Polytopic observers for chaos synchronization

Gilles Millérioux, Jamal Daafouz

Polytopic observers for chaos synchronization

Gilles Millerioux*, Jamal Daafouz†

November 30, 2006

Abstract

In this paper, an observer approach for message-free and message-embedded chaos synchronization issues is investigated. Owing to the fact that for a chaotic motion, the underlying variables range in a compact domain, the chaos generator can be expressed in a polytopic form. Thus, according to the free context or to the embedded context, the synchronization is carried out by designing either a polytopic observer or an unknown polytopic observer. Global synchronization is ensured from the notion of polyquadratic stability which enables to compute the gains of the observers in a systematic way. Those gains are derived from the solutions of a Linear Matrix Inequalities set.

Keywords
chaos synchronization, polytopic systems, observers, poly-quadratic stability

1 Introduction

Chaos synchronization has exhibited an increase of interest in the last decade since the pioneering works reported in [1][2].
On one hand, message-free chaos synchronization has entered the control scene and has become a popular open problem from the control theory point of view [3]. In [4], an attempt has been made to give a general formalism for synchronization in dynamical systems and many special issues devoted to the subject are of particular interest [5][6][7][8]. A wide variety of methods to achieve synchronization of two dynamical systems coupled in a unidirectional way has been investigated. A unidirectional coupling involves a system called *response* forced by an external signal emanating from a system called *drive* which exhibits a chaotic behavior. From the control theory point of view, three main suitable approaches have attracted interest. The first one consists of the reconstruction of the attractors from a sliding window of a finite amount of output measurements

*Gilles Millerioux, CRAN - CNRS UMR 7039 - UHP - ESSTIN, E-mail: millerioux@esstin.uhp-nancy.fr
†Jamal Daafouz, CRAN - CNRS UMR 7039 - INPL - ENSEM, E-mail: Jamal.Daafouz@ensem.inpl-nancy.fr

from the chaotic system [9][10]. Such a method is motivated by the Takens' theorem [11]. The second approach is referred to as controlled synchronization and consists of finding closed loop feedback control to ensure synchronization. This requires the measure of all the state variables of the system. Finally, when only partial information of those variables are available, meaning that only output variables of the *drive* are transmitted to the *response*, observer-based methods can be considered. One of the important survey on chaos synchronization dealing with the observer approach is [12]. For relative recent results, the reader can refer to [13] for observers with linearizable dynamics, [14] for observers derived from the concept of absolute stability , [15] for observers dedicated to systems having a Generalized Hamiltonian Forms , [16][17] for observers of systems having polytopic description and whose design is based upon Linear Matrix Inequalities (LMI).

On the other hand, one of the well-known practical interest of chaos synchronization lies in the potential applications in communications and more specifically in the possibilities of encoding or masking messages by a suitable embedding. Indeed, it is reasonable to think that there is likely a connection between the random-look behaviors exhibited by chaotic systems and the required properties like confusion and diffusion of cryptosystems. Chaos-based encryption is currently an active field of research. A survey of chaos-based encryption schemes with an adequate bibliography incorporating some cryptographic skills are discussed in [18][19]. In [20][21][22], an overview of the techniques currently relevant for transmitting information via a chaotic signal is given. As far as terminology is concerned, in a message-embedded context, the system exhibiting chaos is commonly referred as the *transmitter* whereas the system which must extract the information is named the *receiver*.

In this paper, both message-free and message-embedded chaos synchronization problems are investigated over a unified framework which involves polytopic observers. Indeed, based upon the fact that the chaos generator named *drive* in the message-free context or *transmitter* in the message-embedded context exhibits a chaotic motion, its underlying state variables are constrained to a compact domain. As a consequence, the range and the bounds of those variables can be known such that the dynamical matrices can be expressed in a polytopic way. Then, the error of synchronization can also be written in a polytopic form. By using the notion of poly-quadratic stability [23][24] and a parameter dependent Lyapunov function, the problem of the observer synthesis can be turned into the resolution of a Linear Matrix Inequalities set. The benefits of such an approach rely on the fact that the resulting synchronization is global and the computation of the gains of the observer is carried out in a systematic way.

The layout of the paper is the following. In Section 2, chaotic systems admitting a polytopic description are presented. Then, some background concerning

the notion of polyquadratic stability are presented. Section 3 and Section 4 respectively deals with the message-free and the message-embedded chaos synchronization problem. A systematic procedure is stated for the design of the polytopic observers which must achieve global synchronization in the message-free context and additionnaly the recovering of the masked information in the message-embedded context.

Notation

Throughout the paper, $\mathbf{1}_n$ is the n-dimensional identity matrix and $\mathbf{0}_{n\times m}$ the $n \times m$ null matrix. For a matrix X, X^T stands for its transpose. When being symmetric, $X > 0$ indicates that X is positive definite. $X^\dagger$ corresponds to the Moore-Penrose generalized inverse of X given by $X^\dagger = (X^T X)^{-1} X^T$.

2 Preliminaries

2.1 Chaotic systems with polytopic description

In this section, the class of chaotic systems under consideration are detailed. We concentrate on dynamical systems of which general description is as follows :

$$\left\{ \begin{array}{lcl} x_{k+1} & = & A(\rho_k)x_k \quad + \quad E(\rho'_k) \\ y_k & = & Cx_k \end{array} \right. \tag{1}$$

where $x_k \in \mathbb{R}^n$, $y_k \in \mathbb{R}^m$, $A \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{m\times n}$. Let ρ and ρ' be respectively a L-dimensional and a M-dimensional function. The images under ρ and ρ' are respectively denoted $\rho_k = (\rho_k^1, \ldots, \rho_k^L)^T$ and $\rho'_k = (\rho_k^{'1}, \ldots, \rho_k^{'M})^T$. They are both assumed to be available. The term $A(\rho_k)x_k$ includes all the affine dependence in the dynamics with respect to x_k. Besides A is of class C^1 with respect to the entries of ρ_k such that A can be rewritten in the form $A(\rho_k) = A_0 + \sum_{i=1}^{L} \rho_k^i A_i^{lc}$. A_0 is the matrix derived from $A(\rho_k)$ by keeping its constant entries while setting to zero its time-varying entries. A_i^{lc} is a matrix whose entries are all zero except the one, located at line l and column c, which equals unity. The superscripts l and c depend on i and correspond respectively to the position of ρ_k^i in $A(\rho_k)$. E is a (possible) nonlinear $n-$dimensional function depending on ρ'_k (not necessarily in an affine way).

The quantity ρ_k acts as a time-varying parameter for A and is assumed to be bounded such that A lies in a compact set which may be embedded in a polytope, that is :

$$A(\rho_k) = \sum_{i=1}^{N} \xi_k^i(\rho_k) A_i \tag{2}$$

The A_i's correspond to the vertices of the convex hull $\mathbf{Co}\{A_1, \ldots, A_N\}$, and the ξ_k^i's belong to the compact set $\mathcal{S} = \{\mu_k \in \mathbb{R}^N, \mu_k = (\mu_k^1, \ldots, \mu_k^N)^T,\ \mu_k^i \geq 0\ \forall i \text{ and } \sum_{i=1}^{N} \mu_k^i = 1\}$. The ξ_k^i's can always be expressed as a linear function of the ρ_k^i's.

The class of systems described by (1) includes some usual chaotic systems.

Lur'e systems
Those systems are described by the recursion :

$$x_{k+1} = A_1 x_k + E(y_k)$$

A_1 is a constant dynamical matrix and E is a $n-$dimensional function of the output y_k. Such systems are derived from (1) by letting $A(\rho_k) = A_1$ and $\rho'_k = y_k$. Besides, note that a constant matrix A_1 is a special case of (2) with $N = 1$.

Output injection with time-varying dynamical matrix
Those systems are described by the recursion :

$$x_{k+1} = A(y_k)x_k + E(y_k)$$

Whenever such systems exhibit a chaotic behavior, x_k and so y_k are constrained to a compact domain. As a consequence, y_k is bounded at least in a hypercube since each component y_k^i ranges between two extremal values $\underline{y}_k^i$ and $\overline{y}_k^i$. Hence $A(y_k)$ can be expressed in a polytopic way and verifies (2) by letting $\rho_k = \rho'_k = g(y_k)$, g being a function of y_k such that A is of class C^1 with respect to ρ_k. A polytopic decomposition for such systems is detailed in [17].

Piecewise linear systems
Those systems are described by the recursion :

$$x_{k+1} = A_i x_k + E_i$$

Let the state space $\mathbb{R}^n$ be partitioned into N distinct regions R_i with $\bigcup_{i=1}^{i=N} R_i \subseteq \mathbb{R}^n$. A_i and E_i are constant matrices assigned, with a one-to-one correspondence, to the region R_i visited by x_k at the discrete time k. Piecewise linear systems are derived from (1) as the following. Let ρ (*resp.* ρ') be a scalar function $\mathbb{R}^n \to I$, with $I = \{1, \ldots, N\}$ an index set of N elements, defined by $\rho(x_k) = \rho_k = i$ (*resp.* $\rho'(x_k) = \rho'_k = i$) if x_k visits the region R_i at the discrete time k. Letting $\rho'_k = \rho_k$ and parameterizing $A(\rho_k)$ (*resp.* $E(\rho_k)$) such that $A(\rho_k) = A_i$ (*resp.* $E(\rho_k) = E_i$) when $\rho_k = i$, the usual piecewise linear description above is thus obtained. Now, defining an indicator vector $\xi_k = (\xi_k^1, \ldots, \xi_k^N)^T$ as follows :

$$\xi_k^i = \begin{cases} 1 \text{ if } \rho_k = i \\ 0 \text{ otherwise} \end{cases}$$

Thus, $A(\rho_k)$ can be expressed in the polytopic form (2).

2.2 Poly-Quadratic stability

Poly-Quadratic stability has been introduced in [23] to state necessary and sufficient conditions of existence of parameter dependent Lyapunov functions in the

context of linear parameter varying systems (LPV). The notion of LPV systems was first introduced in [25]. This class of systems is different from standard linear time varying systems counterpart due to the dependence of the system matrices on the variations of the plant dynamics. The study of LPV systems was first motivated by the gain scheduling control design methodology where the design of the controller involves the design of several linear time invariant controllers for a parameterized family of linearized models of a system and the interpolation of the controller gains [26] [25]. Although it seems working well in practice, this heuristic design procedure does not take the parameter variations into account and can not provide any stability or performance guarantees except for slow varying parameters [27]. Also, LPV theory has been found useful to simplify the interpolation and realization problems associated with conventional gain scheduling. Specially, it allows to treat gain scheduling controllers as a single entity with the gain scheduling achieved entirely by the parameter dependent controller [28]. A linear parameter varying system is given by :

$$\nu_{k+1} = \mathcal{A}(\xi_k)\nu_k \tag{3}$$

where ν_k is a n-dimensional state vector and $\xi_k \in \Xi \subset \mathbb{R}^N$ is a bounded time-varying parameter. This system is said polytopic when the dependence of the dynamical matrix on ξ_k is given by :

$$\mathcal{A}(\xi_k) = \sum_{i=1}^{N} \xi_k^i A_i \quad \text{and} \quad \xi_k = (\xi_k^1, \ldots, \xi_k^N)^T, \qquad \xi_k^i \geq 0, \qquad \sum_{i=1}^{N} \xi_k^i = 1 \tag{4}$$

and where A_i are constant matrices called vertices. What is known in the litterature as quadratic stability refers to checking stability of the previous system using classical quadratic Lyapunov function $V(\nu_k) = \nu_k^T P \nu_k$ with P a positive definite matrix. Although any quadratic stability based condition seems numerically useful since it generally leads to LMI feasibility problems [29], this kind of conditions are conservative. In order to reduce such a conservatism, parameter dependent Lyapunov functions (PDLF) have been introduced [30]. This consists in letting the Lyapunov matrix P depend on the parameter vector ξ_k. A general result is given in the following Theorem :

Theorem 1. *System (3) is asymptotically stable if there exists a Lyapunov function*

$$V(\nu_k, \xi_k) = \nu_k^T \mathcal{P}(\xi_k)\nu_k$$

such that

$$\alpha_1(\|\nu_k\|) \leq V(\nu_k, \xi_k) \leq \alpha_2(\|\nu_k\|) \tag{5}$$

and whose difference along the solution of (3) is negative definite descrescent that is

$$\mathcal{L} = V(\nu_{k+1}, \xi_{k+1}) - V(\nu_k, \xi_k) \leq -\alpha_0(\|\nu_k\|) \tag{6}$$

for all $\nu_k \in \mathbb{R}^n$ and $\xi_k \in \Xi$ and where $\alpha_0(.)$, $\alpha_1(.)$ and $\alpha_2(.)$ are κ_∞ functions[1].

[1] A function $\alpha : [0, \infty) \to [0, \infty)$ is a κ_∞ function if it is continuous, striclty increasing, zero at zero and unbounded ($\alpha(s) \to \infty$ as $s \to \infty$).

In practice, this result is too general and it can not be used in its present form since there is no systematic way to build the Lyapunov function $V(\nu_k, \xi_k)$ as a function of the time-varying parameter ξ_k. Based on a similar description of the LPV system (3), Poly-Quadratic stability has been defined in order to check stability of the polytopic LPV system (3) with a parameter-dependent Lyapunov functions (PDLF) of the form:

$$V(\nu_k, \xi_k) = \nu_k^T \mathcal{P} \nu_k \quad \text{with} \quad \mathcal{P} = \sum_{i=1}^{N} \xi_k^i P_i, \quad \xi_k^i \geq 0, \quad \sum_{i=1}^{N} \xi_k^i = 1 \tag{7}$$

where P_i are symmetric positive definite constant matrices of appropriate dimension. Such a PDLF satisfies condition (5) with $\alpha_2(\|\nu_k\|) = \sum_{i=1}^{N} \lambda_{max}(P_i)\|\nu_k\|^2$ and $\alpha_1(\|\nu_k\|) = \varepsilon\|\nu_k\|^2$ with ε a sufficiently small positive scalar. Its difference along the solution of (3) is given by

$$\mathcal{L} = V(\nu_{k+1}, \xi_{k+1}) - V(\nu_k, \xi_k) \tag{8}$$

with

$$V(\nu_{k+1}, \xi_{k+1}) = \nu_{k+1}^T \mathcal{P}_+ \nu_{k+1} \quad \text{and} \quad \mathcal{P}_+ = \sum_{i=1}^{N} \xi_{k+1}^i P_i \tag{9}$$

A necessary and sufficient condition of existence of such a PDLF is proposed in [23]. It consists in checking the feasibility of a set of Linear matrix Inequalities where the unkowns are directly related to the Lyapunov matrices P_i. This condition allows to answer by "yes" or "no" the following question : Is there a Lyapunov function of the form (7) allowing to check that the LPV system (3) is globally asymptotically stable. Before stating this result, a definition of poly-quadratic stability is recalled from [23].

Definition 1. *System (3) is said to be poly-quadratically stable if there exists a positive definite Parameter Dependent quadratic Lyapunov Function V as defined in (7) whose difference along the solution of (3) satisfies*

$$V(\nu_{k+1}, \xi_{k+1}) - V(\nu_k, \xi_k) = \nu_k^T (\mathcal{A}^T \mathcal{P}_+ \mathcal{A} - \mathcal{P}) \nu_k < -\alpha_0(\|\nu_k\|) \tag{10}$$

with α_0 a κ_∞ function.

The following theorem gives a necessary and sufficient condition for the dynamics (3) to be poly-quadratically stable and so for ν_k to converge globally towards zero.

Theorem 2. *The LPV system (3) is poly-quadratically stable if and only if there exist N symmetric matrices $P_1, ..., P_N$ and N matrices $G_1, ..., G_N$ satisfying the following set of Linear Matrix Inequalities :*

$$\begin{bmatrix} P_i & A_i^T G_i^T \\ G_i A_i & G_i + G_i^T - P_j \end{bmatrix} > 0 \tag{11}$$

for all $(i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$. *The Lyapunov function is then given by:*

$$V(\nu_k, \xi_k) = \nu_k^T \big(\sum_{i=1}^{N} \xi_k^i P_i \big) \nu_k$$

The main advantage in using Poly-Quadratic stability to answer the basic problem stated in the beginning of this section relies on the fact that it provides a sufficient condition of asymptotic stability with the following features:

- This condition is numerically well tractable. One has to check the feasibility of a set of Linear Matrix Inequalities (LMI). This reduces to a convex optimization problem for which powerful numerical algorithms and routines are known to exist.

- It is obviously less conservative than the conditions based on checking the existence of a common Lyapunov function. Notice that when imposing the constraint $G_i = S_i = S$, with S a constant matrix, we recover the condition based on looking for a common quadratic Lyapunov function $V(\nu_k, \xi_k) = \nu_k^T P \nu_k$ with $P = S^{-1}$.

- This condition can be used for switched linear systems as explained in [31]. When compared to some existing conditions for stability of switched linear systems which require that the matrices A_i commute for each i, the conservatism is reduced.

- Under arbitrary switching rule, the proposed condition has to be satisfied for all the pairs (i,j) that is to take into account all possible switches from each subsystem to another. However, if all the transitions are not allowed and if one is able to determine a set of all ordered pairs (i,j) of indices denoting the possible switches from a subsystem A_i to another subsystem A_j, the proposed condition can be modified to take into account only these selected pairs of indices. Hence, knowledge of allowed transitions between subsystems is a way to reduce again the conservatism in the case of switched linear systems.

- The extra matrices G_i can be useful when design problems are formulated using this condition. The control or observer gains will depend on this matrices and not on the "Lyapunov" matrices S_i. Hence, if other constraints than stability are fixed they will not affect the Lyapunov matrices but only these extra matrices [32]. This can be less conservative than the results where the control or the observer gains depend explicitly on the Lyapunov matrices (see also [33] where the switched static output feedback problem is presented as an example of this situation).

In next sections, the problems of message-free and message-embedded chaos synchronization are discussed. A motivation of the observer-based approach developed in both cases is previously given.

3 Message-free chaos synchronization

3.1 Synchronization and state reconstruction

Observer-based synchronization is one of possible methods which enables the dynamical system state reconstruction. It is well known that for a single input single output autonomous linear dynamical system of dimension n, a brute method, in view of reconstructing the state vector x_k at the discrete time k, consists in simply inverting a so-called observability matrix Q_0. It stems from the fact that, for a realization (A, C), x_k can be expressed as a linear combination of the n past outputs y_{k-i}, $i = 0, \ldots, n-1$ in the form :

$$x_k = A^{n-1} Q_0^{-1} Y_k \quad \text{with} \quad Q_0 = \begin{bmatrix} C \\ \ldots \\ CA^{n-1} \end{bmatrix} \quad \text{and } Y_k = [y_{k-n+1}, \ldots, y_k]^T$$

provided that Q_0 is invertible or equivalently that the pair (A, C) is observable. A state reconstruction based on past outputs has a counterpart for nonlinear systems given by the Taken's theorem [11].

Theorem 3. *Let Ω be a compact manifold of dimension n. Let φ be a smooth (at least of class C^2) diffeomorphism $\mathbb{R}^n \to \mathbb{R}^n$ and h a smooth function $\mathbb{R}^n \to \mathbb{R}$. Generically, there exists a map ϕ from $\mathbb{R}^n$ to $\mathbb{R}^{l+1}$ such that :*

$$\phi(x_k) = (h(x_k), \ldots, h(\varphi^l(x_k)))$$

for $l \geq 2n$.

Applying such a theorem would enable to reconstruct the state vector x_k of a chaotic map from at least the $2n+1$ past output values. Unfortunately, Taken's theorem does not provide the function ϕ. Besides, it is well known that a direct reconstruction, or equivalently a direct "inversion", suffers from measurement errors and is not viable in practice. It is better to use asymptotical reconstruction, an approach which motivates the use of observers. Let mention that the issue of direct reconstruction is discussed for example in [10][34][9]. Before dealing with polytopic observers, a definition of synchronization is given.

Definition 2 (*Global Synchronization*). *Global synchronization of a drive-response system can be expressed in one of the following formulations involving the respective state vectors x_k and $\hat{x}_k$:*

$$\lim_{k \to \infty} \|x_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0 \tag{12}$$

$$\exists k_f, \|x_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0 \quad \textit{and} \quad \forall k > k_f \tag{13}$$

Eq. (12) corresponds to an asymptotical synchronization while Eq. (13) corresponds to a finite time synchronization.

3.2 Polytopic observers

Consider a *response* system governed by the dynamics of the following observer equation :

$$\left\{ \begin{array}{lcl} \hat{x}_{k+1} & = & A(\rho_k)\hat{x}_k + E(\rho'_k) + L(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k & = & C\hat{x}_k \end{array} \right. \tag{14}$$

The equation of the synchronization error between the *drive* and the *response* is obtained by subtracting (14) from (1).

$$\varepsilon_{k+1} = (A(\rho_k) - L(\rho_k)C)\,\varepsilon_k \tag{15}$$

It is recalled that $A(\rho_k)$ is written in a polytopic form (2) as described in section 2.1. Let define $L(\rho_k)$ as a time-varying gain matrix depending on ρ_k and satisfying the relation :

$$L(\rho_k) = \sum_{i=1}^{N} \xi_k^i(\rho_k) L_i \tag{16}$$

The terms ξ_k^i are the ones involved in the polytopic decomposition (2) of $A(\rho_k)$ and so depend on ρ_k. Eq. (16) means that the gain matrix $L(\rho_k)$ is interpolated from the vertices L_i. They have to be computed in order to ensure global synchronization. From this perspective, substituting (2) and (16) into (15) yields :

$$\varepsilon_{k+1} = \sum_{i=1}^{N} \xi_k^i\,(A_i - L_i C)\varepsilon_k \tag{17}$$

This is a polytopic formulation of the error of synchronization. Next subsection is devoted to conditions for global convergence conditions of (17) and so global synchronization of (1)-(14). They are based upon the notion of poly-quadratic stability presented in section 2.2.

3.3 Conditions of global synchronization

Proposition 1. *Global synchronization of (1)-(14) is achieved whenever the feasibility condition of the following set of Linear Matrix Inequalities is satisfied :*

$$\left[\begin{array}{cc} P_i & A_i^T G_i^T - C^T F_i^T \\ G_i A_i - F_i C & G_i + G_i^T - P_j \end{array} \right] > 0 \tag{18}$$

for all $(i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$

The G_i's, P_i's and F_i's are unknown matrices of appropriate dimensions. The resulting gains L_i are given by $L_i = G_i^{-1} F_i$.

Remark 1. *The formulation (18) differs from the one encountered in [24] but is strictly equivalent. The proof follows exactly the same reasoning.*

4 Message-embedded chaos synchronization

4.1 Input Independent Global Synchronization

We concentrate on the message-embedded scheme depicted on Fig. 1. The plaintext m_k is encrypted by an encryption function e which depends on a chaotic key stream x_k generated by the chaos generator named in this context the *transmitter*. The resulting quantity denoted u_k is embedded in the dynamics of the chaos generator. In the sequel, u_k will be abusively called the information. It is important noting that u_k is not transmitted to the *receiver*, only an output signal y_k, whose dimension is less than the dimension of x_k, is transmitted through the channel to the *receiver*. The *receiver* system must be designed such that u_k can be recovered, given the only available data y_k. Once u_k is recovered, the plaintext m_k can be extracted by applying the decoding function e^{-1} provided that $\hat{x}_k$ is exactly synchronized with x_k. This requirement is the main problem to be overcome.

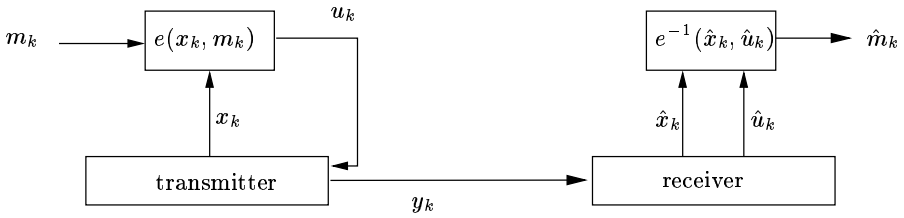

Figure 1: message-embedded scheme

Few methods involving observer-based approaches have been investigated. The design of the observer is based on the consideration of the state reconstruction error dynamics. On one hand, the design can be carried such that its convergence towards zero is guaranteed despite of the presence in the dynamics of a residual term involving u_k. A sufficient condition for the exponential convergence of the state-error dynamics in the case of Lipschitz nonlinearities are given in [35]. For discrete-time systems, dead-beat observers can be designed in order to make the matrix involved in the synchronization error equation to be nilpotent [36][37]. In this case, despite of the fact that the error depends on u_k, it can reach zero after a finite number of steps. This method works for example by performing a zero eigenvalues assignment with discrete-time Lur'e chaotic systems. On the other hand, the design can be performed in such a way the residual term involving u_k no longer appears in the state reconstruction error dynamics. An example is presented in the context of a chaotic inverse system encryption approach with Lur'e systems [38]. The problem has been formally tackled by introducing the notion of Input Independent Global Synchronization (IIGS) in [32][39]. In [39] an Unknown Input Observer Approach dedicated to polytopic systems has been established. Such an approach is recalled here.

Definition 3 (*Input Independent Global Synchronization).* *Input Independent Global Synchronization of a transmitter-receiver system can be expressed in one of the following formulations involving the respective state vectors x_k and $\hat{x}_k$:*

$$\lim_{k\to\infty} \|x_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0 \quad \textit{and} \quad \forall u_k \tag{19}$$

$$\exists k_f, \|x_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0 \quad , \quad \forall k > k_f \quad \textit{and} \quad \forall u_k \tag{20}$$

Eq. (19) and (20) differ from Definition 2 by the fact that $\hat{x}_k$ must coincide with x_k given any u_k.

4.2 Polytopic unknown input observers

In order to achieve an Input Independent Global Synchronization, an Unknown Input Observer approach is presented. Unknown Input Observers have been largely investigated for linear systems [40][41][42][43] or bilinear systems [44]. Extension of such a structure for systems having a polytopic description is presented, the reader can refer to [39] for details.
Let consider the *transmitter* be described by :

$$\left\{ \begin{array}{lcl} x_{k+1} & = & A(\rho_k)x_k + E(\rho'_k) + Bu_k \\ y_k & = & Cx_k \end{array} \right. \tag{21}$$

which differs from (1) by the introduction of an additional term Bu_k involving a so-called "mixing matrix" $B \in \mathbb{R}^{n\times r}$ $(r \geq m)$ and $u_k \in \mathbb{R}^r$. As previously described in subsection 4.1, the term u_k results from an encoding function e such that $u_k = e(x_k, m_k)$. It is assumed that e admits an inverse decoding function e^{-1} such that $m_k = e^{-1}(x_k, u_k)$. As far as the *receiver* part is concerned, a natural extension of the unknown linear input observer structure is proposed.

$$\hat{x}_{k+1} = (PA(\rho_k) - L(\rho_k)C)\hat{x}_k + PE(\rho'_k) + L(\rho_k)y_k + Qy_{k+1} \tag{22}$$

with $P = \mathbf{1}_n - QC$ and $L(\rho_k) = \sum_{i=1}^{N} \xi_k^i(\rho_k)L_i$.
The gains Q and L_i's $(i = 1, \ldots, N)$ must be computed to achieve an Input Independent Global Synchronization of (21)-(22) and consequently the global convergence of the state reconstruction error ϵ_k. Its dynamics is obtained by subtracting (22) from (21) and taking into account the polytopic expression of $L(\rho_k)$ and $A(\rho_k)$:

$$\epsilon_{k+1} = \sum_{i=1}^{N} \xi_k^i(PA_i - L_iC)\epsilon_k + PBu_k \tag{23}$$

4.3 Conditions of Input Independent Global Synchronization

In order to ensure the global convergence of (23) towards zero for any u_k, not only the term PB has to vanish (input independence) but the resulting dynamical equation must converge towards zero (global convergence) as well.

Proposition 2. *The state reconstruction error equation (23) can be made input independent whenever* $rank(CB) = rank(B) = r$.

Indeed, according to the definition of P, the equality $PB = 0$ entails that Q must be subject to :

$$B = QCB \tag{24}$$

Proposition 2 ensures the existence of the solution Q of (24) and its general expression is :

$$Q = B(CB)^{\dagger} + Y(\mathbf{1}_m - (CB)(CB)^{\dagger}) \tag{25}$$

with Y an arbitrary matrix.

Then, whenever Q satisfies (25), $PB = 0$ and so (23) turns into an input independent dynamics :

$$\epsilon_{k+1} = \sum_{i=1}^{N} \xi_k^i (PA_i - L_i C)\epsilon_k \tag{26}$$

This is a polytopic formulation of the error of synchronization. Based on a same reasoning as in section 3.3, the following theorem can thereby be stated :

Theorem 4. *Input Independent Global Synchronization of the message-embedded scheme (21)-(22) is achieved whenever the following conditions are satisfied :*

i) $rank(CB) = rank(B) = r$

ii) the set of LMI's

$$\begin{bmatrix} P_i & (PA_i)^T G_i^T - C^T F_i^T \\ G_i(PA_i) - F_i C & G_i + G_i^T - P_j \end{bmatrix} > 0 \tag{27}$$

is feasible for all $(i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$.

The G_i's, P_i's and F_i's are unknown matrices of appropriate dimensions. The resulting gains L_i are given by $L_i = G_i^{-1} F_i$.

Proof. See [39]. Let just mention that the rank condition *i)* ensures $(CB)^{\dagger}$ to exist in (25) and so $PB = 0$ to be satisfied. □

4.4 Plaintext recovering

The remaining problem lies in the plaintext m_k recovering. The following proposition provides the conditions and a way to recover the original plaintext m_k.

Proposition 3. *If (21)-(22) are Input Independent Global Synchronized, one has* $\hat{d}_{k+1} = u_k$ *and* $\hat{m}_{k+1} = m_k$ *where* $\hat{d}_k$ *and* $\hat{m}_k$ *obey the following recursions :*

$$\begin{array}{lcll} \hat{d}_{k+1} & = & (CB)^{\dagger}(y_{k+1} - CA(\rho_k)\hat{x}_k - CE(\rho'_k)) & a) \\ \hat{m}_{k+1} & = & e^{-1}(\hat{x}_k, \hat{d}_{k+1}) & b) \end{array} \tag{28}$$

Proof. On one hand, if (21)-(22) are IIGS, then $\hat{x}_k = x_k$. Furthermore, premultiply the dynamical equation of (21) by C, then multiply left by $(CB)^\dagger$, (whose existence is ensured by the rank condition *i)* of Theorem 4 yields :

$$u_k = (CB)^\dagger (y_{k+1} - CA(\rho_k)x_k - CE(\rho'_k)) \tag{29}$$

Identifying (29) and (28a) yields $\hat{d}_{k+1} = u_k$.
On the other hand, if (21)-(22) are IIGS, then the equality $\hat{x}_k = x_k$ still holds. Furthermore, $\hat{x}_k = x_k$ and $\hat{d}_{k+1} = u_k$ turns the equality $m_k = e^{-1}(x_k, u_k)$ (derived from the definition of e) into $m_k = e^{-1}(\hat{x}_k, \hat{d}_{k+1})$. Identifying this equality with (28b) yields $\hat{m}_{k+1} = m_k$. This completes the proof. □

Let note that $\hat{m}_{k+1} = m_k$ necessarily leads to a delay when attempting to recover m_k. It stems from the fact that (21) has a relative degree equalling one with respect to u_k.

5 Illustrative examples

5.1 Unknown Input Observer design

An experiment of a message-embedded chaos synchronization scheme involving a *transmitter* of the form (21) is conducted. The distinct matrices of the dynamics are :

$$A(\rho_k) = \begin{bmatrix} \rho_k & 1 & 0 \\ 1 & 0 & 1 \\ -0.7 & 0 & 0.01 \end{bmatrix}, \; B = [0.1 \; 1 \; 1]^T, \; C = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; E = \mathbf{0}_{3\times 1}$$

The nonlinear time-varying parameter ρ_k verifies $\rho_k = x_k^1 x_k^3$, x_k^i being the i^{th} component of the state vector x_k. Note that the special choice of the output matrix C causes ρ_k to be available at each discrete time k as required. The map exhibits a chaotic motion which entails that ρ_k is bounded. Simulation shows that ρ_k ranges between $\underline{\rho} = 0.5627$ and $\overline{\rho} = 0.8028$. Consequently, A lies in a compact set which may be embedded in a polytope and may be expressed in the form of (2). The corresponding vertices are given by :

$$A_1 = \begin{bmatrix} 0.5627 & 1 & 0 \\ 1 & 0 & 1 \\ -0.7 & 0 & 0.01 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0.8028 & 1 & 0 \\ 1 & 0 & 1 \\ -0.7 & 0 & 0.01 \end{bmatrix}$$

A one-dimensional information m_k (the plaintext) is embedded in the chaotic motion through u_k which results from an invertible coding function e. The plaintext consists of a sampled sine wave $m_k = M_m \sin(2\pi k \tilde{f})$ with $\tilde{f} = 0.08$.

In order to first recover u_k, the *receiver* is designed according to (22) and the Theorem 4. The gain Q is computed from (25) with a null arbitrary matrix Y. The gains L_i are computed from (27) using a standard LMI solver. Finally, the plaintext m_k is recovered by applying (28). Simulation results are presented on Fig. 2 and highlight the consistence of the theoretical developments.

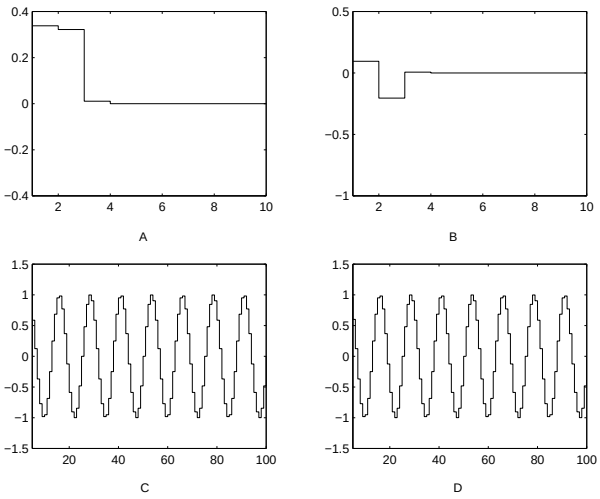

Figure 2: A : error $\|x_k - \hat{x}_k\|$. B : error $m_k - \hat{m}_k$. C : plaintext m_k. D : recovered plaintext $\hat{m}_k$

5.2 Real-time private communication experiment

A chaotic encryption experiment is conducted within a real-time video communication context. For that purpose, a well-known GNU licensed program for video transmission over Internet, *VIC*, has been chosen. A video tape is connected to a computer through the S-Video port of a *Miro Studio PCTV Rave*^{TM} card. Consequently, the video tape data are dynamically captured by the TV-Card and *VIC* manages the transmission protocol over Internet. The card has been configured to work under *Linux* and is driven by the *bttv* and *video4linux* drivers included in the *VIC* package. *VIC*'s default package contains an implementation of DES cryptographic algorithm. However, it also allows to introduce new cryptographic schemes. The encrypting scheme corresponding to the message-embedded framework developed in section 4 has been introduced. The well-known Second order Markov piecewise linear map has been considered as the chaos generator. It induces a chaotic behavior which is reckoned to get some good statistical properties for encryption purposes. Here, the key is the parameterization of the chaotic map. The design of the *transmitter-receiver* obeys the equations (21), (22) and Theorem 4.
With the same key in both sides, the video is correctly displayed in the receiver side. Using slightly different key parameters in both sides of the communication system, the image is badly decrypted which highlights the sensitivity of the algorithm to key parameters. Two capture screen are shown in Figure 3.

Figure 3: Decoder capture screen: matched and mismatched keys

6 Conclusion

Chaos synchronization has been tackled by considering the problem as a special case of an observer design. The general class of considered dynamical systems include in particular Lur'e systems, piecewise linear systems and output injection with time-varying dynamical matrix. Both message-free and message-embedded synchronization issues have been treated. Owing to the chaotic motions specific properties of keeping the underlying state variables in a compact domain, the dynamics can be written in a polytopic form. Hence, the synchronization can be carried out by designing respectively a polytopic observer or an unknown polytopic observer. Global synchronization is ensured by a special Lyapunov approach. The Lyapunov function is a parameter dependent Lyapunov function called poly-quadratic with a structure similar to that of the polytopic system description. The gains of the observer are computed by a systematic procedure involving the solutions of a Linear Matrix Inequalities set.

References

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

[2] Pecora L. M. and Carroll T. L. Driving systems with chaotic signals. *Phys. Rev. A*, 44(8):2374–2383, August 1991.

[3] V. D. Blondel, E. D. Sontag, M. Vidyasagar, and J. C. Willems. *Open Problems in Mathematical Systems and Control Theory.* Communication and Control Engineering. Springer Verlag, 1999.

[4] Blekhman I.I., Fradkov A.L., Nijmeijer H., and Pogromsky A.Y. On self-synchronization and controlled synchronization. *Systems and Control letters*, 31(5):299–305, 1997.

[5] Special Issue. Control of chaos and synchronization. *Syst. Control Letters*, 31:259–322, 1997.

[6] Special Issue. Chaos synchronization and control : theory and applications. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(10):853–1039, 1997.

[7] Special Issue. Control and synchronization of chaos. *International Journal of Bifurcation and Chaos*, 10(4), 2000.

[8] I.I. Blekhman E. Mosekilde, A.L. Fradkov, editor. *Special Issue on Chaos Synchronization and Control*, volume 58. elsevier, 2002.

[9] Sira ramirez H., Ibanez C. A., and Suarez-castanon. Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems. *International Journal of Bifurcation and Chaos*, 12(1):169–177, 2002.

[10] Itoh M., Wu C. W., and Chua L. O. Communications systems via chaotic signals from a reconstruction viewpoint. *International Journal of Bifurcation and Chaos*, 7(2):275–286, 1997.

[11] Takens F. *Detecting strange attractors in fluid turbulence.* Dynamical systems and turbulences. D. Rand and L. S. Young, editors, Springer-Verlag, Berlin, 1981.

[12] Nijmeijer H. and Mareels I. M. Y. An observer looks at synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44:882–890, October 1997.

[13] Huijberts H. J. C., Lilge T., and Nijmeijer H. Nonlinear discrete-time synchronization via extended observers. *International Journal of Bifurcation and Chaos*, 11(7):1997–2006, 2001.

[14] Pogromsky A. and Nijmeijer H. Observer-based robust synchronization of dynamical systems. *International Journal of Bifurcation and Chaos*, 8(11):2243–2254, 1998.

[15] Sira ramirez H. and Cruz hernandez C. Synchronization of chaotic systems :a generalized hamiltonian approach. *International Journal of Bifurcation and Chaos*, 11(5):1381–1395, 2001.

[16] G. Millerioux and J. Daafouz. Global chaos synchronization and robust filtering in noisy context. *IEEE Trans. on Circuits and Systems I: Fundamental Theory and applications*, 48(10):1170–1176, October 2001.

[17] G. Millerioux and J. Daafouz. Polytopic observer for global synchronization of systems with output measurable nonlinearities. *International Journal of Bifurcation and Chaos*, 13(3):703–712, March 2003.

[18] L. Kocarev. Chaos-based cryptography :a brief overview. *IEEE Circuits and Systems Magazine*, 1(3):6–21, 2001.

[19] Jakimoski G. and Kocarev L. Chaos and cryptography :block encryption ciphers based on chaotic maps. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 48(2):163–169, February 2001.

[20] M. J. Ogorzalek. Taming chaos - part I: synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 40(10):693–699, 1993.

[21] M. Hasler. Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, 8(4), April 1998.

[22] T. Yang. A survey of chaotic secure communication systems. *Int. J. of Computational Cognition*, 2004. (available at `http://www.YangSky.com/yangijcc.htm`).

[23] J. Daafouz and J. Bernussou. Parameter dependent lyapunov functions for discrete time systems with time varying parametric uncertainties. *Systems and Control Letters*, 43:355–359, 2001.

[24] J. Daafouz and G. Millerioux. Poly-quadratic stability and global chaos synchronization of discrete time hybrid systems. *Special Issue of Mathematics and Computers in Simulation*, 58:295–307, March 2002.

[25] J.S. Shamma and M. Athans. Analysis of gain scheduled control for nonlinear plants. *IEEE Trans. Autom. Contr.*, 35:898–907, 1990.

[26] W.J. Rugh. Analytical framework for gain scheduling. *IEEE Contr. Sys. Mag.*, 11(1):74–84, 1991.

[27] J.S. Shamma and M. Athans. Guaranteed properties of gain scheduled control for linear parameter varying plants. *Automatica*, 27:559–564, 1991.

[28] F. Wu. An unified framework for lpv system analysis and control synthesis. In *Proceedings of IEEE Conference on Decision and Control*, Sydney, Australia, December 2000.

[29] G. Becker. Additional results on parameter-dependent controllers for lpv systems. In *Proc. of IFAC World Congress*, San fransisco, 1996.

[30] P. Gahinet, P. Apkarian, and M. Chilali. Affine parameter dependent lyapunov functions and real parametric uncertainty. *IEEE Trans. on Automatic Control*, 41:436–442, 1996.

[31] J. Daafouz, G. Millerioux, and C. Iung. A poly-quadratic stability based approach for switched systems. *International Journal of Control*, 75:1302–1310, November 2002.

[32] G. Millerioux and J. Daafouz. An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, pages 1270–1279, October 2003.

[33] J. Daafouz, P. Riedinger, and C. Iung. Stability analysis and control synthesis for switched systems : A switched lyapunov approach. *IEEE Transactions on Automatic Control*, November 2002.

[34] Huijberts H. J. C. and Nijmeijer H. An observer view on synchronization. In Springer Verlag, editor, *Nonlinear Control in the year 2000*, pages 509–520. Isidori A. and Lamnabhi-Laguarrigue F. and Respondek W., 2000.

[35] Liao T-L. and Huang N-S. An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 46(9):1144–1150, 1999.

[36] De angeli A., Genesio R., and Tesi A. Dead-beat chaos synchronization in discrete-time systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 42(1):54–56, 1995.

[37] K-Y Lian, T-S Chiang, and P. Liu. Discrete-time chaotic systems : applications in secure communications. *International Journal of Bifurcation and Chaos*, 10(9):2193–2206, 2000.

[38] H. Zhou and X-T. Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(3):268–271, March 1997.

[39] G. Millerioux and J. Daafouz. Unknown input observers for message-embedded chaos synchronization of discrete-time systems. *International Journal of Bifurcation and Chaos*, 14(4):1357–1368, April 2004.

[40] M. Darouach, M. Zazadinski, and S. J. Xu. Full-order observers for linear systems with unknown inputs. *IEEE Trans. on Automatic Control*, 39(3):606–609, March 1994.

[41] S-K. Chang, W-T. You, and P-L. Hsu. Design of general structured observers for linear systems with unknown inputs. *J. Franklin Inst.*, 334(2):213–232, 1997.

[42] F. Yang and R. W. Wilde. Observers for linear systems with unknown inputs. *IEEE Trans. on Automatic Control*, 33(7):677–681, July 1988.

[43] Y. Guan and M. Saif. A novel approach to the design of unknown input observers. *IEEE Trans. on Automatic Control*, 36(5):632–635, May 1991.

[44] S. H. Lee, J. Kong, and J. H. Seo. Observers for bilinear systems with unknown inputs and application to superheater temperature control. *Control Eng. Practice*, 5(4):493–506, 1997.

[45] Chen, editor. *Controlling Chaos and Bifurcations in Engineering Systems.* CRC Press, 1999.