Adaptive synchronization of chaos for secure communication

S. Boccaletti, A. Farini, and F. T. Arecchi
Istituto Nazionale di Ottica, Largo Enrico Fermi, 6, 150125, Florence, Italy
(Received 14 August 1996)

We introduce a scheme for synchronization of chaos, whereby one combines the original Pecora and Carrols [Phys. Rev. Lett. **64**, 821 (1990)] procedure with an adaptive algorithm for chaos control. Based upon the knowledge of the local variation rates, the algorithm provides synchronization between a message sender and a message receiver and assures security in the communication against external interceptions. The effectiveness of the proposed scheme as well as its robustness are shown for the Lorenz system. [S1063-651X(97)01404-9]

PACS number(s): 05.45.+b, 89.70.+c

The idea of synchronizing two identical chaotic systems that start from different initial conditions was introduced by Pecora and Carrols (PC) [1]. It consists of linking the trajectory of one system to the same values in the other so that they remain in step with each other, through the transmission of a signal. This has been shown to occur when the sub-Liapunov exponents for the subsystem to be synchronized are all negative.

On the other hand, the possibility of encoding a message within a chaotic dynamics [2] through tiny perturbations of a control parameter has been recently shown. This suggests to use chaos synchronization to produce secure message communication between a sender and a receiver. However, several problems arise in assuring security in the communication. The main one is due to the fact that the sender must transmit to the receiver at least one of the system variables. As a result, a clever eavesdropper intercepting the communications can easily reconstruct the whole dynamics, hence decoding the message. To prevent this, Cuomo and Oppenheim [3] have proposed to use chaos to hide messages, so that the transmitted signal is now the sum of a chaotic signal and of a given message, which can be reconstructed by the receiver once synchronized with the sender. However, Perez and Cerdeira [4] have recently shown that messages masked by low-dimensional chaotic processes, once intercepted, can be sometimes readily extracted, so that the attention has been directed to the implementation of the original PC idea to higher dimensional systems [5] where increased randomness and unpredictability may improve security in the communication. But still the possibility of decoding the system through the reconstruction of the signal is not prevented.

Other problems rely on the limitations of the synchronizing procedure, namely, on the fact that synchronization is effective only provided that the subsystem to be synchronized shows negative sub-Liapunov exponents. Thus any additive signal introduced to hide the real message should be an infinitesimal perturbation of the signal itself, thus with the same effect as the natural noise within the communication procedure.

Even though enrichments of the PC method have been done [6] and alternative approaches to synchronization based on nonreplica subsystems have been proposed [7], the problem of security is not fully solved. On the other hand, trust and security in the communication are fundamental issues for confidential transfer of messages and/or information [8].

In this paper we present an adaptive scheme for chaos synchronization whereby one solves the problem of security in the communication against external interceptions. The scheme combines the original PC idea with a new adaptive algorithm for chaos control [9] in order to assure secure communication. Let us suppose to have a message sender (Alice) and a receiver (Bob) in the presence of a spy (James) ready to intercept and decode any communication between them. Alice consists of two identical chaotic systems

$$\begin{aligned} \dot{\mathbf{x}}_1 &= \mathbf{f}(\mathbf{x}_1, \mu), \\ \dot{\mathbf{x}}_2 &= \mathbf{f}(\mathbf{x}_2, \mu), \end{aligned} \tag{1}$$

where μ is a set of control parameters chosen in such a way as to produce chaos, $\mathbf{x}_1$, $\mathbf{x}_2$ are two D-dimensional vectors ($D \geqslant 3$) and $\mathbf{f}$ is a nonlinear function. On the other hand, Bob consists of a third identical system,

$$\dot{\mathbf{x}}_3 = \mathbf{f}(\mathbf{x}_3, \mu). \tag{2}$$

The three systems start from different initial conditions, thus producing unsynchronized dynamics. For the sake of exemplification, in the following the three systems will be represented by the three variable Lorenz system [10]. Then the vectors $\mathbf{x}_j \equiv (x_j, y_j, z_j)$ $(j=1,2,3)$ obey the equations

$$\begin{aligned} \dot{x}_j &= \sigma(y_j - x_j), \\ \dot{y}_j &= r x_j - y_j - x_j z_j, \\ \dot{z}_j &= -b z_j + x_j y_j. \end{aligned} \tag{3}$$

The message Alice must transmit to Bob is encoded in the variable $x_1(t)$. The scheme for the communication is represented in Fig. 1.

The first step is to produce synchronization between $\mathbf{x}_2$ and $\mathbf{x}_3$. For this purpose, Bob sends to Alice the variable $y_3(t)$, which replaces y_2 into the equations for x_2 and z_2. Synchronization is assured by the fact that the sub-Liapunov exponents for the subsystem (x_2, z_2) are both negative [1] (for $\sigma=10$, $b=\frac{8}{3}$ and $r=60$ they are -2.67 and -9.99, respectively).

Then Alice knows the whole actual dynamical state of Bob and consequently can transmit to Bob the perturbation $U(t)$ to be applied to the x_3 equation in order to synchronize the system $\mathbf{x}_3$ to $\mathbf{x}_1$. Alice uses a recently introduced adaptive method for chaos control [9] and recognition [11], which is

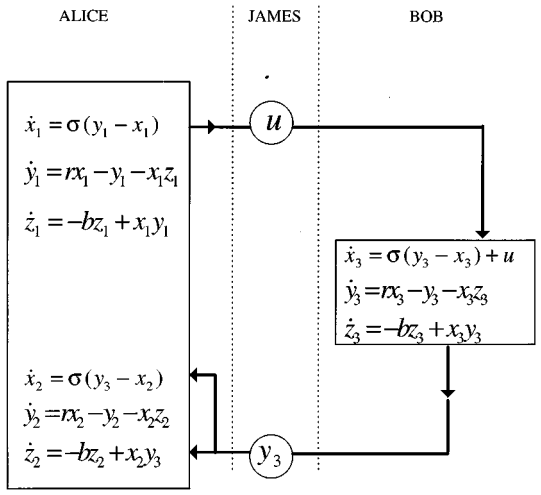

FIG. 1. The scheme for adaptive synchronization. Bob sends to Alice the variable y_3 to synchronize $\mathbf{x}_2$ and $\mathbf{x}_3$. Alice sends to Bob the adaptive correction $U(t)$ to be added to the evolution equation for x_3. James can intercept both $U(t)$ and y_3.

also able to slave a system to a given goal dynamics. In the present case, the system to be slaved is $\mathbf{x}_3$ and the goal dynamics is $\mathbf{x}_1$. Namely, at any of Alice's observation times $t_{n+1}=t_n+\tau_n$ [τ_n being the adaptive observation time interval (OTI) to be specified later], Alice defines the difference between current and target dynamics

$$\delta_{n+1}=x_2(t_{n+1})-x_1(t_{n+1}), \tag{4}$$

and its local variation rate over τ_n,

$$\lambda_{n+1}=\frac{1}{\tau_n}\log\left|\frac{\delta_{n+1}}{\delta_n}\right|. \tag{5}$$

Then Alice updates the new OTI as

$$\tau_{n+1}=\tau_n[1-\tanh(g\lambda_{n+1})]. \tag{6}$$

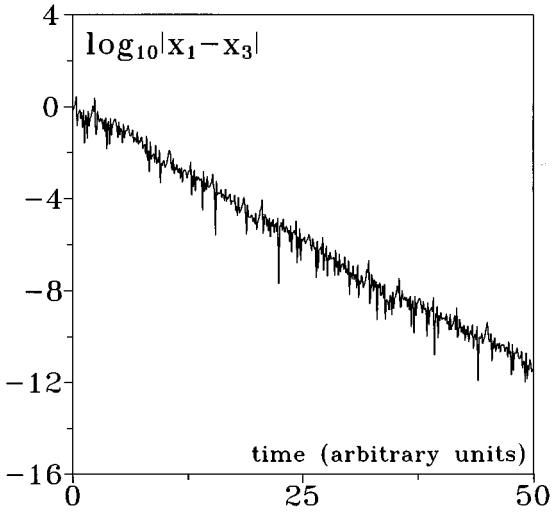

FIG. 2. Temporal evolution of the quantity $\log_{10}(|x_1-x_3|)$ measuring the synchronization between $\mathbf{x}_1$ and $\mathbf{x}_3$, thus indicating how accurate Bob is in receiving and decoding the message sent by Alice. $\sigma=10$, $b=\frac{8}{3}$, $r=60$, $\tau_0=0.01$, $\delta_0=1$, $g=0.011$, $K=0.1$.

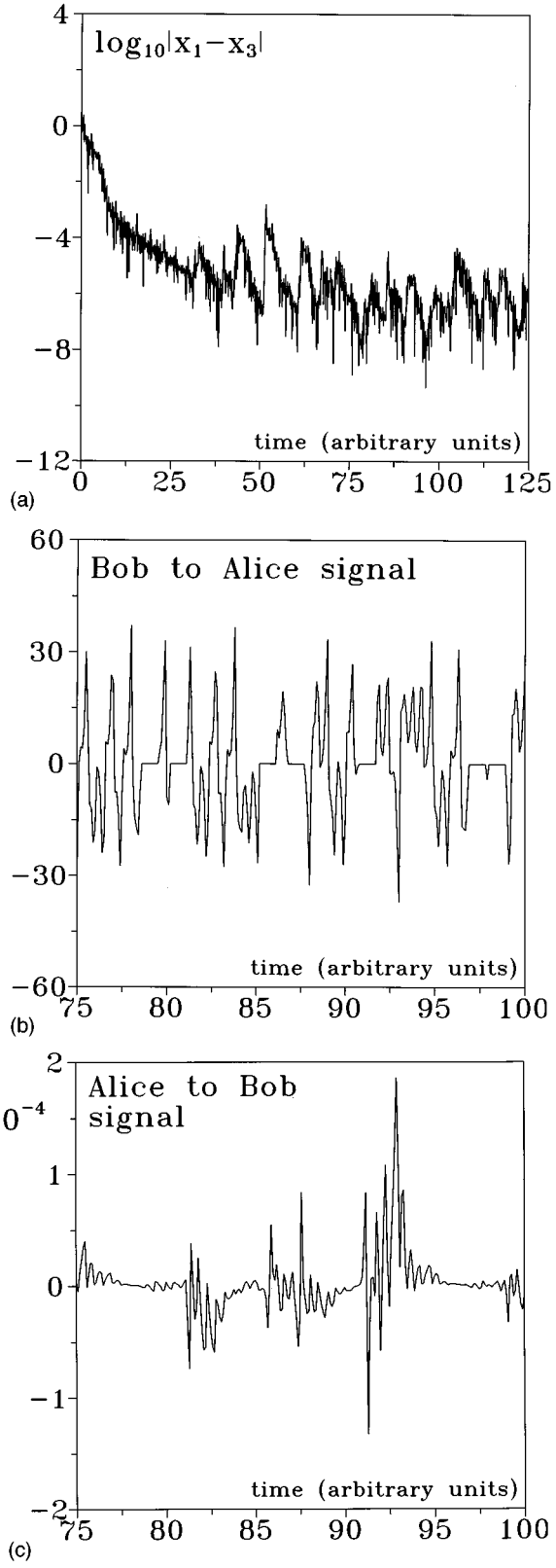

FIG. 3. (a) Temporal evolution of $\log_{10}(|x_1-x_3|)$ for $\theta=10^{-5}$ and $T_0=1>1/\Lambda\simeq 0.71$. The stipulated accuracy in the transmission is preserved in time even though (b) the synchronization signal Bob sends to Alice is affected by large holes, that prevent any reconstruction of the message, and (c) the controlling signal $U(t)$ is kept within a range negligible with respect to the dynamics. Other parameters as in Fig. 2.

The hyperbolic tangent function maps the whole range of $g\lambda$ into the interval $(-1, +1)$. The constant g, strictly positive, represents the sensitivity of the algorithm and it is limited in such a way as to forbid τ_{n+1} from going to zero [11]. Then Alice fixes the new observation at the time $t_{n+2}=t_{n+1}+\tau_{n+1}$. Starting from a given $\tau_0=\tau(t=0)$ and a given $\delta_0=\delta(t=0)$, Alice obtains a sequence of OTI that minimizes the second variations between actual and target dynamics. The analysis of such a sequence leads to the extraction of the main properties of the dynamics [9,11].

The signal Alice sends to Bob is then

$$U(t)=\frac{K}{\tau_{n+1}}[x_1(t)-x_2(t)] \tag{7}$$

($K>0$), which is added to the evolution equation for x_3. $U(t)$ is the product of two factors. The difference between actual and target value of the variable is a continuous time function, while the weighting factor K/τ_{n+1} is updated at discrete times by means of the above iterative algorithm.

Looking at Eq. (5), we easily realize that λ's locally measure how the separation of the actual orbit from the desired one evolves. Indeed, negative λ means that locally the trajectory is collapsing into the desired one and hence the actual dynamics is shadowing the goal behavior, while positive λ implies that the trajectory is locally diverging away from the desired one. Thus, contraction or expansion of τ's reflects the necessity to disturb the system more or less robustly in order to constrain it to shadow the goal dynamics.

In other words, the method introduces a natural adaptation time scale in which the same adaptive dynamics selects the correction term to be added to the evolution equation of x_3. Indeed, $U(t)$ is inversely proportional to the time intervals and hence is weighted by the information extracted from the dynamics itself. As reported in Ref. [10], this natural adaptation time scale is smaller than the time scales of the unstable periodic orbits embedded within the chaotic attractor. Notice that the limit $g=0$ of our algorithm represents the well-known Pyragas' controlling method [12], which has been shown to be effective in the stabilization of unstable periodic orbits both in low- and in high-dimensional chaotic systems.

To demonstrate the effectiveness of the proposed scheme, Fig. 2 reports the temporal behavior of $\Delta x=|x_1-x_3|$, which measures the synchronization between Alice and Bob for $\sigma=10$, $b=\frac{8}{3}$, and $r=60$. Similar results hold also for $|y_1-y_3|$ and $|z_1-z_3|$, thus indicating that the systems $\mathbf{x}_1$ and $\mathbf{x}_3$ are globally synchronized. As a consequence, any message encoded within x_1 is easily received and decoded by Bob.

Let us now discuss the problem of security. James intercepts the two communication signals $U(t)$ and $y_3(t)$. No information on x_1 can be retrieved from $U(t)$ since (i) this signal vanishes as soon as Alice and Bob reach synchronization, and (ii) the weighting factor K/τ_{n+1} is not decided *a priori*, but it is continuously changed by the same dynamics, hence no fixed rule is available to James to decode the signal. One may speculate that, from the knowledge of y_3, James can easily reconstruct the whole attractor corresponding to the system $\mathbf{x}_3$, thus reconstructing the message once $\mathbf{x}_3$ becomes synchronized with $\mathbf{x}_1$. This possibility can easily be prevented, due to the robustness of the method here presented.

Indeed, once Alice and Bob have previously agreed on a given accuracy θ in the reception of the message, each time such an accuracy has been reached (Alice can test it since she has full information on the dynamical state of Bob), Bob stops sending y_3 for a given time T_0. In this time the two systems $\mathbf{x}_2$ and $\mathbf{x}_3$ evolve separately. After T_0 Bob starts again sending y_3 to Alice. If T_0 exceeds the decorrelation time $\tilde{\tau}$ of the system (reciprocal of the maximum Liapunov exponent Λ), then the effective signal sent by Bob to Alice results in the collection of uncorrelated temporal subsequences. Thus, no reconstruction of $\mathbf{x}_3$ is possible by James in this case.

This procedure relies crucially on the robustness of the synchronizing method. In Fig. 3 we report the results for $T_0=1$ and $\theta=10^{-5}$ (notice that in our case $\Lambda\simeq 1.41$, hence $T_0>\tilde{\tau}\simeq 0.71$). Our scheme is able to maintain the stipulated accuracy [Fig. 3(a)] even in the case in which the signal sent by Bob to Alice is affected by large holes [Fig. 3(b)], which prevents any possible external reconstruction of the dynamical state $\mathbf{x}_3(t)$. Finally, Fig. 3(c) shows the controlling signal, which still remains confined within a range negligible with respect to the x_1 dynamics (x_1 variations from -28 to 28). Both things are assured by the adaptive nature of our scheme.

In conclusion, we have presented an adaptive scheme for chaos synchronization that solves the problem of security in the communication even in the case of low-dimensional chaotic systems.

We acknowledge M. Ding for fruitful discussions.

[1] L. M. Pecora and T. L. Carrols, Phys. Rev. Lett. **64**, 821 (1990).
[2] S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781 (1994).
[3] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[4] G. Perez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[5] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, Phys. Rev. Lett. **76**, 904 (1996).
[6] T. C. Newell *et al.*, Phys. Rev. Lett. **72**, 1647 (1994); N. Gershenfeld and G. Grinstein, *ibid.* **74**, 5024 (1995); Lj. Kocarev and U. Parlitz, *ibid.* **74**, 5028 (1995).
[7] M. Ding and E. Ott, Phys. Rev. E **49**, R945 (1994).
[8] T. Beth, Sci. Am. **273** (6), 70 (1995).
[9] S. Boccaletti and F. T. Arecchi, Europhys. Lett. **31**, 127 (1995).
[10] E. N. Lorenz, J. Atmos. Sci. **20**, 130 (1963).
[11] F. T. Arecchi, G. Basti, S. Boccaletti, and A. L. Perrone, Europhys. Lett. **26**, 327 (1994).
[12] K. Pyragas, Phys. Lett. A **170**, 421 (1992).