Observer-based synchronization of multimodels with application to communication systems

Estelle Cherrier*,†, Mohamed Boutayeb†, and José Ragot*
*CRAN UMR CNRS 7039
INPL 2 Avenue de la Forêt de Haye 54516 Vandoeuvre-lès-Nancy Cedex, France
Email : cherrier@eavr.u-strasbg.fr, Jose.Ragot@ensem.inpl-nancy.fr
†LSIIT UMR CNRS 7005
ULP, Pôle API Bd S. Brandt - BP 10413 67412 Illkirch, France
Email : mohamed.boutayeb@ipst-ulp.u-strasbg.fr

***Abstract*— This paper deals with the design of observers for a class of nonlinear systems. Nonlinear multimodels are designed from two (or more) chaotic systems, and an observer-based synchronization scheme is designed. Sufficient conditions of synchronization are established and expressed in terms of Linear Matrix Inequalities (LMIs). This synchronization process is integrated into a complete communication scheme. An illustration of the efficiency of the proposed method is done through the encryption/decryption of a picture.**

I. Introduction

The use of chaos in the field of synchronization and, more generally, in the field of secure communications, is quite recent. For a long time, researches about chaotic phenomena have been strongly related to the studies on nonlinear dynamic systems. Among the scientists who dedicated an important part of their work to chaos, we can cite Poincaré, Van der Pol, Lorenz, Rössler ... They have discovered a large variety of chaotic behaviors (they have left their names to some famous attractors), and some properties characterizing these systems [1], among which: they exhibit a great sensibility to the initial conditions (well-known as the *butterfly effect*), there exist UPOs (Unstable Periodic Orbits) dense in the attractor, they are deterministic systems. Before 1990, the extreme sensibility of chaotic systems to their initial conditions remained a major drawback. But the pioneering work of Pecora and Carroll [2] has opened the researches on chaotic synchronization, and their applications into the field of secure communications. They have shown that two identical chaotic systems are able to synchronize, provided that they are coupled according to the *drive-response principle*, even if the receiver has no information about the initial conditions of the transmitter. More recently, [3] and [4] related the phenomenon of synchronization to a standard (non)linear state estimation problem, so observer-based techniques are generally used to design synchronization schemes [5], [6], [7], [8] ... to mention just a few. Detailed descriptions of the existing methods are surveyed in [9].

In this paper, we propose an observer-based synchronization scheme for a class of nonlinear systems, for communications purposes. The transmitter is designed as a nonlinear multimodel made up of chaotic systems, and we develop a systematic method to design observers for this class of systems, through the resolution of Linear Matrix Inequalities (LMIs).

The theory of multimodels is quite recent. [10] contains an overview on this topic, and some stability problems are discussed in [11], [12]. Multimodels are related to nonlinear systems, whose behavior is represented by a set of local linear models. Then the multimodel describes an approximation of the initial process, and is obtained as a weighted sum of all the local models:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) \left(A_i x(t)\right) \\ y(t) = Cx(t) \end{cases} \tag{1}$$

with

$$\begin{cases} \sum_{i=1}^{p} \mu_i(\xi) = 1 \\ 0 \leq \mu_i(\xi) \leq 1 \ \forall i = 1, p \end{cases} \tag{2}$$

where $x \in \mathbb{R}^n$ is the state vector, and $y \in \mathbb{R}^m$ represents the measured outputs, the matrices A_i, $i = 1, p$ and C being of convenient dimensions.
μ is an interpolation function, in the sense that, at each moment, its value determines how each local is model acts in the dynamics of the global multimodel. Indeed, if $\mu_i(\xi) = 1$, for $i \in \{1, \dots p\}$, according to (1) and (2), only the i^{th} model is active, whereas if $0 < \mu_i(\xi) < 1$, then there exists $j \in \{1, \dots p\}, j \neq i$ such that $\mu_j(\xi) > 0$, so at least two local models are active.
The variable ξ generally depends on the state x, or the measures y.

Here we do not have a classical point of view on multimodels: using the same process of weighted sum, a nonlinear multimodel is created from p chaotic systems:

$$\begin{cases} \dot{x} = \sum_{i=1}^{p} \mu_i(y) \left(A_i x + f_i(x)\right) \\ y = Cx \end{cases} \tag{3}$$

The functions $f_i : \mathbb{R}^n \to \mathbb{R}^n$ are nonlinear functions chosen to ensure that each local model: $\dot{x} = A_i x + f_i(x)$, for $i = 1, p$ exhibits a chaotic behavior. Generally, these functions are characterized by the Lipschitz property, which will be specified later.

The function $\mu(.)$ enables a kind of mixing between the dynamics of the p local chaotic systems, which may protect the synchronization process from an attack based on the delay-reconstruction techniques [13]. Indeed, the signal $y(t)$

transmitted to the receiver is a variable (in time) interpolation of each local model, and does not correspond to an entire time series of a particular chaotic attractor.

This paper presents an observer-based synchronization scheme for the class of systems (3). The layout is as follows. Using the Lyapunov theory, a sufficient condition to guarantee synchronization is derived under a LMI form in section II, first in the case of a multimodel based on two systems, and then the obtained results are extended to a more general case. The efficiency of the proposed approach is tested on a multimodel based on two Chua's circuits in section III. Then section IV illustrates how this synchronization scheme can be applied to secure communications, through the encryption/decryption of a picture.

II. Synchronization of multimodels

This section first details the definition of the multimodel based on two chaotic systems, and the design of an observer for this multimodel. Then a sufficient condition for the synchronization of the observer is established in a systematic procedure, through the resolution of a LMI. This scheme is finally extended to the general case, for a multimodel based on p chaotic systems, $p > 0$.

A. Multimodel based on two systems

Consider two chaotic systems, whose dynamic models are respectively given by:

$$\dot{x} = A_1 x + f_1(x) \tag{4}$$

and:

$$\dot{x} = A_2 x + f_2(x) \tag{5}$$

We define then the following system, as a multimodel based on (4) and (5):

$$\left\{ \begin{array}{rcl} \dot{x} & = & \mu(y)(A_1 x + f_1(x)) \\ & & +(1-\mu(y))(A_2 x + f_2(x)) \\ y & = & Cx \in \mathbb{R} \end{array} \right. \tag{6}$$

The function μ must verify (2). We have chosen $\xi(t) = y(t)$ in (2), since y is the only available signal at the receiver.

We intend to establish the conditions guaranteeing the observer-based synchronization of the multimodel. The observer designed to ensure synchronization with (6) is given by:

$$\begin{array}{rl} \dot{\hat{x}} = & \mu(y)\left(A_1\hat{x} + f_1(\hat{x}) - K_1(y - C\hat{x})\right) \\ & +(1-\mu(y))\left(A_2\hat{x} + f_2(\hat{x}) - K_2(y - C\hat{x})\right) \end{array} \tag{7}$$

The synchronization error vector is defined by $e = x - \hat{x}$, so by derivation it comes:

$$\begin{array}{rl} \dot{e} = & \mu(y)\left((A_1 - K_1C)e + f_1(x) - f_1(\hat{x})\right) \\ & +(1-\mu(y))\left((A_2 - K_2C)e + f_2(x) - f_2(\hat{x})\right) \end{array} \tag{8}$$

To simplify the notations, we set:

$$\mathcal{M} = \mu(y)(A_1 - K_1C) + (1-\mu(y))(A_2 - K_2C) \tag{9}$$

and

$$\tilde{f}_i = f_i(x) - f_i(\hat{x}),\ i = 1, 2 \tag{10}$$

The following theorem provides a sufficient condition for the synchronization of the observer (7) with the multimodel (6):

Theorem 1: :
If the following conditions are verified

1) The functions f_1 et f_2 verify the Lipschitz property, with respective constants k_1 and k_2 :

$$\|f_i(x) - f_i(y)\| \leq k_i\|x - y\|,\ \forall x, y, \quad i = 1, 2 \tag{11}$$

2) There exist a symmetric, positive-definite matrix P and two matrices K_1, K_2 solution of the following LMIs (for $i = 1, 2$):

$$\left(\begin{array}{cc} (A_i - K_iC)^T P + P(A_i - K_iC) + k_i I & P \\ P & -\frac{1}{k_i} I \end{array} \right) < 0 \tag{12}$$

then (7) is an observer for (6): $\hat{x}(t) \to x(t)$ when $t \to \infty$.

Proof: To guarantee that the synchronization error vector e converges towards 0, we introduce the following Lyapunov function:

$$V(t) = e^T(t)Pe(t) \tag{13}$$

where P is a symmetric, positive-definite matrix.
The synchronization error converge asymptotically towards zero if:

- $V(t) > 0$
- $\dot{V}(t) < 0$

for all $e(t) \neq 0$.
Since $P > 0$, the first condition is easily satisfied.
Equations (8), (9), (10) yield to:

$$\dot{V} = \quad e^T\left(\mathcal{M}^T P + P\mathcal{M}\right)e + 2e^T P\left(\mu\tilde{f}_1 + (1-\mu)\tilde{f}_2\right) \tag{14}$$

By applying successively the Cauchy-Schwarz and the Young inequalities, we obtain:

$$2\mu(y)e^T P\tilde{f}_1 \leq \mu(y)(k_1 e^T PPe + k_1 e^T e) \tag{15}$$

and

$$2(1-\mu(y))e^T P\tilde{f}_2 \leq (1-\mu(y))(k_2 e^T PPe + k_2 e^T e) \tag{16}$$

which leads to:

$$\begin{array}{rcl} \dot{V} & \leq & e^T\left(\mathcal{M}^T P + P\mathcal{M} + (\mu(y)k_1 + (1-\mu(y))k_2)P^2\right. \\ & & \left.+(\mu(y)k_1 + (1-\mu(y))k_2)I\right)e \end{array} \tag{17}$$

Consequently, using (9), if the Riccati-like equations are checked:

$$\begin{array}{r} (A_i - K_iC)^T P + P(A_i - K_iC) + k_i P^2 + k_i I < 0, \\ i = 1, 2 \end{array} \tag{18}$$

by using (2) and (9), it yields

$$\dot{V} \leq 0 \tag{19}$$

and $\dot{V}(t) < 0$ if $e(t) \neq 0$.
By making use of the Schur complement, (18) can be rewritten in a LMI form, and we get (12), which completes the proof: the synchronization error vector e converges towards 0, and the observer (7) is asymptotically convergent. ■

Remark 2: The LMIs (12) for $i = 1, 2$ can be solved numerically. If we note $L_i = PK_i$ (which is equivalent to $K_i = P^{-1}L_i$ since P is invertible), we obtain:

$$\begin{array}{l}(A_i - K_iC)^T P + P(A_i - K_iC) + k_iI \\ = A_i^T P + PA_i - C^T L_i^T - L_iC + k_iI\end{array} \quad (20)$$

The right-hand side of this equality is linear in P and L_i, thus the LMIs (12) for $i = 1, 2$ can easily be solved by a standard convex optimization algorithm.

B. Extension to the general case

The previous results can be generalized to the case of a multimodel based on $p > 0$ chaotic systems, defined in the following manner:

$$\left\{\begin{array}{l}\dot{x} = \sum_{i=1}^{p} \mu_i(y)(A_ix + f_i(x)) \\ y = Cx\end{array}\right. \quad (21)$$

with

$$\sum_{i=1}^{p} \mu_i(y) = 1, \ 0 \leq \mu_i \leq 1 \quad (22)$$

Then the observer of (21) is designed similarly to (7):

$$\dot{\hat{x}} = \sum_{i=1}^{p} \mu_i(y)(A_i\hat{x} + f_i(\hat{x}) - K_i(y - C\hat{x})) \quad (23)$$

The Theorem 1 can be generalized:

Theorem 3: : If the following conditions are fulfilled

1) The functions $f_i(.)$, $i = 1, p$ verify the Lipschitz property (11), with respective constants k_i;
2) There exist a symmetric, positive-definite matrix P and p matrices K_i, $i = 1, p$ which verify the p LMIs:

$$\left(\begin{array}{cc}(A_i - K_iC)^T P + P(A_i - K_iC) + k_iI & P \\ P & -\frac{1}{k_i}I\end{array}\right) < 0 \quad (24)$$

for $i = 1, p$.

then (23) is an observer for (21): $\hat{x}(t) \to x(t)$ when $t \to \infty$.

Proof: The demonstration is analogous to that of Theorem 1. With the notation

$$\mathcal{M} = \sum_{i=1}^{p} \mu_i(y)(A_i - K_iC) \quad (25)$$

the following Riccati-like equation has to be solved, generalizing (18):

$$\mathcal{M}^T P + P\mathcal{M} + \sum_{i=1}^{p} \mu_i(y)k_iP^2 + \sum_{i=1}^{p} \mu_i(y)k_iI < 0 \quad (26)$$

■

III. Application to Chua's circuits

The synchronization scheme proposed in the previous section will be tested on a multimodel based on two different Chua's circuits. Indeed, Chua's circuit is well known to exhibit a large variety of chaotic behaviors, and consequently it gives rise to a large variety of chaotic attractors (see [14] for a detailed description).

A. Description of the multimodel

The general dimensionless dynamic model of Chua's circuit is of the form:

$$\left\{\begin{array}{rcl}\dot{x_1} &=& -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} &=& x_1 - x_2 + x_3 \\ \dot{x_3} &=& -\beta x_2 - \gamma x_3\end{array}\right. \quad (27)$$

where the nonlinearity $f(.)$ is given by:

$$f(x_1) = bx_1 + \frac{1}{2}(a - b)(|x_1 + 1| - |x_1 - 1|) \quad (28)$$

So the nonlinear part of Chua's circuit verifies the Lipschitz property, with a constant equal to $\max(|a|, |b|)$.

We have chosen two sets of parameters corresponding to two different chaotic behaviors of (27). The set 1:

$$\begin{array}{l}\alpha_1 = 9, \ \beta_1 = 14, \ \gamma_1 = 0, \ a_1 = -1.14, \\ b_1 = -0.7\end{array} \quad (29)$$

and the set 2:

$$\begin{array}{l}\alpha_2 = 9.5, \ \beta_2 = 15, \ \gamma_2 = 0, \ a_2 = -1.1, \\ b_2 = -0.7\end{array} \quad (30)$$

The attractors corresponding to set 1 and set 2 are quite different, as shown respectively in Fig. 1 and Fig. 2. Now we

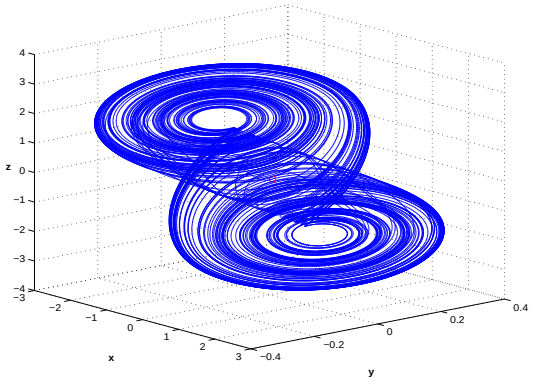

Fig. 1. Chua's circuit 1

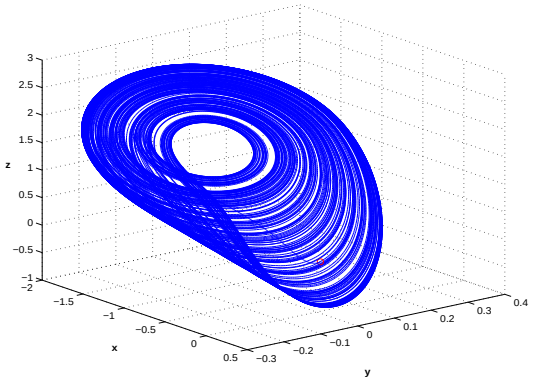

Fig. 2. Chua's circuit 2

build the multimodel (6) from these systems. The function $\mu(.)$ is chosen of the form:

$$\mu(y) = \frac{1 + tanh(\sigma y)}{2} \quad (31)$$

where the parameter σ ensures that $\mu(.)$ enables real transitions between both Chua's circuits, and not only switchings between them. The proofs of Theorem 1 and Theorem 3 are independent of the choice of the function $\mu(.)$, it only matters that conditions (2) are checked.

Remark 4: To reduce the Lipschitz constant of (27), we choose the following matrix in the multimodel:

$$C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \tag{32}$$

with ζ quite small (for example, here we take $\zeta = 0.1$), since the Lipschitz property (11) becomes:

$$\begin{aligned} \|f(x_1) - f(\hat{x_1})\| &= \|f(y - \zeta x_2) - f(y - \zeta \hat{x}_2)\| \\ &\leq k|\zeta|\|x_2 - \hat{x}_2\| \end{aligned} \tag{33}$$

The presence of the parameter ζ in the matrix C changes the value of the Lipschitz constant of $f(.)$: k is multiplied by ζ, with $0 < \zeta < 1$. Here we choose $\zeta = 0.1$, so the Lipschitz constants corresponding to (29) and (30) are respectively $k_1 = 0.114$ and $k_2 = 0.11$.

The simulation of the resulting multimodel leads to the attractor shown in Fig. 3.

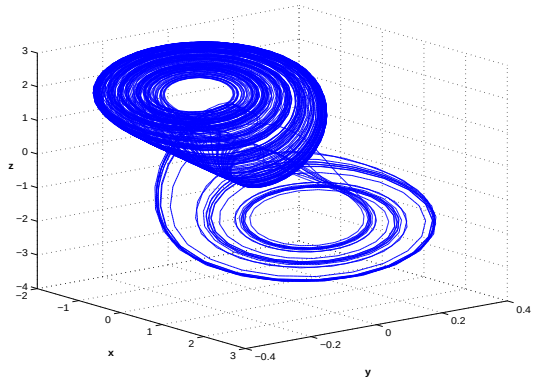

Fig. 3. Multimodel based on two Chua's circuits

B. Experimental simulations

We illustrate the efficiency of the proposed synchronization scheme.

The LMI-based procedure to design the observer gives the following gains:

$$K_1 = \begin{pmatrix} 7.51567564153629 \\ 49.46538889431523 \\ 92.00114168207854 \end{pmatrix} \tag{34}$$

$$K_2 = \begin{pmatrix} 7.78184598227631 \\ 52.22562659668749 \\ 97.38268818155270 \end{pmatrix} \tag{35}$$

and the matrix P is given in (36). The initial conditions chosen for the multimodel are

$$\begin{pmatrix} 0.1 & 0.1 & 0.1 \end{pmatrix}^T \tag{37}$$

and for the observer

$$\begin{pmatrix} 0 & 0.01 & -0.1 \end{pmatrix}^T \tag{38}$$

The function $\mu(y(t))$ is plotted on Fig. 4, where we have chosen $\sigma = 0.5$ in (31). Fig. 5 is a zoom in Fig. 4 and shows that the multimodel based on two Chua's circuits is a real mix between both systems.

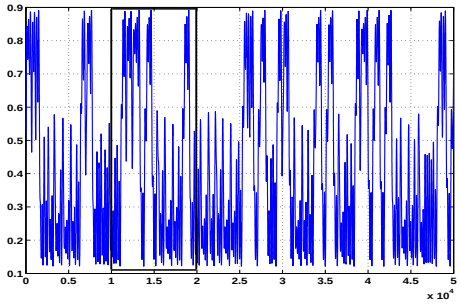

Fig. 4. Plot of the function $\mu(y)$

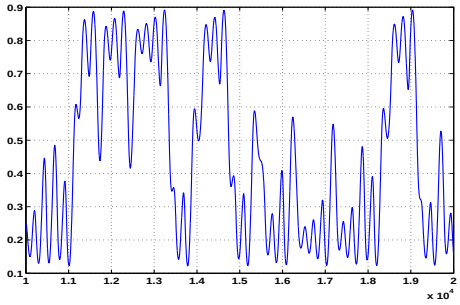

Fig. 5. Zoom in Fig. 4

The synchronization error of each state component is plotted on Fig. 6.

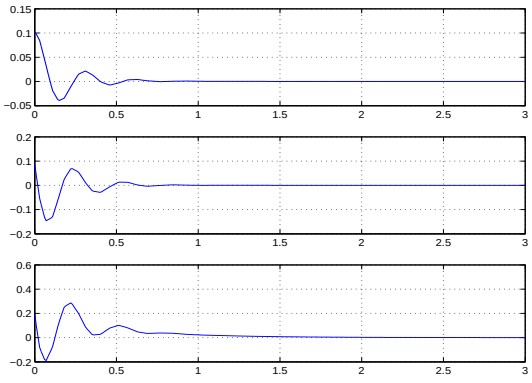

Fig. 6. Synchronization errors

IV. Application to communications

In this section, we propose to apply the previous synchronization scheme in a complete communication process. For this purpose, we choose the encryption method detailed in [8].

$$P = \begin{pmatrix} 1.79292389921732 & -0.91927526256889 & 0.20871307510323 \\ -0.91927526256889 & 1.76061305823448 & -0.61189909748961 \\ 0.20871307510323 & -0.61189909748961 & 0.28073032195374 \end{pmatrix} \quad (36)$$

A. Description of the encryption method

A second chaotic signal y_2 is sent to the receiver (we underline that y_2 is generated independently of y). y_2 is created from the third state of the multimodel-transmitter (27), with a delay depending on the message u:

$$y_2(t) = x_3(t - T_u u(t)) \quad (39)$$

In practice, to enable the recovery of u, $u(t) \in [0, 1]$, and $0 < T_u < T_e$, where T_e will be the discretization step of the numerical integration of the differential equations.
After applying the Taylor-Lagrange formula to expression (39), and a first-order approximation, we obtain (see [8] for the details):

$$x_3(t) - y_2(t) = \dot{x}_3(t) T_u u(t) \quad (40)$$

So, by inversion (under the condition $\dot{x}_3(t) \neq 0$, otherwise expression (40) is replaced by a second-order approximation of the Taylor-Lagrange formula):

$$u(t) = \frac{x_3(t) - y_2(t)}{T_u \dot{x}_3(t)} \quad (41)$$

The decryption formula is easily deduced from (41):

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \quad (42)$$

By replacing the expression of $\dot{\hat{x}}_3$ deduced from (27) and (7), (42) yields to formula (43), with the notations $K_i = \begin{pmatrix} \kappa_{i,1} & \kappa_{i,2} & \kappa_{i,3} \end{pmatrix}^T$, for $i = 1, 2$.

B. Simulations

We propose here to send the famous "Lenna picture", shown in Fig. 7. A discrete signal u is generated, by concatenation of the pixels representing the picture, and u is scaled so that $u \in [0, 1]$. The integration step T_e is chosen equal to 0.01 second. Fig. 8 shows the encrypted message sent to the receiver, and Fig. 9 the recovered picture. The first points of Fig. 9 present some mistakes, since formula (43) is only efficient when synchronization is established, which needs some instants, see Fig. 6. Preamble duration devoted to synchronization depends in particular on the model parameters 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. In our examples, the synchronization time is about two seconds, after that the information signal may be injected.

Fig. 7. Original Lenna picture

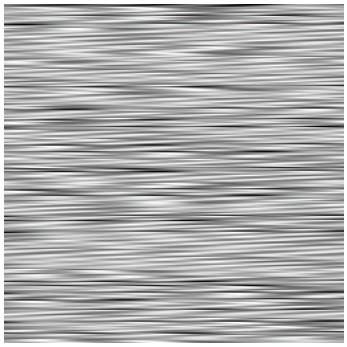

Fig. 8. Encrypted Lenna picture

Fig. 9. Decrypted Lenna picture

V. Conclusion

In this paper we proposed an observer-based synchronization scheme for a class of nonlinear systems, and its application to communications. The transmitter is a multimodel composed of two (or more) chaotic systems. The receiver is designed as an observer of this multimodel, and sufficient conditions for the synchronization of the receiver with the transmitter are established, and expressed in terms of LMIs. Once synchronization is achieved, this can be applied to a communication scheme, and is illustrated through the encryption/decryption of a picture. A future work will consist in a study of the security of the proposed synchronization scheme.

$$\hat{u}(t) = -\frac{1}{T_u}\frac{\hat{x}_3(t) - y_2(t)}{\mu\left(\beta_1\hat{x}_2 + \gamma_1\hat{x}_3 + \kappa_{1,3}(y - \hat{x}_1 - \zeta\hat{x}_2)\right) + (1-\mu)\left(\beta_2\hat{x}_2 + \gamma_2\hat{x}_3 + \kappa_{2,3}(y - \hat{x}_1 - \zeta\hat{x}_2)\right)} \quad (43)$$

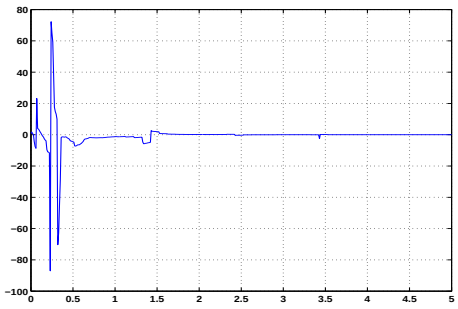

Fig. 10. Reconstruction error

REFERENCES

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

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

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

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

[5] 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.

[6] 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.

[7] S. Celikovský 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.

[8] E. Cherrier, M. Boutayeb, and J. Ragot, "Observers based synchronization and input recovery for a class of chaotic models," in *Proceedings of the Joint 44th IEEE Conference on Decision and Control and European Control Conference, Seville, Spain*, 2005.

[9] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Phys. Reports*, vol. 366, pp. 1–101, 2002.

[10] R. Murray-Smith and T. Johansen, *Multiple Model Approaches to Modeling and Control*. Taylor and Francis, 1997.

[11] Y. Wang, Q. Zhang, and W. Liu., "Stability analysis and design for t-s fuzzy descriptor," in *Proceedings of the 40th IEEE Conference on Decision and Control, Orlando, Florida, USA*, 2001, pp. 3962–3967.

[12] M. Chadli, J. Ragot, and D. Maquin, "Multiquadratic stability and stabilization of continuous-time multiple-model," in *11th IFAC Symposium on Automation in Mining, Mineral and Metal processing, Nancy, France*, 2004.

[13] H. Abarbanel, R. Brown, J. Sidorowich, and L. Tsimring, "The analysis of observed data in physical systems," *Rev. Mod. Phys.*, vol. 65, no. 4, pp. 1331–1392, 1993.

[14] L. Chua, C. Wu, A. Huang, and G.-Q. Zhong, "A Universal Circuit for Studying andGenerating Chaos - Part I and II," *IEEE Trans. Circuit Syst. I*, vol. 40, no. 10, pp. 732–761, 1993.