Parameter-adaptive identical synchronization disclosing Lorenz chaotic masking

A. d'Anjou,[1,*] C. Sarasola,[2,†] F. J. Torrealdea,[1,*] R. Orduna,[1,*] and M. Graña[1,*]
[1]*Computer Science Department, University of the Basque Country, San Sebastian, Spain*
[2]*Material Physics Department, University of the Basque Country, San Sebastian, Spain*
(Received 30 June 2000; published 28 March 2001)

A parameter-adaptive rule that globally synchronizes oscillatory Lorenz chaotic systems with initially different parameter values is reported. In principle, the adaptive rule requires access to the three state variables of the drive system but it has been readapted to work with the exclusive knowledge of only one variable, a potential message carrier. The rule is very robust and can be used to trace parameter modulation conveying hidden messages. The driven system is defined according to a drive-driven type of coupling that guarantees synchronization if parameters are identical. From any arbitrary initial state, the parameters of the driven system are dynamically adapted to reach convergence to the drive parameter values. At this point, synchronization mismatch or parameter tracing is used to unmask any potential hidden message.

DOI: 10.1103/PhysRevE.63.046213 PACS number(s): 05.45.Gg

I. INTRODUCTION

Due to the fact that the power spectrum of a chaotic signal has some components that can remind us of a white noise, deterministic chaos has been extensively studied as a potential carrier able to mask messages that would be virtually impossible to violate through conventional signal processing techniques. However, some nonlinear dynamic forecasting techniques [1,2] based on the reconstruction of the phase-space dynamics have proved to be good at recovering masked messages in some circumstances, challenging the pretended potentiality of chaotic carriers for secure communications. Moreover, some other approaches closer to the control-engineering field are starting to prove their ability to control chaos in some respects [3] and, in particular, to disclose possible messages hidden in a chaotic pattern [4–8].

Four main ways to hide messages in chaotic signals have been reported. One of the methods [9,10] uses small perturbations to make the symbolic dynamics of a chaotic oscillator follow a desired symbol sequence. The other three methods mask a small information-bearing signal in a large chaotic signal. In some cases the message is added directly to the chaotic signal generated by the drive [4,11], in other cases the message is included as part of the differential equations of the transmitter to modulate the carrying variable [12–14] or, finally, the message is introduced as a modulating signal on the values of a parameter from the transmitter system [4,15,16]. These last three techniques owe their success in recovering the message to the phenomenon of synchronization of two chaotic systems.

Synchronization of chaotic systems is an important research field with applications in many areas of science and technology, such as electronics [17,18], lasers [19], chemical and biological systems [20,21], communications [4,12], and extended systems [22]. Chaotic systems may display different degrees of synchronization. Its best realization is called identical synchronization [6,12,13] referring to a full coincidence of states in the drive and driven systems. In phase synchronization [23] the phases of the two systems are synchronized while the amplitudes vary chaotically and are practically uncorrelated. When a shifted-in-time coincidence of states in the drive and driven systems appears it is sometimes referred as lag synchronization [24] and, finally, in generalized synchronization [25] a functional relationship between the drive and driven systems can be found. In order to achieve synchronization two main coupling schemes have been proposed. In one of them, originally reported by Peccora and Carroll [26], one or more signals from the drive system are used to substitute one or more variables in the driven system. In the other scheme, called feedback coupling [27], one or more of the drive system variables are fed as a first order adjusting term added to the corresponding equation in the driven system.

If the drive and driven systems have the same structure and parameter values, identical synchronization can be achieved simply by designing the appropriate coupling scheme, whereas if both systems are different, even slightly, identical synchronization does not occur. This is the rational behind the use of chaotic systems in secure communication: unless the precise parameter values of the transmitter are known, identical synchronization, and consequently message decoding, will not be possible. However, general synchronization persists in a certain range of parameter mismatch between drive and driven systems [25]. This robustness of generalized synchronization has been used to estimate parameters of chaotic systems from a time series by minimizing an average synchronization error with respect to parameter mismatch [28]. Once the actual values of the drive parameters have been discovered, identical synchronization would be possible.

Short [1] and Short and Parker [2] propose a method to unmask messages based on the full reconstruction of the phase space from a time series followed by local estimation of the dynamics of the carrier on every point of the chaotic attractor. This can be done in such a way that the message emerges as a deviation from the underlying dominant dynamics. Perez and Cerdeira [5] extract Lorenz chaotic messages using two-dimensional return maps. In general, these

*FAX: +34 943 219306. Email address: ccpdadaa@si.ehu.es
†FAX: +34 943 212236. Email address: popsayuc@sq.ehu.es

methods need long time series for the phase-space dynamics reconstruction to be reliable and heavy computational cost before the hidden message can be extracted, which make them unsuitable to work on line.

Other methods use parameter-adaptive control techniques to attempt to decode information coded in chaotic signals. Parlitz [6] proposes autosynchronization, that is adaptive control of the parameters driven by the synchronization error, as a way for model parameter estimation and he finds an analytical solution for the adaptive parameter laws for an *ad hoc* variant of the Lorenz system. He also develops a numerical procedure to find local adaptive laws valid for any drive system of known structure, what makes it a potential decoder of great flexibility. The method proposed in [7] by Zhou and Lai also performs a local adaptation of the parameter values of the receiver supposing that an initial estimate of the key parameters is available. It can be used to decode messages masked through parameter modulation but requires the construction of a local empirical Lyapunov function, which again means the procedure is not particularly fit for real-time work. Liao and Tsai [8] design an adaptive observer-based receiver to synchronize the drive system given certain structural conditions for the drive. However, the structural conditions required by the method are quite restrictive about the nonlinearity of the drive system, and the range and nature of the unknown parameters.

In this work we address the problem of reaching identical synchronization to a Lorenz system with unknown parameters via global adaptation of the parameters of a driven system coupled to it according to a Peccora and Carroll [26] type of coupling. The adaptive parameters are controlled to reach convergence to the nominal values of the parameters in the drive system. Identical synchronization is then achieved and the conveyed message can be extracted out of the chaotic signal. The adaptive rule presented in Sec. II needs, in principle, access to the three-state variables of the drive but can be modified to work when only the carrying variable is observable. This is done in Sec. III, and the approach has the advantages of being global, able to be used on line, and successful in recovering the message, with the only requirement of a coarse estimate of one of the drive system parameters. In Sec. IV the proposed scheme is then applied to a communication system for unmasking a hidden message. Finally, Sec. V presents a discussion and a summary of the concluding remarks.

II. PARAMETER-ADAPTIVE RULE. GLOBAL SYNCHRONIZATION

We consider a Lorenz system with parameters σ, ρ, β as the drive system

$$\dot{x}=\sigma(y-x),$$
$$\dot{y}=\rho x-y-xz, \quad \sigma,\rho,\beta>0, \tag{1}$$
$$\dot{z}=xy-\beta z,$$

and the driven system originally proposed by Peccora and Carroll [9]

$$\dot{\hat{x}}=\hat{\sigma}(\hat{y}-\hat{x}),$$
$$\dot{\hat{y}}=\hat{\rho}x-\hat{y}-x\hat{z}, \tag{2}$$
$$\dot{\hat{z}}=x\hat{y}-\hat{\beta}\hat{z},$$

which only requires variable x from the drive and has been widely used as a master-slave coupling scheme for synchronization. It can be easily proved that these systems synchronize when their parameters are set identical,

$$\hat{\sigma}=\sigma, \quad \hat{\rho}=\rho, \quad \hat{\beta}=\beta. \tag{3}$$

Now, we will develop a stable adaptive rule based on the construction of a Lyapunov function that assures stability of the identification system and convergence of the parameters $\hat{\sigma},\hat{\rho},\hat{\beta}$ to their nominal values given by Eq. (3). Let us define the following errors:

$$e_x(t)\equiv\hat{x}(t)-x(t), \quad e_\sigma(t)\equiv\hat{\sigma}(t)-\sigma,$$
$$e_y(t)\equiv\hat{y}(t)-y(t), \quad e_\rho(t)\equiv\hat{\rho}(t)-\rho, \tag{4}$$
$$e_z(t)\equiv\hat{z}(t)-z(t), \quad e_\beta(t)\equiv\hat{\beta}(t)-\beta,$$

then the dynamics of the error variables is given by

$$\dot{e}_x=(e_y-e_x)\hat{\sigma}+(y-x)e_\sigma,$$
$$\dot{e}_y=-e_y+x(e_\rho-e_z), \tag{5}$$
$$\dot{e}_z=xe_y-\beta e_z-\hat{z}e_\beta.$$

Let $\sigma_{\max}>0$ be a higher bound on σ. If a candidate Lyapunov function is chosen as

$$V=\tfrac{1}{2}[e_x^2+\lambda(e_y^2+e_z^2)+e_\sigma^2+e_\rho^2+e_\beta^2], \tag{6}$$

where $\lambda>\lambda^*=\sigma_{\max}/4$ and we select the following adaptive rules:

$$\dot{e}_\sigma=\dot{\hat{\sigma}}=e_x(x-y),$$
$$\dot{e}_\rho=\dot{\hat{\rho}}=-\lambda xe_y, \tag{7}$$
$$\dot{e}_\beta=\dot{\hat{\beta}}=\lambda\hat{z}e_z,$$

with the constraint $0\leqslant\hat{\sigma}\leqslant\sigma_{\max}$, it follows that the time derivative of V along the trajectories of Eq. (5) is given by

$$\dot{V}=-\hat{\sigma}e_x^2+\hat{\sigma}e_xe_y-\lambda e_y^2-\lambda\beta e_z^2$$
$$=-(e_x\sqrt{\hat{\sigma}}-e_y\sqrt{\lambda^*})^2-(\lambda-\lambda^*)e_y^2-\lambda\beta e_z^2\leqslant 0, \tag{8}$$

which guarantees stable convergence to zero of the error system.

Figure 1 shows the errors in variables x,y,z and the parameter trajectories when nominal parameters in the drive system are set to $\sigma=16$, $\rho=45.92$, $\beta=4$, and initial values for the driven system are $\sigma=3$, $\rho=1$, $\beta=1$. As it can be appreciated, convergence of the parameters to their nominal values

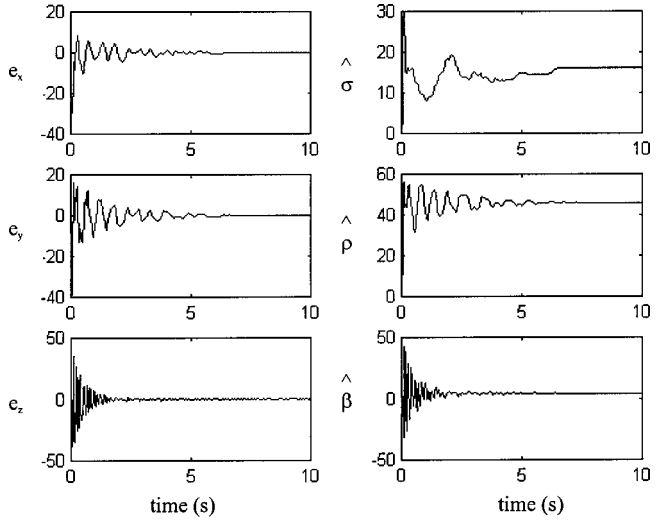

FIG. 1. Convergence of the adaptive parameters to their nominal values and synchronization errors.

is very fast and the driven system synchronizes its three variables to the corresponding ones in the drive system.

III. GLOBAL SYNCHRONIZATION USING ONE VARIABLE ONLY

We have shown that global synchronization to a Lorenz system with its three parameter values unknown can be achieved if the three variables in the drive system are available. Nevertheless, many potential applications of synchronization may require getting synchronization with the information provided by only one of the variables from the drive system. In principle, a possible solution to get a good approximation to the nonaccessible variables is to resort to the derivatives of the accessible one. This approach will permit practical applications as long as the control rules are robust enough and the ratio signal to noise in the derivatives is not too poor.

Aiming at synchronizing variable x with no access to variables y and z, we have from Eqs. (1) and (7),

$$\dot{\hat{\sigma}} = (x-y)e_x = -\frac{\dot{x}}{\sigma}e_x, \tag{9}$$

where σ seems to act as a time constant. So, we could try the following adaptive rule for parameter $\hat{\sigma}$:

$$\dot{\hat{\sigma}} = -\frac{\dot{x}}{\sigma^*}e_x, \tag{10}$$

with $\sigma^* > 0$ being a constant.

Unfortunately, this adaptive rule only works when parameters $\hat{\rho}$ and $\hat{\beta}$ in the driven system are set at their nominal values. But, if we suppose parameters ρ and β are known, the rule obtains identical synchronization, and constant σ^* is not at all critical.

In a similar way, we have also rewritten the adaptive rule for parameter $\hat{\rho}$, from Eq. (7), where only variable x and its first derivative appear,

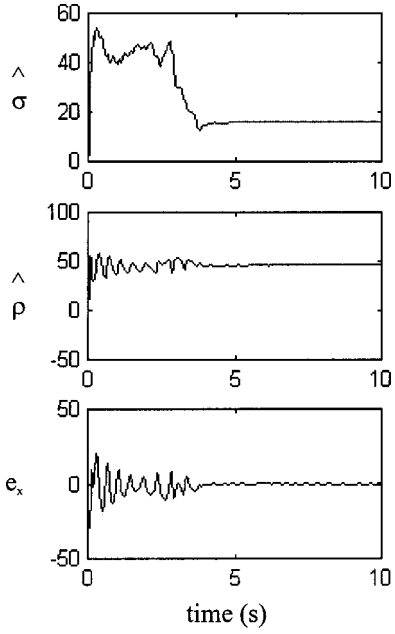

FIG. 2. Adaptation with access to variable x only and parameters σ and ρ unknown. Parameters in the drive system are $\sigma = 16$, $\rho = 45.92$, $\beta = 4$. Initial values for parameters $\hat{\sigma}$ and $\hat{\rho}$ are set arbitrarily, and $\hat{\beta} = \beta = 4$.

$$\dot{\hat{\rho}} = -\lambda x(\hat{y}-y) = -\lambda x(\hat{y}-y+x-x) = -\lambda x\left(\hat{y}-\frac{\dot{x}}{\sigma}-x\right). \tag{11}$$

In this case, the true value of parameter σ is critical. Fortunately, if convergence is to work, we can substitute the parameter σ in Eq. (11) by the adaptive parameter $\hat{\sigma}$ of the driven system, leading to the definitive adaptive rule

$$\dot{\hat{\rho}} = -\lambda x\left(\hat{y}-\frac{\dot{x}}{\hat{\sigma}}-x\right). \tag{12}$$

Thus, we can attain global synchronization of both systems when parameters σ and ρ are unknown using the adaptive rules for $\hat{\sigma}$ and $\hat{\rho}$ given by Eqs. (10) and (12).

Following the reasoning, a rule for the adaptation of parameter $\hat{\beta}$ might also be established resorting to the second derivative of variable x. Nevertheless, the convergence of $\hat{\beta}$ is more sensitive to the actual value of the parameter σ set in the adaptive rule, which makes $\hat{\beta}$ reaching its nominal value in the drive system not such a straightforward task.

Figure 2 shows the convergence of parameters $\hat{\sigma}$ and $\hat{\rho}$ to their nominal values and the error between variables x in the drive and driven systems with $\sigma^* = 12$. The results are very satisfactory and synchronization of variable x has been achieved within limits of precision good enough for most applications. It might very likely be the case that the dynamics of the system is smoothly sensitive to parameter σ, which makes it a relatively mild parameter to control. On the other hand, parameter ρ seems to be wilder but the adaptive rule is robust enough as to be able to overcome convergence diffi-

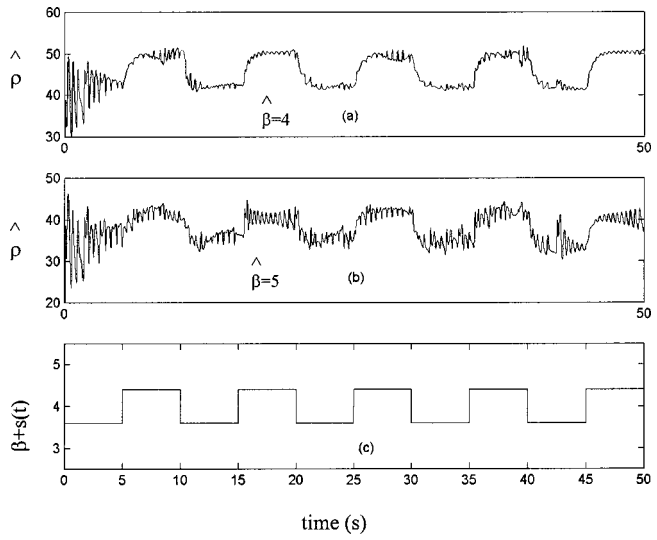

FIG. 3. Trace of $\hat{\rho}$ unmasking the message. In (a) $\hat{\beta}=4$, and in part (b) $\hat{\beta}=5$ (c) shows the parameter modulation at the transmitter.

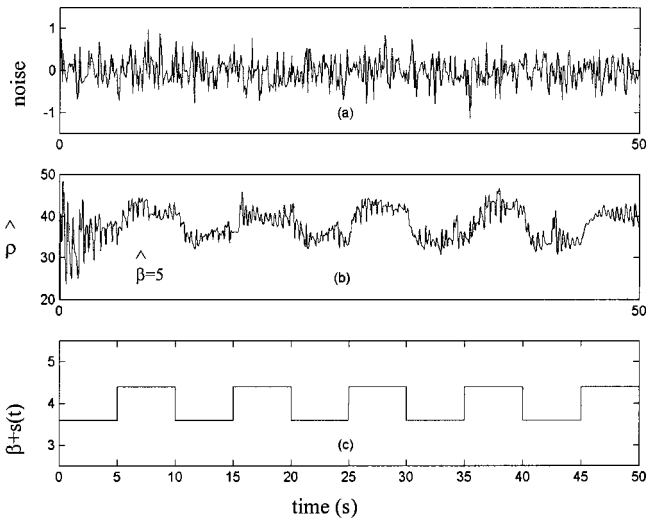

FIG. 4. In (a) the white noise added to the carrier, (b) the trace of $\hat{\rho}$ unmasking the message, and in (c), the parameter modulations at the transmitter.

culties and also potential noise introduced by the derivative. Adaptation of parameter $\hat{\beta}$ is even more critical and requires additional research.

IV. UNMASKING MESSAGES

The adaptive laws that have been presented in the preceding sections can be successfully applied as a procedure to decode information by tracing adapted parameters and by tracing the breaking of the synchronization process produced by the message. For the numerical simulations, our transmitter is a Lorenz system which parameter β is modulated by the message according to Eq. (13),

$$\dot{x}=\sigma(y-x),$$

$$\dot{y}=\rho x-y-xz, \quad \sigma,\rho,\beta>0 \tag{13}$$

$$\dot{z}=xy-[\beta+s(t)]z,$$

and the message $s(t)$ is a square wave that produces a variation in β according to the bit sent, $\beta(0)=3.6$ and $\beta(1)=4.4$. To uncover the message, the receiver sets the parameter $\hat{\beta}$ at a fixed value, and parameters $\hat{\sigma}$ and $\hat{\rho}$ are adapted according to Eqs. (10) and (12). The trace of parameter $\hat{\rho}$ is used to uncover the message.

In Fig. 3 we show simulation results for two fixed values of $\hat{\beta}$, and parameters $\hat{\sigma}$ and $\hat{\rho}$ set at whatever reasonable position at the beginning of synchronization. The message frequency is 0.1 s^{-1} but this particular value is not very critical as different time scales could be used. In Fig. 3(a) parameter $\hat{\beta}$ has been set at 4 but this nominal value is, in fact, never taken at the drive as modulation abruptly moves the parameter up and down its nominal value. In Fig. 3(b), parameter $\hat{\beta}$ has been set at 5, which means a 25% deviation from its nominal value. Nevertheless, even with such a coarse estimate, the adaptive rules are robust enough as to show that a message is being masked by the chaotic signal.

We have tested this robustness of adaptive rules in the presence of noise adding white noise to the scalar signal sent by the transmitter. In Fig. 4 we show the results with $\hat{\beta}=5$, and a normally distributed white noise with a power spectrum density of 0.01 and correlation time of 0.1 s added to the carrier.

V. DISCUSSION

We have reported global identical synchronization to a Lorenz chaotic system without any knowledge about the values of its parameters. A robust adaptive rule has been designed for identifying the Lorenz parameters when an appropriate driven system is coupled to the Lorenz chaotic oscillator. One drawback is that the rule needs access to the three-state variables of the chaotic system and many potential applications of synchronization may require getting synchronization with the information provided by only one of the variables in the drive system. This is the case, for instance, when trying to recover massages hidden in chaotic signals. If access to the full dynamics of the system based on the information provided by only one of the variables is required, it seems natural to resort to the derivatives of the accessible variable. Although, in general, control of temporal trajectories based on derivatives may become unstable due to their poor signal-to-noise ratio, under favorable circumstances, with good quality derivatives and robust rules, it may work within limits of precision still of interest for practical applications. In the case we report here it works perfectly well even in the presence of noise and we have been able to restate the adaptive rule requiring access to variable x only, if parameter β from the drive is known.

This ability to reach identical synchronization has been used to attack messages hidden in a chaotic transmitter. We have shown how the adaptive rules can be used to unmask

messages coded in a Lorenz attractor. Tracing the adaptive parameters when identical synchronization has been reached is a very effective way to decode the message. The method is robust enough as to be able to disclose the message even if parameter β is not precisely known. The procedure works efficiently as long as we have a coarse estimate of parameter β even if the two other parameters are completely unknown. The unmasking is global, can be performed on line without any kind of computational preparation, and works with noisy signals.

This procedure is, to some extent, susceptible to generalization of other systems of known structure. If the full dynamics of the drive is accessible and we are free to define the structure and type of coupling for the receiver, it is always possible to design an autosynchronizing system. For instance, designing a more general coupling that takes as input the whole set of variables from the drive and includes feedback terms, and using a style of the Lyapunov function as the one used in this work, one can always deduct an adaptive law for the parameters that will lead to a state of identical synchronization in the dynamics of the drive and response systems. Once an adaptive rule using the full dynamics of the drive is working, it can be rewritten in such a way that it only requires the accessible variable. Nevertheless, as the nominal values of the drive parameters are unknown, the new adaptive laws will have to depend on their estimated values and, consequently, there will be no *a priori* guarantee for the convergence of the rule. The advantage of a Peccora and Carroll style of coupling is that the receiver only needs the transmitted variable whereas in other styles of couplings is may need the whole set of drive variables. In this last case the substitution of a function of the transmitted variable and its derivatives for the nonaccessible variables has to be done in both the adaptive laws and the receiver itself, which makes the whole system more complex and convergence more critical. Certainly, each case will require its particular analysis and, consequently, to know the structure of the transmitter is a necessary precondition for this procedure to be applied at all.

Thus, the style of on-line parameter-adaptive autosynchronization of the kind reported in this and other works raises doubts on the security of chaotic encryption methods based on chaotic systems of known structure. On the other hand, it seems that as long as the structure of the chaotic transmitter remains as part of the encryption key, these adaptive control-based techniques will still find difficulty in trying to break the security of the transmission.

ACKNOWLEDGMENTS

Support from University of the Basque Country, Project No. UPV 140.226-TA075/99, and from Diputación de Gipuzkoa, Project No. (Z319) OF 344/1999, is acknowledged and appreciated.

[1] K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 957 (1994).
[2] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998).
[3] E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990).
[4] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[5] G. Perez and H. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[6] U. Parlitz, Phys. Rev. Lett. **76**, 1232 (1996).
[7] C. Zhou and C-H. Lai, Phys. Rev. E **59**, 6629 (1999).
[8] T. L. Liao and S. H. Tsai, Chaos, Solitons Fractals **11**, 1387 (2000).
[9] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).
[10] S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781 (1994).
[11] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).
[12] L. Kokarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
[13] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E **53**, 4351 (1996).
[14] L. Kocarev, U. Parlitz, and T. Stojanovski, Phys. Lett. A **217**, 280 (1996).
[15] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992).
[16] H. Dedieu, M. P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **40**, 634 (1993).
[17] V. S. Anishchenko, T. E. Vadivasova, D. E. Postnov, and M. A. Safonova, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 633 (1992).
[18] J. F. Heagy, T. L. Carroll, and L. M. Pecora, Phys. Rev. A **50**, 1874 (1994).
[19] R. Roy and K. S. Thornburg, Jr., Phys. Rev. Lett. **72**, 2009 (1994).
[20] S. K. Han, C. Kurrer, and Y. Karamoto, Phys. Rev. Lett. **75**, 3190 (1995).
[21] B. Blasius, A. Huppert, and L. Stone, Nature (London) **399**, 354 (1999).
[22] S. Boccaletti, J. Bragard, F. T. Arecchi, and H. Mancini, Phys. Rev. Lett. **83**, 536 (1999).
[23] M. G. Rosenblum, A. S. Pikovsky, and J. Kurhs, Phys. Rev. Lett. **76**, 1804 (1996).
[24] M. G. Rosenblum, A. S. Pikovsky, and J. Kurhs, Phys. Rev. Lett. **78**, 4193 (1997).
[25] L. Kokarev and U. Parlitz, Phys. Rev. Lett. **76**, 1816 (1996).
[26] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[27] K. Pyragas, Phys. Lett. A **170**, 421 (1992).
[28] U. Parlitz, L. Junge, and L. Kokarev, Phys. Rev. E **54**, 6253 (1996).