A SIMPLE WAY TO SYNCHRONIZE CHAOTIC SYSTEMS WITH APPLICATIONS TO SECURE COMMUNICATION SYSTEMS

by

Chai Wah Wu and Leon O. Chua

Memorandum No. UCB/ERL M93/73

15 August 1993

A SIMPLE WAY TO SYNCHRONIZE CHAOTIC SYSTEMS WITH APPLICATIONS TO SECURE COMMUNICATION SYSTEMS

by

Chai Wah Wu and Leon O. Chua

Memorandum No. UCB/ERL M93/73

15 August 1993

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

A SIMPLE WAY TO SYNCHRONIZE CHAOTIC SYSTEMS WITH APPLICATIONS TO SECURE COMMUNICATION SYSTEMS

by

Chai Wah Wu and Leon O. Chua

Memorandum No. UCB/ERL M93/73

15 August 1993

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Figure captions

Figure 1 Communication system based on synchronizing master-slave configuration.

Figure 2 Block diagram of secure communication system.

Figure 3 Chua's circuit.

Figure 4 Secure communication system using Chua's circuit and coding function c_1. The diamond-shaped sources are dependent sources. The voltage-controlled voltage source [Chua *et al.*, 1987] senses the voltage v_R across the nonlinear resistor in the transmitter and gives an output voltage v_R. The current-controlled current source senses the current $\tilde{i}_R$ through the nonlinear resistor in the receiver and gives an output current $\tilde{i}_R$.

Figure 5 Simulation of communication system in Fig. 4. (a) Time waveforms of $v_1(t)$ and $\tilde{v}_1(t)$. (b) Recovered information signal $\tilde{m}(t)$.

Figure 6 Effects of parameter mismatch and channel noise. (a) Recovered information signal $\tilde{m}(t)$ using the same setup as for Fig. 5b, except R in the receiver is increased by 0.02%. (b) Recovered information signal $\tilde{m}(t)$ using the same setup as for Fig. 5b, except the additive channel noise is a sine wave with frequency $\frac{5000}{\pi}$ and amplitude 0.001.

Figure 7 Secure communication system using the Lorenz system. (a) Time waveforms of $x(t)$ and $\tilde{x}(t)$. (b) Recovered information signal $\tilde{m}(t)$.

Abstract

In this paper, we give a scheme for synthesizing synchronizing circuits and systems. Synchronization of drive and response system is proved trivially without the need for computing numerically the conditional Lyapunov exponents. We give a definition of the driving and response system having the same functional form, which is more general than the concept of homogeneous driving of Pecora and Carroll [Pecora & Carroll, 1991]. Finally, we show how synchronization coupled with chaos can be used to implement secure communication systems. This is illustrated with examples of secure communication systems which is inherently error-free in contrast with the signal-masking schemes proposed in [Cuomo & Oppenheim, 1993a,b; Kocarev *et al.*, 1992]

1 Introduction

In [Pecora & Carroll 1990,1991; Carroll & Pecora 1991] Pecora and Carroll showed that two chaotic systems in a master-slave configuration can be made to synchronize (i.e. the slave system follows the trajectories of the master system) only if the conditional Lyapunov exponents of the slave system are all negative. This is also a sufficient condition for a large class of systems. In [He & Vaidya, 1992], it was shown by means of a Lyapunov function how systems can be synthesized that will synchronize.

In this paper we will present another way to design nonlinear systems which will synchronize. For the subclass of these systems which are chaotic, we show how secure communication systems can be realized similar to the schemes proposed in [Cuomo & Oppenheim, 1993a,b; Kocarev *et al.*, 1992; Oppenheim *et al.* 1992; Parlitz *et al.*, 1992; Halle *et al.* 1993].

2 Synchronization of Systems in Master-slave Configuration

Pecora and Carroll [Pecora & Carroll, 1991] considered the master-slave synchronization scheme given by:

$$\dot{v} = f(v,u) \quad (1)$$

$$\dot{u} = g(v,u) \quad (2)$$

$$\dot{w} = h(v,w) \quad (3)$$

where $v \in \mathbb{R}^m, u \in \mathbb{R}^k, w \in \mathbb{R}^l$.

The system (1)-(2) is referred to as the *drive* system and the system (3) is the *response* system.

In [Pecora & Carroll, 1991], the driving in (1)-(3) is called *homogeneous driving* when $k = l$ and $g(\cdot,\cdot) = h(\cdot,\cdot)$. This form of driving is considered in detail in [Pecora & Carroll, 1991; He & Vaidya, 1992]. In [Cuomo & Oppenheim, 1993a,b], this homogeneous driving is used in communication systems by augmenting the response system to have the same dimension as the driving system and setting

$$\dot{w} = \begin{pmatrix} \dot{w}_1 \\ \dot{w}_2 \end{pmatrix} = h(v,w) = \begin{pmatrix} f(w_1,w_2) \\ g(v,w_2) \end{pmatrix} \quad (4)$$

where $w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$. Thus the response system has the same "form" as the driving system.

We generalize this concept and define the drive and response system to have the same functional form if the drive and response system have the same dimension ($m + k = l$) and for all u, v the following equation is satisfied

$$h\left(v, \begin{pmatrix} v \\ u \end{pmatrix}\right) = \begin{pmatrix} f(v,u) \\ g(v,u) \end{pmatrix} \tag{5}$$

The master-slave system (1)-(3) satisfying (5) is more general than the homogeneous driving (condition (4)) in [Pecora & Carroll 1990,1991; Carroll & Pecora 1991;He & Vaidya, 1992; Cuomo & Oppenheim, 1993a,b] in that homogeneous driving is a special case of the system (1)-(3) satisfying (5). In fact, the synchronization scheme that we discuss in this paper satisfies (5), but cannot be written as (4).

Here we say that the system (1)-(3) synchronizes if $w(t) \rightarrow \begin{pmatrix} v(t) \\ u(t) \end{pmatrix}$ as $t \rightarrow \infty$[1] for initial condition w_0 in a neighborhood of $\begin{pmatrix} v_0 \\ u_0 \end{pmatrix}$. We call $e = w - \begin{pmatrix} v \\ u \end{pmatrix}$ the synchronization error. If the origin for the error dynamics is asymptotically stable, then the system will synchronize. In [He & Vaidya, 1992;Cuomo & Oppenheim, 1993a,b], the error dynamics is shown to be linear time-varying (nonautonomous), and by using a Lyapunov function the error is shown to converge to zero asymptotically.

To obtain systems which can more easily be shown to synchronize, we want the error dynamics to be linear and autonomous. In particular, we will assume that the master system is of the form:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{f}(\mathbf{x}_\rho) \tag{6}$$

where $\mathbf{A}$ has all its eigenvalues in the open left half plane (i.e. $\dot{\mathbf{x}} = \mathbf{A}\mathbf{x}$ is globally asymptotically stable.) and $\mathbf{x}_\rho = (x_1, x_2, \ldots, x_\rho)^t \in \mathbb{R}^\rho$ is a subvector of the state vector $\mathbf{x}$.

We then have the following drive-response system:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{f}(\mathbf{x}_\rho) \\ \dot{\tilde{\mathbf{x}}} &= \mathbf{A}\tilde{\mathbf{x}} + \mathbf{f}(\mathbf{x}_\rho) \end{aligned} \tag{7}$$

where $\mathbf{x}$ is the state vector of the driving system and $\tilde{\mathbf{x}}$ is the state vector of the response system. In terms of the notation of (1)-(3), $v = \mathbf{x}_\rho$, $\begin{pmatrix} v \\ u \end{pmatrix} = \mathbf{x}$ and $w = \tilde{\mathbf{x}}$. It is clear that

$$\frac{d(\tilde{\mathbf{x}} - \mathbf{x})}{dt} = \mathbf{A}(\tilde{\mathbf{x}} - \mathbf{x}) \tag{8}$$

Since $\mathbf{A}$ has all its eigenvalues in the open left half plane, $\tilde{\mathbf{x}} \rightarrow \mathbf{x}$ as $t \rightarrow \infty$. Therefore the system will synchronize (globally). The rate of convergence can be readily found from the eigenvalues of $\mathbf{A}$. Note that even though the response system is not autonomous, the error system is autonomous.

[1] With this notation, we mean $w(t) - \begin{pmatrix} v(t) \\ u(t) \end{pmatrix} \rightarrow 0$ as $t \rightarrow \infty$.

3 Communication Systems Utilizing Chaos

In communication schemes proposed in [Oppenheim *et al.*, 1992; Kocarev *et al.*, 1992, Parlitz *et al.* 1992, Cuomo & Oppenheim, 1993a,b; Halle *et al.* 1993], the driving system is the transmitter, the response system is the receiver and a subvector $\mathbf{x}_\rho$ of the state vector $\mathbf{x}$ is transmitted causing the receiver to synchronize with the transmitter. This is shown in Fig. 1.

All systems can be put in the form (6), for example, by choosing $\mathbf{A} = 0$ and $\mathbf{x}_\rho = \mathbf{x}$, but practically, it would be desirable to have ρ, the number of component of $\mathbf{x}_\rho$, to be as small as possible, as then less of the state needs to be transmitted. For example, when $\rho = 1$, $\mathbf{x}_\rho = x_1$ and only x_1 needs to be transmitted. The synchronization scheme (7) is simple and straightforward, and many chaotic systems in the literature [Arneodo *et al.* 1981; Brockett, 1982; Sparrow, 1981; Chua, 1992; Ogorzalek, 1989; Nishio *et al.*, 1990] has state equations which can be put in the form (6) such that $\mathbf{x}_\rho = x_1$ and thus a communication system in a master-slave configuration using these chaotic systems can be made to synchronize by using solely x_1 as the transmitted signal.

Given that the driving system behaves in a chaotic manner, we can implement the following secure communication scheme:

The information signal $\mathbf{m}(t)$ is coded with the chaotic signal $\mathbf{x}_\rho(t)$ using a coding function $\mathbf{s}(t) = c(\mathbf{x}_\rho(t), \mathbf{m}(t))$ such that we can decode the information signal uniquely through $\mathbf{m}(t) = d(\mathbf{x}_\rho(t), \mathbf{s}(t)) = d(\mathbf{x}_\rho(t), c(\mathbf{x}_\rho(t), \mathbf{m}(t)))$. We assume that d is continuous in the variable $\mathbf{x}_\rho$. The choice of $c(\cdot,\cdot)$ and $d(\cdot,\cdot)$ must satisfy $\mathbf{s}(t) \approx \mathbf{x}_\rho(t)$ for all appropriate information signals $\mathbf{m}(t)$ for two reasons. First, we want the driving system to remain chaotic and as we see in Fig. 2, $\mathbf{s}(t)$ is fed back in place of $\mathbf{x}_\rho(t)$ in the driving system. To ensure that the driving system remains chaotic, we want $\mathbf{s}(t) \approx \mathbf{x}_\rho(t)$. Second, when we want the communication system to be secure, we want $\mathbf{s}(t) \approx \mathbf{x}_\rho(t)$ so that the occurence of $\mathbf{m}(t)$ is not apparent from looking at $\mathbf{s}(t)$. The signal $\mathbf{s}(t)$ is then transmitted to the receiving system. The overall secure communication system is shown in Fig. 2.

The equations governing the system are given by:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{f}(\mathbf{s}) \\ \dot{\tilde{\mathbf{x}}} &= \mathbf{A}\tilde{\mathbf{x}} + \mathbf{f}(\mathbf{s}) \end{aligned} \tag{9}$$

Again we have $\frac{d(\tilde{\mathbf{x}}-\mathbf{x})}{dt} = \mathbf{A}(\tilde{\mathbf{x}} - \mathbf{x})$ so that $\tilde{\mathbf{x}}(t) \to \mathbf{x}(t)$ and thus $\tilde{\mathbf{m}}(t) = d(\tilde{\mathbf{x}}_\rho(t), \mathbf{s}(t)) \to \mathbf{m}(t)$ as $t \to \infty$ by continuity of d. Note that in the receiving circuit of this system the information signal is recovered completely without degradation, when the circuits are perfectly matched and there are no noise added during transmission, in contrast to the signal masking schemes in [Kocarev *et al.*, 1992; Cuomo & Oppenheim, 1992a,b] where $\tilde{\mathbf{x}} \not\to \mathbf{x}$.

3.1 Example: Chua's Circuit

Chua's circuit (Fig. 3) [Kennedy, 1992a,b; Madan, 1993a,b] is a simple electronic circuit capable of generating chaos and other bifurcation phenomena. The state equations of Chua's circuit are:

$$\begin{aligned} \frac{dv_1}{dt} &= \frac{1}{C_1}[G(v_2 - v_1) - f(v_1)] \\ \frac{dv_2}{dt} &= \frac{1}{C_2}[G(v_1 - v_2) + i_3] \\ \frac{di_3}{dt} &= -\frac{1}{L}v_2 \end{aligned} \tag{10}$$

where

$$G = \frac{1}{R}$$

and

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)\{|v_1 + E| - |v_1 - E|\} \tag{11}$$

Equations (10) can be decomposed into the form (6) in several different ways. For example, in [Halle *et al.*, 1993] and in the x-drive configuration in [Chua *et al.*, 1993], equations (10) are decomposed as:

$$\begin{pmatrix} \frac{dv_1}{dt} \\ \frac{dv_2}{dt} \\ \frac{di_3}{dt} \end{pmatrix} = \begin{pmatrix} 0 & \frac{G}{C_1} & 0 \\ 0 & -\frac{G}{C_2} & \frac{1}{C_2} \\ 0 & -\frac{1}{L} & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ i_3 \end{pmatrix} + \mathbf{f}_1(v_1, v_2, i_3) \tag{12}$$

This corresponds to homogeneous driving.[2]

We will decompose (10) as follows:

$$\begin{pmatrix} \frac{dv_1}{dt} \\ \frac{dv_2}{dt} \\ \frac{di_3}{dt} \end{pmatrix} = \begin{pmatrix} -\frac{G}{C_1} & \frac{G}{C_1} & 0 \\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} \\ 0 & -\frac{1}{L} & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ i_3 \end{pmatrix} + \begin{pmatrix} -\frac{f(v_1)}{C_1} \\ 0 \\ 0 \end{pmatrix} \tag{13}$$

Thus $\mathbf{A} = \begin{pmatrix} -\frac{G}{C_1} & \frac{G}{C_1} & 0 \\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} \\ 0 & -\frac{1}{L} & 0 \end{pmatrix}$ and $\mathbf{x}_p = v_1$.

For positive C_1, C_2, R, and L, the matrix **A** has all its eigenvalues in the open left half plane since they correspond to the linear passive part of the circuit [Chua *et al*, 1987]. Note that equation (13) when used in (7) results in a system which is of the form (5), but not of the form (4).

For information signals $m(t)$ with small amplitude, two possible coding functions are $c_1(v_1(t), m(t)) = v_1(t) + m(t)$ and $c_2(v_1(t), m(t)) = v_1(t)(1 + m(t))$.[3]

The circuit for implementing the secure communication system using c_1 as the coding function is shown

[2] In fact, the first equation is not used in the receiver.

[3] For c_2, the decoding function does not exist when $v_1(t) = 0$. In this case, some error will occur when $v_1(t) \to 0$. For the double-scroll Chua's attractor in Chua's circuit, $v_1(t)$ goes through zero rather quickly, and the error occur in a short time interval [Halle *et al.* 1993].

in Fig. 4. The coding function c_1 injects the signal $m(t)$ into the transmitting circuit. As was shown in [Halle *et al.*, 1992], $m(t)$ gets amplified by the circuit, and for sinusoidal $m(t)$ in a certain frequency amplitude range, the inclusion of $m(t)$ can be apparent from the spectrum of $v_1(t)$. On the other hand, a sinusoid contains very little information, and for an information signal with a broad spectrum, this effect will not be apparent. Nevertheless, we will use c_1 in our computer simulation to illustrate the operation of our system.

Figure 5 shows computer simulations of the synchronization scheme in Fig. 4. The parameters used in both the transmitting and receiving system are $C_1 = 5.56 \times 10^{-9}$, $C_2 = 50 \times 10^{-9}$, $R = 1428$, $L = 7.14 \times 10^{-3}$, $G_a = -0.8 \times 10^{-3}$, $G_b = -0.5 \times 10^{-3}$ and $E = 1$. A square wave of amplitude 0.001 and frequency $\frac{2100}{\pi}$ is used as the information signal $m(t)$. Figure 5a shows the time waveform of $v_1(t)$ in the transmitter and $\tilde{v}_1(t)$ in the receiver. In Fig. 5b we show the recovered information waveform $\tilde{m}(t)$. We see that after some transient behavior, the recovered waveform $\tilde{m}(t)$ approaches the square wave $m(t)$.

3.2 Parameter Mismatch and Channel Noise

The transmitter and the receiver system synchronize under the assumption that the two systems are perfectly matched and that there is no noise introduced during transmission. We ask the question whether the synchronization is robust in the sense that if there is a small mismatch between the transmitter and receiver and the channel noise is small, would the error induced also be small?

Here we provide a simple analysis of the effect of parameter mismatch between the transmitter and receiver and additive channel noise on the synchronization error for the communication system (9). The complete state equations when parameter mismatch and additive channel noise are accounted for are:

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{f}(\mathbf{s}) \\ \dot{\tilde{\mathbf{x}}} &= \tilde{\mathbf{A}}\tilde{\mathbf{x}} + \tilde{\mathbf{f}}(\mathbf{s} + \mathbf{ns}) \end{aligned} \tag{14}$$

where ns is the noise signal. Then the error system is:

$$\frac{d(\tilde{\mathbf{x}} - \mathbf{x})}{dt} = \tilde{\mathbf{A}}(\tilde{\mathbf{x}} - \mathbf{x}) - (\mathbf{A} - \tilde{\mathbf{A}})\mathbf{x} + (\tilde{\mathbf{f}}(\mathbf{s} + \mathbf{ns}) - \tilde{\mathbf{f}}(\mathbf{s})) - (\mathbf{f}(\mathbf{s}) - \tilde{\mathbf{f}}(\mathbf{s})) \tag{15}$$

Thus $(\tilde{\mathbf{x}} - \mathbf{x})$ is the response of a linear system with external input equal to $-(\mathbf{A} - \tilde{\mathbf{A}})\mathbf{x} + (\tilde{\mathbf{f}}(\mathbf{s} + \mathbf{ns}) - \tilde{\mathbf{f}}(\mathbf{s})) - (\mathbf{f}(\mathbf{s}) - \tilde{\mathbf{f}}(\mathbf{s}))$. We assume that $\tilde{\mathbf{f}}$ is continuous and that the chaotic signal $\mathbf{x}$ in the transmitter is bounded. Since $\tilde{\mathbf{A}}$ has all its eigenvalues in the open left half plane, the error $(\tilde{\mathbf{x}} - \mathbf{x})$ will be small (as $t \to \infty$) as long as $\tilde{\mathbf{A}} \approx \mathbf{A}$ and $\tilde{\mathbf{f}} \approx \mathbf{f}$ and ns is small. Thus for small parameter mismatch and small additive channel noise, the error will be small.

Equation (15) also indicate that the contribution of the channel noise ns to the error is small if $\tilde{\mathbf{f}}$ is small. This is intuitive as $\tilde{\mathbf{f}}$ determines how much the receiver is "driven" by the transmitted signal $\mathbf{x}_\rho$.

In Fig. 6a we show the recovered signal in the same setup as in Fig. 5b, except that the linear resistor R in the receiver is increased by 0.02%. In Fig. 6b we use the same setup as in Fig. 5b, with ns equal to a sine wave with frequency equal to $\frac{5000}{\pi}$ and amplitude equal to 0.001.

3.3 Secure Communication System Using the Lorenz System

To illustrate that this method of constructing secure communication systems is not restricted to system of the form (6), we will demonstrate a secure communication system based on the Lorenz System [Lorenz, 1963; Cuomo & Oppenheim, 1993a,b] in which there is no degradation in the recovered signal. Furthermore, to illustrate that not all synchronization schemes satisfy (4), we will use a synchronization scheme which is of the form (5) but not of the form (4).

The master-slave configuration will have the following state equations:

$$\begin{array}{rcl} \frac{dx}{dt} & = & \sigma(y-x) \\ \frac{dy}{dt} & = & (r-\mu)(x+m(t))+\mu x-y-(x+m(t))z \\ \frac{dz}{dt} & = & (x+m(t))y-bz \\ \frac{d\tilde{x}}{dt} & = & \sigma(\tilde{y}-\tilde{x}) \\ \frac{d\tilde{y}}{dt} & = & (r-\mu)(x+m(t))+\mu\tilde{x}-\tilde{y}-(x+m(t))\tilde{z} \\ \frac{d\tilde{z}}{dt} & = & (x+m(t))\tilde{y}-b\tilde{z} \end{array} \tag{16}$$

where $\sigma = 16$, $r = 45.6$, $\mu = 0.98$, and $b = 4$. To show that $\tilde{x}(t) \to x(t)$, we use a Lyapunov function as in [Cuomo & Oppenheim, 1993a,b]. Setting $e_1 = \tilde{x} - x$, $e_2 = \tilde{y} - y$, $e_3 = \tilde{z} - z$, the error dynamics are given by the equations:

$$\dot{e}_1 = \sigma(e_2 - e_1) \tag{17}$$

$$\dot{e}_2 = \mu e_1 - e_2 - (x+m(t))e_3 \tag{18}$$

$$\dot{e}_3 = (x+m(t))e_2 - be_3 \tag{19}$$

The Lyapunov function is given by $E(t) = \frac{1}{2}(\frac{1}{\sigma}e_1^2 + e_2^2 + e_3^2)$, which is a continuously differentiable decrescent positive definite function. Then the derivate of E along trajectories is

$$\dot{E}(t) = -e_1^2 + 1.98e_1e_2 - e_2^2 - be_3^2 \tag{20}$$

$$= -(e_1 - 0.99e_2)^2 - 0.0199e_2^2 - be_3^2 \tag{21}$$

Thus $-\dot{E}(t)$ is a positive definite function and by Lyapunov's direct method [Vidyasagar, 1978], the origin of the error system is (uniformly) asymptotically stable and $e_i \to 0$ as $t \to 0$.

Figure 7 shows computer simulations of the synchronization scheme (16). A sine wave of amplitude 0.01 and frequency $\frac{1.8}{\pi}$ is used as the information signal $m(t)$. Figure 7a shows the time waveform of $x(t)$ in the transmitter and $\tilde{x}(t)$ in the receiver. In Fig. 7b we show the recovered information waveform $\tilde{m}(t) = x(t)+m(t)-\tilde{x}(t)$. We see that after some transient behavior, the recovered waveform $\tilde{m}(t)$ approaches the sine wave $m(t)$.

Acknowledgment

This work is supported in part by the Office of Naval Research under grant N00014-89-J-1402 and by the National Science Foundation under grant MIP 86-14000.

References

A. Arneodo, P. Coullet, & C. Tresser [1981] "Possible new strange attractors with spiral structure," *Commun. Math. Phys.*, **79**, 573–579.

R. W. Brockett [1982] "On conditions leading to chaos in feedback systems," in *Proceedings of the IEEE Conference on decision and control*, 932–936.

T. L. Carroll & L. M. Pecora [1991] "Synchronizing chaotic circuits," *IEEE Transactions on Circuits and Systems*, **38**, 453–456.

L. O. Chua, C. A. Desoer, and E. S. Kuh [1987] *Linear and Nonlinear Circuits* (McGraw-Hill, New York).

L. O. Chua [1992] "The genesis of Chua's circuit," *Archiv für Elektronik und Übertragungstechnik*, 46(4), 250–257.

L. O. Chua, M. Itoh, L. Kocarev, & K. Eckert [1993] "Chaos synchronization in Chua's circuit," *Journal of Circuits, Systems, and Computers*, 3(1), 93–108.

K. M. Cuomo & A. V. Oppenheim [1993a] "Circuit implementation of synchronized chaos with applications to communications," *Physical Review Letters*, **71**(1), 65–68.

K. M. Cuomo & A. V. Oppenheim [1993b] "Chaotic signals and systems for communications," in *Proceedings of 1993 IEEE ICASSP III*, 137–140.

K. S. Halle, L. O. Chua, V. S. Anishchenko, & M. A. Safonova [1992] "Signal amplification via chaos: Experimental evidence," *International Journal of Bifurcation and Chaos*, 2(4), 1011–1020.

K. S. Halle, C. W. Wu, M. Itoh, & L. O. Chua [1993] "Spread spectrum communication through modulation of chaos," *International Journal of Bifurcation and Chaos*, 3(2), 469–477.

R. He & P. G. Vaidya [1992] "Analysis and synthesis of synchronous periodic and chaotic systems," *Physical Review A*, **46**, 7387–7392.

M. P. Kennedy [1992a] "Robust op amp realization of Chua's circuit," *Frequenz*, 46(3–4), 66–80.

M. P. Kennedy [1992b] "Experimental chaos via Chua's circuit," in *Proceedings of the 1st Experimental*

Chaos Conference (S. Vohra, M. Spano, M. Shlesinger, L. Pecora, and W. Ditto, eds.), World Scientific, Singapore, 340–351.

L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, & U. Parlitz [1992] "Experimental demonstration of secure communications via chaotic synchronization," *International Journal of Bifurcation and Chaos*, 2(3), 709–713.

E. N. Lorenz [1963] "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, **20**, 130–141.

R. Madan (Guest Editor) [1993a] *Special Issue on Chua's Circuit: A Paradigm for Chaos, Part I*, vol. 3 of *Journal of Circuit, Systems, and Computers*, World Scientific, Singapore.

R. Madan (Guest Editor) [1993b] *Special Issue on Chua's Circuit: A Paradigm for Chaos, Part II*, vol. 3 of *Journal of Circuit, Systems, and Computers*, World Scientific, Singapore.

Y. Nishio, N. Inaba, & S. Mori [1990] "Chaotic phenomena in an autonomous circuit with nonlinear inductor," in *ISCAS 1990*, 942–945.

M. J. Ogorzalek [1989] "Order and chaos in a third order RC ladder network with nonlinear feedback," *IEEE transactions on circuits and systems*, **36**(9), 1221–1230.

A. L. Oppenheim, G. W. Wornell, S. H. Isabelle, & K. M. Cuomo [1992] "Signal processing in the context of chaotic signals," *Proc 1992 IEEE ICASSP*, **IV**, 117–120.

U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, & A. Shang [1992] "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, 2(4), 973–977.

L. M. Pecora & T. L. Carroll [1990] "Synchronization in chaotic systems," *Physical Review Letters*, **64**, 821–824.

L. M. Pecora & T. L. Carroll [1991] "Driving systems with chaotic signals," *Physical Review A*, **44**, 2374-2383.

C. T. Sparrow [1981] "Chaos in three-dimensional single loop feedback system with a piecewise linear feedback function," *Journal of Mathematical Analysis and Applications*, **83**, 275–291.

M. Vidyasagar [1978] *Nonlinear Systems Analysis* (Prentice-Hall, New Jersey).

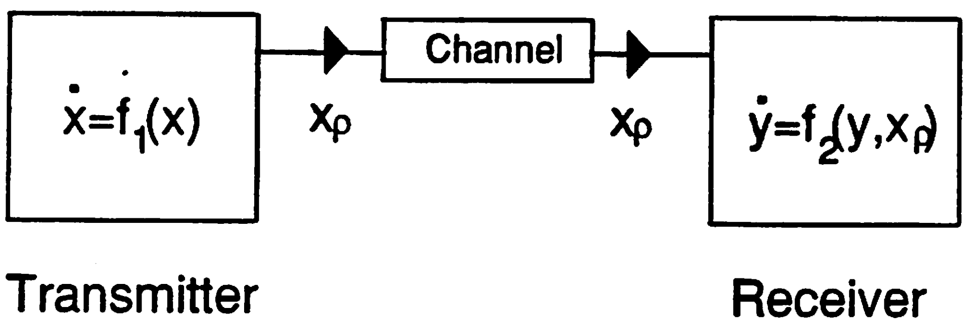
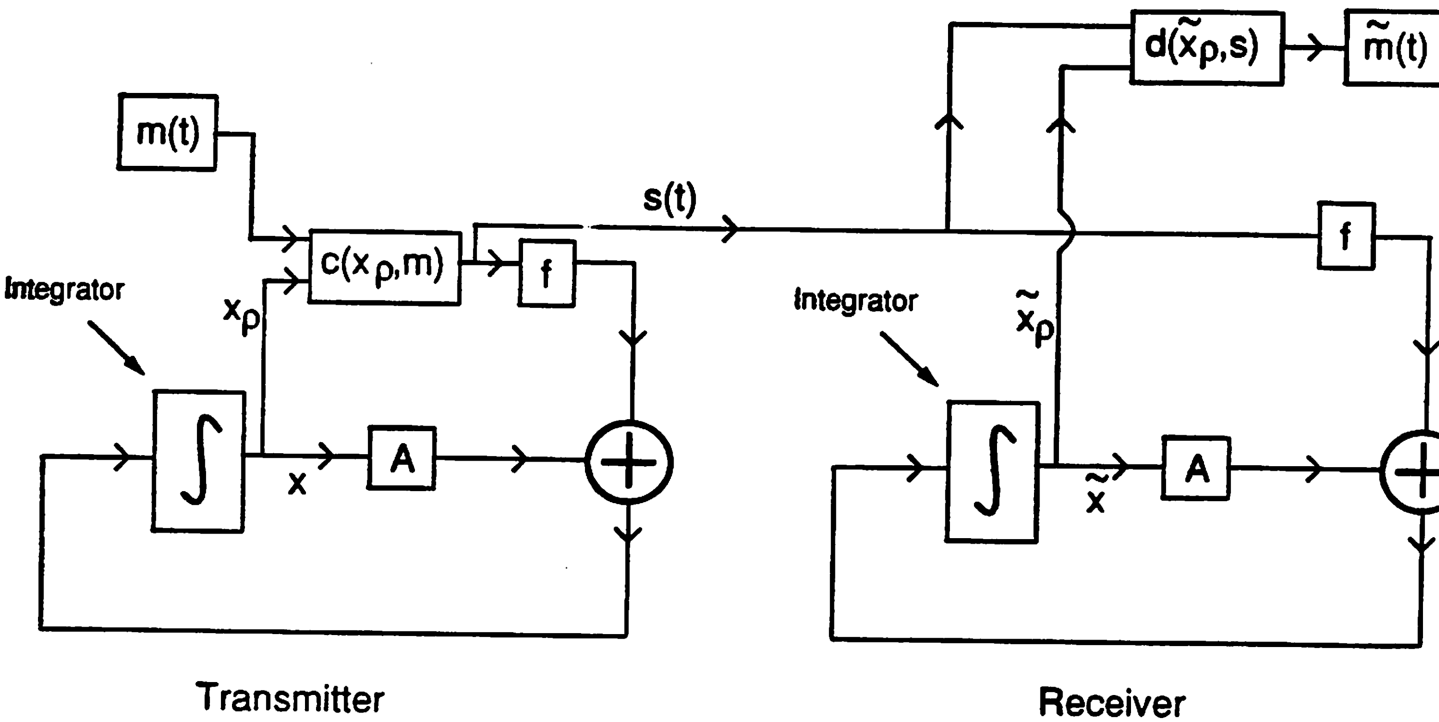


Figure 1



m(t)
c(x ρ,m)
f
s(t)
Integrator
xρ
x
A
Transmitter
d(x̃ρ,s)
m̃(t)
f
Integrator
x̃ρ
x̃
A
Receiver

Figure 2

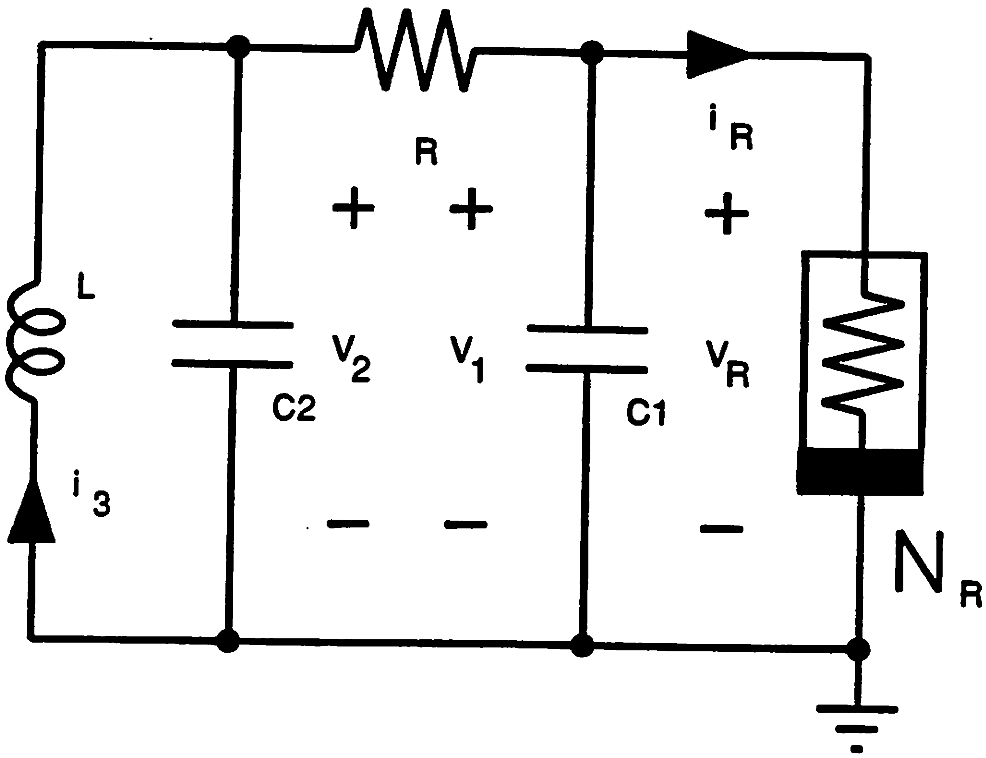
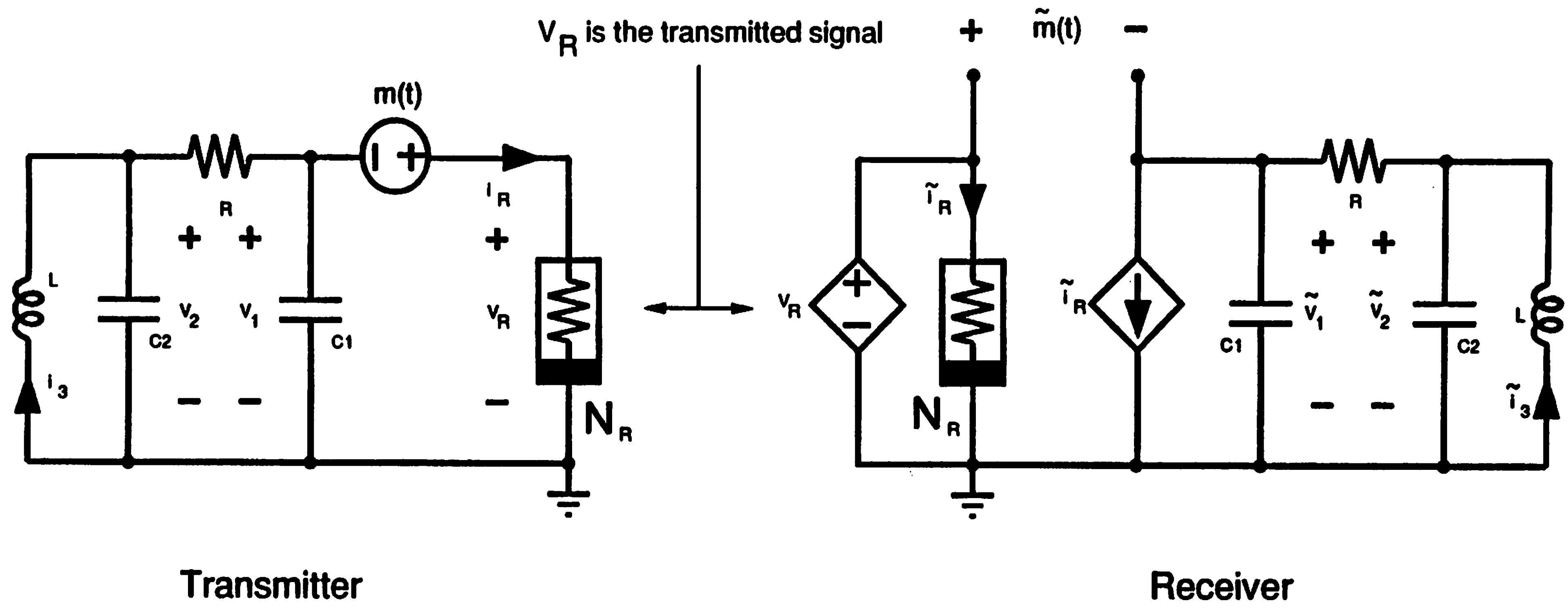


Figure 3



V_R is the transmitted signal
m(t)
i_R
R
L
C2
C1
v_2
v_1
v_R
i_3
N_R
+ m̃(t) −
ĩ_R
v_R
ṽ_1
ṽ_2
ĩ_3
Transmitter
Receiver

Figure 4

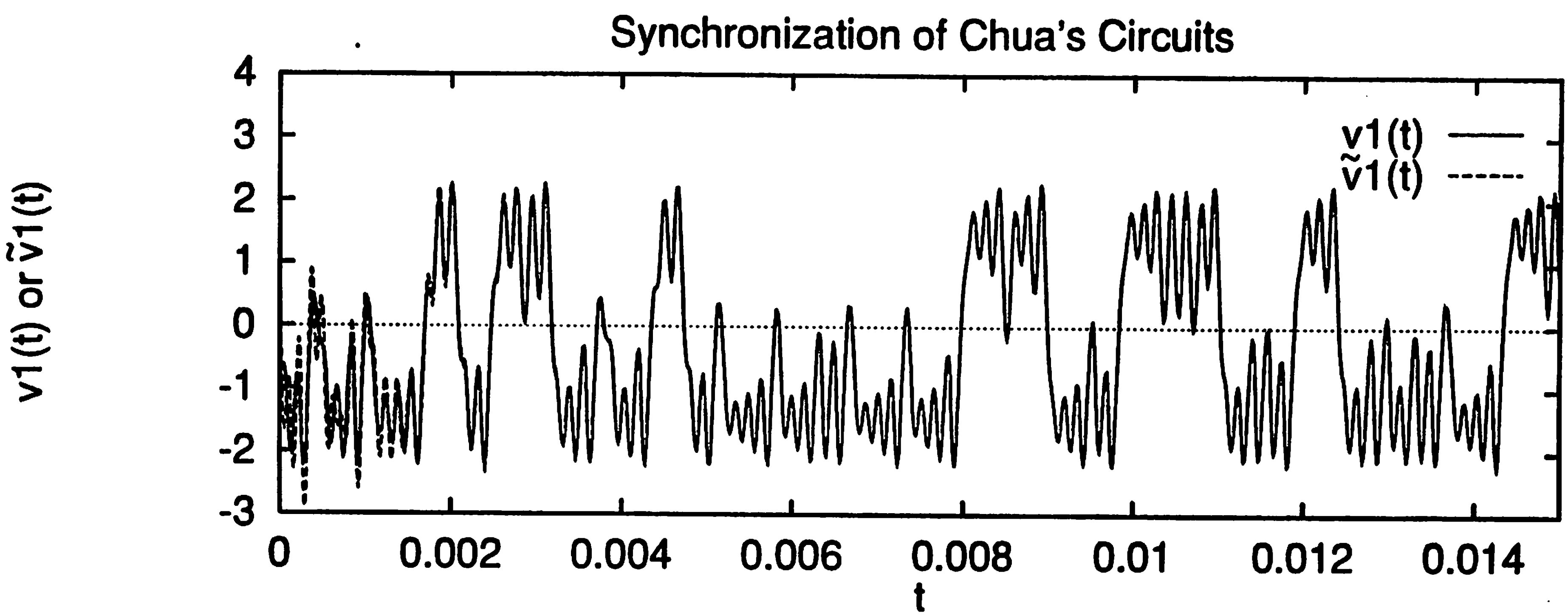

Synchronization of Chua's Circuits
v1(t) or ṽ1(t)
4
3
2
1
0
-1
-2
-3
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
t
v1(t)
ṽ1(t)

Figure 5a

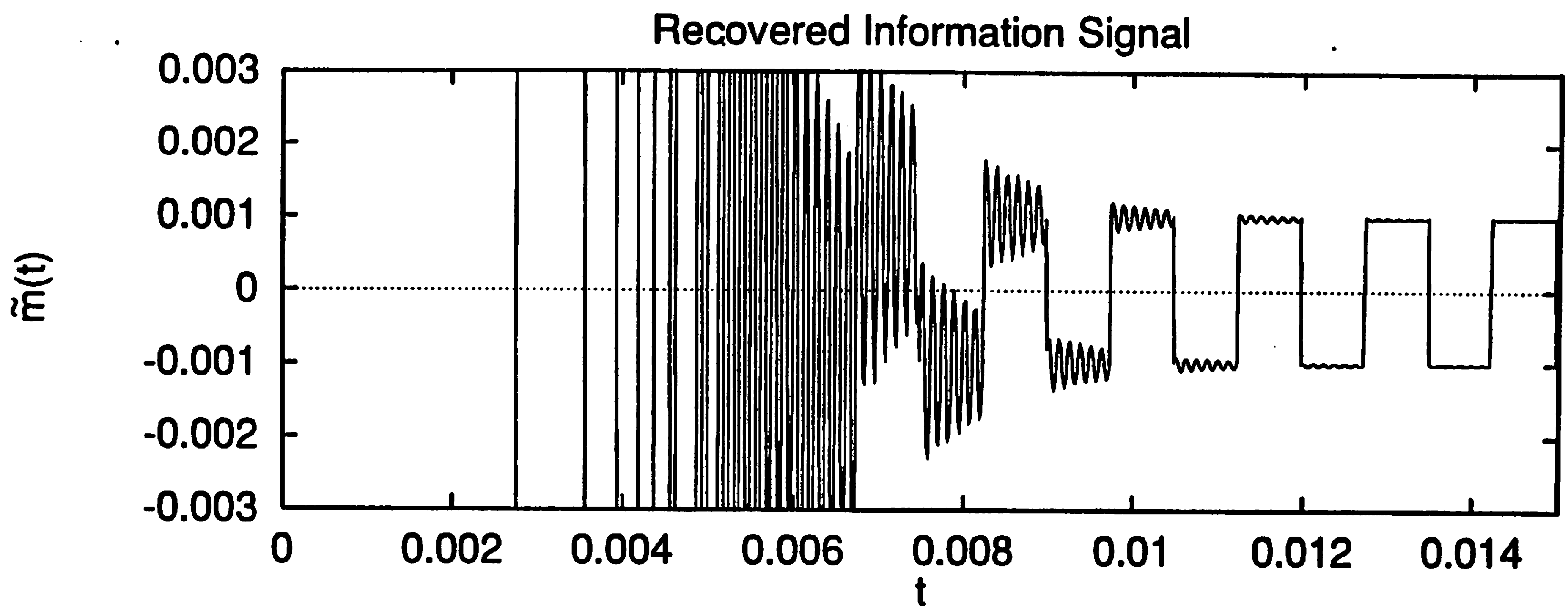

Recovered Information Signal
0.003
0.002
0.001
0
-0.001
-0.002
-0.003
m̃(t)
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
t

Figure 5b

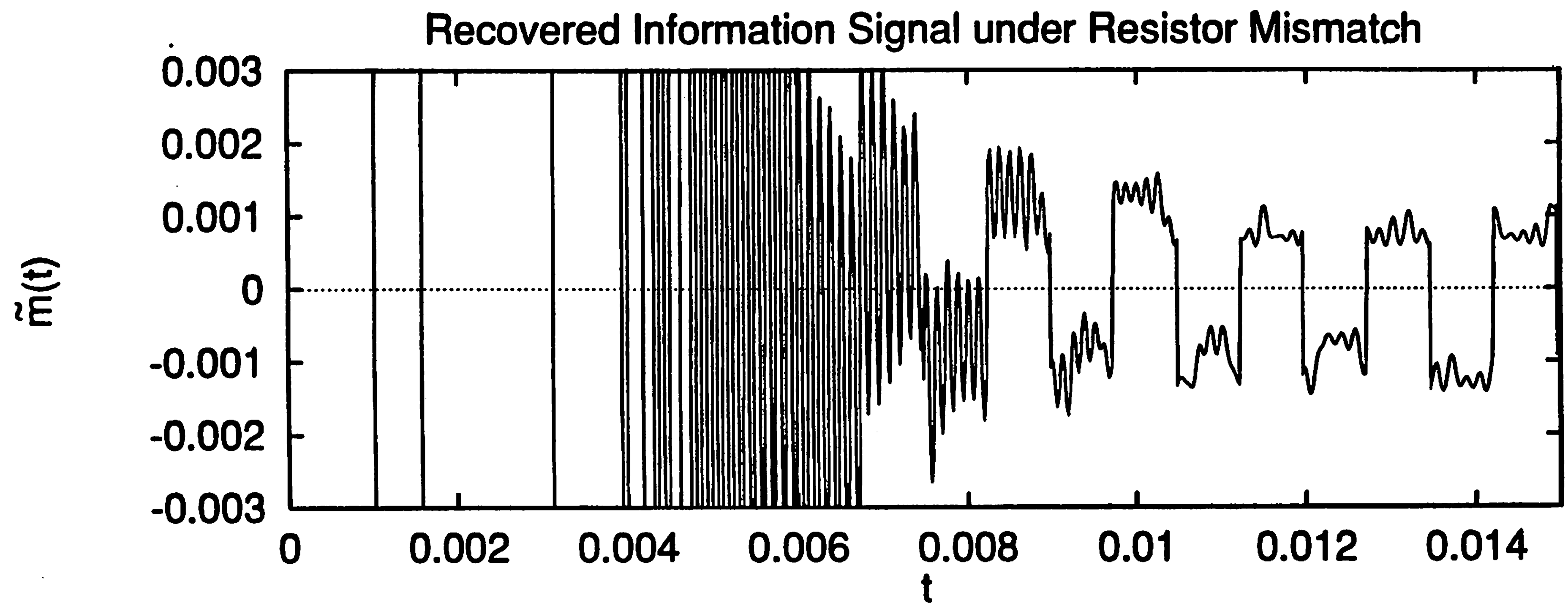
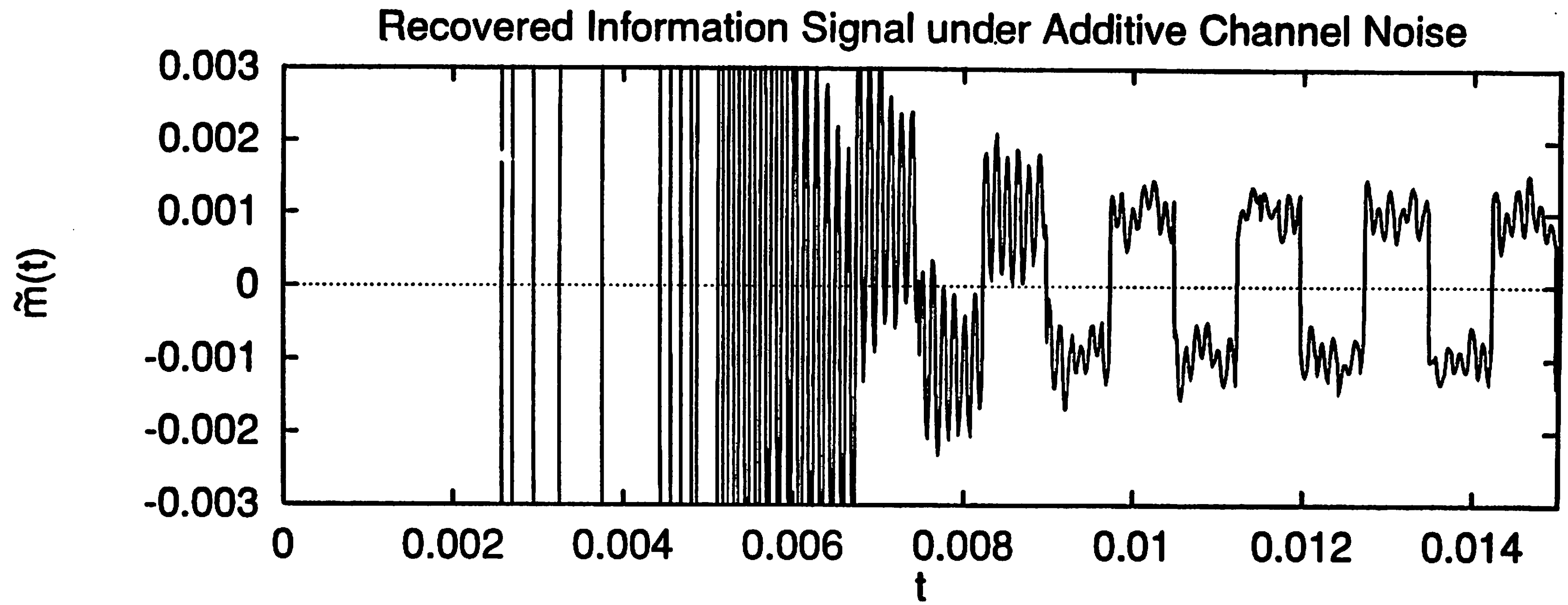
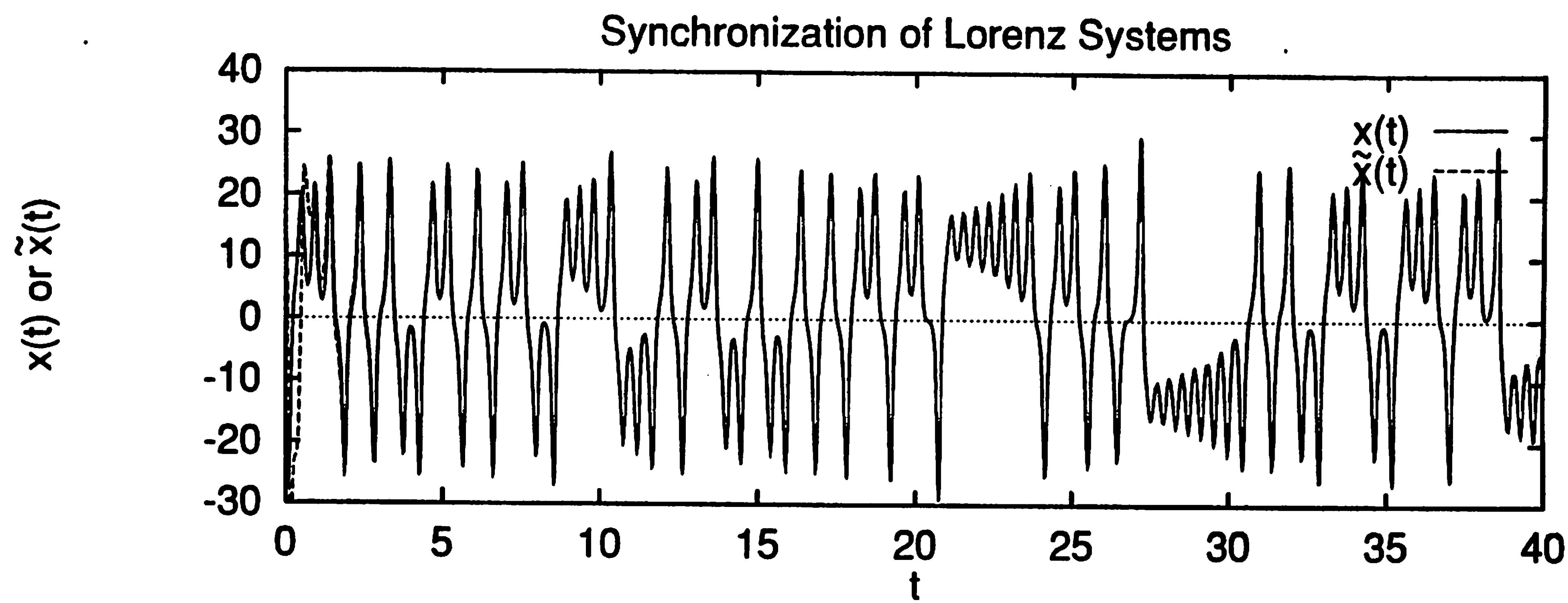

Recovered Information Signal under Resistor Mismatch
0.003
0.002
0.001
0
-0.001
-0.002
-0.003
m̃(t)
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
t

Figure 6a



Recovered Information Signal under Additive Channel Noise
0.003
0.002
0.001
0
-0.001
-0.002
-0.003
$\tilde{m}(t)$
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
t

Figure 6b



Synchronization of Lorenz Systems
x(t) or x̃(t)
40
30
20
10
0
-10
-20
-30
0
5
10
15
20
25
30
35
40
t
x(t)
x̃(t)

Figure 7a

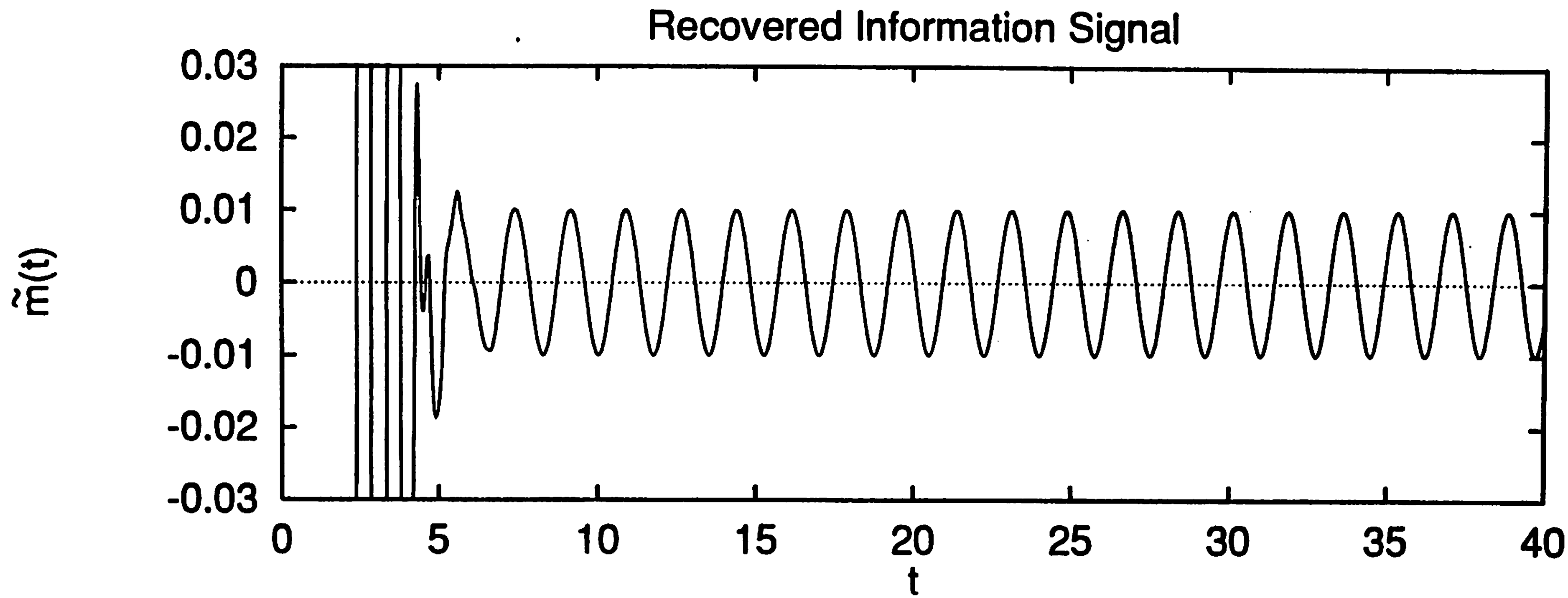

Recovered Information Signal
0.03
0.02
0.01
0
-0.01
-0.02
-0.03
m̃(t)
0
5
10
15
20
25
30
35
40
t

Figure 7b