A note on chaos-based communication schemes

D. López-Mancilla* and C. Cruz-Hernández**
Dirección de Telemática,
Centro de Investigación Científica y de Educación Superior de Ensenada, (CICESE),
with Electronics and Telecom. Dept.,
Km. 107, Carretera Tijuana-Ensenada, Ensenada, B.C., 22860, México
**e-mail: dlopez@cicese.mx*

Recibido el 28 de junio de 2004; aceptado el 17 de marzo de 2005

In this work, a modified chaos-based communication scheme is presented. In particular, we extend the basic scheme for chaotic masking using a single transmission channel proposed by Cuomo and coworkers in 1993. The substantial differences between the traditional scheme and this modified one, significantly affect the reception quality of the sent message, such that this one can faithfully be recovered without filtering at the receiver end, without considering the effect of noise in the transmission channel. Nevertheless, if noise is present, this can be eliminated using a filtering stage. We use two Lorenz systems unidirectionally coupled, the first like a master/transmitter system and the other like a slave/receiver system in order to illustrate with some numerical simulations the effectiveness of the modified scheme.

Keywords: Chaos synchronization; private communications; Lorenz system.

Este trabajo presenta un esquema modificado de comunicación confidencial basado en caos. En particular, se amplía el esquema básico de enmascaramiento caótico que utiliza un canal de transmisión propuesto por Cuomo y colaboradores en 1993. La diferencia esencial entre el esquema tradicional y el esquema modificado, se manifiesta en la calidad de recepción del mensaje transmitido, de tal manera que, éste puede recuperarse sin necesidad de filtrado en el receptor; siempre y cuando no exista ruido en el canal transmisor. No obstante, si éste está presente en el canal, puede eliminarse mediante una etapa de filtrado. Simulaciones numéricas confirman la efectividad de este esquema modificado, que utiliza dos sistemas de Lorenz acoplados unidireccionalmente, uno como maestro/transmisor y otro como esclavo/receptor.

Descriptores: Sincronización de caos; comunicaciones privadas; sistema de Lorenz.

PACS: 05.45.+b; 43.72.+q; 43.50.+y

1. Introduction

Recently, chaos synchronization has received a great deal of interest among researchers from several scientific fields. Different approaches for constructing synchronized chaotic systems are reported in the literature (see *e.g.*, [1-11] and references inside). Synchronization has opened the way to investigate an engineering application of chaos, to design private/secure communication systems [12-17].

In this work, we will focus in this interesting application. In particular, we shall discuss the chaotic communication system proposed by Cuomo and coworkers in Ref. 13 (based on chaos synchronization given by Pecora and Carroll [1]). The main problem with this communication scheme is as follows. In the chaotic signal masking scheme (with a single transmission channel), when the encrypted message is sent through the coupling signal, the states of the slave/receiver system do not synchronize with the corresponding states of the master/transmitter system. Thus, the private message signal is not recovered faithfully at the receiver end, and it is necessary a stage of low-pass filtering; this is because the signal message directly affects the dynamics of the slave/receiver system, and it is necessary that the signal message be too small (in amplitude), such that, an approximate synchronization exist, because of that the additive message could act like an external perturbation in the coupling signal. While smaller it is, more possibilities will be of recovering the message. However, if additive noise is considered in the transmission channel, there will be a difficult, if not impossible task if the amplitude of the coupling signal (including the message) is not large with respect to the noise level [16,21].

On the basis of these considerations, in this work, we extent the basic scheme for chaotic signal masking using a single transmission channel, given as consequence that the sent message can be recovered faithfully without a of low-pass filtering stage, if there is not an additive noise present in the transmission channel, and the signal message need not be too small to the recovered process. It is possible, however, to consider a noise level in the transmission channel, if so, we can to use a low-pass filter at the receiver end with the purpose to eliminate the noise effects only. In Ref. 14 an improved chaotic signal masking scheme is proposed, where the master/transmitter system is modified to remain synchronized with the slave/receiver system in presence of perturbation from the messages. In a similar way that in Ref. 15, we propose a modified chaotic signal masking scheme to achieve *exact synchronization* in presence of messages. At the same time, we mention that the substantial difference with Ref. 15 is that the modified scheme used there, only presented for a particular chaotic system, but the possible effects of a noise signal across the transmission channel are not considered.

The present work is organized as follows: In Sec. 2, we present our proposed modified chaos-based communication scheme. In Sec. 3, we give a description of the chaotic communication scheme with additive noise in the transmission channel. Numerical simulations illustrate the effectiveness

of our proposed modified scheme. Finally, Sec. 4 contains some concluding remarks.

2. Modified chaos-based communication scheme

Let the master system be given by the state equation

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

where $x(t) \in \mathbb{R}^n$ is the state vector. Pecora and Carroll suggested to divide the chaotic system (1) into two subsystems $\dot{v}(t)$ and $\dot{w}(t)$, and to create a new identical subsystem $\dot{w}'(t)$ to system $\dot{w}(t)$, replacing the set of variables $v(t)$ for the corresponding $v'(t)$, and with this new system, we have

$$\dot{v} = g(v, w), \quad \dot{w} = h(v, w), \quad \dot{w}' = h(v, w'),$$

where

$$v = (x_1, \ldots, x_m),$$
$$w = (x_{m+1}, \ldots, x_n),$$
$$g = (f_1(x), \ldots, f_m(x)),$$

and

$$h = (f_{m+1}(x), \ \ldots, f_n(x)).$$

They assure that the subsystems $\dot{w}(t)$ and $\dot{w}'(t)$ will synchronize only if the sub-Lyapunov exponents are all negative [1]. Then, we can take as master system to the Eq. (1) given by the subsystems

$$\dot{v} = g(v, w), \quad \dot{w} = h(v, w), \tag{2}$$

and as slave system to

$$\dot{v}' = g(v', w'), \quad \dot{w}' = h(v, w'). \tag{3}$$

If our purpose is only to achieve chaos synchronization between master and slave systems, then this approach is enough. Nevertheless, if we want to apply this synchronization to chaos-based communication systems we need to do more. For example, the chaotic communication scheme given in Ref. 13 is not effective, because if the message $m(t)$ is sent through the *coupling signal* $v(t)$, then exact synchronization is not achieved, and it is necessary to use a low-pass filtering stage, considering that there is not an additive noise present in the transmission channel. If noise is present, then will be a more difficult if not impossible task to recover the original message. Then, we need to analyze the structure of the receiver system when it is used as a chaotic masking scheme and back again to modify the transmitter system.

2.1. Receiver system

Suppose that a private message $m(t)$ is added to $v(t)$. The new coupling signal $s(t) = v(t) + m(t)$ arrives at the receiver system and modifies its structure, such that the receiver system now takes the form

$$\dot{v}' = g(v', w'), \quad \dot{w}' = h(s, w'). \tag{4}$$

It is easy to notice that the receiver system (4) does not synchronize with the transmitter system (2) using this approach, because that transmitter and receiver systems do not have identical structure. Now, the message $m(t)$ affects the dynamics of the receiver system.

2.2. Transmitter system

So, we need to modify the master system such that the message $m(t)$, also affects directly the dynamics of the master/transmitter system in the same way to that slave/receiver system, *i.e.*,

$$\dot{v} = g(v, w), \quad \dot{w} = h(v + m, w).$$

This is possible because the message $m(t)$ is known by the transmitter system. Thus, we can now guarantee that $w(t)$ synchronizes with $w'(t)$ using the approach proposed by Pecora and Carroll, but including the possible effects generated by $m(t)$ in both systems, no matter which magnitudes or forms of $m(t)$ have, as long as the master system remains in chaotic behavior, because for "secure" communication purpose, *i.e.*, the signal transmission must be chaotic.

2.3. Modified signal masking scheme

Now let us to make a fundamental modification at the scheme presented in Ref. 13. Figure 1 shows:

a) the chaos-based communication scheme for chaotic signal masking proposed by Cuomo *et al.*, and

b) the modified chaos-based communication scheme (both using a single transmission channel).

Note that, in our modified scheme, the signal used for the coupling purpose $v(t)$ is the same one as in the original scheme; and we have added the message in the same way $s(t) = v(t) + m(t)$, although the substantial modifications are, that now, the sent message $m(t)$ has been injected into the subsystem $\dot{w}(t)$ of the transmitter system, and we have added a noise signal $n'(t)$ to the transmission channel, such that $s'(t) = s(t) + n'(t)$, and the recovering of the message become a more difficult problem.

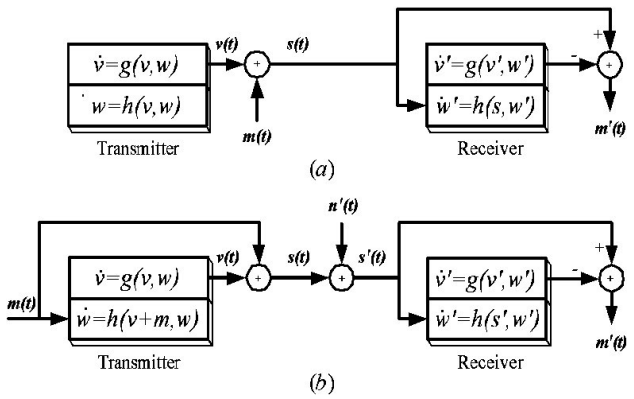

FIGURE 1. a) Chaos-based communication scheme proposed by Cuomo *et al.* b) Modified chaos-based communication scheme.

3. Chaotic Communication Using the Lorenz System

In order to illustrate and compare the modified communication scheme with previous by reported in Ref. 13, we use the *same* Lorenz system given by Ref. 18:

$$\begin{aligned}\dot{x} &= \sigma(y-x),\\ \dot{y} &= rx - y - xz,\\ \dot{z} &= xy - bz.\end{aligned}$$

It is well-known that with the parameter values $\sigma = 10$, $r = 28$, and $b = 8/3$, the Lorenz system exhibits chaotic dynamics. Let us take as master/transmitter system to

$$\begin{aligned}\dot{x} &= \sigma(y-x),\\ \dot{y} &= r(x+m) - y - (x+m)z,\\ \dot{z} &= (x+m)y - bz,\end{aligned} \tag{5}$$

where $v(t) = x(t)$ is taken, like the drive signal. If a signal message $m(t)$ is added to the drive signal, and $n'(t) = 0$, then $s'(t) = s(t) = x(t) + m(t)$ will drive to the slave/receiver system given by

$$\begin{aligned}\dot{x}' &= \sigma(y'-x'),\\ \dot{y}' &= rs - y' - sz',\\ \dot{z}' &= sy' - bz'.\end{aligned} \tag{6}$$

Assuming that the transmitter (5), and receiver (6) systems have the same parameter values, the dynamics of the synchronization error $e(t) = (e_x(t), e_y(t), e_z(t))$ is governed by

$$\begin{aligned}\dot{e}_x &= \sigma(e_y - e_x),\\ \dot{e}_y &= -e_y - se_z,\\ \dot{e}_z &= se_y - be_z,\end{aligned} \tag{7}$$

and, even considering the sent message $m(t)$, transmitter and receiver are synchronized because the error dynamics are globally asymptotically stable at the origin. This can be demonstrated by using the Lyapunov function

$$V(e) = \frac{1}{2}\left(\frac{1}{\sigma}e_x^2 + e_y^2 + e_z^2\right),$$

and its time-derivative along the trajectories of system (7) is given by

$$\dot{V}(e) = -\left(e_x - \frac{1}{2}e_y\right)^2 - \frac{3}{4}e_y^2 - be_z^2.$$

Then, since $V(e)$ is a positive definite function and $\dot{V}(e)$ is a negative definite function, $e(t) \to 0$ as $t \to \infty$. Note that $V(e)$ and $\dot{V}(e)$ are independent functions of $m(t)$. This mean that all states of transmitter and receiver systems synchronize, and if we take the difference $m'(t) = s(t) - x'(t) = x(t) + m(t) - x'(t)$, at the receiver end, when $x'(t) \to x(t)$, we obtain that $m'(t) \to m(t)$ as $t \to \infty$. Due to exact synchronization, it is possible faithfully recovering of $m(t)$.

In order to illustrate the effectiveness of our modified communication scheme, we present some numerical simulations, using an audio signal as the hidden message $m(t)$. All numerical simulations are developed with the same initial conditions $x, y, z(0) = (2, 5, -3)$, and $x', y', z'(0) = (1, -1, 0.5)$ respectively, and with the same parameter values established before, using the same confidential message $m(t)$, and the same filtering stage. Figure 2 shows the private information transmission using the communication scheme proposed by Cuomo *et al* [13], when $n'(t) = 0$:

a) The original audio message $m(t)$,

b) the phase plot in $x(t)$ versus $x'(t)$ plane,

c) the recovered message $m'(t)$ at the receiver end without filtering, and

d) the recovered message $m'(t)$ after a filtering stage.

Clearly, with this scheme the recovered message cannot be recovered faithfully, *i.e.*, $m'(t) \neq m(t)$. Figure 3 shows the private information transmission using the modified chaos-based communication scheme, when $n'(t) = 0$:

a) The original audio message $m(t)$,

b) the phase plot in $x(t)$ versus $x'(t)$ plane,

c) the transmitted drive signal $s(t) = x(t) + m(t)$, and

d) the recovered message $m'(t)$ at the receiver end without filtering.

Note that, with this modified communication scheme, the transmitted (drive) signal $s(t)$ remains in chaotic behavior and the original audio message $m(t)$ is recovered faithfully, *i.e.*, $m'(t) \equiv m(t)$ after synchronization time.

If noise is present, *i.e.*, $n'(t) \neq 0$, then the recovering of the message is more difficult and required a filtering stage will be for both schemes. Figure 4 shows the transmission through a noisy public channel using the communication scheme proposed by Cuomo *et al.*:

a) The original audio message $m(t)$,

b) the transmitted noisy drive signal $s'(t)$,

c) the recovered message $m'(t)$ at the receiver end when noise is present through transmission channel, and

d) the recovered message $m'(t)$ after a filtering stage.

Figure 5 shows the transmission through a noisy public channel using the modified chaos-based communication scheme:

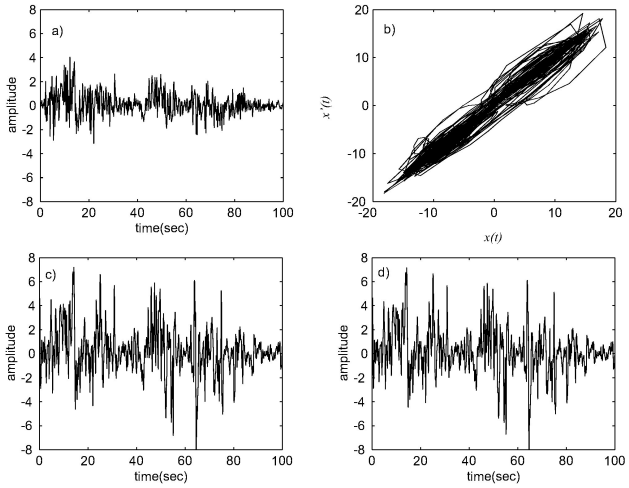

FIGURE 2. Transmission of private information using the communication scheme proposed by Cuomo *et al.*: a) Original audio message $m(t)$, b) phase plot in $x(t)$ versus $x'(t)$ plane, c) recovered message $m'(t)$ at the receiver end without filtering, and d) recovered message $m'(t)$ after a filtering stage.

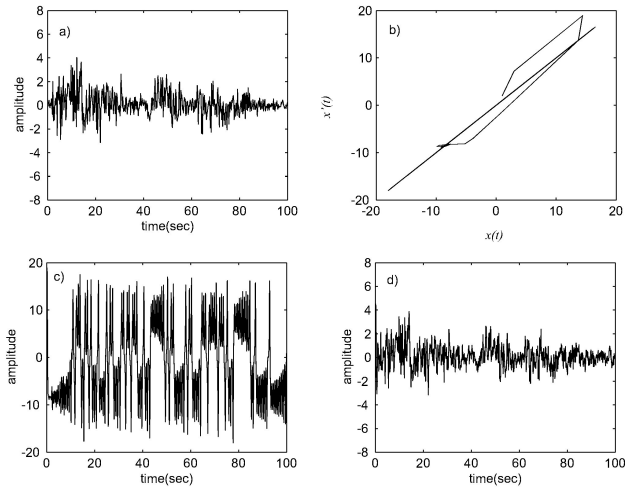

FIGURE 3. Transmission of private information using the modified communication scheme: a) Original audio message $m(t)$, b) phase plot in $x(t)$ versus $x'(t)$ plane, c) transmitted drive signal $s(t)$ including $m(t)$, and d) recovered message $m'(t)$ at the receiver end without filtering.

a) The original audio message $m(t)$,

b) the transmitted noisy drive signal $s'(t)$,

c) the recovered message $m'(t)$ at the receiver end when noise is present through transmission channel, and

d) the recovered message $m'(t)$ after a filtering stage.

In this case, when noise is present, the modified chaos-based communication scheme results to be useful to recover the message with high similarity to the original message $m(t)$, whereas with the other scheme this is not possible, even when $m(t)$ is small enough.

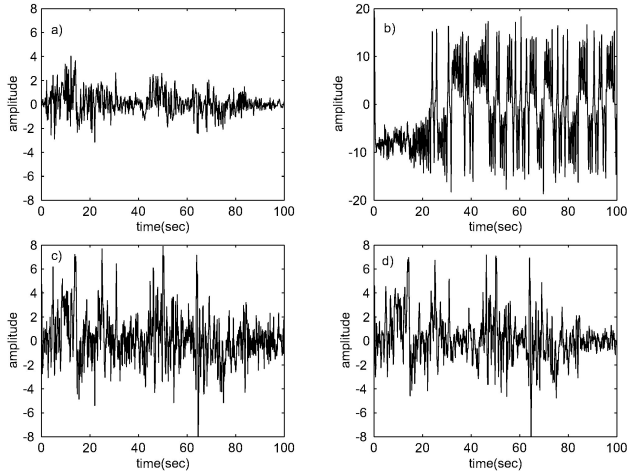

FIGURE 4. Transmission through a noisy public channel using the communication scheme proposed by Cuomo *et al.*: a) Original audio message $m(t)$, b) transmitted noisy drive signal $s'(t)$, c) recovered message $m'(t)$ at the receiver end when noise is present through transmission channel, and d) recovered message $m'(t)$ after a filtering stage.

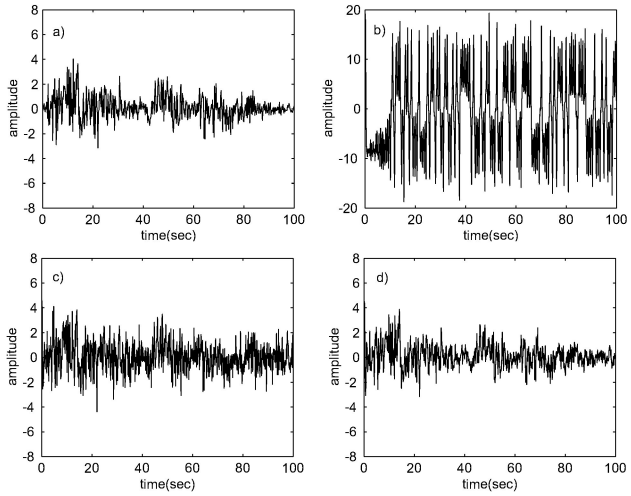

FIGURE 5. Transmission through a noisy public channel using the modified chaos-based communication scheme: a) Original audio message $m(t)$, b) transmitted noisy drive signal $s'(t)$, c) recovered message $m'(t)$ at the receiver end when noise is present through transmission channel, and d) recovered message $m'(t)$ after a filtering stage.

4. Concluding Remarks

In this paper, a modified chaos-based communication scheme has been presented. In particular, this work tries to contribute in the improvement of the basic communication scheme proposed by Cuomo *et al*. Besides, we have also illustrated that the modified chaos-based scheme is able to recover faithfully the hidden message even if a noise level is present through the transmission channel, if the noise magnitude is less than message magnitude. The Lorenz system was used to illustrate the effectiveness of this modified communication scheme over the previous, under identical conditions. The proposed modified scheme does not pretend to be useful for secure communications. Certainly, it has been demonstrated (under particular conditions) that signal masking technique has been broken. So, there is a chance of unmasking the hidden message from the transmitted chaotic signal (see *e.g.*, [19-21]). Nevertheless, the complexity of the transmitted chaotic signal can be increased if we use some methods (see *e.g.*, [17,22]) with this modified communication scheme in order to overcome the mentioned attacks.

Acknowledgments

This work was supported by the CONACYT, México under Research Grant No. 31874-A.

∗∗ Corresponding author: CICESE, Telematics Direction, P.O. Box 434944, San Diego, CA 92143-4944, USA, Phone: +52.646.1750500, Fax: +52.646.1750537, e-mail: ccruz@cicese.mx

1. L.M. Pecora and T.L. Carroll, *Phys. Rev. Lett.* **64** (1990) 821.
2. U. Feldmann, M. Hasler, and W. Schwarz, *Int. J. Circuits Theory and Applications* **24** (1996) 551.
3. H. Nijmeijer and I.M.Y. Mareels, *IEEE Trans. Circuits Syst. I* **44**(10) (1997) 882.
4. Special Issue on Chaos synchronization and control: Theory and applications. *IEEE Trans. Circuits Syst. I*, **44**(10) (1997).
5. G. Chen and X. Dong, *From chaos to order* (World Scientific, Singapore, 1998).
6. C. Cruz-Hernández and H. Nijmeijer, "Synchronization through extended Kalman filtering," *New Trends in Nonlinear Observer Design*, eds. H. Nijmeijer and T.I. Fossen, Lecture Notes in Control and Information Science 244, (Springer-Verlag, Berlin, 1999) p. 469.
7. C. Cruz-Hernández and H. Nijmeijer, *Int. J. Bifurc. Chaos* **10**(4) (2000) 763.
8. Special Issue on Control and synchronization of chaos. *Int. J. Bifurc. Chaos* **10**(3-4) (2000).
9. H. Sira-Ramírez and C. Cruz-Hernández, *Int. J. Bifurc. Chaos* **11**(5) (2001) 1381; *Procs. of American Control Conference (ACC' 2000)* (Chicago, USA, 2001) 769.
10. A. Aguilar and C. Cruz-Hernández, *WSEAS Trans. Systems* **1**(2) (2002) 198.
11. D. López-Mancilla and C. Cruz-Hernández, *WSEAS Trans. Mathematics* **3**(2) (2004) 364.
12. L. Kocarev, K.S. Halle, K. Eckert, and L.O. Chua, *Int. J. Bifurc. Chaos* **2**(3) (1992) 709.
13. K.M. Cuomo, A.V. Oppenheim, and S.H. Strogratz, *IEEE Trans. Circuits Syst. II* **40**(10) (1993) 626.
14. C.W. Wu and L.O. Chua, *Int. J. Bifurc. Chaos* **3**(6) (1993) 1619.
15. V. Milanović and M.E. Zaghloul, *Electronics Lett.* **32**(1) (1996) 11.
16. M. Hasler, *Int. J. Bifurc. Chaos* **8**(4) (1998) 647.
17. C. Cruz-Hernández, *Nonlinear Dynamics & Systems Theory* **4**(1) (2004) 1.
18. E.N. Lorenz, *J. Atmosph. Sci.* **20** (1963) 130.
19. K.M. Short, *Int. J. Bifurc. Chaos* **6**(2) (1996) 367.
20. K.M. Short, *Int. J. Bifurc. Chaos* **4**(4) (1994) 959.
21. G. Pérez and H.A. Cerdeira, *Phys. Rev. Lett.* **74**(11) (1995) 1970.
22. K. Murali, *Int. J. Bifurc. Chaos* **10**(11) (2000) 2489.