IMPULSIVE CONTROL AND SYNCHRONIZATION OF CHAOTIC SYSTEMS AND SECURE COMMUNICATION

by

Tao Yang and Leon O. Chua

Memorandum No. UCB/ERL M97/12

29 January 1997

IMPULSIVE CONTROL AND SYNCHRONIZATION OF CHAOTIC SYSTEMS AND SECURE COMMUNICATION

by

Tao Yang and Leon O. Chua

Memorandum No. UCB/ERL M97/12

29 January 1997

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Impulsive Control and Synchronization of Chaotic Systems and 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.

January 29, 1997

Abstract

Impulsive control of a chaotic system is ideal for designing digital control schemes where the control laws are generated by digital devices which are discrete in time. In this paper, several theorems on the stability of impulsive control systems are presented. These theorems are then used to find the conditions under which the chaotic systems can be asymptotically controlled to the origin by using impulsive control. Given the parameters of the chaotic system and the impulsive control law, an estimation of the upper bound of the impulse interval is given. We also present a theory of impulsive synchronization of two chaotic systems. A promising application of impulsive synchronization of chaotic systems to a secure communication scheme is presented. In this secure communication scheme, the transmitted signals are divided into small time frames. In each time frame, the synchronization impulses and the scrambled message signal are embedded. Conventional cryptographic methods are used to scramble the message signal. Simulation results based on a typical chaotic system; namely, Chua's oscillator, are provided

1 Introduction

Since the seminal paper of Ott, Grebogi and Yorke(OGY)[2], several methods for control and stabilization of chaotic motions have recently been presented[3, 4, 5, 6]. In view of the rich dynamics of chaotic systems, there exists a large variety of approaches for controlling such systems. Some of these approaches include adaptive control[4, 5], error-feedback control[7], time-delay feedback control[7], OGY[2], predictive Poincaré control[8], occasional proportional feedback control[9] and impulsive control[6].

In fact, the predictive Poincaré control and the occasional proportional feedback control are two impulsive control schemes with varying impulse intervals. Impulsive control is attractive because it allows the stabilization of a chaotic system using only small control impulses, and it offers a direct method for modulating digital information onto a chaotic carrier signal for spread spectrum applications. However, due to a lack of effective tools for analyzing impulsive differential equations[1], most impulse control schemes had been designed mainly by trial-and-error. The study of the stability of an impulsive differential equation is much more difficult than that of its "corresponding" differential equation[10]. For example, consider the impulsive system

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x}, & t \neq \tau_i, \\ \Delta\mathbf{x}|_{t=\tau_i} = B\mathbf{x} \end{cases} \tag{1}$$

where A and B are two constant matrices, and $\Delta\mathbf{x}|_{t=\tau_i} \triangleq \mathbf{x}(\tau_i^+) - \mathbf{x}(\tau_i^-)$, $\mathbf{x}(\tau_i^-)$ and $\mathbf{x}(\tau_i^+)$ being the left and right limit of $\mathbf{x}(t)$ at $t = \tau_i$. The solution of the above system is given by

$$\mathbf{x}(t, \mathbf{x}_0) = \mathbf{X}(t, \mathbf{x}_0)\mathbf{x}_0 \tag{2}$$

where

$$\mathbf{X}(t, \mathbf{x}_0) = e^{A(t-\tau_i)} \prod_{t_0 < \tau_j < \tau_i} e^{A(\tau_j - \tau_{j-1})}, \ \tau_0 = t_0, \ \tau_i < t \leq \tau_{i+1} \tag{3}$$

As can be seen from this formula, it is not possible in the general case to give necessary and

sufficient conditions for stability of solutions of the above system in terms of the eigenvalues of the matrix of this system, which is possible for systems of ordinary differential equations with constant coefficients.

In this paper, we investigate the stability of impulsively controlled chaotic systems. First, the stability of the trivial solution of a kind of impulsive differential equation is studied. Then the theoretical results are used to study the conditions under which an impulsive control of Chua's oscillator is asymptotically stable. An estimate of the upper bound of the impulsive interval is also presented.

Then, an impulsive control theory is used to study the impulsive synchronization of two chaotic systems. We first show that the impulsive synchronization problem is an impulsive control problem. Then a theorem is given for guaranteeing the asymptotic stability of impulsive synchronization. Since only the synchronization impulses are sent to the driven system in an impulsive synchronization scheme, the information redundancy in the transmitted signal is reduced. In this sense, even low-dimensional chaotic systems can provide high security. In this paper, we will use impulsive synchronization to develop a new framework for chaotic secure communication.

The organization of this paper is as follows. In section 2, a theory on the stability of impulsive differential equations is given. In section 3, a stability criterion for impulsive control of Chua's oscillator is presented. In section 4, simulation results on the impulsive control of Chua's oscillator are provided. In section 5, the theory and simulation results of impulsive synchronization of Chua's oscillators are presented. In section 6, application of impulsive synchronization to secure communication is presented. In section 7, some concluding remarks are given.

2 Basic Theory of Impulsive Differential Equations

Consider the general nonlinear system

$$\dot{\mathbf{x}} = \mathbf{f}(t, \mathbf{x}) \tag{4}$$

where $\mathbf{f} : \mathbf{R}_+ \times \mathbf{R}^n \mapsto \mathbf{R}^n$ is continuous, $\mathbf{x} \in \mathbf{R}^n$ is the state variable, and

$$\dot{\mathbf{x}} \triangleq \frac{d\mathbf{x}}{dt}.$$

Consider a discrete set $\{\tau_i\}$ of time instants, where

$$0 < \tau_1 < \tau_2 < ... < \tau_i < \tau_{i+1} < ...,$$
$$\tau_i \to \infty \text{ as } i \to \infty$$

Let

$$U(i, \mathbf{x}) = \Delta\mathbf{x}|_{t=\tau_i} \triangleq \mathbf{x}(\tau_i^+) - \mathbf{x}(\tau_i^-) \tag{5}$$

be the "jump" in the state variable at the time instant τ_i. Then this impulsive system is described by

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{f}(t, \mathbf{x}), & t \neq \tau_i \\ \Delta\mathbf{x} = U(i, \mathbf{x}), & t = \tau_i \\ \mathbf{x}(t_0^+) = \mathbf{x}_0, t_0 \geq 0, i = 1, 2, ... \end{cases} \tag{6}$$

This is called an impulsive differential equation[1]. To study the stability of the impulsive differential equation (6) we use the following definitions and theorems[1].

Definition 1: Let $V : \mathbf{R}_+ \times \mathbf{R}^n \mapsto \mathbf{R}_+$, then V is said to belong to class $\mathcal{V}_0$ if

1. V is continuous in $(\tau_{i-1}, \tau_i] \times \mathbf{R}^n$ and for each $\mathbf{x} \in \mathbf{R}^n$, $i = 1, 2, ...,$

$$\lim_{(t,\mathbf{y}) \to (\tau_i^+, \mathbf{x})} V(t, \mathbf{y}) = V(\tau_i^+, \mathbf{x}) \tag{7}$$

exists;

2. V is locally Lipschitzian in $\mathbf{x}$

Definition 2: For $(t, \mathbf{x}) \in (\tau_{i-1}, \tau_i] \times \mathbf{R}^n$, we define

$$D^+V(t, \mathbf{x}) \triangleq \lim_{h \to 0} \sup \frac{1}{h}[V(t + h, \mathbf{x} + h\mathbf{f}(t, \mathbf{x})) - V(t, \mathbf{x})] \tag{8}$$

Definition 3: Comparison system

Let $V \in \mathcal{V}_0$ and assume that

$$\begin{cases} D^+V(t,\mathbf{x}) \leq g(t,V(t,\mathbf{x})), & t \neq \tau_i \\ V(t,\mathbf{x}+U(i,\mathbf{x})) \leq \psi_i(V(t,\mathbf{x})), & t = \tau_i \end{cases} \tag{9}$$

where $g : \mathbf{R}_+ \times \mathbf{R}_+ \mapsto \mathbf{R}$ is continuous and $\psi_i : \mathbf{R}_+ \mapsto \mathbf{R}_+$ is nondecreasing. Then the system

$$\begin{cases} \dot{w} = g(t,w), & t \neq \tau_i \\ w(\tau_i^+) = \psi_i(w(\tau_i)) \\ w(t_0^+) = w_0 \geq 0 \end{cases} \tag{10}$$

is called the comparison system of Eq.(6).

Definition 4:

$$S_\rho = \{\mathbf{x} \in \mathbf{R}^n | \ ||\mathbf{x}|| < \rho\} \tag{11}$$

where $\|\cdot\|$ denotes the Euclidean norm on $\mathbf{R}^n$.

Definition 5: A function α is said to belong to class $\mathcal{K}$ if $\alpha \in C[R_+, R_+]$, $\alpha(0) = 0$ and $\alpha(x)$ is strictly increasing in x.

Assumptions: $\mathbf{f}(t,0) = 0$, $U(i,0) = 0$ and $g(t,0) = 0$ for all i.

Remark: With the above assumptions we find that the trivial solutions of Eqs. (6) and (10) are identical for all times except at the discrete set $\{\tau_i\}$.

Theorem 1(Theorem 3.2.1, page 139, [1]): *Assume that the following three conditions are satisfied:*

1. $V : \mathbf{R}_+ \times S_\rho \mapsto \mathbf{R}_+$, $\rho > 0$, $V \in \mathcal{V}_0$, $D^+V(t,\mathbf{x}) \leq g(t,V(t,\mathbf{x}))$, $t \neq \tau_i$.

2. there exists a $\rho_0 > 0$ *such that* $\mathbf{x} \in S_{\rho_0}$ *implies that* $\mathbf{x} + U(i,\mathbf{x}) \in S_{\rho_0}$ *for all* i *and* $V(t,\mathbf{x}+U(i,\mathbf{x})) \leq \psi_i(V(t,\mathbf{x}))$, $t = \tau_i$, $\mathbf{x} \in S_{\rho_0}$.

3. $\beta(||\mathbf{x}||) \leq V(t,\mathbf{x}) \leq \alpha(||\mathbf{x}||)$ *on* $\mathbf{R}_+ \times S_\rho$,

where $\alpha(\cdot), \beta(\cdot) \in \mathcal{K}$.

Then the stability properties of the trivial solution of the comparison system (10) imply the corresponding stability properties of the trivial solution of (6).

Theorem 2(Corollary 3.2.1., page 142, [1]): *Let* $g(t,w) = \dot{\lambda}(t)w$, $\lambda \in C^1[\mathbf{R}_+, \mathbf{R}_+]$, $\psi_i(w) = d_i w$, $d_i \geq 0$ *for all* i. *Then the origin of system (6) is asymptotically stable if the conditions*

$$\lambda(\tau_{i+1}) + ln(\gamma d_i) \leq \lambda(\tau_i), for\ all\ i,\ where\ \gamma > 1 \tag{12}$$

and

$$\dot{\lambda}(t) \geq 0 \tag{13}$$

are satisfied.

3 Stabilization of Chua's oscillator using impulsive control

In this section, we study the impulsive control of Chua's oscillators[11] by using the theory presented in the previous section. The dimensionless form of a Chua's oscillator is given by[11]

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \tag{14}$$

where $f(x)$ is the piecewise-linear characteristics of the Chua's diode, which is given by

$$f(x) = bx + \frac{1}{2}(a-b)(|x+1| - |x-1|) \tag{15}$$

where $a < b < 0$ are two constants.

Let $\mathbf{x}^T = (x\ y\ z)$, then we can rewrite the Chua's oscillator equation into the form

$$\dot{\mathbf{x}} = A\mathbf{x} + \Phi(\mathbf{x}) \tag{16}$$

where

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}, \Phi(\mathbf{x}) = \begin{pmatrix} -\alpha f(x) \\ 0 \\ 0 \end{pmatrix} \tag{17}$$

The impulsive control of a Chua's oscillator is then given by

$$\begin{cases} \dot{\mathbf{x}} = A\mathbf{x} + \Phi(\mathbf{x}), \ t \neq \tau_i \\ \Delta\mathbf{x}|_{t=\tau_i} = B\mathbf{x} \end{cases} \tag{18}$$

We use the following theorem in order to guarantee the asymptotic stability of the origin of the controlled Chua's oscillator.

Theorem 3: *Let d_1 be the largest eigenvalue of $(I + B^T)(I + B)$, where B is a symmetric matrix, $\rho(I + B) \leq 1$, where $\rho(\cdot)$ denotes the spectral radius of $I + B$. Let q be the largest eigenvalue of $(A + A^T)$ and let the impulses be equidistant from each other and separated by interval Δ. If*

$$0 \leq q + 2|\alpha a| \leq -\frac{1}{\Delta} ln(\xi d_1), \quad where \ \xi > 1 \tag{19}$$

then the origin of the impulsively controlled Chua's oscillator is asymptotically stable.

Proof:

Let us construct the Lyapunov function $V(t, \mathbf{x}) = \mathbf{x}^T\mathbf{x}$. For $t \neq \tau_i$, we have

$$\begin{aligned} D^+V(t,\mathbf{x}) &= \mathbf{x}^TA\mathbf{x} + \mathbf{x}^TA^T\mathbf{x} + \mathbf{x}^T\Phi(\mathbf{x}) + \Phi^T(\mathbf{x})\mathbf{x} \\ &\leq q\mathbf{x}^T\mathbf{x} + 2|\alpha a|\mathbf{x}^T\mathbf{x} \\ &= (q + 2|\alpha a|)V(t,\mathbf{x}) \end{aligned} \tag{20}$$

Hence, condition 1 of Theorem 1 is satisfied with $g(t, w) = (q + 2|\alpha a|)w$.

Since B is symmetric we know $(I + B)$ is also symmetric. By using Euclidean norm we

have

$$\rho(I+B) = ||I+B|| \tag{21}$$

Given any $\rho_0 > 0$ and $\mathbf{x} \in S_{\rho_0}$, we have

$$||\mathbf{x}+B\mathbf{x}|| \leq ||I+B||||\mathbf{x}|| = \rho(I+B)||\mathbf{x}|| \leq ||\mathbf{x}|| \tag{22}$$

The last inequality follows from $\rho(I+B) \leq 1$. Consequently, $\mathbf{x}+B\mathbf{x} \in S_{\rho_0}$.

For $t = \tau_i$, we have

$$\begin{aligned} V(\tau_i, \mathbf{x}+B\mathbf{x}) &= (\mathbf{x}+B\mathbf{x})^T(\mathbf{x}+B\mathbf{x}) \\ &= \mathbf{x}^T(I+B^T)(I+B)\mathbf{x} \\ &\leq d_1 V(\tau_i, \mathbf{x}) \end{aligned} \tag{23}$$

Hence condition 2 of Theorem 1 is satisfied with $\psi_i(w) = d_1 w$. We can see that condition 3 of Theorem 1 is also satisfied. It follows from Theorem 1 that the asymptotic stability of the impulsively controlled Chua's oscillator in Eq.(18) is implied by that of the following comparison system

$$\begin{cases} \dot{\omega} = (q + 2|\alpha a|)\omega, \ t \neq \tau_i \\ \omega(\tau_i) = d_1 \omega(\tau_i) \\ \omega(t_0) = \omega_0 \geq 0 \end{cases} \tag{24}$$

From Eq.(19), we have

$$\int_{\tau_i}^{\tau_{i+1}} (q + 2|\alpha a|)dt + ln(\xi d_1) \leq 0, \xi > 1 \tag{25}$$

and $\dot{\lambda}(t) = q + 2|\alpha a| \geq 0$. It follows from Theorem 2 that the trivial solution of Eq.(18) is asymptotically stable. □

Theorem 3 also gives an estimate for the upper bound Δ_{max} of Δ; namely,

$$\Delta_{max} = \left|\frac{ln(\xi d_1)}{q + 2|\alpha a|}\right|, \ \xi \longrightarrow 1^+ \tag{26}$$

Observe that the upper bound given by Eq.(26) is sufficient but not necessary. Consequently, we can only say that we have a predicted stable region, which is usually smaller than the actual stable region because we can not assert that all other regions are unstable.

4 Simulation results of impulsive control

In the following simulations, we choose the parameters of Chua's oscillator as $\alpha = 15$, $\beta = 20$, $\gamma = 0.5$, $a = -\frac{120}{7}$, $b = -\frac{75}{7}$. A fourth-order Runge-Kutta with step size 10^{-5} is used. The initial condition is given by $(x(0), y(0), z(0)) = (-2.121304, -0.066170, 2.881090)$. The uncontrolled trajectories are shown in Fig.1, which is the Chua's double scroll attractor.

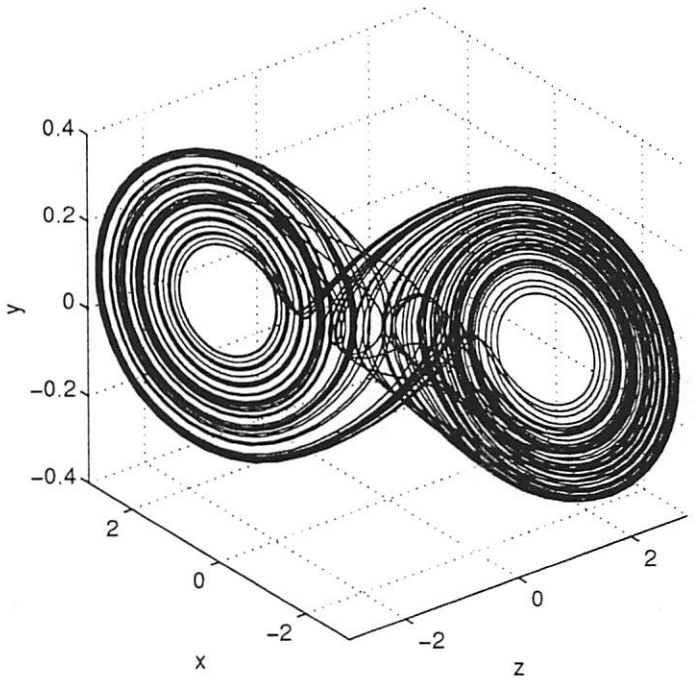


Figure 1: The Chua's double scroll attractor.

4.1 Simulation 1: strong control

In this simulation, we choose the matrix B as

$$B = \begin{pmatrix} k & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{27}$$

where the impulsive control is "strong". It follows from Theorem 3 that $\rho(I+B) \leq 1$ should be satisfied, which implies that $-2 \leq k \leq 0$. By using this B matrix, it is easy to see that

$$d_1 = (k+1)^2 \tag{28}$$

We have

$$A = \begin{pmatrix} -15 & 15 & 0 \\ 1 & -1 & 1 \\ 0 & -20 & -0.5 \end{pmatrix}, A + A^T = \begin{pmatrix} -30 & 16 & 0 \\ 16 & -2 & -19 \\ 0 & -19 & -1 \end{pmatrix} \tag{29}$$

from which we find $q = 20.162180$. Then an estimate of the boundaries of the stable region is given by

$$0 \leq \Delta \leq -\frac{(ln\xi + ln(k+1)^2)}{q + 2|\alpha a|}. -2 \leq k \leq 0 \tag{30}$$

Figure 2 shows the stable region for different ξ's. The entire region below the curve corresponding to $\xi = 1$ is the predicted stable region. When $\xi \longrightarrow \infty$, the stable region shrinks to a line $k = -1$.

The simulation results are shown in Fig.3. Figure 3(a) shows instability for $k = -1.5$ and $\Delta = 1$. The solid waveform, the dash-dotted waveform and the dotted waveform correspond to $x(t)$, $y(t)$ and $z(t)$, respectively. Figure 3(b) shows stable results within the stable region for $k = -1.5$ and $\Delta = 0.002$. One can see that the system asymptotically approaches the origin with a settling time of about 0.05. However, the true stable region is larger than that predicted in Fig. 2. In order to demonstrate this fact, we show in Fig.3(c) the stable results

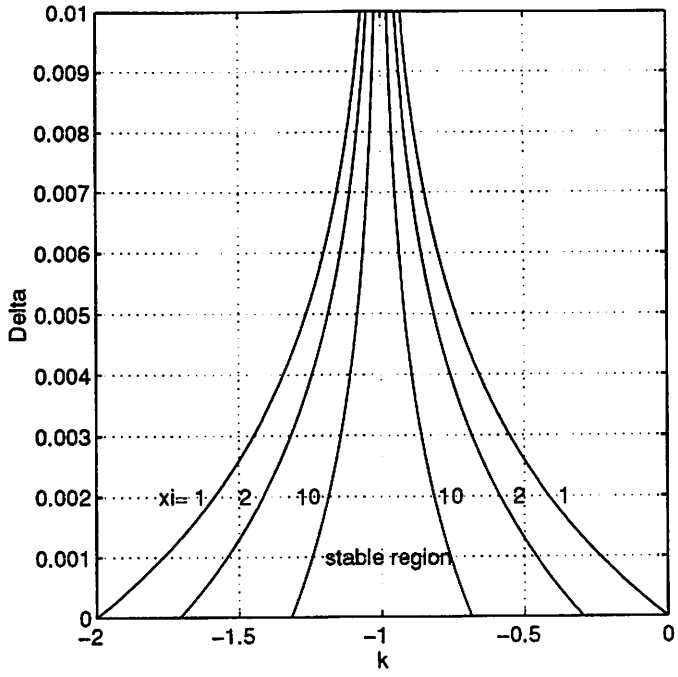


Figure 2: Estimate of the boundaries of stable regions with different ξ's used in simulation 1.

for $k = -1.5$ and $\Delta = 0.05$. We can also see that the system asymptotically approaches the origin with a settling time of about 1.4 which is much larger than that shown in Fig.3(b).

4.2 Simulation 2: weak control

In this simulation, we choose the matrix B as

$$B = \begin{pmatrix} k & 0 & 0 \\ 0 & -0.1 & 0 \\ 0 & 0 & -0.1 \end{pmatrix} \tag{31}$$

where the impulsive control is much weaker than that chosen in simulation 1.

It is easy to see that

$$d_1 = \begin{cases} (k+1)^2, & (k+1)^2 \geq 0.81 \\ 0.81, & elsewhere \end{cases} \tag{32}$$

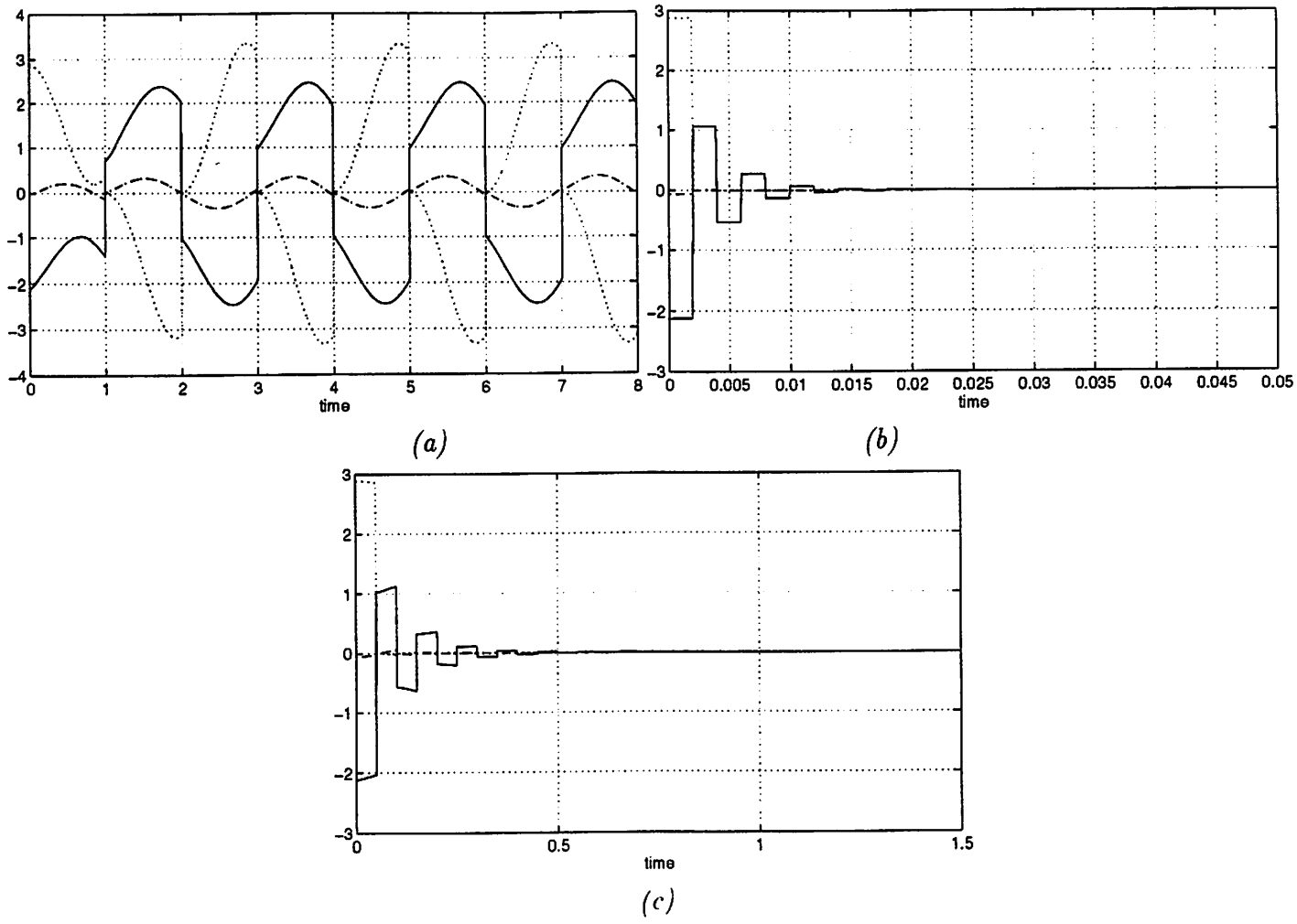


Figure 3: Simulation results. (a) Unstable results outside the stable region. (b) Stable results inside the predicted stable region. (c) Stable results outside the predicted stable region.

An estimate of the boundaries of the stable region is given by

$$0 \leq \Delta \leq \begin{cases} -\frac{ln\xi+ln(k+1)^2}{q+2|\alpha a|}, & (k+1)^2 \geq 0.81 \\ -\frac{ln\xi+ln(0.81)}{q+2|\alpha a|}, & elsewhere \end{cases}, \quad -2 \leq k \leq 0 \tag{33}$$

Figure 4 shows the stable region. The entire region below the curve corresponding to $\xi = 1$ is the predicted stable region. In this case, Δ is always bounded. It seems that we can't control the system to the origin with an arbitrarily prescribed speed because ξ has to satisfy $1 < \xi < \frac{100}{81}$. This is different from the case shown in Fig.2, where any value of $\xi > 1$ is possible.

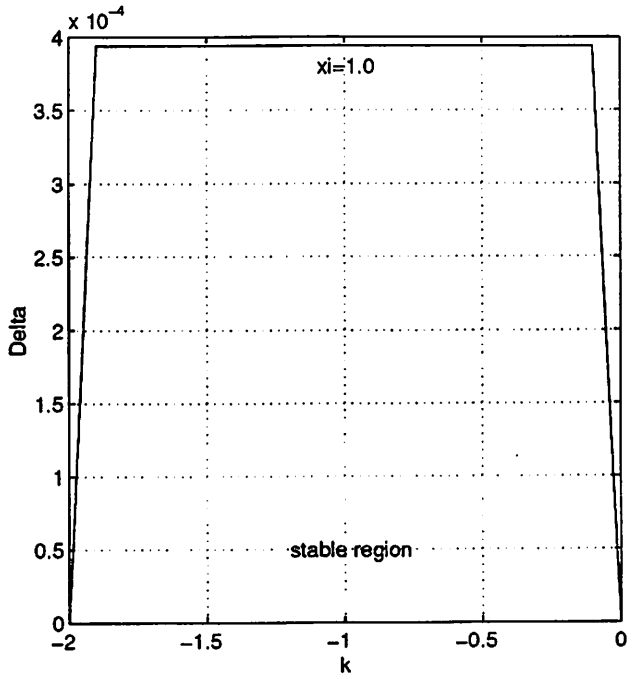


Figure 4: Estimate of the boundaries of stable region used in simulation 2.

The simulation results are shown in Fig.5. Again, the solid waveform, the dash-dotted waveform and the dotted waveform correspond to $x(t)$, $y(t)$ and $z(t)$, respectively. Figure 5(a) shows the instability results for $k = -1$ and $\Delta = 0.4$. Figure 5(b) shows the stable results in the stable region for $k = -1$ and $\Delta = 3 \times 10^{-4}$. The control system asymptotically approaches the origin with a settling time of about 0.05. Also, the true stable region is larger than that predicted in Fig.4. To demonstrate this fact, we show in Fig.5(c) the stable results for $k = -1$ and $\Delta = 0.01$. We can also see that the system asymptotically approaches the origin with a settling time equal approximately to 1, which is much larger than that shown in Fig.5(b).

5 Synchronization of Chua's oscillators using impulsive control

In this section, we study the impulsive synchronization of two Chua's oscillators. One of the Chua's oscillators is called the *driving system* and the other is called the *driven system*. In an

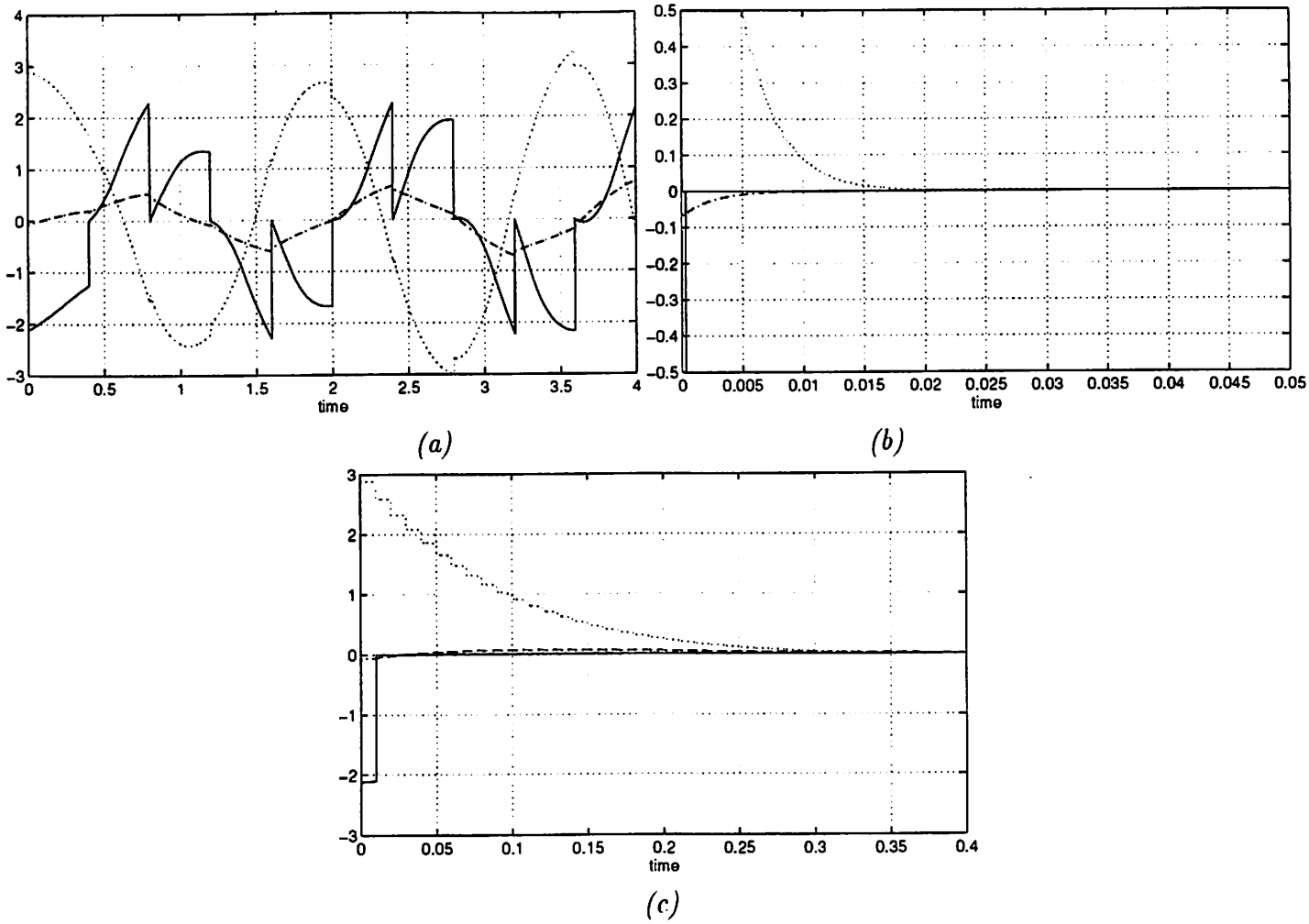


Figure 5: Simulation results. (a) Unstable results outside the stable region. (b) Stable results in the stable region. (c) Stable results outside the stable region.

impulsive synchronization configuration, the driving system is given by Eq.(14). The driven system is given by

$$\dot{\tilde{\mathbf{x}}} = A\tilde{\mathbf{x}} + \Phi(\tilde{\mathbf{x}}) \tag{34}$$

where $\tilde{\mathbf{x}} = (\tilde{x}, \tilde{y}, \tilde{z})$ is the state variables of the driven system.

At discrete instants, $\tau_i, i = 1, 2, ...,$ the state variables of the driving system are transmitted to the driven system and then the state variables of driven system are subject to jumps at these instants. In this sense, the driven system is described by the impulsive differential

equation

$$\begin{cases} \dot{\tilde{\mathbf{x}}} = A\tilde{\mathbf{x}} + \Psi(\tilde{\mathbf{x}}), \ t \neq \tau_i \\ \Delta\tilde{\mathbf{x}}|_{t=\tau_i} = -B\mathbf{e}, i = 1, 2, ... \end{cases} \tag{35}$$

where B is a 3×3 matrix, and $\mathbf{e}^T = (e_x, e_y, e_z) = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})$ is the *synchronization error*. If we define

$$\Psi(\mathbf{x}, \tilde{\mathbf{x}}) = \Phi(\mathbf{x}) - \Phi(\tilde{\mathbf{x}}) = \begin{pmatrix} -\alpha f(x) - \alpha f(\tilde{x}) \\ 0 \\ 0 \end{pmatrix} \tag{36}$$

then the error system of the impulsive synchronization is given by

$$\begin{cases} \dot{\mathbf{e}} = A\mathbf{e} + \Psi(\mathbf{x}, \tilde{\mathbf{x}}), \ t \neq \tau_i \\ \Delta\mathbf{e}|_{t=\tau_i} = B\mathbf{e}, i = 1, 2, ... \end{cases} \tag{37}$$

We use the following theorem to guarantee that our impulsive synchronization is asymptotically stable.

Theorem 4: *Let d_1 be the largest eigenvalue of $(I + B^T)(I + B)$, where B is a symmetric matrix. Assume the spectral radius ρ of $I + B$ satisfies $\rho(I + B) \leq 1$. Let q be the largest eigenvalue of $(A + A^T)$ and assume the impulses are equidistant from each other and separated by an interval Δ. If*

$$0 \leq q + 2|\alpha a| \leq -\frac{1}{\Delta} ln(\xi d_1), \quad \xi > 1 \tag{38}$$

then the impulsive synchronization of two Chua's oscillators is asymptotically stable.

Proof:

Observe that the error system in Eq.(37) is almost the same as the system in Eq.(18) except for $\Psi(\mathbf{x}, \tilde{\mathbf{x}})$. Similarly, let us construct the Lyapunov function $V(t, \mathbf{e}) = \mathbf{e}^T\mathbf{e}$. For $t \neq \tau_i$, we have

$$D^+V(t, \mathbf{e}) = \mathbf{e}^T A\mathbf{e} + \mathbf{e}^T A^T\mathbf{e} + \mathbf{e}^T\Psi(\mathbf{e}) + \Psi^T(\mathbf{e})\mathbf{e}$$

$$
\begin{aligned}
&\leq q\mathbf{e}^T\mathbf{e} + 2|\alpha||f(x) - f(\tilde{x})|e_x \\
&\leq q\mathbf{e}^T\mathbf{e} + 2|\alpha a|\epsilon_x^2 \\
&\leq (q + 2|\alpha a|)\mathbf{e}^T\mathbf{e} \\
&= (q + 2|\alpha a|)V(t, \mathbf{e}) \qquad (39)
\end{aligned}
$$

Hence, condition 1 of Theorem 1 is satisfied with $g(t, w) = (q+2|\alpha a|)w$. The rest of this proof is the same as that of Theorem 3. □

For the rest of this section, we present the simulation results. We choose the matrix B as

$$
B = \begin{pmatrix} -1.5 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \qquad (40)
$$

The initial conditions are given by $(x(0), y(0), z(0)) = (-2.121304, -0.066170, 2.881090)$ and $(\tilde{x}(0), \tilde{y}(0), \tilde{z}(0)) = (0, 0, 0)$. The other parameters are the same as those used in Section 4. Since the stability boundary estimates are the same as those in Section 4, we do not repeat them here. Figure 6 shows the simulation results. Figure 6(a) shows the stable results within our predicted stable region with $k = -1.5$ and $\Delta = 0.002$. The solid line, the dash-dotted line and the dotted line show $e_x(t)$, $e_y(t)$ and $e_z(t)$, respectively. We can see that impulsive synchronization was achieved rapidly. Figure 6(b) shows that if $\Delta = 5$ then our impulsive synchronization is unstable.

6 Application of impulsive synchronization to secure communication

Since the publication of several chaotic cryptanalysis results of *low-dimensional chaos-based* secure communication systems[12, 13], there existed an illusion that such communication schemes were not secure enough. It may be reasonable to exploit hyper-chaos based secure communication systems, but such systems may introduce more difficulties to synchronization.

On the other hand, we can enhance the security of low-dimensional chaos-based secure

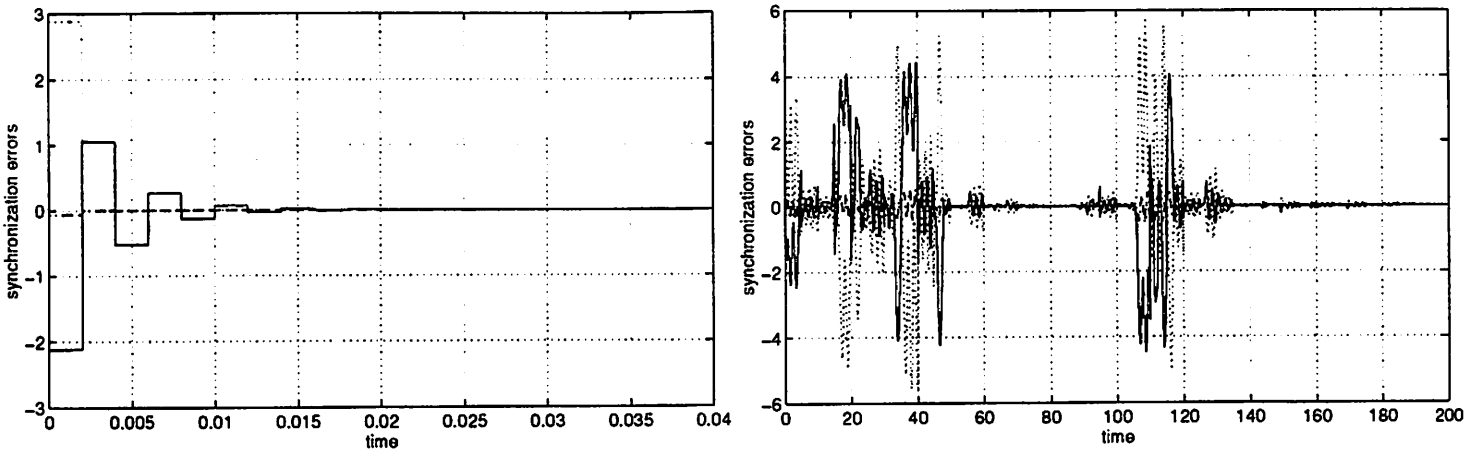


Figure 6: Simulation results of impulsive synchronization. (a) Stable synchronization results inside our predicted stable region. (b) Synchronization can not be achieved when Δ is too large.

communication schemes by combining conventional cryptographic schemes with a chaotic system[14]. To overcome the low security objections against low-dimensional continuous chaos-based schemes, we should overcome the following problems: 1) make the transmitted signal more complex, and 2) reduce the redundancy in the transmitted signal. To achieve the first goal, it is not necessary to use hyper-chaos. In [14] we have presented a method to combine a conventional cryptographic scheme with low-dimensional chaos to obtain a very complex transmitted signal. To achieve the second goal, impulsive synchronization offers a very promising approach.

In this section, we combine the results in [14] and impulsive synchronization to give a new chaotic secure communication scheme. The block diagram of this scheme is shown in Fig.7.

From Fig.7 we can see that this chaotic secure communication system consists of a transmitter and a receiver. In both the transmitter and the receiver, there exist two identical chaotic systems. Also, two identical conventional cryptographic schemes are embedded in both the transmitter and the receiver. Let us now consider details of each block in Fig. 7. The transmitted signal consists of a sequence of time frames. Every frame has a length of T seconds and consists of two regions. In Fig. 8 we show the concept of a time frame and its components. The first region of the time frame is a synchronization region consisting of

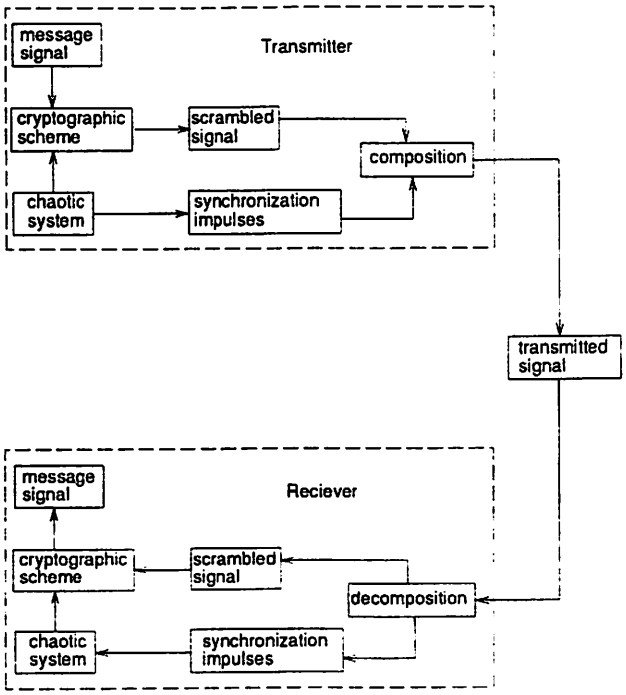


Figure 7: Block diagram of the impulsive-synchronization based chaotic secure communication system.

synchronization impulses. The synchronization impulses are used to impulsively synchronize the chaotic systems in both transmitter and receiver. The second region is the scrambled signal region where the scrambled signal is contained. To ensure synchronization, we have $T < \Delta_{max}$. Within every time frame, the synchronization region has a length of Q and the remaining time interval $T - Q$ is the scrambled signal region.

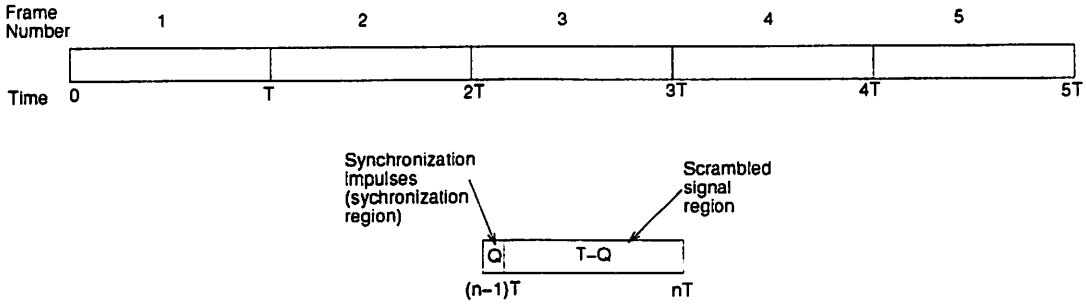


Figure 8: Illustration of the concept of a time-frame and its components.

The composition block in Fig.7 is used to combine the synchronization impulses and the

scrambled signal into the time frame structure shown in Fig.8. The simplest combination method is to substitute the beginning Q seconds of every time frame with synchronization impulses. Since Q is usually very small compared with T, the lost of time for packing a message signal is neglectable. The decomposition block is used to separate the synchronization region and the scrambled signal region within each frame at the receiver end. Then the separated synchronization impulses are used to make the chaotic system in the receiver to synchronize with that in the transmitter. The stability of this impulsive synchronization is guaranteed by our results in Section 5.

In the transmitter and the receiver, we use the same cryptographic scheme block for purposes of bi-directional communication. In a bi-directional communication scheme, every cellular phone should function both as a receiver and a transmitter. Here, the key signal is generated by the chaotic system. The cryptographic scheme is as follows[14]:

We use a continuous n-shift cipher to encrypt the plain signal(message signal). The n-shift cipher is given by

$$e(p(t)) = \underbrace{f_1\Big(...f_1\Big(f_1}_{n}\Big(p(t), \underbrace{k(t)\Big), k(t)\Big), ..., k(t)\Big)}_{n} = y(t) \tag{41}$$

where h is chosen such that $p(t)$ and $k(t)$ lie within $(-h, h)$. Here, $p(t)$ and $k(t)$ denote the plain signal and the key signal, respectively, and $y(t)$ denotes the encrypted signal. The key signal $k(t)$ is chosen as a state variable of the chaotic system. The notation $f_1(\cdot,\cdot)$ denotes a scalar nonlinear function of two variables defined as follow:

$$f_1(x,k) = \begin{cases} (x+k) + 2h, & -2h \le (x+k) \le -h \\ (x+k), & -h < (x+k) < h \\ (x+k) - 2h, & h \le (x+k) \le 2h \end{cases} \tag{42}$$

This function is shown in Fig.9.

The corresponding decryption rule is the same as the encryption rule

$$p(t) = d(y(t)) = e(y(t)) = \underbrace{f_1\Big(...f_1\Big(f_1}_{n}\Big(y(t), \underbrace{-k(t)\Big), -k(t)\Big), ..., -k(t)\Big)}_{n} \tag{43}$$

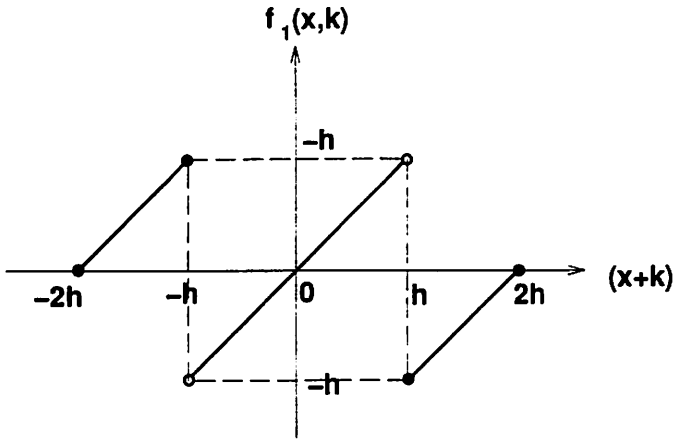


Figure 9 Nonlinear function used in the continuous shift cipher.

To decode the encrypted signal, the same key signal should be used.

The simulation results are as follows. We use an FM scheme to modulate the synchronization impulses such that the synchronization region is located in the initial 1% of every time frame. We choose the frame length as $T = 1s$. In the synchronization region of every time frame, we transmit the impulses of the three state-variables of the Chua's oscillators. The parameter of the encrypted signal is chosen as $h = 0.4$. A continuous 10-shift cipher was used. We choose x and $\tilde{x}$ as the key signals and normalized them to fall within the amplitude range $[-0.4, 0.4]$.

Figure 10 shows the simulation results of the above proposed secure communication system for transmitting a speech signal. Figure 10(a) shows the waveforms of the sampled speech of four Chinese digits "NING"(zero)—"YI"(one)—"ER"(two)—"SANG"(three). The sampling rate is 8K. Figure 10(b) shows the spectrograms of the original speech signal in Fig.10(a), from which we can see the structure of the speech signal. Figure 10(c) shows the waveforms of the received scrambled speech signal and the additive channel noise with $SNR = 16dB$. This additive noise can not change the value of the synchronization impulses which are modulated by FM. Figure 10(d) shows the spectrograms for the scrambled speech signal and the additive channel noise. We can see that the structure of the signal in Fig.10(b) was totally covered by an almost uniformly distributed noise-like spectrum. Figure 10(e) shows the waveforms of the descrambled speech signal. Figure 10(f) shows the spectrograms of the descrambled

speech signal. We can see that some noises were introduced into the recovered results due to the channel noise, and that the spectrograms became a little blur. But the structure of the speech signal was perfectly recovered.

Figure 10 The simulation results. (a) The time-domain waveform of the speech signal. (b) The spectrogram for the original speech signal. (c) The time-domain waveform of the scrambled speech signal. (d)The spectrogram of the scrambled speech signal. (e)The time-domain waveform of the descrambled speech signal. (f) The spectrogram of the descrambled speech signal.

7 Concluding Remarks

In this paper we have presented a theory of impulsive control of chaotic dynamical systems. An estimate of the upper bound of the impulse interval Δ is also presented. Since all of our results are based on solid theoretical analysis and proofs, the results in this paper provide a framework and foundation for future works. We then use this theory to impulsively control and synchronize Chua's oscillators. An application of impulsive chaotic synchronization to secure communication is presented. The chaotic secure communication scheme presented here is a combination of a conventional cryptographic method and impulsive synchronization.

Acknowledgment

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

References

[1] V.Lakshmikantham, D.D.Bainov and P.S. Simeonov, *Theory of Impulsive Differential Equations*, World Scientific, Singapore, 1989.

[2] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, 64, pp. 1196-1199, 1990.

[3] G. Chen and X. Dong, "From chaos to order — Perspectives and methodologies in controlling nonlinear dynamical systems," *Int. J. of Bifur. Chaos*, 3, pp. 1363-1409, 1993.

[4] L.O. Chua, T. Yang, G.Q. Zhong and C.W. Wu, "Adaptive synchronization of Chua's Oscillators," *International Journal of Bifurcation and Chaos*, vol.6, no.1, pp.189-201, 1996.

[5] C.W. Wu, T. Yang and L.O. Chua, "On adaptive synchronization and control of nonlinear dynamical systems," *International Journal of Bifurcation and Chaos*, vol.6, no.3, pp.455-471, , Mar.1996.

[6] T. Stojanovski, L.Kocarev and U.Parlitz. "Driving and synchronizing by chaotic impulses," *Phycs. Rev. E*, vol.43, no.9. pp. 782-785. Sept.1996.

[7] K. Pyragas, "Continuous control of chaos by self-controlling feedback," *Phys. Lett. A.*, 170, pp. 421-428, 1992.

[8] J. Schweizer and M.P. Kennedy, "Predictive Poincaré control: a control theory for chaotic systems, " *Phycs. Rev. E*, vol.52, (no.5, pt.A):4865-4876, Nov. 1995.

[9] E. R. Hunt and G. Johnson, "Keeping chaos at bay," *IEEE Spectrum*, Nov. 1993, pp. 32-36.

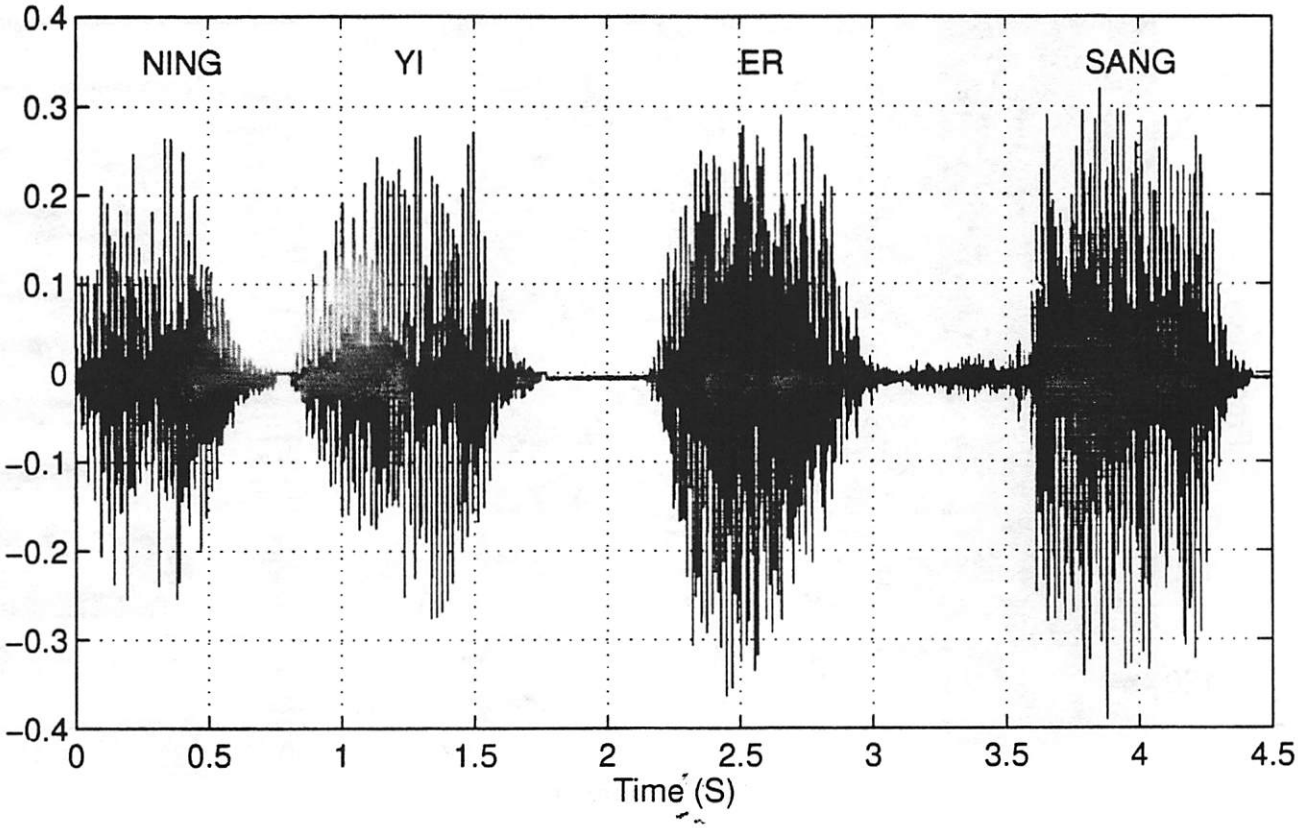
[10] A.M.Samoilenka and N.A. Perestyuk, *Impulsive Differential Equations*, World Scientific, Singapore, 1995.

[11] L.O.Chua, "Global unfolding of Chua's circuit", *IEICE Trans. Fundamentals.*, vol.E76-A, no.5, pp.704-734, May 1993.

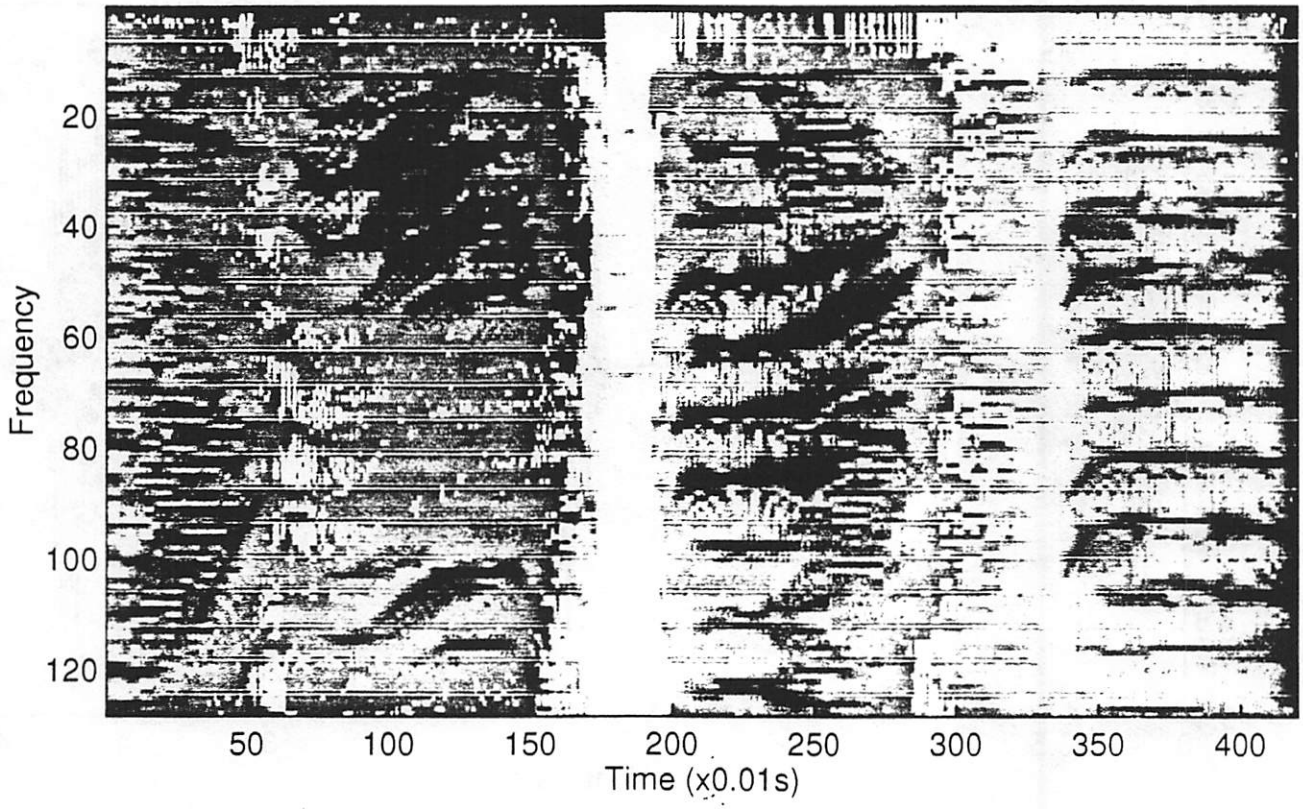
[12] T. Yang, "Recovery of digital signals from chaotic switching", *International Journal of Circuit Theory and Applications*, vol.23, no.6, pp.611-615, Nov.-Dec., 1995.

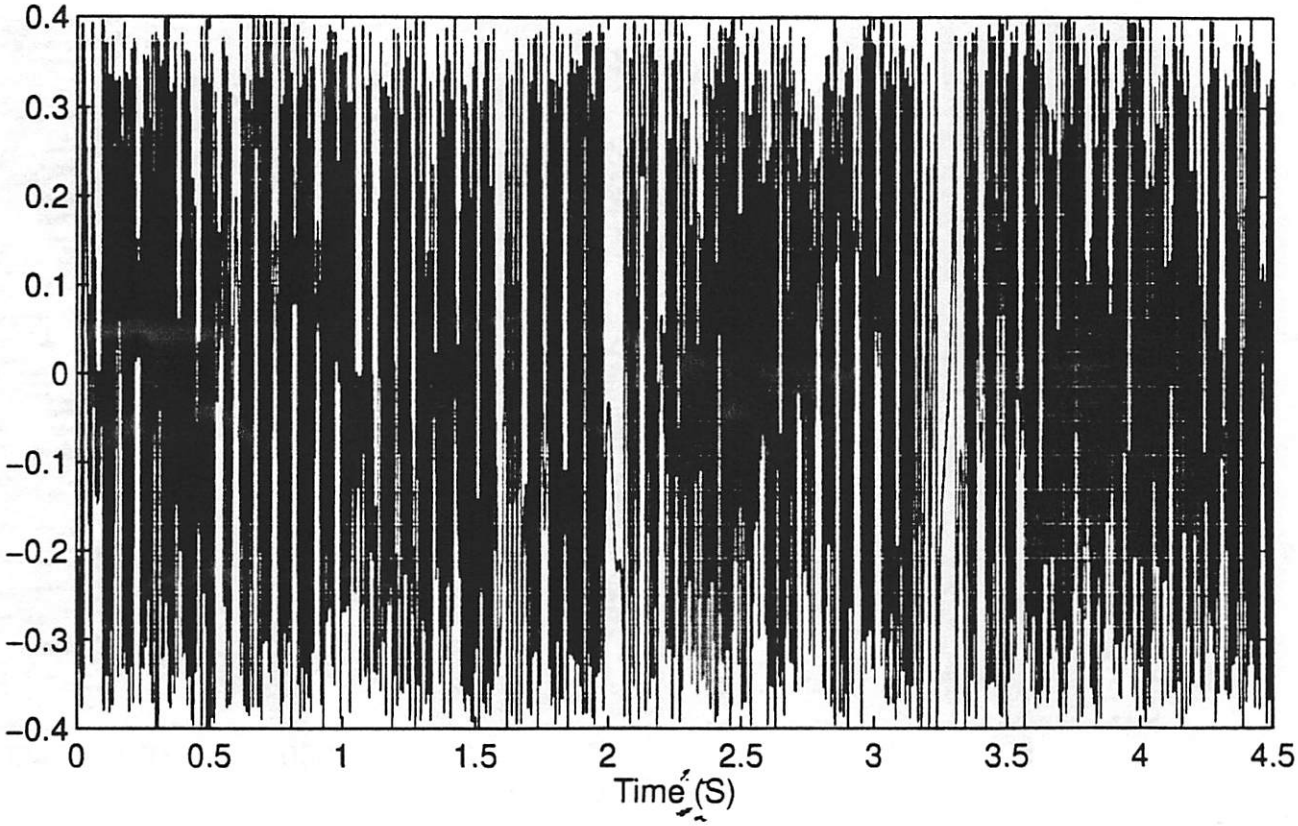
[13] K.M.Short, "Steps toward unmasking secure communications", *International Journal of Bifurcations and Chaos* vol.4, pp.957-977, 1994.

[14] T. Yang, C.W. Wu, and L.O. Chua, "Cryptography based on chaotic systems", *IEEE Transaction on Circuits and Systems—I: fundamental theory and applications*, vol.44, 1997(in press).

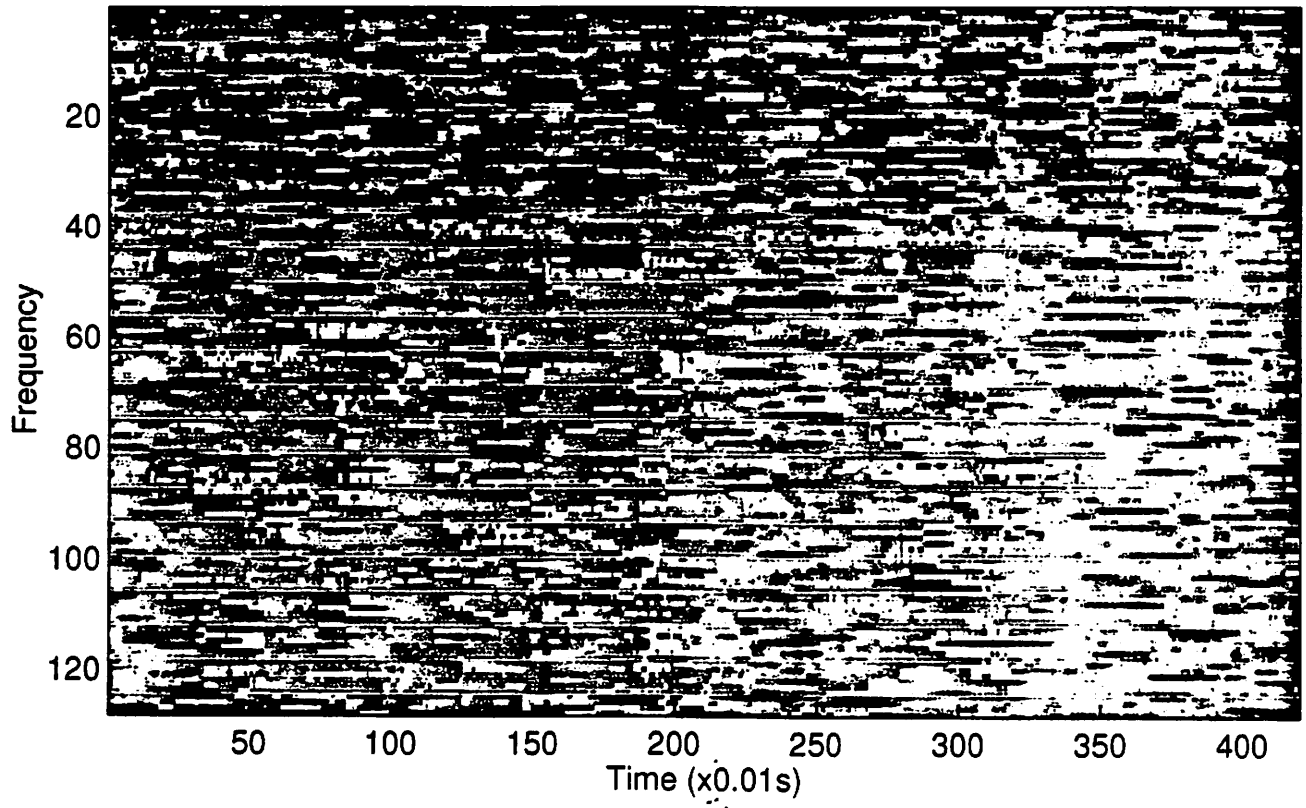


10(a)

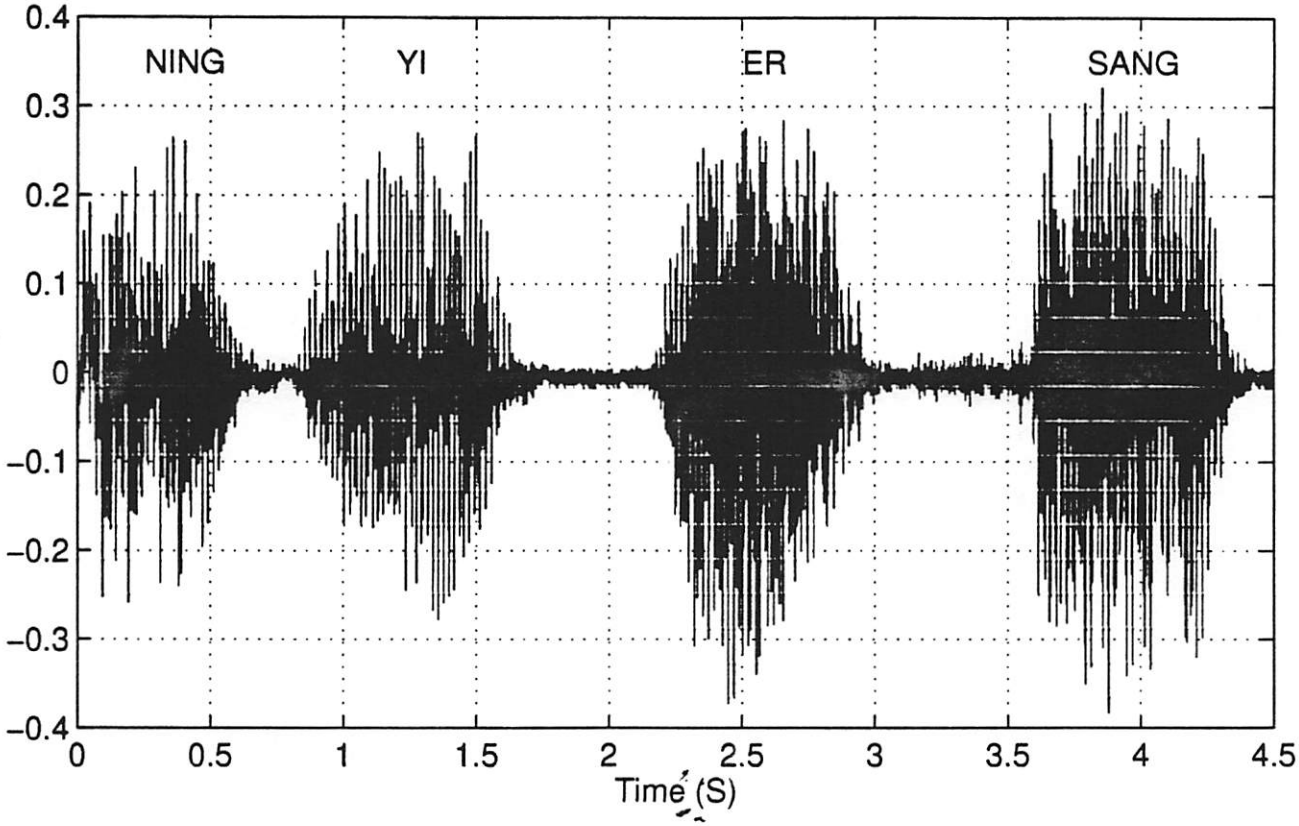

Frequency
20
40
60
80
100
120
50
100
150
200
250
300
350
400
Time (x0.01s)



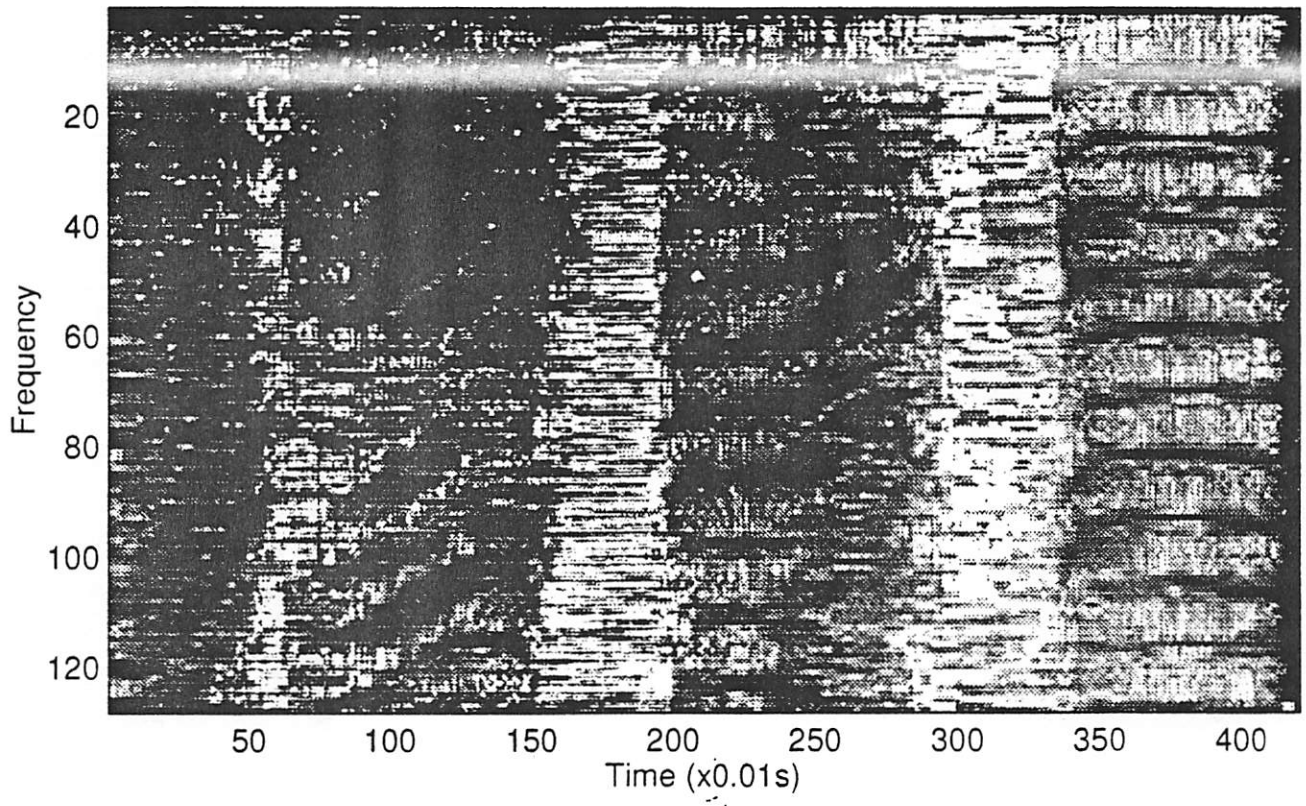
10(c)


Frequency
20
40
60
80
100
120
50
100
150
200
250
300
350
400
Time (x0.01s)

10(d)



10(e)


Frequency
20
40
60
80
100
120
50
100
150
200
250
300
350
400
Time (x0.01s)