一种使用分组密码和混沌序列对图像加密的方法

摘 要

加密具有高相关性的数据，例如图像，对于分组密码来说是一个挑战，因为原始图像的图案可能会在加密后保留，这是由于密码执行的确定性映射。为了克服这一限制，分组密码被用于大量的操作模式中，如密码分组链接、计数器模式。在本文所呈现的工作中，受Rijndael架构启发的随机分组密码利用混沌映射作为熵源。结果表明，与传统的Rijndael算法相比，该算法在更少的循环次数下达到了较好的安全性和鲁棒性指标。

**关键词：高级加密标准；分组密码；混沌映射；图像加密；安全性**

# 一、引言

美国国家标准与技术研究所(NIST)选择了块大小为128位的Rijndael算法，即高级加密标准(AES)，作为其目前推荐的对称密钥加密算法[1]。Rijndael算法支持128位、192位和256位的块和密钥大小，循环数可以是10、12或14，这取决于块和密钥的大小。此密码在每个循环中有四个单位:SubBytes, ShiftRows, MixColumns, AddRoundKey[2]。SubBytes单元提供了密文的置乱[3]并且由S-boxes实现。S-box执行从输入字节到输出字节的双射映射，该映射由伽罗瓦域GF(28)的操作定义。

Rijndael直接作为加密单元的应用相当于电子密码本(ECB)的操作模式。这种模式存在一些缺陷，因为加密是被确切地执行的[2]。这意味着当使用相同的密钥时，相同的明文块被加密成相同的密文块。ECB加密的密文会泄露明文中的重复模式信息。这种特性可以通过使用概率(或非确定性)操作模式来避免[4]，例如，密码块链接(CBC)、密码反馈(CFB)、输出反馈(OFB)、计数器模式(CTR)。这些不确定性的操作模式在明文攻击下是安全的，并允许高效、快速的软件实现[5]。在文献[6]中分析了一种基于CBC的图像加密方案。

近年来一些基于混沌的图像加密算法[7–14]被提出。混沌具有适于图像加密的非周期性、遍历性、对初始条件的敏感性等特性[15]，混沌映射被用来设计一些变换如置乱，置换。这些映射也被用来生成加密算法中使用的伪随机数。然而，通过利用算法的结构，一些基于混沌的图像加密方案已经被差分或已知/选择明文攻击所打破，见示例[5,16–18]。

这项工作的目的是提出基于随机版Rijndael S-box的对称密钥密码体系结构，以便使用ECB操作模式加密图像。这些是较不复杂的AES操作模式的替代方案。在这方面，本文有三个主要贡献：(i) 提出了一种利用混沌映射在S-box中添加熵源并与原始Rijndael算法兼容的方法；(ii) 表明该方案以更少的循环数达到了由一系列安全指标表示的AES操作模式的相同级别的安全性；(iii) 提出Rijndael扩散层的替代方案，在不损害安全性的情况下加快加密过程。

本文的其余部分分为四个部分。在第2节中，描述了AES算法和本工作中使用的混沌映射。图像加密中常用的一些安全指标在第3节中进行了改进。第四节介绍了由混沌映射生成的随机S-box，并分析了其安全性和时间复杂度。本节也提出了一种简化算法。本工作的结论详见第5节。

# 二、预备知识

我们考虑AES所采用的Rijndayl算法的结构，其块大小为128位。此外，我们考虑128位密钥，然后进行10次循环。加密过程首先将128位的信息块转换成一个4×4数组，由状态矩阵表示，其中每个元素是一个字节。同样，密钥也转换为4×4数组。下面简要描述图1的框图中所示的四个AES单元。

|  |
| --- |
|  |
| 图1 单轮AES算法的框图  **Fig. 1.** Block diagram of the AES algorithm per round. |

*(1) SubBytes:*此单元有16个相同、拥有输入字节与输出字节和并行运行的S-boxes，在图1中用表示。在每个S-box中，状态矩阵的一个字节被原始多项式生成的GF（28）中的运算所获得的一个字节替换。第个S-box，输入和输出字节关系为是一个矩阵，是GF（28）中的的乘法逆，是一个非0常向量。

*(2)ShiftRows:*这个单元周期性地将SubBytes单元输出的状态矩阵的第行向左移动个字节，

*(3)MixColumns:* 此过程使用线性变换组合状态矩阵的列。这是密码中主要的扩散元素。每列的四个字节乘以一个4×4矩阵，如下所示。

 (1)

所列4×4矩阵的条目采用十六进制表示法，例如，01代表GF(28)中系数为0000 0001的多项式。

*(4)AddRoundKey:* 将MixColumns单元后的状态矩阵添加到子秘钥矩阵中，形成用于下一轮的新状态矩阵。每轮中使用的子秘钥是通过对原始键（涉及4个S-boxes）进行操作获得的。

附录[2,4]中简要描述了非确定运行模式（CBC、OFB、CFB、CTR）。图2示出了使用这些操作模式对灰度图像进行10轮加密的结果。除了ECB模式（显示原始图像的模式）外，其他模式会生成类似随机加密的图像。

|  |
| --- |
|  |
| 图2 原始图像(a). 10轮的操作模式：ECB (b), CBC (c), OFB (d), CFB (e), CTR (f)  **Fig. 2.** Original image (a). Modes of operation with 10 rounds: ECB (b), CBC (c), OFB (d), CFB (e), CTR (f). |

## 2.1 混沌映射

一维混沌映射生成离散时间序列通过迭代合适的非线性不可逆函数，初始条件为，文献[15]中给出公式：

 (2)

因此，被称为在初值为的一条轨迹。由于瞬态行为，消除前200个样本。的值由128位的随机整数给出，可能由原始密钥生成。混沌映射的例子包括cubic映射[19] (CM) 和logistic映射[15](LM) ，是一个控制参数。通过将非线性变换应用于现有混沌映射（称为种子映射）的输出，开发了具有增强混沌复杂性的新一维混沌映射[20,21]，此映射的一个示例是增强逻辑映射（ELM）[20]，它使用正弦函数作为非线性变换，并定义为[20]：

 (3)

控制参数的范围在之间。将余弦函数应用于两个种子映射的组合，得到了具有复杂行为的混沌映射。例如，tent-logisitic-cosine(TLC)映射在式(4)中给出[21]，如方框1所示，控制参数在区间之间。

 (4)

方框 I

众所周知，混沌映射会产生不相关、类似噪声的非周期序列[15], 混沌系统的一个重要特性是对初始条件非常敏感，这意味着附近的轨迹以指数速度分离。在初始条件下，测量这种灵敏度的一个广泛使用的指标是李亚普诺夫指数。一个混沌系统需具有正Lyapunov指数[15]。

平衡二进制序列是从地图域的一个分区生成的，分为两个区域和，满足[22]，下文用混沌二进制序列表示。因此，如果，则，或者，则。替代离散化方法已经被提出，参见文献[20]。

# 三、安全性度量

本节介绍了文献中常用的安全指标，用于评估图像加密方案抵抗统计攻击的能力[12-14,23,24]。本文中，我们采用大小为512×512像素，灰度值为的单色图像。

*(1)香农熵：*随机性的度量由香农熵给出，定义为：

 (5)

是一个像素具有灰度值并且是灰度值的数值的可能性。例如，的最大值是8位。

*(2)局部香农熵：*式(5)中的香农熵是在整个图像上计算的。另一种措施称为-局部香农熵，考虑局部图像块的随机性[25]，定义为:

 (6)

其中是随机选择的具有个像素的图像的非重叠块的香农熵。用在文献[25]中的参数。在文献[25]中提供了一个基于显著性水平的假设检验统计标准，去决定此测试中是否核准了密码算法。如果在时位于区间，时，位于，时，位于，则此种情况将会发生。

*(3)NPCR和UACI：*图像加密算法在差分攻击方面的强度通常由像素变化率（NPCR）和统一平均变化强度（UACI）来评估。设和是维度的两个加密图像，它们的原始图像在随机位置上相差一个像素。用和分别表示和位置处的灰度值（范围从0到255）。在和之间NPCR和UACI被定义为：

 (7)

 (8)

如果，则，若，则。NPCR的最大分数是100，在这项工作中，对图像和进行了10000次测试，并将NPCR和UACI的平均值制成表格。基于文献[26]中提供的统计标准，如果NPCR的值大于临界值，则在本测试中批准密码算法（显著性等级为），对于大小为512×512像素的图像，三种不同值对应的阈值分别为，，。文献[26]中还提供了通过UACI测试的统计标准。在这种情况下，该指标必须在以下范围内：，指标位于；，位于；，位于。

一个好的密码必须对原始密钥中的更改具有很高的灵敏度。翻转该密钥中的一个位将导致加密图像大不相同。NPCR可用于验证此属性。在这种情况下，使用在随机位置相差一位的两个密钥对原始图像进行加密，生成两个加密图像和。本试验用k-NPCR表示。

*(4)NIST：*NIST测试套装（版本800-22）[27]用于测试序列是否适用于加密应用。这包括15项统计测试，重点关注序列中可能存在的不同类型的非随机性。测试用于确定接受或拒绝具有显著性级的理想随机性假设。在这项工作中，我们采用了，这是密码学中常用的值[27]。在仿真中，代表加密图像的二进制序列是NIST测试套件的输入。

*(5)相关性分析：*相关系数测量水平、垂直和对角线方向上两个相邻像素之间的相关性。我们在给定方向上随机选择对相邻像素，并计算为：



其中，







在高度相关的图像中，的值接近1，而加密图像的此参数的理想值为0。在本文中设。

## 3.1 安全性分析

我们使用了USC-SIPI图像数据库中的141幅原始图像(http://sipi.usc.edu/ database)。该数据库包含不同大小的彩色和灰度图像（例如256×256像素、512×512像素、1024×1024像素），我们调整了一些图像的大小，以便新数据库包含相同大小的512×512像素的图像。此外，一些彩色图像转换为256灰度级的灰度图像。总之，本工作中的所有模拟都使用了一个数据库，其中包含141幅大小为512×512像素的bmp格式灰度图像（每张图像大小为768.1 kB）。

表1显示数据库中所有图像的每个安全度量的最小值和最大值，每个AES操作模式有10轮。ECB模式的最小熵值不接近8位，即使在第十轮中，也观察到相邻像素之间的显著相关性。对于不确定的操作模式，这些指标的值显著提高，所有图像都通过NIST测试。此外，根据第3节所述标准，这些模式的NPCR、UACI、k-NPCR和局部熵的最小值通过了相应的统计测试。使用CTR模式可获得最佳结果。

### 四、混沌映射对AES的修正

非确定性操作模式使用初始化向量来打破ECB模式的确定性行为。在本节中，我们介绍了算法ARQ1，该算法通过混沌映射的迭代在AES S-box中引入熵源。在保持ECB操作模式的同时，将每个S-box的输出字节添加到混沌映射演化生成的随机字节中。该方案在每个S-box中使用固定数量的混沌比特，当混沌比特的数量增加时，可以观察到对密码分析的鲁棒性提高。在这项工作中，我们将这个位数设置为3。对于每个128位的明文块，如第2.1节所述生成的二进制混沌序列被分割成60位的块。前48位用于子字节单元的16个S-boxes，而剩余12位用于子密钥生成单元的4个S-boxes。

在每个S-box中使用三个混沌比特，多项式表示为。由于每个S-box中的运算在GF（28）中定义，因此乘以GF（25）中的原始多项式，得到多项式，已经在章节2给出。这个多项式的系数形成一个字节，称为**h。**选择是为了使**h**在0和1方面尽可能平衡。在这项工作中，多项式是通过穷举搜索选择的。字节**h**按位添加（模块2）到子字节单元中S-box的输出字节。

在第二轮中，在子字节单元的第一轮中使用的48个混沌比特按最后一个S-box中使用的三个比特的基10值循环右移。例如，如果最后一个S-box的多项式为，移位为7位。这一程序在每一轮中重复。这种移位的目的是随机化子字节单元的输出，同时保持每个明文块48个混沌比特不变。在用于获取子密钥的S-boxes中执行类似的程序。

对于使用CM混沌映射的每一轮，ARQ1算法的性能（数据库中所有图像的每个安全度量的最小值和最大值）如表2所示。将NPCR、UACI、k-NPCR和局部熵的最小值与第3节中定义的阈值进行比较，我们得出结论，ARQ1算法在第三轮后通过了相应的统计测试。这些结果表明，ARQ1算法对原始图像或原始密钥中的微小变化高度敏感。观察到，在第七轮之后，熵和相关系数的值达到表1中CTR操作模式所获得的相应值（这一轮在表2中以粗体突出显示）。这也适用于本工作中使用的其他混沌映射。这表明该算法对统计攻击具有很强的鲁棒性。此外，第一轮测试后，NIST测试服中的所有图像均获得批准。我们的结论是，包含混沌比特（在数据路径和子密钥生成中）的改进S-box达到了良好的随机性指标，并且对密码分析具有鲁棒性，只需更少的回合。图3示出了具有七轮的ARQ1算法的原始图像和加密图像在每个方向上的直方图和相关系数。目视检查显示加密图像的直方图均匀分布，ARQ1打破了原始图像相邻像素之间的高度相关性。

为了与现有的密码算法进行比较，我们考虑了来自512×512像素的UCS-SIPI“杂项”数据集的16幅灰度图像。表3和表4显示了ARQ1算法使用三个混沌映射（CM、的ELM、的TLC）对给定图像进行7轮运算后获得的NPCR和UACI值，以及文献[21,28]中报告的该数据集的结果。

据观察，ARQ1算法通过了所有图像和三个混沌映射的NPCR和UACI测试（临界值已在显著性水平等于0.05的情况下计算，即NPCR，UACI).对于某些图像，ARQ1的性能略优于此比较中考虑的密码。如表5所示，局部熵也有相同的趋势。