

Genesisio 混沌系统的非线性反馈同步 及其在保密通信中的应用

陈茂银, 韩正之

(上海交通大学自动化系, 智能工程研究室, 上海 200030)

摘 要: 本文基于 Genesisio 混沌系统的有界状态变量, 提出了一种迭代变换, 实现了混沌同步保密通信. 并且利用线性稳定性理论, 对接收系统设计反馈控制律, 使发射系统和接收系统达到混沌同步, 保证了信号的精确复现. 基于 Genesisio 系统的同步通信系统的计算机仿真, 验证了本文的结果.

关键词: Genesisio 系统; 混沌同步; 非线性反馈; 保密通信

中图分类号: TP273, TN918 文献标识码: A 文章编号: 0372-2112 (2002) 10 1477-04

Nonlinear Feedback Synchronization Method of Chaotic Genesisio System with Application to Secure Communication

CHEN Maoyin, HAN Zhengzhi

(Department of Automation, Shanghai Jiaotong University, Intelligent Engineering Laboratory, Shanghai, 200030, China)

Abstract: Based on variables of chaotic Genesisio system, one iteration transformation is proposed to realize secure communications. With the help of stability theory of linear system, a feedback controller is designed to make receiving system synchronize transmitting system. Furthermore, the transmitted signal is resovered with high quality. The result of this paper is verified by computer simulation.

Key words: Genesisio system; chaos synchronization; nonlinear feedback; secure communications

1 引言

混沌系统具有对初始条件极其敏感的特性, 即使两个完全相同的自治混沌系统, 当系统的初始条件有一微小差异时, 两个系统的运动轨道在同一相空间中将会变得毫不相关. 但是, Pecora 和 Carroll 发现, 一个混沌系统的某些相同的子系统在特定的条件下可以相互同步^[1]. 特别是混沌系统的高度随机性和宽带特性, 使得混沌同步在保密通信、扩频通信等领域显示了良好的应用前景^[1-9], 成为近年来混沌系统研究的主要课题. Genesisio 提出了一种由三个简单的常微分方程以及一个简单非线性项组成的混沌系统^[2]. 在众多的混沌系统同步方案中, Genesisio 混沌系统很少被用来进行保密通信. 本文针对 Genesisio 混沌系统, 提出了一种非线性反馈同步方法, 并将这种方法应用到保密通信. 利用 Genesisio 的两个有界状态变量, 提出了一种迭代变换, 并且利用线性系统的稳定性理论证明了同步的渐近稳定性. 同时给出基于 Genesisio 系统的同步通信系统的计算机仿真结果, 验证了非线性反馈同步的有效性. 而且, 接收系统可以精确地复现信号. 发射系统发射的驱动信号是由发射系统两个状态的组合而成. 这使信号更难破译. 本文中的混沌同步保密通信的框图为图 1.

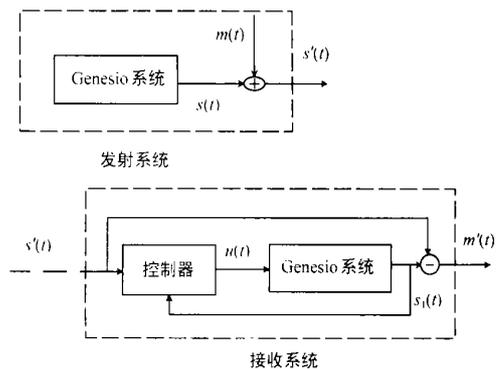


图 1 Genesisio 系统非线性同步保密通信示意图

2 反馈混沌同步方法

利用如下的 Genesisio 系统

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = -\alpha x - by - \alpha + x^2 \end{cases} \quad (1)$$

来实现混沌同步. 其中 a, b, c 是正的常数, 并且 $ab < c$.

在本文中,我们将发射系统的前两个状态的线性组合 $s(t) = s(x(t), y(t))$ 发送到接收系统.在接收端,利用接收到的信息以及接收系统的状态组合 $s_1(t) = (x_1(t), y_1(t))$ 来设计控制律 $u(t) = u(s(t), s_1(t))$,实现接收系统和发射系统的混沌同步.因此,接收系统为

$$\begin{cases} \dot{x}_1 = y_1 \\ \dot{y}_1 = z_1 \\ \dot{z}_1 = -cx_1 - by_1 - \alpha_1 + x_1^2 + u(t) \end{cases} \quad (2)$$

在控制律作用下,接收系统和发射系统实现同步时,有

$$\lim_{t \rightarrow \infty} |x_1 - x| = 0, \lim_{t \rightarrow \infty} |y_1 - y| = 0, \lim_{t \rightarrow \infty} |z_1 - z| = 0$$

在进行同步通信时,小信号 $m(t)$ 直接与驱动信号 $s(t)$ 相加混合在一起发送到接收系统.在接收端,设计控制律 $u(t) = u(s'(t), s_1(t))$.当实现同步通信时,不仅有 $\lim_{t \rightarrow \infty} |x_1 - x| = 0, \lim_{t \rightarrow \infty} |y_1 - y| = 0, \lim_{t \rightarrow \infty} |z_1 - z| = 0$, 而且有 $\lim_{t \rightarrow \infty} |m'(t) - m(t)| = 0$.其中 $m'(t)$ 为复现信号.

3 控制器设计

在本节中,先对三阶系统提出一种迭代变换,然后对 Genesio 系统设计反馈同步控制律,最后证明 Genesio 混沌同步系统的渐近稳定性.

3.1 迭代变换

考虑如下的三阶连续系统

$$\begin{cases} \dot{x}_1 = y_2 \\ \dot{x}_2 = z_3 \\ \dot{x}_3 = -\alpha_0 x_1 - \alpha_1 x_2 - \alpha_2 x_3 \end{cases} \quad (3a)$$

其中 α_i 是系统参数,且 $\alpha_{1,2} > 0$.多项式 $s^3 + \alpha_2 s^2 + \alpha_1 s + \alpha_0$ 不一定是 Hurwitz 稳定的.

定义迭代变换式 $s(t) = x_2 + wx_1$ (4)

因此 $\dot{x}_1 + wx_1 = s(t)$.这里,参数 w 是大于零的数.从控制的角度看, $s(t)$ 可以看成系统 $\dot{x}_1 + wx_1 = u_1(t)$ 的控制作用.于是

$$x_1 = e^{-wt} x_1(0) + e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau$$

求 x_1 的一阶、二阶和三阶导数,得

$$\begin{aligned} \dot{x}_1 &= (-w) e^{-wt} x_1(0) + (-w) e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau + s(t) \\ \ddot{x}_1 &= (-w)^2 e^{-wt} x_1(0) + (-w)^2 e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau \\ &\quad + (-w) s(t) + \dot{s}(t) \\ x_1^{(3)} &= (-w)^3 e^{-wt} x_1(0) + (-w)^3 e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau \\ &\quad + (-w)^2 s(t) + (-w) \dot{s}(t) + \ddot{s}(t) \end{aligned} \quad (5)$$

代入式(3a),得

$$\dot{s} + [(-w) + \alpha_2] s + s[(-w)^2 + \alpha_2(-w) + \alpha_1] + e^{-wt} \left(\int_0^t e^{w\tau} s(\tau) d\tau + x_1(0) \right) [(-w)^3 + \alpha_2(-w)^2 + \alpha_1(-w) + \alpha_0] = 0$$

令 $\Delta = (-w)^3 + \alpha_2(-w)^2 + \alpha_1(-w) + \alpha_0, (-w) + \alpha_2 = \beta_1$ 和 $(-w)^2 + \alpha_2(-w) + \alpha_1 = \beta_0$

所以系统式(3a)变为

$$\dot{s} + \beta_1 s + s\beta_0 + e^{-wt} \left(\int_0^t e^{w\tau} s(\tau) d\tau + x_1(0) \right) \Delta = 0 \quad (6a)$$

注1:如果系统式(3a)形如

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = x_3 \\ \dot{x}_3 = -\alpha_0 x_1 - \alpha_1 x_2 - \alpha_2 x_3 - x_1 f(x_1, x_2, x_3) \end{cases} \quad (3b)$$

其中 $\alpha_{1,2} > 0$.令 $s(t) = x_2 + wx_1, \Delta = (-w)^3 + \alpha_2(-w)^2 + \alpha_1(-w) + \alpha_0 + f, (-w) + \alpha_2 = \beta_1$ 和 $(-w)^2 + \alpha_2(-w) + \alpha_1 = \beta_0$

那么,经过迭代变换后的系统为

$$\dot{s} + \beta_1 s + s\beta_0 + e^{-wt} \left(\int_0^t e^{w\tau} s(\tau) d\tau + x_1(0) \right) \Delta = 0 \quad (6b)$$

注2:式(3a)和(6a)、(3b)和(6b)不一定是等价的.然而,如果系统式(3a)或(3b)是混沌系统,则式(3a)和(6a)、(3b)和(6b)是等价的.这是因为混沌系统对初始条件极其敏感以及映射 $s: (x_1(t), x_2(t)) \rightarrow s(t)$

$$(x_1(t), x_2(t)) \rightarrow s(t) = x_2(t) + wx_1(t)$$

和逆映射 $s^{-1}: s(t) \rightarrow (x_1(t), x_2(t))$

$$x_1 = e^{-wt} x_1(0) + e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau,$$

$$x_2 = (-w) e^{-wt} x_1(0) + (-w) e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau + s(t)$$

都是同胚映射.

3.2 同步控制律设计

为了实现系统同步,对发射系统,定义 $s(t) = y + wx$.相应地,对接收系统,定义 $s_1(t) = y_1 + wx_1$.参数 w 取相同的值.定义系统误差

$$e_1(t) = x_1(t) - x(t), e_2(t) = y_1(t) - y(t),$$

$$e_3(t) = z_1(t) - z(t)$$

系统式(2)减系统式(1),得误差系统

$$\begin{cases} \dot{e}_1 = e_2 \\ \dot{e}_2 = e_3 \\ \dot{e}_3 = -ce_1 - be_2 - \alpha e_3 + e_1(x_1 + x) + u(t) \end{cases} \quad (7)$$

一般的,Genesio 混沌系统的参数 $a, b, c > 0$.令

$$s_e(t) = e_2 + we_1 = s_1(t) - s(t), \text{参数 } w > 0$$

对误差系统式(7)进行迭代变换,得

$$\dot{s}_e + \beta_1 s_e + s\beta_0 + e^{-wt} \left(\int_0^t e^{w\tau} s_e(\tau) d\tau + e_1(0) \right) \Delta = u(t) \quad (8)$$

其中 $\Delta = (-w)^3 + a(-w)^2 + b(-w) + c - (x_1 + x), (-w) + a = \beta_1$ 和 $(-w)^2 + a(-w) + b = \beta_0$.又因为

$$x_1 = e^{-wt} x_1(0) + e^{-wt} \int_0^t e^{w\tau} s_1(\tau) d\tau \text{ 和}$$

$$x = e^{-wt} x(0) + e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau$$

因此,式(8)变为

$$\begin{aligned} \dot{s}_e + \beta_1 s_e + s\beta_0 + e^{-wt} \left(\int_0^t e^{w\tau} (s_1(\tau) - S(\tau)) d\tau + (x_1(0) - x(0)) \right) \times [\Lambda - (e^{-wt} x_1(0) + e^{-wt} \int_0^t e^{w\tau} s_1(\tau) d\tau) - (e^{-wt} x(0) + e^{-wt} \int_0^t e^{w\tau} s(\tau) d\tau)] = u(t) \end{aligned} \quad (9)$$

其中 $\Lambda = (-w)^3 + a(-w)^2 + b(-w) + c$. 因此, 控制律取

$$u(t) = e^{-wt} \int_0^t e^{w\tau} (s_1 - s) d\tau [(-w)^3 + a(-w)^2 + b(-w) + c] - e^{-wt} \int_0^t e^{w\tau} (s_1 + s) d\tau \quad (10)$$

所以, 式(9)变为

$$\begin{aligned} \ddot{s}_e + \beta_1 \dot{s}_e + s_e \beta_0 &= e^{-2wt} \int_0^t e^{w\tau} s_e(\tau) d\tau (x_1(0) + x(0)) \\ &- e^{-wt} (x_1(0) - x(0)) \Lambda + e^{-2wt} (x_1(0) \\ &+ x(0)) (x_1(0) - x(0)) + e^{-2wt} (x_1(0) \\ &- x(0)) \int_0^t e^{w\tau} (s_1 + s) d\tau \end{aligned} \quad (11)$$

为了保证系统式(11)的原点是渐近稳定的, 要适当地选取参数 $w > 0$, 使系数 $\beta_1, \beta_0 > 0$. 这里系统参数 $a, b, c > 0$. 由 Hurwitz 稳定性判据^[7], 可以根据下面的式子选取 w :

- (1) 如果 $a^2 - 4b < 0, w \in (0, a)$;
- (2) 如果 $a^2 - 4b = 0, w \in (0, a/2) \cup (a/2, a)$;
- (3) 如果 $a^2 - 4b > 0, w \in (0, (a - \sqrt{a^2 - 4b})/2) \cup ((a + \sqrt{a^2 - 4b})/2, a)$

定理 1 对于混沌发射系统(1)和接收系统(2), 发射系统发射的驱动信号为 $s(t) = y + wx$, w 根据式(12)来选取. 如果对接收系统施加控制律(10), 误差系统(7)在原点一致渐近稳定, 即发射系统(1)和接收系统(2)同步, 故有

$$\lim_{t \rightarrow \infty} |x_1 - x| = 0, \lim_{t \rightarrow \infty} |y_1 - y| = 0, \lim_{t \rightarrow \infty} |z_1 - z| = 0$$

证明 因为 Genesis 混沌系统状态的有界性, 假设

$\sup_{t > 0} \max(|x_1|, |x|) \leq M_x, \sup_{t > 0} \max(|y_1|, |y|) \leq M_y$, 式(11)介于上界系统

$$\ddot{s}_e + \beta_1 \dot{s}_e + s_e \beta_0 = e^{-wt} [8M_x(M_x + wM_y)t + 2M_x\Lambda + 4M_x^2]$$

和下界系统

$$\ddot{s}_e + \beta_1 \dot{s}_e + s_e \beta_0 = -e^{-wt} [8M_x(M_x + wM_y)t + 2M_x\Lambda + 4M_x^2]$$

之间. 参数 w 根据式(12)来选取. 所以两个系统均是原点渐近稳定的, 故随着时间的推移, 两个系统中的 s_e 均趋于原点. 根据微分方程比较定理^[8], 式(7)是原点一致渐近稳定的, 即 $\lim_{t \rightarrow \infty} s_e(t) = 0$. 这也意味着 $\lim_{t \rightarrow \infty} (e_2(t) + we_1(t)) = 0$. 由式(7)得

$$\lim_{t \rightarrow \infty} e_1(t) = 0, \lim_{t \rightarrow \infty} e_2(t) = 0, \lim_{t \rightarrow \infty} e_3(t) = 0$$

所以 $\lim_{t \rightarrow \infty} |x_1 - x| = 0, \lim_{t \rightarrow \infty} |y_1 - y| = 0, \lim_{t \rightarrow \infty} |z_1 - z| = 0$.

也就是说, 接收系统(1)和发射系统(2)达到同步效果.

定理 2 对于混沌发射系统(1)和接收系统(2), 发射系统发射的驱动信号为 $s(t) = y + wx$, 信号 $m(t)$ 与驱动信号相比幅值较小, 且有界, 即 $\sup_{t > 0} (|m(t)|) \leq M$. 参数 w 根据式(12)来选取. 控制律取为

$$u(t) = e^{-wt} \int_0^t e^{w\tau} (s_1 - s') d\tau [(-w)^3 + a(-w)^2 + b(-w) + c] - e^{-wt} \int_0^t e^{w\tau} (s_1 + s') d\tau \quad (13)$$

其中 $s'(t) = s(t) + m(t)$. 在接收端, 复现信号为 $m'(t) = s'(t) - s_1(t)$. 如果对接收系统施加控制律式(13)时, $m'(t)$ 渐近地趋于 $m(t)$, 即 $\lim_{t \rightarrow \infty} |m'(t) - m(t)| = 0$.

证明 与定理 1 的证明类似.

因为 $\sup_{t > 0} (|m(t)|) \leq M, \sup_{t > 0} \max(|x_1|, |x|) \leq M_x$,

$\sup_{t > 0} \max(|y_1|, |y|) \leq M_y$, 受控的误差系统(7)介于上界系统

$$\ddot{s}_e + \beta_1 \dot{s}_e + s_e \beta_0 = e^{-wt} [8M_x(M_x + wM_y + M)t + 2M_x\Lambda + 4M_x^2]$$

和下界系统

$$\ddot{s}_e + \beta_1 \dot{s}_e + s_e \beta_0 = -e^{-wt} [8M_x(M_x + wM_y + M)t + 2M_x\Lambda + 4M_x^2]$$

之间. 根据微分方程比较定理^[8], 误差系统(7)是原点一致渐近稳定的, 即 $\lim_{t \rightarrow \infty} s_e(t) = 0$. 这也意味着 $\lim_{t \rightarrow \infty} (e_2(t) + we_1(t)) = 0$. 由系统(7)得

$$\lim_{t \rightarrow \infty} (s_1(t) - s(t)) = 0$$

所以 $\lim_{t \rightarrow \infty} m'(t) = \lim_{t \rightarrow \infty} (s'(t) - s_1(t)) = \lim_{t \rightarrow \infty} (s(t) + m(t) - s_1(t)) = \lim_{t \rightarrow \infty} m(t)$, 故 $m'(t)$ 渐近地趋于 $m(t)$.

注 3: 小信号 $m(t)$ 与发射系统(1)的两个状态组合在一起, 这有利于提高信号的保密性能.

注 4: 参数 w 可以在 $(0, a)$ 内自由选取. 如果 a 比较大, 则可以选取较大的 w , 使 $m'(t)$ 能够在较短的时间内渐近地趋于 $m(t)$.

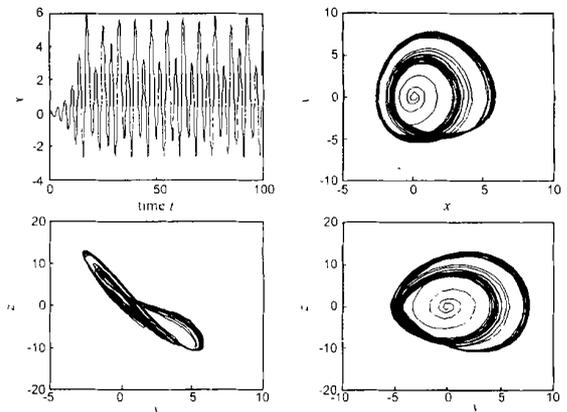


图 2 状态 x 的时间历程以及混沌吸引子

4 数值仿真

对 Genesis 系统取参数 $a = 1.2, b = 2.92$ 和 $c = 6$ 时, 系统是混沌的^[2]. 发射系统和接收系统的初始条件分别取为 $(0.2, 0.1, -0.2)^T, (-0.5, 0.8, 0.4)^T$. 参数 $w = 0.7$. 发射系统状态 x 的时间历程以及混沌吸引子如图 2 所示. 在接收端施加反馈同步控制律后, 系统同步误差变量 e_1, e_2 的对数曲线如图 3 所示. 从图 3 可以看出, 同步误差曲线渐近衰减为零. 当 $t = 40s$, 误差的数量级为 -5 ; 当 $t = 60s$, 误差的数量级为 -7 , 同步速度较快. 图 4 表示同步信号的李萨图形以及反馈控制律曲线. 从图 4 可以看出, 控制律在 $t = 25s$ 左右时等于零. 图 5 表明利用两个混沌状态的组合来进行保密通讯时, 信号更难破译. 图 6 分别是当 $t \in [65, 70]$ 时的信号和复现信号. 信号取为 $0.1 \sin(20t)$. 从图 6 可以看出, 信号复现的精确度较高.

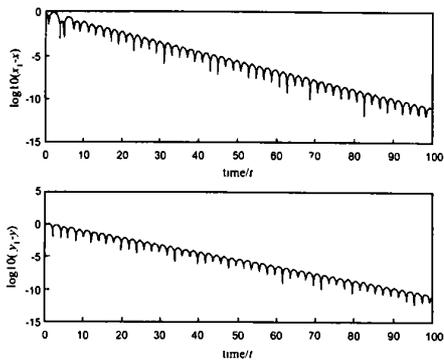
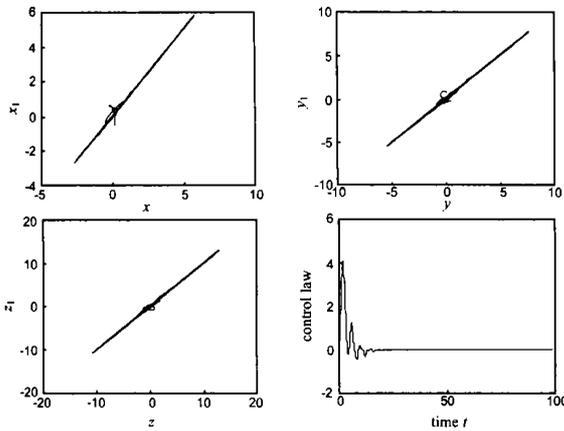
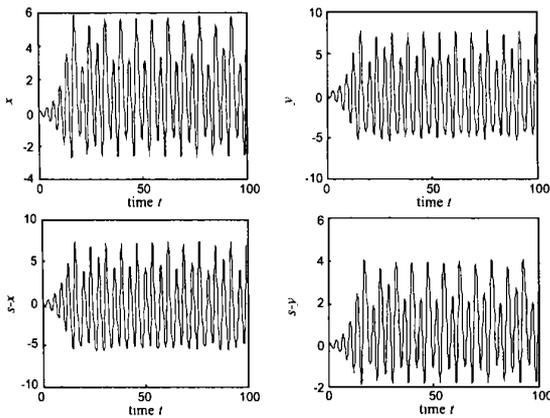
图3 误差变量 e_1 , e_2 的对数曲线

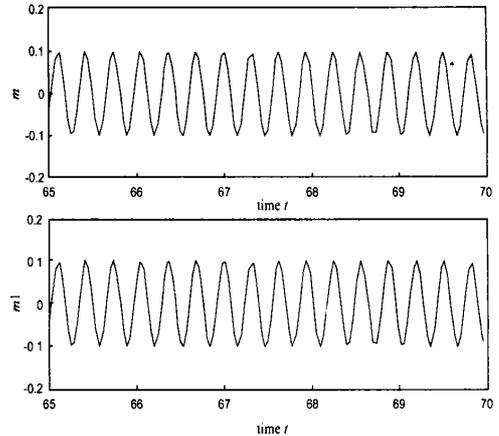
图4 李萨育图形以及反馈控制律曲线

图5 状态 x , y 以及与 s 的差别

5 结论

本文针对 Genesio 系统, 提出了一种非线性反馈同步控制方法, 并将这种方法应用到混沌同步保密通信中. 首先, 利用 Genesio 系统的有界状态变量进行迭代变换; 然后, 利用线性稳定性理论设计控制器, 并证明了同步的渐近稳定性. 最后, 给出了基于 Genesio 混沌系统的计算机仿真结果, 验证了非线性反馈同步的有效性. 在接收端, 可以精确地复现发送的信号, 而且信号与发射系统的两个状态组合在一起, 这使信号更

难破译, 有利于保密通信.

图6 信号 $m(t)$ 以及复现信号 $m'(t)$

参考文献:

- [1] L M, Pecora, T L Camoll. Synchronization in chaotic systems [J]. Phys. Rev. Lett., 199, 64(8): 821- 824.
- [2] R Genesio, A Tesi. Harmonic balance methods for the analysis of chaotic dynamics in nonlinear systems [J]. Automatica, 1992, 28(3): 531- 548.
- [3] 蒋国平, 王锁萍. 蔡氏混沌电路的单向耦合同步研究 [J]. 电子学报, 2000, 28(1): 67- 69.
- [4] Wu C W, Chua L O. A unified framework for synchronization and control of dynamical systems [J]. Int. J. Bif. & Chaos, 1994, 4(4): 979- 998.
- [5] 刘锋, 陈小利等. 混沌系统的反馈同步及其在保密通讯中的应用 [J]. 电子学报, 2000, 28(8): 46- 48.
- [6] Omer Morgul, Moez Feki. A chaotic masking scheme by using synchronized chaotic systems [J]. Phys. Lett. A., 1999, 251(3): 168- 176.
- [7] 吴麒. 自动控制原理 [M]. 北京: 清华大学出版社, 1999.
- [8] 许淞农. 常微分方程稳定性理论 [M]. 上海市: 上海科学技术出版社, 1961.

作者简介:



陈茂银 男, 1975 年生于山东省莱芜县, 上海交通大学电子信息学院自动化系博士, 1997 年毕业于山东曲阜师范大学自动化所, 获硕士学位, 现在的主要研究方向为混沌系统的控制、同步及其相关应用.

韩正之 1947 年出生于浙江, 上海交通大学电子信息学院自动化系博士生导师, 主要研究方向为非线性控制、智能信息系统与混沌系统的控制.