文章编号:1004 - 5694(2001)03 - 0014 - 03

基于 Logistic-Map 的数字混沌调制方法*

唐秋玲,覃团发,林硒
(广西大学 计算机与信息工程学院,南宁 530004)

摘　要:离散混沌动力系统 Logistic-Map 产生的混沌离散序列具有良好的统计特性和对初值非常敏感的特性,利用这些特性,提出一种基于 Logistic-Map 的数字混沌调制方法,并构造相应的保密通信系统,且进行了计算机仿真。在此基础上提出了调制系数宽范围变化的数字混沌调制方法。

关键词:Logistic-Map;混沌序列;混沌调制;固定判决函数
中图分类号:O41　　文献标识码:B

Digital Chaotic Modulation Based on Logistic-Map

TANG Qiu-ling, QIN Tuan-fa, LIN Xi
(*College of Computer and Information Engineering, Guangxi University, Nanning* 530004, *China*)

Abstract: Chaotic discrete sequences produced by Logistic-Map have very good statistic properties and are sensitive to first values. Based on Logistic-Map, a kind of digital chaotic modulation method is given. Then corresponding secure communication system is simulated in computer. It provides an access to put forward another modulation method in which modulation correlation can vary widely.

Key words: Logistic-Map; chaotic sequences; chaotic modulation; fixed verdict-function

0　引　言

自从有了通信,人们就开始研究对通信的窃密和保密。目前,现代通信技术向着大容量、高效率、高效能、高可靠性发展,信息自我保密和信息安全传输也在同步发展。其中利用混沌实现保密通信是保密通信和混沌应用研究的一个重要课题。80 年代末期,混沌理论开始受到密码学界的重视,自英国数学家 Matthews[1] 提出混沌加密方法以来,出现了多种混沌序列密码体制,不仅具有自然的良好性能,而且设计异常容易。进入 90 年代后,特别是由于 Pecora 和 Carroll[2,3] 提出了关于混沌自同步理论后,更使这一课题的研究在国内外进入了高潮[4-9]。由于离散混沌动力系统容易用数字电路实现,而且数字电路具有抗干扰能力强、易于加密、易于大规模集成等特点,在通信领域中正逐步取代模拟通信系统。因此,研究数字混沌保密通信具有一定的现实意义。离散混沌动力系统 Logistic-Map 产生的混沌离散序列具有良好的类随机特性,并且对初值异常敏感,利用这些特点对数字信号进行调制,能提供良好的保密性。本文基于 Logistic-Map 混沌系统,采用固定的判决函数,提出了一种基于 Logistic-Map 的数字混沌调制方法,而构造相应的保密通信系统,且进行了计算机仿真。在此基础上提出了适合于宽范围调制的方法。

* 收稿日期:2001 - 05 - 27
基金项目:广西自然科学基金资助项目(桂科字 9912005);广西教育厅资助项目(桂科[1998]334)
作者简介:唐秋玲(1969-),女,广西兴安人,讲师,主要从事计算机通信的研究与开发。覃团发,男,博士,教授,硕导。

1 Logistic-Map 的混沌特性

离散混沌动力 Logistic-Map 的定义为：

$$x_{n+1} = f(x_n) = 1 - \mu x_n^2 \tag{1}$$

式(1)中，μ 是参数，x_n 是状态，f 把当前 x_n 映射到下一个 x_{n-1}，以初始值 x_0 迭代可以得到一个序列 $\{x_n; n = 0,1,2,3\cdots\}$。若选择 μ 限制在[0,2]区间内，则式(1)将是从 $I = [-1, +1]$ 到它本身的一个非线性映射。μ 逐渐增大时，迭代出现多次突变。研究表明，当 $0 < \mu < 0.75$ 时，迭代为稳定的 1 周期；μ 增大到 0.75 时，迭代出现 2 点周期分岔；μ 增大到 1.25 时，出现 4 点周期分岔。这种 2^n 倍周期分岔随 μ 的增大愈来愈快。$\mu = 1.40115$ 时，迅速达到周期 $N \to \infty$，即进入了混沌状态。由此，我们知道，当 $1.41 < \mu < 2$ 时，除了在某些小范围出现周期窗口外，绝大部分区域 Logistic-Map 是混沌的。当系统工作在混沌状态时，输入不同的初始值，可对应产生一个迭代序列，即混沌序列(图 2 是取 $\mu = 2, x_0 = 0.67$ 产生的混沌序列)。Logistic-Map 混沌序列具有良好的统计特性[7]，它的周期无穷大，且对初始值极端敏感，即使初值存在微小的差别，随时间的演化过程中也会不断被放大，最终无法辨认出来。但只要模型、参数和初值完全一致，混沌序列又会重现。利用混沌序列产生的确定性规律，直接从接收信号中提取混沌载波进行解调，可以恢复出隐藏在混沌序列中的有用信号。

2 混沌调制方法

单位阶跃函数以 0 为固定门限，作为判决函数容易实现。为此，基于 Logistic-Map 并采用该固定判决函数，我们构造了一个数字混沌调制通信系统，如图 1 所示。其中需要发送二进制数字信号 $\{s_k\}$，其中 $s_k = 0,1; k = 0,1,2,3,\cdots$。令：

$$u_{sk} = \begin{cases} 0.2, & s_k = 1 \\ -0.2, & s_k = 0 \end{cases} \tag{2}$$

利用混沌系统式(1)，适当选取参数 μ，并引入一个调制系统 h 对输入信号进行调制，为保证调制系统处于混沌状态，使 $\mu(1 + hu_{sk})$ 保持在[1.41,2]之

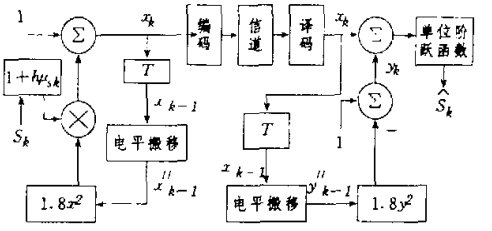

图1 数字混沌调制通信系统

Fig. 1 Digital chaotic modulation communication system

间，我们选取 $\mu = 1.8$，则已调制信号为：

$$x_k = 1 - 1.8x''^2_{k-1}(1 + hu_{sk}) \tag{3}$$

为了拉开接收端电平 Z_k 与判决门限 0 之间的距离，减小判决误差，把发送端绝对值较小的电平进行搬移。搬移门限电平越大，接收端电平 Z_k 与判决门限 0 之间的距离越大，但会增加发送端发送电平 x_k 出现小电平的概率，从而使量化误差增大，故必须适当选取搬移门限电平，我们选取该门限为 0.3，即：

$$x''_{k-1} = \begin{cases} x_{k-1} + 0.3, & 0 \leqslant x_{k-1} \leqslant 0.3 \\ x_{k-1} - 0.3, & -0.3 \leqslant x_{k-1} < 0 \\ x_{k-1}, & \text{其它} \end{cases} \tag{4}$$

取一初值 $x_0(|x_0| > 0.3)$，输入数字信号 $\{s_k\}$，该信号被调制后生成已调制信号 $\{x_k\}$，被编码后从信道发送到接收端。在接收端，若不考虑噪声影响，信号被接收译码后得到的信号为 $\{x_k\}$。信号延迟后设为 y_{k-1}，令：

$$y''_{k-1} = \begin{cases} y_{k-1} + 0.3, & 0 \leqslant y_{k-1} \leqslant 0.3 \\ y_{k-1} - 0.3, & -0.3 \leqslant y_{k-1} < 0 \\ y_{k-1}, & \text{其它} \end{cases} \tag{5}$$

由式(4)和式(5)知 $y''_{k-1} = x''_{k-1}$，故有：

$$y_k = 1 - 1.8y''^2_{k-1} = 1 - 1.8x''^2_{k-1} \tag{6}$$

将 y_k 与接收值 x_k 相减，并考虑噪声的影响，则有：

$$y_k - x_k = 1.8y''^2_{k-1}hu_{sk} + \varepsilon_k = 1.8x''^2_{k-1}hu_{sk} + \varepsilon_k \tag{7}$$

噪声包括信道的传输噪声和发送端信号的量化噪声，若不考虑传输噪声的影响，则 ε_k 为量化噪声，经过式(4)和式(5)的门限处理及适当选取调制系数 h，使得 ε_k 在理想的情况下，可忽略不计。从而有：

$$y_k - x_k = 1.8y^2_{k-1}hu_{sk} = 1.8x''^2_{k-1}hu_{sk} \tag{8}$$

$$s_k = u(y_k - x_k) = s_k \tag{9}$$

其中判决函数 $u(x)$ 是单位阶跃函数，为固定判决函

数，与输入信号无关。根据上式，我们可以判决出解调信号 s_k。

3　计算机仿真

对图 2 的数字混沌调制系统，我们利用 MATLAB 软件在计算机上进行了仿真，调制系数 $h = 0.5$，仿真结果如图 2 至图 5 所示。对照图 3 和图 5 可知，解调后的结果与原输入信号完全相同。

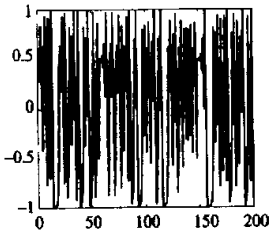

图 2　混沌序列

Fig. 2 Chaotic sequenses

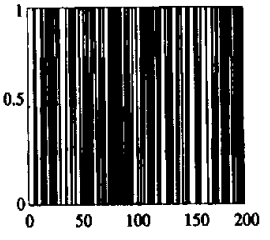

图 3　原输入信号

Fig. 3 Original input signal

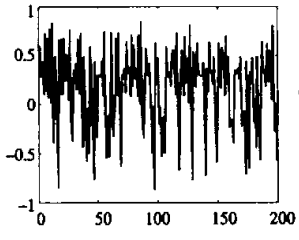

图 4　已调制信号

Fig4. Modutated signal

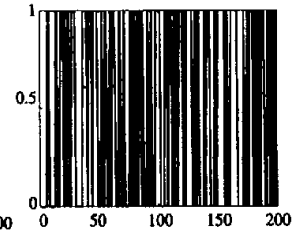

图 5　解调后的输出信号

Fig. 5 Demodulated output signal

4　宽范围的调制方法

在前面提出的混沌调制方法中，为了保证整个调制系统处于混沌状态，因把 $\mu(1 + hu_{ik})$ 限制在 $[1.41, 2]$ 之间，故调制系数 h 的变化范围小。为此，我们提出了一种调制系数 h 能宽范围变化的调制方法，对应的调制系统如图 6 所示。比较第一个调制系统，参数 μ 变为 2，非常明显，$\mu(1+hu_{ik})$ 已超出所讨论的混沌范围 $[1.41, 2]$，已调制信号电平值也超出范围 $[-1, 1]$，故引入限幅机制：

$$x'_{k-1} = x_{k-1} \bmod 1 \tag{10}$$

$$y'_{k-1} = x_{k-1} \bmod 1 \tag{11}$$

然后对 x'_{k-1} 和 y'_{k-1} 进行电平搬移，除此之外，其余各部分均与第一个调制系统相同。

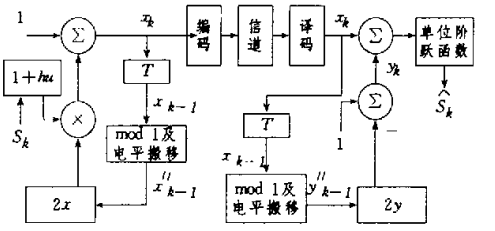

图6　宽范围调制通信系统

Fig. 6 Wide range modulation communication system

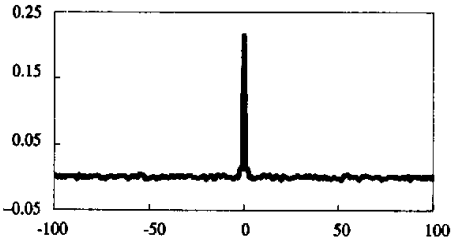

图 7　自相关函数

Fig. 7 Autocorrelation function

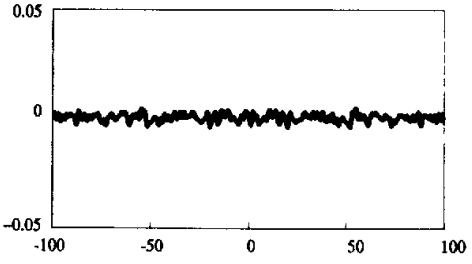

图 8　互相关函数

Fig. 8 Cross correlation function

考虑已调制信号的伪随机特性，我们应用 MATLAB 软件模拟该系统，由随机函数产生随机数字序列 $\{s_k\}$，任取一调制系数 h 和初始值 $x_0(x_0 > 0.3)$ 对输入序列进行调制得到已调制信号。取 $h = 1, x_0 = 0.6$ 对输入序列调制，得已调制信号 1；取 $h = 2, x_0 = 0.6$ 对输入序列调制，得已调制信号 2。图 7 是已调制信号 1 的自相关函数；图 8 是已调制信号 1 和已调制信号 2 的互相关函数，由图 7 和图 8 可知，此时已调制信号的自相关函数近似为 δ 函数，互相关函数近似为 0，具有较好的伪随机特性，从而保密性较强。

5　结束语

本文所提出的混沌数字调制方法，　（下转 45 页）

(上接16页) 充分利用了离散混沌动力系统产生的混沌序列具有类随机性及对初值极端敏感这一特点。利用二进制信息幅度对混沌模型参数进行调制使得有用信息包含在混沌序列之中，而在接收端再利用混沌序列发生的确定性规律完成混沌载波的提取。并通过简单的固定判决函数(单位阶跃函数)对信号进行再生判决恢复出有用信号。另外，由上述两种混沌调制方法构造的保密通信系统密钥为初始值 x_1 和调制系数 h，其中第二种调制方法中调制系数变化范围很宽，这为密钥的选取带来很大的方便；由于引入了电平搬移机制和采用单位阶跃函数作判决函数，因此，极大地降低了量化误差和判决误差，使误码率很低；同时所构造的保密系统结构简单，采用编程或数字硬件电路都易于实现。计算机仿真结果表明，本文提出的混沌调制方法能实现一定的保密性，实用性较强。

参 考 文 献

[1] MATTEWS. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, (4): 29-42.

[2] PECORA L M, CARROLL T L. Synchronization in chaotic system [J]. physRev Lett, 1990, 64: 821.

[3] PECORA L M, CARROLL T L. Synchronizing chaotic circuits[J]. IEEE Trans. on Circuits and Systems, 1991, 38(4): 453-456.

[4] 纪飚，陆佶人. 一种新的混沌同步及保密通信方式[J]. 通信学报，1998，19(9)：47-53.

[5] 周红，凌燮亭. 混沌保密通信原理及其保密性能[J]. 电路与系统学报，1999，1(3)：57-62.

[6] 邓浩，华一满，倪皖荪. 混沌伪随机序列和数字语音保密通信[J]. 通信学报，1999，20(4)：29-35.

[7] 王亥，胡健栋. 改进型 Logistic-Map 混沌序列[J]. 通信学报，1997，18(8)：71-77.

(编辑：郭继笃)