DOI :10.3969/J. ISSN. 1672-6693. 2010. 02. 015

一种基于外部密钥的混沌加密方法*

张 欣, 杨德刚, 朱 凯
(重庆师范大学 信息科学与工程学院, 重庆 400047)

摘要:提出了一种基于斜帐篷映射的混沌加密方法。分析了斜帐篷映射的数学性质,该混沌系统生成的混沌序列具有良好的统计特性。该方法采用 128 位二进制数代替系统参数作为密钥,混沌映射所需的所有参数都由外部密钥计算产生,通过随机改变混沌的迭代次数、分段的频率以及改变混沌的初始值和参数,提高混沌序列的复杂度,增加了混沌系统的安全性。同时引入扩散机制,当明文仅出现微小的变动时,使得对应的密文与变动之前的密文完全不同,增加了密文分析的难度。仿真实验和理论分析都证明该算法具有较高的效率和安全性,能够有效抵抗统计攻击和已知明文攻击。

关键词:Logistic 映射;斜帐篷映射;混沌加密;外部密钥
中图分类号:TP309 **文献标识码**:A **文章编号**:1672-6693(2010)02-0057-04

混沌映射由于具有遍历性、不可预测性、对参数和初始值敏感性等和传统密码学相类似的特性,因此适合用于密码设计。在过去 10 年间,学者们提出了很多基于混沌的加密算法[1-7],其中以 Baptista 的思想最具代表性[1]。他利用 Logistic 映射的参数和初始条件作为密钥,将 Logistic 映射每次迭代的次数作为密文。但他的思想有两个明显的缺陷,首先密文都是聚集在某一个区间内的整数,并且分布不均匀;其次由于需要不断地对 Logistic 映射进行迭代,所以算法的速度较慢,加密大的文件效率较低,比如多媒体文件等。

Kwok-Wo Wong 在文献[2,3]中对 Baptista 的算法进行了改进,提出了动态查询表的加密方法,该方法同样采用 Logistic 映射的参数和初始条件作为密钥,将明文在动态查询表里的索引号作为密文。由于动态查询表中包含 256 个 ASCII 码,所以该方法得到的密文分布为 0 ~ 255。G. Álvarez 在文献[4]中对这种方法进行了详细分析,指出动态查询表的更新实际上是仅仅依靠明文本身,而不是密钥,所以它的演变很容易被预测。由于该算法要不断进行迭代和更新查询表,所以要消耗大量时间,算法的速度也很慢。

N. K. Pareek 在文献[5-6]中分别提出了两种采用外部密钥的加密思想,而不再采用系统参数和初始条件作为混沌映射的密钥,这和传统的加密算法如 DES、AES 等相类似。但是他的方法在产生系统参数和初始条件时有严重的缺陷,对已知明文攻击非常脆弱。

基于以上分析,本文提出一种采用 128 位外部密钥的块加密算法,该方法保留了前人思想中的优点,并将前人算法中存在的缺点进行了改进。

1 基于外部密钥的加密方法

首先,将明文记为 P,密文记为 C,密钥记为 K。

$$P = P_1P_2P_3\cdots P_n \tag{1}$$

$$C = C_1C_2C_3\cdots C_n \tag{2}$$

$$K = K_0K_1K_2\cdots K_{15} \tag{3}$$

这里把明文和密文每 64 位分为一组,其中 P_i,C_i 为任一 64 位明文和密文块,$i \in [1,n]$,把 128 位密钥分成每 8 位一组,K_i 代表任一 8 位子密钥,$i \in [0,15]$。

尽管多数文章都采用 Logistic 映射[1-4,8],但由于 Logistic 映射的分布并不均匀,并且在 $\lambda = 3.828\ 429 \sim 3.841\ 037$ 存在着周期 -3 的窗口[5],所以本文采用分布更加均匀的斜帐篷映射((4)式)来产生混沌系统。Logistic 映射和斜帐篷映射的分布如图 1 所

* 收稿日期:2009-05-22 修回日期:2009-10-20
资助项目:国家自然科学基金(No. 10971240);重庆市科委自然科学基金(No. CSTC2008BB2366,No. CSTC2008BB2364);重庆市教委科技计划(No. KJ090803,No. KJ080805,No. KJ080806,No. KJ080817)
作者简介:张欣,男,硕士研究生,研究方向为混沌密码学;通讯作者:杨德刚,E-mail:ydg42@163.com

示。

$$F(x) = \begin{cases} x/p, x \in [0,p) \\ (1-x)/(1-p), x \in [p,1] \end{cases} \quad (4)$$

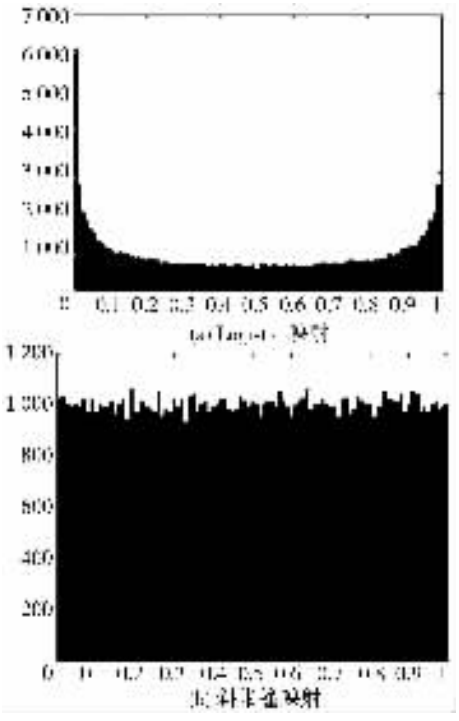

图1 混沌映射变量分布

1) 在进行加密之前首先对混沌系统的参数和初始值进行初始化。确定斜帐篷映射的参数 p,由于 p 的取值范围在(0,1)之间,所以采用(5)式来计算参数 p

$$p = K_r/256 \quad (5)$$

其中 K_r 为 K 中任一子密钥,$r \in [0,15]$。r 是由系统随机产生的一个随机数,这里可以用 C++ 的标准库函数 rand( ) 来产生。使用 rand( ) 时所需的种子值通过密钥 K 由(6)式产生。

$$seed = K_0 + K_1 + K_2 + \cdots + K_{15} \quad (6)$$

斜帐篷映射的初始条件通过(7)~(9)式来产生

$$x_s = (0.A \oplus B)_2 \quad (7)$$

$$A = K_r K_{(r+1) \bmod 16} K_{(r+2) \bmod 16} \cdots K_{(r+7) \bmod 16} \quad (8)$$

$$B = K_{(r+8) \bmod 16} K_{(r+9) \bmod 16} K_{(r+10) \bmod 16} \cdots K_{(r+15) \bmod 16} \quad (9)$$

其中 $(\ )_2$ 指二进制表示,$\oplus$ 指 A 和 B 作异或操作 $(0.A \oplus B)_2$ 指将64位二进制序列 A 和 B 作异或操作以后再除以 2^{64},即将结果表示成(0,1)之间的小数,精度为 2^{-64},mod 是取模运算。

初始迭代次数 N_0 由(10)式得到

$$N_0 = (K_r)_{10} \quad (10)$$

$(K_r)_{10}$ 指的是将子密钥 K_r 转换成十进制整数作为映射的初始迭代次数。

2) 将产生的 p, x_s, N_0 代入(4)式中进行迭代计算,得到精度为 2^{-64} 的二进制小数,记为 x_0($x_0 \in (0,1)$),取 x_0 的64位二进制小数部分,记为 C_0。

3) 对第 $i(1 \leqslant i \leqslant n)$ 个明文块 P_i 的加密方法如下。

首先由系统产生一个新的随机数 $r \in [0,15]$,然后用(11)式计算第 i 次迭代次数 N_i

$$N_i = (K_r K_{(r+1) \bmod 16} K_{(r+2) \bmod 16} \cdots K_{(r+7) \bmod 16} \oplus C_{i-1})_{10} \bmod 256 \quad (11)$$

这里的 $(\ )_{10}$ 指的是将括号内异或得到的64位二进制数每8位转换成相应的十进制数后再求和。用得到的 N_i 对(4)式进行迭代计算,最后得到的结果记为 x_i(64位二进制小数)。

4) 加密方法由(12)式给出

$$C_i = P_i \oplus (x_i \times 2^{64}) \oplus C_{i-1} \quad (12)$$

其中 P_i 为第 i 块64位明文,x_i 为64位二进制小数,C_{i-1} 为第 $i-1$ 次加密得到的密文。

5) 判断 $x_i > r/16$ 是否成立,如果成立则由(13)式计算 x_{new},作为新的 x_i,否则 x_i 不变。

$$x_{new} = (0.((K_r K_{(r+1) \bmod 16} K_{(r+2) \bmod 16} \cdots K_{(r+7) \bmod 16}) \oplus (x_i \times 2^{64})))_2 \quad (13)$$

其中 x_{new} 是64位二进制小数。

6) 重复以上3)~5)步,直到 n 个明文块全部完成加密操作。

解密算法和加密算法完全相同,只需要将(12)式换成(14)式就可以了。

$$P_i = C_i \oplus (x_i \times 2^{64}) \oplus C_{i-1} \quad (14)$$

2 仿真结果分析

混乱和扩散对加密系统具有十分重要的意义[9-11]。混乱指将密文和明文之间的统计特性的关系尽可能复杂化,扩散指将每一位明文和密钥的影响尽可能地作用到较多的输出密文中去,从而隐藏明文的统计特性。

2.1 算法仿真和密文敏感性测试

仿真实验在 IBM R50e(1.3 GHz,256M RAM)的机器上进行,对所提出的算法的混乱特性和扩散特性进行检测。随机选择外部密钥

K = (6AFC83D492CFEB562A41C2EDA7BD 8FF3)$_{16}$

明文 P =" A New Chaotic Cryptography With External Key ",加密后的密文记为 $E(P,K)$,模拟结果如图2

(a)所示。从图中可以看出明文经过加密以后变成了 0 ~255 之间的随机数序列,这说明该加密算法具有良好的混乱特性。

为了检测加密算法对明文和密钥的敏感性,先将明文 P 做小小的变动,即 P' =“ a New Chaotic Cryptography With External Key ”,密钥 K 不变,加密密文记为 $E(P',K)$,模拟结果如图 2(b)所示。从图 2(b)中可以看到,密文 $E(P,K)$ 和密文 $E(P',K)$ 刚开始有重叠现象,即在刚开始加密的时候会出现一小段加密后相同的字符,但是随后绝大多数点都不同。出现连续相同密文的原因是由于开始的微小变动还没有完全扩散的缘故,等到完全扩散以后密文 $E(P,K)$ 和密文 $E(P',K)$ 就会完全不同。

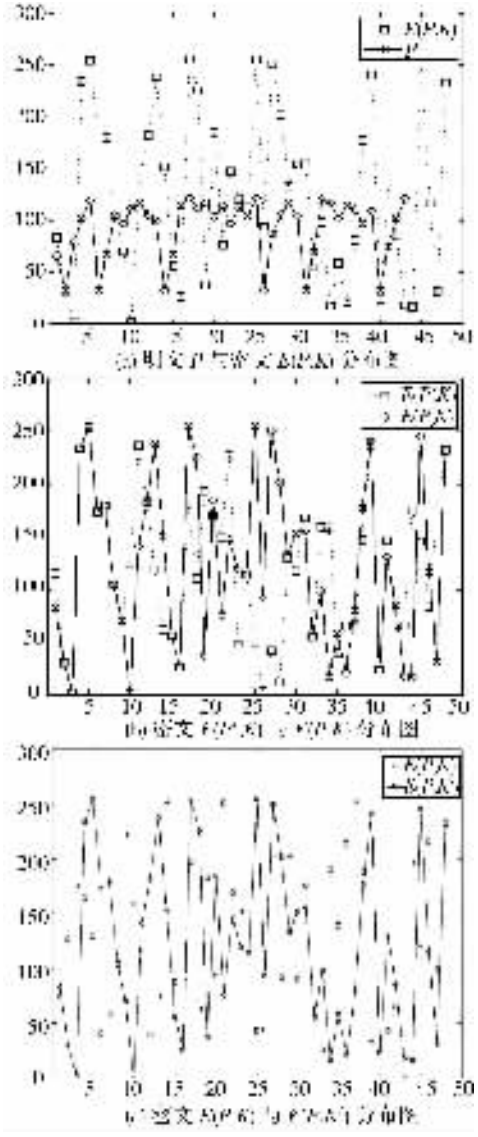

图 2　密文敏感性分析

再保持明文为初始明文不变,将密钥 K 在开头做一个小的变动,即

K' = (3AFC83D492CFEB562A 41C2EDA7BD8FF3)$_{16}$

加密后密文记为 $E(P,K')$,模拟结果如图 2(c)所示。从图 2(c)中可以看出扩散的效果非常理想,基本上不存在点的重叠现象。这是由于斜帐篷映射在完成初始迭代以后产生了完全不同的 C_0,这正是利用了混沌的‘雪崩效应”。

2.2 密文分布测试

通过加密一个 24KB 的文本文档来检测明文和对应密文的分布情况,模拟结果如图 3 所示。图 3(a)是明文的分布柱状图,从中可以看出大多数字符都分布在 100 ~120 和 160 ~255 的范围内,这是由于这篇文章是一篇中英文字符的混合文档。图 3(b)是密文的分布柱状图,密文基本上是均匀的分布在 0 ~255 的范围内,说明了该算法具有较好的抗统计分析能力。

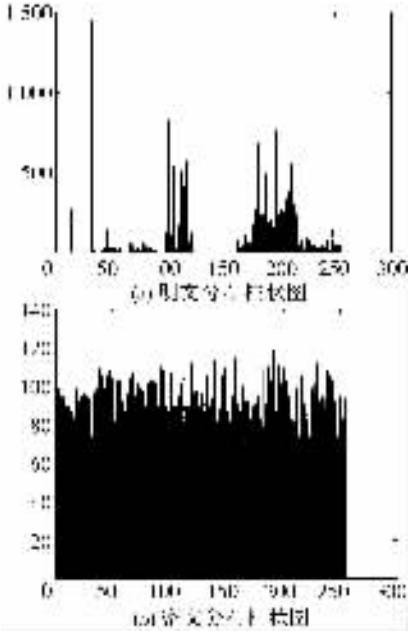

图 3　明文与密文的分布比较

2.3 加密效率分析

除了检测算法的混乱与扩散特性,还要重点关注加密算法的效率,表 1 中列出的是本文提出的算法和参考文献[4,8]的时间消耗对比。

从表 1 中可以看出本文中所提出的算法的速度比参考文献[4]和[8]的速度都要快,这是由于:首先本文不仅仅是依靠迭代方程(4)来进行加密的;其次,本文采用的是块加密技术,在对方程(4)进行完一轮迭代计算以后,总是对 64 位的明文进行加密,而不是采用更小的每 8 位进行加密,这样对相同的明文来说,最后分成的明文块就大大减少了,需要对方程(4)进行迭代计算的计算量也就大大减少

了,从而提高了加密的速度。最后,相对于参考文献[2,3]来说,没有采用动态查询表的技术,这是由于在对动态查询表进行查找和变换时,需要占用大量的时间,所以这也是本文算法速度较快的一个原因。

表1 算法加密效率比较

文件类型	明文/KB	密文/KB	消耗时间/s(本文算法)	消耗时间/s(文献[4])	消耗时间/s(文献[8])
文本文件(*.txt)	24	24	0.02	0.07	0.12
可执行文件(*.exe)	992	992	0.862	2.894	5.167
音频文件(*.mp3)	2 371	2 371	2.053	6.599	12.187
视频文件(*.avi)	3 998	3 998	3.475	11.046	21.01

3 安全性分析

3.1 密钥空间分析

本文中所描述的算法由于采用的是128位密钥加密,所以它有足够大的密钥空间(2^{128})来防止穷尽密钥攻击。虽然利用(7)~(9)式计算出来的x_s只有64位,但斜帐篷映射的参数p和初始迭代次数都是通过(5),(10)式计算出来的,被选中的概率只有$1/(x_{i+1})$,所以它的安全性也足以抵抗穷尽密钥攻击。

3.2 抵抗选择明文攻击

对于一个已知明文P_i,密码分析者可以利用公式$P_i \oplus C_i = A_i$得到密钥,进而通过大量的尝试,可以从中得出一些混沌映射里的轨道信息,从而对该加密系统进行攻击。为了解决这个问题,本文所提出的加密算法中引入了轨道变换机制,即通过公式$x_i > r/16$判断条件是否满足,如果满足那么执行(13)式得到x_{new},将它作为新的x_i代入混沌系统中进行迭代,使得混沌系统的状态值从一个轨道跳变到另一个轨道。而且这种跳变是随机的,所以得到的混沌轨道是长短不一的短周期轨道,这种方法使得密码分析者很难通过大量的明文密文对得到必要的轨道信息,也就使得该算法具有较强的抵抗选择明文攻击的能力。

3.3 扩散效果分析

本文提出的算法中通过(12)式引入了扩散机制,当明文P_i中产生了一点变化后,不仅会影响到本次加密的密文C_i,在加密下一块明文P_{i+1}时由于有C_i的影响使得到的密文C_{i+1}完全不同,进而连续影响以后加密结果。而且C_i的不同还会影响下一轮的迭代次数N_{i+1}的计算,从而得到的x_{i+1}也会不同,有可能通过(13)式影响下一轮迭代时x_{i+1}的取值,即使斜帐篷映射发生轨道跳变,这也会影响到以后所有的密文。所以该算法具有较好的扩散效果。

4 总结

本文首先对Baptista加密算法以及针对他的一些改进算法进行了简短描述,并对算法中所存在的缺陷给出了说明。基于这些算法缺点提出了一种改进的采用128位外部密钥进行加密的思想。由于Logistic映射变量分布的不均匀性和存在着周期为-3的窗口,所以在本文中采用的是斜帐篷映射。通过对该算法进行的混乱特性和扩散特性的检验,以及对密文的分布情况和加密效率进行的模拟实验,都说明了本文提出的算法具有较好的加密性能。最后的安全性分析说明该算法具有足够的安全性,能够抵抗穷尽密钥攻击和选择明文攻击。

参考文献:

[1] Baptista M S. Cryptography with chaos[J]. Phys Lett A, 1998,240:50-57.

[2] Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table[J]. Phys Lett A,2002,298:238-242.

[3] Wong K,Ho S,Yung C. A chaotic cryptography scheme for generating short ciphertext[J]. Phys Lett A,2003,310:67-73.

[4] Ivarez G,Montoya F,Romera M,et al. Cryptanalysis of a discrete chaotic cryptosystem using external key[J]. Phys Lett A,2003,319:334-339.

[5] Pareek N K,Patidar V,Sud K K. Discrete chaotic cryptography using external key[J]. Phys Lett A,2003,309:75-82.

[6] Pareek N K ,Patidar V,Sud K K. Cryptography using multiple one-dimensional chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2005, 10: 715-723.

[7] Xiang T,Wong K W,Liao X F. An improved chaotic cryptosystem with external key[J]. Communications in Nonlinear Science and Numerical Simulation,2008,13:1879-1887.

[8] Wei J,Liao X F,Wong K W,et al. A new chaotic cryptosystem[J]. Chaos,Solitons & Fractals,2006,30:1143-1152.

[9] Kahate A. Cryptography and network security[M]. Beijing: Tsinghua University Press,2005.

[10] 罗璞,陈巧琳,曹长修,等. 一种基于Rijndael的图像加密方法[J]. 重庆邮电大学学报(自然科学版),2006,18(3):382-385.

[11] 朱凯,杨德刚. 一种基于斜帐篷的映射的混沌加密方法[J]. 重庆师范大学学报(自然科学版),2009,26(2):99-103.

A New Chaotic Cryptosystem by Using External Key

ZHANG Xin, *YANG De-gang*, *ZHU Kai*

(College of Information Sciences and Engineer, Chongqing Normal University, Chongqing 400047, China)

Abstract: In this paper, a new chaotic cryptosystem based on skew-tent map is proposed. The mathematic characteristics of this map prove that the chaotic sequence generated from it has good statistical property. This method uses 128-bit binary sequence as key instead of system parameters. All the system parameters required by this chaotic map are calculated by external key. By changing iterating number times, piecewise frequency, chaotic initial conditions and parameters randomly, the chaotic sequence is much more complex and the security of this cryptosystem has improved greatly. At the same time, diffusion mechanism has been introduced in the algorithm. This means that every bit change in the plain image can influence multi-bit in the cipher image. This method ensures that cipher image pixel can change largely and be very different from former cipher image that plain image hasn't been changed when plain image pixel changes slightly, and increases the difficulty of cipher analysis. It has been proved by many simulated experiments and theoretical analysis that this algorithm owns higher efficiency and security and can resist the statistcal and known-plaintext attacks.

Key words: logistic map; skew-tent map; chaotic cryptography; external key

(责任编辑　游中胜)