Synchronization and chaotic masking scheme based on occasional coupling

Ömer Morgül*
Department of Electrical and Electronics Engineering, Bilkent University, 06533 Bilkent, Ankara, Turkey
(Received 18 April 2000)

We present a synchronization and a related chaotic masking scheme for discrete-time systems. This method is based on occasional coupling of transmitter and receiver systems. We show that the synchronization may be achieved and the message can be recovered with acceptable error under certain conditions. Then we show that the proposed schemes are robust with respect to noise and parameter mismatch. We also present some simulation results.

PACS number(s): 05.45.−a, 43.72.+q

I. INTRODUCTION

In the last decade the synchronization of chaotic systems has received a great deal of attention, see [1–18]. One possible application of synchronization is the possibility of using chaotic signals for secure communication (see [4,5,7]). There are various synchronization schemes [9–11,15–18], and in most of these the synchronized system consists of two parts: a generator of chaotic signals, which is called the master (or drive) system, and a receiver, which is called the slave (or response) system. A chaotic signal generated by the master system may be used as an input to the slave system to synchronize the common signals of both systems. After synchronization, one may add the message to the chaotic signal used for synchronization and send this signal as an input to the slave system. This is called chaotic masking, and under certain conditions, one may recover the original message [2,3]. An extensive list of references for various aspects of chaotic systems may be found in Ref. [1].

In this paper, we will consider the discrete-time chaotic systems. Synchronization of such systems, particularly coupled maps, has been investigated by many researchers. In Refs. [6,8], synchronization properties of coupled maps, including the coupled tent maps, were investigated. In Ref. [12], coupled logistic maps were considered. An observer-based synchronization scheme for discrete-time systems was given in [23] (see [9,10] for continuous-time case). In Refs. [6,21] various synchronization schemes and their robustness properties were given. In Ref. [22] some secure communication schemes based on synchronization were proposed.

Recently, a new synchronization scheme based on occasional coupling and its application to communication for continuous-time systems has been given in Refs. [13,14]. In this paper, we will apply the same idea to discrete-time systems and show that similar results hold under certain conditions. We will assume that a synchronization scheme for which the synchronization is achieved exponentially fast is available. The occasional synchronization scheme proposed in this paper consists of the application of synchronization and autonomous phases periodically. In the the synchronization phases, the exponential synchronization scheme mentioned above is used and in the autonomous phases, the response system is switched to a replica of the drive system. In the case of message transmission, the message is masked by the drive signal and sent to the receiver only in the autonomous phases. We will show that under certain conditions, it is possible to achieve synchronization, and in the case of message transmission, it is possible to recover the message with acceptable error. In particular, we will show that with this technique, any message of any length can be transmitted in the ideal case. Moreover, we will show that this technique is robust with respect to noise and parameter mismatch. When such nonidealities are present, we will show that there is a maximum allowable message length for successful message recovery, and if the length of the message exceeds this length, we can divide the message into submessages—each of which having a length smaller than the maximum allowable length—and send each submessage in one message transmission interval.

This paper is organized as follows. In the next section, we will introduce our synchronization scheme and the related message transmission scheme, and prove their basic properties in the ideal case. In Sec. III, we will give some robustness results with respect to noise and parameter mismatch. In Sec. IV, we will present some simulation results, and finally we will give some concluding remarks.

II. OCCASIONAL COUPLING

We consider discrete-time systems in this work. Let the chaotic master system be given as follows:

$$u(k+1)=f(u(k),\mu), \quad y(k)=h(u(k)), \quad k=0,1,2,\ldots, \tag{2.1}$$

where $u\in\mathbf{R}^n$ is the state, $\mu\in\mathbf{R}^p$ is parameter vector, $f:\mathbf{R}^n\times\mathbf{R}^p\rightarrow\mathbf{R}^n$ and $h:\mathbf{R}^n\rightarrow\mathbf{R}^d$ are functions, and $y\in\mathbf{R}^d$ is the measurable output of this system that will be used for synchronization. Let the slave system used for synchronization be given as

$$w(k+1)=g(w(k),y(k),\mu), \quad k=0,1,2,\ldots, \tag{2.2}$$

where $g:\mathbf{R}^n\times\mathbf{R}^d\times\mathbf{R}^p\rightarrow\mathbf{R}^n$ is an appropriate function. Let $e=u-w$ denote the synchronization error. We assume that the error decays exponentially to zero, that is for some $M>0$, $0<\rho<1$, the following holds for any $k>k_0$ and $e(k_0)$:

*Email address: morgul@ee.bilkent.edu.tr

$$\|e(k)\| \leqslant M\rho^{(k-k_0)}\|e(k_0)\|, \tag{2.3}$$

where $\|\cdot\|$ is any norm in $\mathbf{R}^n$. In case Eq. (2.1) is valid for $k_0 \leqslant k < K-1$, then we require that Eq. (2.3) be valid for $k_0 < k \leqslant K$. In this case we say that the synchronization is exponential. Note that we may take $M \geqslant 1$ in Eq. (2.3), without loss of generality. In some cases Eq. (2.3) might hold for sufficiently small $e(k_0)$, i.e., for $\|e(k_0)\| < r$ for some $r > 0$, in which case we say that the synchronization is locally exponential.

We note that some synchronization schemes proposed in the literature are exponential. For example, in Ref. [9], an exponential synchronization scheme for logistic maps is proposed, and it was shown that this scheme is robust with respect to noise and parameter mismatch. In [5], a different synchronization scheme (type 2 in the notation of Ref. [5]) was applied to a skew-tent map, and similar results were obtained. In Refs. [10,11], an observer-based synchronization scheme for continuous-time systems was proposed and it was shown that the proposed scheme yields exponential synchronization that is robust with respect to noise and parameter mismatch. The same methodology could be extended to discrete-time systems, see e.g., [23]. However, we will not pursue this direction.

In Refs. [12,13], a communication scheme for continuous-time systems based on occasional coupling of synchronized systems was proposed. We will apply this methodology to discrete-time systems. Let us rewrite Eq. (2.2) in the following form:

$$w(k+1) = f(w(k),\mu) + s(k)G(w(k),y(k),\mu), \tag{2.4}$$

where $G(w,y,\mu) = g(w,y,\mu) - f(w,\mu)$, and $s(k) = 0,1$ is the switching signal. When $s(k) = 1$, Eq. (2.4) reduces to Eq. (2.2), and when $s(k) = 0$, Eq. (2.4) becomes a copy of Eq. (2.1). As in [12,13], our chaotic masking scheme is based on changing the switching signal s between 0 and 1, periodically. The periods in which $s = 1$ and $s = 0$ are used for synchronization and message transmission, respectively. More precisely, let T_s and T_m be the integers that denote the synchronization and message transmission intervals, respectively. Then, for $j = 1,2,\ldots$ our synchronization scheme is as follows:

i. (jth synchronization phase) For $(j-1)(T_s+T_m) \leqslant k < jT_s + (j-1)T_m$, [i.e., when $k \ (\mathrm{mod}(T_s+T_m)) \in [0,T_s)$], use the master system given by Eq. (2.1) and the slave system given by Eq. (2.4) with $s(k) = 1$. The signal trasmitted to the slave system is y in this period.

ii. (jth autonomous phase) For $jT_s + (j-1)T_m \leqslant k < j(T_s + T_m)$, [i.e., when $k \ (\mathrm{mod}(T_s+T_m)) \in [T_s, T_s+T_m)$], use the master system given by Eq. (2.1) and the slave system given by Eq. (2.4) with $s(k) = 0$. (Note that in this phase Eq. (2.4) becomes a replica of Eq. (2.1), which is an autonomous system).

Note that in the synchronization phase, the error decays exponentially to zero, as given by Eq. (2.3), and in the autonomous phase it may increase, also exponentially fast. However, by arranging T_s and T_m, it may still be possible to obtain an error that decreases exponentially fast *at the beginning of synchronization periods*, and the error in the message recovery will be small [see Eq. (2.19)]. This is the basic rationale in our scheme.

Theorem 1: Consider the system given by Eqs. (2.1) and (2.4), and the synchronization scheme given above. Assume that the function $f(\cdot,\mu)$ is Lipschitz, i.e., the following holds:

$$\|f(u,\mu) - f(w,\mu)\| \leqslant k_1\|u-w\|, \tag{2.5}$$

for some $k_1 > 0$. Assume that Eq. (2.3) holds in the synchronization phases. If $T_s > 0$ and $T_m > 0$ are chosen as

$$T_s > -\frac{\ln M}{\ln \rho}, \quad T_m < -\frac{T_s \ln \rho + \ln M}{\ln k_1}, \tag{2.6}$$

then the error $\|e(k)\|$ decays to zero. Moreover, this decay is exponential, i.e., the following holds for some $\hat{M} > 0$, $0 < \gamma < 1$:

$$\|e(k)\| \leqslant \hat{M}\gamma^k\|e(0)\|. \tag{2.7}$$

Proof: Let us define the following:

$$T_j^s = (j-1)(T_s+T_m), \quad T_j^m = T_j^s + T_s, \quad j = 1,2,\ldots, \tag{2.8}$$

i.e., T_j^s and T_j^m denote the beginning of the jth synchronization and autonomous phases, respectively. Since Eq. (2.3) holds in the jth synchronization phase, we have the following:

$$\|e(k)\| \leqslant M\rho^{(k-T_j^s)}\|e(T_j^s)\|, \quad T_j^s < k \leqslant T_j^m. \tag{2.9}$$

At the jth autonomous phase we have

$$\|e(k+1)\| = \|f(u(k),\mu) - f(w(k),\mu)\| \leqslant k_1\|e(k)\|, \quad T_j^m \leqslant k < T_{j+1}^s, \tag{2.10}$$

hence we have

$$\|e(k)\| \leqslant k_1^{(k-T_j^m)}\|e(T_j^m)\|, \quad T_j^m < k \leqslant T_{j+1}^s. \tag{2.11}$$

Note that if $k_1 < 1$, then the exponential decay is obvious from Eqs. (2.9) and (2.11). Hence we assume $k_1 > 1$ in the sequel. From Eq. (2.9) we obtain

$$\|e(T_j^m)\| \leqslant M\rho^{T_s}\|e(T_j^s)\|. \tag{2.12}$$

Hence we can rewrite Eq. (2.11) as

$$\|e(k)\| \leqslant M\rho^{T_s}k_1^{(k-T_j^m)}\|e(T_j^s)\|, \quad T_j^m < k \leqslant T_{j+1}^s. \tag{2.13}$$

Note that $T_1^s = 0$, hence from Eq. (2.13) we obtain

$$\|e(T_{j+1}^s)\| \leqslant \alpha\|e(T_j^s)\| \leqslant \alpha^j\|e(0)\|, \tag{2.14}$$

where $\alpha > 0$ is defined as

$$\alpha = M\rho^{T_s}k_1^{T_m}. \tag{2.15}$$

By using Eq. (2.6) we obtain

$$\ln \alpha = \ln M + T_s \ln \rho + T_m \ln k_1 < 0, \tag{2.16}$$

hence $\alpha < 1$. Note that since $M \geqslant 1$ and $\rho < 1$, we have $T_s > 0$ in Eq. (2.6), and the first inequality in Eq. (2.6) is required to guarantee $T_m > 0$. By using Eq. (2.14) in Eqs. (2.9) and (2.13) we obtain

$$\|e(k)\| \leqslant \frac{M}{\alpha} \alpha^j \|e(0)\|, \quad T_j^s < k \leqslant T_j^m, \tag{2.17}$$

$$\|e(k)\| \leqslant \alpha^j \|e(0)\|, \quad T_j^m < k \leqslant T_{j+1}^s. \tag{2.18}$$

By using Eq. (2.8) we obtain $j \geqslant (k+T_m)/(T_s+T_m)$ in Eq. (2.17) and $j \geqslant k/(T_s+T_m)$ in Eq. (2.18). By using these inequalities, respectively, in Eqs. (2.17) and (2.18), and by using the fact that $\alpha < 1$, we obtain Eq. (2.7) with $\gamma = \alpha^{1/(T_s+T_m)} < 1$, and $\hat{M} = \max\{M\gamma^{T_m}/\alpha, 1\}$.

Based on the synchronization scheme given above, we propose the following message transmission scheme. Again, let $j = 1,2, \ldots,$ and let m be the message to be transmitted. Then, our message transmission scheme is as follows:

(i) (jth synchronization phase) same as the jth synchronization phase in the synchronization scheme.

(ii) (jth message transmission phase) same as the jth autonomous phase in the synchronization scheme. The signal sent to the receiver is the masked message $y+m$ in this phase.

(iii) (message recovery) In jth message transmission phase, the recovered message $\hat{m}$ is given as

$$\hat{m}(k) = y(k) + m(k) - h(w(k)). \tag{2.19}$$

We have the following result for our scheme.

Theorem 2: Consider the systems given by Eqs. (2.1) and (2.4), and the message transmission scheme given above. Assume that Eq. (2.3) holds in the synchronization phases and Eq. (2.5) holds. Moreover, let h be Lipschitz, i.e., the following holds for some $k_2 > 0$:

$$\|h(u) - h(w)\| \leqslant k_2 \|u - w\|. \tag{2.20}$$

Let $\|e(0)\| \leqslant r$ for some $r > 0$ and let $\epsilon > 0$ be given. Then for any message m of length T_m, there exists a synchronization interval T_s such that the following holds in the message transmission period:

$$\|\hat{m}(k) - m(k)\| \leqslant \epsilon. \tag{2.21}$$

Proof. It can easily be shown that the estimates (2.9)–(2.23) are valid. By using Eqs. (2.19), (2.20), and (2.18) we obtain the following in the jth message transmission phase:

$$\|\hat{m}(k) - m(k)\| \leqslant k_2 \alpha^j \|e(0)\|, \tag{2.22}$$

where α is given by Eq. (2.15). From Eq. (2.22) we see that Eq. (2.21) holds if the following is satisfied:

$$\ln M + T_s \ln \rho + T_m \ln k_1 \leqslant \frac{1}{j} \ln \frac{\epsilon}{r k_2}, \quad j = 1,2, \ldots. \tag{2.23}$$

If $\ln \epsilon / r k_2 < 0$, then Eq. (2.23) is satisfied provided that the following holds:

$$\ln M + T_s \ln \rho + T_m \ln k_1 \leqslant \ln \frac{\epsilon}{r k_2}. \tag{2.24}$$

If $\ln \epsilon / r k_2 \geqslant 0$, then Eq. (2.23) is satisfied provided that the following holds:

$$\ln M + T_s \ln \rho + T_m \ln k_1 \leqslant 0. \tag{2.25}$$

Note that $0 < \rho < 1$, hence $\ln \rho < 0$. Therefore $T_s \ln \rho \to -\infty$ as $T_s \to \infty$. Hence, for any $T_m > 0$, one can find a $T_s > 0$ such that Eq. (2.24) or (2.25) holds.

III. ROBUSTNESS RESULTS

In the previous section, we considered the ideal case. In this section, we will show that the proposed scheme is robust with respect to noise and parameter mismatch. Note that the development of synchronization and message transmission schemes are similar, hence we will consider only the robustness of the message transmission scheme in this section. Robustness of the synchronization scheme can easily be shown by performing similar calculations. We note that similar results were given in Refs. [10–13] for the observer-based synchronization schemes for continuous-time systems, and it was noted that these robustness results are consequences of exponential synchronization. We expect that similar results should hold for the discrete-time systems, and in this section we will prove such a robustness result by using exponential synchronization.

We will assume that the slave system (2.2) has the following form:

$$w(k+1) = g(y(k) + n(k), w(k), \mu'), \tag{3.1}$$

where n is a (random) noise term added to the observation y and μ' is the parameter vector used in the slave system. In the following we will show that the proposed scheme is robust under some mild conditions provided that $M \leqslant 1$ in Eq. (2.3), hence robustness is a consequence of exponential synchronization. This result can be extended to the $M > 1$ case, but the proof involves some advanced Lyapunov stability results and will not be pursued here.

Theorem 2: Let the system given by Eqs. (2.1) and (2.2) satisfy Eq. (2.3) with $M \leqslant 1$. Assume that $g(y,w,\mu)$ is Lipschitz in y and μ, i.e., the following hold for some $k_3 > 0$, $k_4 > 0$:

$$\|g(y_1,w,\mu) - g(y_2,w,\mu)\| \leqslant k_3 \|y_1 - y_2\|, \tag{3.2}$$

$$\|g(y,w,\mu_1) - g(y,w,\mu_2)\| \leqslant k_4 \|\mu_1 - \mu_2\|. \tag{3.3}$$

Now consider the system given by Eqs. (2.1) and (3.1) and assume that $\|n\| \leqslant n_m$ for some $n_m > 0$ and define $\Delta\mu = \mu' - \mu$. Assume that the solutions of Eqs. (2.1) and (3.1) remain bounded. Then there exist constants $c_1 > 0$, $c_2 > 0$, and c_3 such that the following estimate holds:

$$\|e(k)\| \leqslant c_1 n_m + c_2 \|\Delta\mu\| + c_3 \rho^k. \tag{3.4}$$

Proof: Note that Eq. (3.1) can be rewritten as

$$w(k+1)=g(y(k),w(k),\mu)+[g(y(k)+n(k),w(k),\mu')-g(y(k),w(k),\mu')]+[g(y(k),w(k),\mu')-g(y(k),w(k),\mu)]. \quad (3.5)$$

Hence the error e now satisfies

$$e(k+1)=f(u(k),\mu)-g(y(k),w(k),\mu)-[g(y(k)+n(k),w(k),\mu')-g(y(k),w(k),\mu')]-[g(y(k),w(k),\mu')-g(y(k),w(k),\mu)]. \quad (3.6)$$

By using Eqs. (2.1)–(2.3) and Eqs. (3.2) and (3.3) in Eq. (3.6), we obtain

$$\|e(k+1)\|\leqslant\rho\|e(k)\|+k_1n_m+k_2\|\Delta\mu\|. \quad (3.7)$$

By using Eq. (3.7) repeatedly, we obtain

$$\|e(k)\|\leqslant\frac{k_3}{1-\rho}n_m+\frac{k_4}{1-\rho}\|\Delta\mu\|+\left(\|e(0)\|-\frac{k_1n_m+k_2\|\Delta\mu\|}{(1-\rho)\rho^2}\right)\rho^k, \quad (3.8)$$

which has the same form as Eq. (3.4).

Note that when $s(k)=1$, i.e., in the synchronization interval, our scheme uses Eqs. (2.1) and (3.1). Hence, Theorem 2 proves that in the synchronization interval, the synchronization error e remains bounded, hence our scheme is robust with respect to noise and parameter mismatch in this period. For simplicity, let us define e_∞ as follows:

$$e_\infty=\frac{k_3}{1-\rho}n_m+\frac{k_4}{1-\rho}\|\Delta\mu\|. \quad (3.9)$$

Note that $e(k)\to e_\infty$ as $k\to\infty$, hence e_∞ gives an asymptotic bound on the error. Moreover, this bound depends linearly on noise level and parameter mismatch, hence it decreases, (increases) linearly as the noise level and/or parameter mismatch decreases (increases). From a practical point of view, if T_s is sufficiently large, we may expect that the error reaches this bound at the end of each synchronization period.

Next, we will consider the robustness in the message transmission interval. Note that, in this case Eq. (2.4) takes the following form ($s=0$):

$$w(k+1)=f(w(k),\mu'), \quad (3.10)$$

Theorem 3: Consider the systems given by Eqs. (2.1) and (3.10). Assume that $f(u,\cdot)$ is Lipschitz, i.e., the following holds for some $k_5>0$:

$$\|f(u,\mu_1)-f(u,\mu_2)\|\leqslant k_5\|\mu_1-\mu_2\|. \quad (3.11)$$

Let e_∞ be the error bound given by Eq. (3.9) and assume that at the end of each synchronization interval we have $\|e\|\leqslant e_\infty+\epsilon_1$ for some sufficiently small ϵ_1 (Note that, by Eq. (3.8), this is the case if T_s is sufficiently large). Let $\epsilon>0$ satisfy the following:

$$k_2(k_1(e_\infty+\epsilon_1)+k_4\|\Delta\mu\|)<\epsilon. \quad (3.12)$$

Then there exists a maximum allowable message transmission interval $T\geqslant 1$ such that Eq. (2.21) is satisfied for any $T_m\leqslant T$.

Proof: By using Eqs. (2.1) and (3.10) we obtain

$$e(k+1)=[f(u(k),\mu)-f(w(k),\mu)]+[f(w(k),\mu)-f(w(k),\mu')]. \quad (3.13)$$

By using Eqs. (2.5) and (3.11) in Eq. (3.13) we obtain the following in each message transmission period:

$$\|e(k+1)\|\leqslant k_1\|e(k)\|+k_4\|\Delta\mu\|. \quad (3.14)$$

Since $\|\hat{m}(k)-m(k)\|\leqslant k_2\|e(k)\|$, and since $\|e\|\leqslant e_\infty+\epsilon_1$ at the beginning of each message transmission period, by using Eq. (3.14) we obtain the desired result.

Note that in the ideal case, for any length $T_m>0$, we can use our scheme provided that T_s is sufficiently big, and the main reason for this is that we can reduce the error to any level. But in the nonideal case, we cannot guarantee to reduce the error below a certain level (e_∞) that depends on the noise level and parameter mismatch, hence as a result of that we have an upper bound for T_m. If the message length is bigger than this bound, we may divide the message in parts and send each part in one message transmission period.

IV. SIMULATION RESULTS

First we choose the logistic equation for the master system and use the synchronization scheme proposed in [9]. Hence, the master and slave systems in our synchronization scheme are given as follows:

$$u(k+1)=\mu u(k)(1-u(k)),\quad y(k)=h(u(k))=u(k), \quad (4.1)$$

$$w(k+1)=\mu' w(k)(1-w(k))+s(k)[\mu'(1-y(k)-n(k)-w(k))-\rho](y(k)+n(k)-w(k)), \quad (4.2)$$

where $n(k)$ is the (random) noise, and $s(k)$ is the switching signal such that $s(k)=1$ in the synchronization period and $s(k)=0$ in the message transmission period. Note that $h(x)=x$ in this case. Due to the noise term, we may have $w(k+1)>1$ (<0), in which case we set $w(k+1)=1$ ($w(k+1)=0$) to guarantee boundedness of w. Let T_s and T_m denote the synchronization and message transmission period lengths. Let $m(k)$ be the message to be transmitted. For simplicity we will assume that $0\leqslant m\leqslant 1$. Switching signal $s(k)$ can be given as

$$s(k)=\begin{cases}1 & \text{when } k \pmod{(T_s+T_m)}\in[0,T_s)\\ 0 & \text{when } k \pmod{(T_s+T_m)}\in[T_s,T_s+T_m).\end{cases} \quad (4.3)$$

The signal transmitted to the slave system m_s can be given as $m_s(k)=y(k)$ when $s(k)=1$ and $m_s(k)=0.5(y(k)+m(k))$ when $s(k)=0$, or in short:

$$m_s(k)=y(k)+0.5(1-s(k))(m(k)-y(k)). \quad (4.4)$$

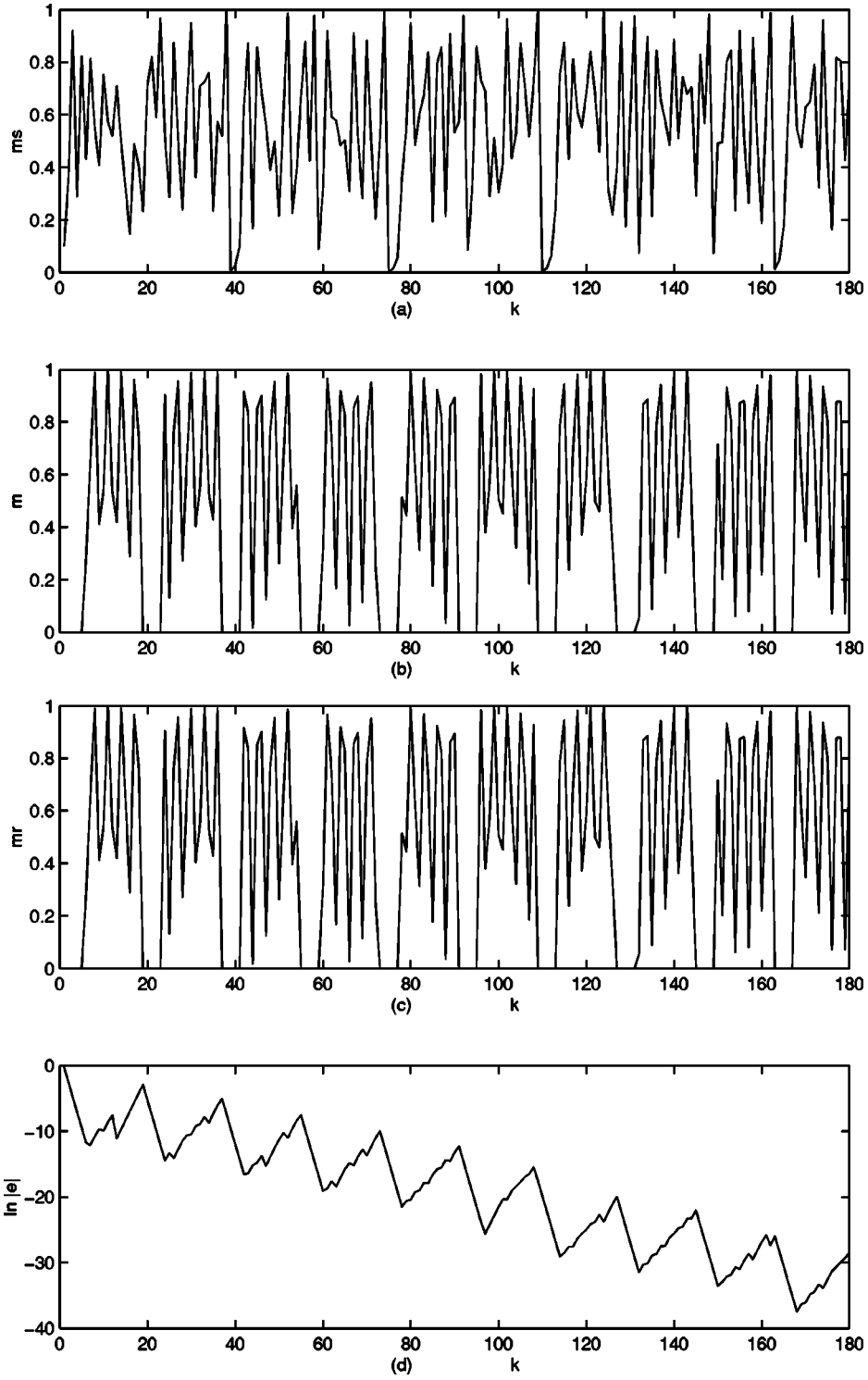

FIG. 1. Simulation results for the logistic map: ideal case. (a) Transmitted signal m_s, (b) Transmitted message m, (c) Recovered message $\hat{m}$, (d) $\ln|e(k)|$.

Note that we have $0 \leqslant m_s \leqslant 1$, which may result in better masking. In the message transmission period, we have

$$\hat{m}(k) = 2m_s(k) - h(w(k)),$$

$$k \pmod{(T_s+T_m)} \in [T_s, T_s+T_m). \tag{4.5}$$

Simple calculation shows that

$$m_s(k) - \hat{m}(k) = ce(k),$$

$$k \pmod{(T_s+T_m)} \in [T_s, T_s+T_m), \tag{4.6}$$

where $c=1$. We note that Eq. (4.5) redefines the recovered message $\hat{m}$, which is first introduced in Eq. (2.19). The apparent difference between Eqs. (4.5) and (2.19) is due to the form of the transmitted signal m_s given by Eq. (4.4). Note that in the message transmission phase we have $m_s(k) = 0.5(y(k)+m(k))$ as explained above, and hence Eqs. (4.5) and (2.19) will have the same form in these phases. We also emphasize that $\hat{m}$ represents the recovered message. We also note that in the Figs. 1–3, we used the symbol m_r for the recovered message instead of $\hat{m}$ for some technical reasons.

We simulated this system for two cases. In the first simu-

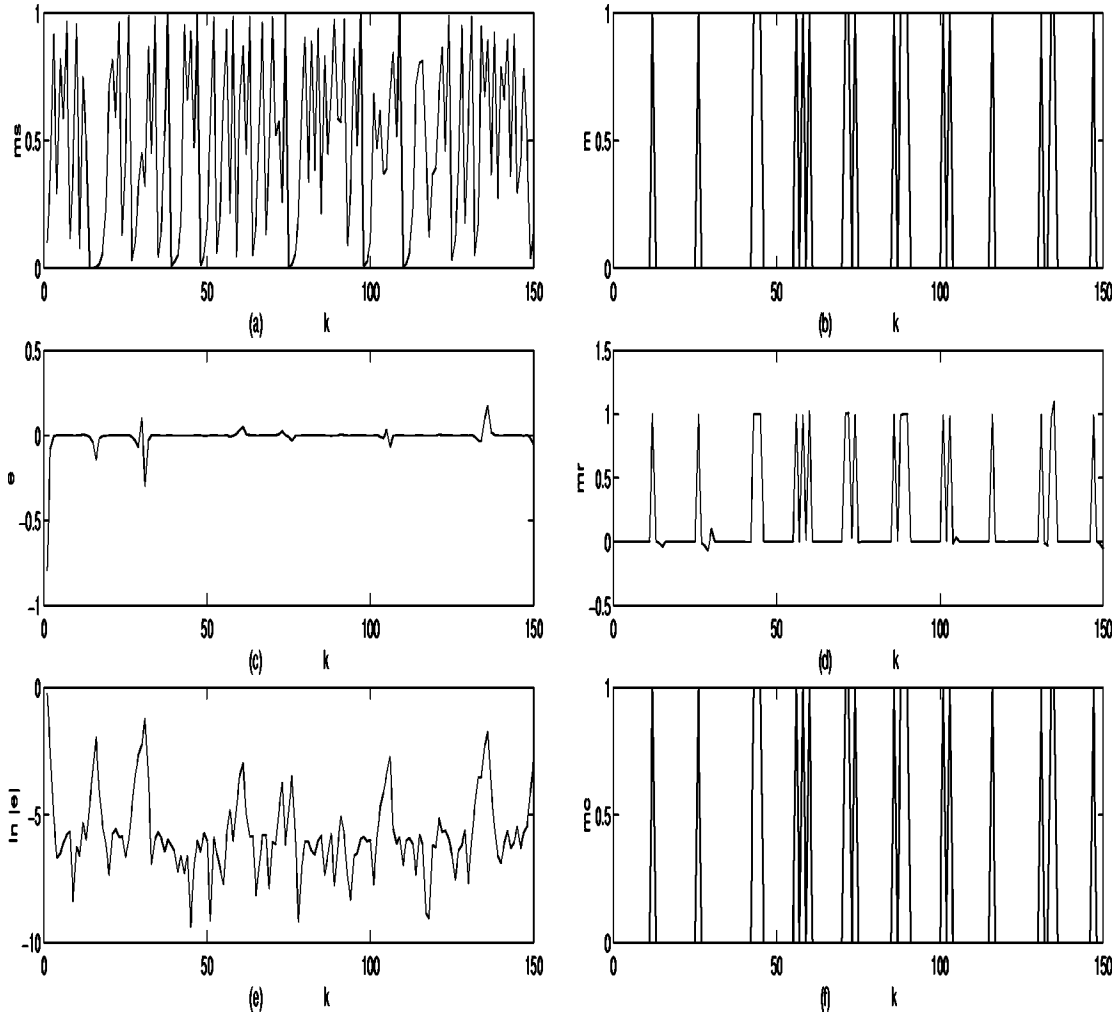

FIG. 2. Simulation results for the logistic map: Nonideal case. (a) Transmitted signal m_s, (b) Transmitted message m, (c) Error $e(k)$, (d) Recovered message $\hat{m}$, (e) $\ln|e(k)|$, (f) Corrected message m_c.

lation we choose the ideal case with $\mu=\mu'=4$, $\rho=0.1$, $n=0$, $T_s=5$, $T_m=13$. The message m is chosen as $m(k)=|\sin(k)|$ for k $(\mathrm{mod}(T_s+T_m))\in[T_s,T_s+T_m)$. The Lipschitz constants that appear in Eqs. (2.5), (2.20), (3.2), (3.3), and (3.11) can easily be found as $k_1=k_3=4$, $k_2=1$, $k_4=k_5=0.25$. The results of this simulation are shown in Fig. 1. Here, Fig. 1(a) and Fig. 1(b) show m_s and m, and apparently the message m is well-masked in m_s. Figure 1(c) shows the recovered message and Fig. 1(d) shows the synchronization error in logarithmic scale (i.e., $\ln|e(k)|$ versus k). (Note that in this case the error becomes extremely small, which necessitates the use of logarithmic scale to show meaningful results.) As can be seen, although the error increases in the message transmission periods, overall it decreases to zero exponentially.

In the second simulation we choose the nonideal case with $\mu=4$, $\mu'=3.99$ $(\Delta\mu=0.01)$, $\rho=0.1$, $T_s=10$, $T_m=5$, and n is a random noise uniformly distributed in $[0,0.001](n_m=0.001)$. As for the message we use the word ''EARTHQUAKE,'' coded by using Baudot code (see [19]). Here, each letter is represented by a five-digit code. Since $m(k)\in\{0,1\}$, the recovered message $\hat{m}$ can be corrected by using simple comparison as follows:

$$m_c(k)=\begin{cases}1 & \text{if} \quad \hat{m}(k)\geqslant 0.55\\ 0 & \text{if} \quad \hat{m}(k)\leqslant 0.45\end{cases}. \tag{4.7}$$

This also increases the tolerable error level [i.e., ϵ in Eqs. (2.24) and (3.12)]. The results of this simulation are shown in Fig. 2. Figures 2(a) and 2(b) show m_s and m, and as can be seen the message is well-masked. The synchronization error e is shown in Fig. 2(c) with normal scale and in 2(e) with logarithmic scale ($\ln|e(k)|$ vs k). The received and corrected messages are shown in Figs. 2(d) and 2(f), respectively. As can be seen, after correction, the message is reconstructed without error.

The main reason for relatively small T_m (or small ratio T_m/T_s) in the above simulations is the large Lipschitz constant k_1. To increase this ratio, we need chaotic systems with smaller k_1. An example of such a system may be given by a tent map as follows:

$$f(u,\mu)=\begin{cases}\mu u & \text{when} \quad 0\leqslant u\leqslant 0.5\\ \mu-\mu u & \text{when} \quad 0.5\leqslant u\leqslant 1,\end{cases} \tag{4.8}$$

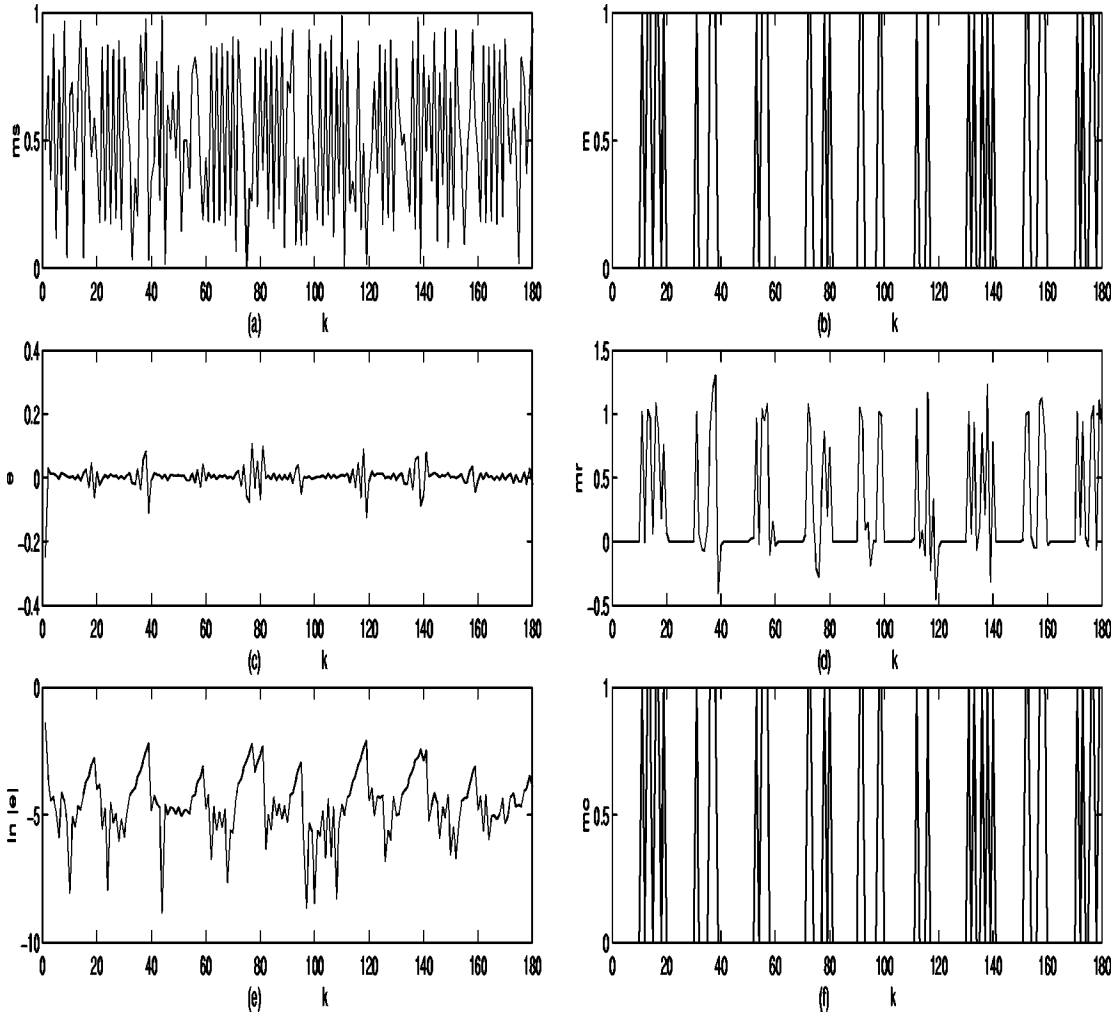

FIG. 3. Simulation results for the tent map: Nonideal case. (a) Transmitted signal m_s, (b) Transmitted message m, (c) Error $e(k)$, (d) Recovered message $\hat{m}$, (e) $\ln|e(k)|$, (f) Corrected message m_c.

and it can be shown that this system is chaotic for $\mu>1$ (see [20]). We also have $k_1=\mu$ for this example. The master system is given as

$$u(k+1)=f(u(k),\mu). \tag{4.9}$$

Note that in this case we have $0\leqslant m_2\leqslant u\leqslant m_1\leqslant 1$. Hence, we scale u to obtain the measured signal y as follows:

$$y(k)=h(u(k))=\frac{u(k)-m_2}{m_1-m_2}, \tag{4.10}$$

hence we have $0\leqslant y\leqslant 1$. For the synchronization, we use the scheme proposed in [6,8], hence the slave system is given by

$$w(k+1)=f[w(k)+s(k)\,\delta(z(k)+n(k)),\mu'],$$

$$z(k)=u(k)-w(k), \tag{4.11}$$

where $s(k)$ is given by Eq. (4.3) and $n(k)$ is a random noise. It can easily be shown that Eq. (2.3) is satisfied with $\rho=\mu(1-\delta)$ (see [5] for a similar computation for a skew-tent map). The transmitted message $m_s(k)$ and the recovered message $\hat{m}(k)$ are given by Eqs. (4.4) and (4.5), respectively. Note that Eq. (4.6) is satisfied in this case for $c=1/(m_1-m_2)$.

We simulated this system with $\mu=1.4$, $\mu'=1.39$ ($\Delta\mu=0.01$), $\rho=0.1$ ($\delta=0.93$), $T_s=10$, $T_m=10$, and n is a random noise, uniformly distributed in $[0,0.01]$ ($n_m=0.01$). The message m is chosen as the sentence ''CHAOS IS BEAUTIFUL,'' again coded by using Baudot code. Since $m(k)\in\{0,1\}$, after message recovery, we can use the message correction as given by Eq. (4.7). The results of this simulation are shown in Fig. 3. Figures 3(a) and 3(b) show m_s and m, and as can be seen the message is well-masked. The synchronization error e is shown in Fig. 2(c) with normal scale and in 2(e) with logarithmic scale ($\ln|e(k)|$ vs. k). The received and corrected messages are shown in Figs. 2(d) and 2(f), respectively. As can be seen, after correction, the message is reconstructed without error.

Comment 1: The usage of alternating synchronization and message transmission phases and the fact that the synchronization signal is only sent in the former phases while the message is only sent in the latter may be useful in certain applications. If only a synchronization scheme is used, there will not be any message to send, hence the message trans-

mission phases may be used for some other purposes, e.g., time multiplexing may be possible. For example, by carefully selecting the lengths of these intervals, it may be possible to synchronize e.g., two chaotic drive systems with their corresponding response parts by using a single communication channel. In such a case, the synchronization signals of the first and second chaotic drive systems will be sent to the corresponding response systems through the channel in the synchronization and message transmission phases, respectively. This approach may even be extended to synchronize more than two chaotic drive systems by using a single channel. However, this point requires careful investigation. As for the chaotic masking scheme, both analog (e.g., nonquantized) and digital messages may be used for message transmission; see the first and second simulations. However, the main application might be the transmission of digital messages through analog communication channels, since such signals are more error tolerant, see the second and third simulations. Also by using the idea of time multiplexing presented above it may be possible to send different messages to different response systems by using a single channel. However, this point also needs careful investigation.

Comment 2: One disadvantage of the proposed scheme is the fact that the message is only sent in the message transmission phases, which reduces the efficiency in using the channel. The quantity $\eta = T_m/(T_s+T_m)$ may be used to determine the efficiency. Since the useful information (message) is only sent in the message transmission phases, η could also be used as an indicator of the carrying capacity of the proposed scheme (i.e., the rate of transmission of useful information versus the total information). Obviously $\eta < 1$, and as η increases, so does the carrying capacity and the efficiency in using the channel. Note that η is larger in the ideal case, and it depends on some factors including the tolerable error level, the noise level, and the parameter mismatch in the nonideal case. In the first simulation presented above, we have $\eta = 0.72$ (ideal case), whereas in the second simulation we obtained $\eta = 0.33$ (nonideal case), which shows a sharp decrease in efficiency. In the third simulation we obtained $\eta = 0.5$. By using the tent map given by Eq. (4.8) and the parameters given in the third simulation, except for T_s and T_m, we obtained efficiencies as large as $\eta = 0.75$ in certain simulations. We note that η may be improved by using different chaotic systems, however this point also requires further investigation.

V. CONCLUSION

In this paper, we consider a synchronization and a related message transmission scheme by using synchronized chaotic systems. As in most synchronization schemes, we assume that a master system generates a chaotic signal that is used as an input in the slave system for synchronization. We assumed that a synchronization scheme for which the synchronization is achieved exponentially fast is available. The occasional synchronization scheme proposed in this paper consists of the application of synchronization and autonomous phases periodically. In the synchronization phases, the exponential synchronization scheme mentioned above is used and in the autonomous phases, the response system is switched to an autonomous system that is a replica of the drive system. In the case of message transmission, the message is masked by the drive signal and sent to the receiver only in the autonomous phases. We showed that under certain conditions, it is possible to achieve synchronization, and in the case of message transmission, it is possible to recover the message with acceptable error. We also proved that the proposed scheme is robust with respect to noise and parameter mismatch under certain conditions. Note that this robustness result is quite general and is due to the exponential synchronization. Hence our results also imply that any scheme that yields exponential synchronization is also robust with respect to noise and parameter mismatch under some conditions. We also presented some simulation results, which indicate that the proposed scheme could be used in some applications. These simulations suggest that the technique is particularly suitable for transmission of digital signals. In this case, the tolerable error level is quite large (e.g., half the message magnitude) and this increases the maximum allowable message length in the nonideal case. Moreover, by using a simple comparison, the message can be recovered exactly.

We do not investigate the security of our scheme, and do not claim any level of security. But we note that our results are independent of message level, whereas in most of the chaotic masking schemes, the message level is required to be sufficiently lower than that of the chaotic carrier. This point may be considered as an advantage of our scheme.

We also did not consider the synchronization of switching signal $s(k)$ between the master and slave systems. Since this signal is periodic, it can easily be generated in master and slave systems separately. Other schemes may be possible, but since researching such schemes is not our main aim, we did not investigate this problem in detail.

[1] G. Chen, *Control and Synchronization of Chaotic Systems (a Bibliography)* (ECE Department, University of Houston, Houston); available from ftp: ftp.egr.uh.edu/pub/TeX/chaos.tex (login name ''anonymous'' password: your email address).

[2] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Trans. Circuits Syst., I. Fundam. Theory Appl. **40**, 626 (1993).

[4] G. Kolumbán, M. P. Kennedy, and L. O. Chua, IEEE Trans. Circuits Syst., I Fundam. Theory Appl. **44**, 927 (1997).

[5] M. Hasler, Philos. Trans. R. Soc. London, Ser. A **353**, 115 (1995).

[6] M. Hasler and Y. L. Maistrenko, IEEE Trans. Circuits Syst., I Fundam. Theory Appl. **44** (10), 856 (1997).

[7] Lj. Kocarev, K. S. Halle, K. S. Eckert, and L. O. Chua, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).

[8] Y. Maistrenko and T. Kapitaniak, Phys. Rev. E **54**, 3285 (1996).

[9] Ö Morgül and E. Solak, Phys. Rev. E **54**, 4803 (1996).

[10] Ö. Morgül and E. Solak, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7** (6), 1307 (1997).

[11] Ö. Morgül, Phys. Rev. Lett. **82**, 77 (1999).
[12] Ö. Morgül, Phys. Lett. A **247**, 391 (1998).
[13] Ö. Morgül and M. Feki, Phys. Rev. E **55**, 5004 (1997).
[14] Ö. Morgül and M. Feki, Phys. Lett. A **251**, 169 (1998).
[15] M. J. Ogorzalek, IEEE Trans. Circuits Syst., I Fundam. Theory Appl. **40** (10), 693 (1993).
[16] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[17] L. M. Pecora and T. L. Carroll, Phys. Rev. A **44**, 2374 (1991).
[18] K. Pyragas, Phys. Lett. A **170**, 421 (1992).
[19] D. Salomon, *Data Compression* (Springer-Verlag, New York, 1998).
[20] S. H. Strogatz, *Nonlinear Dynamics and Chaos* (Addison-Wesley, Reading, MA, 1994).
[21] M. M. Sushchik, Jr., N. F. Rulkov, and H. D. I. Abarbanel, IEEE Trans. Circuits Syst., I Fundam. Theory Appl. **44** (10), 867 (1997).
[22] T. Ushio, IEEE Trans. Circuits Syst., I Fundam. Theory Appl. **43** (6), 500 (1996).
[23] T. Ushio, Int. J. Bifurcation Chaos Appl. Sci. Eng. **9** (3), 541 (1999).