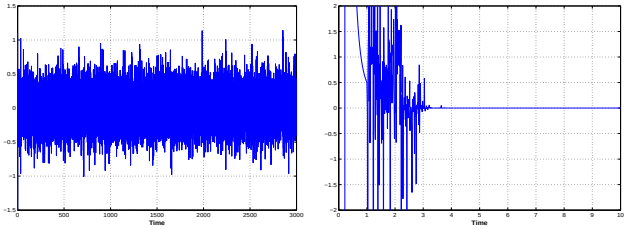


Fig. 5. A sound message



(a) Encrypted signal (b) Recovery error of the sound message

Fig. 6. Encrypted and decrypted sound messages

and Fig. 6(b) shows the good performances, after a transient time necessary to obtain a good synchronization. This can be avoided by systematically sending an empty message added before the information-bearing message u. In this manner, the synchronization step will be achieved when the signal begins to be decrypted. However, preamble duration devoted to synchronization is not discussed. In fact, this point depends in particular on the model parameter values. From a practical point of view, the user may easily estimate the preamble duration for a given set of parameters by experiments, a priori. Therefore, this drawback can easily be bypassed. In our examples, the synchronization time is about two seconds, after that the information signal may be injected.

2) Example 2 - a picture:
The process of encryption is made more visual on this example. The tests are realized with the famous "Lenna picture", see Fig. 7. From this picture, a discrete signal is generated

Fig. 7. Original Lenna picture

as a three-dimension array: each square matrix corresponds to one basic color (red, green, blue). The process to obtain a one-dimensional vector is quite standard: the rows of the first matrix are concatenated, immediately followed by the rows of the second, and the third matrices. Then the coefficients of this vector are normalized to obtain the signal u belonging to $[0,1]$. The encrypted picture corresponding to the transmitted signal y_2 is shown in Fig. 8(a). The recovery of the signal

(a) Encrypted Lenna picture (b) Decrypted Lenna picture

Fig. 8. Encrypted and decrypted pictures

u is illustrated by the curve in Fig. 9, and the corresponding picture in Fig. 8(b).

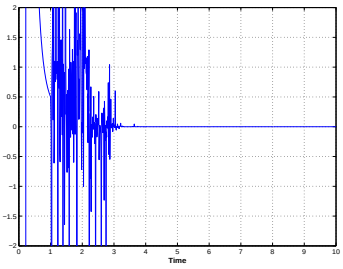


Fig. 9. Recovery error of the message u

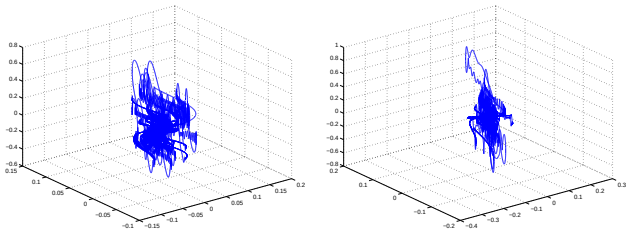
VI. Some security issues

Some recent works [30] point out that the security issues are not always addressed when a new cryptosystem is designed. Therefore, this section is devoted to some security questions. For all the chaotic cryptosystems, the security relies on the parameters of the transmitter. It is often assumed that, without the exact knowledge of these parameters, it is impossible to recover the message. However, this is not always the case (see references in section I), and some specific attacks are regularly

designed to break chaotic encryption schemes (mostly chaotic masking, or modulation).

We would like to show here that our cryptosystem possesses a key, which is represented by the parameter σ. We already mentioned in section II that the presence of the time-delay feedback (4) influences the chaotic behavior of the transmitter (8). The function $H(.)$ only acts on the third state, under the form $\varepsilon \sin(\sigma x_1(t-\tau))$. So the parameter σ defines how fast the chaotic signal x_1 is mixed into the sine function, and the Lipschitz constant of $H(.)$ is equal to $\varepsilon\sigma$. Fig. 10 shows two different attractors, for the values fixed at the beginning of section V.

Therefore, the parameter σ can be used as a secret key. For



(a) $\sigma = 10000$ (b) $\sigma = 10001$

Fig. 10. Attractors for near values of σ

a better visualization of the results, we use the picture in Fig. 7 as the message to be transmitted. The first test is quite simple: we suppose that an intruder obtains the structure of the receiver, and has access to the signals y_1 and y_2, but does not know exactly the value of σ used in the transmitter. On Fig. 11 the deciphered message appears: for the simulation, $\sigma = 10000$ in the transmitter, and at the receiver the value 10001 is chosen (here ε has been set to 1000).

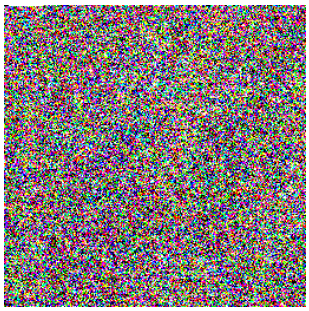


Fig. 11. Deciphered image with a 0.01% mismatch on σ

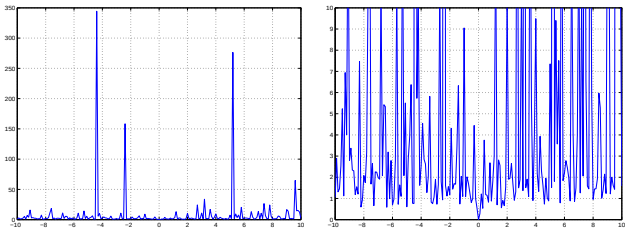
Remark 6: We notice that the sensibility increases with the value of σ: if $\sigma = 100000$, then a 0.001%-mismatch produces the same result as Fig. 11.

Another security test of the cryptosystem is done in the following simulation. If it happens that the same message has to be sent twice, then we must be sure that no information can be deduced from the subtraction of the successive encrypted signals. In fact, a simple change of the value of the key σ shows that our cryptosystem possesses the property of diffusion (required by [30] for example): the image obtained by subtraction of two encryption of the same image, with two different keys is shown in Fig. 12 (the other remarkable property of confusion is more difficult to verify, and will be considered in further studies).

To quantify the sensibility of the deciphering as a function

Fig. 12. Image obtained by subtraction of two encrypted images

of the mismatch on σ, we choose the value $\sigma = 10000$ at the transmitter. Then another value noted $\tilde{\sigma}$, very close to σ is chosen at the receiver, and the reconstruction of the secret message is then analyzed. The value of $\tilde{\sigma}$ is increased of $10^{-5}\sigma$ at each step, starting from 10000, with 100 steps, and decreased in a symmetric manner: the maximum error rate on σ is $100 \times 10^{-5} = 0.1\%$. The corresponding range of variation of $\tilde{\sigma}$ is then 10000 ± 10. For each value of $\tilde{\sigma}$, the norm of the difference $u - \hat{u}$ divided by the total number of points in u is computed, and Fig. 13(a) shows this norm as a function of the mismatch on σ (to cope with the errors due to synchronization, we start the simulations with the same initial conditions for the transmitter and the receiver). Fig. 13(b) shows a zoom on the



(a) (b) Zoom in Fig. 13(a)

Fig. 13. Error rate of the deciphering vs. error rate on σ

amplitude of Fig. 13(a): the deciphering is exact only when the receiver exactly knows the value of σ, that is to say the error rate on σ is equal to zero, or $\tilde{\sigma} = \sigma$.

Remark 7: Generally, concerning most of chaotic cryptosystems, there is an antinomy between the notions of security and robustness. It is often necessary to define a tradeoff which allows a certain robustness to the noise present in the transmission channel, and which also guarantees a sufficient level of security. Our cryptosystem follows this property: if less security is imposed, we can take $\varepsilon = 10$ and $\sigma = 100$. The deciphering remains correct with an uniform noise added on y_1, corresponding to a Signal-to-Noise Ratio (SNR) of 70 dB (see Fig. 14(a)), whereas the result of the deciphering is strongly perturbed for an uniform noise corresponding to a SNR of 35 dB (see Fig. 14(b)). This shows that the synchronization is very sensitive to noise, and must be performed with a high accuracy to ensure a good deciphering.

(a) SNR of 70 dB (b) SNR of 35 dB

Fig. 14. Recovered picture with different SNR w.r.t. y_1

VII. Conclusion

In this paper, the problem of observer-based synchronization and secure communication was addressed. We use a time-delayed chaotic system as a transmitter. A first chaotic signal is sent to assure an observer-based synchronization. For this purpose, both full-order and reduced-order observers were successfully used as the receiver. Sufficient conditions for synchronization in terms of LMIs were established. Then we propose a new encryption method: a second chaotic signal is sent, modulated by a variable delay depending on the message. Some simulations illustrate the efficiency of our observer-based cryptosystem: a sound signal, and the famous "Lenna picture" are encrypted, transmitted, and decrypted. Finally, some security points are discussed, to show that the proposed cryptosystem possesses a key, and the property of diffusion. Future research works will be devoted to a thorough study of the chaotic transmitter.

References

[1] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[2] T. Carroll and L. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuit Syst.*, vol. 38, no. 4, pp. 453–456, 1991.

[3] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos - Part I : fundamentals of digital communications," *IEEE Trans. Circuit Syst. I*, vol. 31, pp. 927–936, 1997,

[4] L. Kocarev, K. Halle, K. Eckert, L. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurc. Chaos*, vol. 2, pp. 709–713, 1992.

[5] K. Cuomo, A. Oppenheim, and S. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuit Syst. II*, vol. 40, no. 10, pp. 626–633, 1993.

[6] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos - Part II : chaotic modulation and chaotic synchronization," *IEEE Trans. Circuit Syst. I*, vol. 31, pp. 1129–1140, 1998.

[7] T. Yang, "A survey of chaotic secure communication systems," *Int. J. of Comput. Cognition*, vol. 2, no. 2, pp. 81–130, 2004.

[8] K.-Y. Lian and P. Liu, "Synchronization with message embedded for generalized lorenz chaotic circuits and its error analysis," *IEEE Trans. Circuit Syst. I*, vol. 47, no. 9, pp. 1418–1425, 2000.

[9] C. Li, X. Liao, and K. Wong, "Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communications," *Physica D*, vol. 194, pp. 187–202, 2004.

[10] H. Dedieu, M. Kennedy, and M. Hasler, "Chaos Shift Keying : Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits," *IEEE Trans. Circuit Syst. I*, vol. 40, no. 10, pp. 634–642, 1993.

[11] K. Halle, C. Wu, M. Itoh, and L. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurc. Chaos*, vol. 3, no. 2, pp. 469–477, 1993.

[12] K. Short, "Steps towards Unmasking Secure Communications," *Int. J. Bifurc. Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[13] T. Yang, L.-B. Yang, and C.-M. Yang, "Breaking chaotic secure communication using a spectrogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998,

[14] T. Yang, C. Wu, and L. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 5, pp. 469–472, 1997,

[15] Z.-P. Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuit Syst. I*, vol. 49, no. 1, pp. 92–96, 2002.

[16] M. Sobhy and A.-E.-D. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurc. Chaos*, vol. 10, no. 12, pp. 2831–2839, 2000.

[17] T. Carroll and L. Pecora, "Cascading synchronized chaotic systems," *Phys. D*, vol. 67, pp. 126–140, 1993.

[18] N. Corron and D. Hahs, "A new approach to communications using chaotic signals," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 5, pp. 373–382, 1997.

[19] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos, Solitons and Fractals*, vol. 19, pp. 919–924, 2004.

[20] S. Tang, H. Chen, S. Hwang, and J. Liu, "Message encoding and decoding through chaos modulation in chaotic optical communications," *IEEE Trans. Circuit Syst. I*, vol. 49, no. 2, pp. 163–169, 2002.

[21] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuit Syst. I*, vol. 46, no. 9, pp. 1144–1150, 1999.

[22] G. Millerioux and J. Daafouz, "Global chaos synchronization and robust filtering in noisy context," *IEEE Trans. Circuit Syst. I*, vol. 48, no. 10, pp. 1170–1176, 2001.

[23] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized state-space observers for chaotic synchronization and secure sommunication," *IEEE Trans. Circuit Syst. I*, vol. 49, no. 3, pp. 345–349, 2002.

[24] Q. Ha and H. Trinh, "State and input simultaneous estimation for a class of nonlinear systems," *Automatica*, vol. 40, pp. 1779–1785, 2004.

[25] S. Čelikovský and G. Chen, "Secure synchronization of a class of chaotic systems from a nonlinear observer approach," *IEEE Trans. Automatic Control*, vol. 50, no. 1, pp. 76–82, 2005.

[26] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking two secure communication systems based on chaotic masking," *IEEE Trans. Circuit Syst. II*, vol. 51, no. 10, pp. 505–506, 2004.

[27] ——, "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," *Chaos*, vol. 14, no. 2, pp. 274–278, 2004.

[28] G. Alvarez and S. Li, "Estimating short-time period to break different types of chaotic modulation based secure communications," 2004, http://arxiv.org/abs/nlin.CD/0406039.

[29] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value," *Chaos, Solitons and Fractals*, vol. 23, no. 5, pp. 1749–1756, 2005.

[30] G. Alvarez and S. Li, "Cryptographic requirements for chaotic secure communications," 2003, http://arxiv.org/abs/nlin.CD/0311039.

[31] X. Wang, G. Chen, and X. Yu, "Anticontrol of chaos in continuous-time systems via time-delay feedback," *Chaos*, vol. 10, no. 4, pp. 771–779, 2000.

[32] X. Wang, G.-Q. Zhong, K.-S. Tang, K. Man, and Z.-F. Liu, "Generating chaos in Chua's circuit via time-delay feedback," *IEEE Trans. Circuit Syst. I*, vol. 48, no. 9, pp. 1151–1156, 2001.

[33] E. Cherrier and M. Boutayeb, "Observer-based approach for synchronization of modified chua's circuit," in *Proceedings of NOLCOS, IFAC Symposium on Nonlinear Control Systems, Stuttgart, Germany*, 2004.

[34] E. Cherrier, M. Boutayeb, and J. Ragot, "Observer-based approach for synchronization of a time-delayed chua's circuit," in *Proceedings of ISCAS, IEEE International Symposium on Circuit and Systems, Kobe, Japan*, 2005.

[35] M. Franz, "Chua's equation with cubic nonlinearity," *Int. J. Bifurc. Chaos*, vol. 6, pp. 2175–2222, 1996.

[36] J. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, vol. 4, pp. 366–393, 1982.

[37] S. Wiggins, *Introduction to applied nonlinear dynamical systems and chaos*. Springer-Verlag, 1990.

[38] O. Morgül and E. Solak, "Observer based synchronization of chaotic systems," *Physical Review E*, vol. 54, no. 5, pp. 4803–4811, 1996.

[39] H. Nijmeijer and I. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 10, pp. 882–890, 1997.

[40] G. Grassi and S. Mascolo, "Nonlinear observer design to synchronize systems via a scalar signal," *IEEE Trans. Circuit Syst. I*, vol. 40, no. 10, pp. 640–656, 1997.
[41] M. Feki, "Observer-based exact synchronization of ideal and mismatched chaotic systems," *Phys. Lett. A*, vol. 309, pp. 53–60, 2003.

Estelle Cherrier was born in 1978. She received the "Diplôme d'Etudes Approfondies" (Masters' Degree) in 2002 with specialization in control from the Institut National Polytechnique de Lorraine (INPL, National Polytechnic Institute of Lorraine) and is currently working toward the Ph.D. degree in control system theory. She is affiliated with the "Centre de Recherche en Automatique de Nancy" (CRAN, Research Center in Automatic Control) and with the "Laboratoire des Sciences de l'Image de l'Informatique et de la Télédétection" (LSIIT, Image Sciences, Computer Sciences and Remote Sensing Laboratory). Her research activities include nonlinear dynamical systems, observers design and the applications in chaos synchronization and secure communications.

Mohamed Boutayeb received the Electrical Engineer degree from the Ecole Hassania des Travaux Publics at Morocco in 1988, the Ph.D. and HDR degrees in Automatic Control from the University Henri Poincaré of Nancy, France, in 1992 and 2000, respectively. He is currently Full Professor at the University Louis Pasteur of Strasbourg, France. His research interests are identification, state estimation and control of dynamical systems.

José Ragot received the "Diplôme d'Ingénieur" (Engineer's Degree) with specialization in control from the Ecole Centrale de Nantes (France) in 1969. Then, he joined the University of Nancy (France) where is received the "Diplôme d'Etudes Approfondies" (Masters' Degree) in 1970. In 1973 he obtained the "Diplôme de Doctorat" (Ph. D. degree) and in 1980 the "Diplôme de Doctorat-es-Science". Since 1985, José Ragot has been a full Professor at the Institut National Polytechnique de Lorraine (INPL, National Polytechnic Institute of Lorraine) and a researcher in the Centre de Recherche en Automatique de Nancy (CRAN). His reseach field of interest includes data validation, process diagnosis, fault detection and isolation, modelisation and identification.