Digital communication by active-passive-decomposition synchronization in hyperchaotic systems

Yu Zhang, Ming Dai, Yiman Hua, Wansun Ni, and Gonghuan Du
Institute of Acoustics, State Key Laboratory of Modern Acoustics, Nanjing University, Nanjing 210093, People's Republic of China

(Received 15 December 1997; revised manuscript received 24 April 1998)

In this paper we investigate the digital speech communication by active-passive-decomposition (APD) synchronization in a hyperchaotic system with a one-way coupled ring map lattice with length *m*. We present an analysis of the synchronous principle, synchronization time, and the sensitivity of synchronization to the parameter differences. Experiments as well as theory demonstrate that the APD method leads to secure encoding, short time synchronization, and recovery without error. [S1063-651X(98)01609-2]

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

I. INTRODUCTION

Chaos synchronization makes it practicable to synchronize two chaotic systems that indicate the sensitive dependence on initial conditions and arouses great interest in light of its potential applications. Recently, the use of chaos synchronization in private communication has been investigated by several authors [1–5]. By synchronization, an information signal modulated by a chaotic signal as a broadband carrier can be recovered efficiently. As it is known, most investigations of private communication that focused on low-dimensional chaotic system did not make the best use of antideciphering. A hyperchaotic system, even a spatiotemporal chaotic system, can make any imitation of keys and attack against communications more difficult and the communication efficiency can be greatly enhanced. Therefore, their application has become a popular topic [3,6]. Recently, Kocarev and Parlitz [2] have proposed their active-passive-decomposition (APD) synchronization in continuous systems. It has turned out that this technique not only yielded a recovery without errors but also led to a more secure encoding. Thus it is very useful for private communication in hyperchaotic system.

Generally, it is difficult to find a region in parameter space where hyperchaos exists. Therefore, Kocarev and Parlitz suggested a method that constructs high-dimensional synchronization system using low-dimensional systems as building blocks. Despite this, for a bit high dimensional system, in particular a spatiotemporal chaotic system, it is difficult to realize under the actual perturbed environment since the inevitable errors of a continuous system exist. In recent years, with the development of the digital technique, there has been a great interest in the dynamics of the coupled map lattice for its easy realization, computation efficiency, and rich spatiotemporal characteristic [7,8]. Moreover, in some parameter regions, it can produce spatiotemporal chaos. Thus it is natural to consider this system as the high-dimensional chaotic dynamic model to investigate synchronization and digital private communication.

In this paper we investigate speech communication by APD synchronization in a one-way coupled ring map lattice with length *m* (*m*-OCRML). We investigate the synchronous principle of *m*-OCRML hyperchaotic systems and derive analytically the synchronization time and the sensitivity of synchronization to parameter differences. It quantitatively presents the theoretical support to the security of hyperchaotic systems in digital communication. We perform a speech communication experiment by the APD technique. The experimental results not only support our analysis, but also demonstrate that APD synchronization in *m*-OCRML systems leads to secure encoding, short time synchronization, and recovery without error.

II. ANALYSIS

We investigate the digital communication using APD synchronization in the *m*-OCRML system. The dynamics of the systems can be described as follows: For the transmitter

$$\begin{aligned}
x_1(n+1)&=(1-\epsilon_1)f(x_1(n),\mu_1)+g(n),\\
x_i(n+1)&=(1-\epsilon_i)f(x_i(n),\mu_i)+\epsilon_i f(x_{i+1}(n),\mu_{i+1})\\
&\quad (i=2,\dots,m-1),\\
x_m(n+1)&=(1-\epsilon_m)f(x_m(n),\mu_m)+\epsilon_m f(x_1(n),\mu_1),\\
g(n)&=\epsilon_1 f(x_2(n),\mu_2)+s(n),
\end{aligned} \tag{1}$$

and the receiver

$$\begin{aligned}
y_1(n+1)&=(1-\epsilon_1')f(y_1(n),\mu_1')+g'(n),\\
y_i(n+1)&=(1-\epsilon_i')f(y_i(n),\mu_i')+\epsilon_i' f(y_{i+1}(n),\mu_{i+1}'),\\
y_m(n+1)&=(1-\epsilon_m')f(y_m(n),\mu_m')+\epsilon_m' f(y_1(n),\mu_1'),\\
s'(n)&=g'(n)-\epsilon_1' f(y_2(n),\mu_2'),
\end{aligned} \tag{2}$$

where m is the length of the OCRML, ϵ_i is the coupling constant, μ_i is the nonlinearity of the nonlinear function $f(x_i(n),\mu_i)$, the subscript i denotes the lattice site index, n is the discrete time, $g(n)$ is the transmitted signal of transmitter, $g'(n)$ is the received signal of receiver, $s(n)$ is the information signal, and $s'(n)$ is the recovered signal. Consider the receiver as a copy of the transmitter, i.e., $\epsilon_j=\epsilon_j'$, $\mu_j=\mu_j'$, and $g(n)=g'(n)$ $(j=1,\dots,m)$. With the decomposition [2] given by $g(n)=\epsilon_1 f(x_2(n),\mu_2)+s_n$, the difference equations for $e_j(n+1)=y_j(n+1)-x_j(n+1)$ are

$$\begin{aligned} e_1(n+1)&=(1-\epsilon_1)f_{x_1}e_1(n),\\ e_i(n+1)&=(1-\epsilon_i)f_{x_i}e_i(n)+\epsilon_i f_{x_{i+1}}e_{i+1}(n),\\ e_m(n+1)&=(1-\epsilon_m)f_{x_m}e_m(n)+\epsilon_m f_{x_1}e_1(n). \end{aligned} \tag{3}$$

The criteria for convergence of $e_j(n+1)$ to zero depend on the conditional Lyapunov multipliers calculated from the eigenvalues of the product [9]

$$J=\prod_{n=1}^{\infty} D_{\mathbf{x}}\mathbf{e}(e_1,e_2,\ldots,e_m), \tag{4}$$

where

$$D_{\mathbf{x}}\mathbf{e}=\begin{bmatrix} (1-\epsilon_1)f_{x_1} & 0 & 0 & \cdots & 0\\ 0 & (1-\epsilon_2)f_{x_2} & \epsilon_2 f_{x_3} & \cdots & 0\\ 0 & 0 & (1-\epsilon_3)f_{x_3} & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \epsilon_m f_{x_1} & 0 & 0 & \cdots & (1-\epsilon_m)f_{x_m} \end{bmatrix}. \tag{5}$$

We assume that the f_{x_j} are bounded. Approximately, with $\epsilon_j \to 1$, the absolute values of the eigenvalues $|\lambda_j|=|(1-\epsilon_j)f_{x_j}| \ll 1$ lead e_j of Eq. (3) to converge to zero (it should be confirmed further by the calculation of the conditional Lyapunov exponents). So synchronization between the transmitter and the receiver with the different initial conditions is realized. Then the recovered signal $s'(n)$ is solved as

$$\begin{aligned} s'(n)&=g'(n)-\epsilon_1' f(y_2(n),\mu_2')\\ &=\epsilon_1\{f(x_2(n),\mu_2)-f(y_2(n),\mu_2')\}+s(n)\approx s(n). \end{aligned}$$

In a real digital communication experiment, the efficiency of communication is affected by at least two factors: synchronization time T_s and deviation of the system parameters. For communication, a short synchronization time is important in practice. We estimate the shortest synchronization time of the m-OCRML system as follows. With $\epsilon_j \to 1$, $t_j(n+1)=(1-\epsilon_j)f_{x_j}t_j(n)$ will converge to zero very quickly. Generally, the convergence rate will approach a certain value so that convergence is achieved at the next iteration. Following this rate, $e_1(n+1)\to 0$ leads to $e_m(n+2)\to 0$, $e_m(n+2)\to 0$ leads to $e_{m-1}(n+3)\to 0$, and so on. Finally, $e_2(n+m)\to 0$. Therefore, the shortest synchronization time can be given as $T_s=m$. In other words, the length of the lattice determines the fastest rate of digital communication.

The sensitivity of synchronization to parameter differences is another important factor that influences synchronization. On the one hand, it may cause difficulty in synchronizing two chaotic systems. On the other hand, even under the same initial conditions, the slight deviation of parameters between two systems may lead to remarkably different results. Therefore, for secure encoding, the sensitivity to the deviation of parameters is very important for private communication. In high-dimensional m-OCRMC system, the deviations of the nonlinearity μ_j and the coupling constant ϵ_j are the main parameters that influence synchronization. Obviously, the sensitivity of synchronization to these parameter differences should be investigated. We consider the influence of $\Delta\mu_j=\mu_j-\mu_j'$ and $\Delta\epsilon_j=\epsilon_j-\epsilon_j'$, respectively, on $\Delta s(n)=s(n)-s'(n)$.

First, considering the influence of $\Delta\mu_j=\mu_j-\mu_j'$ on $\Delta s(n)=s(n)-s'(n)$, Eq. (3) leads to

$$\begin{aligned} e_1(n+1)&=(1-\epsilon_1)[f_{x_1}e_1(n)+f_{\mu_1}\Delta\mu_1],\\ e_i(n+1)&=(1-\epsilon_i)[f_{x_i}e_i(n)+f_{\mu_i}\Delta\mu_i]\\ &\quad+\epsilon_i[f_{x_{i+1}}e_{i+1}(n)+f_{\mu_{i+1}}\Delta\mu_{i+1}],\\ e_m(n+1)&=(1-\epsilon_m)[f_{x_m}e_m(n)+f_{\mu_m}\Delta\mu_m]\\ &\quad+\epsilon_m[f_{x_1}e_1(n)+f_{\mu_1}\Delta\mu_1]. \end{aligned} \tag{6}$$

Here we define $\hat{e}_j(n+1)$ as the principal matrix solution, i.e.,

$$\hat{e}_j(n+1)=D_{\mathbf{x}}\hat{e}_j(n). \tag{7}$$

Taking the linear approximation of $\Delta\mu_2$ and replacing $f_{x_j}e_j(n)$ with $e_j(n+1)$ and $\Delta\mu_j$, etc., we solve $\Delta s(n)$ as

$$\begin{aligned} \Delta s(n)&=s(n)-s'(n)\\ &=\epsilon_1\{f(y_2(n),\mu_2)-f(x_2(n),\mu_2{}')\}\\ &=\epsilon_1\{f_{x_2}e_2(n)+f_{\mu_2}\Delta\mu_2\}\\ &=\sum_{i=2}^{m}\left[\frac{(-1)^i\prod_{j=1}^{i-1}\epsilon_j}{\prod_{j=2}^{i}(1-\epsilon_j)}\,e_i(n+1)\right]\\ &\quad+\frac{(-1)^{m+1}\prod_{j=1}^{m}\epsilon_j}{\prod_{j=2}^{m}(1-\epsilon_j)}\,[f_{x_1}e_1(n)+f_{\mu_1}\Delta\mu_1]. \end{aligned} \tag{8}$$

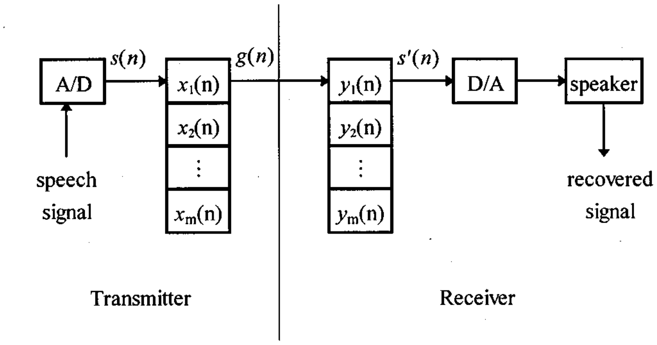

FIG. 1. System diagram of digital speech communication by the APD method.

With $\Delta\mu_j=0$, $j\neq l$, $l\neq 1$, and $j=1,2,...,m$, we obtain the asymptotic solution

$$\Delta s(n)=\sum_{i=2}^{l-1}\left[\frac{(-1)^i\prod_{j=1}^{i-1}\epsilon_j}{\prod_{j=2}^{i}(1-\epsilon_j)}e_j(n+1)\right]+\frac{(-1)^l\prod_{j=1}^{l-1}\epsilon_j}{\prod_{j=2}^{l}(1-\epsilon_j)}e_l(n+1), \qquad (9)$$

$$e_l(n+1)=(1-\epsilon_l)f_{\mu_l}\Delta\mu_l\circ\hat{e}_l(n+1),$$

where $\circ$ denotes convolution, i.e., $x(n)\circ y(n)=\Sigma_{m=-\infty}^{\infty}x(m)y(n-m)$. With $\epsilon_j/(1-\epsilon_j)\gg 1$, keeping the highest-order term, the mean-square value of $\Delta s(n)$ is

$$\sqrt{\langle[\Delta s(n)]^2\rangle}=\epsilon_1\prod_{j=2}^{l-1}\left[\frac{\epsilon_j}{1-\epsilon_j}\right]\Delta\mu_l\sqrt{\langle[f_{\mu_l}\circ\hat{e}_l(n+1)]^2\rangle}. \qquad (10)$$

As an average value $\sqrt{\langle(f_{\mu_l}\circ\hat{e}_l(n+1))^2\rangle}$ is nearly constant with time and thus $\sqrt{\langle[\Delta s(n)]^2\rangle}$ is linear with $\Delta\mu_l$. It is seen that $\sqrt{\langle[\Delta s(n)]^2\rangle}$ is amplified multiplicatively with the increase of l. Therefore, the selection of l is important to improve the sensitivity of synchronization to parameter differences. It is known that for convection in a flow system, a single local disturbance will be amplified as it is convected through the spatial extent [10]. In m-OCRMC systems, the effect that $\Delta\mu_l$ has on the lattice will be amplified through convection with the decrease of the index for the lattice sites. In particular, the effect of $\Delta\mu_1$ will be convected through the whole lattice. Therefore, its influence on the sensitivity is most significant. Performing some reasonable approximations and substitutions, we solve the mean-square value of $\Delta s(n)$ as

$$\sqrt{\langle[\Delta s(n)]^2\rangle}=\frac{\prod_{j=1}^{m}\epsilon_j}{\prod_{j=2}^{m}(1-\epsilon_j)}\times\Delta\mu_1\{\langle[f_{\mu_1}\circ\hat{e}_1(n+1)\circ\hat{e}_m(n+1)-f_{\mu_1}\circ\hat{e}_1(n+1)]^2\rangle\}^{1/2} \qquad (11)$$

The first term of the root-mean square is much smaller than the second one, thus

$$\sqrt{\langle[\Delta s(n)]^2\rangle}=\epsilon_1\prod_{j=2}^{m}\left(\frac{\epsilon_j}{1-\epsilon_j}\right)\Delta\mu_1\sqrt{\langle[f_{\mu_1}\circ\hat{e}_1(n+1)]^2\rangle}, \qquad (12)$$

which states that $\sqrt{\langle[\Delta s(n)]^2\rangle}$ increases linearly with the increase of $\Delta\mu_1$. Also, the sensitivity to the difference of $\Delta\mu_1$ increases with the increase of the length of the lattice m. With large m, the slight deviation of $\Delta\mu_1$ leads to a large distortion in the recovery of information. Therefore, in m-OCRML systems, the hyperchaotic system benefits from secure encoding.

Further, investigating the influence of the deviation of the coupling constants $\Delta\epsilon_j=\epsilon_j-\epsilon_j'$ on $\Delta s(n)=s(n)-s'(n)$, we rewrite Eqs. (3) as

$$e_1(n+1)=-f(x_1(n),\mu_1)\Delta\epsilon_1+(1-\epsilon_1)f_{x_1}e_1(n),$$

$$e_i(n+1)=-f(x_i(n),\mu_i)\Delta\epsilon_i+(1-\epsilon_i)f_{x_i}e_i(n)+f(x_{i+1}(n),\mu_{i+1})\Delta\epsilon_i+\epsilon_i f_{x_{i+1}}e_{i+1}(n),$$

$$e_m(n+1)=-f(x_m(n),\mu_m)\Delta\epsilon_m+(1-\epsilon_m)f_{x_m}e_m(n)+f(x_1(n),\mu_1)\Delta\epsilon_m+\epsilon_m f_{x_1}e_1(n) \qquad (13)$$

Similarly, we obtain

$$\Delta s(n)=\sum_{i=2}^{m}\left\{\frac{(-1)^i\prod_{j=1}^{i-1}\epsilon_j}{\prod_{j=2}^{i}(1-\epsilon_j)}\{e_i(n+1)+\Delta\epsilon_i[f(x_i,\mu_i)-f(x_{i+1},\mu_{i+1})]\}\right\}+f(x_2,\mu_2)\Delta\epsilon_1+\frac{(-1)^{m+1}\prod_{j=1}^{m}\epsilon_j}{\prod_{j=2}^{m}(1-\epsilon_j)}\times f_{x_1}(-f(x_1,\mu_1)\Delta\epsilon_1\circ\hat{e}_1(n+1)), \qquad (14)$$

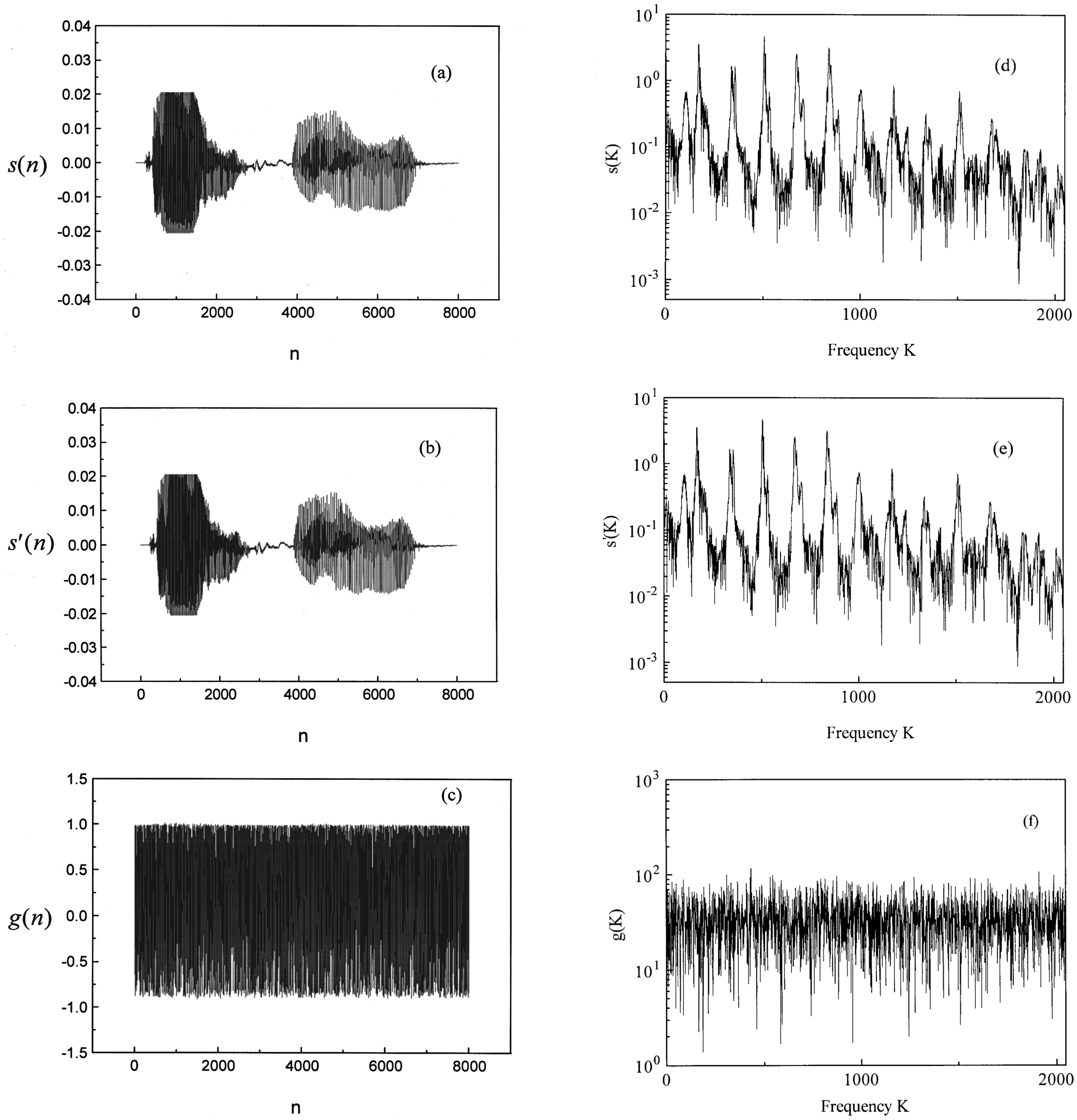

FIG. 2. Modulation or detection process, where $m=10$ and the values in the plots have been normalized. The (a) information signal $s(n)$, (b) recovered signal $s'(n)$, and (c) transmitter sequence $g(n)$ are shown. Their frequency spectra are in (d), (e), and (f), respectively.

where we define $f(x_{m+1},\mu_{m+1})=f(x_1,\mu_1)$. With $\Delta\epsilon_j=0$, $j\neq 1$, Eq. (14) can be reduced to

$$\sqrt{\langle[\Delta s(n)]^2\rangle}=\epsilon_1\prod_{j=2}^{m}\left[\frac{\epsilon_j}{1-\epsilon_j}\right]\times\Delta\epsilon_1\{\langle[f_{x_1}f(x_1,\mu_1)\circ\hat{e}_1(n+1)]^2\rangle\}^{1/2}. \tag{15}$$

A similar result with $\Delta\mu_j$ can be found. Thus we believe that in m-OCRML systems the deviation of the parameters has a significant effect on synchronization as well as private communication. Any slight perturbation of the parameters can be amplified as a multiplication of series, which makes it difficult to imitate keys and decipher in digital communication. However, it should be mentioned that this amplification resulting from the deviation of system parameters will make the above results deviate from the linearity by degrees and approach saturation instead of infinity as predicted by Eqs. (10), (12), (15), etc.

III. EXPERIMENT

According to the analysis, we perform some experiments on speech communication systems. Figure 1 illustrates the systematic diagram resulting from the study of private communication by the APD technique. Here we take the coupling constant $\epsilon_j=0.99$ and the nonlinear function $f(x_j)=1-\mu_j x_j^2$, where the nonlinear parameter $\mu_j=1.9$ corresponds to the single-site system in a chaotic state. We first consider synchronization between the transmitter and the receiver. Synchronization occurs if all the conditional Lyapunov exponents of the receiver are negative. However, this does not exclude the hyperchaotic behavior of the transmitter. With $m=3$, the positive Lyapunov exponent spectra of the m-OCRML systems are $\lambda_1=0.53$, $\lambda_2=0.51$, and λ_3

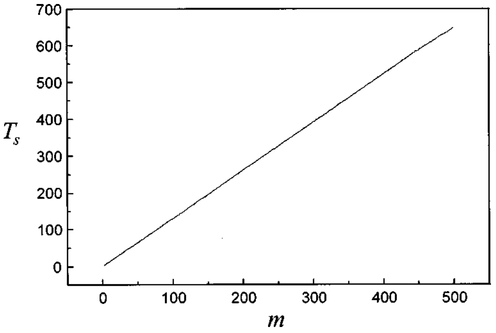

FIG. 3. Dependence of the synchronization time T_s on the lattice length m. For the discrete time $n>T_s$, two systems are synchronous within the computational accuracy.

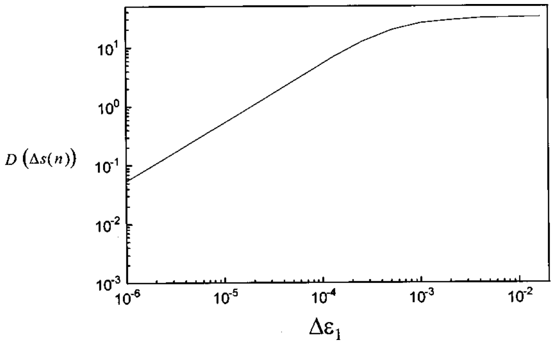

FIG. 5. Dependence of $D(\Delta s(n))$ on the deviation of the coupling constant $\Delta\epsilon_1$.

$=0.49$. The system with more than one positive Lyapunov exponent is hyperchaotic. When synchronization is achieved by the APD method, the speech signal $s(n)$ can be recovered and it is of great quality in listening tests. Figure 2 illustrates the modulation or detection process, in which $m=10$ and the information signal $s(n)$ ‘‘Zhang Ping’’ in Chinese is sampled at 8 kHz. $s(n)$, $s'(n)$, and $g(n)$ are plotted in Figs. 2(a), 2(b), and 2(c), respectively. In order to confirm that no information is revealed in transmission we use a fast Fourier transform routine to calculate the spectra of a segment of $s(n)$, $s'(n)$, and $g(n)$, which are shown as Figs. 2(d), 2(e), and 2(f), respectively. Obviously, the information signal is masked in a broadband, noiselike signal, i.e., no information signal is revealed in the transmission. In Fig. 3 we illustrate the dependence of the synchronization time T_s on the lattice length m for its importance in communication, where T_s is defined as the discrete time n to satisfy $\Delta=\sqrt{(1/m)\Sigma_{j=1}^{m}e_j^2(n)}<10^{-6}$. It shows that T_s increases with the lattice length m. Particularly with $\epsilon_j\rightarrow 1$, our calculation supports the shortest synchronization time $T_s=m$ (here, for simplicity, we do not present this $T_s\sim m$ curve). The experimental results demonstrate that with $m=10$, the synchronization time T_s is fit for the digital speech communication. To study the sensitivity of synchronization to the parameter differences, we define $D(\Delta s(n))=\sqrt{\Sigma[s'(n)-s(n)]^2/\Sigma s^2(n)}$ as the test criterion. Figure 4(a) shows the relation between the slight perturbation of the nonlinear parameters $\Delta\mu_j$ $(j=1,\ldots,m)$ and $D(\Delta s(n))$, where the lines $(L1,\ldots,L10)$ correspond to the parameter differences $(\Delta\mu_1,\ldots,\Delta\mu_{10})$. We find that the sensitivity to parameter differences increases with the increase of the index for the lattice sites (except $\Delta\mu_1$). Figure 4(b) shows that $D(\Delta s(n))$ increases with the increase of $\Delta\mu_1$ and m, where the lines $(L1,\ldots,L4)$ correspond to $m=4,6,8,10$, respectively. Some slight parameter differences have been amplified to the much distorted results. For example, when $\Delta\mu_1=2.0\times10^{-4}$, $D(\Delta s(n))$ approach 3, so that no speech can be heard in the recovered signals. Similarly, the relation between the slight perturbation of the coupling constant $\Delta\epsilon_1$ and $D(\Delta s(n))$ is given in Fig. 5. These relations $T_s\sim m$, $\Delta\mu_j\sim D(\Delta s(n))$, and $\Delta\epsilon_1\sim D(\Delta s(n))$ are consistent with the theoretical predictions. They are important for communication safety. Simply, we calculate the following. For one-dimensional chaos, suppose that the probability of the imitation of the key $\Delta\mu_1$ is $1/T$ (where T is determined by computational accuracy, e.g., $T=10^6$ with $m=10$ in our experiment.). Then, for an m-dimensional hyperchaotic system, this probability can be reduced to $(1/T)^m$ (e.g., 10^{-60} with $m=10$ in our work). In particular, we have demonstrated that any error of parameters will make the distortion remarkably amplified as the multiplication of the series. It is almost impossible to reproduce the chaotic sequence to decipher from the transmitted signals without knowing all the details of the m-OCRML hyperchaotic system. Hyperchaotic systems, particularly spatiotemporal chaotic systems, can lead to great security in digital communication.

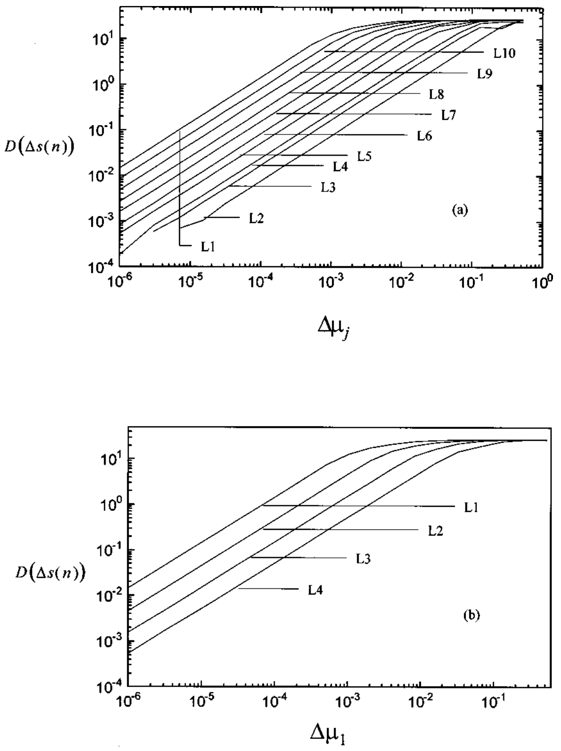

FIG. 4. Dependence of $D(\Delta s(n))$ on the deviation of the nonlinear parameters. $D(\Delta s(n))$ is dimensionless. (a) $D(\Delta s(n))$ vs $\Delta\mu_j$ $(j=1,\ldots,m)$, where lines $L1,\ldots,L10$ correspond to the parameter differences $\Delta\mu_1,\ldots,\Delta\mu_{10}$. (b) $D(\Delta s(n))$ vs $\Delta\mu_1$, where lines $L1,\ldots,L4$ correspond to the lattice length $m=4,6,8,10$.

IV. CONCLUSION

We have studied digital speech private communication by the APD method in the m-OCRML system. We presented analytically the synchronous principle, synchronization time, and sensitivity of synchronization to parameter differences. Digital speech communication has been carried out. The results not only support the theoretical prediction, but also present a good experimental realization in digital communication by hyperchaotic synchronization. The security and recovery without error made the application of APD synchronization in high-dimensional systems very useful and encouraging for digital private communication.

ACKNOWLEDGMENT

The work was partly supported by the National Natural Science Foundation of China.

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

[2] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).

[3] J. H. Xiao, G. Hu, and Z. L. Qu, Phys. Rev. Lett. **77**, 4162 (1996).

[4] T. L. Carroll, J. F. Heagy, and L. M. Pecora, Phys. Rev. Lett. **76**, 904 (1996).

[5] Y. H. Yu, K. Kwak, and T. K. Lim, Phys. Lett. A **197**, 311 (1995).

[6] G. Hu, J. H. Xiao, F. G. Xie, and Z. L. Qu, Phys. Rev. E **56**, 2738 (1997).

[7] I. Aranson, D. Golomb, and H. Sompolinsky, Phys. Rev. Lett. **68**, 3495 (1992).

[8] F. H. Willeboordse and K. Kaneko, Phys. Rev. Lett. **73**, 533 (1994).

[9] L. M. Pecora and T. L. Carroll, Phys. Rev. A **44**, 2374 (1991).

[10] D. Auerbach, Phys. Rev. Lett. **72**, 1184 (1994).