混沌电子邮件加密软件的设计及实现

赵 亮[1],廖晓峰[1],肖 迪[1,2],周 庆[1]
ZHAO Liang[1],LIAO Xiao-feng[1],XIAO Di[1,2],ZHOU Qing[1]

1.重庆大学 计算机学院,重庆 400030
2.重庆大学 机械工程学院,重庆 400030
1.Department of Computer Science,Chongqing University,Chongqing 400030,China
2.Department of Mechanical Engineering,Chongqing University,Chongqing 400030,China
E-mail:zhaoliang@cqu.edu.cn

ZHAO Liang,LIAO Xiao-feng,XIAO Di,et al.Design and implementation of chaotic email encryption soft ware.Computer Engineering and Applications,2009,45(6):101-104.

Abstract: For protecting the security of email transmission on the Internet,this paper proposes a fast and easy-to-realize email encryption algorithm based on the one dimension piecewise linear chaotic model.A kind of software for encrypting and decrypting text files has also been implemented based on the proposed algorithm.Finally,the security is analyzed from three sides which include statistical properties,sensitivity to cipher-text and resistance to known attacks and so on mainly.Simulation results indicate the reliability of the system.

Key words: email encryption;chaotic encryption;one dimension piecewise linear chaotic model;look-up table

摘 要:为了保护在网络中所传输邮件的安全性,基于一维分段线性混沌模型,设计了安全高速且易于实现的电子邮件混沌加密软件,给出了对文本文件加密和解密的算法、具体实现和效果,最后主要从统计特性、密文敏感性以及抗攻击性等三方面对安全性进行了分析,证明了系统的可靠性。

关键词:电子邮件加密;混沌加密;一维分段线性混沌模型;查询表
DOI:10.3778/j.issn.1002-8331.2009.06.029 **文章编号:**1002-8331(2009)06-0101-04 **文献标识码:**A **中图分类号:**TP309.7

1 前言

随着计算机网络和通信技术的快速发展,通过电子邮件传输数据的方式变得越来越普及。但是如果缺乏足够的保密措施,电子邮件数据就有可能被盗用、暴露或篡改。因此,研究如何对电子邮件数据进行保护成为安全领域内研究的热点之一。

自2005年以来,国内外出现了多个关于邮件加密的专利技术[1-6],但这些专利技术主要侧重于电子邮件加密的外围技术,如身份认证和密钥管理,而对于电子邮件加密的核心技术,即电子邮件加密算法都没有详细地描述。

另一种国际上比较流行的电子邮件加密技术是PGP(Pretty Good Privacy),该项技术采用DES算法对电子邮件内容进行加密。但是DES算法对于目前大型计算机的计算能力来讲已经不够安全,因此被美国NIST(National Institute of Standard and Technology)机构建议用AES算法取代。然而,AES加密算法对于电子邮件保护还是可能存在如下的缺点:

(1)可能存在不安全因素:AES算法是美国NIST通过的加密算法,并向全世界推广。根据美国的法律和海关政策,美国将限制美国政府不能破解的算法出口到其它国家。由此可以猜测AES算法很可能存在一些不安全的因素,使得美国或其它某些国家能够破解此算法。由于电子邮件可能涉及一些较机密的信息,因此AES算法不适合用于加密电子邮件。

(2)AES算法比较复杂:128位的AES算法由10轮加密构成,每轮加密又由Addkey、SubByte、ShiftRow和MixCoulmn四个加密操作构成,因此实施起来比较复杂。对于加密邮件数据特别是庞大的电子邮件附件来说效率比较低。

因此,很有必要借助新兴的加密技术,设计出一个新的电子邮件加密算法。基于一维分段线性混沌模型,设计了电子邮件混沌加密软件,该软件安全可靠且易于实现。

2 分段线性混沌系统简介

混沌运动是非线性确定性系统的一种内在类随机过程的表现[7]。而混沌系统则是这种运动的具体实现。通过研究人员长期的观察和研究,发现一个完全的混沌系统除了具有高复杂度和易于实现等特性外,一般还具有以下一些特别的优点[8]:随机

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60573047,No.60703035)。
作者简介:赵亮(1982-),男,硕士研究生,主要研究领域:信息安全、混沌加密、数字水印;廖晓峰(1964-),男,博士后,博士生导师,主要研究领域:人工神经网络、非线性动力学系统;肖迪(1975-),男,博士后,副教授,主要研究领域:信息安全、混沌加密;周庆(1979-),男,博士研究生,讲师,主要研究领域:信息安全、数字水印。
收稿日期:2008-01-14 **修回日期:**2008-04-01

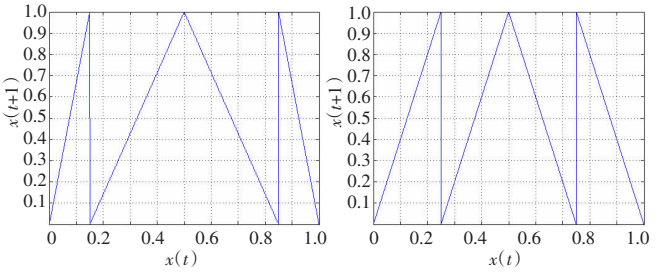
性，即混沌系统能够以确定性的方式产生长周期的伪随机序列；敏感性，即混沌系统对状态初值和系统敏感，即所谓的“蝴蝶效应”；简单性，即混沌系统通常以简单的运算产生复杂的行为；遍历性，即混沌系统能等概率地经过所有的状态。正是因为混沌所具有的这些特点使得它可以应用于信息加密和保密通信。

在本软件的混沌加密技术及系统的设计中，采用了一维分段线性混沌系统进行混沌加密，其数学模型的表达形式[9]如下：

$$X(t+1)=F_p(X(t))=\begin{cases}\dfrac{X(t)}{p}, & 0\leqslant X(t)<p\\ \dfrac{X(t)-p}{0.5-p}, & p\leqslant X(t)<0.5\\ \dfrac{1-X(t)-0.5}{0.5-p}, & 0.5\leqslant X(t)<1-p\\ \dfrac{1-X(t)}{p}, & 1-p\leqslant X(t)<1\end{cases} \quad (1)$$

其中 $X\in[0,1]$，$P\in(0,0.5)$，$\{X(t)\}$是在[0,1]中进行遍历，并且$\{X(t)\}$是均匀分布在[0,1]中[9-10]。

当 p 分别取值为 0.15 和 0.25 时，这时的分段线性混沌映射图如图 1。



(a)p=0.15 的分段线性混沌映射　(b)p=0.25 的分段线性混沌映射

图 1　一维分段线性混沌映射图

3　基于混沌的电子邮件加解密算法

本电子邮件加密系统的核心算法建立在前期工作的基础之上。在文献[11]中，对文献[12]中所提出的基于动态查询表的算法进行了有效的安全改进，本电子邮件加密系统则在此基础上，进一步与编码、电子邮件收发协议等关键技术相结合，并且软件在实施过程中采用了一维分段线性混沌系统。和其他应用在电子邮件中的加密方法相比，通过一维分段线性混沌系统进行加密，既能保证邮件的安全性，并且由于一维分段线性混沌系统在结构上比较简单，还能保证对电子邮件加密实施的相对容易性。以下是算法的主要内容。

由于分段线性混沌系统均匀的分布在[0,1]之间，所以算法中查询表的创建是把[0,1]区间等分为 256 个小区间，按从小到大的顺序与 ASC Ⅱ 值为 0 到 255 的字符对应起来，即 [0.000 0,0.003 9] 对应 ASC Ⅱ 值为 0 的字符、[0.003 9,0.007 8] 对应 ASC Ⅱ 值为 1 的字符 [0.996 1,1.000 0] 对应 ASC Ⅱ 值为 255 的字符。

在整个加解密算法中，p^* 为每次修改查询表所进行的交换次数；r 为对整个数据进行加密的次数，其中只有第一次加密为加密数据，剩余的 $r-1$ 次加密只是为了得到更好的查询表；p 为一维分段线性混沌模型的参数。

3.1　加密算法

(1)输入一个密钥，把它转换为满足分段线性混沌模型的初值 $X(t_0)$，并创建一个初始的查询表，同时输入 p^*、r、p 作为邮件系统参数。

(2)加密第一个明文单元 M 时(M 是 8 位，其中 p^* 和 r 均作为明文单元首先进行加密)，以 $X(t_0)$代入分段线性混沌模型(1)进行迭代，直到轨道第一次进入该明文单元所对应的小区间，此时的迭代次数就是该明文单元加密后的密文；同样，在加密第个明文单元时，以当前的值代入分段线性混沌模型(1)进行迭代，直到轨道第一次进入该明文单元所对应的小区间，此时的迭代次数就是该明文单元加密后的密文。

(3)在每次加密下一个明文单元前，需要对查询表进行更新变换，比如在加密第 i+1 个明文单元前，算法将交换查询表的第 i 栏和第 j 栏，第 j 栏的确定方法如下：

$$v=Y \bmod N \quad (2)$$

其中 V 是两栏之间的间隔，Y 是 $X(t_i)$小数点后第 2、3、4 位数所构成的一个十进制数，N 是查询表中元素的个数(在本软件中为 256)。

$$j=(i+v) \bmod N \quad (3)$$

(4)依次类推对全部明文进行加密得到相应的密文(对应的迭代次数)。

(5)对此密文进行 Uuencode 编码得到可发送密文，并进行 Base64 编码，然后完成发送。

3.2　解密算法

(1)打开待解密的邮件密文。

(2)输入一个与加密相同的密钥，同时把它转换为满足分段线性混沌模型的初值，并创建一个与加密时相同的初始查询表(p^*、r、p 与加密时相同)。

(3)对邮件密文先进行反向 Base64 编码，然后进行 Uudecode 解码得到解密用的密文。

(4)因为密文实质就是特定的迭代次数，所以首先从第一个解码后的数据单元开始，输入初值 $X(t_0)$到一维分段线性混沌模型(1)，进行相应次迭代，根据求出的 X 实际值找到查询表中的对应栏解密出相应的 p^* 的值，并对查询表进行更新变换(按公式(2)、(3))。然后再以相同的方法输出 r 的值并更新变换查询表(按公式(2)、(3))。

(5)对邮件数据进行相同的 r 轮解密，并对查询表进行 p^* 次更新变换，得到解密后的明文。

在图 2 中，假设要加密第 4 个 8 位的元素并且当前的 x=0.310 0，则通过公式(2)、(3)，可以得到 j=(4+100)mod 256=104，则第 4 栏和第 104 栏进行交换，又由于 p^*=3，所以还要进行(p^*-1)次交换，则按照文献[12]中交换递推公式 i 和(i+

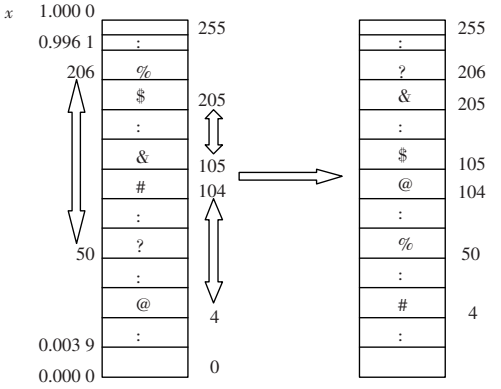


图 2　更新查询表的变换(p^*=3)

Y)mod N 交换；(i+Y+1)mod N 和(i+2Y+1)mod N 交换；(i+2Y+2)mod N 和(i+3Y+2)mod N 交换……(i+(p−1)Y+p−1)mod N 和(i+pY+p−1)mod N 交换，第 105 和第 205 栏进行交换，第 206 和第 50 栏交换。

4　混沌电子邮件系统加解密的具体实现

本软件在具体实现时取系统变量为 p=0.253、p*=18、r=2、N=256，并把它们应用在一维分段线性混沌模型(1)和查询表递推变换公式中，程序通过用户输入的密钥对混沌系统的整个初值进行变换和重载。程序是在 Microsoft Visual C++6.0 编程环境下运用 C++语言进行编写，可有效的完成对文本文件的加密。此软件在应用过程中应能完成以下主要功能：

(1)创建账户用于收发邮箱中的邮件和附件并查看账户邮箱中的新邮件和新附件。

(2)直接完成写邮件和删除邮件操作并在写完邮件和附件之后，可分别对邮件和附件用分段线性混沌系统进行加密，保证邮件和附件通信的安全性。

其中第 2 点是本软件完成的主要功能。在完成功能 2 的步骤中，采用了一维分段线性混沌映射，与 logistic 映射相比较，它能均匀地分布于 0 和 1 之间[10,12]，产生很强的随机性，而分段线性混沌系统中取 p=0.253 而不是 0.25 主要是要避免混沌系统在迭代过程中出现连续的 0 值，从而无法实现随机性，在加密和解密过程中引入动态更新的查询表技术能提高加密的速度以及密文的安全性，并且能实现消息的认证以及数据的完整性和一致性。由于加密后密文为算法迭代的次数，所以对加密后的数据流进行 Uuencode 编码能得到最终编码后的密文，这样可以保证所得到的邮件密文以统一的文件形式在网络中传输。而在完成邮件收发的过程中，按照 Base64 编码方式进行，并遵照 Internet 上常用的传送和接收电子邮件的标准：SMTP 和 POP3 协议。

以下是对本软件的具体运行流程，其中图 3 是本软件的运行后的用户界面。

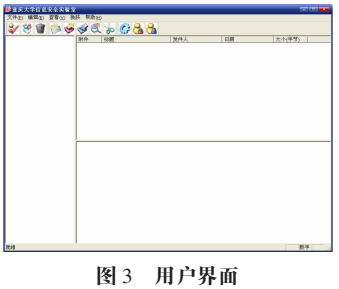


图 3　用户界面

(1)启动程序进入主窗口，进行账号的创建。

(2)写用户所要发送的邮件，其中包括收件人地址、主题和内容(如图 4(a))。

(3)输入用户密钥并检验合格后界面线程启动，点击“加密”按钮。

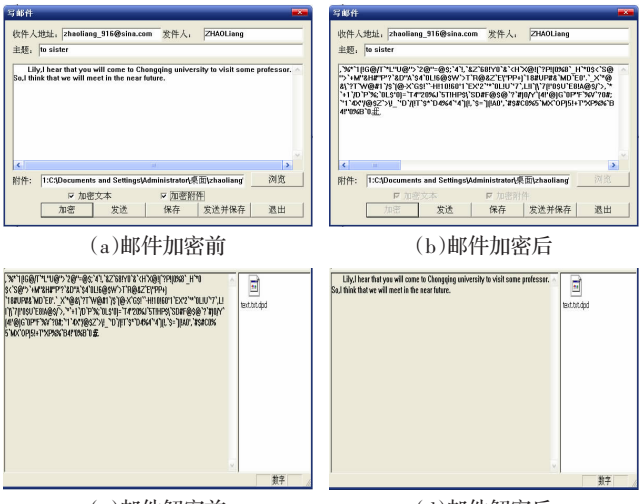
(4)线程启动后，完成对电子邮件数据的加密(如图 4(b))。

(5)邮件加密后点击“发送并保存”完成对电子邮件的输出。

(6)接收端收到发送来的邮件，完成对邮件的解密(如图 4(c)和图 4(d))。

5　安全性分析

通过加密运算，真实的文本数据信号被混沌信号掩盖，即明文被密文所取代，在整个网络信道中传输的是加密后的混沌信号，这样保证了文本数据信号的安全性，使得在网络中传输的密文很难被破译。



(a)邮件加密前　(b)邮件加密后

(c)邮件解密前　(d)邮件解密后

图 4　邮件系统的加解密流程

5.1　统计特性分析

由于一维分段线性混沌系统对初始值和系统参数特别敏感，所以可以应用它产生足够大的混沌序列流空间，满足混沌加密的需要。通过对混沌序列流空间的二进制序列进行检测，可以看出其中 0 和 1 的分布基本均匀(如表 1)。并且，为了评价此混沌序列流空间的随机性，应用美国国家标准与技术委员会(NIST)所推荐的随机性测试软件(US NIST RNG test software)对当初始值取 0.012 353 32 且 p 取 0.253 时迭代 20、40、60……40 000 次后的混沌序列空间(与表 1 中的序列取法相同(见表 1 注))的主要性能进行测试，发现其测试结果均满足随机性要求(如表 2)。

表 1　0、1 分布统计

初始值	参数 p	0 的个数	1 的个数	0 占百分比/(%)	1 占百分比/(%)
0.012 353 32	0.253	8 069	7 931	50.400	49.600
0.012 353 32	0.153	8 015	7 985	50.100	49.900
0.123 219 76	0.253	8 124	7 876	50.775	49.225

注：其中程序步长均设定为 0.005，表 1 是当初始值为 0.012 353 32 或 0.123 219 76 且 p=0.253 或 0.153 时迭代 20、40、60……40 000 次时取迭代值小数点后第 2、3、4 位所组成的十进制数取模 256 后二进制化的混沌序列空间中 0 和 1 的分布情况。

因此，从以上统计分析可以证明应用分段混沌系统得到的序列满足随机性要求。

5.2　密钥和明文敏感性分析

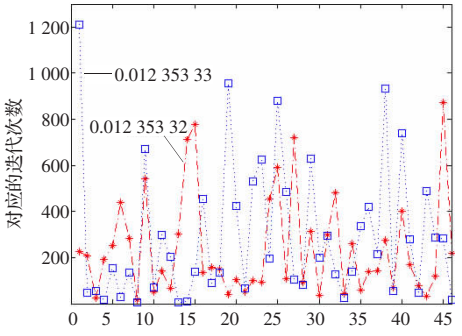
一个好的加密系统，其密文必须对密钥很敏感，即密钥很小的一点变化，会导致密文发生很大的变化[14]。因为一维分段线性混沌系统具有很强的非线性，所以一般情况下，对明文进行加密后，密文对密钥和明文都有非常好的敏感性。

为了测试密钥的敏感性，做了以下对比实验：当参数 p 为 0.253，取密钥即初始值为“0.012 353 32”，对明文“My name is ZHAO Liang，I come from Mianyang.”进行加密；当其它条件不变，仅将密钥即初始值由“0.012 353 32”改为“0.012 353 33”，对同样的明文进行加密。实验结果如图 5(a)和表 3 所示，当对密

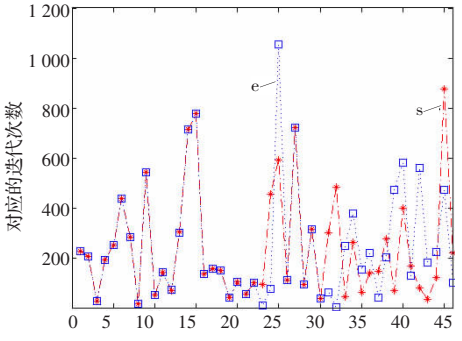
表 2 随机性测试结果

测试名	测试值(p 值)	是否通过	测试名	测试值(p 值)	是否通过
频率测试	0.275 279	是	重叠模板匹配测试	0.490 782	是
块内频率测试	0.700 733	是	Lempel-Ziv 压缩测试	1.000 000	是
游程测试	0.992 492	是	线性复杂度测试	0.468 092	是
块内最长游程测试	0.653 236	是	序列测试 *	0.310 445	是
二值矩阵秩测试	0.618 200	是	近似熵测试	0.614 064	是
离散傅立叶变换(频域)测试	0.538 167	是	累积和测试 *	0.327 956 5	是
非重叠模板匹配测试 *	0.492 724	是			

注:其中各种测试的详细描述请参考文献[13],非重叠模板匹配测试、串行测试和累积和测试由于有两个及以上的测试值,因此用星号 * 标出,并且用平均值作为其测试的最终结论值。测试所用的设定阈值为 0.01。



(a)密钥的敏感性对比图



(b)明文的敏感性对比图

图 5 密钥和明文的敏感性分析图

表 3 图 5(a)统计结果

密文相同个数	密文不同个数	最大迭代次数(i)	最大迭代数(c)	最小迭代次数(i)	最大迭代次数(c)
0	46	874	1 209	16	4

表 4 图 5(b)统计结果

密文相同个数	密文不同个数	最大迭代次数(i)	最大迭代数(p)	最小迭代次数(i)	最大迭代次数(p)
14	21	874	1 054	16	3

注:表中密文即是对明文进行加密后的迭代次数,"i"表示当初始值为 0.012 353 32,参数为 0.253 时对明文(1)的密文情况;"c"表示当初始值为 0.012 353 33,参数为 0.253 时对明文(1)的密文情况;"p"表示当初始值为 0.012 353 32,参数为 0.253 时对明文(2)的密文情况。而在表 4 中,密文相同和不同个数的统计是一个从明文为"s",另一个为"e"处开始的,所以在实验中首先去掉了改变处前面相同的字符个数。

钥稍微有点改变后,密文将完全不同。

为了测试明文的敏感性,又做了以下对比实验:当参数 p 为 0.253,密钥即初始值取为"0.012 353 32"时,分别对明文"My name is ZHAO Liang,I come from Mianyang."和"My name ie ZHAO Liang,I come from Mianyang."进行加密。可以看出,两段明文中只有一个"s"和"e"的差异,然而如图 5(b)和表 4 所示的实验结果,只要明文稍微有点改变,则从改变处开始,将有超过一半的密文出现变化。

由此可以看出密钥和明文都有着很好的敏感性。

5.3 抗攻击分析

由于文献[12]中所提出的算法存在安全漏洞,可能被攻击者利用用来攻击动态查询表,即在不知道当前迭代轨道 X 精确值的情况下,预测出交换后字符的位置。而在改进方案中,是由当前 X 值的小数点后面的第 2、3、4 位数构成一个十进制数对 256 取余来决定字符的交换位置,使得字符的交换和当前精确的值关联起来,所以完全消除了原攻击赖以存在的基础。类似地,攻击者之所以能用选择明文攻击和已知明文攻击来全部或部分恢复出密钥流,也完全是依赖于以下的事实:攻击者可以在不知道当前迭代轨道精确值的情况下,预测出查询表的更新规律。在改进方案中,由于把字符的交换和当前精确的值关联起来,原来攻击赖以存在的基础已经被消除,所以原来的攻击也就不再可能了。抗碰撞是指找到两个不同的输入 $x'\neq x$,得出的散列结果 $h(x')$、$h(x)$相同的可能性很小。而生日攻击本质上和碰撞问题相似,是两个随机输入数据散列出相同值的概率问题。在改进算法中,查询表的更新过程和迭代轨道的精确值密切相关,而且还引入了多轮多对查询表栏的交换机制,这可以确保消息或密钥的任意微小改变,通过迭代过程的不断扩散放大,将最终导致完全不同的散列结果。由于篇幅所限,关于抗攻击的详细分析可以参见文献[11]。

5.4 其他性能分析

Shneier 在他的经典著作[15]中写到过:"一个好的密钥空间应该很大,以至于强力攻击是小可能的"。而本算法取方程的初始状态作为密钥,密钥空间巨大,完全满足加密要求,并可以防止密钥搜索攻击;且由于混沌系统对于初值和参数极其敏感,所以,不可能由迭代值反向推出初始状态。

相对于许多传统的加解密和散列方案,虽然在文献[11]中提出的改进算法相对较慢,但由于此算法是将加解密和散列运算以组合的方式同时进行,因此,如将该改进算法应用到相应的领域内,将可以极大地提高这些领域内应用的效率。

6 结束语

介绍了一种基于一维分段线性混沌系统的电子邮件加密

(下转 133 页)