探究改进混沌掩盖保密通信的方案

冯威赫

（复旦大学 08 级材料科学系材料物理专业 08300300044）

【摘要】利用混沌实现保密通信常见的有两种方式[1]，一种是混沌编码保密通信，另一种是混沌掩盖保密通信。混沌编码方式保密效果好，但不能对模拟信号进行加密。混沌掩盖方式可以对模拟和数字信号进行加密，但加密效果不理想。本文主要探究如何改进混沌掩盖方式保密效果，采用了四阶蔡氏电路加强系统同步效果、改进了加密器和解密器以加强混沌信号掩盖效果。

【关键字】混沌 保密通信 掩盖 同步 四阶蔡氏电路

引言

混沌是指发生在确定性系统中的貌似随机的不规则运动。一个确定性理论描述的系统，其行为却表现为不确定性－－不可重复、不可预测，这就是混沌现象[2]。进一步研究表明，混沌是非线性动力系统的固有特性，是非线性系统普遍存在的现象。在现实生活和实际工程技术问题中，混沌是无处不在的。

由于混沌具有对初值极端敏感和长期不可预测的特性,使得其特别符合保密通信的要求。它的起源应该追溯到 1990 年 Pecora 和 Carroll 提出的混沌同步的概念。近年来，混沌保密通信已经成为了混沌学发展的重要方向之一。目前已衍生出多种混沌加密方式，如混沌掩盖、混沌参数调制、混沌编码、混沌扩频、混沌数字码分多址等[3]。其中适合普通大学实验室进行的主要有混沌掩盖和混沌编码两种方式。混沌编码方式保密效果好，但是不能对模拟信号进行加密，使得其应用范围大大减小。而混沌掩盖方式应用范围广阔，原理简单实现容易,但存在的致命缺点是加密效果并不理想。

本文从改善混沌信号掩盖效果和改善同步效果两方面入手,提出了可行的增强混沌掩盖加密效果的有效方案。本文首先利用软件模拟了基本情况下的混沌掩盖通信系统并用面包板和蔡氏电路实验箱搭建了实际的通信电路进行验证。之后就改善混沌信号掩盖效果的问题，对加密电路和解密电路进行了改造并用软件模拟了效果。最后就改善系统同步效果提出了将普通蔡氏电路改造为四阶蔡氏电路的方案，并进行了软件模拟。

一. 利用基本蔡氏电路搭建混沌掩盖保密通信系统

蔡氏电路（Chua's Circuit），是 1983 年由蔡少堂（Leon O.Chua）提出的一种能够实现混沌现象的最简单的电路之一。它（如图 1 所示）的主要元件有可调电阻 R（电路方程中以电导 G=1/R 做参数，以下方程求解过程都用 G 来表示，而涉及实验的内容采用 R 表示）、电容 C_1 和 C_2、电感 L 以及非线性负阻 Nr。它的运行状态可以用以下方程组来描述：

$$\begin{cases} C_1 \dfrac{dU_1}{dt} = G(U_2 - U_1) - g(U_1) \\ C_2 \dfrac{dU_2}{dt} = G(U_1 - U_2) + I_L \\ L \dfrac{dI_L}{dt} = -U_2 \end{cases}$$

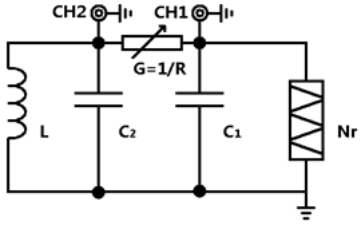


图 1 蔡氏电路示意图

其中 U_1 为 C_1（或负阻 Nr）两端的电压，U_2 为 C_2（或 L）两端的电压，I_L 为通过 L 的电流，g(U) 为非线性负阻的 I-V 特性函数，其表达式为：

$$g(U)=G_bU+\frac{G_b-G_a}{2}(|U-E|-|U+E|)$$

非线性系统必须包含如下原件：一个非线性原件如非线性负阻，用来产生非线性信号；一个电阻，用来耗散能量；以及至少三个用来储存能量的储能元件。图 1 中的蔡氏电路含有三个储能元件，故称为三阶蔡氏电路。

混沌掩盖保密通信的原理十分简单:利用蔡氏电路产生混沌信号,发送端利用加法器将有用信号与混沌信号叠加，完成加密。接收端利用减法器将接收到的信号减去混沌信号即可得到有用信号。由于混沌对初始条件的极端敏感性,发送端与接收端蔡氏电路必须严格同步才能完成信号的正常传送。

图 2 为混沌掩盖保密通讯原理图[4]。左边的蔡氏电路为发送端，右边为接收端。两者 U_1 通过同步线相连。

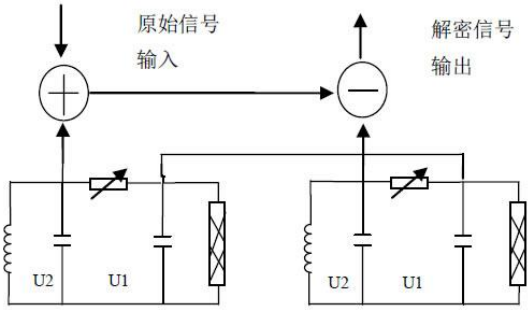


图 2　混沌掩盖保密通信原理图

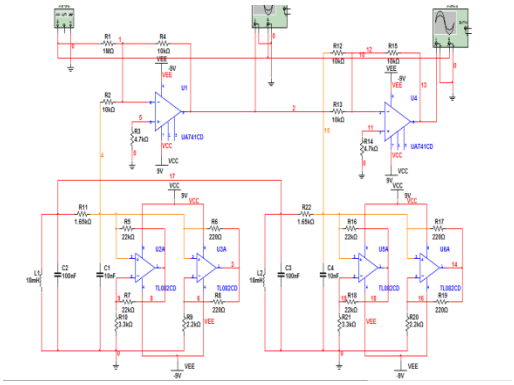


图 3　Muitisim 模拟电路图

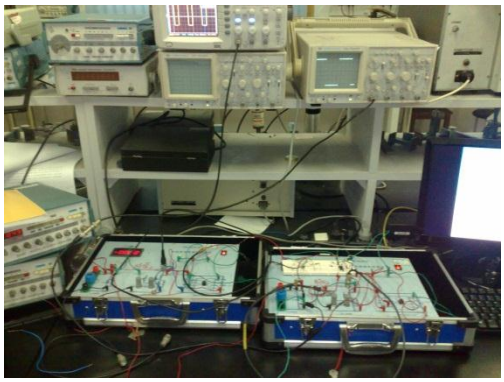


图 4　实验中搭建的混沌掩盖保密通信电路

图 3 为用 NI Multisim 软件搭建的三阶蔡氏电路混沌掩盖保密通信系统，图 4 为实际实验中搭建的电路。

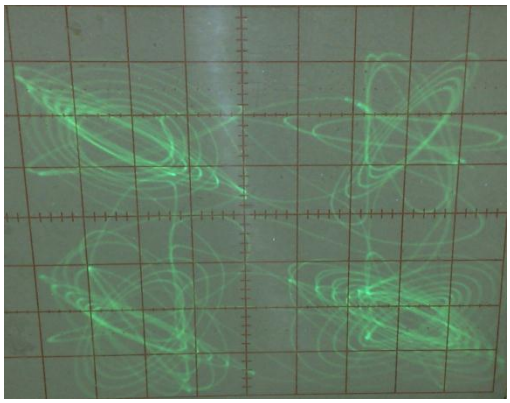


图 5　未同步时的两电路信号

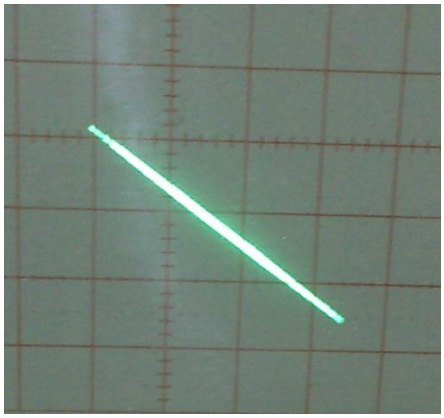


图 6　U_1 同步后的系统同步线

实验时用断开接地的信号发生器产生的 50Hz 方波作为有用信号。先将两蔡氏电路都调至双吸引子混沌状态，将两者 U_1 用同步线相连。发送端 U_2 与加密电路相连作为掩盖信号，

接收端 U_2 与解密电路相连作为解密信号。

在进行加密通信之前先用示波器查看一下两蔡氏电路的状态。图 5 为未经同步的两蔡氏电路混沌信号。可以看到，尽管两电路均已调至双吸引子状态，但由于初始信号的细微不同，导致两电路信号完全不同步，无法用于加密通信。

图 6 为将两者 U_1 用同步线相连后的信号。可以看到，在连接同步线之后两电路的同步情况很好，同步线呈 45 度直线，虽然内部仍有一些结构，但已达到实验要求。

当 U_1 作同步信号，U_2 作掩盖信号时，同步信号状态如图 6 所示，系统的掩盖效果和解密效果如图 7、图 8 所示。可以看出，此时混沌信号的掩盖效果并不好，仍然可以看出方波的形状。不过因为此时系统同步状态很好，所以解密质量相当好，解密所得信号几乎没有毛刺，与原信号一致。

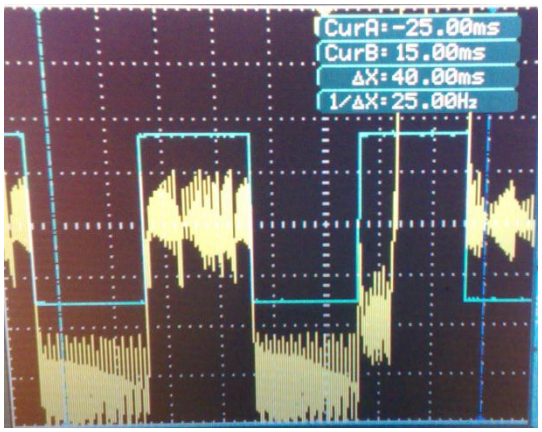


图 7　掩盖信号

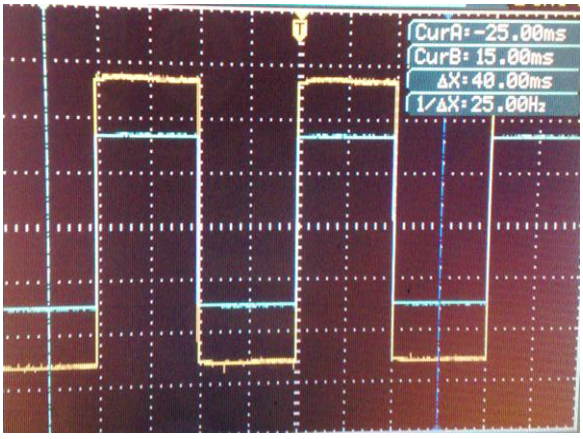


图 8　解密信号

当 U_2 作同步信号，U_1 作掩盖信号时，同步信号状态如图 9 所示，系统的掩盖效果和解密效果如图 10、图 11 所示。此时的掩盖信号质量大大增加，已基本看不出方波的形状，说明加密效果较好。但此时的解密质量很差，不仅信号有大量毛刺，连方波本身形状都有所变化。这是因为此时系统的同步状态并不理想，虽然同步线大致呈 45 度直线，但内部结构众多，线宽较大，导致解密效果不理想。

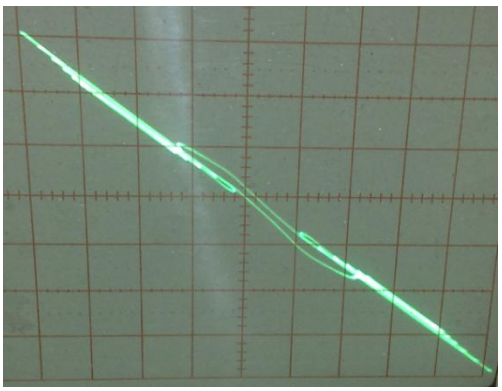


图 9　U_2 同步后的系统同步线

图 10

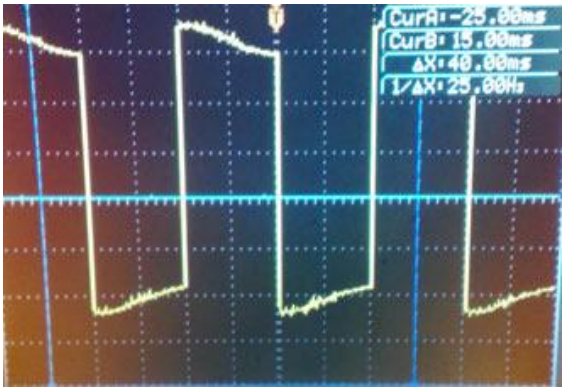


图 11

二. 改造加密和解密电路以增强掩盖效果

从上文中我们可以看出，U_1 作同步线时解密质量是相当好的，只是此时的掩盖信号质量稍差，仍可看出有用信号的形状，下面将从改造加密和解密电路入手改善这一问题。

在参考文献[4]中，曹宇学长用同相加法器作为加密电路，用差动减法器作为解密电路。本实验中加密和解密电路均采用反相加法器，可以达到同样的效果。

反相加法器（加密电路）电路图如图 12 所示，利用 uA741 运放配合外围电路实现加法功能。输出表达式为：

$$V_{O+}(\mathrm{t}) = -(\frac{R_{4+}}{R_{1+}}V_{\mathrm{i}1+}(t) + \frac{R_{4+}}{R_{2+}}V_{i2+}(t))$$

设$V_{\mathrm{i}1+}(t)$为有用信号，$V_{i2+}(t)$为混沌信号。当元件参数按图中标注时，有：

$$V_{O+}(\mathrm{t}) = -(V_{\mathrm{i}1+}(t) + V_{i2+}(t))$$

所得混沌掩盖信号与有用信号反相。

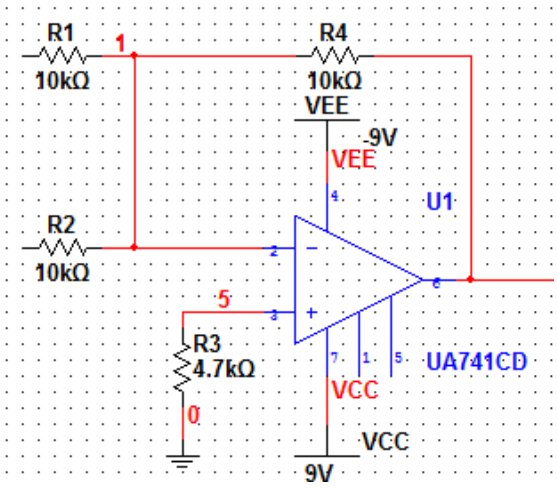


图 12　反相加法器电路图

本实验中解密电路采用反相加法器实现。输出表达式为：

$$V_{O-}(\mathrm{t}) = -(\frac{R_{4-}}{R_{1-}}V_{\mathrm{i}1-}(t) + \frac{R_{4-}}{R_{2-}}V_{i2-}(t))$$

在本实验中，有

$$V_{\mathrm{i}1-}(t) = V_{O+}(\mathrm{t})$$

$$V_{i2+}(t) = V_{i2-}(t) = \text{混沌信号}$$

按图中标注数据可得

$$V_{O-}(\mathrm{t}) = -\big(V_{\mathrm{i}1-}(t) + V_{i2-}(t)\big) = -\Big(-\big(V_{\mathrm{i}1+}(t) + V_{i2+}(t)\big) + V_{i2-}(t)\Big) = V_{\mathrm{i}1+}(t)$$

即可实现加密解密功能。

图 13 为R_{1+}=10kΩ时的混沌掩盖信号软件模拟图。可以看出，此时混沌掩盖质量相当差，几乎就是在方波上叠加了一个小的混沌信号，原方波信号清晰可见。

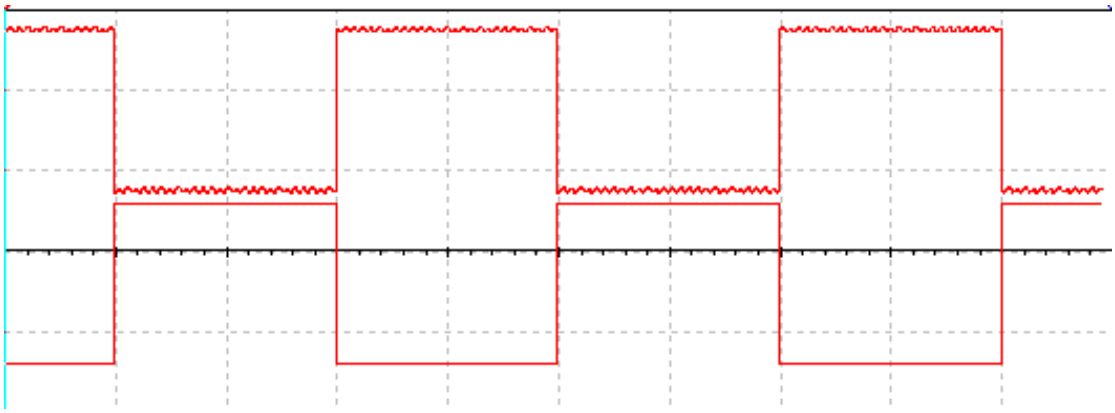


图 13

考虑反相加法器的输出表达式可以发现，若改变 R_1 和 R_2 的比值，就可以改变方波信号与混沌信号的幅度比。这样我们只需要增大 R_1 和 R_2 的比值就可以增强混沌效果，当然相应的解密电路输入的混沌信号阻抗要与加密输入的混沌信号相匹配。通过不断对比试验发现，当取R_{1+}=1MΩ，其余电阻不变时，掩盖效果最好。如图 14 所示。

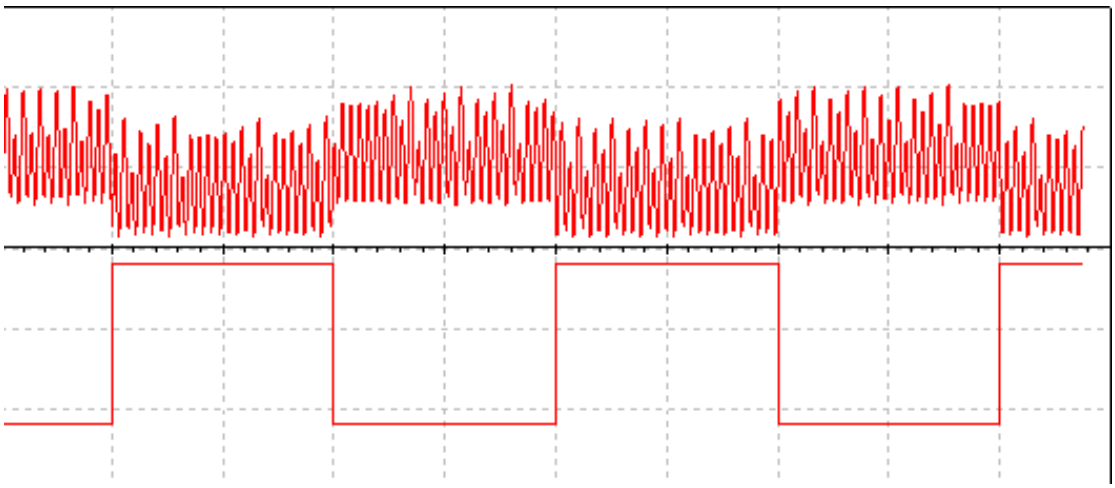


图 14

这时的掩盖效果有了明显提升，基本已看不出方波形状。但此时叠加信号的幅度明显减小，大约只有原方波信号的 15%。虽然 Multisim 中模拟所得的解密结果非常漂亮，但是考虑到实际电路中存在的干扰等问题，过小的叠加信号幅度会给解密造成很大困难。比较好的解决方案是在电路中加一放大器将叠加信号放大后再进行解密。

三. 利用四阶蔡氏电路搭建混沌掩盖保密通信电路

由【一】中分析可知，当采用 U_2 作同步信号，U_1 作掩盖信号时，影响系统解密质量的主要原因就是两蔡氏电路的同步质量较差。如果采用 U_1 作同步信号，U_2 作掩盖信号，并采用【二】中方法增强掩盖效果后，由于叠加信号幅度变小，导致干扰相对增大，要想获得较好的解密效果，对系统的同步质量要求非常高。

由此可见，系统的同步质量是影响混沌掩盖保密通信效果的一个重要因素。

本方法中采用的四阶蔡氏电路[5]是在原三阶电路的 L 臂上加上一个由 R_3 和 C_3 组成的 RC 并联电路，使电路由三阶提高到四阶。采用四阶蔡氏电路的优势是一方面可以加强同步质量，另一方面可以产生更加复杂的混沌信号，增加信号的不可预测性，从而增强保密效果，减小被破解的风险。

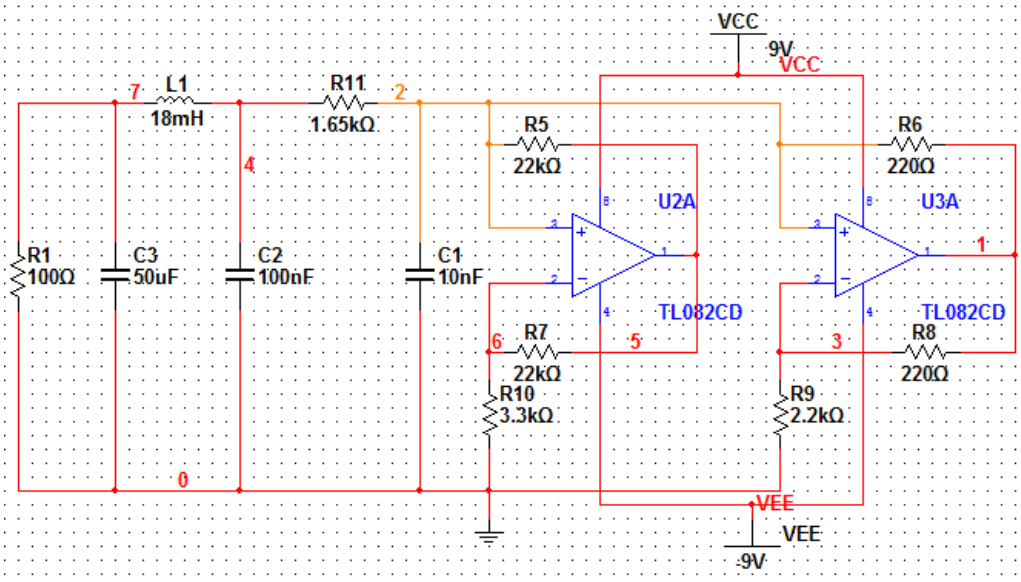


图 15　四阶蔡氏电路示意图

四阶蔡氏电路的电路图如图 15 所示。用它代替图 3 混沌掩盖保密通信系统电路图中的三阶电路，重新进行软件模拟。采用用 U_1 作同步信号，U_2 作掩盖信号。得到的叠加信号如图 16 所示。

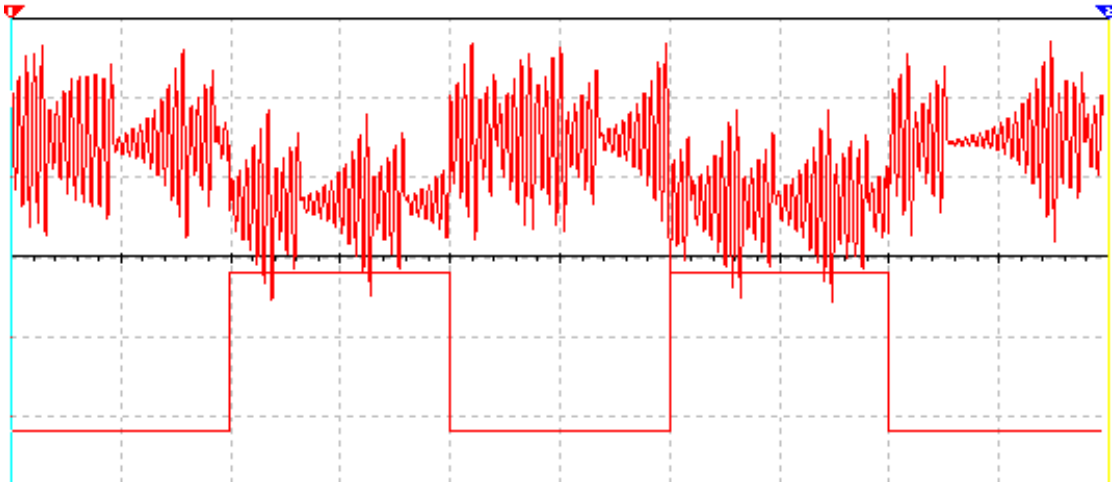


图 16

很明显地可以看到，在相同的情况下，四阶蔡氏电路所得到的叠加信号的掩盖效果要明显好于三阶电路，已经完全无法看出原方波信号的形状。解密输出信号非常完美，如图 17 所示（上为原方波信号，下为解密输出信号，二者幅度比为 40:1）

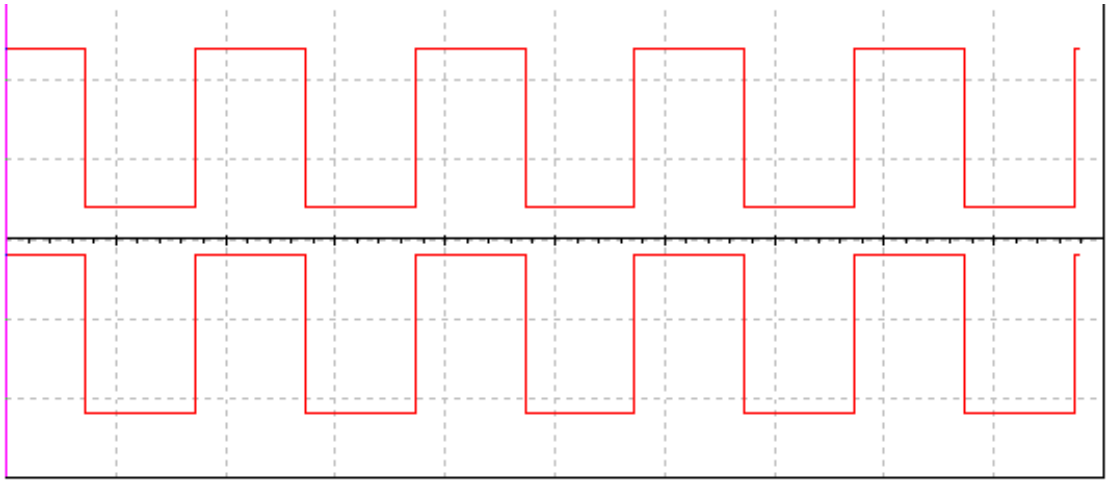
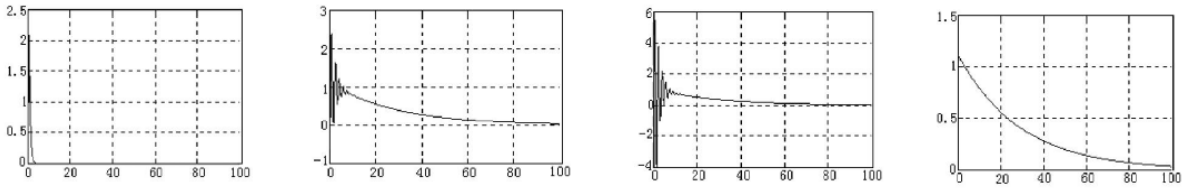


图 17

图 18 为参考文献[5]中的四阶蔡氏电路同步信号误差图（未找到 Multisim 中如何作出同步信号误差图，只好选用他人数据）



(a) error($x - \hat{x}$)　(b) error($y - \hat{y}$)　(c) error($z - \hat{z}$)　(d) error($w - \hat{w}$)

图 18　各相应状态变量的同步误差图(数量级均为 10^{-3})

从图 18 的误差可以看出响应电路的状态变量经过短时间的波动后，才逐渐与驱动电路的状态变量达到严格同步。这主要是因为数值积分时，采用的是迭代方法，两系统由不同的初始状态开始，直至最后完全同步需要有一短暂的迭代过程。经过这一过渡过程之后，就可达到

严格同步。与蔡氏电路的同步误差相比,该变型电路各相应状态变量的同步误差要小大约两个数量级[6]。

结束语

本文利用 Multisim 软件和实验室现有设备探究了混沌保密通信的实现方法，并就改进混沌掩盖保密通信从两个方面提出了不同方案,分别进行了软件模拟,并对结果进行了分析。混沌保密通信作为一种行之有效的保密通信方法，随着技术的不断进步，在将来必定有更加广阔的应用前景。

参考文献

[1]张玉兴等,《非线性电路与系统》，北京机械工业出版社，2007

[2]百度百科，“混沌”词条，2010.12.27 更新

[3]禹思敏，吕金虎,《基于文氏电桥的超混沌保密通信及其DSP实现》，Proceedings of the 26th Chinese Control Conference，July 26-31，2007，Zhangjiajie，Hunan，China

[4]曹宇，《基于蔡氏电路的混沌保密通信实验》，复旦大学近代物理实验课程论文，2009

[5]王玉芳,《四阶变型蔡氏电路的混沌同步及其保密通信》,青岛大学学报(自然科学版)2005年6月第18期第2版

[6]杨林保，李先梅，《自适应模型0跟踪控制的蔡氏电路的同步》，鄂州大学学报，1997