

## 基于输出控制的混沌同步保密通信系统

黄丽莲 尹启天

(哈尔滨工程大学信息与通信工程学院 哈尔滨 150001)

**摘要:** 该文提出一种基于混沌系统输出线性化的反馈控制方法, 将混沌系统的非线性部分线性化, 从而将复杂的非线性混沌系统的同步问题转化为简单的线性混沌系统的稳定性问题, 然后通过极点配置理论, 用线性化的方法同步两个非线性混沌系统。基于这种同步方法设计出混沌保密通信系统, 系统的一条通道用来传输输出信号, 另一条通道传输通过遮掩和调制隐藏后的信息信号。仿真结果表明这种保密通信系统是有效的。

**关键词:** 混沌同步; 保密通信; 非线性系统; 反馈控制; 输出控制

中图分类号: TN918

文献标识码: A

文章编号: 1009-5896(2009)10-2402-04

## A Chaos Synchronization Secure Communication System Based on Output Control

Huang Li-lian Yin Qi-tian

(College of Information and Communication, Harbin Engineering University, Harbin 150001, China)

**Abstract:** In this paper, based on output linearization feedback control, the nonlinear function of the chaotic system is linearized, then the complex synchronization of the nonlinear chaotic system is converted into the stable problem of the linearization system. Then a nonlinear controller is given by pole assignment. Furthermore based on the scheme above, a system of secure communication is proposed. One channel of the system is output of the chaotic transmitter, the other one transmits the information-bearing signal. Finally a numerical example is used to show the effectiveness of the proposed technique.

**Key words:** Chaos synchronization; Secure communication; Nonlinear system; Feedback control; Output control

### 1 引言

混沌系统的线性化, 是工程技术中一种常用方法。经典的线性化方法是: 在系统的平衡点附近取线性近似, 得到线性化系统。这种线性化方法只适用于接近平衡点的邻域, 当系统工作范围增大时, 这种方法将会产生较大误差<sup>[1]</sup>。因此, 它不适用于系统状态远离平衡点的非线性系统的控制。克服线性近似方法缺点的有效途径是采用通过反馈而实现的精确线性化的方法, 而混沌同步多数是从状态变量去考虑。这种<sup>[2-10]</sup>同步方法的基本思想是在系统可以转化为规范型的前提下, 由两个混沌系统的输出之差和输出的各阶导数之差构造误差方程, 再设计反馈控制使两个混沌系统同步<sup>[11-13]</sup>。

利用混沌同步进行保密通信是国际研究的一大热点, 正在发展为高新技术的一个新领域。目前已提出的大多数基于混沌同步的保密通信研究<sup>[14-16]</sup>都集中在混沌同步方法上。本文使用了双通道混沌保密通信系统的方案, 这种方案把同步与信息传递

分开进行, 在发送端与接收端建立两条通道, 一条通道用来保证驱动系统与响应系统的同步, 一条通道用来传输信息, 原理图如图 1 所示。

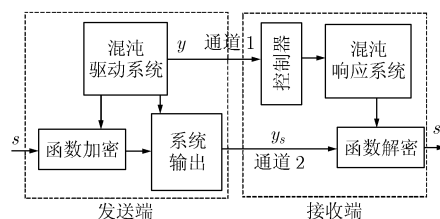


图 1 双通道混沌保密通信系统原理图

在图 1 中, 通过混沌系统的状态信息和设计好的加密函数把信息信号  $s$  进行加密处理得到信息  $y_s$ , 通过一条单一通道 2 传输, 另一条通道 1 用来传输驱动系统的状态信息给控制器, 控制器控制响应系统保证两个系统同步, 并且通过响应系统的状态信息和相应的解密函数对接收到的信息进行解密恢复出信息  $s_d$ , 最后完成保密通信。

### 2 控制器的设计

对于一类单输入-单输出仿射非线性系统, 以非

线性系统

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \quad (1)$$

为例, 其中,  $x \in R^n, y \in R, f, g$  为  $n$  维光滑向量场,  $x$  是系统的状态变量,  $y$  是输出,  $h(x)$  为光滑函数。设系统式(1)在  $x_0$  处相对阶为  $r(r \leq n)$ , 令  $\varphi_i(x) = L_f^{i-1}h(x), i = 1, 2, \dots, r$ 。若  $r$  严格小于  $n$ , 则总能找到  $n - r$  个函数  $\phi_{r+1}(x), \phi_{r+2}(x), \dots, \phi_n(x)$ , 使得映射  $\varphi(x) = [\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x)]^T$  在  $x_0$  处有非奇异的 Jacobi 矩阵。并且我们总是可以选择  $\varphi_{r+1}(x), \varphi_{r+2}(x), \dots, \varphi_n(x)$ , 使得  $L_g\phi_i(x) = 0, \forall r + 1 \leq i \leq n, \forall x \in U_0$ 。

进一步取  $[\varphi_{r+1}(x), \varphi_{r+2}(x), \dots, \varphi_n(x)]^T = [\lambda_1(x), \lambda_2(x), \dots, \lambda_{n-r}(x)]^T$ 。在变换  $z = \varphi(x) = [\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x)]^T = [h(x), L_f h(x), \dots, L_f^{r-1}h(x), \lambda_1(x), \lambda_2(x), \dots, \lambda_{n-r}(x)]^T$  下由于系统相对阶为  $r$ , 故对任意  $k < r - 1, L_g L_f^k h(x) = 0$ , 而  $L_g L_f^{r-1}h(x) \neq 0$ , 因此可以对有  $z = [z_1, z_2, \dots, z_n]^T$  进行向量求导数, 假设非线性系统式(3)的相对阶为  $r = n$ , 则得到标准型的坐标变换为

$$\begin{aligned} \dot{z}_1 &= z_2, \dot{z}_2 = z_3, \dots, \dot{z}_{n-1} = z_n, \dot{z}_n = a(z) + b(z)u \\ &= v, y = z_1 \end{aligned} \quad (2)$$

其中  $a(z) = L_f^r h(\varphi^{-1}(z)), b(z) = L_g L_f^{r-1}h(\varphi^{-1}(z))$ 。显然在  $z_0 = \phi(x_0)$  的一个邻域内,  $b(z) \neq 0$ , 故可选取如下控制律:

$$u = \frac{1}{b(z)}(-a(z) + v) \quad (3)$$

**定理** 设有另一个混沌系统的信号输出  $y_R(t)$ , 并定义驱动系统输出与响应系统输出之间的误差为:  $e(t) = y(t) - y_R(t)$ , 选择反馈控制信号:  $u = \frac{1}{b(z)}(-a(z) + y_R^{(n)}(t) - \sum_{i=1}^n c_{i-1}(z_i - y_R^{(i-1)}(t)))$  时, 其中,  $c_0, c_1, \dots, c_{n-1}$  为待定常数, 两个混沌系统能实现状态的同步。

**证明** 定义驱动系统输出与响应系统输出之间的误差为  $e(t) = y(t) - y_R(t)$ , 则有

$$e^{(i-1)}(t) = y^{(i-1)}(t) - y_R^{(i-1)}(t) = z_i(t) - y_R^{(i-1)}(t)$$

反馈信号又可以写为

$$\begin{aligned} u &= \frac{1}{b(z)} \left( -a(z) + y_R^{(n)}(t) - \sum_{i=1}^n c_{i-1} e^{(i-1)} \right) \\ &= -\frac{1}{b(z)} (a(z) - y_R^{(n)}(t) + \mathbf{C}\mathbf{E}) \end{aligned} \quad (4)$$

其中  $\mathbf{C} = [c_0, c_1, \dots, c_{r-1}]$ ,  $\mathbf{E} = [e, e', \dots, e^{(r-1)}]$ 。代入式(2)中有

$$\begin{aligned} \dot{z}_n &= a(z) + \left[ -a(z) + y_R^{(n)}(t) - \sum_{i=1}^n c_{i-1} e^{(i-1)} \right] \\ &= y_R^{(n)}(t) - \sum_{i=1}^n c_{i-1} e^{(i-1)} \end{aligned} \quad (5)$$

又由于  $\dot{z}_n = y^{(n)}(t)$ , 故有

$$e^{(r)} + c_{r-1} e^{(r-1)} + \dots + c_1 e' + c_0 e = 0 \quad (6)$$

由于  $c_0, c_1, \dots, c_{r-1}$  可以任意设置, 因此, 式(9)对应的微分方程的特征根可以任意配置。我们可以设置  $c_0, c_1, \dots, c_{r-1}$  使得所有特征根均位于复平面的左半开平面, 这样可以使  $\lim_{t \rightarrow \infty} \|y_R(t) - y(t)\| \rightarrow 0$  成立, 两个混沌系统的输出同步, 又由于误差  $e \rightarrow 0$ , 两个混沌系统的状态同步。

### 3 仿真研究

#### 3.1 构建混沌发送系统和接收系统

应用定理, 以 Chua 电路为例进行仿真研究。

Chua 混沌系统方程如下:

$$\begin{cases} \dot{\hat{x}} = \mathbf{A}\hat{x} + \mathbf{B}f(x) \\ y = \mathbf{C}\hat{x} \end{cases} \quad (7)$$

其中  $\hat{x} = [x_1 \ x_2 \ x_3]^T$ , 非线性函数为:  $f(x_1) = bx_1 + 0.5(a - b)(|x_1 + 1| - |x_1 - 1|)$ 。

$$\text{各参数取 } \mathbf{A} = \begin{bmatrix} -\rho & \rho & 0 \\ 1 & -1 & 1 \\ 0 & \sigma & 0 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} -\rho \\ 0 \\ 0 \end{bmatrix}, a = -1.27,$$

$b = -0.68, \rho = 10, \sigma = 14.87$ , 系统是混沌的。并且  $\mathbf{C} = [0 \ 0 \ 1]$ 。

构造混沌响应系统:

$$\begin{cases} \dot{\hat{x}} = \mathbf{A}\hat{x} + \mathbf{B}f(\hat{x}) + \mathbf{G}u \\ \hat{y} = \mathbf{C}\hat{x} \end{cases} \quad (8)$$

其中  $\hat{x} = [\hat{x}_1 \ \hat{x}_2 \ \hat{x}_3]^T$ ,  $\mathbf{C} = [0 \ 0 \ 1]$ ,  $\mathbf{G} = [1 \ 0 \ 0]^T$ 。

#### 3.2 混沌接收系统的反馈线性化

根据定理, 将系统式(11)作为接收系统, 将它进行反馈线性化, 得到接收系统的相对阶为 3, 可以进行完全反馈线性化, 并且标准化方程为

$$\begin{cases} \dot{z}_1 = z_2 \\ \dot{z}_2 = z_3 \\ \dot{z}_3 = a(z) + b(z)u \\ \hat{y} = z_1 \end{cases} \quad (9)$$

其中  $b(z) = -\sigma$ ,  $a(z) = -(\rho + 1)z_3 - \rho\sigma z_1 - \sigma z_2 + \rho\sigma f(-(1/\sigma)(z_2 + z_3) - z_1)$ 。

控制器

$$u = -\frac{1}{b(z)}(a(z) - \hat{y}^{(3)}(t) + CE) \quad (10)$$

3.3 反馈控制器的设计

定义误差变量系统为

$$E = \begin{bmatrix} \hat{y} - y \\ \dot{\hat{y}} - \dot{y} \\ \ddot{\hat{y}} - \ddot{y} \end{bmatrix} = \begin{bmatrix} e_3 \\ -\sigma e_2 \\ -\sigma(e_1 - e_2 + e_3) \end{bmatrix} \quad (11)$$

其中  $e_i, i = 1, 2, 3$  为状态误差, 简化表示为

$$CE = 0$$

其中  $C = [c_0, c_1, c_2]$ 。

将系统式(11)变换成对应的微分方程为

$$\begin{aligned} \begin{bmatrix} \dot{s}_0 \\ \dot{s}_1 \\ \dot{s}_2 \end{bmatrix} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -c_0 & -c_1 & -c_2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} [c_0 \quad c_1 \quad c_2] \begin{bmatrix} s_0 \\ s_1 \\ s_2 \end{bmatrix} \end{aligned}$$

根据前面介绍的方法设置极点  $[-5, -1 + i, -1 - i]$ , 通过 Matlab 中的函数 Place() 计算求得  $C = [c_0, c_1, c_2] = [-10 \quad -12 \quad -7]$ 。通过理论分析, 驱动系统与相应系统在输出反馈控制器的作用下达到同步, 仿真结果如图 1 所示。从图 1 可以看到, 驱动系统和响应系统的状态误差最终都趋于零。因此可以运用这两个能够达成同步的混沌系统作为保密通信发射系统和接收系统的主要部分, 来设计基于反馈同步的双通道保密通信方案。

3.4 保密通信系统的设计

这里选择信息信号  $s = \sin(0.5t) + 0.3\sin(10t)$ , 以 Chua 混沌系统为例构建发送端系统如下:

$$\dot{x} = Ax + Bf(x)$$

$$y = Cx$$

$$y_s = x_2 \cdot x_3 + (1 + x_1^2) \cdot s$$

设计混沌接收端系统如下:

$$\dot{\hat{x}} = A\hat{x} + Bf(\hat{x}) + u$$

上式中  $y$  为发送系统输出,  $u$  为驱动系统和响应系统的同步控制器。

通过相应的解调函数恢复出原信息为

$$s_d = (-\hat{x}_2 \cdot \hat{x}_3 + y) / (1 + \hat{x}_1^2)$$

通过 Matlab 仿真, 得到如下仿真结果。

仿真结果如图 2, 图 3 所示。图 2 为驱动系统与响应系统状态误差图, 可以看到经过一个暂态过程后, 系统的误差最终趋于零, 实现了同步。从图 3 中的曲线可以看到, 信息信号是通过一条独立通道传输, 而控制信号是通过另一条通道传输, 信息信号是不会影响系统特征的。在图 3(d) 可以看到, 系统经过短暂时间后原信息信号与恢复信号差即  $s - s_d \rightarrow 0$  说明信息信号得到正确传输。

4 结论

通过上述理论分析把非线性混沌系统通过系统的输出线性化, 使得非线性系统完全线性化, 从而使得同步的控制器设计变得简单, 不同于基于状态误差的控制器设计, 这种控制器也是有效的。同时, 针对这种控制同步方法的特点, 设计了混沌保密通信系统, 这种通信系统采用了双通道通信方式, 同步控制信号和信息信号分开传输, 便于系统分析, 同时采用系统的状态通过调制和掩盖来加密信息信号的方法使得信息信号得以保密传输。通过 Chua 电路的实际数值仿真实例设计了同步控制器和保密通信系统, 并且验证了系统的信息信号是可靠传输的, 通过仿真图可以看到加密效果。

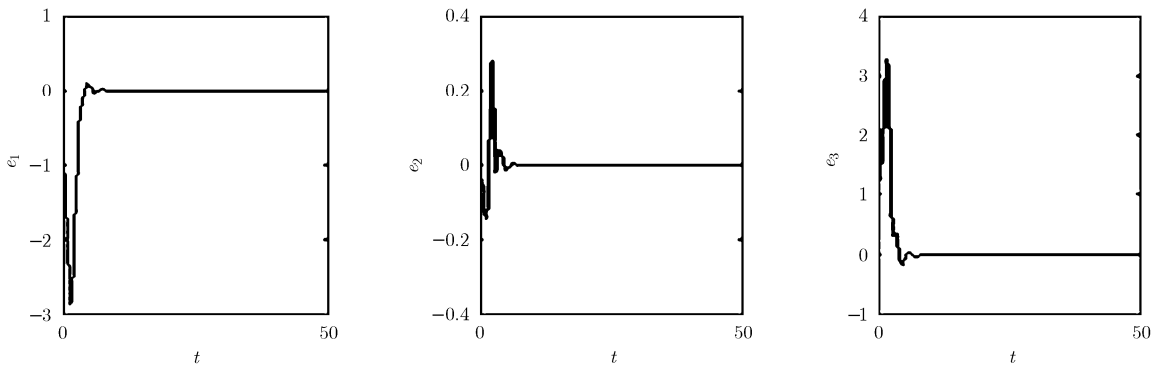


图 2 驱动系统与响应系统状态误差图

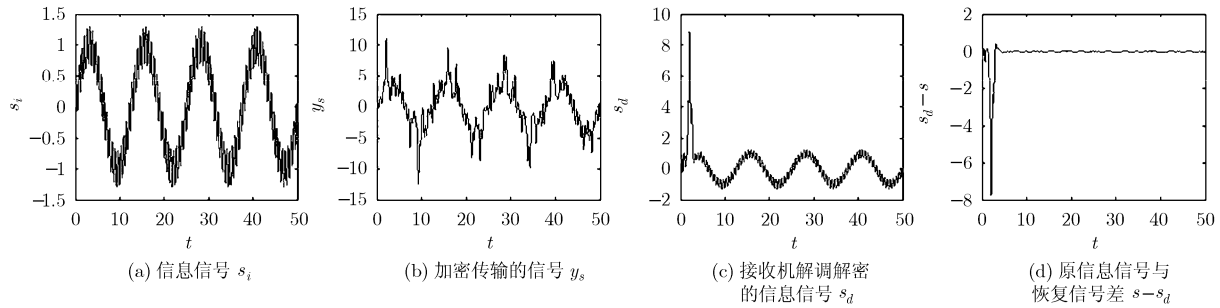


图 3 保密通信系统仿真

## 参考文献

- [1] 刘小河. 非线性系统分析与控制引论. 北京: 清华大学出版社, 2008: 38-40.
- [2] 成雁翔, 王光瑞. 用非线性反馈实现混沌的同步化. 物理学报, 1995, 44(9): 1383-1389.  
Cheng Yan-xiang and Wang Guang-rui. Synchronization of chaos by nonlinear feedback. *Acta Physica Sinica*, 1995, 44(9): 1383-1389.
- [3] Bu S L, Wang S Q, and Ye H Q. An algorithm based on variable feedback to synchronize chaotic and hyperchaotic systems. *Physica D: Nonlinear Phenomena*, 2002, 164(1-2): 45-52.
- [4] Lu J H, Zhou T S, and Zhang S C. Chaos synchronization between linearly coupled chaotic systems. *Chaos, Solitons and Fractals*, 2002, 14(4): 529-541.
- [5] 宋杨. 混沌同步化的线性反馈理论. 大连铁道学院学报, 1998, 19(4): 9-12.  
Song Yang. The theory of synchronization of chaos by linear feedback. *Journal of Dalian Railway Institute*, 1998, 19(4): 9-12.
- [6] Chen M Y and Han Z Z. Controlling and synchronizing chaotic Genesis system via nonlinear feedback control. *Chaos, Solitons and Fractals*, 2003, 17(4): 709-716.
- [7] Zhu F L. The design of full-order and reduced-order adaptive observers for nonlinear Systems. 2007 IEEE International Conference on Control and Automation. Guangzhou, China, May 30 to June 1, 2007: 529-534.
- [8] Jiang Z P. A note on chaotic secure communication systems. *IEEE Transactions on Circuits and Systems-I* 2002, 49(1): 92-96.
- [9] Amel B, Thouraya K, and Jean-Claude V. On practical observers for nonlinear uncertain systems. *Systems & Control Letters*, 2008, 57(5): 371-377.
- [10] 杨涛, 邵惠鹤. 一类混沌系统的同步方法. 物理学报, 2002, 51(4): 742-748.  
Yang Tao and Shao Hui-he. Synchronization for a class of chaotic systems. *Acta Physica Sinica*, 2002, 51(4): 742-748.
- [11] Zhou J and Meng J. Adaptive output control of a class of uncertain chaotic systems. *Systems & Control Letters*, 2007, 56(6): 452-460.
- [12] Didier L and Cesar C. Output synchronization of chaotic systems under non vanishing perturbations. *Chaos, Solitons and Fractals*, 2008, 37(4): 1172-1186.
- [13] Sun H J and Cao H J. Chaos control and synchronization of a modified chaotic system. *Chaos, Solitons and Fractals*, 2008, 37(5): 1442-1455.
- [14] 戴志诚, 汪秉文. 基于混沌同步的保密通信. 系统工程与电子技术, 2007, 29(5): 699-702.  
Dai Zhi-cheng and Wang Bing-wen. Secure communication based on chaotic synchronization. *Systems Engineering and Electronics*, 2007, 29(5): 699-702.
- [15] 赵柏山, 朱义胜. 一种改进的混沌掩盖技术. 电子与信息学报, 2007, 29(3): 699-701.  
Zhao Bai-shan and Zhu Yi-sheng. An improved secure communication system based on chaotic masking. *Journal of Electronics & Information Technology*, 2007, 29(3): 699-701.
- [16] 孙克辉, 牟俊, 周家令, 等. 统一混沌系统的混沌观测器同步控制及其应用. 控制理论与应用, 2008, 25(4): 794-798.  
Sun Ke-hui, Mo Jun, and Zhou Jia-ling, et al.. Synchronization control and its application for the unified chaotic system based on chaos observer. *Control Theory & Application*, 2008, 25(4): 794-798.

黄丽莲: 女, 1972年生, 博士, 副教授, 研究方向为复杂动态网络、混沌系统的控制与同步。

尹启天: 男, 1979年生, 硕士生, 研究方向为混沌系统的同步控制及其在保密通信中的应用。