Analogue private communication based on hybrid chaotic systems with delays

Gang Zheng, Woihida Aggoune, Jean-Pierre Barbot

Analogue private communication based on hybrid chaotic systems with delays

G. Zheng * **W. Aggoune** * **J.-P. Barbot**[*, **]

* *Equipe Commande des Systèmes (ECS), ENSEA, 6 Av. du Ponceau, 95014 Cergy, France (e-mail: {Zheng, Aggoune, Barbot}@ ensea.fr).*
** *Equipe Projet ALIEN INRIA, France*

Abstract: Since most of private communication schemes based on chaotic synchronization are not robust again plain-texts attacks, the introduction of delays in the schemes can be regarded as an efficient method to improve the security degree with respect to such attack. As an extension of our recent work, this paper proposes a new analogue private communication scheme based on hybrid chaotic systems with delays. The proposed scheme is based on the notation of weakly left invertibility of switched systems, and an illustrative example is given for the purpose of highlighting the feasibility of the proposed method.

Keywords: Chaotic systems, hybrid systems, weakly left invertibility, numerical differentiation

1. INTRODUCTION

After Pecora and Carroll (1990) successfully synchronized two identical chaotic systems with different initial conditions, chaos synchronization has been intensively studied in various fields. Since the work of Nijmeijer and Mareels (1997), unidirectional synchronization can be viewed as a special case of observer design problem, i.e. the state reconstruction from measurements of an output variable under the assumption that the system structure and parameters are known. For the private communication system based on the synchronization of chaotic systems, a receiver (an observer from a control theory point of view) is designed in order to be synchronized with respect to the transmitter (a chaotic system with unknown inputs from a control theory point of view) and to reconstruct the confidential messages (the unknown inputs of the chaotic systems from a control theory point of view). Many techniques arising from observation theory have been applied to the problem of synchronization, such as observers with linearizable dynamics in Huijberts et al. (2001), adaptive in Fradkov et al. (2000), generalized hamiltonian form based observers in Sira-Ramirez and Cruz-Hernandez (2001), algebraic method in Sira-Ramirez and Fliess (2006), Barbot et al. (2007) or inverse system in Feldmann et al. (1996). However, for most of private communication schemes based on chaotic synchronization and message inclusion, it is shown that they are not robust to known plain-texts attacks (see Anstett et al. (2006)). According to the famous Kerkhoff (1883) principe, it is assumed that hackers know all the details about the cryptosystem except the secret key. Roughly speaking, if the keys are only the parameters of chaotic systems, it can be proved that all the "useful" [1] parameters can be identifiable when trying the known plain-texts attacks.

[1] It means the parameters which play a role in the message transmission.

Recently, in Zheng et al. (2008) delays were used in chaotic systems in order to improve the robustness of cryptosystems with respect to known plain-texts attacks, since delays are more difficult to be identified (see Richard (2003)). As an extension of our previous work, we propose a new strategy in this paper for the purpose of improving the robustness of private communication, and this extension is based on hybrid systems with delays. From control theory point of view, the problem of recovering the message in the private communication scheme based on chaotic synchronization can be regarded as a left invertibility problem (Hirschorn (1979), Singh (1982), Respondek (1990)), on which the new private communication scheme is also based. Some sufficient conditions are also given in order to solve the left invertibility problem for systems with delays. In addition, as there exist lost packets in the private communication in practice, a resynchronization technique will be proposed as well.

This paper is organized as follows: Section 2 gives a presentation of the problem statement. In Section 3, a new scheme based on hybrid chaotic systems with delays is proposed. Then the robustness of the proposed scheme is analyzed in Section 4. And Section 5 is devoted to highlighting the feasibility of the proposed scheme by an illustrative example.

2. PROBLEM STATEMENT

This section is devoted to analyzing the robustness of most proposed schemes. Without loss of generality, we consider first a n-dimensional chaotic system in the following generic form:

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

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

Hence, the private communication system based on (1) can be represented in the following form:

$$\begin{cases} \dot{x} = f(x, K) + g(x, K)\, u \\ y = h(x) \end{cases} \tag{2}$$

where $K \in R^q$ is the key vector, $y \in R$ is the output vector and $u \in R$ represents the confidential information to be transmitted. The vector fields $f : R^n \times R^q \to R^n$, $g : R^n \times R^q \to R^n$ and $h : R^n \to R$ are assumed to be sufficiently smooth on U.

In this paper, we focus only on the analysis of the scheme based on inverse system, which implies, according to (2), one can express all states and unknown inputs as functions of the original outputs y, their time derivatives and the key vector as follows (see Diop and Fliess (1991) for details):

$$\begin{cases} x = \Xi\left(y, \dot{y}, ..., y^{(n-1)}, K\right) \\ u = \Psi\left(y, \dot{y}, ..., y^{(n-1)}, K\right) \end{cases} \tag{3}$$

However, (3) cannot resist against known plain-texts attacks when all plain-texts are known. Indeed, consider the second equation of (3) at different instants t_i for $1 \leq i \leq l$, it is possible to obtain several independent equations with respect to K:

$$u(t_i) = \Psi\left(y(t_i), \dot{y}(t_i), ..., y^{(n-1)}(t_i), K\right) \tag{4}$$

Remark 1. If we can obtain $q = l$ independent equations from (4), thus all useful parameters are identifiable. If $l < q$, which means that $q - l$ parameters are not identifiable, then they can not play the role of the key. Thus, the knowledge of these parameters is not necessary for recovering the message and those parameters are of no interest in the transmitter design.

Consequently such a scheme is not robust against known plain-texts attacks. For the data transmission scheme based on discrete chaotic system, the similar expression between all states and unknown inputs could be deduced as that of (3), replacing time derivatives of outputs by time delays of outputs. Analogously, those schemes are not robust against known plain-texts attacks as well.

3. PROPOSED SCHEME

In order to overcome this drawback, in Zheng et al. (2008) we proposed a more robust scheme with respect to known plain-texts attacks by introducing delays in multi-input multi-output continuous chaotic system, which is also a part of the unknown parameters (part of the key). Consequently, the introduction of the delay operator into the input-output relation equation seems to exhibit a robust characteristics with respect to known plain-texts attacks. Inspired by the work of *Tan et al. (2008)*, as an extension of our previous work, we propose a new analogue private communication scheme based on hybrid chaotic systems with delays, which is described in Fig. 1. For the transmitter, the switching signal is generated by the discrete system with the message and the partition block. It was used to activate the corresponding chaotic subsystem for the purpose of encoding the message. For the receiver, the received signal is decoded according to activated subobserver, determined by the switching signal generated by the discrete system and partition block in the receiver.

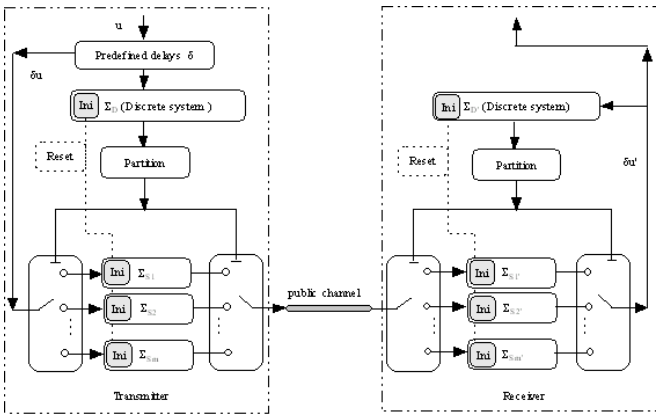

Fig. 1. Scheme for private communication system based on hybrid chaotic systems with delays.

3.1 Description of transmitter

The discrete system (Σ_D) of the transmitter in this scheme can be described as

$$\Sigma_D : \begin{cases} z(k+1) = F(z(k), u(k\eta), K) \\ y_D = H(z(k)) \end{cases} \tag{5}$$

where $z \in R^{N_D}$ is the state vector, $K \in R^q$ is the key vector, $y_D \in \mathcal{O}$ is the output vector where $\mathcal{O}$ is the output space such that $\mathcal{O} \subseteq R^{O_D}$, $u \in R$ represents the confidential information and η represents the sampled period. The vector fields $F : R^{N_D} \times R \times R^q \to R^{N_D}$ and $H : R^{N_D} \to \mathcal{O}$ are assumed to be sufficiently smooth. Since Σ_D is discrete chaotic system, such that it is sensitive to its initial condition and parameters, hence those variables (initial condition and some critique parameters of Σ_D) can be served as part of keys.

The function of partition block in the scheme acts as a generator of switching signal from y_D (the output of Σ_D).

Definition 1. Given the output space of Σ_D, its associated partition $S_1, \ldots, S_m$ can be defined

$$\bigcup_{i=1}^{m} S_i = \mathcal{O} \text{ and } S_i \bigcap S_j = \emptyset, \text{ for } 1 \leq i, j \leq m, i \neq j$$

Consequently, the switching signal generated by the discrete system and partition block can be defined as follows.

Definition 2. The switching signal is a piecewise constant function $\mathcal{S} : R_0^+ \times \mathcal{O} \times \mathcal{N} \times \mathcal{N} \to \mathcal{M}$ where R_0^+ represents the non negative real, $\mathcal{N}$ represents the natural and $\mathcal{M} = \{1, \ldots, m\} \subset \mathcal{N}$. For a given $y_D \in \mathcal{O}$, we have

$$\mathcal{S}(t, y_D, I, I_0) = \begin{cases} i, & \text{if } y_D(t) \subset S_i \subseteq \mathcal{O} \text{ and } mod(t, I\eta) = 0 \\ i_0, & \text{if } mod(t, I_0\eta) = 0 \end{cases}$$

where $I \in \mathcal{N}$ is a predefined natural characterizing iteration times of the discrete system, $I_0 \in \mathcal{N}$ represents a predefined positive reinitialization period of the proposed scheme, $i \in \mathcal{M}$ is the value of the switching signal, $i_0 \in \mathcal{M}$ is the default value of the switching signal, determined by the initial conditions of z and u in (5) and $mod(a, b)$ represents a modulo b.

The generated switching signal plays the role to determine how and when to activate a subsystem. A simple determi-

nation rule can be defined as follows.

Rule 1. Activate the jth subsystem when $\mathcal{S}(t, y_D, I, I_0) = j$ for $t \in R_0^+$, $y_D(t) \subseteq \mathcal{O}$, $I \in \mathcal{N}$, $I \in \mathcal{N}$ and $j \in \mathcal{M}$.

Remarks 1. i) The reinitialization procedure will be proposed in Section 4 to handle loss packets during data transmission. A predefined period is given by $I_0\eta$, and at the reinitialization instant the switching signal will be reset, the same as those of the discrete system and the switched systems in the scheme, which will be explained in the next section.

ii) It can be seen that the associated partition of the output space $\mathcal{O}$ of Σ_D is not unique, and the activate rule of subsystem can be different as well. Hence the partition manner and the activate rule can be served as part of keys in order to improve the robustness of the proposed scheme.

3.2 Left invertibility of delayed system

In order to simplify the presentation of the description of transmitter, we introduce the following notations. Classically, $\delta_i \in R_0^+$ for $i \in \mathcal{N}$, denotes the delay operator defined for any function $a(\cdot)$, such as $\delta_i a(t) = a(t - \tau_i)$. As usual, $\delta_i^0 a(t) = a(t)$, and recursively, one has $\delta_i^k a(t) = \delta_i(\delta_i^{k-1} a(t))$, for $k \geq 1$. Moreover, the delay operator satisfies: $\delta_i (a + b) = \delta_i a + \delta_i b$ and $\delta_i (a \cdot b) = \delta_i a \cdot \delta_i b$. For any function f, we note

$$f_{\delta_i}(x(t)) = f(\delta_i x(t)) = f(x(t - \tau_i)) \tag{6}$$

which is homogeneous with the delay τ_i for state x (i.e. it contains only the delay τ_i), satisfying $f_{\delta_i} = \delta_i f$ and $f(0) = 0$. Let us remark that the derivative and the delay operators are commutative, i.e. $\frac{\partial f_{\delta_i}}{\partial x} = \delta_i \frac{\partial f}{\partial x}$, based on which the derivative of Lie can be extended to systems with delays.

Let us now consider the switched system in the transmitter. In the following we will focus on the left invertibility problem of the jth subsystem, hence for the sake of simplicity we drop the superscript j, and then the jth single-input single-output subsystem: Σ_j for $j \in \mathcal{M}$ is described as follows

$$\Sigma_{S_j} : \begin{cases} \dot{x} = f_0(x, K) + f_{\delta_1}(x, K) + g_2(x, K)\delta_2 u + g_{\delta_3}(x, K)u \\ x(t) = \phi(t), \;\; u(t) = \psi(t) \quad t \in [-\tau_m, 0] \\ y = h(x) \end{cases} \tag{7}$$

where $x \in R^{N_j}$, $K \in R^q$, $u \in R$, $y \in R$ and δ_i for $1 \leq i \leq 3$ represents the time delays of x or u for the jth subsystem. The functions $\phi(t) \in \mathcal{C}([-\tau_m, 0], R^n)$ and $\psi(t) \in \mathcal{C}([-\tau_m, 0], R^n)$ represent the initial condition of the jth subsystem, defined over the interval $[-\tau_m, 0]$, where τ_m is a positive constant such that $\tau_m = \max\{\tau_1, \tau_2, \tau_3\}$, $\mathcal{C}([-\tau_m, 0], R^n)$ is the Banach space of continuous function mapping $[-\tau_m, 0]$ into R^n, with the norm $\|\phi\| = \sup_{t \in [-\tau_m, 0]} |\phi(t)|$ with the Euclidean norm of $\phi(t) \in R^n$ denoted by $|\phi(t)|$. The functions f_0 and g_2 are smooth functions of x without delays, while f_{δ_1} and g_{δ_3} are smooth functions which are homogeneous with δ_1 and δ_3, respectively. Moreover we note $f_{\delta_1} = f_1$ and $g_{\delta_3} = g_3$ for the sake of simplicity.

Inspired by the work *of Vu and Liberzon (2008) and Tanwani and Liberzon (2008)*, we define the weakly left invertibility for system (7) as follows.

Definition 3. System (7) is weakly left invertible if unknown input $u(t)$ and state $x(t)$ can be recovered for any t from the knowledge of the output $y(t)$ for $t \in [0, b]$ with b positive, the initial condition of states $\phi(t)$ and initial condition of input $\psi(t)$ for $t \in [-\tau_m, 0]$.

In order to prove our main result, we introduce the following technical definitions.

Definition 4. An *input-output relation* for system (7) is defined as

$$L_{g_i} L_{f_{j_k}} \cdots L_{f_{j_1}} h \neq 0 \tag{8}$$

with $i \in \{2, 3\}$ and $j_l \in \{0, 1\}$ with $0 \leq l \leq k < n$, where j represents the number of input-output relation. Moreover for each input-output relation j, it is associated with a delay index $d_j = \left(\sum_{l=1}^{k} \tau_{j_l}\right) + \tau_i$ for $j_l \in \{0, 1\}$ and $i \in \{2, 3\}$. The *input-output relation set* for system (7) is the set of all input-output relations for this system.

Remark 2. Obviously, as the derivative of u is also unknown, the input-output relation with the derivative of the input is not considered. However, if we take into account the derivative of the input, then a derivative of Lie-Backlun must be considered.

Now similarly to systems without delays, we define the relative degree for system (7) as follows.

Definition 5. The relative degree r of system (7) is equal to $k^* + 1$ where k^* is the greatest value of k in the input-output relation set which satisfies the rank condition

$$\text{Rank} \begin{pmatrix} dh \\ dL_{f_l} h \\ \vdots \\ dL_{f_{j_k}} \cdots L_{f_{j_1}} h \end{pmatrix} = k^* + 1$$

At the relative degree r, we also associate a delay index d_r which is the smallest delay index of all input-output relations with $k = k^*$ which satisfies the rank condition.

Remark 3. If $L_{g_2} L_{f_0} h = 0$ and $L_{g_2} L_{f_1} L_{f_0} h \neq 0$, this implies that the delay in this Lie derivative between the input and the output is equal to $\tau_2 + \tau_1$. This fact is the starting point of the previous definition and it is with the rank condition the origin of the next theorem.

From the previous definition, we are able to give the following theorem.

Theorem 1. System (7) is weakly left invertible if:

- the relative degree r for this system is equal to n;
- all delay indices of input-output relations with $k < n - 1$ are strictly greater than d_r.

Proof 1. From the definition of the relative degree, it is clear that from the knowledge of the previous state and input we can recover the input at time $t - d_r$. Moreover from the same definition of relative degree, the system is 'observable' with respect to the knowledge of previous states and input. Consequently we can 'observe' or estimate the state at least at time $t - d_r$. Consequently system (7) is weakly left invertible in the sense of Definition 3.

3.3 Description of receiver

The receiver part in the scheme is to decode the encoded messages receiving through the public channel. At the end

of receiver, the discrete system $\hat{\Sigma}_D$ is the same structure used in the transmitter, i.e.

$$\hat{\Sigma}_D : \begin{cases} \hat{z}(k+1) = F(\hat{z}(k), \hat{u}(k\eta), K) \\ \hat{y}_D = H(\hat{z}(k)) \end{cases} \tag{9}$$

where $\hat{z}$, $\hat{u}$ and $\hat{y}_D$ are of the same dimension as those defined in Σ_D for the transmitter, representing their estimates. K represents the key shared by both the transmitter and receiver.

Proposition 1. If all the subsystems are weakly left invertible and the key K of the proposed scheme contains the following elements:

- for discrete system Σ_D: the initial conditions of messages and states, and some parameters of Σ_D;
- the partition manner and activate rule;
- for each subsystem Σ_{S_j} for $j \in \mathcal{M}$: the initial conditions of states and messages, some parameters and time delays of x and u for Σ_{S_j};

then we can design a receiver, which might successfully recover the messages encoded by the transmitter.

Proof 2. It can be seen that if the initial conditions and some parameters of the discrete system are used as part of keys, and if one knows the initial condition of u, one can have $\hat{y}_D \to y_D$ if one can prove $\hat{u} \to u$. Moreover, if the partition manner and activate rule are served as part of keys as well, one has $\hat{\mathcal{S}} \to \mathcal{S}$ which implies the switching signal could be recovered and consequently the correct corresponding subsystem might be activated. According to Theorem 1, one can design an observer in order to retrieve the encoded messages (i.e. $\hat{u} \to u$) from the active subsystem, provided one knows the initial conditions, the parameters and time delays of x and u for the active subsystem. It should be noted that this recovery of message may be with delays, and that is the reason why in Fig. 1 a block of predefined delays is placed in front of the discrete system for the purpose of keeping the applied input synchronized. Consequently, if the key K contains all the elements mentioned above, one can design a receiver, which might successfully recover the messages encoded by the transmitter.

Concerning the observer design for each subsystem, according to Theorem 1 one can deduce an input-output relation with delays for the purpose of reconstructing the message. Based on Barbot et al. (2007), an algebraic observer can be applied for this situation. This algebraic approach is based on the numerical differentiation technique used in Sira-Ramirez and Fliess (2006), Fliess and Sira-Ramirez (2004), Fliess et al. (2006), Fliess et al. (2008) and Mboup et al. (2007). Roughly speaking, for an analytic signal $x(t)$, its Taylor expansion at $t = 0$ can be written as $x(t) = \sum_{i=0}^{\infty} x^{(i)}(0)\frac{t^i}{i!}$. Then the corresponding truncated Taylor expansion is $x_N(t) = \sum_{i=0}^{N} x^{(i)}(0)\frac{t^i}{i!}$ with $\frac{d^{N+1}}{dt^{N+1}} x_N(t) = 0$. Rewrite it in the well-known notation of operational calculus:

$$x_N(s) = \sum_{i=0}^{N} \frac{x^{(i)}(0)}{s^{i+1}}$$

where $\frac{d}{ds}$ corresponds to the multiplication by $-t$ in the time domain. By multiplying both sides $\frac{d^j}{ds^j} s^{N+1}$ with $0 \leq j \leq N$ and s^{-v} with $v > N$, it yields the following triangular linear equations

$$s^{-v}\frac{d^j(s^{N+1}x_N)}{ds^j} = s^{-v}\frac{d^j}{ds^j}\left(\sum_{i=0}^{N} x^{(i)}(0)s^{N-i}\right) \tag{10}$$

and we can obtain the numerical differentiation of $x(t)$ by applying the inverse Laplace transform to (10).

4. ANALYSIS OF ROBUSTNESS

For a new proposed private communication scheme, one of the main tasks is to analyze its robustness with respect to attacks.

4.1 Robustness to known plain-texts attacks

Due to the introduced delays for the state variables and the inputs, the proposed scheme becomes robustness against known plain-texts attacks. More precisely, one can obtain the input-output relation with delays, hence at different instants t it is possible to obtain independent equations with respect to K, such that

$$u = \Psi(y, \ldots, y^{(n-1)}, \delta y, \ldots, \delta y^{(n-1)}, \tilde{\delta} u, \ldots, \tilde{\delta} u^{(n-1)}, K) \tag{11}$$

where δ and $\tilde{\delta}$ represent the delays for the output and input, respectively. However since at each instant t, the output and the derivative of the output with delays are not known because the delays are part of key, it becomes more difficult to identify K according to (11). Consequently the proposed scheme seems more robust than schemes without delays to the known plain-texts attacks.

Another firewall against known plain-texts attacks of the proposed scheme is the combination effect of the discrete system affected by the unknown input and the partition block, which implicitly implies that one can find out a relation between the unknown input and the generated switching signal

$$i(t) = \Gamma(t, z, u, K) \tag{12}$$

In the situation of known plain-texts attacks, according to the relation (12) it is possible to identify some part of keys of K with the knowledge of the generated switching signal $i(t)$. However, since (12) is function of the unknown input u, for different u the output space of the discrete system is different, and after the partition block the generated switching signal $i(t)$ becomes difficult to be predicted, which signifies that the combination technique seems to be robust to the known plain-texts attacks.

4.2 Robustness to lost packets

From practical point of view, there exists an eventuality of lost packets during the data transmission, which will lead absolutely bad estimate of the states and messages. Since the chaotic system is quite sensitive to the initial condition and its parameters, those bad estimates will make future estimates totally worst. In order to rectify the bad influence of the lost packet during data transmission, we impose reinitilization rule in the proposed scheme.

Rule 2. At the instant $t_{reset} \in R_0^+$, i.e. $mod(t_{reset}, I_0\eta) = 0$, then set $\mathcal{S}(t_{reset}^+, y_D, I, I_0) = i_0 \in \mathcal{M}$, and reinitialize

the active subsystem $\Sigma_{S_{i_0}}$ at the instant t_{reset} by setting $x(t_{reset}) = \phi(t)$ and $u(t_{reset}) = \psi(t)$ for $t \in [t_{reset} - \tau_m, t_{reset}]$.

Since this rule is shared by both the transmitter and receiver, if there exists lost packets phenomenon, the bad estimates of messages will occur only until the next reset time. When the reinitialization operation is imposed for the transmitter and the receiver, a new synchronization is established, and consequently the influence of lost packets for future estimates of state variables and messages is avoided.

5. ILLUSTRATIVE EXAMPLE

This section is devoted to illustrating the feasibility of the proposed scheme. We choose the simple Logistic map as the discrete chaotic system described in the scheme:

$$\Sigma_D : \begin{cases} z(k+1) = \mu z(k)(1 - z(k)) + 0.01u(k\eta) \\ y_D = z(k) \end{cases} \quad (13)$$

with $\mu = 1.38$, $u(t) = 1 + sin(t)cos(15t + 20)$, $\eta = 0.0001s$, and with the initial condition $z(0) = 0.01$ and $u(0) = 0$. The partition of the output space of (13) is set to be $S_1 = [0, 0.6]$ and $S_2 =]0.6, 1]$. The predefined constant variable I is set to be 2000 and $I_0 = 40000$, $i_0 = 1$. Hence the switching signal is defined

$$\mathcal{S}(t, z, I, I_0) = \begin{cases} 1, \text{ if } 0 \le z \le 0.6 \text{ and } mod(t, 2) = 0 \\ 2, \text{ if } 0.6 < z \le 1 \text{ and } mod(t, 2) = 0 \\ 1, \text{ if } mod(t, 20) = 0 \end{cases}$$

The uniform distribution of output space is illustrated in Fig. 2.

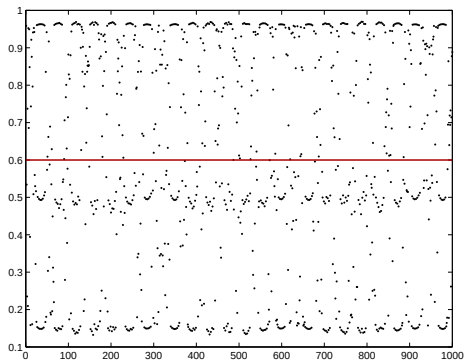

Fig. 2. Uniform distribution of the output state space of discrete system (13)

Concerning the switched systems described in the transmitter, we consider only two subsystems for the sake of simplicity. The first chaotic system is based on Lorenz system. After introducing delays into the state variable and input, it can be written in the following form:

$$\Sigma_{s_1} : \begin{cases} \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} a(x_2 - x_1) \\ x_1(b - x_3) - x_2 \\ x_1x_2 - cx_3 + x_2\delta_1 u + \delta_1 x_1 u \end{pmatrix} \\ y = x_1 \end{cases} \quad (14)$$

with $a = 10$, $b = 28$, $c = 8/3$, $\delta_1 u = u(t - \tau_1)$ and $\delta_1 x_1 = x_1(t - \tau_1)$ where $\tau_1 = 7$ms. In the simulation, the initial conditions of $x_1(t)$ and $u(t)$ for $t \in [-\tau_1, 0]$ are randomly generated over the time interval $[-\tau_1, 0]$.

Note $f_0 = \begin{pmatrix} a(x_2 - x_1) \\ x_1(b - x_3) - x_2 \\ x_1x_2 - cx_3 \end{pmatrix}$, $g_2 = \begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix}$ and $g_3 = \begin{pmatrix} 0 \\ 0 \\ \delta_1 x_1 \end{pmatrix}$, and one can find the following input-output relation $L_{g_3}L_{f_0}L_{f_0}h \neq 0$ if $-ax_1\delta_1 x_1 \neq 0$. It is easy to check such input-output relation has a regular relative degree 3 since

$$\text{Rank} \begin{pmatrix} dh \\ dL_{f_0}h \\ dL^2_{f_0}h \end{pmatrix} = 3$$

and consequently Theorem 1 is satisfied. More precisely, the state variables and the unknown message can be represented by the output and its derivative as follows:

$$\begin{cases} x_2 = \dfrac{\dot{y}}{a} + y \\ x_3 = b - \dfrac{\dot{x}_2 + x_2}{x_1} \\ u = \dfrac{\dot{x}_3 + cx_3 - x_1x_2 - x_2\delta_1 u}{\delta_1 x_1} \end{cases}$$

hence one can easily design a subobserver for Σ_{S_1}. The second subsystem is based on Chen chaotic system. Analogously by introducing the delays, Σ_{S_2} can be described as follows:

$$\Sigma_{s_2} : \begin{cases} \begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} \beta(x_2 - x_1) \\ x_1(\gamma - \beta) - x_1x_3 + \gamma x_2 \\ x_1x_2 - \rho x_3 + x_2\delta_2 u + \delta_1 x_2 u \end{pmatrix} \\ y = x_1 \end{cases} \quad (15)$$

with $\beta = 35$, $\gamma = 28$, $\rho = 3$ and $\tau_2 = 6$ms. It is easy to check that Theorem 1 is also fulfilled and the state variables and the unknown input can be recovered.

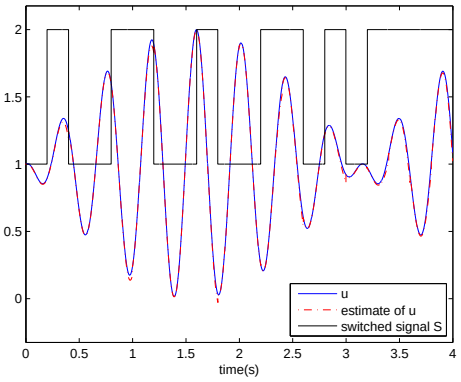

Fig. 3. Confidential message and its recovery.

By applying the algebraic approach to calculate the numerical differentiation (see Mboup et al. (2007)), the simulation results are depicted in Fig. 3, where only confidential message and its recovery are given. It is clear that the encode message u is reconstructed when the active subsystem is correctly determined.

6. CONCLUSION

This paper proposed a new analogue private communication scheme based on hybrid chaotic systems with delays in order to improve the security degree. The proposed scheme

is based on the weakly left invertibility problem and sufficient conditions are given in this paper in order to solve such a problem. Moreover, the robustness of the proposed scheme is discussed from two aspects: the robustness to known plain-texts attacks and robustness to lost packets. In addition, the algebraic derivative method is adopted to compute the successive derivatives of the output. Finally an example is studied in order to illustrative the proposed scheme.

REFERENCES

Anstett, F., Millerioux, G., and Bloch, G. (2006). Chaotic cryptosystems: Cryptanalysis and identiability. *IEEE Transactions on Circuits and Systems - Part I*, 53(12), 2673–2680.

Barbot, J.P., Fliess, M., and Floquet, T. (2007). An algebraic framework for the design of nonlinear observers with unknown inputs. *IEEE Conference on Decision and Control*, 384–389.

Diop, S. and Fliess, M. (1991). Nonlinear observability, identifiability and persistent trajectories. *in Proc. of 36th IEEE Conf. on Decision and Control.*

Feldmann, U., Hasler, M., and Schwarz, W. (1996). Communication by chaotic signals: The inverse system approach. *International Journal of Cricuit Theory and Applications*, 24, 551–576.

Fliess, M., Join, C., and Sira-Ramirez, H. (2008). Nonlinear estimation is easy. *International Journal of Modelling Identification and Control*, 4(1), 12–27.

Fliess, M. and Sira-Ramirez, H. (2004). Reconstructeurs d'état. *Comptes Rendus de l'Académie des Sciences - Series I*, 338(1), 91–96.

Fliess, M., Join, C., and Sira-Ramirez, H. (2006). Complex continuous nonlinear systems: their black box identification and their control. *in Proc. of the 14th IFAC Symposium on System Identification.*

Fradkov, A., Nijmeijer, H., and Markov, A. (2000). Adaptive observer-based synchronization for communication. *International Journal of Bifurcation and Chaos*, 10, 2807–2813.

Hirschorn, R. (1979). Invertibility of nonlinear control systems. *SIAM Journal on Control and Optimization*, 17, 287–289.

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

Kerkhoff, A. (1883). La cryptographie militaire. *Journal des sciences militaires*, IX, 5–83.

Mboup, M., Join, C., and Fliess, M. (2007). A revised look at numerical differentiation with an application to nonlinear feedback control. *in Proc. of the 15th Mediterranean Conference on Control and Automation.*

Nijmeijer, H. and Mareels, I. (1997). An observer looks at synchronization. *IEEE Transactions on Circuits and Systems-1: Fundamental theory and Applications*, 44(10), 882–891.

Pecora, L. and Carroll, T. (1990). Synchronization in chaotic systems. *Physical Review Letters*, 64(8), 821–824.

Respondek, W. (1990). Right and left invertibility of nonlinear control systems. *in Nonlinear Controllability and Optimal Control, ed., Sussmann H. J. (Marcel Dekker, New York)*, 24, 133–176.

Richard, J.P. (2003). Time-delay systems: an overview of some recent advances and open problems. *Automatica*, 39(10), 1667–1694.

Singh, S. (1982). Invertibility of observable multivariable nonlinear system. *IEEE Transactions on Automatic and Control*, 27, 487–489.

Sira-Ramirez, H. and Cruz-Hernandez, C. (2001). Synchronization of chaotic systems: a generalized hamiltonian approach. *International Journal of Bifurcation and Chaos*, 11(5), 1381–1395.

Sira-Ramirez, H. and Fliess, M. (2006). An algebraic state estimation approach for the recovery of chaotically encrypted messages. *International Journal of Bifurcation and Chaos*, 16(2), 295–309.

Tan, P.V., Millerioux, G., and Daafouz, J. (2008). Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications. *in Proc. of the 47th IEEE Conf. on Decision and Control.*

Tanwani, A. and Liberzon, D. (2008). Invertibility of nonlinear switched systems. *in Proc. of the 47th IEEE Conf. on Decision and Control.*

Vu, L. and Liberzon, D. (2008). Invertibility of switched linear systems. *Automatica*, 44(4), 949–958.

Zheng, G., Boutat, D., Floquet, T., and Barbot, J.P. (2008). Secure data transmission based-on multi-input multi-output delayed chaotic system. *International Journal of Bifurcation and Chaos*, 18(7), 2063–2072.