CHAOTIC SIGNALS AND SYSTEMS FOR COMMUNICATIONS

Kevin M. Cuomo *Alan V. Oppenheim*

Research Laboratory of Electronics
Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139

ABSTRACT

Chaotic systems provide a rich mechanism for signal design and generation for communications and a variety of signal processing applications. Because chaotic signals are typically broadband, noise-like, and difficult to predict they potentially can be utilized in various contexts for masking information-bearing waveforms and as modulating waveforms in spread spectrum systems. In this paper, we propose and demonstrate with a working circuit two approaches to communications based on synchronized chaotic signals and systems. In the first approach a chaotic masking signal is added at the transmitter and regenerated and subtracted at the receiver. The second approach utilizes modulation of the coefficients of the chaotic system in the transmitter and corresponding detection of synchronization error in the receiver to transmit binary-valued bit streams. We demonstrate both approaches using a transmitter circuit with dynamics that are governed by the chaotic Lorenz system. A synchronizing receiver circuit which exploits the ideas of synchronized chaotic systems is used for signal recover.

1. INTRODUCTION

Chaotic systems are nonlinear deterministic systems which can exhibit erratic and irregular behavior. The limiting trajectories of dissipative chaotic systems are attracted to a region in state space which forms a set having fractional dimension and zero volume. 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" and exhibit a sensitive dependence on initial conditions in the sense that any two arbitrarily close initial conditions will lead to trajectories which rapidly diverge.

A particular class of chaotic systems possesses a self-synchronization property [1, 2]. A chaotic system is self-synchronizing if it can be decomposed into at least two subsystems: a drive system and a stable response subsystem(s) that synchronize when coupled with a common drive signal. For some synchronizing chaotic systems the ability to synchronize is robust. For example, the chaotic Lorenz system is decomposable into two separate response subsystems that will each synchronize to the drive system when started from any initial condition. This property leads to some interesting applications, such as spread spectrum communication and signal masking as discussed in [3, 4].

In section 2 we describe the synchronizing characteristics of the Lorenz system of equations and their implementation as an analog circuit. In section 3 we discuss and demonstrate the implementation of the chaotic signal masking technique introduced in [3, 4] utilizing the Lorenz circuit. In section 4 we discuss and demonstrate an approach to binary communication utilizing coefficient modulation in the Lorenz circuit.

2. THE CIRCUIT EQUATIONS

The Lorenz system consists of a set of autonomous ordinary differential equations having a three-dimensional state space. These equations arise in the study of thermal convection [5] and are given by

$$\begin{aligned} \dot{x} &= \sigma(y-x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz \end{aligned} \tag{1}$$

where σ, r, and b are constant coefficients of the system. For our investigations, we use the values $\sigma = 16, r = 45.6$, and $b = 4$ which places the Lorenz system in a chaotic regime.

An interesting property of equation (1) is that it is decomposable into two stable subsystems [1, 2]. Specifically, a stable (x_1, z_1) response subsystem can be defined by

$$\begin{aligned} \dot{x}_1 &= \sigma(y - x_1) \\ \dot{z}_1 &= x_1 y - b z_1 \end{aligned} \tag{2}$$

and a stable (y_2, z_2) response subsystem by

$$\begin{aligned} \dot{y}_2 &= rx - y_2 - x z_2 \\ \dot{z}_2 &= x y_2 - b z_2 \ . \end{aligned} \tag{3}$$

Equation (1) can be interpreted as the drive system since its dynamics are independent of the response subsystems. Equations (2) and (3) represent dynamical response systems which are driven by the drive signals $y(t)$ and $x(t)$ respectively. The eigenvalues of the Jacobian matrix for the (x_1, z_1) response subsystem are equal to $(-\sigma, -b)$. Since they are both negative, $|x_1 - x|$ and $|z_1 - z| \to 0$ as $t \to \infty$. Also, it can be shown numerically that the Lyapunov exponents of the (y_2, z_2) response subsystem are both negative and thus $|y_2 - y|$ and $|z_2 - z| \to 0$ as $t \to \infty$.

The two response subsystems can be used together to regenerate the full-dimensional dynamics which are evolving at the drive system. Specifically, if the input signal to the

This work was sponsored in part by the Air Force Office of Scientific Research under Grant Number AFOSR-91-0034-A, in part by a subcontract from Lockheed Sanders, Inc. under ONR Contract Number N00014-91-C-0125, and in part by the Defense Advanced Research Projects Agency monitored by the Office of Naval Research under Grant N00014-89-J-1489. K. M. Cuomo is supported in part through the MIT/Lincoln Laboratory Staff Associate Program.

0-7803-0946-4/93 $3.00

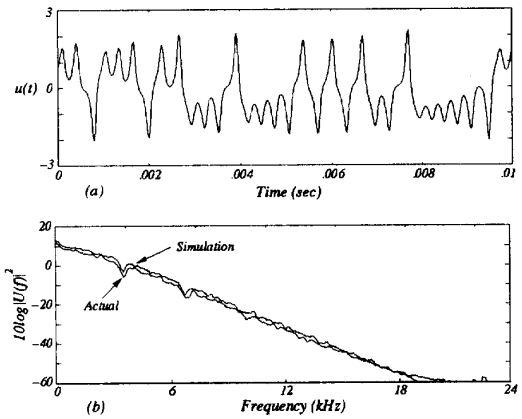

Figure 1: *Circuit Data: (a) A sample function of $u(t)$. (b) Averaged power spectrum of $u(t)$.*

(y_2, z_2) subsystem is $x(t)$, then the output $y_2(t)$ can be used to drive the (x_1, z_1) subsystem and subsequently generate a "new" $x(t)$ in addition to having obtained, through synchronization, $y(t)$ and $z(t)$. It is important to recognize that the two response subsystems given by equations (2) and (3) can be combined into a single system having a three-dimensional state space. This produces a full-dimensional response system which is structurally similar to the drive system (1). Further discussion of this result is given below where we describe the circuit implementation.

A direct implementation of equation (1) with an electronic circuit presents several difficulties. For example, the state variables in equation (1) occupy a wide dynamic range with values that exceed reasonable power supply limits. However, this difficulty can be eliminated by a simple transformation of variables. Specifically, we define new variables by $u = x/10, v = y/10$, and $w = z/20$. With this scaling, the Lorenz equations are transformed into

$$\begin{aligned} \dot{u} &= \sigma(v-u) \\ \dot{v} &= ru - v - 20uw \\ \dot{w} &= 5uv - bw \ . \end{aligned} \tag{4}$$

This system, which we refer to as the transmitter, can be more easily implemented with an electronic circuit because the state variables all have similar dynamic range and circuit voltages remain well within the range of typical power supply limits. We emphasize that our analog circuit implementation of (4) is exact, and not based on a piecewise linear approach as was used in [6].

To illustrate the chaotic behavior of the transmitter circuit, an analog-to-digital (A/D) data recording system was used to sample the appropriate circuit outputs at a 48 kHz rate and with 16-bit resolution. Figure 1(a) and (b) show a sample function and averaged power spectrum corresponding to the circuit waveform $u(t)$. The power spectrum is broad-band which is typical of a chaotic signal. Figure 1(b) also shows a power spectrum obtained from a numerical simulation of the Lorenz equations. As we see, the performance of the circuit and the simulation are consistent. Figure 2(a) and (b) show the circuit's chaotic attractor projected onto the uv-plane and uw-plane respectively. These data were obtained from the circuit using the stereo recording capability of the A/D system. Specifically, x-axis signals were applied to the left channel and y-axis signals were applied to the right channel, and then simultaneously sampled at a 48-kHz rate and with 16-bit resolution. The circuit's attractor is consistent with numerical simulation. A more detailed analysis of the transmitter circuit is given in [7].

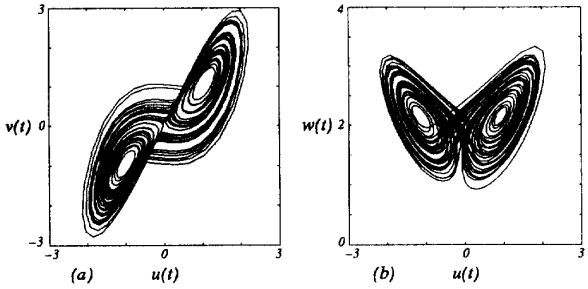

Figure 2: *Circuit Data: (a) Chaotic attractor projected onto uv-plane. (b) Chaotic attractor projected onto uw-plane.*

A full-dimensional response system which will synchronize to the chaotic signals evolving at the transmitter (4) is given by

$$\begin{aligned} \dot{u}_r &= \sigma(v_r - u_r) \\ \dot{v}_r &= ru - v_r - 20uw_r \\ \dot{w}_r &= 5uv_r - bw_r \ . \end{aligned} \tag{5}$$

This system is referred to as the "u-drive" system or as the receiver in light of the various communications applications made possible using this system. For simplicity in notation we will refer to the transmitter state variables collectively by the vector $\mathbf{d} = [u, v, w]$ and to the receiver variables by the vector $\mathbf{r} = [u_r, v_r, z_r]$ when convenient.

It is straightforward to show analytically that synchronization in the Lorenz system is a global property of the nonlinear error dynamics between the transmitter and receiver. First, the dynamical errors, $\mathbf{e}$, are defined as

$$\mathbf{e} = \mathbf{d} - \mathbf{r} \ .$$

Under the condition of perfect coefficient matching between the transmitter and receiver a set of equations which govern the error dynamics are given by

$$\begin{aligned} \dot{e}_1 &= \sigma(e_2 - e_1) \\ \dot{e}_2 &= -e_2 - 20u(t)e_3 \\ \dot{e}_3 &= 5u(t)e_2 - be_3 \ . \end{aligned} \tag{6}$$

The origin of the error system is asymptotically stable provided that $\sigma, b > 0$. This result follows by considering the three-dimensional Lyapunov function defined by $E(\mathbf{e}, t) = \frac{1}{2}(\frac{1}{\sigma}e_1^2 + e_2^2 + 4e_3^2)$. The time rate of change of $E(\mathbf{e}, t)$ along trajectories is given by

$$\begin{aligned} \dot{E}(\mathbf{e}, t) &= \tfrac{1}{\sigma}e_1\dot{e}_1 + e_2\dot{e}_2 + 4e_3\dot{e}_3 \\ &= -(e_1 - \tfrac{1}{2}e_2)^2 - \tfrac{3}{4}e_2^2 - 4be_3^2 \\ &< 0 \end{aligned} \tag{7}$$

which shows that $E(\mathbf{e}, t)$ decreases for all points in the systems state space. Furthermore, since the divergence of the vector field of (6) is a negative constant, equal to $-(\sigma + b + 1)$, it follows that any error volume will go to zero exponentially fast.

3. CHAOTIC SIGNAL MASKING

In this section, we discuss and demonstrate with a working circuit, chaotic signal masking. Our objective is to demonstrate the signal masking idea described in [3, 4] and to

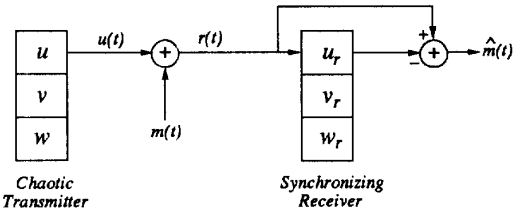

Figure 3: *Chaotic Signal Masking System.*

further illustrate that synchronizing chaotic systems offer potential opportunity for novel approaches to secure communications. 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. The basic idea is to use the received signal to regenerate the masking signal at the receiver and subtract it from the received signal to recover $m(t)$. This can be done with the synchronizing receiver circuit since the ability to synchronize is robust, *i.e.* is not highly sensitive to perturbations in the drive signal and thus can be done with the masked signal. While there are many possible variations, consider, for example, a transmitted signal of the form $r(t) = u(t)+m(t)$. It is assumed that for masking, the power level of $m(t)$ is significantly lower than that of $u(t)$. The 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

$$\begin{aligned} \dot{u}_r &= 16(v_r - u_r) \\ \dot{v}_r &= 45.6r(t) - v_r - 20r(t)w_r \\ \dot{w}_r &= 5r(t)v_r - 4w_r \ . \end{aligned} \tag{8}$$

If the receiver has synchronized with $r(t)$ as the drive, then $u_r(t) \simeq u(t)$ and consequently $m(t)$ is recovered as $\hat{m}(t) = r(t) - u_r(t)$. Figure 3 illustrates the approach.

In [3] the feasibility of the approach was demonstrated through numerical simulation with almost perfect signal recovery. Using the working transmitter and receiver circuits, we demonstrate the performance of this system in figure 4 with a segment of speech from the sentence "He has the bluest eyes". The waveforms were obtained by sampling the appropriate circuit outputs at a 48 kHz rate and with 16-bit resolution. Figure 4(a) and (b) show the original speech, $m(t)$, and the recovered speech signal, $\hat{m}(t)$, respectively. Clearly, the speech signal has been recovered. Although more distortion is evident in the recovered waveform with the actual circuit implementation as compared with the numerical simulation in [3], the output is very intelligible in informal listening tests. Figure 5 illustrates that the power spectra of the chaotic masking signal, $u(t)$, and the speech are highly overlapping with an average signal-to-masking ratio of approximately -20dB.

4. CHAOTIC DIGITAL COMMUNICATION

In this section, we propose the use of synchronized chaotic systems to transmit and recover binary-valued bit streams. Synchronized chaotic systems are well suited to this application because the chaotic signals they produce have noise-like characteristics and the receiver is robust to uncertainties in the transmitter's initial condition.

The error dynamics of the Lorenz u-drive system are exponentially stable provided that the transmitter and receiver coefficients are identical. This suggests a way in

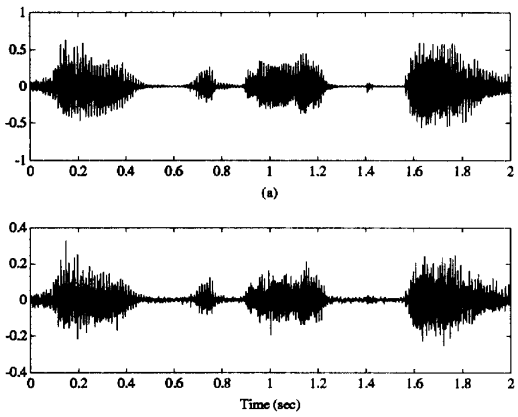

Figure 4: *Circuit Data: Speech Waveforms: (a) Original. (b) Recovered.*

which an information-bearing waveform could be embedded in a chaotic carrier and extracted at the receiver. The basic idea is to modulate a transmitter coefficient with the information-bearing waveform and to transmit the chaotic drive signal. Because of the modulation embedded in the carrier a time-varying coefficient mismatch exists between the transmitter and receiver. Upon reception, the coefficient mismatch will produce a synchronization error between the received drive signal and the receiver's regenerated drive signal with an error signal amplitude that depends on the modulation present. Using the synchronization error the coefficient mismatch can be detected and exploited in various ways for information transfer.

This modulation/detection process is illustrated in figure 6. In this figure, the coefficient "b" of the transmitter equations (4) is modulated by the information waveform, $m(t)$. The coefficients σ and r could also be used as the modulation coefficient, however, in [7] we show that there are some advantages to choosing b as the modulation coefficient. The information is carried over the channel by the chaotic signal $u_m(t)$ and the received signal, $r(t) = u_m(t) + n(t)$, serves as the driving input to the receiver. At the receiver the modulation is detected by forming the difference between $r(t)$ and the reconstructed drive signal, $u_r(t)$. If we assume that the signal-to-noise ratio of $r(t)$ is large, the error signal $e_1(t) = r(t) - u_r(t)$ will have a small average power if no modulation is present. However if, for example, the information waveform is a binary-valued bit stream, with a "1" representing a coefficient mismatch and a "0" representing no coefficient mismatch, then $e_1(t)$ will be relatively large in amplitude during the time period that a "1" is transmitted and small in amplitude during a "0" transmission. The synchronizing receiver can thus be viewed as a form of matched filter for the chaotic transmitter signal $u(t)$.

For purposes of demonstrating the technique, we use a square-wave for the information-bearing waveform as illustrated in figure 7(a). The square-wave produces a variation in the transmitter coefficient "b" with the zero-bit and one-bit coefficients corresponding to $b(0) = 4$ and $b(1) = 4.4$ respectively. The resulting modulated drive signal, $u_m(t)$, is used as the drive input to the synchronizing receiver system as depicted in figure 6. For transmission privacy it is

important that the characteristics of the drive signal not be significantly altered by the presence of the modulation. A comparison of the averaged power spectrum of the drive signal with and without the embedded square-wave present shows that the power spectra are very similar and the presence of the embedded square-wave is not at all obvious [7]. Figure 7(b) shows the synchronization error power, $e_1^2(t)$, at the output of the receiver circuit. As expected, the coefficient mismatch between transmitter and receiver produces significant synchronization error power during a "1" transmission and very little error power during a "0" transmission. Also evident from this figure is the fast response time of the receiver at the transitions between the zero and one bits. Figure 7(c) illustrates that the square-wave modulation can be reliably recovered by lowpass filtering the synchronization error power waveform and applying a threshold test.

5. CONCLUSIONS

In this paper, we described and demonstrated with a working circuit, two approaches to private communications based on chaotic signals and systems. Using a signal masking approach we have shown that analog signals can be privately transmitted and recovered at the intended receivers. Also, signals represented as binary-valued bit streams can be privately communicated by modulating a transmitter coefficient with the information-bearing waveform and detecting the information with a synchronizing receiver circuit. These approaches were demonstrated using a transmitter circuit with dynamics that are governed by the chaotic Lorenz system. A synchronizing receiver circuit which exploits the ideas of synchronized chaotic systems was used for signal recover. We are actively investigating these methods as well as alternative approaches to secure communications based chaotic signals and systems.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821-824, Feb. 1990.

[2] T. L. Carroll and L. M. Pecora, "Synchronizing Chaotic Circuits," *IEEE Transactions on Circuits and Systems*, vol. 38, no. 4, pp. 453-456, April 1991.

[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Isabelle, "Spread Spectrum Modulation and Signal Masking Using Synchronized Chaotic Systems," *MIT Research Laboratory of Electronics Technical Report 570*, Feb. 1992.

[4] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signal Processing in the Context of Chaotic Signals," *Proc. IEEE ICASSP-92*, Mar. 1992.

[5] E. N. Lorenz "Deterministic Nonperiodic Flow," *Journal of the Atmospheric Sciences*, vol. 20, pp. 130-141, 1963.

[6] R. Tokunaga, M. Komuro, T. Matsumoto, and L. O. Chua "Lorenz Attractor From an Electrical Circuit With Uncoupled Continuous Piecewise-Linear Resistor," *Intl. Jrnl. of Ckt. Theory and Applications*, vol. 17, pp. 71-85, 1989.

[7] K. M. Cuomo and A. V. Oppenheim "Synchronized Chaotic Circuits and Systems for Communications," *MIT Research Laboratory of Electronics Technical Report 575*, Nov. 1992.

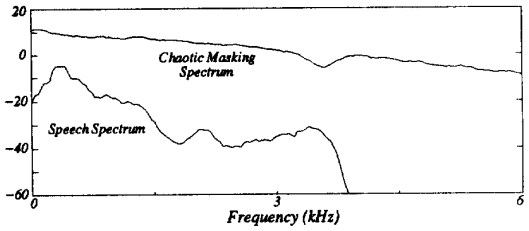

Figure 5: *Circuit Data: Power Spectra of Chaotic Masking and Speech Signals.*

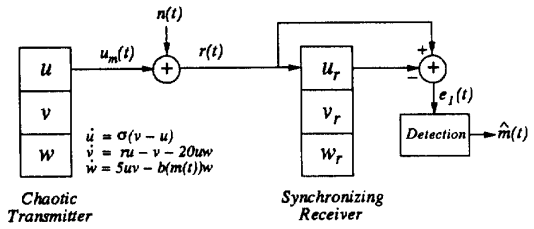

Figure 6: *Chaotic Communication System.*

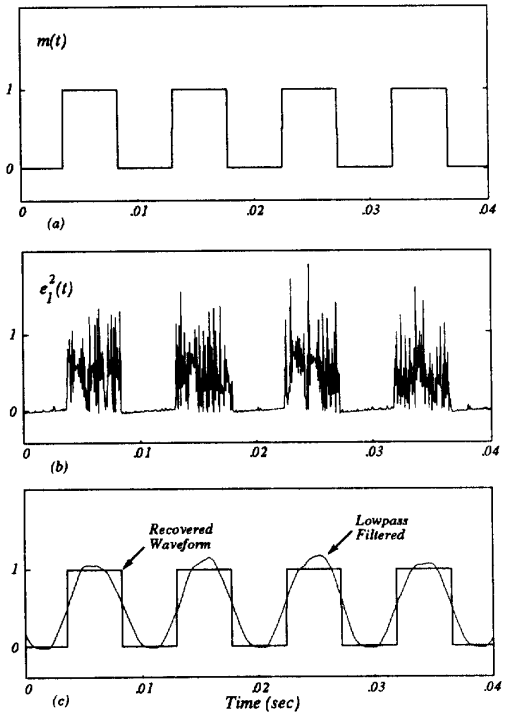

Figure 7: *Circuit Data: (a) Modulation Waveform. (b) Synchronization Error Power. (c) Recovered Modulation Waveform.*