文章编号: 1001-0920(2004)10-1167-04

一种结合猫映射与Logistic映射的语音加密算法

樊 雷, 茅耀斌, 孙金生
(南京理工大学 自动化系, 江苏 南京 210094)

摘 要: 将猫映射(cat map)与Logistic映射相结合, 构造了一种语音加密算法. 该算法首先将语音数据堆叠成二维, 然后利用二维猫映射将数据的位置置乱, 最后利用一维Logistic映射构造替换表, 对数据进行扩散. 密码分析表明, 该算法具有较高的安全性, 能够抵抗统计攻击、差分攻击和已知密文攻击. 与传统的DES算法相比, 该算法加密速度更快, 适用于实时语音加密.

关键词: 猫映射; Logistic映射; 混沌加密; 语音加密
中图分类号: TP13 **文献标识码**: A

Novel voice encryption algorithm jointly using cat map and Logistic map

FAN Lei, MAO Yao-bin, SUN Jin-sheng
(Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China. Correspodent: SUN Jing-sheng, E-mail: sunjs@mail.njust.edu.cn)

Abstract: A voice encryption algorithm combining cat map and Logistic map is proposed. The algorithm first piles voice data up into two-dimensional array, then iteratively uses cat map to scramble positions of the data in the array and diffuses the value of each components through a substitution table derived from Logistic map. Cryptanalysis shows that the proposed algorithm is of highly secure in face of many attacks such as differential attacks, known ciphertext attacks, and etc. Comparing with traditional ciphers, for instance, DES, the new algorithm is superior in encryption speed, which makes it suitable for real time application.

Key words: cat map; Logistic map; chaotic encryption; voice encryption

1 引 言

自Pecora和Carroll发现混沌可以自同步[1]以来, 混沌在保密通信上的应用引起了众多学者的关注[2,3]. 早期的研究主要集中于利用混沌同步的方法对通信信道进行保护, 即首先利用混沌信号的类噪声和宽频谱特性将信息调制到混沌信号上, 然后通过同步混沌信号在接收端将调制的信号解调出来. 但近年的研究发现, 基于混沌同步的保密通信方法存在诸如安全性、可实现性等方面的问题[4]. 其实, 除利用混沌的自同步特性进行信道的保护外, 还可利用混沌的另一些特性来构造密码, 对数字化的信息进行信源加密[5,6]. Shannon指出: 好的加密系统应具有对初始条件的敏感性, 以及能将明文充分置乱并改变其统计特性[4], 而这与混沌的本质特性——混迭特性对初始条件和参数的敏感性相一致. 因此可利用混沌的上述特性来设计流密码或分组密码, 特别是利用混沌的拓扑传递性来快速置乱和扩散明文数据, 以达到改变明文统计特性的目的. 这一

收稿日期: 2003-10-03; **修回日期**: 2004-02-19.
基金项目: 国家自然科学基金资助项目(60174005); 江苏省自然科学基金资助项目(BK2004421; BK2004132).
作者简介: 樊雷(1979—), 男, 江苏大丰人, 硕士生, 从事混沌语音加密的研究; 孙金生(1967—), 男, 吉林伊通人, 教授, 博士, 从事容错控制、网络拥塞控制等研究

点对于多媒体数据的加密尤为重要,因为对于诸如语音、图像、视频这些多媒体信息而言,由于其固有的大数据量、高冗余性等特性,传统的对称和非对称密码不太适用[7].

本文利用猫映射和Logistic映射,构造出一种快速分组加密算法.该算法利用猫映射对数据块中各元素的位置进行置乱,并利用Logistic映射构造替换表,通过对各元素值的替换达到改变数据块统计特性的目的.实验结果表明,该算法具有较高的安全性和快速性,能够抵抗统计攻击、差分攻击、已知密文攻击.

2 基于猫映射和Logistic映射的语音加密算法

猫映射的数学表达式如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod 1. \tag{1}$$

其中:$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$,mod 1表示只取实数的小数部分.为将猫映射用于加密,需要对它进行适当处理.首先将猫映射扩展到$N \times N$矩阵,并进行离散化,有

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N. \tag{2}$$

然后引入加密参数,加密参数可通过改变矩阵A的元素来获得.为保证工程实现的可行性,可采用如下变换阵:

$$A_d = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix}, \tag{3}$$

其中a和b都取小于N的整数.

为在加密过程中使密文的统计特性得到改变,每次扩散操作引入一次替换操作,替换操作是采用混沌的Logistic映射

$$x_{n+1} = 4x_n(1 - x_n) \tag{4}$$

来构造替换表,再用该替换表对置乱后的明文按采样点进行替换.替换表的构造按以下步骤实现:

1) 将区间[0,1]均匀地分成256个子区间$\{s(0), s(1), \cdots, s(255)\}$,每个区间分别赋予一个0～255之间的整数值作为索引,即$V(s(i)) = i$.记$s(i)$的上下界分别为$s_d(i)$和$s_u(i)$,$s(i)$中的任意一个数s满足$s_d(i) \leq s < s_u(i)$.

2) 任取一个初始值,经过N轮迭代后,开始记录迭代结果所在区间,并用这些区间的索引值组成一个整数序列.若第$n(n > N)$次迭代获得的数值在区间s_k中,则得到的整数值为k.如此迭代下去,可获得一个有256个不重复数据的序列$\{k_0, k_1, \cdots, k_{255}\}$,$k_i \in \{0, 1, \cdots, 255\}$.

3) 如果原来相空间分割对应的整数序列为$\{0, 1, \cdots, 255\}$,现在的序列为$\{k_0, k_1, \cdots, k_{255}\}$,则得到的映射关系为$k_i = f(i)$.这就是所要构造的替换表,记为$j = f(k)$.

加密时,首先将一维信号按序堆叠为二维$N \times N$矩阵,然后利用猫映射的混迭特性对二维矩阵的位置进行置乱,也就是以a和b为控制参数,利用式(2)和(3)进行置乱操作.每轮置乱后,利用上述替换表进行一次扩散操作.加密时的扩散操作公式为

$$C_i = f(P_i) \oplus C_{i-1}, \tag{5}$$

其中C_0为初始值,取$C_0 = K$.

解密时,对加密时的替换表逆向输出,得到一个一一映射的逆替换表$k = f^{-1}(j)$.解密时的逆扩散操作公式为

$$P_i = f^{-1}(C_i \oplus C_{i-1}). \tag{6}$$

其中C_0为初始值,取$C_0 = K$.每轮逆扩散后,再进行一次逆置乱操作.逆置乱的猫映射逆变换公式为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A_d^{-1} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \tag{7}$$

其中

$$A_d^{-1} = \begin{bmatrix} 1 & -a \\ -b & ab+1 \end{bmatrix}.$$

最后对二维$N \times N$矩阵按行输出,即可得到解密后的一维信号.

注意到在各种加密模式中,分组大小一般以64位为一组,因此每8个字节设定$C_i = C_0$(若$i \bmod 8 = 0$,则$C_i = C_0$),并在每次循环过程中都改变C_0值.这样在加密时明文改变一位,密文将以8为底数、循环次数为指数进行扩散.

本文采用Visual C++ 6实现了上述猫映射与Logistic映射相结合的混沌分组加密算法,结合PCM和ADPCM编码实现了局域网内的安全语音实时通信.

3 安全性分析

3.1 密钥空间分析

算法中引入如下几个参数作为密钥:

1) 猫映射系统参数a和b:$a > 0$,$b > 0$是自然数,对于8位PCM采样的数据,取$a < 256$,$b < 256$;

2) Logistic映射初始值x_0:是一个双精度浮点型数据,由于计算机字长的限制,在算法的仿真实验中,Logistic映射的计算精度取万分之一;

3) 混迭初始值K:取$0 < K < 256$;

4) 加密轮数 k: 实际使用时一般取 $4 \leq k \leq 8$.

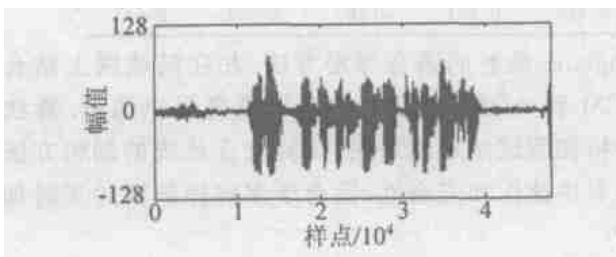
综上可知, 总的可用密钥数为

$$255 \times 255 \times 10\,000 \times 255 \times 5 = 829\,068\,750\,000.$$

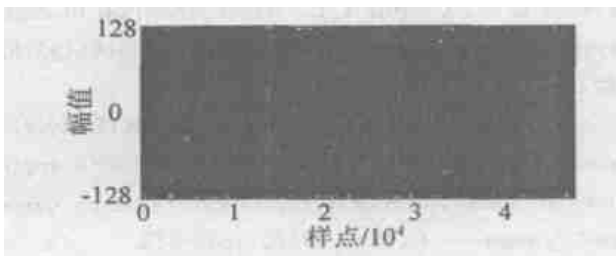
假设密码分析人员采用穷举法以 1 百万次/s 的速度穷举搜索攻击, 则需要大约 230 h 才能完全破译, 这时双方的通话早已结束. 因此, 要想在实时的语音通信环境中尝试如此多的密钥是不现实的. 而这只是在每轮中使用相同密钥的结果, 如果在加密过程中每一轮都使用不同的密钥, 那么随着加密轮数的增多, 密钥的数量将是一个天文数字, 使得密钥被破译的可能性更小.

3.2　密钥敏感性分析

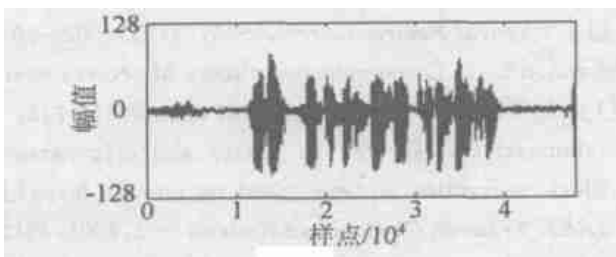
根据分组密码测度中的严格雪崩准则, 改变密钥中的任一比特, 应导致密文分组中大约一半比特的变化[8], 即密钥的雪崩现象. 从图 1 可以看出, 加密后的语音信号与原始语音信号 (PCM 格式, 8 kHz, 8 位采样, 下同) 相比, 已经均匀地分布在取值



(a)　原始语音



(b)　加密后语音



(c)　解密后语音

图 1　原始语音以及加解密后的结果

所属空间; 从图 2 可以看出, 密钥的稍许改变将带来密文的巨大变化. 由 Shannon 对高强度理想密码和唯一性距离的定义[9] 可知, 对于已知密文攻击, 用此种方法加密后的密文对密钥的贡献很小, 即

$$H(K \mid E_1 \cdots E_n) \approx H(K).$$

因此可抵抗统计攻击和已知密文攻击.

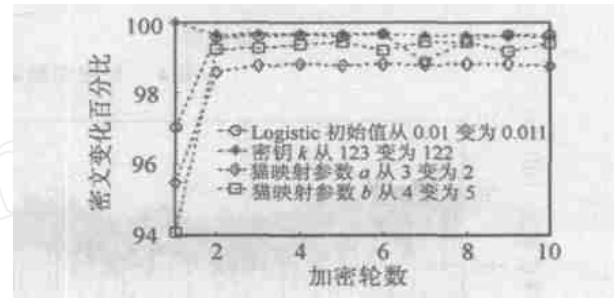


图 2　对密钥的敏感性

3.3　差分攻击分析

根据分组密码测度中的严格雪崩准则, 改变明文分组的任一比特, 将导致密文分组中大约一半的比特变化[8], 即明文的雪崩现象. 在测试语音段的 48 000 个样点中, 每 1 600 个样点随机改变一个样点值的一位后, 密文和原密文随着轮数的改变而变化的情况如图 3 所示. 从图中不难发现, 密文的改变随着加密轮数的增大而迅速上升, 加密轮数大于 4 以后, 密文的改变达到 93.69%. 明文的稍许改变会带来密文的巨大变化, 随着循环次数的增加, 被影响的像素点将呈指数上升, 这增加了差分攻击的难度, 因此可抵抗一定的差分攻击.

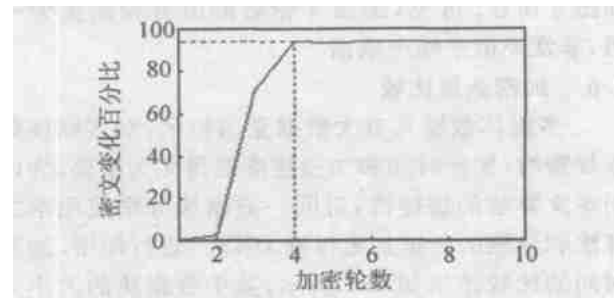
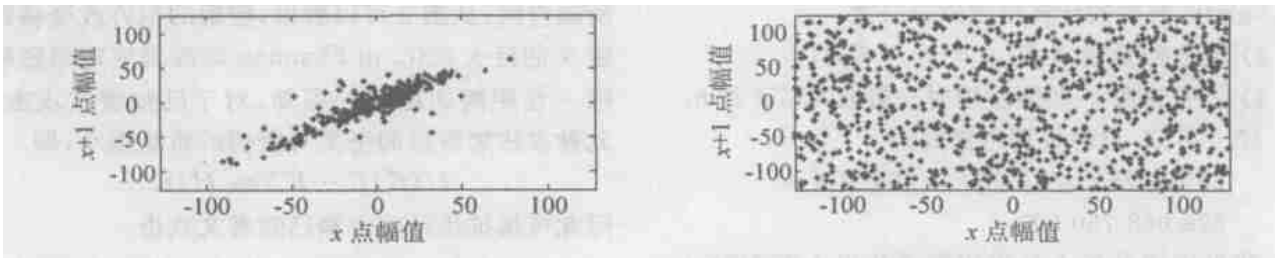


图 3　明文改变一位后密文改变的百分比

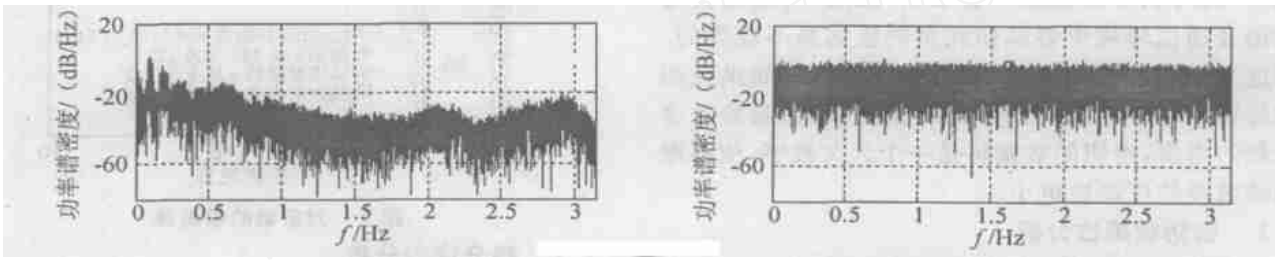
3.4　相关性分析

在测试语音段首先随机选取 1 000 对相邻的语音数据, 记为 (x_i, x_{i+1}), x_i 和 x_{i+1} 分别代表该位置的语音信号采样值; 然后计算二者之间的线性相关系数, 并以相邻两点语音采样值为坐标, 得到加密前后相邻两点语音采样值的相关图 (图 4). 在测试语音段随机选取 1 000 对数据进行试验, 结果是加密前的相关系数一般在 0.9 左右, 而加密后的相关系数一般都降到 0.05 以下. 由此可见, 加密前的语音数



(a) 加密前 (b) 加密后

图 4 加密前后语音相邻两点相关性分析



(a) 原始语音 (b) 加密后语音

图 5 语音频谱图

表 1 加密时间比较

算 法	DES	结合猫映射与Logistic 映射的语音加密							
	加密	1 轮	2 轮	3 轮	4 轮	5 轮	6 轮	7 轮	8 轮
运行时间	0.501	0.070	0.160	0.240	0.320	0.401	0.480	0.551	0.641

据具有强相关性, 经加密后这种相关性被完全破坏, 数据均匀地分布在整个取值空间上.

3.5 频谱图分析

实验参数为: $a = 3, b = 4, x_0 = 0.01, K = 123$. 原始测试语音的频谱和加密 4 轮后的语音频谱如图 5 所示. 可见, 加密 4 轮后的语音频谱更为平坦, 非常类似于噪声频谱.

3.6 加密速度比较

多媒体数据具有大数据量的特征, 对多媒体数据加密时, 加密时间和加密速度显得尤为重要. 为说明本文算法的快速性, 对同一数据块分别使用本文算法和传统的数据加密标准DES[9] 进行加密. 加密时间的比较结果如表 1 所示, 其中数据块的大小为 1 600 000 个字节. 从加密时间看, 用本文算法加密 6 轮仍比DES 加密速度快, 而对本文算法的仿真结果分析表明, 经过 4 轮加密已取得良好的加密效果, 但加密时间只有DES 加密的 64%.

利用该算法, 作者构造了结合PCM 与ADPCM 语音编码的加密方案, 并在局域网内进行语音传输试验, 取得了良好的效果.

4 结 论

本文利用混沌映射特性提出一种结合猫映射与Logistic 映射的语音加密方法, 并在局域网上结合PCM 和ADPCM 编码实现了语音保密通信. 算法分析和测试结果都表明, 该算法比传统的加密方法具有快速性和安全性, 适合于多媒体数据的实时加密.

参考文献(References):

[1] Pecora L M, Carroll T L. Synchronization in chaotic systems[J]. *Physical Review Letters*, 1990, 64(8): 821-824.

[2] Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of Lorenz-based chaotic circuits with applications to communications[J]. *IEEE Trans on Circuits and Systems — II*, 1993, 40(10): 626-633.

[3] Kocarev U, Parlitz L. General approach for chaotic synchronization with applications to communication [J]. *Physical Review Letters*, 1995, 74(25): 5028-5031.

[4] Shannon C E. Communication theory of secrecy system [J]. *Bell System Technical J*, 1949, 28(4): 656-715.

[5] Jakimoski G, Kocarev L. Chaos and cryptography: Block encryption ciphers based on chaotic maps[J]. *IEEE Trans on Circuits and Systems — I*, 2001, 48(2): 163-169.

(下转第 1174 页)

证明 由系统结构的规范分解定理知, 通过引入线性非奇异变换, 可将系统分解为能控能观测、能控不能观测、不能控能观测和不能控不能观测 4 部分, 而输入输出特性只能反映系统的能控能观测部分. 因此, 系统的 BIBO 稳定只是意味着其能控能观测部分为渐近稳定的, 它既不表明也不要求系统的其他部分是渐近稳定的. □

推论 3 设线性定常系统(1) 是能控能观测的, 则其内部稳定性与外部稳定性是等价的.

证明 利用推论 1, 可知由内部稳定性可导出外部稳定性. 根据推论 2 的证明, 可知此时外部稳定意味着内部稳定. □

4 实例验证

给定某粘弹性系统如下:

$$mD^2x(t) + cD^{\alpha}x(t) + kx(t) = u(t),$$
$$x(0) = a_1, \dot{x}(0) = a_2.$$

其中: m, c, k 分别表示质量、阻尼系数和弹性系数; $u(t)$ 表示施加外力; $D^{\alpha}x(t)$ $(0 < \alpha < 1)$ 表示位移函数 $x(t)$ 的 α 阶导数. 取 $m = 1, c = 1.5, k = 1, \alpha = 0.5, a_1 = 0, a_2 = 1, u(t) = 1$ (单位阶跃输入), 则其状态空间描述为

$$D^{0.5}x(t) = Ax(t) + Bu(t),$$
$$y(t) = Cx.$$

其中

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1.5 & 0 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, C = [1 \quad 0 \quad 0 \quad 0].$$

矩阵 A 的特征值为

$$\lambda_{1,2} = 0.7479 \pm 1.0299i,$$
$$\lambda_{3,4} = -0.7479 \pm 0.2407i.$$

显然定理 2 满足, 故原系统是稳定的.

5 结 论

本文讨论了分数阶线性定常系统的外部和内部稳定性条件及其相互关系, 并通过一个粘弹性系统的实例验证了其正确性. 实际上, 分数阶线性定常系统是传统整数阶线性定常系统的推广, 即当系统的微分阶次 $\alpha = 1$ 时, 本文所有关于分数阶系统的结论都与传统整数阶系统是一致的.

参考文献(References):

[1] Miller K S, Ross B. *An Introduction to the Fractional Calculus and Fractional Differential Equations* [M]. New York: John Wiley and Sons, 1993.

[2] Oldham K B, Spanier J. *The Fractional Calculus* [M]. New York: Academic, 1974.

[3] Podlubny I. *Fractional Differential Equations* [M]. San Diego: Academic Press, 1999.

[4] Carpinteri A, Mainardi F. *Fractals and Fractional Calculus in Continuum Mechanics* [M]. Wien: Springer, 1997.

[5] Oustaloup A, Sabatier J, Lanusse P. From fractal robustness to CRONE control [J]. *Fractional Calculus and Applied Analysis*, 1999, 2(1): 1-30.

[6] Podlubny I. Fractional-order systems and-controllers [J]. *IEEE Trans on Automatic Control*, 1999, 44(1): 208-214.

[7] Ikeda F, Kawata S. An optimal design of fractional differential active mass dampers for structures equipped with viscoelastic dampers [A]. *5th Int Conf on Motion and Vibration Control* [C]. Movic, 2000. 223-228.

[8] Tenreiro Machado J A. Analysis and design of fractional-order digital control systems [J]. *J of Systems Analysis, Modelling and Simulation*, 1997, 27(1): 107-122.

[9] 郑大钟. 线性系统理论 [M]. 北京: 清华大学出版社, 1990. 121-124.

(上接第 1170 页)

[6] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps [J]. *Int J Bifurcation and Chaos*, 1998, 8(6): 1259-1284.

[7] Cheng H, Li X. Partial encryption of compressed images and video [J]. *IEEE Trans on Signal Processing*, 2000, 48(8): 2439-2451.

[8] 冯登国, 吴文玲. 分组密码的设计与分析 [M]. 北京: 清华大学出版社, 2000.

[9] Schneier B. 吴世忠, 祝世雄, 张文政, 等译. 应用密码学: 协议、算法与 C 源程序 [M]. 北京: 机械工业出版社, 2000.