

基于单驱动变量的混沌广义投影同步及在保密通信中的应用

李 农^{1)†} 李建芬²⁾

1) 空军工程大学工程学院, 西安 710038)

2) 空军工程大学理学院, 西安 710051)

(2008 年 2 月 1 日收到, 2008 年 3 月 20 日收到修改稿)

基于单向耦合提出一种只需传递一个驱动变量实现混沌系统广义投影同步方法. 通过改变广义投影同步的比例因子, 获得任意比例于原驱动混沌系统输出的混沌信号. 由于只需传递一个信号, 比起已有的方法具有更高的实用价值. 理论推导和数值仿真进一步表明了该方法的有效性. 最后, 基于统一混沌系统的广义投影同步, 给出了一种安全性更好的混沌保密通信方案.

关键词: 混沌系统, 单驱动变量, 广义投影同步, 统一混沌系统

PACC: 0545

1. 引 言

自 Pecora 和 Carroll 于 20 世纪 90 年代初首先提出用 PC 方法^[1]实现混沌系统同步后, 混沌同步已经引起了学者们的广泛兴趣. 十多年来, 混沌研究是非线性科学领域的热点问题之一, 而混沌的同步由于其物理、通信、信息科学、医学、生物工程等领域的巨大应用潜力和发展前途, 已经引起广泛关注, 并且取得了大量的研究成果. 针对混沌系统的同步现象研究可以分为以下几个方面: 混沌系统完全同步^[1] (CS), 混沌系统相同步^[2] (PS), 混沌系统延迟同步^[3] (LS), 混沌系统广义同步^[4-8] (GS), 混沌系统投影同步^[9, 10]等. 完全同步是指从不同初始点出发的两个混沌系统, 随着时间的推移其轨道趋于一致. 相同步是指两个混沌系统轨道的相位差锁定在 2π 以内, 而它们的振幅仍然保持混沌状态且互不相关. 延迟同步是指具有固定时间延迟的两个混沌系统轨道是一致的. 广义同步是指在主从混沌系统的轨道之间建立一个函数关系. 投影同步是指主从混沌系统的轨道的振幅成正比, 且相位相同.

最近, 人们又提出一种被称为“广义投影同步”的方法^[11-15], 该方法将投影同步和广义同步联系起来. 通过改变投影同步的比例因子, 使得响应信号任意比例于原驱动混沌系统输出的混沌信号. 当比例因子分别取大于零和小于零时, 可获得同相位和反相位的广义投影同步. 显然, 混沌系统的完全同步和反同步都可视为广义投影同步的特例. 但是, 现有这些广义投影同步方法都需要向响应系统传递多个甚至全部驱动变量, 其实用性较低. 同时, 大部分方法通常只针对某一具体的混沌系统使得适用范围较窄.

本文针对一类混沌系统, 提出一种只需向响应系统传递一个驱动变量既可实现混沌系统全部变量的广义投影同步的方法, 且同步控制器的设计具有一定的规律性. 只要能通过一个线性耦合项实现完全同步的混沌系统均可采用该方法, 与现有方法相比实用性强、适用范围宽. 利用线性系统的稳定性理论给出了相应的证明. 数值仿真进一步表明了该方法的有效性. 最后, 基于统一混沌系统的广义投影同步, 提出了一种具有更好保密性能的混沌保密通信方案.

† E-mail: ln2807@163.com

2. 单向耦合同步方案描述

考虑具有如下形式的一类非线性系统:

$$\dot{x} = Ax + f(x), \quad (1)$$

这里 $x \in R^n$ 是 n 维状态向量, $A \in R^{n \times n}$ 是常系数矩阵, $f(x) \in R^n$ 是系统的非线性部分, 为连续光滑函数.

将系统 (1) 作为驱动系统, 响应系统为

$$\dot{y} = Ay + f(y) + u, \quad (2)$$

这里 $u = (u_1, u_2, \dots, u_n)$ 为同步控制器.

任取初始值, 若使

$$\lim_{t \rightarrow \infty} \|x - y\| = 0 \quad (3)$$

成立, 则称系统 (1) 和 (2) 获得完全同步.

定义系统 (1) 和 (2) 的同步误差为 $e_w = x - y$, 则误差系统为

$$\begin{aligned} \dot{e}_w &= \dot{x} - \dot{y} \\ &= Ax - Ay + f(x) - f(y) - Ke_w, \quad (4) \end{aligned}$$

由中值定理, 得: $f(x) - f(y) = D(\xi)e_w$, $D(\xi)$ 为 f 的雅克比矩阵.

在 (4) 式中, 矩阵 $K = \text{diag}(k_1, k_2, \dots, k_n)$ 为反馈增益矩阵, $k_i > 0$. 因此有

$$\dot{e}_w = (A + D(\xi) - K)e_w = A_f(t)e_w, \quad (5)$$

方程 (5) 是一个时变的齐次线性方程组, 选择适当的 K 若使 $A_f(t)$ 的特征值均具有负实部, 则可使 $\lim_{t \rightarrow \infty} \|e_w(t)\| \rightarrow 0$ 成立, 即系统 (1) 和 (2) 获得完全同步. 实际上, 大部分的混沌系统仅通过一个耦合项即可获得完全同步, 即选择 $K = \text{diag}(0, \dots, k_i, \dots, 0)$, 如著名的 Chua's 电路, Lorenz 系统, Rössler 系统等等.

3. 广义投影同步

对于驱动系统 (1) 和响应系统 (2), 任取初始值, 若使

$$\lim_{t \rightarrow \infty} \|x - \alpha y\| = 0 \quad (6)$$

成立, 则称系统 (1) 和 (2) 获得广义投影同步. α 称为比例因子, 其中 $\alpha = 1$ 为混沌系统完全同步, $\alpha = -1$ 为混沌系统反相位同步, 都是混沌广义投影同步的特殊情况.

定义系统 (1) 与 (2) 的同步误差为 $e = x - \alpha y$, 则误差系统为

$$\begin{aligned} \dot{e} &= \dot{x} - \alpha \dot{y} \\ &= Ax - \alpha Ay + f(x) - \alpha f(y) - \alpha u \\ &= Ae + f(x) - f(\alpha y) + f(\alpha y) - \alpha f(y) - \alpha u \\ &= Ae + D(\xi)e + f(\alpha y) - \alpha f(y) - \alpha u. \quad (7) \end{aligned}$$

设计同步控制器为 $\alpha u = f(\alpha y) - \alpha f(y) + Ke$, 即

$$u = \frac{1}{\alpha} [f(\alpha y) - \alpha f(y) + Ke], \quad (8)$$

(8) 式中, 矩阵 $K = \text{diag}(0, \dots, 0, k_i, 0, \dots, 0)$ 为反馈增益矩阵, $k_i > 0$. 因此有

$$\dot{e} = (A + D(\xi) - K)e = A_f(t)e, \quad (9)$$

方程 (9) 与单向耦合完全同步的误差系统 (5) 具有相同的形式, 当 $\alpha = 1$ 时即为混沌系统完全同步, 选择适当的 k_i 值, 若使 $A_f(t)$ 的特征值均具有负实部, 则可使 $\lim_{t \rightarrow \infty} \|e(t)\| \rightarrow 0$ 成立, 即系统 (1) 和 (2) 获得广义投影同步. 因此, 只要可以通过单向耦合达到完全同步的系统均可采用控制器 (8) 式, 使系统达到广义投影同步.

另外, 由 (8) 式可见, 同步控制器只需驱动系统的一个状态变量, 仅仅在第 i 个控制器中输入驱动系统的一个变量 x_i , 即

$$u_i = \frac{1}{\alpha} [f_i(\alpha y) - \alpha f_i(y) + k(x_i - \alpha y_i)],$$

其他控制器的表达式只与响应系统的变量有关, 即

$u_j = \frac{1}{\alpha} [f_j(\alpha y) - \alpha f_j(y)]$ ($j \neq i$). 所以, 本文提出的方法只需向响应系统传递一个驱动变量 x_i .

下面以统一系统为例说明本文提出的方案. 统一系统是 2002 年, 吕金虎、陈关荣等人^[16, 17]提出的一个新的混沌系统, 这一系统连接 Lorenz 系统^[18]和 Chen 系统^[19], 统一系统的数学模型为

$$\begin{aligned} \dot{x}_1 &= -(25a + 10)x_1 - x_2, \\ \dot{x}_2 &= (28 - 35a)x_1 + (29a - 1)x_2 - x_1x_3, \\ \dot{x}_3 &= x_1x_2 - [(a + 8)3]x_3, \quad (10) \end{aligned}$$

其中 $a \in [0, 1]$ 为系统参数, 系统均为混沌态, 当 $a \in [0, 0.8]$ 时, 系统属于广义 Lorenz 系统, $a \in [0.8, 1]$ 时, 属于广义 Chen 系统, $a = 0.8$ 属于广义 Lü 系统^[20].

将系统 (10) 作为驱动系统, 响应系统为

$$\begin{aligned} \dot{y}_1 &= -(25a + 10)y_1 - y_2 + u_1, \\ \dot{y}_2 &= (28 - 35a)y_1 + (29a - 1)y_2 - y_1y_3 + u_2, \\ \dot{y}_3 &= y_1y_2 - [(a + 8)3]y_3 + u_3. \quad (11) \end{aligned}$$

由 (11) 式, 有

$$A = \begin{bmatrix} -(25a + 10) & (25a + 10) & 0 \\ (28 - 35a) & (29a - 1) & 0 \\ 0 & 0 & -(a + 8)3 \end{bmatrix},$$

$$f(y) = \begin{bmatrix} 0 \\ -y_1 y_3 \\ y_1 y_2 \end{bmatrix}.$$

选择控制器为

$$u_1 = 0,$$

$$u_2 = \frac{1}{\alpha} [f_2(\alpha y) - \alpha f_2(y) + k(x_2 - \alpha y_2)]$$

$$= -(\alpha - 1)y_1 y_3 + \frac{1}{\alpha} k e_2,$$

$$u_3 = (\alpha - 1)y_1 y_2.$$

1) 选择系统参数 $a = 0$, 此时系统(10)为 Lorenz 系统, 驱动系统(1)与响应系统(2)的初始点分别选取为 $x(0) = [-0.01 \ 0.3 \ 0.1]$, $y(0) = [0 \ 0 \ 0]$, 反馈系数 $k = 10$, 比例因子 $\alpha = -0.5$, 模拟结果见图 1 和图 2.

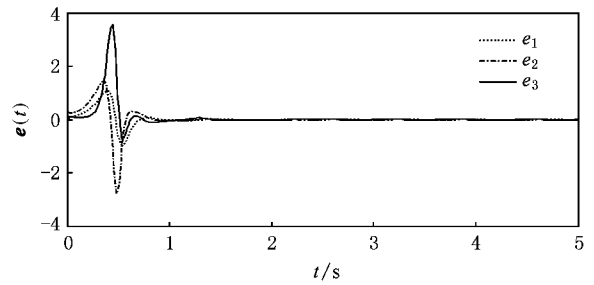


图 1 比例因子 $\alpha = -0.5$, 系统参数 $a = 0$ 时, 系统(10)和(11)的同步误差曲线 e_1, e_2, e_3

2) 选择系统参数 $a = 1$, 系统(10)属于 Chen 系统, 驱动系统(1)与响应系统(2)的初始点分别选取为 $x(0) = [-0.01 \ 0.3 \ 0.1]$, $y(0) = [0 \ 0 \ 0]$, 反馈系数 $k = 10$, 比例因子 $\alpha = 3$. 模拟结果见图 3 和图 4.

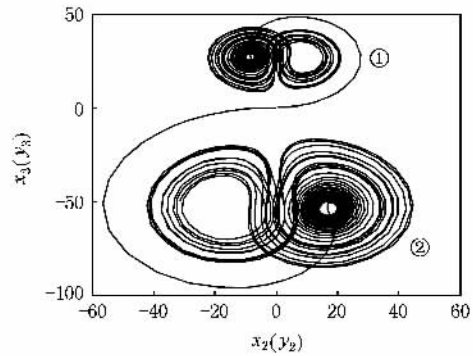
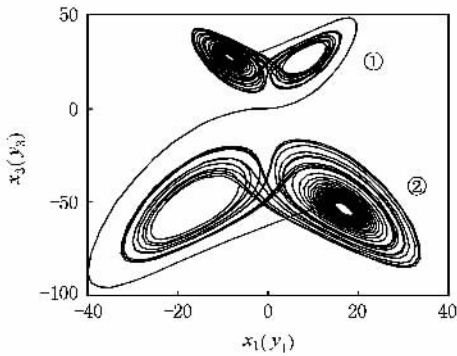


图 2 比例因子 $\alpha = -0.5$, 系统参数 $a = 0$ 时, 系统(10)和(11)二维平面上反相位广义投影

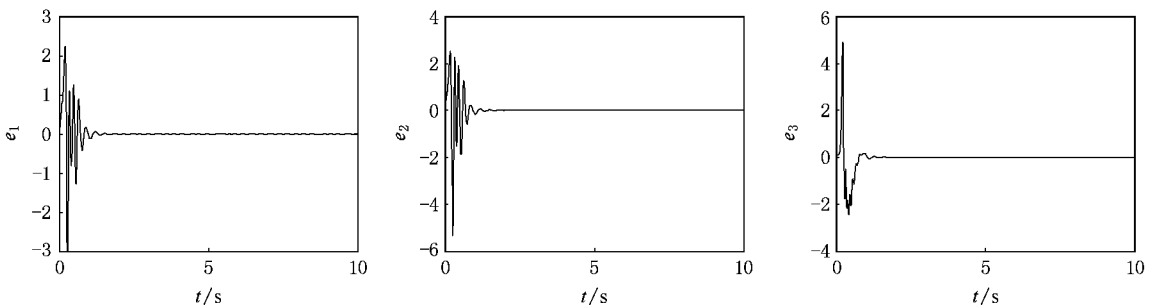


图 3 比例因子 $\alpha = 3$, 系统参数 $a = 1$ 时, 系统(10)和(11)的同步误差曲线 e_1, e_2, e_3

图 1 和图 3 分别展示了比例因子分别为 -0.5 和 3 , 系统参数 $a = 0$ 和 1 时, 误差信号 e_1, e_2, e_3 随着时间的变化快速趋于零的情况, 说明了两个相同混沌系统按照比例因子的渐近达到广义投影同步;

图 2 和图 4 展示了混沌吸引子在平面上的投影同步, 其中图 2 中①号相图是驱动系统的混沌吸引子, ②号为响应系统的混沌吸引子, 二者呈现反相位投影同步. 图 4(a)与(b)分别为 $\alpha = 3, a = 1$ 时, 驱动系

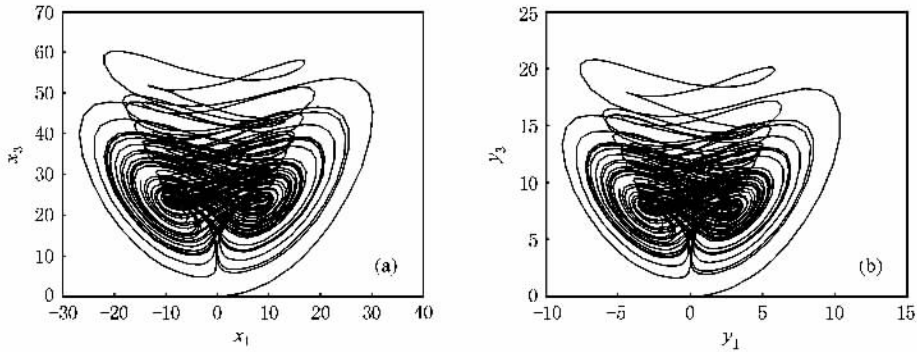


图 4 比例因子 $\alpha=3$, 系统参数 $a=1$ 时, 系统(10)和(11)二维平面上同相位广义投影同步

统和响应系统的混沌吸引子, 此时, 二者呈现同相位投影同步。

4. 在保密通信中的应用

文献[21]提出了一种统一系统的投影同步方案并基于传统的自适应通信方法将其应用到了保密通信, 该文构造的通信系统的数学模型为

发射系统:

$$\begin{aligned} \dot{x} &= -(25\theta + 10)(x - y) + m(t), \\ \dot{y} &= (28 - 35\theta)x + (29\theta - 1)y - xz, \\ \dot{z} &= xy - \frac{\theta + 8}{3}z. \end{aligned} \quad (12)$$

接收系统:

$$\begin{aligned} \dot{x}_1 &= -(25\theta + 10)(x_1 - y_1) \\ &\quad + p(t) - k_1(x_1 - \alpha x), \\ \dot{y}_1 &= (28 - 35\theta)x_1 + (29\theta - 1)y_1 \\ &\quad - x_1z + k_2(y_1 - \alpha y), \\ \dot{p} &= q(x_1 - \alpha x), \\ k_1 &= (x_1 - \alpha x)^2, \\ k_2 &= (y_1 - \alpha y)^2, \end{aligned} \quad (13)$$

(13) 式中 q 为正的常数. 理论推导表明^[61], 只有当 $\alpha(dm/dt) \approx 0$ 时上述系统才可以达到投影同步, 此时可通过 $\lim_{t \rightarrow \infty} p(t) \rightarrow m(t)$ 恢复出原信息信号. 因此该方法要求信息信号 $m(t)$ 的频率必须远低于混沌系统的振荡频率且比例因子 α 不能太大. 同时, 从(12)式中可见, 信息信号 $m(t)$ 是直接注入到驱动系统, 所以其幅度不能太大, 否则系统将失去混沌态. 从(13)式中可见, 该方法需向接收系统传递驱动系统的全部变量, 因而实用性较低、安全性不高.

为了解决上述问题, 利用本文提出的混沌广义

投影同步方法, 仍然以统一系统为例, 基于文献[22]提出的混沌保密通信方法构造如下的通信系统:

发射系统:

$$\begin{aligned} \dot{x}_1 &= -(25a + 10)(x_1 - x_2), \\ \dot{x}_2 &= (28 - 35a)x_1 + (29a - 1)x_2 \\ &\quad - x_1x_3 + k(m(t) - w_1), \\ \dot{x}_3 &= x_1x_2 - [(a + 8)/3]x_3, \\ \dot{w} &= \mu(m(t) - w). \end{aligned} \quad (14)$$

发射信号: $s(t) = x_2 + m(t)$.

接收系统:

$$\begin{aligned} \dot{y}_1 &= -(25a + 10)(y_1 - y_2) + u_1, \\ \dot{y}_2 &= (28 - 35a)y_1 + (29a - 1)y_2 - y_1y_3 + u_2, \\ \dot{y}_3 &= y_1y_2 - [(a + 8)/3]y_3 + u_3. \end{aligned} \quad (15)$$

选择控制器为

$$\begin{aligned} u_1 &= 0, \\ u_2 &= -(\alpha - 1)y_1y_3 + \frac{1}{\alpha}k(s - \alpha y_2 - w_2), \\ u_3 &= (\alpha - 1)y_1y_2, \\ w'_2 &= \mu(s - \alpha y_2 - w_2), \end{aligned}$$

其中 μ 是一个用于控制速度的增益常数, w_1 和 w_2 分别为收发两端连接的自适应控制器, 它们的引入, 可提高被传送的信息信号的幅值, 因该方法是将信号 $m(t)$ 与跟踪该信号的自适应控制器 w_1 的误差注入到发射系统, 而不是直接将信号 $m(t)$ 注入, 因此当 $m(t)$ 的幅值较大时, 系统可以依然保持混沌态. 由(14)和(15)式可推出误差系统与信息信号无关, 因此该方法对信息信号 $m(t)$ 的频率和比例因子 α 的大小没有限制. 特别是该方案只需向接收系统传递一路信号 $s(t) = x_2 + m(t)$, 实用性较强、安全性较高.

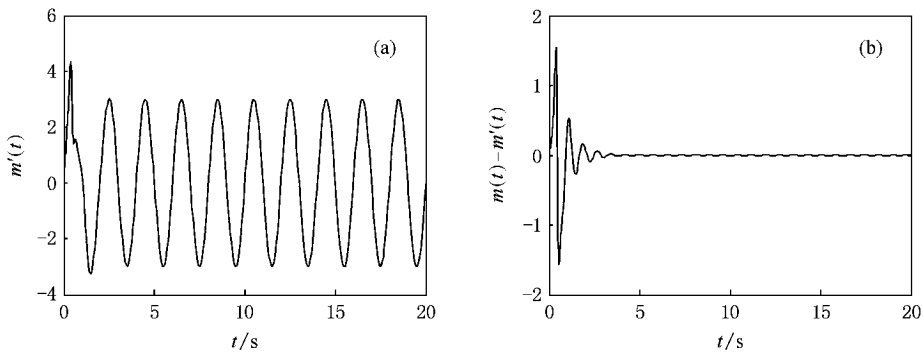


图5 通信系统的模拟结果 (a)为恢复的信号 $m'(t) = s - \alpha y_2$, $\alpha = -0.5$ (b)为原信号与恢复信号之间误差的时域波形

选择系统参数 $\alpha = 0$, 比例因子 $\alpha = -0.5$, 耦合系数为 10, 增益常数 $\mu = 10$, 信息信号 $m(t) = 3\sin\pi t$. 对上述通信系统进行模拟, 结果如图 5.

上述通信方法还可推广到其他的混沌系统, 如著名的 Chua's 电路及最近由吕金虎、陈关荣等人提出的非线性电路里的多卷波系统^[23, 24]等.

5. 结 论

本文提出一种普遍适用的混沌广义投影同步方

法, 凡是可以通过单向耦合实现完全同步的混沌系统, 均可采用本文提出的方法达到广义投影同步. 控制器具有统一的设计规律, 该方法的特点是只需向响应系统传递一个驱动变量即可实现混沌广义投影同步, 比起已有的方法具有更高的实用价值. 从仿真图中可以非常直观地看出投影的结果. 最后, 基于本文提出的同步方法构造了实用性较强的保密通信系统, 由于只需向接收系统传递一路信号, 且信息信号 $m(t)$ 的幅度、频率和比例因子 α 的大小都没有限制, 从而具有实用性好、安全性高的特点.

- [1] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
- [2] Rosenblum M G, Pikovsky A S, Kurths J 1996 *Phys. Rev. Lett.* **76** 1804
- [3] Taherion S, Lai Y C 1999 *Phys. Rev. E* **59** 6247
- [4] Kocarev L, Parlitz U 1996 *Phys. Rev. Lett.* **76** 1816
- [5] Yang S S, Duan K 1998 *Chaos, Solitons & Fractals* **10** 1703
- [6] Li G H 2004 *Acta Phys. Sin.* **53** 999 (in Chinese) [李国辉 2004 物理学报 **53** 999]
- [7] Zhang W P, Tang G N, Luo X S 2005 *Acta Phys. Sin.* **54** 3497 (in Chinese) [张伟平、唐国宁、罗晓曙 2005 物理学报 **54** 3497]
- [8] Wang X Y, Meng J 2008 *Acta Phys. Sin.* **57** 726 (in Chinese) [王兴元、孟娟 2008 物理学报 **57** 726]
- [9] Liu J, Chen S H, Lu J A 2003 *Acta Phys. Sin.* **52** 1595 (in Chinese) [刘杰、陈士华、陆君安 2003 **52** 1595]
- [10] Wang X Y, Wang Y 2007 *Acta Phys. Sin.* **56** 2498 (in Chinese) [王兴元、王勇 2007 物理学报 **56** 2498]
- [11] Yan J P, Li C P 2005 *Chaos, Solitons & Fractals* **26** 1119
- [12] Min F H, Wang Z Q 2007 *Acta Phys. Sin.* **56** 6239 (in Chinese) [闵富红、王执铨 2007 物理学报 **56** 6239]
- [13] Li C P, Yan J P 2006 *Chaos, Solitons and Fractals* **30** 140
- [14] Li G H 2007 *Chaos, Solitons and Fractals* **32** 1454
- [15] Li G H 2006 *Chaos, Solitons and Fractals* **30** 77
- [16] Chen G R, Lü J H 2003 *Dynamics of the Lorenz System Family: Analysis Control and Synchronization* (Beijing: Science Press) p141 (in Chinese) [陈关荣、吕金虎 2003 Lorenz 系统族的动力学分析、控制与同步(北京:科学出版社)第 141 页]
- [17] Lü J H, Chen G R 2002 *Int. J. Bifurcation and Chaos* **12** 2917
- [18] Lorenz E N 1963 *J. Atmos. Sci.* **20** 130
- [19] Chen G R, Ueta T 1999 *Int. J. Bifurcation and Chaos* **9** 1465
- [20] Lü J H, Chen G R 2002 *Int. J. Bifurcation and Chaos* **12** 659
- [21] Hu M F, Xu Z Y 2007 *Chin. Phys.* **16** 3231
- [22] Li J F, Li N 2002 *Chin. Phys.* **11** 1124
- [23] Lü J H, Chen G R 2006 *Int. J. Bifurcation and Chaos* **16** 775
- [24] Lü J H, Yu S, Leung H, Chen G R 2006 *IEEE Trans Circuits Syst.* **1** **53** 149

Generalized projective synchronization of chaotic system based on a single driving variable and its application in secure communication

Li Nong^{1)†} Li Jian-Fen²⁾

¹⁾ *The Engineering Institute, Air Force Engineering University, Xi'an 710038, China*

²⁾ *The Sciences Institute, Air Force Engineering University, Xi'an 710051, China*

(Received 1 February 2008 ; revised manuscript received 20 March 2008)

Abstract

A generalized projective synchronization method is proposed based on unidirectional coupled synchronization by only transmitting a single driving variable. The proposed method allows us to arbitrarily direct the scaling factor to a desired value. Since chaos synchronization can be achieved by transmitting a single variable from driving system to response system, this method is more practical. Theoretical deduction and computer simulation show the effectiveness of the proposed method. A scheme for secure communication, which can increase the security of a communication system, is presented based on generalized projective synchronization of unified chaotic system.

Keywords : chaotic system, single driving variable, generalized projective synchronization, unified chaotic system

PACC : 0545