过抽样混沌序列的语音通信加密应用

刘淑聪,姚振静,王 薇,郭纯生,宋燕星

防灾科技学院仪器系,河北三河 065201

摘要 通过对混沌系统特性的研究,设计出一种安全性高、加密速度快的通信加密方案。首先根据数字混沌序列的特性对混沌的迭代过程进行改进,实现对 Chebyshev 混沌序列的过抽样处理。设计语音信号传输系统,在发送端实现混沌序列对语音信号的加密,调制后进入高斯白噪声信道,在接收端接收到密文后对加密语音信号进行解调和解密,得到解密后的语音信号。实验证明,过抽样技术应用在混沌扩频通信中,可以极大地提高无线通信的保密性。

关键词 混沌系统;过抽样混沌映射;混沌加密;系统仿真

中图分类号 TN918.91 **文献标识码** A **doi** 10.3981/j.issn.1000-7857.2011.07.011

Voice Communication Encryption Application of Oversampled Chebyshev Chaotic Sequences

LIU Shucong, YAO Zhenjing, WANG Wei, GUO Chunsheng, SONG Yanxing

Department of Istrument, Institute of Disaster Prevention, Sanhe 065201, Hebei Province, China

Abstract With the development of the multimedia and digital communication, people obtain increasingly more information and communicate with each other much more easily. For protecting information from eavesdropper, the encryption processing for large amounts of data is necessary. Although there are different demands for the encryption algorithm in different applications, however the demand for security and speediness are common. By studying the characteristic of chaotic system, a communication encryption program with high speed and security is designed. To construct encryption algorithm, some improvement has done on the chaotic iteration process according to the characteristic of digital chaotic, the oversampled to the Chebyshev chaotic maps (OSCM) is realized. Also, voice signal transmission systems were designed to encrypt the original voice signals by using the oversample of chaotic sequence at the sending port. After the modulation, the signals passed through the AWGN channel. The encrypted voice signals are demodulated and decrypted after receiving the ciphertext at the receiving port, and then the decrypted voice signal are received. Experiments show that the application of over sampling technology in the chaotic spread spectrum communication can greatly increase the confidentiality of wireless communications.

Keywords chaotic system; oversampled chaotic map; chaotic encryption; system simulation

0 引言

随着网络技术的发展,多媒体通信成为人们信息交流的重要方式,信息的安全与保密显得越来越重要[1-2]。混沌(chaos)是“无序中的有序”,其中有序是指其确定性,而无序则是指其最终结果的不可预测性。它通常是指一类确定性非线性系统长期动力学行为所表现出的似随机性。混沌运动有别于一般的周期和准周期运动,它的运动周期轨道不是单一轨道,而是一簇轨道的包络。混沌系统具有对初始条件的敏感依赖性、长期预测的不可能性和短期预测的可能性、非周期性、有界性、混沌中的有序性等特点[3-4],所以混沌序列非常适合应用于信息加密技术。目前,混沌序列在扩频通信方面的应用研究受到越来越多的关注[5-6]。为了提高通信信息安全性,本文根据数字混沌序列的特性,提出对混沌序列进行过抽样处理,并用于信息加密中。

1 Chebyshev 混沌扩频序列

Chebyshev 混沌映射是一种一维混沌映射,其迭代方程简单,易于实现。k 阶 Chebyshev 混沌映射产生混沌扩频序列映

收稿日期:2010-08-20;修回日期:2011-02-21

作者简介:刘淑聪,助教,研究方向为信号处理,电子信箱:luckycong2009@sina.com

射为[7]

$$x_{n+1}=\cos(2^k\cos^{-1}x_n)\quad x_n\in(-1,1)\quad (k=1,2,\cdots)\qquad (1)$$

这是一个将区间[-1,1]映射到区间[-1,1]的满映射。满映射的绝大多数初值均导致非周期轨道,只有可数无穷多个初值导致不稳定的周期轨道。这可数无穷多个初值所组成的集合的测度为0。于是,除去测度为0的点外,在线段中任取一点作初值,迭代都会趋向混沌轨道。

若将Chebyshev映射产生的混沌扩频序列应用于码分多址扩频系统,需要足够多的扩频地址码序列,但只需将不同的初始值$x_i(i=1,2,\cdots,m)$分配给用户即可,这是因为混沌映射对初始值极其敏感。图1显示当初值分别为0.1和0.10001的8阶Chebyshev函数值,可以看出经数次迭代后,其函数值差别已相当大。

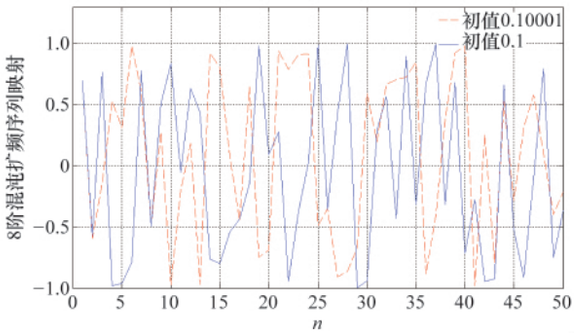

图1　初值为0.1和0.10001的8阶Chebyshev函数

Fig. 1　Eight-steps Chebyshev functions with the initial value of 0.1 and 0.10001

2　过抽样混沌映射特性

2.1　过抽样混沌映射的定义

如果一个混沌映射符合如下关系,则称其为过抽样混沌映射(Oversampled Chaotic Map,OSCM)[6]:

$$x_{n+1}=\underbrace{f(f\cdots(f}_{p}(x_{n\cdot k})))=f^{(p)}(x_n,k)\qquad (2)$$

其中,$x_{n+1}=f(x_n,k)$是一维混沌映射(也称源映射),p为不小于3的自然数。由此可知,过抽样序列是通过对源映射序列进行每隔$p-1$点的抽样实现的新序列,参数p的引用大大增加了映射迭代产生的序列数量。OSCM序列的产生过程本质上可以认为是对时间离散的混沌数字信号序列的抽取过程。这样,对混沌序列的过抽样给混沌序列映射引入了新参数——迭代次数,将原本的一维映射变为了二维映射,由于在每次迭代中会产生信息丢失,增加了混沌序列的复杂程度。即使窃听者知道传送者产生混沌序列的模型和用于迭代的初值,但不知道过抽样率,也很难将信息破译。因此,OSCM序列的安全性较Chebyshev源映射更好,有更强的抗破译性能。基于过抽样的高维映射混沌扩频通信可以有很好的应用前景。图2为Chebyshev混沌序列的OSCM(p=4)序列。

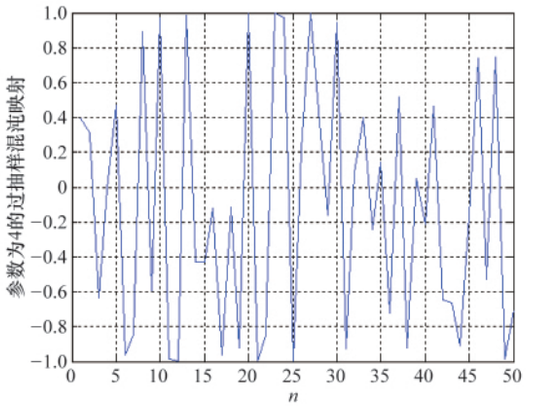

图2　Chebyshev混沌序列的OSCM(p=4)序列

Fig. 2　OSCM (p=4) sequence of Chebyshev chaotic sequence

2.2　过抽样混沌映射的保密特性

OSCM序列不仅是混沌的,而且其混沌性强于源映射序列并随p的增大而进一步增强。因此,过抽样混沌序列具有比源映射序列更强的对初值的敏感性,如图3所示。

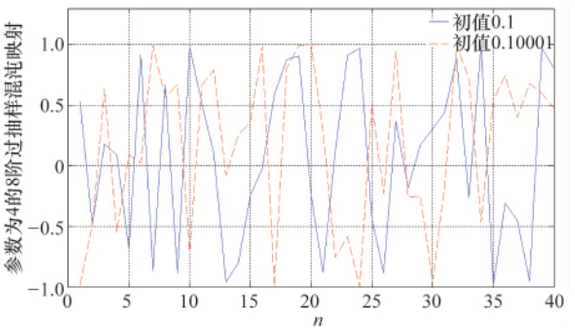

图3　初值为0.1和0.10001的8阶过抽样Chebyshev函数

Fig. 3　Eight-steps oversampled Chebyshev functions with the initial value of 0.1 and 0.10001

由图3可以看出,虽然初值仅相差10^{-5},但得到的两个序列完全不一样。这样的初值敏感性能保证过抽样混沌序列拥有丰富的码元,可用过抽样混沌序列实现多址。

在通信中,窃听者要对直扩调制的信息进行解密,必须了解扩频序列的结构和变化规律。扩频序列产生依靠参数越多,系统的保密性就越好。分析式(2)可以发现,OSCM比一维混沌映射增加了一个参变量p,从而增加了混沌映射的复杂程度,迫使窃听者在解密过程中必须通过截短分析多掌握一个参数。,同时p变化范围可以很大,p每变化一次,都会引起这个序列的巨大改变,很难通过对OSCM序列的截短分析找出其映射函数原型。

3　过抽样序列在语音保密通信中的应用

语音混沌保密通信系统如图4所示。

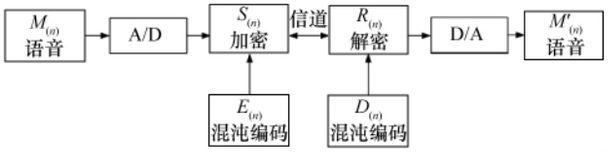

图 4　语音混沌保密通信系统

Fig 4　Voice chaotic secure communication system

通信系统中加密运算过程可表示为

$$S_{(n)}=M_{(n)}\oplus E_{(n)} \tag{3}$$

其中,$S_{(n)}$为加密后的信号,$M_{(n)}$为发送端语音信号,$E_{(n)}$为发送端混沌加密信号,⊕为异或运算符。

接收端解密过程为加密过程的逆运算:

$$M'_{(n)}=R_{(n)}\oplus D_{(n)} \tag{4}$$

其中,$R_{(n)}$为接收端接收到的加密信号,对于理想信道,$R_{(n)}=S_{(n)}$;$D_{(n)}$为接收端的混沌序列;$M'_{(n)}$为解密输出信号。显然,当系统同步时,即 $D_{(n)}=E_{(n)}$时,有 $M'_{(n)}=M_{(n)}$,从而实现语音保密通信。本文采用 Chebyshev 混沌序列与语音信号相混叠的方法实现过抽样混沌加密,在 Matlab 的 Simulink 环境下实现系统的仿真。图 5 为原始语音信号的波形与解密出的语音波形。

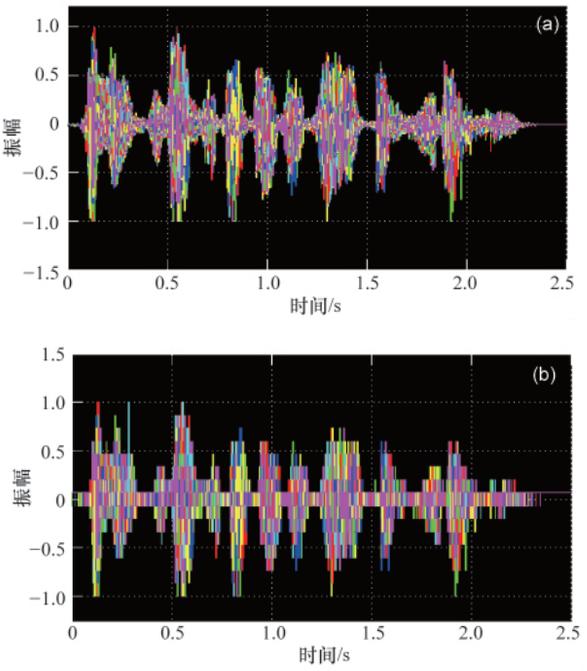

图 5　原始语音信号的波形(a)与解密出的语音波形(b)

Fig. 5　Original voice signal waveform (a) and the decrypted voice waveform (b)

4　混沌扩频系统与 OSCM 扩频系统信号误码率分析

不同信噪比对语音掩盖的程度不同,为了比较原混沌扩频系统与 OSCM 扩频系统作用下通信信号误码率的大小,假定语音信号强度和混沌噪声强度的信噪比一定,即 SNR 为定值,则混沌扩频系统与 OSCM 扩频系统分别解密出的通信信号误码率如表 1 所示。从表 1 可以得出,二者解密出的信号误码率与原扩频序列系统的误码率基本相同。由此可见,过抽样技术在信号加密通信应用中,不仅保持了原系统的准确性,而且进一步增强了通信的保密程度。

表 1　混沌扩频系统与 OSCM 扩频系统作用下语音信号的误码率

Table 1　Bit error rates of voice signals in chaotic spread-spectrum systems and OSCM spread-spectrum systems

SNR/dB	信号误码率/%	
	混沌扩频系统	OSCM 扩频系统
−30	49.97	50.03
−20	49.51	49.53
−10	45.42	45.41
0	18.55	18.78
10	0.001	0.001

当 SNR=0 时,很难从扬声器中听到语音信号,其误码率经仿真得出结果为 18.78%;当 SNR=10dB 时,可以较为清楚地听到解密后的语音信号,其误码率仿真结果为 0.001%,如表 1 所示。

由表 1 和图 6 可以看出,SNR 越高,系统的误码率越低;在 SNR=−10dB 左右,误码率开始急速减小,在 SNR 接近 5dB 时,曲线逐渐平稳。试验表明,在不同的 SNR 下对语音信号进行 OSCM 加密时,当 SNR>5dB 时接收端能够接收到较为清晰的语音信号。因此,在使用过抽样混沌序列对语音通信进行加密时,信噪比宜大于 5dB,此时接收到的语音信号较为清晰,能够较好地实现通信。

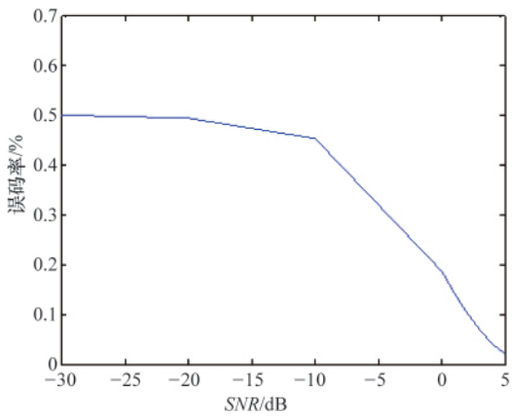

图 6　OSCM 扩频系统中语音信号在不同 SNR 时的误码率

Fig. 6　BER of voice signals in OSCM spread-spectrum systems with different SNR

5　结论

在本文数字语音混沌系统的实现中,密码序列的产生仅

由一个迭代公式和一个初始条件 $x(0)$ 决定。由于混沌序列对初始值的敏感性,微小差异也会导致外加混沌密码序列的很大不同,从而不能实现语音信号的通信,因而以初始条件作为密钥的数字语音混沌系统具有高度的保密性。过抽样混沌映射较一维混沌映射增加了一个参变量 p,增加了混沌映射的复杂程度,进一步提升了系统的保密性。实验证明,过抽样技术在混沌扩频通信中的应用进一步拓展了保密通信的范围,提高了信息安全性,在军事通信和未来个人通信中有广阔的发展前景。

参考文献(References)

[1] 管春阳, 高飞. 一种基于混沌序列的加密算法 [J]. 北京理工大学学报, 2003, 23(3): 363-366.
Guan Chunyang, GaoFei. *Transactions of Beijing University of Technology*, 2003, 23(3): 363-366.

[2] 赵艳红, 张春, 吴楚. 扩频通信中数字混沌序列的产生[J]. 信息工程大学学报, 2000, 1(3): 40-43.
Zhao Yanhong, Zhang Chun, Wu Chu. *Journal of Information Engineering University*, 2000, 1(3): 40-43.

[3] 詹明. 基于混沌的数字保密通信研究[D]. 西安: 西南交通大学, 2004.
Zhan Ming. Reasearch on digital confidentiality communication based onchaos[D]. Xi'an: Southwest Jiaotong University, 2004.

[4] 丁源源. 混沌及其保密通信技术研究[D]. 武汉: 武汉理工大学, 2004.
Ding Yuanyuan. Reasearch on chaos and confidentiality communications technology[D]. Wuhan: Wuhan University of Technology, 2004.

[5] 于银辉, 刘伟, 朱珺, 等. 二相和四相过抽样混沌序列的平衡性[J] . 吉林大学学报: 工学版, 2006, 36(5): 799-802.
Yu Yinhui, Liu Wei, Zhu Jun, *et al*. *Journal of Jilin University: Engineering and Technology Edition*, 2006, 36(5): 799-802.

[6] 吴新平, 范正平, 陈彩莲. 混沌控制及其在保密通信中的应用 [M]. 北京: 国防工业出版社, 2002.
Wu Xinping, Fan Zhengping, Chen Cailian. Chaos control and its application in secure communication [M]. Beijing: National Defence Industry Press, 2002.

[7] 于银辉, 马生忠, 刘卫东. Chebyshev 二相混沌扩频序列平衡性 [J]. 吉林大学学报: 信息科学版, 2004, 22(3): 228-231.
Yu Yinhui, Ma Shengzhong, Liu Weidong. *Journal of Jilin University: Information Science Edition*, 2004, 22(3): 228-231.

(责任编辑　代丽)

·学术动态·

"第二届不确定理论国际会议"征文

由国际不确定理论学会 ICUT 主办,中国运筹学会协办的"第二届不确定理论国际会议"将于 2011 年 8 月 6—11 日在北京召开。

征文范围:Uncertain calculus,Uncertain control,Uncertain differential equation,Uncertain inference,Uncertain logic,Uncertain process,Uncertain programming,Uncertain statistics,Uncertainty theory,Applications in artificial intelligence,Applications in control,Application in data mining,Applications in finance,Applications in industrial engineering,Applications in information science,Applications in machine learning,Applications in management science,Applications in operations research,Applications in risk analysis,Applications in robotics。

征文截止日期:2011 年 4 月 6 日。

联系方式:清华大学数学科学系(100084) Xiaowei Chen;电话:010-62787724;电子信箱:icut@math.tsinghua.edu.cn;会议网址:http://orsc.edu.cn/icut/icut2011/。

·学术动态·

"第十届全国信息隐藏暨多媒体信息安全学术大会(CIHW)"征文

中国电子学会将于 2012 年 3 月在北京召开"第十届全国信息隐藏暨多媒体信息安全学术大会(CIHW)"。

征文内容:信息隐藏理论与模型、软件保护;隐密术与隐密分析、多媒体数据检索及认证;数字水印、无线通信安全;网络信息安全、数据传输安全;数字取证、信息内容安全;密码学、数字版权管理。

联系人:郭老师;电子信箱:service@leaderstudio.net;电话:010-62262770;会议网址:www.leaderstudio.net。