High gain observer based synchronization for a class of time-delay chaotic systems: application to secure communications.

Estelle Cherrier, Mohammed M'Saad

High gain observer based synchronization for a class of time-delay chaotic systems. Application to secure communications.

Estelle Cherrier, Mohammed M'Saad

Abstract—This work investigates high gain observer design to synchronize a time-delay chaotic system. It is shown that the underlying class of nonlinear systems can be put into the canonical observable form, and thus high gain observer design framework can be extended to chaotic synchronization problem. Our approach is motivated by its simplicity of implementation: the observer gain synthesis relies on the explicit resolution of a time-invariant algebraic Lyapunov equation, which leads to a single parameter design. The proposed synchronization scheme is validated in a real-time experimental setup, based on Analog/Digital dSpace electronic device. At the end of the paper an information transmission process is provided, based on the previous synchronization scheme.

Index Terms—Chaos synchronization, high-gain observer, time-delay system

I. INTRODUCTION

If state estimation of linear systems has been widely treated through the last four decades, the nonlinear case, which concerns most of physical processes, remains however an open and very active research field. Among the recent applications of nonlinear state estimation theory, chaotic synchronization represents a pregnant issue, even if the words "chaos" and "synchronization" themselves have seemed incompatible for a long time. Indeed, on the one hand, the word "synchronization" come from the Greek roots $\sigma\upsilon\gamma$ (*syn*), which means "with", and $\chi\rho o\nu o\varsigma$(*chronos*), which means "time". Hence we can give a first definition of synchronization notion: it characterizes two systems having the same behavior at the same time. In fact, synchronization effects have been observed since the XVIIth century, when the Dutch mathematician Huygens noticed the synchronization of two pendulum clocks placed against the same wall. Consequently, synchronization was reserved to periodic systems (two signals were said synchronized if their periods were identical). On the other hand, among nonlinear systems, chaotic systems are characterized by a very complex behavior, asymptotically aperiodic. *A priori*, the nature of chaotic systems would seem to challenge the notion of synchronization. No further attention was paid to this issue, until 1983, and the work of Yamada and Fujisaka [1]. They noticed that, by coupling oscillators which on their own evolved chaotically, it was possible under certain hypotheses to force them to evolve in an identical manner. This happened even if the two

systems did not start with the same initial conditions. Despite this breakthrough, the subject of chaotic synchronization seemed to have no obvious applications until 1990. In their pioneering paper [2], Pecora and Carroll gave necessary and sufficient conditions under which two chaotic systems would synchronize. They also indicated that by using chaotic synchronization it might be possible to communicate in a secure way, by using the chaotic signal as a mask, used to hide the information-bearing message. This promising application gave rise to a huge number of papers concerned with chaotic synchronization. For general surveys on this subject, the reader is referred to the references [3], [4], [5]. Then synchronization has become a state estimation issue. The papers [6], [7] have shown that it is possible to estimate chaotic systems states, using nonlinear control theory. Indeed, the chaotic transmitter belongs to the wide class of nonlinear dynamical systems, whereas the receiver can be viewed as a nonlinear observer of the transmitter system. Furthermore, nonlinear estimation theory can be used to design a receiver which synchronizes with the driving system. This nonlinear control point of view brings many approaches to the receiver conception problem, and the underlying synchronization analysis problem. Among the huge amount of references on this subject, we can quote [8], which builds an observer-based synchronization scheme, guaranteeing an exponential synchronization. A generalization to a larger class of nonlinearities is proposed in [9]. [10] details a particular observer design, whose gain can be expressed in function of the desired convergence speed. But other approaches can also be found in the tremendous literature. For instance, the synchronization problem is addressed as a chaos suppression issue in [11]. [12] has established a synchronization criterion based on a linear feedback control, applied to Chua's circuit. [13] deals with a reduced-order observer-based exponential synchronization scheme, while [14] considers synchronization as a control problem. A comparison between different synchronization schemes, applied to well-known chaotic systems is performed in [15]. Sliding mode observers theory and an integral observer are used for synchronization purposes, respectively in [16] and [17]. [18] deals with synchronization of a class of time-delay chaotic systems, and proposes a phase-modulation based transmission scheme. More recently, a new family of chaotic systems has been exhibited, relying on the multimodel framework, and a dedicated synchronization process is detailed in [19]. Some adaptive unknown input observer have been proposed, for

The authors are with GREYC UMR 6072 CNRS, Boulevard du Maréchal Juin, 14050 Caen France.
E-mail: estelle.cherrier@greyc.ensicaen.fr

example in [20] or [21]. The former develops an adaptive unknown input observer for a chaotic transmitter whose linear part is affected by a time-delay, while the latter is also concerned with a robust approach to cope with parametric uncertainties and external disturbances. A new transmitter is dealt with in [22], called unified chaotic system: when a parameter is varied, the chaotic attractor is topologically equivalent to a Lorenz attractor, or a Chen or a Lü one. Most of the mentioned papers address a chaotic synchronization problem and propose an application to secure transmissions, but rarely with a security analysis or a precise exhibition of what the secret key is. This point will be discussed at the end of our paper.

In many papers that can be read in the literature, as in several aforementioned papers, the observer gain design relies on the resolution of a Linear Matricial Inequality (LMI), thanks to numerical convex optimization algorithms, provided that conservative assumptions are fulfilled. What we propose in this paper is a chaotic synchronization scheme using high-gain observer framework, extending our recent results detailed in [23]. In this latter paper, a high gain observer was proposed in the presence of one (or more) variable and known delay. The exponential convergence of the observer relies on the resulting solution of an algebraic Lyapunov equation and leads to an explicit expression of the observer gain.

The layout of this paper is as follows. Section II presents high gain observer design for a class of nonlinear time-delay chaotic systems with a synchronization purpose. The obtained results are applied in section III to information transmission, and tested both in simulation and through real-time experimental setup, based on Analog/Digital dSpace electronic device.

Notations: throughout this paper, $x_\tau(t)$ stands for $x(t - \tau)$.

II. HIGH-GAIN OBSERVER BASED SYNCHRONIZATION

This section presents a new observer based synchronization scheme, relying on high gain design framework, for a class of nonlinear time-delay systems.

A. Time-delay chaotic transmitter

It is claimed in some papers dealing with cryptanalysis (see [24] for example) that hyperchaotic systems are well suited for security purpose when used in synchronization and communication schemes. Besides, the presence of a delay in the dynamics of a nonlinear systems leads to an hyperchaotic behavior, this has been detailed in ref. [25]. Therefore we consider the following class of time-delay chaotic systems:

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

with

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

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

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

Fig. 1 shows the bifurcation diagram of system (1) when the parameter σ is varied. The reader is referred to ref. [18] for a thorough study of this chaotic transmitter. Once the transmitter
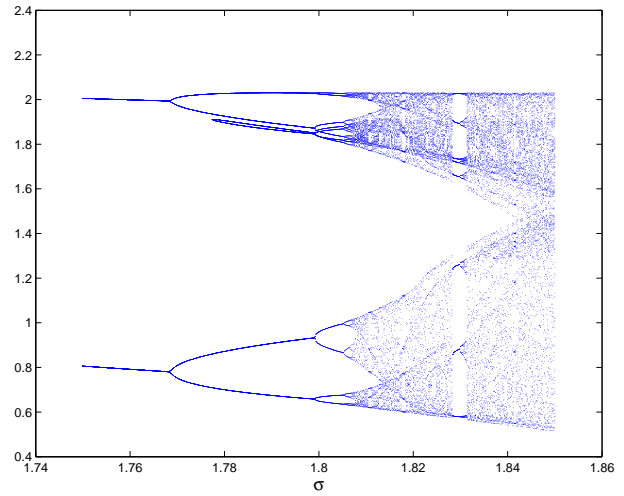

Fig. 1. Bifurcation diagram

has been chosen, we address in next subsection the dedicated receiver design, using high gain observer framework.

B. High gain observer synthesis

Since the pioneering paper of Gauthier *et al.* [26], which presents a high gain observer for a class of nonlinear systems called uniformly observable for all inputs, the general high gain framework has been extended to larger classes of nonlinear systems [27] (MIMO systems), [23] (time-delay systems), as well as larger problems (including state estimation), such as adaptive observers [28], to mention just a few.

We present in this paper an extension of the results established in reference [23] about high gain observer design in the presence of one (or more) variable and known delay. This class of high gain observers has, to the authors knowledge, not yet been applied to time-delay chaotic synchronization. The advantage of this approach principally remains in its simplicity of implementation, in the sense that the observer gain is obtained from the resolution of an algebraic Lyapunov equation, and can be given explicitly.

The main results of reference [23] are now briefly summed up.

Consider the following class of nonlinear systems [23]:

$$\begin{cases} \dot{x}(t) = Ax(t) + g(u(t), u_\tau(t), x(t), x_\tau(t)) \\ y(t) = Cx(t) \end{cases} \tag{5}$$

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}$, $u \in \mathbb{R}^m$, are respectively the state, the (scalar) output and the input of system (5).

A is the *anti-shift* matrix:

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix} \quad (6)$$

and the matrix C is defined by:

$$C = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} \quad (7)$$

The components of the nonlinear function $g : \mathbb{R}^{m+2n} \to \mathbb{R}^n$ are noted g_i, $i = 1, n$ and each one of them has a triangular structure w.r.t. x and x_τ, *i.e.* :

$$g_i(u, u_\tau, x, x_\tau) = g_i(u, u_\tau, x_1, \dots, x_i, x_{\tau,1}, \dots, x_{\tau,i}) \quad (8)$$

We introduce two matrices Δ_θ and S, which belong to the general high gain framework, as follows :

$$\Delta_\theta = diag \begin{bmatrix} 1 & \dfrac{1}{\theta} & \dots & \dfrac{1}{\theta^{n-1}} \end{bmatrix} \quad (9)$$

where θ is a strictly positive real number ;
S is the unique solution of the algebraic Lyapunov equation below:

$$S + A^T S + SA - C^T C = 0 \quad (10)$$

As in most of works dealing with high gain synthesis, we make the following assumption (*cf.* [27]) :

- (H1) The function g is global Lipschitz w.r.t. x and x_τ, uniformly in u.

Consider the following candidate observer:

$$\begin{cases} \dot{\hat{x}}(t) &= A\hat{x}(t) + g(u(t), u_\tau(t), \hat{x}(t), \hat{x}_\tau(t)) \\ & \quad -\theta \Delta^{-1} S^{-1} C^T C(\hat{x}(t) - x(t)) \end{cases} \quad (11)$$

We give the main theorem of ref. [23] ensuring the convergence of observer (11):
Theorem 1:
Under hypothesis (H1), there exists $\theta_0 > 0$ such that for all $\theta > \theta_0$, system (11) is an exponential observer for system (5).

Now we will show how the chaotic transmitter (1) can be put into the canonical form (5)-(9) by an appropriate coordinate change:

$$\begin{cases} \dot{z}(t) = Az(t) + g(u(t), u_\tau(t), z(t), z_\tau(t)) \\ y(t) = Cz(t) \end{cases} \quad (12)$$

with A and C respectively defined by (6) and (7), and g of the form (8).
The appropriate coordinate change is given by [26]:

$$z(t) = \phi(x(t)) = \begin{pmatrix} x_1(t) \\ L_g x_1(t) \\ L_g^2 x_1(t) \end{pmatrix} \quad (13)$$

where $L_g f$ stands for the Lie derivative operator. If we note ϕ_i, $i = 1, 3$ the three components of ϕ, we obtain:

$$\begin{aligned} \phi_1(x(t)) &= x_1(t) \\ \phi_2(x(t)) &= -\alpha x_1(t) + \alpha x_2(t) - \alpha \delta \tanh(x_1(t) \\ \phi_3(x(t)) &= \alpha(\alpha+1)x_1(t) + \alpha^2 \delta(1+\delta)\tanh(x_1(t)) \\ & \quad + \alpha^2 \delta \tanh(x_1(t))^2(-x_1(t) + x_2(t)) \\ & \quad - \alpha^2 \delta^2 \tanh(x_1(t))^3 \\ & \quad - \alpha(\alpha + 1 + \alpha\delta)x_2(t) + \alpha x_3(t) \end{aligned}$$

$$(14)$$

Then following the results of [23], one can explicitly compute the observer gain for the canonical system (12):

$$K_z = \theta \Delta_\theta S^{-1} C^T$$

Once this is achieved, one has to find the expression of the observer gain in the original coordinates, which can be expressed as:

$$K = \left(\frac{\partial \phi}{\partial x}\right)^{-1} K_z$$

where $\left(\dfrac{\partial \phi}{\partial x}\right)$ stands for the Jacobian matrix of function ϕ.
It has been shown in [27] that only the diagonal terms of this Jacobian matrix are necessary, the other terms being controlled. It is also worth noticing the property below [26]:

$$S^{-1} C^T = \begin{pmatrix} C_n^1 & C_n^2 & \dots & C_n^n \end{pmatrix}$$

where $C_n^p = \dfrac{n!}{p!(n-p)!}$.

To conclude this section, we have proposed a new synchronization scheme, based on high gain observer framework, which has been recalled, for a time-delay chaotic transmitter.

III. REAL-TIME APPLICATION AND SECURE TRANSMISSION

The aim of this section is twofold. First we illustrate the effectiveness of the proposed synchronization scheme in simulations using Matlab, then in real-time experimental setup, based on Analog/Digital dSpace electronic device. Finally this synchronization process will be included in a complete communication system.

A. Real-time synchronization

We recall the model of the chosen transmitter, and the numerical values of its parameters:

$$\begin{cases} \dot{x}_1(t) &= -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) &= x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &= -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)) \end{cases} \quad (15)$$

with

α	β	γ	δ	ε	σ	τ
9	14	5	-1	10	10^2	0.1

TABLE I
PARAMETERS OF SYSTEM (15)

For the simulation, we choose a fourth-order Runge-Kutta integration solver, with a constant step fixed to 1 ms.

The following initial conditions have been fixed for the transmitter and the receiver:

$$\begin{cases} x(t) = \hat{x}(t) = (0\ 0\ 0)^T \text{for } t \in [-\tau, 0[\\ x(0) = (0.1\ 0.1\ 0.1)^T \\ \hat{x}(0) = (-0.1\ -0.1\ -0.1)^T \end{cases} \qquad (16)$$

The value of the tuning parameter θ has been set to 10.

A comparison between the transmitter states and the receiver state is depicted in figure 2 and shows that identical synchronization is achieved after a few seconds. This synchronization time can be shortened by using larger values for θ. However this tuning must be made carefully, since the larger θ is, the less robust (to additive noise on the transmitted signal $y(t)$) the observer is.
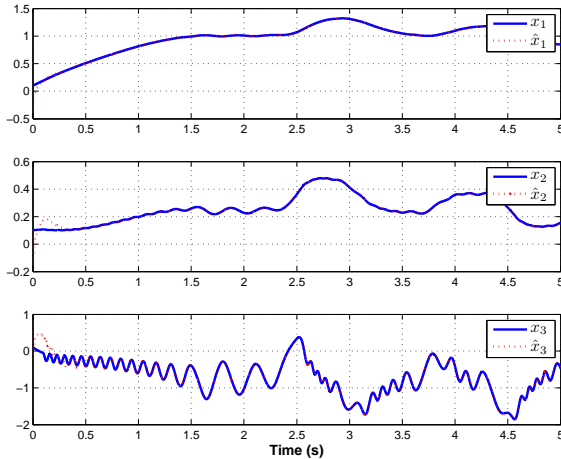
Fig. 3.   Real-time synchronization

Fig. 2.   Synchronization of the transmitter states and the receiver states

Now experimental results are performed on two calculators (Transmitter / Receiver) communicating through Analog/Digital dSpace electronic devices. At the first calculator, the Matlab-Simulink software simulates the chaotic model and transmits the output signal $y(t)$ through the dspace card (using a coaxial cable) to the receiver. At the receiver, the second calculator uses the proposed high gain observer based approach for synchronization. Fig. 3 shows the experimental results. It can be noticed that experimenting real transmission conditions inevitably lead to some degradations of the performances: while the first state x_1 seems exactly recovered, some unaccuracies appear during the synchronization of the second and the third states. These problems have been taken into account and are under study.

B. Application to information transmission

One proposes to integrate the previous high gain observer based synchronization scheme into a complete communication process. The information transmission is performed using the two-channel principle, as in [18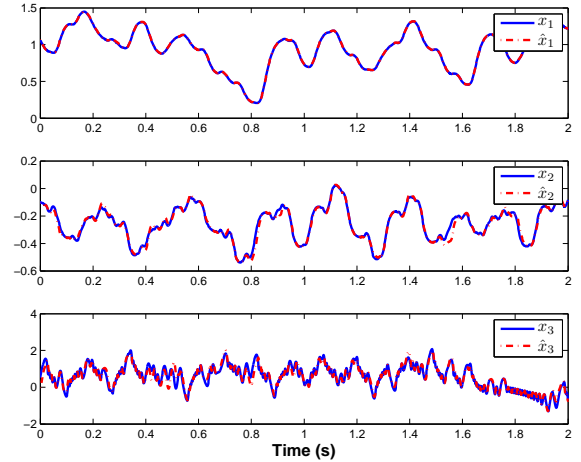]: a first signal (corresponding to $y(t)$ defined in (5)) is sent to the receiver, for synchronization purpose only. No information about the message is contained in this signal. Then, once synchronization is achieved at the receiver end, a second signal $y_2(t)$ containing the information (corresponding to an encryption of the message) is sent. To be able to decrypt the information, the receiver must possess the secret key, given by the transmitter. This point has been discussed in [18], where it has been shown that the parameter σ of the transmitter (5) can play the role of the secret key. In this case, we are dealing with a symmetric cryptosystem, since the same key is used to encrypt and decrypt the information. For lack of place, the security of the proposed communication scheme will not be longer discussed here, it would deserve an entire paper.

We give now the expression of the second signal $y_2(t)$ which is used to conceal the information, noted $u(t)$:

$$y_2(t) = x_3(t - T_u u(t)) \qquad (17)$$

where we suppose without restriction that $u(t) \in [0, 1]$ and T_u is chosen equal to the fixed integration step.

Then the decryption formula is given by (see [18] for a detailed proof):

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \qquad (18)$$

where $\hat{u}(t)$ stands for the deciphered message.

Fig. 4 shows the effectiveness of the proposed cryptosystem when the following message is chosen: $u(t) = 0.5(1 + \sin(2\pi f_o t))$ with $f_o = 0.2$Hz.

Since the obtained results within the experimental setup were not totally satisfying, we decide not to make a real-time transmission trial. We prefer to perform a deeper study of high gain observer based synchronization. This paper is the first step in our approach.

IV. CONCLUSION

In this paper we addressed a chaotic synchronization problem. We propose a specific solution for a class of time-delay
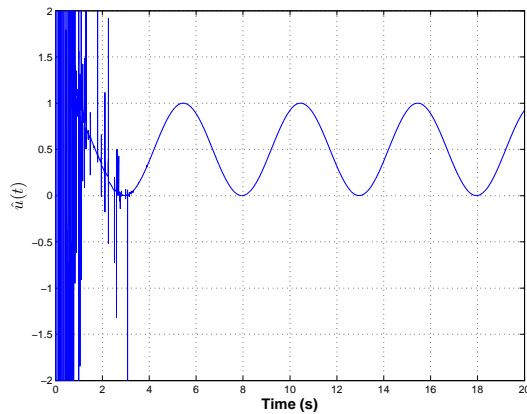
Fig. 4. Decrypted message $u(t) = 0.5(1 + \sin(2\pi f_o t))$

hyperchaotic transmitters, by designing a high-gain observer as a receiver. We first showed that the considered transmitter belongs to the class of uniformly observable nonlinear systems which is dealt with in the high gain framework. Then we detailed the conception of the receiver, whose efficiency has been tested not only in simulation using Matlab, but also in real-time experiment, using dSpace Analog/Digital device. At the end of the paper, the proposed synchronization scheme has been used to design a two-channel communication scheme based on chaotic phase modulation. This paper represents a first step in using high gain techniques for chaotic synchronization purpose. Further real-time experimentations of chaotic cryptosystems are under study.

REFERENCES

[1] T. Yamada and H. Fujisaka, "Stability theory of synchronized motion in coupled-oscillator systems," *Prog. Theor. Phys.*, vol. 69, no. 1, pp. 32–47, 1983.
[2] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.
[3] L. Pecora, T. Carroll, G. Johnson, and D. Mar, "Fundamentals of synchronization in chaotic systems, concepts and applications," *Chaos*, vol. 7, no. 4, pp. 520–543, 1997.
[4] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Physics Reports*, vol. 366, pp. 1–101, 2002.
[5] M. Aziz-Alaoui, "Synchronization of chaos," *Encyclopedia of Mathematical Physics*, vol. 5, pp. 213–226, 2006.
[6] O. Morgül and E. Solak, "Observer based synchronization of chaotic systems," *Physical Review E*, vol. 54, no. 5, pp. 4803–4811, 1996.
[7] H. Nijmeijer and I. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 10, pp. 882–890, 1997.
[8] 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.
[9] 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.
[10] J. Alvarez-Ramirez, H. Puebla, and I. Cervantes, "Convergence rate of observer-based approach for chaotic synchronization," *Phys. Lett. A*, vol. 289, pp. 193–198, 2001.
[11] R. Femat, R.Jauregui-Ortiz, and G. Solís-Perales, "A chaos-based communication scheme via robust asymptotic feedback," *IEEE Trans. Circuit Syst. I*, vol. 48, no. 10, pp. 1161–1169, 2001.
[12] G.-P. Jiang and W. Zheng, "An LMI criterion for linear-state-feeback based chaos synchronization of a class of chaotic systems," *Chaos, Solitons and Fractals*, vol. 26, pp. 437–443, 2005.
[13] M. Feki, "Observer-based chaotic synchronization in the presence of unknown inputs," *Chaos, Solitons and Fractals*, vol. 15, pp. 831–840, 2003.
[14] 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.
[15] M. Haeri and B. Khademian, "Comparison between different synchronization methods of identical chaotic systems," *Chaos, Solitons and Fractals*, vol. 29, no. 4, pp. 1002–1022, 2006.
[16] M. Chen, D. Zhou, and Y. Shang, "A new observer-based synchronization scheme for private communication," *Chaos, Solitons and Fractals*, vol. 24, pp. 1025–1030, 2005.
[17] G. Jiang, W. Zheng, W. Tang, and G. Chen, "Integral-observer-based chaos synchronization," *IEEE Trans. Circuit Syst. II*, vol. 53, no. 2, pp. 110–114, 2006.
[18] E. Cherrier, M. Boutayeb, and J. Ragot, "Observers based synchronization and input recovery for a class of nonlinear systems," *IEEE Trans. Circuit Syst. I*, vol. 53, no. 9, 2006.
[19] E. Cherrier, M. Boutayeb, J. Ragot, and M. Aziz-Alaoui, "Observer-based exponential synchronization of chaotic multimodels," in *Proceedings of the European Control Conference, Kos, Greece*, 2007.
[20] D. Li, Z. Wang, J. Zhou, J. Fang, and J. Ni, "A note on chaotic synchronization of time-delay secure communication systems," *Chaos, Solitons and Fractals*, vol. 38, no. 4, pp. 1217 – 1224, 2008.
[21] S. Bowong and J. Tewa, "Unknown inputs' adaptive observer for a class of chaotic systems with uncertainties," *Mathematical and Computer Modelling*, vol. 48, no. 11-12, pp. 1826 – 1839, 2008.
[22] J. Grzybowski, M. Rafikov, and J. Balthazar, "Synchronization of the unified chaotic system and application in secure communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 6, pp. 2793 – 2806, 2009.
[23] E. Cherrier, A. Sboui, M. Farza, and M. M'Saad, "Observateurs grand gain pour une classe de systmes non linaires retard," in *Proceedings of the IEEE Conférence Internationale Francophone d'Automatique, Bucarest, Roumania*, 2008.
[24] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[25] J. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, vol. 4, pp. 366–393, 1982.
[26] J. Gauthier, H. Hammouri, and S. Othman, "A simple obsever for nonlinear systems: Application to bioreactors," vol. 37, no. 6, pp. 875–880, 1992.
[27] M. Farza, M. M'Saad, and L. Rossignol, "Observer design for a class of MIMO nonlinear systems," *Automatica*, vol. 40, pp. 135–143, 2004.
[28] M. Farza, M. M'Saad, T. Maatoug, and M. Kammoun, "A set of adaptive observers for a class of mimo nonlinear systems," in *Proceedings of the Joint 44th IEEE Conference on Decision and Control and European Control Conference, Seville, Spain*, 2005.