基于 Logistic 映射混沌加密算法的研究

韩凤英[1,2]，朱从旭[1]
（1. 中南大学信息科学与工程学院，湖南 长沙 410600；2. 长沙航空职业技术学院，湖南 长沙 410124）

摘要：分析 Logistic 混沌映射的加密算法原理，提出基于该算法的加密方法，并从算法的安全性、效率等方面进行性能分析。最后采用 Matlab 开发工具完成该混沌加密算法的设计，用该算法对实例进行加密仿真。

关键词：Logistic 映射；序列密码；混沌加密
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1671－9654(2007)01－030－05

A Research of Chaos Encryption Algorithm Based on Logistic Mapping

HAN Feng－ying[1,2], ZHU Cong－xu[1]
(1. *Information Science and Engineering College, South Central University, Changsha Hunan* 410600;
2. *Changsha Aeronautical Vocational and Technical College, Changsha Hunan* 410124)

Abstract: It analyses the encryption algorithm principle based on the Logistic chaos mapping, proposes a kind of encryption, and from aspects of algorithm security, efficiency and so on, gives the performance analysis. Finally, it uses the Matlab development kit to complete this design, and carries on the encryption simulation with this algorithm targeting on a example.

Key words: logistic mapping; sequence password; chaos encryption

混沌系统迭代产生的时间序列对初始条件敏感，结构复杂难以分析和预测，可以提供具有良好的随机性、相关性、复杂性的伪随机序列[1]，混沌时间序列理论上具有类随机性，破坏了相关分析的适用性，保密性得以加强。同时混沌系统产生的时间序列密码具有丰富的源泉，应用混沌密码进行加密已成为现代密码学新方向。

1 混沌加密原理

混沌是人们在对某些非线性动态系统的研究中发现的，这个动态系统表现出不可预测性，不可分解性，但又有一定的规律性，它对初始参数有高度的敏感性，初始状态只有微小差别的两个混沌系统在较短的时间后就会产生两组完全不同的、互不相关的混沌序列值[2]。

混沌序列密码系统（见图1）的加密端和解密端是两个独立的、完全相同的混沌系统，两系统间不存在耦合关系。明文信息在加密端加密后直接发往解密端，解密端可以在全部接收后再解密，也可以利用其它技术如线程同步等建立同步关系后进行实时解密。此方法的安全性依赖于混沌信号的超长周期、类随机性和混沌系统对初始状态、系统参数的敏感性。混沌序列密码加密方法灵活多变，可以充分利用混沌信号的特性构造复杂的加密函数。

逻辑斯蒂（Logistic）模型

$$X_{n+1} = uX_n(1 - X_n) \quad (1)$$

该抛物线映射蕴含着现代混沌理论的基本思想，包括倍周期到混沌、分岔图等非线性理论的基本框架和模式[3]。其中，$0 < \mu \leq 4$ 称为分支参数，

收稿日期：2006－10－08
作者简介：韩凤英（1975－），湖南宁乡人，教师，在读硕士研究生，研究方向为信息安全。
朱从旭（1963－），湖南武冈人，副教授，博士，硕士生导师，研究方向为混沌密码学与数字水印技术。

$X_{n+1} \in (0,1)$。当 $1 \leqslant \mu < \mu 1 = 3.0$ 时,系统的稳态解为不动点,即周期1解;当 $\mu = \mu 1 = 3.0$ 时,系统的稳态解由周期1变为周期2,这是二分叉过程;当 $\mu = \mu 2 = 3.449489$ 时,系统的稳态解由周期2分叉为周期4;当 $\mu = \mu 3 = 3.544090$ 时,系统的稳态解由周期4分叉为周期8;当 μ 达到极限值 $\mu_\infty = 3.5699456$ 时,系统的稳态解是周期 2^∞ 解,即 $3.5699456 < \mu \leqslant 4$ 时,logistic 映射呈现混沌状态。当 $\mu = 4$ 时,具有下列典型的混沌特征:

1)随机性。当 b=4 时,Logistic 映射在有限迭代内不稳定运动,随后其长时间的动态行为将显示随机性质。

2)规律性。尽管{Xn}体现出随机性质,但它是由确定性方程(1)导出的,初值 X0 确定后 Xn 便已确定,即其随机性是内在的,这就是混沌运动的规律性。

3)遍历性。混沌运动的遍历性是指混沌变量能在一定范围内按其自身规律不重复地遍历所有状态。

4)对初值的敏感性。初值 X0 的微小变化将导致序列{Xn}远期行为的巨大差异。

5)具有分形的性质。混沌的奇异吸引子在微小尺度上具有与整体自相似的几何结构。

2　混沌加密算法的设计

混沌加密密码是序列密码,混沌序列密码系统(见图1)的加密端和解密端是两个独立的、完全相同的混沌系统,两系统间不存在耦合关系。明文信息在加密端加密后直接发往解密端,解密端在全部接收后再解密方法的安全性依赖于混沌信号的超长周期、类随机性和混沌系统对初始状态、系统参数的敏感性。混沌序列密码加密方法灵活多变,可以充分利用混沌信号的特性构造复杂的加密函数。

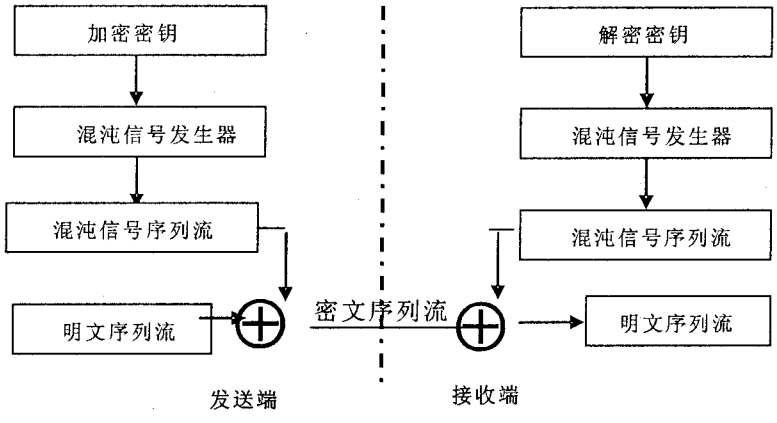

图1　混沌序列密码系统

3　混沌加密算法的优点

1)安全性高

混沌系统对初始值和参数非常敏感,可以提供很大的密钥集合,完全满足加密的需要,通过对混沌系统生成的二进制序列进行检验,0和1的分布均匀,游程符合随机数要求,可以认为是随机序列,而且混沌加密属于流密码,对分组加密的攻击方法是无效的,同时对选择明文密文攻击方法,由于混沌的单向性和混沌信号的迭代处理,异或操作后密钥流的推断几乎不可能[4]。

2)代价小

算法的代价包括时间代价和空间代价,时间代价又分为准备时间和加密时间。通常,加密前的准备时间主要是用来完成生成子密钥,加密时间主要是在子密钥的控制下对明文数据进行变换,混沌加密属于流密码的范畴,它的准备时间非常短;加密时由于只对数据的各个位进行异或操作,其时间主要花费在密钥流的生成操作上,相对于目前流行的分组加密算法,其时间花费也是很少的。空间代价分为算法实现的静止空间和运行态空间 L。静止空间指算法变成程序后本身所占用的空间,一般表现为执行代码的长度。运行态空间指在加密过程

中算法所需要的临时空间。混沌加密算法没有 S-box 空间,临时变量也比较少,而且,它通过循环产生密钥流,循环过程中需要寄存的变量有限,因此,其运行时占用的空间很少,在空间代价上是比较优秀的[2]。

3)易于实现

混沌加密算法其加密和解密过程是可以重用的,这样其所占用的空间大大缩小 它的软件和硬件实现特性都比较好,可用 C、C++、Java、Matlab 等语言实现算法。

4 混沌加密算法的具体实现

在混沌加密算法的实现中,主要考虑混沌信号的序列流如何得到,为了得到混沌序列流,设计了以下的方法(如图2)。

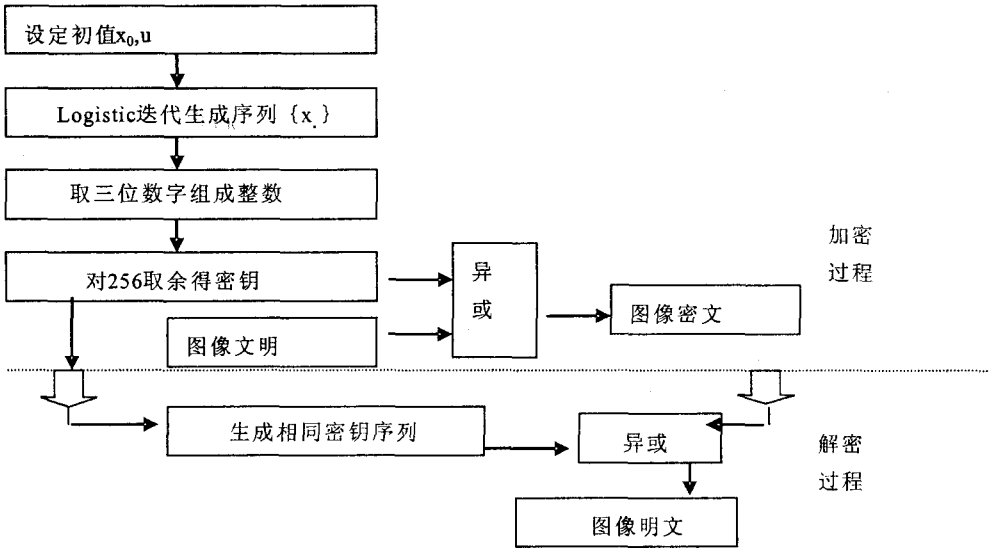

图2 混沌加密算法

5 仿真实例

选择 Lenna 图像(64×64),选择密钥参数分别为 u=3.58,X0=0.278,将此方法用 Matlab 仿真,其仿真结果如下:图3是原始图像,图4是用此方法加密后的结果,图5是用此方法解密后的结果。

图3 原图

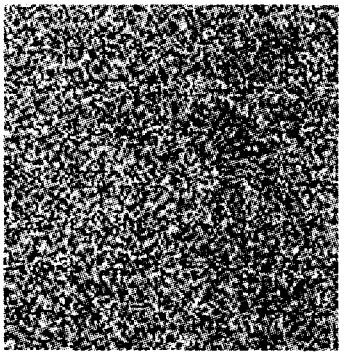

图4 加密后

图5 解密后

从上图可以看出,加密后的图像没有留下原图的痕迹,而解密后的图像与原图像看不出差别,此方法加密效果良好。

6 结束语

介绍了基于 logistic 映射的混沌加密算法的设计与实现。混沌作为信息加密的伪随机序列发生器,是可靠的,而且一维混沌系统(如 logistic 映射)

具有形式简单、产生的混沌时序时间短等优点,有着广泛的应用前景。但是一维混沌系统的随机性有限,产生的密钥空间太小,现在对具有多个指数的超混沌系统的研究越来越多,使用多混沌系统进行加密可以成倍增强系统的安全性。

参考文献:

[1] SCHUSTER HG.. Deterministic Chaos, An Introduction (Second Revised Edition) [M]. Federal Republic of Germany: VCH, 1988.

[2] Baptista MS. Cryptography with chaos[J]. Physics Letters A, 1998(8):50~54.

[3] 黄润生. 混沌及其应用[M]. 武汉:武汉大学出版社, 2005.

[4] 丘水生. 混沌保密通信的若干问题及混沌加密新方案[J]. 华南理工大学学报, 2002(11).

[5] 邓绍江. 基于Logistic映射混沌加密算法的设计与实现[J]. 重庆大学学报, 2004(4).

[6] SCHNEIER B. 应用密码学协议算法与C源程序[M]. 北京:机械工业出版社, 1996.

[7] 郝柏林. 从抛物线谈起——空气动力学引论[M]. 上海:上海科技教育出版社, 1997.

[8] 邓绍江, 李传东, 等. 基于耦合Logistic映射的伪随机位发生器及其在混沌序列密码算法中的应用[J]. 计算机科学, 2003(12):95~98.

[9] 王育民, 刘建伟. 通信网的安全——理论与技术[M]. 西安:西安电子科技大学出版社, 1999.

[10] 邓绍江, 李传东. 混沌理论及其在密码学的应用[J]. 重庆建筑大学学报, 2003, 25(5):123~127.

[责任编辑　刘　敏]

(上接第29页)工程训练中心通过测试并投入实验教学中。实践结果证明,该PLC变频调速模型电梯系统具有很高的教学实用性,能够很好地帮助学生学习PLC课程并使其对控制系统有感性认识。

参考文献:

[1] 田瑞庭. 可编程序控制器技术[M]. 北京:机械工业出版社, 1995.

[2] 蔡行建, 黄文钰. 深入浅出西门子S7-200PLC[M]. 北京:北京航空航天大学出版社, 2003.

[3] 肖工赠, 蒋胜泉. VVVF变频器在电梯系统改造中的应用[J]. 华东地质学院学报, 2000(3).

[4] 黄立培, 张学. 变频器应用技术及电动机调速[M]. 北京:人民邮电出版社, 1998.

[5] 宗群, 雷小峰, 等. PLC在变压变频调速电梯控制系统中的应用[J]. 电气传动, 1999(2).

[责任编辑　刘　敏]