新型超混沌系统的错位投影同步及在保密通信中的应用

闵富红,吴薛红

(南京师范大学 电气与自动化工程学院,江苏 南京 210042)

[摘要] 提出了一种新型的混沌系统错位投影同步方案,实现驱动系统与响应系统中所有状态向量的相互错位投影同步,即状态向量不是按照原有的对应关系成比例投影同步.这里以新型的四维超混沌 Tang 系统和 Qi 系统为例,研究两种错位投影同步方案. 基于 Lyapunov 系统稳定性理论,构造合适的非线性反馈控制器,分别实现了超混沌系统的同结构和异结构的错位投影同步.然后,利用改进的混沌掩盖方法,将该同步方案应用到保密通信中,在发送端将混沌信号与信息信号加密并发送,最后从接收端系统中不失真地恢复出有用信号,数值仿真结果表明了该方案的可行性和良好的保密特性.

[关键词] 错位投影同步,超混沌系统,非线性反馈控制器,保密通信

[中图分类号] TP391.9 [文献标识码] A [文章编号]1672-1292(2011)01-0013-06

Mismatch Project Synchronization for Hyper-Chaotic Systems and Its Application to Secure Communication

Min Fuhong, Wu Xuehong

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

Abstract: The new mismatch project synchronization is proposed in the paper, which can direct the state vectors between the driver system and response system to synchronize in disorder. Based on the Lyapunov stability theory, two schemes of synchronization are studied and the nonlinear controllers are designed to achieve mismatch projective synchronization for two same or different hyper-chaotic systems. Here Tang system and Qi system are taken as examples. Then this method is applied to secure communication through improved chaotic masking algorithm. The useful signal is mixed with hyper-chaotic signals before transmitted, and is recovered undistorted through the synchronized receiver. Simulation results are presented to demonstrate the effectiveness of the proposed method.

Key words: mismatch project synchronization, hyper-chaotic system, nonlinear feedback controller, secure communication

混沌作为一种复杂的非线性运动行为,在物理学、化学、工程学和信息学等领域得到了广泛的研究,且取得了大量的研究成果.为了更好地利用混沌,近年来学者们提出了许多不同的混沌同步方案,实现了许多复杂混沌系统的同结构与异结构同步,同步方案主要包括完全同步、相位同步、滞后同步、广义同步、投影同步[1-6]等.文献[6]设计了线性反馈控制器实现两个 Jerk 方程的完全同步,并将之应用到混沌保密通信中;文献[7]设计了合适的非线性控制器,实现了一个 Lorenz,Chen 以及 Rössler 系统的投影同步,并将其用于信号加密中.文献[8]以 Lorenz 系统为例,设计了合适的控制器,实现 Lorenz 混沌系统的错位同步.

本文考虑在已有的同步方案基础上,提出了一种新型的同步方案,即错位投影同步.它要求混沌系统同步时,驱动系统与响应系统中的状态向量,至少有一对状态向量不按照比例因子的大小同步,而是与其他的任意状态向量成比例最终趋于一致.该方案不同于以往的同步方法,当两个混沌系统错位投影同步时,混沌系统的阶数增加,同步方案的种类也随之增加.例如,两个四阶混沌系统错位同步有 23 种方案,两个五阶混沌系统的同步有 119 种,当然也可以是不同阶的混沌系统错位投影同步.将这种方案应用到保密通信,增加了解密的难度,因而在信号加密方面有着很好的应用前景.这里以新型超混沌 Tang 系统和超混

收稿日期: 2010-05-31.

基金项目: 国家自然科学基金(51075275)、江苏省普通高校自然科学研究计划(08KJB510006).

通讯联系人: 闵富红,博士,副教授,研究方向:混沌系统同步与控制. E-mail: minfuhong@njnu.edu.cn

沌 Qi 系统为例,基于 Lyapunov 系统稳定性理论,采用不同的错位投影同步方案,分别设计合适的非线性反馈控制器,实现两个初始值不同的新型四维超混沌 Tang 系统的同结构错位投影同步,以及实现超混沌 Tang 系统和超混沌 Qi 系统的异结构错位投影同步,并且将其应用到信号保密通信中,信息信号在发送端被混沌信号加密,在输出端被不失真地恢复. 该种同步方案可以有效地对信息信号掩盖,并且难以解密,抗破译能力强.

1　超混沌吸引子的描述

最近,Tang LR 等[9]提出一个含有 8 个参数的、且拓扑结构简单的超混沌系统,该系统仅有 3 个平衡点,易于电路实现,产生比较宽的混沌序列,对数字加密领域的研究具有重要意义,其数学模型如下:

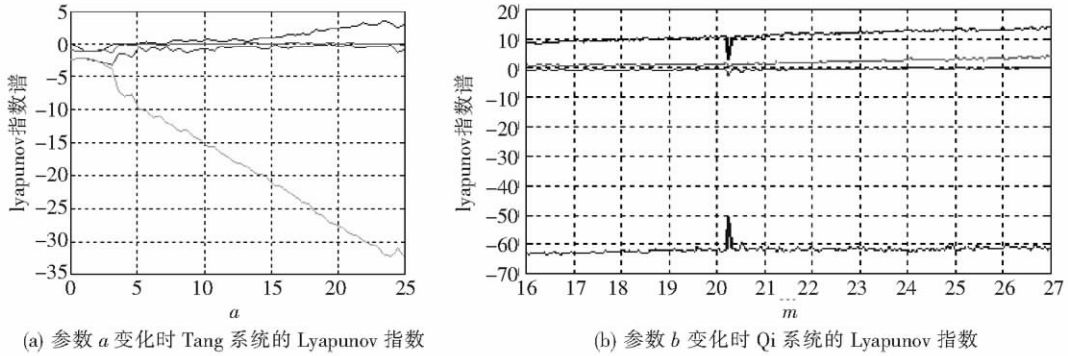
$$\begin{cases} \dot{x}_1 = -ax_1 + bx_2, \\ \dot{x}_2 = cx_1 - x_1x_3 - dx_2 - x_4, \\ \dot{x}_3 = x_1x_2 - ex_3 - fx_1 + gx_4, \\ \dot{x}_4 = h(x_2x_3 - x_4), \end{cases} \tag{1}$$

当给定参数 $a = 20.5, b = 68.8, c = 42, d = 0.6, e = 4, f = 4.5, g = 5, h = 0.8$ 时,该系统存在典型的超混沌吸引子[9]. 当改变参数 a 时,得到 Lyapunov 指数谱如图 1(a) 所示.

Qi GY 等学者[10]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,是迄今为止混沌行为遍历范围最大的吸引子,更加有利于信号的加密,有很好的应用价值,数学模型如下:

$$\begin{cases} \dot{z}_1 = l(z_2 - z_1) + z_2z_3, \\ \dot{z}_2 = m(z_1 + z_2) - z_1z_3, \\ \dot{z}_3 = -nz_3 - qz_4 + z_1z_2, \\ \dot{z}_4 = -pz_4 + \beta z_3 + z_1z_2, \end{cases} \tag{2}$$

其中 l, m, n, p, q, β 是系统参数. 当 $l = 50, n = 13, p = 8, q = 33, \beta = 30$ 时,改变参数 m,得到的 Lyapunov 指数谱如图 1(b) 所示,有两个正的指数,该系统特性呈现超混沌,吸引子参见文献[10].



(a) 参数 a 变化时 Tang 系统的 Lyapunov 指数　　(b) 参数 b 变化时 Qi 系统的 Lyapunov 指数

图 1　两个超混沌系统的 Lyapunov 指数

Fig.1　Lyapunov exponents spectrums of two different systems

2　同结构的超混沌 *Tang* 系统错位投影同步

设超混沌系统(1) 为驱动系统,实现两个初始值不同的新型超混沌 Tang 系统的错位投影同步,那么受控的响应系统为:

$$\begin{cases} \dot{y}_1 = -ay_1 + by_2 + u_1, \\ \dot{y}_2 = cy_1 - y_1y_3 - dy_2 - y_4 + u_2, \\ \dot{y}_3 = y_1y_2 - ey_3 - fy_1 + gy_4 + u_3, \\ \dot{y}_4 = h(y_2y_3 - y_4) + u_4, \end{cases} \tag{3}$$

如果设计的控制器 u_1,u_2,u_3,u_4,使得驱动系统(1) 与响应系统(3) 的所有状态向量不构成对应关系同步,而是系统状态向量的相互错位关系投影同步,即满足$\lim\limits_{t\to\infty}|\ y_j-\alpha x_i\ |=0,(\ i,\ j=1,2,3,4,i\neq j)$,那就是新型的状态向量错位投影同步. 对于四维系统存在$(4!-1)=23$种错位同步方案的组合. 同理,可以实现驱动系统(2) 与响应系统(3) 的异结构错位投影同步,即满足$\lim\limits_{t\to\infty}|\ y_j-\alpha z_i\ |=0,(\ i,\ j=1,2,3,4,i\neq j)$.

这里定义其中一种错位投影同步方案,令误差为: $e_1=y_2-\alpha x_1,e_2=y_3-\alpha x_2,e_3=y_4-\alpha x_3,e_4=y_1-\alpha x_4$, 比例因子 α 为常数,那么得到同步误差系统方程为:

$$\begin{cases}\dot e_1=cy_1-y_1y_3-dy_2-y_4-\alpha(-ax_1+bx_2)+u_2,\\ \dot e_2=-ey_3-fy_1+gy_4+y_1y_2-\alpha(cx_1-x_1x_3-dx_2-x_4)+u_3,\\ \dot e_3=h(y_2y_3-y_4)-\alpha(x_1x_2-ex_3-fx_1+gx_4)+u_4,\\ \dot e_4=-ay_1+by_2-\alpha(h(x_2x_3-x_4)+u_1.\end{cases}\tag{4}$$

定理 1　如果选择如下的非线性反馈控制函数

$$\begin{cases}u_1=-by_2+\alpha(hx_2x_3+(a-h)x_4),\\ u_2=-cy_1+y_1y_3+y_4+\alpha(bx_2+(d-a)x_1),\\ u_3=-gy_4-y_1y_2+\alpha(cx_1-x_1x_3+(e-d)x_2+(f-1)x_4),\\ u_4=-hy_2y_3+gy_1+\alpha((h-e)x_3-fx_1+x_1x_2).\end{cases}\tag{5}$$

那么能够实现初始值不同的驱动系统(1) 和响应系统(3) 的同结构错位投影同步.

证明　将式(5) 代入式(4),得到如下误差系统方程:

$$\begin{cases}\dot e_1=-de_1,\\ \dot e_2=-ee_2-fe_4,\\ \dot e_3=-he_3-ge_4,\\ \dot e_4=-ae_4.\end{cases}\tag{6}$$

现在系统(1) 和系统(3) 的错位投影同步问题转化为误差系统(6) 的稳定性问题. 构造 Lyapunov 函数 $\boldsymbol{V}=\frac{1}{2}\boldsymbol{e}^{\mathrm{T}}\boldsymbol{e}$,对 $\boldsymbol{V}$ 关于时间 t 求导,可得:

$$\dot{\boldsymbol{V}}=\dot{\boldsymbol{e}}^{\mathrm{T}}\boldsymbol{e}=e_1\dot e_1+e_2\dot e_2+e_3\dot e_3+e_4\dot e_4=-de_1^2-ee_2^2-fe_2e_4-he_3^2-ge_3e_4-ae_4^2=$$

$$\begin{bmatrix}e_1 & e_2 & e_3 & e_4\end{bmatrix}\begin{bmatrix}-d & 0 & 0 & 0\\ 0 & -e & 0 & -f/2\\ 0 & 0 & -h & -g/2\\ 0 & -f/2 & -g/2 & -a\end{bmatrix}\begin{bmatrix}e_1\\ e_2\\ e_3\\ e_4\end{bmatrix}=-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{e},\tag{7}$$

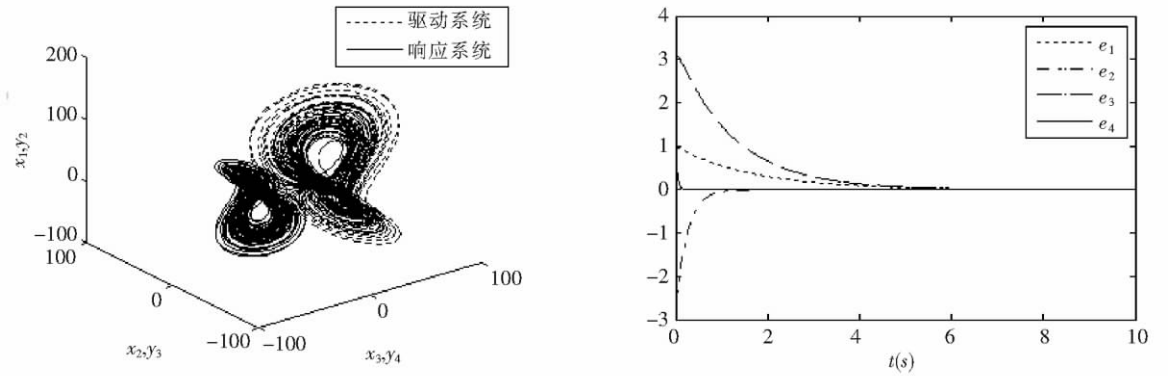
由于在系统(1) 式中已经规定系统参数的值,且都为正常数,那么计算出矩阵 $\boldsymbol{Q}$ 的各阶顺序子矩阵都是大于零的常数,则矩阵 $\boldsymbol{Q}$ 为正定矩阵. 可见 $\dot{\boldsymbol{V}}$ 为负定,则误差系统(6) 是在原点渐近稳定的. 可见,在非线性反馈控制器(5) 作用下,能够实现驱动系统(1) 和响应系统(3) 的所有状态向量错位投影同步.

下面数值仿真选取步长为0.01. 驱动系统(1) 和响应系统(3) 的初始值设为(0, -1,1, -0.5,1,1, -2,2.5),则误差初始值为(1, -2.6,3.1, -2). 为了使得系统处于超混沌状态,选取系统参数 $a=20.5$, $b=68.8,c=42,d=0.6,e=4,f=4.5,g=5,h=0.8$. 比例因子 $\alpha=-0.6$. 仿真结果如图 2. 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 -0.6,反向快速地达到错位投影同步,误差曲线为单调衰减,且响应速度快.

3　异结构的超混沌系统错位投影同步

在数字保密通信中,如果能够实现异结构超混沌系统的错位投影同步,将会明显扩大混沌同步的通信方案,提高通信的保密性和安全性.

根据定义 1,以系统(2) 作为驱动系统,系统(3) 作为响应系统. 同样,u_1,u_2,u_3,u_4 是要设计的非线性



(a) 错位投影同步时的系统混沌吸引子　　(b) 错位投影同步误差响应曲线

图 2　同结构 Tang 超混沌系统错位投影同步仿真结果

Fig.2　Mismatch project synchronization for two Tang hyper-chaotic system

反馈控制器,异结构错位投影同步方案仍有 23 种. 现在定义另一种状态向量的错位同步, 误差信号 $e_1 = y_3 - \alpha z_1, e_2 = y_4 - \alpha z_2, e_3 = y_1 - \alpha z_3, e_4 = y_2 - \alpha z_4$,其中常数 α 为比例因子,那么得到同步误差系统方程为:

$$\begin{cases} \dot{e}_1 = -ey_3 - fy_1 + gy_4 + y_1y_2 - \alpha(l(z_2 - z_1) + z_2z_3) + u_3, \\ \dot{e}_2 = h(y_2y_3 - y_4) - \alpha(m(z_1 + z_2) - z_1z_3) + u_4, \\ \dot{e}_3 = -ay_1 + by_2 - \alpha(z_1z_2 - nz_3 - qz_4) + u_1, \\ \dot{e}_4 = cy_1 - y_1y_3 - dy_2 - y_4 - \alpha(z_1z_2 + \beta z_3 - pz_4) + u_2. \end{cases} \tag{8}$$

定理 2　若选择非线性反馈控制器如下:

$$\begin{cases} u_1 = -by_2 + \alpha(z_1z_2 + (a - n)z_3 - qz_4), \\ u_2 = -cy_1 + y_1y_3 + \alpha(z_2 + \beta z_3 + z_1z_2 + (d - p)z_4), \\ u_3 = -gy_4 - y_1y_2 + \alpha(lz_2 + fz_3 + z_2z_3 + (e - l)z_1), \\ u_4 = -hy_2y_3 + \alpha((m + h)z_2 + mz_1 - z_1z_3). \end{cases} \tag{9}$$

则就能实现驱动系统(2) 和响应系统(3) 的对应状态向量错位投影同步.

证明　将式(9) 代入式(10),误差系统方程如下:

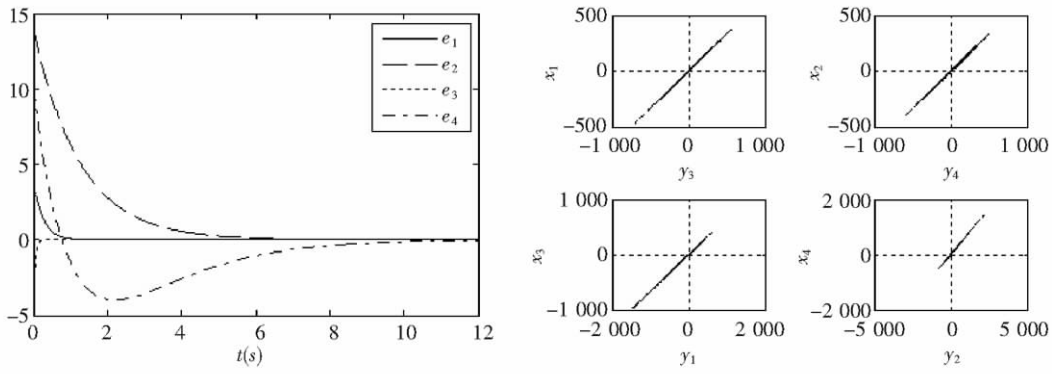
$$\begin{cases} \dot{e}_1 = -ee_1 - fe_3, \\ \dot{e}_2 = -he_2, \\ \dot{e}_3 = -ae_3, \\ \dot{e}_4 = -de_4 - e_2. \end{cases} \tag{10}$$

显然,误差系统方程的系数矩阵为:

$$\boldsymbol{A} = \begin{bmatrix} -e & 0 & -f & 0 \\ 0 & -h & 0 & 0 \\ 0 & 0 & -a & 0 \\ 0 & -1 & 0 & -d \end{bmatrix}. \tag{11}$$

计算出误差系统矩阵的特征值为 $\lambda_1 = -e, \lambda_2 = -h, \lambda_3 = -a, \lambda_4 = -d$. 在系统(1) 和系统(2) 式中,系统参数的值为正常数,那么误差系统特征值都是负实数,可见误差系统随着时间变化单调衰减,在原点渐进稳定. 进一步表明了在控制器(9) 作用下,实现了超混沌 Qi 系统(2) 和超混沌 Tang 系统(3) 的异结构错位投影同步.

同样数值仿真时,选取仿真步长为 0.01. 系统参数 $l = 50, m = 25, n = 13, p = 8, q = 33, \beta = 30$ 时,比例因子 $\alpha = 1.5$. 设驱动系统和响应系统的初始值分别为(2, −6,5, −4,3,4,6,5) ,那么误差初始值为(3,14, −4.5,10) . 从图3 可知,状态向量 $x_1, y_3; x_2, y_4; x_3, y_1$ 以及 x_4, y_2 分别按照比例因子 1.5 的大小,快速对应同步,且同步误差曲线单调衰减很快. 可见,不同结构的两个超混沌系统,同样可以实现错位投影同步.



(a) 同步误差响应曲线　　(b) 同步的状态向量对应图

图 3　异结构超混沌系统的错位投影同步仿真结果

Fig.3　Mismatch project synchronization for different hyper-chaotic systems

4　错位投影同步在保密通信中的应用

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,由于同步方案的增加,使得其具有更强的抗破译能力. 下面将混沌系统异结构错位投影同步的方案应用于保密通信中,且采用改进的混沌掩盖保密通信方案[11].

设需要传输的信息信号为 $s(t)$,令 $w(t) = z_1 + s(t)$ 为发送器和接收器之间的通信信号,是信息信号与混沌信号 z_1 的混叠信号,使其分别反馈到发送端和接收端,在接收端从 y_3 中可以不失真地还原出有用信号,那么混叠了传输信号的发送端系统模型如下:

$$\begin{cases} \dot{z}_1 = l(z_2 - z_1) + z_2 z_3, \\ \dot{z}_2 = m(w + z_2) - w_1 z_3, \\ \dot{z}_3 = -nz_3 - qz_4 + w_1 z_2, \\ \dot{z}_4 = -pz_4 + \beta z_3 + w_1 z_2. \end{cases} \tag{12}$$

则接收端的系统模型为:

$$\begin{cases} \dot{y}_1 = -ay_1 + by_2 + u_1, \\ \dot{y}_2 = cy_1 - y_1 w - dy_2 - y_4 + u_2, \\ \dot{y}_3 = y_1 y_2 - ey_3 - fy_1 + gy_4 + u_3, \\ \dot{y}_4 = h(y_2 w - y_4) + u_4. \end{cases} \tag{13}$$

其中,设计的非线性反馈控制器为:

$$\begin{cases} u_1 = -by_2 + \alpha(wz_2 + (a-n)z_3 - qz_4), \\ u_2 = -cy_1 + y_1 w + \alpha(z_2 + \beta z_3 + wz_2 + (d-p)z_4), \\ u_3 = -gy_4 - y_1 y_2 + \alpha(lz_2 + fz_3 + z_2 z_3 + (e-l)z_1), \\ u_4 = -hy_2 w + \alpha((m+h)z_2 + mw - wz_3). \end{cases} \tag{14}$$

同样,鉴于在控制器(14)作用下,式(12)与式(13)的同步误差系统模型与式(10)一致,故省略其同步稳定性的证明.

当加密后的系统(12)和(13)实现异结构的错位投影同步,其同步误差单调,渐进趋于零,即 $e_1 \to 0$ 时,有 $e_1 = y_3 - \alpha x_1 \to 0$. 那么,从接收端可以恢复出有用信号 $s'(t)$,即 $s'(t) = w(t) - y_3/\alpha = x_1 + s(t) - y_3/\alpha \to s(t)$,进一步说明了发送器发送的信息信号,在混沌序列掩盖下能够不失真地被接收器接收并恢复. 数值仿真时,初始值选取同前,比例因子 $\alpha = 2$. 设传送的有用信号 $s(t) = 25\mathrm{square}(5t)$ 为幅值很大的方波信号. 设 $es(t) = s(t) - s'(t)$ 为恢复信号与有用信号的误差. 图 4 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 $w(t)$、接受端恢复的有用信号 $s'(t)$、以及恢复信号与传送信号的误差信号. 可知传送的有用信息信号能够快速进行混沌加密通信. 这里传送的信号幅值范围很大,是因为超混沌

系统的状态向量幅值很大,同时由于比例因子的作用,也确保了混沌载波对信息信号的有效掩盖. 鉴于同样的驱动系统和响应系统,可以产生多种的错位投影同步方案,这些为混沌通信的破译增加了难度,进一步表明了该通信方案具有很好的安全性和抗破译能力.

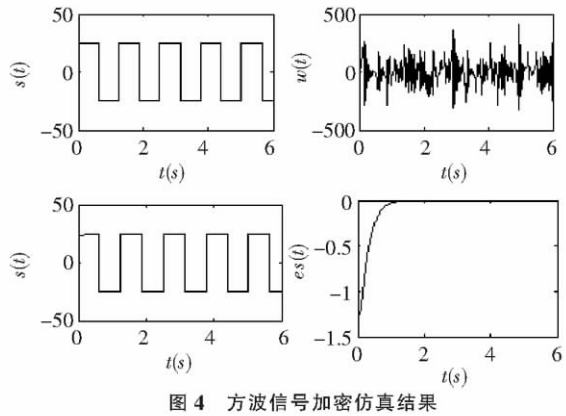


图 4　方波信号加密仿真结果

Fig.4　The simulation results for square signal

5　结论

本文提出了新型的混沌系统错位投影同步方案,且基于 Lyapunov 稳定性理论,分别设计了合适的非线性反馈控制器,实现了两个同结构 Tang 系统的错位投影同步,以及 Tang 系统和 Qi 系统的异结构错位投影同步. 使用了两种不同错位投影同步方案. 通过改变比例因子,获得了任意比例的输出向量,数值仿真表明其有效性. 且将该同步方法应用到保密通信中,可方便地不失真地恢复出有用信号. 总之,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,还可以推广到分数阶混沌系统的同结构或者异结构的投影同步,混沌系统的向量维数越高,错位投影同步种类越多,混沌加密后信息越难解密,从而为混沌保密通信开辟了新的路径,提供了新思路.

[参考文献](References)

[1] Taherion S, Lai Y. Experimental observation of lag synchronization in coupled chaotic systems [J]. Int J Bifurc Chaos, 2000, 10(11): 2 587-2 594.

[2] 闵富红,王执铨. 复杂 Dynamos 混沌系统的追踪控制与同步 [J]. 物理学报, 2008,57(1):31-36.
Min Fuhong, Wang Zhiquan. Generalized projective synchronization and tracking control of complex Dynamos systems [J]. Acta Physica Sinica, 2008, 57(1):31-36. (in Chinese)

[3] Rosenblum M, Pikovsky A, Kurth J. Phase synchronization in chaotic oscillators [J]. Phys Rev Lett, 1996, 76(11): 1 804-1 810.

[4] Cai Na, Jing Yuanwei, Zhang Siying. Generalized projective synchronization of different chaotic systems based on antisymmetric structure [J]. Chaos Solitons and Fractals, 2009, 42(2):1 190-1 196.

[5] Li Guohui. Projective lag synchronization chaotic systems [J]. Chaos Solitons and Fractals, 2009, 41(5):2 630-2 634.

[6] Nana B, Woafo P, Domngang S. Chaotic synchronization with experimental application to secure communication [J]. Commun Nonliear Sci Numer Simulat,2009,14(5):2 266-2 276.

[7] Li Kezan, Zhao Mingchao, Fu Xinchu. Projective synchronization of driving-response systems and its application to secure communication [J]. IEEE Trans on Circuits and systems I, 2009, 56(10):2 280-2 291.

[8] 胡满峰,徐振源. Lorenz 混沌系统的非线性反馈错位同步控制 [J]. 系统与工程电子技术, 2007, 29(8): 1 346-1 348.
Hu Manfeng, Xu Zhenyuan. Nonlinear feedback mismatch synchronization of Lorenz chaotic systems [J]. Systems Engineering and Electronics, 2007, 29(8): 1 346-1 348. (in Chinese)

[9] 唐良瑞,李静,樊冰. 一个新四维超混沌系统及其电路实现 [J]. 物理学报, 2009,58(3):1 446-1 455.
Tang Liangrui, Li Jing, Fan Bing. A new four dimensional hyperchaotic system and its circuit simulation [J]. Acta Physica Sinica, 2009, 58(3):1 446-1 455. (in Chinese)

[10] Qi G Y, Michaël A, Barend J, et al. A new hyperchaotic system and its circuit implementation [J]. Chaos Solitons Fract, 2009, 40(5): 2 544-2 549.

[11] Milanovic V, Zaghloul M E. Improved masking algorithm chaotic communications systems [J]. Electronic Letters, 1996, 32(1): 11-12.

[责任编辑: 刘　健]