基于复合混沌序列的动态密钥AES加密算法

闫乐乐 李 辉
(电子科技大学航空航天学院 成都 611731)

摘 要 为了解决传统AES算法因种子密钥固定和密钥空间确定所导致的安全性降低的问题,将混沌序列加密和传统AES算法相结合,提出一种基于复合混沌序列的动态密钥AES加密算法并完成软件实现。该算法采用私钥构造加解密两端的同参Logistic和Tent双混沌系统,通过迭代与明文长度相关的次数产生交叉复合混沌序列,进而量化映射为AES分组的动态初始密钥进行AES加解密。安全性分析、统计检测和性能测试实验的结果表明,该算法具有安全性高、适应性强、运算速度快等优点,非常适用于跨平台无线数据安全传输等应用场合。

关键词 Logistic映射,Tent映射,混沌序列,AES算法
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.06.022

Dynamic Key AES Encryption Algorithm Based on Compound Chaotic Sequence

YAN Le-le LI Hui
(School of Aeronautic and Astronautic, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract To solve the traditional AES(Advanced Encryption Standard) algorithm's security reduction problem caused by the unchanged seed key and fixed key space, combining with the chaotic sequence cipher and AES algorithm, this paper proposed a dynamic seed key AES encryption algorithm based on compound chaotic sequences and finished the software implementations. The algorithm uses the private key to construct the same-parameters' dual chaotic system at both ends of the encryption and decryption. The chaotic sequence is generated and cross-combined through two chaotic systems(logistic and tent) by a number of iterations that related to the plaintext length, and then mapped into the dynamic initial seed keys for the AES block cipher. Through the security analysis, statistical test and performance test, the analytical results demonstrate that the proposed algorithm has the advantages of high security, strong adaptability and fast operation speed, and it is very suitable for cross platform wireless secure data transmission applications.

Keywords Logistic map, Tent map, Chaotic sequences, AES algorithm

1 引言

信息安全日益重要,AES(Advanced Encryption Standard)算法作为分组对称加密方法,凭借其高效率、强安全性和良好的软硬件适应性,早已标准化并得到广泛应用,保护着各领域敏感信息的安全。

鉴于AES在众多加密算法中的重要地位,全世界范围内对其研究分析的热度不断升温。如何改进AES算法或利用AES算法设计更加安全高效的加密算法是密码学界研究和分析的重点。肖慧娟等人提出了用混沌信号改造AES加密算法的观点[1],通过级联混沌与AES系统来解决密钥产生和管理难题,但此方案并不具体;朱灵波等人通过改进AES的ECB工作模式,减小了时空消耗[2],但是其在尾端处理的实现上过于复杂;陈红等人提出用Logistic映射产生混沌序列量化后的二进制数代替AES算法的初始密钥[3],但是其混沌序列产生和量化方法的效率不高;赵芮等人提出二维双混沌密钥发生器的AES改进算法[4],克服了AES算法密钥唯一的缺点,但是其混沌序列代替所有轮密钥的思想在实现上复杂度过高,二维双混沌系统的计算效率也不高,造成效率下降明显;Chen D等人提出了基于二维Logistic映射的AES密钥生成和拓展算法[5],增强了子密钥之间的独立性,从而提高了算法的安全性和鲁棒性,但其缺乏对算法效率方面的考虑;Hraoui S等人通过对图像加密领域中标准的AES算法和Logistic混沌映射序列加密算法的加密强度和效率进行实验分析,得到AES算法更安全、混沌加密速度更快的结论[6];Challita N等人将分段线性混沌映射函数PWLCM引入简单

到稿日期:2016-05-11 返修日期:2016-09-25 本文受四川省科技计划项目:面向国产第三代核电站的核级输配电系列开关设备关键技术研究及其产业化(2015GZ0028),高铁安全保障关键技术研究(2016GZ0335)资助。
闫乐乐(1990-),男,硕士生,主要研究方向为系统工程与信息安全,E-mail:gladele@163.com;李 辉(1963-),男,博士,教授,主要研究方向为模式识别与智能系统。

AES算法的S变换和行移位变换环节中，提出了增强的AES算法[7]并应用于无线传感器网络中医学图像的加密，增强了算法鲁棒性；Pradhan C等人在标准AES算法的基础上增加了利用一维或混合混沌序列加密方法对AES的种子密钥进行加密的环节，提出了混沌改进型AES算法[8]，其虽然在效率上相比标准AES算法稍有下降，但在一定程度上增强了算法的安全性，为基于混沌的AES算法的改进提供了思路。

上述基于AES的改进算法在安全性、适应性、效率等综合方面考虑不足，无法满足当前跨平台无线数据加密的实际需求。为了解决上述问题，克服传统AES算法种子密钥固定的缺点，在保证高效率的同时提高算法的安全性，本文将混沌序列加密与AES分组加密相结合，提出一种基于复合混沌序列的AES加密算法。

2 分组AES加密与混沌加密

在序列加密算法中，混沌序列加密算法凭借其简单且密码学特性好的优点得到了越来越广泛的使用。前人的研究也表明了将混沌序列加密引入AES算法的好处。下面介绍分析AES算法和两种混沌映射，为后文的基于复合混沌序列的AES加密算法的设计与实现做铺垫。

2.1 AES算法介绍

AES加密算法中的数据分组是进行序列运算的基本单元，每次序列变换过程中的结果可抽象描述为一个状态，以二维的字节数组矩阵形式表示，其行数固定为4；列数 Nb 由分组长度决定，是分组长包含字的个数。在AES标准中数据分组长度为128位，所以 $Nb=4$。其密钥长度 Nk 和加密轮数 Nr 是可变的，关系如表1所列。

表1 密钥长度与加密轮数的关系

AES类型	密钥长度 Nk/字	加密轮数 Nr
AES_128	4	10
AES_192	6	12
AES_256	8	14

AES算法的设计原型是Square算法，设计策略是宽轨迹策略，原理上是采用多轮代替置换网络结构。每一轮变换都需要进行3层子操作。

1)非线性层。进行字节代换ByteSub变换，起到混淆作用，可用S盒查表法提高运算速度。

2)线性混合层。包括行移位ShiftRow和列混合MixColumn变换(最后一轮没有)，起到每轮的扩散作用。

3)轮密钥加层。轮密钥加AddRoundKey变换是将状态矩阵与轮密钥矩阵进行简单的异或操作。轮密钥的产生通过密钥扩展KeyExpantion来实现，其将种子密钥扩展为加密或解密所需要的 $Nk+1$ 组子密钥。具体密钥拓展方案可参考文献[9]。

本文以AES_256为例，加解密流程如图1所示。明文数据分组首先与初始密钥的前128位异或后(白化处理)进入14轮变换操作得到密文，前13轮以同样的方式变换，第14轮没有列混合变换，解密过程为加密过程的逆过程。从一维的角度来看，AES_256将以字节为单位分块后的明文经过上述变换加密后得到等长的分组密文。

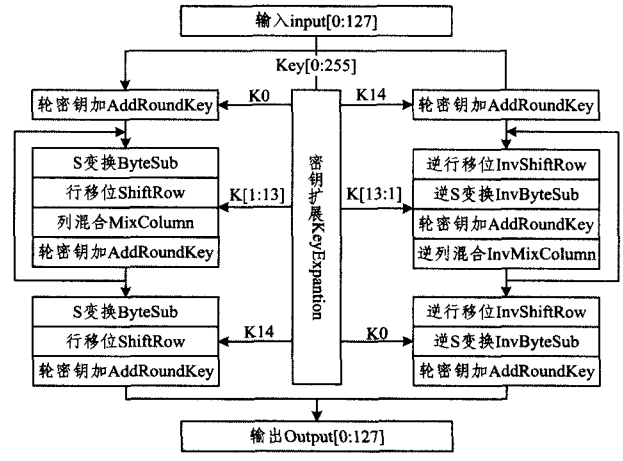


图1 AES_256加解密流程图

2.2 混沌序列加密算法

混沌现象具有良好的非周期性、随机性、对初始状态及控制参数极其敏感、容易产生分岔等特性，是一种确定性伪随机过程，迭代模型可以用非线性方程表示。混沌系统的迭代输出序列看似存在杂乱无章的噪声，但用于加密时能很好地掩盖有用信息。混沌系统由解析方程、控制参数和初始条件完全确定。只有相同的初始控制参数和相同的初始值才可以复原混沌信号。所以混沌加密是一种对称序列密码体制，具有快速、简单、实时性好的优势，在信息加密领域的应用逐渐增多。

下面分析两种经典的一维混沌系统模型：Logistic和Tent映射。

2.2.1 Logistic映射

Logistic映射作为一种典型的混沌动力学系统[10]，其解析方程为：

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

其中，x 为混沌变量；$\mu\in(0,4]$ 为控制混沌方程形态的参数。

当 μ 值确定后，对于任意初始值 $x_0\in(0,1)$，迭代相同次数可得到确定并且相同的数值序列。随着 μ 值的不断增大，系统特性也存在不同呈现，当增大到一定程度时，序列值呈现出不确定性，没有收敛到固定值，且具有遍历性。反复经历此过程会产生周期分叉现象。

当 $2.6\leqslant\mu\leqslant4$ 时，Logistic映射的分岔图如图2所示。由图2可知，当 μ 值大于3.57后，系统开始呈现混沌态，所产生的混沌序列的随机性较好。

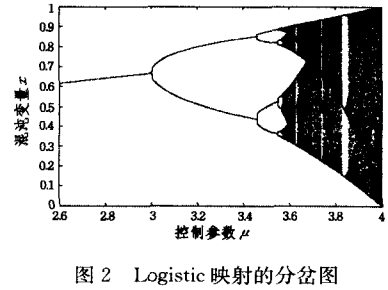


图2 Logistic映射的分岔图

当 $\mu=4$ 时，Logistic 映射序列呈现极大的散布性，对迭代初值异常敏感，表现出明显的混沌特征，被称为满映射混沌状态。此时混沌变量的运动形式有如下特征。

1)概率密度分布函数为[11]：

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}}, & 0<x<1\\ 0, & \text{other}\end{cases} \tag{2}$$

$\rho(x)$不依赖于初值 x_0，产生的混沌序列具有遍历性。但是其混沌变量的分布是不均匀的，在分布曲线两端出现奇异性。

2)混沌序列中轨迹点的均值为：

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}x_n=\int_0^1 x\rho(x)\mathrm{d}x=0.5 \tag{3}$$

Logistic 混沌序列直观上类似于噪声。在不知道初始参数的情况下序列值是无法预测的。

该混沌系统下的 Logistic 映射对初值和控制参数的依赖性较强，即使是极微小的初值扰动，经过较少的迭代次数后相同的混沌系统就会生成完全不同的混沌序列值。Logistic 映射混沌系统初值的敏感性和迭代快速发散性的 Matlab 仿真如图 3 所示。

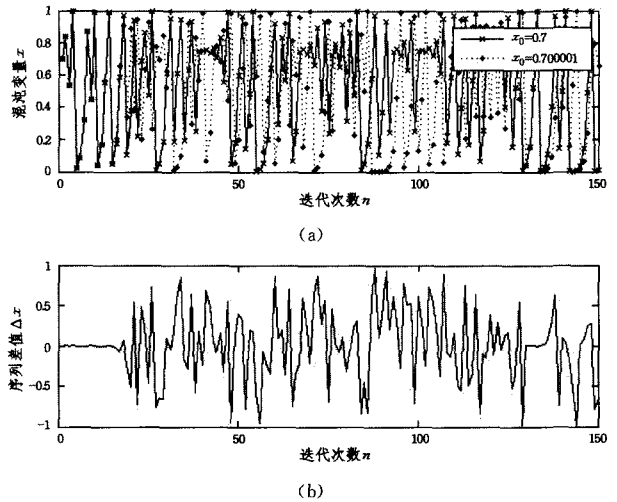


图 3　Logistic 映射的初值敏感性与迭代发散性

图 3(a)中虚线和实线分别表示混沌变量初值在 0.7 和 0.700001 时经过 Logistic 映射迭代 150 次产生的混沌序列，图 3(b)表示图 3(a)对应的在两个差别很小的初值下对应混沌的序列差值。由图 3 可知，仅经过大概 20 次迭代后初值存在初始参数微扰的混沌系统产生的混沌数值序列与原序列不能重合，而且差值在正负 1 间无规律。

2.2.2　Tent 映射

Tent 映射也可称作帐篷映射，是一种分段线性映射[12]，其典型动力学方程可描述为：

$$y_{n+1}=\begin{cases}\lambda * y_n, & 0<y_n<0.5\\ \lambda*(1-y_n), & 0.5<y_n<1\end{cases} \tag{4}$$

其中，y 为混沌变量，$\lambda\in(0,2)$为控制参数。当 λ 值确定后，对于任意初始值 $y_0\in(0,1)$，可迭代得到一个确定的数值序列。

当 $1\leqslant\lambda<2$ 时，Logistic 映射的分岔图如图 4 所示。由图 4 可知，当 λ 值为 1.4～2 时，系统进入混沌态，尤其是当 λ 接近 2 时，产生的混沌序列的随机性较好。

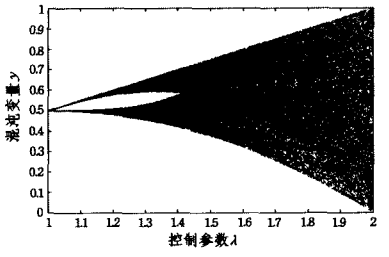


图 4　Tent 映射的分岔图

3　基于复合混沌序列的 AES 加密算法

3.1　AES 算法问题分析

在传统的 ECB(电子密码本)模式下，AES 算法的种子密钥是固定不变的，即每组明文分组采用相同的初始密钥。在其加密过程中密钥扩展方案虽然能够避免轮密钥和种子密钥的简单数学关系，但由于其密钥扩展方案本身的可逆性，使得轮密钥的泄露可以减少推导出种子密钥的工作量和复杂度。一旦固定的种子密钥被破解，整个加密系统信息安全将面临严重威胁。

传统 AES 算法虽然经过验证能抵抗当今已知的密码分析和攻击，但是 AES 是一种迭代型密码，攻击者可以根据轮密钥与种子密钥的关系来得出种子密钥的绝大多数比特位，然后进行较少量计算的穷举攻击，即有可能实现破解。公开加密算法的可靠性绝大部分取决于密钥，而 AES 算法的密钥空间由密钥长度决定，是完全确定的，这更有利于穷举攻击[1]。看似庞大的密钥空间实际上会被缩小。

可见传统的 AES 算法存在种子密钥固定和密钥空间确定的缺点。

3.2　算法的设计思路

为了解决传统 AES 算法存在的种子密钥固定和密钥空间确定导致安全性降低的问题，应当寻找既能动态产生种子密钥用于 AES 加密，而又不会在密钥的产生和管理上花费太多资源而影响 AES 算法高效率优势发挥的方法。

经过上文对两种混沌系统的分析，可以利用一维混沌系统良好的初值敏感性、伪随机性和非周期性等密码学特性，结合 AES 分组对称加密算法的加密速度快、效率高、低内存需求的优势，提出一种基于复合混沌序列的动态密钥 AES 数据加解密算法。该算法可继承一维混沌系统计算量小、复杂度高、随机性好的保密学特性，同时克服了传统 AES 加密算法密钥空间确定及种子密钥唯一的缺点，进一步提高了加密强度，同时不会对加密系统的实时性产生较大的影响。该算法的设计思路如图 5 所示。

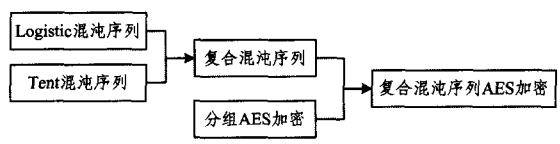


图 5　基于复合混沌序列的 AES 加密算法的设计思路

该算法通过构建 Logistic 和 Tent 混沌系统映射产生的混沌序列组合成的复合混沌序列作为明文分组 AES 块加密算法的初始动态密钥，逐块进行分组 AES 加密得到密文。

混沌系统各参数可作为加密系统的混沌密钥。这样，所有明文数据块都使用不同的密钥进行加密，从而构成“一次一密”加密系统。由于每个明文密文对所提供的真实密钥信息都极其有限，攻击者即便获取了多组明文密文对并破解出种子密钥，也无法破解出混沌密钥。

3.3 算法的具体描述

算法以 AES_256 为基础，采用私钥在加解密两端构造相同参数的复合混沌系统，迭代与明文长度相关的次数产生混沌序列进而产生 AES 算法的动态初始密钥进行 AES 块加解密。算法的基本流程如图 6 所示。

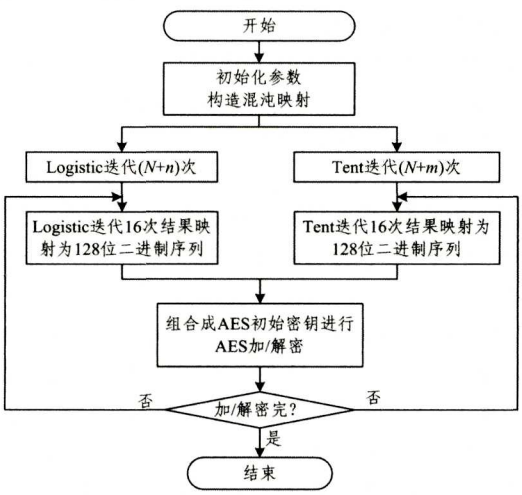


图 6 复合混沌 AES 算法的基本流程

加解密基本流程描述如下。

1)混沌系统构建与参数初始化

首先通过使用秘密信道或公钥加密体制选择传递包含有 Logistic 和 Tent 映射控制参数 μ 和 λ、初始值 x_0 和 y_0 与基本迭代次数 N 的私钥，分别在加密和解密端构造参数相同的 Logistic 和 Tent 映射系统。根据待加密明文的长度 len 可得到明文分块参数 n 和 m，其中，n 表示分块组数 $len/16$，m 表示分块后的剩余字节数 $len\%16$。

2)混沌序列产生和二进制量化

分别进行 Logistic 迭代 $N+n$ 次、Tent 迭代 $N+m$ 次以使混沌序列充分离散化，这样使得混沌系统参数本身与明文长度相关，在加密中利用了明文特性。而后每加密一个数据块都将两个混沌方程再连续迭代 16 次，选择每一个混沌实数序列小数点后有效位数的任意 3 位及以上(比如后 5 位)组成的整数对 256 取模完成混沌二进制序列量化[13]。将这样的两组 16 个混沌实数序列量化后的离散二进制结果以一定方式(交叉)组合作为 256 位 AES_256 算法块加密种子密钥。这样每个混沌实数可以量化为 8 个随机二进制序列，量化方法比文献[3]中每个混沌变量以 0.5 为阈值、分隔量化为 0、1 序列的方法更高效。

3)AES 动态加密和尾端处理

利用步骤 2)中产生的混沌种子密钥序列，逐块进行 AES 加密得到相应密文块。最后剩余的 m 个字节明文直接通过两个混沌二进制序列异或后的结果的前 $8m$ 位逐位进行异或得到尾密文，整个加密过程如图 7 所示。这种直接利用混沌序列加密的尾端处理机制能极大地减小计算量。

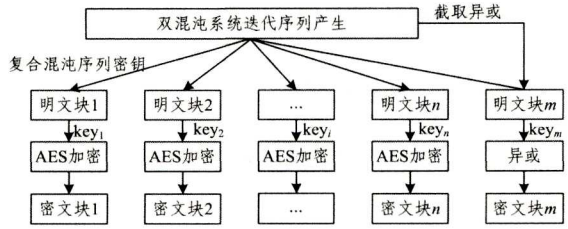


图 7 基于混沌的动态 AES 加密过程

经过以上步骤，依次将块密文合并且连接尾密文，最终可以得到与明文等长的复合混沌序列 AES 加密的密文。

按照以上算法描述，利用 C 语言编写实现了基于复合混沌序列的 AES 加密算法。其主要包括以下几个模块：1)双混沌序列产生模块，包括 Logistic 迭代函数、Tent 迭代函数；2)复合混沌序列量化模块，将两个混沌系统产生的实数序列量化拓展为 AES 动态加密种子密钥；3)复合混沌序列 AES 加密模块；4)混沌序列 AES 解密模块。

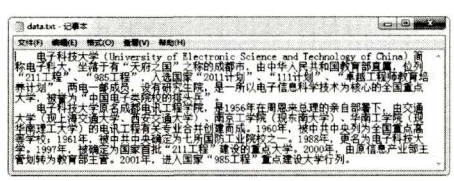
4 实验结果与分析

4.1 安全性分析

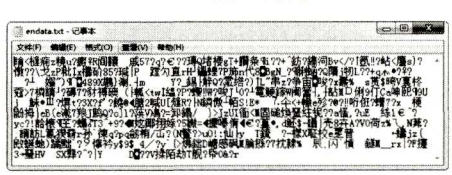
4.1.1 有效性与敏感性验证

为了验证算法加解密的有效性和密钥敏感性，在 PC 平台下运用该算法进行文本文件加解密实验。

当选择加密参数(混沌密钥)为 $\mu=4.0$，$x_0=0.8$；$\lambda=1.79$，$y_0=0.134$，$N=100$ 时，对长度为 810 字节的 TXT 文本文件进行加密，结果如图 8 所示。



(a)加密前文本信息

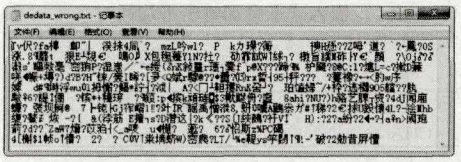


(b)加密后文本信息

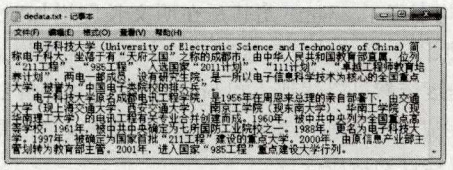
图 8 文本文件加密结果

在对应的解密实验中，当稍微改变任意解密密钥参数(本实验将 x_0 扰动为 $0.8+10^{-16}$)时，经过文件解密后文本信息显示为乱码；只有当解密密钥与加密密钥完全相同时才能正确解密出明文。解密实验结果如图 9 所示，说明此算法对初始参数异常敏感，其密钥敏感性非常好。

从密钥更换的有效性的角度考虑，好的加密算法应当对密钥变化极其敏感，满足密钥雪崩准则，即细微改变密钥后应导致密文中大约一半比特的变化。本文经过进一步的统计得出，在加密实验中极小的密钥变化(10^{-16})将导致密文中比特变化率为 49.45%，密钥雪崩现象明显，从而验证了算法的密钥依赖性和有效性。



(a)错误解密结果



(b)正确解密结果

图 9　文本文件解密结果

此外，经过原理分析可以看出本文算法与传统 ECB 模式下的 AES 算法相比，其对同结构(长度)明文的细微变化的敏感程度相同，只影响到明文变化所处分组位置的密文变化，但是对明文块的排序情况和明文总长度变化异常敏感。在稍微改变明文总长度而不改变原来内容或者打乱明文块顺序的情况下，得到的密文与之前得到的密文大相径庭，与明文特征也毫无关系，明文扩散性较好。其原因是复合混沌密钥与明文长度相关，而且是动态变化的，这种混沌密钥产生过程与 AES 加密过程的级联关系极大地增强了系统的复杂度和安全性。

4.1.2　密钥空间

理论上传统的 AES_256 算法的密钥空间确定为 $2^{256}\approx 1.16\times10^{77}$。

本文提出的算法中可充当密钥的参数包括 Logistic 混沌系统的控制参数 μ 和初值 x_0，Tent 混沌系统的控制参数 λ 和初值 y_0，以及基本迭代次数 N，如表 2 所列。32 位处理器中 double 型的数据精度为小数点后 16 位有效数字。

表 2　密钥空间分析

参数名称	数据类型	取值范围	空间大小
μ	double	[3.57,4.0]	$K\mu\approx0.43\times10^{16}$
x_0	double	(0,1)	$Kx0\approx1\times10^{16}$
λ	double	(1.4,2.0)	$K\lambda\approx0.6\times10^{16}$
y_0	double	(0,1)	$Ky_0\approx1\times10^{16}$
N	正整数	(50,+∞)	$Kn(+\infty)$

总的密钥空间大小为：

$$K=K\mu\times Kx_0\times K_\lambda\times Ky_0\times Kn\approx0.258\times Kn\times10^{64} \quad (5)$$

可见，在理论上本算法的密钥空间与传统 AES_256 相差不大，但很有效，具有多级控制且不确定的特点。基本迭代次数的取值 Kn 是不确定且足够大的正整数，加上叠加迭代次数(m、n)与明文的总长度相关，使密钥空间具有不确定性，提高了采用盲目的穷举法暴力破解密文信息的难度，从而能抵抗穷尽密钥搜索攻击。

4.2　统计检测

统计检测实际上是指随机性检测，其目的是查看验证算法的密码学特性，主要包括密文随机性、明密文独立性等验证，可以通过相关性检测、频数检测和扑克检测实现。

4.2.1　相关性检测

混沌序列的非周期性是在理论上数值计算精度为无限时的理想特性。而在计算机应用领域中，序列长度和计算精度总是有限的，因此序列也必然呈现周期性和相关性。可通过相关性分析来判断二进制序列的随机性。

两个长度为 N 的二进制序列$\{S_1(i)\}$和$\{S_2(i)\}$的互相关函数为[14]：

$$R_{S_1,S_2}(m)=\frac{1}{N}\sum_{i=0}^{N-1}[S_1(i)-\overline{S_1}][S_2(i+m)-\overline{S_2}] \quad (6)$$

其中，$\overline{S_1}$、$\overline{S_2}$为序列均值，m 为相关间隔。当两序列相同时，变为自相关函数。对于两个相同混沌二进制序列，当序列长度 N 趋近于无穷大时，自相关函数值为：

$$R_\infty=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}[S(i)-\overline{S}][S(i+m)-\overline{S}]=\begin{cases}1/4, & m=0\\ 0, & m\neq0\end{cases} \quad (7)$$

本文对所提算法中使用的 Logistic、Tent 和复合序列 3 种混沌二进制序列进行一定长度的截断($N=640$)，并进行归一化自相关函数仿真，结果如图 10 所示。

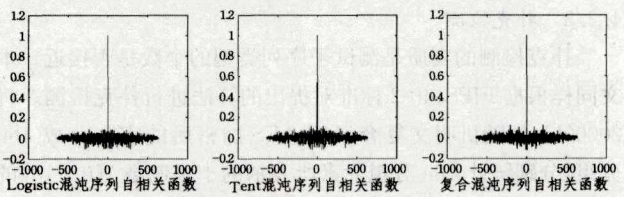
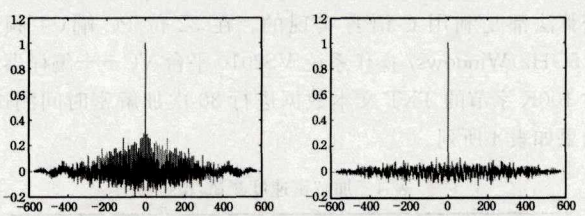


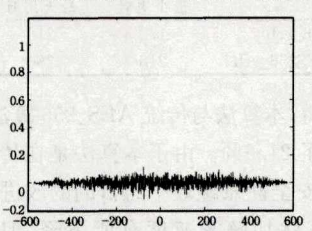
图 10　3 种混沌二进制序列归一化自相关函数

由图 10 可知，3 种混沌二进制序列的自相关性能都较好，自相关函数接近于 δ 函数，具有类随机性。其中复合混沌序列的自相关性能更加优越，Logistic 混沌序列其次。通过测量 3 种序列的频数可以得到三序列的平衡度分别为 49.5%，51.4%，49.8%，说明经过复合后的混沌二进制序列的平衡度和随机性相比单混沌序列得到了改善。

对 4.1.1 节加密实验中截取的前 576 位明密文二进制序列进行自相关和互相关性实验，结果如图 11 所示。



(a)归一化明文序列自相关函数　(b)归一化密文序列自相关函数



(c)明密文序列互相关函数

图 11　明密文二进制序列的相关性检测结果

可以看出，密文的自相关特性要明显好于明文，密文序列自相关旁瓣和明密文互相关函数值均接近于 0。说明经过复合混沌 AES 加密后的密文具有良好的随机性，且与明文不相关。

4.2.2 频数检测

本文根据美国国家标准和技术委员会(NIST)发布的具有权威性和代表性的联邦信息处理标准 FIPS140-2[15],对提出的算法进行频数检测。检测原理是统计 20000bit 的待测密文序列中 1 出现的个数 X。当 $9725<X<10275$ 时测试通过。本文对不同统计特征情况下 20000bit 明文加密后的密文序列进行频数检测,结果如表 3 所列。

表 3 密文频数检测

明文(1 占比)	0	20%	40%	60%	80%	100%	随机
密文频数	10026	10028.2	10022	9989.7	10033	10034	9959.5

表 3 中除了明文全 0 或全 1 的情况,其他条件下测定的密文中 1 的频数均为多次(20 次)实验取平均值的结果。

由表 3 可知,不管明文具有明显的统计特性还是随机性,其对应的密文随机性都较好,即密文不依赖于明文的统计特性,说明该算法明密文的独立性很好,能有效抵抗差分攻击。

4.2.3 扑克检测

扑克检测的实质是测试子序列类型的个数是否接近。本文同样根据 FIPS140-2 标准对提出的算法进行扑克检测。将 20000bit 的随机明文复合混沌 AES 加密后的密文分成 4bit 分组,分别统计 4bit 分组元素所表示的十进制数 $i(0\sim15)$ 的个数 $f(i)$,利用

$$X=(16/5000)*(\sum_{i=0}^{15}[f(i)^2])-5000 \quad (8)$$

计算出统计量 X,当 $2.16<X<46.17$ 时通过测试。经过 30 次扑克测试,统计量 X 均落在范围[9.13,23.18]内,均值为 14.22,都通过了扑克测试。可见,本算法的密文随机性较好,能够抵御统计分析等常见攻击。

4.3 软件性能

软件性能测试的目的是评估算法在各个平台上的实现速度和适应性。本文研究的 AES_256 算法和复合混沌 AES 加密算法都是利用 C 语言实现的。在 32 位 PC 端(主频为 2.5GHz)Windows7 操作系统 VS2010 平台 VC++编译器下对 100K 字节的 TXT 文本数据进行 30 次加解密时间测试,结果如表 4 所列。

表 4 加解密速度测试/ms

加密算法	加解密耗时		
	最少用时	最大用时	平均耗时
AES_256_ecb	172	218	194.5
CHAOS_AES256_ecb	218	250	236.6

由表 4 可得,本算法与传统 AES_256 算法相比在实现速度上平均下降了 21.6%。由于本算法是在传统 AES 算法的基础上以提高安全性兼顾效率为目的的改进算法,其效率下降是必然的,虽然加解密速度有所下降,但依然可以超过 3Mbps,继承了 AES 算法高效率的优点。相比于文献[4]中算法以大程度牺牲加密效率(加密时间是传统 AES 算法的 4~6 倍),一味追求安全性的做法,本算法具有明显的效率优势。

将本算法移植到 VxWorks 操作系统下的嵌入式平台(主频为 400MHz)并进行多次对比实验,结果如表 5 所列。

表 5 嵌入式平台加解密平均耗时/ms

加密算法	明文长度/kB		
	1	5	10
AES_256_ecb	17	85	170
CHAOS_AES256_ecb	20	110	230

表 5 表明加解密速度比传统 AES_256 算法的效率有所下降,平均下降了 27%。尤其是在明文长度增加时,效率下降明显,原因是其算法复杂度随明文长度增加而增加。但是加解密速度依然可以达到 400kbps。因此利用该算法可以很方便地完成跨平台加密系统的构建,在保证高效的同时具有很好的灵活性和适应性。

结束语 将复杂的 AES 密钥变化映射为简单的混沌系统参数变化,利用级联思想在继承 AES 加密算法优点的同时以牺牲很小的执行效率为代价进一步增强了算法的安全性。

从应用角度考虑,本算法目前已经应用于可变帧长的电力数据包无线加密传输,为高安全级别智能输配电网信息实时保密通信提供了新的方法和思路。本算法配合公钥密码机制可构成安全、灵活、高效的密码体制,以应用到其他实时保密通信场合。

参 考 文 献

[1] XIAO H J,QIU S S,DENG C L. Image Encryption Scheme Based on AES and Chaotic Series Encryption[J]. Computer Engineering,2007,33(23):154-155. (in Chinese)
肖慧娟,丘水生,邓成良. 基于混沌映射和 AES 算法的图像加密方案[J]. 计算机工程,2007,33(23):154-155.

[2] ZHU L B,DAI G Z,LIU H. An Optimized Data Stream Encryption and Decryption Implementation of AES Algorithm with Improved-ECB(IECB) Mode[J]. Computer Engineering and Applications,2006,42(12):1-5. (in Chinese)
朱灵波,戴冠中,刘航. 一种改进 ECB 模式的 AES 算法加解密优化方案[J]. 计算机工程与应用,2006,42(12):1-5.

[3] CHEN H,CHEN Y. Research on AES Algorithm Based on Chaos[J]. Journal of Beijing Technology and Business University(Natural Science Edition),2009,27(5):57-60. (in Chinese)
陈红,陈谊. 一种基于混沌的 AES 算法的研究[J]. 北京工商大学学报(自然科学版),2009,27(5):57-60.

[4] ZHAO R,WANG Q S,WEN H P. Design of AES algorithm Based on Two Dimensional Logistic and Chebyshev Chaotic Mapping[J]. Microcomputer Information,2008,24(33):43-45. (in Chinese)
赵芮,王庆生,温会平. 基于二维 Logistic 与 Chebyshev 映射 AES 混沌加密算法[J]. 微计算机信息,2008,24(33):43-45.

[5] CHEN D,QING D,WANG D. AES Key Expansion Algorithm Based on 2D Logistic Mapping[C]// Fifth International Workshop on Chaos-Fractals Theories and Applications. 2012:207-211.

[6] HRAOUI S,GMIRA F,JARAR A O,et al. Benchmarking AES and chaos based logistic map for image encryption[C]// 2013 ACS International Conference on Computer Systems and Applications (AICCSA). IEEE,2013:1-4.

(下转第 160 页)

探讨[J]. 中国空间科学技术,2004,24(1):31-36.

[8] LI J Y. The design and implementation of SCPS-SP/IPSec protocol conversion[D]. Harbin: Heilongjiang University, 2013. (in Chinese)
李敬媛. SCPS-SP/IPSec 协议转换的方案设计与实现[D]. 哈尔滨:黑龙江大学,2013.

[9] YANG Y H. Research on the authenticated encryption technology in CCSDS[D]. Shenyang: Shenyang Aerospace University, 2011. (in Chinese)
杨亚辉. CCSDS 认证加密技术研究[D]. 沈阳:沈阳航空航天大学,2011.

[10] LI H X. Research on data encryption/decryption strategy of CCSDS space communication system[D]. Shenyang: Shenyang Ligong University, 2011. (in Chinese)
李海霞. CCSDS 空间通信系统中数据加密/解密策略研究[D]. 沈阳:沈阳理工大学,2011.

[11] LI H, FAN X X, MI J N, et al. Analysis of security technologies in integrated space-air-ground networks[J]. Journal of CAEIT, 2014,9(6):592-597. (in Chinese)
李华,范鑫鑫,秘建宁,等. 空天地一体化网络安全防护技术分析[J]. 中国电子科学研究院学报,2014,9(6):592-597.

[12] XU W, WANG T, LI L. The multi-level self-adaptive space communication security protocol[C]// Proceedings of the International Conference on Information Technology, Computer Engineering and Management Sciences. 2011:246-249.

[13] GONG C Q, YANG Y H. Research on the authenticated encryption technology in CCSDS[C]// Proceedings of the International Conference on Computational Intelligence and Industrial Application. 2010:321-329.

[14] AKYILDIZ I F, AKAN O B, CHEN C, et al. The state of the art in interplanetary Internet[J]. IEEE Communications Magazine, 2004,42(7):108-118.

[15] LIU J F, ZHOU M T. Research and taxonomy of replay attacks on security protocol[J]. Computer Application Research, 2007, 24(3):135-139. (in Chinese)
刘家芬,周明天. 对安全协议重放攻击的分类研究[J]. 计算机应用研究,2007,24(3):135-139.

[16] 廖勇,郭修琼. 一种 SCPS-SP 多安全等级及抗重放功能的设计方法:201510489336.3[P]. 2015-08-11

[17] SCPS Reference Implementation [EB/OL]. [2016-07-25]. http://www.openchannelfoundation.org.

[18] NS2[EB/OL]. [2016-07-25]. http://www.isi.edu/nsnam/ns.

[19] CCSDS. Space communications protocol specification(SCPS)-transport protocol: CCSDS 714.0-B-2, Blue Book[S]. 2006.

(上接第 138 页)

[7] CHALLITA N, BAKHACHE B. Enhancement of S-AES using chaos for the support of biomedical applications[C]// International Conference on Advances in Biomedical Engineering. IEEE, 2013:175-178.

[8] PRADHAN C, BISOI A K. Chaotic Variations of AES Algorithm[J]. International Journal of Chaos, Control, Modelling and Simulation, 2013, 2(2):19-25.

[9] DAEMEN J, RIJMEN V. AES Proposal: The Rijndael Block Cipher (V2)[EB/OL]. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf, 1999.

[10] ZHAO Y, LI X M. The Application of Compound Chaotic Encryption Algorithm in Power System Information Security[C]// The 26th Academic Annual Meeting of Chinese Colleges major in Power System Automation and Chinese Institute Of Electrical Engineering Power System Specialized Committee. 2010: 193-193. (in Chinese)
赵云,李晓明. 复合混沌加密算法在电力系统信息安全中的应用[C]//中国高等学校电力系统及其自动化专业第二十六届学术年会暨中国电机工程学会电力系统专业委员会 2010 年年会. 2010:193-193.

[11] CAI J, CHEN X, XIANG X D. Substitution-Permutation Network Structured Image Encryption Algorithm Based on Chaotic Map[J]. Computer Science, 2014, 41(9):158-164. (in Chinese)
蔡俊,陈昕,向旭东. 一种基于混沌的代换-置换结构图像加密算法[J]. 计算机科学,2014,41(9):158-164.

[12] AN Y M, HAO R F, ZHANG Z X, et al. The Generation and Analysis of Pseudo Chaotic Sequences Based on Tent Map[J]. Journal of Taiyuan University of Technology, 2008(S1):71-74. (in Chinese)
闫永梅,郝润芳,张朝霞,等. 基于 Tent 映射的伪混沌序列的产生和分析[J]. 太原理工大学学报,2008(S1):71-74.

[13] JIA K J, LIANG J, DU T H, et al. Chaotic Encryption Algorithm Based on Logistic Map Applied in Remote Monitoring of Transportation[J]. Control and Instruments in Chemical Industry, 2012, 39(12):96-100. (in Chinese)
贾科进,梁杰,杜太行,等. 运输远程监控中基于 Logistic 映射的混沌加密算法[J]. 化工自动化及仪表,2012,39(12):96-100.

[14] YU J F, YANG W G, LU W T, et al. Analysis of the Full Mapping Logistic Sequence's Generation and Performance[J]. Telecommunication Engineering, 2013(2):140-145. (in Chinese)
余金峰,杨文革,路伟涛,等. 满映射 Logistic 数字混沌序列的产生及性能分析[J]. 电讯技术,2013(2):140-145.

[15] STANDARDSTECHNOLOGY N I O. Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules[J/OL]. http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf, 2004.

[16] ELBADAWY A M, MOKHTAR A, EL-MASRY W A, et al. A new chaos Advanced Encryption Standard (AES) algorithm for data security[C]//2010 International Conference on Signals and Electronic Systems (ICSES). IEEE, 2010:405-408.

[17] MUHAYA F B, USAMA M, KHAN M K. Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption[C]// International Conference on Emerging Intelligent Computing Technology and Applications. Springer-Verlag, 2009:6-23.

[18] YUAN K, HAN Z, LI Z. An Improved AES Algorithm Based on Chaos[C]// International Conference on Multimedia Information Networking and Security. IEEE, 2009:326-329.