采用混沌技术提高军事通信的保密性*

段锁力,王曙钊,徐成果
(空军工程大学 理学院,陕西 西安 710051)

摘 要:阐述了混沌通信一般原理,分析了其保密性能,用改进型蔡氏电路实现了单向耦合同步,进而设计了一种更为可靠的基于 Lorenz 系统实现的二阶级联混沌保密通信系统。仿真结果表明,这种方法可行且可提高军事通信的安全性、保密性。

关键词:蔡氏电路 Lorenz 系统 单向耦合 二阶级联

军用通信需要很好的保密性。目前,军用通信加密方式和方法都可能通过多种手段进行解密,不能保证绝对加密。混沌通信信息加密研究起源于 20 世纪 90 年代,由于混沌信号的非周期性、连续宽带频谱、类似噪声的特性,使它具有天然的隐蔽性。所以混沌用于保密通信有着广泛的前景。本文首先介绍一种改进型蔡氏电路并利用其实现单向耦合同步的保密通信;然后通过 Lorenz 系统实现两级混沌加密,以此来提高军事通信的保密性能;最后进行数值仿真。

1 混沌保密通信原理及系统构成

混沌保密通信方式多种多样,其基本思路是相同的,即把被传送的信号与某一混沌系统产生的混沌信号相互作用,生成混合类噪声信号,实现对信息源加密。该混合信号发送到接收器上后,再由一相应混沌系统分离出其中的混沌信号,即解密,进而恢复出信息源[1-3]。混沌应用于保密通信,必须解决三个方面的问题[4]:制造出鲁棒性强的同步信号;信号的调制和解调;信号的可靠传输。图 1 给出了混沌保密通信的基本框图。

2 单向耦合混沌遮掩保密通信系统

下面介绍的是利用一种改进型蔡氏电路实现单向耦合同步混沌掩盖通信系统。蔡氏电路动力学方程为[5-6]:

$$c_1\dot{v}_{c_1}=(v_{c_2}-v_{c_1})/R-f(v_{c_1}) \tag{1}$$

$$c_2\dot{v}_{c_2}=(v_{c_1}-v_{c_2})/R+i_L \tag{2}$$

$$L\dot{i}_L=-v_{c_2} \tag{3}$$

式中,$f(v_{c_1})=m_0v_{c_1}+(m_1-m_0)(|v_{c_1}+1|-|v_{c_1}-1|)/2$

其硬件实现电路如图 2 所示。

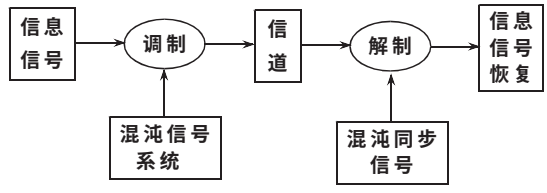

图 1 混沌保密通信基本框图

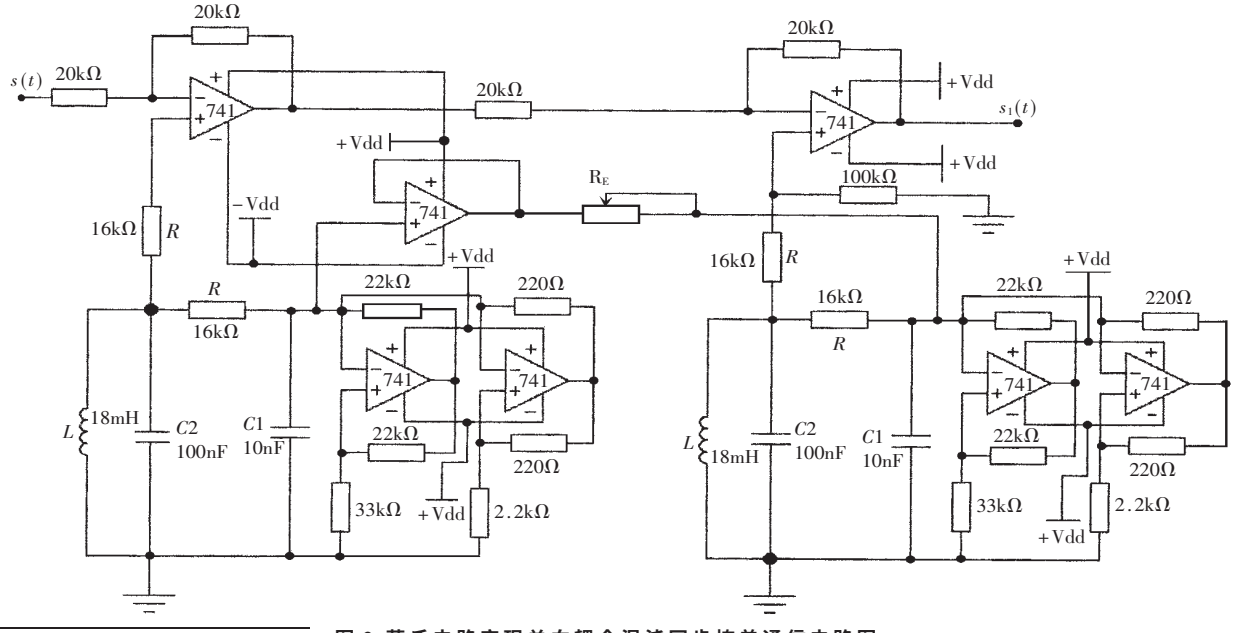

图 2 蔡氏电路实现单向耦合混沌同步掩盖通信电路图

* 基金项目:总装武器预研基金(413040403)。

其中，蔡氏电路中的电感采用参考文献[7]中所给出的一种利用普通集成运放、线性电阻和电容组成的模拟电感电路实现，如图 3 所示，其等效电感 $L=C4R1R3R5/R2$。

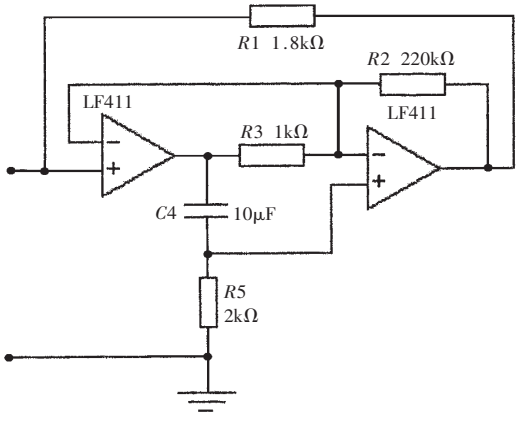

图 3 等效电感电路

图 2 电路参数为：$C1=10\text{nF}$，$C2=100\text{nF}$，$L=18\text{mH}$，$R=16\text{k}\Omega$，$s(t)$为发送信息，$s_1(t)$为收端解调出的信息，R_E 为单向耦合电阻，改变其大小可使接收端和发送端的蔡氏电路实现单向耦合同步。

3 一种二阶级联混沌保密通信系统

由于单向耦合同步保密通信系统均采用小信号调制（混沌遮掩）的方法，要求信号的能量小于混沌信号的能量，为保证解调精度为 1/10 或者更小，可采用基于相空间重构的攻击法、基于混沌同步的分析方法、基于噪声消减技术的破译法等，这些都是有效的[8]，但安全性差，不能满足军事通信的要求，不能保证军事通信的绝对安全。

为了进一步提高混沌保密通信安全性，设计了一种二阶级联的混沌保密通信系统，图 4 给出了二阶级联混沌保密通信系统方块图。

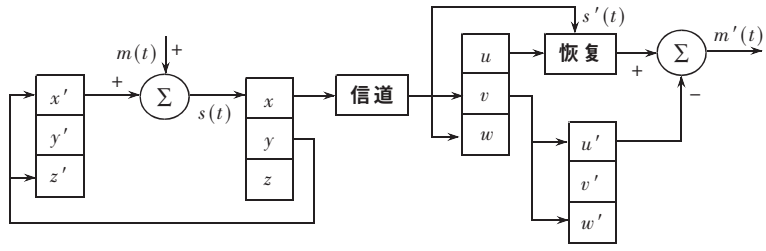

图 4 二级联混沌保密通信方案原理图

此系统的工作原理：在发射端，第一级为主系统(x,y,z)，第二级为子系统(x',z')，由主变量 y 驱动。接收端的第一级主系统为(u,v,w)，其子系统(u',w')由变量 v 来驱动。由于子系统(x',z')，(u',w') 的条件——李亚普诺夫指数均为非正数，系统可以达到同步[9]。

下面是基于 Lorenz 系统实现二阶混沌保密通信系统的仿真。此二阶 Lorenz 混沌系统的动力学方程为：

发射端：

$$\dot{x}=a(y-x'-m(t)) \tag{4}$$

$$\dot{y}=-xz+cx-y \tag{5}$$

$$\dot{z}=xy-bz \tag{6}$$

$$\dot{x}'=a(y-x') \tag{7}$$

$$\dot{y}'=x'z'+cx'-y' \tag{8}$$

$$\dot{z}'=x'y'-bz' \tag{9}$$

接收端：

$$\dot{u}=a(v-u) \tag{10}$$

$$\dot{v}=-xw+cx-v \tag{11}$$

$$\dot{w}=xv-bw \tag{12}$$

$$\dot{u}'=a(v-u) \tag{13}$$

$$\dot{v}'=-u'w'+cu'-v' \tag{14}$$

$$\dot{w}'=u'v-bw' \tag{15}$$

当 $a=10.0$，$b=8/3$，$c=28$ 时，进入混沌状态；当 $m(t)=A\sin(\omega t)$ 时，选取适当的 A、ω，可以实现很好的保密通信。通过 Matlab 进行仿真，图 5(a)是(x,y,z)的混沌吸引子，图 5(b)是(x',y',z')的混沌吸引子，图 5(c)是(u,v,w)的混沌吸引子，图 5(d)是(u',v',w')的混沌吸引子。

图 6(a)、(b)、(c)、(d)分别表示 $x'(t)$、$x(t)$、$s(t)$、$u(t)$的时间信号。

解密信号 $m'(t)$如图 7 所示。由图 7 可见，经过短暂

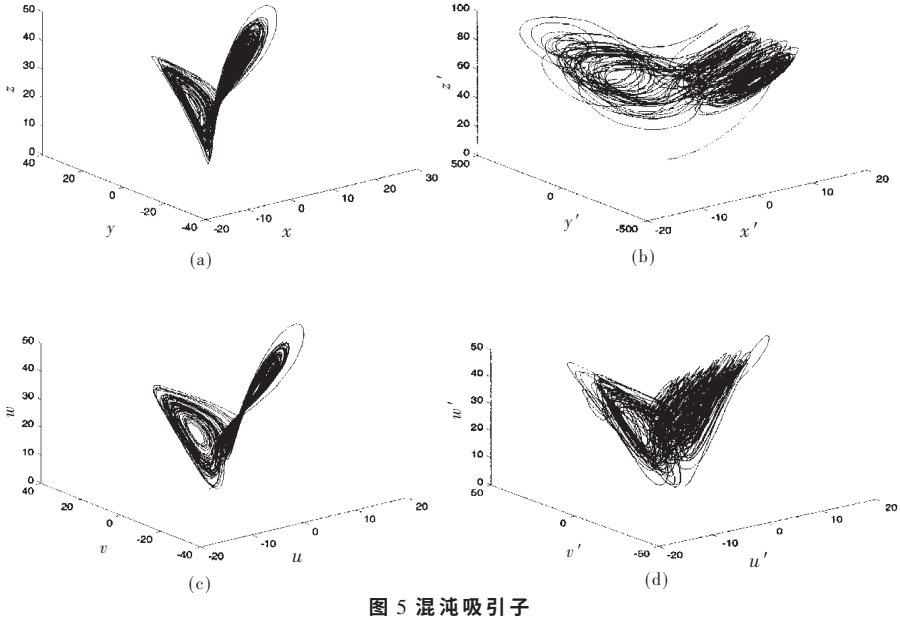

图 5 混沌吸引子

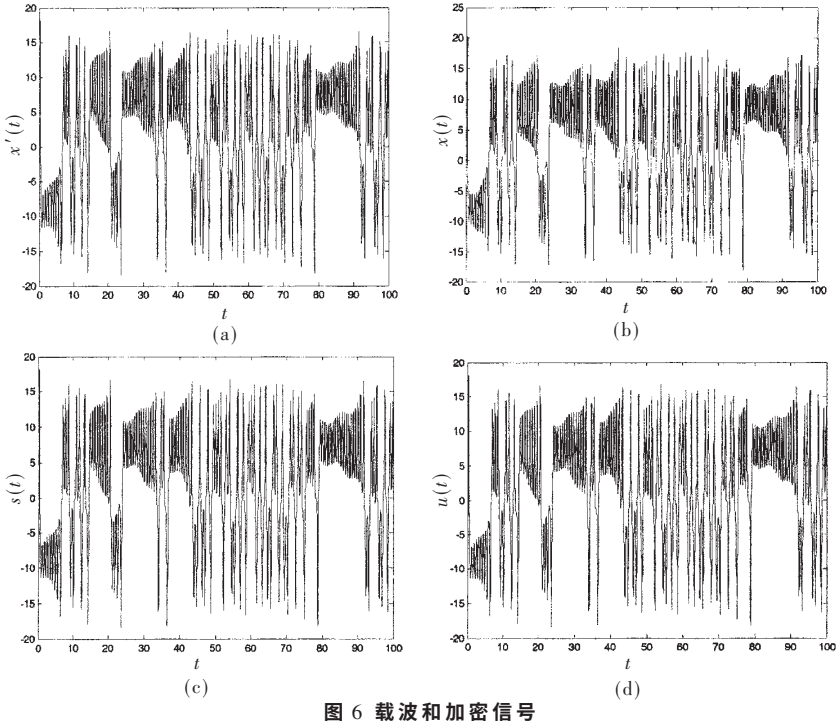

图 6 载波和加密信号

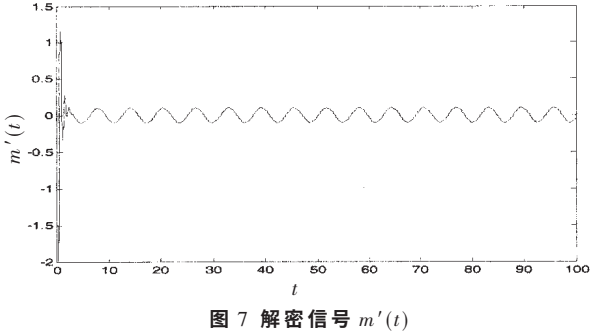

图 7 解密信号 $m'(t)$

的瞬态后，很好地实现了对信号的解密。

本文针对军事通信安全性保密性要求高的特点，利用一种混沌加密技术来提高军事通信的保密性能，实现了单向耦合同步的混沌遮掩保密通信，并且基于 Lorenz 系统实现了一种二阶级联混沌保密通信系统，最后通过数值仿真得到了很好的效果。

参考文献

[1] 王 玫，仇洪冰，郑继禹.混沌保密通信方法研究[J].通信保密，1997，69(1)：8-12.

[2] 程极泰. 浑沌的理论与应用[M]. 上海：上海科学技术文献出版社，1992.

[3] 杨秀丽，王路唐，黄肇明.混沌通信技术概述[J].微计算机信息，2004，20(12)：119-122.

[4] 兀旦辉，柯熙政，刘小河.混沌保密通信进展[J].现代电子技术，2003，14：50-53.

[5] 陈关荣，吕金虎.Lorenz 系统的动力学分析、控制和同步[M].北京：科技出版社，2003.

[6] 兀旦晖，宋玲芳. 一种基于两级混沌调制保密通信方案的研究[J].西安：陕西科技大学学报，2006，24(3)：104-109.

[7] 邱关源.现代电路理论[M].北京：高等教育 出版社，2001.

[8] 翁贻方，翁莉娟，张蕾.提高混沌同步保密通信安全性的设计方案研究[J].电子与信息学报，2004，26(7)：1057-1063.

[9] 关新平，范正平，陈彩莲，等.混沌控制及其在保密通信中的应用[M].北京：国防工业出版社，2002.

[10] 强 浩. 混沌同步在保密通信中的应用[D].南京：南京理工大学，2004.

（收稿日期：2006-09-19）