Digital communication robust to transmission error via chaotic synchronization based on contraction maps

Chang-song Zhou[1] and Tian-lun Chen[2,1]
[1] *Department of Physics, Nankai University, Tianjin 300071, China*
[2] *CCAST (World Laboratory), Beijing 100080, China*

(Received 13 December 1996)

Most of the methods proposed for communication using chaotic dynamics deal with analog communication. A method for digital communication is presented in this paper, with the chaotic carrier being digitized. Quantization of the chaotic carrier destroys the exact synchronization, which however, does not prevent the receiver from decoding the message correctly. It is demonstrated by numerical simulations that digital communication is very robust to transmission errors resulting from channel noise. [S1063-651X(97)10208-2]

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

I. INTRODUCTION

Recently, potential applications of chaotic dynamics to secure communication have drawn great research attention. The main idea is to employ chaos as a broadband carrier for encoding and masking information signals. Most approaches proposed to realize this basic idea are based on synchronization of chaotic systems to mask and recover analog messages [1,2] and digital messages [2–4]. Other methods include controlling chaotic system to follow a desired wave form in which a message is encoded [5], and making use of the quick decay of a correlation function for chaotic signals [6]. However, chaotic dynamical systems exhibit regular geometric structures which are often far from random when viewed in some suitable phase space. Some researchers have shown that it is possible to reveal the hidden information by recreating the geometric structure with some prediction-based methods [7], particularly when the hidden signals are added to the chaotic carrier at very low power, or it is possible to find some suitable return maps which allow the information to be extracted [8].

In all the above methods, the chaotic carrier signal transmitted from the transmitter to the receiver is analog, which seems to be a natural requirement for the methods based on synchronization of chaotic systems, because the chaotic carrier not only bears the message but also drives the receiver to synchronize with the transmitter. Since chaotic synchronization is sensitive to external interferences, any form of alternation to the driving signal may spoil the exact synchronization and make it difficult or even impossible to decode or unmask the hidden message correctly. As a result, as a special form of alternation, quantization of the chaotic carrier, which is necessary for digital communication, may destroy the synchronization which is necessary for correct decoding or unmasking of the message in the receiver. So it seems difficult to realize digital communication based on chaotic synchronization.

However, almost all modern communications are digital. For future implementation of communication using chaos, it is necessary to explore digital communication in this field. Lately, Stojanovski, Kocarev, and Parlitz [9] have shown that, under some conditions, the state of a chaotic system driven by chaotic impulses from another chaotic system may comply to the state of the driving system in the sense of generalized synchronization. When the chaotic impulses are quantized, the synchronization differences are restricted within some amplitude, which can be employed to realize digital communication.

In this paper, we present a method for transmission binary message by digitized chaotic carrier. The method is based on an analog communication method we previously proposed for robust transmission of a binary message via chaotic synchronization [10]. The analog communication method is briefly described in Sec. II and the digital communication method in Sec. III. The validity and robustness of the digital communication is demonstrated with the Hénon map in Sec. IV.

II. ANALOG COMMUNICATION SYSTEM

The analog communication system [10] for transmission binary message employs chaotic synchronization based on contract maps [11]. A chaotic discrete-time system

$$x(n+1)=f(x(n)) \quad (x\in\mathbb{R}^M) \tag{1}$$

is partitioned into two parts

$$x(n+1)=g(x(n))+h(x(n)), \tag{2}$$

where g is a contraction map on a closed set $\Omega\subset\mathbb{R}^M$, namely

$$\|g(x)-g(y)\|\leqslant\alpha_g\|x-y\|. \tag{3}$$

α_g is the contraction constant of g on Ω, $0\leqslant\alpha_g<1$.

A drive-response system can be constructed as

$$x(n+1)=g(x(n))+h(x(n)), \tag{4}$$

$$y(n+1)=g(y(n))+h(x(n)), \tag{5}$$

which will achieve in-phase synchronization if $x(n)$ and $y(n)$ are confined in Ω for each $n\geqslant 0$, because

$$\begin{aligned}\|x(n+1)-y(n+1)\| &= \|g(x(n))-g(y(n))\| \\ &\leqslant \alpha_g \|x(n)-y(n)\|\end{aligned} \tag{6}$$

and

$$\lim_{n\to\infty} \|x(n)-y(n)\| = 0. \tag{7}$$

On the other hand, if map g also satisfies

$$\|g(x)+g(y)\| \leqslant \alpha_g' \|x+y\| \tag{8}$$

for any x and y in a closed set Ω' with $0 \leqslant \alpha_g' < 1$, the following drive-response system

$$x(n+1) = g(x(n)) + h(x(n)), \tag{9}$$

$$y(n+1) = g(y(n)) - h(x(n)) \tag{10}$$

will achieve antiphase synchronization if $x(n)$ and $y(n)$ are in Ω' for $n \geqslant 0$, because

$$\begin{aligned}\|x(n+1)+y(n+1)\| &= \|g(x(n))+g(y(n))\| \\ &\leqslant \alpha_g' \|x(n)+y(n)\|\end{aligned} \tag{11}$$

and

$$\lim_{n\to\infty} \|x(n)+y(n)\| = 0. \tag{12}$$

For the purpose of communication, we employ a chaotic system f which can be partitioned as $f = g + h$, and g satisfies both

$$\|g(x) \pm g(y)\| \leqslant \alpha_g \|x \pm y\| \tag{13}$$

for any $x,y \in \Omega$ with $0 \leqslant \alpha_g < 1$. The system has a chaotic attractor A in Ω and that $-A = \{-x | x \in A\}$ is also in Ω. For simplicity, we further require that $h(x)$ be a scalar signal.

The main idea of the present communication method is to encode the two symbols 1 and -1 of a binary message with the in-phase and antiphase synchronization of the above chaotic system respectively.

We employ the scheme proposed in [6] to encode the binary message. Each symbol $b^k \in \{-1,1\}$ is represented by N elements of $h(x(n))$ $(n = 1+(k-1)N, \ldots, kN)$, and the transmitted signal $s(n)$ is given by

$$s(n) = b^k h(x(n)). \tag{14}$$

The communication system is constructed as follows:

$$\begin{aligned} x(n+1) &= g(x(n)) + h(x(n)) \quad \text{transmitter}, \\ s(n) &= b^k h(x(n)) \quad \text{transmitter signal}, \\ y(n+1) &= g(y(n)) + s(n) \quad \text{receiver}. \end{aligned} \tag{15}$$

It is seen from Eq. (15) that

$$y(n+1) = \begin{cases} g(y(n)) + h(x(n)), & b^k = 1, \\ g(y(n)) - h(x(n)), & b^k = -1. \end{cases} \tag{16}$$

So in- (anti)phase synchronization between the transmitter and the receiver is achieved after a transient when $b^k = 1$ (-1) if N is large enough. When the message sequence switches between $+1$ and -1, the communication system will switch between in- and antiphase synchronization accordingly. To decode the message from the received signal $s(n)$, it is required that $\mathrm{sgn}(h(-x)) = \mathrm{sgn}(h(x))$ so that $s(n)h(y(n)) = h^2(x(n)) \geqslant 0$ for $b_k = 1$, while $s(n)h(y(n)) = -h(x(n))h(-x(n)) \leqslant 0$ for $b^k = -1$ after the transient process. By computing the correlation function

$$C^{kN} = \sum_{n=1+(k-1)N}^{kN} s(n)h(y(n)), \tag{17}$$

the message is recovered correctly as

$$b_R^k = \begin{cases} -1, & C^{kN} < 0 \\ 1, & C^{kN} > 0. \end{cases} \tag{18}$$

In practice, the transmitted signal is inevitably contaminated with some external noise $e(n)$, and received as $r(n) = s(n) + e(n)$, which enters into the receiver to drive the response system. To recover the message in the presence of external noise, the correlation function between $r(n)$ and $h(y(n))$ is computed instead of that between $s(n)$ and $h(y(n))$ in Eq. (17).

We can evaluate the performance of the method by estimating the recovery error probability [6]

$$P_e = P(b_R^k \neq b^k). \tag{19}$$

It has been shown in Ref. [10] that although exact synchronization of the chaotic systems is destroyed by external noise, the encoded message may also be retrieved with very low recovery error probability. So the method is robust to external noise, and its robustness may be by far higher than other methods based on synchronization to transmit binary messages [3,4].

III. DIGITAL COMMUNICATION SYSTEM

To realize digital communication, the chaotic carrier signal $s(n)$ is digitized with a quantizer [9] which equally divides the amplitude range $(-A,A)$ of the chaotic carrier $s(n)$ into Q blocks, each with a length $\Delta = 2A/Q$, taking the medium value of the block where $s(n)$ is as the the digitized signal $s_Q(n)$. So $s_Q(n)$ takes a value from the set $\{\Delta(2k+1-Q)/2,\ k = 0,1,2,\ldots,Q-1\}$.

With a proper code $(d_{L-1}(n), \ldots, d_1(n), d_0(n))$ $(d_i \in \{0,1\})$, $s_Q(n)$ is sent to the receiver, and is restored to drive the response system in the receiver. The communication system can be written as

$$\begin{gathered} x(n+1) = g(x(n)) + h(x(n)), \\ s(n) = b^k h(x(n)), \\ s(n) \to s_Q(n), \\ s_Q(n) \to (d_{L-1}(n), \ldots, d_1(n), d_0(n)) \quad \text{transmitter}, \end{gathered} \tag{20}$$

$$\begin{gathered} (d_{L-1}(n), \ldots, d_1(n), d_0(n)) \to s_Q(n), \\ y(n+1) = g(y(n)) + s_Q(n), \quad \text{receiver}. \end{gathered} \tag{21}$$

With the above quantization, we have $|\zeta|=|s_Q(n)-s(n)|\leqslant\Delta/2=A/Q$. Let us examine the in-phase synchronization error $e_{\rm in}(n)=\|y(n)-x(n)\|$ ($b^k=1$) in the noise-free case. It is seen from Eqs. (20) and (21) that

$$\begin{aligned}e_{\rm in}(n+1)&=\|y(n+1)-x(n+1)\|\\&=\|g(y(n))-g(x(n))+s_Q(n)-s(n)\|\\&\leqslant\|g(y(n))-g(x(n))\|+|s_Q(n)-s(n)|\\&\leqslant\alpha_g e_{\rm in}(n)+\frac{\Delta}{2},\end{aligned}\tag{22}$$

from which we obtain

$$e_{\rm in}(n)\leqslant\frac{\Delta}{2(1-\alpha_g)}=\frac{A}{Q(1-\alpha_g)}\tag{23}$$

for $n\to\infty$. Similarly, the antiphase synchronization error $e_{\rm an}(n)=\|x(n)+y(n)\|$ ($b^k=-1$) has

$$e_{\rm an}(n)\leqslant\frac{\Delta}{2(1-\alpha_g)}=\frac{A}{Q(1-\alpha_g)}\tag{24}$$

for $n\to\infty$.

The limited synchronization errors will bring limited perturbations to the correlation function which is now

$$C_Q^{kN}=\sum_{n=1+(k-1)N}^{kN}s_Q(n)h(y(n)).\tag{25}$$

A message bit b^k can be correctly decoded as long as C_Q^{kN} has the same sign as C^{kN}, the correlation function of the analog communication [Eq. (17)]. The validity of the digital communication will be demonstrated in Sec. IV with specific chaotic system, the Hénon map.

IV. SIMULATION OF THE METHOD

To show the validity of the method, we consider the Hénon map

$$\begin{aligned}x_1(n+1)&=1.2-x_1^2(n)+x_2(n),\\x_2(n+1)&=0.3x_1(n),\end{aligned}\tag{26}$$

which has a chaotic attractor A in $\mathbb{R}^2$. We partition the system as follows:

$$\begin{aligned}g(x_1,x_2)&=\begin{pmatrix}0&0.9\\0.3&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix},\\h(x_1,x_2)&=\begin{pmatrix}-x_1^2+0.1x_2+1.2\\0\end{pmatrix}.\end{aligned}\tag{27}$$

It is evident that

$$\|g(x)\pm g(y)\|\leqslant0.9\|x\pm y\|\tag{28}$$

for any $x,y\in\mathbb{R}^2$. $h(x(n))=0.1x_2(n)-x_1^2(n)+1.2$ is now a scalar chaotic sequence within $(-1.25,\ 1.25)$, i.e., $A=1.25$. All requirements are met.

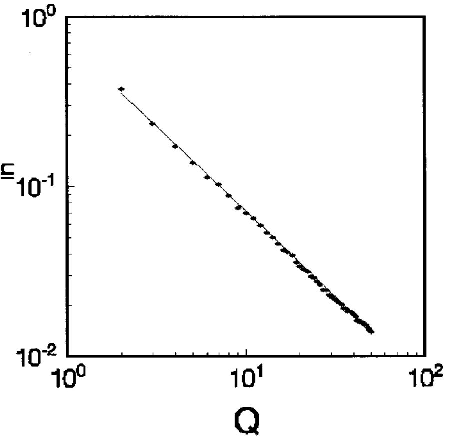

FIG. 1. Average value of the synchronization difference $\|y(n)-x(n)\|$ as a function of Q.

First, we examine the synchronization error resulting from the digitized driving signal $s_Q(n)$. With a large N, e.g., $N=5000$, the average value $\overline{e}_{\rm in}$ of the error $\|y(n)-x(n)\|$ ($b^k=1$) is estimated for different Q, as plotted in Fig. 1. The plot can be fitted as $\overline{e}_{\rm in}=0.71/Q$. The average value $\overline{e}_{\rm an}$ of the antiphase synchronization error $\|y(n)+x(n)\|$ follows the same law as $\overline{e}_{\rm in}$.

Next, we study the effect of the quantization of the chaotic carrier on the correlation function C_Q^{kN}. $(1/N)C_Q^{kN}$ is calculated as a function of Q with $N=5000$ and is shown in Fig. 2. As can be seen in this figure that, with the increase of Q, C_Q^{kN} comes to C^{kN} quickly, and C_Q^{kN} keeps the same sign as C^{kN} for both $b^k=1$ and $b^k=-1$ for all the $Q\geqslant2$, indicating that the message sequence can be decoded without error when N is rather large.

In practice, however, much smaller N, for example $N=25$, may be more desirable in communication. In such a case, the correlation function has large fluctuations and it is possible that $\mathrm{sgn}(C_Q^{kN})=-\mathrm{sgn}(C^{kN})$ for some b^k, resulting in recovery errors of the message. To examine it, we estimate the recovery error probability P_e with respect to Q in the

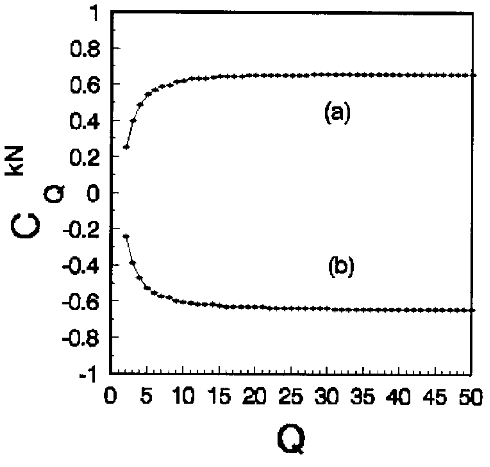

FIG. 2. The normalized correlation function $(1/N)C_Q^{kN}$ with respect to Q. $N=5000$ is used in the calculation. (a) $b^k=1$, (b) $b^k=-1$.

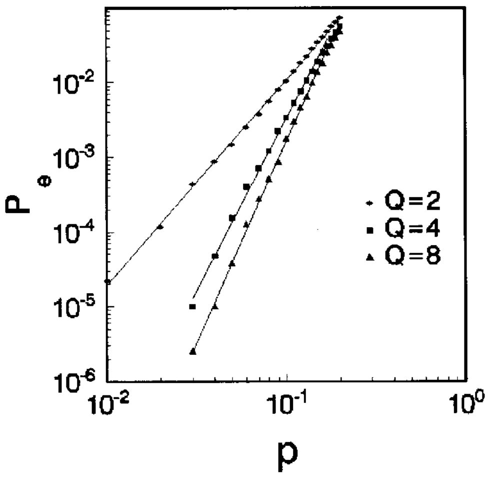

FIG. 3. The recovery error probability P_e as a function of the transmission error probability p for $Q=2$, 4, and 8.

noise-free case, using a random message sequence up to $K=4.5\times10^5$ bits for each Q. No error is detected for all the $Q\geqslant2$.

The above discussion is based on the fact that there is no noise in the transmission channel, and the digitized driving signal $s'_Q(n)$ restored at the receiver is the same as $s_Q(n)$. In practice, the channel noise is unavoidable. An advantage of digital communication over analog communication is that the digital sequence $(d_{L-1}(n),\ldots,d_1(n),d_0(n))$ of $s_Q(n)$ is discernible in the noise environment, provided that the noise level is not too high. However, errors may occur at some position, depending on the nature of the external noise as well as the transmitted signal. For the simplicity of the discussion, we assume in this paper that errors occur with an equal probability p in each position and independently in different positions. Most digital communication systems have some error-detecting and correcting scheme which, however, may not be able to correct all the errors. We will not consider such a scheme here. Without considering the error-correcting process, the driving signal $s'_Q(n)$ restored from a digital sequence containing errors is not the same as the original $s_Q(n)$, but has a difference $\xi(n)=s'_Q-s_Q(n)$. Driven by $s'_Q(n)$, the receiver may recover the message with errors.

In the following, we examine the performance of the digital system in the presence of channel noise, which results in an error probability p during transmission. For the convenience of simulation, we consider the cases $Q=2^L$. In such a case, each of the Q digitized values $\Delta(2k+1-Q)/2$ $(k=0,1,2,\ldots,Q-1)$ is represented by the corresponding digital code of k, namely, $\Sigma_{i=0}^{L-1}d_i2^i=k$. If an error occurs at position i, $d_i=0$ is received as 1 or 1 as 0.

The recovery error probability P_e of the message is estimated with respect to p, using a random message sequence up to $K=4.5\times10^5$ bits [totally LKN bits of $d_i(n)$ are transmitted] in each simulation. The results for $Q=2$, 4, and 8 in the region $p=0-0.2$ are shown in Fig. 3. No recovery error $(P_e=0)$ is detected with the above message sequence when $p\leqslant0.02$ for $Q=4$ and 8. The system is very robust to transmission errors. For example, when p is as large as 0.1, the recovery error probability is only 1.74×10^{-3} for $Q=8$. The plots can be approximately fitted with

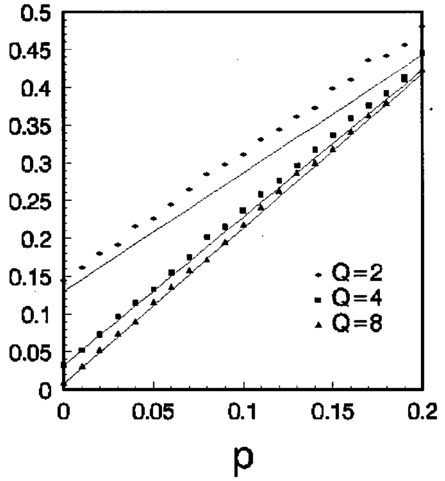

FIG. 4. The mean-square value $\overline{\varepsilon^2}$ as a function of p. The solid lines are the analytical results of Eq. (30).

$$P_e=\sigma p^\tau. \tag{29}$$

The constants σ and τ are estimated, giving $\sigma=6.09$ and $\tau=2.75$ for $Q=2$, $\sigma=127.33$ and $\tau=4.59$ for $Q=4$, and $\sigma=402.69$ and $\tau=5.39$ for $Q=8$.

Noting that the probability of $\xi(n)=s'_Q(n)-s_Q(n)\neq0$ is $1-(1-p)^L$, which is approximately Lp when p is small, so it seems that the larger the Q $(Q=2^L)$ is, the worse the performance of the system would be. However, the above results have shown that the performance is better with larger Q. To investigate into the reason, let us examine the distribution of the difference $\xi(n)$. $\xi(n)$ takes values from the set $\{\Delta k,\ k=-(Q-1),-(Q-1)+1,\ldots,Q-1\}$. When p is small, it is very rare that two or more than two errors occur in the L positions of the sequence $(d_{L-1}(n),\ldots,d_1(n),d_0(n))$ of $s_Q(n)$. If neglecting the cases of two or more than two errors in the L positions, then $\xi(n)$ will take values $\pm\Delta2^i$ $(i=0,1,\ldots,L-1)$, resulting from a single error in the position $d_i(n)$ only, with the probability p. For the simplicity of discussion, we also assume that $s(n)$ is uniformly distributed in $(-A,A)$, so that $\zeta(n)=s_Q(n)-s(n)$ is uniformly distributed in $(-\Delta/2,\Delta/2)$ and independent of $\xi(n)$. So digital communication begets a total deviation $\varepsilon(n)=\xi(n)+\zeta(n)$ to the analog driving signal $s(n)$. $\varepsilon(n)$ is a random number in the region $[-A(2-1/Q),A(2-1/Q)]$, with mean value 0. Let us look into the mean square value of $\varepsilon(n)$,

$$\begin{aligned}\overline{\varepsilon^2}=\overline{\xi^2}+\overline{\zeta^2}&=\frac{\Delta^2}{12}+p\Delta^2\sum_{i=0}^{L-1}(2^i)^2\\&=\frac{\Delta^2}{12}+p\Delta^2\,\frac{(4^L-1)}{3}=\frac{A^2}{Q^2}\left[\frac{1}{3}+p\,\frac{4(Q^2-1)}{3}\right].\end{aligned}\tag{30}$$

$\overline{\varepsilon^2}$ decreases with the increasing of Q at fixed p, which may account for the better performance at larger Q. This analysis is supported by the simulation for estimating $\overline{\varepsilon^2}$. As seen in Fig. 4, the estimated $\overline{\varepsilon^2}$ (dots) is close to Eq. (30) for Q

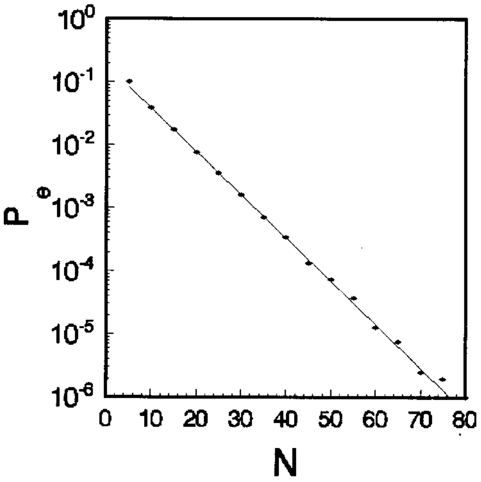

FIG. 5. P_e as a function of N for $Q=4$ and $p=0.1$.

$=4$ and 8. The difference at $Q=2$ may be due to the fact that, in the present system, $s(n)$ is not really symmetrical about 0 and uniformly distributed in $(-A,A)$.

The robustness of our communication system is due to the encoding method with which one should transmit LN bits of $d_i(n)$ to transmit a message bit b^k. One can expect that the system performs better with larger N. With $Q=4$ and $p=0.1$, we have examined $N=5-80$. As seen in Fig. 5, P_e follows an exponential law

$$P_e=0.184\exp(-0.158N). \qquad (31)$$

A similar exponential law holds for other Q and p. Noting that at $p=0.1$, in the case $Q=8$ and $N=25$, one needs to transmit $LN=75$ bits to transmit a message bit with $P_e=1.74\times10^{-3}$, while in the case $Q=4$ and $N=30$, $LN=60$ and $P_e=1.61\times10^{-3}$, so in a certain noise environment, a proper choice of Q and N may both enhance the efficiency (small LN) and robustness (small P_e) of the communication system.

With the above results, we conclude that digitizing the analog chaotic carrier for digital communication does not cause the system to fail to recover the message correctly; on the contrary, the message can be recovered with a very low error probability P_e, even though the transmission has a rather high error probability due to high noise level in the channel.

Let us look into the communication system in Ref. [9], where quantization of the carrier signal with length Δ leads to a synchronization difference not exceeding 4Δ, which enables the system to transmit digital information added to the digitized chaotic impulses, provided that the minimal distance $\Delta_{\rm inf}$ between the information digits is no less than $2(4\Delta)$. For the case $\Delta_{\rm inf}=2(4\Delta)$ and $Q=128=2^7$ in Ref. [9], if an error occurs in position $d_i(n)$ (only considering a single error in the L positions as in the above discussion) so that $|\xi(n)|=\Delta 2^i>2(4\Delta)$, i.e., $i>3$, then the synchronization difference must have exceeded the allowed amplitude 4Δ, and this information digit is recovered incorrectly. The recovery error probability P_e is at least $(L-4)p$, and increases with increasing Q, indicating that this system is sensitive to transmission errors. However, if the channel noise is not very high so that the error probability p is very low, this system can work reliably.

V. DISCUSSION

Secure communication using chaos may have promising practical applications in the future. For the purpose of implementation of this idea with modern communication technology, taking advantage of digital communication, it is important to investigate the possibility of digital communication in the field of secure communication using chaos, which now mainly focuses on analog communication.

Robustness of the methods to external noise is another important issue when considering practical application of the methods. Most methods based on chaotic synchronization to recover the information are sensitive to external noise, because external noise will destroy the exact synchronization and beget errors to the decoded information. Digital communication is robust to external noise, but transmission errors may also occur if the noise level is high in the channel. The recently proposed digital communication method [9] based on chaotic synchronization is sensitive to transmission errors.

We presented a method for digital communication, with binary symbols 1 and -1 being encoded with in-phase and antiphase chaotic synchronization between the transmitter and the receiver, respectively. Although quantization of the analog chaotic carrier destroyed the exact synchronization, the limited synchronization errors enable the receiver to recover the message correctly.

The present method is very robust to transmission errors. Thus it is suitable for communication in very noisy environments. On the other hand, the robust method can also be regard as an error-correcting scheme. The feasibility of the method enables it to be used for different aims concerning the efficiency or robustness of the communication by adjusting Q and N.

ACKNOWLEDGMENTS

This project was supported by the National Basic Research Project ‘‘Nonlinear Science’’ and the National Nature 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), and references therein.

[3] U. Parlitz, L. O. Chua, Lj. Kocarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992).

[4] H. Dedieu and M. Hasler, IEEE Trans. Circuits Syst. **40**, 634 (1993).

[5] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).

[6] U. Parlitz and S. Ergezinger, Phys. Lett. A **188**, 146 (1994).

[7] K. M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959 (1994).

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

[9] T. Stojanovski, L. Kocarev, and U. Parlitz, Phys. Rev. E **54**, 2128 (1996).

[10] C. S. Zhou and T. L. Chen, Phys. Lett. A **225**, 60 (1997).

[11] T. Ushio, Phys. Lett. A **198**, 14 (1995).