一种基于双混沌映射的加密算法设计与应用 *

李 恩, 吴 敏, 熊永华
(中南大学 信息科学与工程学院, 长沙 410083)

摘 要: 提出了一种基于 logistic 和 Henon 的双混沌映射加密算法,通过级联一维混沌系统和二维混沌系统,利用复合迭代所产生的混沌序列对明文进行加密,开发了算法的模拟实验平台。实验结果表明,与传统 DES 和基于 Lorenz 的加密相比,该算法在加密强度和运算效率上达到了较好的均衡。

关键词: 逻辑映射; Henon 映射; 混沌映射; 加密; 解密
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2009)04-1512-03

Design and application of encryption algorithm based on double chaos map

LI En, WU Min, XIONG Yong-hua
(*School of Information Science & Engineering*, *Central South University*, *Changsha* 410083, *China*)

Abstract: The paper presented an encryption algorithm of double chaotic map based on logistic and Henon. By cascading one-dimensional chaos system and two-dimensional chaos system, used chaotic series produced by composite reconstruction in encryption for plain text. It exploited the simulated experiment platform of the algorithm. Compared with conventional DES encryption and encryption algorithm based on Lorenz, the simulation shows that the new algorithm has good performance in balancing encryption intension and operation efficiency.

Key words: logistic map; Henon map; chaos map; encryption; decryption

混沌现象是一种由确定性系统产生、对初值极为敏感、类似随机的过程,混沌信号具有类噪声、宽频谱等特性,非常适合于序列加密[1,2],因此将混沌理论应用于加密,已成为近年来的一个研究热点。混沌理论是一门新兴的交叉理论,其应用于密码学上,具有保密性强、随机性好、密钥量大、更换密钥方便等特点;此外,在抗干扰性、截获率、信号隐蔽等方面同样具有潜在的优势。尽管混沌加密具有上述特点和优势,但目前混沌理论在密码学上的实际应用中还存在诸多难点与问题,如混沌系统在计算机或其他数字系统实现时,由于对混沌映射的参数和状态模拟精度的限制,使混沌序列表现出短周期、强相关及局部线性的缺点,在较小精度实现下的混沌系统不适合加密。

为解决上述混沌系统安全稳定应用方面的问题,国内外研究人员从提高保密性能出发进行了许多的探索和研究。例如文献[3,4]将混沌加密与常规加密级联,利用混沌信号不可预测性以及常规密码系统的成熟密钥空间设计技术和安全性易于评估的特性,设计出的混合密码使两类系统优点互补,但这样的系统大多是通过硬件实现的,因其运算量大,对硬件要求较高;文献[5,6]将多个混沌模型混合,该算法密钥空间大、对明文和密钥敏感,可以抵抗利用差分特性、统计特性和相空间重构对系统进行的攻击,但该算法选用多个混沌模型后,也同样导致计算量大增,仅适合于对安全性较高的场合;文献[7,8]通过伪随机序列加入扰动,使得混沌加密序列的周期更长、复杂度更高,但其参数选择和判定目前还存在一定的困难。因此,现有的对混沌理论加密的研究,往往只考虑到安全性,而没有顾及到算法的运算效率,或过多地考虑运算效率而忽视了算法的安全强度,在实时性高的场合应用难度较大。

1 双混沌映射的加密与解密模型

混沌加密是利用混沌系统产生混沌序列作为密钥序列,利用该序列对明文加密,密文经信道传输到接收方;混沌是确定的,由非线性系统的方程、参数和初始条件完全决定,只要系统参数和初始条件相同,可以完全重构出来,因此接收方容易构造出与发送方同样的混沌系统,实现同步,从而将明文信号提取出来实现解密[9]。目前已有很多混沌和超混沌系统模型供人们研究。其中一维的有 logistic 映射混沌系统[10]、Tent 映射[11]等;二维的有 Cat 映射[12]、Dufing 方程[13]等;三维的有 Lorenz 系统[14]、蔡氏混沌系统[15]等;四维的有 Rossler 超混沌系统等[16]。三维和四维的高维混沌系统相对于一维和二维的混沌系统有更大的密钥空间,其安全性较高,但其用到较频繁的浮点运算,对计算机的计算精度要求高,同时也降低了计算速度。由于高维混沌系统的应用尚处于不成熟阶段,一维 logistic 映射和二维 Henon 混沌系统更加适合于广泛应用。

1.1 Logistic 映射与 Henon 映射

1) Logistic 映射 该映射由生物学家 R. May 于 1976 年提出,是一个简单又具有重要意义的非线性迭代方程[10]: $x_{n+1} = \mu x_n(1-x_n)$。其中: $x_n \in (0,1)$; 控制参数 $\mu \in (0,4]$。该方程形式是完全确定的,也不包含任何随机因素,当 $3.569\,945\,6 < \mu \leqslant 4$ 时,由该映射产生的序列呈现出混沌态;当取 $\mu = 4$ 时,获得典型的 logistic 映射: $x_{n+1} = 4x_n(1-x_n)$。

收稿日期: 2008-07-19; **修回日期**: 2008-09-09 **基金项目**: 国家杰出青年科学基金资助项目(60425310)

作者简介: 李恩(1979-),男,湖南双峰人,硕士研究生,主要研究方向为多媒体通信与信息安全(hunanlien@163.net);吴敏(1963-),男,广东化州人,教授,博导,主要研究方向为鲁棒控制与智能系统;熊永华(1979-),男,湖北洪湖人,讲师,博士研究生,主要研究方向为多媒体通信与信息安全.

Logistic 映射的优点可概括为:a)对初始值非常敏感。对于相差 10^{-16} 的初始值,迭代出来的轨迹差别也十分明显;混沌动力系统具有确定性,给定相同的初始值,其相应的轨迹肯定相同,可以轻而易举地获得数量极多的非相关序列,因此一般情况下,很难从一段有限长度的序列来推断出混沌系统的初始条件。b)形式简单。只要混沌映射的参数和初始条件就可以方便地生成、复制混沌序列;不必浪费空间来存储很长的整个序列。c)具备白噪声的统计特性,可以用于需要噪声调制的众多应用场合。

总体来看,logistic 混沌模型的迭代方程简单,混沌加密参数只有一个,这决定了其加密运算速度很快,特别比高维的混沌系统要快很多,但其密钥空间较小,安全性稍差。

2)Henon 映射　天文学家 Henon 从研究球状星云团以及从 Lorenz 吸引子得到启发,在 1976 年提出了一个二维非线性混沌系统。其方程如下[17]:

$$\begin{cases} x_{k+1} = 1 + y_k - ax_k^2 \\ y_{k+1} = bx_k \end{cases} \tag{1}$$

其中,当 $1.05 < a < 1.8$,$b = 0.3$ 时,系统产生混沌现象。Henon 映射的一大特点是对初始值有极其敏感的依赖性。将其对初值的敏感性充分体现在加密算法对明文和密钥的扩散性与混乱上,只要算法在初值或明文上有很小的改动,所得到的密文就"面目全非"。此外,Henon 映射还具有优良的伪随机性,其轨道的演化是非周期、不收敛的,具有很好的随机性和不可预测性。由于 Henon 映射是一个具有两个参数的平面映射族,且只有一个非线性项,该映射可称为高维情形中最简单的非线性映射。

从混沌理论可知,二维的 Henon 映射产生的混沌伪随机序列完全满足均匀分布、δ-link 的自相关、O 互相关的性质。本文应用经典的 Henon 映射,主要是基于三个方面的原因:a)理论上对其混沌行为的研究比较深入;b)它具有很好的密码学特性;c)Henon 映射是二维的,可提供的密钥空间比较大。

1.2　双混沌映射模型框架

基于单一混沌系统或多个混沌系统的混沌加密算法,其设计的关键是对混沌映射的选择,不同的混沌映射在算法实现复杂度、算法时间和空间复杂度以及安全性等方面都有较大差异。本文所提出双混沌加密算法就是从算法的实现、速度和安全性考虑,既能达到较小的时间和空间复杂度,又能有较大的密钥空间和较高的安全性,避免单混沌系统可能出现的信息泄露问题。由此将 logistic 加密速度快和 Henon 的参数选择范围广、密钥空间大的特点结合起来,提出一种基于 logistic 混沌映射和 Henon 映射的混沌系统。其混沌加/解密框图如图 1 所示。

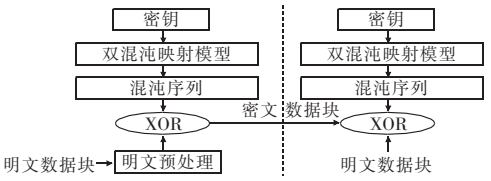

图 1　双混沌映射加密解密框图

不同的文件内部格式不一样,但任何文件都是以二进制形式存放在计算机中的,这一特性使得系统能够处理不同类型的文件。用户首先对明文数据进行预处理,通过编程以二进制的方式打开文件;然后选用初始值和输入参数,并将这些数作为双混沌映射模型的密钥,从而得到一个混沌序列;混沌序列与明文数据进行异或运算得到密文;解密过程与加密过程基本对应,通过双混沌映射模型,用相同的密钥输入得到混沌序列与密文异或计算得到明文。

1.3　加密与解密算法

图 1 中所提到的双混沌映射模型详细设计如图 2 所示。选定 Henon 和 logistic 映射的初始值 x_0、y_0 和三个内部参数 a、b、u 作为密钥,算法中的 x_n、y_n、x'_n 为中间迭代结果。具体算法如下:

a)针对式(1),先选定 Henon 映射的初始值 x_0、y_0 和两个参数 a、b 作为密钥。

b)迭代 10 次,得到 x_n、y_n。

c)将 $x_0 \times y_0$ 的乘积值 M 取绝对值,将 $|M| - [|M|]$ 得到的数作为 logistic 方程 $x_{n+1} = \mu x_n(1 - x_n)$ 的初始值,并以 u 为参数。如果 $|M| - [|M|] = 0$,则返回到 a),重新输入初始值或参数。

d)迭代 10 次,得到 x'_n。

e)计算 $x'_n \times 100$,并取乘积的 2,4,6,8,10 位组成一个五位二进制数与 256 取余,得到一个位密钥流,与明文作异或运算,就形成一个密文字节。

f)迭代 10 次,得到 x_{n+1}、y_{n+1}、x'_{n+1},反复执行 e)和 f),直到所有明文字节都加密完毕。

其中:b)和 d)迭代次数保证了 Henon 映射和 logistic 映射都进入混沌迭代状态,而为了保证运算速度,次数仅选 10 次;步骤 c)是为了保证 logistic 映射输入初始值为 0 ~ 1 的数。

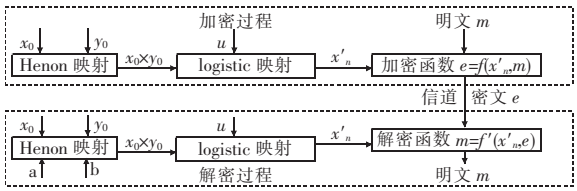

图 2　双混沌映射模型图

2　实验结果与性能分析

2.1　实验平台设计

双混沌映射加/解密实验平台主要要求能够读取图片,然后选择双混沌加/解密算法对图片进行加密、解密、显示、存储、传输等操作,并记录各种算法的相关性能参数。实验平台的应用软件在 Windows 操作系统、Visual Basic 6.0 环境下开发完成,主要包括以下四个模块(图 3):

a)文件加载模块。主要用来选择需要加密或解密的文件,由 DriveListBox 控件、DirListBox 控件、FileListBox 控件、CheckBox 控件及 LoadFile 函数组成。

b)加密参数输入模块。五个 Lable 控件用来显示 logistic 映射和 Henon 映射参数输入的说明内容;五个 TextBox 控件用来输入初始条件和控制参数;Check-Box 控件用来改变 TextBox 控件的 PasswordChar 属性,可以设置输入的数据是否显示。

c)加密效果显示模块。采用两个 FileBox 控件:一个用来当做输入文件的容器;一个用来显示加密文件内容,配合 HScrollbar 控件和 VScrollBar 控件在容器内实现加密文件的浏览。

d)常用控件模块。为保存加密或解密的文件,引入 CommonDialog 控件。三个 CommandButton 控件和 VScrollBar 控件,一个用来对特加密文件进行加密或解密,一个用来保存加密或解密的文件,另一个为退出。保存文件是通过 SaveFile 语句实

现的。

2.2　实验结果

通过本文所设计的双混沌映射加/解密实验平台软件,读取一幅图片,用复合迭代所产生的混沌序列对图片进行加密和解密。下面首先用本文设计的加密测试软件进行安全性测试。图4(a)是在一组内部参数设置下加密的效果图。其参数为 $\mu=3.835$, $a=1.01$, $b=0.3$, $x_0=0.200\ 000\ 000$, $y_0=0.100\ 000\ 000$。对加密后的图像采用相同的密钥解密后的效果图如图 4(b);(c)是将 x_0 设为 0.200 000 001、y_0 设为 0.100 000 001,其他值不变的情况下得到的效果图。可见,即使密钥存在细微的差别,也不能够对密文正确地解密。仿真结果表明,算法对密钥非常敏感,这说明本文提出的基于双混沌映射的混合混沌系统对系统参数及初始条件是非常敏感的。

图 3　双混沌映射加/解密实验平台软件界面

(a) 初始加密显示效果

(b) 正确解密显示效果

(c) 错误解密显示效果

图 4　加密效果

再用本文算法与 DES 加密和基于 Lorenz 加密进行加/解密速度比较。实验运行计算机为 2.8 GHz CPU/1 GB RAM/Microsoft Windows XP 操作系统。其实验结果如表 1 所示。可见,本文加密方法的加/解密速度很快,因此很适用于大数据量、实时性要求高的消息加密。

表 1　三种加密算法加/解密速度比较

测试图像	基于双混沌映射的密码		基于 Lorenz 的密码		DES 算法	
名称 长×宽	加密/s	解密/s	加密/s	解密/s	加密/s	解密/s
apple 128×128	0.02	0.01	0.05	0.03	0.50	0.44
boats 256×256	0.03	0.02	0.06	0.05	1.92	1.87
forest 640×480	0.08	0.06	0.22	0.22	8.83	8.20
city 1 024×768	0.21	0.21	1.2	1.35	22.42	23.18
children 2 048×2 048	0.73	0.70	3.44	3.32	122.10	120.68

2.3　性能分析

本文提出的算法选定三个内部控制参数和两个初始状态作为密钥,密钥空间是很大的,单以两种映射的初值所形成的密钥空间计算已达 2×10^{32} 个。即使在已知加密算法使用 logistic 和 Henon 映射的情况下,绕过穷举密钥攻击转而通过穷举间接获得三个内部控制参数也是不可能实现的。与单个混沌系统产生的伪随机序列相比,本文设计的双混沌系统序列密码具有更高的安全性。另外,因为混沌加密属于序列密码,分组加密的攻击方法对它是无效的。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。而分析 DES 和 AES 算法的加密方式可知其主要是反复替代和置换,因此加密时间较长,而其 56 位的密钥在当前看来也显得不足。

双混沌映射加密属于流密码的范畴,其准备时间非常短。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和复杂的高维混沌加密系统,本文算法动力学方程简单,计算机处理的都是简单的基本运算,其加密效率很高。双混沌映射加密算法没有 S-box 空间,由于采用的双混沌映射都只是一维和二维的线性映射,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很少,实现简单。因此,其运行时占用的空间很少。

3　结束语

本文结合运用 Henon 和 logistic 映射,通过建模和设计软件,使两个不同的混沌信号经过非线性函数变换后所产生的混沌载波完全不同于这两个混沌映射本身,实现了对消息的安全快速加密,安全性能等价于高维混沌系统的加密,且大大缩短了加密时间,实时性较高,在消息加密中有一定的应用价值。

参考文献:

[1] MASUD N, AIHARA K. Cryptosystems with discretized chaotic maps [J]. IEEE Trans on Circuit and Systems, 2002, 49(1): 28-40.

[2] KOCAREV L, JAKIMOSKI G. Logistic map as a block encryption algorithm[J]. Physics Letters A, 2001, 289(4): 199-275.

[3] LI Shu-jun, MOU Xuan-qin, CAI Yuan-long. Improving security of a chaotic encryption approach[J]. Physics Letters A, 2001, 290(3-4): 127-133.

[4] 范艺,刘雄英,丘水生. 混沌加密与常规加密复合的图像保密通信系统[J]. 计算机工程, 2005, 31(20): 44-45.

[5] FEI Peng, QIU Shui-sheng, MIN Long. An image encryption algorithm based on mixed chaotic dynamic systems and external keys[J]. IEEE Trans on Circuits Syst I, 2005, 46(5): 1135-1139.

[6] 彭军,廖晓峰,张伟. 基于复合混沌系统的图像加密[J]. 计算机工程, 2006, 32(7): 34-36.

[7] ZHOU Liang-qiang, CHEN Fang-qi, CHEN Yu-shu. Chaotic behavior on reduction of perturbed KdV equation in form of parametric excitation[J]. Trans of Nanjing University of Aeronautics & Astronautics, 2007, 24(4): 283-287.

[8] 高洁,袁家斌,徐涛,等. 一种基于混合反馈的混沌图像加密算法[J]. 计算机应用, 2008, 28(2): 434-436.

[9] MATTEWS R. On the derivation of a chaos encryptional algorithm [J]. Cryptologia, 1989, 13: 29-42.

[10] KOCAREV L, MAGGIO G M, OGORZALEK M, *et al*. Special issue on application of chaos in modern communication systems [J]. IEEE Trans on Circuits and Systems-I: Fundamental Theory and Applications, 2001, 48(12): 1394-1404.

[11] HASLER M, MAISTRENKO Y L. An introduction to the synchronization of chaotic systems: coupled skew tent maps[J]. IEEE Trans on CAS-I, 1997, 44(10): 856-866.

[12] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cap maps[J]. Chaos, Solitons and Fractals, 2004, 21: 749-761.

[13] CHEN Hong-bin, LI Yi, HOU Xiao-jie. Exact multiplicity for periodic solutions of duffing type [J]. Nonlinear Analysis and Theory, Method and Application, 2003, 55(1): 115-124.

[14] CUOMO K M, OPPENHEIM A V, STROGATZ S H. Synchro-nization of Lorenz-based chaotic circuits with applications to communications [J]. IEEE Trans on Circuits and Systems-Ⅱ, 1993, 40(10): 226-233.

[15] BORRESEN J, LYNCH S. Further investigation of hysteresis in Chua's circuit[J]. International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, 2002, 12(1): 129-134.

[16] 翁妙凤,王敏. 用进化 RBF 神经网络控制 Rossler 混沌系统[J]. 信息与控制, 2001, 30(7): 600-602.

[17] FRIDRICH J. Image encryption based on chaotic maps[C]//Proc of IEEE International Conference on Man and Cybernetic Computational. 1997: 1105-1100.