CHANNEL-INDEPENDENT CHAOTIC SECURE COMMUNICATION

by

Tao Yang and Leon O. Chua

Memorandum No. UCB/ERL M96/77

5 December 1996

CHANNEL-INDEPENDENT CHAOTIC SECURE COMMUNICATION

by

Tao Yang and Leon O. Chua

Memorandum No. UCB/ERL M96/77

5 December 1996

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Channel-Independent Chaotic Secure Communication

Tao Yang and *Leon O. Chua*
Electronics Research Laboratory and
Department of Electrical Engineering and Computer Sciences,
University of California at Berkeley,
Berkeley, CA 94720, U.S.A.

Abstract

The generalized synchronization (GS) of two identical chaotic systems through an unknown channel is studied. First, some theoretical results of GS through an unknown channel are derived. Finally, an application of GS to channel-independent chaotic secure communication is presented.

1 Introduction

The basic setup in most chaos-based synchronization schemes for secure communication systems consists of a specially-designed transmitter and a receiver. To enhance the degree of security, we always send a chaotic signal to the receiver. It is well-known, however, that if the transmitted signal is too "simple", then security cannot be guaranteed[Yang, 1995, Short, 1994]. On the other hand, if a more complex signal, e.g., a hyper-chaotic signal, is used as the transmitted signal, the robustness of the synchronization will be weakened. Moreover, it will be very difficult to design adaptive methods for compensating the inevitable parameter mismatch and channel distortions [Chua *et al.*, 1996a, Chua *et al.*, 1996b, Wu *et al.*, 1996].

A simple method had been proposed [Yang *et al.*, 1996] for enhancing the security of low-dimensional secure communication schemes so that it would be difficult to break them with current cryptanalysis techniques for chaotic systems[Yang, 1995, Short, 1994].

Non-ideal channels pose a serious problem in chaos-based secure communication schemes. The experimental results in [Chua *et al.*, 1996a, Chua *et al.*, 1996b] have demonstrated that a time-varying or distorted channel can desynchronize the systems. In [Chua *et al.*, 1996a] and [Chua *et al.*, 1996b], the authors used an adaptive channel compensation method to overcome the non-ideal channel problem. Recently, Carroll [1996] presented an amplitude-independent synchronization scheme, which was very promising for overcoming the non-ideal channel problem. In this letter, we study the channel-independent synchronization problem in the more general framework of *generalized synchronization*(GS)[Kocarev & Parlitz, 1996, Rulkov *et al.*, 1996].

While most previous works would scramble the message signal with only one chaotic state variable, Yang *et al.* [1996] had presented a message scrambling scheme which used two chaotic state-variables. In this letter, we propose the possibility of utilizing the non-ideal channel property to scramble the message signal. This channel scrambling scheme is used to overcome the time series identification attack scheme presented in [Short, 1994], which is sensitive to the amplitude of the transmitted signal.

2 Generalized synchronization through non-ideal channels

Consider two dynamical systems

$$\begin{cases} \dot{\mathbf{x}} = f(\mathbf{x}) & \leftarrow \textit{driving system} \\ \dot{\mathbf{y}} = g(\mathbf{y}, h(\mathbf{x})) & \leftarrow \textit{driven system} \end{cases} \tag{1}$$

where $\mathbf{x} \in R^n, \mathbf{y} \in R^m$, $h : R^n \mapsto R^m$ is an arbitrary function.

Definition 1: *Generalized synchronization(GS)[Kocarev & Parlitz, 1996, Rulkov* et al., *1996]*

The two systems in (1) are said to be in a state of generalized synchronization, henceforth

referred to as GS, if there exist a transformation $H : R^n \mapsto R^m$, a manifold $M = \{(\mathbf{x}, \mathbf{y}) | \mathbf{y} = H(\mathbf{x})\}$, and a set $B \subset R^n \times R^m$ with $M \subset B$ such that all trajectories of (1) with initial conditions in B approach M as $t \longrightarrow \infty$.

Remark: Synchronization in the normal sense is a special case of GS with $m = n$, and $H(\mathbf{x}) = \mathbf{x}$.

Assume that a chaotic system can be decomposed into two parts

$$\dot{\mathbf{x}} = \phi(\mathbf{x}) + \psi(\mathbf{x}) \tag{2}$$

where $\phi(\mathbf{x})$ satisfies the condition

$$\phi(\lambda \mathbf{x}) = \lambda \phi(\mathbf{x}) \tag{3}$$

where $\lambda \in R$ is a nonzero constant. Let the signal $\psi(\mathbf{x})$ be transmitted to the driven system and consider the unidirectional synchronization scheme

$$\begin{cases} \dot{\mathbf{x}} = \phi(\mathbf{x}) + \psi(\mathbf{x}) & \leftarrow \textit{driving system} \\ \dot{\mathbf{y}} = \phi(\mathbf{y}) + \lambda\psi(\mathbf{x}) & \leftarrow \textit{driven system} \end{cases} \tag{4}$$

where $\lambda \neq 0$ is the channel gain.

Theorem 1: *If $\phi(\mathbf{x})$ is decreasing in $D \in R^n$, $\mathbf{x}_0 \in D$ and $\frac{1}{\lambda}\mathbf{y}_0 \in D$, then the two dynamic systems in Eq.(4) are GS via the transformation*

$$H(\mathbf{x}) = \lambda \mathbf{x} \tag{5}$$

Proof: Since $\lambda \neq 0$, let $\mathbf{z} = \frac{1}{\lambda}\mathbf{y}$ and recast the driven system in Eq.(4) into

$$\begin{aligned} \dot{\mathbf{z}} &= \frac{1}{\lambda}\phi(\mathbf{y}) + \psi(\mathbf{x}) \\ &= \phi(\frac{1}{\lambda}\mathbf{y}) + \psi(\mathbf{x}) \\ &= \phi(\mathbf{z}) + \psi(\mathbf{x}) \end{aligned} \tag{6}$$

Let the error be $\mathbf{e} = \mathbf{x} - \mathbf{z}$ so that the error system is given by

$$\dot{\mathbf{e}} = \phi(\mathbf{x}) - \phi(\mathbf{z}) \tag{7}$$

Since $\frac{1}{\lambda}\mathbf{y}_0 \in D$, we have $\mathbf{z}_0 \in D$. Construct the Lyapunov function

$$V = \frac{1}{2}\mathbf{e}^T\mathbf{e} \tag{8}$$

Observe that

$$\dot{V} = \mathbf{e}^T\dot{\mathbf{e}} = \mathbf{e}^T(\phi(\mathbf{x}) - \phi(\mathbf{z})) \leq 0 \tag{9}$$

Since $\phi(.)$ is decreasing in D, by hypothesis, the last inequality is satisfied, and the **x**-**z** system is identically synchronized (synchronization in the common sense) as $t \longrightarrow \infty$, i.e.,

$$\lim_{t\to\infty} \mathbf{y}(t) = \lim_{t\to\infty} \lambda\mathbf{z}(t) = \lambda\mathbf{x}(t) \tag{10}$$

It follows that $\mathbf{y} = H(\mathbf{x}) = \lambda\mathbf{x}$ is the associated GS transformation.□

Example

Consider the Chua's oscillator defined by[Chua, 1993]

$$\begin{cases} \dot{x} = \alpha[y - x - f(x)] \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \tag{11}$$

where

$$f(x) = bx + \frac{1}{2}(a - b)(|x + 1| - |x - 1|) \tag{12}$$

Equation (11) can be decomposed as follow:

$$\underbrace{\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix}}_{\dot{\mathbf{x}}} = \underbrace{\begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}}_{\phi(\mathbf{x})} + \underbrace{\begin{pmatrix} -\alpha f(x) \\ 0 \\ 0 \end{pmatrix}}_{\psi(\mathbf{x})} \tag{13}$$

If $\phi(\mathbf{x})$ is decreasing globally[1], we have $D = R^3$. It follows that we only need to transmit a scalar signal $f(x)$ for achieving GS. The receiver system is simply:

$$\underbrace{\begin{pmatrix} \dot{x}_1 \\ \dot{y}_1 \\ \dot{z}_1 \end{pmatrix}}_{\dot{\mathbf{x}}_1} = \underbrace{\begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}}_{\phi(\mathbf{x}_1)} + \lambda \underbrace{\begin{pmatrix} -\alpha f(x) \\ 0 \\ 0 \end{pmatrix}}_{\psi(\mathbf{x})} \tag{14}$$

Our simulation results are shown in Fig.1. Fig.1(a) shows the attractor of the driving system, which resembles the lower branch of a Chua's spiral attractor. The Lissajous figures, henceforth called the GS plots between the three respective pairs of variables x_1 vs. x, y_1 vs. y, and z_1 vs. z, are shown in Figs.1(b), 1(c), and 1(d), respectively. Observe that the

[1] We can choose α, β and γ such that the following matrix

$$\begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}$$

is negative definite. It follows from Theorem 4 in [Wu & Chua, 1994] that $\phi(\mathbf{x})$ is decreasing globally.

associated GS transformation function $H(\cdot)$ for these systems is *linear* in accordance with Eq.(5) of Theorem 1. Comparing the two attractors in Figs.1(a) and 1(e) one can see that they have the same shape. Indeed, they are scaled versions of each other.

3 Secure Communication

In this section, we propose an application of the preceding channel-independent GS schemes to chaotic secure communication of *binary* signals. Our proposed scheme is significant because practical channels are always distorted. We will use a chaotic switching scheme to scramble the binary message signal. At the transmitter end, the binary signal is used to switch some parameter of the function $\psi(\mathbf{x})$ between two parameter sets, which correspond to bit-0 and bit-1, respectively. At the receiver end, our parameter change can be detected by comparing the received signal and a state-variable signal generated by the receiver. The block diagram of our proposed scheme is shown in Fig.2. Observe that before the signal is transmitted to the channel, we use a *random* gain to scramble it. Observe also that a clock signal is used to ensure that during the time period of every bit, the adaptable gain is kept unchanged.

Observe that our random signal can be a *truly random signal*[2] sampled from the real physical world and that both the transmitter and the receiver do not need to know anything about this random sequence. However, for an intruder trying to figure out the message signal from the transmitted signal by using standard identification methods, he has to figure out first what the random sequence is. This security improvement scheme can be efficiently used to protect our system from such possible eavesdropper *attack* proposed in [Short, 1994].

In the following illustrations, we will use Chua's oscillators as the chaotic transmitter and receiver. For convenience of hardware implementation, we will use the following actual circuit equations of Chua's oscillator

$$\begin{cases} \frac{dv_1}{dt} = \frac{1}{C_1}[G(v_2 - v_1) - f(v_1)] \\ \frac{dv_2}{dt} = \frac{1}{C_2}[G(v_1 - v_2) + i_3] \\ \frac{di_3}{dt} = \frac{1}{L}[-v_2 - R_0 i_3] \end{cases} \tag{15}$$

[2]Here, a *truly random signal* means that even the transmitter cannot reproduce this random signal.

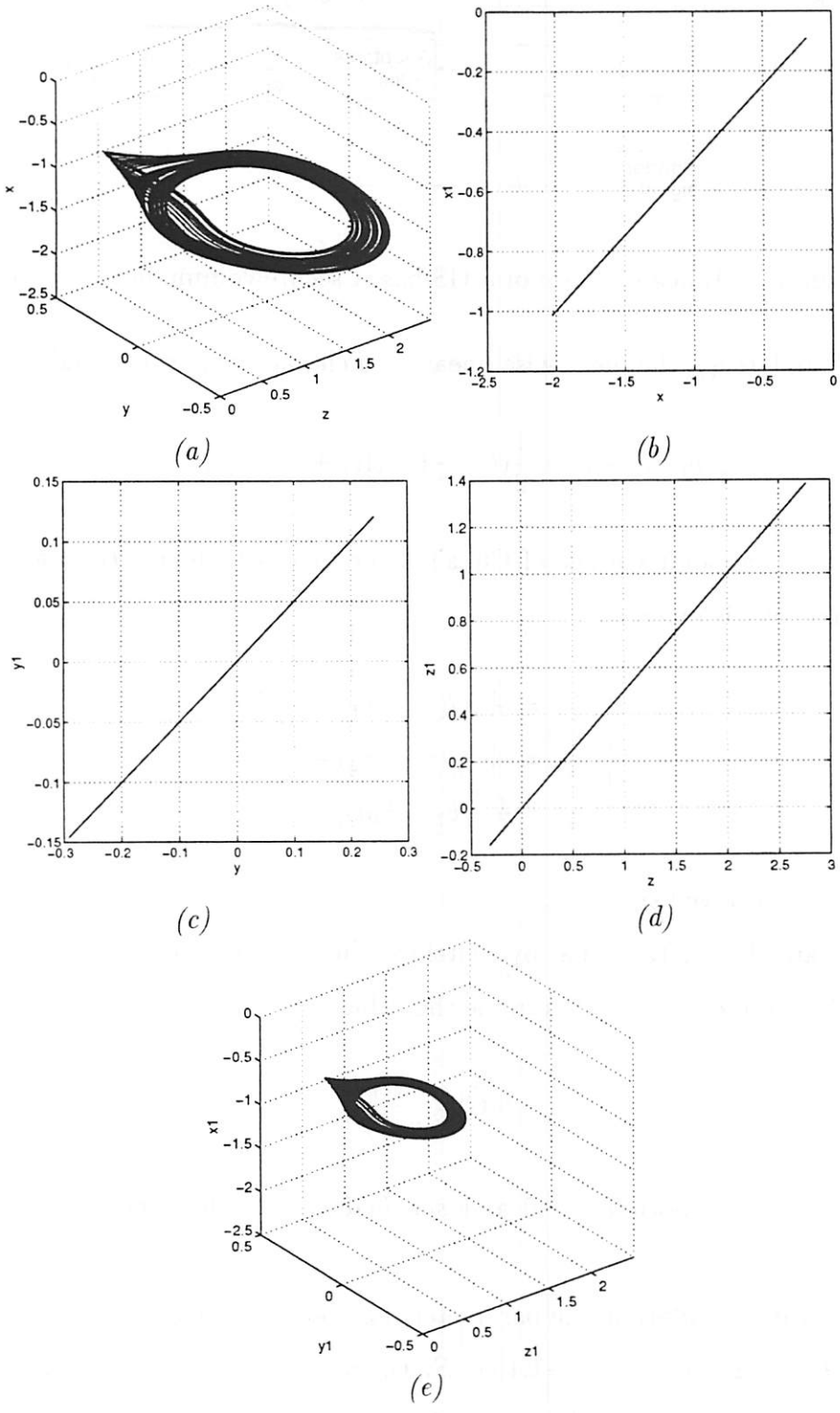


Figure 1: Simulation results with a linear channel with unknown gain. (a) Attractor of the driving system. (b) the $x - x_1$ GS plot. (c) the $y - y_1$ GS plot. (d) the $z - z_1$ GS plot. (e) Corresponding attractor of the driven system.

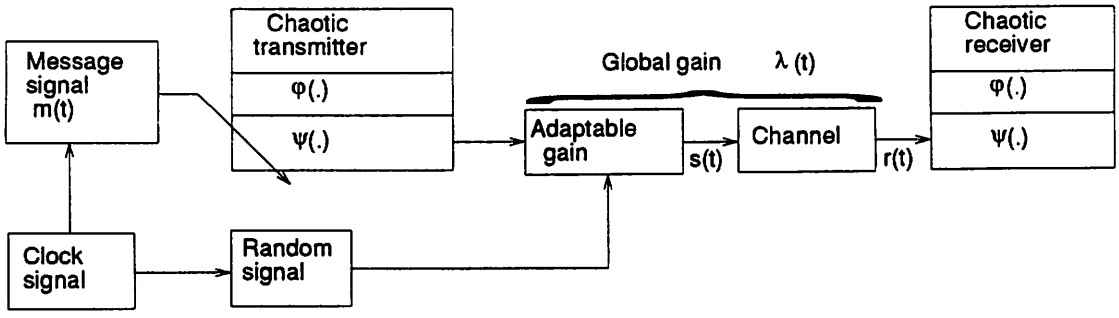


Figure 2: Block diagram of a GS-based secure communication scheme.

where $G = \frac{1}{R}$ and $f(v_1)$, the piece-wise linear $v - i$ characteristics of Chua's diode, is given by

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{16}$$

where E is the breakpoint voltage of Chua's diode. We will choose $f(v_1)$ as our transmitted signal. The receiver is given by:

$$\begin{cases} \frac{d\hat{v}_1}{dt} = \frac{1}{C_1}[G(\hat{v}_2 - \hat{v}_1) - r(t)] \\ \frac{d\hat{v}_2}{dt} = \frac{1}{C_2}[G(\hat{v}_1 - \hat{v}_2) + \hat{i}_3] \\ \frac{d\hat{i}_3}{dt} = \frac{1}{L}[-\hat{v}_2 - R_0\hat{i}_3] \end{cases} \tag{17}$$

where $r(t)$ is the received signal.

We modulate the digital signal by switching the value of the two parameters G_a and G_b in Eq.(16). At the receiver, we determine the value of

$$\hat{G} \triangleq \frac{r(t)}{\hat{v}_1(t)} \tag{18}$$

at the moments when both $\dot{\hat{v}}_1 = 0$ and $sgn(\hat{v}_1)\ddot{\hat{v}}_1 < 0$, where $\hat{v}_1(t)$ is the voltage across capacitor C_1.

In the following simulation, the parameters for coding *bit-0* are: $C_1 = 17nF$, $C_2 = 178nF$, $G = 1mS$, $L = 12mH$, $G_a = -1.139mS$, $G_b = -0.711mS$, $E = 1V$, $R_0 = 20\Omega$. The parameters for coding *bit-1* are the same except for $G_a = -1.189mS$ and $G_b = -0.611mS$. A fourth-order Runge-Kutta method with fixed step-size $10^{-5}s$ is used in our simulation.

To recover the binary message signal at the receiver end, let us study first the difference

between the $|\hat{v}_1|$-$\hat{G}$ maps when different parameter sets and channel gains are used. For each fixed parameter set, the values of $|\hat{v}_1|$ and $\hat{G}$ will vary as we change the channel gain parameter λ. Let us plot the values of $|\hat{v}_1|$ and $\hat{G}$ in the $|\hat{v}_1|$ vs. $\hat{G}$ plane as λ varies from 0.01 to 1, as shown in Fig.3(a) in two colors: the "red" curve corresponding to *bit 0*, and the "blue" curve corresponding to *bit 1*. It should be noted that only those points corresponding to the moments when $\dot{\hat{v}}_1 = 0$ and $sgn(\hat{v}_1)\ddot{\hat{v}}_1 < 0$ are plotted. The difference between these two "bit detection" plots are significant. In fact, it is the direct foundation for recovering the message signal from the received signal. When the transmitter parameters are switched between two parameter sets the corresponding $|\hat{v}_1|$-$\hat{G}$ plot will switch between these two curves. Observe that the spacings between these two plots are essentially independent of the channel gain λ. Hence, to recover the binary message signal, we only have to measure the peaks of $|\hat{v}_1(t)|$ and the corresponding values of $\hat{G}$. The waveform of $r(t)$(in red) for coding bit-0 with $\lambda = 1$ is shown in Fig.3(b). The waveform of $r(t)$(in blue) for coding bit-1 with $\lambda = 1$ is shown in Fig.3(c). Observe that these two waveforms reveal no discernible qualitative differences between them and it is not obvious at all that they hide a binary message.

The message recovering process is as follows. First, we use the received signal to derive a $|\hat{v}_1|$-$\hat{G}$ "bit-detection" map. We can even fabricate this map together with the receiver to serve as another hardware key. In practical applications, the receiver recovers the message signal by matching the GS results with the $|\hat{v}_1|$-$\hat{G}$ bit detection map.

In particular, it is very important for our chaotic switching method to work at a high bit-rate—both from security considerations[Yang, 1995], and for increasing transmission efficiency. To achieve this goal, we can set up a look-up table at the transmitter end. Whenever a bit change occurs (i.e., from bit-1 to bit-0 or from bit-0 to bit-1), the transmitter randomly selects a point in the stable attractor corresponding to the next bit. This point should satisfy the condition that $f(v_1)$ is the same as that of the last instant of the former bit. This can be easily implemented by finding v_1 from $f(v_1)$ and then using v_1 to locate the point. Our simulation results are shown in Fig.4. Fig.4(a) shows the received signal. Fig.4(b) shows the randomly changed (or scrambled) global channel gain $\lambda(t)$ (in blue), the binary message signal (in green) and the recovered signal(in red). From Fig.4(b) one can see that the digital signal can be easily recovered by using a moving average filter and thresholding.

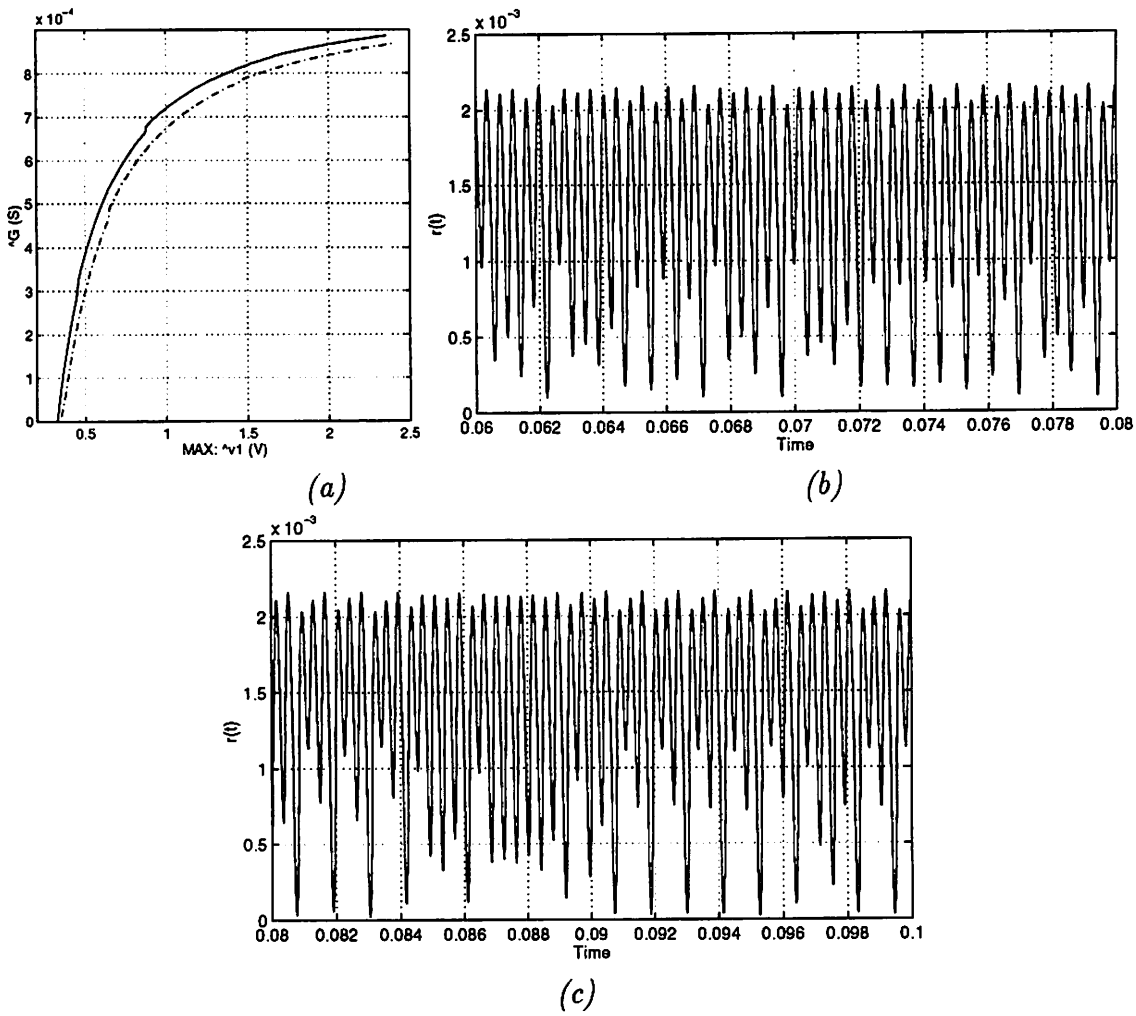
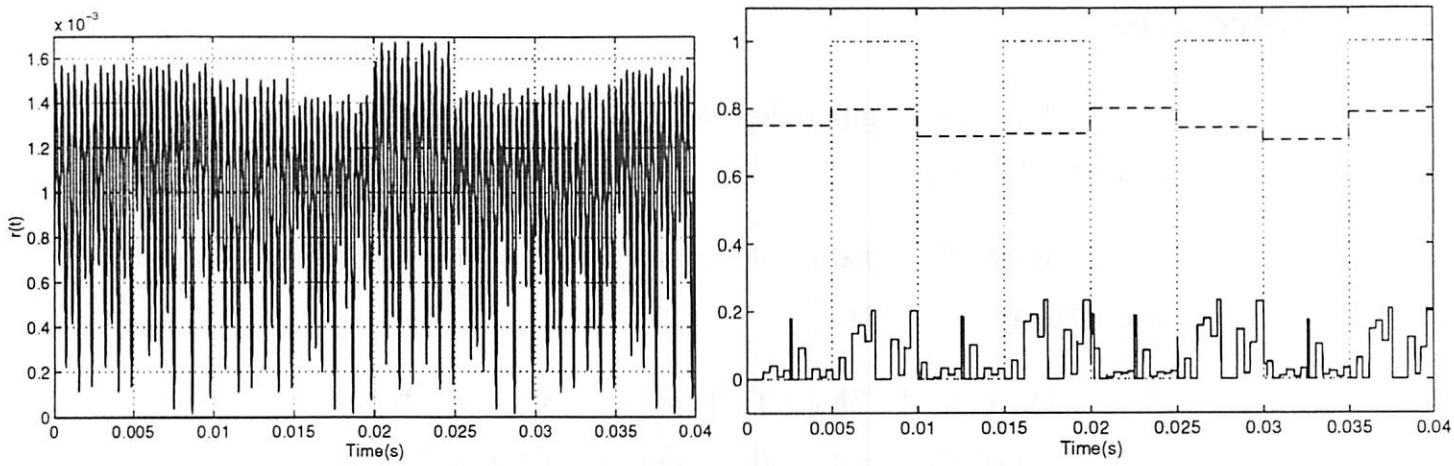


Figure 3: Bit detection maps corresponding to two qualitatively similar waveforms. (a) The difference between the two $|\hat{v}_1|$-$\hat{G}$ plots corresponding to the two parameter sets for coding bit-0 and bit-1. (b) Waveform of $r(t)$ for coding bit-0. (c) Waveform of $r(t)$ for coding bit-1.



(a) *(b)*

Figure 4: Simulation results of channel-independent chaotic switching. (a) The received signal. (b) The message signal (green), recovered signal(red) and the global channel gain(blue).

4 Concluding Remarks

One disadvantage of a chaotic-synchronization based spread-spectrum communication is its sensitivity to variations in the channel gain. In this letter, we present a new scheme which is insensitive to channel distortions. Since the amplitude of our transmitted signal is scrambled by a randomly varying gain, it would be nearly impossible to apply any identification-based method to break the security of our proposed scheme.

Acknowledgment

This work is supported by the Office of Naval Research under grant No. N00014-96-1-0753.

References

Carroll, T.L.[1996] Amplitude-independent chaotic synchronization. *Phys. Rev. E*, **53**(4):3117–3122.

Chua, L.O.[1993] Global unfolding of Chua's circuit. *IEICE Trans. Fundamentals*, **E76-A**(5):704–734.

Chua, L.O., Yang, T., Zhong, G.Q., & Wu, C.W.[1996] Adaptive synchronization of Chua's oscillators. *International Journal of Bifurcation and Chaos*, **6**(1):189–201.

Chua, L.O., Yang, T., Zhong, G.Q., & Wu, C.W.[1996] Synchronization of Chua's circuits with time-varying channels and parameters. *IEEE Transaction on Circuits and Systems—I: fundamental theory and applications*, **43**(10):862–868.

Kocarev, L. & Parlitz, U.[1996] Generalized synchronization, predictability, and equivalence of unidirectionally coupled dynamical systems. *Phys. Rev. Lett.*, **76**(11):1816–1819.

Rulkov, N. F., Sushchik, M. M., & Tsimring, L. S.[1996] Generalized synchronization of chaos in directionally coupled chaotic systems. *Phys. Rev. E*, **51**(2):980–994.

Short, K.M.[1994] Steps toward unmasking secure communications. *International Journal of Bifurcations and Chaos*, **4**(4):957–977.

Wu, C. W. & Chua, L. O.[1994] A unified framework for synchronization and control of dynamical systems. *International Journal of Bifurcations and Chaos*, **4**(4):430–447.

Wu, C.W., Yang, T., & Chua, L.O.[1996] On adaptive synchronization and control of nonlinear dynamical systems. *International Journal of Bifurcations and Chaos*, **6**(3):455–471.

Yang, T.[1995] Recovery of digital signals from chaotic switching. *International Journal of Circuit Theory and Applications*, **23**(6):611–615.

Yang, T., Wu, C.W. & Chua, L.O.[1996] Cryptography based on chaotic systems. *IEEE Transaction on Circuits and Systems—I: fundamental theory and applications.* accepted for publication.