一种基于斜帐篷映射的混沌加密方法*

朱 凯,杨德刚,陈守刚
(重庆师范大学 数学与计算机科学学院,重庆 400047)

摘要:提出一种基于斜帐篷映射的混沌加密方法,该算法在加密过程中,借助明文信息和外部密钥动态地修改查询表,每加密一个明文,都更新一次查询表,通过斜帐篷映射借助动态查询表动态地生成 8 位子密钥,密钥为斜帐篷映射的初始条件 x_0、控制参数 p 和一个外部密钥 K。理论分析和仿真实验表明,该算法能有效地抵抗统计攻击、差分攻击,具有较高的安全性。

关键词:混沌;加密;密钥;斜帐篷映射
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1672-6693(2009)02-0099-04

随着 Internet 技术的飞速发展,计算机网络技术正日益广泛地应用到社会各个领域。与此同时,信息的安全与保密显得越来越重要[1]。如何保证网上敏感信息的安全已经成为当今网络技术研究的一个热点。近几年来,研究人员提出了许多基于混沌的加密算法[2-14]。然而混沌在本质上是确定的,计算机的有限精度和混沌序列的离散化导致了混沌动力系统的性能退化。

本文提出了一种基于斜帐篷映射的混沌加密方法。在加密过程中,依靠明文信息和外部密钥动态的变化查询表,通过斜帐篷映射依靠动态查询表动态地生成 8 位子密钥,极大地提高密码系统的随机性、复杂性。因此,从计算安全性角度,提高了算法的抗明文攻击能力。

1 基于斜帐篷映射的混沌加密方法

1.1 混沌映射的选择

利用混沌技术设计加密系统时常采用如下的思想:1)选择一个适当的混沌映射,以设定的映射中的参数值和初始状态作为加密算法的主密钥;2)对映射进行迭代,产生子密钥序列;3)利用这些子密钥序列来加密明文。混沌映射的选择是设计加密算法时的关键步骤之一,除了注重映射本身的特点之外,还应关注映射中参数的个数和参数的取值范围。

斜帐篷映射是一个简单的离散混沌系统,它的映射关系为

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

其中控制参数 $p\in(0,1)$,系统处于混沌状态。而 Logistic 映射 $x_{n+1}=\mu x_n(1-x_n)$,其中 μ 为控制参数,当 $3.569\,946<\mu<4$,$x\in(0,1)$ 系统工作于混沌状态。由此可见斜帐篷映射参数的取值范围更大,并且斜帐篷映射的变量密度比 Logistic 映射要稳定[3],故本文以斜帐篷映射来产生混沌系统。

1.2 子密钥的产生

如何根据选定的混沌映射产生相应的子密钥序列是在设计加密系统时应注意的另一个重要问题。因为子密钥序列直接作用于明文,其自身的特性对密码系统的安全性有非常重要的影响。当前已有许多混沌序列的生成算法,虽然利用这些算法可获取一些具有均匀分布和随机统计特性的子密钥序列,但是这些子密钥序列常仅依靠于混沌映射中设定的参数值和初始状态(主密钥)。即主密钥一旦确定,相应的子密钥序列也确定下来,对不同的明文均采取相同的子密钥序列进行加密。这为攻击者进行选择明文攻击提供了一定的条件[4]。为了保证加密系统的安全性,在设计子密钥序列的生成算法时,可将明文的信息引入其中,使子密钥不仅与主密钥相关,还与明文相关。同时要注意子密钥序列对明文的依赖性不能过大,以免造成信息的泄漏。

1.3 查询表的更新

为了提高混沌加密系统的安全性,每加密一个

* 收稿日期:2008-11-17 修回日期:2009-01-20
资助项目:重庆市科委自然科学基金(CSTC,No. 2008BB2366,No. 2007BB2231);重庆市教委科技计划项目(No. KJ080805,No. KJ080817,No. KJ070801),重庆师范大学校级基金(No. 2008XLB003,No. 2008XLZ007)
作者简介:朱凯,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。

明文,都更新一次查询表[1]。如图1为初始查询表。$[X_{\min},X_{\max})\subseteq(0,1)$被分成$S$个$\varepsilon$区间,则区间的集合为$X=\{X_i\mid X_i=[X_{\min}+(i-1)\varepsilon,X_{\min}+i\varepsilon),i=1,2,\cdots,S\}$,这里$\varepsilon=(X_{\max}-X_{\min})/S$。明文消息字符的集合记为$A=\{a_1,a_2,\cdots,a_s\}$。$X$中的小区间和明文字符间的关联映射$f$定义为如下的双射:

$$f:X=\{X_1,X_2,\cdots,X_S\}\rightarrow A=\{a_1,a_2,\cdots,a_s\}$$

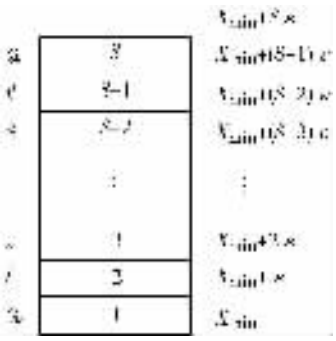


图1 查询表

设明文P_i在表中的区间是S,表的更新过程[4-6]如下。

$$f_{(S)}\leftrightarrow f_{(S+v_1 \bmod 256)};$$

$$f_{(S+v_1+1 \bmod 256)}\leftrightarrow f_{(S+v_1+v_2+1 \bmod 256)};$$

$$f_{(S+v_1+v_2+2 \bmod 256)}\leftrightarrow f_{(S+v_1+v_2+v_3+2 \bmod 256)};$$

$$\cdots$$

$$f_{(S+v_1+\cdots+v_{n-1}+n-1 \bmod 256)}\leftrightarrow f_{(S+v_1+\cdots+v_n+n-1 \bmod 256)}。$$

共交换n次,最后$f_{(S+v_1+\cdots+v_n+n \bmod 256)}\leftrightarrow f_{(S+v_1 \bmod 256)}$。其中$v_t$为两交换区间的距离,$n$为交换次数。总共交换了$n+1$次。

1.4 加密算法

将外部密钥(K),明文(P)和密文(C)表示为

$$P=P_1P_2P_3\cdots P_n$$

$$C=C_1C_2C_3\cdots C_n$$

其中,外部密钥为二进制表示,$K_i\in\{0,1\}$,s为其长度。明文和密文划分成一系列长度为8b的块P_i和C_i,n为密文和明文的长度。

算法的加密过程中,密钥为斜帐篷映射的初始条件x_0、控制参数p和一个外部密钥K,其中$K=AB$,A、B各64位。本文提出的混沌加密过程如下。

1)两个斜帐篷映射f_1和f_2的控制参数p分别取0.79,0.37。$y=(0.A\oplus B)_2$。y的二进制表示为$y=0.b_1'b_2'\cdots b_j'$;

2)将x_0代入f_1迭代N_0次(N_0一般不小于250),$x=r=f_{1(x_0)}^{N_0}$,$y=f_{2(y)}^{N_0}$。这里$f_{(.)}^t$表示以·为初始条件迭代t次;

3)设$x=0.b_1b_2\cdots b_j$为x的二进制表示。加密第i个明文,$C_i=P_i\oplus k$,其中子密钥$k=(b_1\cdots b_8)_2\oplus(b_9\cdots b_{16})_2$;

4)判断是否完成,完成进入6),否则迭代f_1,当$r=f_{1(r)}^n\in X_j(j=1,2,\cdots,S)$,$f(X_j)=m_1$或$f(X_j)=m_2$时,迭代停止。其中$m_1=(P_i+(b_1'\cdots b_8')_{10})\bmod 256$,$m_2=P_i\oplus(b_9'\cdots b_{16}')_{10}$。以1.3节所提到的方法更新查询表,其中$v=n/Z_1$,$t=n/Z_2$,$Z_1$,$Z_2$最好为小于256的素数且$Z_1>Z_2$。$v_i=2^{i-1}v \bmod Z_1$;

5)$x=r\oplus x$,$y=x\oplus y$,$y=f_{2(y)}^1$,转到3);

6)结束。

算法的解密过程与加密过程类似,只需要第3)步中的$C_i=P_i\oplus k$改成$P_i=C_i\oplus k$。

2 算法分析及仿真

本算法在CPU为奔腾1.86 GHz,内存512 MB的Windows XP操作系统中,采用C语言实现。

2.1 密钥空间分析

好的加密算法的密钥空间应该足够大。在算法中,由于增加了K,比通常只用x_0,p作为密钥的算法空间要多$(2^{64}-1)2^{128}$。这对于抵抗穷举攻击具有重要的意义。此外,每加密一个字符就变动次查询表,增加了攻击者破解密文的难度。

2.2 混乱与扩散性能分析

混乱和扩散对以计算机为基础的加密技术具有十分重要的意义[14]。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位中去,从而隐藏明文的统计特性。为了说明算法的混乱和扩散特性,以"A Encryption Algorithm Based on Chaos"为例,分别对明文、控制参数、初始值和外部密钥进行微小的改变。

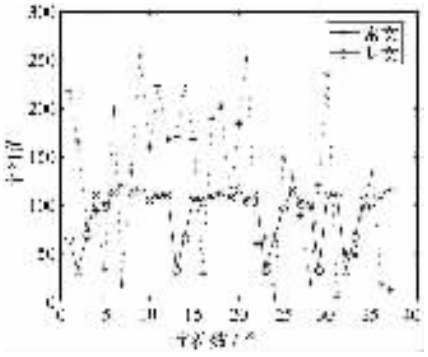
1)将第一个字符'A'改成'a';

2)将f_1的控制参数$p=0.79$改成$p=0.790\ 000\ 1$;

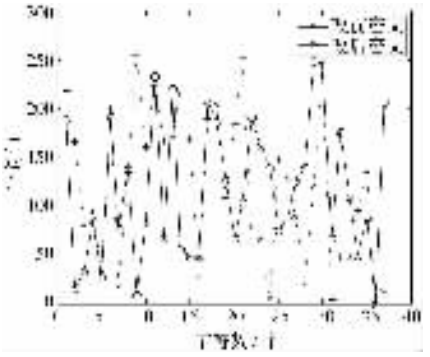
3)将初始条件$x_0=0.002\ 34$改成$x_0=0.002\ 341$;

4)将外部密钥K,"1234567890abcdef"改成"1234567890abcdgf"。

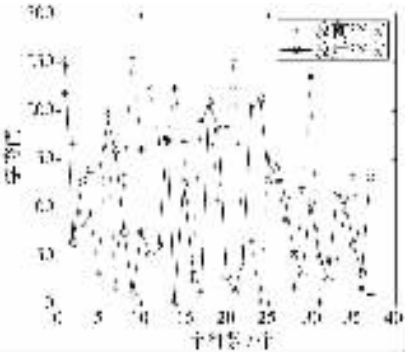
本文提出的加密算法对以上变化进行实验的效果如图2所示。其中,图(a)为进行微小变化前明文与密文的对比,体现了良好的混乱性。图(b)到图(e)依次为上面4种微小变化前密文和变化后密文的对比,体现了良好的扩散性。



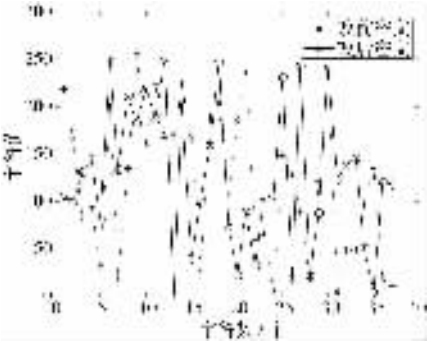
(a) 变化前的明文和密文对比



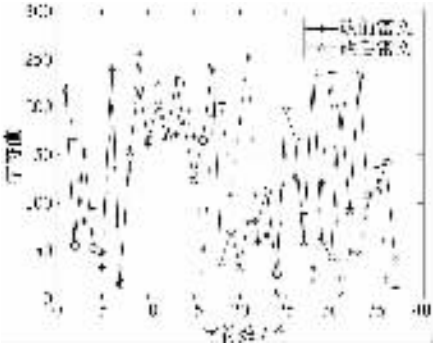
(b) 变化后的密文和变化前的密文对比



(c) 变化后的密文和变化前的密文对比



(d) 变化后的密文和变化前的密文对比



(e) 变化后的密文和变化前的密文对比

图 2　混乱与扩散性能分析

2.3 算法效率

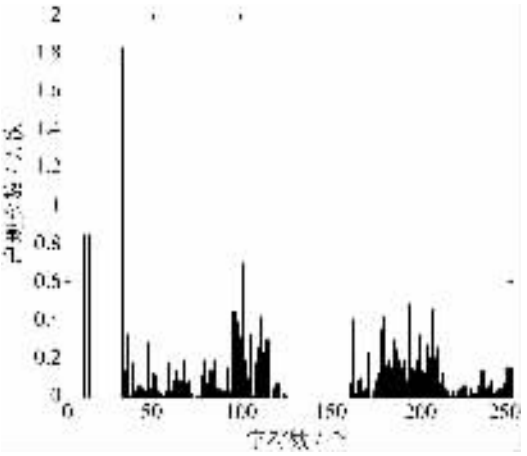
选择如下文件进行加密测试:1) Txt 文件;2) Word 文件;3) 音频文件。测试结果如表 1(表中 3/3 表示加密时间/解密时间分别为 3s/3s)。

2.4 统计特性

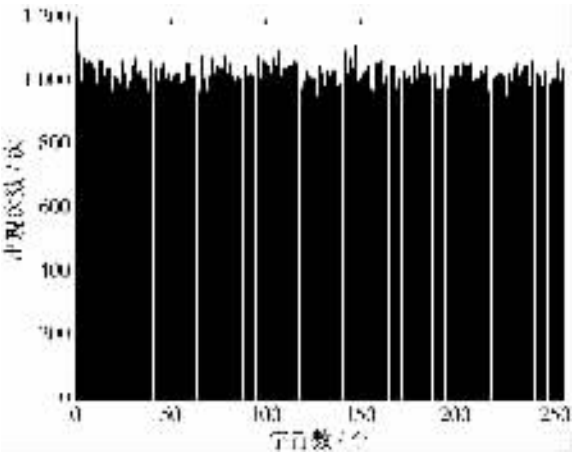
通过统计分析可以破解许多加密算法,但这种加密系统的扩散与混淆特性对统计分析具有较强的抵抗力。这一点可以从图 3 的明文分布和密文分布看出,加密明文的密文分布比较均匀。

表 1　算法时间比较表　　s

	文献[2]加密算法	文献[4]加密算法	本文所提算法
Txt 文件(256K)	3/3	3/3	2/2
Word 文件(857K)	9/9	10/10	5/5
音频文件(3 543K)	42/42	45/45	23/23



(a) 明文分布



(b) 密文分布

图 3　统计特性

3 结论

本文提出了一种基于斜帐篷映射的混沌加密方法,理论分析和仿真实验表明,本算法具有良好的密钥敏感性和很大的密钥空间,同时具有较好的抗统计攻击、差分攻击能力。由于子密钥的生成依靠明文,也使算法能够抵抗选择明文攻击。

参考文献:

[1] 邹显春. 基于 Intranet 的安全策略研究[J]. 西南大学学报(自然科学版),2001,26(1):17-20.

[2] Baptista M S. Cryptography with chaos[J]. Physics Letters A,1998,240:50-54.

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

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

[5] Alvarez G,Montoya F,Romera M,et al. Cryptanalysis of dynamic look-up table based chaotic cryptosystems[J]. Physics Letters A,2004,326:211.

[6] Wei J,Liao X,Wong K,et al. Chaos[J]. Solitons and Fractals,2006(30):1143-1152.

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

[8] Wong W K,Lee L P,Wong K W. A modified chaotic cryptographic method[J]. Computer Physics Communication,2001,138:234-236.

[9] Zhang L,Liao X,Wang X. An image encryption approach based on chaotic maps[J]. Chaos,Solitons and Fractals,2005(24):759-765.

[10] Zhou H,Ling X. Generating chaotic secure sequences with desired statistical properties and high security[J]. International Journal of Bifurcation and Chaos,1997(7):205-213.

[11] Wong K W. A combined chaotic cryptographic and hashing scheme[J]. Physics Letters A,2003,307:292-298.

[12] 董来启,李峰,宋建军,等. 基于混沌神经网络理论的城市深基坑沉降量预测模型[J]. 四川兵工学报,2008,29(2):94-102.

[13] 鲁光辉. 参数控制噪声干扰下的动态电路混沌控制[J]. 西华师范大学学报(自然科学版),2006,27(4):368-373.

[14] Atul Kahate. 密码学与网络安全(影印版)[M]. 北京:清华大学出版社,2005.

A Chaotic Encryption Algorithm Based on Skew Tent Map

ZHU Kai, YANG De-gang, CHEN Shou-gang

(College of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047, China)

Abstract: With the rapid development and extensive applications of computer technology, network technology, communication technology, and Internet in particular, the security of network information is becoming increasingly key problems that must be solved urgently. The applying chaos theory to secure communication and information encryption has already become one of the hot research projects on the combination of nonlinear science and information science, and it is a novel branch of high-tech research fields. In this paper, a chaotic encryption algorithm based on skew tent map is proposed. In the process of encryption, its update look-up table depends on plaintext and external key, the 8-bit subkey is dynamically generated with skew tent map and depends on updating look-up table, the key is initial condition x_0 of skew tent map, control parameter p and a external key K. Theoretical analysis and simulated experiments show that the algorithm can resist the statistic and differential attacks, and the algorithm has high security.

Key words: chaos; encryption; key; skew tent map

(责任编辑 游中胜)