文章编号: 1008-1542(2011)02-0157-05

耦合混沌系统的自适应同步及其在保密通信中的应用

于 茜, 罗永健

(西安通信学院研究生管理大队, 陕西西安 710106)

摘 要: 混沌系统同步是混沌保密通信的关键环节, 要想准确恢复所传输的信息, 收发双方的混沌系统必须保持同步, 在实际应用中, 系统参数会随着环境的变化而变化, 因此研究参数未知混沌系统的同步更具有实际应用价值。针对参数完全未知的单向耦合混沌系统, 实现了自适应同步, 给出了严格的数学证明, 并将同步的混沌系统应用到改进的混沌保密通信方案中。计算机仿真表明, 混沌系统能够快速达到同步, 有用信号可以有效地在接收端恢复出来。

关键词: 单向耦合; 自适应; 混沌同步; 混沌掩盖

中图分类号: TN918 文献标志码: A

Adaptive synchronization of coupled system and its application to secure communication

YU Qian, LUO Yong-jian

(Administrant Brigade of Postgraduate, Xi'an Communications Institute, Xi'an Shaanxi 710106, China)

Abstract: Chaotic systems synchronization is the key step of chaos secure communications. The chaos synchronization must be realized if one wants to get the exact transformed information. In practice, the parameters is changable along with environment. In this paper, the synchronization of two unidirectionally coupled systems is proposed based on the adaptive technique when the parameters of the master system are completely unknown and different from those of the slave system. According to the Lyapunov stability theory, the rigorous proof is given for the stability of error system. Then the approach is applied to chaos-based secure communication. Numerical simulations are included to verify the effectiveness and feasibility of the proposed theorems.

Key words: unidirectionally coupled system; adaptive; chaos synchronization; chaos-masking

自从 1990 年美国海军实验室的 PECORA 等首次在电子线路上观察到混沌同步现象[1], 混沌同步问题的研究受到广泛重视并成为近年来非线性科学中一个重要的课题和研究热点。经过近 20 年的研究, 混沌同步迅速应用到物理学、化学、生物学、电子学、信息科学和保密通信等领域, 混沌同步方法层出不穷, 如线性与非线性反馈同步法[2-3], 耦合同步法[4], 脉冲同步法[5-6], 延迟反馈同步法[7]等。大多数方法都是针对参数确定的系统进行研究, 但是在实际应用中, 系统的部分或全部参数有可能是未知的(且随着时间变化, 导致参数也发生变化使其不确定性经常发生), 因此一些学者针对参数不确定的混沌系统进行了一定的研究, 如 YASSEN 基于 Lyapunov 稳定性理论, 研究了参数完全未知的 Rössler 系统和 Lü 系统的自适应同步[8], PARK 研究了参数完全未知的超 Chen 混沌系统的自适应同步[9], 但两文都是针对具体的系统展开研究, 没有建立理论模型; ZHOU 等研究了线性和非线性双向耦合的超混沌系统的同步[10], 虽然建立了抽象模型, 但是系统参数是完全已知的, 没有研究参数完全未知的情况, 并且根据 WU 等的研究[11], 采用双向耦合容易改

收稿日期: 2010-10-11; 责任编辑: 陈书欣

作者简介: 于 茜(1986-), 女, 河北廊坊人, 硕士研究生, 主要从事保密通信方面的研究。

变发射端 Chua's 电路的混沌特性,因此需要采用单向耦合使得在同步过程中接收系统不会影响发射系统,而只是通过调节接收系统,使之与发射系统同步。

针对以上文献的不足,笔者基于 Lyapunov 稳定性理论,研究了一类基于单向耦合的参数完全未知的混沌系统的自适应同步,该方法针对完全未知参数的混沌系统模型,给出了严格的自适应同步的数学证明,并将该同步方法应用到改进的混沌掩盖保密通信方案中,实现了保密通信。

1 问题描述

混沌系统可描述如下:

$$\dot{x}(t) = f(x) + F(x)\theta, \tag{1}$$

其中:$x \in \mathbf{R}^n$ 是状态变量;$f(x): \mathbf{R}^n \to \mathbf{R}^n$ 和 $F(x): \mathbf{R}^n \to \mathbf{R}^{n\times p}$ 均为非线性函数,分别表示系统中与参数无关和有关的部分;θ 为参数变量。

以系统(1)为驱动系统,构造与系统(1)耦合的同结构的响应系统为

$$\dot{y}(t) = f(y) + F(y)\theta^* + D(x - y), \tag{2}$$

其中:$y \in \mathbf{R}^n$ 为状态变量;θ^* 是 θ 的估计值;D 为耦合系数矩阵,且有 $D = \mathrm{diag}(d_1, d_2, \cdots, d_i)$, $i = 1, 2, \cdots, n$。

定义系统的误差为 $e(t) = y(t) - x(t)$,同时,将参数看作随时间变化的状态变量,因此有参数误差系统 $e_\theta = \theta^* - \theta$,则

$$\dot{e} = f(y) + F(y)\theta^* - De - f(x) - F(x)\theta。 \tag{3}$$

假设 f 和 F 均满足局部 Lipschitz 条件,则可以得到 $\|f(y) - f(x)\| \leqslant \alpha\|y - x\| = \alpha e$,因此有 $\|f(y) - f(x)\| = L_1(x, y)e$,其中 $\|L_1(x, y)\| \leqslant \alpha$。同理可得到 $\|F(y) - F(x)\| \leqslant \beta e$ 且有 $\|F(y) - F(x)\| = L_2(x, y)e$。设 $L_1(x, y) = (a_{ij})_{n\times n}$, $L_2(x, y) = (b_{ij})_{n\times n}$, $e = [e_1, e_2, \cdots, e_j]^{\mathrm{T}}$,则有 $f_i(y) - f_i(x) = \sum_{j=1}^{n} a_{ij}e_j$, $F_i(y) - F_i(x) = \sum_{j=1}^{n} b_{ij}e_j$,记 $f_{\theta_k} = \dot{e}_{\theta_k} = \dot{\theta}_k^* - \dot{\theta}_k = \dot{\theta}_k^*$,因此可将式(3)改写为如下形式:

$$\dot{e}_i = f_i(y) - f_i(x) - d_ie_i + F_i(y)\theta_k^* - F_i(x)\theta_k = \sum_{j=1}^{n} a_{ij}e_j + \sum_{j=1}^{n} b_{ij}e_j\theta_k - d_ie_i + F_i(y)e_{\theta_k}, \tag{4}$$

其中,$i = 1, 2, \cdots, n$; $j = 1, 2, \cdots, n$; $k = 1, 2, \cdots, n$。

定 理

选择未知参数自适应控制律

$$f_{\theta_k} = -r_kF_i(y)e_i, \tag{5}$$

驱动系统(1)与响应系统(2)从不同的初始值出发可达到渐近同步,其中 r_k 为自适应增益。

证 明

定义 Lyapunov 函数为 $V = \frac{1}{2}\sum_{i=1}^{n} e_i^2 + \frac{1}{2}\sum_{k=1}^{n}\frac{1}{r_k}(\theta_k^* - \theta_k)^2$,那么对 Lyapunov 函数沿着式(4)求导得到

$$\begin{aligned}
\dot{V} = & \sum_{i=1}^{n}\dot{e}_ie_i + \sum_{k=1}^{n}\frac{1}{r_k}\dot{\theta}_k^*e_{\theta_k} = \\
& \sum_{i=1}^{n}[e_i(\sum_{j=1}^{n}a_{ij}e_j + \sum_{j=1}^{n}b_{ij}e_j\theta_k - d_ie_i + F_i(y)e_{\theta_k})] + \sum_{k=1}^{n}\frac{1}{r_k}e_{\theta_k}f_{\theta_k} = \\
& \sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij} + b_{ij}\theta_k)e_ie_j - \sum_{i=1}^{n}d_ie_i^2 + \sum_{i=1}^{n}F_i(y)e_ie_{\theta_k} + \sum_{k=1}^{n}\frac{1}{r_k}e_{\theta_k}f_{\theta_k} = \\
& \sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij} + b_{ij}\theta_k)e_ie_j - \sum_{i=1}^{n}d_ie_i^2 + e_{\theta_k}(\sum_{\substack{i=1\\k=1}}^{n}F_i(y)e_i + \frac{1}{r_k}f_{\theta_k})。
\end{aligned} \tag{6}$$

在式(6)中,令参数自适应控制律为式(5),可得到

$$\dot{V} = \sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij} + b_{ij}\theta_k)e_ie_j - \sum_{i=1}^{n}d_ie_i^2 \leqslant \sum_{i=1}^{n}\sum_{j=1}^{n}|a_{ij} + b_{ij}\theta_k| \cdot |e_ie_j| - \sum_{i=1}^{n}d_ie_i^2。 \tag{7}$$

可以把式(7)转换成二次型的形式,即 $\dot{V} \leqslant -e^{\mathrm{T}}\boldsymbol{P}e$,其中 $e = [e_1, e_2, \cdots, e_i]^{\mathrm{T}}$, $\boldsymbol{P}$ 是对称矩阵。显然,$e = 0$ 为系统(7)的平衡状态,为了保证系统在平衡状态时一致渐近稳定,需使 $e \neq 0$ 时,$\dot{V}$ 负定,那么矩阵 $\boldsymbol{P}$ 应正定。

2　超 Lorenz 混沌系统的自适应同步

2.1　理论分析

对于 5 阶超 Lorenz 混沌系统, 其系统方程为[12]

$$\begin{cases} \dot{x}_1 = \theta_1(x_2 - x_1) + x_4 + x_5, \\ \dot{x}_2 = \theta_2 x_1 - x_2 - x_1 x_3 + x_5, \\ \dot{x}_3 = x_1 x_2 - \theta_3 x_3 + x_5, \\ \dot{x}_4 = -x_2 x_3 + \theta_4 x_4, \\ \dot{x}_5 = -\theta_5 x_1。 \end{cases} \tag{8}$$

当 $\theta_1 = 10$, $\theta_2 = 8/3$, $\theta_3 = 28$, $\theta_4 = -6$, $\theta_5 = 3$ 时, 系统(8) 产生超混沌行为。

以系统(8) 为驱动系统, 构造与其耦合的响应系统为

$$\begin{cases} \dot{y}_1 = \theta_1^*(y_2 - y_1) + y_4 + y_5 + d_1(x_1 - y_1), \\ \dot{y}_2 = \theta_2^* y_1 - y_2 - y_1 y_3 + y_5 + d_2(x_2 - y_2), \\ \dot{y}_3 = y_1 y_2 - \theta_3^* y_3 + y_5 + d_3(x_3 - y_3), \\ \dot{y}_4 = -y_2 y_3 + \theta_4^* y_4 + d_4(x_4 - y_4), \\ \dot{y}_5 = -\theta_5^* y_1 + d_5(x_5 - y_5), \end{cases} \tag{9}$$

式中, 参数 θ_1^*, θ_2^*, θ_3^*, θ_4^*, θ_5^* 需要估计, 耦合系数 d_1, d_2, d_3, d_4, d_5 未知。

根据式(1) —式(7) 的描述与推导, 可得到

1) 未知参数自适应控制律为

$$f_{\theta_1} = -\gamma_1 e_1(y_2 - y_1),\ f_{\theta_2} = -\gamma_2 y_1 e_2,\ f_{\theta_3} = \gamma_3 y_3 e_3,\ f_{\theta_4} = -\gamma_4 y_4 e_4,\ f_{\theta_5} = \gamma_5 y_5 e_5。 \tag{10}$$

2) 令 $M_3 > |y_3|$, $M_{22} > |y_2|$, $M_{21} > |x_2|$, 有

$$\boldsymbol{P} = \begin{bmatrix} d_1 + \theta_1 & -\frac{1}{2}(\theta_1 + \theta_2 + M_3) & -\frac{1}{2}M_{22} & -\frac{1}{2} & -\frac{1}{2}|1 - \theta_5| \\ -\frac{1}{2}(\theta_1 + \theta_2 + M_3) & d_2 + 1 & 0 & -\frac{1}{2}M_3 & -\frac{1}{2} \\ -\frac{1}{2}M_{22} & 0 & d_3 + \theta_3 & -\frac{1}{2}M_{21} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2}M_3 & -\frac{1}{2}M_{21} & d_4 - \theta_4 & 0 \\ -\frac{1}{2}|1 - \theta_5| & -\frac{1}{2} & -\frac{1}{2} & 0 & d_5 \end{bmatrix}。 \tag{11}$$

根据霍尔维茨定理, 可得到矩阵 $\boldsymbol{P}$ 的各阶主子式均大于 0, 可使得矩阵 $\boldsymbol{P}$ 正定, 从而可以求得耦合系数矩阵 D 的值。

2.2　数值仿真

采用 Matlab 7.1 中的龙格-库塔算法来求解微分方程系统(8) 和系统(9), 设定迭代步长为 0.001 s, 响应系统中需要估计的参数 θ_1^*, θ_2^*, θ_3^*, θ_4^*, θ_5^* 的初始值均取为 0。系统(8) 和系统(9) 的初始状态分别设置为 $x_1(0) = 1$, $x_2(0) = 2$, $x_3(0) = 3$, $x_4(0) = 2$, $x_5(0) = 1$, $y_1(0) = 9$, $y_2(0) = 6$, $y_3(0) = 3$, $y_4(0) = 6$, $y_5(0) = 9$, 选取 $M_3 = 60$, $M_{22} = 40$, $M_{21} = 40$, 则耦合系数取 $d_1 = 137$, $d_2 = 160$, $d_3 = 10$, $d_4 = 50$, $d_5 = 2$, 选择自适应增益 $\gamma_1 = \gamma_2 = \gamma_5 = 1$, $\gamma_3 = 2$, $\gamma_4 = 3$。图 1 显示了误差动力学系统随时间 t 的变化。图 2 显示了未知参数 θ_1^*, θ_2^*, θ_3^*, θ_4^*, θ_5^* 随时间更新的过程。

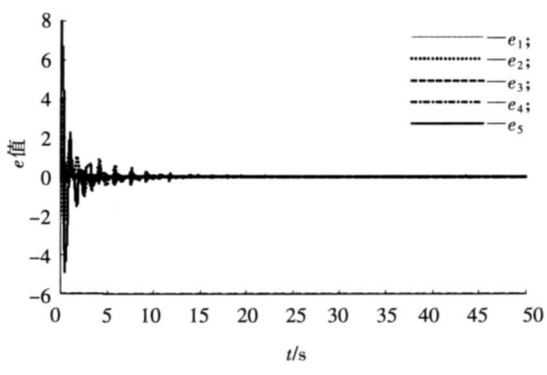


图 1　同步误差动力学系统随时间变化曲线

Fig. 1　Dynamics of error system changing with time

由图 1 可看出, 在自适应控制律式(10) 的作用下, 完

全未知参数的超 Lorenz 系统很快能实现同步, 且渐近稳定; 由计算可知, 仿真 10 s 后同步误差小于 0.01, 仿真 20 s 后同步误差小于 0.001。同时, 如图 2 所示, 未知参数在 25 s 内均可以较准确地估计出来, 并且逐渐接近已知的参数值, 在仿真 25 s 后估计误差小于0.1, 仿真35 s 后估计误差小于0.01, 仿真 50 s 后估计误差小于 0.001。

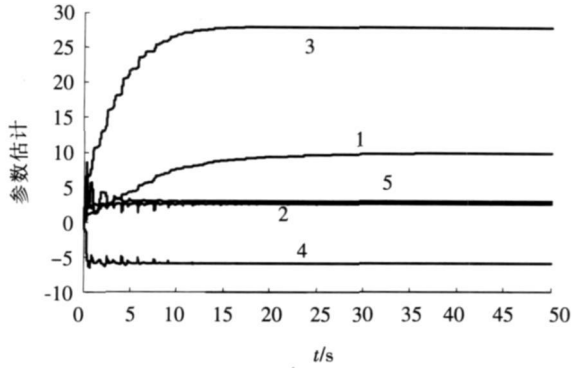


图 2 未知参数估计曲线

Fig. 2 Unknown parameters estimation

3 自适应同步法在保密通信中的应用

3.1 保密通信方案

混沌掩盖是最早研究的混沌保密通信方案, 它利用了 Pecora-Carrol 的自同步定理。基本原理是以具有逼近于高斯白噪声统计特性的混沌信号为载体来掩藏信息, 在接收端利用同步后的混沌信号去掩盖, 从而恢复出有用信息。为保证同步, 该方案要求信息信号的功率远小于混沌信号, 因此 LI Jian-fan, 李农等提出了改进方案[13-14], 其关键是: 注入到发送端系统的信号是信息信号与该信号的自适应控制器的误差, 因此当信息信号的幅值较大时, 在接收端采用自适应控制器维持收发系统的混沌同步。

下面基于改进的混沌保密通信方案, 采用笔者所提的同步方法, 利用超 Lorenz 混沌系统为所要传输的信息信号 $m(t)$ 加密, 则保密通信方案为

$$\text{发射系统:}\begin{cases}\dot{x}_1=\theta_1(x_2-x_1)+x_4+x_5+k(m(t)-w_1),\\ \dot{x}_2=\theta_2x_1-x_2-x_1x_3+x_5,\\ \dot{x}_3=x_1x_2-\theta_3x_3+x_5,\\ \dot{x}_4=-x_2x_3+\theta_4x_4,\\ \dot{x}_5=-\theta_5x_1,\\ \dot{w}_1=\mu(m(t)-w_1),\end{cases}\qquad \text{发射信号: } s(t)=x_1+m(t)。 \tag{12}$$

$$\text{接收系统:}\begin{cases}\dot{y}_1=\theta_1^*(y_2-y_1)+y_4+y_5+d_1(s-w_2-y_1),\\ \dot{y}_2=\theta_2^*y_1-y_2-y_1y_3+y_5+d_2(x_2-y_2),\\ \dot{y}_3=y_1y_2-\theta_3^*y_3+y_5+d_3(x_3-y_3),\\ \dot{y}_4=-y_2y_3+\theta_4^*y_4+d_4(x_4-y_4),\\ \dot{y}_5=-\theta_5^*y_1+d_5(x_5-y_5),\\ \dot{w}_2=\mu(s-y_1-w_2),\end{cases}\qquad \text{恢复信号: } m'(t)=s-y_1。 \tag{13}$$

其中: μ 是用于控制速度的增益常数; k 是反馈控制常数; w_1 和 w_2 分别为发射端与接收端信息信号的自适应控制器, 由式(12)和式(13)可知误差系统与信息信号无关, 因此该方法对信息信号 $m(t)$ 的幅值大小没有限制, 实用性较强, 安全性较高。

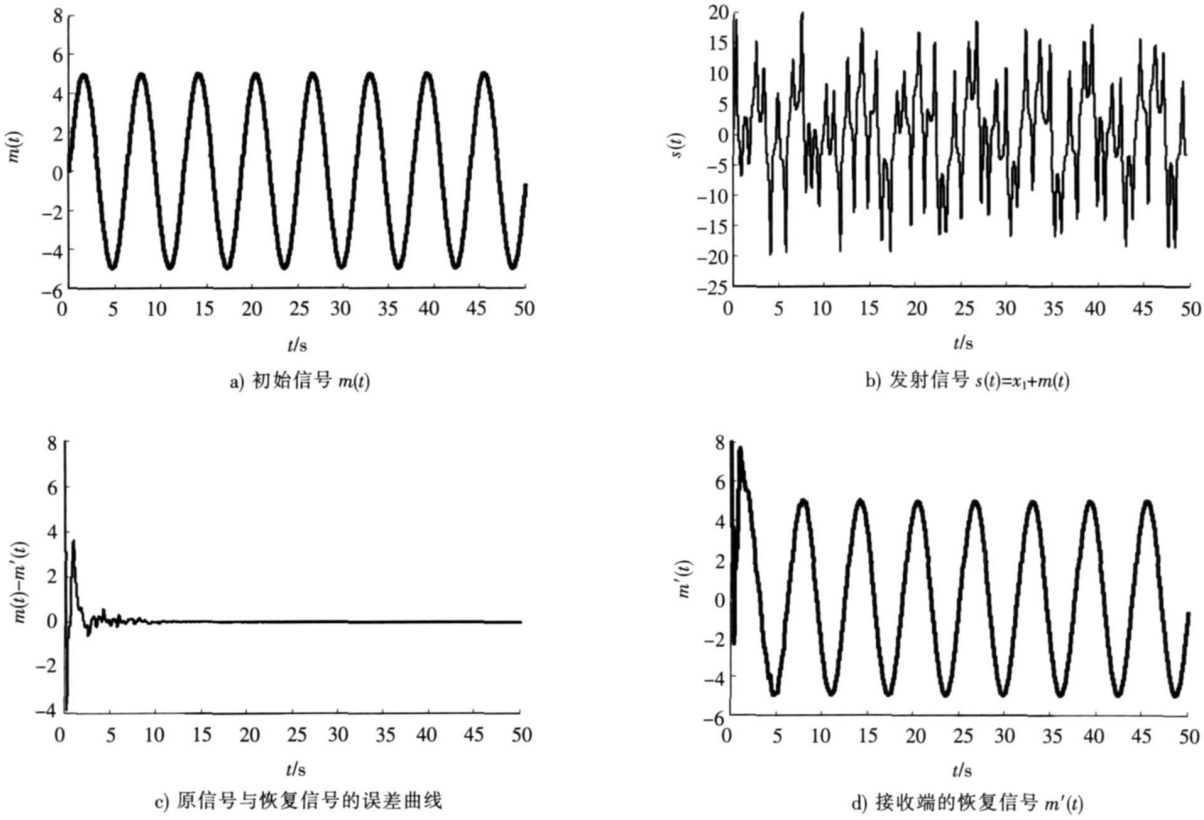
3.2 计算机仿真

假设信息信号 $m(t)=5\sin t$, 增益常数 $\mu=137$, 反馈控制常数 $k=137$, 采用改进的混沌掩盖保密通信方案后, 仿真结果如图 3 所示。

从图 3 中结果来看, 在驱动系统与响应系统同步的前提下, 信息信号可以较为准确地恢复出来。

4 结 语

超混沌系统同步的应用潜力很大, 已成为国内外混沌应用研究的一个热点。笔者针对参数完全未知的混沌系统, 构造了其单向耦合系统, 应用 Lyapunov 稳定性理论给出了严格的数学证明, 实现了超混沌系统的自适应同步, 然后将同步的混沌系统应用到一种改进的混沌掩盖保密通信方案中。计算机仿真表明混沌系统能够快速达到同步, 且经过一段暂态过程, 信息信号可以较为准确地恢复出来。



a) 初始信号 $m(t)$　　b) 发射信号 $s(t)=x_1+m(t)$

c) 原信号与恢复信号的误差曲线　　d) 接收端的恢复信号 $m'(t)$

图 3　混沌掩盖通信仿真

Fig. 3　Chaotic masking communications simulation

参考文献:

[1] PECORA L M, CARROLL T L. The synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(4): 821-830.

[2] 单　梁, 刘光杰, 李　军, 等. Liu 混沌系统的线性反馈和状态观测器同步[J]. 系统仿真学报(Journal of System Simulation), 2007, 19(6): 1 335-1 338.

[3] CHEN Mao-yin, HAN Zheng-zhi. Controlling and synchronizing chaotic Genesio system via nonlinear feedback control[J]. Chaos, Solitons & Fractals, 2003, 17(4): 709-716.

[4] GE Zheng-ming, TSEN Pu-chien. Chaos synchronization by variable strength linear coupling and Lyapunov function derivative in series form[J]. Nonlinear Analysis, 2008, 69(12): 4 604-4 613.

[5] 马铁东, 张化光. 一类参数不确定统一混沌系统的脉冲同步[J]. 系统仿真学报(Journal of System Simulation), 2008, 20(18): 4 923-4 926.

[6] HAERI M, DEHGHANI M. Robust stability of impulsive synchronization in hyperchaotic systems[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(3): 880-891.

[7] 赖宏慧, 张小红. Lorenz 系统族的自时滞混沌同步研究[J]. 计算机应用与软件(Computer Applications and Software), 2009, 26(8): 38-40.

[8] YASSEN M T. Adaptive synchronization of Rossler and Lü systems with fully uncertain parameters[J]. Chaos, Solitons & Fractals, 2005, 23(5): 1 527-1 536.

[9] PARK J H. Adaptive synchronization of hyperchaotic Chen system with uncertain parameters[J]. Chaos, Solitons & Fractals, 2005, 26(3): 959-964.

[10] ZHOU Jin, LU Jun-an, WU Xiao-qun. Linearly and nonlinearly bidirectionally coupled synchronization of hyperchaotic systems[J]. Chaos, Solitons & Fractals, 2007, 31(1): 230-235.

[11] WU C W, CHUA L O. Synchronization in an array of linearly coupled dynamical systems[J]. IEEE Transactions on Circuits and Systems-Ⅰ: Fundamental Theory and Applications, 1995, 42(8): 430-447.

[12] 李华青, 罗小华, 代祥光. 一个超混沌系统及其投影同步[J]. 电子学报(Acta Electronica Sinica), 2007, 37(3): 654-657.

[13] LI Jian-fen, LI Nong. A secure communication method for a high-power information signal based on chaotic masking[J]. Chinese Physics, 2002, 11(11): 1 124-1 127.

[14] 李　农, 李建芬, 张智军. 一种改进的混沌掩盖通信方法[J]. 系统工程与电子技术(Systems Engineering and Electronics), 2004, 2(5): 583-585.

[15] 侯沿滨, 向廷元. 时滞超混沌系统的同步[J]. 河北工业科技(Hebei Journol of Industrial Science & Technology), 2002, 19(2): 4-7.