一种基于数字信道的连续混沌通信系统

汪芙平,王赞基,郭静波
(清华大学电机工程与应用电子技术系,北京 100084)

摘 要: 提出一种将连续混沌系统和数字信道相结合的混沌通信实现方案. 该方案中混沌调制和解调过程通过数值积分以软算法的方式实现,携带信息的混沌信号离散化成数字信号通过数字信道传输. 详细讨论了该系统的设计方法,提供的一些自由参数可以实现系统在保密性、信息传输速率和通信质量等方面的均衡. 该系统结构简单,与传统的数字通信相比,在获得较高保密性的同时,其通信速率和通信质量基本不受影响.

关键词: 混沌; 保密通信; 数字通信
中图分类号: TN914 **文献标识码**: A **文章编号**: 0372-2112 (2003) 01-0127-04

A Novel Continuous Chaotic Communication System Based on Digital Communication Channel

WANG Fu-ping, WANG Zan-ji, GUO Jing-bo
(*Department of Electrical Engineering, Tsinghua University, Beijing* 100084, *China*)

Abstract: A novel chaotic communication scheme combining the continuous chaotic system with the digital communication channel is proposed, in which the chaotic modulation and demodulation module are realized with software and the continuous chaotic signals carrying the hidden information are transmitted in digital form. The designing method of the proposed communication scheme is described in detail and the optimal selections of the related parameters to balance the performances of the system in security, transmission rate and transmission quality are discussed. The proposed communication system is easy to practically realize and compared with the conventional digital communication system, the performance of the transmission rate and transmission quality is not lowered while the security of information transmission is obtained.

Key words: chaos; secure communication; digital communication

1 引言

混沌通信近十年来受到广泛关注,因为它可以实现一定意义上的扩频,同时又具有较高的保密性. 但目前已有的将连续混沌系统用于通信的绝大多数方案很难实际实现. 主要原因是:没有很好的办法克服信道畸变[1-2],同时混沌调制和解调的电路实现相当困难[3].

为克服以上困难,本文提出一种将连续混沌系统和数字信道相结合的实现方案. 图 1 给出了该方案的具体框架,其中传输的是模拟信息 $i_0(t)$. 方案的基本思路是,首先将模拟信源 $i_0(t)$ 以抽样频率 f_s(对应抽样时间间隔 τ_s) 转换成离散信号 $i(n)$; $i(n)$ 作为混沌调制模块的输入,通过插值转换成连续变量,参与调制模块中混沌系统的演化;混沌调制过程以数值积分方式实现,输出离散信号 $s(n)$; $s(n)$ 具有混沌信号的特性,它作为信息 $i(n)$ 的载体通过数字通信系统传送到接收端,接收信号记为 $r(n)$;在混沌解调模块中, $r(n)$ 先通过插值转换成连续变量 $r(t)$, $r(t)$ 驱动接收端混沌系统实现与发送端混沌系统的同步,在同步状态下信息信号 $\hat{i}(n)$ 得到恢复,这个过程同样以数值积分的方式实现;最后, $\hat{i}(n)$ 经过D/A过程转换成模拟信号的形式,完成通信的过程.

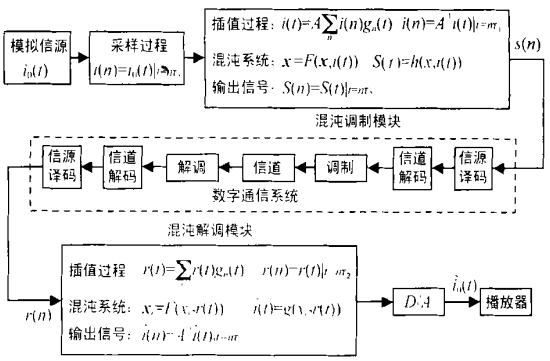

图 1 连续混沌系统和数字信道相结合的混沌通信系统的框架

方案中采用软算法可以实现任意形式的混沌调制和解调过程,很容易做到发送端和接收端系统参数的精确匹配. 利用数字通信系统传输信号,通信的误码率可以限制在非常低的水平,因而方案中接收信号 $r(t)$ 相对 $s(t)$ 的误差主要由模拟信号转换为数字信号的量化过程以及连续信号和离散信号

收稿日期:2001-07-30;修回日期:2002-05-09

互相转换的抽样和插值过程引起. 这些误差可以控制在一定范围内,能够保证混沌同步的精确实现.

软算法为混沌的调制和解调过程提供了很大的灵活性,可以实现混沌信号频带的扩展和压缩,这对提高混沌通信系统的通信速率和保密性至关重要. 该系统的设计目标是,在获得较高保密性的同时,它的通信速率和通信质量基本达到传统数字通信系统的水平.

2 系统设计

系统设计主要表现为混沌调制和解调模块中三个自由参数 τ_1、τ_2 和 A 的选取. 设计的目标就是兼顾系统的保密性、信息的传输速率和信息传输质量三项指标,使系统性能在总体上达到最优.

在调制和解调模块中,混沌源和调制、解调方式的选择直接影响系统的保密性能,这些内容在已发表的工作中[4,5]有较详细的论述,本文将不涉及这些内容. 为便于说明,本文以 Lorenz 系统作为混沌源. 混沌调制方程为: $dx/dt = \sigma(y - x)$, $dy/dt = (R - \mu)\cdot s(t) + \mu x - y - s(t)\cdot z$, $dz/dt = s(t)\cdot y - bz$,其中 $s(t) = x(t) + i(t)$ 为传输信号. 混沌解调方程: $dx_r/dt = \sigma(y_r - x_r)$, $dy_r/dt = (R - \mu)\cdot r(t) + \mu x_r - y_r - r(t)\cdot z_r$, $dz_r/dt = r(t)\cdot y_r - bz_r$. 解调的信息信号 $\hat{i}(t) = r(t) - x_r(t)$. 当参数选取为 $\sigma = 16.0$, $R = 45.92$, $b = 4.4$, $\mu = 0.98$ 时,从理论上可以证明[6],当 $t \to \infty$ 时,有 $x_s(t) = x_r(t)$;若有 $r(t) = s(t)$,则 $\hat{i}(t) = i(t)$.

2.1 τ_1 的选取

τ_1 是离散信号 $\{i(n)\}$ 插值时相邻样本点间的时间间隔. τ_1 的取值决定了混沌信号 $s(t)$ 的带宽,可解释如下:设 $i(t)$ 对应物理信号 $i_0(t)$,它的物理频率不变;以 $i(t)$ 作为参照,随着 τ_1 的变化,$s(t)$ 时域波形将以尺度 τ_1 伸缩,因此频谱带宽与 τ_1 成正比.

τ_1 取值应保证 $s(t)$ 中 $i_0(t)$ 被完全掩藏,此时从 $s(t)$ 的波形和频谱上无法看出 $i_0(t)$ 的特征,从而通信具有较高的保密性. 图 2 给出 Lorenz 信号的一段波形及功率谱,信号能量主要集中在 0～10Hz 范围内. 设需要传送图 3 所示的模拟信号,信号能量主要集中在 100Hz ～ 400Hz 范围内. 若 Lorenz 混沌调制系统直接以物理形式实现,由于 $x(t)$ 和 $i(t)$ 的频谱并不重叠(如图 4 中 $\tau_1 = 0.000125$s 那条曲线所示),通过线性滤波可以实现二者分离,因而系统不具备保密性. 现在以插值和数值积分方式实现,通过调节 τ_1 展宽 Lorenz 信号的频带,可以实现 $s(t)$ 对 $i(t)$ 的完全隐藏. 令 $\tau_s = 0.000125$s, $A = 20$, τ_1 分别为 τ_s、$8\tau_s$、$16\tau_s$、$40\tau_s$ 和 $80\tau_s$ 时,$s(t)$ 的功率谱如图 4 所示. 可以看出,随着 τ_1 增大,$i(t)$ 的频率成分逐渐被完全掩藏.

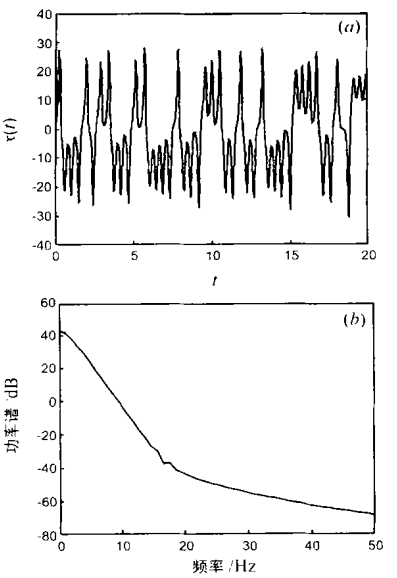

图 2 Lorenz 混沌信号. (a) 波形图; (b) 功率谱

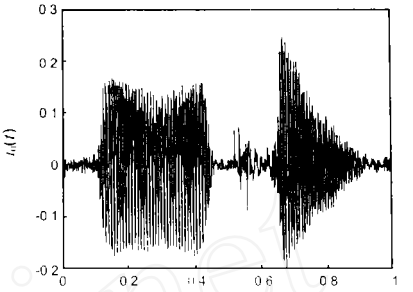

图 3 一段模拟输入信号波形

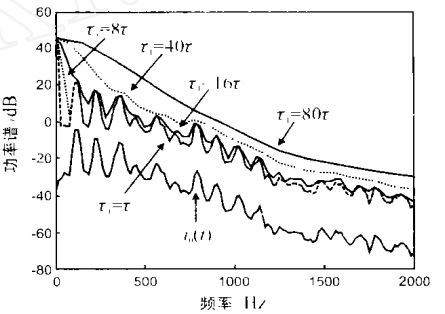

图 4 输入信号及调制信号的功率谱

对 Lorenz 混沌调制系统而言,τ_1 越大,则 $i_0(t)$ 被 $s(t)$ 隐藏得越好,从而通信系统保密性越高. 但 τ_1 也不能无限增大. 因为 $s(t)$ 的频带越宽,在传送该信号时所需信道的频带也越宽,但通信的信道宽度是受限的.

2.2 τ_2 的选取

τ_2 是对混沌调制信号 $s(t)$ 进行采样的时间间隔. 对 τ_2 取值有两方面要求: τ_2 应足够小,这样 $s(t)$ 才能尽可能精确地传送到接收端,实现发送、接收端混沌系统的精确同步;同时 τ_2 又要尽可能大,因为 τ_2 越大,则传输 $s(t)$ 所需的数据量越小,信息的传输速率越高. 如果 $s(t)$ 有限带宽,截止频率为 f_c,根据采样定律,要求 $\tau_2 < 1/(2f_c)$. 在图 1 中,若取 $i(t)$ 的截止频率为 $f_s/2$,其中 f_s 是模拟信源 $i_0(t)$ 的抽样频率,由于 τ_1 的取值使得 $s(t)$ 和 $i(t)$ 的频带重合,因而 $s(t)$ 的截至频率也应为 $f_s/2$,因此取 $\tau_2 = \tau_1$.

2.3 A 的选取

A 是在混沌调制模块中为调节输入信号 $i(n)$ 的幅度而设立的放大系数. 对输入信号进行放大,主要目的是改善接收端解调信号 $\hat{i}(n)$ 的信噪比,从而最终提高信号 $i_0(t)$ 的传输质量. $\hat{i}(n)$ 中的噪声来自数字通信系统中的量化噪声以及主要由量化噪声决定的同步误差. 记这些噪声为 $v(t)$,则 $\hat{i}(n)$ 可写成

$$\hat{s}(n) = A^{-1}\hat{s}(t)\big|_{t=n\tau_1} = A^{-1}i(t)\big|_{t=n\tau_1} + A^{-1}v(t)\big|_{t=n\tau_1}$$
$$= i(n) + A^{-1}v(n)$$

这样的 $\hat{s}(n)$ 信噪比可写成

$$SNR_{\hat{s}(n)} = 10\lg\frac{A^2 P_{i(n)}}{P_{v(n)}} = 10\lg\frac{P_{i(n)}}{P_{v(n)}} + 20\lg A \qquad (1)$$

其中 $P_{v(n)}$ 和 $P_{i(n)}$ 分别表示噪声 $v(n)$ 和模拟采样信号 $i(n)$ 的功率. 由图 1 知,由于 $P_{i(n)}$ 值固定不变,在量化间隔数一定的情况下,量化误差和同步误差主要取决于传输信号 $s(n)$ 的统计性质. $s(n)$ 的统计特性主要由混沌系统动力性质决定,故 $P_{v(n)}$ 基本上也保持不变. 所以式(1)右边第一项基本保持不变. 因而增大 A 的值可以明显提高 $\hat{s}(n)$ 的信噪比. 以 2.5s 内通信结果进行统计,其中信噪比估计公式为

$$SNR = 10\log\left(\sum_{n=1}^{N}(\hat{s}(n) - i(n))^2 / \sum_{n=1}^{N} i(n)^2\right)$$

图 5 给出了 $\hat{s}(n)$ 的信噪比的估计值和 A 的关系曲线,结果和式(1)相当吻合.

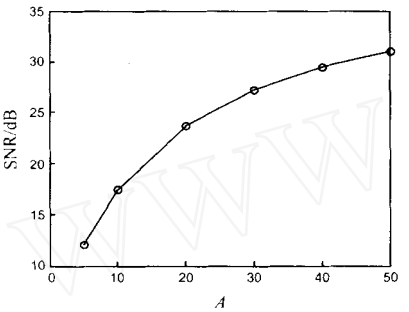

图 5　接收信息信噪比与参数 A 的关系曲线

显然增大 A 可以明显提高通信的质量. 但随着 A 增大,在 τ_1 取值受限的情况下,实现 $s(t)$ 对 $i(t)$ 的掩藏变得困难,因而 A 的取值不能过大.

3　系统性能分析

根据传输信息信号的具体情况,选取参数 $\tau_1 = \tau_2 = 0.01$、$A = 20$. 下面分别考察系统的保密性、信息传输速率和通信质量.

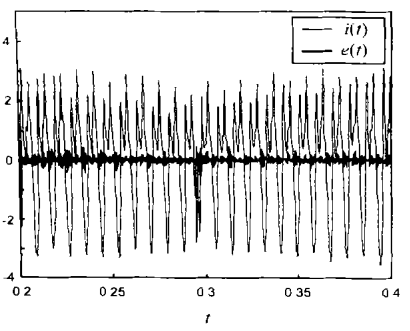

图 6　信息信号 $i(t)$ 和扰动信号 $e(t)$ 波形

混沌通信的保密性曾受到质疑[7],原因是为实现混沌信号对信息信号在频域上的完全掩蔽,要求信息信号的幅值相对混沌信号非常小. 此时信道中的传输信号可以看作含有小扰动(对应于信息信号)的混沌信号,利用混沌信号的确定性动力机制应用相空间方法可以分离出小扰动,即掩藏的信息信号. 在本文中,A 和 τ_1 的合理取值使得 $i(n)$ 在 $s(n)$ 的频域上被完全隐藏,同时 $i(t)$ 的幅值与 $s(t)$ 相当,因而线性滤波和相空间方法都不能提取有效信息. 参照文献[7]的做法,利用相空间方法提取的扰动信号 $e(t)$ 如图 6 所示,该信号形似随机噪声,不包含 $i(t)$ 的任何信息.

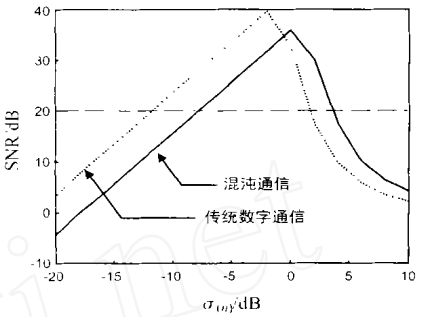

图 7　$\hat{s}(n)$ 信噪比关于 $i(n)$ 功率的关系曲线

本文的通信方案中信息传输速率取决于 τ_2/τ_1 的值,以及量化环节所要求的量化间隔数. τ_2/τ_1 越大、量化间隔数越少,通信速率越高. 图 1 中 $\tau_2 = \tau_1$,因此要达到传统数字通信系统的速率,图 1 系统必须选取与传统数字通信系统相同的量化间隔数. 采用均匀量化器,取量化间隔数 $L = 256$,$i(n)$ 为白噪声形式,得到两种通信系统的 $\hat{s}(n)$ 信噪比关于 $i(n)$ 功率的关系曲线,如图 7 所示. 从中可以看出,在指定的信噪比水平(如 20dB)下,这两个系统的输入动态范围相近(约 12dB),也即量化间隔数相同时,它们的通信质量接近. 因此,与传统的通信系统相比较,本文提出的通信方案在获得较高保密性的同时,系统的信息传输速率和通信质量基本不受影响.

4　结论

本文提出了一种新的利用连续混沌系统进行通信的方案,通过对系统的具体设计以及对系统性能的检验,可以得出如下结论:

(1)将混沌信号以数字形式传输,借助数字通信的可靠性,避免了信道畸变对混沌同步的影响. 发送端和接收端混沌信号之间的误差主要由模拟信号转换为数字信号的量化过程以及连续信号和离散信号互相转换的抽样和插值过程引起. 这些过程中的误差可以人为控制在相当低的水平,能够保证发送、接收端混沌系统以较高精度实现同步.

(2)自由参数 τ_1、τ_2 和 A 的适当取值使通信系统保密性、信息传输速率和通信质量等多种性能得到均衡实现. 与传统的通信系统相比较,在获得较高的保密性的同时,该系统的通信效率和通信质量并没有受太大影响.

(3)本文所提出的混沌通信系统的实现方案仅仅在传统数字通信系统的两端增加了混沌调制和解调环节,因而非常容易实现,从而具有很强的实用性.

参考文献:

[1] Rulkov N F, et al. Synchronization methods for communication with

chaos over band-limited channels [J]. Int. J. Circ. Theor. Appl., 1999,27:555 - 567.

[2] Sharma N, et al. Exploring synchronization to combat channel distortions in communication with chaotic system [J]. Int. J. Bifurcation and Chaos, 2000, 10(4):777 - 785.

[3] Chua L O. Chua's circuit: ten years later [J]. IEICE Trans. Fundamentals, 1994, E77 - A(1):1811 - 1821.

[4] Carroll T L. Communicating with use of filtered, synchronized, chaotic signals [J]. IEEE Trans. Circuits Syst., 1995, 42(3):105 - 110.

[5] Yang T, et al. Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication [J]. IEEE Trans. Circuits Syst. I, 1997, 44(10):976 - 988.

[6] Wu C W, et al. A simple way to synchronize chaotic systems with applications to secure communications [J]. Int. J. Bifurcation and Chaos, 1993, 3:1619 - 1627.

[7] Short K M. Steps toward unmasking secure communications [J]. Int. J. Bifurcation and Chaos, 1994, 4(4):959.

作者简介:

汪芙平 男,1974 年 12 月出生于安徽省东至县,分别于 1997 年和 2001 年在清华大学电机系获工学学士和工学博士学位,目前主要研究领域包括非线性信号处理,混沌通信.

王赞基 男,1946 年 11 月生于福建,清华大学教授,博导,主要研究领域包括电路与系统、非线性信号处理、电力通信等.