Open access • Journal Article • DOI:10.1109/TAC.2007.914264

Finite-Time Observers: Application to Secure Communication — Source link

Wilfrid Perruquetti, Thierry Floquet, Emmanuel Moulay

Published on: 31 Mar 2008 - IEEE Transactions on Automatic Control (IEEE)

Topics: Nonlinear system, Synchronization, Observability, Secure communication and Canonical form

Finite time observers: application to secure communication

Wilfrid Perruquetti, Thierry Floquet, Emmanuel Moulay

Finite time observers: application to secure communication

Wilfrid Perruquetti, Thierry Floquet and Emmanuel Moulay

Abstract

In this paper, control theory is used to formalize finite time chaos synchronization as a nonlinear finite time observer design issue. This paper introduces a finite time observer for nonlinear systems that can be put into a linear canonical form up to output injection. The finite time convergence relies on the homogeneity properties of nonlinear systems. The observer is then applied to the problem of secure data transmission based on finite time chaos synchronization and the two-channel transmission method.

Index Terms

Finite time observers, finite time synchronization, two-channel transmission, secure communication.

I. Introduction

A lot of encryption methods involving chaotic dynamics have been proposed in the literature since the 90's. Most of them consists of transmitting informations through an insecure channel, with a chaotic system. The synchronization mechanism of the two chaotic signals is known as *chaos synchronization* and has been developed for instance in [1]. The idea is to use the output of the drive system to control the response system so that they oscillate in a synchronized manner.

W. Perruquetti and T. Floquet are with the LAGIS (UMR CNRS 8146), Ecole Centrale de Lille, Cité Scientifique, 59651 Villeneuve d'Ascq Cedex, France and with Centre de recherche INRIA futurs, Equipe Projet ALIEN. (e-mail: wilfrid.perruquetti@ec-lille.fr, thierry.floquet@ec-lille.fr)

E. Moulay is with IRCCyN (UMR-CNRS 6597), 1 rue de la Noë, B.P. 92 101, 44321 Nantes CEDEX 03, France (e-mail: Emmanuel.Moulay@irccyn.ec-nantes.fr)

Since the work [2], the synchronization can be viewed as a special case of observer design problem, i.e the state reconstruction from measurements of an output variable under the assumption that the system structure and parameters are known. This approach leads to a systematic tool which guarantees chaos synchronization of a class of observable systems. Different observer based methods were developed: adaptive observers [3], backstepping design [4], Hamiltonian forms [5] or sub-Lyapunov exponents [1]. Nevertheless, during the chaos synchronization of continuous systems, the convergence of the error is always asymptotic as in [6]. Instead of attempting the construction of an asymptotic nonlinear observer for the transmitter or coding system, a *finite time chaos synchronization* for continuous systems (in the sense that the error reaches the origin in finite time) can be developed. Finite time observers for nonlinear systems that are linearizable up to output injection have been proposed in [7] and [8] using delays or in [9] and [10] using discontinuous injection terms. Recently, an algebraic method (using module theory and non-commutative algebra) leading to the non asymptotic estimation of the system states has been developed in [11] and applied to chaotic synchronization in [12]. In this work, an homogeneous finite time observer is introduced. This observer yields the finite time convergence of the error variables without using delayed or discontinuous terms. Then, it is applied to the finite time synchronization of chaotic systems and combined with the conventional cryptographic method called *two-channel transmission* in order to design a cryptosystem. The technique of two channel transmission has been proposed in [13]. Other cryptography techniques for secure communications exist such as the parameter modulation developed in [14].

The paper is organized as follows. The problem statement and some definitions are given in Section II. An homogeneous finite time observer is developed in Section III. On the basis of this observer, a two-channel transmission cryptosystem is built and is applied in Section IV to the Chua's circuit that is relevant to secure communications (see e.g. [15] and [16]).

II. Problem statement and definitions

Let us consider a nonlinear system of the form:

$$\dot{x} = \eta\,(x, u) \tag{1}$$

$$y = h(x) \tag{2}$$

where $x \in \mathbb{R}^d$ is the state, $u \in \mathbb{R}^m$ is a known and sufficiently smooth control input, and $y(t) \in \mathbb{R}$ is the output. $\eta : \mathbb{R}^d \times \mathbb{R}^m \to \mathbb{R}^d$ is a known continuous vector field. It is assumed that the system (1)-(2) is locally observable [17] and that there exist a local state coordinate transformation and an output coordinate transformation which transform the nonlinear system (1)-(2) into the following canonical observable form:

$$\dot{z} = Az + f(y, u, \dot{u}, ..., u^{(r)}) \tag{3}$$

$$y = Cz \tag{4}$$

where $z \in \mathbb{R}^n$ is the state, $r \in \mathbb{N}_{>0}$ and

$$A = \begin{pmatrix} a_1 & 1 & 0 & 0 & 0 \\ a_2 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & 0 & 0 & 0 & 1 \\ a_n & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 0 & ... & 0 \end{pmatrix}. \tag{5}$$

The transformations involved in such a linearization method for different classes of systems with $n = d$ can be found in [18], [19], [20], [21]. One can have $n > d$ in the case of system immersion [22], [23].

Then, the observer design is quite simple since all nonlinearities are function of the output and known inputs. Asymptotic stability can be obtained using a straightforward generalization of a linear Luenberger observer. Finite time sliding mode observers have already been designed for system (3)-(4) (see e.g. [9], [10]). However, they rely on discontinuous output injections and on a step-by-step procedure that can be harmful for high order systems. In this paper, a finite time observer based on continuous output injections is introduced.

Notions about finite time stability and homogeneity are recalled hereafter.

Finite time stability

Consider the following ordinary differential equation:

$$\dot{x} = g(x), \quad x \in \mathbb{R}^n. \tag{6}$$

Note $\phi^{x_0}(t)$ a solution of the system (6) starting from x_0 at time zero.

Definition 1: The system (6) is said to have a unique solution in forward time on a neighbourhood $\mathcal{U} \subset \mathbb{R}^n$ if for any $x_0 \in \mathcal{U}$ and two right maximally defined solutions of (6), $\phi^{x_0} : [0, T_\phi[\rightarrow \mathbb{R}^n$ and $\psi^{x_0} : [0, T_\psi[\rightarrow \mathbb{R}^n$, there exists $0 < T_{x_0} \leq \min\{T_\phi, T_\psi\}$ such that $\phi^{x_0}(t) = \psi^{x_0}(t)$ for all $t \in [0, T_{x_0}[$.

Let us consider the system (6) where $g \in C^0(\mathbb{R}^n)$, $g(0) = 0$ and where g has a unique solution in forward time. Let us recall the notion of finite time stability involving the settling-time function given in [24, Definition 2.2] and [25].

Definition 2: The origin of the system (6) is *Finite Time Stable* (FTS) if:

1) there exists a function $T : \mathcal{V} \setminus \{0\} \rightarrow \mathbb{R}_+$ ($\mathcal{V}$ is a neighbourhood of the origin) such that for all $x_0 \in \mathcal{V} \setminus \{0\}$, $\phi^{x_0}(t)$ is defined (and unique) on $[0, T(x_0))$, $\phi^{x_0}(t) \in \mathcal{V} \setminus \{0\}$ for all $t \in [0, T(x_0))$ and $\lim\limits_{t \rightarrow T(x_0)} \phi^{x_0}(t) = 0$.
   T is called the *settling-time function* of the system (6).
2) for all $\epsilon > 0$, there exists $\delta(\epsilon) > 0$ such that for every $x_0 \in (\delta(\epsilon)\mathcal{B}^n \setminus \{0\}) \cap \mathcal{V}$, $\phi^{x_0}(t) \in \epsilon\mathcal{B}^n$ for all $t \in [0, T(x_0))$.

The following result gives a sufficient condition for system (6) to be FTS (see [26], [27] for ODE, and [28] for differential inclusions):

Theorem 3: Let the origin be an equilibrium point for the system (6), and let r be a continuous function on an open neighborhood $\mathcal{V}$ of the origin. If there exist a Lyapunov function $V : \mathcal{V} \rightarrow \mathbb{R}_+$ and a function $r : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ such that

$$\dot{V}(x) \leq -r(V(x)), \tag{7}$$

along the solutions of (6) and $\varepsilon > 0$ such that

$$\int_0^\varepsilon \frac{dz}{r(z)} < +\infty, \tag{8}$$

then the origin is FTS.

The interested reader can find more details on finite time stability in [29], [30], [31], [32], [33], [34].

Homogeneity

Definition 4: A function $V : \mathbb{R}^n \rightarrow \mathbb{R}$ is *homogeneous of degree* d with respect to the weights $(r_1, \ldots, r_n) \in \mathbb{R}^n_{>0}$ if

$$V(\lambda^{r_1} x_1, \ldots, \lambda^{r_n} x_n) = \lambda^d V(x_1, \ldots, x_n)$$

for all $\lambda > 0$.

Definition 5: A vector field g is *homogeneous of degree* d with respect to the weights $(r_1, \ldots, r_n) \in \mathbb{R}^n_{>0}$ if for all $1 \leq i \leq n$, the $i-$th component g_i is a homogeneous function of degree $r_i + d$, that is

$$g_i\left(\lambda^{r_1}x_1, \ldots, \lambda^{r_n}x_n\right) = \lambda^{r_i+d}g_i\left(x_1, \ldots, x_n\right)$$

for all $\lambda > 0$. The system (6) is homogeneous of degree d if the vector field g is homogeneous of degree d.

Theorem 6: [25, Theorem 5.8 and Corollary 5.4] Let g be defined on $\mathbb{R}^n$ and be a continuous vector field homogeneous of degree $d < 0$ (with respect to the weights $(r_1, \ldots, r_n)$). If the origin of (6) is locally asymptotically stable, it is globally FTS.

III. A CONTINUOUS FINITE TIME OBSERVER

Assume that the system (1)-(2) can be put into the observable canonical form (3)-(4). An observer for this system is designed as follows

$$\begin{pmatrix} \frac{d\hat{z}_1}{dt} \\ \vdots \\ \frac{d\hat{z}_n}{dt} \end{pmatrix} = A \begin{pmatrix} z_1 \\ \hat{z}_2 \\ \vdots \\ \hat{z}_n \end{pmatrix} + f(y, u, \dot{u}, ..., u^{(r)}) - \begin{pmatrix} \chi_1\left(z_1 - \hat{z}_1\right) \\ \chi_2\left(z_1 - \hat{z}_1\right) \\ \vdots \\ \chi_n\left(z_1 - \hat{z}_1\right) \end{pmatrix} \tag{9}$$

where the functions χ_i will be defined in such a way that the observation error $e = z - \hat{z}$ tends to zero in finite time. Set $e = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \end{bmatrix}^T$. The observation error dynamics is given by

$$\begin{cases} \dot{e}_1 = e_2 + \chi_1\left(e_1\right) \\ \dot{e}_2 = e_3 + \chi_2\left(e_1\right) \\ \vdots \\ \dot{e}_{n-1} = e_n + \chi_{n-1}\left(e_1\right) \\ \dot{e}_n = \chi_n\left(e_1\right) \end{cases} \tag{10}$$

Denote $\lceil x \rfloor^{\alpha} = |x|^{\alpha} sgn\left(x\right)$ for all $x \in \mathbb{R}$ and for $\alpha > 0$. The following result holds:

Lemma 7: Let $d \in \mathbb{R}$ and $(k_1, \dots, k_n) \in \mathbb{R}^n_{>0}$. Define $(r_1, \dots, r_n) \in \mathbb{R}^n_{>0}$ and $(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n_{>0}$ such that

$$r_{i+1} = r_i + d, \ 1 \le i \le n-1, \tag{11}$$

$$\alpha_i = \frac{r_{i+1}}{r_1}, \ 1 \le i \le n-1, \tag{12}$$

$$\alpha_n = \frac{r_n + d}{r_1}, \tag{13}$$

and set

$$\chi_i(e_1) = -k_i \lceil e_1 \rfloor^{\alpha_i}, \ 1 \le i \le n.$$

Then, the system (10) is homogeneous of degree d with respect to the weights $(r_1, \dots, r_n) \in \mathbb{R}^n_{>0}$.

Proof of Lemma 7 is obvious.

Denote $\alpha_1 = \alpha$.

Lemma 8: If $\alpha > 1 - \frac{1}{n-1}$, the system (10) is homogeneous of degree $\alpha - 1$ with respect to the weights $\{(i-1)\alpha - (i-2)\}_{1 \le i \le n}$ and $\alpha_i = i\alpha - (i-1), \ 1 < i \le n$.

Proof: Let us normalize the weights by setting $r_1 = 1$. Then $r_2 = \alpha$ and

$$d = r_2 - r_1 = \alpha - 1.$$

From (11) and (12)-(13), one obtains recursively that:

$$r_i = (i-1)\alpha - (i-2), \ 1 < i \le n,$$

$$\alpha_i = i\alpha - (i-1), \ 1 < i \le n.$$

Since $r_1 > \ldots > r_n > 0$, one has:

$$\alpha > \frac{n-2}{n-1} = 1 - \frac{1}{n-1}.$$

The result follows from Lemma 7. ■

The system (10) is then given by:

$$\begin{cases} \dot{e}_1 = e_2 - k_1 \lceil e_1 \rfloor^{\alpha} \\ \dot{e}_2 = e_3 - k_2 \lceil e_1 \rfloor^{2\alpha - 1} \\ \vdots \\ \dot{e}_{n-1} = e_n - k_{n-1} \lceil e_1 \rfloor^{(n-1)\alpha - (n-2)} \\ \dot{e}_n = -k_n \lceil e_1 \rfloor^{n\alpha - (n-1)} \end{cases} \tag{14}$$

denoted shortly

$$\dot{e} = \psi(\alpha, e). \tag{15}$$

Lemma 9 (Tube Lemma): Consider the product space $X \times Y$, where Y is compact. If N is an open set of $X \times Y$ containing the slice $\{x_0\} \times Y$ of $X \times Y$, then N contains some tube $W \times Y$ about $\{x_0\} \times Y$, where W is a neighborhood of x_0 in X.

Theorem 10: Set the gains $(k_1, \ldots, k_n)$ such that the matrix

$$A_o = \begin{pmatrix} -k_1 & 1 & 0 & 0 & 0 \\ -k_2 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -k_{n-1} & 0 & 0 & 0 & 1 \\ -k_n & 0 & 0 & 0 & 0 \end{pmatrix}$$

is Hurwitz. Then, there exists $\epsilon \in \left[1 - \frac{1}{n-1}, 1\right)$ such that for all $\alpha \in (1 - \epsilon, 1)$, the system (15) is globally finite time stable.

Proof: Set

$$1 - \frac{1}{n-1} < \alpha < 1.$$

Homogeneity: From Lemma 8, the system (15) is homogeneous of degree $\alpha - 1 < 0$ with respect to the weight $\{(i-1)\alpha - (i-2)\}_{1 \leq i \leq n}$.

Asymptotic stability: Consider the following differentiable positive definite function

$$V(\alpha, e) = y^T P y \tag{16}$$

where

$$y = \begin{pmatrix} \lceil e_1 \rfloor^{\frac{1}{q}} \\ \lceil e_2 \rfloor^{\frac{1}{\alpha q}} \\ \vdots \\ \lceil e_i \rfloor^{\frac{1}{[(i-1)\alpha - (i-2)]q}} \\ \vdots \\ \lceil e_n \rfloor^{\frac{1}{[(n-1)\alpha - (n-2)]q}} \end{pmatrix},$$

$q = \prod_{i=1}^{n-1} ((i-1)\alpha - (i-2))$ is the product of the weights and P is the solution of the following Lyapunov equation

$$A_o^T P + P A_o = -I.$$

As V is proper,

$$\mathcal{S} = \{e \in \mathbb{R}^n : V(1, e) = 1\}$$

is a compact set of $\mathbb{R}^n$. Define the function

$$\begin{array}{rccc} \varphi : & \mathbb{R}_{>0} \times \mathcal{S} & \to & \mathbb{R} \\ & (\alpha, e) & \mapsto & \langle \nabla V(\alpha, e), \psi(\alpha, e) \rangle \end{array}$$

Since A_o is Hurwitz, the system

$$\dot{e} = A_o \, e$$

is globally asymptotically stable and corresponds to the system (15) with $\alpha = 1$. Since φ is continuous, $\varphi^{-1}(\mathbb{R}_{<0})$ is an open subset of $\Lambda \times \mathcal{S}$ containing the slice $\{1\} \times \mathcal{S}$. Since $\mathcal{S}$ is compact, it follows from the Tube Lemma 9 that $\varphi^{-1}(\mathbb{R}_{<0})$ contains some tube $(1 - \epsilon_1, 1 + \epsilon_2) \times \mathcal{S}$ about $\{1\} \times \mathcal{S}$. For all $(\alpha, e) \in (1 - \epsilon_1, 1 + \epsilon_2) \times \mathcal{S}$

$$\langle \nabla V(\alpha, e), \psi(\alpha, e) \rangle < 0.$$

Thus, the system (15) is locally asymptotically stable. It can also be shown to be globally asymptotically stable as follows. Note that

$$V(\alpha, \lambda^{r_1} e_1, \ldots, \lambda^{r_n} e_n) = \lambda^{\frac{1}{q^2}} V(\alpha, e_1, \ldots, e_n)$$

with $r_i = (i-1)\alpha - (i-2)$ for $1 \le i \le n$. Thus

$$e \mapsto V(\alpha, e)$$

is homogeneous of degree $\frac{1}{q^2}$ with respect to the weights $\{(i-1)\alpha - (i-2)\}_{1 \le i \le n}$. From [35], it can be deduced that

$$e \mapsto \langle \nabla V(\alpha, e), \psi(\alpha, e) \rangle$$

is homogeneous of degree $\frac{1}{q^2} + \alpha - 1$ with respect to the weights $\{(i-1)\alpha - (i-2)\}_{1 \le i \le n}$ and thus is negative definite. This imply that, for $\alpha \in (1 - \epsilon_1, 1 + \epsilon_2)$,

$$e \mapsto V(\alpha, e)$$

is a Lyapunov function for the system (15).

From Theorem 6, it follows that the system is globally finite time stable.

■

IV. Cryptosystem and its application to the Chua's circuit

Several chaotic systems, as the three-dimensional Genesio-Tesi system [36], the Lur'e-like system or the Duffing equation [37], belong to the class of systems (3-4). Let us show that the proposed observer can be useful to perform finite time synchronization of this class of chaotic systems and secure data transmission. For a two-channel transmission, the system governing the transmitter is given by:

$$\dot{z} = A\, z + f\left(y\right) \tag{17}$$

$$y = z_1 \tag{18}$$

$$s\left(t\right) = \nu_e\left(z(t), m(t)\right). \tag{19}$$

The first channel is used to convey the output $y = z_1$ of the chaotic system (17). The function ν_e encrypts the message $m\left(t\right)$ and delivers the signal $s\left(t\right)$ which is transmitted via the second channel. The receiver gets $z_1\left(t\right)$ on the first channel. An observer is designed as follows:

$$\begin{pmatrix} \frac{d\hat{z}_1}{dt} \\ \vdots \\ \frac{d\hat{z}_n}{dt} \end{pmatrix} = A \begin{pmatrix} z_1 \\ \hat{z}_2 \\ \vdots \\ \hat{z}_n \end{pmatrix} + f\left(y\right) + \mathcal{O}_n\left(y - \hat{z}_1\right) \tag{20}$$

where

$$\mathcal{O}_n\left(y - \hat{z}_1\right) = \begin{pmatrix} k_1 \left\lceil z_1 - \hat{z}_1 \right\rfloor^{\alpha} \\ k_2 \left\lceil z_1 - \hat{z}_1 \right\rfloor^{2\alpha-1} \\ \vdots \\ k_n \left\lceil z_1 - \hat{z}_1 \right\rfloor^{n\alpha-(n-1)} \end{pmatrix}.$$

The error dynamics $e = z - \hat{z}$ is given by the system (15). With a good choice of α and $\left\{k_i\right\}_{1 \leq i \leq n}$, Theorem (10) implies that the error dynamic $e\left(t\right)$ converges to the origin in finite time. As a consequence, the message $m\left(t\right)$ can be completely recovered after the finite time synchronization by the system

$$\begin{cases} \text{System (20)} \\ \hat{y} = \hat{z}_1 \\ \hat{m} = \nu_d\left(\hat{z}, s\right) \end{cases}.$$

where the decoding function ν_d is defined by $\nu_d\left(z\left(t\right), s\left(t\right)\right) = m\left(t\right)$.

The Chua's circuit belongs to the class of chaotic systems which can be put into the observable canonical form. (3)-(4) The equations of a Chua's oscillator are given by:

$$\begin{cases} C_1\dot{x}_1 = \frac{1}{R}\left(x_2 - x_1\right) + h\left(x_1\right) \\ C_2\dot{x}_2 = \frac{1}{R}\left(x_1 - x_2\right) + x_3 \\ L\dot{x}_3 = -x_2 - rx_3 \end{cases} \tag{21}$$

where L is a linear inductor, R and r two linear resistors, C_1 and C_2 two linear capacitors,

$$h\left(x\right) = G_2x_1 + \tfrac{1}{2}\left(G_1 - G_2\right)\left(\left|x_1 + B\right| - \left|x_1 - B\right|\right)$$

is the piecewise linear Chua's function. The chosen output is $y = x_1$.

Using the transformation $z = Tx$ with

$$T = \begin{bmatrix} 1 & 0 & 0 \\ \frac{1}{C_2R} + \frac{r}{L} & \frac{1}{C_1R} & 0 \\ \frac{1}{C_2L}\left(1 + \frac{r}{R}\right) & \frac{r}{C_1LR} & \frac{1}{C_1C_2R} \end{bmatrix}$$

the system (21) is transformed into the observable canonical form (17)-(18) with

$$A = \begin{bmatrix} -\frac{1}{C_1R} - \frac{1}{C_2R} - \frac{r}{L} & 1 & 0 \\ -\frac{1}{L}\left(\frac{r}{C_1R} + \frac{r}{C_2R} + \frac{1}{C_2}\right) & 0 & 1 \\ \frac{-1}{C_1C_2RL} & 0 & 0 \end{bmatrix},$$

$$f(y) = \begin{pmatrix} \frac{1}{C_1} \\ \frac{1}{C_1}\left(\frac{1}{C_2R} + \frac{r}{L}\right) \\ \frac{1}{C_1C_2L}\left(1 + \frac{r}{R}\right) \end{pmatrix} h\left(y\right).$$

In the simulations, the numerical values of the Chua's circuit are $C_1 = 10.04$ nF, $C_2 = 102.2$ nF, $R = 1747\ \Omega$, $r = 20\Omega$, $L = 18.8$ mH, $G_1 = -0.756$ mS, $G_2 = -0.409$ mS, $H = 1$ V. The gains of the observer have been set as follows: $\alpha = 0.7, k_1 = 1000, k_2 = 240, k_3 = 24$. The observation error dynamics $e = z - \hat{z}$ is then given by

$$\begin{cases} \dot{e}_1 = e_2 - 1000\left\lceil e_1 \right\rfloor^{0.7} \\ \dot{e}_2 = e_3 - 240\left\lceil e_1 \right\rfloor^{0.4} \\ \dot{e}_3 = -24\left\lceil e_1 \right\rfloor^{0.1} \end{cases}. \tag{22}$$

and $e\left(t\right)$ converges to the origin in finite time (see Fig. 1 and 2). A message $m\left(t\right)$ can be sent and recovered after the delay due to the finite time synchronization by using the previous algorithm (see Fig. 3).

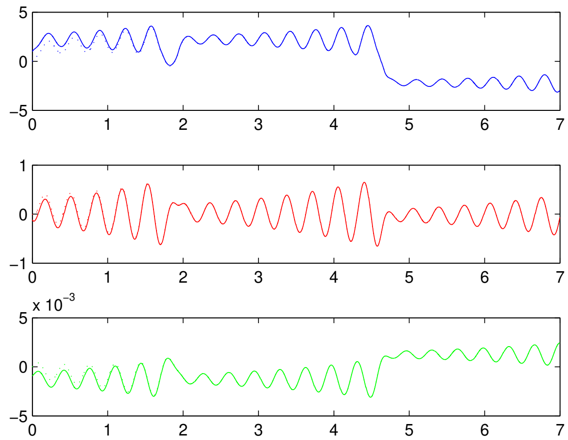

Fig. 1. State of the system (21) and its estimate

Remark 11: It is possible to increase the security of the transmission by introducing some observation singularities in the system (17). In this case, finite time convergence is a useful property (see [38]).

V. CONCLUSION

In this paper, a continuous finite time observer based on homogeneity properties has been designed for the observation problem of nonlinear systems that are linearizable up to output injection. It does not involve any discontinuous output injections and step-by-step procedure, as it is the case, for instance, for sliding mode observers. It has been applied to finite time chaos synchronization and to secure data transmission using the two-channel transmission method.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[2] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, vol. 44, no. 10, pp. 882–890, 1997.

[3] A. Fradkov, H. Nijmeijer, and A. Markov, "Adaptive observer-based synchronization for communication," *Internat. J. Bifur. Chaos Appl. Sci. Engrg.*, vol. 10, no. 12, pp. 2807–2813, 2000.

[4] S. Mascolo and G. Grassi, "Controlling chaos via backstepping design," *Phys. Rev. E (3)*, vol. 56, no. 5, pp. 6166–6169, 1997.

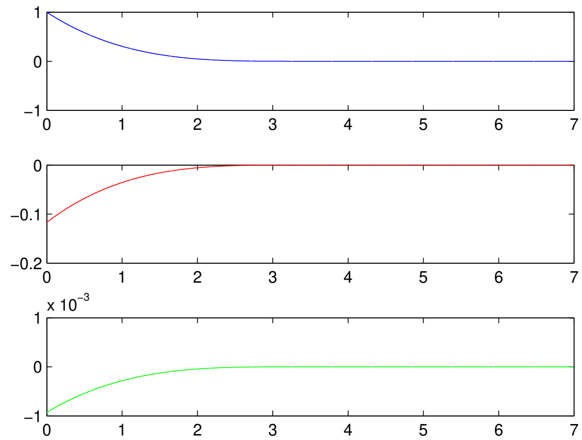

Fig. 2. Observation error

[5] D. López-Mancilla, C. Cruz-Hernández, and C. Posadas-Castillo, "A modified chaos-based communication scheme using hamiltonian forms and observer," *Journal of Physics: Conference Series*, vol. 23, pp. 267–275, 2005.

[6] G. Grassi and S. Mascolo, "Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal," *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, vol. 44, no. 10, pp. 1011–1014, 1997.

[7] R. Engel and G. Kreisselmeier, "A continuous-time observer which converges in finite time," *IEEE Trans. Automatic Control*, vol. 47, no. 7, pp. 1202–1204, 2002.

[8] F. Sauvage, M. Guay, and D. Dochain, "Design of a nonlinear finite-time converging observer for a class of nonlinear systems," *Journal of Control Science and Engineering*, 2007.

[9] S. V. Drakunov and V. I. Utkin, "Sliding mode observers. tutorial," 1995.

[10] W. Perruquetti, T. Floquet, and P. Borne, "A note on sliding observer and controller for generalized canonical forms," in *IEEE Conference on Decision and Control*, Tampa, Florida, USA, 1998, pp. 1920 – 1925.

[11] M. Fliess and H. Sira-Ramírez, "Reconstructeurs dŠetat," *C. R. Acad. Sci. Paris Sér. I Math.*, vol. 338, pp. 91–96, 2004.

[12] H. Sira-Ramírez and M. Fliess, "An algebraic state estimation approach for the recovery of chaotically encrypted messages," *Internat. J. Bifur. Chaos Appl. Sci. Engrg.*, vol. 16, pp. 295–309, 2006.

[13] Z. P. Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, vol. 49, no. 1, pp. 92–96, 2002.

[14] T. Yang and L. Chua, "Secure communication via chaotic parameter modulation," *IEEE Trans. Circuits Systems I Fund. Theory Appl.*, vol. 43, no. 9, pp. 817–819, 1996.

[15] R. Lozi, "Secure communications via chaotic synchronization in chua's circuit and bonhoeffer-van der pol equation: numerical analysis of the errors of the recovered signal," in *IEEE International Symposium on Circuits and Systems*, Seattle, USA, 1995, pp. 684–687.

[16] M. Itoh, H. Murakami, and L. Chua, "Performance of yamakawa's chaotic chips and chua's circuits for secure communications," in *IEEE International Symposium on Circuits and Systems*, London, England, 1994, pp. 105–108.

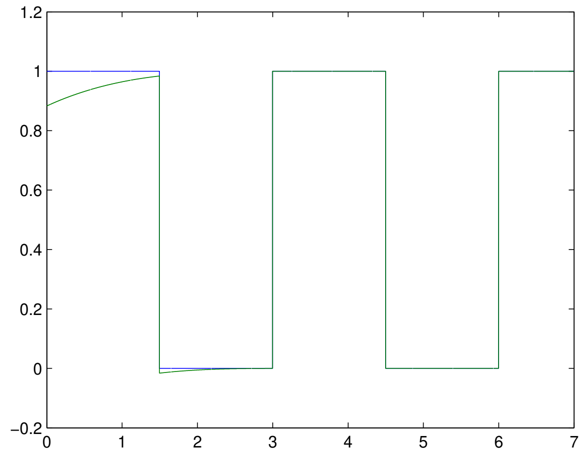

Fig. 3. The message and its reconstruction

[17] R. Hermann and A. J. Krener, "Nonlinear controllability and observability," *IEEE Trans. Automat. Control*, vol. 22, no. 5, pp. 728–740, 1977.

[18] A. Glumineau, C. H. Moog, and F. Plestan, "Algebro-geometric conditions for the linearization by input-output injection," *IEEE Trans. Automat. Control*, vol. 41, pp. 598–603, 1996.

[19] A. J. Krener and A. Isidori, "Linearization by output injection and nonlinear observers," *Systems Control Lett.*, vol. 3, pp. 47–52, 1983.

[20] A. J. Krener and W. Respondek, "Nonlinear observers with linearizable error dynamics," *SIAM J. Control Optim.*, vol. 23, no. 2, pp. 197–216, 1985.

[21] X. H. Xia and W. B. Gao, "Nonlinear observer design by observer error linearization," *SIAM J. Control Optim.*, vol. 27, pp. 199–216, 1989.

[22] J. Back, K. T. Yu, and J. H. Seo, "Dynamic observer error linearization," *Automatica J. IFAC*, vol. 42, pp. 2195–2200, 2006.

[23] P. Jouan, "Immersion of nonlinear systems into linear systems modulo output injection," *SIAM J. Control Optim.*, vol. 41, no. 6, pp. 1756–1778, 2003.

[24] S. P. Bhat and D. S. Bernstein, "Finite time stability of continuous autonomous systems," *SIAM J. Control Optim.*, vol. 38, no. 3, pp. 751–766, 2000.

[25] A. Bacciotti and L. Rosier, *Liapunov Functions and Stability in Control Theory*. 2nd ed. Springer, Berlin, 2005.

[26] E. Moulay and W. Perruquetti, "Finite time stability of non linear systems," in *IEEE Conference on Decision and Control*, Hawaii, USA, 2003.

[27] W. Perruquetti and S. Drakunov, "Finite time stability and stabilisation," in *IEEE Conference on Decision and Control*, Sydney, Australia, 2000.

[28] E. Moulay and W. Perruquetti, "Finite time stability of differential inclusions," 2005.

[29] S. P. Bhat and D. S. Bernstein, "Geometric homogeneity with applications to finite-time stability," *Math. Control Signals*

Systems, vol. 17, pp. 101–127, 2005.

[30] V. T. Haimo, "Finite time controllers," *SIAM J. Control Optim.*, vol. 24, no. 4, pp. 760–770, 1986.

[31] Y. Hong, J. Huang, and Y. Xu, "On an output feedback finite-time stabilization problem," *IEEE Trans. Automat. Control*, vol. 46, pp. 305–309, 2001.

[32] E. Moulay and W. Perruquetti, *Finite-time stability and stabilization: state of the art*. Lecture Notes in Control and Information Sciences, Springer-Verlag, 2006, vol. 334, in Advances in Variable Structure and Sliding Mode Control.

[33] ——, "Finite time stability and stabilization of a class of continuous systems," *J. Math. Anal. Appl.*, vol. 323, no. 2, pp. 1430–1443, 2006.

[34] Y. Orlov, "Finite time stability of homogeneous switched systems," in *IEEE Conference on Decision and Control*, Hawaii, USA, 2003, pp. 4271–4276.

[35] L. Rosier, "Homogeneous Lyapunov function for homogeneous continuous vector field," *Systems Control Lett.*, vol. 19, pp. 467–473, 1992.

[36] M. Y. Chen, Z. Z. Han, and Y. Shang, "General synchronization of genesio-tesi systems," *Internat. J. Bifur. Chaos Appl. Sci. Engrg.*, vol. 14, pp. 347–354, 2004.

[37] M. Feki, "Observer-based exact synchronization of ideal and mismatched chaotic systems," *Phys. Lett. A*, vol. 309, pp. 53–60, 2003.

[38] J. Barbot, I. Belmouhoub, and L. Boutat-Baddas, *Observability Normal Forms in "New Trends in Nonlinear Dynamics and Control and their Applications"*. LNCIS, Springer-Verlag, 2004.