第 58 卷 第 3 期 2009 年 3 月
1000-3290/2009/58(03)/1467-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.3,March,2009

基于一阶时滞混沌系统参数辨识的保密通信方案*

王明军 王兴元†

(大连理工大学电子与信息工程学院,大连 116024)

(2008 年 6 月 9 日收到;2008 年 9 月 10 日收到修改稿)

基于参数调制原理,针对一阶时滞 Logistic 混沌系统设计了相应的参数观测器,仅传递单路信号就可以成功辨识出系统中的未知参数,从而恢复出调制在参数中的模拟信号,并在此基础上采用不同频率信号代替‘0’或‘1’,设计出具体的数字保密通信方案.数值仿真验证了本方法的有效性.

关键词:观测器,混沌保密通信,参数调制,滤波

PACC:0545,0555

1. 引 言

1990 年,Pecora 和 Corroll 提出了“混沌同步”的概念,并在电路实验中实现了两个耦合混沌系统的同步[1,2].由于混沌同步在保密通信、信号处理和生命科学等方面有十分广泛的应用前景和巨大的市场潜在价值,引起了人们极大的关注,并对此进行了广泛深入地研究[3—6].迄今已提出并实现了基于同步的混沌保密通信方案有 Oppenheim 和 Kocarev 等的混沌遮掩保密通信[7,8];Dedieu 等的混沌开关保密通信[9];Halle 等的混沌调制保密通信[10];Sushchik 等的脉冲位置调制保密通信[11].尤其是最近几年,人们在混沌保密通信方面做了许多工作[12—16],还提出了无需同步的保密通信技术[17],进一步扩大了混沌在保密通信中应用的范围.彭海朋等实现了一阶时滞 Logistic 混沌系统的参数辨识[18],本文在此基础上,将有用信号调制在一阶时滞 Logistic 混沌系统的参数中,通过观测器对未知参数以指数速度加以辨识,恢复出所调制的信号.本保密通信方案只需传递单路信号即可实现,以不同频率的模拟信号代替‘0’或“1”,辅以滤波方法即可实现数字保密通信.数值仿真结果证明了该方法的有效性.

2. 系统描述

一阶时滞 Logistic 系统[19]由三维自治方程组

$$\dot{x}(t) = -\lambda x(t) + rx(t-\tau) \times (1 - x(t-\tau)), \quad (1)$$

来描述.式中 x 为系统的状态变量,λ,r 为系统的控制参数,τ 表示延迟时间(秒).当 $\lambda = 26$,$r = 104$ 和 $\tau = 0.5$ 时,系统(1)呈现混沌状态[19],由相空间重构法得到的系统(1)的混沌吸引子如图 1 所示.

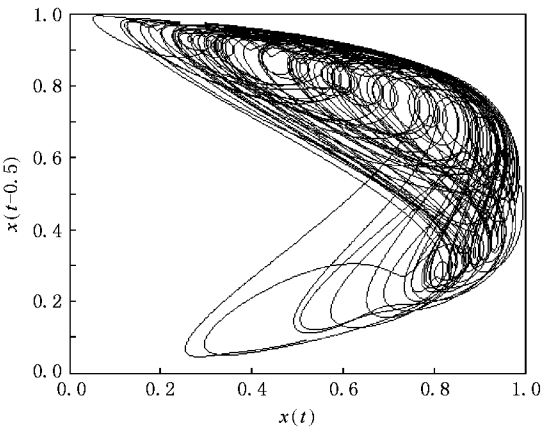

图 1 系统(1)的混沌吸引子

令 $\lambda = 26$,$r = 104$ 和 $\tau = 0.5$,使系统(1)呈现混沌行为.一般来说,当混沌系统某个参数发生小幅度变化时,原系统仍能维持混沌状态.通过仿真实验,作者发现当 $25.5 \leqslant \lambda \leqslant 26.5$ 时系统(1)可保持混沌状态且满足 $x > 0$.分别取 $\lambda = 25, 25.5, 26.5, 27$,系统(1)的混沌吸引子如图 2 所示.

* 国家自然科学基金(批准号:60573172),高等学校博士学科点专项科研基金(批准号:20070141014)和辽宁省自然科学基金(批准号:20082165)资助的课题.

† 通讯联系人. E-mail:wangxy@dlut.edu.cn

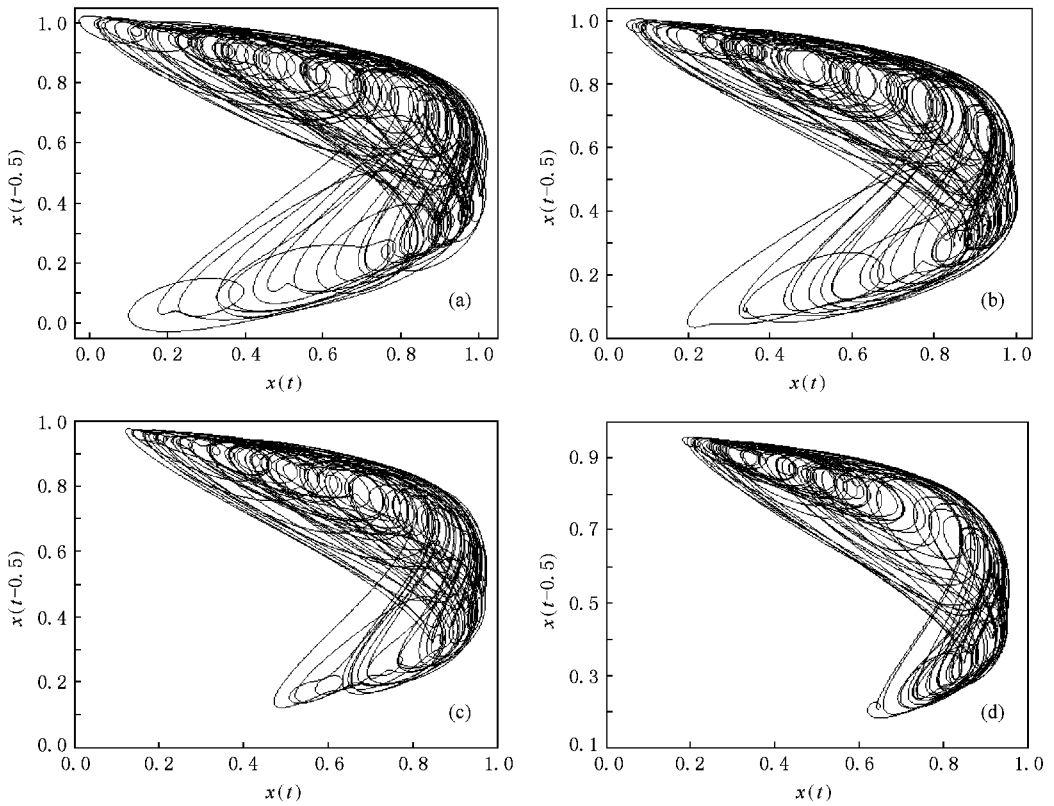

图 2 参数 λ 取值发生变化时系统(1)的混沌吸引子 (a) $\lambda = 25$;(b) $\lambda = 25.5$;(c) $\lambda = 26.5$;(d) $\lambda = 27$

3. 保密通信方案

令 $s(t)$ 为有用信号;$r(t) = f(s(t))$,f 为指定的变换函数;使用 $r(t)$ 对参数 λ 进行扰动,即 $\lambda = 26 + r(t)$;通过仿真实验,当 $-0.5 \leqslant r(t) \leqslant 0.5$,即 $25.5 \leqslant \lambda \leqslant 26.5$ 时系统(1)处于混沌状态且状态变量 $x(t)$ 在参数扰动情况下不会发生明显变化.实际应用中有用信号都是有界的,假定 $m \leqslant s(t) \leqslant M$,使用如下变换:

$$r(t) = f(s(t)) = \frac{s(t) - m}{M - m} - 0.5, \quad (2)$$

就可以将任意取值范围内的信号调制到系统(1)中.接收方使用观测器辨识出系统(1)的未知参数 λ,再恢复出扰动信号 $r'(t)$,利用如下变换:

$$s'(t) = (M - m)(r'(t) + 0.5) + m, \quad (3)$$

即可恢复出有用信号 $s'(t)$.

设接收方的参数观测器为

$$\begin{aligned} \dot{\delta} &= -k\delta + k^2 \ln(x(t)) \\ &\quad + krx(t-\tau)(1 - x(t-\tau))/x(t), \\ \hat{\lambda} &= \delta - k\ln(x(t)), \end{aligned} \quad (4)$$

这里 $x(t)$ 为发送方传递过来的混沌信号,$x(t-\tau)$ 为延迟时间 τ 后的混沌信号;δ 为辅助变量;$\hat{\lambda}$ 为辨识出来的未知参数;$k > 0$,是控制辨识速度的参数,仍取 $r = 104$,$\tau = 0.5$.设误差 $e = \hat{\lambda} - \lambda$,下面简要说明该观测器能够辨识系统(1)中的参数 λ:

$$\begin{aligned} \dot{e} &= \dot{\hat{\lambda}} - \dot{\lambda} = \dot{\delta} - k\dot{x}(t)/x(t) - \dot{\lambda} \\ &= -k\delta + k^2 \ln(x(t)) + krx(t-\tau) \\ &\quad \times (1 - x(t-\tau))/x(t) - k\dot{x}(t)/x(t) - \dot{\lambda} \\ &= -k\delta + k^2 \ln(x(t)) + k\lambda - \dot{\lambda} \\ &= -k(\hat{\lambda} + k\ln(x(t))) + k^2 \ln(x(t)) + k\lambda - \dot{\lambda} \\ &= -k(\hat{\lambda} - \lambda) - \dot{\lambda} = -ke - \dot{\lambda}. \end{aligned}$$

由上式可知,当 λ 值恒定时,有 $\dot{\lambda} = 0$,该观测器能够准确辨识出参数 λ 的值,且 k 越大辨识速度越快.由于该观测器以指数速度进行辨识,所以当 λ 为慢时变信号,或 λ 在一个周期内的大部分时间里变化缓慢,仍然可以用该观测器进行辨识.由仿真实验可知,当 $25.5 \leqslant \lambda \leqslant 26.5$ 时,系统(1)的状态变量 $x(t) > 0$,因此可以确保该观测器是有效的.值得一

提的是，本方案采用一阶时滞混沌系统，只需要传递单路信号就可以实现保密通信.

将系统(1)表示为

$$x(t) = \varphi(x(t), x(t-\tau), \lambda),$$

系统(4)表示为

$$\dot{\delta} = \psi(\delta, x(t), x(t-\tau)),$$

$$\hat{\lambda} = \phi(\delta, x(t)),$$

则该保密通信方案可由图 3 来描述.其中 f 代表(2)式中的变换函数，$\bar{\lambda} = 26$.

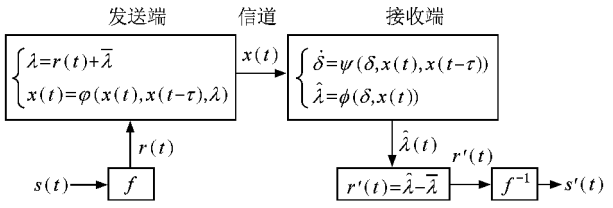

图 3　基于参数观测器的保密通信方案原理图

1) 取模拟信号进行仿真实验.令 $k = 5$，$s(t) = 3 + \sin(2t)$，则 $m = 2$，$M = 4$.代入(2)式有

$$r(t) = f(s(t)) = \frac{1 + \sin(2t)}{2} - 0.5$$

$$= 0.5\sin(2t),$$

利用观测器得出 $\hat{\lambda}$，从而得到 $r'(t) = \hat{\lambda} - 26$.代入(3)式得到

$$s'(t) = 2(r'(t) + 0.5) + 2 = 2r'(t) + 3,$$

$s'(t)$即是恢复出来的有用信号.仿真结果如图 4 所示.其中图 4(a)表示所传递的有用信号，图 4(b)表示发送端发出的混沌信号，图 4(c)表示接收端恢复出的有用信号.由图 4 可以看出尽管该观测器对于慢时变信号存在误差，但在精度要求不太高的情况下并不妨碍有用信号的恢复.

对 $x(t)$作功率谱分析，所得结果如图 5(a)所表示，图 5(b)是图 5(a)的局部放大图，可见这种保密通信方法在传递慢时变模拟信号时能有效抵御谱攻击[20].

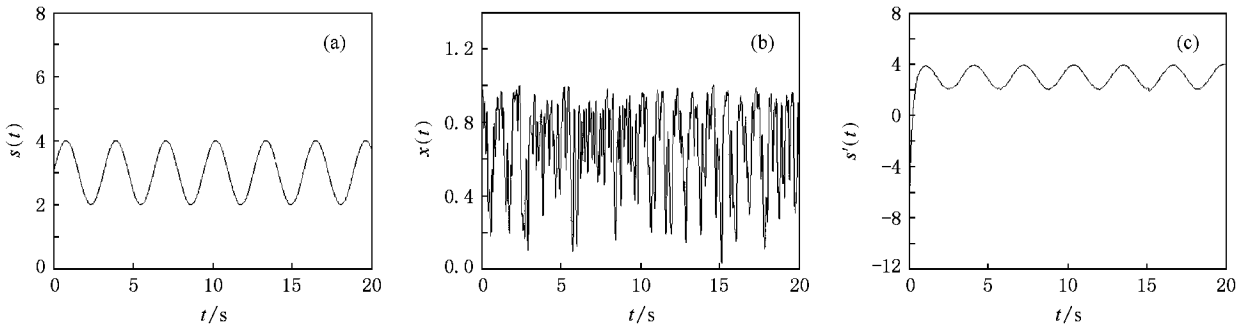

图 4　$s(t) = 3 + \sin(2t)$的保密通信仿真实验结果

2)取数字信号进行仿真实验.假定所传信号为 0110001001，如果以脉冲信号表示该数字信号，简便起见，则可以选取 $s(t)$如图 6(a)所示，将 $s(t)$调制在 λ 中，然后在接收端辨识该脉冲信号实现数字保密通信. Álvarez 等曾以滤波攻击方法破解了这类数字保密通信方案[21]，因此本文以频率替代振幅

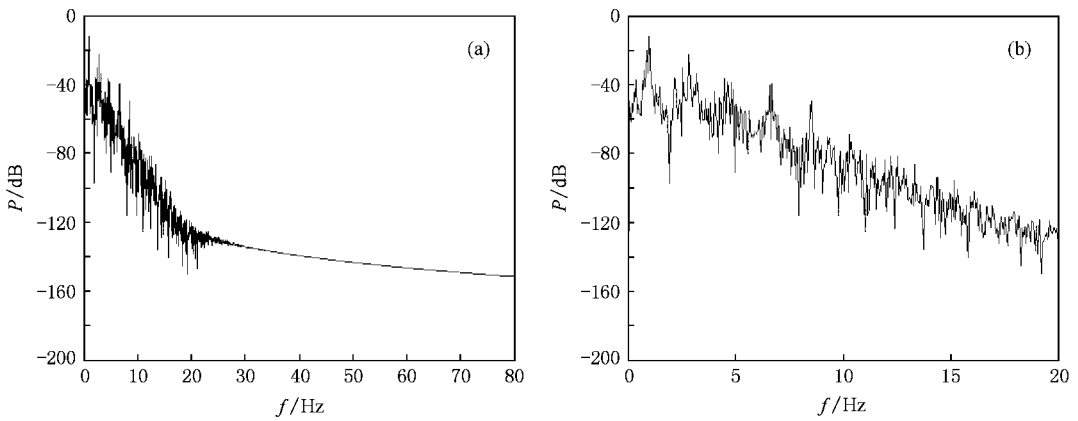

图 5　$x(t)$的功率谱图

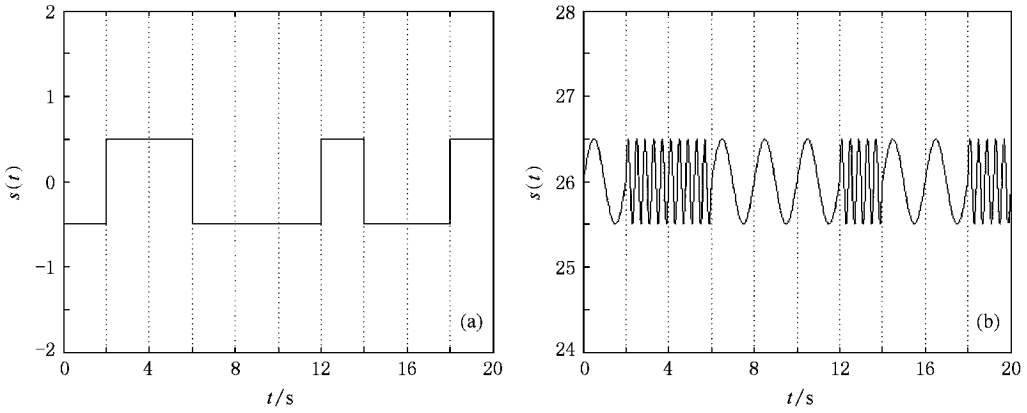

图 6 代替数字信号 0110001001 的连续信号 $s(t)$

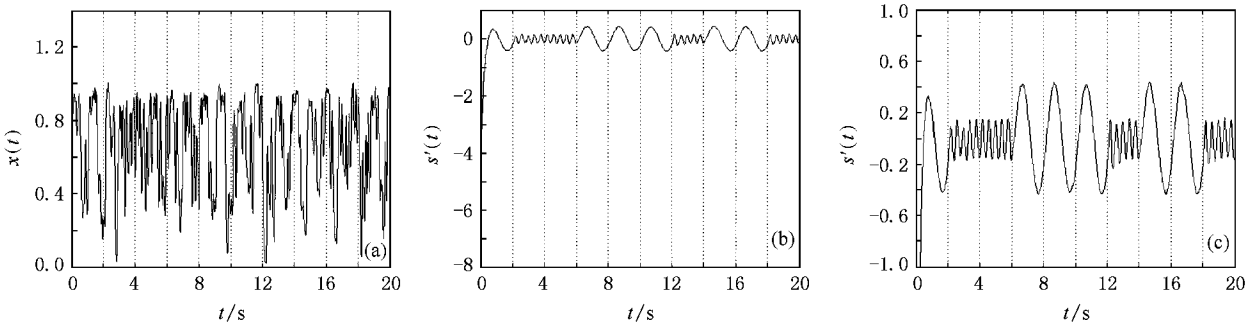

图 7 数字保密通信仿真实验结果

来对数字信号“0”和“1”进行编码,“0”时调制 $0.5\sin(\pi t)$;“1”时调制 $0.5\sin(5\pi t)$,则 $s(t)$ 如图 6(b)所示,仍令 $k=5$,接收端的仿真结果如图 7 所示.

图 7(a)表示所传递的混沌信号,图 7(b)表示所辨识出的信号,图 7(c)为图 7(b)的局部放大图,显然提高频率加大了辨识误差,但由图 7 可见这种误差主要是振幅方面的,频率并未受明显影响,因此仍可以准确传递数字信号.为便于观察,设计截止频率为 1.8 Hz 的 4 阶 Butterworth 高通滤波器 $s'(t)$ 对进行高通滤波,该滤波器的频率幅度响应如图 8(a)所示,滤波结果 $s''(t)$ 如图 8(b)所示.显然由初始阶段经历了不到 2 s 的追踪之后,就可以将数字信号准确地恢复出来.

图 9(a)对传递‘0’和‘1’这两种情况,即 $\lambda=26+0.5\sin(\pi t)$ 和 $\lambda=26+0.5\sin(5\pi t)$ 所发出的 $x(t)$ 功率谱进行了对比,可见两者差异并不明显.图 9

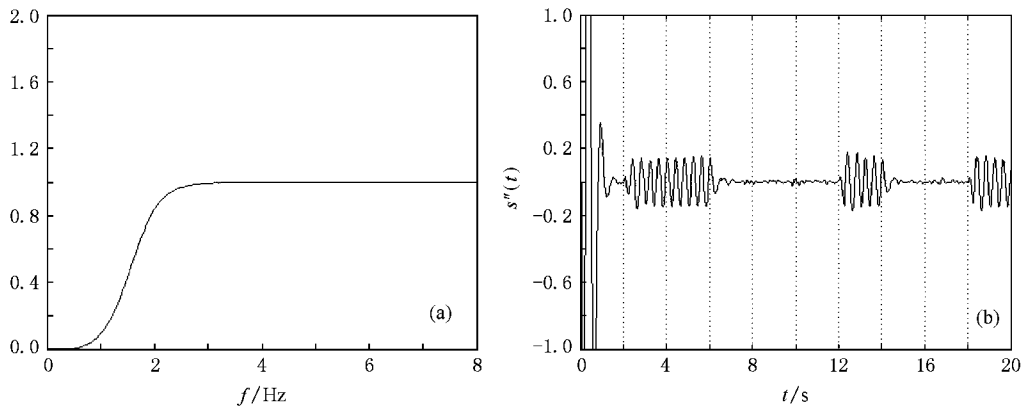

图 8 滤波器的频幅响应及滤波结果

(b)对 $\lambda=25.5$ 和 $\lambda=26.5$ 所发出的 $x(t)$ 功率谱进行了对比，在大于 15 Hz 时两者的差异较明显，Álvarez 等也正是基于此提出了高通滤波方法成功破解了这类数字保密通信方案[21]．通过功率谱对比可以发现，本文借助信号频率的不同来传递不同的数字信号，能够提供更高的保密性．作者也进行了大量仿真实验，证明了该数字保密通信方案能够有效抵制滤波攻击．

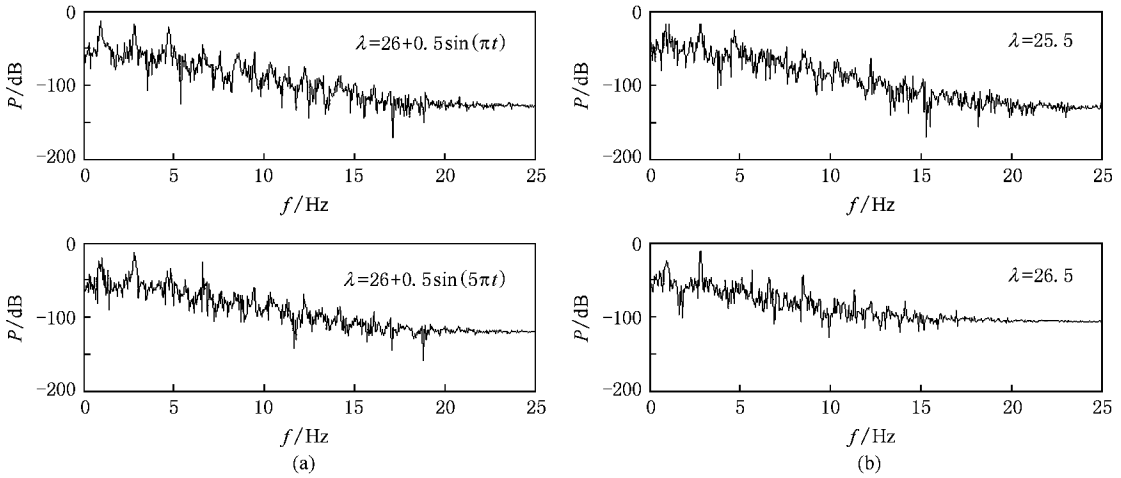

图 9　分别传递‘0’和‘1’，$x(t)$ 的功率谱对比图

4. 结　论

本文基于参数调制的原理，将有用信号调制在发送端的一阶时滞 Logistic 混沌系统的参数中，在接受端利用观测器辨识出未知参数，恢复出调制在其中的有用信号．本文的保密通信方案只需传递单路信号，不但能较准确的传递模拟信号，且能安全可靠地传递数字信号．数值仿真验证了本方法的有效性．

实际通信中，信道中不可避免含有噪声，本文中的保密通信方案基于参数的近似辨识，主要侧重于数字保密通信，只需要近似恢复不同频率的正弦信号，以解调信号的频率来区分‘0’和‘1’，因此在一定程度上对噪声具有鲁棒性．考虑到本文所传递的混沌信号介于 0 至 1 之间，幅度较小，因此可放大一定倍数再进行传输．假定放大倍数为 10，使所传信号介于 0 至 10 之间，通过仿真实验，当信道中的随机噪声低于 0.1 时，可准确恢复出数字信号．此外由于混沌信号处于低频区域，在接收端对收到的混沌信号进行低通滤波，则可以有效消除信道中的高频噪声．

[1] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[2] Carroll T L, Pecora L M 1991 *IEEE Trans. Circuits Systems* **38** 453

[3] Chen G, Dong X 1998 *From Chaos to Order: Methodologies, Perspectives and Applications* (Singapore: World Scientific) chapt. 1

[4] Wang G R, Yu X L, Chen S G 2001 *Chaotic Control, Synchronization and Utilizing* (Beijing: National Defence Industry Press) chapt. 7 (in Chinese) [王光瑞、于熙龄、陈式刚 2001 混沌的控制、同步与利用(北京：国防工业出版社)第七章]

[5] Wang X Y 2003 *Chaos in the Complex Nonlinearity System* (Bejjing: Electronics Industry Press) chapt. 2 (in Chinese) [王兴元 2003 复杂非线性系统中的混沌(北京：电子工业出版社)第二章]

[6] Chen G R, Lü J H 2003 *Dynamical Analyses, Control and Synchronization of the Lorenz system family* (Beijing: Science Press) chapt. 2 (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)第二章]

[7] Oppenheim A V, Wornell G W, Isabelle S H, Cuomo K M 1992 *Proc. IEEE IGASSP* **4** 117

[8] Kocarev L, Halle K S, Eckert K, Chua L O, Parlitz U 1992 *Int. J. Bifur. Chaos* **2** 709

[9] Dedieu H, Kennedy M P, Hasler M 1993 *IEEE Trans. Circuits Systems* Ⅱ **40** 634

[10] Halle K S, Wu C W, Itoh M, Chua L O 1993 *Int. J. Bifur. Chaos* **3** 469

[11] Sushchik M, Rulkov N, Larson L 2000 *IEEE Commun. Lett.* **4** 128

[12] Mu J, Tao C, Du G H 2003 *Chin. Phys.* **12** 381

[13] Li J F, Li N, Lin H 2004 *Acta Phys. Sin.* **53** 1694 (in Chinese) [李建芬、李　农、林　辉 2004 物理学报 **53** 1694]

[14] Sun L, Jiang D P 2006 *Acta Phys. Sin.* **55** 3283 (in Chinese) [孙 琳、姜德平 2006 物理学报 **55** 3283]
[15] Lu J G, Xi Y G 2005 *Chin. Phys.* **14** 274
[16] Wang X M, Zhang J S 2006 *Phys. Lett.* A **357** 323
[17] Ryabov V B, Usik P V, Vairiv D M 1999 *Int. J. Bifur. Chaos* **9** 1181
[18] Peng H P, Li L X, Yang Y X, Zhang X H, Gao Y 2007 *Acta Phys. Sin.* **56** 6245 (in Chinese) [彭海朋、李丽香、杨义先、张小红、高 洋 2007 物理学报 **56** 6245]
[19] Tian Y C, Gao F R 1998 *Physica* D **117** 1
[20] Yang T, Yang L B, Yang C M 1998 *Phys. Lett.* A **247** 105
[21] Álvarez G, Montoya F, Romera M, Pastor G 2004 *Chaos, Solitons Fract.* **21** 783

A secure communication scheme based on parameter identification of first order time-delay chaotic system *

Wang Ming-Jun Wang Xing-Yuan†
(*School of Electronic & Information Engineering, Dalian University of Technology, Dalian* 116024, *China*)
(Received 9 June 2008; revised manuscript received 10 September 2008)

Abstract

Based on parameter modulation theory, a parameter observer is designed for the first order time-delay Logistic chaotic system. The unknown parameter of this system can be identified by transmitting a single signal, then the useful signal modulated in the parameter will be recovered successfully. By choosing different frequency signals as "0" and "1", a practical digital secure communications scheme is designed. Numerical simulation shows the effectiveness of the method.

Keywords: observer, chaos secure communications, parameter modulation, altering
PACC: 0545, 0555

* Project supported by the National Natural Science Foundation of China (Grant No. 60573172), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20070141014) and the Natural Science Foundation of Liaoning Province (Grant No. 20082165).

† Corresponding author. E-mail: wangxy@dlut.edu.cn