文章编号:1000 - 582X(2004)04 - 0061 - 03

基于 Logistic 映射混沌加密算法的设计与实现*

邓绍江,肖　迪,涂凤华
(重庆大学 计算机学院,重庆　400030)

摘　要:序列密码作为主要密码技术之一,它的的安全强度完全决定于它所产生的伪随机序列的好坏。混沌系统能产生具有对初值敏感、难以预测的性能良好的伪随机序列,所以很适于序列密码。通过对基于 Logistic 混沌映射的加密算法原理的分析,提出了一个基于该算法的加密方法,并从算法的安全性、效率等方面进行了性能分析。最后采用 Visual C++开发工具完成了该混沌加密算法的设计,并用该算法对一个实例进行了加密。

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

1　混沌加密原理

混沌现象是非线性确定性系统中的一种类似随机的过程,把两个十分相近的初值带入同一个混沌函数进行迭代运算,经过一定阶段的运算后,数值序列变得毫不相关。它隶属于确定性系统却难于预测,隐含于复杂系统但又不可分解,看似"混乱无序",实则颇有规律。混沌信号的非周期性、连续宽带频谱、类似噪声的特性,使它具有天然的隐蔽性;对初始条件高度敏感,又使混沌信号具有长期不可预测性。混沌信号的隐蔽性、不可预测性、高复杂度和易于实现等特性都特别适用于保密通信。

Logistic 映射是一个典型非线性混沌方程,它虽然简单却体现出混沌运动的基本性质。

Logistic 映射如式(1):

$$X_{n+1} = bX_n(1 - X_n) \quad X_n \in [0,1] \qquad (1)$$

其中 b 为控制参量,b 值确定后,由任意初值 $X_0 \in [0,1]$,可迭代出一个确定的时间序列 $X_1, X_2, \cdots, X_n$,对于不同的 b 值,系统(1)将呈现不同的特性,随着参数 b 的增加,系统(1)不断地经历倍周期分叉,最终达到混沌。称当 $b=4$ 时由系统(1)产生的序列 $\{X_n\}$ 运动形式具有典型的下列混沌特征:

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 $\{X_n\}$ 体现出随机性质,但它是由确定性方程(1)导出的,初值 X_0 确定后 X_n 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 X_0 的微小变化将导致序列 $\{X_n\}$ 远期行为的巨大差异,如图 1 所示。图 1 是两个初值 $X_{10}=0.100\,001$,$X_{20}=0.100\,002$ 以迭代 30 次得到序列 $\{X_{1n}\}$ 和 $\{X_{2n}\}$。可以看出,虽然初值相差 1.0e - 6,但迭代 30 次后两个序列便完全不一样了。

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。

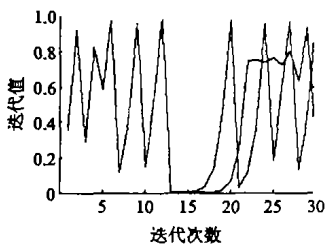

图 1　取 $X_{10}=0.100\,001$,$X_{20}=0.100\,002$ 作为初值迭代 30 次

* 收稿日期:2003 - 11 - 15
基金项目:重庆大学基础及应用基础研究基金资助项目(717411039)
作者简介:邓绍江(1971 -),男,重庆人,重庆大学博士研究生,主要从事信息安全方面的研究。

2 混沌加密算法的设计

混沌是一种确定性系统，除了用物理系统可以实现外，混沌的数学模型也适合用计算机来实现混沌迭代运算。笔者采用计算机实现混沌系统，可以回避构造物理同步混沌系统时面临的技术难题。在普通的计算机上即可实现，可以直接用于计算机网络的保密应用。计算机系统中可以精确地重现混沌迭代系统的所有初始状态，用计算机进程同步的思想实现混沌迭代系统的同步算法。初始状态和同步策略就是密码，这是物理混沌模型不具备的特点，所以不需要使用复杂的物理混沌同步控制方法。

混沌加密密码实际是一种序列密码。混沌序列密码系统(见图 2)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，也可以利用其他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。

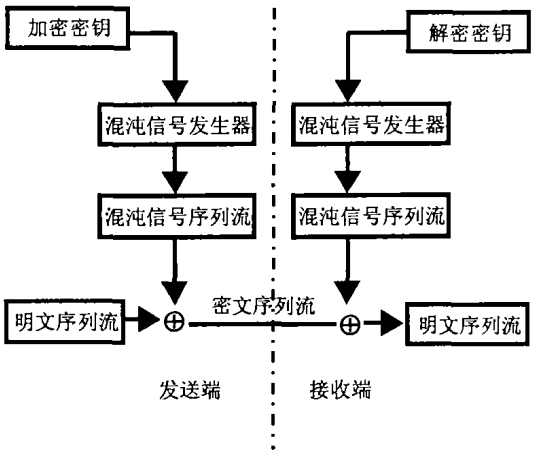

图 2 混沌加密原理

3 混沌加密算法优点

1) 安全性高

由于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，完全满足加密的需要。并且由于混沌的遍历特性，可以使得密钥均匀地分布在密钥空间中。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，可以认为是随机序列。

2) 代价小

评定一个算法的优劣，必须看它的空间代价和时间代价。在时间代价上，混沌加密实际上属于流密码的范畴，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，根据分析，相对于目前流行的分组加密算法，其时间花费也是很少的。在空间代价上，分为算法实现的静止空间和运行态空间。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。

3) 易于实现

混沌加密算法可以用来加密和解密，同时也可以用作随机数发生器。笔者提出的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。

4 混沌加密算法的具体实现

在混沌密码方法的实现中，主要要考虑混沌信号的序列流如何得到，为了得到混沌序列流，首先我们设计了下面的方法：选取一个迭代的初始值 X_0 和参数 b，让 Logistic 公式迭代 M 次，得到 X_1，取出 X_1 的第 2、4、6 位组成一个整数并与 256 求余得到 X'_1，用 X'_1 与明文做异或运算得到该明文的密文 c。然后在对 Logistic 公式进行迭代进行对第二个明文的加密，以此类推直至整个明文加密完毕。

笔者把此方法用 C++做了实现。图 3，图 4 是用此程序实现的加密结果。

序列密码是主要密码技术之一，它的主要原理是，通过有限状态随机产生性能优良的伪随机序列，使用该序列加密信息流得到密文序列。一种伪随机序列产生的重要原则是：所产生的序列应该有较好的随机性和不重复性，每个密钥值之间又要有一定的相关性以便于解密函数的操作。序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏，而用混沌函数可以产生性能良好的伪随机序列，这些序列具有对初值的敏感性、难以预测性、可重复性等特性，故可用作密钥序列对明文进行加密。本文介绍了一类产生混沌随机序列的函数系统 Logistic 系统，进一步介绍了基于Logistic 系统的混沌数据加密方法，同时用 C++语言实现了该算法，并进行了安全性分析。

图 3 加密前的文本

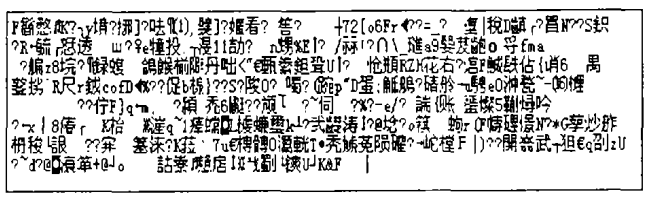

图 4 加密后的文本

5 结束语

介绍了基于 logistic 映射的混沌加密算法的设计与实现。可以看出，混沌作为信息加密的伪随机序列发生器，是可靠的，而且有着广泛的应用前景。但是，一维混沌系统的随机性有限，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] 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.

[2] 白少华. 一种基于 Lorenz 系统的混沌加密算法的设计和分析[J]. 科技情报开发与经济，2003，13(5)：192－193.

[3] 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.

[4] 邓绍江，李传东，廖晓峰. 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.

[5] 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.

[6] 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.

Design and Implementation of Chaos Encrytion Algorithm based on Logistic Formula

DENG Shao-jiang, XIAO Di, TU Feng-hua

(College of Computer, Chongqing University, Chongqing 400030, China)

Abstract: The security of stream cipher, which is known as one of the main cipher techniques, dependents completely on the quality of generated pseudo-stochastic sequences. Chaotic systems can produce the pseudo-stochastic sequences with the properties of excessive dependence on initial conditions and the difficulty in forecasting, therefore, these systems are suitable to the stream cipher. A new encryption algorithm is proposed by analyzing the principle of the chaos encryption algorithm based on logistic formula. Moreover, the security and performance of the proposed algorithm is also estimated. Finally, an example is given to demonstrate our method via the Visual C++.

Key words: logistic formula; stream cipher; chaos encryption

(编辑　张　苹)