7 May 2001

PHYSICS LETTERS A

ELSEVIER

Physics Letters A 283 (2001) 96–108

www.elsevier.nl/locate/pla

More secure communication using chained chaotic oscillators

Hector Puebla, Jose Alvarez-Ramirez *

Division de Ciencias Basicas e Ingenieria, Universidad Autonoma Metropolitana-Iztapalapa, Apartado Postal 55-534, Mexico D.F., 09340 Mexico

Received 1 December 2000; received in revised form 27 February 2001; accepted 6 March 2001
Communicated by C.R. Doering

Abstract

In this Letter, a strategy for more secure communication using chaotic signals is presented. In this approach, the transmitter is composed by a chain of chaotic oscillator where the input to the first oscillator is modulated by the information signal and the transmitted signal is the output of the last oscillator. The receiver is a linear asymptotic approximation to the inverse of the transmitter system and contains an integral feedback to cope with nonlinearities and parameter variations. The functioning of the information encoding/decoding system is illustrated with a cascade of colpitts and Chua's circuits. © 2001 Published by Elsevier Science B.V.

Keywords: Chaotic communications; Chained encoding; Approximate inverse; Integral feedback; Chua's and colpitts circuits

1. Introduction

Secure communications masked with chaotic oscillators has attracted the attention of many researchers. Since its introduction by the pioneering work of Pecora and Carroll [1], it has been demonstrated that a drive signal from a chaotic system could be used to synchronize a second chaotic system. In recent years, several approaches were proposed to give a uniform view on modulating and demodulating information using chaotic signals [2–6]. In schemes based on *inverse system masking* (ISM) methods (see, for instance, [2,3,7,8]), an information signal is modulated by applying it as an input to chaotic system, and the modulated signal is tapped from the output wide-band signal of the chaotic system. In this way, the chaotic system can be interpreted as a nonlinear filter acting on the information signal. The ISM technique needs a receiver/demodulator which, in principle, can estimate the information signal accurately by inverting the chaotic (nonlinear filter) transmitter. That is, demodulation is possible if we can deduce the input to the system using only information in the output signal. Several demodulation procedures have been proposed to approximate the exact inverse of the transmitter. The basic idea is to use approximate differentiators to approximate time-derivatives of the received signal [5,9]. Corron and Hahs [10] proposed a nonlinear filter to overcome the use of differentiations. In this way, Corron and Hahs's nonlinear filter can be interpreted as an approximation to the time-derivative of the transmitted signal. Under the assumption

* Corresponding author. Fax: +52-5-8044900.
E-mail address: jjar@xanum.uam.mx (J. Alvarez-Ramirez).

0375-9601/01/$ – see front matter
PII: S0375-9601(01)00226-2

that the information signal has small-in-the-mean variations, the procedure led to both numerical and experimental successful applications on the Chua's circuit. The main drawback of Corron and Hahs's procedure is that it requires the implementation of nonlinear analog operations, such as multiplication and division. This, in principle, makes the practical implementation of the demodulator more difficult and expensive. Recently, Alvarez-Ramirez et al. [6] proposed a feedback demodulation procedure with integral actions to approximate the inverse of the chaotic system. A rigorous proof of the stability and noise effects of the demodulation procedure was given via results from standard singular perturbation systems.

Although ISM methods have been proven to be more secure than the so-called *additive signal masking* (ASM) methods [5] where the basic idea behind the chaotic masking is to hide the original information or the message inside a chaotic signal by direct addition [11–13], available ISM methods are based on a single chaotic oscillator. In this way, intruders have to get only a single demodulation key in order to recover the information signal. Since security is the main task of chaotic signal masking, from a practical viewpoint, it would be desirable to dispose of modulation procedures with more complex masking protocols in order to make the decoding as difficult as possible. the main idea is to use hyperchaotic signals in order to trouble the information signal recovering via chaotic attractor reconstruction methods (based on the Taken's theorem). A possibility is to use a network of chaotic oscillators where, similar to the single chaotic oscillator case, an information signal is modulated by applying it as an input to the chaotic network, and the modulated signal is tapped from the output wide-band signal of the chaotic network. Also, at the receiver, the information signal is recovered via the inverse or an approximation of the inverse of the chaotic network. It seems that a chain of (not necessarily equal) chaotic systems is the simplest network configuration [14]. This Letter is aimed at this objective. Specifically, a strategy for more secure communication using a class of chaotic oscillators is presented. In this approach, the transmitter is composed by a chain of chaotic oscillator where the input to the first oscillator is modulated by the information signal and the transmitted signal is the output of the last oscillator. The receiver is a linear asymptotic approximation to the inverse of the transmitter system and contains an integral feedback to cope with nonlinearities and parameter variations. The functioning of the information encoding/decoding system is illustrated with a cascade of colpitts and Chua's circuits.

This Letter is organized as follows. Section 2 presents the class of chaotic oscillators, which are the building blocks for the chaotic network. Section 3 presents the modulation /demodulation procedure for a single chaotic oscillator. Section 4 extends the procedure of Section 3 to a chain of chaotic oscillators. Section 5 uses numerical simulations to illustrate the functioning of the proposed masking procedure. Section 6 closes the Letter with some concluding remarks.

2. A class of Lur'e systems

The low-dimensional building blocks to construct the chaotic networks are given by the so-called Lur'e systems. Possibly after a change of coordinates, a Lur'e systems can be described by (see [15])

$$\begin{aligned} \dot{x} &= a_1 x + a_2 z + b\sigma(c_1 x + c_2 z), \\ \dot{z} &= a_3 x + Dz, \end{aligned} \tag{1}$$

where $x \in \mathbb{R}$, $z \in \mathbb{R}^n$ are the states and a_1, a_2, a_3, b, c_1, c_2 and D are vectors and matrices of suitable dimensions. The Lur'e system (1) is a linear dynamical system, feedback interconnected to a single static nonlinearity $\sigma : \mathbb{R} \to \mathbb{R}$. We will take the following assumptions:

Assumption 1. *The nonlinear function $\sigma(\cdot)$ is continuously differentiable and globally Lipschitz, i.e., $|\sigma(\xi_1) - \sigma(\xi_2)| \leqslant k_\sigma |\xi_1 - \xi_2|$, for all $\xi_1, \xi_2 \in \mathbb{R}$.*

Assumption 2. *The matrix $D \in \mathbb{R}^n \times \mathbb{R}^n$ is exponentially stable, i.e., all its eigenvalues are located in the open left-half part of the complex plane.*

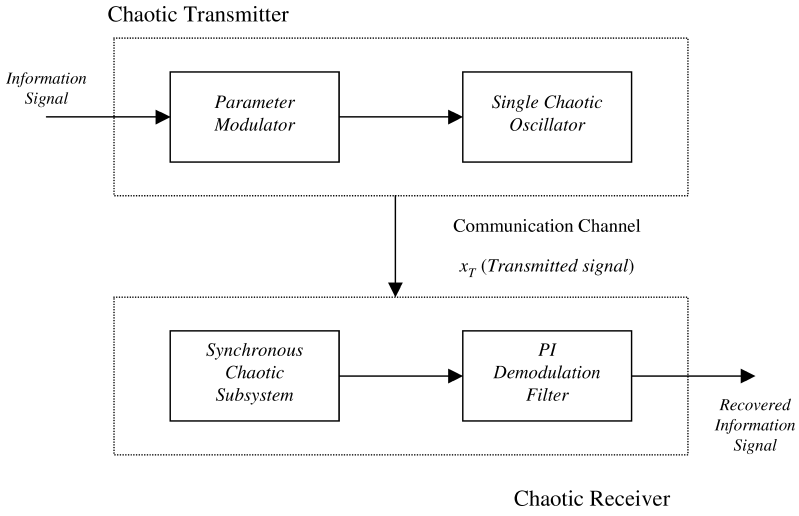

Fig. 1. Single modulation/demodulation chaotic communication design with a proportional-integral demodulation filter.

In some models, e.g., Chua's circuit, the nonlinearity $\sigma(\cdot)$ can be nondifferentiable at a countable number of points. In this case, the nonlinear function $\sigma(\cdot)$ can be closely approximated by a continuously differentiable one without serious degradation of the dynamic properties of the system.

It is not hard to see that several well-known chaotic circuits, including the Chua's and colpitts [16] circuits, can be interpreted as Lur'e systems of the class described above. In the Chua's circuit, $\sigma(c_1x + c_2z) = \alpha_1 x + (1/2)(\alpha_0 - \alpha_1)(|x+\alpha_3| - |x-\alpha_3|)$ is a continuous three piecewise-linear function with saturation and x is a capacitor voltage. In colpitts circuits, the nonlinearity $\sigma(c_1x + c_2z)$ corresponds to the continuous two-segment piecewise-linear driving-point (DP) characteristic of a nonlinear resistor [16].

3. Single modulation/demodulation design

Most of the material in this section has been borrowed from Alvarez-Ramirez et al. [6] (see also [17]). For the sake of clarity and completeness in presentation, we provide an brief outline of the modulation/demodulation procedure.

The general format of our approach is shown in Fig. 1 (see [5,9,10]). In the transmitter, an information signal is encoded using modulation of a parameter in the chaotic system. In the receiver, a synchronous chaotic system is augmented with a feedback demodulator designed specifically to continuous extract the information signal from the modulation waveform. Proper choice of drive channel and modulation parameter assures synchronization in the receiver, independent of the modulation. This approach fits within the most general definition of ISM methods, such as given in [18]. The main difference of our approach is the construction of the demodulator which, in contrast to previous approaches, contains an integral feedback to induce certain robustness capabilities into the demodulation loop. It should be pointed out that, for the sake of simplicity in presentation, the procedure is presented for a class of Lur'e systems, although it can be easily generalized to another classes of systems.

Let $s(t)$ denote the information signal. Moreover, let the subscripts T and R denote, respectively, transmitter and receiver signals. Assume that it is physically reliable to inject the information signal into the transmitter as follows:

$$\begin{aligned} \dot{x}_T &= a_1x_T + a_2z_T + b\sigma(c_1x_T + c_2z_T) + hs, \\ \dot{z}_T &= a_3x_T + Dz_T, \end{aligned} \tag{2}$$

where h is a given transmitter parameter to keep the system within its chaotic regime. We will take the state $x_T(t)$ as the transmitted signal. To have a wide-band signal $x_T(t)$, the information signal $s(t)$ is kept in the chaotic regime. The transformation of the information signal $s(t)$ into the transmitted signal $x_T(t)$ is called *modulation* [5].

Let $y(t)$ be the received signal. In the absence of noise and nonlinearities in the transmission line, we have $y(t) = x_T(t)$. At the receiver end, a replica of the transmitter circuit is taken to recover the information signal:

$$\begin{aligned} \dot{x}_R &= a_1 x_R + a_2 z_R + b\sigma(c_1 x_R + c_2 z_R) + h\overline{s}, \\ \dot{z}_R &= a_3 x_R + D z_R, \end{aligned} \tag{3}$$

where $\overline{s}$ is the recovered information signal. The transformation of the received signal $y(t)$ into the recovered information signal $\overline{s}(t)$ is called *demodulation*. Consider the following *exact* demodulation procedure based on the inverse feedback function:

$$\overline{s} = h^{-1}\big[\dot{y} - a_1 x_R - a_2 z_R - b\sigma(c_1 x_R + c_2 z_R) - \tau_D^{-1}(x_R - y)\big], \tag{4}$$

where $\tau_D > 0$ is a demodulation time-constant. In what follows, we will assume that $y(t) = x_T(t)$. The demodulation procedure (4) gives an exponentially exact information signal. That is, $\overline{s}(t) \to s(t)$ exponentially. In fact, using the fact that $y = x_T$, Eqs. (4) and (3) lead to the following system:

$$\begin{aligned} \dot{x}_R &= \dot{x}_T - \tau_D^{-1}(x_R - x_T), \\ \dot{z}_R &= a_3 x_R + D z_R. \end{aligned}$$

Introduce the synchronization errors $e_x = x_R - x_T$ and $e_z = z_R - z_T$. Then, the above system together with system (2) give

$$\begin{aligned} \dot{e}_x &= -\tau_D^{-1} e_x, \\ \dot{e}_z &= a_3 e_x + D e_z. \end{aligned} \tag{5}$$

System (5) is a cascade linear system. Since D is exponentially stable by assumption, we have that $e(t) \to 0$ exponentially, where $e \stackrel{\text{def}}{=} (e_x, e_z) \in \mathbb{R} \times \mathbb{R}^n$. On the other hand, Eq. (4) and the fact that $\dot{y} = \dot{x}_T = a_1 x_T + a_2 z_T + b\sigma(c_1 x_T + c_2 z_T) + hs$ lead to the following equality:

$$\overline{s} = s + h^{-1}\Big[-\big(a_1 + \tau_D^{-1}\big)e_x - a_2 e_z - b\big(\sigma(c_1 x_R + c_2 z_R) - \sigma(c_1 x_T + c_2 z_T)\big)\Big]. \tag{6}$$

Consequently, $\overline{s}(t) \to s(t)$ exponentially.

Remark 1. The damping term $\tau_D^{-1}(x_R - x_T)$ in the demodulation procedure (4) was introduced to overcome the necessity of identical initial conditions in transmitter and receiver systems. Since A is an exponentially stable matrix, there exist two positive constants α_z and λ_z such that $\|\exp(At)e_z(0)\| \leqslant \alpha_z \exp(-\lambda_z t)\|e_z(0)\|$, where $e_z(0)$ denotes the initial condition $e_z(t=0)$. Consequently, since the synchronization error dynamics given by Eqs. (5) are in cascade form, $\overline{s}(t)$ converges exponentially to $s(t)$ with a rate of the order of $\lambda^* \stackrel{\text{def}}{=} \min\{\tau_D^{-1}, \lambda_z\}$. Since τ_D is a tunable parameter, the velocity at which the information signal can be recovered is limited in general by the dynamics of the undriven z-subsystem.

Although the demodulation procedure (4) recovers exponentially the *exact* information signal, its implementation requires the nonlinearity $\sigma(c_1 x_R + c_2 z_R)$ and the time-derivative of the transmitted signal y. This is a serious drawback since nonlinearities and differentiators are not easily realized in practice. To solve this problems, we will propose a demodulation procedure that overcome the use of nonlinearities and differentiators. The idea put forward is to try to recover the performance induced by the exact feedback demodulator (4). This can be achieved, in theory, by estimating nonlinearities and time-derivatives via *linear* filters.

We have that $y = x_T$, so the x-subsystem of the receiver system (3) can be written as

$$\dot{e}_x = -\dot{y} + b\sigma(c_1 x_R + c_2 z_R) + a_1 x_R + a_2 z_R + h\overline{s}. \tag{7}$$

Since the designed demodulator procedure must be free of the nonlinearity $\sigma(c_1 x_R + c_2 z_R)$ and the time-derivative $\dot{y}$, the function

$$m(\dot{y}, \sigma) = -\dot{y} + b\sigma(c_1 x_R + c_2 z_R) \tag{8}$$

can be interpreted as a modeling error that is unavailable for feedback demodulator design. For simplicity in notation, let us use $m(t)$ to denote the modeling error signal $m(\dot{y}(t), \sigma(t)) = -\dot{y}(t) + b\sigma(c_1 x_R(t) + c_2 z_R(t))$. The exact feedback demodulator (4) can be written as

$$\overline{s} = h^{-1}\big[-m - a_1 x_R - a_2 z_R - \tau_D^{-1} e_x\big]. \tag{9}$$

Our idea is to use an observer to estimate the modeling error signal $m(t)$ and use the estimated signal $\overline{m}(t)$ to approximate the exact demodulator (9). This approximation is obtained just by using the estimated signal $\overline{m}(t)$ instead the real signal $m(t)$ in (9):

$$\overline{s} = h^{-1}\big[-\overline{m} - a_1 x_R - a_2 z_R - \tau_D^{-1} e_x\big]. \tag{10}$$

From (7), we have the equivalence $m(t) \equiv \dot{e}_x - a_1 x_R - a_2 z_R - h\overline{s}$. Hence, we propose the following observer to get the estimate $\overline{m}(t)$:

$$\dot{\overline{m}} = \tau_e^{-1}(m - \overline{m}) = \tau_e^{-1}\big(\dot{e}_x - a_1 x_R - a_2 z_R - h\overline{s} - \overline{m}\big), \tag{11}$$

where $\tau_e > 0$ is an estimation time-constant.

Remark 2. Let $\varepsilon \stackrel{\text{def}}{=} m - \overline{m}$ be the estimation error. Observer (11) can be interpreted as a type of gradient estimator [19]. In fact, the estimation $\overline{m}(t)$ is updated along the direction of the quadratic function $(1/2)\varepsilon^2$. In the context of control theory (see, for instance, [19]), Eq. (11) becomes a reduced-order observer when the modeling error signal $m(t)$ is seen as an additional state of the receiver system.

By using (9) in (11), we get

$$\dot{\overline{m}} = \tau_e^{-1}\big(\dot{e}_x + \tau_D^{-1} e_x\big). \tag{12}$$

Of course, observer (12) cannot implemented as it stands since it requires the time-derivative of the synchronization error $\dot{e}_x$. This can be easily overcame if we introduce the variable $w = \tau_e \overline{m} - e_x$, so that estimator (12) becomes equivalent to the following first-order filter:

$$\dot{w} = \tau_D^{-1} e_x, \qquad \overline{m} = \tau_e^{-1}(w + e_x). \tag{13}$$

Remark 3. Summarizing, the proposed demodulation procedure is composed by the feedback function (10) that approximates the exact demodulator (4) and the first-order filter (13) that provides a dynamic estimate of the modeling error signal $m(t)$:

$$\left.\begin{aligned} &\overline{s} = h^{-1}\big[-\overline{m} - a_1 x_R - a_2 z_R - \tau_D^{-1} e_x\big], \quad e_x = x_R - x_T \\ &\dot{w} = \tau_D^{-1} e_x, \qquad \overline{m} = \tau_e^{-1}(w + e_x) \end{aligned}\right\} \text{PI single demodulator,} \tag{14}$$

where the signals x_R and z_R are produced by a replica of the chaotic oscillators:

$$\left.\begin{aligned} &\dot{x}_R = a_1 x_R + a_2 z_R + b\sigma(c_1 x_R + c_2 z_R) + h\overline{s} \\ &\dot{z}_R = a_3 x_R + D z_R \end{aligned}\right\} \text{synchronizator.} \tag{15}$$

This procedure becomes an approximation of the inverse system, which provides an exponentially converging estimate $\overline{s}(t)$ of the information signal $s(t)$.

Notice that the proposed PI demodulator is linear and its implementation does not require time-derivatives of the transmitted signal. This easy its implementation either in an analog format.

Remark 4. We can interpret demodulator (10), (13) as a traditional proportional-integral (PI) feedback function acting on the synchronization error e_x. In fact, by using (13) in (10) we get

$$\overline{s} = h^{-1}\big[-\tau_e^{-1}(w + e_x) - a_1 x_R - a_2 z_R - \tau_D^{-1} e_x\big], \qquad \dot{w} = \tau_D^{-1} e_x.$$

Equivalently,

$$\overline{s} = h^{-1}\left[-a_1 x_R - a_2 z_R - \big(\tau_D^{-1} + \tau_e^{-1}\big)e_x - \tau_D^{-1}\tau_e^{-1}\int_0^t e_x(\theta)\,d\theta\right],$$

where θ is a dummy time argument. That is, the proposed demodulator is composed by the linear feedback $-h^{-1}(a_1 x_R + a_2 z_R)$ and the traditional PI feedback function $K_P e_x + K_I \int_0^t e_x(\theta)\,d\theta$, where the proportional K_P and integral K_I gains are given as

$$\begin{aligned} K_P &= -h^{-1}\big(\tau_D^{-1} + \tau_e^{-1}\big), \\ K_I &= -(h\tau_D\tau_e)^{-1}. \end{aligned} \tag{16}$$

In this way, the implementation of the PI demodulator (14) is quite simple because is a linear, differentiator-free feedback function.

Remark 5. Using results from the stability of singularly perturbed systems and low-pass filtering, Alvarez-Ramirez et al. [6] were able to prove the following two results:

(a) There exists a positive constant $\tau_e^{\max}$ such that, for all $0 < \tau_e < \tau_e^{\max}$, $|s(t) - \overline{s}(t)|_a = \mathcal{O}(\tau_e)$. This means that the recovering error $|s(t) - \overline{s}(t)|_a$ can be made as small asymptotically by reducing the estimation time-constant $\tau_e > 0$.

(b) The information signal $s(t)$ can be recovered with arbitrarily small errors via the proposed feedback demodulator in cascade configuration with maybe high-dimensional low-pass filtering.

These results guarantee stability of the modulation/demodulation procedure in the presence of small modulation/demodulation mismatches and zero-mean transmission noise.

4. Network modulation/demodulation design

The single modulation/demodulation design presented before is the departing point for the network case. The idea is to use the masking properties discussed above in a chain of chaotic oscillators as illustrated in Fig. 2. In this case, the modulators is composed by a series of n single chaotic oscillators connected in a series configuration. The input to the first oscillator is modulated by the information signal $s(t)$, the input of the second oscillator is modulated by the output of first oscillator, and so on:

$$\begin{aligned} \dot{x}_{T,1} &= a_{1,1}x_{T,1} + a_{1,2}z_T + b_1\sigma_1(c_{1,1}x_{T,1} + c_{1,2}z_{T,1}) + \overbrace{h_1 s}^{\text{first masking}}, \\ \dot{z}_{T,1} &= a_{3,1}x_{T,1} + D_1 z_{T,1}, \end{aligned}$$

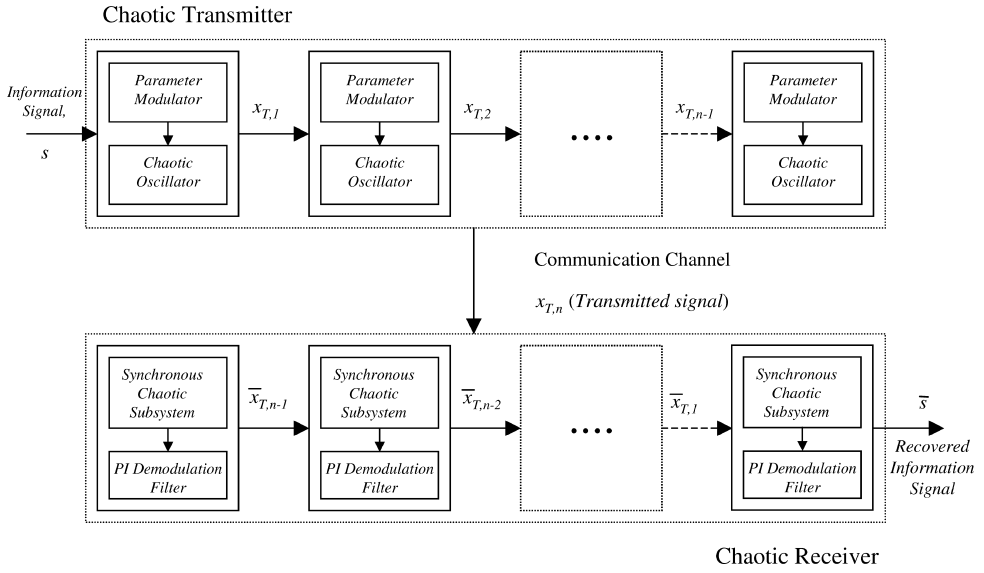

Fig. 2. Network modulation/demodulation chaotic communication design with proportional-integral filters.

$$
\begin{aligned}
\dot{x}_{T,2} &= a_{2,1}x_{T,2} + a_{2,2}z_{T,2} + b_2\sigma_2(c_{2,1}x_{T,2} + c_{2,2}z_{T,2}) + \overbrace{h_2x_{T,1}}^{\text{second masking}}, \\
\dot{z}_{T,2} &= a_{2,3}x_{T,2} + D_2z_{T,2}, \\
&\vdots \\
\dot{x}_{T,n} &= a_{n,1}x_{T,n} + a_{n,2}z_{T,n} + b_n\sigma_n(c_{n,1}x_{T,n} + c_{n,2}z_{T,n}) + \overbrace{h_nx_{T,n-1}}^{n\text{th masking}}, \\
\dot{z}_{T,n} &= a_{n,3}x_{T,n} + D_nz_{T,n},
\end{aligned}
\tag{17}
$$

where the parameters $\{h_1, h_2, \ldots, h_n\}$ are tuned to keep the individual systems within the chaotic regime. The transmitted signal is taken as the output of the last oscillator, $y_T = x_{T,n}$. Commonly, this system connection produces a signal $y_T = x_{T,n}$ within the hyperchaotic regime [20]. That is, the transmitted signal possesses at least two positive Lyapunov exponent, hence making more difficult the intruder's demodulation to recover the information signal [21].

The demodulation procedure is aimed to provide an approximation to the inverse $x_{T,n} \to s$ of the modulation procedure (17). This can be made as an extension of the single oscillator case. In fact, the jth masking in (17) is given by

$$
\begin{aligned}
\dot{x}_{T,j} &= a_{j,1}x_{T,j} + a_{j,2}z_{T,j} + b_j\sigma_j(c_{j,1}x_{T,j} + c_{j,2}z_{T,j}) + h_jx_{T,j-1}, \\
\dot{z}_{T,j} &= a_{j,3}x_{T,j} + D_jz_{T,j},
\end{aligned}
\tag{18}
$$

with $y_{T,j} = x_{T,j}$. Then, the demodulation procedure for system (18) can be formulated as follows: Given the jth "transmitted" signal, recover the $(j-1)$th "information" signal $x_{T,j-1}$. Notice that, while the modulation procedure is in forward form (i.e., from i to n), the demodulation procedure is in backward form (i.e., from n to i). This demodulation jth demodulation procedure is basically of the same type as the one described in Section 3.

Hence, the recovered $(j-1)$th "information" signal $\overline{x}_{T,j-1}$ are obtained from the jth demodulator:

$$\left.\begin{aligned} &\overline{x}_{T,j-1} = h_j^{-1}\big[-\overline{m}_j - a_{j,1}x_{R,j} - a_{j,2}z_{R,j} - \tau_{D,j}^{-1}e_{x,j}\big], \quad e_{x,j} = x_{R,j} - \overline{x}_{T,j} \\ &\dot{w}_j = \tau_{D,j}^{-1}e_{x,j}, \qquad \overline{m}_j = \tau_{e,j}^{-1}(w_j + e_{x,j}) \end{aligned}\right\} j\text{th PI demodulator,} \tag{19}$$

where the signals x_R and z_R are produced by a replica of the chaotic oscillators:

$$\left.\begin{aligned} &\dot{x}_{R,j} = a_{j,1}x_{R,j} + a_{j,2}z_{R,j} + b_j\sigma_j(c_{j,1}x_{R,j} + c_{j,2}z_{R,j}) + h_j\overline{x}_{T,j-1} \\ &\dot{z}_{R,j} = a_{j,3}x_{R,j} + D_j z_{R,j} \end{aligned}\right\} j\text{th synchronizator.} \tag{20}$$

Notice that the synchronization error $e_{x,j} = x_{R,j} - \overline{x}_{T,j}$ was computed with respect to the jth recovered "information" signal $\overline{x}_{T,j}$ obtained from the jth demodulator (recall that demodulation is made in backward form). The demodulation procedure is started at the nth demodulator with $x_{T,n}$ and $\overline{x}_{T,n-1}$, respectively, as the received and recovered signals with $e_{x,n} = x_{R,n} - x_{T,n}$ as the synchronization error. In the same way, the demodulation procedure is ended at the first demodulator with $\overline{x}_{T,1}$ and $\overline{s}$, respectively, as the received and recovered signals with $e_{x,1} = x_{R,1} - \overline{x}_{T,1}$ as the synchronization error.

Remark 6. The results for the single chaotic oscillator case as reported by Alvarez-Ramirez et al. [6] can be easily extended to the series case as follows:

(a) There exists a positive constant $\tau_e^{\max}$ such that, for all $0 < \tau_{e,j} < \tau_e^{\max}$, $j = 1, 2, \ldots, n$, the recovering error $|s(t) - \overline{s}(t)|_a = \mathcal{O}(|\tau_e|)$, where $|\tau_e|$ is the norm of the vector $(\tau_{e,1}, \tau_{e,2}, \ldots, \tau_{e,n})^{\mathrm{T}} \in \mathbb{R}^n$. This means that the recovering error $|s(t) - \overline{s}(t)|_a$ can be made as small asymptotically by reducing the estimation time-constants $\tau_{e,j} > 0$, $j = 1, 2, \ldots, n$.

(b) The information signal $s(t)$ can be recovered with arbitrarily small errors via the proposed feedback demodulator in cascade configuration with maybe high-dimensional low-pass filtering.

Remark 7. The chained masking procedure (17) is more secure than the single masking procedure. In fact:

(a) Hyperchaotic transmitted signals reduces drastically the chances of an intruder to recover the information signals via non-model based procedures, e.g., attractor reconstructions.

(b) In addition to n individual demodulation keys, an intruder would require the order of the chain. That is, the position at which each individual chaotic oscillator is located at the masking chain, is also required. An intruder having only the individual demodulation keys but not the order, must look at $n!$ combinations to find the correct one. In this way, for a moderate chain size $n = 10$, there exist 3,628,800 combinations.

5. Examples

In this section, simulation results are presented for communication systems built using the Chua's and colpitts circuits. These demonstrations show the effectiveness of the proposed network modulation/demodulation procedure. For completeness, a brief description of this oscillators is in order.

- The Chua's circuit is a simple electronic circuit that is widely used for demonstrating nonlinear dynamics and chaos. We have taken the following representation for Chua's circuit (see Eqs. (1)):

$$\begin{aligned} &\dot{x} = a\big[z_1 - \sigma(x)\big], \\ &\dot{z}_1 = x - z_1 + z_2, \\ &\dot{z}_2 = -dz_1, \end{aligned} \tag{21}$$

with nonlinear characteristic

$$\sigma(x) = \alpha_1 x + \frac{1}{2}(\alpha_0 - \alpha_1)(|x + \alpha_3| - |x - \alpha_3|) \tag{22}$$

and parameters $a = 9$, $d = 14.286$, $\alpha_0 = -1/7$, $\alpha_1 = 2/7$, $\alpha_3 = 1$, in order to obtain the double scroll family attractor [22]. The nonlinearity $\sigma(x)$ (linear characteristic with saturation) is globally Lipschitz and is nondifferentiable at a countable number (actually, two) of points. Hence, Chua's circuit (21), (22) belongs to the class of Lur'e system (1) where $a_1 = 0$, $a_2 = (a, 0)$, $b = -a(\alpha_0 - \alpha_1)$, $c_1 = 1$, $c_2 = (0, 0)$, $a_3 = (1, 0)$, and

$$D = \begin{bmatrix} -1 & 1 \\ -d & 0 \end{bmatrix}.$$

It is clear that D is exponentially stable. The term $hs(t)$ is equivalent to inject a current-mode signal in the transistor, hence making possible its analog (hardware) implementation. We have taken h about 0.25 to keep the Chua's circuit within the chaotic regime.

- On the other hand, colpitts circuits also belong to the class of Lur'e systems. We have taken the following representation for colpitts circuit (see Eqs. (1)):

$$\begin{aligned} \dot{x} &= C_2^{-1}\left[-R_{\mathrm{EE}}^{-1}(V_{\mathrm{EE}} + x) - z_2 - \sigma(x)\right], \\ \dot{z}_1 &= C_1^{-1}[z_2 - I_c], \\ \dot{z}_2 &= L^{-1}[V_{cc} + x - z_1 - R_L z_2], \end{aligned} \tag{23}$$

where x, z_1 and z_2 represents transistor voltage, capacitor voltage and inductor current, respectively; $\sigma(x)$ is the transistor current and is modeled as a two-segment piecewise linear voltage-controlled resistor N_R and a linear current-controlled current source:

$$\begin{aligned} \sigma(x) &= \begin{cases} 0, & \text{if } x \leqslant V_{\mathrm{TH}}, \\ R_{\mathrm{ON}}^{-1}(x - V_{\mathrm{TH}}), & \text{if } x > V_{\mathrm{TH}}, \end{cases} \\ I_c &= \beta_F \sigma(x), \end{aligned}$$

where R_{ON} is the small-signal on-resistance of the base–emitter junction and β_F is the forward current gain of the device. For colpitts circuits, we have that

$$D = \begin{bmatrix} 0 & C_1^{-1} \\ -L^{-1} & -L^{-1}R_L \end{bmatrix}, \tag{24}$$

which is an exponentially stable matrix. For the following set of circuit parameters, the colpitts circuit display chaotic behavior: $V_{\mathrm{CC}} = 5$ V, $R_L = 35\ \Omega$, $L = 98.5\ \mu$H, $C_1 = 54$ nF, $C_2 = 54$ nF, $R_{\mathrm{EE}} = 400\ \Omega$, $V_{\mathrm{EE}} = -5$ V, $V_{\mathrm{TH}} = 0.75$ V, $R_{\mathrm{ON}} = 100\ \Omega$, $\beta_F = 200$ [23]. As in Chua's circuit, the term $hs(t)$ is equivalent to inject a signal in current-mode in the transistor. We have tuned h about 0.15 to keep the colpitts circuit within the chaotic regime.

5.1. Chua–colpitts configuration

We have taken a Chua–colpitts ($n = 2$) configuration with a continuously differentiable information signal $s(t)$. Moreover, we have set the demodulation time-constants as $\tau_{D,1} = 0.005$, $\tau_{D,2} = 0.01$ and the estimation time-constants as $\tau_{e,1} = 0.005$, $\tau_{e,2} = 0.01$. Fig. 3 presents the (x, z_1)-phase plane for both oscillators, which shows the chaotic nature of the transmitter dynamics. Notice that if an intruder can reconstruct the generated attractor

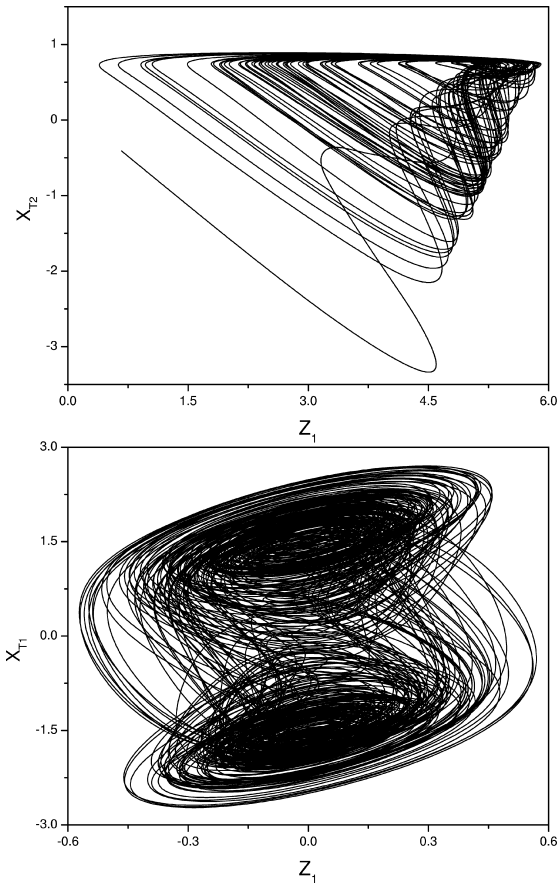

Fig. 3. Chaotic attractors from the transmitter subsystem for the Chua–colpitts configuration.

with the transmitted signal, only the last attractor (for this example the colpitts attractor) could be reconstructed. However, with only this information is very difficult to access to the encoded information. Fig. 4(a) shows the output of Chua's and colpitts circuits in the modulator scheme. Fig. 4(b) shows the recovered signal with the first demodulation procedure, and Fig. 4(c) shows the recovered signal with the second demodulation procedure corresponding to the colpitts and Chua's circuit output, respectively, in the modulation subsystem. This demonstrate the cascade nature of the demodulation design, where intermediate encoding signals are required in order to recover the actual information signal $s(t)$. The dot line in Figs. 4(b) and (c) shows the transmitted state x_{T1} and the encoded information signal $s(t)$, respectively. However, after a brief transient, the corresponding recovered signals are indistinguishable in the figures. The insert in Figs. 4(b) and (c) shows the recovering errors $\overline{x_{T1}}(t) - x_{T1}(t)$ and $\overline{s}(t) - s(t)$ for the demodulation procedure. Notice that, since the convergence $s(t) \to \overline{s}(t)$ is governed by the dynamics of the response subsystem (see Remark 2), very small values of $\tau_e > 0$ have effects on fine modes of the recovered signal $\overline{s}(t)$ only.

5.2. *Chua–Chua–Chua configuration*

In the second numerical example we consider a Chua–Chua–Chua ($n = 3$) configuration, but with different circuit parameter values. In this case, the masking procedure is more secure than in the (single) $n = 1$ and $n = 2$

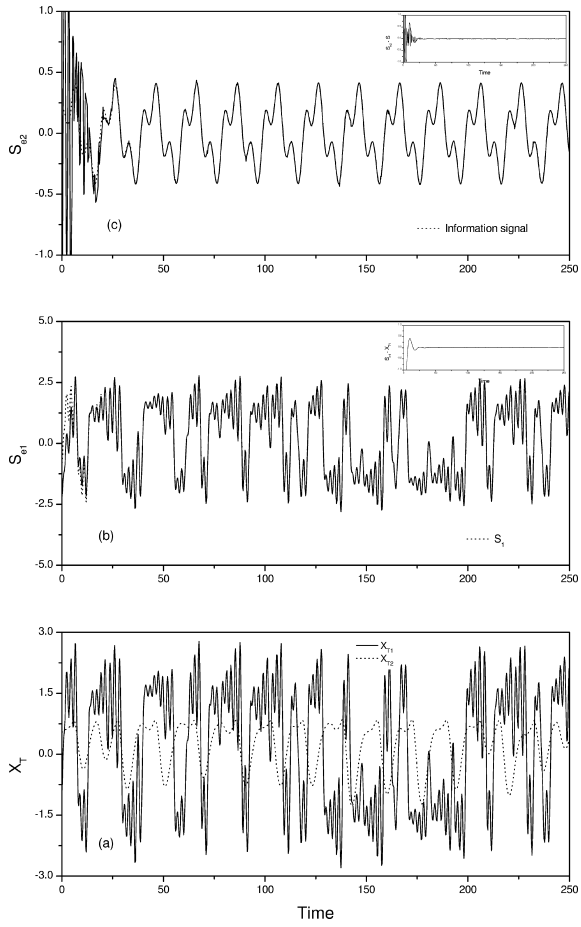

Fig. 4. (a) Time behavior of the transmitted signals and recovered signals (b) $\overline{x}_{T1}(t)$ (s_{e1}) and (c) $\overline{s}$ (s_{e2}) with the first and second demodulation procedures, respectively. The insert shows the recovering errors.

cases because of the higher-dimensional chaotic nature of the transmitted signal. In fact, it can be seen as a self-folding of the chaotic signal via nonlinear filtering transformation. Fig. 5(a) shows the chaotic attractor generated by the last chaotic subsystem in the modulation scheme. Fig. 5(b) shows the time behavior of the transmitted and the encoded information signals. Fig. 6 shows the recovered signals for the first (a), second (b) and third (c) demodulation procedures. We can see from Fig. 6(c) that the structure of the information signal was perfectly recovered. It can be seen that there is some information lost that propagates from the first to last decoder. However, this lost information can be minimized if we take smaller values of the estimation time-constants. We can see that some noises were introduced into the recovered results due small values of τ_e. However, this is not a serious drawback since this signal noise can be removed by means of low-pass filtering (e.g., second-order Butterworth filtering). In order to have access to the information signal, an intruder must be have the individual decoding algorithms and the order of the parameters in the Chua–Chua–Chua configuration.

In simulations above, we have used continuously differentiable signals. However, similar results are obtained with noncontinuous signals (i.e., $\{0, 1\}$-bit signal). Moreover, one can also use more complicated configurations without any difficulty.

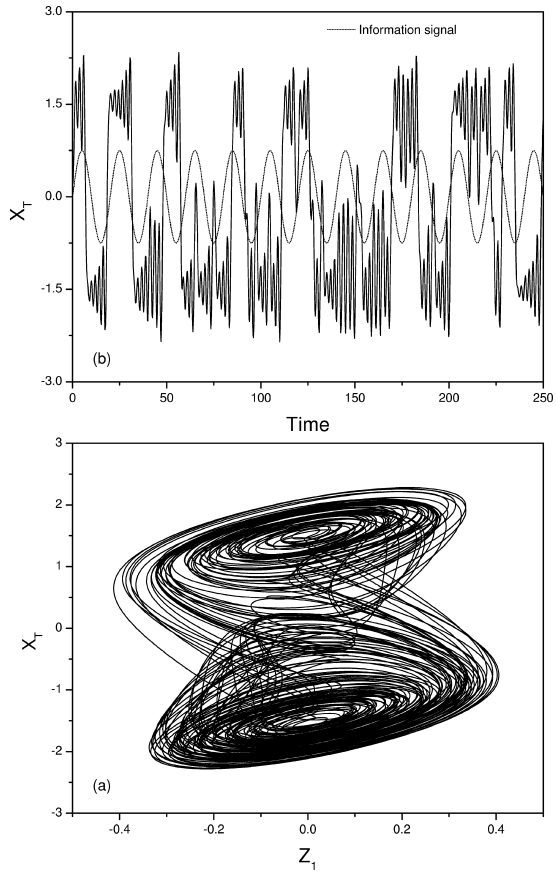

Fig. 5. (a) Chaotic attractor from the third transmitter subsystem and (b) time behavior of the transmitted and encoded information signals for the Chua–Chua–Chua configuration.

6. Conclusions

In this Letter, we have discussed a general method for encoding information signals based on low-dimensional chaotic oscillators. The modulation/demodulation (encoding/decoding) procedure is based on inverse dynamics methods where the nonlinear oscillator is used as a nonlinear filter. At the receiving channel, the information signal is recovered via a feedback approximation to the encoder inverse. The encoding procedure allows us to use a series of different chaotic oscillator to enhance the security of the communication system. Numerical examples of continuous systems were presented to illustrate the basic ideas and also to indicate possible directions of future research.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] C.W. Wu, L.O. Chua, Int. J. Bifurcation Chaos 4 (88) (1994) 979.
[3] U. Feldmann, M. Hasler, W. Schwarz, Int. J. Circuit Theory Appl. 24 (1996) 551.
[4] C.W. Wu, G.Q. Zhong, L.O. Chua, J. Circ. Syst. Comput. 6 (1996) 227.
[5] M. Itoh, C.W. Wu, L.O. Chua, Int. J. Bifurcation Chaos 7 (1997) 275.

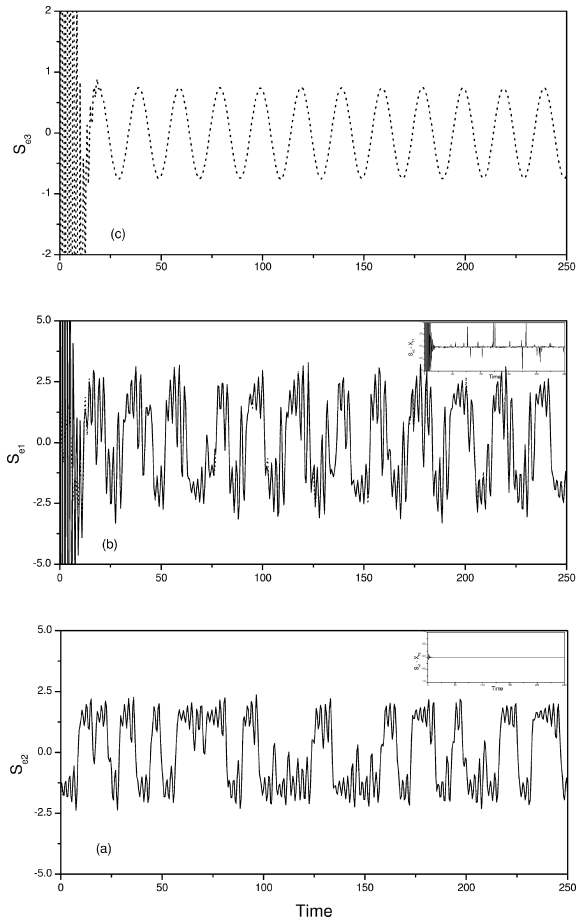

Fig. 6. Recovered signal with the (a) first $\overline{x}_{T2}(t)$ (s_{e1}), (b) second $\overline{x}_{T1}(t)$ (s_{e2}), and (c) third $\overline{s}(t)$ (s_{e3}) demodulation procedures in the Chua–Chua–Chua configuration. The insert shows the recovering errors.

[6] J. Alvarez-Ramirez, H. Puebla, J. Solis-Daun, Int. J. Bifurcation Chaos (2000), to be published.
[7] G. Heidari-Bateni, C.D. McGillem, M.F. Tenorio, in: Proc. Int. Commun. Conf., 1992, p. 1232.
[8] D.R. Frey, IEEE Trans. Circuits Syst. II 40 (1993) 660.
[9] A. Oksasoglu, T. Akgul, IEEE Trans. Circuits Syst. I 44 (1997) 75.
[10] N.J. Corron, D.W. Hahs, IEEE Trans. Circuits Syst. I 44 (1997) 373.
[11] K.M. Cuomo, A.V. Oppenheim, Int. J. Bifurcation Chaos 3 (1993) 1629.
[12] T.L. Carroll, L.M. Pecora, IEEE Trans. Circuits Syst. II 40 (1993) 646.
[13] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, U. Parlitz, Int. J. Bifurcation Chaos 2 (1992) 709.
[14] U. Parlitz, L. Kocarev, T. Stojanovski, H. Preckel, Phys. Rev. E 53 (1996) 4351.
[15] J.A. Suykens, P.F. Curran, L.O. Chua, IEEE Trans. Circuits Syst. I 46 (1999) 841.
[16] M.P. Kennedy, IEEE Trans. Circuits Syst. I 41 (1994) 771.
[17] H. Puebla, J. Alvarez-Ramirez, Phys. Lett. A 276 (2000) 245.
[18] M. Hasler, in: Proc. ISCAS Tutorial, 1994, p. 314.
[19] P.A. Ioannou, J. Sun, Robust Adaptive Control, Prentice-Hall, Upper Saddle River, NJ, 1996.
[20] V.S. Anishchenko, T. Kapitaniak, M.A. Safanova, O.V. Sosnovzeva, Phys. Lett. A 192 (1994) 207.
[21] X.F. Wang, Z.Q. Wang, IEEE Trans. Circuits Syst. I 45 (1998) 1101.
[22] L.O. Chua, Int. J. Circuit Theory Appl. 22 (1994) 279.
[23] M.P. Kennedy, IEEE Trans. Circuits Syst. I 42 (1995) 376.