文章编号:1001-893X(2001)05-0108-04

一种结构简捷的混沌调制保密通信系统电路*

陈 倩,黄卡玛,刘长军,王文轲,郭忠海

(四川大学电子信息学院,四川 成都 610064)

【摘要】介绍了一种硬件实现较简单的混沌调制保密通信系统电路,并分析系统的同步原理,由编程计算对发射系统进行仿真,最后构建了相应的实验电路,在此基础上进行了传送音频信号的实验,给出了实验结果。

关键词:保密通信;混沌调制技术;实验

中图分类号:TN918 文献标识码:A

一、引 言

随着现代通信技术的迅猛发展,社会生活的各个领域日益依赖于通信,这使得信息安全和通信保密问题越来越得到人们的重视。目前,信息安全和通信保密问题已成为现代通信研究的一个重要领域。

自然界和社会生活中某些事物的运动或变化常具有二重性。一方面,它们服从于法则,严格得象力学法则一样;另一方面,它们又对系统的初始条件非常敏感,其长期行为具有不可预测性或随机性。这类现象称之为"混沌"。混沌的最根本特征是系统状态对初始条件的灵敏依赖性,初始条件的微小差别会随时间的演化而使系统的状态差别越来越大,这使得混沌系统的长期行为不可预测,然而,在这混乱状态中,也确实存在有规律性或确定性的成分。所以,混沌信号的属性、混沌系统特定条件下的同步机制和同步敏感性正符合保密通信的要求[6]。

近20年来,保密通信工作者一直致力于研究将混沌理论用于保密通信,国际上也提出了许多可行的方法。本文将要介绍的这种方法属于混沌参数调制,将模拟信息信号通过对系统参数的调制得到携带信息的混沌信号。信号传送到接收端,采用特设的动态混沌滤波器从混沌调制波中提取出信息信号从而达到对其恢复的目的[1]。由于将所传输的信息隐藏在系统参数内,因而在保密性能上优于混沌掩盖方式[5]。如果驱动信道和调制参数选择恰当,则可确保接收系统与发送系统达到同步。在此基础上构建的实验电路不仅易于硬件实现且接收端具有较强的抗噪声、抗干扰能力。

二、混沌保密通信系统的基本组成及硬件电路

混沌同步理论表明,利用混沌进行通信时,系统同步是一个关键问题。在一定条件下,一个混沌系统的输出信号可以驱动另一个子系统,使子系统达到相同的状态。仅在此情况下才能产生与加密系统相同的混沌序列,使解密系统正确解密。图1是一个典型的混沌同步保密通信系统示意图。在发射端,模拟信息信号通过调制发送(驱动)系统的参数得到混沌调制信号而被加密;在接收端,利用混沌同步信号中的混沌系统参数信息解调出原模拟信息信号[4]。

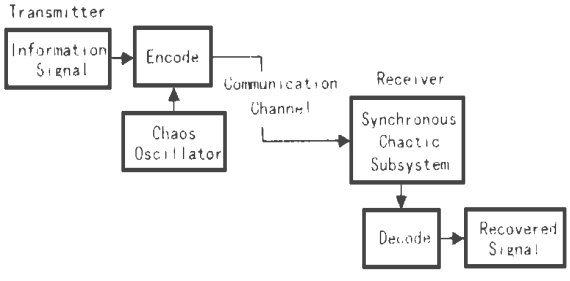

图1 混沌同步保密通信系统框图

* 收稿日期:2001-06-22

作者简介:陈倩(1975—),女,四川绵阳人,硕士研究生.

实验电路如下：

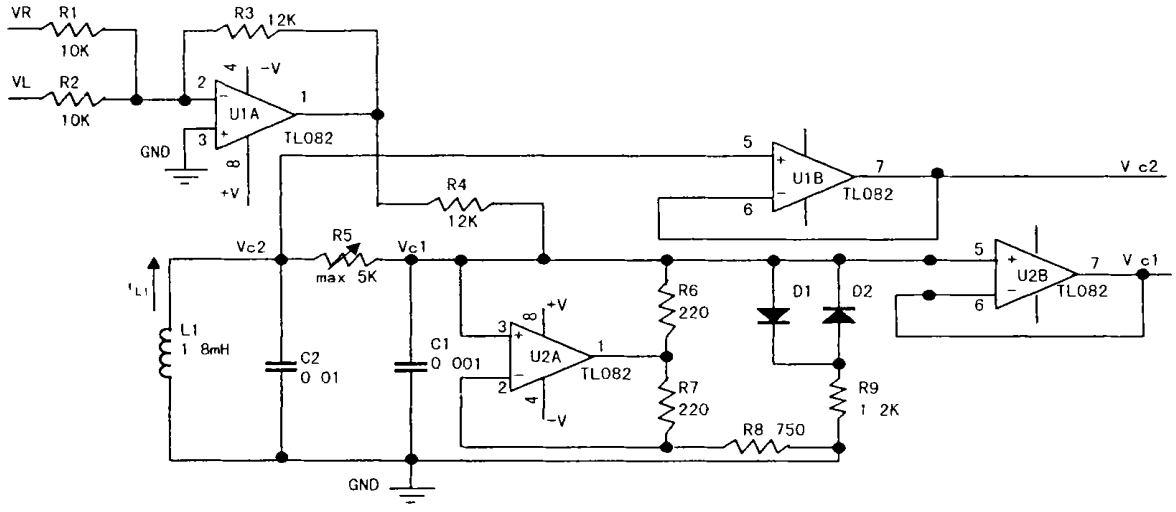

图2 发送系统电路原理图

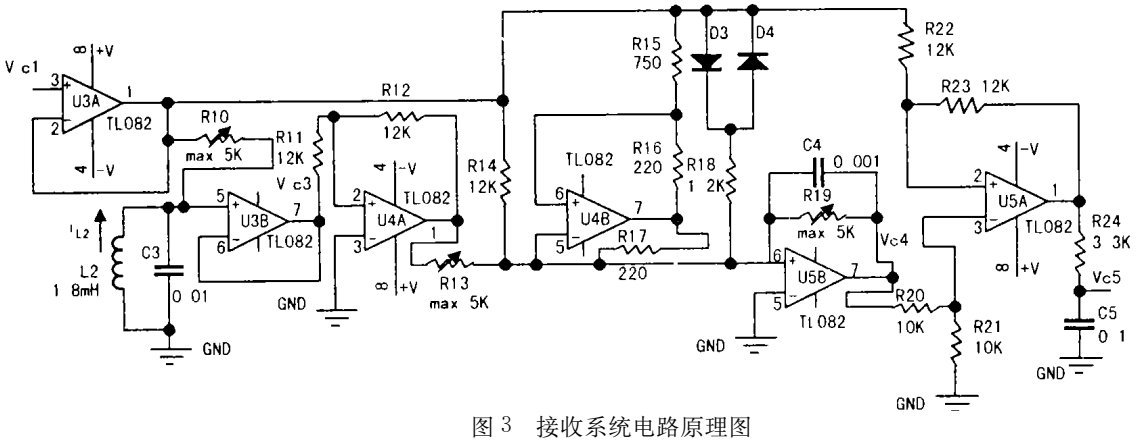

图3 接收系统电路原理图

图2、图3中收发系统匹配的充分条件为：

$I_2 = I_1, C_3 = C_2, C_4 = C_1,$

$R_{10} = R_{19} = R_3, R_{17} = R_6, R_{18} = R_9,$

$R_{11} = R_{12}, R_{14} = R_1, R_{15} = R_8,$

$R_{16} = R_7, R_{20} = R_{21}, R_{22} = R_{23}$

要求收、发 Chau's 电路的元件参数相同，元件取值如图2、图3所示。电阻的单位为Ω，电容的单位为μF，电感的单位为mH。电阻误差为5%，运放选用双运放(TL082)，二极管采用硅二极管，R_5、R_{10}、R_{13}和R_{19}选用最大阻值为5 kΩ的可调电阻器。音频信号由VL和VR端加入(由于系统只能传输一路信号，所以在输入端将两路信号混合)，发送端音频信号被调制在混沌信号Vc1之中，得到一个类似于白噪声的已调混沌信号V'c1经信道传输到接收端，在收发系统系统参数匹配的情况下，接收端通过非线性滤波器进行与之相应的逆变换，则可解调出原音频信号由Vc5输出。系统状态方程如下：

发送系统：

$$\begin{aligned}\frac{dx}{d\tau} &= \alpha[y-(1+\gamma)x-\Phi(x)+\gamma\lambda]\\ \frac{dx}{d\tau} &= x-y+z\\ \frac{dx}{d\tau} &= -\beta y\end{aligned} \tag{1}$$

其中，$\Phi(x)=ax+\frac{b-a}{2}(|x+1|-|x-1|)$，

$\tau=\frac{t}{R_5C_2}$，$x=\frac{v_{C1}}{V_{0n}}$，$y=\frac{v_{C2}}{V_{0n}}$，$z=\frac{R_5 i_{L1}}{V_{0n}}$，

V_{0n}为二极管正向导通电压。

$$\alpha=\frac{C_2}{C_1},\ \beta=\frac{R_5^2C_2}{L_1},\ \gamma=\frac{R_5}{R_4},$$

$$\alpha=\frac{R_5}{R_2}-\frac{R_5R_7}{R_6R_8},\ b=-\frac{R_5R_7}{R_6R_8}$$

输入调制 $\lambda=\frac{R_3}{V_{0n}}\left(\frac{\upsilon_R}{R_1}+\frac{\upsilon_L}{R_2}\right)$

接收系统：

$$\frac{dy_r}{d\tau}=x-y_r+z_r$$

$$\frac{dz_r}{d\tau}=-\beta y_r \qquad (2)$$

$$\frac{dw_0}{d\tau}=\alpha[y_r-(1+\gamma)x-\Phi(x)]+kx-kw_0$$

$$\frac{d\lambda_f}{d\tau}=q_f\left(\frac{w_0-x}{\gamma}-\lambda_f\right)$$

其中

$$y_r=\frac{\upsilon_{C3}}{V_{0n}},\ z_r=\frac{R_5 i_{L2}}{V_{On}},\ w_0=\frac{\upsilon_{C4}}{V_{on}},\ \lambda_f=\frac{\upsilon_{C5}}{\gamma V_{on}}$$

两个滤波器常数为：

$$k=a,\ q_f=\frac{R_5C_2}{R_{24}C_5}$$

方程(1)中 $\Phi(x)$ 为 Chau's 二极管伏安特性函数。由接收系统状态方程不含 λ 参数(即与 λ 无关)可知，接收系统和发送系统实现同步与发送系统的调制无关。如果接收系统状态方程中含有 λ 参数，则混沌载波被调制后，收、发系统将可能发生参数不匹配，导致接收系统与发送系统同步的能力降低。其次，接收系统中未出现 X 的状态方程，于是可将其用于解调。

三、计算仿真

对发端主系统电路进行数值模拟，采用差分法求解方程(1)得到结果如图 4，由此可判断发端混沌电路可起振[2]。

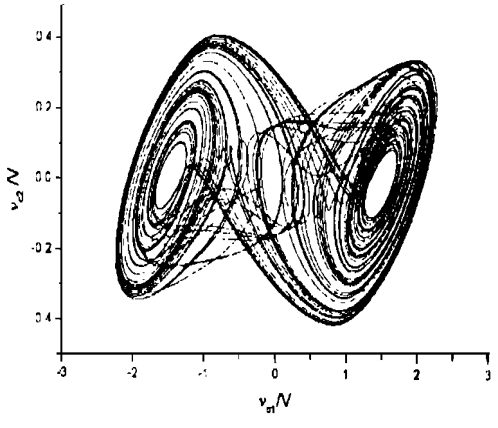

图 4 计算模拟发送端混沌吸引子 (单位:V)

四、硬件实验结果

实验表明，若采用图中所示元件，当调节至 1.315 kΩ 时，加密(发送)系统将产生较适宜的混沌载波。如果采集 V'c1 和 V'c2 作为 X 和 Y 输入，则在示波器上可以观测到混沌的 2 个吸引子(如图 5 所示)，通过这样的观测可以判断混沌电路是否起振。从两个混沌系统中分别采集电压 V'c3 和 V'c2，通过示波器采集这两个电压信号分别作为 X 和 Y 输入，则可以观测到两个信号是否达到同步(如图 6 所示)。当两个混沌系统达到同步状态后，示波器上将显示为一条细线；未达到同步时，则为一条很宽的亮带[3]。

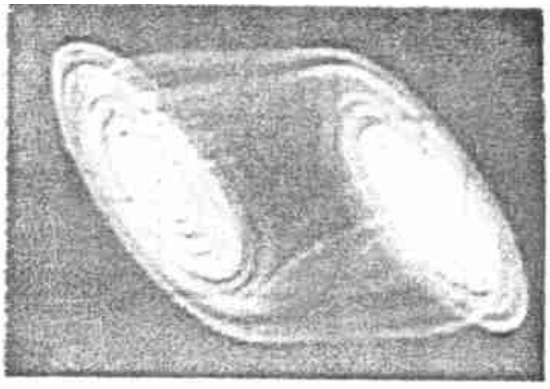

图 5 发端系统吸引子

图 6 收、发系统达到同步

用图 2、图 3 所示电路进行了传送语音信号的实验。在发送系统的 V_R、V_L 端加入语音信号，通过混沌参数调制后，语音信号被加密而无法听辨。当传输到接收系统解密后，用扬声器能还原出清晰、逼真的语音信号。

在本实验中，调节的阻值会直接影响混沌载波信号，调节 R_{10}、R_{13} 和 R_{19} 可在一定程度上对其它电

路元件因精度不高而引入的误差提供补偿，从而提高输出信号的质量，即调节 R_{10}、R_{13}、和 R_{19}，将直接影响接收端语音信号的输出，且输出信号对的变化很敏感。当 $R_{10}=1.332\ k\Omega$，$R_{13}=1.526\ k\Omega$，$R_{19}=1.361\ k\Omega$ 时得到较理想的语音输出。

五、结 束 语

本文介绍了一种在硬件实现上很简捷的混沌保密通信系统电路，本实验系统最大的优点在于参数的调制不影响系统的同步。其次，通过实验结果还可知本方案具有安全性，且电路实现较简单，具有实用性。但由于混沌保密通信技术还不很成熟，一些研究成果还不能很快发挥其应用价值。因此，下一步将通过更深入的实验优化系统，采取适当的技术措施，开发出高保密水平、独具混沌特色的保密通信系统。

参 考 文 献

[1] Ned J·Corron, Daniel W·Hahs· A new approach to communication using chaotic signal [J] s· IEEE Trans · CAS－I, 1997;44(5)·pp373－382,

[2] Tao Yang, Chai Wah Wu, and Leon O·Chua· Cryptography Based on Chaotic Systems [J]· IEEE· Trans· CAS－I, 1997,44(5)· pp469－472

[3] Louis M·Pecora and Thomas L·Carroll· Synchronization in Chaotic Systems[J]· PHYSICAL REVIEW LETTERS, 1990, 64(8), pp821－824

[4] Tao Yang and Leon O·Chau Secure communication via chaotic parameter modulation[J]· IEEE Trans CAS－I, 1996, 43(9)·pp817－819

[5] 刘剑波，张树京，宋文涛· 混沌通信技术研究[J]· 通信技术，2001(1)：42～43

[6] 赵思真，赵思正· 混沌同步及其在保密通信中的应用[J]· 保密通信，1997(1)：1～7

A Simple－structured Chaotic Modulation Circuit for Secure Communication System

CHEN Qian, HUANG Ka－ma, LIU Chang－jun, WANG Wen－ke, GUO Zhong－hai

(Department of Radio, Sichuan University, Chengdu 610064, China)

Abstract: A simple－structured Chaotic modulation circuit for secure communication system is introduced in this paper· After analyzing its synchronous theory and simulating the transmitter through computer calculation, the authors design an experimental hardware circuit· Several experiments are made to test this circuit and satisfactory results are obtained·

Key words: Secure communication; Chaotic modulation technology; Experiment

上海贝尔正式签订 CDMA 智能网合同

9月12日，上海贝尔与联通新时空正式签订合同，在上海、广东、天津、广西、新疆、河北等六省市合力打造精品 CDMA 智能网，提供共计 387.4 CAPS 的业务处理能力，约占此次联通新时空 CDMA 智能网一期工程总处理能力的 1/3。这是上海贝尔与联通新时空继建设 CDMA 网络后的再次合作。

此次由上海贝尔提供的 CDMA 智能网系统采用了先进的 CORBA 总线、F－DPE 总线技术和 N＋1 负荷分担(Load Sharing)工作方式。该方式能够提供充足的冗余量来承担突发大话务量的冲击，安全性和抗过负荷能力更强。

在联通新时空 CDMA 智能网一期工程中，上海贝尔也是唯一一家采用基于服务器方式处理信令的厂商，即 SCP 不仅完全实现与其他厂家 SSP 的对接，同时 SCP 内部可以根据 SSP 上传的不同协议参数，来选择相应的业务逻辑，实现固网、GSM 网、CDMA 网的充分融合。该方式因具备充分的扩展性和可持续发展能力而得到了业界的认可，美国近 80％的 800 号业务平台以及欧洲众多的智能网系统均是基于此种服务器信令处理方式的。

(金 典)