一种自适应的图像加密算法的分析及改进

周 庆, 胡 月, 廖晓峰
(重庆大学计算机学院, 重庆 400044)

摘 要: 陈刚等人近来提出了一种新颖的自适应图像加密算法, 可有效地抵抗已知明文分析. 分析表明该算法易受选择明文攻击. 为提高其安全性和加密速度, 基于自适应排列提出了一种新的快速图像加密算法. 实验结果表明, 与现有的两个优秀的加密算法相比, 新的算法在安全性和加密速度方面均有更好的表现.

关键词: 密码学; 图像加密; 自适应; 密码分析
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2009) 12-2730-05

Analysis and Improvement of a Self-Adaptive Image Encryption Algorithm

ZHOU Qing, HU Yue, LIAO Xiao-Feng
(*College of Computer Science, Chongqing University, Chongqing* 400030, *China*)

Abstract: Recently, Chen etc. proposed a novel self-adaptive image encryption algorithm. The analysis shows that it is vulnerable to chosen plaintext attack. Then the original algorithm is revised based on self-adaptive image encryptoin technique. The experiments show that the revised algorithm has better performance on both security and speed than two known algorithms.

Key words: cryptography; image encryption; self-adaptive; cryptanalysis1

1 引言

随着网络带宽和计算机处理能力的高速增长, 数字图像在当今社会的各个领域被广泛使用. 由于网络的开放性, 涉及国家安全、商业利益和个人隐私的图像需要进行加密, 以保护其安全. 将传统的加密标准, 如 IDEA 和 AES 直接应用到图像的加密上存在一定的缺陷. 因为传统的加密算法主要为一维的数据流设计, 没有考虑二维图像的特性, 如空间有序性、视觉冗余性、相关性等等. 这使得传统加密算法在加密数据量较大的图像时要耗费较长的时间.

与一般的二进制数据不同, 数字图像具有明显的空间有序性, 因此可以通过改变这种有序性来设计快速的图像加密算法. 改变有序性最有效的方法是对图像像素进行排列(permutation)操作, 即改变各像素的位置, 但保持像素的值不变. 经排列后的图像其空间有序性和局部相关性受到破坏, 呈现一种类似噪声的形式, 表面上可达到保密要求. 排列操作的另一个优势是运算速度特别快, 因为它只涉及内存的读写操作. 但是仅采用排列的加密算法不能抵抗已知明文攻击.

在图像加密算法中, 研究最广泛的是基于混沌系统的加密算法. 混沌是非线性动力系统中出现的一种确定性的类随机过程, 具有遍历性、混合性、确定性以及对初始条件和控制系数的敏感性等特点, 这使得混沌系统很适合用于信息保密. 同时, 高维混沌映射可对图像进行排列, 如文献[1~3]分别采用了类标准映射、Henon 映射、混沌置乱等多种技术实现图像加密.

除了基于混沌系统的图像加密技术外, 还有其它一些基于像素排列的图像快速加密算法被提出, 如文献[4~6]分别提出了基于 T 矩阵、SCAN 语言和拟仿射变换的图像加密技术. 这些算法丰富了图像加密的手段.

从本质上讲, 基于混沌系统或像素排列的图像加密都采用同一框架, 即对图像进行多轮加密, 在每一轮中首先进行像素排列以破坏图像的空间有序性, 然后采用类 CBC 的模式来增强扩散效果. 近年来, 研究者们提出了一些新图像加密技术, 如基于神经网络的图像加密[7]、基于 Feistel 网络结构的图像加密[8]以及自适应图像加密技术[9].

2007 年, 张翌维等人提出了一种基于 Feistel 网络结构的图像加密框架[8]. 图像被分为左右两部分, 分别作为 Feistel 结构的左半部分和右半部分的输入; 经过多轮迭代后将左右两个部分再组合成密文输出. 在每一轮中

收稿日期: 2008-09-18; 修回日期: 2009-05-27
基金项目: 国家自然科学基金(No. 60573047, 60703035); 重庆市科委自然科学基金(No. 2009BA2024, 2009BB2208); 国家重点实验室项目(No. 2007DA10512709207)

采用混沌"猫映射"对像素进行排列, 用单向耦合映射格子产生轮密钥.

陈刚等人则提出了一种新颖的图像加密技术, 与传统的图像加密技术不同, 它只采用排列操作即可有效地抵抗已知明文攻击[9]. 该算法根据图像自身的信息对像素进行排列, 故称为自适应图像加密算法(self-adaptive image encryption algorithm). 由于排列操作便于计算机高效实现, 在单轮加密中, 自适应图像加密比其它加密技术更快.

密码分析是密码学的另一个研究重点, 常见的密码分析方法包括唯密文分析、已知明文分析和选择明文分析等. 选择明文分析是指攻击者选择一定数量的明文, 并得到这些明文加密后的密文, 最后根据这些明文-密文对推导出密钥的分析方法[10]. 选择明文分析是一种非常有效的密码分析方法, 例如差分分析和线性分析就属于典型的选择明文分析方法. 通常, 当一个攻击方法的复杂性低于穷举攻击时, 该攻击方法是有效的, 同时也说明加密算法不安全[11].

在本文中, 我们首先对文献[9]提出的自适应加密算法进行安全性分析, 通过选择明文分析成功地恢复了原算法的密钥, 表明原算法是不安全的. 为了提高其安全性和加密速度, 我们基于自适应排列技术设计了一种新的图像加密算法. 实验结果表明, 新的算法在安全性能上与文献[8]相当, 部分安全性能优于文献[8], 在加密速度上则明显快于文献[8]和文献[9].

2　自适应图像加密算法及其分析

2.1　自适应图像加密算法描述

采用传统的排列变换对图像进行加密, 无论使用何种变换方式或加密的轮数为多少, 都容易受到已知明文攻击. 攻击者通过对比明文和密文可获得关于排列的部分信息. 而一般只需要几对明文和密文图像就能恢复出绝大部分排列信息. 排列变换的这一安全缺陷源于其排列操作仅与密钥相关, 而与明文无关. 为了改进这一缺陷, 文献[9]创新性地提出了一种自适应的图像加密算法, 根据明文控制排列变换, 从而抵抗已知明文攻击. 该算法过程如图 1 所示(其中 *key* 为 128 比特的密钥):

step1:　　$i=1$.
step2:　　if $key[i]=0$
使用下半部分像素对上半部分像素进行排列;
使用上半部分像素对下半部分像素进行排列.
　　if $key[i]=1$
使用右半部分像素对左半部分像素进行排列;
使用左半部分像素对右半部分像素进行排列.
step3:　　if $i<128$　　$i=i+1$; 转到 step2:
　　else 程序结果.

图 1　自适应图像加密的算法描述

在图 1 中, 算法的关键步骤是使用图像的一半像素对另一半像素进行排列, 其详细过程如下:

(1) 对图像的一半像素按从小到大进行排列, 得到由每个像素的排序序号组成的矩阵;

(2) 将图像的另一半像素按此序号矩阵进行排列.

2.2　安全性分析

安全性是加密算法最重要的指标. 在本节中, 我们指出文献[9]的几个安全缺陷并给出相应的攻击方法.

2.2.1　安全缺陷一

观察一: 原加密算法不改变图像像素的统计信息. 由于排列只改变像素的位置, 不改变像素的值, 因此无论排列多么复杂, 图像像素的统计信息保持不变. 特别地, 加密前后图像的直方图是相同的. 由于直方图表示了明文像素的概率分布, 而原算法未能掩盖此信息, 故存在安全上的缺陷.

2.2.2　安全缺陷二

观察二: 设明文图像 $\boldsymbol{I}$ 为 $2L\times 2L$ 的零矩阵($L>11$), 除 $\boldsymbol{I}(L+1,1)$ 和 $\boldsymbol{I}(2L,2L)$ 的值为 1 外, 其它像素值均等于 0(见图 2). 对该图像进行自适应加密, 若当前密钥位为 0(即图像分为上下两部分进行排列), 图像保持不变; 若当前密钥位为 1(即图像分为左右两部分进行排列), 图像在"第四象限"值为 1 的像素将与其左边的 0 像素的进行换位(若 1 像素在 $L+1$ 列, 则与上一行最后一列的像素进行换位), 其它所有像素保持不变.

	第 1 列	…	第 $L+1$ 列	…	第 $2L$ 列
第 1 行	0	0	0	0	0
…	0	…	0	…	0
第 $L+1$ 行	1	0	0	0	0
…	0	…	0	…	0
第 $2L$ 行	0	0	0	0	1

图 2　用于获取密钥信息所选择的明文

根据这一现象, 可对加密算法进行选择明文分析. 选择的明文为图 2 所示的矩阵, 再根据密文图像"第四象限"中 1 像素的位置可判断出密钥中比特 1 的个数. 例如, 根据以上原则选择的 26* 26 的明文图像, 若密文图像第 22 行第 18 列的像素为 1, 则说明 1 像素移动了 58 次, 故密钥中含有 58 个比特 1.

该选择明文攻击可降低对加密算法的攻击复杂度. 例如, 在已知密钥中比特 1 的个数为 58 时, 可能的密钥个数等于组合数$\binom{58}{128}$, 约为 2^{123}, 比穷举全部 2^{128} 个密钥的时间减少了 32 倍. 由于该选择明文攻击是比穷举攻击更有效的攻击方法, 故文献[9]的算法存在较严重的安全缺陷.

2.2.3　安全缺陷三

前一小节采用的攻击方法只使用了一对明文和密文, 当选择更多的明文和密文对, 则可完全恢复出加密密钥.

观察三: 设明文图像 $\boldsymbol{I}$ 为 $2L\times 2L$ 的像素矩阵, 除 $\boldsymbol{I}(2L,L)$ 的值等于 0, $\boldsymbol{I}(L+1,1)$ 的值等于 2 外, 其它像

素值均等于 1(见图 3). 使用长度为 L 比特的密钥对该图像进行自适应排列, 无论密钥的前 $L-1$ 比特的值是什么, 前 $L-1$ 次的排列结果都是相同的, 但第 L 次排列的结果将根据第 L 比特的值有所不同. 若第 L 比特为 0, 则 $I(2,1)=2$, 若第 L 比特为 1, 则 $I(2,1)=1$.

	第 1 列	…	第 L 列	第 $L+1$ 列	…	第 $2L$ 列
第 1 行	1	1	1	2	1	1
…	1	…	1	1	…	1
第 $2L$ 行	1	1	0	1	1	1

图 3 用于恢复密钥所选择的明文

根据以上观察, 采用选择明文分析可完全恢复出密钥, 共需 128 对明文- 密钥对, 算法如图 4 所示.

```
Step1:   L= 128
Step2:   设置明文为图 3 所示的 2L × 2L 的像素矩阵 I 获取 I 对应的密文 C
         If L= 128
             D= C;
         Else
             用 key(L+ 1: 128) 对 C 解密得到 D( D 等于 I 经 key( 1: L) 加密的结果
         End if
         If D(2, 1)= 2
             key(L)= 0
         Else
             key(L)= 1
         End if
Step 3:  L= L- 1
         IF L> 0
             Goto Step2
         Else
             输出 key
         End if
```

图 4 可恢复密钥的选择明文攻击算法

根据图 4 中的算法, 仅采用 128 个选择明文- 密文对即可完全恢复出算法的密钥.

2.3 加密速度

加密速度是加密算法除安全性以外最重要的性能指标. 文献[9]算法的每一轮加密只包含排列和排序两种操作. 其中排列的时间复杂度为 $o(n)$ (n 为图像的像素个数), 且每个像素的排列只涉及一次内存读和写操作, 因此运算速度极快. 排序是一个稍微复杂的操作, 一般情况下其最低时间复杂度为 $o(n\log n)$, 对于普通大小的图像, 其运算速度很快. 由于图像的像素值均为一定范围内的整数(典型地, 为 0 到 255 之间的整数), 对较大的图像可采用“桶”排序方法, 从而将时间复杂度降为 $o(n)$. 由此可见, 该算法在一轮加密中运算速度很快.

然而, 基于安全性的考虑, 密钥的长度至少应为 128 比特, 也就是说加密的轮数至少为 128 轮, 这使得加密完所有轮数要耗费较长的时间.

3 改进的自适应图像加密算法

上一节, 我们分析了文献[9]的安全性和加密速度. 在安全性方面, 该算法有两个缺点, 一是加密不改变像素的分布, 二是对于某些明文, 密文不受密钥的影响. 在速度方面, 完成 128 轮图像加密的速度较慢. 尽管有以上的缺点, 但原算法所具有的操作简单、敏感性高和单轮加密速度快的优点却值得保留. 在这一节中, 我们以文献[9]的算法为核心部件, 提出了一种新的快速图像加密算法.

3.1 算法概述

为了保留原算法中单轮加密简单高效的优点, 在一轮的加密过程中, 仅包含轮密钥异或、S 盒替代以及自适应排列三种操作. 图 5 显示了一轮加密的流程图.

轮密钥异或是指将 4* 4 的轮密钥矩阵重复平铺成与原图像相同大小的矩阵, 然后将对应的像素进行按位异或运算. 其中轮密钥的产生过程在 3.2 节中说明.

S 盒替代是算法中唯一的非线性运算. 为了有效地抵抗差分分析和线性分析, 应精心选择安全的 S 盒. 在本算法中, 我们采用 AES 加密标准中的 S 盒[12].

每轮的最后一步使用自适应的排列操作. 与文献[9]不同的是, 新算法中的自适应排列并不由密钥控制, 而是使用固定的方式: 奇数轮采用上下排列模式, 偶数轮采用左右排列模式.

注意以上三种操作均是可逆的, 因此算法能够正确解密.

3.2 轮密钥产生算法

加密的每一轮需要不同的轮密钥, 即大小为 4* 4 的字节矩阵, 共 128 比特. 加密和解密均为 8 轮, 因此共需产生 8 个轮密钥. 图 6 显示了轮密钥产生的详细过程, 其初始输入为 128 比特的外部密钥.

观察图 6 可以发现, 轮密钥产生过程与加密过程非

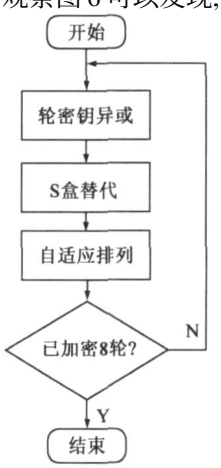

图5 图像的加密过程

图6 轮密钥产生过程

常相似, 包括异或、S 盒替代和自适应排列三种操作. 唯一不同的是加密过程中参与异或运算的是轮密钥, 而在轮密钥产生过程中参与异或运算的是 4* 4 的固定矩阵. 这种相似性使得算法在硬件实现时可减少需要的逻辑门数, 从而降低成本.

3.3 性能分析

为了实现简单高效的要求, 新的加密算法采用多轮加密, 加密轮数为 8 轮, 每轮仅包含了异或、替换和排列等快速操作, 保证了整个算法非常高的加密速度.

加密的基本操作经过仔细的选择. 异或操作引入轮密钥对密文的影响, S 盒替换实现对单个像素的混乱和扩散效果, 而自适应排列则将单个像素或密钥的单个字节的改变扩散到整幅图像中. 因此, 即使密钥出现 1 比特的变化, 密文也会显著变化, 不会出现原算法中不同密钥加密产生相同密文的情况. 此外, 增加的异或操作及 S 盒替换有效地改变了密文像素值的分布, 去除了文献[9] 加密前后直方图相同的缺点. S 盒的选择还提高了算法抵抗差分分析与线性分析等选择明文分析的能力.

与文献[9] 相同, 算法采用 128 位的外部密钥, 这保证新的算法可以抵抗穷举攻击.

4 实验结果与对比分析

本节主要考查改进的图像加密算法的各种安全特性, 同时我们还将该算法的性能与两个同类算法作了对比. 在实验中, 明文为 128* 128 的"Lena"图像, 密钥为 4* 4 的零矩阵.

4.1 直方图

图 7 列出了"Lena"图像加密后的直方图, 以及加密前后的直方图对比. 从图中可以看出加密后的直方图比较均匀, 掩盖了明文图像各像素的分布.

4.2 明文敏感性检测

雪崩效应是衡量加密算法的重要指标之一[10]. 所谓雪崩效应是指当明文或密钥改变一位时, 密文应有接近一半的比特发生改变. 这一特性也称为密文对明文或密钥的敏感性. 我们将"Lena"图像最后一个像素的最后一比特由 1 置为 0, 并对比加密后密文的变化. 表 1 列出了各轮加密后密文位的改变率. 从表 1 可以看出, 经过两轮加密后, 密文位的变化稳定在 0.5 左右, 即出现雪崩效应.

表 1　明文改变一位后密文位的改变率

轮数	1	2	3	8	9
改变率	0.330	0.501	0.502	0.498	0.502

4.3 密钥敏感性检测

密钥敏感性检测当密钥改变一位时, 密文的变化率. 我们将密钥的最后一个比特由 0 置为 1, 并对比加密后密文的变化. 表 2 列出了各轮加密后密文位的改变率. 从表 2 可以看出, 同样经过两轮加密后, 密文位的变化稳定在 0.5 左右.

表 2　密钥改变一位后密文位的改变率

轮数	1	2	3	8	9
改变率	0.483	0.501	0.502	0.500	0.501

4.4 密文的相关性检测

在连续色调图像中, 相邻象素的相关性通常很高, 好的图像加密算法应去除这种相关性. 我们从明文和密文图像的水平、竖直和对角三个方向随机地选取 1000 对像素, 并计算了对应的相关系数. 表 3 对比了加密前后三个方向上的相关系数. 表 3 说明加密后, 相邻密文像素之间的相关性接近于 0.

表 3　明文和密文图像中相邻象素的相关系数

	明文	密文
水平	0.9186	-0.0124
竖直	0.8345	0.0203
对角	0.8029	-0.0143

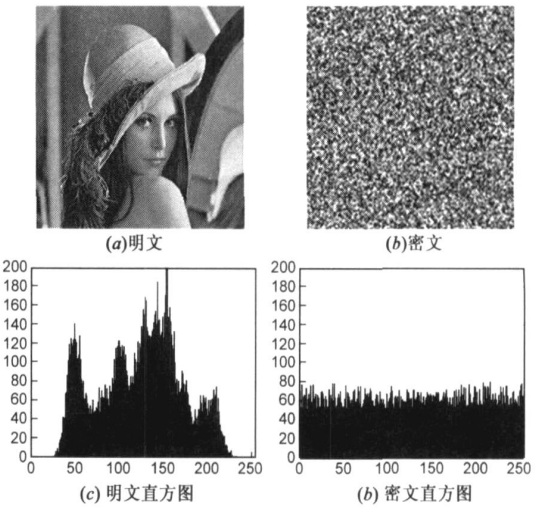

图7

4.5 与同类算法的对比

本小节将本文提出的算法与文献[9] 和文献[8] 提出的图像加密算法进行对比. 文献[8] 提出的图像加密算法采用了 Feistel 网络结构, 排列操作采用广义猫映射, 子密钥生成则采用单向耦合映射格子. 更详细的实验结果请参见文献[8] .

在安全性方面, 本文提出的算法与文献[8] 大致相当. 特别在明文和密钥的敏感性方面, 本文提出的算法性能更优, 只需两轮即可达到完全雪崩效应, 而文献[8] 中的算法则需要 7 轮. 与文献[9] 相比, 改进算法去除了原算法中的两个弱点.

在加密速度方面, 本文提出的算法明显优于文献[8] 和文献[9] 的算法. 表 4 列出了三种加密算法加密相似大小图像所需的时间(采用 Matlab 代码编写, 均运行

在同一平台: 1. 5GHz Celeron CPU, 512M 内存). 这主要是因为文献[8]中采用了大量的乘法: 平均每轮每个像素需要进行 7 次乘法, 其中猫映射 4 次, 灰度扩散 1 次, 单向耦合映射格子 2 次. 由于乘法运算通常比替换和异或操作慢几十倍, 从而使文献[8]中的加密速度较慢. 文献[9]中的算法则由于加密轮数太多而耗费了大量的计算时间.

表 4 三种加密算法的加密时间

加密算法	文献[8]	文献[9]	本文
图像大小	90* 180	128* 128	128* 128
加密时间(秒)	2.13	1.24	0.15

5 结束语

陈刚等人最近提出了一种自适应的图像加密算法, 该算法具有加密操作简单、单轮加密速度快, 并可有效地抵抗已知明文攻击, 代表一类新的图像加密技术. 然而经本文研究发现, 单纯使用自适应加密具有严重的安全缺陷, 无法抵抗选择明文分析: 选用一个明文-密文对即可找到比穷举攻击更好的破解方法; 选用 128 个明文-密文对则可完全恢复出密钥; 对加密速度的分析也说明原算法的性能需进一步提高. 本文将自适应排列这一新的图像加密技术与传统的分组加密操作相结合, 提出的改进算法具有安全、简单和高效的特点, 适于计算机软件及各类数字硬件实现. 实验结果表明, 该算法在安全性上与文献[8]相当, 部分安全性能优于文献[8], 在加密速度上则明显快于文献[8]和文献[9].

参考文献:

[1] 李昌刚, 韩正之, 张浩然. 一种基于随机密钥及"类标准映射"的图像加密算法[J]. 计算机学报, 2003, 26(4): 465-470.
Li Changgang, Han Zhengzhi, Zhang Haoran. An image encryption algorithm based on random key and quasi-standard map[J]. Chinese Journal of Computers, 2003, 26(4): 465-470. (in Chinese)

[2] 张瀚, 王秀峰, 等. 一种基于混沌系统及 Henon 映射的快速图像加密算法[J]. 计算机研究与发展, 2005, 42(12): 2137-2142.
Zhang Han, Wang Xiufeng, et al. A fast image encryption algorithm based on chaos system and Henon map[J]. Journal of computer research and development, 2005, 42(12): 2137-2142. (in Chinese)

[3] 蒋建国, 李援, 梁立伟. H.264 视频加密算法的研究及改进[J]. 电子学报, 2007, 35(9): 1724-1727.
Jiang Jianguo, Li Yuan, Liang Liwe, Research and improvement of the video encryption algorithm for H.264[J]. Acta Electronic Sinica, 2007, 35(9): 1724-1727. (in Chinese)

[4] Zhang M R, Shao G C, Yi K C. T-matrix and its applications in image processing[J]. Electronics Letters, 2004, 40(25): 1583-1584.

[5] Maniccam S, Bourbakis N. Image and video encryption using SCAN patterns[J]. Pattern Recognition, 2004, 37(4): 725-737.

[6] 朱桂斌, 曹长修, 等. 基于仿射变换的数字图像置乱加密算法[J]. 计算机辅助设计与图形学学报, 2003, 15(6): 711-713.
Zhu Guibin, Cao Changxiu, et al. An image scrambling and encryption algorithm based on affine transformation[J]. Journal of Computer Aided Design & Computer, 2003, 15(6): 711-713. (in Chinese)

[7] 丁群, 陆哲明, 孙晓军. 基于神经网络密码的图像加密[J]. 电子学报, 2004, 32(4): 677-679.
Ding Qun, Lu Zheming, Sun Xiaojun. The image encryption based on neural network cipher[J]. Acta Electronic Sinica, 2004, 32(4): 677-679. (in Chinese)

[8] 张翌维, 王育民, 沈绪榜. 基于混沌映射的一种交替结构图像加密算法[J]. 中国科学 E 辑: 信息科学, 2007, 37(2): 183-190.
Zhang Liwei, Wang Yuming, Shen Xubang. Image encryption algorithm based on chaotic maps and Feistel networks[J]. Science in China (Series E: Information Sciences), 2007, 37(2): 183-190. (in Chinese)

[9] Chen Gang, Zhao Xiaoyu, Li Junli. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, 16(11): 1975-1982.

[10] Schneier B. Applied Cryptography[M]. Hoboken, New Jersey: John Wiley & Sons, 1996.

[11] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Lecture Notes on Computer Science, 1991, 537(1): 1-20.

[12] FIPS-197, Announcing the Advanced Encryption Standard [S].

作者简介:

周 庆 男, 1979 年出生, 重庆人, 博士, 副教授, 主要研究领域为多媒体信息安全技术. E-mail: tzhou@cqu.edu.cn.

胡 月 女, 1979 年出生, 重庆人, 博士, 主要研究领域为密码学技术. E-mail: huyue@cqu.edu.cn.

廖晓峰 男, 1964 年出生, 四川通江人, 博士, 教授, 主要研究领域为信息安全与计算智能技术. E-mail: xfliao@cqu.edu.cn.