

Spread Spectrum Modulation and Signal Masking Using Synchronized Chaotic Systems

RLE Technical Report No. 570

Kevin M. Cuomo,¹ Alan V. Oppenheim, and Steven H. Isabelle

February 1992

**Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139-4307**

This work was supported in part by the Air Force Office of Scientific Research under Grant AFOSR-91-0034-A and in part by a subcontract from Lockheed Sanders, Inc., under the U.S. Navy Office of Naval Research Contract N00014-91-C-0125.

¹Supported by the MIT Lincoln Laboratory Staff Associate Program, Lexington, Massachusetts 02173.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE FEB 1992		2. REPORT TYPE		3. DATES COVERED 00-02-1992 to 00-02-1992	
4. TITLE AND SUBTITLE Spread Spectrum Modulation and Signal Masking Using Synchronized Chaotic Systems				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Massachusetts Institute of Technology, Research Laboratory of Electronics, 77 Massachusetts Avenue, Cambridge, MA, 02139-4307				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 44	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Abstract

Chaotic dynamical systems are nonlinear deterministic systems which often exhibit erratic and irregular behavior. The signals that evolve in these systems are typically broadband, noise-like and similar in many respects to a stochastic process. Because of these properties chaotic signals potentially provide an important class of signals which can be utilized in various communications, radar and sonar contexts for masking information-bearing waveforms and as modulating waveforms in spread spectrum systems.

Recently, it has been demonstrated that the chaotic Lorenz and Rössler systems can be decomposed into a drive system and a stable response subsystem which will synchronize when coupled with a common drive signal. This property has several practical applications and suggests novel approaches to secure communication and signal masking. In addition to the Lorenz and Rössler systems, we discuss and demonstrate that the continuous-time Double Scroll system and discrete-time Henon map are also decomposable into synchronizing subsystems. We then propose and explore in a preliminary way how synchronized chaotic systems can be used for spread spectrum communication and for various signal masking purposes.

Contents

1	Introduction	1
2	Synchronization in Chaotic Systems	3
2.1	Chaotic System Decomposition and Synchronization	3
2.2	Continuous-Time Systems	5
2.2.1	The Lorenz System	5
2.2.2	The Rössler System	8
2.2.3	The Double Scroll	12
2.3	Discrete-Time Henon Map	13
3	Applications to Spread Spectrum and Signal Masking	19
3.1	Spread Spectrum Communication	19
3.1.1	Whitening Filter	22
3.1.2	Modulator/Demodulator	25
3.1.3	Simulation	30
3.2	Chaotic Signal Masking	30
4	Summary and Conclusions	35

List of Figures

1	Decomposition of a Chaotic Dynamical System	4
2	Lorenz Chaotic Attractor and Waveforms	7
3	Synchronization of Drive and Response Signals in Lorenz System	9
4	Rössler Chaotic Attractor and Waveforms	11
5	Synchronization of Drive and Response Signals in Rössler System	12
6	Double Scroll Chaotic Attractor and Waveforms	14
7	Synchronization of Drive and Response Signals in Double Scroll System	15
8	Three-Dimensional Henon Map Chaotic Attractor and Waveforms	17
9	Synchronization of Drive and Response Signals in Henon Map	18
10	Chaotic Spread Spectrum System	21
11	Chaotic Signal Whitening	23
12	A PDF for a Chaotic Spreading Waveform	26
13	Direct Sequence Modulation Using Chaotic Signals	27
14	Experimental PDF's	28
15	A Modulator/Demodulator Based on Synchronized Chaotic Signals	29
16	Simulation of a Chaotic Spread Spectrum System	31
17	Simulated Power Spectra	32
18	Chaotic Signal Masking System	33
19	Speech Waveforms: Original, Transmitted, and Recovered	34

1 Introduction

The signals that evolve in chaotic dynamical systems form a highly structured set in the system's state space. However, scalar observations often appear unstructured and exhibit a broad Fourier spectrum. Chaotic systems are characterized by a "sensitive dependence on initial conditions" and have at least one positive Lyapunov exponent. Thus, long-term predictability of chaotic signals is difficult at best since small uncertainties in the initial state of the system will be exponentially amplified. The limiting trajectories of a chaotic system are attracted to a region in state space which forms a set having fractional dimension and zero volume. Furthermore, all trajectories on this limiting set are locally unstable, yet remain bounded within some region of the system's state space. These sets are termed "strange attractors" [Ruelle and Takens, 1971] and are composed of an infinite complex of surfaces packed closely together [1].

These characteristics of a nonlinear system would seem to defy synchronization, which, if true, would produce unattractive models for signal processing or communication applications. However, as recently reported by Pecora and Carroll [2, 3], chaotic systems which can be decomposed into a drive system and a stable response subsystem will synchronize if they are coupled with a common drive signal. Specifically, if several independent copies of the response subsystem are each linked to the drive system by a common drive signal, then the state space trajectories of the individual subsystems will synchronize to each other and to the state space trajectory of the drive system.

The combination of apparent stochastic behavior, unpredictability, and synchronizability from a purely deterministic system suggests novel approaches to secure communication. The ability to synchronize remote systems through the use of a common drive signal provides the potential for coherent communication over noisy channels. In particular, the seemingly random and aperiodic nature of chaotic signals can make the information they carry difficult to detect and exploit without knowledge of the transmitter characteristics and parameters.

In this report we propose and explore in a preliminary way, various applications in which synchronization in chaotic systems can be exploited in signal processing and communications. Specifically, we consider both continuous-time (CT) and discrete-time (DT) chaotic signals and systems for spread spectrum communication and for chaotic signal masking.

2 Synchronization in Chaotic Systems

In this section, we provide a brief outline of the theory of chaotic system decomposition and synchronization [2, 3]. Then we apply this theory to three continuous-time (CT) chaotic systems and the discrete-time (DT) Henon map. In each case, the CT chaotic systems will be represented by a set of p first order ordinary differential equations of the form, $\dot{\mathbf{x}} = \mathbf{F}(\mathbf{x})$. Similarly, the DT chaotic system will be represented by a set of p first order difference equations of the form, $\mathbf{x}_{n+1} = \mathbf{F}(\mathbf{x})$. Since $\mathbf{F}$ does not depend explicitly on time, these systems are autonomous.

2.1 Chaotic System Decomposition and Synchronization

The general theory of decomposing a chaotic system into a drive and response subsystem has been reported by Pecora and Carroll [2, 3]. We provide only a brief outline of these ideas so that the reader will understand our approach.

The basic idea is to decompose $\dot{\mathbf{x}} = \mathbf{F}(\mathbf{x})$ into drive and response subsystems, i.e. to express it in the form

$$\dot{\mathbf{d}}_1 = \mathbf{D}_1(\mathbf{d}_1, \mathbf{d}_2) \quad (1)$$

$$\dot{\mathbf{d}}_2 = \mathbf{D}_2(\mathbf{d}_1, \mathbf{d}_2) \quad (2)$$

In (1) the vector $\mathbf{d}_1$ is q -dimensional and in (2) the vector $\mathbf{d}_2$ is $(p - q)$ -dimensional. In this form (2) will be referred to as the response with drive input $\mathbf{d}_1$. A second response subsystem is formed by duplicating the set of states corresponding to the $\mathbf{D}_2$ subsystem and replacing the variables $\mathbf{d}_2$ by new variables $\mathbf{r}$. This leads to a response subsystem of the form

$$\dot{\mathbf{r}} = \mathbf{D}_2(\mathbf{d}_1, \mathbf{r}) \quad (3)$$

Viewed as a single system, equations (1) and (2) can be interpreted as a chaotic drive system with (3) forming a response subsystem which is driven by the chaotic signals

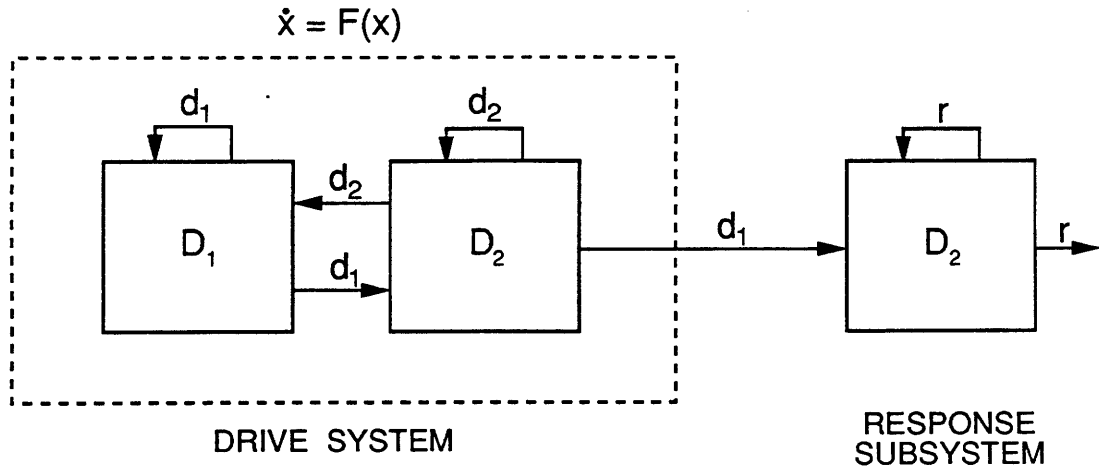


Figure 1: Decomposition of a Chaotic Dynamical System

d_1 . Figure 1 illustrates the drive decomposition and response augmentation procedure. Although the drive and response subsystems are coupled through the signals d_1 , the dynamics of the drive system are not influenced by the response subsystem. This allows for independent copies of the response subsystem to be constructed with each coupled to the drive system through the variables d_1 . Pecora and Carroll have shown that under chaotic driving and with certain stability conditions, the independent copies of the response subsystem will robustly synchronize to each other and to the drive system variables d_2 defined in (2). Several practical consequences of this property are discussed in Section 3. A condition for the synchronization of the drive and response subsystems is discussed below.

Synchronization of the drive system and response subsystem can be studied by first forming the incremental system $\mathbf{v} = \mathbf{r} - \mathbf{d}_2$ and then considering the conditions under which $|\mathbf{v}| = |\mathbf{r} - \mathbf{d}_2| \rightarrow 0$ as $t \rightarrow \infty$. In the limit of small $\mathbf{v}$ the linearized system becomes,

$$\dot{\mathbf{v}} = J(\mathbf{d}_1, \mathbf{r})\mathbf{v}$$

where $J(\mathbf{d}_1, \mathbf{r}) = \partial \mathbf{D}_2(\mathbf{d}_1, \mathbf{r})$ is the Jacobian matrix of the response subsystem with re-

spect to the response variables. A condition for synchronization is that $J(\mathbf{d}_1, \mathbf{r})$ have conditional Lyapunov exponents which are all negative. The term conditional is applied because in general $J(\mathbf{d}_1, \mathbf{r})$ depends on the drive signal $\mathbf{d}_1$, which in our case is also assumed to be chaotic. Typically, an analytical determination of the conditional Lyapunov exponents is not possible and numerical approaches, such as the QR decomposition method of Eckmann and Ruelle [4], are necessary to calculate them. The results given here are phrased in the context of CT systems, but apply with a minor variation, to DT systems.

2.2 Continuous-Time Systems

In this subsection we describe the behavior of three CT chaotic systems which are drive decomposable and can be augmented with synchronizing response subsystems. Specifically, we will consider the Lorenz, Rössler, and Double Scroll systems. Each of these systems has a three-dimensional state space.

2.2.1 The Lorenz System

A well-known example of a system which can behave chaotically is the Lorenz system which arises in the study of thermal convection [1]. This system is represented by

$$\begin{aligned}\dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz\end{aligned}\tag{4}$$

where σ, r , and b are positive constant parameters of the system. Many researchers have investigated the behavior of this system over a wide range of parameter values. We choose to operate in the chaotic regime and adopt the values $\sigma = 16, b = 4$, and $r = 45.92$ as studied in [2].

To study the behavior of (4) numerical integration was performed using a fourth-order Runge-Kutta method with a fixed step size of .002. The integrations were computed for

7500 time steps (15 s) and the first 2500 points were discarded to ensure that the trajectories have converged to the attractor. The resulting chaotic attractor projected onto the xy -plane and the waveforms $x(t)$, $y(t)$, and $z(t)$ are shown in figures 2(a) through 2(d), respectively. The waveforms are broad-band and unpredictable, whereas the state space projection is highly structured.

The Lorenz system can be augmented with a pair of states that are duplicates of (x, z) to form a stable response subsystem. These augmented states form the (x', z') response subsystem, which is represented by

$$\begin{aligned}\dot{x}' &= \sigma(y - x') \\ \dot{z}' &= x'y - bz'\end{aligned}$$

The original system (4) can be viewed as the drive system since its dynamics are independent of the response subsystem (x', z') . The signal $y(t)$ serves the purpose of a driving or coupling signal between the drive and response systems. We assume that the constant b has the same value in both the drive and response. By a straightforward calculation, we find that the eigenvalues of the Jacobian matrix for the response subsystem are equal to $(-b, -\sigma)$, and consequently are constant real valued quantities, independent of the drive signal $y(t)$. In this case, the eigenvalues correspond to the conditional Lyapunov exponents and since they are both negative we should expect that $|x' - x|$ and $|z' - z| \rightarrow 0$ exponentially fast. This is in fact the case, as has been shown empirically.

By a similar augmentation procedure, a second stable response subsystem can be constructed, specifically (y', z') driven by $x(t)$. This subsystem is represented by

$$\begin{aligned}\dot{y}' &= rx - y' - xz' \\ \dot{z}' &= xy' - bz'\end{aligned}$$

Once again, we assume that the constants r and b have the same values in both the drive and response subsystems. Calculation of the Lyapunov exponents for the (y', z') subsystem is not as analytically straightforward as those for (x', z') since in this case

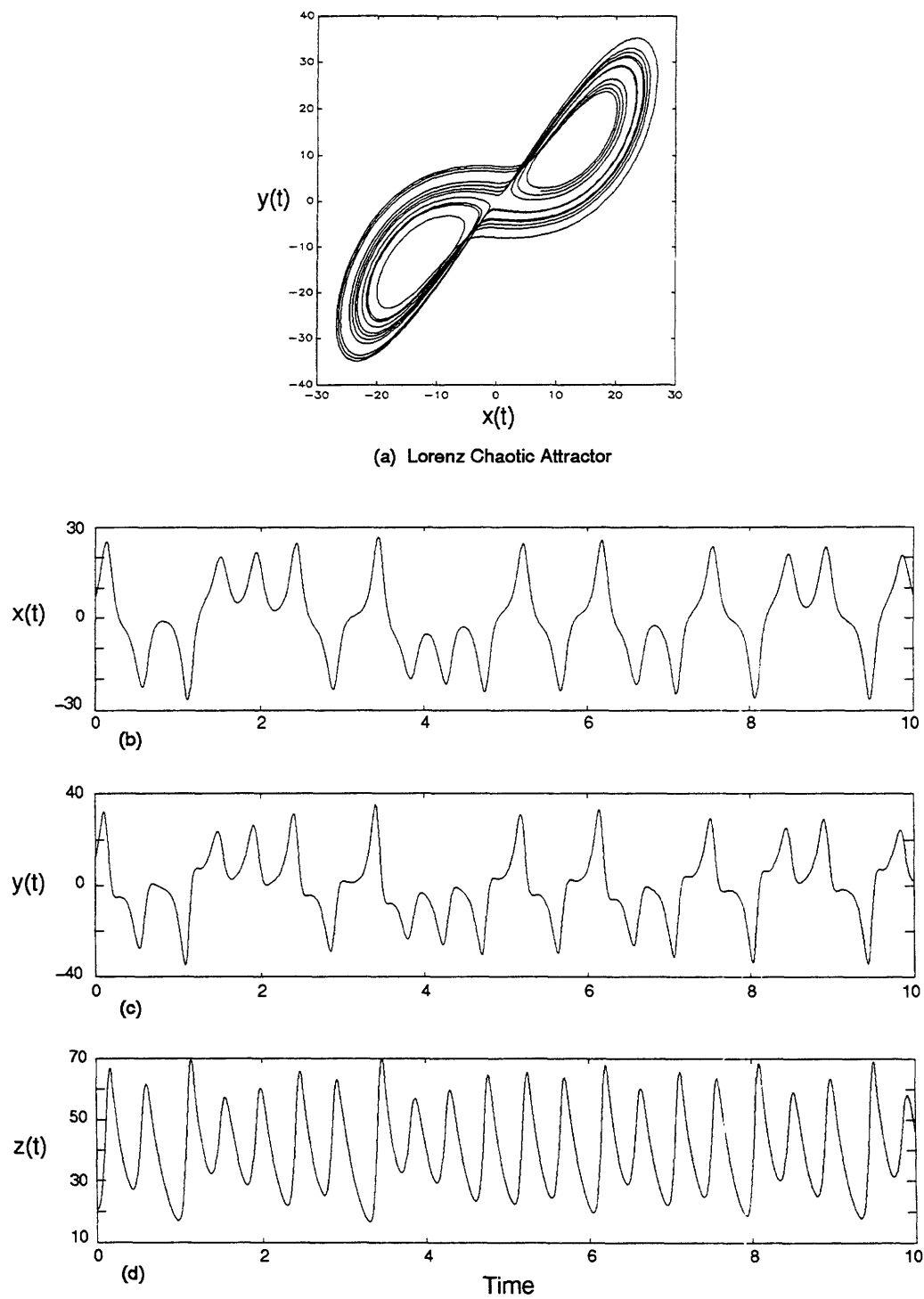


Figure 2: Lorenz Chaotic Attractor and Waveforms

they depend on the drive signal $x(t)$. Numerical estimates for the exponents equal to $(-2.5, -2.5)$ were obtained using the QR decomposition method of Eckmann and Ruelle [2, 4]. Consequently, we expect that this subsystem should also synchronize to the drive exponentially fast.

As an illustration of this synchronization behavior, consider figures 3(a) and 3(b), which show a comparison between the (x, z) drive signals (solid curves) and the zero-state (ZS) response of the (x', z') subsystem (dashed curves) when driven by $y(t)$. Similarly, figures 3(c) and 3(d) show a comparison between the (y, z) drive signals and the ZS response of the (y', z') subsystem when driven by $x(t)$. In both cases, rapid synchronization of the drive and response signals is apparent. It should be noted that synchronization of the response subsystems to the drive signals is achieved over a wide range of initial conditions, and once obtained, appears to be stable. In section 3, we will present some interesting communication and signal processing applications of this nonlinear dynamical behavior.

A third response subsystem is possible, specifically (x', y') driven by $z(t)$, but it always appears to be unstable, as evidenced by the positive values of at least one conditional Lyapunov exponent. We have also confirmed empirically that the (x', y') subsystem does not synchronize to the drive system when driven by $z(t)$.

2.2.2 The Rössler System

The Rössler system is another example of a CT chaotic system which can be augmented with a set of states to form a stable response subsystem which synchronizes to the drive. The Rössler system is represented by

$$\begin{aligned}\dot{x} &= -y - z \\ \dot{y} &= x + ay \\ \dot{z} &= b + z(x - c)\end{aligned}\tag{5}$$

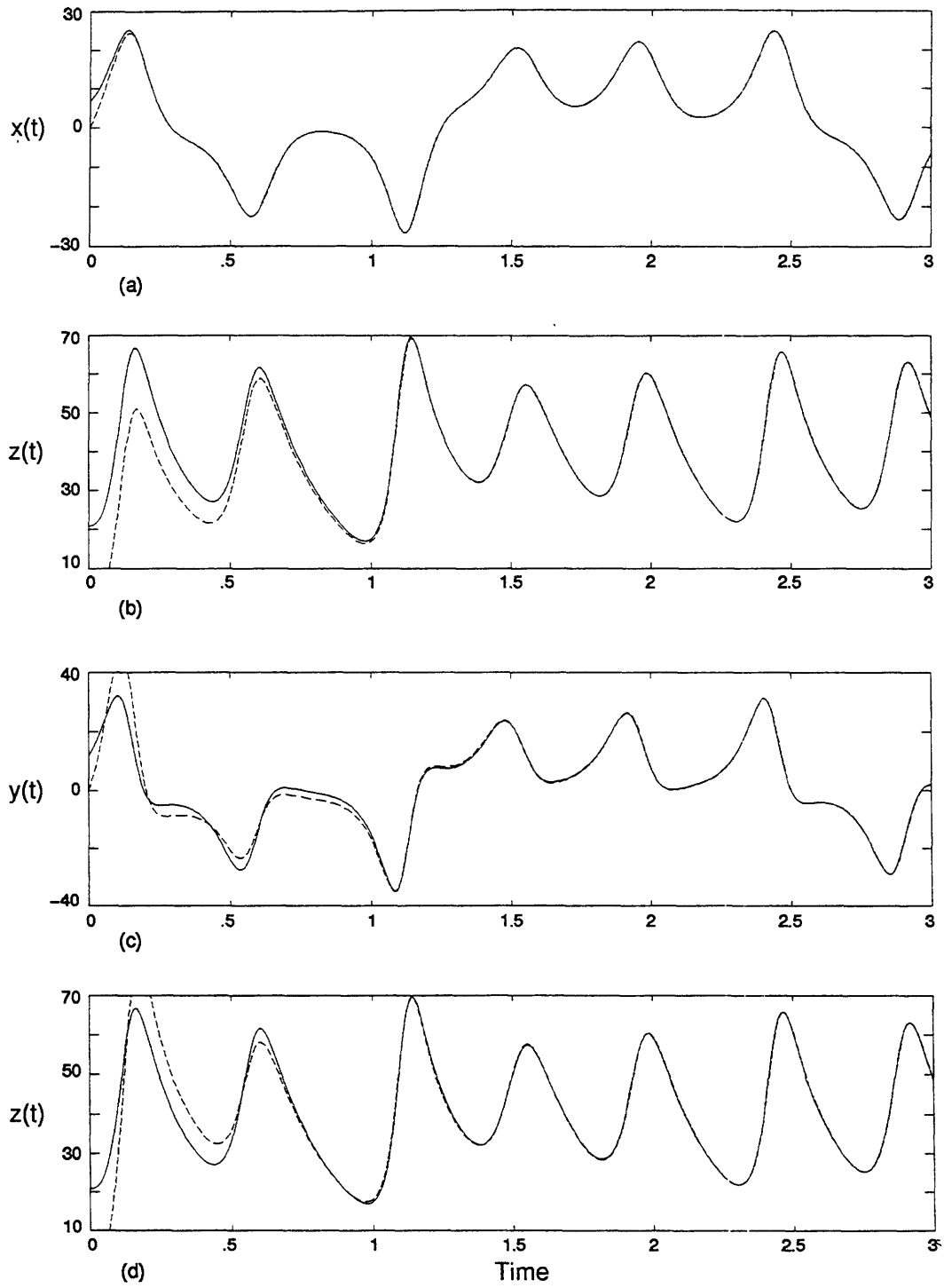


Figure 3: Synchronization of Drive and Response Signals in Lorenz System

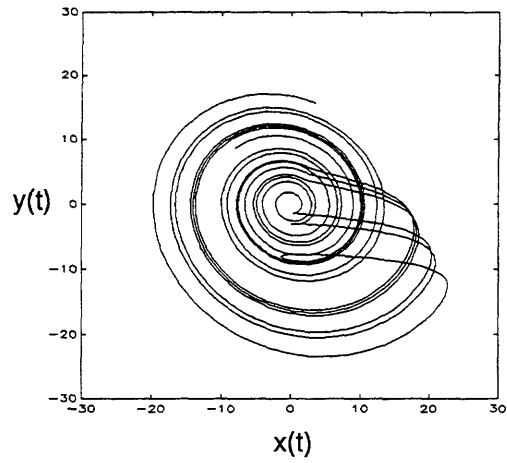
where a, b , and c are positive constant parameters of the system. The Rössler system is perhaps the simplest example of a CT chaotic system, as it has minimum dimension, two of the states are governed by linear equations, and there is only a single quadratic nonlinearity. Still, this system can behave chaotically for certain parameter values. We choose the values $a = .2, b = .2$, and $c = 11$ which place the operation of this system in a chaotic regime.

Numerical integration of the Rössler system (5) was computed for 7500 time steps (150 s) with a fixed step size of .02. The first 2500 points were discarded to ensure that the trajectories have converged to the attractor. The resulting chaotic attractor projected onto the xy -plane is shown in figure 4(a). The aperiodic and broad-band behavior of this system is more clearly illustrated in figures 4(b) through 4(d), which show the waveforms $x(t), y(t)$, and $z(t)$, respectively.

By augmenting the Rössler system with a pair of states that are duplicate copies of (x, z) , a stable response subsystem, (x', z') , is obtained. The (x', z') subsystem is represented by

$$\begin{aligned}\dot{x}' &= -y - z' \\ \dot{z}' &= b + z'(x' - c)\end{aligned}$$

where the parameters b and c are assumed to have the same values in both the drive and response subsystems. The values of the conditional Lyapunov exponents for this subsystem are both negative. Thus, the response subsystem is expected to synchronize with the drive system. As an illustration, figures 5(a) and 5(b) show a comparison between the (x, z) drive signals and the ZS response of the (x', z') subsystem when driven by $y(t)$. It is quite apparent that synchronization is achieved. However, the time scale for the synchronization to occur is about five times slower than for the Lorenz system. Experiment has also shown that the other possible response subsystems are unstable since they have at least one positive Lyapunov exponent and do not synchronize to the drive.



(a) Rössler Chaotic Attractor

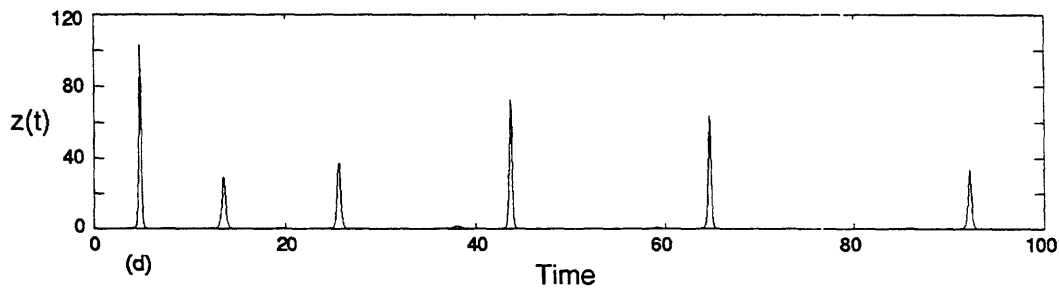
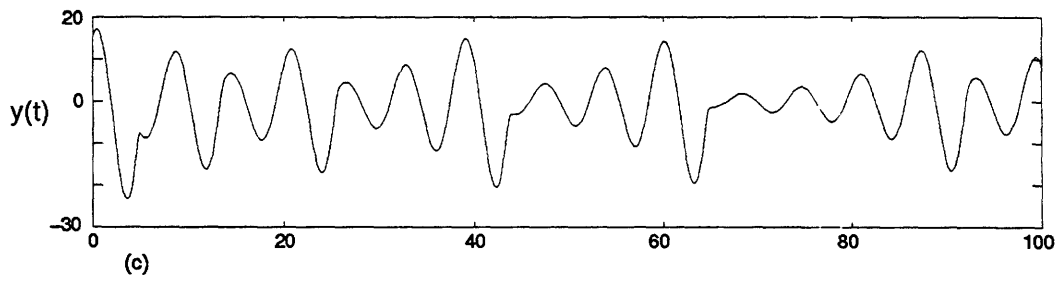
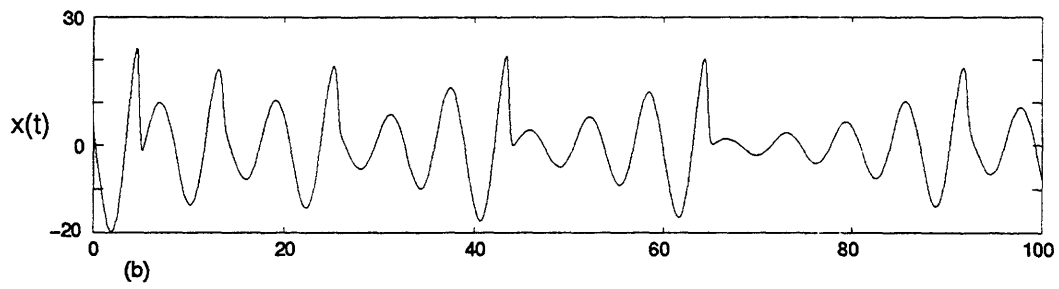


Figure 4: Rössler Chaotic Attractor and Waveforms

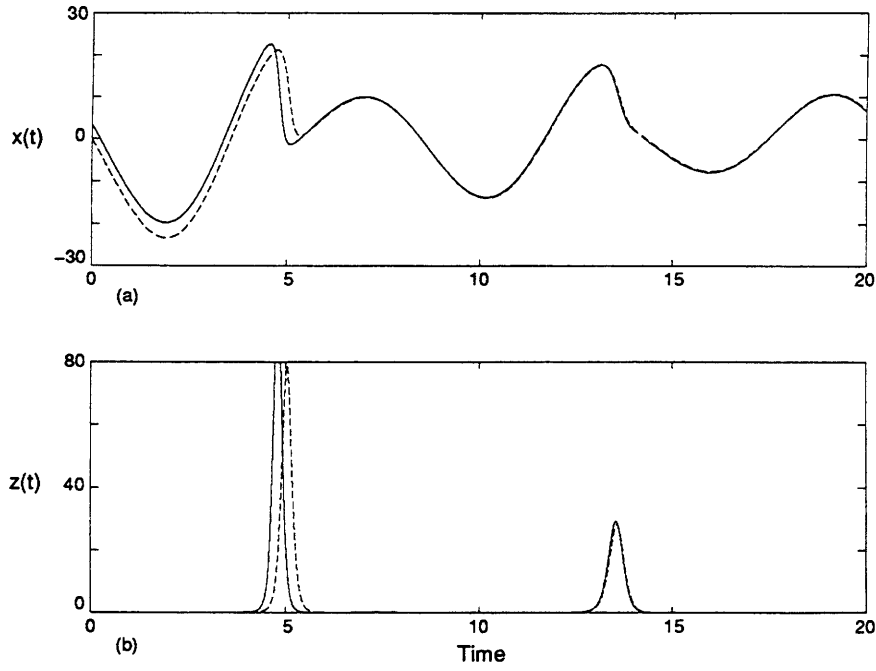


Figure 5: Synchronization of Drive and Response Signals in Rössler System

2.2.3 The Double Scroll

The Double scroll equations [5] provide a third example of a CT chaotic system which can be augmented with a pair of states to form a stable response subsystem. The double scroll equations are represented by

$$\begin{aligned}\dot{x} &= \alpha(y - h(x)) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y\end{aligned}\tag{6}$$

where $h(x)$ is the piecewise linear function

$$h(x) = \begin{cases} a_1x + (a_0 - a_1) & x \geq 1 \\ a_0x & -1 \leq x \leq 1 \\ a_1x - (a_0 - a_1) & x \leq -1 \end{cases}$$

These equations describe the dynamics of a simple electronic circuit, the chaotic behavior of which has been studied extensively [6, 7]. For the parameter values that we have chosen, $\alpha = 9$, $\beta = 100/7$, $a_0 = -1/7$, and $a_1 = 2/7$, chaotic solutions result.

Numerical integrations of the double scroll system (6) were computed for 7500 time steps (150 s) with a fixed step size of .02. The first 2500 points were discarded to ensure that the trajectories have converged to the attractor. The resulting chaotic attractor projected onto the xz -plane is shown in figure 6(a). The waveforms $x(t)$, $y(t)$, and $z(t)$ are shown in figures 6(b) through 6(d) respectively. By augmenting the double scroll system (6) with a pair of states that are duplicates of (y, z) we have found that a stable response subsystem, (y', z') results. The (y', z') subsystem is represented by

$$\begin{aligned}\dot{y}' &= x - y' + z' \\ \dot{z}' &= -\beta y'\end{aligned}$$

The conditional Lyapunov exponents for this subsystem are independent of the drive signal $x(t)$ and can be determined analytically to be equal to $(-1/2, -1/2)$. Thus, we expect that (y', z') will synchronize to the drive variables (y, z) . This is confirmed by figures 7(a) and 7(b) which show a comparison between the (y, z) drive signals and the ZS response of the (y', z') subsystem when driven by $x(t)$. Synchronization of the drive and response signals is achieved on a time scale which is similar to that of the Rössler system but which is about five times slower than the Lorenz system.

2.3 Discrete-Time Henon Map

The classical two-dimensional Henon map displays a broad spectrum of nonlinear dynamical behavior, such as, bifurcations, strange attractors, and fractal dimension. This DT dynamical system is represented by

$$\begin{aligned}x[n+1] &= 1 + y[n] - \alpha x^2[n] \\ y[n+1] &= bx[n]\end{aligned}$$

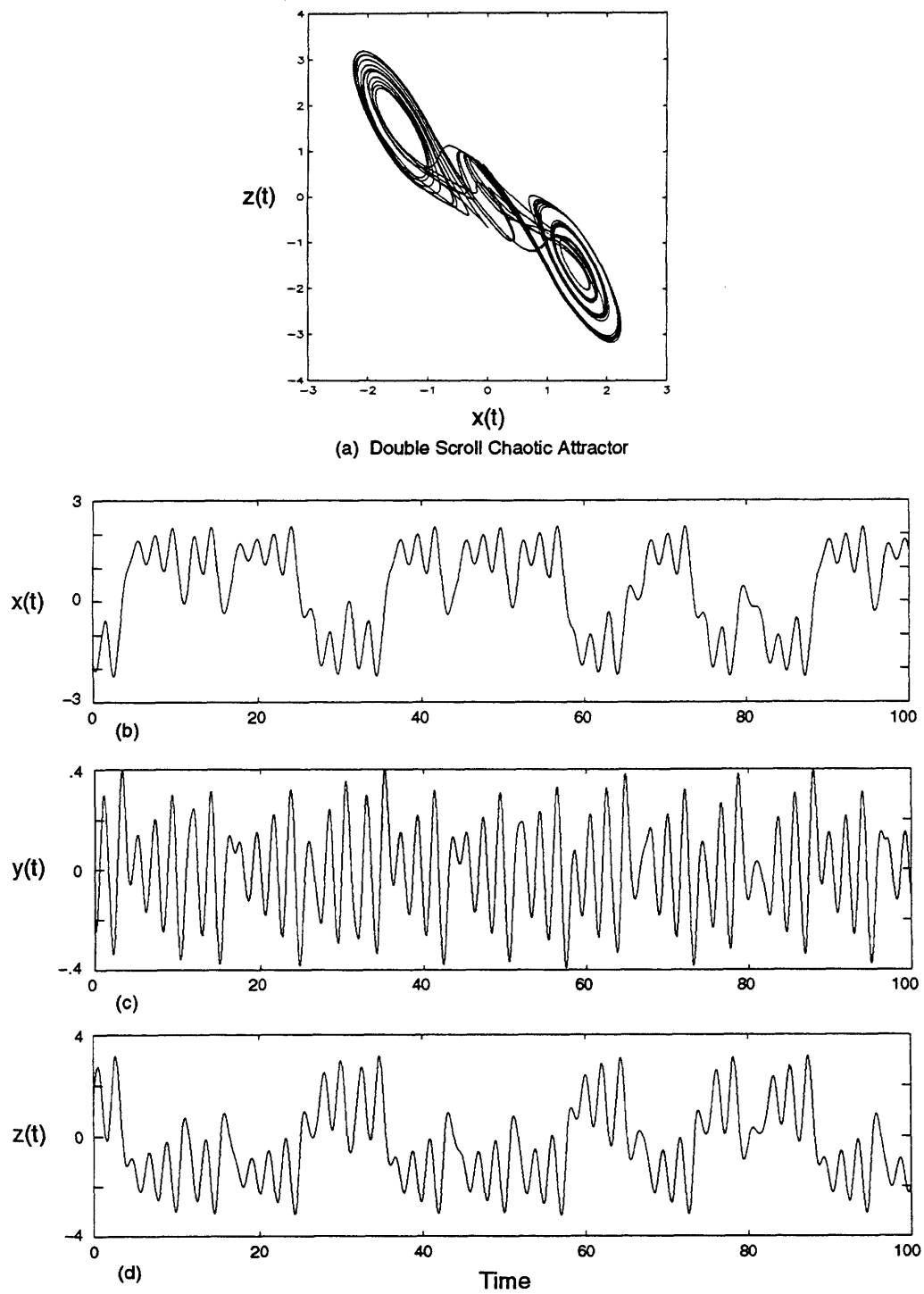


Figure 6: Double Scroll Chaotic Attractor and Waveforms

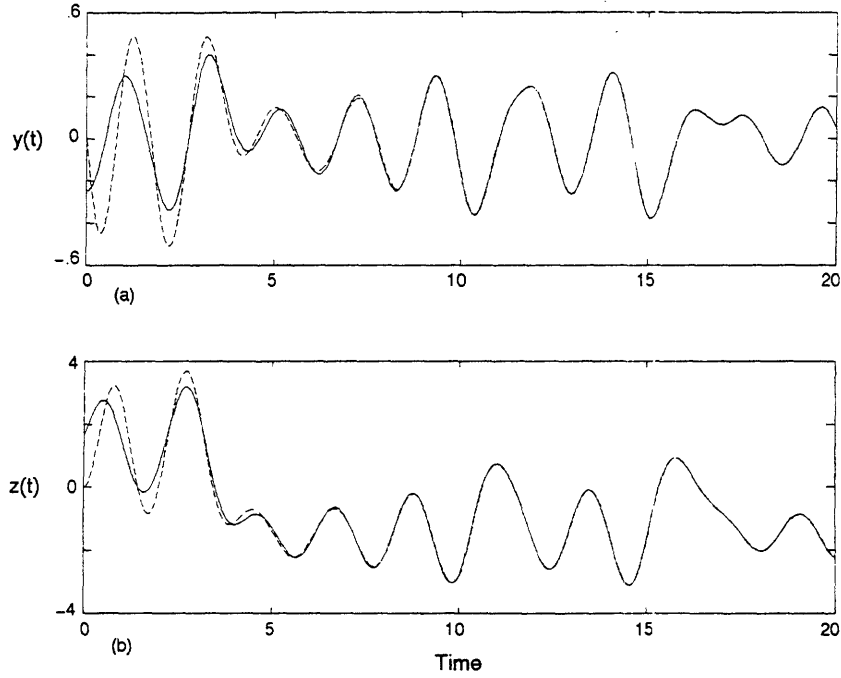


Figure 7: Synchronization of Drive and Response Signals in Double Scroll System

and defines a mapping of the plane R^2 into itself. Although this system is two-dimensional and has only a single nonlinear term, it can display incredibly complicated dynamics.

The state augmentation procedures, discussed in Section 2.1, when applied to the two-dimensional Henon map do not yield stable response subsystems. However, the two-dimensional Henon map has been modified to three-dimensions [8] by replacing the parameter α by a variable gain term $z[n]$ and driving $z[n]$ with $x[n]$. The modified three-dimensional Henon map is represented by

$$\begin{aligned}
 x[n+1] &= 1 + y[n] - z[n]x^2[n] \\
 y[n+1] &= bx[n] \\
 z[n+1] &= z[n] - 1/2 + \beta x^2[n]
 \end{aligned} \tag{7}$$

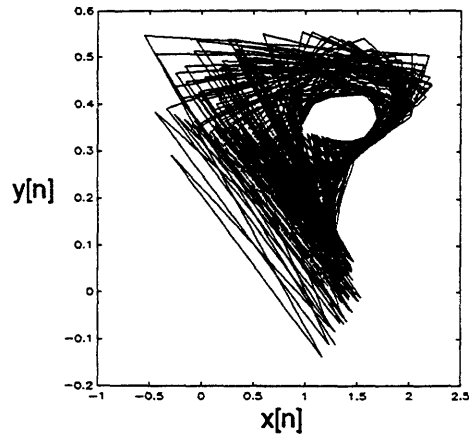
Several important points regarding (7) are worth noting. First, both the two-dimensional and three-dimensional representations depend on only two parameters. The parameter b controls the amount of dissipation per iteration in both systems. Thus, a constant

rate of area contraction is preserved in the three-dimensional mapping. In the three-dimensional system, the parameter β controls the amount of nonlinear coupling from the z component. Varying β produces a wide range of nonlinear dynamical behavior. To operate in a chaotic regime we have chosen the values $b = .25$ and $\beta = .279$. Other parameter values would also produce chaotic behavior. However, the above values also lead to a stable response subsystem. As an illustration, figures 8(a) through 8(d) show the chaotic attractor and DT sequences $x[n]$, $y[n]$, and $z[n]$ which were obtained by iterating the map for 2000 time steps and discarding the first 1000 points. Note that the DT sequences are similar in appearance to a random process and possess a broad Fourier spectrum.

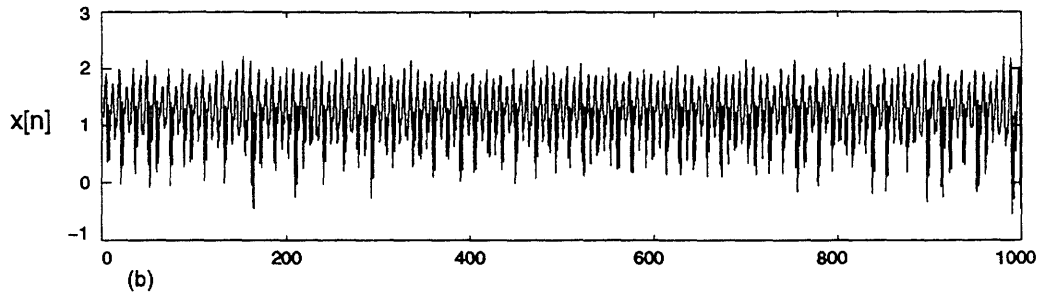
We have found that the three-dimensional Henon map can be augmented with a pair of states to form a stable response subsystem. This subsystem is represented by

$$\begin{aligned}x'[n+1] &= 1 + y'[n] - z[n]x'^2[n] \\ y'[n+1] &= bx'[n]\end{aligned}$$

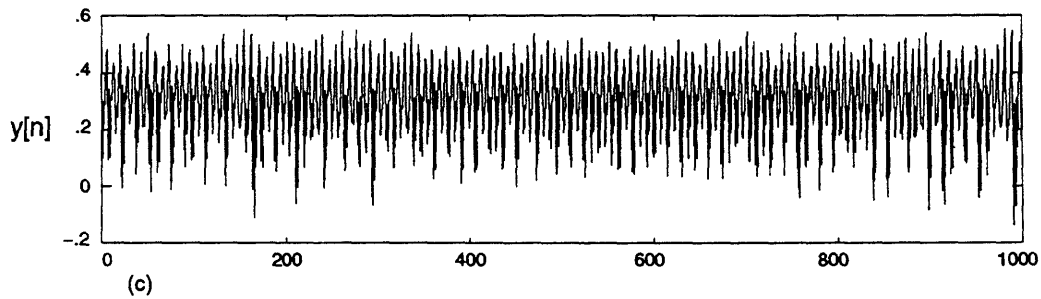
where the augmented pair of states (x', y') are driven by $z[n]$. The conditional Lyapunov exponents of this system are approximately $(-.57, -.82)$. Since they are both negative we expect that the response subsystem will synchronize to the drive exponentially fast. This behavior has been confirmed empirically as figures 9(a) and 9(b) indicate. Again the rapid synchronization is apparent between the drive variables and the ZS response of the response subsystem. Furthermore, the synchronization is robust and stable from a wide range of initial conditions.



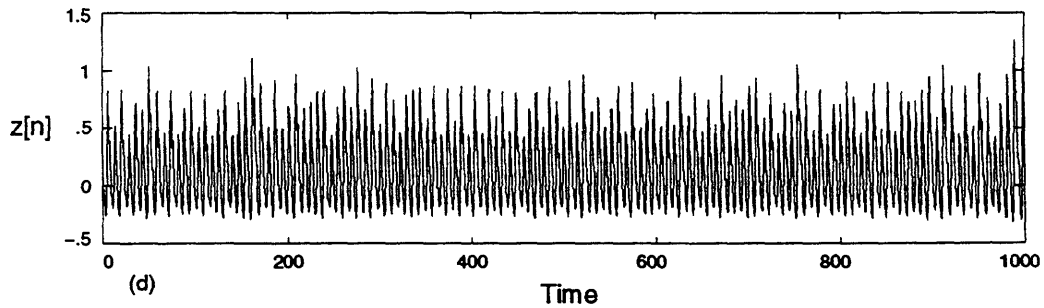
(a) Three-Dimensional Henon Map Chaotic Attractor



(b)



(c)



(d)

Time

Figure 8: Three-Dimensional Henon Map Chaotic Attractor and Waveforms

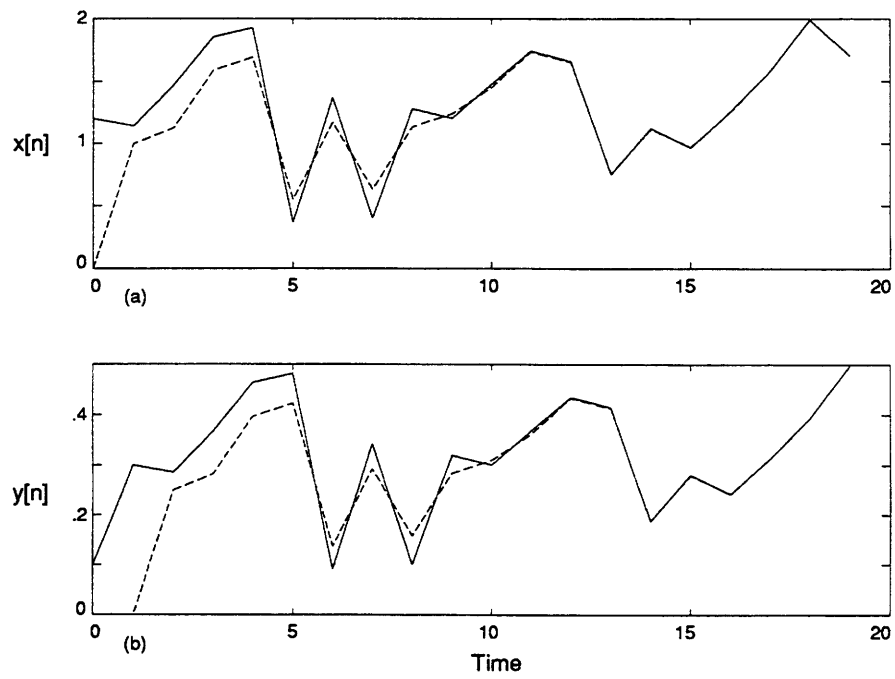


Figure 9: Synchronization of Drive and Response Signals in Henon Map

3 Applications to Spread Spectrum and Signal Masking

Because chaotic signals are typically broadband and noise-like, they potentially provide a class of signals which can be utilized in various communications, radar and sonar contexts for masking information-bearing signals and as modulating waveforms in spread spectrum systems [9]. A particularly intriguing approach is suggested by exploiting the synchronizing characteristics of certain classes of chaotic dynamical systems. We are actively exploring a number of ways in which this synchronization property can be used in spread spectrum communication systems and for various signal masking purposes.

3.1 Spread Spectrum Communication

A major goal of a spread spectrum (S^2) communication system is to protect communication signals against interference and exploitation by unintended listeners. In some contexts it is important that the unintended listener not be able to determine whether a communication signal is present or not. This requires the communication signals to have a low probability of detection (LPD), and are commonly referred to as LPD signals. A somewhat separate requirement is for the communication signals to have a low probability of intercept (LPI). LPI signals may be detectable, but extracting features from them is difficult. Often both LPD and LPI capabilities are desired [10].

To achieve these objectives, a S^2 system usually operates with a communication bandwidth, B , which is much wider than the message bandwidth. Since a bit interval of T seconds results in a message bandwidth of approximately $1/T$ Hz, the communication bandwidth consists of approximately BT nonoverlapping signal intervals. Different S^2 modulation strategies can utilize this wide communication bandwidth to create uncertainty about the presence of a signal in different ways. For example, Frequency Hopping (FH) involves shifting all of the signal energy among the BT nonoverlapping signal in-

tervals in an unpredictable but deterministic way. Without knowledge of the hopping algorithm or strategy, an unintended listener will have difficulty staying tuned to the correct signal interval and this will result in a poor intercept SNR. However, FH signals may be detected if an unintended listener can simultaneously cover all signal intervals.

A second method is called Direct Sequence (DS). In DS, a broad-band modulation waveform is used to spread the signal energy over the entire communication bandwidth at each instant of time. An unintended listener using an intercept bandwidth of $1/T$ Hz only receives a fraction of the signal power. On the other hand, if the intercept bandwidth is equal to the communication bandwidth, B , then the received noise is increased by a factor of about BT . In either case, the SNR of the intercepted signal is significantly reduced.

With DS, the required signal spreading is achieved by modulating the message signal with a noise-like waveform that has a nearly uniform power spectrum over the communication bandwidth. The modulation waveform should display considerable complexity and unpredictability when viewed by an unintended listener, while in fact being completely deterministic and easily recreated at the various communication receivers. Chaotic signals are good candidates as modulation waveforms for S^2 communication systems because of their broad-band and noise-like characteristics. Furthermore, synchronized chaotic systems can be used at the communication receivers to coherently despread the received signal.

Many variations of S^2 communication systems based on synchronized chaotic systems are possible. Consider, for example, figure 10 which illustrates one possible approach. The primary signal processing components of the transmitter consist of a chaotic drive system, followed by a whitening filter and a DS modulator. The receiver consists of a synchronizing chaotic response subsystem, followed by an identical whitening filter and a demodulator. The RF section of this system has been omitted for clarity. We assume that the transmitter and communication receiver are linked through a common drive signal, $d(t)$. As discussed in Section 2, if the transmitter and communication

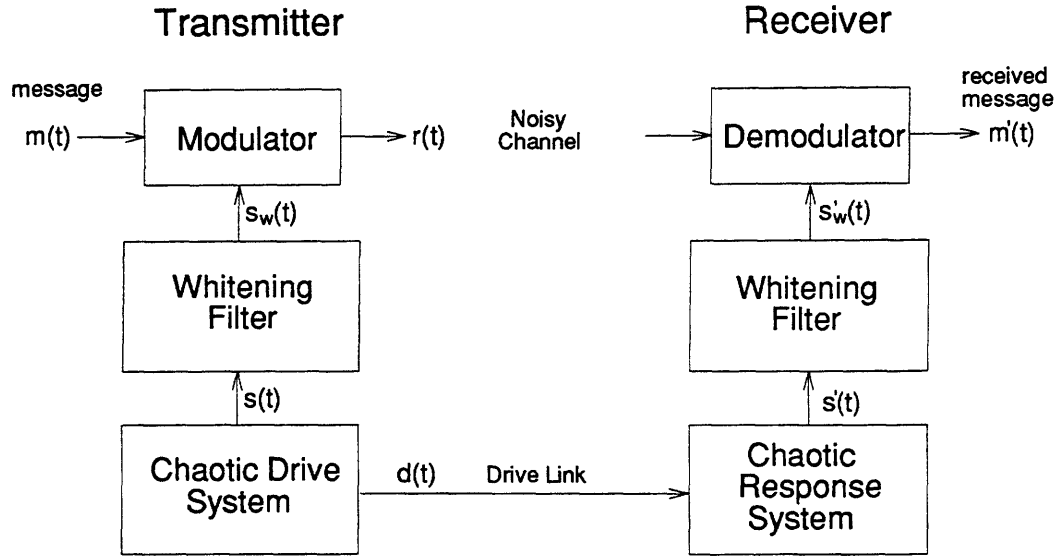


Figure 10: Chaotic Spread Spectrum System

receiver form a chaotic drive system and a stable response subsystem respectively, then the output signal of the response subsystem, $s'(t)$, will synchronize to the signal, $s(t)$, present at the transmitter. The purpose of the whitening filter is to produce a nearly uniform power spectrum from the chaotic signal, $s(t)$. The whitened signal, $s_w(t)$, will be a nearly ideal spreading signal because of its broad and uniform Fourier spectrum. If the message signal, $m(t)$, is multiplied by $s_w(t)$ at the modulator, the transmitted signal, $r(t) = m(t)s_w(t)$, will also have a broad Fourier spectrum. By properly scaling $s_w(t)$, the average power in $r(t)$ will be nearly the same as the average power in $m(t)$. Since $r(t)$ occupies a bandwidth which is larger than the bandwidth of $m(t)$ by a factor of approximately BT , there must be a corresponding decrease in the power spectral density of $r(t)$. By making the communication bandwidth very large, the transmitted signal can, in principle, be hidden in the background noise, which would make it very difficult to detect.

The communication receivers can easily recover the transmitted message since the despreading signal, $s'_w(t)$, will be identical to the spreading signal, $s_w(t)$, once the trans-

mitter and receiver have synchronized. If the demodulator performs the inverse of the modulation operation then $m(t)$ can be recovered. The required SNR of the recovered message is the same as that required from a conventional system having the same error rate and baseband modulation scheme.

The whitening filter is an important component in the overall S^2 system. The details of its design and implementation are discussed in Section 3.1.1. In Section 3.1.2, we discuss two simple modulation/demodulation schemes which use chaotic spreading signals. In Section 3.1.3, we present a simulation of the S^2 communication system shown in figure 10 and discuss its performance.

3.1.1 Whitening Filter

Ideally, the spreading signals used in a DS S^2 communication system would have a nearly uniform power spectrum over the entire communication bandwidth. Although chaotic signals generally possess a broad Fourier spectrum, the signal energy is usually not uniform over a wide range of frequencies. As an example, consider figures 11(a) and 11(b) which shows a sample function, $x[n]$, from the three-dimensional DT Henon map and its corresponding averaged power spectrum. Distinctive spectral peaks are evident in the power spectrum, which would make $x[n]$ less than ideal as a spreading signal. However, significant spectral whitening can be obtained by processing $x[n]$ with a linear time-invariant (LTI) filter having an appropriate frequency response. It is straightforward to design a whitening filter that is based on the estimated power spectrum, or equivalently the autocorrelation function, of $x[n]$. Classically, the filter can be derived by forming a linear estimate of $x[n]$ in terms of the N most recent values and minimizing the mean-square (MS) estimation error. Specifically, let the estimate of $x[n]$ be

$$\hat{x}[n] = \sum_{k=1}^N a_k x[n-k] \quad (8)$$

where the a_k are to be determined so that the MS error

$$P = E \{ (x[n] - \hat{x}[n])^2 \}$$

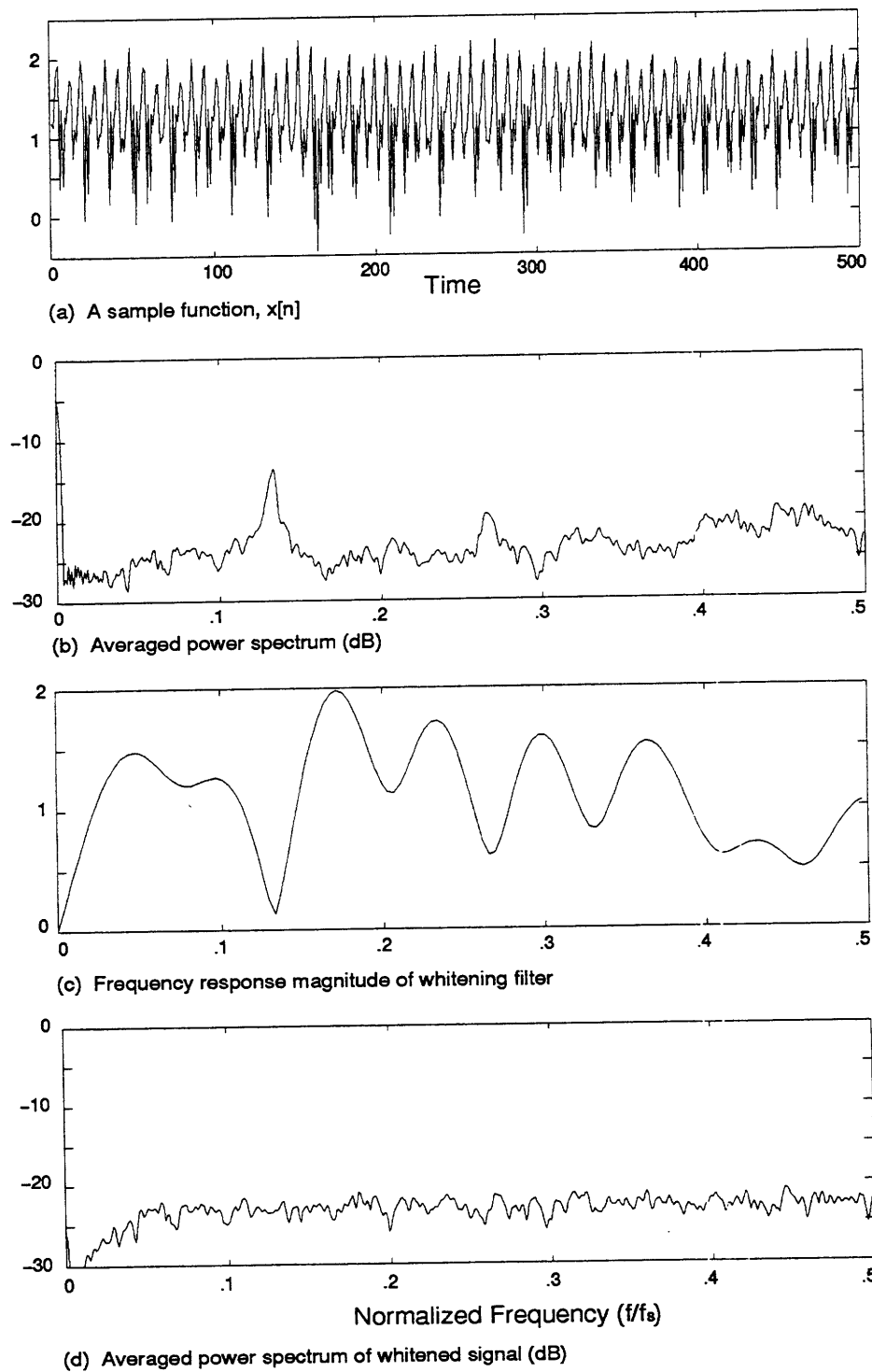


Figure 11: Chaotic Signal Whitening

is minimized. The stochastic orthogonality principle leads to the following system of N equations

$$E \left\{ \left(x[n] - \sum_{k=1}^N a_k x[n-k] \right) x[n-m] \right\} = 0 \quad m = 1, \dots, N$$

This system of equations can be written in matrix form as

$$\begin{aligned} R_{11}a_1 + R_{12}a_2 + \dots + R_{1N}a_N &= R_{01} \\ R_{21}a_1 + R_{22}a_2 + \dots + R_{2N}a_N &= R_{02} \\ \vdots & \\ R_{N1}a_1 + R_{N2}a_2 + \dots + R_{NN}a_N &= R_{0N} \end{aligned} \tag{9}$$

where the R_{ij} are the estimated autocorrelation coefficients of $x[n]$. The system (9) can be solved recursively for the N constants, a_k , using Levinson's algorithm.

In (8), the a_k can be interpreted as the impulse response of an LTI system. The transfer functions

$$\begin{aligned} H(z) &= \sum_{k=1}^N a_k z^{-k} \\ E(z) &= 1 - \sum_{k=1}^N a_k z^{-k} \end{aligned}$$

correspond to the prediction and error filters for $x[n]$, respectively. The finite-impulse-response (FIR) filter $E(z)$, when applied to $x[n]$, will have as its output a white noise-like sequence, $x_w[n]$, corresponding to the estimation error. Therefore, $E(z)$ can be used as a whitening filter for $x[n]$. As an illustration, figures 11(c) and 11(d) show the magnitude of the frequency response for a 20-point whitening filter and the averaged power spectrum of $x_w[n]$. Notice that the power spectrum of $x_w[n]$ is nearly uniform over a wide range of frequencies, and therefore, $x_w[n]$ will be a nearly ideal spreading signal.

As indicated in figure 10, a whitening filter can be applied to the output of the chaotic drive system to produce a whitened signal, $s_w(t)$. In order to perform message despreading at the receiver, an identical whitening filter is required at the output of the chaotic response system.

3.1.2 Modulator/Demodulator

In this subsection we explore two of many possible approaches to S^2 modulation based on chaotic signals and systems. Our objective is to illustrate some basic ideas and to point out that synchronized chaotic systems seem to offer considerable opportunity for novel approaches to secure communication. We consider our proposed methods as preliminary and plan to continue investigating these and other alternative approaches.

An important consideration in the design of an S^2 communication system is invertibility of the modulation process. The communication receivers must be able to recover $m(t)$ from $r(t)$ without ambiguity or numerical sensitivities. Direct multiplication by $s_w(t)$ at the modulator has the disadvantage that division is required at the demodulator to recover $m(t)$. Since $s_w(t)$ can take on values which are nearly zero, the resulting demodulation process is numerically sensitive. This sensitivity can be eliminated by “hard-limiting” $s_w(t)$ to produce a new spreading signal, $\tilde{s}_w(t)$, which takes on only integer values of plus or minus unity depending on the sign of $s_w(t)$. However, hard-limiting has the disadvantage that the spreading waveform produced could be easily removed by simply squaring the received signal. In effect, by simply hard-limiting $s_w(t)$ we are losing some of the benefits of using continuous-valued chaotic signals as spreading waveforms.

A more secure approach is to use the continuous-valued chaotic signal $s_w(t)$ as a modulation waveform but to modify its probability density function (PDF) so that the sample values are equally probable and that values near zero are not possible. For example, a desirable PDF might have the form shown in figure 12. A PDF of this form would eliminate the numerical sensitivities at the demodulator and has an advantage over the hard-limiter in that the spreading signal cannot be removed by a simple squaring operation. Of course, a real-valued continuous signal cannot change sign without passing through zero. Therefore, certain difficulties may arise when attempting to realize the PDF of figure 12 using a physical CT system. Note that this is not an issue for DT

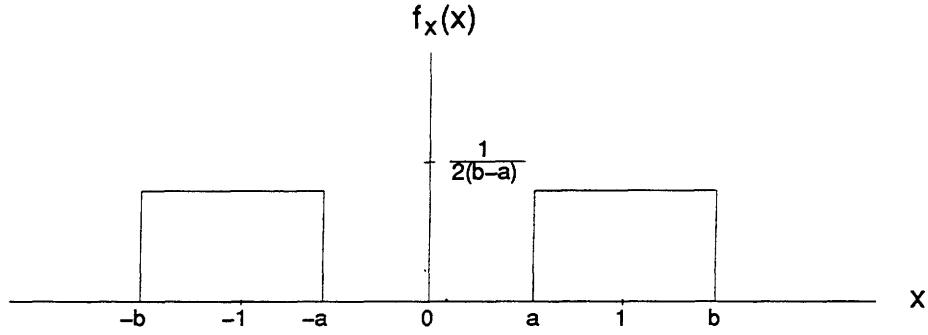


Figure 12: A PDF for a Chaotic Spreading Waveform

realizations based on finite difference equations. Therefore, we continue by assuming that chaotic signals having a PDF of the form in figure 12 can be generated by some means, for example, by using complex-valued CT representations or by using DT systems.

In general, a PDF of the form shown in figure 12 can be obtained from a random process, x , by first performing a nonlinear mapping of the form, $y = 2F_x(x) - 1$, where $F_x(x)$ is the cumulative distribution function (CDF) of the random process x . This mapping has the property of converting a random process having an arbitrary density function into a new random process which has a density function which is uniform in $(-1,1)$. By adding a second independent process to y , the resulting process, $\tilde{y}$, will have a density function which is the convolution of the two density functions for the processes being added. If the second process is chosen to be the output of a hard-limiter with equal probabilities of plus and minus unity, then $\tilde{y}$ will have a PDF similar to that shown in figure 12. In general, the second independent process could be obtained from a separate chaotic system. However, since x is a whitened process, a second *linearly* independent process to be added to y can be obtained from x by a simple delay operation, since samples spaced a few time steps apart are uncorrelated. Experiment has shown that this approach produces density functions which are very similar to that illustrated in figure 12.

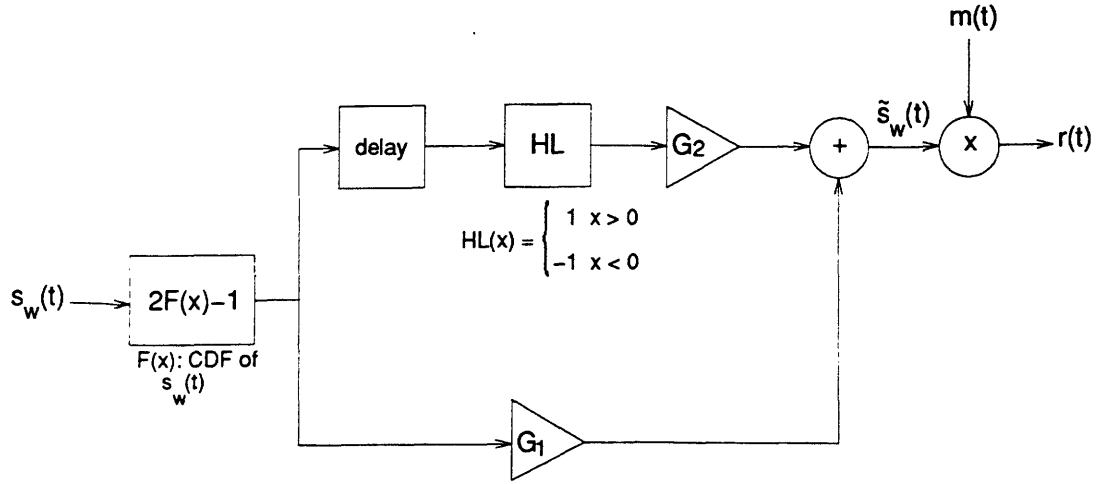


Figure 13: Direct Sequence Modulation Using Chaotic Signals

A DS modulator based on this approach is illustrated in figure 13. The input is the whitened chaotic signal $s_w(t)$ and the output is the transmitted signal $r(t) = m(t)\tilde{s}_w(t)$. The spreading waveform $\tilde{s}_w(t)$ has a PDF of the form shown in figure 12. The gain constants G_1 and G_2 are related to a and b of figure 12 by

$$G_1 = (b - a)/2$$

$$G_2 = (a + b)/2$$

If a and b are chosen to satisfy the equality $b^3 - a^3 = 3(b - a)$, then $\tilde{s}_w(t)$ will be a zero-mean deterministic process with a variance equal to unity. A demodulator which is similar to figure 13 can be implemented at the receiver to recover the message. However, in this case the multiplication operation is replaced by division at the receiver.

As an illustration, figure 14(a) shows the PDF of the whitened chaotic signal $x_w[n]$ from the three-dimensional DT Henon map. Notice that most of the sample values of $x_w[n]$ are concentrated around zero and therefore if $x_w[n]$ is used directly division by near zero values at the receiver would be required. Figure 14(b) shows the corresponding PDF for $\tilde{x}_w[n]$, which is in good agreement with the expected PDF. In this example we have chosen the values $a=.50$ and $b=1.43$.

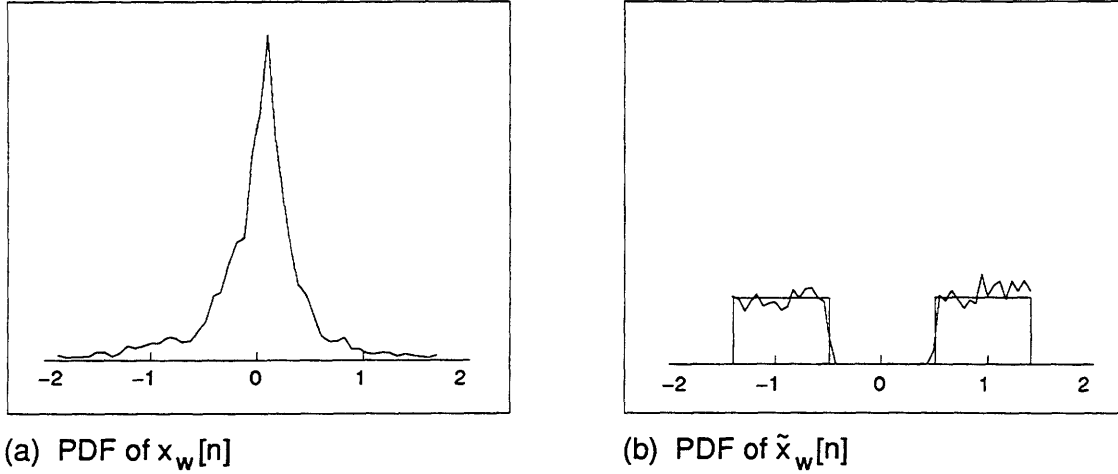


Figure 14: Experimental PDF's

Certainly, more elaborate modulation schemes could be devised which would avoid the necessity for performing division at the demodulator and still retain the benefits of using continuous-valued spreading signals. As one example, consider figure 15 which shows a modulation/demodulation scheme which avoids direct division and uses complex-valued signal representations. With this approach a positive-valued DS spreading waveform multiplies the message signal. This is followed by subsequent phase modulation by $e^{jd(t)}$. The transmitted signal has the form $r(t) = m(t)\tilde{s}_w(t)e^{jd(t)}$, where $d(t)$ is the chaotic drive link signal of figure 10. This approach has certain advantages that are worth noting. For example, a separate drive link is not required since the drive signal $d(t)$ is transmitted over the same channel. This has the additional advantage that initial synchronization difficulties, due to unknown time delays between transmitter and receiver, are to a large extent eliminated.

This example also shows an interesting way of using synchronizing chaotic systems to demodulate the received signal. As illustrated, the argument, $d(t)$, of the complex-valued received signal is used to drive a synchronizing chaotic response system which subsequently generates the waveform to be used as the despreading signal. In principle, this approach could be implemented in an analog system which uses quadrature

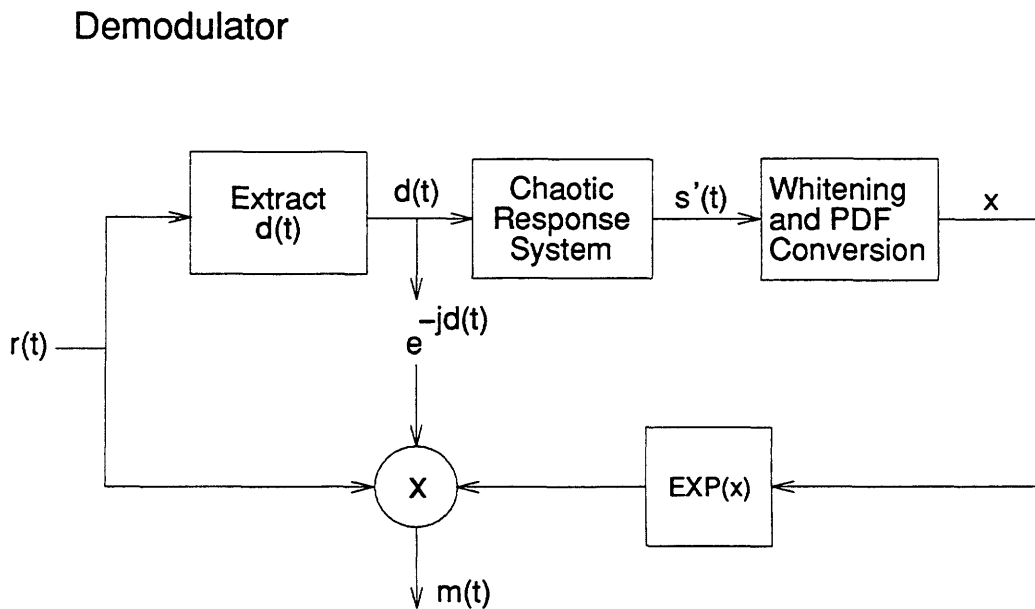
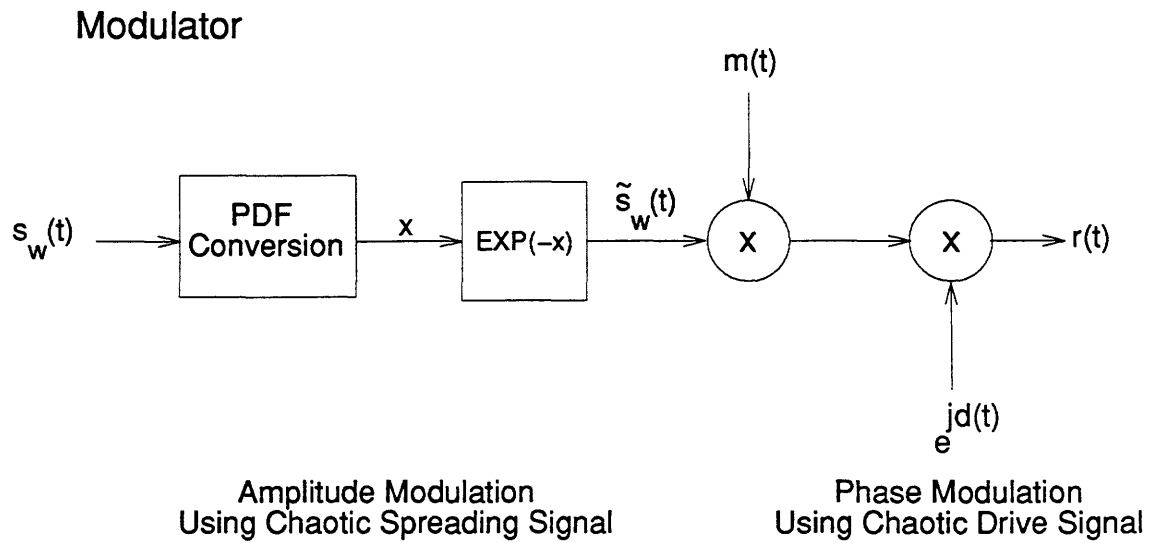


Figure 15: A Modulator/Demodulator Based on Synchronized Chaotic Signals

modulation.

3.1.3 Simulation

We demonstrate the chaotic S^2 system illustrated in Figure 16 which uses the DS modulation scheme illustrated in figure 13. In this simulation, the message signal, $m[n]$, is a tone-burst signal and it is multiplied by the chaotic spreading waveform, $\tilde{x}_w[n]$, derived from the DT Henon map. The Henon (x, y) subsystem forms the chaotic response system at the receiver. As discussed in Section 2.3, the response subsystem will rapidly synchronize to the output signal of the drive system. The despreading signal, $\tilde{x}'_w[n]$, at the receiver is then derived from the output of the synchronized chaotic response system. Subsequent division of the received signal by the despreading waveform allows the tone-burst signal to be recovered. In the noiseless case the message signal can be perfectly recovered at the receiver.

For the case illustrated, Gaussian channel noise has been added to the transmitted spread spectrum signal. The signal-to-noise ratio of the recovered tone-burst signal is approximately 20dB. Figures 17(a) through 17(c) show the power spectrum of the tone-burst signal, the received spread spectrum signal, and the recovered signal, respectively. It is evident from figure 17(b) that the detection or parameter estimation of the tone-burst would be difficult by an unintended listener. However, as figure 17(c) suggests, the communication receivers would have little difficulty.

3.2 Chaotic Signal Masking

In signal masking, a noise-like masking signal is added at the transmitter to the information-bearing signal $m(t)$ and at the receiver the masking is removed. Several researchers [11, 12, 13] have been considering the use of noise reduction algorithms as an approach to retrieving information masked by chaotic signals. A very different approach which we are exploring is to use the received signal to regenerate the masking signal at the re-

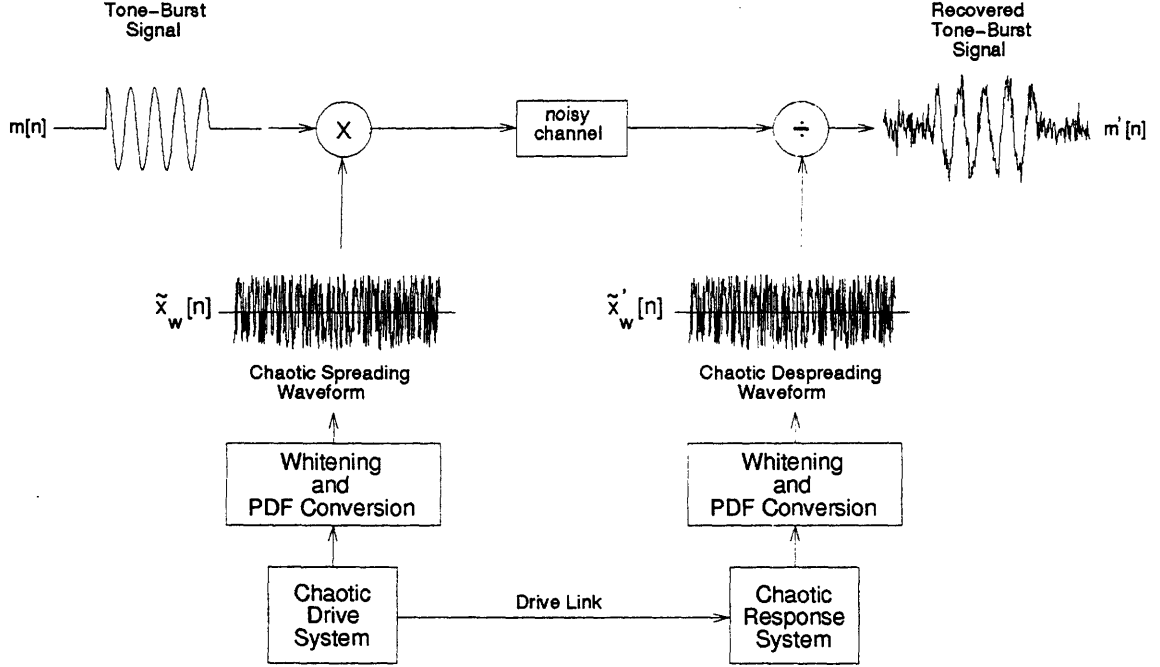
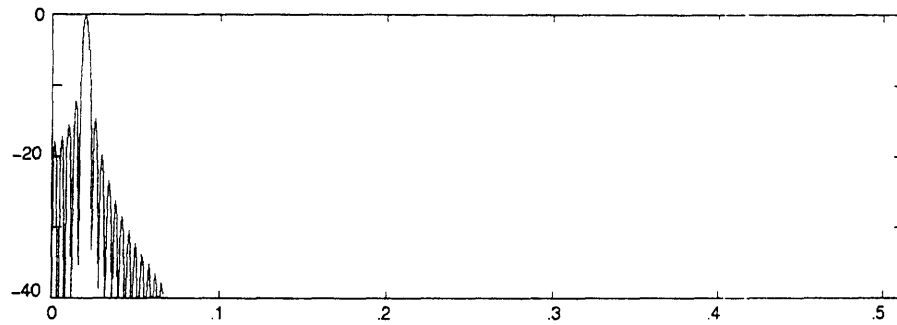


Figure 16: Simulation of a Chaotic Spread Spectrum System

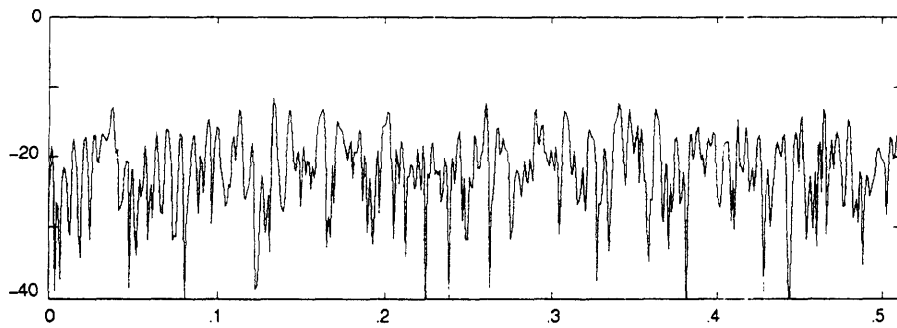
ceiver and subtract it from the received signal to recover $m(t)$. Surprisingly, this can be done with synchronized chaotic systems since at least for some systems the ability to synchronize is robust, i.e. is not highly sensitive to perturbations in the synchronizing drive and thus can be done with the masked signal. While there are many possible variations, consider, for example, the chaotic Lorenz system represented by the dynamical equations

$$\begin{aligned}\dot{x} &= 16(y - x) \\ \dot{y} &= 45.92x - y - xz \\ \dot{z} &= xy - 4z\end{aligned}$$

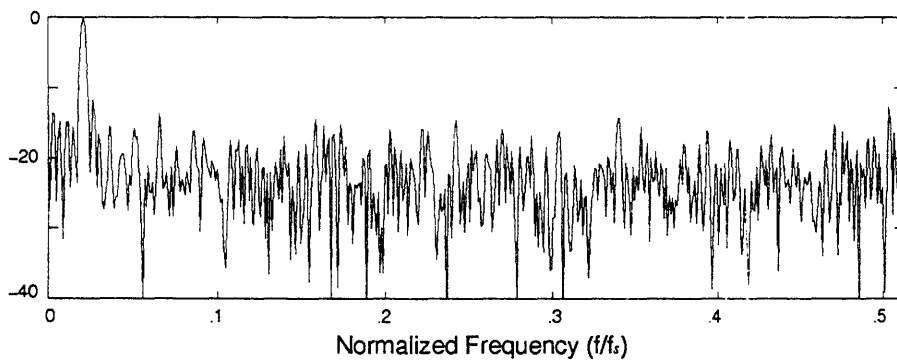
As discussed in section 2, both the (x, z) and (y, z) subsystems are stable and consequently either x or y can be used as the synchronizing drive. Choosing x as the drive and the chaotic masking, the transmitted signal is $r(t) = x(t) + m(t)$ and it is assumed that for masking the power level of $m(t)$ is significantly lower than that of $x(t)$. The



(a) Power Spectrum of Tone-Burst Signal (dB)



(b) Power Spectrum of Received Spread Spectrum Signal (dB)



(c) Power Spectrum of Recovered Tone-Burst Signal (dB)

Figure 17: Simulated Power Spectra

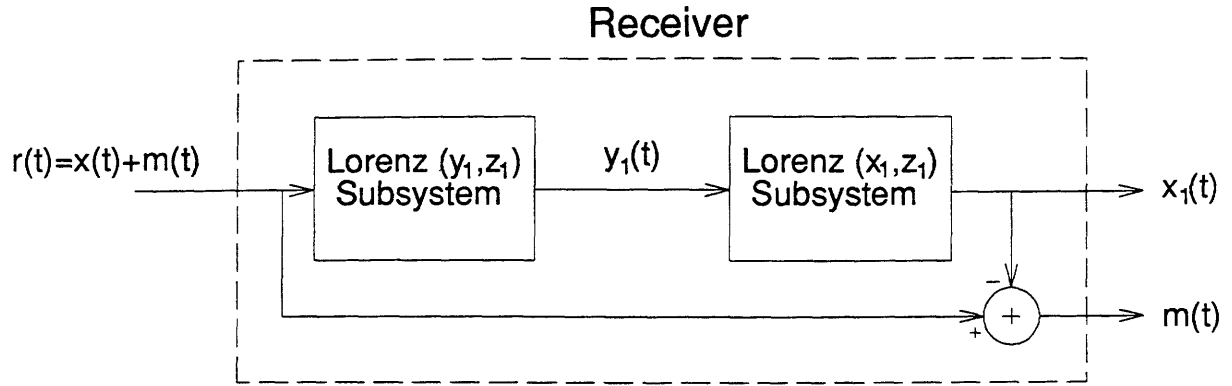


Figure 18: Chaotic Signal Masking System

basic strategy then is to exploit the robustness of the synchronization using $r(t)$ as the synchronizing drive at the receiver. The dynamical system implemented at the receiver is

$$\begin{aligned}\dot{x}_1 &= 16(y_1 - x_1) \\ \dot{y}_1 &= 45.92r - y_1 - rz_1 \\ \dot{z}_1 &= ry_1 - 4z_1\end{aligned}$$

If the receiver has synchronized with $r(t)$ as the drive, then $x_1(t) = x(t)$ and consequently $m(t)$ is recovered as $\hat{m}(t) = r(t) - x_1(t)$. Figure 18 illustrates the approach.

We illustrate the performance of this system in figure 19 with a segment of speech from the sentence “He has the bluest eyes”. Figure 19(a),(b) and (c) show the original speech, the transmitted signal and the recovered speech respectively. The power spectra of the chaotic masking signal and the speech are highly overlapping and the overall signal-to-masking ratio is approximately -20dB. Clearly, the speech signal has been recovered. Also evident in figure 19(c) is the relatively rapid synchronization at the onset of the received signal.

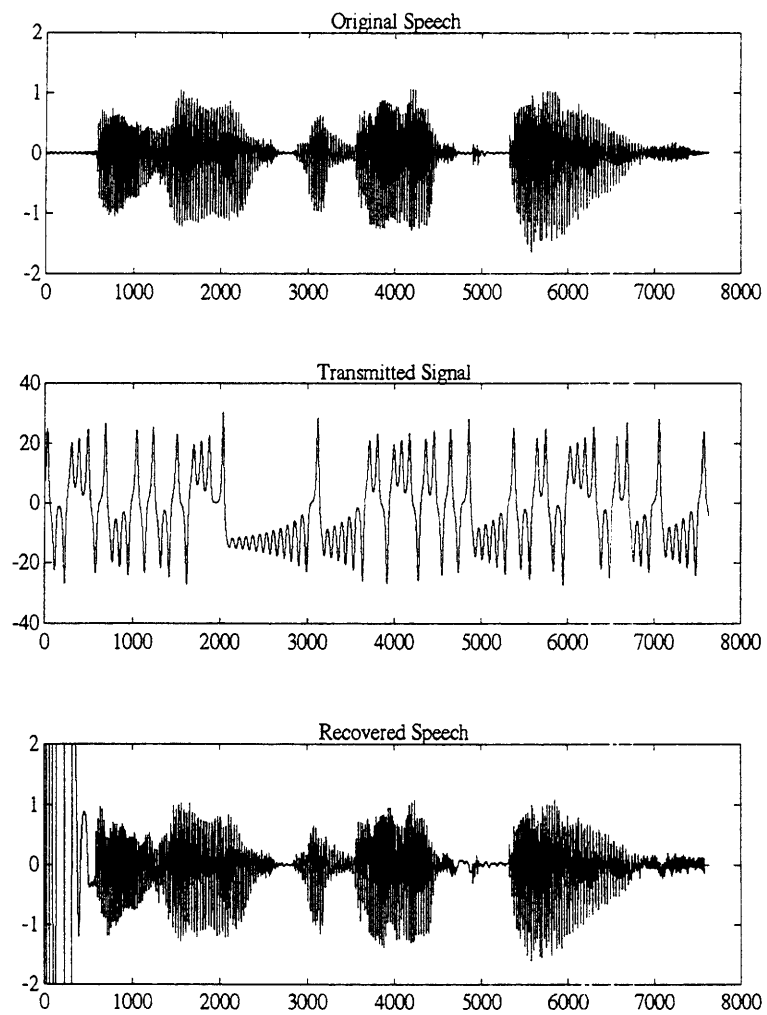


Figure 19: Speech Waveforms: Original, Transmitted, and Recovered

4 Summary and Conclusions

Although chaotic systems are deterministic, the signals that evolve in these systems are typically broadband, noise-like and similar in many respects to sample functions of a stochastic process. Because of these properties chaotic signals potentially provide an important class of signals which can be utilized in various communications, radar and sonar contexts for masking information-bearing waveforms and as modulating waveforms in spread spectrum systems. In addition, a chaotic system which can be decomposed into a drive system and a stable response subsystem will synchronize when coupled with a common drive signal [2, 3]. This property has several practical applications and suggests novel approaches to signal masking and secure communication.

We have discussed and demonstrated the ability of three continuous-time chaotic systems (Lorenz, Rössler, and Double Scroll) and the discrete-time Henon map to synchronize. Each of these systems are decomposable into synchronizing subsystems and have a three-dimensional state space. We have also proposed and explored in a preliminary way various applications in which synchronizing chaotic systems can extend our signal processing and communication abilities. We plan to continue exploring a number of ways in which synchronized chaotic systems can be used in spread spectrum communication and for various signal masking purposes.

References

- [1] E. N. Lorenz. "Deterministic Nonperiodic Flow". *Journal of the Atmospheric Sciences*, 20:130–41, 1963.
- [2] L. M. Pecora and T. L. Carroll. "Synchronization in Chaotic Systems". *Physical Review Letters*, 64(8):821–24, 1990.
- [3] T. L. Carroll and L. M. Pecora. "Synchronizing Chaotic Circuits". *IEEE Transactions on Circuits and Systems*, 38(4):453–56, 1991.
- [4] J. P. Eckmann and D. Ruelle. "Ergodic Theory of Chaos and Strange Attractors". *Reviews of Modern Physics*, 57(3):617–56, 1985.
- [5] T. S. Parker and L. O. Chua. "*Practical Numerical Algorithms for Chaotic Systems*". Springer-Verlag, New York, 1989.
- [6] T. Matsumoto, L. O. Chua, and K. Tokumasu. "Double Scroll via a Two-Transistor Circuit". *IEEE Transactions on Circuits and Systems*, CAS-33:828–35, 1986.
- [7] T. Matsumoto, L. O. Chua, and M. Komuro. "The Double Scroll Bifurcations". *International Journal of Circuit Theory and Applications*, 14(1):117–46, 1986.
- [8] D. L. Hitzl and F. Zele. "A Three-Dimensional Dissipative Map with Three Routes to Chaos". *Lockheed Technical Report*, Unpublished, 1984.
- [9] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo. "Signal Processing in the Context of Chaotic Signals". *Proceedings IEEE ICASSP*, 1992.
- [10] D. L. Nicholson. "*Spread Spectrum Signal Design: LPE and AJ Systems*". Computer Science Press, Inc., Rockville, Maryland, 1988.
- [11] H. D. I. Abarbanel. "Chaotic Signals and Physical Systems". *Proceedings IEEE ICASSP*, 1992.

- [12] C. Meyers, A. Singer, B. Shin, and E. Church. "Modeling Chaotic Systems with Hidden Markov Models". *Proceedings IEEE ICASSP*, 1992.
- [13] C. Meyers, S. Kay, and M. Richard. "Signal Separation for Nonlinear Dynamical Systems". *Proceedings IEEE ICASSP*, 1992.

