Synchronized pseudorandom systems and their application to speech communication

Yu Zhang,[1,*] Chao Tao,[2] Gonghuan Du,[2] and Jack J. Jiang[1]
[1]*Department of Surgery, Division of Otolaryngology Head and Neck Surgery, University of Wisconsin Medical School, Madison, Wisconsin 53792-7375, USA*
[2]*Institute of Acoustics, State Key Lab of Modern Acoustics, Nanjing University, Nanjing 210093, People's Republic of China*
(Received 11 June 2004; published 18 January 2005)

An approach to the synchronization of pseudorandom systems is proposed and applied to secure speech communication. The encoding signal produced by the pseudorandom synchronization scheme passes the random test, and shows much more complex dynamics, better random properties, and greater sensitivity to parameter mismatches than that produced by the active-passive decomposition scheme. Also, two coupled pseudorandom systems can be exactly synchronized despite their different initial states or seeds. Pseudorandom encoding and synchronization may yield great security in communication.

DOI: 10.1103/PhysRevE.71.016217 PACS number(s): 05.45.Xt, 02.50.−r, 02.90.+p, 05.90.+m

Despite extreme sensitivity to initial conditions, two chaotic systems can be synchronized using some techniques [1–3] like active-passive decomposition (APD), which has shown potential applications in secure communization. The uses of hyperchaotic or spatiotemporal chaotic systems have received considerable attention [4–7]. However, recent studies have shown that return map [8], nonlinear dynamic forecasting [9], and chaos synchronization via parameter adaption [10–13] may be used to extract messages encoded by a chaotic signal. In order to further improve security, the dynamics of the encoding signal need to be more complex. A pseudorandom number (PRN) generator with infinite degrees of freedom and statistical properties approaching a true random number series represents a better candidate for encoding messages in secure communication. PRN generators have already been applied in stochastic optimization, Monte Carlo simulation, and molecular dynamics [14–18]. However, traditionally, the pseudorandom algorithm and initial state value or seed of a PRN generator need to be exactly determined in order to reproduce the same PRN series. It is difficult to determine the output of a single PRN generator without knowing its initial value.

In contrast to previous studies based on chaotic systems [1–7], in this paper we introduce pseudorandom synchronization to PRN generators. In terms of complexity, the random test, and sensitivity to parameter mismatches, the encoder produced by the pseudorandom synchronization scheme is compared with that produced by the APD scheme of chaos synchronization. The pseudorandom encoding signals have much more complex dynamics, better random properties, and greater sensitivity to parameter mismatches than the chaotic signals, and are capable of effectively masking a message. Furthermore, the scheme of pseudorandom synchronization is applied to secure speech communication based on a pseudorandom one-way coupled ring map lattice. Two suitably coupled pseudorandom systems are synchronized despite different initial states.

A PRN generator is a deterministic algorithm that produces pseudorandom output approaching the statistical properties of a true random number series [14–18]. We consider that a system with pseudorandom dynamics can be written in terms of the following equations with nonpseudorandom and pseudorandom operators:

$$\mathbf{X}_{n+1} = \mathbf{F}(\mathbf{X}_n, \xi_n), \quad \xi_{n+1} = \mathbf{PR}(\mathbf{X}_n, \xi_n), \tag{1}$$

where $\mathbf{X}_n = (x_n(1), x_n(2), \ldots, x_n(m))$. ξ_n is the pseudorandom variable produced by a pseudorandom number generator $\mathbf{PR}(\bullet)$, such as a linear congruential generator [14–18]. To synchronize the pseudorandom drive system, we create a response system driven by the pseudorandom variable ξ_n as

$$\mathbf{Y}_{n+1} = \mathbf{F}(\mathbf{Y}_n, \xi_n). \tag{2}$$

For the difference $\mathbf{e}_n = \mathbf{X}_n - \mathbf{Y}_n$, if the difference $\mathbf{e}_{n+1} = \mathbf{F}(\mathbf{X}_n, \xi_n) - \mathbf{F}(\mathbf{Y}_n, \xi_n)$ has an asymptotically stable zero solution, then the two pseudorandom systems are synchronous, i.e., $\lim_{n\to\infty} \|\mathbf{X}_n - \mathbf{Y}_n\| = 0$. Chaotic synchronization methods, such as the APD scheme, have been previously investigated [1–7], where the drive and response systems are defined as chaotic, and ξ_n is defined as a chaotic driving signal. However, chaos with a finite dimension differs from random white noise with infinite degrees of freedom. Chaotic systems with finite dimensions and large robustness to parameter mismatches in synchronization cannot qualify as good PRN generators since such systems may not pass the random test and may be decoded by using the parameter estimate method [10–13]. In comparison with such chaotic systems like the logistic map and the spatiotemporal coupled map lattice, the following calculations show that the pseudorandom series representing a simulation of random noise have much more complex dynamics, better random properties, and greater sensitivity to parameter mismatches than the chaotic systems. Thus, in this paper, we investigate the applications of pseudorandom systems, where the drive system is defined as a pseudorandom system and ξ_n is a pseudorandom variable because of the randomization operator $\mathbf{PR}(\bullet)$. Considering different initial states of two PRN generators (1) and (2), we introduce the synchronization technique. Under the driving pseudorandom function ξ_n, two pseudorandom systems

*Electronic address: zhang@surgery.wisc.edu

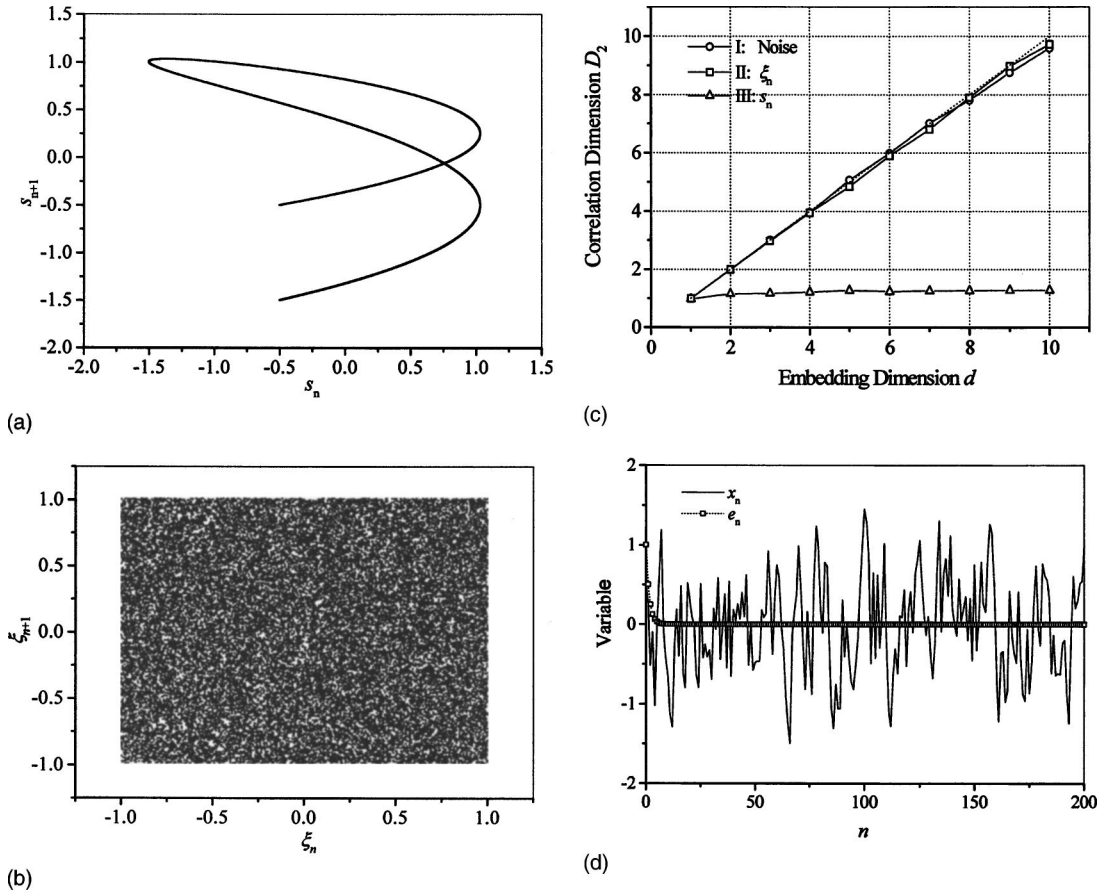

FIG. 1. (a) The reconstructed phase space (s_n, s_{n+1}). (b) (ξ_n, ξ_{n+1}). (c) D_2 vs d, where curves I, II, and III correspond to CONG, ξ_n, and s_n, respectively. (d) The drive variable x_n and the synchronization error e_n.

can be synchronized despite different initial conditions. We therefore call this scheme *pseudorandom synchronization* (PRS). A series of deterministic algorithms for PRN generators have been proposed [14,16,19]. We previously applied a truncated synchronization [20,21], which represents a specific case of PRS. PRN algorithms can be chosen with flexibility, which may lead to more general applications of the PRS scheme.

To illustrate this scheme for synchronizing pseudorandom systems, we consider the following decomposition based on the logistic map in the first example:

$$x_{n+1} = 0.5x_n + \xi_n,$$

$$\xi_n = 2g_n/(2^{31} - 1) - 1,$$

$$g_{n+1} = (16\,807 \times \{g_n + \mathrm{int}[(1 - 2x_n^2 - 0.5x_n) \times (2^{31} - 1)]\}) \mathrm{mod}(2^{31} - 1), \quad (3)$$

where the pseudorandom variable ξ_n within the interval $[-1,1]$ is produced based on the linear congruential generator CONG, $\eta_{n+1} = (16\,807 \times \eta_n) \mathrm{mod}(2^{31} - 1)$ [14]. As a comparison, the APD scheme [2] is applied to the drive system where $x_{n+1} = 0.5x_n + s_n$ and $s_n = 1 - 2x_n^2 - 0.5x_n$.

Figure 1 shows that ξ_n produced by PRS has more complex dynamics than s_n produced by APD. The dynamics of s_n and ξ_n can be reconstructed using the time delay technique [22]. The proper time delay can be determined by using the mutual information method [23]. For the time series s_n with length $N = 20\,000$, a time-delay vector $\{s_n, s_{n+1}, \ldots, s_{n+(d-1)}\}$ reconstructs the phase space where d is the embedding dimension. The reconstructed phase space (s_n, s_{n+1}) displays a simple structure in Fig. 1(a). However, in the reconstructed phase space (ξ_n, ξ_{n+1}), a cloud of points does not present any structure [see Fig. 1(b)]. To quantitatively describe the complexities of s_n and ξ_n, we calculate the correlation dimension D_2 [24]. Figure 1(c) shows the relationship between the estimated D_2 and d, where the curves I, II, and III correspond to the CONG pseudorandom series, ξ_n, and s_n, respectively. When d is increased, the estimated dimension of s_n approaches $D_2 = 1.0 \pm 0.01$; however, the estimated dimensions of ξ_n and CONG series do not converge. Unlike s_n produced by APD, ξ_n produced by PRS exhibits much more complex dynamics, which may be difficult to decode using return map [8] and nonlinear dynamic prediction [9].

Furthermore, ξ_n shows good statistical properties. A pure random process with uniform distribution on $[-1, 1]$ has a mean of 0 and a standard deviation of $\sqrt{1/3} \approx 0.5774$. ξ_n in Fig. 1 has a mean value of 0.0066 and a standard deviation of 0.5767, representing a good simulation of uniform noise. In order to test the randomness of s_n, ξ_n, and CONG, the chi-square test and Kolmogorov-Smirnov test were per-

formed [25], where each signal with length 20 000 was divided into 20 classes. The χ^2 values and Kolmogorov-Smirnov D values of s_n, ξ_n, and CONG are calculated as (8140, 0.1660), (14.748, 0.0061), and (10.147, 0.0061), respectively. At the 0.05 significance level, the critical values of the chi-square test with 19 degrees of freedom and Kolmogorov-Smirnov test are (30.144, 0.009 62). ξ_n and CONG both pass these two random tests (χ^2 value <30.144 and D value $<0.009\,62$), but s_n fails since its χ^2 value and D value exceed the critical values. Differing from the chaotic s_n, ξ_n represents a PRN series. The pseudorandom variable ξ_n drives the response system as $y_{n+1}=0.5y_n+\xi_n$. For the difference $e_n=x_n-y_n$, we have $e_{n+1}=0.5e_n$. Thus, although starting from different initial conditions, two pseudorandom systems are finally synchronous, that is, $|x_n-y_n| \to 0$ when $n\to\infty$, as shown in Fig. 1(d).

One-way coupled ring map lattice (OCRML) has been applied as a spatiotemporal system to secure speech communication [4]. As an application of the PRS scheme, we performed digital speech communication based on a pseudorandom one-way coupled ring map lattice (PR-OCRML) with length m. The drive system is

$$x_{n+1}(1) = (1-\varepsilon)[1-\mu x_n^2(1)] + \varepsilon\xi_n/(2^{31}-1),$$

$$x_{n+1}(l) = (1-\varepsilon)[1-\mu x_n^2(l)] + \varepsilon[1-\mu x_n^2(l+1)] \quad (l=2,3,\ldots,m),$$

$$x_n(m+1) = x_n(1),$$

$$\xi_n = g_n + i_n,$$

$$g_n = (16807 \times \mathrm{int}\{[1-\mu x_n^2(2)] \times (2^{31}-1)\}) \mathrm{mod}(2^{31}-1), \tag{4}$$

where n denotes the discrete time, and l denotes the lattice site index. As a comparison, we also considered the OCRML system to which we previously applied the APD scheme [4]. Similar to the system (3), the driving signal ξ_n of the PR-OCRML system has a complex reconstructed phase space and its estimated dimension increases with the embedding dimension. For the normalized ξ_n within $[-1, 1]$, the mean value and standard deviation are estimated as 0.0032 and 0.5749, respectively. The chi-square test and Kolmogorov-Smirnov test are performed for the driving signals from the OCRML and PR-OCRML systems with $m=3$. The normalized ξ_n from the PR-OCRML system passes the random tests (χ^2 value $=22.014<30.144$ and D value $=0.0067<0.0136$), but the driving signal from the OCRML system fails (χ^2 value $=7718$ and D value $=0.1653$). Thus ξ_n produced by the PR-OCRML system can be applied as a PRN series. To synchronize the pseudorandom system (4), we have the response system

$$y_{n+1}(1) = (1-\varepsilon')[1-\mu' y_n^2(1)] + \varepsilon'\xi_n/(2^{31}-1)$$

$$y_{n+1}(l) = (1-\varepsilon')[1-\mu' y_n^2(l)] + \varepsilon'[1-\mu' y_n^2(l+1)] \quad (l=2,3,\ldots,m),$$

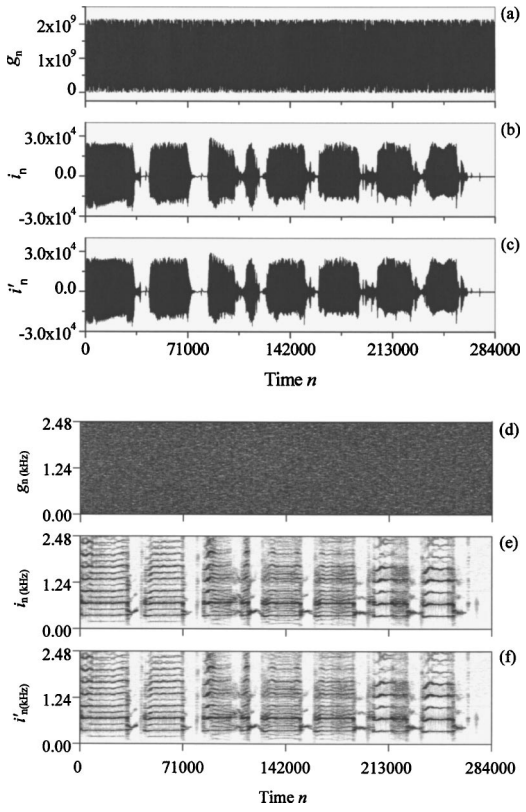

FIG. 2. Speech secure communication, where the (a) pseudorandom masking signal g_n, (b) the message i_n, and (c) the recovered signal i_n' are shown. Their corresponding spectrograms are in (d), (e), and (f), respectively.

$$y_n(m+1) = y_n(1), \tag{5}$$

with the driving variable ξ_n. $x_n(k)$ and $y_n(k)$ are bounded satisfying $|x_n(k)|<M$ and $|y_n(k)|<M$, where M is constant and $k=1,2,\ldots,m$. For $\varepsilon=\varepsilon'$, $\mu=\mu'$, and $e_n(k)=x_n(k)-y_n(k)$, we have the difference dynamics:

$$e_{n+1}(1) = -(1-\varepsilon)\mu(1)[x_n(1)+y_n(1)]e_n(1),$$

$$e_{n+1}(l) = -(1-\varepsilon)\mu(l)[x_n(l)+y_n(l)]e_n(l) - \varepsilon\mu(l+1)[x_n(l+1)+y_n(l+1)]e_n(l+1),$$

$$e_{n+1}(m+1) = e_{n+1}(1). \tag{6}$$

When the system parameters μ and ε satisfy $|e_{n+1}(k)/e_n(k)| \leqslant 2(1-\varepsilon)\mu M \ll 1$, two pseudorandom systems can be synchronized, that is, $\lim_{n\to\infty}|x_n(k)-y_n(k)|=0$. In secure speech communication, we apply the PRN series to encode the message i_n as $\xi_n=g_n+i_n$. With two synchronous systems $g_n(x_n(2))=g_n(y_n(2))$, we can recover the exact message by $i_n'=\xi_n-g_n(y_n(2))$. Figure 2 shows the performance of speech communication using the PRS scheme where $m=3$, $\mu=1.9$, and $\varepsilon=0.99$, and the message i_n is a pathological voice with multiple vowel /a/ scenarios generated by a patient with right vocal polyps, sampled at 20 kHz with 16-bit resolution. Figures 2(a)–2(c) show the time series of the pseudorandom masking signal g_n, the message i_n, and the recovered signal

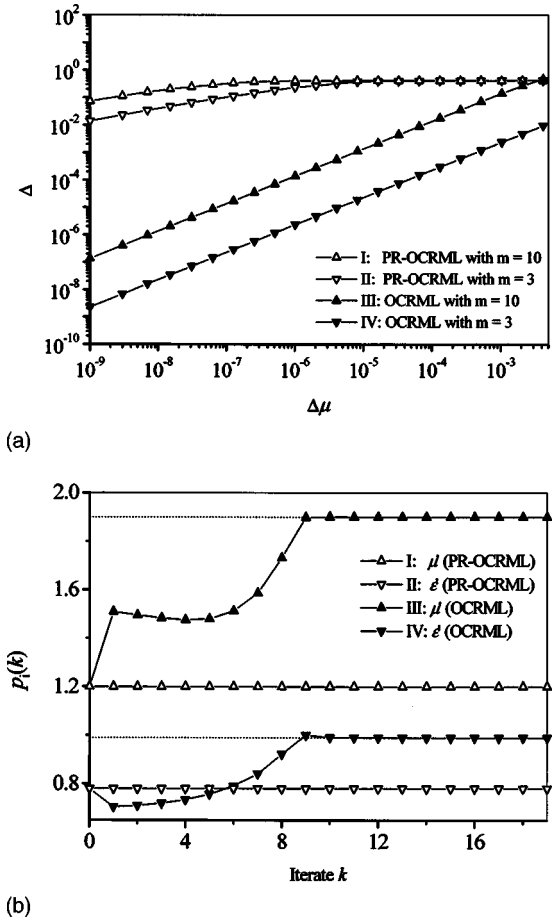

FIG. 3. (a) The error Δ versus the parameter difference $\Delta\mu$, where curves I and II correspond to the PR-OCRML systems with $m=10$ and 3, respectively, and curves III and IV correspond to the OCRML systems with $m=10$ and 3, respectively. (b) The response parameters $p_i(k)$ estimated using the parameter adaption technique [13], where the dotted lines represent the drive parameters $\mu=1.99$ and $\varepsilon=0.9$. Curves I and II correspond to the PR-OCRML system with $m=3$, and curves III and IV correspond to the OCRML system with $m=3$.

i_n', respectively. The corresponding spectrograms of g_n, i_n, and i_n' are illustrated in Figs. 2(d)–2(f), where x and y axes represent time and frequency components. Disordered voices from patients with laryngeal pathologies may produce subharmonic patterns and broadband spectra [26], as shown in Fig. 2(e). Thus, to mask all frequency components of the disordered voice i_n, the masking signal g_n should have a noiselike broadband spectrum. A pseudorandom signal can mask the broadband disordered voice well. In particular, using PRS, the encoded message can be exactly recovered.

The PRS scheme also has extreme sensitivity to parameter mismatches between the drive and response systems. Figure 3(a) shows the relationship between the error Δ and the parameter difference $\Delta\mu=\mu'-\mu$, where

$$\Delta=\sqrt{\frac{1}{N}\sum_{n=1}^{N}[(i_n'-i_n)/(2^{31}-1)]^2}.$$

Curves I and II correspond to the PR-OCRML systems with $m=10$ and 3, and curves III and IV correspond to the OCRML systems with $m=10$ and 3. When $\Delta\mu=0$, the error $\Delta=0$ is yielded and the message is exactly recovered. However, a slight parameter mismatch $\Delta\mu=10^{-5}$ of the PR-OCRML systems with $m=3$ results in a large distortion Δ saturating to 0.408, so that noise is heard in the response system. Increasing the lattice length m will amplify the distortion Δ [4]; however, even with the same length m, the PR-OCRML system is much more sensitive to parameter mismatches than the OCRML system.

The sensitivity of the PRS scheme to parameter mismatches makes decoding the message through estimation of system parameters difficult. Previous studies have suggested that even if a synchronization scheme is robust to parameter mismatches, applying parameter adaption to the response system may estimate the drive parameters [10–13]. We previously proposed an iterative approach of parameter adaptions [13]. Using this technique, μ and ε of the response OCRML system with $m=3$ can be estimated, as shown in Fig. 3(b), where the drive parameters are $\mu=1.99$ and $\varepsilon=0.9$. Although the original values of the response parameters are $\mu'=1.2$ and $\varepsilon'=0.8$, their asymptotical values converge to 1.99 and 0.9, respectively. In contrast to this, the parameter adaption technique cannot estimate the PR-OCRML parameters. A sufficiently small parameter mismatch of the PR-OCRML systems yields a very large synchronization error, so that the parameter adaption technique cannot target its control to approach the drive parameters. Thus communication using the PRS scheme is highly secure against the decoding of system parameters or keys.

In conclusion, we have proposed a scheme to synchronize two pseudorandom systems and showed its potential application in pseudorandom communication. In comparison with the chaotic signal produced by APD scheme, the pseudorandom signal produced by this pseudorandom synchronization scheme passes the random test, and has much more complex dynamics, better random properties, and greater sensitivity to parameter mismatches. These findings show that pseudorandom number generators with infinite degrees of freedom represent a better candidate for signal encoding. Traditionally, the pseudorandom algorithm and initial state value or seed of a pseudorandom number generator must be exactly known to reproduce the pseudorandom number series. However, by using this pseudorandom synchronization scheme, two coupled pseudorandom systems can be exactly synchronized despite their different initial states or seeds (or the initial seed of a pseudorandom number generator is unnecessarily required). The pseudorandom synchronization scheme can effectively mask and exactly recover a broadband disordered voice. Synchronization techniques may be applied to generally deterministic systems, such as chaotic systems and PRN generators. The research records of patients with laryngeal pathologies, including voice data and patient information, should be kept confidential and available only to those investigators involved in a given study. For secure online transmissions of voice data, pseudorandom synchronization might potentially present a valuable scheme for secure data communication. Moreover, there is a large amount of flexibility in choosing the PRN algorithms and decomposition methods in pseudorandom synchronization. It allows the convenient integration of different pseudorandom algorithms [14–21]

into this pseudorandom synchronization scheme. Pseudorandom synchronization represents an interesting way to combine the features of pseudorandom number generators and synchronization techniques, and might be applied to general situations, such as spread-spectrum communication.

The authors thank Professor J. C. Sprott for discussions. This work was supported by the NIH Grant No. 1-RO1DC05522-01 from the National Institute of Deafness and Other Communication Disorders and NSF of China (Grant Nos. 10074035 and 19834040).

[1] L. M. Pecora and T. L. Carroll, Phys. Rev. A **44**, 2374 (1991).
[2] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
[3] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, and C. S. Zhou, Phys. Rep. **366**, 1 (2002).
[4] Y. Zhang, M. Dai, Y. M. Hua, W. S. Ni, and G. H. Du, Phys. Rev. E **58**, 3022 (1998).
[5] V. S. Udaltsov, J. P. Geoedgebuer, L. Larger, and W. T. Rhodes, Phys. Rev. Lett. **86**, 1892 (2001).
[6] S. H. Wang *et al.*, Phys. Rev. E **66**, 065202 (2002).
[7] J. Garcia-Ojalvo and R. Roy, Phys. Rev. Lett. **86**, 5204 (2001).
[8] G. Perez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[9] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998).
[10] U. Parlitz, Phys. Rev. Lett. **76**, 1232 (1996).
[11] A. d'Anjou, C. Sarasola, F. J. Torrealdea, R. Orduna, and M. Grana, Phys. Rev. E **63**, 046213 (2001).
[12] C. Tao and G. H. Du, Phys. Lett. A **311**, 158 (2003).
[13] C. Tao, Y. Zhang, G. H. Du, and J. J. Jiang, Phys. Rev. E **69**, 036204 (2004).
[14] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, Phys. Rev. Lett. **69**, 3382 (1992).
[15] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes in C*, 2nd ed. (Cambridge University Press, Cambridge, England, 1992).
[16] B. M. Gammel, Phys. Rev. E **58**, 2586 (1998).
[17] K. V. Tretiakov and K. W. Wojciechowski, Phys. Rev. E **60**, 7626 (1999).
[18] I. Vattulainen, Phys. Rev. E **59**, 7200 (1999).
[19] W. S. Ni, Y. M. Hua, H. Deng, T. F. Qin, Prog. Phys. (in Chinese) **16**, 645 (1996).
[20] Y. Zhang, M. Dai, Y. M. Hua, and G. H. Du, Electron. Lett. **35**, 2087 (1999).
[21] Y. Zhang, G. H. Du, and J. J. Jiang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **13**, 691 (2003).
[22] J. D. Farmer and J. J. Sidorowich, Phys. Rev. Lett. **59**, 845 (1987).
[23] A. M. Fraser and H. L. Swinney, Phys. Rev. A **33**, 1134 (1986).
[24] P. Grassberger and I. Procaccia, Physica D **9**, 189 (1983).
[25] V. K. Rohatgi, *An Introduction to Probability Theory and Mathematical Statistics* (John Wiley & Sons, New York, 1976).
[26] J. J. Jiang and Y. Zhang, Electron. Lett. **38**, 294 (2002).