第 53 卷 第 6 期 2004 年 6 月
1000-3290/2004/53(06)/1694-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.53,No.6,June,2004

适合传输快变信息信号的混沌调制保密通信

李建芬[1)] 李 农[2)] 林 辉[1)]

[1)](西北工业大学自动化学院,西安 710072)

[2)](空军工程大学工程学院,西安 710038)

(2003 年 7 月 24 日收到;2003 年 9 月 8 日收到修改稿)

提出一种新的混沌调制通信方法.利用一个自适应控制器跟踪信息信号的误差对产生混沌载波的发射系统进行参数调制.同时,信息信号直接与混沌载波相乘作为发射信号驱动接收系统.在接收端,另一个自适应控制器维持收发系统的混沌同步并恢复出信息信号.由于同步误差与信息信号无关,从而实现了大幅度、快时变信息信号的混沌调制通信.理论分析和数值模拟的结果表明该方法增强了低维混沌系统的通信保密性.

关键词:混沌调制,保密通信,自适应控制器,蔡氏电路

PACC:0545

1. 引 言

随着混沌同步概念的提出,利用混沌进行保密通信就成为当前混沌研究领域的热点.基于混沌进行保密通信的方法已多有报道[1—18],一般通信方法可分为 混沌掩盖、混沌调制、混沌键控和混沌参数调制等.混沌掩盖是直接将信息信号加到混沌载波上,而混沌调制是用信息信号来调制混沌载波,混沌参数调制技术将所传输的信息信号隐藏在系统参数中,在接收端通过恢复相应的参数来提取所传输的信息信号.上述方法通常需要信息信号的强度足够小,易受到攻击[10—12].

一个混沌动力学系统通常有许多参数对系统的动态行为起着控制作用,在混沌参数调制系统中,一般是用信息信号直接对某些参数进行调制,由于受到系统动力学行为的限制,信息信号的动态范围不能太大.为了有效地提取混沌系统参数,自适应技术被引入到参数估计中来,如 Lyapunov 指数跟踪的方法[14],自适应参数估计方法[15]等,它们的共同缺点是不能传输快时变的信息信号[13].本文提出的方法是用一个自适应控制器跟踪信息信号的变化,并用误差信号来调制系统参数,同时,用信息信号对发射的混沌信号进行二次调制,即将信息信号与混沌信号的乘积作为发射信号传输给接收端.在接收端,通过另一个控制器维持系统同步,并解调出原信息信号.该方法的特点是同步误差与信息信号的变化率无关,因此信息信号的频率只取决于自适应控制器的响应速度,同时由于注入到发射系统的调制信号是跟踪误差,所以信息信号的幅值可以适当的增大.从而,提高了混沌调制通信的保密性.

2. 混沌调制与解调

蔡氏电路的归一化状态方程[13]为

$$\dot{x} = Ax + Df(x_1) = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix} x + \begin{bmatrix} -\alpha \\ 0 \\ 0 \end{bmatrix} f(x_1),$$

式中 $x \in R^3$ 为归一化状态向量;$A \in R^{3\times 3}$,$D \in R^{3\times 1}$ 为系数矩阵,非线性函数为 $f(x_1) = bx + 0.5(a-b)[|x_1+1| - |x_1-1|]$,其中 a,b 为分段线性电阻的归一化斜率.本文以蔡氏电路为例提出的混沌调制保密通信方案如图 1 所示,其状态方程分别为

发射系统

$$\begin{aligned} \dot{x} &= Ax + Df(x_1) + K(s(t) - w)x_1, \\ \dot{w} &= \mu(|s(t)x_1| - w|x_1|), \end{aligned} \tag{1}$$

发射信号 $y = x_1 s(t)$.

接收系统

$$\begin{aligned} \dot{\hat{x}} &= A\hat{x} + Df(\hat{x}_1) + K(s(t)x_1 - \hat{w}\hat{x}_1), \\ \dot{\hat{w}} &= \mu(|s(t)x_1| - \hat{w}|\hat{x}_1|). \end{aligned} \tag{2}$$

其中 $s(t)$ 为信息信号,x_1,$\hat{x}_1$ 分别表示 x,$\hat{x}$ 的第一个分量,$K = [k\ 0\ 0]^{\mathrm{T}}$ 是反馈系数矩阵,w 和 $\hat{w}$ 分别

为收发两端连接的自适应控制器的输出，μ 是一个用于控制速度和稳定性的增益常数.

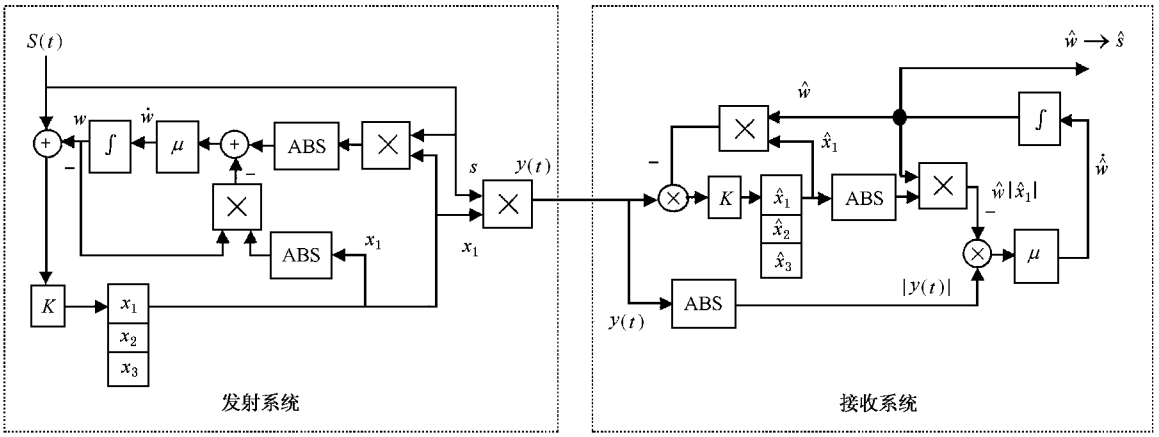

图 1　通信系统原理框图

从(1)式和图 1 可见，该方法是将信号 $s(t)$ 与 w 的误差注入到发射系统，而不是直接将信号 $s(t)$ 注入，只要 $s(t)$-w 比混沌信号小得多，就可使系统保持混沌态，而发射信号为信息信号与混沌信号的乘积.系统的同步误差分析如下：

设

$$e(t) = [e_1, e_2, e_3, e_4]^{\mathrm{T}} = [x_1 - \hat{x}_1, x_2 - \hat{x}_2, x_3 - \hat{x}_3, w - \hat{w}]^{\mathrm{T}},$$

由(1)，(2)式得系统误差方程为

$$\dot{e})(t) = \begin{bmatrix} -\alpha - kw & \alpha & 0 & -k\hat{x}_1 \\ 1 & -1 & 1 & 0 \\ 0 & -\beta & -\gamma & 0 \\ 0 & 0 & 0 & -\mu|\hat{x}_1| \end{bmatrix} e + \begin{bmatrix} -\alpha \\ 0 \\ 0 \\ 0 \end{bmatrix} (f(x_1) - f(\hat{x}_1)) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -\mu w(|x_1| - |\hat{x}_1|) \end{bmatrix}.$$

由于 $f(*)$ 为分段线性连续函数，斜率分别为 a 和 b，且 $a < b < 0$，因此 $a(x_1 - \hat{x}_1) \leqslant f(x_1) - f(\hat{x}_1) \leqslant b(x_1 - \hat{x}_1)$.设

$$f(x_1) - f(\hat{x}_1) = \delta(t)(x_1 - \hat{x}_1),$$

其中 $\delta(t)$ 为时变参数，且 $a < \delta < b$，则

$$\dot{e}(t) = \begin{bmatrix} -\alpha - kw - \delta(t) & \alpha & 0 & -k\hat{x}_1 \\ 1 & -1 & 1 & 0 \\ 0 & -\beta & -\gamma & 0 \\ 0 & 0 & 0 & -\mu|\hat{x}_1| \end{bmatrix} e + \begin{bmatrix} 0 \\ 0 \\ 0 \\ -\mu w(|x_1| - |\hat{x}_1|) \end{bmatrix} = A_f(t)e + u(t). \quad (3)$$

(3)式为一阶变系数非齐次线性微分方程组，因此它的解具有下面形式：

$$e(t) = \phi(t)e(0) + \phi(t)\int_0^t \phi^{-1}(\tau)u(\tau)\mathrm{d}\tau, \quad (4)$$

其中 $\phi(t)$ 是 $A_f(t)$ 的基本矩阵.由(4)式看出，只要求出 $\phi(t)$，$e(t)$ 总是可以计算出来的.但是，只有在少数情况下，$\phi(t)$ 可以由 $A_f(t)$ 算出，故一般只能用数值解法来求解.通过计算 $A_f(t)$ 的特征值随时间的变化规律可知，当 $\mu = 0, k = 0$ 时，$A_f(t)$ 的特征值为(0, 0.1634 + 3.1528j, 0.1634 - 3.1528j, -4.9469)，显然，此时 $A_f(t)$ 是不稳定的.当 $\mu = 10, k = 10$ 时，可以使 $A_f(t)$ 的四个特征值几乎全部具有负的实部(见图 2)，这时同步误差 $e(t)$ 主要取决于(4)式的第二项，而第二项与 $|x_1| - |\hat{x}_1|$ 有关，随着 $A_f(t)$ 在零点的渐进稳定，$e(t)$ 亦逐步减小，进而亦使 $|x_1| - |\hat{x}_1|$ 逐步减小，当 $e(t)$ 小到允许的误差范围内时，就可以认为系统同步则有 $\hat{x}_1 \to x_1, \hat{x}_2 \to x_2, \hat{x}_3 \to x_3, \hat{w} \to w \to s(t)$，即可将原信息信号解调出来.

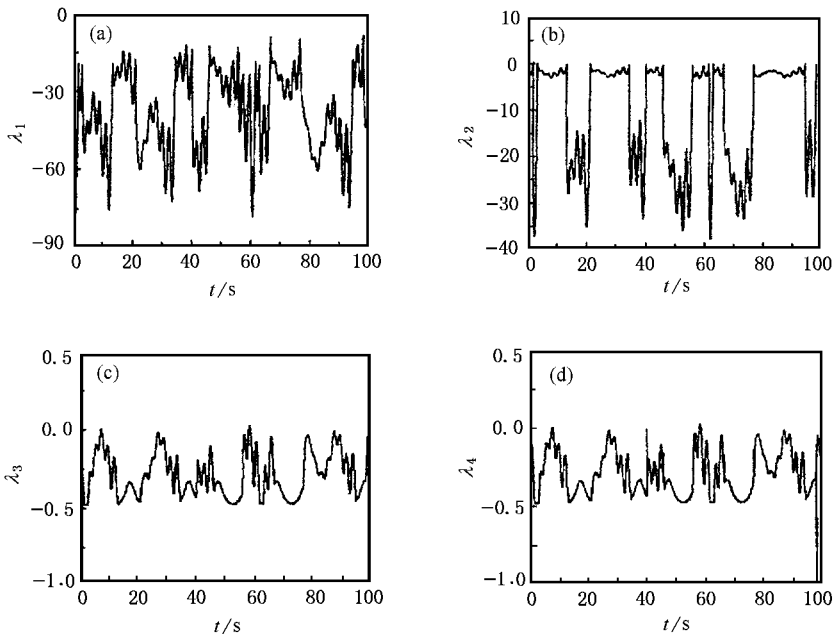

图 2 当 $\mu = 10$，$k = 10$ 时 $A_f(t)$ 的四个特征值的实部随时间的变化关系

3. 数值计算

采用 MATLAB 进行数值模拟，参数选择为 $\alpha = 10$，$\beta = 14.31$，$\gamma = 0.12$，$a = -1.39$，$b = -0.75$ 时，电路处于混沌状态. 另选择 $\mu = 10$，$k = 10$，信息信号 $s(t)$ 分别是基频为 0.1(归一化频率)的方波和正弦波，模拟结果如图 3 至图 6 所示.

图 3 为混沌信号 $x_1(t)$ 及其频谱 $X_1(\omega)$，图中可见混沌信号的中心频率约在 0.1. 图 4 为方波信号 $s(t)$ 及其频谱 $S(\omega)$，可见方波信号主频带位于混沌信号的中心频带内. 图 5 是信息信号 $s(t)$ 与混沌信号 $x_1(t)$ 直接相乘构成的发射信号 $y(t)$. 图 6 为恢复的信息信号 $\hat{s}(t)$ 和系统的同步误差.

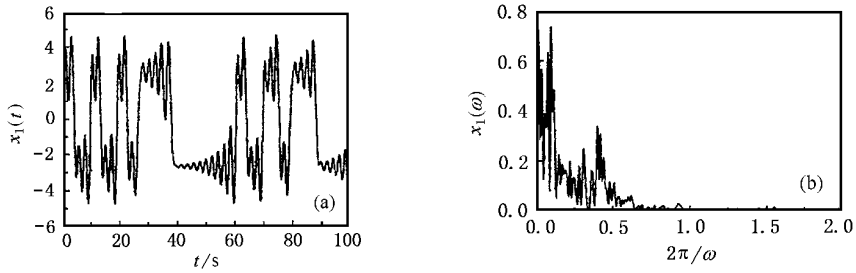

图 3 混沌信号 $x_1(t)$ 的时域波形和频谱

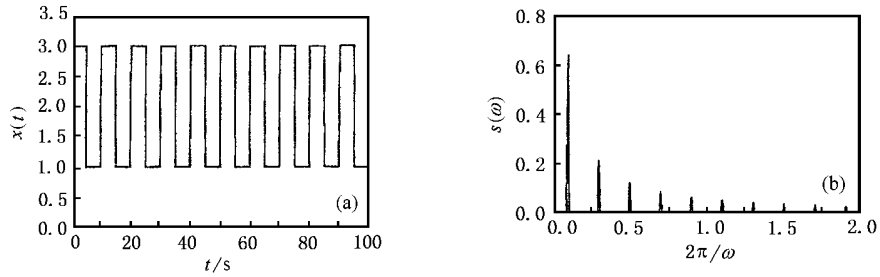

图 4 信息信号 $s(t)$ 为方波时的时域波形和频谱图

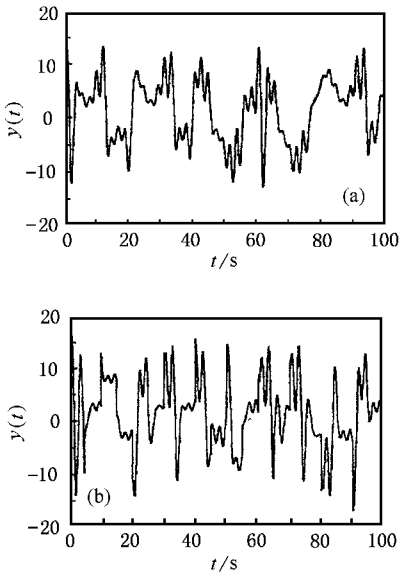

图 5　信息信号 $s(t)$ 分别为正弦波和方波时的发射信号 $y = x_1 s(t)$

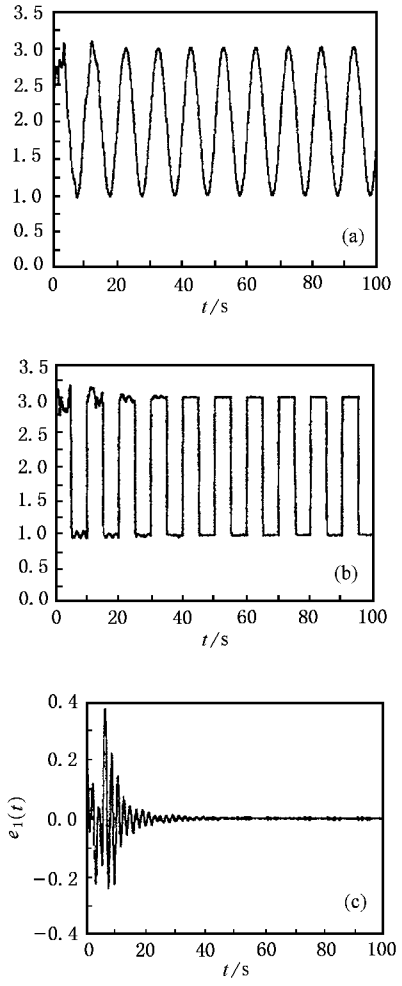

图 6　恢复的信息信号 $\hat{s}(t)$ 及同步误差 $e_1 = x_1 - \hat{x}_1$

4. 保密性能分析

Perez 等人[12]指出，对于只有一个正的指数的弱混沌系统，它们在适当的回归映像上一般表现为曲线或分段曲线．小的信号调制后表现为这些曲线上的毛刺，可以通过对比识别．本文所提方案，发射的混沌信号 $y = x_1 s(t)$ 经过了两次调制，由其重构出的回归映射不再被吸引到纯净映射曲线附近，图 7 是混沌信号 x_1 与发射信号 y 的线性回归映射散点图，其中(a)为纯净的连续混沌信号 x_1 得到的映射图，(b)是系统经误差信号调制后的 x_1 得到的映射图，(c)为由发射信号 $y = x_1 s(t)$ 得到的映射图．显然，破译者接收到加密信号后，很难通过神经网络或回归方法把混沌信号所遵守的方程近似地重构出来，因而无法进行非线性噪声减缩加以破译．

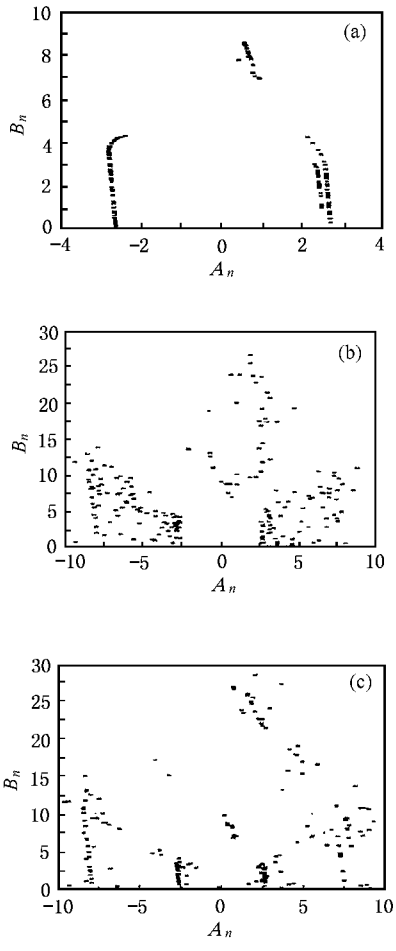

图 7　混沌信号 x_1 与发射信号 y 的回归映射散点图　(a)纯净 x_1 的映射，(b)经误差信号调制后的 x_1，(c)发射信号 y 的映射

5. 结 论

本文提出了一种新的混沌参数调制通信方法，实现了大幅度、快时变信息信号的混沌调制通信，具有电路实现简单，抗破译能力强的特点.不但可传输模拟信号，还可传输数字信号，适用于可通过单向耦合同步的系统.

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

[2] Cuomo K M and Oppenheim A V 1993 *IEEE Trans. CAS-I* **40** 626

[3] Lozi R and Chua L O 1993 *Int. J. Bifurc. Chaos* **3** 1319

[4] Parlitz U, Chua L O, Kocarev L, Halle K S and Shang A 1992 *Int. J. Bifurc. Chaos* **2** 973

[5] Dedieu H, Kennedy M P and Hasler M 1993 *IEEE Trans. CAS-II* **40** 634

[6] Corron N J and Hahs D W 1997 *IEEE Trans. CAS-I* **44** 373

[7] Carroll T L 1995 *IEEE Trans CAS-I* **42** 105

[8] Yang T and Chua L O 1996 *IEEE Trans. CAS-I* **43** 817

[9] Yang T, Wu C W and Chua L O 1997 *IEEE Trans. CAS-I* **44** 469

[10] Short K M 1994 *Int. J. Bifurc. Chaos* **4** 959

[11] Stark J and Arumugam B V 1992 *Int. J. Bifurc. Chaos* **2** 413

[12] Perez G and Cerdeira H A 1995 *Phys. Rev. Lett.* **74** 1970

[13] He Z Y, Li K, Yang L X and Shi Y H 2000 *IEEE Trans. CAS-I* **47** 397

[14] Ramaswamy R and Sinha S 1998 *Phys. Rev.* E **57** 2507

[15] Markov A Y *COC'97 Proceedings* **3** 76

[16] Li J F and Li N 2002 *Chin. Phys.* **11** 1124

[17] Zhang J S and Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese) [张家树、肖先锡 2001 物理学报 **50** 2121]

[18] Kuang J Y, Deng K and Huang R H 2001 *Acta Phys. Sin.* **50** 1856 (in Chinese) [匡锦瑜、邓 昆、黄荣怀 2001 物理学报 **50** 1856]

Secure communication method for fast-varying information signal based on chaotic modulation

Li Jian-Fen[1)] Li Nong[2)] Lin Hui[1)]

[1)] (*Northwestern University of Polytechnology, Xi'an* 710072, *China*)

[2)] (*Institute of Engineering, Air Force Engineering University, Xi'an* 710038, *China*)

(Received 24 July 2003; revised manuscript received 8 September 2003)

Abstract

A new secure communication method based on chaotic modulation is proposed. The parameter of the transmitting system procreated chaotic carrier is modulated by errors from an adaptive controller and information signal. At the same time, the information is directly multiplied by the chaotic carrier in transmission to drive the receiving system. In the receiver, another adaptive controller is used to maintain chaotic synchronization of the transmitting and receiving systems and to recover information signal. Since the synchronization error is independent of information signal, the chaotic modulation for large-amplitude and fast-varying information signals can be achieved. The results of theoretic analysis and numerical simulation show that the proposed method enhances the degree of security of low-dimensional chaotic systems.

Keywords: chaotic modulation, secure communications, adaptive controllers, Chua's circuits

PACC: 0545