MULTIPLE SECURE COMMUNICATION BASED ON CHAOS

G. Zheng * **D. Boutat** ** **J-P. Barbot** * **T. Floquet** ***

* *Equipe Commande des Systèmes (ECS), ENSEA, 6 Av. du Ponceau, 95014 Cergy.*
** *LVR, ENSI-Bourges/Université d'Orléans, 10, Bd. Lahitolle, 18020 Bourge.*
*** *LAGIS UMR CNRS 8146, Ecole Centrale de Lille, BP 48, Cité Scientifique, 59651 Villeneuve-d'Ascq.*

Abstract: This paper deals with the design of a multiple secure communication system based on chaos. And its main idea is to use the left inversion theory. A simple example for a given 4D-chaotic system is presented to highlight the proposed method.

Keywords: Chaotic Synchronization, Left invertibility, Secure Communication, Observability Bifurcation

1. INTRODUCTION

Since chaotic system is extremely sensitive to its initial conditions and parameters, its application to secure communication has provoked a great deal of interests, especially after Carroll and Pecora's outstanding work on successfully synchronizing two chaotic systems (Pecora et *al.*, 1990).

Till now, most chaos-based communication systems are based on chaotic synchronization technique, where the receiver system tries to synchronize the transmitter system by a signal transmitted through a public channel. Actually, this synchronization can be studied as an observer design problem, since the work of H. Nijmeijer and I. Mareels in (Nijmeijer et *al.*, 1997).

After synchronization, the confidential message can be recovered differently according to the type of protocol (or algorithm) which is used to encode the confidential message. Generally secure communications by chaos can be divided into four basic protocols: chaotic masking (Kovarev et *al.*, 1992), chaotic switching (Parlitz et *al.*, 1992), chaotic modulation (Wu et *al.*, 1993) and inverse system approach (Feldmanne et *al.*, 1996).

However, these basic secure communication systems based on chaos only focus on encrypting a single input (or message), and it can be called single secure communication system. In this paper, we propose a method to establish a multiple secure communication system based on chaos. A simple example is given in order to illustrate the proposed method.

The paper is organized as follows. In section 2, a brief presentation of the problem and the main goal of our work are given. In section 3, we show how to design a multiple secure communication system based on a given chaotic system. An illustrative example that highlights the proposed methods is given in section 4.

2. PROBLEM STATEMENT

As far as we know, most proposed methods based on chaos for secure communication application do not involve the direct multiple inputs due to

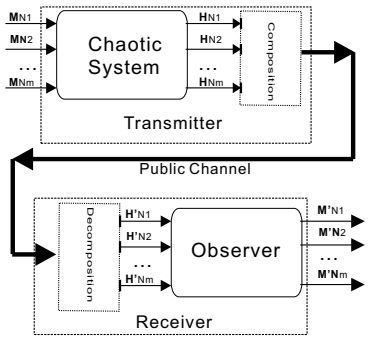

Fig. 1. Scheme for multiple secure communication system

the basic knowledge that a signal input secure communication system can be easily extended into a multiple one by composition technologies (such as time division multiplexing, frequency modulation, code division multiplexing and so on) in order to convert the multiple inputs into a single one. This is a very convenient and economic means, but the drawback of this kind of scheme is that all the inputs share the same risk to be broken. In fact, some of the proposed secure communication systems based on chaos have been broken (Pérez et *al.*, 1995), (Short et *al.*, 1994), (Yang et *al.*, 1998).

How to disperse the risk? An intuitive solution would be not to apply the composition directly to the multiple inputs. Under this consideration, we propose a new scheme, in which, for the transmitter system, the composition is used to combine the multiple outputs of the transmitter system, instead of combining the multiple inputs directly. For the receiver system, an observer-based approach to solve the left invertible problem is applied. This scheme can then be seen as a version for multi-input multi-output system of the traditional inverse system approach proposed in (Feldmanne et *al.*, 1996). Fig. 1 is the basic diagram for this consideration. According to this scheme, the multiple inputs possess different risks to be broken, i.e., even if message M_{N1} in Fig. 1, for example, has been broken, the others still remain unbroken. However, one of the main problems for this scheme is that it is impossible to establish a transmitter that contains all the inputs when the number of inputs is huge enough. This means that it is difficult to distribute every user a private channel. Of course, it is also not economic, which forces us to go back to the single input system. But why not divide the uses into several groups according to different requirements or emergent levels? In this case, different groups (M_{N1}, M_{N2},..., M_{Nm} in Fig. 1) have different security degrees, and all users in the same group share the same possibility to be broken because they are combined as a single input. This idea is just like the concept QoS (Quality of Service) in Network.

Consequently, our problem statement is: Given a chaotic system, is it possible or not to establish a multiple secure communication system?

This problem will be solved from the viewpoint of nonlinear control theory. Then a simple secure communication system based on a 4D chaotic system is constructed in order to illustrate the proposed method.

3. MULTIPLE SECURE COMMUNICATION SYSTEM

Let us consider a n-dimensional chaotic system which can be represented in a more generic form as follows:

$$\dot{x} = f(x, p) \tag{1}$$

where U is an open set of R^n, $x \in U$ is the state vector, $p \in R^k$ represents the parameter vector and $f : R^n \times R^k \to R^n$ is analytic.

With system (1), the aim is to establish a multiple secure communication system which can be represented in the following form:

$$\begin{cases} \dot{x} = f(x, p) + \sum_{i=1}^{m} g_i(x, p)\, u_i \\ y = [h_1(x), ..., h_p(x)]^T \end{cases} \tag{2}$$

where x, p, and the vector field f have been defined in equation (1). $y \in R^p$ is the output vector and $u \in R^m$ represents the confidential information to be transmitted. The vector fields $g_i = [g_{i1}, \ldots, g_{im}]^T$ and $h = [h_1, \ldots, h_p]^T$ are assumed to be sufficiently smooth on U, where $f_i, h_j \in R$ and $g_k \in R^n$, $i \in [1, n]$, $j \in [1, p]$, $k \in [1, m]$,. Without loss of generality, it is assumed that, for all $x \in U$, the distribution $span\{g_1, \ldots, g_m\}$ and the codistribution $span\{dh_1, \ldots, dh_p\}$ are nonsingular.

Definition 1. The vector relative degree ρ of system (2) is defined by $\rho = \{\rho_1, ..., \rho_p\}$, where $\rho_i = \min\{s \text{ such that } L_{g_k} L_f^{s-1} h_i \neq 0 \text{ for } k = 1 : m\}$, $i = 1 : p$.

Definition 2. (Isidori 1989, Chapter 5) System (2) in the case of $p = m$ has a strong relative degree $\{r_1, ..., r_m\}$ at point x_0 if

i) $L_{g_j} L_f^k h_i = 0$, for all $1 \leq j \leq m, 1 \leq i \leq m, k < r_i - 1$, for all x in a neighborhood of x_0,

ii) the $m \times m$ matrix

$$\Gamma(x) = \begin{bmatrix} L_{g_1} L_f^{r_1 - 1} h_1(x) & \cdots & L_{g_m} L_f^{r_1 - 1} h_1(x) \\ \vdots & \ddots & \vdots \\ L_{g_1} L_f^{r_m - 1} h_m(x) & \cdots & L_{g_m} L_f^{r_m - 1} h_m(x) \end{bmatrix}$$

is nonsingular at $x = x_0$.

In system (2), the number of the output is exactly equal to that of the input. In this case, the so-called Observability Matching Condition in (Perruquetti 2000, Chapter 4) is equivalent to the following theorem.

Theorem 1. If system (2) has a strong relative degree $r = r_1 + \ldots + r_m = n$, all the states and all the unknown inputs can be recovered.

In (Isidori 1989, Chapter 5), sufficient and necessary conditions ensuring the existence of outputs (and how they can be constructed) such that the strong relative degree of the system is $r = n$ are given. From this, a multiple secure communication system can be established easily. However, this method does not lead to an enough complexity of computation of decryption. Therefore in order to improve the security, the complexity is increased by choosing outputs such that $r < n$. Even in this case, it will be shown that it is also possible to reconstruct all unknown messages, provided that this system satisfies some special conditions.

Here the left invertibility algorithm given in (Barbot et *al.*, 2005) is recalled. It is assumed that $p \geq m$, and that the system (2) has a vector relative degree $\rho = \{\rho_1, ..., \rho_p\}$. It should be noted that in this paper we do not consider the case of infinite relative degree. Let us define the following sets that will be used in the sequel:

- Φ is the codistribution spanned by the time derivatives of the measured the outputs affected by the inputs:
  $$\Phi = span\{dh_1, ..., dL_f^{\rho_1 - 1}h_1, ..., dL_f^{\rho_p - 1}h_p\}$$
- Ω is a basis of Φ:
  $\Omega = \{dh_1, ..., dL_f^{r_1 - 1}h_1, ..., dh_p, ..., dL_f^{r_p - 1}h_p\}$
  and $\mathcal{L}$ is the related distribution:
  $\mathcal{L} = span\{h_1, ..., L_f^{r_1 - 1}h_1, ..., h_p, ..., L_f^{r_p - 1}h_p\}$
  where $r = \dim \Omega = \sum_{i=1}^{p} r_i$.
- $\Omega_{\mathcal{L}}$ is the module spanned by Ω over $\mathcal{L}$, and $\Omega^1_{\mathcal{L}}$ is the submodule spanned by
  $$\{dh_1, ..., dL_f^{r_1 - 2}h_1, ..., dh_p, ..., dL_f^{r_p - 2}h_p\}$$
  over $\mathcal{L}$ where $L_f^{-1}h_j = 0$ and $L_f^0 h_j = h_j$.
- G is the smallest involutive distribution that contains $\{g_1(x), ..., g_m(x)\}$. Note $k = dim G$, $m \leq k \leq n$.
- $G^{\perp}$ is the annihilator of G:
  $G^{\perp} = span\{\alpha_1, ..., \alpha_{n-k}\}$, where the α_i are one-forms such that for all $\lambda \in G$, $l_\lambda \alpha_i = 0$ for $i = 1 : n - k$, where $l_\lambda \alpha = \alpha(\lambda)$ is the inner product of the vector field λ and α.

Assume $r < n$. There exists a transformation $(\xi, \eta) = \phi(x)$ such that the system (2) can be locally transformed into the following normal form:

$$\begin{cases} \dot{\xi}^i_1 = \xi^i_2 \\ \vdots \\ \dot{\xi}^i_{r_i - 1} = \xi^i_{r_i} \\ \dot{\xi}^i_{r_i} = L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i - 1} h_i(x) u_j \\ \dot{\eta} = p(\xi, \eta) + q(\xi, \eta) u \\ y_i = \xi^i_1 \end{cases} \tag{3}$$

where

$$\xi = \left[\xi^1 \ \cdots \ \xi^p \right]^T$$

and

$$\xi^i = \begin{bmatrix} \xi^i_1 \\ \vdots \\ \xi^i_{r_i} \end{bmatrix} = \begin{bmatrix} h_i(x) \\ \vdots \\ L_f^{r_i - 1} h_i(x) \end{bmatrix}, \text{ for } i \in [1, p].$$

If $r < n$ and if the distribution $span\{g_1, \ldots, g_m\}$ is not involutive, u can not be obtained using classical observation algorithm. In (Barbot et *al.*, 2005), the authors provide an algorithm that, under sufficient conditions, allows for the recovery of both the state and the unknown inputs in finite time. The main idea of this algorithm is to find extra information through functions of the outputs and their time derivatives. Let us define:

$$V = \left[L_f^{r_1} h_1(x) \ \cdots \ L_f^{r_p} h_p(x) \right]^T + \Gamma(x) u \tag{4}$$

$$= \left[y_1^{(r_1)} \ \cdots \ y_p^{(r_p)} \right]^T \tag{5}$$

that can be known using the normal form (3). Assume there exist $1 \times p$ vector functions $K(x) = [k_1(x), ..., k_p(x)] \in \mathcal{L}(x)$, with $K(x) \neq 0$ such that

$$K\Gamma = 0 \tag{6}$$

and define a dummy output as follows:

$$\bar{y} = \bar{h}(x) = KV = \sum_{i=1}^{p} k_i(x) L_f^{r_i} h_i(x).$$

If $\bar{y} \notin \mathcal{L}(x)$, it can be considered as a suitable fictitious output in order to estimate more states [1]. Set $y \triangleq \left[y, \bar{y} \right]^T$. The system has a new vector relative degree with respect to this output. If $r = n$ (with this new y), it has been shown in (Barbot et *al.*, 2005) that both the state x and the unknown inputs u can be estimated in finite time.

The following proposition gives some equivalent conditions that guarantee the existence of a solution to equation (6) and thus, the existence of a proper fictitious output.

[1] It should be noticed that there may exist a submanifold of singularity $S = \{x \in U \text{ such that } \bar{h}(x) \in \mathcal{L}(x)\}$.

Proposition 1. (Barbot et *al.*, 2005) The following conditions are equivalent:

i) Equation (6) has a non trivial solution $K(x)$, and $\bar{y} = KV \notin \pounds(x)$.

ii) the set of equivalence classes $E = \frac{G^{\perp} \cap \Omega_{\pounds}}{G^{\perp} \cap \Omega^{1}_{\pounds}}$ of elements of $G^{\perp} \cap \Omega_{\pounds}$ modulo $G^{\perp} \cap \Omega^{1}_{\pounds}$ is such that $E \neq \varnothing$,

iii) $\Xi = \{\alpha \in G^{\perp} \cap \Omega_{\pounds}$ such that $l_f \alpha \notin \pounds\} \neq \varnothing$.

3.1 Example for Multiple Secure Communication

In this section, in order to highlight the proposed method, we will use a 4D chaotic system to construct a simple multiple secure communication system. A sliding mode observer to synchronize the transmitter and the receiver will be designed.

3.1.1. Qi's Chaotic System This 4D autonomous system proposed by Qi in (Qi et *al.*, 2005), is described as follows:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -dx_4 + x_1 x_2 x_3 \end{cases} \tag{7}$$

where $x_i (i = 1, 2, 3, 4)$ are the state variables, and a, b, c, d are all positive real constant parameters.

In (Qi et *al.*, 2005), this 4D dynamic system has been exhaustively analyzed. Here we just introduce some basic characteristics of this system. Firstly, in order to ensure the dissipativity of the system, the parameters should satisfy:

$$b - (a + c + d) < 0 \tag{8}$$

Under this condition, the behavior of system (7) could be analyzed according to different choices of the parameters:

Set $a = 35,\ b = 10,\ c = 1$. If $d \in (0, 21.88]$, system (7) is chaotic with a positive Lyapunov exponent. If $d \in (21.88, 26.8]$, system (7) has a periodic attractor. If $d \in (26.8, 33]$, system (7) becomes chaotic again. It should be noticed that at this time, this strange attractor is quite different from the previous one. When d varies in $(33, 36.5]$, system (7) evolves to a limit cycle. Finally, when $d > 36.5$, the system's attractor is a fixed point.

3.1.2. Example In order to improve the security, the main interest of the procedure with several outputs is to have the problem of left invertibility with fictitious outputs $\bar{y}$. Furthermore, parts of the private key are in $\bar{y}$ and the singular manifolds. As argued in section 3, even if the system's strong relative degree is less than its dimension, it is possible to recover all the states and the confidential messages. In order to illustrate this case, we consider the following transmitter which is based on the chaotic system (7):

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 + m_1 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_3 + x_1 x_2 x_4 + x_3 m_2 \\ \dot{x}_4 = -dx_4 + x_1 x_2 x_3 - x_4 m_2 \end{cases} \tag{9}$$

where $g_1 = [\,1\ 0\ 0\ 0\,]^T$ and $g_2 = [\,0\ 0\ x_3\ -x_4\,]^T$. It is assumed that m_1 and m_2 are small, that $m_2 > 0$, and that the following condition is satisfied

$$m_2 + d - c > 0. \tag{10}$$

Suppose that the outputs are set as $y = \begin{pmatrix} x_1 & x_2 \end{pmatrix}^T$, a straightforward calculation shows that the strong relative degree of the system is $r = 3$. So following the lines of the algorithm proposed in (Barbot et *al.*, 2005), let us calculate

$$\Gamma = \begin{pmatrix} L_{g_1} h_1 & L_{g_2} h_1 \\ L_{g_1} L_f h_2 & L_{g_2} L_f h_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b - x_3 x_4 & 0 \end{pmatrix}.$$

One can choose $K = \begin{pmatrix} b - x_3 x_4, & -1 \end{pmatrix}$such that $K\Gamma = 0$.

Set

$$\pounds(x) = span\{h_1, h_2, L_f h_2\}$$

Since

$$L_f h_2 = b(x_1 + x_2) - x_1 x_3 x_4 = x_3 x_4 mod\{x_1, x_2\}$$

one has $\pounds(x) = span\{x_1, x_2, x_3 x_4\}$.Then the following fictitious output can be defined:

$$\begin{aligned} \bar{y} &= K \begin{bmatrix} L_f h_1 \\ L_f^2 h_2 \end{bmatrix} = (b - x_3 x_4)\, \dot{y}_1 - \ddot{y}_2 \\ &= \left(x_3^2 + x_4^2\right) mod \pounds(x) \end{aligned}$$

because $\bar{y} \notin \pounds(x)$. Thus, item i) of Proposition 1 is satisfied. Then, let us set

$$y \triangleq \left[\, x_1,\ x_2,\ x_3^2 + x_4^2 \,\right]^T.$$

With this new output y, the dimension of the set $\Phi = span\{dx_1, dx_2, dx_3 x_4, d\left(x_3^2 + x_4^2\right)\}$ is equal to 4. This means that one can recover all the state in finite time. A straightforward consequence is the fact that $span\{g_1, g_2\}$ is regular, which implies that the unknown messages can also be reconstructed in finite time. For this, let us design a sliding mode observer as follows:

$$\begin{cases} \dot{\hat{x}}_1 = a\left(x_2 - x_1\right) + x_2 \tilde{x}_3 \tilde{x}_4 + E_1 \lambda_1 sign(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = b(x_1 + x_2) + \lambda_2 sign(x_2 - \hat{x}_2) \\ \dfrac{d\left(\hat{x}_3 \hat{x}_4\right)}{dt} = -\left(c + d\right) \tilde{x}_3 \tilde{x}_4 \\ \qquad\qquad + E_2 \lambda_3 sign(\tilde{x}_3 \tilde{x}_4 - \hat{x}_3 \hat{x}_4) \\ \dfrac{d\left(\hat{x}_3^2 + \hat{x}_4^2\right)}{dt} = -2c\tilde{x}_3^2 - 2d\tilde{x}_4^2 + 4x_1 x_2 \tilde{x}_3 \tilde{x}_4 \\ \qquad\qquad + 2E_3 \lambda_4 sign\left(\left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right) \end{cases} \tag{11}$$

with

$$E_1 = \begin{cases} 1 \ x_2 = \hat{x}_2 \\ 0 \text{ otherwise} \end{cases}$$
$$E_2 = \begin{cases} 1 \text{ if } E_1 = 1 \text{ and } x_1 = \hat{x}_1 \\ 0 \text{ otherwise} \end{cases}$$
$$E_3 = \begin{cases} 1 \text{ if } E_2 = 1 \text{ and } \tilde{x}_3\tilde{x}_4 = \hat{x}_3\hat{x}_4 \\ 0 \text{ otherwise} \end{cases}$$
$$E_3 = \begin{cases} 1 \text{ if } E_3 = 1 \text{ and } \tilde{x}_3^2 + \tilde{x}_4^2 = \hat{x}_3^2 + \hat{x}_4^2 \\ 0 \text{ otherwise} \end{cases}$$

and with the auxiliary states

$$\tilde{x}_3\tilde{x}_4 = -\frac{\lambda_2 sign(x_2 - \hat{x}_2)}{x_1}$$
$$\tilde{x}_3^2 + \tilde{x}_4^2 = \frac{E_2\lambda_3 sign(\tilde{x}_3\tilde{x}_4 - \hat{x}_3\hat{x}_4)}{x_1x_2}.$$

Let us also define

$$\tilde{m}_1 = E_2\lambda_1 sign(x_1 - \hat{x}_1)$$
$$\tilde{m}_2 = \frac{E_4\lambda_4 sign\left(\left(\ \tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right)}{\tilde{x}_3^2 - \tilde{x}_4^2}.$$

The error dynamics is defined by $e_i = x_i - \hat{x}_i$. One has:

$$\dot{e}_2 = -x_1x_3x_4 - \lambda_2 sign(x_2 - \hat{x}_2).$$

Select $v = \frac{1}{2}e_2^2$, then one gets

$$\begin{aligned} \dot{v} &= e_2\dot{e}_2 \\ &= e_2\left(-x_1x_3x_4 - \lambda_2 sign(e_2)\right) \end{aligned}$$

The states are bounded. So, choosing $\lambda_2 > \left|-x_1x_3x_4\right|_{\max}$, one has $\dot{v} < 0$. Then a sliding motion appears after a finite time t_1 on $e_2 = 0$. Writing that $\dot{e}_2 = 0$ gives :

$$-x_1x_3x_4 = \lambda_2 sign(e_2).$$

Then

$$\tilde{x}_3\tilde{x}_4 = -\frac{\lambda_2 sign(e_2)}{x_1} = x_3x_4$$

and $E_1 = 1$. One also has:

$$\dot{e}_1 = m_1 - E_1\lambda_1 sign(e_1)$$

For the same reasons, if $\lambda_1 > \max\{m_1\}$, there exists t_2, such that $e_1 = \dot{e}_1 = 0$, for $t > t_2 > t_1$. Then:

$$m_1 - \lambda_1 sign(e_1) = 0$$

and $E_2 = 1$, which gives

$$\tilde{m}_1 = E_2\lambda_1 sign(e_1) = m_1.$$

From system (9), it can be computed that:

$$\frac{d\left(x_3x_4\right)}{dt} = -\left(c + d\right)x_3x_4 + x_1x_2\left(x_3^2 + x_4^2\right)$$

and

$$\begin{aligned} \frac{d\left(x_3^2 + x_4^2\right)}{dt} &= -2cx_3^2 - 2dx_4^2 + 4x_1x_2x_3x_4 \\ &\quad +2\left(x_3^2 - x_4^2\right)m_2. \end{aligned} \tag{12}$$

Set $e_{34} = x_3x_4 - \hat{x}_3\hat{x}_4$. Its dynamics is given by:

$$\dot{e}_{34} = x_1x_2\left(x_3^2 + x_4^2\right) - E_2\lambda_3 sign(e_{34})$$

So after a finite time t_3, $e_{34} = \dot{e}_{34} = 0$, if $\lambda_3 > \left|x_1x_2\left(x_3^2 + x_4^2\right)\right|_{\max}$. One obtains

$$x_1x_2\left(x_3^2 + x_4^2\right) - \lambda_3 sign(e_{34}) = 0$$

and this gives

$$\tilde{x}_3^2 + \tilde{x}_4^2 = \frac{E_2\lambda_3 sign(\tilde{x}_3\tilde{x}_4 - \hat{x}_3\hat{x}_4)}{x_1x_2} = x_3^2 + x_4^2.$$

Define

$$\tilde{x}_3\tilde{x}_4 = A$$
$$\tilde{x}_3^2 + \tilde{x}_4^2 = B$$

There are two groups of solutions:

$$S_1 : \begin{cases} \tilde{x}_{3_1}^2 = \dfrac{B + \sqrt{B^2 - 4A^2}}{2} \\ \tilde{x}_{4_1}^2 = \dfrac{B - \sqrt{B^2 - 4A^2}}{2} \end{cases}$$
and
$$S_2 : \begin{cases} \tilde{x}_{3_2}^2 = \dfrac{B - \sqrt{B^2 - 4A^2}}{2} \\ \tilde{x}_{4_2}^2 = \dfrac{B + \sqrt{B^2 - 4A^2}}{2} \end{cases} \tag{13}$$

Suppose that S_1 is the correct solution. From (12), the confidential message can be recovered correctly as follows:

$$-c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)m_{2_1} = C. \tag{14}$$

In this case, one has for S_2:

$$-c\tilde{x}_{3_2}^2 - d\tilde{x}_{4_2}^2 + \left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right)m_{2_2} = C. \tag{15}$$

With equations (14) and (15), one has:

$$m_{2_2} = \frac{-c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)m_{2_1} + c\tilde{x}_{3_2}^2 + d\tilde{x}_{4_2}^2}{\left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right)} \tag{16}$$

Note that $\tilde{x}_{3_1}^2 = \tilde{x}_{4_2}^2$ and $\tilde{x}_{3_2}^2 = \tilde{x}_{4_1}^2$. Equation (16) becomes

$$\begin{aligned} m_{2_2} &= \frac{-c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)m_{2_1} + c\tilde{x}_{4_1}^2 + d\tilde{x}_{3_1}^2}{\left(\tilde{x}_{4_1}^2 - \tilde{x}_{3_1}^2\right)} \\ &= c - d - m_{2_1} \end{aligned}$$

According to equation (10), $m_{2_2} < 0$. Thus, m_{2_2} can not be a correct message because $m_2 > 0$. Following this way, the correct solution corresponding to $\tilde{x}_3^2$ and $\tilde{x}_4^2$ can be found.

Let us set $e_{3^2+4^2} = \left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)$. This gives:

$$\dot{e}_{3^2+4^2} = 2(x_3^2 - x_4^2)m_2 - 2E_3\lambda_4 sign\left(e_{3^2+4^2}\right)$$

Thus, tuning $\lambda_4 > \left|(x_3^2 + x_4^2)m_2\right|_{\max}$ ensures that $e_{3^2+4} = \dot{e}_{3^2+4^2} = 0$, after a finite time t_4, and:

$$(x_3^2 - x_4^2)m_2 - \lambda_4 sign\left(e_{3^2+4^2}\right) = 0$$

which gives

$$\tilde{m}_2 = \frac{E_4\lambda_4 sign\left(e_{3^2+4^2}\right)}{\tilde{x}_3^2 - \tilde{x}_4^2} = m_2.$$

Figure 2 exhibits the states of the transmitter and those of the receiver. Figure 3 illustrates the

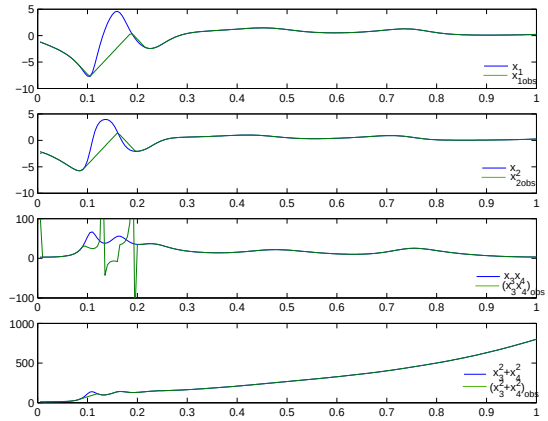

Fig. 2. States observation for transmitter and the receiver

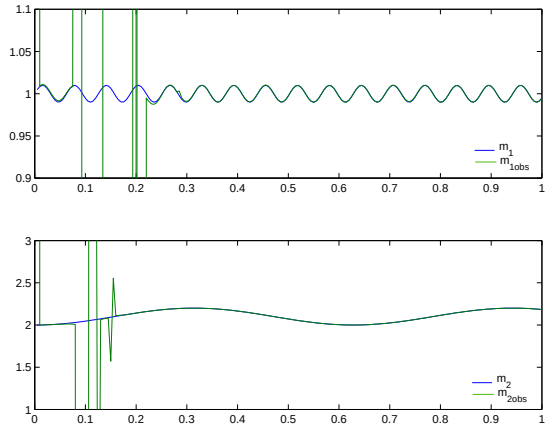

Fig. 3. Message observation for transmitter and the receiver

original messages and their estimation. Figure 2 shows that the states of the receiver converge fast to those of the transmitter. It can be seen in Figure 3 that, once the state is estimated, the confidential messages are well reconstructed.

4. CONCLUSION

This paper considered the drawback of a single input secure communication system based on chaos. Then a new multiple one has been proposed in order to disperse the risk of breaking. In addition, how to establish this type of multiple secure communication system has been illustrated. At the same time, a strategy about how to improve the security degree has been explained. Finally a simple example has been constructed under the guide of the proposed method.

REFERENCES

Qi G.Y., Du S.Z., Chen G.R. et al. On a four-dimensional chaotic system. *Chaos, Solitons and Fractals, 23(2005).*

Barbot J.P, Boutat D. and Floquet T. A new observation algorithm for nonlinear system with unknown inputs. *CDC-ECC, seville, Dec 2005.*

Perruquetti W. and Barbot J.P. Sliding Mode Control in Engineering. *M. Dekker, 2002.*

Pecora L. M. and Carroll T. L. Synchronization in chaotic systems. *Physical Review Letters 64, 821-824, 1990.*

Isidori A. Nonlinear control systems. *2nd edition, Springer-Verlag, 1989.*

Feldmanne U., Hasler M. and Schwarz W. Communication by chaotic signals: The inverse system approach. *Int. J. Cricuit Theory and Applications 24. 551-576,1996.*

Nijmeijer H. and Mareels I. M. Y. An observer looks at synchronization. *IEEE Trans. on Circuits and Systems-1: Fundamental theory and Applications, Vol 44, No 10, pp 882-891, 1997*

Barbot J.P., Belmouhoub I. and Boutat-Baddas L. Observability Normal Form. *In W. Kang et al., editior, LNCIS 295, New trends in nonlinear dynamics and control. Springer Verlag, 2003*

Kovarev L., Eckert K. S., Chua L. O. and Parlitz U. Experimental demonstration of secure communications via chaotic synchrionization. *Int. J. Bifurcation and Chaos 2, 709-713, 1992.*

Parlitz U., Chua L. O., Kocarev L. et al. Transmission of digital signals by chaotic synchronization. *Int. J. Bifurcation and Chaos 2, 973-977, 1992.*

Wu C. W. and Chua L. O. A simple way to synchronize chaotic systems with applications to secure communications systems. *Int. J. Bifurcation and Chaos 3, 1619-1627, 1993.*

Pérez G. and Cerdeira H. A. Extracting messages masked by chaos. *Physical Review Letters 74, 1970-1973, 1995.*

Short K. M. Steps toward unmasking secure communications. *Int. J. Bifurcation and Chaos 4, 959-977, 1994.*

Yang T., Yang L. B. et al. Breaking chaotic switching using generalized synchronization: Examples. *IEEE Trans. Circuits and Systems-I 45, 1062-1067, 1998.*