基于AONT的混沌图像加密算法研究

郭展榕　金　泽
中国人民警察大学　河北　廊坊　065000

摘　要：基于混沌的密码学是一个非常有前途的新兴领域，它提供了大量特别适用于信息加密、保密通信、扩频通信、智能卡加密、数字水印等的技术。混沌系统的许多基本特征如不确定性、不可重复性和不可预测性都与好的密码的属性——混乱和扩散相联系。目前大多数基于混沌的加密研究都没有集中在加密操作模式方面。本文使用了一种基于混沌的全有或全无变换（AONT）图像加密模式。这种加密操作模式能够保证在不解密所有密文块的前提下，无法还原任何一个明文块信息，一般在混沌加密算法后使用。结果表明，全有或全无变换加密模式在加密的整体效率上几乎没有开销，并且实现了安全增益。

关键词：混沌密码学；Logistic映射；Cat映射；AONT加密；图像加密

1 绪论

数字图像往往承载了许多秘密或者个人信息，如何安全且有效地传送这些图像是一个迫切需要解决的问题。在过去的二十年中，基于混沌的密码学一直在发展，为开发图像加密的创新方案带来了新的见解。Salleh等人[1]使用Logistic映射成功克服了安全图像加密的主要目标，消除了弱密钥。Pichler等人[2]使用了Baker变换的广义版本进行图像加密。Chen等人[3]将二维混沌Cat映射推广到三维，用于设计实时安全的对称加密方案，并证明了新方案的高效和高度安全性。根据应用程序的需求，可以使用不同的操作模式对映像进行加密。最常见的操作模式是电子码本（ECB）和密码分组链接（CBC）。CBC模式有一些缺点。首先，它是可分离加密模式，对手可以通过解密一个密文块来确定一个明文块。其次，如果攻击者知道加密算法、操作方式，并拥有密文，可以通过翻转比特方法获得大量泄露信息。Rivest[4]提出了一种强不可分离的无密钥模式，称为全有或全无变换（AONT），用于在加密前将长消息转换到固定长度的块中执行。不可分离模式意味着在不解密所有密文块的情况下，无法还原出任何一个明文块。AONT模式的思想是减慢攻击者的暴力搜索速度，降低的因素与加密消息中的密文块数量相等，同时保持相同的密码密钥长度。根据Canda等人[5]的说法，Rivest的AONT方案的安全性取决于明文消息的长度，因此几乎没有实现显著的安全性改进。他们提出了一个不可分离的方案，比Rivest的AONT方案快得多。与Rivest的方案不同，他们的方法是在消息加密后应用，即使是短消息也能提供安全增益。然而，上述大多数方案都忽略了加密操作模式方面。在本文中，我们提出了一种结合混沌加密和AONT操作模式的新方案，结果表明，全有或全无变换加密模式在加密的整体效率上几乎没有开销，并且实现了安全增益。

2 基于混沌的加密算法

2.1 一维Logistic映射

Logistic映射是基于混沌密码学中最常用的混沌系统之一。模型为$X_{n+1} = \mu X_n$（$1-X_n$），其中$\mu \in$（3.7,4）并且$X_n \in$（0,1）分别为系统参数和变量。当$\mu > 3.7$时，系统稳定的周期性轨道消失，进而导致混沌。该模型重复n次，次数等于图像中的像素数，产生一系列伪随机数，这些伪随机数按比例放大并四舍五入为0到255范围内的整数（对于8位图像）。然后，生成的伪随机值与图像像素值进行异或运算以生成加密图像。

2.2 二维Cat映射

猫映射（Cat映射），是一种在有限区域内进行反复折叠、拉伸变换的混沌映射方法，一般应用于多媒体混沌加密中。变换公式为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (N)$$

其中x_n，y_n表示变换前灰度图中像素的位置，x_{n+1}，y_{n+1}表示变换之后的像素位置，a,b为参数，n表示当前变换的次数，N为图像的长或宽（该算法只适用于长宽相等的图像），mod为模运算。反变换公式为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (N)$$

Cat映射具有良好的扩散特性，因此用于像素值的转置。换位后，加密图像的像素值去除了相关性。无论如何，它们都不能单独使用，因为换位后像素值的分布保持不变，极有可能被统计攻击破解。

3 加密模式

3.1 密码分组链接（CBC）模式

CBC模式的加密过程：（1）将明文按照固定长度分组。（2）初始化向量（IV）作为第一个分组的加密参数。（3）将当前明文分组与前一个密文分组进行异或运算。（4）对异或结果进行加密操作，得到当前分组的密文。（5）将当前分组的密文作为下一个分组的参数，重复第3步至第4步，直到所有明文分组都加密完成。

CBC模式的解密过程：CBC模式的解密过程与加密过程相似，只是在每一步的操作中，加密和解密的顺序互换。

3.2 全有全无变换（AONT）模式

这种模式具有一个有趣的性质，即在确定一个消息块之前必须解密整个密文，这种性质被称作不可分离的。这意味着针对全有或全无加密的蛮力搜索会减慢一个等于密文中块数的因子。假设$x = x_1, x_2, \cdots, x_s$是$s$个消息块，$y = y_1, y_2, \cdots, y_s$是$s$个密文块，AONT变换步骤如下：

（1）对于$1 \leqslant i \leqslant s\text{-}1$，$y_i = x_i + x_s$。

（2）$y_s = x_1 + \ldots + x_{s-1} + \lambda x_s$，其中$\lambda > 2$。

给定$y = y_1, y_2, \cdots, y_s$，还原消息块$x$的操作如下：

（1）对于$x_s = \gamma(x_1 + \cdots + x_{s-1} - y_s)$，其中$\gamma = (s - 1 - \lambda)^{-1}$，逆操作在有限域$F_{256}$中进行。

（2）对于$1 \leqslant i \leqslant s\text{-}1$，$x_i = y_i - x_s$。

4 算法设计

本章提出了一种基于混沌加密和AONT操作模式的新方案。

4.1 混沌加密算法

该方案由两个混沌密码组成：一维Logistic密码和二维Cat密码。首先，输入明文图片像素矩阵，然后使用一维Logistic映射基于CBC模式替换整个图片的像素值，最后对替换后的图片像素值使用二维Cat映射进行置换。密钥由Logistic映射的初始值和参数组成，用于生成实现混淆的伪随机数序列和Cat映射需要的参数。该方案如图1所示。

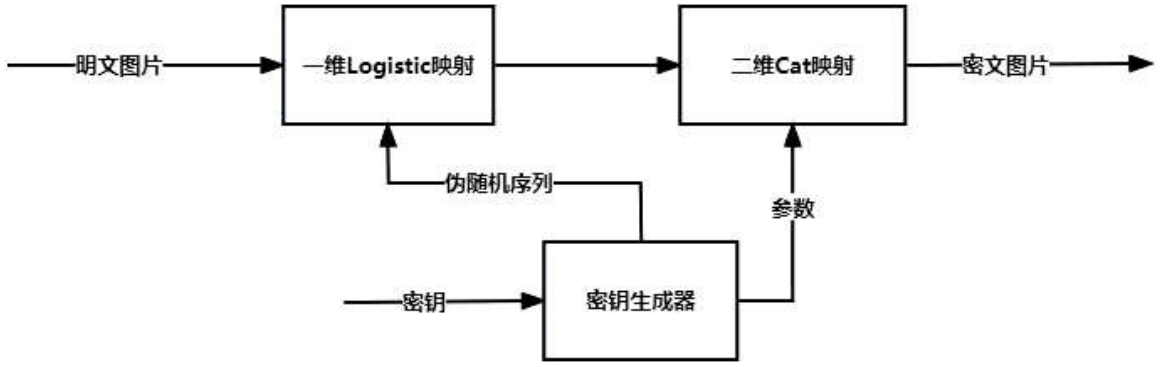

图1 混沌加密算法流程图

4.2 AONT模式

我们使用Canda等人提出了加密模式，即在混沌加密算法后再使用AONT，这样AONT的输入就是高度随机化的。在AONT后从密钥生成器中导出一个伪随机数来加密AONT最后一个输出块，这样就能保证在不知道全部AONT后的输出块的时候，无法还原出使用混沌加密算法后的任意一个块。

整个加密过程包括如下三个步骤：

（1）使用图4.1中的混沌加密算法对像素矩阵进行加密。

（2）将加密后的像素矩阵分成s个块，对这s个块进行AONT变换，产生s个输出块。

（3）从密钥生成器中导出一个伪随机数来加密最后一个输出块。

4.3 性能分析

使用图1所示的加密体系结构对不同大小的图像进行加密。一维Logistic映射用于生成一系列伪随机浮点数，这些浮点数的个数等于图像中的像素数。这些浮点数按比例放大并四舍五入为0-255范围内的整数（对于8位图像）。然后，将它们与图像的像素值进行异或运算。替换密码在CBC模式下运行。之后，使用二维Cat映射对替换图像进行转置。最后，将AONT应用于生成的输出块，并让最后一个输出块与随机数进行异或操作。

实现加密方法的集成开发环境是Matlab。测试是在具有3.10GHz和16GB RAM的Intel i5-11300H CPU上进行的。加密前，一维logistic映射初始参数X_n和μ分别设置为0.1和4。二维Cat映射参数a，b分别为3和5，变换次数为10。AONT模式中λ和γ分别为3和142，生成的随机数为150。

图2中展示了像素值为512*512加密前后的图片效

果，并在表1中展示了不同图片像素大小下加密算法中混沌加密和AONT所分别使用的时间。

图2 加密前后对比图

表1 加密时间（单位/秒）

	128*128	256*256	512*512
混沌加密	0.371	1.562	6.095
AONT	0.016	0.095	0.832
随机数加密	0.001	0.006	0.038
整个加密算法	0.388	1.663	6.965

从表1中可以看出，相比之下，AONT模式对整体运行时间的影响可以忽略不计。通过计算可知，像素值为512*512的原图熵值为6.8735，加密图的熵值为7.933，因此加密后的图像熵值更大。对于8位的灰度图来说，最大的信息熵值是8，7.933更接近于8，说明加密后图像的混乱程度大。

5 结论

混沌密码与传统密码相比具有保密性强，随机性好，密钥量大，更换密钥方便等优点，此外，在抗干扰性、截获率、信号隐蔽等方面同样具有潜在的优势。在本文中使用了一种将混沌加密与全有或全无变换操作模式相结合的新方案并对该方案进行了评估。结果表明，使用该方案加密图片效果良好，全有或全无变换操作模式在实现了安全增益的同时在加密的整体效率上几乎没有开销。

参考文献

[1]Salleh M, Ibrahim S, Isnin IF. Image Encryption Algorithm Based on Chaotic Mapping[J]. Teknologi, 2003(39): 1-12.

[2]Pichler F, Scharinger J. Finite dimensional generalized baker dynamical systems for cryptographic applications[C]. International Conference on Computer Aided Systems Theory, 1995(1030): 465-476.

[3]Chen G, Mao Y, Chui C K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons & Fractals, 2004(21): 749-761.

[4]R L Rivest. All-or-nothing encryption and the package transform[J]. Lecture Notes in Computer Science, 1997: 210–218.

[5]Canda V, Vanler, Trung T. A new mode of using all-or-nothing transforms[C]. IEEE International Symposium on Information Theory. 2006(33): 159–168.