Secure Communication Based on Multi-input Multi-output Chaotic System with Large Message Amplitude

Gang Zheng, Driss Boutat, Thierry Floquet, Jean-Pierre Barbot

Secure Communication Based on Multi-input Multi-output Chaotic System with Large Message Amplitude

G. Zheng[a,1], D. Boutat[b], T. Floquet[c] and J.P. Barbot[d]

[a] *INRIA Rhône-Alpes, 655 avenue de l'Europe, 38334 St. Ismier Cedex, France.*

[b] *LVR/ENSI, 10 Boulevard de Lahitolle, 18020 Bourges, France.*

[c] *LAGIS UMR CNRS 8146, Ecole Centrale de Lille, BP 48, Cité Scientifique, 59651 Villeneuve-d'Ascq and Équipe Projet ALIEN, INRIA Lille - Nord Europe, France*

[d] *ECS/ENSEA, 6 Avenue du Ponceau, 95014 Cergy-Pontoise and Équipe Projet ALIEN, INRIA Lille - Nord Europe, France.*

1

Abstract

This paper deals with the problem of secure communication based on Multi-Input Multi-Output (MIMO) chaotic systems. Single input secure communication based on chaos can be easily extended to multiple ones by some combinations technologies, however all the combined inputs possess the same risk to be broken. In order to reduce this risk, a new secure communication scheme based on chaos with MIMO is discussed in this paper. Moreover, since the amplitude of messages in traditional schemes is limited because it would affect the quality of synchronization, the proposed scheme is also improved into an amplitude-independent one.

Key words: MIMO, Chaos, Observer, Synchronization, Left Invertibility Problem

1 Introduction

Over the past decade, synchronization of chaotic systems and its potential application to secure communication have received a lot of attentions since Pecora and Carrol proposed a method to synchronize two identical chaotic systems [19]. Up to now, many chaos-based secure communication systems

[1] Corresponding author. E-mail: gang.zheng@inrialpes.fr

have been proposed, which can be roughly classified into the following categories: chaotic masking (addition method) [14] , chaotic switching [18], chaotic modulation (inclusion method) [24], digital communication [7] and inverse system approach [9]. One can refer to [27] for a recent survey.

Although chaotic synchronization with a single input has been widely investigated, such as adaptive synchronization [8,12], feedback-control synchronization [16], impulsive synchronization [4,25] etc, the case of multi-input systems has not received a lot of attention. For multi-input systems, it is well-known that the problem becomes similar to the case of systems with a single input if multiplexing techniques before encoding the messages are used. Nevertheless, although multiplexing techniques appear to be a very convenient and economical means, the main drawback of this kind of scheme is that all the messages have the same risk to be broken [28,29]. Actually, it is known that some of the proposed secure communication systems based on chaos with single input have been broken [1,15,20,23,26]. In [28,29], MIMO systems were used in order to increase the robustness of chaos based secure communication schemes.

Another drawback of secure communication using synchronization of chaotic system is the limitation of the amplitude of the confidential messages. Usually, they have to be small enough in order to be masked by the chaotic signal (addition method) or in order to preserve the chaotic behavior (inclusion method). This constraint obviously limits the ratio of the transferred information with respect to the channel signal. This paper presents a scheme based on MIMO systems that allows to involve messages whose amplitudes are higher than the chaotic signals. This approach relies on observer design for MIMO systems [17] and is concerned with the left invertibility theory [22].

This paper is organized as follows: in Section 2, the problem statement is described. In Section 3, a new scheme, in which the amplitude of messages can be greatly increased with respect to the chaotic signals, is discussed. Section 4 is devoted to highlight the feasibility of the proposed scheme by an illustrative example.

2 Problem statement

As mentioned in the introduction, traditional methods suffer from two drawbacks: all the messages can be broken at the same time and their amplitudes are limited. Solutions can be brought by using MIMO systems.

2.1 How to decrease the risk to be broken?

In order to decrease the risk for the encoded messages to be broken at the same time, the following scheme can be derived. For the transmitter, the composition is used to combine the outputs, instead of combining directly the inputs. At the end of the receiver, an observer-based approach is applied in order to solve the left invertibility problem. This scheme can then be seen as a MIMO version of the traditional inverse system approach proposed in [9]. Fig. 1 is the basic diagram for this consideration.

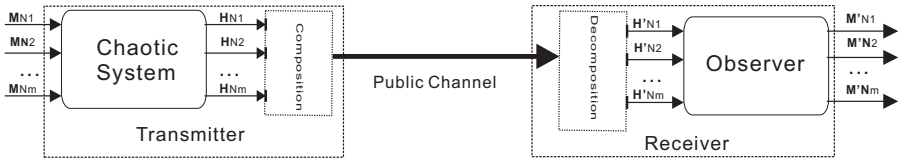

Fig. 1. Scheme for multiple secure communication system

According to this scheme, the multi-input possesses different risks to be broken, i.e., even if, for instance, the message M_{N_1} in Fig. 1 has been broken, the other ones still remain unbroken. Note that if it is impossible to establish a transmitter that contains all the inputs (sometimes the number of inputs is very large), the users can be divided into several groups according to different requirements or emergent levels. Under this case, different groups (M_{N1}, M_{N2},..., M_{Nm} in Fig. 1) have different degrees of security, and all users in the same group share the same probability to be broken since they are combined as a single input. This secure communication scheme based on chaos with MIMO was exhaustively described in [28], and was extended to systems with delays in [29].

2.2 How to increase the amplitude of messages?

This problem is the subject of this paper. In traditional schemes, the amplitude of the messages has to be smaller than that of the chaotic system's signal. For example, in the masking method, a fundamental requirement is that the spectrum of the chaotic scalar signal should be infinitely broad, flat, and of higher power density than that of the messages to be encoded. In other words, the message's power spectrum should be buried into that of the chaotic signal. Therefore, in order to maintain synchronization between the transmitter and the receiver, and to ensure that the chaotic signal masks the messages, the dynamic range of the messages has to be significantly smaller than that of the chaotic scalar. Moreover, the addition of a message signal to the chaotic scalar at the transmitter can degrade the quality of the synchronization between the transmitter and the receiver, and even result in the loss of synchronization if the amplitude of the messages is too large. In modulation schemes, the

amplitude of messages should also be smaller than that of the chaotic signal in order not to destroy the system chaotic behavior.

Actually, in traditional schemes, the limitation of the message amplitude comes from the fact that only one scalar signal is used to synchronize the transmitter and the receiver and that, simultaneously, this scalar signal is used to transmit the encoded message. That is why a trade-off has to be found. So if those two tasks can be split by using more signals (that means the number of outputs is strictly larger than that of inputs), the amplitude of the messages can be increased. In the next section, a new scheme based on MIMO systems is proposed to enable the transmission of multiple messages with large amplitude and the way to construct this type of system is detailed.

3 Scheme with large message amplitude

In traditional schemes, the functions of synchronization and encryption are realized using a single scalar signal. Here, the basic idea is to separate those functions using multiple signals so that the amplitude of the messages can be increased.

The following transmitter is designed (see Fig 2). It is composed of a chaotic system: $\Sigma_C \in R^{N_C}$, for the purpose of generating the chaotic signal, and a dynamical system (that could also be a chaotic one): $\Sigma_D \in R^{N_D}$, in order to encode the message. Both outputs of Σ_C and Σ_D can be used to design an observer.

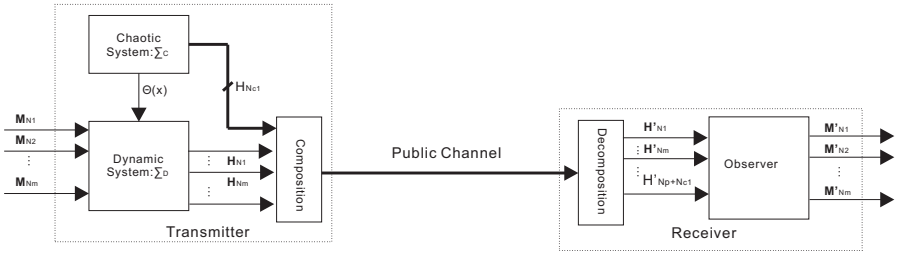

Fig. 2. Scheme based on combined subsystems concerning with message's amplitude

The main idea is that the inputs are firstly scrambled by a chosen dynamic system, and not by the chaotic system directly. Moreover, in order to take advantage of the characteristic of the chaotic system, Σ_D is driven by θ, some function of the state of Σ_C. According to Fig. 2, the task of synchronization is achieved by $H_{Nc1} \in R^{N_{C1}} \subset R^{N_C}$, the output of Σ_C. The output of Σ_D, $(H_{N1}, .., H_{Np})^T \in R^{N_{DO}} \subset R^{N_D}$, is used to transmit the encoded messages. In such a way, the amplitude of the messages can be greatly increased. Obviously, the single input single output version of such a scheme is exactly the same as

the one stated in [25], in which the authors used the impulsive samples of Σ_C, instead of H_{Nc1}, to achieve the synchronization.

In order to increase the security, the scheme is modified as follows (see Fig. 3). H_{Nc1} is recovered from the output of Σ_D instead of being transmited directly to the receiver. For this, at least N_{C1} signals are added to the output of Σ_D in order to recover the synchronization signal for Σ_C. Consequently, the number of outputs N_{DO} of the dynamical system Σ_D in the scheme given in the Figure 3 has to be greater than or equal to $(N_m + N_{C1})$. Moreover, since the chaotic system is not a function of the unknown inputs (the messages to be encoded), the systems Σ_C and Σ_D can be coupled via a function ϕ which depends on a part of the state of Σ_D and which is small enough in order not to break the chaotic behavior of system Σ_C. In this scheme, only the outputs of Σ_D are used to design an observer.

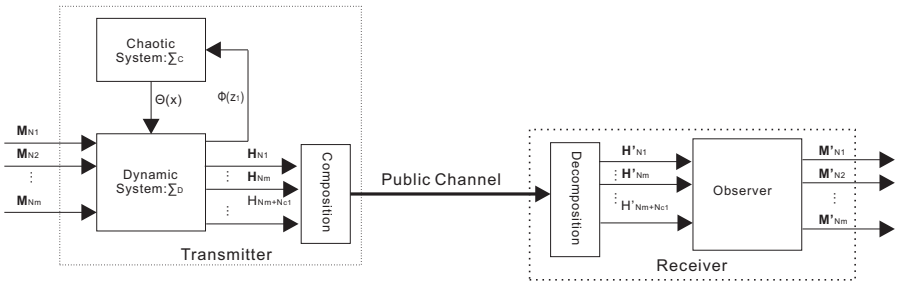

Fig. 3. Improved scheme based on combined subsystems concerning with message's amplitude

According to this scheme, the transmitter system can be described as follows:

$$\Sigma_C : \{\dot{x} = f_C(x, \phi(z_1))$$
$$\Sigma_D : \begin{cases} \dot{z} = \begin{bmatrix} \dot{z}_1 \\ \dot{z}_2 \end{bmatrix} = f_D(z, \theta(x)) + \sum_{i=1}^{N_m} g_i(z, \theta(x)) m_i \\ = \begin{bmatrix} f_{D_1}(z, \theta(x)) \\ f_{D_2}(z, \theta(x)) \end{bmatrix} + \begin{bmatrix} \sum_{i=1}^{N_m} g_{i_1}(z, \theta(x)) m_i \\ \sum_{i=1}^{N_m} g_{i_2}(z, \theta(x)) m_i \end{bmatrix} \\ y_D = h_D(z) \end{cases} \quad (1)$$

where $x \in R^{N_C}$ and $z = \left[z_1^T, z_2^T\right]^T \in R^{N_D}$ ($z_1 \in R^{N_{D1}}$ and $z_2 \in R^{N_{D2}}$) are the state vectors of the system Σ_C and Σ_D, respectively. $m = \begin{bmatrix} m_1 \cdots m_{N_m} \end{bmatrix}^T \in R^{N_m}$ are the messages to be encoded, and $\phi(z_1) \in R^{N_\phi} \subset R^{N_{D1}}$, $\theta(x) \in R^{N_\theta} \subset R^{N_C}$. It is assumed that the functions $f_C : R^{N_C} \times R^{N_\phi} \to R^{N_C}$, $f_{D_1} : R^{N_D} \times R^{N_\theta} \to R^{N_{D1}}$, $f_{D_2} : R^{N_D} \times R^{N_\theta} \to R^{N_{D2}}$, $g_{i_1} \in R^{N_D} \times R^{N_\theta} \to R^{N_{D1}}$, $g_{i_2} \in R^{N_D} \times R^{N_\theta} \to R^{N_{D2}}$, and $h_D : R^{N_D} \to R^{N_{DO}}$ are analytic.

In order to be able to reconstruct the messages, the following hypothesis is needed:

Hypothesis 1 *A transmitter in the form (1) can be designed such that the left invertibility problem can be solved, i.e. an observer corresponding to the designed transmitter can be implemented.*

This hypothesis can be guaranteed by an appropriate choice of the functions f_D, f_C and g. In [2], an algorithm for finite time state estimation and left invertibility of nonlinear systems has been proposed and sufficient conditions have been discussed. This constructive algorithm can be used to choose the functions f_D, f_C and g. Then, both the states and the unknown inputs can be recovered via finite time observers, such as, for instance, algebraic based observers [3] or step-by-step sliding mode observers [10,11]. In this scheme, z_1 can be recovered directly from the measurements y_D without the knowledge of m. Therefore, it is possible to estimate all the states of Σ_C with the knowledge of the inputs z_1. After that, for the system Σ_D, using y_D and the known inputs $\theta(x)$, it is also possible to reconstruct all the remaining states and the unknown input m. The details of the observer design is not discussed here but a step-by-step sliding mode observer is fully described in the example given in the following section.

4 Illustrative example

In this section, two messages with great amplitudes are encoded using the well-known Chua's circuit (as a chaotic oscillator) coupled with an arbitrary dynamical system. Based on the Chua's oscillator [5], the subsystem Σ_C can be designed as follows:

$$\Sigma_C : \dot{x} = \begin{bmatrix} -\alpha\left(x_1 - x_2 - \bar{f}(x_1)\right) \\ x_1 - x_2 + x_3 \\ -\beta x_2 - \gamma x_3 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \rho z_3 \end{bmatrix} \tag{2}$$

where $x = \begin{bmatrix} x_1, & x_2, & x_3 \end{bmatrix}^T$, α, β, and γ are three non zero constants and $\bar{f}(x_1)$ is the piecewise-linear characteristic of the Chua's diode given by:

$$\bar{f}(x_1) = bx_1 + \frac{1}{2}(a-b)\left(|x_1+1| - |x_1-1|\right)$$

where $a < b < 0$ are two constants. ρ is defined as a small constant such that the chaotic behavior of the system (2) is not destroyed. z_3 is one of the state

variables of the following dynamical system:

$$\Sigma_D : \dot{z} = \begin{bmatrix} -ez_1 \\ -\omega z_3 \\ -gz_3 + \omega z_2 \\ -lz_4 + z_3 \end{bmatrix} + \begin{bmatrix} kx_1 + x_2 m_1 \\ 0 \\ qx_1 + x_2 m_1 \\ nx_2 + x_3 m_2 \end{bmatrix} \tag{3}$$

where $z = \begin{bmatrix} z_1,\ z_2,\ z_3,\ z_4 \end{bmatrix}^T$ and e, k, ω, g, q, l and n are constant scalar, chosen such that $k \neq q$ and $\omega \neq 0$. m_1, m_2 are the two messages to be encoded. Note that, in equation (2), the term ρz_3 plays the role of $\phi(z_1)$ and that, in equation (3), x_1, x_2 and x_3 stand for $\theta(x)$ (see Fig. 3).

The output is chosen to be $y = \begin{bmatrix} z_1,\ z_2,\ z_4 \end{bmatrix}^T$. Then, a sliding mode observer is designed as follows in order to reconstruct the unknown messages:

$$\begin{aligned} \hat{\Sigma}_C : & \begin{cases} \dot{\hat{x}}_1 = E_2 \kappa_1 \text{sign}\left(\tilde{x}_1 - \hat{x}_1\right) \\ \dot{\hat{x}}_2 = E_3 \kappa_2 \text{sign}\left(\tilde{x}_2 - \hat{x}_2\right) \end{cases} \\ \hat{\Sigma}_D : & \begin{cases} \dot{\hat{z}}_1 = \lambda_2 \text{sign}\left(z_1 - \hat{z}_1\right) \\ \dot{\hat{z}}_2 = \lambda_1 \text{sign}\left(z_2 - \hat{z}_2\right) \\ \dot{\hat{z}}_3 = E_1 \lambda_3 \text{sign}\left(\tilde{z}_3 - \hat{z}_3\right) \\ \dot{\hat{z}}_4 = E_4 \lambda_4 \text{sign}\left(z_4 - \hat{z}_4\right) \end{cases} \end{aligned} \tag{4}$$

The auxiliary variables involved in (4) are defined by:

$$\begin{aligned} \tilde{z}_3 &= -\frac{E_1 \lambda_1 \text{sign}_{\text{eq}}\left(z_2 - \hat{z}_2\right)}{\omega}, \\ \tilde{x}_1 &= \frac{\lambda_2 \text{sign}_{\text{eq}}\left(z_1 - \hat{z}_1\right) + ez_1 - g\tilde{z}_3 + \omega z_2 - E_1 \lambda_3 \text{sign}_{\text{eq}}\left(\tilde{z}_3 - \hat{z}_3\right)}{k - q} \\ \tilde{x}_2 &= \frac{E_2 \kappa_1 \text{sign}_{\text{eq}}\left(\tilde{x}_1 - \hat{x}_1\right)}{\alpha} + \tilde{x}_1 - \bar{f}(\tilde{x}_1) \end{aligned}$$

with $\kappa_i > 0$, $i \in [1, 2]$, $\lambda_j > 0$, $j \in [1, 4]$ and:

$$E_1 = \begin{cases} 1 \text{ if } z_2 = \hat{z}_2 \\ 0 \text{ otherwise} \end{cases},$$

$$E_2 = \begin{cases} 1 \text{ if } E_1 = 1,\ z_1 = \hat{z}_1 \text{ and } \tilde{z}_3 = \hat{z}_3 \\ 0 \text{ otherwise} \end{cases},$$

$$E_3 = \begin{cases} 1 \text{ if } E_2 = 1 \text{ and } \tilde{x}_1 = \hat{x}_1 \\ 0 \text{ otherwise} \end{cases},$$

$$E_4 = \begin{cases} 1 \text{ if } E_3 = 1 \text{ and } \tilde{x}_2 = \hat{x}_2 \\ 0 \text{ otherwise} \end{cases}.$$

The term sign_{eq} is the so-called equivalent information injection available once a sliding motion is obtained (by analogy with the well known equivalent control, that is to say the control value required to maintain an ideal sliding motion). It actually represents the mean value of the signum function in sliding mode and can be obtained in finite time via a low pass filter or by some continuous approximation of the signum function [6]. One also sets:

$$\begin{aligned} \tilde{x}_3 &= E_3 \kappa_2 \text{sign}_{\text{eq}}\left(\tilde{x}_2 - \hat{x}_2\right) - \tilde{x}_1 + \tilde{x}_2 \\ \tilde{m}_1 &= \frac{\lambda_2 \text{sign}_{\text{eq}}\left(z_1 - \hat{z}_1\right) - k\tilde{x}_1 + ez_1}{\tilde{x}_2} \\ \tilde{m}_2 &= \frac{E_4 \lambda_4 \text{sign}_{\text{eq}}\left(z_4 - \hat{z}_4\right) + lz_4 - \tilde{z}_3 - n\tilde{x}_2}{\tilde{x}_3}. \end{aligned}$$

Proof of the observer convergence

The convergence of the state variables and the reconstruction of the messages are obtained with a step-by-step procedure. The following observation errors are defined:

$$e_{z_i} = z_i - \hat{z}_i,\ i \in [1, 4]$$

$$e_{x_j} = x_j - \hat{x}_j,\ j \in [1, 2]$$

First step: from (3) and (4), the dynamics of e_{z_2} is given by:

$$\dot{e}_{z_2} = -\omega z_3 - \lambda_1 \text{sign}\left(e_{z_2}\right)$$

It is known that if $\lambda_1 > \sup_{\forall t>0} |\omega z_3|$, a sliding motion appears on $e_{z_2} = 0$ after a finite time t_1. Then, the analysis of the resulting equivalent dynamics on the sliding surfaces (obtained by writing that $\dot{e}_{z_2} = 0$) provides the following algebraic equation

$$\lambda_1 \text{sign}_{\text{eq}}\left(z_2 - \hat{z}_2\right) = -\omega z_3.$$

Consequently

$$\tilde{z}_3 = -\frac{\lambda_1 \text{sign}_{\text{eq}}\left(e_{z_2}\right)}{\omega} = z_3.$$

Second step: For $t > t_1$, $\tilde{z}_3 = z_3$ and $E_1 = 1$ because $e_{z_2} = 0$. So, the dynamics of the observation errors e_{z_1} and e_{z_3} are given by:

$$\begin{aligned}
\dot{e}_{z_1} &= -ez_1 + kx_1 + x_2 m_1 - \lambda_2 \text{sign}\left(e_{z_1}\right) \\
\dot{e}_{z_3} &= -gz_3 + wz_2 + qx_1 + x_2 m_1 - \lambda_3 \text{sign}\left(\tilde{z}_3 - \hat{z}_3\right) \\
&= -gz_3 + wz_2 + qx_1 + x_2 m_1 - \lambda_3 \text{sign}\left(e_{z_3}\right).
\end{aligned}$$

Choosing

$$\begin{aligned}
\lambda_2 &> \sup_{\forall t>0} \left| -ez_1 + kx_1 + x_2 m_1 \right| \\
\lambda_3 &> \sup_{\forall t>0} \left| -gz_3 + wz_2 + qx_1 + x_2 m_1 \right|,
\end{aligned}$$

a sliding motion appears after a finite time $t_2 > t_1$ on $e_{z_1} = e_{z_3} = 0$ and $E_2 = 1$. Writing also that $\dot{e}_{z_1} = \dot{e}_{z_3} = 0$ yields the two following algebraic relations:

$$\lambda_2 \text{sign}_{\text{eq}}\left(z_1 - \hat{z}_1\right) = -ez_1 + kx_1 + x_2 m_1 \tag{5}$$

$$\lambda_3 \text{sign}_{\text{eq}}\left(\tilde{z}_3 - \hat{z}_3\right) = -gz_3 + wz_2 + qx_1 + x_2 m_1 \tag{6}$$

Substracting (6) from (5), one obtains:

$$\frac{\lambda_2 \text{sign}_{\text{eq}}\left(z_1 - \hat{z}_1\right) + ez_1 - \lambda_3 \text{sign}_{\text{eq}}\left(\tilde{z}_3 - \hat{z}_3\right) - g\tilde{z}_3 + wz_2}{k - q} = x_1$$

and thus $\tilde{x}_1 = x_1$.
Third step: because, for $t > t_2$, $\tilde{x}_1 = x_1$ and $E_2 = 1$, one has:

$$\begin{aligned}
\dot{e}_{x_1} &= -\alpha\left(x_1 - x_2 - \bar{f}(x_1)\right) - \kappa_1 \text{sign}\left(\tilde{x}_1 - \hat{x}_1\right) \\
&\quad -\alpha\left(x_1 - x_2 - \bar{f}(x_1)\right) - \kappa_1 \text{sign}\left(e_{x_1}\right)
\end{aligned}$$

If $\kappa_1 > \sup_{\forall t>0} \left| -\alpha\left(x_1 - x_2 - \bar{f}(x_1)\right)\right|$, after a finite time $t_3 > t_2$, a sliding motion appears on $e_{x_1} = 0$, $E_3 = 1$ and the equivalent dynamics is given by:

$$\kappa_1 \text{sign}_{\text{eq}}\left(\tilde{x}_1 - \hat{x}_1\right) = -\alpha\left(x_1 - x_2 - \bar{f}(x_1)\right).$$

This implies that

$$\tilde{x}_2 = \frac{\kappa_1 \text{sign}_{\text{eq}}\left(\tilde{x}_1 - \hat{x}_1\right)}{\alpha} + \tilde{x}_1 - \bar{f}(\tilde{x}_1) = x_2$$

Fourth step: after t_3, one obtains:

$$\begin{aligned}\dot{e}_{x_2} &= x_1 - x_2 + x_3 - \kappa_2 \text{sign}\,(\tilde{x}_2 - \hat{x}_2) \\ &= x_1 - x_2 + x_3 - \kappa_2 \text{sign}\,(e_{x_2})\end{aligned}$$

Set $\kappa_2 > \sup_{\forall t>0} |x_1 - x_2 + x_3|$, then $e_{x_2} = 0$ and $E_4 = 1$ after a finite time $t_4 > t_3$. Writing that $\dot{e}_{x_2} = 0$, one gets the following equivalent dynamics:

$$\kappa_2 \text{sign}_{\text{eq}}\,(\tilde{x}_2 - \hat{x}_2) = x_1 - x_2 + x_3$$

which yields

$$\tilde{x}_3 = \kappa_2 \text{sign}_{\text{eq}}\,(\tilde{x}_2 - \hat{x}_2) - \tilde{x}_1 + \tilde{x}_2 = x_3$$

Thus, after t_4, one gets the estimate of all the state variables $z = \begin{bmatrix} z_1,\ z_2,\ z_3,\ z_4 \end{bmatrix}^T$ and $x = \begin{bmatrix} x_1,\ x_2,\ x_3 \end{bmatrix}^T$.

The messages are reconstructed as follows. From (5), one has after t_2:

$$x_2 m_1 = \lambda_2 \text{sign}_{\text{eq}}\,(z_1 - \hat{z}_1) + e z_1 - k x_1$$

and $\tilde{x}_1 = x_1$ and $\tilde{x}_2 = x_2$ after t_3. Thus, after t_3, an estimate of m_1 is given by:

$$\tilde{m}_1 = \frac{\lambda_2 \text{sign}_{\text{eq}}\,(z_1 - \hat{z}_1) - k\tilde{x}_1 + e z_1}{\tilde{x}_2} = m_1.$$

Moreover, one has

$$\dot{e}_{z_4} = -l z_4 + z_3 + n x_2 + x_3 m_2 - \lambda_4 \text{sign}\,(e_{z_4})$$

If $\lambda_4 > \sup_{\forall t>0} |-l z_4 + z_3 + n x_2 + x_3 m_2|$, there exists a finite time $t_5 > t_4$ such that $e_{z_4} = 0$. Finally, analyzing the equivalent sliding motion, one obtains:

$$\tilde{m}_2 = \frac{\lambda_4 \text{sign}_{\text{eq}}\,(z_4 - \hat{z}_4) + l z_4 - \tilde{z}_3 - n\tilde{x}_2}{\tilde{x}_3} = m_2,$$

and this ends the proof.

Figure 4 gives the chaotic behaviour of the system. In Figure 5 are depicted the behaviour of the states of the system (2) (i.e. Σ_C) in A and (3) (i.e. Σ_D) in B, as well as their estimates. The solid lines represent the trajectories of the transmitter with initial conditions $x_1(0) = z_1(0) = z_2(0) = z_3(0) = z_4(0) = 1$, and $x_2(0) = x_3(0) = 0$. Their corresponding estimates are depicted by the dash lines and the initial conditions of the observer are $\hat{x}_1(0) = \hat{z}_1(0) = -1$, $\hat{x}_2(0) = \hat{z}_2(0) = 1$, $\hat{x}_3(0) = 0.01$, $\hat{z}_3(0) = \hat{z}_4(0) = 0$. It can be seen that the states of systems (2) and (3) converge towards those of the observer in finite time. After convergence of the states, the two confidential messages with great amplitudes m_1 and m_2 are successfully reconstructed (see Fig. 6).

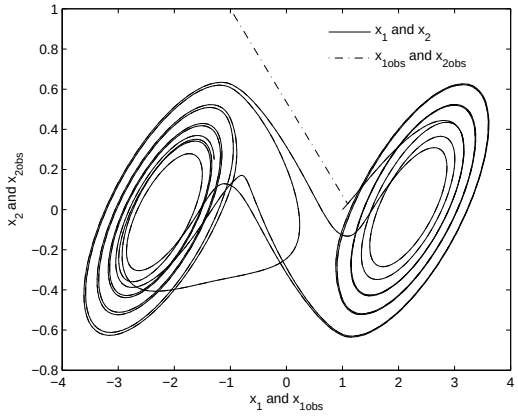

Fig. 4. The chaotic behaviour.

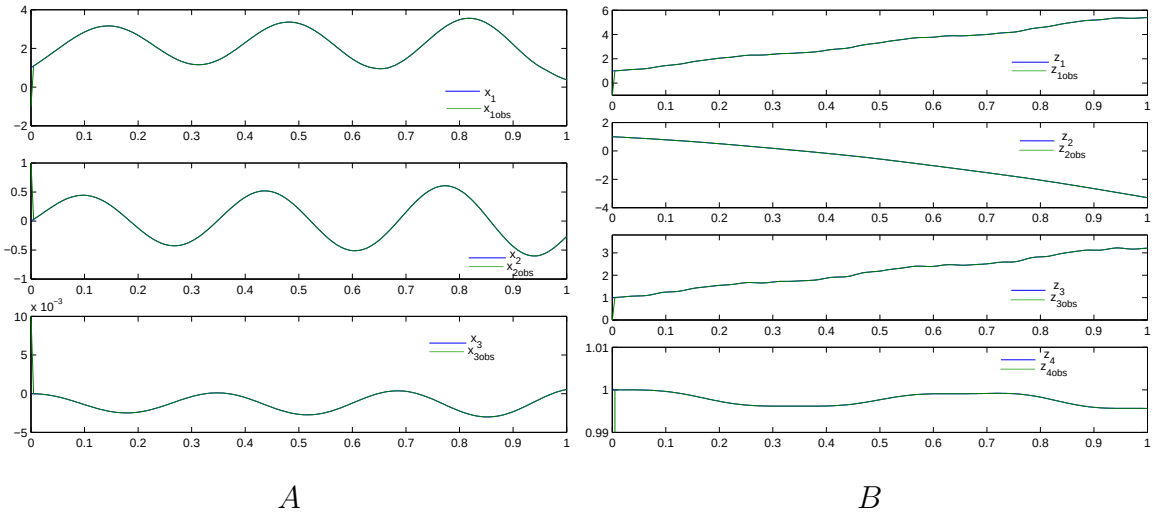

Fig. 5. The states of Σ_C in A, Σ_D in B (solid lines) and their estimates (dash lines).

5 Conclusion

In this article, an amplitude-independent scheme based on MIMO nonlinear chaotic systems was designed for secure communication. It allows for the transmission of messages with great amplitudes, which could degrade the quality of the synchronization in the majority of methods. An example has been given in order to highlight the efficiency of the proposed approach.

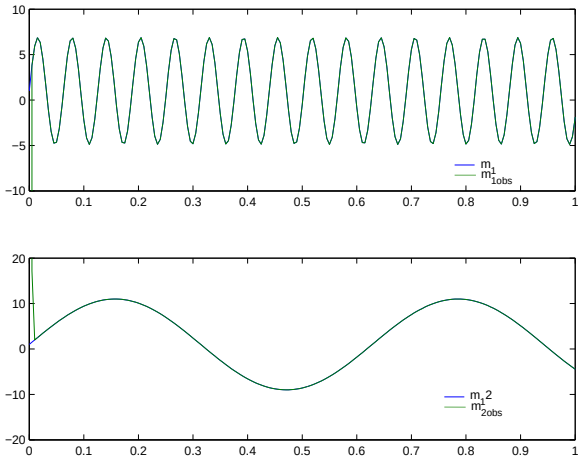

Fig. 6. The messages (solid lines) and their estimates (dash lines).

References

[1] G. Àlvarez, F. Montoya, et al, Cryptanalyzing a discrete-time chaos synchronization secure communication system, *Chaos, Solitons & Fractals*, 21(2004)(3), pp. 689-694.

[2] J.P. Barbot, D. Boutat and T. Floquet, A new observation algorithm for nonlinear system with unknown inputs, *in Proc. of IEEE Conf. on Decision and Control-European Control Conf.*, Sevilla, Spain, (2005).

[3] J.-P. Barbot, M. Fliess and T. Floquet, An algebraic framework for the design of nonlinear observers with unknown inputs, *in Proc. of IEEE Conf. on Decision and Control*, New-Orleans, USA, (2007).

[4] Y. Chen, C. Chang, Impulsive synchronization of Lipschitz chaotic systems, *Chaos, Solitons & Fractals*, (2007), In Press.

[5] L.O. Chua, Global unfolding of Chua's circuit, *IEICE Trans. Fundamentals of Electronics, Communications, Computer Science*, (1993), pp. 704-734.

[6] C. Edwards and S. K. Spurgeon, *Sliding mode control: theory and applications*, Taylor and Francis, Eds, (1998).

[7] M. Feki, B. Robert, G. Gelle and M. Colas, Secure digital communication using discrete-time chaos synchronization, *Chaos, Solitons & Fractals*, 18(2003)(4), pp. 881-890.

[8] M. Feki, An adaptive chaos synchronization scheme applied to secure communication, *Chaos, Solitons & Fractals*, 18(2003)(1), pp. 141-148.

[9] U. Feldmann, M. Hasler and W. Schwarz, Communication by chaotic signals: The inverse system approach, *Int. J. Cricuit Theory and Applications*, 24(1996), pp. 551-576.

[10] T. Floquet, J.P. Barbot, Simultaneous robust state observation and unknown input estimation, *International Workshop on Variable Structure Systems*, Barcelona, Spain, (2004).

[11] T. Floquet, J.P. Barbot, Super twisting algorithm based step-by-step sliding mode observers for nonlinear systems with unknown inputs, *International Journal of Systems Science*, 38(2007), pp. 803–815.

[12] H. Fotsin, S. Bowong and J. Daafouz, Adaptive synchronization of two chaotic systems consisting of modified Van der Pol-Duffing and Chua oscillators, *Chaos, Solitons & Fractals*, 26(2005)(1), pp. 215-229.

[13] A. Isidori, Nonlinear control systems, 2nd edition, Springer-Verlag, (1989).

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

[15] S. Li, G. Àlvarez and G. Chen, Breaking a chaos-based secure communication scheme designed by an improved modulation method, *Chaos, Solitons & Fractals*, 25(2005)(1), pp.109-120.

[16] S. Liu and G. Chen, Nonlinear feedback-controlled generalized synchronization of spatial chaos, *Chaos, Solitons & Fractals*, 22(2004)(1), pp. 35-46.

[17] H. Nijmeijer and I.M.Y. Mareels, An observer looks at synchronization, *IEEE Trans. on Circuits and Systems-1: Fundamental theory and Applications*, 44(1997)(10), pp. 882-891.

[18] U. Parlitz, L.O. Chua et al, Transmission of digital signals by chaotic synchronization, *Int. J. Bifurcation and Chaos*, 2(1992), pp. 973-977.

[19] L.M. Pecora and T.L. Carroll, Synchronization in chaotic systems, *Physical Review Letters*, 64(1990), pp. 821-824.

[20] G. Pérez and H.A. Cerdeira, Extracting messages masked by chaos, *Physical Review Letters*, 74(1995), pp. 1970-1973.

[21] W. Perruquetti and J.P. Barbot, Sliding Mode Control in Engineering, M. Dekker, (2002).

[22] W. Respondek, Right and Left Invertibility of Nonlinear Control Systems, in *Nonlinear Controllability and Optimal Control*, ed., Sussmann H. J. (Marcel Dekker, New York), (1990), pp. 133-176.

[23] K.M. Short, Steps toward unmasking secure communications, *Int. J. Bifurcation and Chaos*, 4(1994), pp. 959-977.

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

[25] T. Yang and L.O. Chua, Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication, *IEEE Trans. Circuits and Systems-I*, 44(1997), pp. 976-988.

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

[27] T. Yang, A survey of chaotic secure communication systems, *Int. J. Comp. Cognition*, 2(2004)(2), pp. 81-130.

[28] G. Zheng, D. Boutat, T. Floquet and J.P. Barbot, Multiple Secure Communication Based on Chaos, *in Proc. of 1st IFAC Conf. on Analysis and Control of Chaotic Systems,* CHAOS'06, Reims, France, (2006).

[29] G. Zheng, D. Boutat, T. Floquet and J.P. Barbot, Secure Data Transmission Based on Multi-input Multi-output Delayed Chaotic System, *Int. J. Bifurcation and Chaos*, (2008), In press.