Efficient signal transmission by synchronization through compound chaotic signal

K. Murali and M. Lakshmanan
Centre for Nonlinear Dynamics, Department of Physics, Bharathidasan University, Tiruchirappalli 620 024, India
(Received 22 January 1997)

The idea of synchronization of chaotic systems is further extended to the case where all the drive system variables are combined suitably to obtain a compound chaotic signal. An appropriate feedback loop is constructed in the response system to achieve synchronization among the variables of the drive and response systems. We apply this approach to transmit both analog and digital data signals in which the quality of the recovered signal is higher and the encoding is more secure. [S1063-651X(97)05107-6]

PACS number(s): 05.45.+b, 43.72.+q, 47.52.+j

The concept of synchronized chaos [1–22] allows for the possibility of building a set of chaotic dynamical systems such that their common signals are synchronized. In general there are two methods of chaos synchronization which have been studied extensively [1–8]. In the first method, due to Pecora and Carroll [1], a stable subsystem of a chaotic system is synchronized with a separate chaotic subsystem under suitable conditions. This method has been further extended to cascading chaos synchronization with multiple stable subsystems [1–5]. The second method to achieve chaos synchronization is due to the approach of one-way coupling, in which two identical chaotic systems are synchronized without requiring construction of any stable subsystems [6–8]. In both these approaches only one chaotic signal from the drive system is utilized to drive the response systems. In the present paper, the idea of synchronization of chaotic systems is further extended to the case where all the drive system variables are combined suitably so that a compound chaotic drive signal is so produced to drive the response system. A feedback loop in the response system is constructed appropriately to achieve synchronization among the variables of the drive and response systems. The present method is entirely different from the recently proposed method of synchronization through active-passive decomposition (APD) of dynamical systems [18] in which suitable combinations of chaotic signals are used to drive both drive and response chaotic systems. In this approach the response system has to be suitably modified to achieve synchronization. However, the proposed method in which both drive and response systems are totally unaltered is entirely different and it can be easily implemented in practical situations for communications.

The present method of chaos synchronization is described as follows. Let us consider an arbitrary N-dimensional (chaotic) dynamical system

$$\dot{\mathbf{z}}=\mathbf{f}(\mathbf{z}). \tag{1}$$

Now let us consider the following form of the drive system equations:

$$\dot{\mathbf{x}}=\mathbf{f}(\mathbf{x})+\epsilon[v(t)-x_j(t)], \tag{2}$$

$$\dot{\mathbf{y}}=\mathbf{f}(\mathbf{y})+\epsilon[u(t)-y_j(t)], \tag{3}$$

where $\mathbf{x}$ and $\mathbf{y}$ are identical copies of $\mathbf{z}$. In Eqs. (2) and (3) the terms proportional to the coupling strength ϵ are nonzero only for the jth components. If $v(t)=y_j(t)$ and $u(t)=x_j(t)$ then Eqs. (2) and (3) are two identical mutually coupled chaotic systems. This kind of mutually coupled chaotic systems has been well studied in detail and for appropriate ϵ values, the systems (2) and (3) self-synchronize with each other [9,10]. Now the two mutually coupled self-synchronized systems (2) and (3) are considered together as a single *drive* system. Then the concept of chaos synchronization through *drive-response* formalism can be established by considering the *response* system equations as

$$\dot{\mathbf{x}}_{\mathbf{r}}=\mathbf{f}(\mathbf{x}_{\mathbf{r}})+\epsilon_r[v_r(t)-(x_r)_j(t)]. \tag{4}$$

Equation (4) is the copy of Eq. (1) driven by the signal $v_r(t)=v(t)$ through one-way coupling [6–8]. Here ϵ_r is the one-way coupling parameter. If the maximal Lyapunov exponent of Eq. (4) is negative under the influence of the chaotic signal $v_r(t)$ added to the jth component of the response system vector field $\dot{\mathbf{x}}_{\mathbf{r}}=\mathbf{f}(\mathbf{x}_{\mathbf{r}})$, then $\|\mathbf{x}_{\mathbf{r}}-\mathbf{y}\|\rightarrow\mathbf{0}$ for $t\rightarrow\infty$. Synchronization between systems (2) and (3) occurs if the dynamical system describing the evolution of the difference $\mathbf{e}=\mathbf{x}-\mathbf{y}$,

$$\dot{\mathbf{e}}=\dot{\mathbf{x}}-\dot{\mathbf{y}}, \tag{5}$$

possesses a stable fixed point at the origin $\mathbf{e}=\mathbf{0}$. Also synchronization between systems (4) and (3) occurs if the dynamical system describing the evolution of the difference $\mathbf{e}_{\mathbf{r}}=\mathbf{x}_{\mathbf{r}}-\mathbf{y}$,

$$\dot{\mathbf{e}}_{\mathbf{r}}=\dot{\mathbf{x}}_{\mathbf{r}}-\dot{\mathbf{y}}, \tag{6}$$

possesses a stable fixed point at the origin $\mathbf{e}_{\mathbf{r}}=\mathbf{0}$. This can be further proved by using (global) Lyapunov functions [3,13].

However, it is not necessary that only one of the drive variables alone is used for synchronization with the response system $(v_r(t)=y_j(t))$. One can also combine and modify the drive signal appropriately, and then the transformation can be undone at the response system for synchronization. Along these lines, Carroll recently reported the synchronization of chaotic systems using filtered signals [19]. Alternatively, instead of using one drive signal variable, one can transform the drive system variables by appropriate linear or

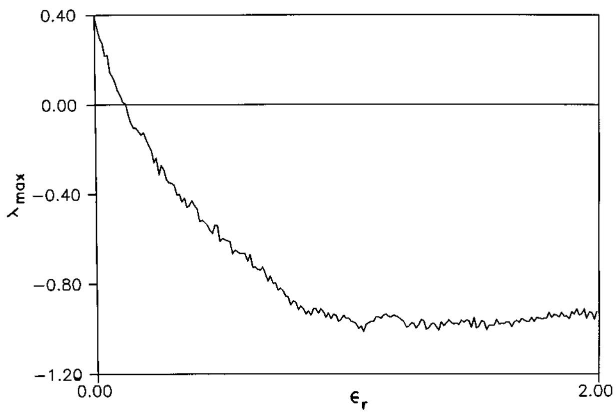

FIG. 1. Maximal conditional Lyapunov exponent $\lambda_{\max}$ versus ϵ_r of the response system equations (23)–(25).

nonlinear combinations (can be treated as *encryption key function*) to produce a compound chaotic signal for use as the drive signal for synchronization with the response system [22]. A suitable feedback loop can be devised in the response system to achieve synchronization among the variables of the drive and response systems. This approach of synchronization can be described as follows for the drive system (1) and (2). *The drive encryption key is*

$$K_d = h(\mathbf{y}), \tag{7}$$

where $h(\mathbf{y})$ is the linear or nonlinear encryption key function. *The compound drive signal is*

$$d(t) = v(t) + K_d. \tag{8}$$

The response system (4) is altered as follows. *The response encryption key is*

$$K_r = h(\mathbf{x_r}) \tag{9}$$

and the regenerated drive signal is

$$v_r(t) = d(t) - K_r, \tag{10}$$

$$\dot{\mathbf{x}}_\mathbf{r} = \mathbf{f}(\mathbf{x_r}) + \epsilon_r(v_r(t) - (x_r)_j(t)). \tag{11}$$

In this case also if the dynamical equation for the difference $\mathbf{e_r} = \mathbf{x_r} - \mathbf{y}$,

$$\dot{\mathbf{e}}_\mathbf{r} = \dot{\mathbf{x}}_\mathbf{r} - \dot{\mathbf{y}}, \tag{12}$$

possesses a stable fixed point at the origin $\mathbf{e_r} = \mathbf{0}$, then synchronization between systems (11) and (3) occurs for suitable ϵ_r. In general, however, the stability has to be checked numerically using the fact that synchronization occurs if the maximal Lyapunov exponent of Eq. (11) is negative under the influence of regenerated drive signal at the response system for appropriate one-way coupling parameter ϵ_r [3,6–8,13].

To demonstrate the above scheme of chaos synchronization we consider the well-known Chua circuit model. The model drive equations are represented as

$$\dot{x}_1 = \alpha\{[x_2 - x_1 - g(x_1)] + \epsilon[v(t) - x_1]\}, \tag{13}$$

$$\dot{x}_2 = x_1 - x_2 + x_3, \tag{14}$$

$$\dot{x}_3 = -\beta x_2, \tag{15}$$

$$\dot{y}_1 = \alpha\{[y_2 - y_1 - g(y_1)] + \epsilon[u(t) - y_1]\}, \tag{16}$$

$$\dot{y}_2 = y_1 - y_2 + y_3, \tag{17}$$

$$\dot{y}_3 = -\beta y_2, \tag{18}$$

where $g(x) = bx + 0.5(a-b)(|x+1| - |x-1|)$ and $a = -1.27$, $b = -0.68$, $\alpha = 10.0$, and $\beta = 14.87$. If $v(t) = y_1$ and $u(t) = x_1$ then for appropriate values of mutual coupling parameter ϵ (we choose here $\epsilon = 1.5$), the above system of Eqs. (13)–(18) self-synchronizes. After synchronization $x_1 = y_1$, $x_2 = y_2$, and $x_3 = y_3$. Now let us consider the drive encryption key function as *the drive encryption key*

$$K_d = y_2, \tag{19}$$

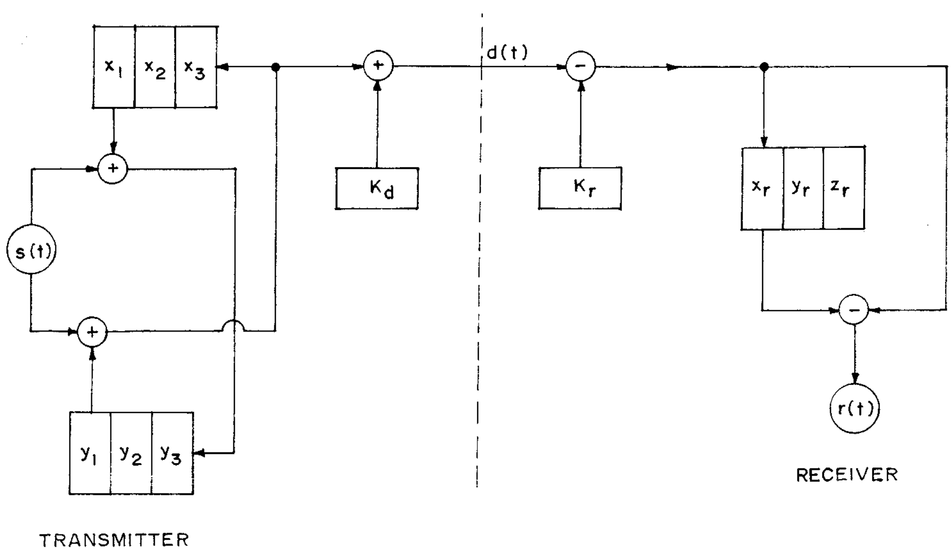

FIG. 2. Schematic diagram of the signal transmission method using compound chaotic signal.

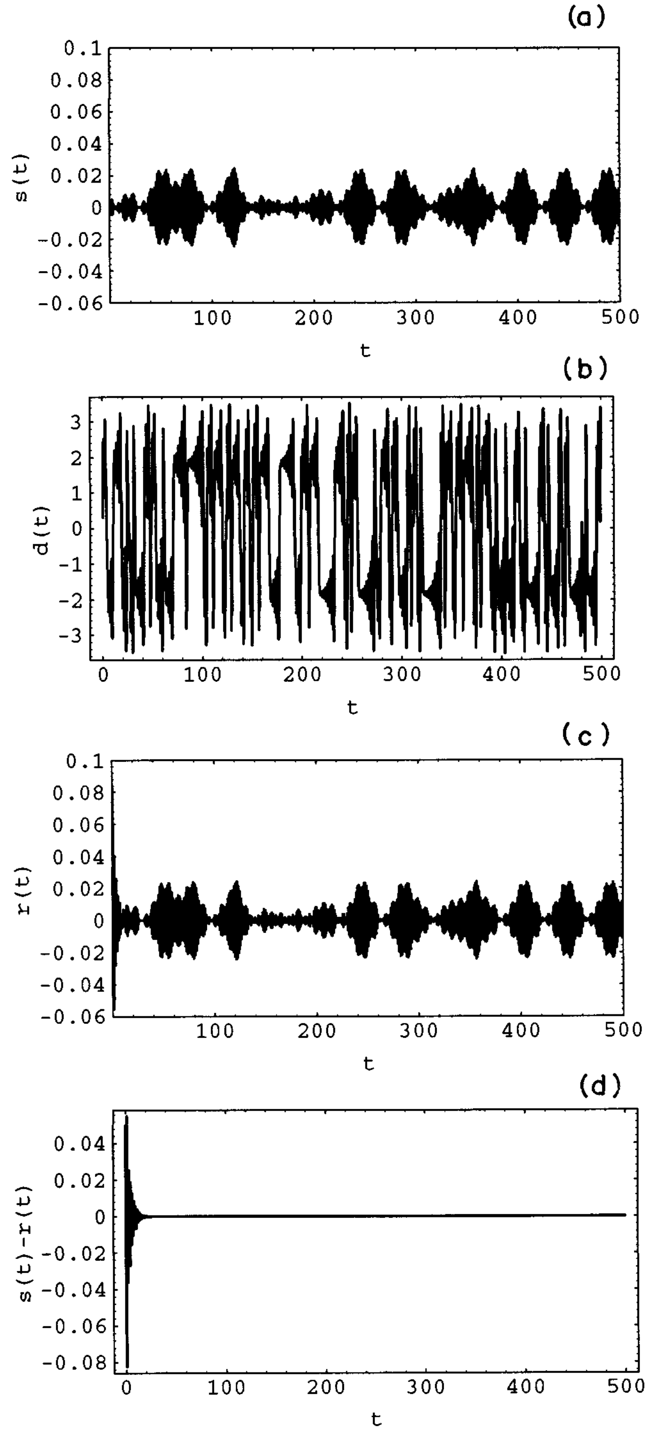

FIG. 3. Numerical encoding and decoding of a *speechlike signal* $s(t)$ using the systems (13)–(20) and (21)–(25) for $\epsilon_r = 1.5$ and $\epsilon = 1.5$. (a) Information signal $s(t)$, (b) transmitted compound chaotic signal $d(t)$, (c) recovered information signal $r(t)$ [using Eq. (38)], (d) error signal $s(t)-r(t)$. Note the perfect recovery of the signal $s(t)$.

and the compound drive signal

$$d(t)=v(t)+K_d=y_1+y_2. \tag{20}$$

Then the response system equations are *the response encryption key*

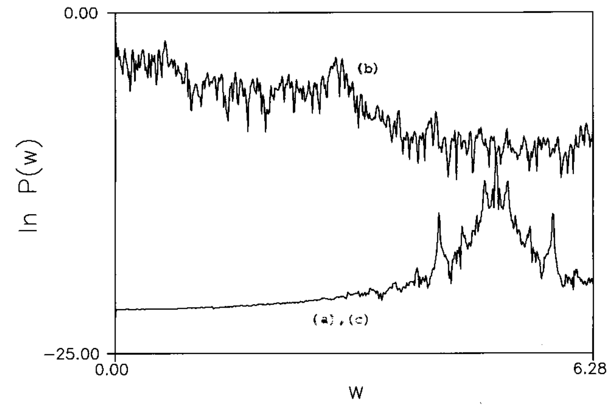

FIG. 4. Power spectrum of the information signal $s(t)$ (a), transmitted signal $d(t)$ (b), and recovered signal $r(t)$(c). Note again the coincidence of the spectrum of (a) and (c).

$$K_r=y_r, \tag{21}$$

and the regenerated drive signal

$$v_r(t)=d(t)-K_r=d(t)-y_r, \tag{22}$$

$$\dot{x}_r=\alpha\{[y_r-x_r-g(x_r)]+\epsilon_r[v_r(t)-x_r]\}, \tag{23}$$

$$\dot{y}_r=x_r-y_r+z_r, \tag{24}$$

$$\dot{z}_r=-\beta y_r. \tag{25}$$

The difference system ($\mathbf{e=x-y}$) of Eqs. (13)–(15) and Eqs. (16)–(18) is

$$\dot{e}_1=\alpha[(e_2-e_1-s_ie_1)-2\epsilon e_1], \tag{26}$$

$$\dot{e}_2=e_1-e_2+e_3, \tag{27}$$

$$\dot{e}_3=-\beta e_2, \tag{28}$$

where $s_i=a$ or b ($i=1$ or 2) which is determined from $g(x)$ [10,22]. It is easy to prove that the temporal derivative of the Lyapunov function

$$E=(\beta/2)e_1^2+(\alpha\beta/2)e_2^2+(\alpha/2)e_3^2 \tag{29}$$

is negative,

$$\dot{E}=\beta e_1\dot{e}_1+\alpha\beta e_2\dot{e}_2+\alpha e_3\dot{e}_3 \tag{30}$$

$$=-\alpha\beta(e_1-e_2)^2-\alpha\beta(a+2\epsilon)e_1^2, \tag{31}$$

for all e_1,e_2,e_3 when $\epsilon>-a/2$. (Note that $a<b<0$ and $a=-1.27$) [10,13].

Also, the difference system of Eqs. (16)–(20) and Eqs. (21)–(25) is given as

$$\dot{e}_x=\alpha[(e_y-e_x-s_ie_x)-\epsilon_r(e_x+e_y)], \tag{32}$$

$$\dot{e}_y=e_x-e_y+e_z, \tag{33}$$

$$\dot{e}_z=-\beta e_y, \tag{34}$$

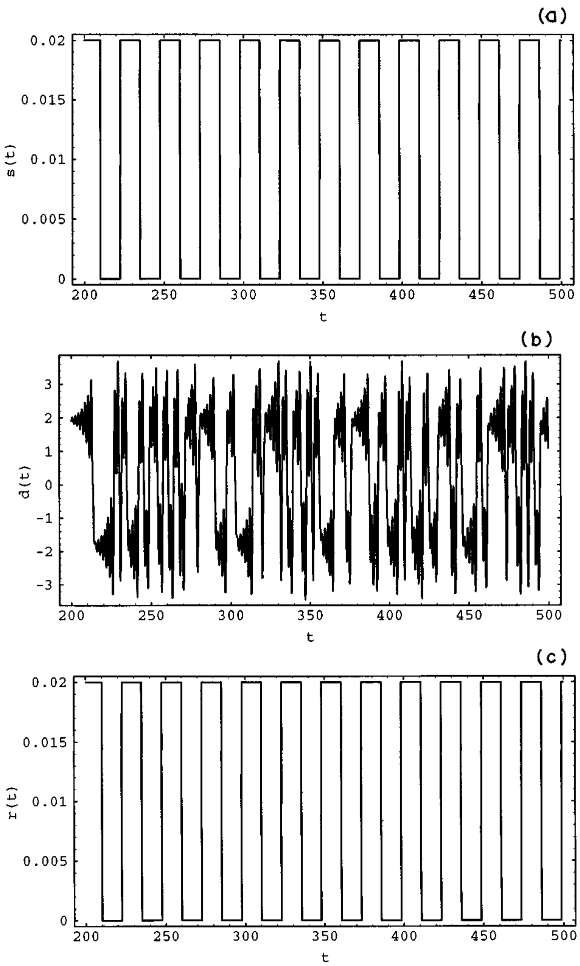

FIG. 5. Numerical encoding and decoding of a *digital signal* $s(t)$ using the systems (13)–(20) and (21)–(25) for $\epsilon_r = 1.5$ and $\epsilon = 1.5$. (a) Information signal $s(t)$, (b) transmitted compound chaotic signal $d(t)$, (c) recovered information signal $r(t)$ [using Eq. (38)].

where $e_x = (x_r - y_1)$, $e_y = (y_r - y_2)$, and $e_z = (z_r - y_3)$. It is again easy to prove that the temporal derivative of the Lyapunov function

$$E = (\beta/2)e_x^2 + [\alpha\beta(1+\epsilon_r)/2]e_y^2 + [\alpha(1+\epsilon_r)/2]e_z^2 \quad (35)$$

is negative,

$$\dot{E} = \beta e_x \dot{e}_x + \alpha\beta(1+\epsilon_r)e_y\dot{e}_y + \alpha(1+\epsilon_r)e_z\dot{e}_z \quad (36)$$

$$= -\alpha\beta[(e_x - e_y)^2 + \epsilon_r e_y^2] - \alpha\beta(a+\epsilon_r)e_x^2 \quad (37)$$

for all e_x, e_y, e_z when $\epsilon_r > -a$. In Eq. (37) the equality sign applies only at the origin; therefore, the synchronization between the drive system equations [Eqs. (16)–(20)] and response system equations [Eqs. (21)–(25)] is globally asymptotically stable. This can be further checked numerically by computing the maximal Lyapunov exponent of the response system Eqs. (23)–(25) as a function of the one-way coupling parameter ϵ_r as shown in Fig. 1. It is evident from this figure that the response system is synchronized with the drive counterpart, which is confirmed by a change in the sign of the maximal conditional Lyapunov exponent of the response system from positive to negative [1–8].

The above scheme of synchronization may be used to construct transmitter-receiver systems for encoding and masking information data signals. The schematic representation of this approach is depicted in Fig. 2. To send the information signal $s(t)$ from the transmitter to receiver using the familiar *chaos signal masking technique* [2,4,5,11,18], now the signals $v(t)$ and $u(t)$ are modified as $v(t) = y_1 + s(t)$ and $u(t) = x_1 + s(t)$, respectively. The significance of this type of encoding the message signal $s(t)$ is not only to add the signal to certain chaotic carrier but also to simultaneously drive the self-synchronizing transmitter dynamical system. As a consequence this type of encoding ensures security (because of the chosen compound encryption key) and also avoids the typical distortion errors [because of internal modulation of self-synchronizing drive system with signal $s(t)$] that occur for almost all previous communication schemes based on chaos synchronization [11,18]. By employing this scheme, signal is recovered at the response system Eqs. (23)–(25) as *the recovered signal:*

$$r(t) = v_r(t) - x_r(t) = s(t). \quad (38)$$

Figure 2 shows the numerical simulation results of the encoding and decoding of a *speech-like signal* and its recovery using the systems (13)–(25) and (38). Figure 2(d) establishes the perfect signal recovery in which the error signal $s(t) - r(t)$ approaches zero as $t \to \infty$. Figure 3 depicts the power spectrum of the information signal $s(t)$, the actual transmitted compound chaotic signal $d(t)$, and the recovered information signal $r(t)$. From the results, it is clear that the detection of the information signal $s(t)$ is not possible either from the transmitted signal [Fig. 3(b)] or from its power spectrum (Fig. 4) (due to its broadband nature). Due to the nature of this scheme not only can analog signals be transmitted but digital signals can also be transmitted. Figure 5 shows the transmission of a digital bit data using Eqs. (13)–(25). From the simulation results, the recovered information signal is almost identical to the information signal.

In the above example, we have considered the *drive encryption key function* K_d as a linear one. However, one can also consider suitable nonlinear functions using the drive state variables of Eqs. (13)–(18) such as $y_2^2, y_2y_3, y_2x_2, y_2y_3x_2x_3, \ldots$. The analysis again confirms our above assertions. Details will be published separately.

In conclusion, we have introduced a procedure of achieving an efficient synchronization using a compound chaotic signal. The compound drive chaotic signal has been generated by using suitable encryption functions and with appropriate feedback loop at the receiver, synchronization among the variables of the drive and response has been established. Further, its application in secure communications of analog and digital signals has been demonstrated and perfect signal recovery is achieved. Due to the present scheme of efficient encoding of message signals with suitable encryption key functions, security of the transmitted signals is greatly enhanced.

This work has been supported through a research project by the Department of Science and Technology, Government of India.

[1] L. Pecora and T. Carroll, Phys. Rev. Lett. **64**, 821 (1990); T.L. Carroll and L.M. Pecora, IEEE Trans. Circuits Syst. **38**, 453 (1991); Int. J. Bifurc. Chaos **2**, 659 (1992); Physica D **67**, 126 (1993).

[2] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, and U. Parlitz, Int. J. Bifurc. Chaos **2**, 709 (1992); U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, and A. Shang, *ibid.* **2**, 973 (1992).

[3] R. He and P.G. Vaidya, Phys. Rev. A **46**, 7387 (1992).

[4] K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993); K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz, Int. J. Bifurc. Chaos **3**, 1629 (1993).

[5] K. Murali and M. Lakshmanan, Phys. Rev. E **48**, R1624 (1993).

[6] K. Pyragas, Phys. Lett. A **181**, 203 (1993); A. Kittel, K. Pyragas, and R. Richter, Phys. Rev. E **50**, 262 (1994).

[7] K. Murali and M. Lakshmanan, Phys. Rev. E **49**, 4882 (1994).

[8] T. Kapitaniak and L.O. Chua, Int. J. Bifurc. Chaos **4**, 477 (1994); T. Kapitaniak, L.O. Chua, and G.Q. Zhong, *ibid.* **4**, 483 (1994).

[9] N. F. Rulkov, A. R. Volkovskii, A. Rodriguez-Lozano, E. Del Rio, and M.G. Velarde, Int. J. Bifurc. Chaos **2**, 669 (1992); Chaos Solitons Fractals **4**, 201 (1994); N.F. Rulkov, L.S. Tsimring, and H.D.I. Abarbanel, Phys. Rev. E **50**, 314 (1994).

[10] L. O. Chua, M. Itoh, Lj. Kocarev, and K. Eckert, J. Circuits Syst. Comput. **3**, 93 (1993).

[11] K.S. Halle, C.W. Wu, M. Itoh, and L.O. Chua, Int. J. Bifurc. Chaos **3**, 469 (1993).

[12] H. Dedieu, M.P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst.-II **40**, 634 (1993).

[13] G. Chen and X. Dong, J. Circuits Syst. Comput. **3**, 139 (1993).

[14] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993); S. Hayes, C. Grebogi, E. Ott, and A. Mark, *ibid.* **73**, 1781 (1994).

[15] K.M. Cuomo, Int. J. Bifurc. Chaos **4**, 727 (1994).

[16] C.W. Wu and L.O. Chua, Int. J. Bifurc. Chaos **3**, 1619 (1993); **4**, 979 (1994); IEEE Trans. Circuits Syst.-I **42**, 430 (1995).

[17] G. Perez and H.A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).

[18] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995); U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E **53**, 4351 (1996).

[19] T.L. Carroll, Phys. Rev. E **50**, 2580 (1994); IEEE Trans. Circuits Syst.-I **42**, 105 (1995).

[20] J. Güémez and M.A. Matías, Phys. Rev. E **53**, 3059 (1996).

[21] M. Lakshmanan and K. Murali, *Chaos in Nonlinear Oscillators: Controlling and Synchronization* (World Scientific, Singapore, 1996).

[22] K. Murali and M. Lakshmanan, Int. J. Bifurc. Chaos (to be published).