第36卷 第15期 计 算 机 工 程 2010年8月
Vol.36 No.15 Computer Engineering August 2010
·安全技术· 文章编号：1000—3428(2010)15—0151—02 文献标识码：A 中图分类号：TN918.8

一种语音混沌保密通信方案的DSP实现

朱延钊
(华南理工大学计算中心，广州 510640)

摘 要：针对混沌通信的技术实现问题，提出用第一类分段 Lorenz 系统通过驱动-响应式同步的方法实现语音混沌保密通信的方案，包括利用数字化处理技术，对连续时间系统作离散化处理，以及用 5509 系列数字信号处理器实现该方案的系统设计原理与具体实现过程。理论分析与硬件实现结果证明了该方法的可行性。

关键词：混沌；保密通信；DSP 实现

DSP Realization for Voice Chaotic Secrecy Communication Scheme

ZHU Yan-zhao
(Computer Center, South China University of Technology, Guangzhou 510640)

【Abstract】 According to the technology for realizing chaos communication, a scheme for the implementation of voice chaotic secrecy communication is proposed by means of the first type piecewise-linear Lorenz system and drive-response method, including utilizing digital processing technology, continuous time system discretization, and the system design principle of the scheme by using 5509 series digital signal processors. Theoretical analysis and hardware implementation results demonstrate the effectiveness of the presented scheme.

【Key words】 chaos; secrecy communication; DSP realization

1 概述

混沌在保密通信中的应用是近年来重要的发展方向之一。文献[1]提出了混沌同步的概念，以及混沌信号所具有的宽带功率谱、冲击式、对初始条件高度敏感等特性，在保密通信领域中获得了实际应用[2]。文献[3]提出利用光纤技术实现混沌保密通信的最新结果。

在技术实现方面，用数字信号处理器和现场可编程门阵列等先进的现代数字信号处理工具来实现混沌保密通信已成为一个实际可行的发展方向[4-5]。

在第一类分段 Lorenz 系统和驱动-响应式同步方法[6]的基础上，提出一种实现语音混沌保密通信的新方案。在技术实现方面，由于用模拟电路参数离散性较大和失配等问题，还原出的信号质量得不到保证。解决方案之一是采用数字化处理技术，为此，需要对分段 Lorenz 系统的无量纲连续时间状态方程作离散化处理，从而能用 DSP 技术产生混沌信号与实现混沌保密通信。在此基础上，用 5509 系列 DSP 实现该方案，并给出了系统设计原理与硬件实现结果。

2 第一类分段Lorenz系统及其驱动-响应式同步

第一类分段 Lorenz 系统的无量纲状态方程的数学表达式为[6]

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=\mathrm{sgn}(x)(c-z)\\ \dot{z}=|x|-bz\end{cases} \tag{1}$$

其中，$a=0.9$，$b=0.1$，$c=2$。$\mathrm{sgn}(x)$ 为符号函数。根据式(1)，得分段 Lorenz 系统的混沌吸引子相图的数值模拟结果如图 1 所示。

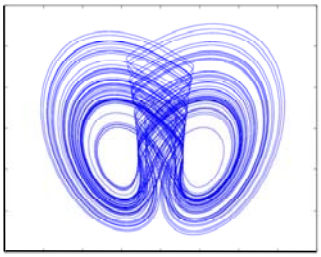
根据混沌系统的驱动-响应式同步的原理[1]，设 $x^{(1)}$、$y^{(1)}$、$z^{(1)}$ 分别为驱动系统的 3 个状态变量，得分段 Lorenz 驱动系统无量纲状态方程为

$$\begin{cases}\dot{x}^{(1)}=a(p-x^{(1)})\\ \dot{y}^{(1)}=\mathrm{sgn}(x^{(1)})(c-z^{(1)})\\ \dot{z}^{(1)}=|x^{(1)}|-bz^{(1)}\end{cases} \tag{2}$$

其中，$p=y^{(1)}+s$，s 为输入语音信号，为不使驱动和响应混沌系统发散，仿真结果表明，s 应满足 $|s|<|y^{(1)}|/100$。现通过 p 来驱动响应系统。设 $x^{(2)}$、$y^{(2)}$、$z^{(2)}$ 分别为响应系统的 3 个状态变量，得分段 Lorenz 响应系统的无量纲状态方程为

$$\begin{cases}\dot{x}^{(2)}=a(p-x^{(2)})\\ \dot{y}^{(2)}=\mathrm{sgn}(x^{(2)})(c-z^{(2)})\\ \dot{z}^{(2)}=|x^{(2)}|-bz^{(2)}\end{cases} \tag{3}$$

驱动系统式(2)与响应系统式(3)可实现同步，图 2 给出了其中变量 x 的同步相图，对于变量 y 和 z 也有类似的结果，此处不再重复。



作者简介：朱延钊(1971－)，男，讲师，主研方向：通信安全，单片机应用

收稿日期：2010-02-20 **E-mail**：13719197849@139.com

图 1　分段 Lorenz 系统的混沌吸引子相图

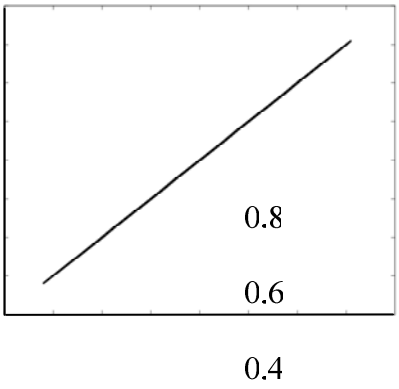


图 2　变量 x 的同步相图

3　第一类分段Lorenz系统的离散化

根据式(2)和式(3)，可用模拟电子电路来实现用分段 Lorenz 系统加密的基带传输混沌保密通信系统。实验结果表明，由于模拟电路参数的离散性和失配等问题，使得还原出语音信号的质量得不到保证，失真较大。解决这一问题的有效途径是采用现代数字信号处理技术来实现。为便于 DSP 实现，对式(2)和式(3)表示的连续时间状态方程作离散化处理，即令 $\dot{u}^{(i)} \approx [u^{(i)}(n+1)-u^{(i)}(n)]/\Delta T$ 。其中，$u \in \{x,y,z\}$，$i=1,2$；ΔT 为满足 Nyquist 准则的取样时间。根据式(2)，得离散化后驱动系统的迭代方程为

$$\begin{cases} x^{(1)}(n+1) = \Delta T a[\,p(n)-x(n)^{(1)}] + x^{(1)}(n) \\ y^{(1)}(n+1) = \Delta T \,\mathrm{sgn}(x^{1}(n))[c - z^{(1)}(n+1)] + y^{(1)}(n) \\ z^{(1)}(n+1) = \Delta T[\,|\,x^{(1)}(n+1)\,| - b z^{(1)}(n+1)] + z^{(1)}(n) \end{cases} \tag{4}$$

其中，$p(n) = y^{(1)}(n) + s(n)$，$s(n)$ 为离散化后的输入语音信号。同理，根据式(3)，得离散化后响应系统的迭代方程为

$$\begin{cases} x^{(2)}(n+1) = \Delta T a[\,p(n)-x(n)^{(2)}] + x^{(2)}(n) \\ y^{(2)}(n+1) = \Delta T \,\mathrm{sgn}(x^{2}(n))[c - z^{(2)}(n+1)] + y^{(2)}(n) \\ z^{(2)}(n+1) = \Delta T[\,|\,x^{(2)}(n+1)\,| - b z^{(2)}(n+1)] + z^{(2)}(n) \end{cases} \tag{5}$$

其中，离散化后各个参数分别为 $a=0.9$，$b=0.1$，$c=2$。根据 Nyquist 取样定理，得第一类分段 Lorenz 离散化取样时间为 $\Delta T = 1/(2\xi f_C) = 0.03$。其中，$f_C = 2.5\times10^4$ Hz 为三分贝截止频率，$\xi = 0.67\times10^{-3}$ 为频率归一化因子。

当式(4)和式(5)实现同步时，$x^{(1)}(n) = x^{(2)}(n)$，$y^{(1)}(n) = y^{(2)}(n)$，$z^{(1)}(n) = z^{(2)}(n)$。得接收端解调后的信号为

$$\hat{s}(n) = p(n) - y^{(2)}(n) = s(n) + y^{(1)}(n) - y^{(2)}(n) = s(n) \tag{6}$$

由此可知，当驱动系统与响应系统实现同步时，可在接收端不失真地解调出原信号。

4　DSP混沌保密通信的实现

DSP(Digital Signal Processor)是一种用于实时、快速实现各种数字信号处理算法的器件。本方案采用了 5509 系列的 DSP 作为技术实现。根据式(4)、式(5)以及驱动-响应式同步原理，得 5509 系列 DSP 进行语音混沌保密通信的技术实现框图如图 3 所示。其具体设计与实现过程如下：

(1)利用立体声音频编码解码芯片将输入的语音信号 $s(t)$ 转换成离散信号 $s(n)$。

(2)任意给定式(4)和式(5)中各一组互不相等并且不全为零的循环迭代初始值。

(3)在发送端，5509 系列 DSP 根据式(4)作循环迭代运算，产生迭代序列 $x^{(1)}(n)$、$y^{(1)}(n)$、$z^{(1)}(n)$、$p(n)$，$n=0,1,\cdots$。

(4)在中断控制信号控制下，$p(n)$ 经 I/O 口传输到接收端。

(5)在接收端，5509 系列 DSP 根据式(5)和式(6)作循环迭代运算，产生迭代序列 $x^{(2)}(n)$、$y^{(2)}(n)$、$z^{(2)}(n)$、$\hat{s}(n)$，$n=0,1,\cdots$。

(6)利用立体声音频编码解码芯片，将 $x^{(2)}(n)$、$z^{(2)}(n)$、$\hat{s}(n)$ 中的 2 路转换模拟信号，并送到示波器上显示。例如，将 $x^{(2)}(n)$、$z^{(2)}(n)$ 转换成模拟信号，可用示波器观察混沌吸引子相图。若将 $\hat{s}(n)$ 转换成模拟信号 $\hat{s}(t)$，可用示波器同时观察输入端语音信号 $s(t)$ 和接收端解调出语音信号 $\hat{s}(t)$ 的时域波形。

(7)由于是有线通信系统，它是一种较为理想的通信情况。因此，当利用中断信号控制收发同步时，即使是在远距离通信过程中，系统同步方案也能满足实际应用的要求。

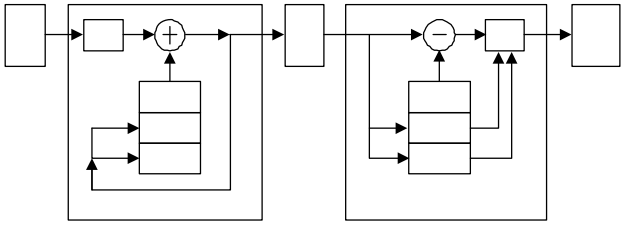


图 3　语音混沌保密通信的技术实现框图

5　硬件实现结果

根据图 3 所示的方案进行 DSP 硬件实验，得实验结果如图 4~图 6 所示。其中，图 4 为 5509 系列 DSP 产生的第一类分段 Lorenz 系统的混沌吸引子相图。图 5 为参数严格匹配时语音信号解调的实验结果，上图为输入语音 $s(t)$，下图为解调后语音信号 $\hat{s}(t)$。根据图 5 的实验结果可知，由于 5509 系列 DSP 为 32 位浮点运算，具有很高的运算精度，从而保证了当接收端混沌系统与发送端混沌系统之间的参数匹配时，恢复出的语音信号具有很高的保真度。另一方面，根据图 3 所示方案实现混沌通信时，其安全性主要体现在对发送端与接收端参数 a、b、c 匹配的高度敏感性。当接收端与发送端之间的任何一个参数失配大于 1%时，就无法解调出原语音信号，实验结果如图 6 所示，其上图为输入语音信号，下图则示出了无法正确解调出原语音信号的结果。

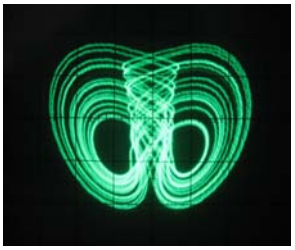


图 4　混沌吸引子实验结果

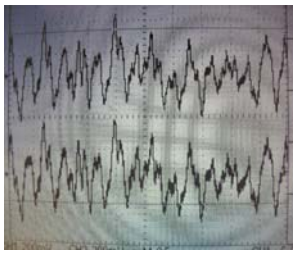


图 5　参数匹配时语音的解调

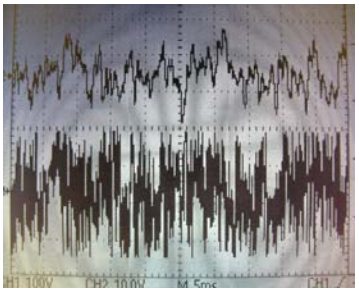


图 6　参数失配时无法解调出的原语音信号

（下转第 155 页）