一种实用的混沌保密编码方法

张 勇，陈天麒，陈 滨
(电子科技大学电子工程学院 成都 610054)

【摘要】基于实用符号动力学的基础理论，提出了一种实用的混沌保密编码方法，该方法借助于单峰的logistic映射处于混沌吸引子状态时产生的符号序列作为密钥，对信源编码信号进行加密。使用数字可编程芯片TMS320VC5402实现了实时保密编码，并对混沌符号密钥的相似性作了分析。研究表明，该方法在实际应用中具有推广价值。

关 键 词 符号动力学； 混沌保密； 符号密钥； 硬件实现
中图分类号 TN918.4； O157.4 文献标识码 A

A Practical Method of Chaos Secret Coding

ZHANG Yong，CHEN Tian-qi，CHEN Bin
(School of Electronic Engineering, UEST of China Chengdu 610054)

Abstract Based on the foundation theory of applied symbolic dynamics, we get a practical method of chaos secret coding, i.e. use the strange attractor of logistic map to produce the symbol secret key to modulate the source code. Then, we realize the real-time secret coding on the digital chip TMS320VC5402 and analyze the similarity of symbol secret keys. The results show that this method has extended value for the practical usage.

Key words symbolic dynamics; chaos secret; symbol secret keys; hardware implement

混沌保密通信是混沌应用研究的一个重要课题。基于混沌同步的伴随保密通信方法具有很多不足之处。一方面，用于通信的混沌同步抗噪声和干扰能力太差，研究表明，一旦混沌失去同步，基于混沌同步的混沌保密通信就会失败；另一方面，叠加在同步耦合信号上的有用信号幅度很小，与噪声水平差不多，故同步耦合信号受到噪声污染后，即使收发双方混沌系统仍能够保持同步，也很难恢复出有用信号。这种方法对于几乎不受外部干扰的电路系统同步保密通信是可行的[1]。

混沌保密通信的另一种方法是混沌编码通信。相对于伴随通信方法来说，混沌编码通信属于数字通信的范畴。混沌编码通信已有了较深入的研究，主要有基于动力方程的参数区间化编码方法、不同混沌吸引子间的切换编码和混沌序列区间化编码方法等，文献[2]是在蔡氏电路数字通信上实现的。本文提出一种基于实用符号动力学的基础理论符号加密方法。

1 实用符号动力学

符号动力学可以应用于混沌编码。实用动力符号学的主要研究内容包括8方面[3]：

1) 给出符号序列的排序规则，即比较符号序列大小的规则；
2) 给出“允字条件”，即判断符号序列是否合法(是否属于允许序列)的规则；
3) 产生一定长度内所有允许序列的方法；

收稿日期：2003 – 07 – 02
作者简介：张 勇(1975–)，男，博士生，主要从事混沌信号处理方面的研究.

4) 由已知较短的允许符号序列生成更多更长的合法序列的“合成法则”；

5) 用符号序列计算拓扑熵、复杂性等特征量的方法；

6) 给出各种不同周期轨道的数目和总数；

7) 对于具体的映射，给出计算产生某些类符号字所对应的参数值的方法；

8) 当动力学系统具有某种对称性的时候，参数变化的过程中会出现轨道对称性质的破缺和恢复，给出描述这些现象的方法等。

对于单峰的logistic映射，定义峰点为超稳定点或临界点 C，每一个 x_i 对应一个符号 s_i，记为：

$$s_i = \begin{cases} R & x_i > C \\ C & x_i = C \\ L & x_i < C \end{cases} \tag{1}$$

引用式(1)的规定和混沌吸引子的特性，对于任意一个混沌序列，当参量不同或是初值不同时，将产生完全不同的符号序列。对于logistic映射：

$$x_{k+1} = \mu x_k (1 - x_k) \tag{2}$$

式中 脚标 k 为时间步进单位。由混沌吸引子的特性，不同的 μ 和不同的初始 x_0 将会得到完全不同的符号序列。

在实验中，作如下约定：

$$b_i = \begin{cases} 1 & s_i = R \text{ 或 } s_i = C \\ 0 & s_i = L \end{cases} \tag{3}$$

定义 $\{b_i\}$ 序列为混沌保密编码的混沌序列。

2 混沌编码原理

混沌编码与通信意义上的信源编码和信道编码不同。信源编码可以视为一种信息压缩的编码方式，信道编码以纠错为目的的抗干扰冗余编码，这两种编码方案在目前数字通信中得到了广泛的应用。混沌编码是以保密为目的的编码方案，一般是对信源编码后的数字信号进行的二次编码，混沌编码建立在符号动力学的基础上。目前一维映射的符号动力学已经近似达到完美的程度，高维映射的符号动力学与一维映射的符号动力学有本质的区别，它正处在不断发展的过程中，但这个过程也在不断完善混沌编码的理论。

可以借助于周期轨道的揉序列直接对采样离散信号进行混沌编码，也可以先使用经典编码方法对信源进行编码，再使用混沌符号序列对编码信号进行加密。后者相对于前者来说，更加容易实现。而且，它们均可以使用ASIC技术做成专用的混沌编码器。在通信双方约定了初始值或是参量后，混沌保密通信可以避开混沌同步环节。在一些保密性要求极高的环境下，也可采用自适应或类似跳频通信的方法间歇同步地改变参量或是初始值。

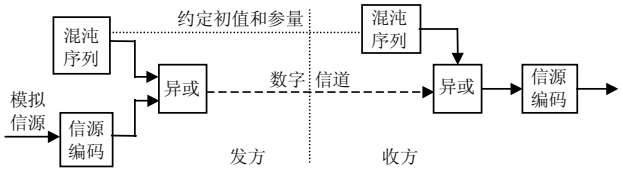

图1 混沌保密数字通信结构框图

混沌保密编码的具体实现步骤为：

1) 使用信源编码方法得到数字信号序列；

2) 约定初始值和参量，使用式(1)～(3)产生出符号序列；

3) 将混沌序列对有用数字信号序列进行调制，如异或运算等，得到保密序列；

4) 接收方收到保密序列后，内部产生出完全相同的混沌序列，进行混沌解码，还原出有用信号序列。混沌保密编码的实现框图如图1所示。

3 实验和相似性分析

3.1 实　验

如图1所示，采用不同的信源编码方案和不同的混沌序列及其初值或参量值就可以得到完全不同的混沌保密序列。实际通信中，可以使用自适应增量调制编码(Adaptive Delte Modrlator, ADM)信源编码和logistic映射，本文采取了脉冲调制编码(Pulse Code Modulator, PCM)编码和logistic映射。实际的硬件实验平台结构框图如图2示，数字信号处理器(Digital Signal Processor, DSP)内部的软件流程框图如图3所示。

图2　实验硬件平台结构图

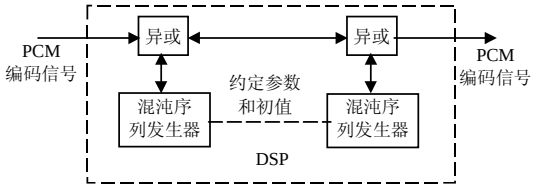

图3　DSP内部完成的软件流程框图

实验中选取了logistic 映射的参数和初值分别为 $\mu = 4.0$ 和 $x_0 = 0.4$，在图2中输入端送入语音信号，在输出端可以听到清晰的语音输出，实时性和保密性很好。

为了更直观地说明问题，下面给出了使用MATLAB的SIMULINK插件绘出的实时动态仿真结果，图4所示为原始PCM语音信号，采样率为22.05 kHz，图5所示为混沌加密后的信号，图6所示为解密后的信号，图7所示为原始PCM信号的频谱，图8所示为混沌加密后的信号的频谱，图9所示为解密后的信号的频谱。所有仿真均假定为在DSP内部完成[4]，故按8位无符号整型数来处理，所以图4～9中可以看到明显的直流分量，图4～6的幅度是没有考虑量纲的8位无符号整型数值。

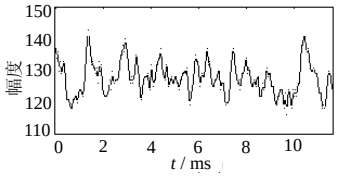

图4　原始PCM信号

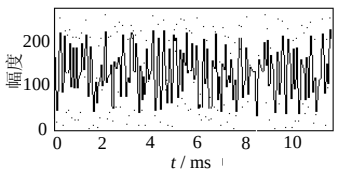

图5　加密后的信号

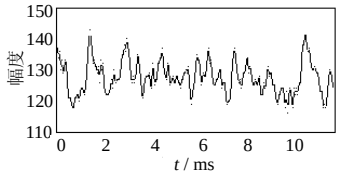

图6　解密后的信号

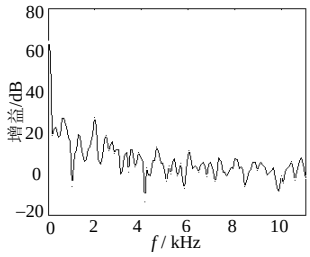

图7　原始信号频谱

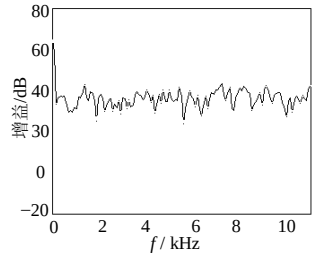

图8　加密后的信号频谱

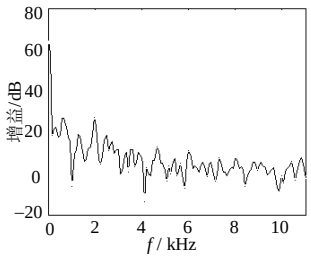

图9　解密后的信号频谱

在实际数字通信系统中，常常还需要作信道编码等抗干扰和噪声的处理。而且，数字信道本身也具有

较强的抗干扰和噪声能力，只要受污染后的数字信号极性不变(即1或–1在接收端能被正确判决出来)，通信就可以正常进行。因此仿真实验没有考虑干扰和噪声的影响。

3.2 相似性分析

给定 $\mu = 4.0$ 时，取初值分别为x_0=0.399 999 99、 $x_0 = 0.4$ 和x_0=0.400 000 01，产生单峰logistic映射处于混沌吸引子状态下的混沌序列，将“0”视为“–1”，3个同时间标准、同长的序列作积并求和。假设序列长度为 N，则当求得结果为 N 时，表示两序列相同；当求得结果为 $-N$ 时，则序列相反。以上两种情况下都易于被窃听，而求得的结果接近于0时则最难被窃听，即使通过建立相空间模型在局部找到了误差只有10^{-8}数量级的初值，也没有任何真正密钥的信息。假设有两个序列 $\{a_i\}_{i=1}^{N}$ 和 $\{b_i\}_{i=1}^{N}$，定义相似性为 $SIM = \left|\sum_{i=1}^{N}(a_i b_i)\right| / N$。当相似性越小时，保密性能越好。设由初值$x_0$=0.399 999 99、$x_0$=0.400 000 00和$x_0$=0.400 000 01生成的序列分别记为$A$、$B$和$C$，$SIM_{AB}$代表序列$A$和$B$的相似性，表1为混沌态时三个序列的相似性分析结果，表中可以看出序列间具有很小的相似性。

表1 序列间的相似性

N	SIM_{AB}	SIM_{BC}	SIM_{AC}
10	0.400 0	0.200 0	0.000 0
10^2	0.140 0	0.040 0	0.060 0
10^3	0.002 0	0.032 0	0.034 0
10^4	0.005 2	0.000 8	0.000 4

事实上，表1的结果也反映了混沌序列具有弱的互相关特性，这个特性比伪随机序列更加优越[5]。另一方面，混沌序列的移位自相关特性要比伪随机序列强一些，但是，窃听方无法获得真正的密钥信息，这个不足可以得到补偿。

4 结 论

本文提出的混沌保密编码方法时间复杂度和空间复杂度都比较小，不但可以在通用数字信号处理器上实现该混沌加密方法，而且可以使用ASIC技术设计专用混沌加密芯片。此外，该方法还克服了传统用于数字通信加密的伪随机序列具有周期性和一定的规律的缺点。

参 考 文 献

[1] Cuomo K M, Oppenheim V. Circuit implementation of synchronized chaos with applications to communications[J]. Phys Rev Lett, 1993, 71: 65

[2] Parlitz U, Chua L O, Kocarev L, et al. Transmission of digital signals by chaotic synchronization[J]. J Bif & Chaos, 1992, 2: 973-977

[3] 郑伟谋, 郝柏林. 实用符号动力学[M]. 上海: 上海科技教育出版社,1994

[4] 张 勇. C/C++语言硬件程序设计——基于TMS320C5000系列DSP[M]. 西安: 西安电子科技大学出版社, 2003

[5] Gold R. Optimal binary sequences for spread spectrum multiplexing[J]. IEEE Trans Inform Theory, 1967,13:619-621

编 辑 漆 蓉