一种新的混沌掩盖保密通信方案

朱双鹤，　李小春，　曲　毅，　曹国雄，　王国红
（空军工程大学 电讯工程学院，陕西 西安　710077）

摘　要：提出了反馈式多变量混沌掩盖保密通信方案。理论研究及计算机模拟表明，该方案极大地改善了通信效果，其安全性和可靠性优于一般的混沌掩盖通信方案。

关键词：混沌掩盖；保密通信；蔡氏电路
中图分类号：TN914　　**文献标识码**：A　　**文章编号**：1009－3516(2002)06－0037－05

混沌是二十世纪非线性科学领域的重大发现。80年代初，蔡少棠教授首次提出了产生混沌的电路[1]，90年代初 Pecora 和 Caroll 提出两个耦合的混沌系统可以实现同步，这些突破性的进展[2-3]，使得混沌理论应用于通信领域成为国际电子学前沿的一个研究热点。混沌保密通信、混沌载波数字通信、混沌序列直扩/跳频通信以及参数分割多址混沌通信等使得混沌通信成为现代通信的一个重要研究方向。

混沌用于保密通信的基本思想是，把被传输的信息信号加在由混沌发送系统产生的混沌信号上，生成混合类噪声信号，该信号被接收后由相应的混沌系统分离其中的混沌信号进而恢复出原信息信号，由于混沌信号的特性，截获者很难破译这种逼近于高斯白噪声的信号。而混沌掩盖式保密通信就是在发送端将混沌信号 $c(t)$ 对有用的信息信号 $m(t)$ 进行混沌掩盖形成混掩盖信号 $s(t)$，在接收端则利用同步后的混沌信号进行去掩盖(解调)，从而恢复出有用信号 $m(t)$，其原理如图1所示。

此方法的特点是用 $s(t)$ 去驱动响应系统，只要 $m(t)$ 的功率比 $c(t)$ 的功率小得多(1:100)两系统同步后，$m(t)$ 可从响应系统恢复出来，即：

$$\hat{m}(t) = s(t) - c_r(t) = c(t) + m(t) - c_r(t) \approx m(t)$$

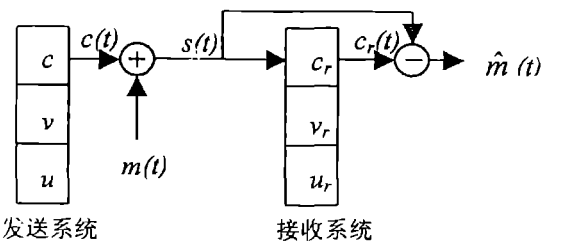


图1　混沌掩盖通信

为了防止干扰，语音信号的幅值不可能很小，当语音信号幅值增大到使调制比小于20 dB时，驱动系统和响应系统将失去同步，因而无法恢复出语音信号。目前大多数混沌掩盖系统都采用了蔡氏电路和 Lorenz 电路，它们结构简单，易于产生混沌信号，但都属于低维系统，基本是通过一个状态变量传递混沌信号，其安全性和可靠性都较差[4]。为了克服上述缺点，人们不断探索新的通信方案，文献[5～6]分别提出了多级混沌掩盖系统或多级调制系统。

基于混沌特点和混沌掩盖原理，本文提出了一种新的混沌掩盖保密通信方案，利用易于实现的蔡氏电路，采用反馈式多状态变量作为驱动信号，从而提高了信息信号与掩盖信号功率比，极大地提高了通信质量，安全性和可靠性得到了提高，向混沌实用化迈进了一大步。

1　基本原理和实现方案

收稿日期：2002－03－06
基金项目：陕西省自然科学基金项目(2001X32)
作者简介：朱双鹤(1940－)，男，河南清丰人，教授，主要从事混沌理论及智能信息处理研究.

1.1 蔡氏电路的藕合同步

混沌同步是指从不同的初始条件出发的两个混沌系统,随着时间推移,它们的轨线逐渐一致并保持下去。同步的方法有多种[7],主要有驱动响应同步,输出反馈同步,自适应同步,脉冲同步,D-B 同步等。同步是实现通信的关键条件。

混沌掩盖保密通信应用驱动——响应同步法。有两个结构参数完全相同的混沌系统

$$\dot{x} = f(x, h(t)) \tag{1}$$

$$\dot{y} = f(y, h(t)) \tag{2}$$

设 $s(t) = h(t)$ 为驱动变量,式(1)、(2)分别称为驱动系统和响应系统,二者通过单向状态变量藕合在一起.即驱动系统中的混沌信号通过 $s(t)$ 作用于响应系统,若两系统变量差值 $e = x - y$ 的微分方程

$$\dot{e} = f(y, s(t)) - f(x, s(t))$$

在 $e = 0$ 处有一个稳定点,则上面的两个系统存在稳定的同步态 $x = y$,将 $s(t) = h(t)$ 送入响应系统中,当非线性系统(2)所有的李雅普诺夫指数为负数时[8],同步得以维持。该方法的最大优点在于 $s(t)$ 的选择比较灵活,很适合于保密通信。有人用蔡氏电路构成两个混沌系统基于自同步藕合方法实现了混沌系统的同步[9]。

1.2 多状态传递变量同步

我们应用两个或多个变量或与系统参数的组合作为驱动信号来实现混沌系统的同步。考虑 n 维动力系统

$$\frac{\mathrm{d}x}{\mathrm{d}t} = F(x, s(t)) \qquad x \in \mathbf{R}^n \tag{3}$$

其中 $s(t)$ 为选择的驱动信号,即

$$s(t) = h(t) \text{ 或 } s(t) = h(x, s)$$

将系统复制为

$$\frac{\mathrm{d}x}{\mathrm{d}t} = F(y, s(t)) \qquad y \in \mathbf{R}^n \tag{4}$$

系统(4)受系统(3)中 $s(t)$ 的驱动,如果两个系统对应状态差满足

$$\lim_{t\to\infty} e_i = \lim_{t\to\infty} (y_i - x_i) = 0$$

则存在同步态。为此构造蔡氏电路同步系统[10-11]

$$\begin{aligned} \frac{\mathrm{d}x}{\mathrm{d}t} &= \alpha(y - m_1 x + 1/2(m_0 - m_1)[|x+1| - |x-1|]) \\ \frac{\mathrm{d}y}{\mathrm{d}t} &= x - y + z \\ \frac{\mathrm{d}z}{\mathrm{d}t} &= -\beta y \end{aligned} \tag{5}$$

选择 $s(t) = y + 1/2\ (m_0 - m_1)[|x+1| - |x-1|]$,则复制系统为

$$\begin{aligned} \frac{\mathrm{d}x}{\mathrm{d}t} &= \alpha(-m_1 x + s(t)) \\ \frac{\mathrm{d}y}{\mathrm{d}t} &= x - y + z \\ \frac{\mathrm{d}z}{\mathrm{d}t} &= -\beta y \end{aligned} \tag{6}$$

将系统误差定义为 $e_1 = x - x$,$e_2 = y - y$,$e_3 = z - z$ 则

$$\begin{aligned} \dot{e}_1 &= -\alpha r_1 \\ \dot{e}_2 &= e_1 - e_2 + e_3 \\ \dot{e}_3 &= -\beta e_2 \end{aligned} \tag{7}$$

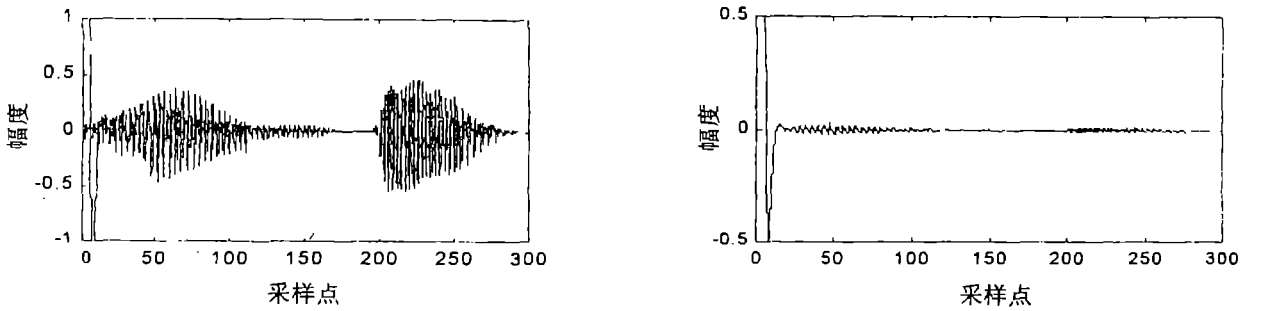
由线性稳定性理论,若式(7)的雅可比矩阵

$$J=\begin{bmatrix}-\alpha & 0 & 0\\ 1 & -1 & 1\\ 1 & -\beta & 0\end{bmatrix}$$

的所有特征值的实部都小于零,则有

$$\lim_{t\to\infty} e_i = 0 \qquad i=1,2,3$$

故两系统同步。利用图 1 所示的混沌掩盖通信方案,由蔡氏电路构成的混沌系统,其参数取值为 $\alpha=10$, $\beta=100/7$, $m_0=1/7$, $m_1=-2/7$,取两系统的初始条件都为[-1,0.2,0.1],信息信号 $m(t)=0.05\cos(0.5t)$,计算机仿真结果如图 2 所示。



(a)原语音与恢复语音　　(b)恢复语音误差

图 2　基于多状态传递变量同步的混沌通信仿真图

由于发送信号为多个系统变量复合信号组成,进行相空间重构的可能性很小,故有比较好的抗破译能力。仿真结果发现当信息信号增大 4 倍时,两系统不再同步,信息信号无法恢复,这是该系统的缺点。

1.3　反馈式多传输变量同步方法

如前所述,由于信息信号的增大使得收发系统不再是对等的两个系统。欲使两系统重新同步。我们将发送信号 $s(t)=c(t)+m(t)$ 反馈到发送端,不但用来驱动接受系统,还用来驱动发送系统,如图 3 所示。

仍然采用蔡氏电路,使发送系统为

$$\begin{aligned} x &= \alpha(-m_1 x + s(t))\\ y &= x - y + z,\ z = -\beta y \end{aligned} \tag{8}$$

驱动信号 $c(t)=y+1/2(m_0-m_1)[|x+1|-|x-1|]$,发送信号 $s(t)=c(t)+m(t)$

接收系统为

$$\begin{aligned} \dot{x} &= \alpha(-m_1 x + s(t))\\ \dot{y} &= x - y + z,\ \dot{z} = -\beta y \end{aligned} \tag{9}$$

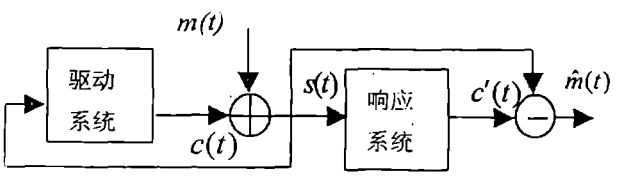


图 3　反馈式多变量混沌掩盖通信

系统误差 $e_1=x-\dot{x}$, $e_2=y-\dot{y}$, $e_3=z-\dot{z}$

由式(8)、(9)有

$$\begin{aligned} \dot{e}_1 &= -m_1\alpha e_1\\ \dot{e}_2 &= e_1 - e_2 + e_3\\ \dot{e}_3 &= -\beta e_2 \end{aligned} \tag{10}$$

式(10)Jaconbian 矩阵为

$$J=\begin{bmatrix}-m_1\alpha & 0 & 0\\ 1 & -1 & 1\\ 1 & -\beta & 0\end{bmatrix}$$

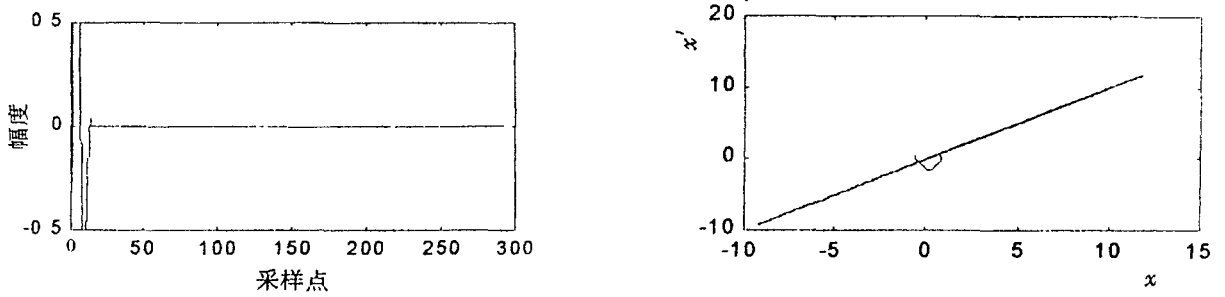
m_0, m_1, α, β 取值同前,它对应的特征值为

$$\lambda_1 = -1.0171 + \mathrm{j}3.5214, \quad \lambda_2 = -1.0171 - \mathrm{j}3.5214, \quad \lambda_3 = -1.8229$$

其实部均为负,由线性稳定性定理

$$\lim_{t\to\infty} e_i = 0 \qquad i=1,2,3$$

即 $t\to\infty$,$x\to x$,$y\to y$,$z\to z'$ 两个系统同步。$m(t)=0.05\cos(0.5t)$ 时仿真结果,如图 4 所示。当 $m(t)=0.7\cos(0.5t)$ 时,仿真表明两系统仍能保持同步,有效恢复信息信号。



(a)恢复语音误差 (b)信号 x、x' 同步

图 4 基于反馈式多传输变量同步法的混沌通信仿真图

2 仿真结果分析及结论

理论分析和计算机实验结果表明,本文提出的反馈式多变量混沌掩盖通信系统结构简单,易于实现,极大地改善了通信效果,非常适用于保密通信。

仿真实验中发现在有参数差异情况下,信息信号恢复的质量仍较好,它和一般自同步造成的参数差异引起硬件实现困难相比较更具有实用性。

从安全角度来看,由于多变量反馈驱动,此时发送系统不再是自治系统,其动态行为更复杂,重构吸引子更困难,保密性更强。

以上结论也适用于 Rossler、Lorenz 混沌系统,不同的是这两种混沌系统都存在二次项,其同步条件不能利用线性稳定性定理[12]。

仿真是在理想信道下进行的,实际上信道带宽是有限的,存在噪声干扰等。此时通信效果将受到影响。在带宽有限情况下如何实现最佳同步可参考文献[13],消除噪声干扰等问题有待深入研究。

参考文献:

[1] Chua LO. The Genesis of Chua's Circuit [J]. Archive für Elektronic und Ubertragung stechnik,1992,46(4):250 - 257.

[2] Pecora LM,Carroll TL. Synchronization in chaotic System [J]. Phys. revLett,1990,(4):36 - 39.

[3] 杨绿溪,吴 球. 保密通信中混沌掩盖法实现方案研究[J]. 数据采集与处理,1998,(1):1 - 4.

[4] Toshimitsa Ushio. Connntrol of Chaotic Synchronization and Secure Communication System[J]. IEEE Symposium on Emerging Techologies and Factory Automation,1994,(5):231 - 233.

[5] 匡锦瑜. 一种多级混沌同步通信系统[J]. 电子学报,1999,36(6):25 - 28.

[6] 黄显高,徐建学. 基于区间同步实现保密通信[J]. 西安交通大学学报,1999,27(2):34 - 37.

[7] 戴旭初,徐佩霞. 混沌同步方法及其若干问题[J]. 电路与系统学报,1998,2(1):20 - 23.

[8] 葛 真,徐 云. 非线性电路及混沌[M]. 重庆:重庆大学出版社,1989.

[9] 钟国群. 蔡氏电路混沌同步保密通信[J]. 电路与系统学报,1996,1(1):19 - 29.

[10] 李小春,朱双鹤,王国红,等. 混沌信号产生电路的研究[J]. 空军工程大学学报(自然科学版),2001,2(5):56 - 59.

[11] 曲 毅,沈明华,朱双鹤. Rossler 混沌系统的脉冲同步在通信中的应用[J]. 空军工程大学学报(自然科学版),2001,2(6):63 - 65.

[12] 吴景棠. 非线性电路原理[M]. 北京:国防工业出版社,1990.

[13] 朱双鹤,李小春,车育生. 带宽有限情况下混沌同步的研究[A]. 中国第十六届电路与系统学术会议论文集[C]. 宁波:宁波大学出版社,2001. 177 - 179.

(编辑:门向生)

A New Chaotic Masking Scheme with Applications to Secure Communications

ZHU Shuang - he, Li Xiao - chun, QU Yi, Cao Guo - xiong, Wang Guo - hong
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: A new approach for secure communication via chaotic of multivariation feedback is proposed. Theory analysis and computer experiments show that the communication quality is improved by using the approach, the security and reliability is better than the general methods of chaotic masking communication.

Keywords: Chaotic masking; Secure Communication; Chua's Circuits

(上接第 17 页)

4　结论

本测量方案优点是结构简单,容易实现,测量操作方便。如果在图象处理方面采用细分技术,其测量精度还可进一步提高。如象元细分 4 倍,则测角量化误差减小到 6.59″,系统测量误差达到 0.014 mm。

参考文献:

[1] 苏大图. 光学测试技术[M]. 北京:北京理工大学出版社,1996.
[2] 周　剑,赵　宏,陈文艺,等. 双光束刚体三维位移测量术[J]. 光电工程,1998,(5):57 - 64.
[3] 郝煜栋,赵　洋,李达成. 光学投影式三维轮廓测量技术[J]. 光学技术,1998,25(4):68 - 72.
[4] 唐圣彪,屠大维,程　胜. 激光同步扫描三角测距成像的设计[J]. 光电子 · 激光,2002,13(1):56 - 58.
[5] 沙定国. 实用误差理论与数据处理[M]. 北京:北京理工大学出版社,1993.

(编辑:门向生)

An Untouched Optical Method of Measuring the Deformation of Aircraft Engine Vane

LI Yun - xia[1], MENG Wen[1], ZHAO Shang - hong[1], LI Ying - hong[2]
(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. The Engineering Institute, Air Force Engineering University, Xi'an Shaanxi 710038, China)

Abstract: This paper presents an untouched optical measuring method in finding out the deformation of an aircraft engine vane. In this paper the principle of measurement is expounded, the source of error is analyzed and the precision of the measurement is estimated. This method has the advantage of high precision, and is simple in operation and convenient in use.

Key Words: linear CCD; intersection measurement; laser illuminate; engine vane