

# 一种基于混沌调制的语音保密通信系统

广州广东工业大学信息工程学院(510643) 禹思敏  
 广州华南理工大学电子与信息学院(510640) 丘水生

**摘要:** 提出一种用蔡氏电路实现混沌调制的语音保密通信方案,分析了系统的同步性能,在此基础上设计硬件实验电路,进行传送语音信号的硬件实验研究,并给出了实验结果。

**关键词:** 蔡氏电路 混沌同步 混沌调制 混沌通信

近年来,国际上相继提出了将混沌同步理论应用于保密通信领域的各种方法,其中主要包括混沌掩盖<sup>[1]</sup>、混沌参数调制<sup>[2]</sup>、混沌移相键控(CSK)<sup>[3]</sup>和混沌数字码分多址((CD)<sup>2</sup>MA)<sup>[4]</sup>等。为了进一步提高混沌通信系统的保真度和安全性能,人们正在探索新的传输方案<sup>[5-7]</sup>。

本文提出一种用蔡氏电路实现两级混沌调制的语音保密通信方案。在发端,利用蔡氏电路对发送信号进行两级混沌调制,在收端对其进行逆变换解调出原信号。根据单向耦合法实现收发系统的同步,并分析了同步的收敛特性。通过所设计的电路进行了传送语音信号的硬件实验研究,在收端,用扬声器能还原出清晰而逼真的语音信号。

## 1 语音混沌保密通信硬件实验系统的建立

采用蔡氏电路实现两级混沌调制的语音保密通信方案硬件实验系统电路如图1所示。图中收发蔡氏电路的元件参数相同: $R=1.75\text{k}\Omega$ , $L=19.2\text{mH}$ , $C_1=9.8\text{nF}$ , $C_2=100.5\text{nF}$ , $r=10\Omega$ 。 $N_R$ 为蔡氏二极管,其伏安特性函数为 $f(V)=G_b V+1/2(G_a-G_b)(|V+E|-|V-E|)$ ,式中 $G_a=-0.76\text{mS}$ , $G_b=-0.41\text{mS}$ , $E=1\text{V}$ ,可用双运放(TL082)和6个线性电阻构成 $N_R$ <sup>[8]</sup>,如图2所示,其伏安特性如图3所示。该系统的工作过程如下:在发端首先用混沌信号 $v_{c2}$ 对有用信息 $s(t)$ 进行第一级调制后变为 $s_m(t)$ ,再通信线性变换 $T$ 后成为 $s'_m(t)$ ,经VCCS后以电流 $i_s(t)$ 的方式作用于发端系统( $v_{c1}, v_{c2}, i_L$ ),实现第二级调制。线性变换 $T$ 的设置不仅能增加系统的安全性,而且可限制 $s'_m(t)$ 的大小,防止过调制现象。经两级混沌调制后,有用信息 $s(t)$ 被调制在混

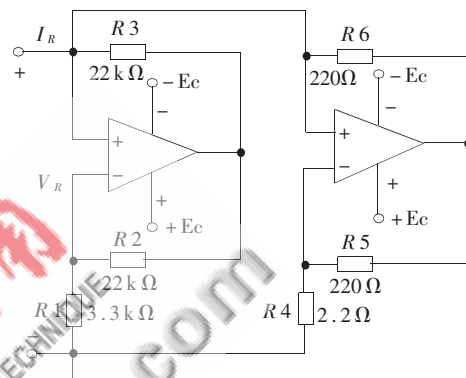


图2 蔡氏二极管的组成

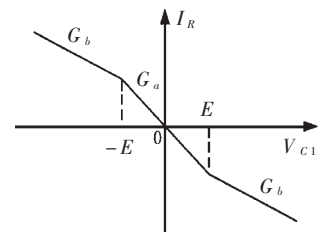


图3 蔡氏二极管的伏安特性

沌信号 $v_{c1}$ 之中,形成一个类似于白噪声的混沌扩频信号。发端系统的输出信号 $v_{c1}$ 经信道传至收端,在收发系统参数匹配的情况下,收端再进行与之相应的逆

变换,则可解调出信号 $\hat{s}(t)$ 。

## 2 系统的工作原理

### 2.1 收发系统之间的同步

由图1,可得发端蔡氏电路的状态方程为:

$$C_1 dV_{c1}/dt = (V_{c2} - V_{c1})/R - f(V_{c1}) + i_s \quad (1)$$

$$C_2 dV_{c2}/dt = (V_{c1} - V_{c2})/R + i_L \quad (2)$$

$$L di_L/dt = -V_{c2} - ri_L \quad (3)$$

收端蔡氏电路的状态方程为:

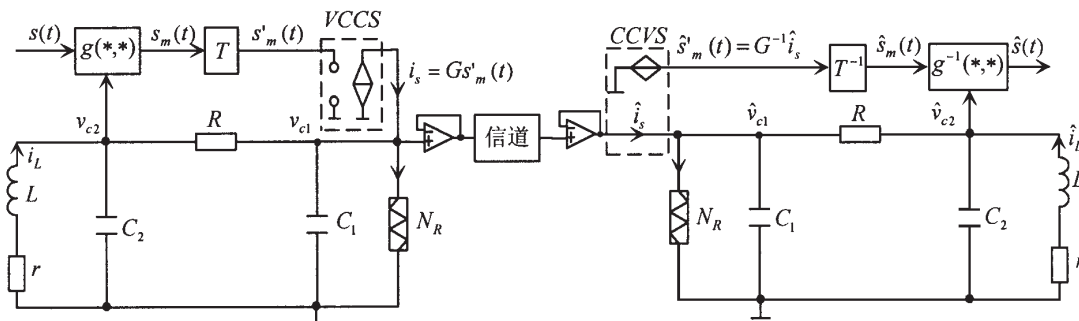


图1 语音混沌保密通信硬件实验电路

$$C_1 d\hat{V}_{c1}/dt = (\hat{V}_{c2} - \hat{V}_{c1})/R - f(\hat{V}_{c1}) + \hat{i}_s \quad (4)$$

$$C_2 d\hat{V}_{c2}/dt = (\hat{V}_{c1} - \hat{V}_{c2})/R + \hat{i}_L \quad (5)$$

$$L d\hat{i}_L/dt = -\hat{V}_{c2} - r\hat{i}_L \quad (6)$$

图 1 中由于收发两端电压跟随器的作用,有:

$$\hat{V}_{c1} = V_{c1} \quad (7)$$

设收发两端电容  $C_2$  的误差电压为  $x = \hat{V}_{c2} - V_{c2}$ , 电感  $L$  的误差电流为  $y = \hat{i}_L - i_L$ , 由 (2)、(3)、(5)、(6) 和 (7) 五个方程, 可得误差信号状态方程的矩阵形式为

$$\begin{bmatrix} dx/dt \\ dy/dt \end{bmatrix} = \begin{bmatrix} -1/RC_2 & 1/C_2 \\ -1/L & -r/L \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = J_F \begin{bmatrix} x \\ y \end{bmatrix} \quad (8)$$

(8) 式的特征方程为  $|\lambda I - J_F| = 0$ , 对其求解可得如下两个特征值

$$\lambda_{1,2} = -0.5b \pm 0.5\sqrt{b^2 - 4c} \quad (9)$$

式中  $b = 1/RC_2 + r/L > 0$ ,  $c = r/RC_2L + 1/LC_2 > 0$ ,  $\lambda_1$  和  $\lambda_2$  的实部为负, 故误差方程 (8) 式全局收敛和稳定,  $|x| = |\hat{V}_{c2} - V_{c2}| \rightarrow 0, \hat{V}_{c2} \rightarrow V_{c2}, |y| = |\hat{i}_L - i_L| \rightarrow 0, \hat{i}_L \rightarrow i_L$ , 因此, 收发两端的蔡氏电路可实现同步。

### 2.2 信号的调制与解调

收发两端参数匹配并且达到同步后, 可将信号解调出来。发端的混沌调制信号为

$$i_s = GTg(V_{c2}, s(t)) \quad (10)$$

在收端进行与之相应的逆运算, 得

$$\hat{s}(t) = g^{-1}(\hat{V}_{c2}, T^{-1}G^{-1}\hat{i}_s) \quad (11)$$

由于收发系统之间已实现同步,  $\hat{V}_{c1} = V_{c1}, \hat{V}_{c2} = V_{c2}$ ,

再由 (1) 式和 (4) 式, 有:  $\hat{i}_s = i_s$ , 将这些结果代入 (10) 和 (11) 式, 得:

$$\hat{s}(t) = s(t) \quad (12)$$

由此可知, 收端系统能解调出原信号  $s(t)$ 。

式中  $g(*, *)$  可以是加减乘除运算或者是更复杂的混合运算,  $g^{-1}(*, *)$  为  $g(*, *)$  的逆运算。在硬件实验中,  $g(*, *)$  取加法运算,  $g^{-1}(*, *)$  取减法运算,  $T$  为衰减系数,  $T^{-1}$  为放大系数,  $G$  和  $G^{-1}$  则分别为 VCCS 和 CCVS 的  $G$  参数和  $R$  参数, 其中  $T=0.5, T^{-1}=2, G=0.05\text{mS}, G^{-1}=20\text{k}\Omega$ , VCCS、CCVS 可由运放电路来实现。限于篇幅, 这里不再详述。

### 3 系统的保真度和安全性能

按照 (12) 式, 当电路参数精确匹配时, 收端可不失真地解调出信号  $S(t)$ , 从理论上讲, 该系统具有较高的保真度。在硬件实验过程中, 对收发电路的元件严格配对, 所有电阻均用精密可调电阻, 收端电感  $L$  用仿真电感构成, 如图 4 所示。调节电阻  $R_5$ , 可实现收发两端电感的严格匹配。

另一方面, 只有当收端电路参数与发端电路参数

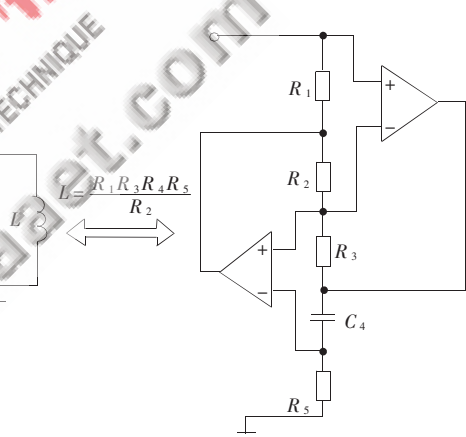


图 4 仿真电感 L 及其等效电路

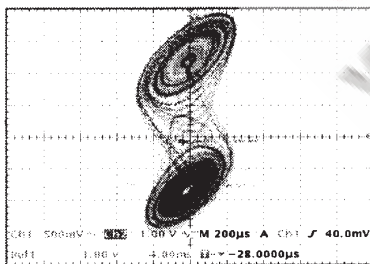


图 5 发端混沌吸引子

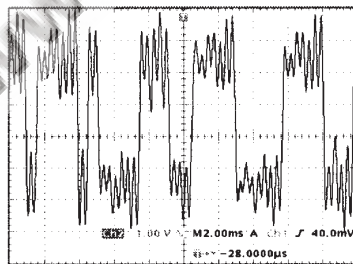


图 6 发端信号的混沌调制波形

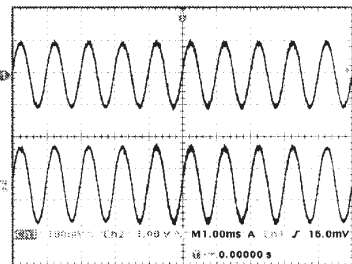


图 7 正弦波信号的解调

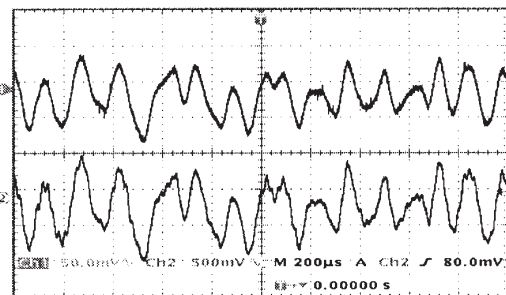


图 8 语言信号的解调

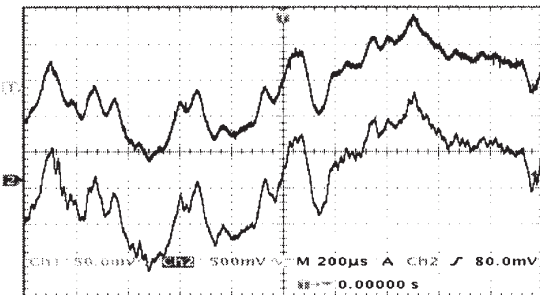


图 9 音乐信号的解调

(接上页)

精确匹配时,才能将有用信息  $s(t)$  解调出来,  $R$ 、 $C_1$ 、 $C_2$ 、 $L$  等起到了密钥参数的作用,因此,该系统又具有安全性。由于本方案采用了两级混沌调制,增加了对信号破译的难度,它和一般的单级混沌系统相比,安全性能得到了改善。

#### 4 硬件实验结果

图 5 为发端电路被  $s(t)$  调制后的双涡卷混沌吸引子,图 6 为发端信号的混沌调制波形,图 7 为正弦波信号的解调波形,图 8 为语言信号的解调波形,图 9 为音乐信号的解调波形,将  $\hat{s}(t)$  放大后输入扬声器,能还原出非常清晰而逼真的语音信号。在图 7~9 的三张图片中,上端波形为输入信号  $s(t)$ ,下端波形为解调出的信号  $\hat{s}(t)$ 。文中所有图片均取自于数字存储式示波器 TDS3012。

本文提出一种用蔡氏电路实现语音信号传输的混沌通信方案,在此基础上进行了语音传输保密通信的硬件实验。通过对该方案的研究,得出如下结论:(1)具有较好的幅频响应特性,改善了保真度,能满足传送语音信号的要求;(2)采用了两级混沌调制,改善了系统的安全性能。同时,电路参数  $R$ 、 $C_1$ 、 $C_2$  和  $L$  等起到了密钥参数的作用,在事先不知道发端电路参数的情况下,要想破译有用信号有一定的难度。因此,本方

案具有安全性;(3)电路实现并不复杂,具有实用性。

#### 参考文献

- 1 Kocarev L, Halle K S. Experimental demonstration of secure communications via chaotic synchronization. Int. J. Bifurc. Chaos, 1992; 2(3):709~713
- 2 Yang T, Chua L O. Secure communication via chaotic parameter modulation. IEEE Trans. CAS- I, 1996; 43(9): 817~819
- 3 Dedieu H, Kennedy M P. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronization Chua's circuits. IEEE Trans. CAS- I, 1993; 40(10): 634~642
- 4 Yang T, Chua L O. Chaotic digital code-division multiple access (CDMA) communication systems. Int. J. Bifurc. Chaos, 1997; 7(12): 2789~2805
- 5 Yang T, Wu C W. Cryptography based on chaotic systems. IEEE Trans. CAS- I, 1997; 44(5): 469~472
- 6 Panas A I, Yanag T. Experimental results of impulsive synchronization between two Chua's circuits. Int. J. Bifurc. Chaos, 1998; 8(3): 639~644
- 7 Hasler M. Synchronization of chaotic systems and transmission of information. Int. J. Bifurc. Chaos, 1998; 8(4): 647~659
- 8 Kennedy M P. Robust op amp realization of Chua's circuit. Frequenz, 1992; 46(3,4): 66~80

(收稿日期:2000-10-15)