基于 Lorenz 系统切换混沌同步的保密通讯

刘扬正[①②]　姜长生[②]　林长圣[①]　熊　新[①]　石　磊[①]
[①](南京工程学院非线性物理研究所　南京　210013)
[②](南京航空航天大学自动化学院　南京　210016)

摘　要：该文提出利用 Lorenz 系统切换混沌同步实施保密通讯的方法。构建了有一定关联的两个 Lorenz 混沌系统，并通过选择器在系统间随机切换；用同一种控制方法既能实现不同 Lorenz 系统的混沌同步，又能实现相同 Lorenz 系统的混沌同步；发送系统可以在 Lorenz 混沌系统间随机转换，传输信道中混沌调制信号也随之不断变化；接收系统将混沌调制信号解调后，即可获取有用信号。由于发送系统的可选择性，导致保密信号的多样性和随机性，因此该保密通讯方法具有更好的保密性能。

关键词：保密通讯；混沌同步；Lorenz 系统
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)11-2641-04

Chaotic Synchronization Secure Communications Based on the Lorenz Systems Switch

Liu Yang-zheng [①②]　Jiang Chang-sheng[②]　Lin Chang-sheng[①]　Xiong Xin[①]　Shi Lei[①]
[①](*Institute of Nonlinear Physics*, *Nanjing Institute of Technology*, *Nanjing* 210013, *China*)
[②](*College of Automatic Engineering*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 210016, *China*)

Abstract: A chaotic synchronization secure communication method based on several Lorenz systems switch is proposed. These Lorenz systems are built, which are relevant and can be switched each other via the choicer. Chaotic synchronization of these systems is realized using same nonlinear feedback control method. The transmitter can be switched discretionarily among several chaotic systems, bring on ceaseless changing of the chaotic carriers in transport channel. In the receiver, the chaotic carriers are retrieved from the received signals, then the information signals are recovered. The experiment result shows that this chaotic synchronization secure communications method based on several chaotic systems switch is better in security because of the transmitter can be switched and the chaotic carriers can be changed discretionarily.

Key words: Secure communication; Chaos synchronization; Lorenz system

1　引言

由于混沌信号具有内禀随机性、拟噪声、连续宽频谱分布等特点，因此，利用混沌信号进行保密通讯成为当前科学技术领域研究的热点课题之一[1−4]。为了提高保密通讯的安全性能，到目前为止，混沌同步技术大体经历了 3 个发展阶段：低维混沌系统同步[1−3]；高维超混沌系统同步[4,5]；时空混沌系统同步和阵列混沌系统同步[6,7]。基于相同混沌系统或超混沌系统同步的保密通讯，密钥是混沌系统的结构。由于要求系统参数的精确匹配以及传输信道中保密信号的单一性和重复性，利用相同混沌系统或超混沌系统同步进行保密通讯，保密性能并不是非常理想[8]。文献[6,7]提出用单向环形阵列发送有着相同耦合单元的线形阵列，环上和链上对应的振子达到同步，利用这种空间周期性混沌同步实现保密通讯，由于可以任意选取环中的混沌变量作为掩盖信号，增加了系统重构的难度，因此具有较好的保密性能。由于环上和链上的系统数目多达几十个，整个系统的物理实现难度较大。

最近，两个不同系统之间的混沌同步问题引起了人们的广泛重视[9,12]。本文提出基于不同系统切换混沌同步的保密通讯方法。首先构建有一定关联的多个不同的混沌系统，这些系统可以通过选择器随机切换；然后用统一的控制方法实现这些不同系统间的混沌同步；在发送端，将传输的有用信号与混沌信号进行调制，由于发送系统可以在多个不同的混沌系统间随机切换，使得传输信道中混沌调制信号也随机变化，在接收端，接收系统将接收到的混沌调制信号进行解调，即可获取有用信号。由于发送系统的可选择性，导致传输信道中混沌调制信号的多样性和随机性，因此，该保密通讯方法不仅具有更好的保密性能，而且通讯时不需要附加通讯协议[13]，操作简便，易于物理实现。本文以Lorenz系统为例

2006-04-27 收到，2006-10-16 改回
国家自然科学基金(90405011)，江苏省高校自然科学研究基金(05KJD120083)和南京工程学院自然科学研究基金(KXJ06047)资助课题

对该保密通讯方法的实现过程进行详细的说明。

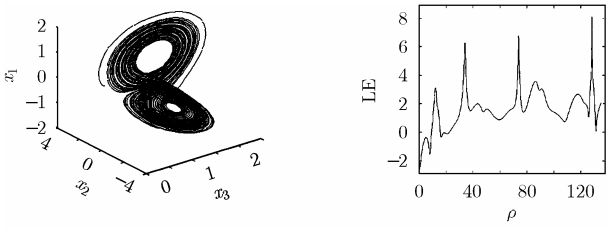
2 多系统混沌同步

经典Lorenz系统[3]是一个典型的三阶自治非线性系统，为了电路实现的方便，根据文献[3]对系统的变量进行变换，Lorenz系统方程表述为

$$\left.\begin{aligned}\dot{x}_1 &= -\sigma x_1 + \sigma x_2\\ \dot{x}_2 &= \rho x_1 - x_2 - 20x_1x_3\\ \dot{x}_3 &= -\gamma x_3 + 5f(x_1,x_2)\end{aligned}\right\} \tag{1}$$

式中系统参数 σ,ρ,γ 保持不变，非线性函数 $f(x_1,x_2)$ 可以变化。当 $f(x_1,x_2)=x_1x_2$ 时，式(1)就是传统的 Lorenz 系统; 当 $f(x_1,x_2)=x_1^2$ 时，式(1)是传统的 Lorenz 系统的一种变形，称之为变形 Lorenz 系统。二系统可用如图 4 的电路实现，图中开关 K 的切换，可以实现二系统间的转换。下面对这两种 Lorenz 系统的动力学行为进行分析比较。

二系统具有相同的平衡点 P^0 (0，0，0)，P^+ ($\sqrt{\gamma(\rho-1)}$，$\sqrt{\gamma(\rho-1)}$，$\rho-1$)和 P^- ($-\sqrt{\gamma(\rho-1)}$，$-\sqrt{\gamma(\rho-1)}$，$\rho-1$)。二系统在 P^0 处的特征值相同，而在 P^+ 和 P^- 处的特征值性质相同但大小不相等。系统参数为 $\sigma=10,\rho=28,\gamma=8/3$ 时，Lorenz 系统 Jacob 矩阵在 P^+ 和 P^- 处的特征值皆为 $\lambda_{11}=-13.8238$，$\lambda_{12,13}=0.07842\pm10.2062i$；图 1(a)表示 Lorenz 系统在系统参数为 $\sigma=10,\rho=28,\gamma=8/3$ 时的相图，图 1(b)表示 Lorenz 系统的系统参数 $\sigma=10,\gamma=8/3$ 保持不变，系统的最大 Lyapunov 指数(LE)随系统参数 ρ 变化的情况。

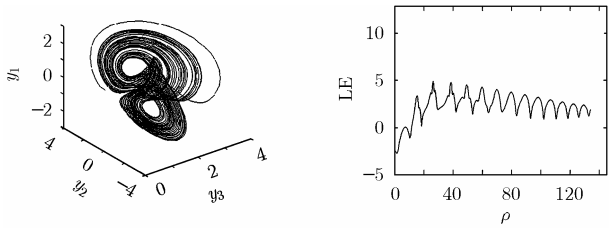


(a) Lorenz 系统的三维相图　(b) Lorenz 系统的最大 Lyapunov 指数谱

图 1

系统参数为 $\sigma=10,\rho=28,\gamma=8/3$ 时，变形 Lorenz 系统 Jacob 矩阵在 P^+ 和 P^- 处的特征值皆为 $\lambda_{21}=-16.9266$，$\lambda_{22,23}=1.6278\pm9.0798i$；图 2(a)表示变形 Lorenz 系统在系统参数为 $\sigma=10,\rho=28,\gamma=8/3$ 时的相图；图 2(b)表示变形 Lorenz 系统的系统参数 $\sigma=10,\gamma=8/3$ 保持不变，系统的最大 Lyapunov 指数(LE)随系统参数 ρ 变化的情况。

比较二系统相图和在 P^+ 和 P^- 处的特征值，说明二系统在相空间中流的演化速度存在一定差异；二系统在参数为 $\sigma=10,\rho=28,\gamma=8/3$ 时，系统的最大 Lyapunov 指数都大于零，说明 Lorenz 系统与变形 Lorenz 系统是相互关联的混沌系统。



(a) 变形Lorenz 系统的三维相图　(b) 变形Lorenz 系统的最大Lyapunov 指数谱

图 2

下面讨论利用非线性反馈控制实现 Lorenz 系统与变形 Lorenz 系统的混沌同步问题。假设式(1)为发送系统，变形 Lorenz 系统为接收系统，非线性反馈控制器 $u_i(t)(i=1,2,3)$ 作用在接收系统上，接收系统方程为

$$\left.\begin{aligned}\dot{y}_1 &= \sigma(y_2-y_1)+u_1\\ \dot{y}_2 &= \rho y_1 - y_2 - 20y_1y_3 + u_2\\ \dot{y}_3 &= 5y_1^2 - \gamma y_3 + u_3\end{aligned}\right\} \tag{2}$$

需要确定使系统式(1)和系统式(2)达到混沌同步时非线性反馈控制器 u_i 的形式。

令误差变量 $e_i=x_i-y_i(i=1,2,3)$，由式(1)，式(2)得到误差系统方程：

$$\left.\begin{aligned}\dot{e}_1 &= -\sigma e_1 + \sigma e_2 - u_1\\ \dot{e}_2 &= (\rho-20y_3)e_1 - e_2 - 20x_1e_3 - u_2\\ \dot{e}_3 &= 5(f(x_1,x_2)-x_1^2) + 10x_1e_1 - 5e_1^2 - \gamma e_3 - u_3\end{aligned}\right\} \tag{3}$$

系统式(1)，式(2)的同步问题转化为式(3)的稳定性问题，只要式(3)在原点处渐近稳定，即可达到同步的目的。取非线性反馈控制器 u_i 的形式为

$$\left.\begin{aligned}u_1 &= 0\\ u_2 &= (\rho-20y_3)e_1\\ u_3 &= 5(f(x_1,x_2)-x_1^2)+ke_3\end{aligned}\right\} \tag{4}$$

式中 k 为反馈控制增益。式(4)是一个变结构非线性反馈控制器，其结构随着非线性函数 $f(x_1,x_2)$ 的变化而改变，$f(x_1,x_2)$ 的变化通过图 4 中开关 K 的切换实现。根据线性系统的稳定性理论[3]，确定二系统达到混沌同步时反馈控制增益的阈值。将式(4)代入式(3)并写成 $\dot{\boldsymbol{x}}=\boldsymbol{A}(t)\boldsymbol{x}+\boldsymbol{O}(\boldsymbol{x},t)$ 的形式：

$$\begin{bmatrix}\dot{e}_1\\ \dot{e}_2\\ \dot{e}_3\end{bmatrix} = \begin{bmatrix}-\sigma & \sigma & 0\\ 0 & -1 & -20x_1\\ 10x_1 & 0 & -\gamma-k\end{bmatrix}\begin{bmatrix}e_1\\ e_2\\ e_3\end{bmatrix} + \begin{bmatrix}0\\ 0\\ -5e_1^2\end{bmatrix} \tag{5}$$

定理 对于相互关联的两个 Lorenz 混沌系统，在如式(4)的变结构非线性反馈控制器作用下，存在有限值 $\tilde{k}$，当反馈控制增益 $k>\tilde{k}$ 时，二系统达到混沌同步。

证明 由式(5)可知，误差变量的零点是误差系统的平衡

点。根据线性系统的稳定性理论[3]，误差系统式(5)的线性矩阵：

$$\boldsymbol{A}(t)=\begin{bmatrix}-\sigma & \sigma & 0\\ 0 & -1 & -20x_1\\ 10x_1 & 0 & -\gamma-k\end{bmatrix} \tag{6}$$

为时变矩阵，因为混沌 Lorenz 系统与变形 Lorenz 系统都是奇异吸引子，系统变量在有限的区域内变化，因此 $\boldsymbol{A}(t)$ 对所有的 t 有界。$\boldsymbol{A}(t)$ 的特征方程

$$F(\lambda)=\lambda^3+a_1\lambda^2+a_2\lambda+a_3 \tag{7}$$

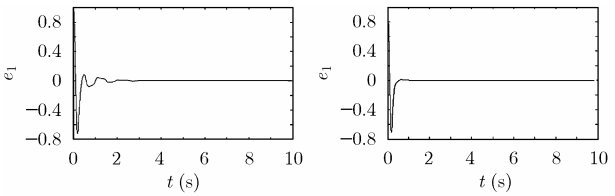
其中 $a_1=\sigma+\gamma+k+1$，$a_2=\sigma(\gamma+k+1)+\gamma+k$，$a_3=\sigma(\gamma+k)+200\sigma x_1^2$。

根据 Hurwitz 稳定性判据[3]，由式(7)解得，$k>\dfrac{-(\sigma+1)^2+\sqrt{(\sigma-1)^2(\sigma+1)+800\sigma x_1^2}}{2(\sigma+1)}-\gamma$。由于混沌 Lorenz系统是奇异吸引子，系统变量 x_1 在有限的区域内变化，因此存在有限值 $\tilde{k}$，当反馈控制增益 $k>\tilde{k}$ 时，使式(7)是稳定的多项式，矩阵 $\boldsymbol{A}(t)$ 的所有特征值都具有负实部，因此线性系统 $\dot{\boldsymbol{e}}=\boldsymbol{A}(t)\boldsymbol{e}$ 的零解一致渐近稳定。

误差系统式(5)的非线性项 $\boldsymbol{O}(\boldsymbol{e},t)=\begin{bmatrix}0 & 0 & -5e_1^2\end{bmatrix}^{\mathrm{T}}$，对所有的 t 有 $\boldsymbol{O}(\boldsymbol{0},t)=0$，且 $\lim\limits_{\|\boldsymbol{e}\|\to 0}\dfrac{\|\boldsymbol{O}(\boldsymbol{e},t)\|}{\|\boldsymbol{e}\|}=0$ 对 t 一致成立。所以误差系统式(5)在其原点处渐近稳定，在非线性反馈控制作用下系统式(1)与系统式(2)混沌同步。定理得证。

由此可见，当 $f(x_1,x_2)=x_1x_2$ 时，用式(4)所示的变结构非线性反馈控制器实现 Lorenz 系统与变形 Lorenz 系统的混沌同步；当 $f(x_1,x_2)=x_1^2$ 时，用式(4)所示的变结构非线性反馈控制器实现变形 Lorenz 系统与变形 Lorenz 系统的混沌同步。实际操作通过图 4 中开关 K 的切换实现。

数值实验时取系统初值为 $(x_1(0),x_2(0),x_3(0),y_1(0),y_2(0),y_3(0))=(1.5,1.5,1.5,0.5,0.5,0.5)$，当反馈控制增益 $k=20$ 时，驱动系统为 Lorenz 系统，响应系统为变形 Lorenz 系统，在非线性反馈控制作用下很快实现混沌同步，数值实验结果如图 3(a)所示。保持系统初值和反馈控制增益不变，驱动系统和响应系统皆为变形 Lorenz 系统时，在非线性反馈控制作用下也很快实现混沌同步，数值实验结果如图 3(b)所示。



(a) Lorenz 系统与变形 Lorenz 系统混沌同步　　(b) 变形 Lorenz 系统与变形 Lorenz 系统混沌同步

图 3

3　保密通讯实施方案

由于 Lorenz 系统和变形 Lorenz 系统存在一定的关联，两系统的系统参数相同，只是某个非线性函数不同，因此电路实现非常方便。根据式(1)设计的发送系统电路如图 4 所示。通过图中开关 K 的切换，一个电路可以实现 Lorenz 系统和变形 Lorenz 系统两个系统的功能。在电路硬件实现时，运算放大器选用 LM324，模拟乘法器选用 AD633JN，其它元件的取值如图中标示。

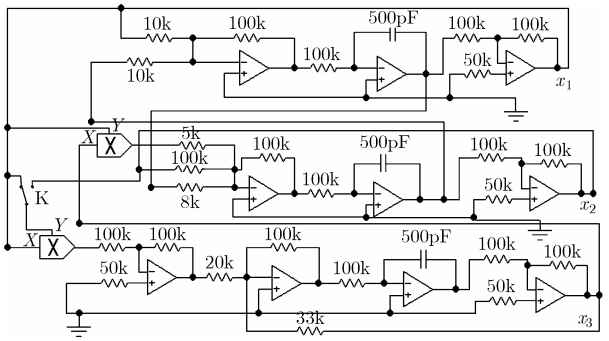


图 4　发送系统电路图

在实现了两个 Lorenz 系统混沌同步的基础上，提出利用多系统切换混沌同步实现保密通讯的策略。因为发送系统和接收系统非线性反馈混沌同步既可以在不同系统之间实现，也可以在相同系统之间实现，因此，发送系统和接收系统存在多种组合方式。如果接收系统确定，与之对应的发送系统有多种选择，例如选定变形 Lorenz 系统作为接收系统，在发送端，发送系统可以是 Lorenz 系统，也可以是变形 Lorenz 系统，只要拨动开关就可实现系统切换。在实施保密通讯时，将需要传送的信息与发送系统某个变量的信号进行调制，随机拨动开关，就使得被传送的信息有时隐藏在 Lorenz 系统的信号中，有时又隐藏在变形 Lorenz 系统的信号中。利用多系统切换混沌同步实现保密通讯的原理图如图 5 所示。

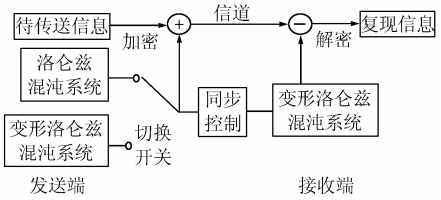
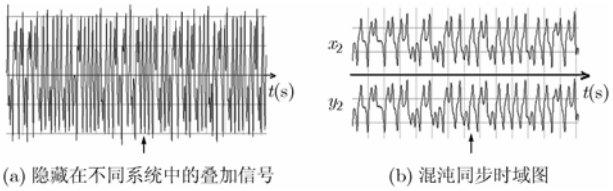


图 5 切换保密通讯原理图

图 6(a)就是将振幅为 0.2V，频率为 10kHz 的正弦波信号前半段时间调制在 Lorenz 系统的变量 x_2 中，后半段时间调制在变形 Lorenz 系统的变量 x_2 中(以图中箭头为界)。在接受端，由于接收系统与每一个发送系统都能实现混沌同步，因此，只要将接收到混合信号进行解调即可获得需要传送的信息。图 6(b)表示前半段时间发送系统为 Lorenz 系统，

后半段时间发送系统为变形 Lorenz 系统(以图中箭头为界)，接收系统皆为变形 Lorenz 系统，发送系统的变量 x_2 与接收系统的变量 y_2 实现混沌同步的时域图。



(a) 隐藏在不同系统中的叠加信号 (b) 混沌同步时域图

图 6

基于相同系统同步的混沌保密通讯技术，只有系统结构一个密钥，可以采用系统结构重构技术进行破解[8,14]。而基于多个不同系统切换混沌同步的混沌保密通讯技术，含有多个不同的系统结构和系统随机切换算法两个密钥。由于发送系统存在的多种可能的选择性，导致了信道中传输信号的多样性和随机性，这种混沌保密通讯方法无疑增加了破解的难度，破译者要面对多个不同的系统，系统重构更加困难；而且由于多个发送系统具有不同的动力学行为，奇异吸引子的流形完全不同，信道中传输信号因系统的随机切换而不断变化，因而极大地提高了混沌保密通讯的保密性能。

4 结束语

本文提出利用多个不同系统切换混沌同步实施混沌保密的方法，具有以下 3 个特点：(1)发送系统可在多个关联系统中随机转换，发送系统的选择具有灵活性。(2)信道中的保密信号具有变化的随机性和形式的多样性，提高了混沌保密通讯的保密性能。(3)实现关联系统的混沌同步，同步控制方法简单，物理实现容易。因此本文提出的多系统随机切换混沌保密方法具有很好的应用前景。

参 考 文 献

[1] Pecora L M and Carroll L T. Synchronization in chaotic systems[J]. *Phys. Rev. Lett.*, 1990, 64(8): 821–824.

[2] Carroll L T and Pecora L M. Cascading synchronized chaotic systems[J]. *Physica D*, 1993, 67(1): 126–140.

[3] 王光瑞,于熙龄，陈式刚. 混沌的控制、同步与利用[M]. 北京：国防工业出版社, 2001, 第七章.

[4] Ali M K and Fang J Q .Synchronization of chaos and hyperchaos using linear and nonlinear feedback functions[J]. *Phys. Rev.E*, 1997, 55(5): 5285–5289.

[5] Peng J H, Ding E J, Ding M and Yang W. Synchronizing hyperchaos with a sclar transmitted signal[J]. *Phys. Rev. Lett.*, 1996, 76(6): 904–907.

[6] Cuomo K M and Oppenheim A V. Circuit implementation of synchronization chaos with applications to communication[J]. *Phys. Rev. Lett.*, 1993, 71(1): 65–68.

[7] Deng X L and Huang H B. Spatial period synchronization of chaos in coupled ring and linear array of chaotic system [J]. *Phys. Rev.E*, 2002, 65(5): 055202-1-055202-3.

[8] 翁贻方, 翁莉娟, 张蕾. 提高混沌同步保密通讯安全性的设计方案研究[J].电子与信息学报，2004, 26(7): 1057–1063.
Weng Yi fang, Weng Li-juan, and Zhang Lei. Research on chaotic synchronized secure communication schemes to improve security [J]. *Journal of Electronics & Information Technology*, 2004, 26(7): 1057–1063.

[9] Park J H. Chaos synchronization between two different chaotic dynamical systems[J]. *Chaos, Solitons & Fractals*, 2006, 27(2): 549–554.

[10] Yassen M T. Chaos Synchronization between two different chaotic systems using active control[J]. *Chaos, Solitons & Fractals,* 2005, 23(1): 131–140.

[11] 刘扬正, 费树岷. Genesio-Tesi 和 Coullet 混沌系统之间的非线性反馈同步[J]. 物理学报，2005，54(8)：3486–3490.
Liu Yang-zheng and Fei Shu-min. Synchronization in the Genesio-Tesi and Coullet systems with nonlinear feedback controlling [J]. *Acta Physics Sinica*, 2005，54(8)：3486–3490.

[12] 刘扬正, 费树岷. Sprott-B 和 Sprott-C 系统之间的耦合混沌同步[J]. 物理学报, 2006, 55(3): 1035–1039.
Liu Yang-zheng, and Fei Shu-min. Chaos synchronization between the Sprott-B and Sprott-C with linear coupling [J]. *Acta Physics Sinica,* 2006, 55(3): 1035–1039.

[13] 张家树,肖先赐.基于广义混沌映射切换的混沌同步保密通讯[J]. 物理学报, 2001, 50 (11): 2121–2125.
Zhang Jia-Shu and Xiao Xian-ci. Chaos synchronization secure communications based on the extended chaotic maps switch [J]. *Acta Physics Sinica*, 2001, 50(11): 2121–2125.

[14] 谢鲲,雷敏,冯正进.一种增强混沌系统保密性能的新方法[J]. 电子与信息学报, 2004, 26(9): 1401-1406.
Xie Kun, Lei Min, and Feng Zheng-jin. A new method for improving the encryption property of the chaotic system [J]. *Journal of Electronics & Information Technology*, 2004, 26(9): 1401–1406.

刘扬正： 男，1964 年生，副教授，主要研究方向为混沌控制与同步及其应用.

姜长生： 男，1942 年生，教授，博士生导师，主要研究方向为非线性系统自适应控制.

林长圣： 男，1954 年生，教授，主要研究方向为非线性系统特性分析和计算物理.