Multichannel digital communications by the synchronization of globally coupled chaotic systems

K. Yoshimura*

NTT Communication Science Laboratories 2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan

(Received 11 November 1998)

A multichannel digital communication method using the synchronization of globally coupled chaotic systems is proposed. The proposed method allows several binary messages to be transmitted simultaneously by just one transmitted chaotic signal, provided that outputs of different units are uncorrelated. We demonstrate the communication method on a model system consisting of Lorenz-like units. We also show how to systematically construct high-dimensional synchronizing units, based on the idea of cascaded systems. Furthermore, the dynamics of the coupled chaotic systems is discussed with particular attention paid to the correlation between the motions of different units. $[S1063-651X(99)15408-4]$

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

I. INTRODUCTION

The synchronization of coupled chaotic systems was first shown to be possible more than ten years ago in the pioneering work of Fujisaka and Yamada $[1]$. In 1990, the seminal paper of Pecora and Carroll [2] demonstrated that unidirectionally coupled chaotic systems, so-called master-slave systems, can also be synchronized. Since their ground-breaking work, researchers have come to realize the potential application of chaotic synchronization to secure communications.

This topic has received a great deal of attention recently. A number of communication schemes using chaos synchronization have been proposed and some of them have been implemented by electronic circuits: chaotic signal masking [3], communications based on active-passive decomposition [4,5], communications by parameter estimation [5,6], digital communications by single parameter switching in a chaotic transmitter $[7]$, and digital communications based on inphase and antiphase synchronization $\lceil 8 \rceil$. The above investigations, however, focused mainly on low-dimensional chaotic systems. Yet, as is well known, the low-dimensionality of attractors is the origin of weaknesses for security; since a low-dimensional attractor has a rather simple geometric structure, its description in terms of various measures is possible and can be used by an intruder to find the hidden messages.

In fact, some of the above chaotic communication schemes have already been broken. The chaotic signal masking was broken by a cryptanalytic attack using the return map $[9]$. In the parameter switching communication scheme it was shown that the two attractors corresponding to the two different parameter values (i.e., "one" and "zero") can be distinguished by observing some statistical quantity of the transmitted signal and, consequently, the retrieval of the encoded binary messages is possible $[10]$.

One way to cope with the problem of weak security is to use high-dimensional chaotic systems for the transmitter and the receiver. The use of high-dimensional chaotic systems increases security; these systems will make it more difficult to describe the attractor's structure and attack the communications; it will also be difficult to imitate the key parameters. The synchronization of high-dimensional chaotic systems has already been shown to be possible $[4,11]$. Several chaotic communication schemes using high-dimensional chaotic systems have been proposed $[12–14]$. Recently, the implementation of a synchronizing high-dimensional chaotic system using optoelectronic systems has also been demonstrated $[15,16]$.

In this paper, we investigate the possibility of multichannel communications based on high-dimensional chaos. In addition to an increase in the security, the communication efficiency can be enhanced because a large number of information signals can be transmitted simultaneously. The communication schemes proposed in $[12,13]$ have also achieved chaos-based multichannel communications using the synchronization of one-way coupled maps and globally coupled maps, respectively. These communication schemes need to transmit two signals: one for synchronizing the receiver system to the transmitter system and the other, an information-bearing signal. However, the proposed chaosbased multichannel communications can be achieved by transmitting just one signal. The scheme uses the synchronization of globally coupled chaotic systems.

The globally coupled chaotic systems used in our communication scheme are required to have a property that enables the output signals from different units to be uncorrelated with each other, in order to achieve the multichannel communications. Different parameter values are assigned to each unit to make the globally coupled chaotic systems possess this property. We investigate the relationship between the parameter differences and the correlations among the output signals, and show that there are two different cases; in one case, the output signals rapidly become uncorrelated as the parameter differences increase, and in the other case, the output signals remain highly correlated even for large parameter differences. We then discuss the reason why the two different cases occur from the viewpoint of the generalized synchronization between the units.

The present paper is organized as follows. In Sec. II we show the construction of the synchronizing globally coupled systems. In Sec. III we describe our communication scheme. In Sec. IV we present a model system to demonstrate our *Electronic address: kazuyuki@cslab.kecl.ntt.co.jp communication scheme and report results obtained from nu-

merical experiments. We also discuss the correlations among output signals from the viewpoint of generalized synchronization. In Sec. V we describe a method to systematically construct high-dimensional synchronizing units, and conclusions are offered in Sec. VI.

II. CONSTRUCTION OF SYNCHRONIZING GLOBALLY COUPLED SYSTEMS

In this section, the basic concept of synchronization by active-passive decomposition is introduced and synchronizing globally coupled systems are constructed.

A. Synchronizing systems by active-passive decomposition

Consider an arbitrary *n*-dimensional autonomous dynamical system

$$
\frac{dz}{dt} = F(z),\tag{1}
$$

where $z \in \mathbb{R}^n$. One can always formally rewrite an autonomous dynamical system of the form (1) into the nonautonomous system

$$
\frac{dx}{dt} = f(x, s(t)),\tag{2}
$$

where $x \in \mathbb{R}^n$ is the new state vector corresponding to *z* and $s(t)$ is some scalar function of time given by

$$
s(t) = h(x). \tag{3}
$$

It has been shown in $[4]$ that for a suitable choice of the function *h*, a copy of the above nonautonomous system that is driven by the same signal $s(t)$,

$$
\frac{dx'}{dt} = f(x', s(t)),\tag{4}
$$

synchronizes with drive system (2) for any initial conditions $x(0)$ and $x'(0)$, i.e., $||x-x'|| \to 0$ for $t \to \infty$. The synchronization of the pair of drive system (2) and response system (4) occurs if the equation describing the time evolution of the difference $e = x' - x$,

$$
\frac{de}{dt} = f(x', s) - f(x, s) = f(x + e, s(t)) - f(x, s),
$$
 (5)

possesses a global asymptotically stable fixed point at the origin $e=0$. In general, this has to be checked by numerically integrating Eq. (5). In some cases, however, this can be proven by using a Lyapunov function. In the synchronizing case, system (2) tends to the origin when it is not driven, $s(t) = 0$. Therefore, the decomposition given by *f* and *h* is called an *active-passive decomposition* (APD) [4].

Example. The Lorenz system; as an example for synchronizing systems by APD, we consider the Lorenz systems

$$
\frac{dx}{dt} = -\sigma(x - s),
$$

$$
\frac{dy}{dt} = \rho x - y - xz,
$$

$$
\frac{dz}{dt} = xy - \beta z,
$$
 (6)

with $s = y$ for the drive system and

$$
\frac{dx'}{dt} = -\sigma(x'-s),
$$

\n
$$
\frac{dy'}{dt} = \rho x' - y' - x'z',
$$
\n(7)
\n
$$
\frac{dz'}{dt} = x'y' - \beta z',
$$

for the response system. Though these coupled Lorenz systems can be rigorously proven to synchronize for any initial conditions; here, we describe a rough proof given in $[4]$. Subtracting the first equation of Eqs. (6) from that of Eqs. (7), the equation for the difference $e_x = x' - x$ becomes e_x $= -\sigma e_x$. Therefore, the difference e_x converges to zero. If $e_x=0$ is assumed, the equations describing the time evolutions of the other two differences $e_y = y' - y$ and $e_z = z' - z$ can be written in the limit $t \rightarrow \infty$ as

$$
\frac{de_y}{dt} = -e_y - xe_z,
$$

\n
$$
\frac{de_z}{dt} = xe_y - \beta e_z.
$$
\n(8)

The function

$$
L_1 = \frac{1}{2} (e_y^2 + e_z^2) \tag{9}
$$

can be used as a Lyapunov function for Eq. (8) . The time derivative of L_1 is

$$
\frac{dL_1}{dt} = -(e_y^2 + \beta e_z^2) \le 0.
$$
 (10)

This means that e_y and e_z converge to zero and, therefore, that the coupled Lorenz systems (6) and (7) synchronize for any initial conditions. As seen in the above proof, it should be noted that the synchronization can be achieved for an arbitrary driving signal *s*(*t*).

B. Globally coupled systems

In this subsection, we construct synchronizing globally coupled chaotic systems whose units are the active-passive decomposed dynamical systems coupled by the function *s*(*t*).

We consider *N* dynamical systems

$$
\frac{dx_i}{dt} = f_i(\mathbf{x}_i, s(t)), \quad i = 1, 2, \dots, N,
$$
\n(11)

FIG. 1. An illustration of globally coupled drive systems and response systems.

where $x_i \in \mathbb{R}^n$ and $s(t) \in \mathbb{R}$. These unit systems are globally coupled by the function

$$
s(t) = h(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N), \tag{12}
$$

and used for the drive systems. The function $s(t)$ is used as the driving signal and the response systems are

$$
\frac{dx'_i}{dt} = f_i(x'_i, s(t)), \quad i = 1, 2, ..., N.
$$
 (13)

We place the following assumption on each unit.

Assumption 1. Every *i*th unit $\dot{x}_i = f_i(x_i, s(t))$ and its copy $\dot{x}'_i = f_i(x'_i, s(t))$ synchronize for any driving signal $s(t)$ and any initial conditions $\mathbf{x}_i(0)$ and $\mathbf{x}'_i(0)$, i.e., for any $s(t)$ and any initial conditions, $\|\mathbf{x}_i - \mathbf{x}'_i\| \to 0$ for $t \to \infty$.

It is evident that all of the response units (13) synchronize with the corresponding drive units (11) via the driving signal (12) if the above assumption is satisfied. A schematic illustration for the globally coupled drive systems and the response systems is presented in Fig. 1.

III. ENCODING BINARY MESSAGES

In the following, we describe a communication method that makes it possible to transmit several binary messages simultaneously by just one transmitted signal, by utilizing the synchronizing globally coupled chaotic systems constructed in the previous section.

As the transmitter system, we use the globally coupled systems (11) constructed in the previous section,

$$
\frac{dx_i}{dt} = f_i(x_i, s(t)), \quad i = 1, 2, \ldots, N,
$$

with a particular choice of *h* of the form

$$
s(t) = \sum_{i=1}^{N} a_i \phi(\mathbf{x}_i),
$$
 (14)

where a_i , $i=1,2,\ldots,N$ are coefficients and $\phi: \mathbf{R}^n \to \mathbf{R}$ is a scalar function. Binary messages $b_i \in \{-1,1\}, i=1,2,\ldots,N$ are encoded into the coefficients a_i in the manner

$$
a_i = a_{i,0} + b_i \delta,\tag{15}
$$

where $a_{i,0}$, $i=1,2,\ldots,N$ are constants and δ is a small positive constant. The signal $s(t)$ is transmitted to the receiver units of the form (13) . It should be noted that $s(t)$ is used not only for transmitting *N* binary messages simultaneously but also for synchronizing the receiver units with the transmitter units. Here we make a crucial assumption to the globally coupled systems.

Assumption 2. Correlations between different units are sufficiently small, i.e.,

$$
|\langle \phi_i, \phi_j \rangle| = \left| \frac{1}{T} \int_0^T \phi_i(t) \phi_j(t) dt \right| \ll 1 \quad \text{for} \quad i \neq j, \tag{16}
$$

where $\phi_i(t)$ stands for $\phi(x_i(t))$ and *T* is some time interval.

If the above assumption is satisfied, the binary messages can be recovered by the following procedure. We denote $\phi(\mathbf{x}_i')$ by ϕ'_i , which is calculated at the receiver systems. If we calculate the correlation between *s* and ϕ'_{k} we obtain the equality

$$
\langle s, \phi'_k \rangle = \sum_{i=1}^N (a_{i,0} + b_i \delta) \langle \phi_i, \phi'_k \rangle \tag{17}
$$

from Eq. (14). The functions ϕ_i can be replaced by ϕ'_i because the receiver systems synchronize with the transmitter. If knowledge about f_i is unavailable, it is not possible to reproduce the functions ϕ_i at the receiver and, therefore, it is not possible to recover the messages by the following procedure. Replacing ϕ_i by ϕ'_i and solving Eq. (17) with respect to $b_k \delta$, we obtain

$$
b_k \delta = \frac{1}{\langle \phi'_k, \phi'_k \rangle} \left(\langle s, \phi'_k \rangle - \sum_{i=1}^N a_{i,0} \langle \phi'_i, \phi'_k \rangle - \sum_{i \neq k} b_i \delta \langle \phi'_i, \phi'_k \rangle \right). \tag{18}
$$

The last term in the right hand side cannot be estimated at the receiver systems since the messages b_i are unknown. Because of assumption 2, however, the last term may be neglected and the equality

$$
b_k \delta \approx \frac{1}{\langle \phi'_k, \phi'_k \rangle} \left(\langle s, \phi'_k \rangle - \sum_{i=1}^N a_{i,0} \langle \phi'_i, \phi'_k \rangle \right) \tag{19}
$$

approximately holds.

If all of the cross correlations are equal to zero, terms except $i = k$ in the sum on the right hand side of Eq. (19) can also be neglected. However, as they are small but not zero, we retain these terms to estimate the original messages as accurately as possible. The right hand side (rhs) of Eq. (19) can be calculated at the receiver systems and the binary message b_k is recovered as

$$
b_k = \begin{cases} 1 & \text{if } \text{rhs} > 0, \\ -1 & \text{if } \text{rhs} < 0. \end{cases} \tag{20}
$$

A sufficient condition for recovering the messages without error is given by

$$
\sum_{i \neq k} \left| \frac{\langle \phi_i, \phi_k \rangle}{\langle \phi_k, \phi_k \rangle} \right| < 1 \quad \text{for} \quad k = 1, 2, \dots, N. \tag{21}
$$

In fact, Eq. (18) is rewritten as

$$
b_k \delta \left(1 + \sum_{i \neq k} \frac{b_i \langle \phi'_i, \phi'_k \rangle}{b_k \langle \phi'_k, \phi'_k \rangle} \right)
$$

=
$$
\frac{1}{\langle \phi'_k, \phi'_k \rangle} \left(\langle s, \phi'_k \rangle - \sum_{i=1}^N a_{i,0} \langle \phi'_i, \phi'_k \rangle \right).
$$
 (22)

It can be easily seen that the total sum inside the parentheses on the left hand side is positive when condition (21) is satisfied. Therefore, the sign of the right hand side, which is estimated at the receiver systems, is equal to that of b_k . This means that the original binary messages are recovered without error at the receiver.

IV. EXAMPLE OF A COMMUNICATION SYSTEM

We present a model system consisting of Lorenz-like units, able to satisfy assumptions 1 and 2, to demonstrate the communication method proposed in the previous section. We will show results obtained from numerical experiments for the transmission of messages on the model. It is crucially important for our communication method to satisfy assumption 2. Therefore, we will also investigate the relationship between the parameter differences and the cross correlations of the output signals from different units.

A. Globally coupled Lorenz-like systems

We couple the *N* Lorenz-like units

$$
\frac{dx_i}{dt} = -\sigma_i(x_i - \gamma s),
$$

\n
$$
\frac{dy_i}{dt} = \rho_i x_i - \mu_i y_i - \nu_i x_i z_i,
$$
\n(23)

$$
\frac{d z_i}{dt} = \nu_i x_i y_i - \beta_i z_i,
$$

with the coupling function

$$
s = \sum_{i=1}^{N} (a_{i,0} + b_i \delta) y_i,
$$
 (24)

where γ , σ_i , ρ_i , μ_i , ν_i , and β_i are positive parameters for the transmitter. To make the dynamics of different units uncorrelated, we assign different parameter values to each unit. The units in the receiver are

FIG. 2. Transmitted signal *s*(*t*).

$$
\frac{dx'_i}{dt} = -\sigma_i(x'_i - \gamma s),
$$

\n
$$
\frac{dy'_i}{dt} = \rho_i x'_i - \mu_i y'_i - \nu_i x'_i z'_i,
$$

\n
$$
\frac{dz'_i}{dt} = \nu_i x'_i y'_i - \beta_i z'_i.
$$
\n(25)

The synchronization of every pair of corresponding units can be easily proven in the same way as describe in Sec. II. As for assumption 2, we will show by numerical integration that it can be satisfied when the parameter differences are introduced appropriately. Besides assumptions 1 and 2, it is also required for the transmitter dynamical system that its attractor be bounded. This is guaranteed for the present model [Eqs. (23) and (24)] by the following proposition.

Proposition 1. Let $h: \mathbb{R}^{2N} \to \mathbb{R}$ be a continuous function of $y_1, \ldots, y_N, z_1, \ldots, z_N$. If $s = h(y_1, \ldots, y_N, z_1, \ldots, z_N)$ then there is a region $D \subset \mathbb{R}^{3N}$ such that every trajectory of the coupled dynamical system (23) enters *D* and never leaves it thereafter (see Appendix A).

B. Numerical Experiments

We show the results of numerical experiments on the transmitter-receiver systems [Eqs. (23) – (25)] to demonstrate our communication method. Numerical integration of the equations was carried out by the fourth-order Runge-Kutta scheme. We set $N=2$ for simplicity of the analysis (given in the next subsection). The other parameter values are as follows: $\gamma = 2.0$, $\beta_1 = \beta_2 = 8/3$, $\sigma_1 = 10.0$, $\sigma_2 = 14.0$, ρ_1 = 30.0, ρ_2 = 26.0, μ_1 = 1.0, μ_2 = 0.75, ν_1 = 1.0, ν_2 = 1.25, $a_{1,0} = a_{2,0} = 1.0$, and $\delta = 0.1$. The time interval *T* for transmitting a single set of binary messages is set as $T=5$.

The signal $s(t)$ is plotted against time t in Fig. 2 and it appears to be chaotic. The encoded binary message sequences are shown in Fig. $3(a)$, where the horizontal axis represents the time, each row corresponds to each channel *i* $=$ 1 or 2, and the filled and open cells represent the binary messages $+1$ and -1 , respectively. The binary message sequences recovered at the receiver are shown in Fig. $3(b)$. It can be seen that the first pair of bits in the sequences is not recovered correctly because the synchronization is still not

FIG. 3. Numerical simulation of a communication method with two channels. (a) Original binary messages. (b) Recovered binary messages. FIG. 4. Cross correlation versus parameter Δ : (i) solid line, (ii)

achieved. However, the other binary messages are perfectly recovered.

C. Correlation and parameter differences

In our communication method, assumption 2, which requires the dynamics of different units to be uncorrelated, is crucially important. Therefore, we investigate how the cross correlation decreases as the parameter differences increase.

We consider coupled Lorenz-like systems (23) of $N=2$ with $a_{1,0} = a_{2,0} = 1.0$ and no encoded messages, i.e., $s = y_1$ $+y_2$. The normalized cross correlation is defined by

$$
C_{12} \equiv \frac{\langle y_1, y_2 \rangle}{\sqrt{\langle y_1, y_1 \rangle \langle y_2, y_2 \rangle}},
$$
\n(26)

where the time average in each correlation is taken over the period $T=120$. We fix the parameters of the first unit except γ as $\beta_1=8/3$, $\sigma_1=10.0$, $\rho_1=30.0$, $\mu_1=1.0$, and $\nu_1=1.0$. Different parameter values are assigned to the second according to the following three cases: (i) four parameters are different ($\sigma_2 = \sigma_1 + \Delta$, $\rho_2 = \rho_1 - \Delta$, $\mu_2 = \mu_1 - 0.0625\Delta$, ν_2 $= v_1 + 0.0625\Delta$) and the coupling parameter is $\gamma = 2.0$, (ii) two parameters are different $(\sigma_2 = \sigma_1 + \Delta, \ \rho_2 = \rho_1 - \Delta)$ and $\gamma=0.5$, and (iii) only one parameter is different ($\rho_2=\rho_1$ $(-\Delta)$ and $\gamma=2.0$, where Δ is a parameter that controls the extent of the parameter differences.

Figure 4 displays the normalized cross correlation C_{12} plotted as a function of Δ for the above three cases. The cross correlation rapidly decreases in case (i) as Δ increases. In contrast to this, the two units are highly correlated and C_{12} remains at unity or only slightly decreases with increasing Δ in the other cases (ii) and (iii).

What is a difference in the dynamics between the highly correlating cases and the uncorrelating case? We now proceed to investigate what kind of phenomenon causes the highly correlated motions. It is conceivable that generalized synchronization (GS) occurs between the two units. GS was studied for unidirectionally coupled (master-slave) systems in $[17–19]$ and also for mutually coupled systems, like our systems, in [20]. A definition of GS can be given as follows.

Definition. Let $x_1, x_2 \in \mathbb{R}^n$ be state variables of a pair of dynamical systems $\dot{x}_1 = g_1(x_1, x_2)$ and $\dot{x}_2 = g_2(x_1, x_2)$. The

dashed line, and (iii) dashed-dotted line.

systems x_1 and x_2 are said to synchronize in a generalized sense if there exists an invertible map $\psi: \mathbb{R}^n \to \mathbb{R}^n$, a manifold $M = \{ (x_1, x_2) | x_2 = \psi(x_1) \}$, and a subset $B \subset \mathbb{R}^{2n}$ with $M \subset B$, such that all of the trajectories with initial conditions in basin *B* approach *M* as $t \rightarrow \infty$.

Roughly speaking, GS is said to occur if one state variable is uniquely determined by the other via the functional relation $x_2 = \psi(x_1)$ after the transient motions. The following proposition enables us to numerically examine whether such a functional relation exists between the state variables X_1 $=(x_1, y_1, z_1)$ and $X_2=(x_2, y_2, z_2)$, under the assumption that ψ is continuously differentiable (ψ and $\psi^{-1} \in C^1$).

Proposition 2. Let $x_1, x_2 \in \mathbb{R}^n$ be state variables of a pair of dynamical systems $\dot{x}_1 = g_1(x_1, x_2)$ and $\dot{x}_2 = g_2(x_1, x_2)$. The attractor Ω of these coupled systems is assumed to be bounded. If there is a function from the x_1 space to the x_2 space, such that $x_2 = \psi(x_1)$ for any points on Ω with ψ $\in C¹$, then the correlation dimension of Ω is equal to that of its projection $\Pi_1(\Omega)$ to the x_1 space (see Appendix B).

This proposition implies that there is no function from X_1 to X_2 $[X_2 = \psi(X_1)]$ with $\psi \in C^1$, if Ω and $\Pi_1(\Omega)$ do not have the same correlation dimensions, where $\Omega(\subset \mathbb{R}^3 \times \mathbb{R}^3)$ and $\Pi_1(\Omega)(\subset \mathbf{R}^3)$ stand for the attractor of the whole system and its projection to the phase space of the first unit, respectively.

We measure the correlation dimensions $D_2(\Omega)$ and $D_2(\Pi_1(\Omega))$. Figure 5 displays $D_2(\Omega)$ and $D_2(\Pi_1(\Omega))$ for cases (i)–(iii) as a function of Δ , where the thick and thin lines refer to $D_2(\Omega)$ and $D_2(\Pi_1(\Omega))$, respectively; the line type distinguishes the three cases as (i) solid line, (ii) dashed line, and (iii) dashed-dotted line. Some sharp decreases of the correlation dimensions correspond to the windows where stable periodic attractors emerge.

Apart from the window, both $D_2(\Omega)$ and $D_2(\Pi_1(\Omega))$ increase as Δ increases in case (i). They are apparently different and the difference also increases. In case (ii), $D_2(\Omega)$ slowly increases and saturates at about 2.5. The apparent difference between $D_2(\Omega)$ and $D_2(\Pi_1(\Omega))$ can also be found in this case. These results indicate that, for cases (i) and (ii), function $X_2 = \psi(X_1)$ does not exist in C^1 . (A function that is not continuously differentiable might exist; we

FIG. 5. Correlation dimensions of Ω and $\Pi_1(\Omega)$ plotted versus parameter Δ . Each thick line refers to $D_2(\Omega)$ and each thin line refers to $D_2(\Pi_1(\Omega))$. The line type distinguishes three cases: (i) solid line, (ii) dashed line, and (iii) dashed-dotted line.

cannot deny this possibility.) In both of the two cases, $D_2(\Pi_2(\Omega))$ was also different from $D_2(\Omega)$. This indicates that a function in the opposite direction $X_1 = \psi'(X_2)$ does not exist in C^1 .

In contrast to the previous cases, in case (iii), Ω and $\Pi_1(\Omega)$ have the same correlation dimensions for any Δ . This suggests the existence of a continuously differentiable and invertible map. In fact, we can find the continuously differentiable and invertible map ψ :(x_1, y_1, z_1) $\rightarrow (x_1, (\rho_2 / \rho_1) y_1, (\rho_2 / \rho_1) z_1)$ in this case: the second unit becomes identical to the first under the transformation X_2 $=\psi(X_1)$. This GS causes nondecreasing in the cross correlation as Δ increases in case (iii).

It is not still clear what kind of phenomenon occurs and causes the highly correlated motions in case (ii). On this point, it is conceivable that there persists a rough correspondence between the state variables X_1 and X_2 as the parameter differences increase, instead of an exact one-to-one correspondence.

Consider points (X_1, X_2) on the attractor Ω . As a functional relation does not exist, at least in $C¹$, if one state variable, X_1 or X_2 , is fixed, the other state variable is not uniquely determined; i.e., for a fixed state variable \tilde{X}_1 (or (X_2) , the set $W_1 = \{X_2 | X_1 = \tilde{X}_1, (X_1, X_2) \in \Omega\}$ (or W_2 $=\{X_1 | X_2 = \tilde{X}_2, (X_1, X_2) \in \Omega\}$ contains several points; W_1 and W_2 consist of a single point when GS occurs. We can find a ball U_1 (U_2) that covers W_1 (W_2) since Ω is bounded. Let $r_1(\tilde{\pmb{X}}_1)$ $[r_2(\tilde{\pmb{X}}_2)]$ be the infimum of the radius of such a ball and \overline{r}_1 (\overline{r}_2) be its average taken with respect to \widetilde{X}_1 (\widetilde{X}_2) over the attractor Ω . The averaged radii \overline{r}_1 and \overline{r}_2 can be regarded as parameters that express to what degree the correspondence between X_1 and X_2 is close to a one-to-one correspondence; the correspondence between X_1 and X_2 becomes close to one-to-one when \overline{r}_1 and \overline{r}_2 become small, and there is a one-to-one correspondence when $\bar{r}_1 = \bar{r}_2 = 0$. In terms of predictability, \overline{r}_1 (\overline{r}_2) gives an average error in predicting X_2 (X_1) from the knowledge of X_1 (X_2) only. The

FIG. 6. Parameter Θ plotted versus Δ : (i) solid line, (ii) dashed line, and (iii) dashed-dotted line.

averaged radii \bar{r}_1 and \bar{r}_2 may be useful to examine whether there persists a rough correspondence between X_1 and X_2 . However, it is impossible to numerically calculate them. Therefore, we define parameters similar to \overline{r}_1 and \overline{r}_2 as follows. Let $\{(X_1^{(i)}, X_2^{(i)})\}, i = 1, 2, ..., m$ be a time series obtained from the trajectory after the transient behavior. Using this time series, we define the parameters Θ_1 and Θ_2 as

$$
\Theta_{1,2} = \frac{1}{m} \sum_{i=1}^{m} \frac{H(\epsilon - \|X_{1,2}^{(j)} - X_{1,2}^{(i)}\|) \|X_{2,1}^{(j)} - \langle X_{2,1}^{(j)}\rangle_{i}\|}{\sum_{j=1}^{m} H(\epsilon - \|X_{1,2}^{(j)} - X_{1,2}^{(i)}\|)}.
$$
\n(27)

where *H* is the Heaviside function

$$
H(x) = \begin{cases} 0 & (x < 0), \\ 1 & (x \ge 0), \end{cases}
$$
 (28)

 ϵ is a small positive constant, and $\langle X_{2,1}^{(j)} \rangle_i$ is the average defined by

$$
\langle \mathbf{X}_{2,1}^{(j)} \rangle_i = \frac{\sum_{j=1}^m H(\epsilon - \|\mathbf{X}_{1,2}^{(j)} - \mathbf{X}_{1,2}^{(i)}\|) \mathbf{X}_{2,1}^{(j)}}{\sum_{j=1}^m H(\epsilon - \|\mathbf{X}_{1,2}^{(j)} - \mathbf{X}_{1,2}^{(i)}\|)}.
$$
(29)

We used the norm $\|\mathbf{X}_k\| = |x_k| + |y_k| + |z_k|$ for the convenience of computation. Parameters Θ_1 and Θ_2 measure to what precision a state variable can be determined when the other state variable is determined within the error ϵ .

We calculated the average $\Theta = (\Theta_1 + \Theta_2)/2$ as a function of Δ for cases (i)–(iii). Figure 6 displays the results. The quantity Θ steeply increases with increasing Δ except the point of the periodic window in (i), indicating that the correspondence between X_1 and X_2 comes to break down. In contrast, Θ is almost constant in (iii). This is consistent with the existence of GS. The result for case (ii) is interesting. The quantity Θ gradually increases as Δ increases up to 2.5, and then it saturates at a small value. This saturation of Θ means that, even for a large Δ , the correspondence between X_1 and X_2 persists to a certain degree. We therefore say that the systems are in a *near generalized synchronization* (NGS) state when there exists such a rough correspondence between the state variables. It may be concluded that NGS prevents decreases of the cross correlation in case (ii).

As shown in the above analysis, GS or NGS can occur in coupled systems used for transmitters. Each of them can make the dynamics of different units highly correlated. Therefore, GS and NGS are undesirable for the proposed communication method and should be avoided. We can avoid GS and NGS if we introduce sufficiently large parameter differences according to an appropriate manner, e.g., case (i), and subsequently our communication method can work well as demonstrated by numerical experiments. In this case, it was observed that the attractor of the coupled systems recovers the high dimensionality and the correlation becomes small. Apart from its relevancy in the communication method, NGS may be an interesting phenomenon. It may be worth studying whether NGS occurs in chaotic systems with other types of couplings, e.g., diffusive couplings.

V. CASCADED SYSTEMS

It is desirable to use a high-dimensional dynamical system for each unit in order to make the attacking more difficult. Moreover, the use of high-dimensional unit systems can be expected to lead to smaller cross correlations between different units, avoiding GS and NGS and, therefore, makes it possible to transmit a larger number of information signals simultaneously. A method that enables us to systematically construct a high-dimensional synchronizing system using low-dimensional building blocks has been proposed in $[4,5]$; the constructed high-dimensional system is called *cascaded systems*.

Connecting the building blocks in series, we can construct the *i*th units of the form

$$
\frac{d\mathbf{x}_{ij}}{dt} = f_{ij}(\mathbf{x}_{ij}, s_{ij}(t)), \quad i = 1, 2, ..., N, \quad j = 0, 1, ..., K,
$$
\n(30)

where

$$
s_{10} = \dots = s_{N0} = s = \sum_{i=1}^{N} a_i \phi(\mathbf{x}_{iK})
$$
 (31)

and s_{ii} ($j=1,\ldots,K$) is a function of x_{ii-1} given by

$$
s_{ij} = h_{ij}(\mathbf{x}_{ij-1}).\tag{32}
$$

A configuration of the *i*th unit is illustrated in Fig. 7. These *N* units are coupled by the function *s* and form the drive system. The signal *s* is transmitted to a response system which consists of the copies of these units

$$
\frac{d\mathbf{x}_{ij}'}{dt} = f_{ij}(\mathbf{x}_{ij}', s_{ij}'(t)),
$$
\n(33)

i th unit system S χ_{ik}

FIG. 7. An illustration of a scheme for constructing highdimensional unit systems.

$$
s'_{ij} = h_{ij}(\mathbf{x}'_{ij-1}), \quad j = 1, \dots, K. \tag{34}
$$

We assume that every pair of system x_{ij} and system x'_{ij} satisfies assumption 1, i.e., $\|\mathbf{x}_{ij} - \mathbf{x}'_{ij}\| \to 0$ for $t \to \infty$ if $s_{ij} = s'_{ij}$. Then, it is easy to see that all of the systems x_i synchronize with the corresponding systems x_{ij} one after another. Therefore, our communication method can be applied provided that assumption 2 is satisfied. Messages are encoded into the coefficients *ai* as well.

As an example, we consider the cascaded systems

$$
\frac{dx_i}{dt} = -\sigma_i(x_i - s),
$$

\n
$$
\frac{dy_i}{dt} = \rho_i x_i - \mu_i y_i - \nu_i x_i z_i,
$$
 (35)
\n
$$
\frac{dz_i}{dt} = \nu_i x_i y_i - \beta_i z_i,
$$

and

$$
\frac{du_i}{dt} = -u_i - \kappa_i v_i + s_{i1},
$$

\n
$$
\frac{dv_i}{dt} = \kappa_i u_i - \eta_i v_i^3,
$$
\n(36)

where s and s_{i1} are defined by

$$
s = \sum_{i=1}^{N} (a_{i,0} + b_i \delta) v_i,
$$
 (37)

and

$$
s_{i1} = y_i \sin(\omega_{yi} y_i) + z_i \sin(\omega_{zi} z_i)
$$
 (38)

and σ_i , ρ_i , μ_i , ν_i , β_i , κ_i , η_i , ω_{vi} , and ω_{zi} are positive parameters. The cascaded systems (35) and (36) and their copies can be shown to synchronize by using Lyapunov functions. Synchronization of the first system (35) with its copy is proven in the same way as described in Sec. II. Therefore, we can assume $s_{i1} = s'_{i1}$. If $s_{i1} = s'_{i1}$ is assumed, the equations governing the differences $e_{ui} = u'_i - u_i$ and e_{vi} $= v_i' - v_i$ are

$$
\frac{de_{ui}}{dt} = -e_{ui} - \kappa_i e_{vi},
$$

where $s'_{i0} = s$ and

FIG. 8. Transmitted signal *s*(*t*).

$$
\frac{de_{vi}}{dt} = \kappa_i e_{ui} - \eta_i e_{vi} (v_i^2 + v_i v_i' + v_i'^2).
$$
 (39)

Using the Lyapunov function

$$
L_2 = \frac{1}{2} (e_{ui}^2 + e_{vi}^2), \tag{40}
$$

we obtain

$$
\frac{dL_2}{dt} = -e_{ui}^2 - \frac{1}{2}e_{vi}^2\{v_i^2 + v_i'^2 + (v_i + v_i')^2\} \le 0.
$$
 (41)

This shows that the second system (36) and its copy synchronize with each other. It can also be shown that there exists a bounded region in \mathbb{R}^{5N} into which any trajectory eventually enters; we do not describe the proof here.

We show results obtained from numerical experiments on the cascaded systems (35) and (36) with a size $N=8$. For each *i*, the parameter values are randomly chosen in the following ranges: $\sigma_i \in [10,20], \ \rho_i \in [30,60], \ \mu_i \in [0.25,1], \ \nu_i$ $\epsilon[1,2], \quad \beta_i \in [8/3,17/3], \quad \kappa_i \in [3,12], \quad \eta_i \in [0.2,1], \quad \omega_{vi}$ $\in [0.5,4]$, $\omega_{zi} \in [0.25,1]$, and $a_{i,0} \in [0.5,1]$. The parameter δ is set to 0.1 and the time interval *T* for transmitting a single set of binary messages is set as $T=20$. The signal $s(t)$ is plotted against time *t* in Fig. 8 and it is apparently chaotic. The encoded binary message sequences are shown in Fig. $9(a)$ and the binary message sequences recovered at the receiver are shown in Fig. $9(b)$. The first column of the message sequences is not recovered correctly because the synchronization is still not achieved. The other binary messages are perfectly recovered. This numerical result shows that the simultaneous transmission of a large number of binary messages is possible by using high-dimensional unit systems.

VI. CONCLUSIONS

A multichannel digital communication method using the synchronization of globally coupled chaotic systems has been proposed. One of the advantages of the method is that several binary messages can be transmitted simultaneously by just one transmitted signal. We presented a model system consisting of Lorenz-like units and demonstrated our communication method by numerical experiments. Based on the

FIG. 9. Numerical simulation of a communication method with eight channels. (a) Original binary messages. (b) Recovered binary messages.

idea of cascaded systems, we also described a method that systematically constructs a high-dimensional synchronizing unit system. The use of high-dimensional unit systems may make communications more secure. In addition, it has been shown by numerical experiments on a model system that the simultaneous transmission of a larger number of binary messages is possible by using high-dimensional unit systems since the cross correlations between different units become smaller.

We investigated the dynamics of the coupled Lorenz-like systems with a size $N=2$, focusing our attention on the correlation of the dynamics of the two different units. It was shown that GS or NGS occurs under some parameter conditions and also that they lead to highly correlated motions, which are undesirable for the present communication method. However, it was also shown that GS and NGS can be avoided under appropriate choices of the parameter values and that our communication method can work well in turn. In this case, it was observed that the attractor of the coupled systems recovers the high dimensionality and the correlation becomes small.

ACKNOWLEDGMENT

The author would like to thank K. Arai for reading the manuscript and making a number of helpful suggestions.

APPENDIX A: PROOF OF PROPOSITION 1

Proof. Consider the Lyapunov function

$$
L = \sum_{i=1}^{N} \frac{1}{2} \left\{ y_i^2 + \left(z_i - \frac{\rho_i}{\nu_i} \right)^2 \right\}.
$$
 (A1)

The time derivative of *L* is

$$
\frac{dL}{dt} = \sum_{i=1}^{N} \left[-\left\{ \mu_i y_i^2 + \beta_i \left(z_i - \frac{\rho_i}{2 \nu_i} \right)^2 \right\} + \frac{\beta_i}{4} \left(\frac{\rho_i}{\nu_i} \right)^2 \right].
$$
\n(A2)

We define the region $D_0 = \{ (x,y,z) | L \geq -\epsilon_0, \epsilon_0 > 0 \} \subset \mathbb{R}^{3N}$, where $x=(x_1,\ldots,x_N),$ $y=(y_1,\ldots,y_N),$ and z $=(z_1, \ldots, z_N)$. The region D_0 is bounded with respect to the y and z coordinates from Eq. $(A2)$. Therefore, there exists the supremum of L in D_0 and we let C be the supremum. We define the region $D_1 = \{(x,y,z) | L \leq C + \epsilon_1, \epsilon_1 > 0 \} \subset \mathbb{R}^{3N}$, which is bounded with respect to the *y* and *z* coordinates from Eq. $(A1)$. Because of this definition, it holds that $D_0 \subset D_1$, and $\dot{L} \leq -\epsilon_0$ outside of D_1 . If an arbitrary trajectory $\Gamma(t)$ starts from a point outside of D_1 , then the value of *L* associated with points on the trajectory must decrease as time goes by and $\Gamma(t)$ will enter D_1 within a finite time T_1 . Furthermore, all of the trajectories pass inwards through the boundary ∂D_1 since $\dot{L} \leq -\epsilon_0$ on ∂D_1 . Therefore, the trajectory $\Gamma(t)$ once entering D_1 will stay inside D_1 for $t \ge T_1$.

There exists a constant *M* such that $|s|$ $=$ $|h(y_1, \ldots, y_N, z_1, \ldots, z_N)|$ $\leq M$ in D_1 because *h* is a continuous function of *y* and *z* and is therefore bounded in D_1 . If we formally integrate the first equation of Eqs. (23) , then we have

$$
x_i(t) = x_i(T_1)e^{-\sigma_i(t-T_1)} + \int_{T_1}^t e^{-\sigma_i(t-\tau)} \gamma \sigma_i s(\tau) d\tau.
$$
\n(A3)

Using the fact that $|s| < M$ for $t \ge T_1$ we have the inequality

$$
|x_i(t)| \le |x_i(T_1)|e^{-\sigma_i(t-T_1)} + \gamma \sigma_i M \int_{T_1}^t e^{-\sigma_i(t-\tau)} d\tau
$$

$$
\le |x_i(T_1)|e^{-\sigma_i(t-T_1)} + \gamma M.
$$
 (A4)

Since the first term on the right hand side decreases and goes to zero as time goes by, there exists $T_2(>T_1)$ such that for all *i*, $|x_i(t)| \leq 1 + \gamma M$ for $t \geq T_2$. If we define *D* $= D_1 \cap \{ (x,y,z) | |x_i| \leq 1 + \gamma M, i = 1,2,...,N \},$ then it holds that $\Gamma(t) \in D$ for $t \ge T_2$.

APPENDIX B: PROOF OF PROPOSITION 2

Proof. For simplicity, suppose the norm $\|\mathbf{x}\| = (\vert x_1 \vert)^q$ $+\cdots+|x_k|^q$ ^{1/*q*} in **R**^{*k*}, where *q* is a positive integer. Let

 $\{(x_1^{(i)}, x_2^{(i)})\}, i = 1, 2, \ldots, m$ be a time series obtained from the trajectory. The correlation dimension of Ω is defined by [21]

$$
D_2(\Omega) = \lim_{\epsilon \to 0} \frac{\log C(\epsilon)}{\log \epsilon},
$$
 (B1)

where the correlation integral $C(\epsilon)$ is defined by

$$
C(\epsilon) = \lim_{m \to \infty} \frac{1}{m^2} \sum_{i,j=1}^{m} H(\epsilon - \| (x_1^{(i)}, x_2^{(i)}) - (x_1^{(j)}, x_2^{(j)}) \|),
$$
\n(B2)

where *H* is the Heaviside function. The correlation dimension of $\Pi_1(\Omega)$ is defined in the same way through the correlation integral $C_1(\epsilon)$ calculated from the time series $\{x_1^{(i)}\}$.

The inequality $D_2(\Pi_1(\Omega)) \le D_2(\Omega)$ is trivial. Therefore we prove the opposite, $D_2(\Pi_1(\Omega)) \ge D_2(\Omega)$. Consider an arbitrary pair such that $||x_1^{(i)} - x_1^{(j)}|| \le \epsilon$. For such a pair, we have the inequality

$$
|| (x_1^{(i)}, x_2^{(i)}) - (x_1^{(j)}, x_2^{(j)})|| = || (x_1^{(i)}, \psi(x_1^{(i)})) - (x_1^{(j)}, \psi(x_1^{(j)}))||
$$

$$
\le ||x_1^{(i)} - x_1^{(j)}|| + ||\psi(x_1^{(i)}) - \psi(x_1^{(j)})||.
$$

Since Ω is assumed to be bounded and $\psi \in C^1$, there is a constant *K* such that $\|\psi(x_1^{(i)}) - \psi(x_1^{(j)})\| \le K \|x_1^{(i)} - x_1^{(j)}\|$. Then we have

$$
\| (x_1^{(i)}, x_2^{(i)}) - (x_1^{(j)}, x_2^{(j)}) \| \le (1 + K) \epsilon \equiv \tilde{\epsilon}.
$$
 (B3)

From the inequality $(B3)$, we have

$$
\log C_1(\epsilon) \le \log C(\tilde{\epsilon}).\tag{B4}
$$

If we divide both sides by $\log \epsilon$ (<0) and take the limit ϵ \rightarrow 0, we obtain

$$
\lim_{\epsilon \to 0} \frac{\log C_1(\epsilon)}{\log \epsilon} \ge \lim_{\epsilon \to 0} \frac{\log C(\tilde{\epsilon})}{\log \epsilon} = \lim_{\tilde{\epsilon} \to 0} \frac{\log C(\tilde{\epsilon})}{\log \tilde{\epsilon}}.
$$
 (B5)

This shows that $D_2(\Pi_1(\Omega)) \ge D_2(\Omega)$. Hence, we have $D_2(\Pi_1(\Omega))=D_2(\Omega)$.

- [1] H. Fujisaka and T. Yamada, Prog. Theor. Phys. **69**, 32 (1983).
- [2] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 $(1990).$
- [3] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 $(1993).$
- [4] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
- [5] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E 53, 4351 (1996).
- [6] N. Sharma and P. G. Poonacha, Phys. Rev. E **56**, 1242 (1997).
- [7] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang,

Int. J. Bifurcation Chaos Appl. Sci. Eng. 2, 973 (1992).

- [8] T. Ushio, T. Innami, and S. Kodama, IEICE Trans. Fundamentals Electron. Commun. Comput. Sci. **E-79A**, 1689 (1996).
- [9] G. Pérez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 $(1995).$
- [10] T. Yang, Int. J. Circuit Theory Applications 23, 611 (1995).
- [11] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, Phys. Rev. Lett. 76, 904 (1996).
- @12# J. H. Xiao, G. Hu, and Z. Qu, Phys. Rev. Lett. **77**, 4162 $(1996).$
- [13] N. Oketani and T. Ushio, IEICE Trans. (in Japanese) **J-79A**, 1427 (1996).
- [14] U. Parlitz, L. Kocarev, T. Stojanovski, and L. Junge, Physica D 109, 139 (1997).
- @15# J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).
- [16] L. Larger, J. P. Goedgebuer, and F. Delorme, Phys. Rev. E 57, 6618 (1998).
- [17] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, Phys. Rev. E 51, 980 (1995).
- [18] H. D. I. Abarbanel, N. F. Rulkov, and M. M. Sushchik, Phys. Rev. E 53, 4528 (1996).
- [19] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **76**, 1816 $(1996).$
- [20] K. Josić, Phys. Rev. Lett. **80**, 3053 (1998).
- [21] P. Grassberger, Phys. Lett. 97A, 227 (1983).