文章编号: 1000−8152(2008)04−0794−05

统一混沌系统的混沌观测器同步控制及其应用

孙克辉[1], 牟 俊[2], 周家令[1], 钟 科[1]

(1. 中南大学 物理科学与技术学院, 湖南 长沙 410083; 2. 大连轻工业学院 信息科学与工程学院, 辽宁 大连 116034)

摘要: 根据连续时间混沌系统可由单变量及其导数重构相空间的原理, 采用混沌观测器同步方法, 研究了统一混沌系统的同步控制问题. 基于连续系统的稳定性准则, 提出了统一混沌系统的混沌观测器同步定理. 将该同步方法应用于保密通信, 设计了基于时分复用的混沌掩盖保密通信新方案, 并对该方案的保密性能进行了分析. 基于MATLAB的数值仿真结果证明了同步控制方法和保密通信方案的有效性.

关键词: 混沌观测器; 统一混沌系统; 时分复用; 混沌掩盖

中图分类号: TP273 **文献标识码**: A

Synchronization control and its application for the unified chaotic system based on chaos observer

SUN Ke-hui[1], MOU Jun[2], ZHOU Jia-ling[1], ZHONG Ke[1]

(1. School of Physic Science and Technology, Central South University, Changsha Hunan 410083, China
2. School of Information Science and Engineering, DaLian Institute of Light Industry, Dalian Liaoning 116034, China)

Abstract: According to the principle of phase-space reconstruction of a continuous time chaotic system by a single variable and its derivative, the synchronization of a unified chaotic system is investigated by employing the chaos observer synchronization method. A theorem about chaos observer synchronization of unified chaotic system is put forward based on the stability rule for continuous systems. Applying this synchronization method to security communications, we designed a new scheme of chaotic masking security communications based on the technology of time division multiple, and carried out its performance analysis. Simulation results on Matlab 6.5 confirm that both the synchronization approach and the security communications scheme are effective.

Key words: chaos observer; unified chaotic system; time division multiple(TDM); chaos masking

1 引言(Introduction)

自1990年Pecora和Carroll[1]提出驱动–响应法实现混沌系统同步以来, 混沌同步理论及其在保密通信领域的应用成为非线性科学的研究热点[2]. 文献[3]研究了只含一个非线性项的观测器问题, 但观测器的设计使用了系统的多个状态变量或全部状态变量, 而系统的所有状态变量并非都能用物理方法测量出来, 另外, 有些混沌系统含有多个非线性项. 文献[4]研究了一类3维混沌系统吸引子的可观测性问题, 得出了利用系统标量输出及其对时间的导数可以对吸引子进行观测的结论, 为通过设计具有物理意义的混沌系统观测器实现同步控制提供了理论依据. 最近, 吕金虎、陈关荣等人提出了具有单参数、全域性混沌特性的统一混沌系统[5], 已成为研究混沌控制和同步以及混沌保密通信的新模型, 在保密通信领域具有广泛应用前景[6].

本文以统一混沌系统为研究对象, 通过利用单变量驱动混沌观测器研究统一混沌系统的同步问题, 并设计了基于时分复用的混沌掩盖保密通信新方案, 在MATLAB6.5仿真平台上, 对混沌观测器同步方法和保密通信方案进行了动态仿真.

2 基于混沌观测器的同步控制原理(Principle of synchronization control based on chaos observer)

2.1 混沌观测器设计原理(Principle of chaos observer design)

对于如下混沌系统

$$\begin{cases} \dot{x} = F(x), \\ s = h(x), \end{cases} \tag{1}$$

收稿日期: 2006−02−24; 收修改稿日期: 2007−01−05.
基金项目: 国家自然科学基金资助项目(60672041); 中南大学文理基金资助项目(0601053).

其中: $t \in \mathbb{R}^n$, $F: \mathbb{R}^n \to \mathbb{R}^n$, s是系统的标量输出. 设$k(x)$是一个标量可微函数, $V(x)$是一个矢量场, $V: \mathbb{R}^n \to \mathbb{R}^n$. 标量可微函数$k(x)$沿矢量场$V(x)$的李导数定义为$L_v k$, 则$L_v k =< V(x), \mathrm{grad}\, k(x) >$, 其中$<,>$为欧几里德内积, 标量可微函数$k(x)$沿矢量场$V(x)$的第$i$次李导数定义为$L_v^i k =< V(x), \mathrm{grad}\, L_v^{i-1} k(x) >$.

引理 1 [4]　如果映射$\phi = [h(x), L_f h(x), \cdots, L_f^{(n-1)} h(x)]$是微分同胚的, 则利用标量输出$s$和它的$i(i \leqslant n-1)$次李导数可以观测混沌系统(1)的所有状态变量, 同时 $x = \phi^{(-1)}[s(t), s^{(1)}(t), \cdots, s^{(n-1)}(t)]^{\mathrm{T}}$.

如果选择某一状态变量作为系统(1)的输出, 则系统(1)其余状态变量可表示为$x_j = g_i(x_i, \dot{x}_i, \cdots, x_i^{(n-1)})$, 其中$j \neq i$, 故系统(1)可改写为

$$\dot{x} = Ax + g(x_i, \dot{x}_i, \cdots, x_i^{(n-1)}). \tag{2}$$

其中: A为常数矩阵, $g(x_i, \dot{x}_i, \cdots, x_i^{(n-1)})$ 是包含了系统(1)的所有非线性项的$n \times 1$阶矩阵.

引理 2 [7]　设系统(1)的输出为

$$\begin{aligned} s(x) = {} & g(x_i, \dot{x}_i, \cdots, x_i^{(n-1)}) + \\ & B \times [g_1(x_i, \dot{x}_i, \cdots, x_i^{(n-1)}), \cdots, \\ & x_i, \cdots, g_n(x_i, \dot{x}_i, \cdots, x_i^{(n-1)})]^{\mathrm{T}}. \end{aligned} \tag{3}$$

其中: $B = \mathrm{diag}\{b_1, b_2, \cdots, b_n\}$, 若适当选择对角矩阵$B$, 使矩阵$A - B$的特征值具有负实部, 则系统$\dot{y} = F(y) + s(x) - s(y)$是混沌系统(1) 的混沌观测器. 其中

$$\begin{aligned} s(y) = {} & g(y_i, \dot{y}_i, \cdots, y_i^{(n-1)}) + \\ & B \times [g_1(y_i, \dot{y}_i, \cdots, y_i^{(n-1)}), \cdots, \\ & y_i, \cdots, g_n(y_i, \dot{y}_i, \cdots, y_i^{(n-1)})]^{\mathrm{T}}. \end{aligned} \tag{4}$$

2.2　统一混沌系统的混沌观测器设计(Design of chaos observer based on unified chaos system)

2002年, 吕金虎、陈关荣等人提出了一个新的混沌系统, 该系统将Lorenz吸引子和Chen吸引子连接起来, 而文献[8]提出的Lü系统只是它的一个特例, 故文献[5]称其为统一混沌系统. 统一混沌系统的数学模型$\dot{x} = F(x)$可写为

$$\begin{cases} \dot{x}_1 = (25\alpha + 10)(x_2 - x_1), \\ \dot{x}_2 = (28 - 35\alpha)x_1 - x_1 x_3 + (29\alpha - 1)x_2, \\ \dot{x}_3 = x_1 x_2 - (\alpha + 8)x_3/3. \end{cases} \tag{5}$$

当参数$\alpha \in [0, 1]$时, 系统处于混沌态. 统一混沌系统是一个由单参数控制的连续混沌系统, 具有统一性和全域性混沌特性. 系统只用一个参数α就可以控制整个系统, 根据VANĚČEK和ČELIKOVSKY在文献[9]中的定义, 当$\alpha \in [0, 0.8)$时, 统一系统属于广义Lorenz系统; 当$\alpha \in (0.8, 1]$时, 统一系统属于广义Chen系统; 而当$\alpha = 0.8$时, 统一系统属于Lü系统, 当α由零逐渐增加到1时, 系统也由广义的Lorenz系统逐渐过渡到广义的Chen系统, 具有统一性.

选择x_1作为系统(5)的输出变量, 则

$$\begin{cases} x_1 = g_1(x_1, \dot{x}_1, \ddot{x}_1) = x_1, \\ x_2 = g_2(x_1, \dot{x}_1, \ddot{x}_1) = \dot{x}_1/(25\alpha + 10) + x_1, \\ x_3 = g_3(x_1, \dot{x}_1, \ddot{x}_1) = \\ [-\ddot{x}_1/(25\alpha + 10) + \dot{x}_1(4\alpha - 11)/(25\alpha + \\ 10) + (27 - 6\alpha)x_1]/x_1. \end{cases} \tag{6}$$

其中$x_1 \neq 0$. 将式(5)改写为

$$\dot{x} = Ax + g(x_1, \dot{x}_1, \ddot{x}_1). \tag{7}$$

其中:

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

$$g(x_1, \dot{x}_1, \ddot{x}_1) = \begin{bmatrix} 0 \\ \dfrac{\ddot{x} - (4\alpha - 11)\dot{x}}{25\alpha + 10} - (27 - 6\alpha)x_1 \\ \ddot{x}\dot{x}/(25\alpha + 10) + x_1^2 \end{bmatrix}.$$

若选择$s(x) = g(x_1, \dot{x}_1, \ddot{x}_1) + B \times [x_1, g_2(x_1, \dot{x}_1, \ddot{x}_1), g_3(x_1, \dot{x}_1, \ddot{x}_1)]^{\mathrm{T}}$ 为系统(5)的输出, 则统一混沌系统的混沌观测器为

$$\begin{aligned} \dot{y} = {} & F(y) + s(x) - s(y) = \\ & Ay + g(y_1, \dot{y}_1, \ddot{y}_1) + s(x) - s(y). \end{aligned} \tag{8}$$

其中: $s(y) = g(y_1, \dot{y}_1, \ddot{y}_1) + B \times [y_1, g_2(y_1, \dot{y}_1, \ddot{y}_1), g_3(y_1, \dot{y}_1, \ddot{y}_1)]^{\mathrm{T}}$, y_1为接收端混沌观测器的输出, 则混沌观测器的其他变量为

$$\begin{cases} y_1 = g_1(y_1, \dot{y}_1, \ddot{y}_1) = y_1, \\ y_2 = g_2(y_1, \dot{y}_1, \ddot{y}_1) = \dot{y}_1/(25\alpha + 10) + y_1, \\ y_3 = g_3(y_1, \dot{y}_1, \ddot{y}_1) = \\ [-\ddot{y}_1/(25\alpha + 10) + \dot{y}_1(4\alpha - 11)/(25\alpha + \\ 10) + (27 - 6\alpha)y_1]/y_1 \end{cases} \tag{9}$$

以混沌系统(5)为驱动系统, 以混沌观测系统(8)为响应系统, 以x_1为驱动变量, 则可得驱动-响应系统同步的同步定理.

定理 1　设系统(4)的输出为

$$\begin{aligned} s(x) = {} & g(x_1, \dot{x}_1, \ddot{x}_1) + B \times \\ & [x_1, g_2(x_1, \dot{x}_1, \ddot{x}_1), g_3(x_1, \dot{x}_1, \ddot{x}_1)]^{\mathrm{T}}, \end{aligned}$$

其中$B = \mathrm{diag}\{b_1, b_2, b_3\}$, 当$b_3 > -(8 + \alpha)/3$, 且$b_1$和$b_2$同时满足: $b_1 + b_2 + 11 - 4\alpha > 0$, $(b_1 + 25\alpha + 10)(b_2 - 29\alpha + 1) + (35\alpha - 28)(25\alpha + 10) > 0$时,

响应系统(8)与驱动系统(5)可实现渐进同步.

证 定义响应系统与驱动系统的变量误差为$e = y - x$, 则误差系统的动力学方程为

$$\dot{e} = \dot{y} - \dot{x} = F(y) - F(x) + s(x) - s(y). \quad (10)$$

由式(7)和式(8)得

$$\dot{e} = \dot{y} - \dot{x} = (A - B)e. \quad (11)$$

其中

$$A - B = \begin{bmatrix} -25\alpha - 10 - b_1 & 25\alpha + 10 & 0 \\ 28 - 35\alpha & 29\alpha - 1 - b_2 & 0 \\ 0 & 0 & \dfrac{-8 - \alpha - 3b_3}{3} \end{bmatrix}.$$

根据连续系统的稳定性准则可知, 当$b_3 > -(8+\alpha)/3$, 且b_1和b_2同时满足$b_1 + b_2 + 11 - 4\alpha > 0$, $(b_1 + 25\alpha + 10)(b_2 - 29\alpha + 1) + (35\alpha - 28)(25\alpha + 10) > 0$时, 矩阵$A - B$的特征值都具有负实部, 故误差系统(10)在原点处是渐近稳定的, 即有$\lim\limits_{t\to\infty} e = 0$或$\lim\limits_{t\to\infty}(y - x) = 0$, 因此响应系统(8)与驱动系统(5)同步. 证毕.

2.3 同步仿真(Synchronization simulation)

利用MATLAB6.5仿真平台, 对基于统一混沌系统的混沌观测器同步进行仿真研究, 取系统初值分别为: $x_1(0) = 1$, $x_2(0) = 1$, $x_3(0) = 1$; $y_1(0) = 15$, $y_2(0) = 15$, $y_3(0) = 15$; $b_1 = 5$, $b_2 = 24$, $b_3 = 0$; 系统参数$\alpha = 0.8$. 设$|e| = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2 + (y_3 - x_3)^2}$. 由于此时$A - B$矩阵的特征根分别为–35, –2.93, –1.8, 所以同步系统收敛, 同步仿真所得同步误差曲线如图1所示. 可见, 系统约在$t = 2$ s内能实现精确同步.

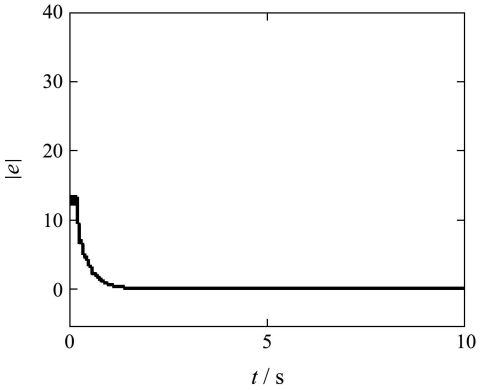


图 1 统一混沌系统的同步误差曲线

Fig. 1 Synchronization error curve of unified chaotic system

3 基于时分复用的混沌掩盖保密通信方案(Scheme of chaos masking secure communication based on time division multiple)

混沌掩盖、混沌参数调制、混沌键控和混沌扩频是目前混沌保密通信研究中竞争最为激烈的4项技术[2].

3.1 时分复用保密通信原理(Principle of secure communication based on TDM)

所谓时分复用就是把时间分割成周期性的帧, 每一帧再分割成若干个时隙, 各路信号占有各自的时隙, 实现在同一信道上传输多路信号的方法. 这里的时分复用有两层含义: 一方面, 在单路信号的传输系统中, 采用时分复用方案实现驱动信号和混沌掩盖信号的交替传输. 设驱动混沌观测器的驱动变量为$x_1(t)$, 而所要发送的有用信号为$m(t)$. 将信号传输分成周期为T 的帧, 驱动变量的抽样周期为$T/2$, 由驱动量与有用信号组成的掩盖信号的抽样周期也为$T/2$, 这样, 驱动信号与混沌掩盖信号交替传输, 单路信号传输的帧结构如图2(a)所示. 另一方面, 在多路信号(n路)的传输系统中, 采用时分复用方案实现多路驱动信号和多路混沌掩盖信号的交替传输. 设某一路驱动混沌观测器的驱动变量为$x_{i1}(t)$, 而所要发送的有用信号为$m_i(t)$. 将信号传输分成周期为$T/2n$的帧, 驱动变量的抽样周期为$T/2n$, 由驱动量与有用信号组成的掩盖信号的抽样周期也为$T/2n$, 这样, 驱动信号与混沌掩盖信号交替传输, 多路信号传输的帧结构如图2(b)所示. 采用时分复用的方式, 不仅可以节省信道资源, 提高系统的有效性, 而且可使信道中的信号更具随机性, 提高系统的安全性.

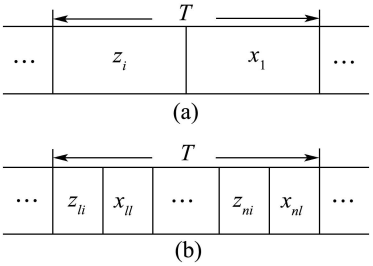


图 2 信道中信号传输的帧格式

Fig. 2 The fame of signal transmission in channel

3.2 混沌保密通信仿真(Simulation of chaos secure communication)

在MATLAB6.5仿真平台上, 采用混沌观测器同步方案, 取驱动量为$x_1(t)$, 设待传输的有用信号$m(t) = 10\sin(0.2t)$, 其波形如图3所示. 为了实现对$m(t)$的保密传输, 将$m(t)$与混沌变量$x_2(t)$实现加性或乘性掩盖, 另外, 为了增强保密性, 对有用信号采用压缩系数$k = 0.01$的比例环节, 即保密信号为$z_1(t) = 0.01m(t) + x_2(t)$或$z_1(t) = 0.01m(t) \cdot x_2(t)$, 当系统参数$\alpha = 0.8$, 系统初值$x_1(0) = 1$, $x_2(0) = 1$, $x_3(0) = 1$, $y_1(0) = 15$, $y_2(0) = 15$, $y_3(0) = 15$, 矩阵元素$b_1 = 5$, $b_2 = 24$, $b_3 = 0$时, 对基于统一混沌系统的混沌保密通信系统进行仿真研究. 按照时分复用混沌掩盖保密通

信方案, 得信道中传输的信号波形如图4所示, 其中图4(a)为信道中加性掩盖信号与混沌信号交替传输波形, 图4(b)为信道中乘性掩盖信号与混沌信号交替传输波形. 采用本文所述同步方法, 在接收端对信号进行去掩盖, 恢复信号波形如图5所示, 其中图5(a)为去加性掩盖后的恢复信号波形, 图5(b)为去乘性掩盖信号后的恢复信号波形. 可见, 除同步建立时间外, 恢复的信号与原有用信号完全一致, 实现了信号的保密传输.

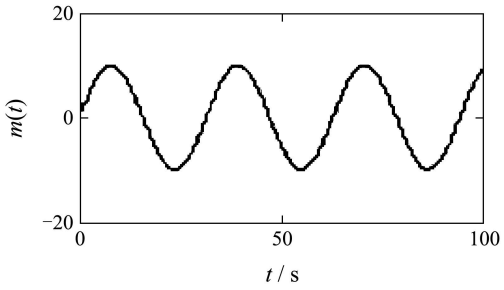
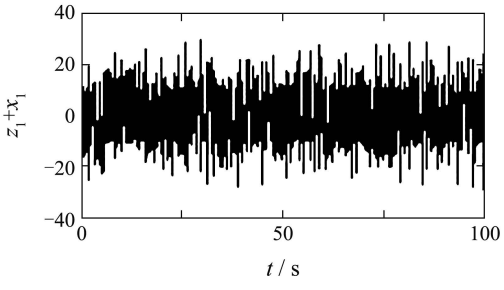
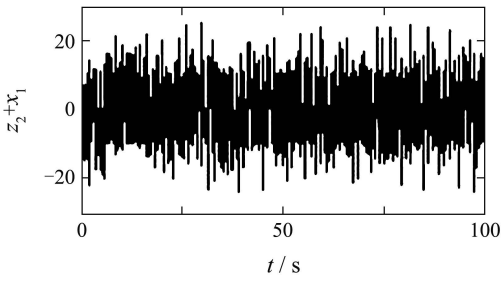


图 3　发送端待传输的有用信号$m(t) = 10\sin(0.2t)$

Fig. 3　The information signal wave in sender



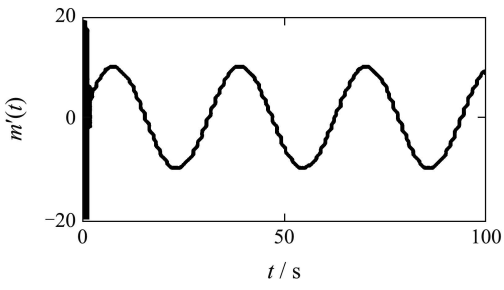
(a) $z_1(t) = 0.01m(t) + x_2(t)$与$x_1(t)$的交替传输信号



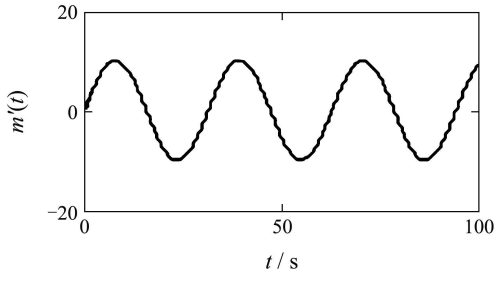
(b) $z_2(t) = 0.01m(t) \cdot x_2(t)$与$x_1(t)$的交替传输信号

图 4　信道中传输的信号波形

Fig. 4　The signal wave in channel



(a) $m'(t) = 100(z_1(t) - x_2(t))$



(b) $m'(t) = 100(z_2(t)/x_2(t))$

图 5　接收端去掩盖后的有用信号波形

Fig. 5　The unmasked signal waver in receiver

3.3　保密性能分析(Analysis of secure performance)

由理论分析和保密通信仿真可知, 采用基于时分复用的混沌掩盖保密通信方式, 信道中传输的信号与随机信号极其相似, 可以很好的达到保密通信的效果. 而接收端解调出的有用信号在混沌系统与状态观测器实现精确同步之前是乱的, 但是实现了精确同步后, 即可精确恢复出原有用信号. 系统的保密性体现在以下几个方面:

1) 采用压缩系数$k = 0.01$的比例环节, 确保了混沌载波对信息信号的有效掩盖, 使得信道中传输的已调信号呈现混沌类噪声波形, 从而实现信息的加密传输.

2) 采用乘性或加性掩盖方式, 驱动变量与掩盖变量分开, 提高了系统的保密性.

3) 采用时分复用方式, 增加了信道中信号的复杂性, 避免了多信道传输, 提高了传输效率.

4) 密钥空间大, 抗破译能力强. 密钥空间的大小直接关系到保密系统的安全性能, 在此方案中, 不同参数的统一混沌系统可以产生不同的混沌信号, 所以混沌系统参数α可作为密钥; 由于混沌系统对初值敏感, 故初值x_0可以作为密钥; 掩盖有用信号的掩盖变量也可作为密钥; 此外, 掩盖方式(加密函数z)和数据复用方式也可作为密钥, 故密钥空间大. 若计算机字长32位, 精度为10^{-14}, 在本文提出的保密通信方案中, 选择参数α和系统初始值$x_1(0), x_2(0), x_3(0)$作为密钥, 则此时穷举密钥空间约为2^{208}, 而目前常用的3DES的密钥空间也只有2^{168}. 可见该方案的密钥空间巨大, 足以抵抗穷举攻击.

此外, 由于在信道中的信号经有用信号和混沌信号掩盖, 同步驱动变量与混沌掩盖变量交替传输, 以及比例压缩和时分复用传输后, 使基于预测和回归映射的破译方法失效[10].

4 结论(Conclusion)

本文采用混沌观测器方法, 设计了统一混沌系统的混沌观测器同步方案, 并在此基础上设计了时分复用混沌保密通信方案, 实现了基于混沌观测器同步的保密通信. 该同步方案的优点是不需计算同步系统的条件Lyapunov指数, 驱动信号为任意的单个混沌变量. 时分复用保密通信方案的优点是采用单信道传输, 传输效率高; 信道传输信号为类似随机信号, 安全性高. 仿真结果表明, 同步方案同步建立时间短, 同步的动态性能好; 保密通信方案达到了预期的效果. 如何提高该混沌保密通信系统的同步性能和抗破译能力将是作者下一步研究内容.

参考文献(References):

[1] PECORA L M, CARROLL T L. Synchronization in chaotic system[J]. *Physical Reveiw Letters*, 1990, 64(8): 821 – 824.

[2] 方锦清. 驾驭混沌与发展高新技术[M]. 北京: 原子能出版社, 2002.

[3] GRASSI G, MASCOLO S. Nonlinear observer design to synchronize hypechaotic systems via a scalar signal[J]. *IEEE Transactions on Circuits and Systems*, 1997, 44(10): 1101 – 1104.

[4] YANG S X. On observability of 3D continuous-time autonomous chaotic systems based on scalar output measurement[J]. *International Journal of Bifurcation and Chaos*, 2002, 12(5): 1159 – 1162.

[5] LÜ J H, CHEN G R, CHENG D Z, et al. Bridge the gap between the Lorenz system and the Chen system[J]. *International Journal of Bifurcation and Chaos*, 2002, 12(12): 2917 – 2926.

[6] LU J A, WU X Q, LÜ J H. Synchronization of an unified chaotic system and the application in secure communication[J]. *Physical Letter A*, 2002, 305(6): 365 – 370.

[7] 周平. 一类3维连续混沌系统观测器[J]. 物理学报, 2003, 52(5): 1108 – 1111.
(ZHOU Ping. Observers for a class of 3D continuous chaotic systems [J]. *Acta Physica Sinica*, 2003, 52(5): 1108 – 1111.)

[8] LÜ J H, CHEN G R. A new chaotic attractor coined[J]. *International Journal of Bifurcation and Chaos*, 2002, 12(3): 659 – 661.

[9] VANĚČEK A, ČELIKOVSKY S. *Control Systems: From Linear Analysis to Synthesis of Chaos*[M]. London: Pretice-Hall, 1996.

[10] 赵耿, 郑德玲, 赵林惠. 一类数字混沌保密语音通信系统的保密性能分析[J]. 北京科技大学学报, 2001, 23(3): 287 – 292.
(ZHAO Geng, ZHENG Delin, ZHAO Linhui. Analysis on security of a secure speech communication system based on digital chaos[J]. *Journal of University of Science and Technology Beijing*, 2001, 23(3): 287 – 292.)

作者简介:

孙克辉 (1968—), 男, 教授, 博士, 研究方向为混沌同步及其保密通信研究, E-mail: kehui@mail.csu.edu.cn;

牟 俊 (1981—), 男, 硕士研究生, 研究方向为混沌保密通信;

周家令 (1979—), 男, 硕士研究生, 研究方向为混沌保密通信;

钟 科 (1980—), 男, 硕士研究生, 研究方向为OFDM通信.