Encoding messages using chaotic synchronization

U. Parlitz,[1] L. Kocarev,[2] T. Stojanovski,[2] and H. Preckel[1]
[1]*Drittes Physikalisches Institut, Universität Göttingen, Bürgerstraβe 42-44, D-37073 Göttingen, Federal Republic of Germany*
[2]*Department of Electrical Engineering, St. Cyril and Methodius University, Skopje, P.O. Box 574, Republic of Macedonia*

(Received 5 July 1995)

We discuss a general approach for chaotic synchronization of dynamical systems that is based on an active-passive decomposition (APD) of given dynamical systems. It is shown how this approach can be used to construct high-dimensional synchronizing systems in a systematic way using low-dimensional systems as building blocks. Furthermore, two methods for encoding messages are considered that are both based on synchronization. Using these methods the quality of the reconstructed information signal is higher and the encoding is more secure compared to other encryption methods based on synchronization. The main ideas are illustrated using experimental and numerical examples based on continuous and discrete dynamical systems.

PACS number(s): 05.45.+b, 43.72.+q, 47.52.+j

I. INTRODUCTION

Synchronization of periodic signals is a well-known phenomenon in physics, engineering, and many other scientific disciplines. However, even chaotic systems may be linked in a way such that their chaotic oscillations are synchronized. In particular the case of one directional coupling has been investigated very intensely during the last years [1–5] because of its potential application in communication systems [6–17]. There, an information signal containing a message is transmitted using a chaotic signal as a broadband carrier and the synchronization is necessary to recover the information at the receiver. Different implementations of this basic idea have been suggested. For example, in Refs. [8,9,11] the information signal is added to the chaotic signal and in Refs. [8,10] a parametric modulation is used for the transmission of digital signals. Other approaches to use chaotic dynamics for communication include controlling techniques to encode binary messages [18] and methods that make use of the quick decay of the correlation function for chaotic signals [19].

In this paper we discuss a general approach for constructing synchronizing chaotic dynamical systems and two improved methods for encoding messages using chaotic synchronization [12–16]. The basic idea of the synchronization approach consists in a decomposition of a given (chaotic) system into an active and a passive part, where different copies of the passive part synchronize when driven by the same active component. The general description of this *active-passive decomposition* (APD) and some examples for illustration are given in Sec. II A. The relation of this approach to the most important methods for controlling chaos and for synchronization is discussed in Sec. II B. In Sec. III we show how synchronization may be used to encode messages in a dynamical way where the information is not just added to some chaotic carrier but drives the dynamical system of the transmitter. Such a dynamical modulation yields more secure encoding and may also be used to avoid the typical distortion errors that occur for almost all previous communication schemes based on synchronization [8,9]. Two different encoding-decoding schemes are discussed. The method used in Sec. III A enables an exact reconstruction of the information signal whereas the autosynchronization approach presented in Sec. III B may lead to implementations that are more robust with respect to noise. For both methods numerical and experimental (analog computer) examples are given that are based on an APD of the well-known Rössler system. Section III C contains a comparison of the APD-based encoding methods with other encryption methods based on synchronization. In Sec. IV we demonstrate how active-passive decomposition may be used to construct systematically high-dimensional systems with hyperchaotic attractors that are very useful for private communication. A realization of the APD and the exact encoding method in the context of discrete dynamical systems is given in Sec. V. There we use as an example a random number generator for encoding an information signal. In this case the chaotic carrier is very high dimensional and difficult to decode without the knowledge about the dynamical system used.

II. SYNCHRONIZATION OF CONTINUOUS SYSTEMS

In this section the basic concept and some terminology are introduced using continuous dynamical systems. The generalization to discrete systems is straightforward and will be discussed in Sec. V.

A. Constructing synchronizing systems by active-passive decomposition

Consider an arbitrary N-dimensional (chaotic) dynamical system

$$\dot{\mathbf{z}}=\mathbf{F}(\mathbf{z}). \tag{1}$$

The goal is to rewrite this autonomous system as a nonautonomous system that possesses certain synchronization properties. Formally, we may write

$$\dot{\mathbf{x}}=\mathbf{f}(\mathbf{x},\mathbf{s}), \tag{2}$$

where $\mathbf{x}$ is the new state vector corresponding to $\mathbf{z}$ and $\mathbf{s}$ is some vector valued function of time given by

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

or

$$\dot{\mathbf{s}}=\mathbf{h}(\mathbf{x},\mathbf{s}). \tag{4}$$

The pair of functions **f** and **h** constitutes a decomposition of the original vector field **F** (see also the example that follows). The crucial point of this decomposition is that for suitable choices of the function **h** any system

$$\dot{\mathbf{y}}=\mathbf{f}(\mathbf{y},\mathbf{s}) \tag{5}$$

that is given by the *same* nonautonomous vector field **f**, the *same* driving s, but *different* variables **y**, synchronizes with the original system (2), i.e., $\|\mathbf{x}-\mathbf{y}\|\to 0$ for $t\to\infty$. More precisely, synchronization of the pair of (identical) systems (2) and (5) occurs if the dynamical system describing the evolution of the difference $\mathbf{e}=\mathbf{y}-\mathbf{x}$,

$$\dot{\mathbf{e}}=\mathbf{f}(\mathbf{y},\mathbf{s})-\mathbf{f}(\mathbf{x},\mathbf{s})=\mathbf{f}(\mathbf{x}+\mathbf{e},\mathbf{s})-\mathbf{f}(\mathbf{x},\mathbf{s}),$$

possesses a stable fixed point at the origin $\mathbf{e}=\mathbf{0}$. In some cases this can be proved using stability analysis of the linearized system for small **e**,

$$\dot{\mathbf{e}}=D\mathbf{f}(\mathbf{x},\mathbf{s})\cdot\mathbf{e}$$

or using (global) Lyapunov functions. In general, however, the stability has to be checked numerically using the fact that synchronization occurs if all conditional Lyapunov exponents of the nonautonomous system (2) are negative. In this case system (2) is a passive system and we call the decomposition an active-passive decomposition of the original dynamical system (1). The technical notion of conditional Lyapunov exponents was introduced by Pecora and Carroll [1] in order to study the synchronization of subsystems. In the following we will show that the APD provides a unifying and generalizing framework for their approach and other methods for synchronizing and controlling of chaotic systems.

Example: The Rössler system: As an example for the active-passive decomposition introduced above we will use in this paper the well-known Rössler system

$$\dot{z}_1=2+z_1(z_2-4),$$
$$\dot{z}_2=-z_1-z_3, \tag{6}$$
$$\dot{z}_3=z_2+0.45z_3.$$

An APD of the Rössler vector field is for example given by

$$\dot{x}_1=2-4x_1+x_2^2-sx_2,$$
$$\dot{x}_2=-x_2-x_3+s, \tag{7}$$
$$\dot{x}_3=x_2+0.45x_3$$

with

$$s=x_2-x_1 \tag{8}$$

and

TABLE I. Examples of active-passive decompositions of the Rössler system (6). The conditional Lyapunov exponents λ_i were computed with respect to the natural logarithm.

$\dot{x}_1=2-4x_1+3(x_2+x_3)+s$		$\lambda_1=-0.08$
$\dot{x}_2=-x_1-x_3$	$s=x_1x_2-3(x_2+x_3)$	$\lambda_2=-0.08$
$\dot{x}_3=x_2+0.45x_3$		$\lambda_3=-3.39$
$\dot{x}_1=2+x_1(x_2-4)$		$\lambda_1=-0.43$
$\dot{x}_2=-2x_1-2x_3+s$	$s=x_1+x_2+x_3$	$\lambda_2=-0.52$
$\dot{x}_3=x_2+0.45x_3$		$\lambda_3=-3.15$
$\dot{x}_1=2+x_1(x_2-4)$		$\lambda_1=-0.12$
$\dot{x}_2=-x_1-x_3$	$s=x_3$	$\lambda_2=-0.22$
$\dot{x}_3=x_2+0.45s$		$\lambda_3=-3.20$

$$\dot{y}_1=2-4y_1+y_2^2-sy_2,$$
$$\dot{y}_2=-y_2-y_3+s,$$
$$\dot{y}_3=y_2+0.45y_3.$$

In this case the differential equations for the error $\mathbf{e}=\mathbf{y}-\mathbf{x}$ read

$$\dot{e}_1=-4e_1+e_2(x_2+y_2-s),$$
$$\dot{e}_2=-e_2-e_3,$$
$$\dot{e}_3=e_2+0.45e_3.$$

The decomposition (7),(8) of the original differential equation (6) yields a stable e_2-e_3 system with complex eigenvalues $-0.275\pm i\sqrt{0.474375}$. Therefore, e_2 and e_3 converge to zero for $t\to\infty$ and the differential equation for e_1 may for this limit be written as $\dot{e}_1=-4e_1$; i.e., the difference e_1 also vanishes and the x and the y systems synchronize. Note that this proof holds for arbitrary bounded functions $s(t)$. This feature is of importance for applications in communication that will be discussed in Sec. III. Other APD's of the Rössler system that yield synchronizing chaotic systems are given in Table I.

Instead of decomposing a given chaotic system one may also synthesize it starting from a stable linear system $\dot{\mathbf{x}}=A\cdot\mathbf{x}$ given by some matrix A where an appropriate nonlinear function $\mathbf{s}=\mathbf{h}(\mathbf{x})$ is added such that the complete system

$$\dot{\mathbf{x}}=A\cdot\mathbf{x}+\mathbf{s}$$

is chaotic [13]. It is easy to verify that in this case the error dynamics is given by the stable system $\dot{\mathbf{e}}=A\cdot\mathbf{e}$ and synchronization occurs for all initial conditions and arbitrary signals s. In this way synchronized chaotic systems may be designed with specific features for applications.

B. Comparison with other methods for synchronizing and controlling of chaos

In the following we briefly discuss the relation of the APD to other methods for synchronizing and controlling chaotic systems.

1. The method of Pecora and Carroll

The most popular method for constructing synchronizing (sub) systems was introduced by Pecora and Carroll [1]. They decompose a given dynamical system,

$$\dot{\mathbf{u}}=\mathbf{g}(\mathbf{u}),$$

into two subsystems,

$$\dot{\mathbf{v}}=\mathbf{g}_{\mathbf{v}}(\mathbf{v},\mathbf{w}),$$

$$\dot{\mathbf{w}}=\mathbf{g}_{\mathbf{w}}(\mathbf{v},\mathbf{w})$$

with $\mathbf{v}=(u_1,\ldots,u_k)$ and $\mathbf{w}=(u_{k+1},\ldots,u_N)$. It can be shown that any second system

$$\dot{\mathbf{w}}'=\mathbf{g}_{\mathbf{w}}(\mathbf{v},\mathbf{w}')$$

that is again given by the same vector field $\mathbf{g}_{\mathbf{w}}$, the same driving $\mathbf{v}$, but different variables $\mathbf{w}'$ synchronizes $(\|\mathbf{w}'-\mathbf{w}\|\rightarrow 0)$ with the original w subsystem if the conditional Lyapunov exponents of the w system are all negative. The coupling is one directional and the v system and the w system are referred to as the *drive system* and the *response system*, respectively. It is easy to see that the APD approach includes this scheme if we use Eq. (4) with

$$\begin{array}{ccccccc}\mathbf{s} & \leftrightarrow & \mathbf{v}, & \mathbf{h} & \leftrightarrow & \mathbf{g}_{\mathbf{v}},\\ \mathbf{x} & \leftrightarrow & \mathbf{w}, & \mathbf{f} & \leftrightarrow & \mathbf{g}_{\mathbf{w}},\\ \mathbf{y} & \leftrightarrow & \mathbf{w}'. & & & \end{array}$$

However, in the case of Pecora-Carroll synchronization only a finite number of possible decompositions exists, which is bounded by the number of different subsystems $N(N-1)/2$. In general, only a few of the possible response subsystems possess negative conditional Lyapunov exponents and may be used to implement synchronizing systems. In the case of the Rössler system, for example, only the following decomposition into a drive system,

$$\dot{s}=x_2+0.45s, \tag{9}$$

and a response system,

$$\begin{aligned}\dot{x}_1&=2+x_1(x_2-4),\\ \dot{x}_2&=-x_1-s,\end{aligned} \tag{10}$$

leads to synchronization [1]. On the other hand, with the more general decomposition discussed in this paper many different pairs of synchronizing systems may be constructed (see, for example, Table I). Therefore, the APD may be viewed as a generalization of the method of Pecora and Carroll that leads to a larger variety of realizations for chaotic synchronization.

2. The method of Hübler

The method for constructing synchronizing systems by active-passive decomposition is also related to the controlling method introduced by Hübler [20]. Hübler proposed the following scheme. Let

$$\dot{\mathbf{u}}=\mathbf{E}(\mathbf{u})+\mathbf{H} \tag{11}$$

be some (experimental) system that is driven by some force $\mathbf{H}$. The task is to define $\mathbf{H}$ such that the dynamics of this system converges to some goal dynamics that is given by

$$\dot{\mathbf{v}}=\mathbf{G}(\mathbf{v}). \tag{12}$$

In his work Hübler proposed to use

$$\mathbf{H}=\mathbf{G}(\mathbf{v})-\mathbf{E}(\mathbf{v}). \tag{13}$$

With this choice controlling (i.e., $\|\mathbf{u}-\mathbf{v}\|\rightarrow 0$ for $t\rightarrow\infty$) is possible if the conditional Lyapunov exponents of Eq. (11) are all negative. The connection between Hübler's method and the APD becomes more clear if we use Eq. (13) to rewrite Eq. (12) for the goal dynamics as

$$\dot{\mathbf{v}}=\mathbf{E}(\mathbf{v})+\mathbf{H}=\mathbf{Z}(\mathbf{v},\mathbf{H}).$$

Then Hübler's method for controlling may be expressed in the framework of the APD in the following way:

$$\begin{array}{ccccccc}\mathbf{x} & \leftrightarrow & \mathbf{v}, & \mathbf{s},\mathbf{h} & \leftrightarrow & \mathbf{H},\\ \mathbf{y} & \leftrightarrow & \mathbf{u}, & \mathbf{f} & \leftrightarrow & \mathbf{Z}.\end{array}$$

In his original work Hübler admits only additive controlling forces, but this can of course be generalized to parametric forces [21]. The main difference between Hübler's method and the APD consists in the goals: controlling a given experimental system versus encoding messages using synchronized systems. For the latter we may freely choose suitable dynamical systems and decompositions. Even more, the message to be encoded drives the x system (see Sec. III), which corresponds to a nonautonomous goal dynamics.

3. The method of Pyragas

Finally we would like to mention the controlling method of Pyragas [22] where some function of the type $c(u_j(t)-v_j(t))$ is added to the jth component of the vector field $\dot{\mathbf{u}}=\mathbf{g}(\mathbf{u})$ of the system to be controlled. The parameter c has to be chosen suitably and the function $v_j(t)$ is, for example, a prerecorded signal from the unperturbed system or a second identical system $\dot{\mathbf{v}}=\mathbf{g}(\mathbf{v})$. The controlling force used by Pyragas is a special case of the so-called modified method of Fujisaka and Yamada [2] that was introduced by Brown, Rulkov, and Tracy [23]. It differs from Pyragas' method only in the sense that not only are scalar functions used for the driving but multidimensional couplings $A(\mathbf{u}-\mathbf{v})$, where A is some coupling matrix. In general this kind of feedback controlling method may thus be written as

$$\dot{\mathbf{u}}=\mathbf{g}(\mathbf{u})+A(\mathbf{u}-\mathbf{v}).$$

The relation to the APD is given by:

$$\begin{array}{ccc}\mathbf{s},\mathbf{x} & \leftrightarrow & \mathbf{v},\\ \mathbf{y} & \leftrightarrow & \mathbf{u},\\ \mathbf{f}(\mathbf{x},\mathbf{s}) & \leftrightarrow & \mathbf{g}(\mathbf{v})+A(\mathbf{v}-\mathbf{v})=\mathbf{g}(\mathbf{v}),\\ \mathbf{f}(\mathbf{y},\mathbf{s}) & \leftrightarrow & \mathbf{g}(\mathbf{u})+A(\mathbf{u}-\mathbf{v}).\end{array}$$

In the previous discussion of synchronization methods, the function $\mathbf{s}$ was assumed to be vector valued in general. For the examples and in the following, however, we will consider only cases with scalar signals s that are most interesting for practical applications of synchronization in communication.

III. ENCODING INFORMATION SIGNALS

The synchronizing systems obtained using the APD described in the previous section may be used to build transmitter-receiver systems for encoding and masking information signals. In the following we describe two methods that possess different features that may be useful for practical applications.

A. Exact reconstruction of the information signal

With the first method [12–16] the information signal i is included in the function h describing the scalar signal s. If h is invertible with respect to i,

$$i=h^{-1}(\mathbf{x},s,\dot{s}),$$

then the information recovered at the receiver,

$$i_R=h^{-1}(\mathbf{y},s,\dot{s}),$$

converges to the original information i if the transmitter (x system) and the receiver (y system) synchronize.

To demonstrate the proposed method for encoding messages experimentally we have implemented the following decomposition of the Rössler system (6) on an analog computer (Telefunken RAT 700):

transmitter:

$$\begin{aligned}\dot{x}_1&=2+x_1(x_2-4),\\ \dot{x}_2&=-x_1-x_3,\\ \dot{x}_3&=x_2-x_3+s;\end{aligned}\tag{14}$$

transmitted signal:

$$s=1.45x_3+i;\tag{15}$$

receiver:

$$\begin{aligned}\dot{y}_1&=2+y_1(y_2-4),\\ \dot{y}_2&=-y_1-y_3,\\ \dot{y}_3&=y_2-y_3+s.\end{aligned}\tag{16}$$

Figure 1(a) shows a typical chaotic oscillation of the experimentally implemented Rössler system without external information signal ($i=0$) and Fig. 1(b) the corresponding power spectrum. In Fig. 2 the variable x_2 of the transmitter is plotted versus the corresponding variable y_2 of the receiver for $i=0$. The resulting curve lies on the diagonal indicating the synchronization of the transmitter and the receiver. Figure 3 shows the results for a sinusoidal information signal. Neither in the transmitted signal [Fig. 3(a)] nor in its power spectrum [Fig. 3(b)] is the sinusoidal information signal easy to detect. Only a small peak is visible in the spectrum at the frequency of the sine function, which is not higher than the other peaks of the chaotic broadband spectrum. Figures 3(c) and 3(d) show the recovered signal i_R and its power spectrum, respectively. Note the high signal-to-noise ratio of 40 dB, indicating a good quality of the reconstruction. Figure 4 shows the experimental results for a sinusoidal signal with varying frequency, i.e., a *frequency sweep*. Again the information cannot be detected in the transmitted signal [Fig. 4(a)] or its power spectrum [Fig. 4(b)]. The quality of the reconstructed information signal i_R [Fig. 4(c)] is for all frequencies quite good and the corresponding power spectrum [Fig. 4(d)] differs only for high frequencies from the original spectrum

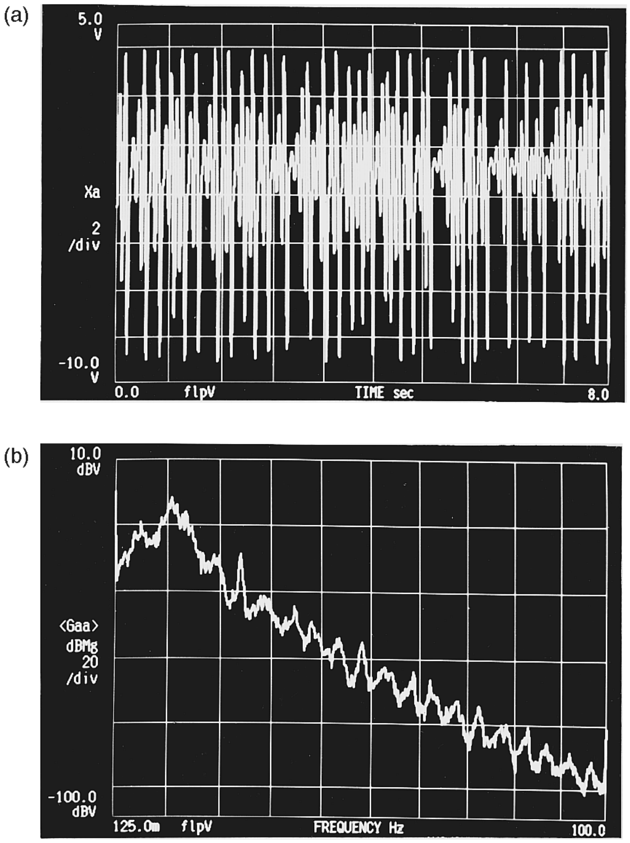

FIG. 1. Chaotic oscillations of a single experimental Rössler system implemented on an analog computer (Telefunken RAT 700). (a) Time series x_1. (b) Power spectrum of the time series shown in (a).

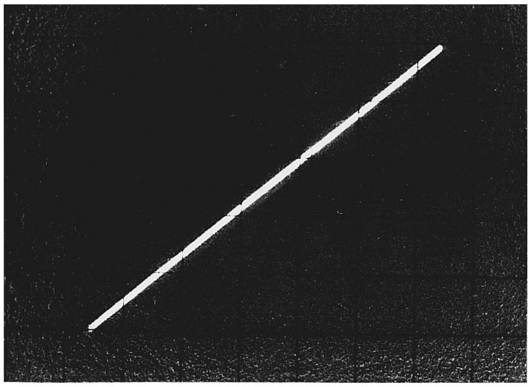

FIG. 2. Synchronization of the two experimental Rössler systems (14)–(16) without information signal. Plotted are the variables x_2 vs y_2.

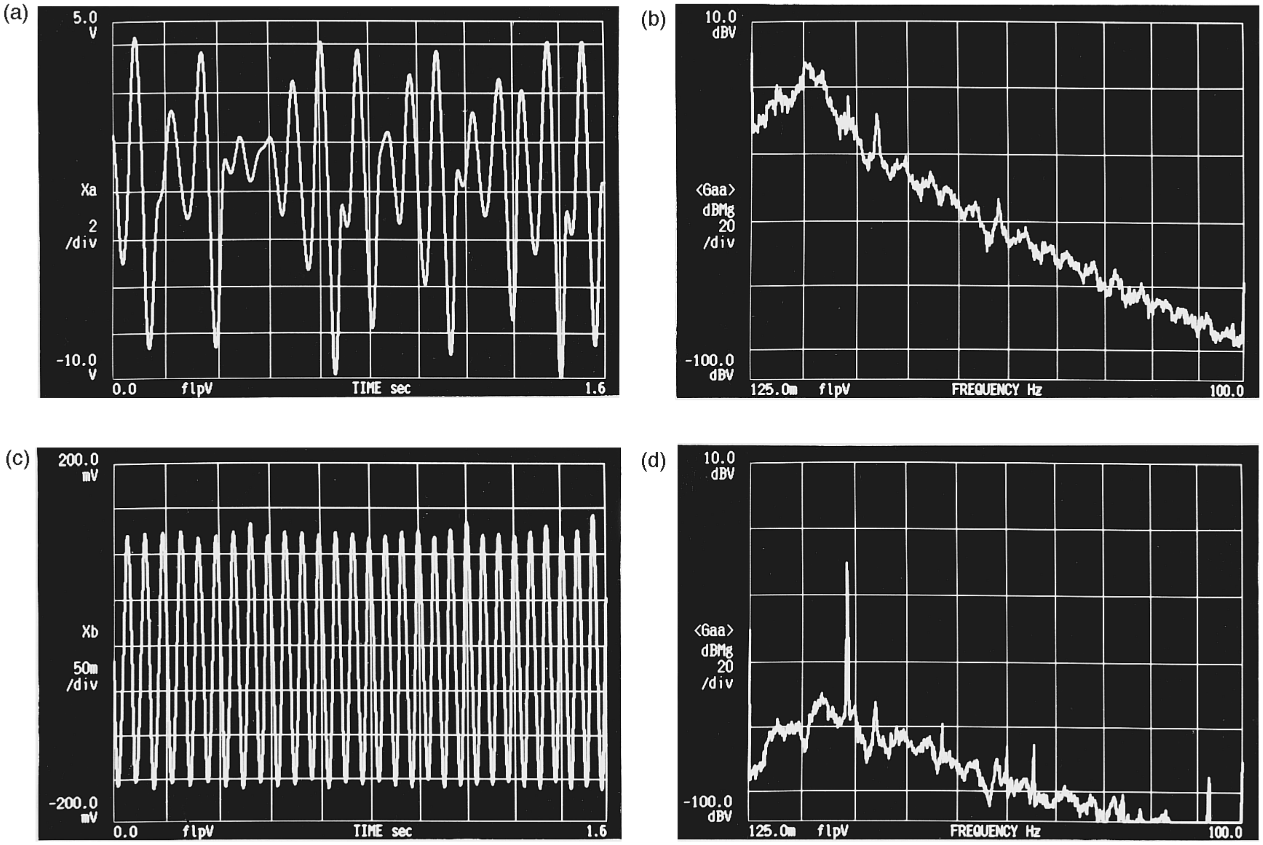

FIG. 3. Experimental encoding and decoding of a sinusoidal information signal $i(t)$ using the systems (14)–(16). (a) Transmitted signal $s(t)=1.45x_3(t)+i(t)$. (b) Power spectrum of the transmitted signal $s(t)$. (c) Recovered information $i_R(t)=s(t)-1.45y_3(t)$. (d) Power spectrum of the recovered information $i_R(t)$.

(not shown here). Note that the spectrum of the transmitted signal [Fig. 4(b)] is very similar to the spectrum of the single Rössler system shown in Fig. 1(b). An important feature of this example is the fact that the spectrum of the information signal [Fig. 4(d)] and the spectrum of the chaotic oscillations of the Rössler system [Fig. 1(b)] are located in approximately the same frequency range. Therefore, it is impossible to separate them using standard linear filters.

B. Information reconstruction using autosynchronization

The second method for encoding and decoding a message using chaotic dynamical systems is based on *autosynchronization*. Autosynchronization means that the second dynamical system (the receiver) may adapt its parameters to those of the first system (the transmitter) using an additional feedback loop. The controlling force of the feedback loop depends on the signal $s(t)$ from the transmitter and an analogous signal $s_R(t)$ that is derived from the state variables of the receiver. In the case of synchronization $s(t)$ equals $s_R(t)$ and the controlling force becomes zero. To illustrate this method we start from the APD (7),(8) of the Rössler system given in Sec. II A. The information signal $i(t)$ is injected into the first equation of the transmitter but is *not* included in the transmitted signal $s(t)$. The resulting communication scheme can be summarized as follows:

Transmitter:

$$\dot{x}_1=2-4x_1+x_2^2-sx_2+i(t), \tag{17}$$

$$\dot{x}_2=-x_2-x_3+s,$$

$$\dot{x}_3=x_2+0.45x_3;$$

transmitted signal:

$$s=x_2-x_1; \tag{18}$$

receiver:

$$\dot{y}_1=2-4y_1+y_2^2-sy_2+y_4,$$

$$\dot{y}_2=-y_2-y_3+s,$$

$$\dot{y}_3=y_2+0.45y_3, \tag{19}$$

$$\dot{y}_4=a(s_R-s),$$

where $s_R=y_2-y_1$, $i_R=y_4$, and a is a free convergence parameter. For the differences $e_k=y_k-x_k$ $(k=1,2,3)$ and $e_4=y_4-i$ the following differential equations hold:

$$\dot{e}_1=-4e_1+e_2(x_2+y_2-s)+e_4,$$

$$\dot{e}_2=-e_2-e_3,$$

$$\dot{e}_3=e_2+0.45e_3,$$

$$\dot{e}_4=a(s_R-s)-di/dt.$$

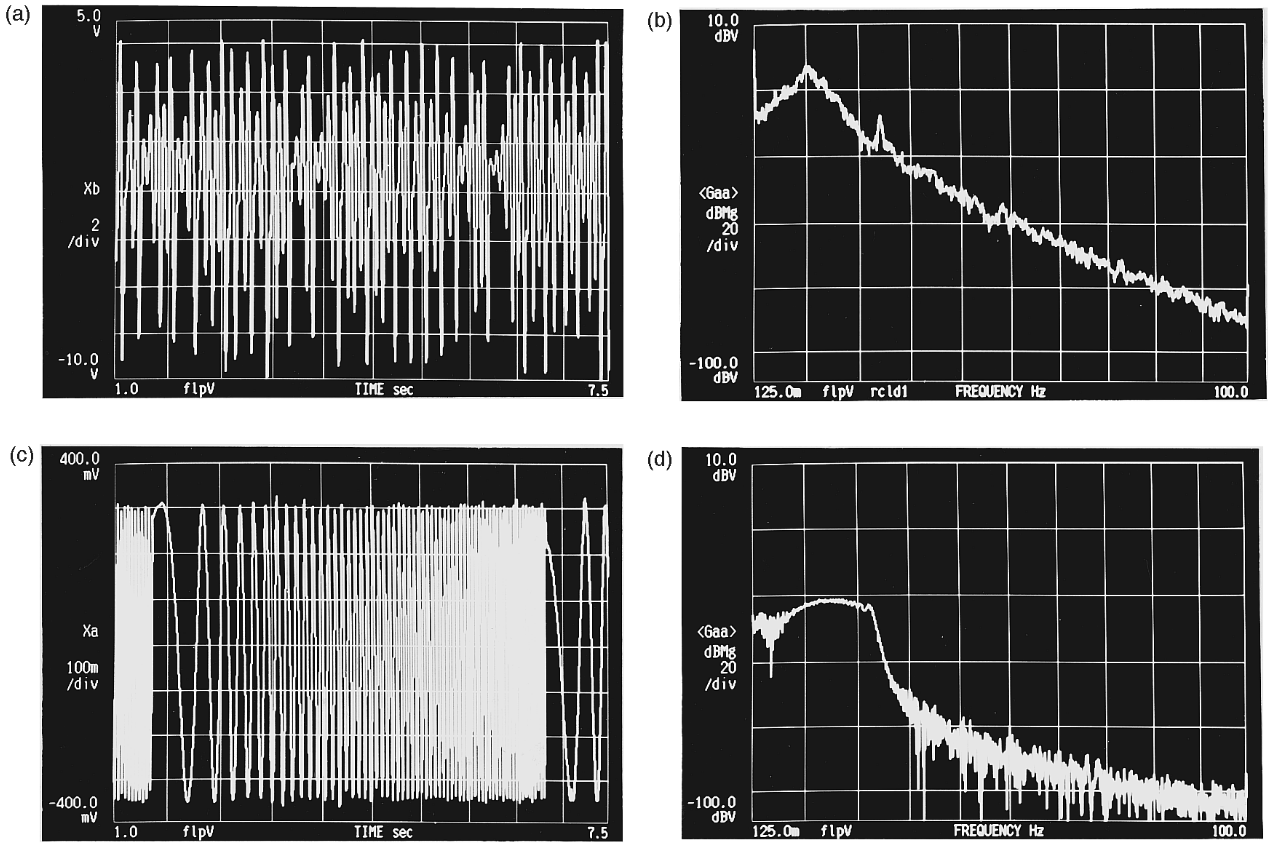

FIG. 4. Experimental encoding and decoding of a sinusoidal information signal $i(t)$ with periodically varied frequency (frequency sweep) using the systems (14)–(16). (a) Transmitted signal $s(t)=1.45x_3(t)+i(t)$. (b) Power spectrum of the transmitted signal $s(t)$. (c) Recovered information $i_R(t)=s(t)-1.45y_3(t)$. (d) Power spectrum of the recovered information $i_R(t)$.

As in example (7) the e_2-e_3 subsystem is stable and $e_2,e_3\to 0$. In the limit $t\to\infty$ we thus obtain a two-dimensional system that may be written as

$$\dot{e}_1=-4e_1-e_4,$$

$$\dot{e}_4=a(s_R-s)-di/dt$$

or

$$\ddot{e}_4+4\dot{e}_4+ae_4=-4\frac{di}{dt}-\frac{d^2i}{dt^2}. \qquad (20)$$

The variable $e_4=y_4-i=i_R-i$ describing the reconstruction error is thus governed by the well-known differential equation (20) for a damped linear oscillator. If the information signal is constant $(di/dt=0)$ the reconstruction error e_4 converges exponentially to zero, oscillating with a frequency $\sqrt{a-4}$ if $a>4$. The error remains small if the information signal changes only slowly compared to the time scale of the error dynamics. In principle the error of this example can be estimated quantitatively using the theory of linear systems. A numerical example where the information signal is given by a triangular information signal and $a=10$ is shown in Fig. 5. This encoding method was also implemented on the analog computer using the following systems:

Transmitter:

$$\dot{x}_1=2+x_1(x_2-4), \qquad (21)$$

$$\dot{x}_2=-x_1-x_3,$$

$$\dot{x}_3=x_2-x_3+s+i;$$

transmitted signal:

$$s=1.45x_3; \qquad (22)$$

receiver:

$$\dot{y}_1=2+y_1(y_2-4),$$

$$\dot{y}_2=-y_1-y_3,$$

$$\dot{y}_3=y_2-y_3+s+y_4, \qquad (23)$$

$$\dot{y}_4=a(s-s_R),$$

where $s_R=1.45y_3$ and $i_R=y_4$. Note that in contrast to the similar example given in Sec. III A here the transmitted signal is not a sum of a chaotic signal and the information signal. Therefore, if i is, for example, a pure sinusoidal signal there is no additional peak in the power spectrum of s [compare Fig. 3(b)]. Another difference from the method discussed in Sec. III A is the fact that here the reconstructed signal $i_R=y_4$ follows the variations of i with some delay or inertia and is permanently in a transient state. This can best be seen for a rectangular information signal as shown in Fig. 6. After each change of the signal $i(t)$ [Fig. 6(a)] the recon-

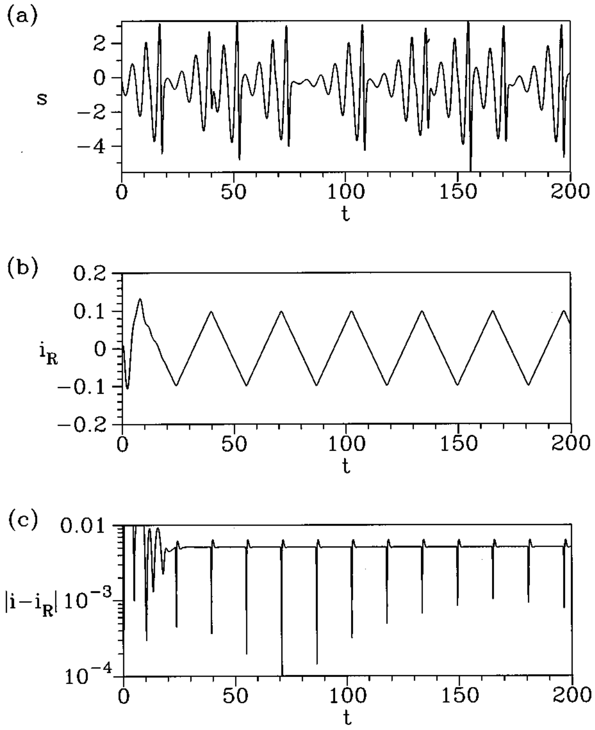

FIG. 5. Numerical encoding and decoding of a triangular information signal $i(t)$ using the communication system (17)–(19). (a) Transmitted signal $s(t)$. (b) Recovered information $i_R(t)=y_4$. (c) Difference $|i(t)-i_R(t)|$ between the original and the recovered information signal.

structed information [Fig. 6(b)] needs some time to converge to the new value. Similar to the first example the transient is approximately exponential and is given by the time scale of the error dynamics. In any practical application one should therefore use a chaotic system that oscillates with frequencies that are (much) higher than the characteristic frequencies of the information signal. In this case any variation of $y_4=i_R$ depends on many oscillations of the transmitted signal; i.e., the transmission becomes (very) redundant. The redundancy, however, can be exploited to reconstruct the information almost exactly and to make the communication more robust with respect to noise. A more detailed investigation of this problem will be given elsewhere. Furthermore, it is possible to use autosynchronization to encode several information signals using a *single* chaotic carrier [24].

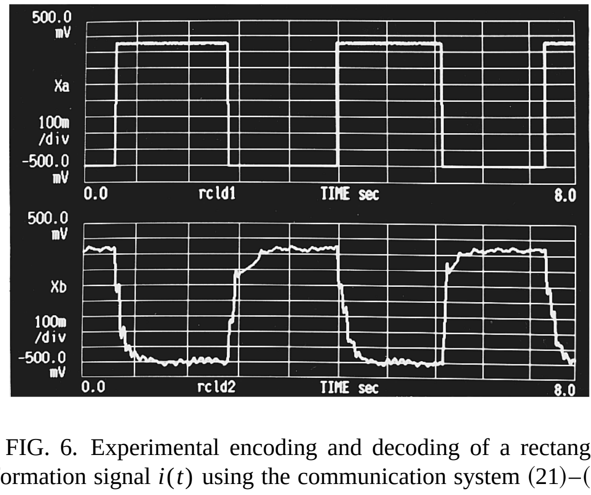

FIG. 6. Experimental encoding and decoding of a rectangular information signal $i(t)$ using the communication system (21)–(23). (a) Information signal $i(t)$. (b) Recovered information $i_R(t)=y_4$.

C. Comparison with other encryption methods based on synchronization

The APD-based methods for encoding messages using synchronization differ from previously suggested schemes [1,8,9,12] in the fact that *the information is not just added to a chaotic carrier but also drives the dynamical system constituting the transmitter*. This has some important consequences. With the exact encoding method (Sec. III A) the information can be recovered at the receiver without any distortion errors. In contrast, if the information signal is just added to a chaotic signal, the receiver can only generate an approximation of the original state variables of the transmitter, because its dynamics is also influenced by the added information signal, which is not the case for the dynamics of the transmitter. The resulting distortion error vanishes only if the amplitude of the information signal is very (infinitesimally) small. If, however, the amplitude of the information signal is very small then it is in general very sensitive to any noise in the transmission channel. Even worse, the transmitted signal consists in this case mainly of a (low-dimensional) chaotic signal that can be modeled using time delay embedding and then be subtracted from the transmitted signal to obtain the information signal. This can be done efficiently using methods for nonlinear noise reduction [25] where the information signal is in this case treated as noise. Of course, such encoding is not very secure and therefore not useful for private communication. The synchronization and encoding schemes discussed in this paper try to avoid these drawbacks because they yield (exact) reconstructions of the information signal based on a transmitted signal that is more complicated and high dimensional. Note that also the decomposition of Pecora and Carroll [Eqs. (9) and (10)] can be used in this sense to implement the improved encoding methods. One simply may add the information signal to the right-hand side of Eq. (9) for example. The receiver then has to generate the temporal derivative $\dot{s}$ from s in order to recover the information as $i_R=\dot{s}-y_1+y_2$. Another possible application consists in encoding digital (binary) informations by switching between different chaotic sources. In contrast to schemes based on Pecora-Carroll decomposition [10], with the APD it is not necessary to use a cascade of two subsystems in order to verify the synchronization in the receiver. It suffices to compute a new "transmitted signal" s_R from the state variables of the receiver and compare it with the actually received signal s.

The practical question of robustness of the synchronization with respect to parameter differences and additional noise will be discussed in detail elsewhere. First simulations yielded results that are comparable to analogous investigations for Pecora-Carroll synchronization.

IV. CASCADED SYSTEMS

For encoding messages it is desirable to use high-dimensional chaotic carriers in order to make the decoding as difficult as possible. In the following we describe a strategy

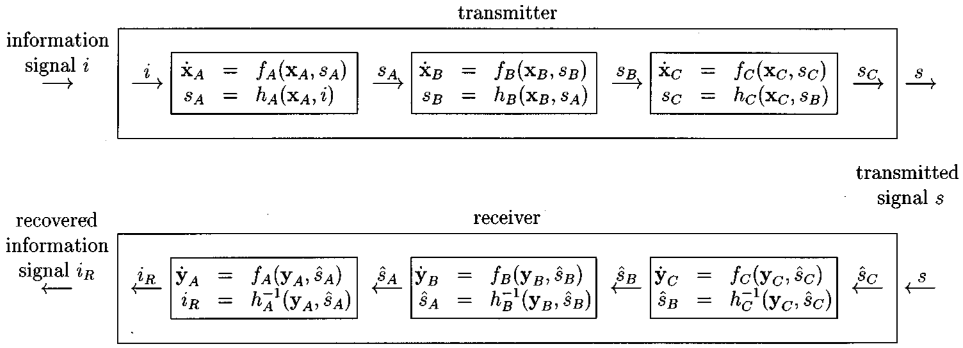
transmitter
information signal i
i
$\dot{\mathbf{x}}_A = f_A(\mathbf{x}_A, s_A)$
$s_A = h_A(\mathbf{x}_A, i)$
s_A
$\dot{\mathbf{x}}_B = f_B(\mathbf{x}_B, s_B)$
$s_B = h_B(\mathbf{x}_B, s_A)$
s_B
$\dot{\mathbf{x}}_C = f_C(\mathbf{x}_C, s_C)$
$s_C = h_C(\mathbf{x}_C, s_B)$
s_C
s
transmitted signal s
receiver
recovered information signal i_R
i_R
$\dot{\mathbf{y}}_A = f_A(\mathbf{y}_A, \hat{s}_A)$
$i_R = h_A^{-1}(\mathbf{y}_A, \hat{s}_A)$
$\hat{s}_A$
$\dot{\mathbf{y}}_B = f_B(\mathbf{y}_B, \hat{s}_B)$
$\hat{s}_A = h_B^{-1}(\mathbf{y}_B, \hat{s}_B)$
$\hat{s}_B$
$\dot{\mathbf{y}}_C = f_C(\mathbf{y}_C, \hat{s}_C)$
$\hat{s}_B = h_C^{-1}(\mathbf{y}_C, \hat{s}_C)$
$\hat{s}_C$
s

FIG. 7. General scheme for constructing high-dimensional communication systems. The synchronization of the transmitter and the receiver is based on the mutual synchronization of (here, three) low-dimensional chaotic systems that constitute their building blocks.

to construct systematically high-dimensional synchronizing systems using low-dimensional building blocks. The idea is to use the synchronization properties discussed above in a series or cascade of systems as illustrated in Fig. 7. If all pairs of systems $\mathbf{f}_A(\mathbf{x}_A, s_A) - \mathbf{f}_A(\mathbf{y}_A, s_A)$, $\mathbf{f}_B(\mathbf{x}_B, s_B) - \mathbf{f}_B(\mathbf{y}_B, s_B)$, $\mathbf{f}_C(\mathbf{x}_C, s_C) - \mathbf{f}_C(\mathbf{y}_C, s_C)$, etc. synchronize then the information can be recovered at the receiver as

$$\begin{aligned} i_R &= h_A^{-1}(\mathbf{y}_A, \hat{s}_A) = h_A^{-1}(\mathbf{y}_A, h_B^{-1}(\mathbf{y}_B, \hat{s}_B)) \\ &= h_A^{-1}(\mathbf{y}_A, h_B^{-1}(\mathbf{y}_B, h_C^{-1}(\mathbf{y}_C, s))) = H(\mathbf{y}, s), \end{aligned}$$

where $\mathbf{y} = (\mathbf{y}_A, \mathbf{y}_B, \mathbf{y}_C)$ denotes the state of the complete receiver. The low-dimensional systems $\mathbf{f}_A(\mathbf{x}_A, s_A)$, $\mathbf{f}_B(\mathbf{x}_B, s_B)$, $\mathbf{f}_C(\mathbf{x}_C, s_C)$ constituting the building blocks may be different systems or three identical copies of the same system. As an example we consider here the latter case where the APD of the Rössler system given in the last row of Table I is used for each block with

$$s_{\rm out} = h(\mathbf{x}, s_{\rm in}) = x_3 + 0.25 s_{\rm in}.$$

The factor 0.25 is necessary to avoid divergence of the perturbed Rössler systems. This problem is a special feature of the Rössler system and can be avoided by using dynamical systems that are stable for all initial conditions. Figure 8 shows an example where the information signal is the spoken word "24" recorded with a microphone (16 bit resolution, sampling rate 8000 Hz). To verify the fact that the transmitter possesses a hyperchaotic attractor for $i = 0$ we have computed the (ordinary) Lyapunov exponents of this nine-dimensional system. The result are three positive exponents (0.112,0.082,0.080), two vanishing and four negative exponents $(-0.011, -2.86, -2.93, -3.18)$. The Lyapunov dimension of the hyperchaotic attractor thus is $D_L = 6.09$.

Similar to the cascaded systems presented here it is also possible to use low-dimensional chaotic systems in parallel in order to construct high-dimensional synchronizing systems. Furthermore, the APD approach allows also to include (linear) filters in the definition of h in a way that the transmitted signal s fulfills, for example, some given constraints for the bandwidth of the transmission channel. These generalizations will be discussed in more detail elsewhere.

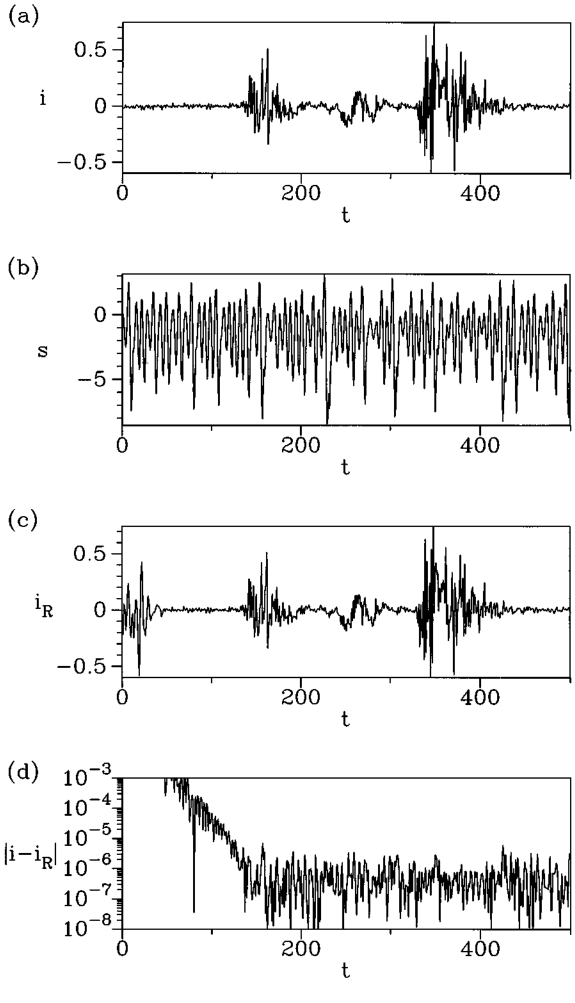

FIG. 8. Numerical simulation of a high-dimensional communication scheme based on a cascade of three chaotic Rössler systems. (a) Information signal $i(t)$ = spoken word "24." (b) Transmitted signal $s(t)$. (c) Recovered information signal $i_R(t)$. (d) Difference $|i(t) - i_R(t)|$ between the original and the recovered information signal.

V. SYNCHRONIZATION OF DISCRETE SYSTEMS

In this section we consider the APD of discrete dynamical systems and give two examples for encoding schemes that yield exact reconstructions of the information signal.

Encoding information signals: In general the communication scheme discussed in Sec. III A can for discrete systems be summarized as follows:

Transmitter:

$$\mathbf{x}(n+1)=f(\mathbf{x}(n),s(n)); \tag{24}$$

transmitted signal:

$$s(n)=h(\mathbf{x}(n),i(n));$$

or

$$s(n+1)=h(\mathbf{x}(n),s(n),i(n)); \tag{25}$$

receiver:

$$\mathbf{y}(n+1)=f(\mathbf{y}(n),s(n)), \tag{26}$$

where $\mathbf{x}(n),\mathbf{y}(n)$ are N-dimensional vectors and $x_m,y_m,s,i \in I$ with $I\subset \mathrm{IR}$ or $I=\{0,1,2,\dots,L-1\}$. As in the continuous case we assume the following. (i) The dynamical system f has a finite attractor. If the scheme is used for encoding information this attractor should be chaotic for $i=0$. (ii) The transmitter and the receiver synchronize, i.e., $\mathbf{y}(n)\rightarrow\mathbf{x}(n)$ for $n\rightarrow\infty$. (iii) The information i can be obtained uniquely from the equation for $s(n)$; i.e., there exists a function $i(n)=h^{-1}(\mathbf{x}(n),s(n),s(n+1))$. If the transmitter and the receiver synchronize the recovered information

$$i_R(n)=h^{-1}(\mathbf{y}(n),s(n),s(n+1))$$

converges to the original message i because $\mathbf{y}\rightarrow\mathbf{x}$.

Example 1: Continuous variables: In our first example, the equations of the transmitter read

$$x_m(n+1)=\alpha_m x_m(n)+\beta_m s(n)(\mathrm{mod}\ \ 1)$$

for $m=1,\dots,N$ where the transmitted signal $s(n+1)=h(\mathbf{x}(n),s(n),i(n))$ is given by

$$s(n+1)=s(n)+\sum_{m=1}^{N} x_m(n)+i(n)(\mathrm{mod}\ \ 1).$$

The range of the modulo function (mod 1) is $[0,1)$ and α_m,β_m are parameters (real numbers) such that $|\alpha_m|<1$ and $\beta_m>1$. The first condition $|\alpha_m|<1$ assures the synchronization between the transmitter and the receiver, while choosing $\beta_m>1$ we construct a hyperchaotic discrete dynamical system. In this case the transformation $i(n)=h^{-1}(\mathbf{x}(n), s(n),s(n+1))$ is given by

$$i(n)=s(n+1)-s(n)-\sum_{m=1}^{N} x_m(n)(\mathrm{mod}\ \ 1).$$

The equations of the receiver are

$$y_m(n+1)=\alpha_m y_m(n)+\beta_m s(n)(\mathrm{mod}\ \ 1)$$

for $m=1,\dots,N$. Using the error variable $\mathbf{e}=\mathbf{x}-\mathbf{y}$ the error dynamics may be described by

$$\begin{aligned} e_m(n+1)&=\alpha_m(x_m(n)-y_m(n))(\mathrm{mod}\ \ 1),\\ &=\alpha_m e_m(n)(\mathrm{mod}\ \ 1). \end{aligned}$$

Since $|\alpha_m|<1$, $e_m\rightarrow 0$. Therefore, the transmitter and the receiver synchronize globally, i.e., for all initial conditions. For $n\rightarrow\infty$ the information is recovered as

$$i_R(n)=s(n+1)-s(n)-\sum_{m=1}^{N} y_m(n)(\mathrm{mod}\ \ 1).$$

Note that for this example one can use any transformation h for $s(n+1)=h(\mathbf{x}(n),s(n),i(n))$ provided only that it can be inverted uniquely for $i(n)$ and yields a chaotic system for $i=0$.

Example 2: Discrete variables from a finite alphabet: For our second example we assume that the state variables of the transmitter and receiver, the information signal, and the transmitted signal are letters in some finite alphabet $\{0,1,2,\dots,L-1\}$. The equations of the transmitter are

$$\begin{aligned} x_1(n+1) &= s(n) && (\mathrm{mod}\ \ L),\\ x_m(n+1) &= x_{m-1}(n) && (\mathrm{mod}\ \ L) \end{aligned}$$

for $m=2,\dots,N$. The transmitted signal is given by

$$s(n+1)=\alpha_0 s(n)+\sum_{m=1}^{N} \alpha_m x_m(n)+i(n)(\mathrm{mod}\ \ L).$$

with $\alpha_0=14$, $\alpha_1=129$, $\alpha_2=35$, $\alpha_3=58$, $\alpha_4=24$, $\alpha_5=119$, $\alpha_6=25$, $\alpha_7=31$, $\alpha_8=55$, $\alpha_9=1$, $N=9$, and $L=251$. The receiver may be written as

$$\begin{aligned} y_1(n+1) &= s(n) && (\mathrm{mod}\ \ L),\\ y_m(n+1) &= y_{m-1}(n) && (\mathrm{mod}\ \ L), \end{aligned}$$

with $m=2,\dots,N$ and the recovered information is computed as follows:

$$i_R(n)=s(n+1)-\alpha_0 s(n)-\sum_{m=1}^{N} \alpha_m y_m(n)(\mathrm{mod}\ \ L).$$

The error dynamics is given by

$$\begin{aligned} e_1(n+1) &= 0 && (\mathrm{mod}\ \ L),\\ e_m(n+1) &= e_{m-1}(n) && (\mathrm{mod}\ \ L) \end{aligned}$$

for $m=2,\dots,N$ and it is easy to verify that, independently of the initial values of the state variables of the receiver, all error variables equal zero after N time steps. As a consequence, the recovered information signal $i_R(n)$ equals the original signal $i(n)$ for all $n\geqslant N$; i.e., the first N transmitted digits are arbitrary. Note that in contrast to the previous example, here perfect synchronization is achieved after a finite number of time steps. The main properties of this example are listed below:

(i) For $i=0$, this model is a pseudorandom generator. The choice of L and the other parameters determines the quality

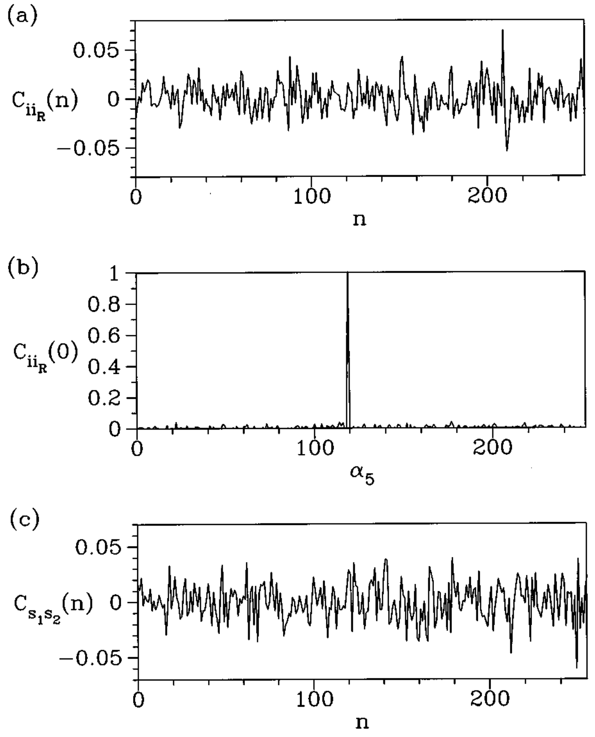

FIG. 9. Properties of the discrete communication scheme using variables from a finite alphabet (example 2). The values of the nonvanishing parameters are $\alpha_0=14$, $\alpha_1=129$, $\alpha_2=35$, $\alpha_3=58$, $\alpha_4=24$, $\alpha_5=119$, $\alpha_6=25$, $\alpha_7=31$, $\alpha_8=55$, and $\alpha_9=1$ where $N=9$ and $L=251$. The information signal $i(n)$ is given by a random sequence of integers from the set $\{0,\ldots,250\}$. (a) $C_{ii_R}(n)$ vs n. The values of the parameters in the receiver are the same as in the transmitter, except for $\alpha_6=26$. (b) $C_{ii_R}(0)$ vs α_5. The values of the other parameters in the receiver are the same as in the transmitter. (c) $C_{s_1 s_2}(n)$ for the same information but slightly different initial conditions. All values of the parameters in the receiver are the same as in the transmitter.

of the generator. For example, it is well known that it constitutes a "good" random number generator for $N=55$, $L=2^{32}$, $\alpha_7=\alpha_{15}=\alpha_{23}=\alpha_{54}=1$, and $\alpha_m=0$ for $m \neq 7,15,23,54$ [27]. This example also belongs to the class of linear self-synchronizing digital data scramblers [17].

(ii) Synchronization in this model is very sensitive to exact values of the parameters. Assume that the values of the parameters of the transmitter and the receiver are the same, except for one value, say α_m. In this case, it is easy to see that e_m will never tend to zero. For an information signal $i(n)$ that is given by a random sequence of integers from the set $\{0,\ldots,250\}$ we have numerically calculated the normalized cross covariance $C_{ii_R}(n)$ defined as

$$C_{XY}(n)=\frac{\sum_k [X(k)-\overline{X}][Y(k+n)-\overline{Y}]}{\sqrt{\sum_k [X(k)-\overline{X}]^2 \sum_k [Y(k)-\overline{Y}]^2}}.$$

Figure 9(a) shows $C_{ii_R}(n)$ versus n for the case that all the values of the parameters in the receiver are the same as in the transmitter, except for α_5. The original information $i(n)$ and the recovered message $i_R(n)$ are practically uncorrelated. To demonstrate the dependence on parameter mismatch Fig. 9(b) shows $C_{ii_R}(0)$ versus α_5. The values of the cross covariance are very small except for the case where the parameters of the transmitter and the receiver are exactly the same ($\alpha_5=119$).

(iii) The initial conditions of the state variables of the transmitter and the receiver can be chosen completely at random. If two initial conditions are different, then the transmitter generates two different signals $s_1(n)$ and $s_2(n)$ for the same information i. Let us denote the initial conditions for s_1 and s_2 by $\mathbf{x}^1(0)$ and $\mathbf{x}^2(0)$, respectively. Figure 9(c) shows $C_{s_1 s_2}(n)$ for $x_4^1(0)-x_4^2(0)=1$ and $x_m^1(0)=x_m^2(0)$, $m\neq 4$. In general, the transmitter may form as many different transmitted signals for the same information as different initial conditions (orbits) exist. Therefore, a given message may be encoded in this case in $L^N=251^{10}$ different ways.

Furthermore, this example may also be written as

$$s(n)=F(s(n-1),s(n-2),\ldots,s(n-N))+i(n)$$

and the receiver recovers the information then as

$$i_R(n)=s(n)-F(s(n-1),s(n-2),\ldots,s(n-N)).$$

In general any function $s(n)=F(s(n-1),s(n-2),\ldots,s(n-N),i(n))$ that generates a chaotic time series for $i=0$ and that is invertible with respect to i with $i=F^{-1}(s(n),s(n-1),s(n-2),\ldots,s(n-N))$ may be used in this way for encoding and decoding messages [26].

VI. CONCLUSION

In this paper we have discussed a general method for constructing (high-dimensional) synchronized chaotic systems. Furthermore, two improved encoding-decoding schemes were investigated that are both based on (chaotic) synchronization. The first encryption method allows us to recover the information signal exactly, and the second approach offers new features to design more robust communication systems based on synchronization. Numerical, experimental, and analytical examples of continuous and discrete systems were presented to illustrate the basic ideas and to indicate also possible directions of future research. For the (discrete) encryption methods we expect applications, for example, in *spread spectrum communication* [28] and *secret-key cryptography* [29]. The autosynchronization used for the second encryption method may also be applied to system identification and parameter estimation.

ACKNOWLEDGMENTS

The authors thank Professor W. Lauterborn, T. Kurz, and R. Mettin for support and stimulating discussions and thank G. Kirschmann-Schröder for her kind assistance with the photographs. L.K. thanks the DAAD for financial support. This work was also supported in part by the Macedonian Ministry of Science and the DFG (SFB 185).

[1] L. Pecora and T. Carroll, Phys. Rev. Lett. **64**, 821 (1990); T.L. Carroll and L.M. Pecora, IEEE Trans. Circuits Syst. **38**, 453 (1991); Int. J. Bifurcation Chaos **2**, 659 (1992); Physica D **67**, 126 (1993); T.L. Carroll, Phys. Rev. E **50**, 2580 (1994).

[2] H. Fujisaka and T. Yamada, Prog. Theor. Phys. **69**, 32 (1983).

[3] T. Sugawara, M. Tachikawa, T. Tsukamoto, and T. Shimizu, Phys. Rev. Lett. **72**, 3502 (1994).

[4] R. He and P.G. Vaidya, Phys. Rev. A **46**, 7387 (1992).

[5] I.I. Blekhman, P.S. Landa, and M.G. Rosenblum, Appl. Mech. Rev. **48**, 733 (1995).

[6] J.K. John and R.E. Amritka, Phys. Rev. E **49**, 4843 (1994).

[7] K. Murali and M. Lakshmanan, Phys. Rev. E **49**, 4882 (1994).

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

[9] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos **2**, 709 (1992).

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

[11] K. Murali and M. Lakshmanan, Phys. Rev. E **48**, R1624 (1993).

[12] K.S. Halle, C.W. Wu, M. Itoh, and L.O. Chua, Int. J. Bifurcation Chaos **3**, 469 (1993).

[13] C.W. Wu and L.O. Chua, Int. J. Bifurcation Chaos **3**, 1619 (1993).

[14] L. Kocarev and U. Parlitz, in *Proceedings of Nonlinear Dynamics of Electronic Systems, Krakow, Poland, 29–30 July 1994)* (University of Mining and Metallurgy, Krakow, Poland, 1994).

[15] L. Kocarev and T. Stojanovski, IEICE Trans. Fundamentals **E78-A**, 1142 (1995).

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

[17] J.E. Savage, Bell Syst. Tech. J. **46**, 449 (1967).

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

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

[20] A. Hübler and E. Lüscher, Naturwissenschaften **76**, 67 (1989); E. Jackson and A. Hübler, Physica D **44**, 407 (1990).

[21] R. Mettin, Phys. Rev. E **51**, 4065 (1995).

[22] K. Pyragas, Phys. Lett. A **181**, 203 (1993); A. Kittel, K. Pyragas, and R. Richter, Phys. Rev. E **50**, 262 (1994).

[23] R. Brown, N.F. Rulkov, and E.R. Tracy, Phys. Rev. E **49**, 3784 (1994); Phys. Lett. A **194**, 71 (1994).

[24] U. Parlitz, Phys. Rev. Lett. **7b**, 1232 (1996); U. Parlitz and L. Kocarev, Int. J. Bifurcation Chaos (to be published).

[25] P. Grassberger, R. Hegger, H. Kantz, C. Schaffrath, and T. Schreiber, CHAOS **3**, 127 (1993).

[26] J.B. Kadtke and J.S. Brush, in *Proceedings of the 38th Symposium on Optical Instrumentation and Applied Engineering, San Diego, CA. 1993*, edited by L. M. Pecora, SPIE Prod. Vol. 2038 (SPIE, Bellingham, WA, 1994).

[27] P. Grassberger, Phys. Lett. A **181**, 43 (1993).

[28] R.L. Pickholtz, D.L. Schilling, and L.B. Milstein, IEEE Trans. Commun. **30**, 855 (1982).

[29] J.L. Massey, Proc. IEEE **76**, 533 (1988).