

# 超混沌 Qi 系统的错位投影同步及其 在保密通信中的应用\*

闵富红<sup>†</sup> 王恩荣

(南京师范大学电气与自动化工程学院, 南京 210042)

(2009 年 8 月 30 日收到; 2010 年 3 月 10 日收到修改稿)

提出了一种新型的混沌系统同步方法, 即错位投影同步, 要求驱动系统和响应系统中的所有状态向量, 至少有一对不是按照原有的对应关系成比例同步, 而是按照向量的错位关系成比例投影同步. 以新型的四维超混沌 Qi 系统为例, 分析出 23 种混沌系统的同步方案. 针对其中一种同步, 基于 Lyapunov 稳定性理论, 设计有效的非线性控制器, 实现初始值不同的两个超混沌 Qi 系统错位投影同步. 另外, 将该方法应用于混沌保密通信中, 基于改进的混沌掩盖通信原理, 在发送端使用超混沌信号对信息信号进行加密并发送, 最后从同步后的接收端系统不失真地恢复出有用信号. 数值仿真表明, 该方案有着良好的通信和保密特性.

**关键词:** 超混沌系统, Qi 系统, 错位投影同步, 保密通信

**PACC:** 0545

## 1. 引 言

混沌作为一种复杂的非线性运动行为, 由于其在信号处理、生命科学、工程等领域中的巨大潜力和发展前途, 已经引起了国内外科研工作者的重视, 并且取得了大量的研究成果. 文献[1]详细阐述了混沌同步的发展史, 且介绍了各种混沌同步方法, 有完全同步, 相位同步, 广义同步, 滞后同步, 投影同步等<sup>[1-7]</sup>. 这些方法各有千秋, 其中投影同步方案对数字保密通信有更大的潜在应用前景. 目前, 在混沌控制与同步中, 出现了一个新的概念, 即“错位”. 文献[8]提出了一种错位自适应控制方法, 有效地将 Lorenz 混沌系统控制到非稳定的平衡点. 文献[9]基于 Lyapunov 稳定性理论, 采用非线性反馈控制方法研究了 Lorenz 混沌系统的错位同步. 所谓错位同步, 在混沌系统同步中它不同于完全同步, 要求驱动系统的状态向量中, 至少有一个状态向量不与响应系统中的状态向量相对应, 而是与其他的任意状态向量最终趋于一致.

本文提出将广义投影同步与错位同步相结合,

形成一种新型的同步方案, 称作“错位投影同步”. 其要求在控制器的作用下, 驱动系统与响应系统中的状态向量, 至少有一对不是按照原来的对应关系成比例投影同步, 而是向量的错位关系成比例同步, 从而为混沌在信息加密方面的应用开辟了新的路径. 以新型四维超混沌 Qi 系统<sup>[10]</sup>为例研究, 该系统在大参数范围内遍历, 因而特别适合于混沌加密, 有利于信息信号的加密与掩盖. 文中针对一种错位投影同步的形式, 构造了非线性反馈控制器, 实现了超混沌 Qi 系统的同结构错位投影同步. 最后, 将该同步方案应用到保密通信中, 且利用改进的混沌掩盖通信方案, 将有用的信号进行加密、掩盖和不失真地恢复.

## 2. 问题的描述

考虑如下耦合的两个非线性混沌系统:

$$\begin{cases} \dot{x} = F(x), \\ \dot{y} = G(y) + u(x, y), \end{cases} \quad (1)$$

其中  $u$  是控制器的输入,  $u(0, 0) = 0$ .  $x, y \in R^n$ ,  $x = (x_1, x_2, \dots, x_n)^T$ ,  $y = (y_1, y_2, \dots, y_n)^T$ ,  $F, G$  为  $R^n \rightarrow R^n$  的可微函数. 系统(1)中的第 1 式为驱动系统, 第

\* 国家自然科学基金(批准号: 51075275, 60774060), 江苏省普通高校自然科学研究计划(批准号: 08KJB510006)资助的课题.

<sup>†</sup> E-mail: minfuhong@njnu.edu.cn

2 式为响应系统.

如果存在这样的矩阵  $\tilde{\alpha} \in R^{n \times n}$ , 要求该矩阵每行每列同时有且仅有一个非零元素值  $\alpha$ , 矩阵中其他  $n^2 - 1$  元素都为 0, 且设系统误差  $e_i = y_j - \alpha x_i, i, j = 1, 2, \dots, n, \alpha$  为比例因子, 使得从不同初始值出发的混沌系统有  $\lim_{t \rightarrow \infty} \|e_i\| = \lim_{t \rightarrow \infty} \|y_j - \alpha x_i\| = 0$ . 那么当  $i = j$  时, 就是一般意义下的广义投影同步; 当  $i$  和  $j$  至少有一对值不相等时, 就是新型的错位投影同步, 其要求驱动系统的所有状态向量与响应系统的状态向量, 至少有一对向量不按照原有的对应关系成比例投影同步, 而是按照向量的错位关系投影同步.

1) 矩阵  $\tilde{\alpha}$  的种类有  $n!$  种. 当矩阵  $\tilde{\alpha}$  为对角矩阵时, 就是广义投影同步; 当矩阵  $\tilde{\alpha}$  不是对角矩阵时, 就是所谓的错位投影同步, 此时  $\tilde{\alpha}$  的种类有  $(n! - 1)$  种, 也就是错位投影同步方案有  $(n! - 1)$  种. 实际上, 广义投影同步可以看作错位投影同步的特例. 可以想象, 这样的同步方法对数字保密通信隐藏有很重要的价值, 抗破译能力强.

2) 在系统(1)分式中, 当  $F = G$ , 就成为同结构的错位投影同步; 当  $F \neq G$ , 就成为异结构的错位投影同步. 同时, 该方案可以推广到分数阶的同结构或异结构的错位投影同步, 使得其有更广泛的应用范围.

### 3. 超混沌 Qi 系统的错位投影同步

Qi 等<sup>[10]</sup>最近构造了一个新型的四维超混沌系统, 该系统随着参数的改变能够产生复杂的动力学行为, 相空间具有很大的遍历范围, 数学模型如下:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3, \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3, \\ \dot{x}_3 = -cx_3 - ex_4 + x_1x_2, \\ \dot{x}_4 = -dx_4 + fx_3 + x_1x_2, \end{cases} \quad (2)$$

其中  $a, b, c, d, e, f$  是系统参数. 当  $a = 50, c = 13, d = 8, e = 33, f = 30$  时, 改变参数  $b$ , Lyapunov 指数谱如图 1 所示, 有两个正的指数, 系统特性呈现超混沌, 吸引子参见文献[5].

令系统(2)为驱动系统, 通过构造合适的非线性控制器实现新型超混沌 Qi 系统的错位投影同步, 那么受控的响应系统为

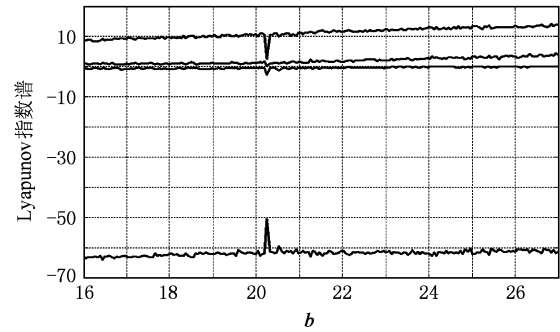


图 1 参数  $b$  变化时 Qi 混沌系统的 Lyapunov 指数

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) + y_2y_3 + u_1, \\ \dot{y}_2 = b(y_1 + y_2) - y_1y_3 + u_2, \\ \dot{y}_3 = -cy_3 - ey_4 + y_1y_2 + u_3, \\ \dot{y}_4 = -dy_4 + fy_3 + y_1y_2 + u_4. \end{cases} \quad (3)$$

混沌 Qi 系统(2)是四维系统, 驱动系统(2)与响应系统(3)的广义错位投影同步有  $(4! - 1) = 23$  种. 设  $n_i, i = 1, \dots, 2, 3$ , 利用数字 1, 2, 3 和 4 分别代表两个混沌系统的对应状态向量, 有如下的 23 种状态向量错位组合, 分别为

$$\begin{aligned} & n_1(1, 1), (2, 2), (3, 4), (4, 3); \\ & n_2(1, 1), (2, 3), (3, 2), (4, 4); \\ & n_3(1, 1), (2, 3), (3, 4), (4, 2); \\ & n_4(1, 1), (2, 4), (3, 2), (4, 3); \\ & n_5(1, 1), (2, 4), (3, 3), (4, 2); \\ & n_6(1, 2), (2, 1), (3, 3), (4, 4); \\ & n_7(1, 2), (2, 1), (3, 4), (4, 3); \\ & n_8(1, 2), (2, 3), (3, 1), (4, 4); \\ & n_9(1, 2), (2, 3), (3, 4), (4, 1); \\ & n_{10}(1, 2), (2, 4), (3, 1), (4, 3); \\ & n_{11}(1, 2), (2, 4), (3, 3), (4, 1); \\ & n_{12}(1, 3), (2, 1), (3, 2), (4, 4); \\ & n_{13}(1, 3), (2, 1), (3, 4), (4, 2); \\ & n_{14}(1, 3), (2, 2), (3, 1), (4, 4); \\ & n_{15}(1, 3), (2, 2), (3, 4), (4, 1); \\ & n_{16}(1, 3), (2, 4), (3, 1), (4, 2); \\ & n_{17}(1, 3), (2, 4), (3, 2), (4, 1); \\ & n_{18}(1, 4), (2, 1), (3, 2), (4, 3); \\ & n_{19}(1, 4), (2, 1), (3, 3), (4, 2); \\ & n_{20}(1, 4), (2, 2), (3, 1), (4, 3); \\ & n_{21}(1, 4), (2, 2), (3, 3), (4, 1); \end{aligned}$$

$$n_{22}(1,4), (2,3), (3,1), (4,2);$$

$$n_{23}(1,4), (2,3), (3,2), (4,1).$$

如果驱动系统(2)和响应系统(3)分别对应的状态向量组合为(1,1), (2,2), (3,3), (4,4),那就是混沌系统完全同步,或者组合为广义投影同步,不能形成系统状态向量的错位.对于以上23种错位同步,这里研究第九种 $n_9$ ,其余种类都可以用类似方法进行分析.定义错位投影同步误差为

$$\begin{cases} e_1 = y_2 - \alpha x_1, \\ e_2 = y_3 - \alpha x_2, \\ e_3 = y_4 - \alpha x_3, \\ e_4 = y_1 - \alpha x_4. \end{cases} \quad (4)$$

得到如下的误差系统动力学方程

$$\begin{cases} \dot{e}_1 = b(y_1 + y_2) - y_1 y_3 - \alpha(a(x_2 - x_1) + x_2 x_3) + u_2, \\ \dot{e}_2 = -cy_3 - ey_4 + y_1 y_2 - \alpha(b(x_1 + x_2) - x_1 x_3) + u_3, \\ \dot{e}_3 = -dy_4 + fy_3 + y_1 y_2 - \alpha(-cx_3 - ex_4 + x_1 x_2) + u_4, \\ \dot{e}_4 = a(y_2 - y_1) + y_2 y_3 - \alpha(-dx_4 + fx_3 + x_1 x_2) + u_1. \end{cases} \quad (5)$$

**定理 1** 选择如下的非线性反馈控制函数

$$\begin{cases} u_1 = -ay_2 - y_2 y_3 + \alpha((a-d)x_4 + fx_3 + x_1 x_2), \\ u_2 = -ke_1 - by_1 + y_1 y_3 + \alpha(ax_2 - (b+a)x_1 + x_2 x_3), \\ u_3 = ey_4 - y_1 y_2 + \alpha(bx_1 + (b+c)x_2 - x_1 x_3), \\ u_4 = -fy_3 - y_1 y_2 + \alpha((d-c)x_3 - ex_4 + x_1 x_2), \end{cases} \quad (6)$$

其中,反馈控制增益 $k > b$ ,且系统参数 $b > 0$ ,就能够实现驱动系统(2)和响应系统(3)的状态向量错位投影同步.

**证明** 将(6)式代入(5)式,得到如下误差方程

$$\begin{cases} \dot{e}_1 = -(k-b)e_1 \\ \dot{e}_2 = -ce_2, \\ \dot{e}_3 = -de_3, \\ \dot{e}_4 = -ae_4. \end{cases} \quad (7)$$

因而分析驱动系统(2)和响应系统(3)的错位投影同步,转化为分析误差系统(7)的稳定性问题.

构造 Lyapunov 函数为  $V = \frac{1}{2}e^T e$ ,对  $V$  关于时

间  $t$  求导,可得

$$\begin{aligned} \dot{V} &= \dot{e}^T e = e_1 \dot{e}_1 + e_2 \dot{e}_2 + e_3 \dot{e}_3 + e_4 \dot{e}_4 \\ &= -(k-b)e_1^2 - ce_2^2 - de_3^2 - ae_4^2. \end{aligned} \quad (8)$$

由于参数 $a, b, c, d$ 都为正常数,且 $k > b$ ,一定有 $\dot{V}$ 负的,且半负定,则误差系统(7)是大范围渐近稳定的.可见,在非线性控制器(6)的作用下,实现驱动系统(2)和响应系统(3)的状态向量错位投影同步.

取仿真步长为0.01进行数值仿真.系统参数为 $a = 50, b = 25, c = 13, d = 8, e = 33, f = 30$ ,反馈控制增益 $k = 30$ ,比例因子 $\alpha = 2$ .驱动系统(2)和响应系统(3)的初始值设为(2,5, -1, -1, 3, 2, 1, 4),那么误差系统的初始值为(-2, -9, 6, 5).图2为错位投影同步的误差曲线,是单调衰减,系统响应速度快.图3为错位投影同步的状态向量的时序图.可见,状态向量 $x_1, y_2; x_2, y_3; x_3, y_4$ 以及 $x_4, y_1$ 分别按照比例因子2的大小,快速对应同步.根据图2和图3,说明了本文提出方案的有效性,及错位投影同步的可行性,且同步精度高.

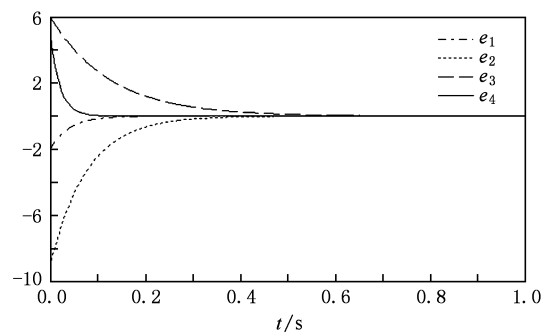


图2 误差曲线图

#### 4. 错位投影同步在保密通信中的应用

混沌同步的实现,解决了混沌保密通信技术的一大难点问题,使得混沌保密通信成为可能<sup>[11,12]</sup>.本文提出的新型错位投影同步,为混沌通信提供了一种更新的加密形式,具有更强的抗破译能力.这里将本文的错位投影同步方法应用于保密通信中,采用了1996年由Milanovic等<sup>[12]</sup>提出的改进混沌掩盖保密通信方案.其原理是,在发送器中引入了合成信号的反馈,这样在发送端和接受端的混沌系统中,分别引入了有用信号和混沌信号组成的混合

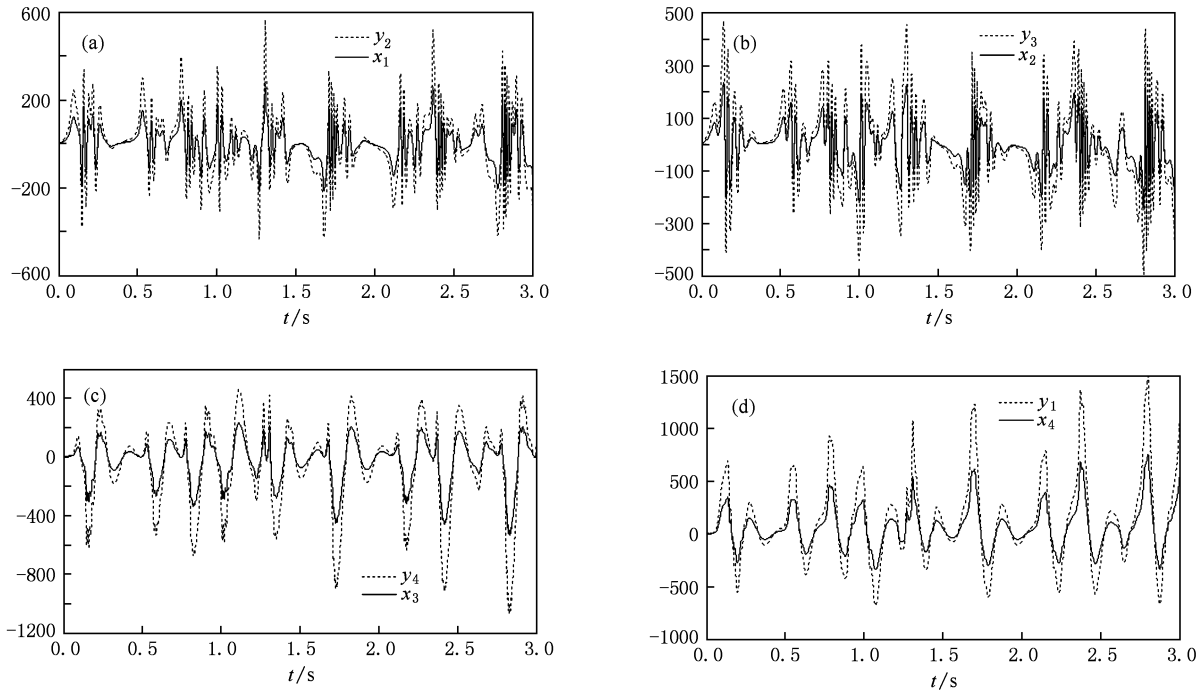


图3 错位投影同步的向量时序图

信号的反馈,同步精度提高了,克服了普通的混沌掩盖同步法的一些缺点.

设需要传输的信息信号为  $s(t)$ , 则  $m(t) = x_1 + s(t)$  为发送器和接收器之间的通信信号, 且是信息信号与混沌信号  $x_1$  的混叠信号. 该信号分别反馈在发送端和接收端, 结合了传输信号的发送端动力学模型如下:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3, \\ \dot{x}_2 = b(m + x_2) - mx_3, \\ \dot{x}_3 = -cx_3 - ex_4 + mx_2, \\ \dot{x}_4 = -dx_4 + fx_3 + mx_2. \end{cases} \quad (9)$$

接收端的动力学方程为

$$\begin{cases} \dot{y}_1 = a(m - y_1) + my_3 + u_1, \\ \dot{y}_2 = b(y_1 + y_2) - y_1y_3 + u_2, \\ \dot{y}_3 = -cy_3 - ey_4 + y_1m + u_3, \\ \dot{y}_4 = -dy_4 + fy_3 + y_1m + u_4, \end{cases} \quad (10)$$

上式中, 令非线性反馈控制器为

$$\begin{cases} u_1 = -am - my_3 + \alpha((a-d)x_4 + fx_3 + mx_2), \\ u_2 = -ke_1 - by_1 + y_1y_3 + \alpha(ax_2 - (b+a)x_1 + x_2x_3), \\ u_3 = ey_4 - y_1m + \alpha(bm + (b+c)x_2 - mx_3), \\ u_4 = -fy_3 - y_1m + \alpha((d-c)x_3 - ex_4 + mx_2). \end{cases} \quad (11)$$

同样, 在(11)式中的非线性反馈控制增益是  $k > b$  的常数. 由于(9)式与(10)式的错位投影同步误差系统模型与(4)式一致, 故其同步稳定性的证明略.

当错位投影同步实现时, 其误差单调衰减, 趋于零, 则有  $e_1 \rightarrow 0$  时, 则  $e_1 = y_2 - \alpha x_1 \rightarrow 0$ . 接收端的恢复信号为  $s'(t)$ , 即

$$\begin{aligned} s'(t) &= m(t) - \frac{1}{\alpha}y_2 \\ &= x_1 + s(t) - \frac{1}{\alpha}y_2 \rightarrow s(t), \end{aligned} \quad (12)$$

这表明了同步发生时, 发送器发送的信息信号能够不失真地被接收器所接收并恢复.

取比例因子  $\alpha = 2$  数值仿真, 初始值同前. 设传送的有用信号为  $s(t) = 45\text{square}(5t)$  的方波信号. 令  $es(t) = s(t) - s'(t)$  为恢复信号与有用信号的误差. 仿真结果如图4, 图中分别表示传送的有用信号  $s(t)$ 、有用信号与混沌信号的混叠信号  $m(t)$ 、接收端恢复的有用信号  $s'(t)$ 、以及恢复信号与传送信号的误差信号. 另外, 若  $p(t) = 10 \sin(4\pi t)$  为传送的有用信号, 那么有用信号与混沌信号进行混叠后的信号为  $q(t) = x_1 + p(t)$ , 将  $q(t)$  分别反馈到发送端和接收端, 同样设  $p'(t)$  为从接收端恢复的信号,  $ep(t) = p(t) - p'(t)$  为误差信号, 仿真结果如图5.

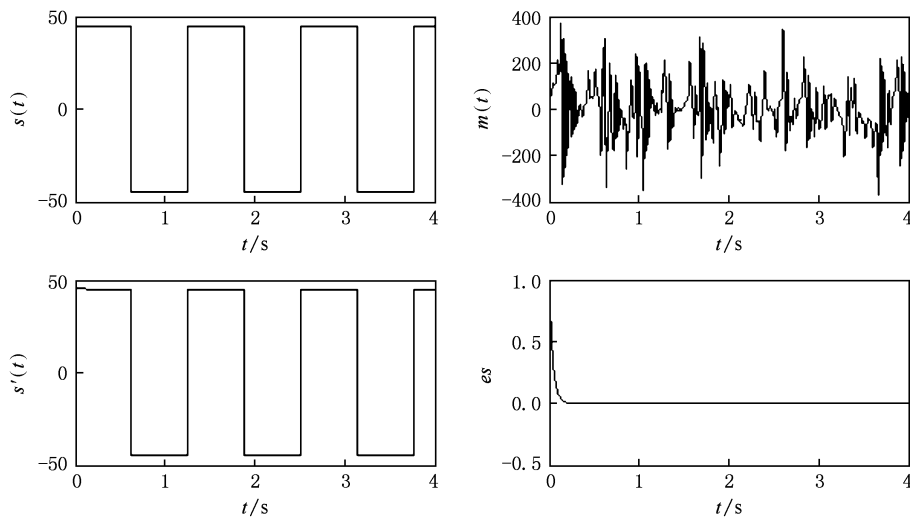


图4 方波信号加密仿真结果

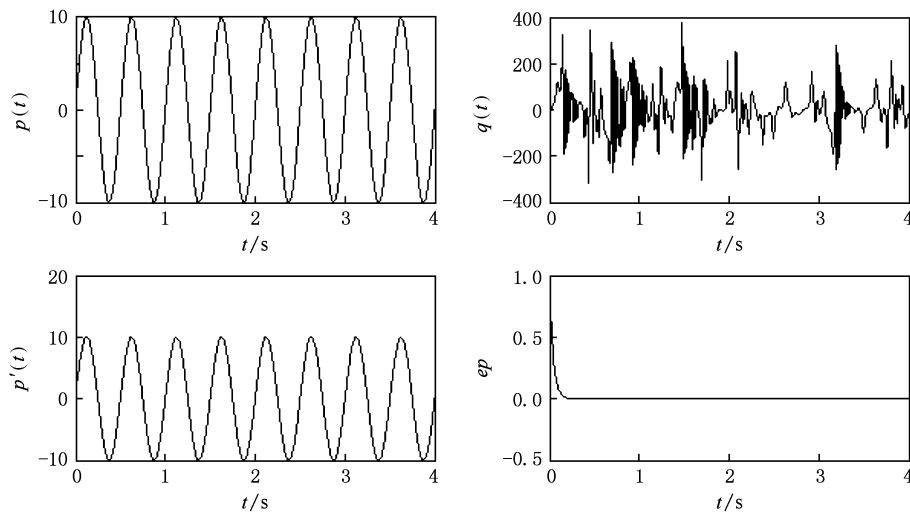


图5 正弦信号加密仿真结果

可见,无论传送的有用信息信号是方波信号还是正弦信号,都能够快速被混沌信号加密并进行通信传输,且不失真地恢复,说明了该错位投影同步方案的有效性.

## 5. 结 论

本文提出了一种新型的错位投影同步方案,为混沌保密通信开辟了新的路径.以四维超混沌 Qi 系统为例,设计了合适的非线性反馈控制器,且利用

稳定性理论分析误差系统的稳定性,实现了初始值不同的同结构的两个 Qi 混沌系统错位投影同步.同时,将之应用到混沌信号的加密通信中,将正弦信号及方波信号等信息信号与混沌信号进行加密和传送,最终能够不失真地从接收端恢复.文中提出的新型混沌系统同步方案,不仅适用于整数阶混沌系统的同步,还可推广到分数阶混沌系统的同结构或者异结构的错位投影同步,且混沌系统的向量维数越高,错位投影同步种类越多,为混沌保密通讯提供了新的思路.

- [1] Luo A C J 2009 *Commun Nonlinear Sci Numer Simulat* **14** 1901
- [2] Qi W, Wang Y H 2009 *Chin. Phys. B* **18** 1404
- [3] Taherion S, Lai Y 2000 *Int. J. Bifurc. Chaos.* **10** 2587
- [4] Rosenblum M, Pikovsky A, Kurth J 1996. *Phys. Rev. Lett.* **76** 1804
- [5] Guo LX, Hu MF, Xu ZY 2010 *Chin. Phys. B* **19** 020512
- [6] Min F H, Wang Z Q 2008 *Acta Phys. Sin.* **57** 31 (in Chinese)  
[ 闵富红、王执铨 2008 物理学报 **57** 31 ]
- [7] Meng J, Wang X Y 2009 *Acta Phys. Sin.* **58** 819 (in Chinese)  
[ 孟 娟、王兴元 2009 物理学报 **58** 819 ]
- [8] Tao C H, Lu J A, Chen S H 2004 *Systems Engineering and Electronics* **29** 1346 (in Chinese) [ 陶朝海、陆君安、陈士华 2004 系统工程与电子技术 **26** 81 ]
- [9] Hu M F, Xu Z Y 2007 *Systems Engineering and Electronics* **29** 1346 (in Chinese) [ 胡满峰、徐振源 2007 系统与工程电子技术 **29** 1346 ]
- [10] Qi G Y, Michael A, Barend J, Chen GR 2009 *Chaos. Solitons Fract.* **40** 2544
- [11] Li K Z, Zhao M C, Fu X C 2009 *IEEE Trans. On Circuits and systems I* **56** 2280
- [12] Milanovic V, Zaghoul M E 1996 *Electronic letters.* **32** 11

## Dislocated projective synchronization of Qi hyper-chaotic system and its application to secure communication \*

Min Fu-Hong<sup>†</sup> Wang En-Rong

(School of Electronic Engineering and Automation, Nanjing Normal University, Nanjing 210042, China)

(Received 30 August 2009; revised manuscript received 10 March 2010)

### Abstract

This paper focuses on a new type of dislocated projective synchronization, in which, the state variables of drive system and response system, at least one pair is required not to synchronize in proportion to the original corresponding state variable, but to realign the projective synchronization in proportion to dislocation relation of vectors. Here a new Qi hyper-chaotic system is taken for example, which has 23 synchronized schemes. Using the Lyapunov stability theory, a nonlinear controller is presented and a kind of disorder projective synchronization for Qi system is successfully completed. Then this method is applied to secure communication through improved chaotic masking. The information signal is mixed with the chaotic signal before being transmitted, and is recovered without distortion through the synchronized receiver. Simulation results show that the scheme has a good performance.

**Keywords:** hyper-chaotic system, Qi system, dislocated projective synchronization, secure communication

**PACC:** 0545

\* Project supported by the National Natural Science Foundation of China (Grant No. 51075225, 60774060), the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 08KJB510006).

<sup>†</sup> E-mail: minfuhong@njnu.edu.cn