DOI: 10.16218/j.issn.1001-5051.2020.01.007

一种抗差分攻击的图像加密算法*

吕 翔[1], 王晓洁[1], 杨刘洋[2], 楼梦佳[3], 陈明峰[1], 邓雨亭[1], 付 娜[1]
(1.浙江师范大学 物理与电子信息工程学院,浙江 金华 321004; 2.重庆市潼南中学,重庆 402660; 3.浙江师范大学 经济与管理学院,浙江 金华 321004)

摘 要: 为构造一种基于混沌序列、置换矩阵和拉丁方的图像加密算法,首先将加密图像矩阵与基于 Logistic 模型的混沌序列构成的矩阵进行像素值异或,完成图像的预处理;然后使其嵌入一个更大的随机矩阵并标记;最后运用置换矩阵和完备拉丁方进行若干次图像像素位置的置乱.仿真结果及参数计算表明:该算法加/解密效果理想,密钥大小适中,密钥空间巨大,加密时间短,并且能够抵抗多种攻击.

关键词: 图像加密; 拉丁方; 混沌序列; 矩阵变换; 差分攻击
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 1001-5051(2020)01-0039-07

An image encryption algorithm against differential attack

LYU Xiang[1], WANG Xiaojie[1], YANG Liuyang[2], LOU Mengjia[3],
CHEN Mingfeng[1], DENG Yuting[1], FU Na[1]
(1. *College of Physics and Electronic Information Engineering, Zhejiang Normal University, Jinhua* 321004, *China*; 2. *Tongnan Senior School, Chongqing* 402660, *China*; 3. *College of Economics and Management, Zhejiang Normal University, Jinhua* 321004, *China*)

Abstract: An image encryption algorithm based on chaotic sequences, permutation matrices and Latin squares was constructed. Firstly, an XOR operation was performed between a grey-scale map and a matrix composed of a chaotic sequence based on the Logistic model in order to complete image preprocessing. Secondly, it was embedded in a larger random matrix and marked. Thirdly, the positions of image pixels were scrambled by permutation matrices and a complete Latin square. It was showed by simulation and parameter calculations that the encryption was effective, the key size was moderate, the key space was large, the encryption time was short and had ideal performance to resist various attacks.

Key words: image encryption; Latin square; chaotic sequence; matrix transformation; differential attack

0 引 言

随着计算机网络的快速发展,数字图像可以高速传送到世界的任意角落.然而,恶意的未经授权的用户也可以利用这种便利来窃取所传播图像的信息,从而对图像的持有者造成伤害.因此,数字图像安全问题已经成为计算机领域广泛关注的一个重要主题.由于图像的一些固有特征,例如数据冗余属性和相邻像素之间的强相关性,使得图像加密与文本加密稍有不同.因此,数据加密算法(data encryption standard,DES)[1]、高级加密标准

* 收文日期: 2018-09-04; 修订日期: 2019-03-01
基金项目: 浙江省科技厅创新团队项目(2010R5007)
作者简介: 吕 翔(1979—),男,浙江金华人,副教授,博士.研究方向:通信系统;通信编码理论;组合数学.

(advanced encryption standard,AES)[2]等传统加密方案已不完全适合新时代图像的加密.

为了克服这个缺点,近年来已有许多学者相继提出了专门为数字图像设计的加密系统[1-24],如:基于光学手段的图像加密算法[3-8];基于全息技术的图像加密算法,这种算法属于硬件加密,对物理环境、光学器件要求较高;基于计算机软件的加密方法,如 Arnold 变换和幻方像素变换等[9-14],可有效克服硬件加密代价昂贵的缺点,但这类算法不具备抗差分攻击的能力.虽然,基于混沌或者超混沌系统的图像加密方案[15-21,25-28]安全性较高,可以抵抗统计和差分攻击,但是算法比较复杂、耗时长,且由于此方案具有雪崩效应这种固有特性,密图有微小改变,解密后的图像与原图相比都有很大的改变,使得此类方案对椒盐噪声、剪切攻击等的影响过于敏感[25,29].

为解决以上问题,本文构造了既可抗差分攻击又可抗椒盐噪声等攻击的图像加密算法.算法的基本思路是在加密图像中嵌入了一定的冗余信息,利用冗余信息的随机性及嵌入位置的随机性来达到抗差分攻击的目的.仿真结果及参数计算表明,该算法加/解密的效果理想,在原图为256×256时,密钥大小适中,占比为 1.1%,密钥空间巨大,可达 $10^{1\,248}$,加密时间短,约为 0.788 0 s.并且本文所提算法能够在抵抗差分攻击的同时抵抗椒盐噪声攻击等其他类型攻击.与文献[22]相比,本文算法预处理效果更佳,加密速度快,冗余信息小.与文献[25-27]相比,本算法加密速度更快,在抗差分攻击的同时能够抵抗更多类型的攻击.

1 抗差分攻击的图像加密算法

1.1 算法相关知识

定义 1[21] Logistic 映射是一类简单却被广泛应用的动力系统,其映射为

$$x_{k+1}=\mu x_k(1-x_k). \tag{1}$$

式(1)中:$0\leqslant\mu\leqslant4$ 是分支参数;$x_k\in(0,1)$.当 $3.569\,9\cdots\leqslant\mu\leqslant4$ 时,Logistic 映射处于混沌状态.

定义 2[23] 设一个集合由 n 个元素构成,记该集合为 P,用 P 的元素构造拉丁方 A,如果 A 中的各元素与其相邻元素组成的元素对互异,则称拉丁方 A 为 n 阶完备拉丁方(complete Latin square,CLS).

定义 3[23] 置换矩阵是一个方形二进制矩阵,它在每行和每列中只有一个 1,在其他位置则为 0.

引理 1[23] 在完备拉丁方中任意交换 2 个元素的位置,总共可以产生 $n(n-1)/2$ 个不同的完备拉丁方.

引理 2[23] 完备拉丁方的构造方法同文献[22].

引理 3[23] 由完备拉丁方可生成行扩展数对矩阵,构造方法同文献[22].

引理 4[23] n 阶置换矩阵共有 $n!$ 种不同的排列方式.

1.2 本研究所提图像加密算法的具体过程

本文研究的图像置乱加密算法是像素灰度值置乱和像素位置置乱相结合的方法.具体加密的步骤如图 1 所示.

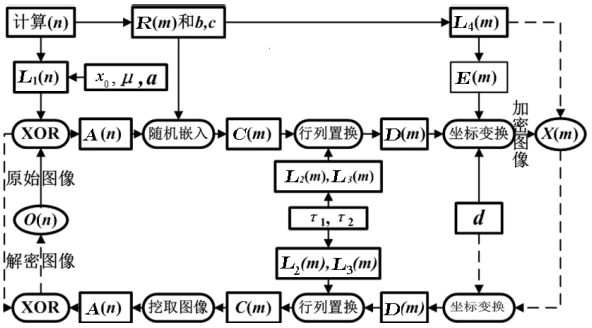


图 1 一种抗差分攻击的加密算法流程图及其逆过程

第 1 步:由定义 1 生成一个混沌序列,舍弃前 a 个数,然后逐行填充生成一个与待加密图像 $O(n)$ 相同大小的 $n\times n$ 混沌矩阵 $\boldsymbol{L}_1(n)$,序列初值为 x_0,参数为 μ.

第 2 步:将 $\boldsymbol{O}(n)$ 与 $\boldsymbol{L}_1(n)$ 进行一次像素值异或操作得到矩阵 $\boldsymbol{A}(n)$.

第 3 步:生成随机矩阵 $\boldsymbol{R}(m)$,大小为 $m\times m$,同时生成一个随机坐标(b,c) $(0\leqslant b,c\leqslant m-n-1)$.

第 4 步:在矩阵 $\boldsymbol{A}(n)$ 的周围加上全 0 的标记,得到矩阵 $\boldsymbol{B}(n+1)$.

第 5 步:根据 b 和 c 规定的坐标,用矩阵 $\boldsymbol{B}(n+1)$ 替换 $\boldsymbol{R}(m)$ 中相应的像素,得到冗余图像 $C(m)$,这样完成随机嵌入过程.

第 6 步:生成一个与矩阵 $\boldsymbol{C}(m)$ 相同大小的置换矩阵 $\boldsymbol{L}_2(m)$,$\boldsymbol{L}_3(m)$,分别用置换矩阵所对应的置换 τ_1,τ_2 作为密钥.

第 7 步:用 $\boldsymbol{L}_2(m)$ 左乘 $\boldsymbol{C}(m)$,用 $\boldsymbol{L}_3(m)$ 右乘

$C(m)$,进行相应的行列置换,得到初步位置置换矩阵 $D(m)$.

第 8 步: 生成一个与矩阵 $D(m)$ 相同大小的完备拉丁方 $L_4(m)$.

第 9 步: 按照引理 3,将完备拉丁方 $L_4(m)$ 构造成行扩展数对矩阵 $E(m)$,对矩阵 $D(m)$ 进行以 $E(m)$ 为原则的若干次位置置乱变换,置乱方式参见文献[22],得到加密后的图像 $X(m)$.

在加/解密过程中,明文为待加密图像 $O(n)$,密文为 $X(m)$,密钥为混沌序列初值 x_0、参数 μ,舍弃参数 a,置换矩阵所对应的置换 τ_1,τ_2,完备拉丁方位置置乱次数 d. 密钥可以表示为六元组(x_0,μ,a,τ_1,τ_2,d). 解密操作是其逆过程,具体见图 1.

2　算法仿真与参数计算

本算法仿真实验环境为 MATLAB 6.5,处理器型号为 Intel(R) Core(TM) i5-7300HQ CPU@ 2.50 GHz 2.50 GHz. 在此环境下对一幅 256×256 的原始灰度图 $O(256)$ 进行相应的仿真.

2.1　预处理阶段统计特性分析

以 256 阶 Lena 灰度图(见图 2(a))作为待加密图,进行算法仿真. 首先进行预处理,将原图像与混沌矩阵 $L_1(256)$ 进行像素值异或操作得到预处理图 $A(256)$(见图 3(a)). Lena 灰度图预处理前/后的效果图和像素分布直方图如图 2 和图 3 所示.

文献[22]中的预处理方法是将图像与拉丁方进行像素值异或,得到的预处理图及其直方图见图 4. 将原图像与随机矩阵进行像素值异或操作得预处理前/后的效果图和像素分布直方图,如图 5 所示.

由图 2、图 3 比较可得,预处理加密后的图像 $A(256)$ 比原始图像 $O(256)$ 信息隐藏得更好. 观察二者的直方图可知,后者的像素值分布更均匀.

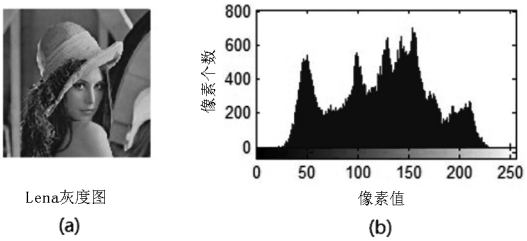


图 2　原始 Lena 图及其直方图

从图 3(a) 与图 4(a) 的对比可以看出,本文用混沌矩阵预处理效果比文献[22]中用拉丁方预处理的效果更好. 从图 3(a) 与图 5(a) 的对比可以看出,本文预处理效果与用随机矩阵处理效果相当,但密钥只与初始值 x_0、参数 μ 及舍弃参数 a 有关,与随机矩阵相比显得非常小.

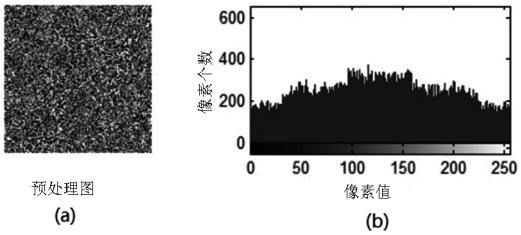


图 3　混沌矩阵预处理图及其直方图

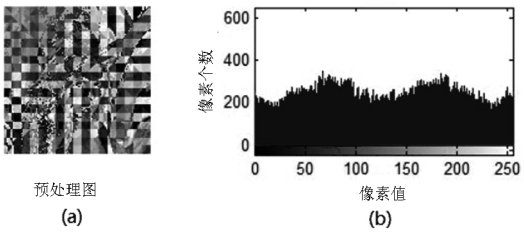


图 4　拉丁方预处理图及其直方图

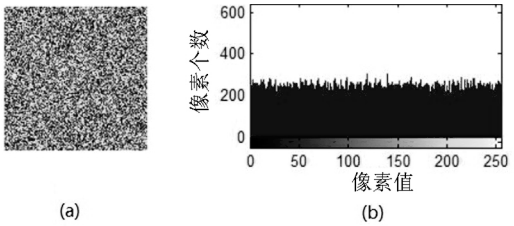


图 5　随机矩阵预处理图及其直方图

2.2　后期加密过程及效果的展示

先对预处理后的 $A(256)$ 添加全零标记,得到标记图像 $B(257)$,再用 MATLAB 中 randint() 函数生成一系列随机整数,将其填充为随机噪声图像 $R(304)$,将标记图 $B(257)$ 上文第 5 步过程规则进行嵌入,得到冗余图 $C(304)$,见图 6(c). 然后对此图进行一次行列置换,最后用完备拉丁方生成的扩展矩阵 $E(304)$ 进行若干次图像像素位置置乱,如图 7 所示.

(a) 为 256 阶混沌矩阵预处理图; (b) 为预处理图镶进随机图; (c) 为加标记后的图像

图 6　密图的嵌入及其效果图

(a)为 304 阶置换矩阵;(b)为行列置换后的图像;
(c)为 4 次拉丁方置乱后的最终加密图像

图 7 行列置换及拉丁方置乱后的效果图

本文引入置换矩阵,使得只需几次拉丁方位置置乱便达到理想的置乱效果.图 8(a)~8(d)分别为 2 次、4 次、6 次和 10 次拉丁方置乱变换的效果图,经过相关参数计算,4 次拉丁方置乱变换后的图像加密效果已经较佳.考虑加密时间因素,本文选 4 次作为最终置乱次数.与文献[22]中的 10 次坐标变换相比,加密时间稍有缩短.同时本文算法由于引入多个数学问题,增加了加密复杂性和破解的难度.

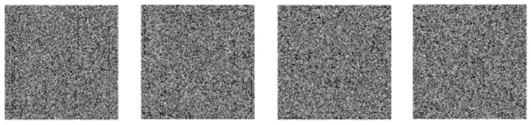


图 8 不同次拉丁方置乱变换效果图

2.3 密钥特性分析

首先分析密钥空间大小.本文所提算法的密钥由 3 个子密钥构成.第 1 个子密钥由混沌序列特性和计算机精度决定,这里取精度为小数点后 10 位,x_0 可取空间大小约为 10^{11},μ 可取空间大小约为 10^{10},a 可取空间合理范围约为 10^3,则第 1 个子密钥空间大小约为 10^{24}.由引理 3 可知,第 2 个子密钥为置换矩阵所对应的置换 τ_1,τ_2,其空间大小为 $m!\times m!$,本文为 $304!\times 304!$,大约为 $10^{1\,248}$.第 3 个子密钥为拉丁方置乱的次数,可取空间大小约为 $10^0\sim 10^2$.因此,由以上 3 个子密钥构成的密钥空间约为 $10^{1\,272}\sim 10^{1\,274}$,非常巨大,从而可抵抗枚举攻击.

其次分析密钥敏感性.本文做了 3 个仿真来研究密钥的微小变化对最终加密图的影响.仿真 1 将混沌序列初始值 x_0 从 3.888 888 变为 3.888 889,2 个值仅相差 0.000 001;仿真 2 研究置换矩阵的敏感性,密钥仅相差 1 对数值;仿真 3 研究拉丁方位置置乱次数的敏感性,置乱次数仅相差 1 次.3 个仿真所涉及的具体参数及得到的加密图不变点之比如表 1 所示.

表 1 密钥敏感性分析表

密钥位置	x_0	τ_1,τ_2	d
差值	0.000 001	1	1
不变点比	0.007 0	0.035 2	0.004 3

由表 1 可知,在解密时,即使有极微小的密钥改变,不变点比也很小,这说明加密图像对密钥充分敏感.

最后分析密钥本身大小.本文按照在MATLAB中所占字节计算,此密钥所占字节为 726 Bytes,原图$O(256)$大小为 65 536 Bytes,密钥大小与原图大小比值为 1.1%,密钥存储空间占比合理.

由以上分析知,本文所提算法密钥空间大,密钥敏感性强,密钥存储空间小.

3 加密特性的计算及抗攻击仿真

3.1 加密特性的计算

本算法的加密特性参数[24]主要从以下 4 个方面进行计算:不动点比、信息熵、相邻像素自相关度和运行时间.

3.1.1 不动点比

由表 2 可知,$A(256)$的不动点比相当的低,进一步经过置换矩阵位置置乱和 4 次基于完备拉丁方扩展矩阵的位置置乱,加密图像 $X(304)$ 的不动点比更低.

表 2 目标图与加密图的不动点比值

图像	$A(256)$ 与 $O(304)$	$X(304)$ 与 $A(304)$
不动点比	0.037 888	0.004 286

3.1.2 信息熵

由表 3 可知,$A(256)$的信息熵为 7.964 5,已经接近香农极限值 8.而嵌入后再经过位置置乱的最终加密图 $X(304)$ 的信息熵为 7.971 5,更接近极限值 8,说明本算法在打乱图像像素分布方面性能良好.

表 3 信息熵比较表

图像	$O(256)$	$A(256)$	$X(304)$
信息熵	7.446 6	7.964 5	7.971 5

3.1.3 相邻像素自相关度

自相关度是衡量图像加密效果的一个指标,其值越小,加密效果越好.本文计算每个像素点和其周围邻近像素点的自相关度,得到的结果如表 4所示.

表 4　图像自相关度表

图像	O(256)	A(256)	X(304)
自相关度/(10^{-6})	92.892	12.056	7.074 2

从表 4 可以看出,预处理后的图像比原始图像的自相关度低,最终加密图的自相关度最低.

3.1.4　运行时间比较

本文对比了其他算法[25-27]的加密时间,从表 5可以看出,在具有较高复杂度的密钥空间的加密方法中,本文算法比参考文献中的算法有更高的运行效率.

表 5　运行时间比较　　s

图像大小	本文	文献[25]	文献[26]	文献[27]
256×256	0.778 0	1.19	12.9	1.04
512×512	3.012 2	/	/	2.85

由以上分析可知,本文算法不动点比低,信息熵大,相邻像素相关性小,运行时间较短,总体加密特性较佳.

3.2　抗一般性攻击仿真实验

3.2.1　抗椒盐噪声攻击仿真

对未加椒盐噪声和加椒盐噪声(随机噪声点数占总像素 10%)的解密 Lena 图进行了比较,如图 9所示,发现不变点比值为 90.34%,故该算法可以在一定程度上抵抗椒盐噪声的攻击.

3.2.2　抗高斯白噪声攻击分析

对未加高斯噪声和加了高斯噪声(均值为 0,方差为 0.001)的解密 Lena 图进行了比较,见图 10.左边子图为受噪声影响的加密图,中间子图为原图,右边子图为解密图.可知该算法可以在一定程度上抵抗高斯噪声的攻击.

图 9　抗椒盐噪声攻击及其解密恢复图

图 10　抗高斯白噪声攻击及其解密恢复图

3.2.3　抗剪切噪声攻击分析

本文所提算法的抗剪切噪声攻击的性能也较好.图 11 ~ 图 13 分别是受到 1/16,1/4,1/2 剪切攻击后的解密图.由图可知,本算法在一定程度上保留了原来图像的特征.这是因为位置置乱的扩散性,使得原图像素打乱分散到加密图像的各个位置,所以剪切某块区域之后还保留了原图像的部分信息,因此,解密图像仍有较好的效果.

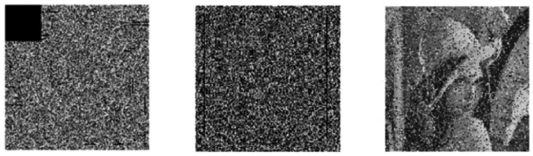


图 11　抗 1/16 剪切攻击及其解密恢复图

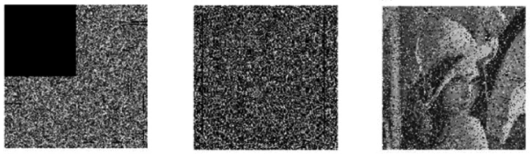


图 12　抗 1/4 剪切攻击及其解密恢复图

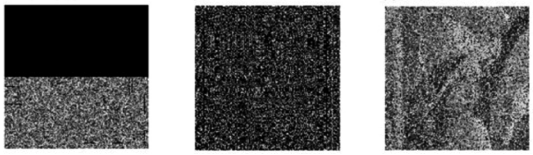


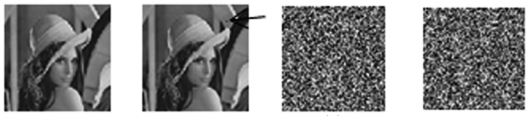
图 13　抗 1/2 剪切攻击及其解密恢复图

4　抗差分攻击仿真及性能分析

4.1　抗差分攻击仿真实验

本文研究的图像加密算法可以抵抗差分攻击.差分攻击的基本思想是: 通过分析特定明文差分对相应的密文差分的影响来破解密钥.在本文所提算法中,因为使待加密图像隐藏在一幅随机大图中进行传输,且位置是随机的,所以本算法对 2 幅非常接近的原图进行加密时,也会获得差异很大的加密图,因此,获得了抗差分攻击的能力.仿真实验如下:

以 256 阶的 Lena 灰度图为例,图 14 中的(b)是(a)变动一个像素(箭头处)后的图像.对这 2 幅图进行本算法的加密处理,分别得到图 14(c)和图 14(d),不同点比值高达 96.5%.可见攻击者发动差分攻击时,即使每次变动很少的一些值,加密图也会发生高达 95.0%以上的变化,这是因为笔者所引入的随机图及嵌入的位置在每次加密时都会发生很大的改变,引入了很大的随机性.



(a)为256阶Lena灰度图;(b)为差分处理后Lena灰度图;(c)为Lena灰度图的加密图;(d)为差分处理后的加密图

图14 抗差分攻击实验图

4.2 相关参数及性能分析

在抗差分攻击的分析中通常依据以下2个参数:像素改变率(number of pixels changing intensity,*NPCR*)和一致平均改变率(unified average changing intensity,*UACI*),具体定义见文献[22].

选择像素值只在一个点上有差异的2幅256×256原图,经过加密后得到2幅加密图,计算其相应的*NPCR*和*UACI*值,如此做9次独立的仿真实验,所得数据见图15与图16.

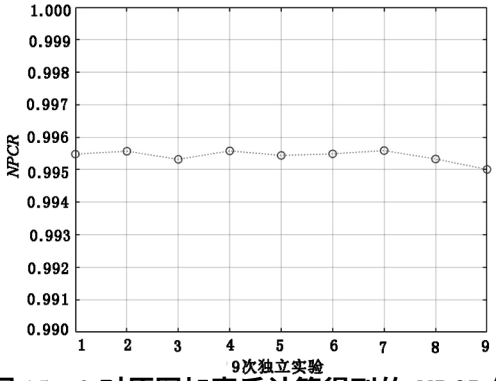


图15 9对原图加密后计算得到的*NPCR*值

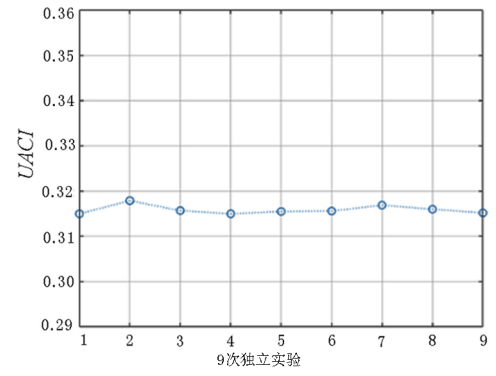


图16 9对原图加密后计算得到的*UACI*值

由图15可知,*NPRC*值在各次实验中保持在99.5%~99.6%;由图16可知,*UACI*值也较高,为33.0%~34.0%.

这说明原始图像的微小改变会对最终的加密图产生显著影响(*NPRC*值高达99.5%~99.6%,*UACRI*也可达33.0%~34.0%).而评价一个算法是否能有效抵抗差分攻击,就看其对原始图像的变化是否敏感.以上仿真实验表明,本文所提算法具有很强的抗差分攻击能力.

为了研究所选随机大图的大小对抗差分攻击性能的影响,笔者又做了以下3个仿真实验,分别选取为304,280,264阶的随机大图,所得数据见表6.

表6 不同阶数随机大图的差分特性表

随机大图阶数	304	280	264
NPCR	0.995 8	0.995 7	0.994 7
UACI	0.316 8	0.311 8	0.309 9

由表6可知,在相当大的范围内,随机大图选取的大小对抗差分攻击的特性几乎没有影响.即使随机大图非常接近原图大小,如264阶,也可取得较好的抗差分攻击特性,这是由于在本文算法中嵌入位置的随机性所保证的.因此,本文所提算法的所需冗余量可以非常小,在264阶随机大图时,冗余信息仅占6%.

综上,本文所提算法既可在付出代价非常小(冗余仅需6%)的情况下有效抵抗差分攻击,又可有效抵抗椒盐噪声、剪切攻击等其他类型的攻击.而文献[25-27]算法由于没有引入冗余,所以为了抵抗差分攻击,使解密过程中对于密图中的像素值的改变相对敏感,故本文算法在抵抗噪声攻击方面的表现优于文献[25-27].

5 结 论

近年来,随着信息技术的快速发展和互联网的广泛运用,信息安全的重要性越发凸显.本文提出的基于混沌序列、拉丁方和置换矩阵的图像加密算法和已有算法相比具有以下优势:

首先,预处理阶段经过混沌矩阵异或后图像的像素已经比较均匀,与随机矩阵的像素值置乱效果相当,但大大缩小了密钥大小.且与文献[22]中仅用拉丁方异或的预处理方法相比,有更好的效果.在仿真实验中,密钥大小仅占原图大小的1.1%.

其次,引入了置换矩阵,使得拉丁方位置置乱仅需要4次便可以达到理想的效果,使运行时间比文献[25-27]所提算法都要短,并且由于采用多种加密方式,密钥空间更大,达到$10^{1\,272}\sim10^{1\,274}$,使得破解更加困难.

再次,该算法具有良好的抵抗各种攻击的性

能.仿真分析表明,该算法可以抵抗差分攻击,同时可以抵抗椒盐噪声、高斯噪声和剪切噪声.这是由于本文所提算法中引入的冗余具有较大的随机性和无规律性,造成差分攻击的困难,并且可以在冗余量非常小的情况下就达到以上性能.

综上,本文所提的算法具有构造简单、密钥大小适中、密钥空间巨大、加密效果好、耗时短、能够同时抵抗多种攻击等优点.

参考文献:

[1] 郭志川,程义民,王以孝,等.基于 DES 加密的流媒体实时隐秘传输和硬件实现[J].系统工程与电子技术,2005,27(7):1311-1314.
[2] 向涛,余晨韵,屈晋宇,等.基于改进 AES 加密算法的 DICOM 医学图像安全性研究[J].电子学报,2012,40(2):406-411.
[3] 张国平,黄淼,马丽.基于 MGSA 融合波分复用的光学彩色图像加密[J].激光杂志,2015,36(7):63-68.
[4] 李建军,梁利利,张福泉.基于混合相位掩码与 Gyrator 小波变换的光学图像加密算法[J].光学技术,2018,44(6):717-726.
[5] 刘杰,白廷柱,沈学举,等.基于联合功率谱分区复用的光学多图像加密方法与实验[J].中国激光,2018,45(12):246-255.
[6] 肖宁,李爱军.基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法[J].电子测量与仪器学报,2017,31(6):876-884.
[7] CAI J J,SHEN X J,LIN C.Imagesencryption based on joint transform correlator and vector decomposition[J].Journal of Optoelectronics Laser,2015,26(5):1005-1009.
[8] CHEN H,TANOUGAST C,LIU Z J.Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains[J].Optics and Lasers in Engineering,2017,98(10):1-8.
[9] TANG Z J,ZHANG X Q.Secure image encryption without size limitation using arnold transform and random strategies[J].Journal of Multimedia,2011,6(2):202-206.
[10] 叶满珠,廖世芳,王新芳.基于幻方变换的图像置乱新算法[J].自动化与仪器仪表,2016(2):216-218.
[11] 吴成茂.离散 Arnold 变换改进及其在图像置乱加密中的应用[J].物理学报,2014,63(9):91-110.
[12] 徐潇,马峻,赵飞乐,等.Arnold 变换和混沌映射的计算全息多图像同步加密[J].激光杂志,2018,39(6):57-60.
[13] 徐光宪,李玉华,张鑫.基于幻方变换的抗剪切扩频水印算法研究[J].清华大学学报(自然科学版),2013,53(8):1087-1090.
[14] 王冬梅.奇数阶幻方变换数字图像的准周期[J].浙江工业大学学报,2005,33(3):292-294.
[15] 周蕊,于晓明,焦占亚.一种基于混沌序列的数字图像加密算法[J].微电子学与计算机,2010,27(12):62-68.
[16] BEHNIA S,AKHSHANI A,MAHMODI H,et al.A novel algorithm for image encryption based on mixture of chaotic maps[J].Chaos Solutions Fractals,2008,35(2):408-419.
[17] ALVAREZ G,LI S J.Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption[J].Communications in Nonlinear Science and Numerical Simulation,2009,14(11):3743-3749.
[18] RAO K D,KUMAR K P,KRISHNA P V M.A new and secure cryptosystem for image encryption and decryption[J].IETE Journal of Research,2011,57(2):165-171.
[19] 杨璐,邵利平,郭毅,等.基于迷宫置换和 Logistic 混沌映射的图像加密算法[J].计算机应用,2014,34(7):1902-1908.
[20] 刘晓衡,廖春龙,朱从旭,等.像素位置与比特双重置乱的图像混沌加密算法[J].通信学报,2014,35(3):216-223.
[21] 燕善俊,余邵平.基于 Logistic 混沌序列的灰度图像加密算法[J].计算机工程与应用,2008,44(36):179-180;208.
[22] 吕翔,杨刘洋,刘梦梦,等.基于嵌入冗余信息方式的图像加密方案与实现[J].浙江师范大学学报(自然科学版),2018,41(1):31-38.
[23] 彭立,朱光喜.不同置换矩阵对基于分块 H 矩阵的 LDPC 码性能的影响[J].计算机学报,2008,31(5):789-792.
[24] 吕翔,杨刘洋,刘中帅.一种无损伤的图像加密算法与实现[J].浙江师范大学学报(自然科学版),2017,40(2):153-160.
[25] SURYANTO Y,URYADI,RAMLI K.A new image encryption using color scrambling based on chaotic permutation multiple circular shrinking and expanding[J].Multimedia Tools and Applications,2017,76(15):16831-16854.
[26] QIN Y,WANG Z P,PAN Q N,et al.Optical color-image encryption in the diffractive-imaging scheme[J].Optics and Lasers in Engineering,2016,77:191-202.
[27] SU Y G,TANG C,GAO G N,et al.Optical encryption scheme for multiple color images using complete trinary tree structure[J].Optics and Lasers in Engineering,2017,98:46-55.
[28] TONG X J.Novel bilateral-diffusion image encryption algorithm with compound chaos and LFSR[J].Image Science Journal,2012,60(5):294-304.
[29] 王静,蒋国平.一种超混沌图像加密算法的安全性分析及其改进[J].物理学报,2011,60(6):83-93.

(责任编辑　杜利民)