一个通过混沌同步实现保密通信的新方法 [1]

尹元昭

(中国科学院电子学研究所 北京 100080)

摘 要 提出一个通过混沌同步实现保密通信的新方法。用变型蔡氏电路为例，数值模拟证明了这个方法是非常成功的。它的优点是信息信号能够和混沌载波信号一样大，因此当仅发射一个信号时也能达到很高的信噪比，并实现极好的混沌同步与高保真的信号恢复。

关键词 混沌同步，混沌保密通信，变型蔡式电路

中图号 TN918.1

1 引 言

混沌保密通信中有两种实现信号掩蔽的方法。一是将来自发射机的混沌信号加到信息信号上，然后将该复合信号发射给接收机，使接收机和发射机同步，用来自接收机的混沌信号移去复合信号中的信号使所得信息得到恢复 [1] 。另一是用信息信号调制发射机中的参量，使发射信号是一个包含信息信号的混沌信号，再通过接收机的同步来恢复信息信号 [2] 。这两种方法都是用包含信息信号的混沌信号来使接收机和发射机同步的。为了实现良好的同步，信息信号必须比混沌信号小很多。由于实际的系统中总是存在噪声和干扰，这就要求系统有极高的信噪比。对于非常小的信息信号来说，这是难以实现的。

我们已经提出了用两个发射信号的方法 [3,4] ，一是混沌信号，用于控制接收机使它与发射机同步，另一是包含信息信号的混沌信号，实现信息保密。这样就能增大信息信号，从而提高了信噪比。但是由于有两个发射信号，该方法实用上是不方便的。本文提出了一种新方法，只需一个发射信号也能用大的信息信号，从而解决了信噪比问题，克服了上述诸多方法的缺点。

2 用变型蔡氏电路和新方法的通信系统

用变型蔡氏电路 [3,4] 和新方法的通信系统如图 1 所示。混沌信号 $V_{C_1}^{(1)}$ 和信息信号 Signal 相加，将这复合信号发射给接收机，并通过电容 C_2 支路反馈回到发射机，使接收机和发射机同步。在接收机端，从复合信号中减去同步信号 $V_{C_1}^{(2)}$ ，使信息信号得到恢复。

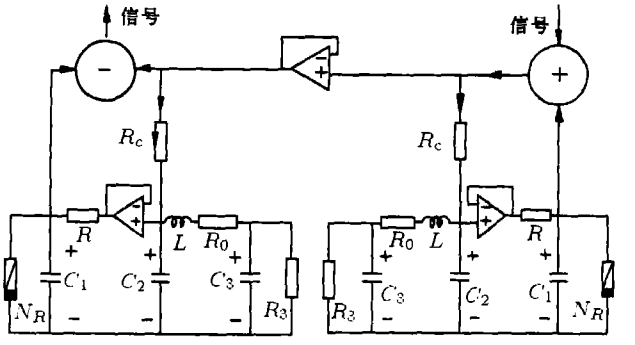

图 1 用变型蔡氏电路的混沌保密通信系统

[1] 1999-05-21 收到，1999-10-13 定稿
国家自然科学基金资助项目

应用基尔霍夫定律得到系统的微分方程为

$$\left.\begin{aligned}
C_1\frac{\mathrm{d}V_{C_1}^{(1)}}{\mathrm{d}t} &= G(V_{C_2}^{(1)}-V_{C_1}^{(1)})-f(V_{C_1}^{(1)})\\
C_2\frac{\mathrm{d}V_{C_2}^{(1)}}{\mathrm{d}t} &= i_L^{(1)}+G_c(V_{C_1}^{(1)}+\mathrm{Signal}-V_{C_2}^{(1)})\\
L\frac{\mathrm{d}i_L^{(1)}}{\mathrm{d}t} &= V_3^{(1)}-V_{C_2}^{(1)}-R_0i_L^{(i)}\\
C_3\frac{\mathrm{d}V_{C_3}^{(1)}}{\mathrm{d}t} &= -i_L^{(i)}-G_3V_{C_3}^{(1)}\\
C_1\frac{\mathrm{d}V_{C_1}^{(2)}}{\mathrm{d}t} &= G(V_{C_2}^{(2)}-V_{C_1}^{(2)})-f(V_{C_1}^{(2)})\\
C_2\frac{\mathrm{d}V_{C_2}^{(2)}}{\mathrm{d}t} &= i_L^{(2)}+G_c(V_{C_1}^{(1)}+\mathrm{Signal}-V_{C_2}^{(2)})\\
L\frac{\mathrm{d}i_L^{(2)}}{\mathrm{d}t} &= V_{C_3}^{(2)}-V_{C_2}^{(2)}-R_0i_L^{(2)}\\
C_3\frac{\mathrm{d}V_{C_3}^{(2)}}{\mathrm{d}t} &= -i_L^{(2)}-G_3V_{C_3}^{(2)}
\end{aligned}\right\}\tag{1}$$

其中 $G=1/R$, $G_3=1/R_3$, $G_c=1/R_c$, R_c 是耦合电阻，$f(v)=G_bV+0.5(G_a-G_b)\times[|V+B_P|-|V-B_P|]$ 是蔡氏二极管的数学表达式。因为有信息信号输入系统，这组方程是非自洽的。

通过下列变换:

$$\begin{aligned}
x^{(1)}&=V_{C_1}^{(1)}/B_p,\ y^{(1)}=V_{C_2}^{(1)}/B_p,\ z^{(1)}=i_L^{(1)}/B_pG,\ w^{(1)}=V_{C_3}^{(1)}/B_p\\
x^{(2)}&=V_{C_1}^{(2)}/B_p,\ y^{(2)}=V_{C_2}^{(2)}/B_p,\ z^{(2)}=i_L^{(2)}/B_pG,\ w^{(2)}=V_{C_3}^{(2)}/B_p\\
\tau&=tG/C_2,\ \alpha=C_2/C_1,\ \beta=C_2/LG^2,\gamma_1=G_3/G,\ \gamma_2=C_2/C_3\\
\gamma_3&=G_c/G,\ \gamma_4=R_0G,\ a=G_a/G,\ b=G_b/G,S_0=\mathrm{Signal}/B_p\\
g(x)&=bx+0.5(a-b)[|x+1|-|x-1|]
\end{aligned}$$

可使方程组 (1) 变成下列无量纲的方程组:

$$\left.\begin{aligned}
\dot{x}^{(1)} &= -\alpha(x^{(1)}-y^{(1)}+g(x^{(1)}))\\
\dot{y}^{(1)} &= z^{(1)}+\gamma_3(x^{(1)}+S_0-y^{(1)})\\
\dot{z}^{(1)} &= -\beta(y^{(1)}-w^{(1)}+\gamma_4z^{(1)})\\
\dot{w}^{(1)} &= -\gamma_2(z^{(1)}+\gamma_1w^{(1)})\\
\dot{x}^{(2)} &= -\alpha(x^{(2)}-y^{(2)}+g(x^{(2)}))\\
\dot{y}^{(2)} &= z^{(2)}+\gamma_3(x^{(1)}+S_0-y^{(2)})\\
\dot{z}^{(2)} &= -\beta(y^{(2)}-w^{(2)}+\gamma_4z^{(1)})\\
\dot{w}^{(2)} &= -\gamma_2(z^{(2)}+\gamma_1w^{(2)})
\end{aligned}\right\}\tag{2}$$

3 数值模拟

我们用数值模拟来证明本方法用于混沌保密通信的卓越性能。所取的参数如下: $C_1 = 10\text{nF}$, $C_2 = 99.34\text{nF}$, $L = 18.46\text{mH}$, $R_0 = 10\Omega$, $R = 1.64\text{k}\Omega$, $B_P = 1\text{V}$, $G_a = -0.76\text{mS}$, $G_b = -0.41\text{mS}$, 从而给出 $\alpha = 9.934$, $\beta = 14.47$, $a = -1.2464$, $b = -0.6724$ 。初条件对于发射机为 $V_{c_1}^{(1)} = 1.5\text{V}$, $V_{c_2}^{(1)} = 0$, $V_{c_3}^{(1)} = 0$, $i_L^{(1)} = 0$; 对于接收机为 $V_{c_1}^{(2)} = 1.6\text{V}$, $V_{c_2}^{(2)} = 0.1\text{V}$, $V_{c_3}^{(2)} = 0.1\text{V}$, $i_L^{(2)} = 0$ ，以便证明同步对发射机和接收机的初条件的差异不敏感。耦合电阻 $R_c = 3\text{k}\Omega$ 。

在模拟中，信息信号为一个矩形波，有二个振幅，如图 2 所示。大振幅为 S_i ，小振幅是大振幅的一半。我们取 $S_i = 1\text{V}$ ，以便证明即使信息信号和混沌信号有同一量级，也能得到极好的同步。矩形波的重复频率 $f = 0.69\text{kHz}$ ，周期 $T = 1.45\text{ms}$ 。

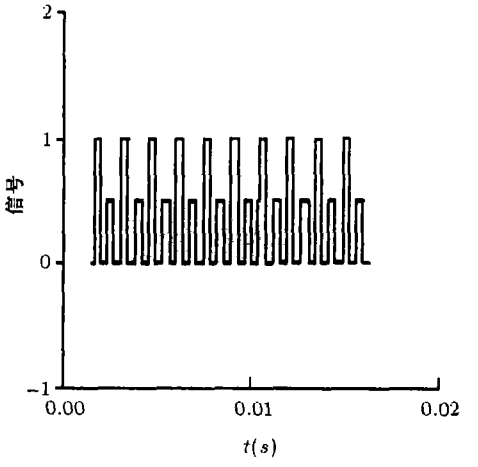

图 2 输入的信息信号

利用变型蔡氏电路的混沌保密通信的典型结果如图 3 所示。图 3(a) 是发射机中 $V_{C_1}^{(1)}$ 和 $V_{C_2}^{(1)}$ 的相图，它是双涡蔡氏吸引子。图 3(b) 是接收机的 $V_{C_1}^{(2)}$ 随发射机的 $V_{C_1}^{(1)}$ 的变化。它是一条通过原点的 45° 直线，表明接收机和发射机很好同步。图 3(c) 是用来掩蔽信息信号的 $V_{C_1}^{(1)}$ 波形。图 3(d) 是发射机给接收机的 $V_{C_1}^{(1)}$+ 信息信号的波形，由图可见只要信息信号比 $V_{C_1}^{(1)}$ 小就无法探测出来。图 3(e) 是同步误差 $|V_{C_1}^{(2)} - V_{C_1}^{(1)}|$ 随时间 t 的变化，可见因为同步误差随时间指数减小，所以能实现极好的同步，在小于 10^{-4}s 的时间内达到同步，并变得越来越好。图 3(f) 是恢复的信息信号，它和图 2 所示的原始的信息信号完全一致。在图 3 中 $R_3^{(1)} = R_3^{(2)} = 100\Omega$, $C_3^{(1)} = C_3^{(2)} = 50\mu\text{F}$ ， $R_c = 3\text{k}\Omega$, $S_i = 1.0\text{V}$, $f = 0.69\text{kHz}$ 。

我们可以改变 R_3, C_3, R_c, S_i, f ，在一定的范围内都能实现如图 3 所示的极好的同步和信号恢复。限于篇幅，就不将它们的模拟结果在这里一一列出了。

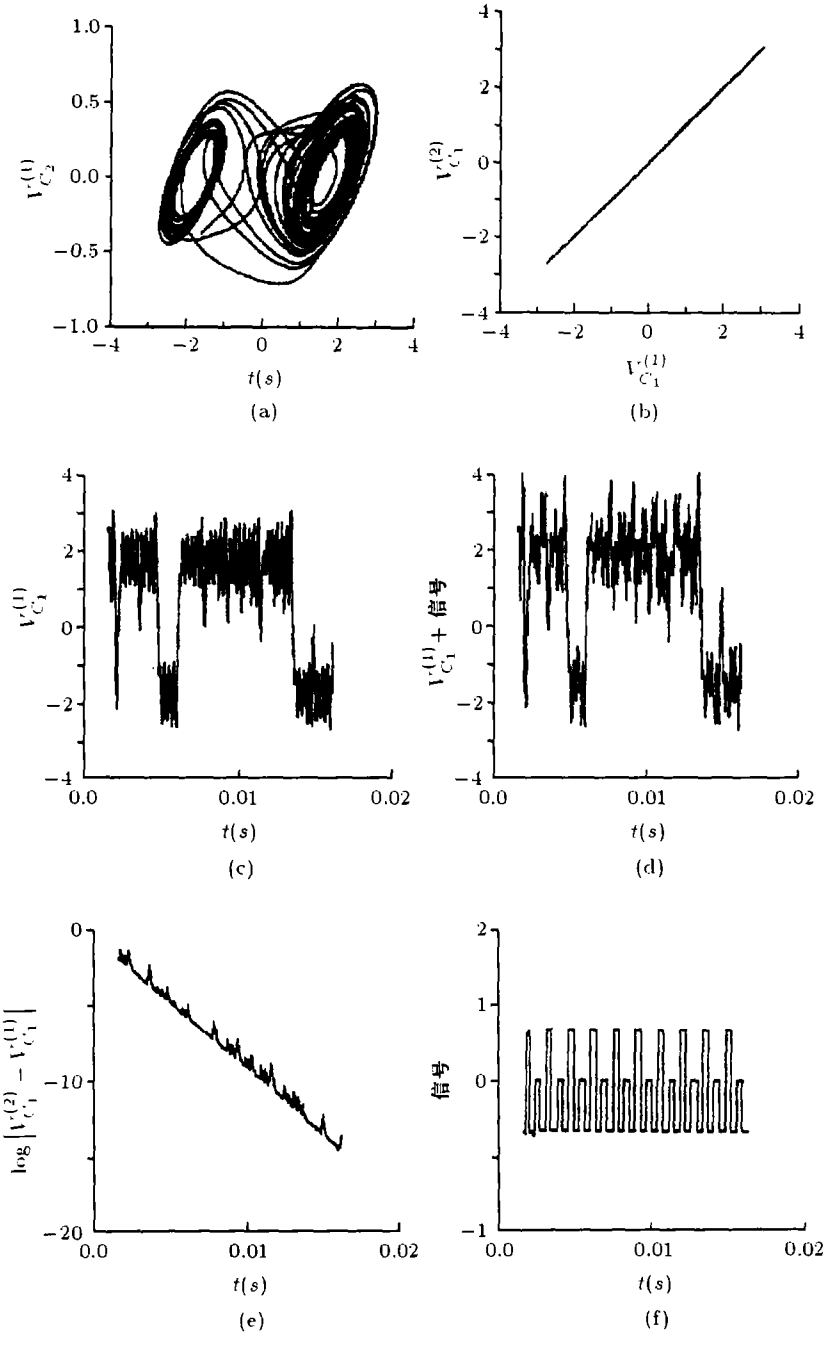

图 3　对图 1 的系统进行数值模拟的结果

4 结　论

从上述的数值模拟结果我们可以得出下列结论：(1) 用新的混沌保密通信方法，能得到非常精确的同步，有极好的鲁棒性。混沌电路很简单，发射机和接收机是相同的，不需要进行分解 [1]，只需一个发射信号，也能得很高的信噪比。(2) 虽然变型蔡氏电路和蔡氏电路用本方法都能得到相似的同步，但是用变型蔡式电路比蔡氏电路有下列优点；第一，我们能保持蔡氏电路参数不变，仅改变 R_3 或 C_3 就能得到各种不同的混沌状态。这使混沌保密通

信更加方便、灵活和保密性更好。第二，变型蔡氏电路是四维的，比蔡氏电路多一维，是产生超混沌的最低维数的混沌电路。我们可利用超混沌来实现更强的保密性。第三，在变型蔡氏电路中即使电感的内阻 R_0 很大也能产生混沌状态，而蔡氏电路就不行，这对实际应用是有利的。

参 考 文 献

[1] L. J. Kocarev, *et al.*, Experimental demonstration of secure communications via chaotic synchronization, Int. J. Bifurcation and Chaos, 1992, 2(3), 709–713.

[2] U. Parlitz, *et al.*, Transmission of digital signals by chaotic synchronization, Int. J. Bifurcation and Chaos, 1992, 2(4), 973–977.

[3] Y. Z. Yin, Synchronization of chaos in a modified Chua's circuit using continuous control, Int. J. Bifurcation and Chaos, 1996, 6(11), 2101–2117.

[4] Y. Z. Yin, Experimental demonstration of chaotic synchronization in the modified Chua's circuits, Int. J. Birurcation and Chaos, 1997, 7(6), 1401–1410.

A NEW WAY TO SECURE COMMUNICATION VIA CHAOTIC SYNCHRONIZATION

Yin Yuanzhao

(*Institute of Ecletronics, Academia Sinica, Beijing* 100080, China)

Abstract This paper puts foward a novel way to achieve chaotic synchronization. Take the modified Chua's circuit as example, the numerical simulation shows this way is very successful. The message signal can be as large as the chaotic carrier signal, so the signal-to-noise ratio can be very high even when only one signal is transmitted. The synchronization is excellent and the retrieved signal is virtually perfect.

Key words Chaotic synchronization, Chaotic secure communication, The modified Chua's circuit

尹元昭： 男，1937 年生，研究员，中国电子学会高级会员，主要从事强流电子束产生相干辐射，如自由电子激光器等和电磁理论中的非线性问题，如混沌等的研究工作.