基于Logistic映射与排序变换的图像加密算法

陆大兴,廖晓峰,韩 洁,李 明
(重庆大学 计算机学院,重庆 400045)

摘 要:提出了一种新的基于混沌映射与排序变换的图像加密算法。混沌序列具有容易生成、对初始条件敏感以及具备白噪声的统计特性等优点。该算法利用混沌映射对初值的敏感性和伪随机性,通过对生成的混沌序列排序来得到图像置乱的地址变换码,由于排序的不规则性,因此新的混沌图像置乱算法具有较强的保密性能。通过对该算法的置乱性能分析并进行仿真实验,结果表明,新算法具有良好的图像加密性能。

关键词:混沌映射;排序变换;置乱
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)12-0027-04

Picture Scrambling Algorithm Based on Logistic Mapping and Sort Transformation

LU Da-xing, LIAO Xiao-feng, HAN Jie, LI Ming
(College of Computer Science of Chongqing University, Chongqing 400045, China)

Abstract: Proposed a new algorithm of images scrambling based on the chaotic mapping and sort transformation. Chaotic sequences have several good properties including the ease of their generation, their sensitive dependence on initial condition and noise like. The new algorithm utilizes the sensitivity of the original state and the uniqueness of the chaos mapping, obtains the address codes of the images transposition by the sort transformation of the chaotic sequence. Due to the strong irregularity of sort transformation, the new chaotic images scrambling algorithm possesses high level security. Also analyzes the scrambling performance of the new algorithm in a statistical way. The results of the analysis indicate that the algorithm bears nice scrambling capability.

Key words: chaos mapping; sort transformation; transposition

0 引 言

随着互联网技术的飞速发展,各种各样的信息需要通过网络来传输,信息的安全与保密显得越来越重要。当前,对信息安全问题的研究已取得很大进展,其中数字图像加密是重要的一个分支。数字图像置乱变换[1]不仅可以在空间域上进行,还可以在其频率域上进行。

传统的加密技术将其作为普通的数据流进行加密,不考虑其自身的特点,有一定的局限性。数字图像的置乱方法分为:

(1)用分形图形学的方法对空间曲线进行填充[1,2]。

(2)利用其它数学知识[3,4]和奇特现象进行数字图像置乱的方法[5,6]。

这些方法针对数字图像的加密和解密一般采用同一算法来进行。其中用混沌映射的方法是比较流行的方法。混沌现象是在非线性动力系统中出现的具有对初始条件的敏感依赖性、类噪声、非周期性、确定性的、类随机的过程,这种过程即非周期又不收敛,其状态完全可以重现[7~10]。因此,利用它可以构造出非常好的图像信息加密系统。

1 基于混沌映射与排序变换的图像置乱算法设计

1.1 混沌系统加密算法设计

Logistic映射[11,12]是一个非常简单,却又具有重要意义的非线性迭代方程,它具有确定的形式,并且系统不包含任何随机因素,但系统却能产生看似完全随机的,对参量的动态变化和初值极为敏感的混沌现象[13],所以文中选用Logistic映射迭代来产生混沌序列。

收稿日期:2007-03-10
作者简介:陆大兴(1971-),男,四川人,硕士,研究方向为混沌密码学、信息安全;廖晓峰,博士,教授,研究方向为混沌理论与控制、信息安全等。

文中以 256 × 256 的图像 I 为例。

第一步:选取下列迭代方程:

$$x_{n+1} = 1 - 2x_n^2 \quad (1)$$

其中 x_n 为映射变量,它的取值范围为:

$$-1 < x_n < 1$$

第二步:给定初值 x_1,由(1)式迭代 $N-1$ 次得到 $(x_1, x_2, \cdots, x_n)$ 序列,并对它们排升(或降)序得新的序列:$(x'_1, x'_2, \cdots, x'_n)$。

第三步:定位 x_i 在 x'_i 中的位置序数,得到序数序列记为:$r(t,:) = (r_1, r_2, \cdots, r_n)$(其中 $t = 1,2,\cdots,256$)。

第四步:以 r 为图像 I 的像素矩阵 A 的第一(或 N)行的地址置换码,对矩阵 A 进行行地址变换。

第五步:以 r 为图像 I 的像素矩阵 A 的第一(或 N)列的地址置换码,对矩阵 A 进行列地址变换。

第六步:循环一到五步,直到矩阵 I 全部行、列变换完为止,即图像加密完成。为达到更好的效果,也可以再重复一个循环,一般一个循环周期完成就可以了。

MATLAB 例程如下:

```
A=imread('lena.bmp'); %%读入被加密图像
B=A;
key=0.400001; %%输入加密密钥
N=256; %%定义图像矩阵大小
x1=zeros(1,256);
x2=zeros(1,256);
r=A; %%定义变量空间
for t=N:-1:1;
    x1(1)=key;
    for n=1:N-1;
      x1(n+1)=1-2*x1(n)^2;
    end; %%产生混沌序列
    [x2,r(t,:)]=sort(x1); %%产生地址变换码
    key=x1(N);
    B(r(t,:),t)=A(:,t);
    B(t,r(t,:))=A(t,:);
    A=B; %%图像矩阵变换
end;
imwrite(A,'lena01.bmp'); %%产生加密后的图像
```

1.2 解密算法设计

当用户输入正确的密钥后,将加密算法逆向运算,即前三步循环 N 次,得到 $r(N\times N)$ 和 $s(N\times N)$ 的矩阵,第四、五步交换,并把"第一(或 N)行/列"改为"第 N(或一)行/列",再循环 N 次就得到解密图像了。

MATLAB 例程如下:

```
A=imread('lena01.bmp'); %%读入被加密图像
B=A;
key=0.400001; %%输入解密密钥
N=256;
x1=zeros(1,256);
x2=zeros(1,256);
r=A; %%定义变量空间
for t=N:-1:1;
    x1(1)=key;
    for n=1:N-1;
      x1(n+1)=1-2*x1(n)^2;
    end; %%产生混沌序列
    [x2,r(t,:)]=sort(x1); %%产生地址变换码
    key=x1(N);
end;
s=1;
for u=1:N;
    B(s,:)=A(s,r(u,:));
    B(:,s)=A(r(u,:),s);
    A=B;
    s=s+1;
end; %%图像矩阵变换
imwrite(A,'lena02.bmp'); %%产生解密后的图像
```

2 基于排序变换的混沌图像置乱性能分析

由迭代方程式(1)来产生混沌实值序列,并进行置乱算法统计分析。用于图像置乱的灰度图像 I 大小取为 256 × 256pixels。基于排序变换[14]的混沌图像置乱性能分析如下。

2.1 时间复杂度分析

如采用量化方法,同样采用行置换,则首先必须将混沌映射区间[-1,1]划分为 256 个连续子区间,为取得最佳量化速度,则要使点 x_n 落入各个子区间的概率相等。由 Logistic 轨道分布的概率密度函数[7]

$$\rho(x) = \frac{1}{\pi\sqrt{1-x_2}} \quad \text{其中 } x \in (-1,1)$$

易知,各划分点为:

$$L_k = -\cos(k\pi/256) \quad (k = 0,1,2,\cdots,256)$$

若随机选取 1 000 个初值,并通过对迭代产生的混沌序列进行量化来产生置换地址码,则遍历 256 个地址码的时间特性如表 1 所示。

表 1 迭代次数

最大迭代次数	最小迭代次数	平均迭代次数
4590	2505	3321.4

由表 1 可以看出,用量化方案来产生置换地址码不仅所需迭代次数非常多,而且同初值的关系也较大。另外,通过实验也发现,由于随着地址码的增加,遍历全部地址码所需迭代次数增加迅速,因此使得采用量化方案的置换对较大的图像不得不采用局部置乱或分块置乱技术,这样从整体上说,就降低了置乱的效果。

由于多值量化也需大量的比较运算,所以基于排序变换的混沌置换地址码生成方案较量化方案在时间复杂度上相对较低。由于新算法所用混沌映射迭代次数大大减少,且与初值无关,从而使得加密解密的速度有很大提高。

2.2 不动点分析

如果原图像像素点经过置乱变换后,像素点的地址没有发生变化,则称此像素点为该置乱变换的不动点。不动点的数目越少,置乱的效果就越好,保密性也就越高。表 2 是对 256×256pixels 大小的灰度图像,采用随机选取的 10 000 个初值,通过基于排序变换的混沌图像行置乱算法构造的置乱变换的不动点统计分析的结果。

表 2　不动点统计结果

不动点最多	不动点最少	不动点平均
45 个	38 个	40 个

由表 2 可以看出,由于基于排序变换的混沌图像行置乱算法的不动点的个数只占整幅图像所有像素点的 0.38%～0.45% ,因此取得了很好的置乱效果。

2.3 像素点自然序分析

如果原图像中相邻的像素点,置乱后它们的地址虽然都发生变化,但仍然相邻,则称之为自然序。若置乱后图像的自然序越少,则置乱的效果越好,保密性也就越高。表 3 是对 256×256pixels 大小的灰度图像,采用随机选取的 10 000 个初值,通过基于排序变换的图像混沌行置乱算法置乱后,图像每个 4×4 方阵内自然序点出现比例的统计分析结果。

表 3　自然序点统计结果

自然序点所占比例最大	自然序点所占比例最小	自然序点所占比例平均
0.066 0	0.057 5	0.061 0

从表 3 可以看出,经基于排序变换的混沌置乱算法置乱后,加密图像中每个 4×4 方阵内出现的自然序个数比例在 7% 以下,由于相邻的像素点基本都被拆散,从而取得了很好的置乱效果。

3 计算机仿真结果

使用 MATLAB 6.5 进行仿真实验如图 1 所示。图(d)是当 key = 0.400 001 时利用该方法来对 256×256 大小的 lena 灰度图像进行置乱后的图像,(b)、(c)是只对 lena 分别进行行和列置乱所得的图像,图(e)是密钥正确时所得的解密图像,(f)是 key = 0.400 002 时所得的解密图像。由实验结果可见:使用该算法对图像进行加密,加密后的图像已不能看出原图像的任何轮廓,当 key 略有差异时,就根本不能正确解密图像,密钥为(－1,1)之间的任何实数,密钥空间也足够大,由此可见该算法具有较高的安全性。

4 抗攻击实验

4.1 剪切和篡改攻击

图 1(g)和(i)是对已加密图像进行剪切或篡改,解密后得到的图像(h)、(j)仍然可辨清轮廓,由于该算法对图像各点置乱较均匀,无论剪切任何部位的一定面积图像,解密后的图像都可基本辨清其轮廓。

4.2 噪声污染

图 1(k)中加入 Speckle 噪声,(m)加入 Gaussian 噪声,(l)和(n)是它们的解密图像,由图可以看出:该算法有较好的抗噪声性能。

5 结　论

提出一种基于混沌映射与排序变换的图像置乱算法,该算法克服了普通混沌图像置乱算法在混沌序列整数化时对混沌序列随机性造成破坏的缺陷,由于排序变换的强不规则性,增加了算法对混沌映射初始值的敏感度与置乱的复杂度,从而使得新的混沌图像置乱算法具有较高的安全保密性能,密钥空间为(－1,1)之间的全体实数,密钥空间足够大。另外,由于在仿真时,对混沌序列的排序是通过对向量操作的方式进行,时间复杂度也得到了很好的控制,通过对新算法置乱性能的分析结果表明,该算法具有良好的置乱性能。

参考文献:

[1] 蒋金山,曾德炉.基于椭圆曲线公钥密码体制的数字图像加密技术[J].微型机与应用,2004(5):50－52.

[2] 童向杰,丁德胜.几种基于等偏爱曲线的图像处理技术[J].电子器件,2005,28(1):6－9.

[3] 丁　玮,闫伟齐,齐东旭.基于 Arnold 变换的数字图像置乱技术[J].计算机辅助设计与图形学学报,2001,13(4):339－341.

[4] 李　敏,费耀平.基于队列变换的数字图像置乱算法[J].计算机工程,2005,31(1):148－152.

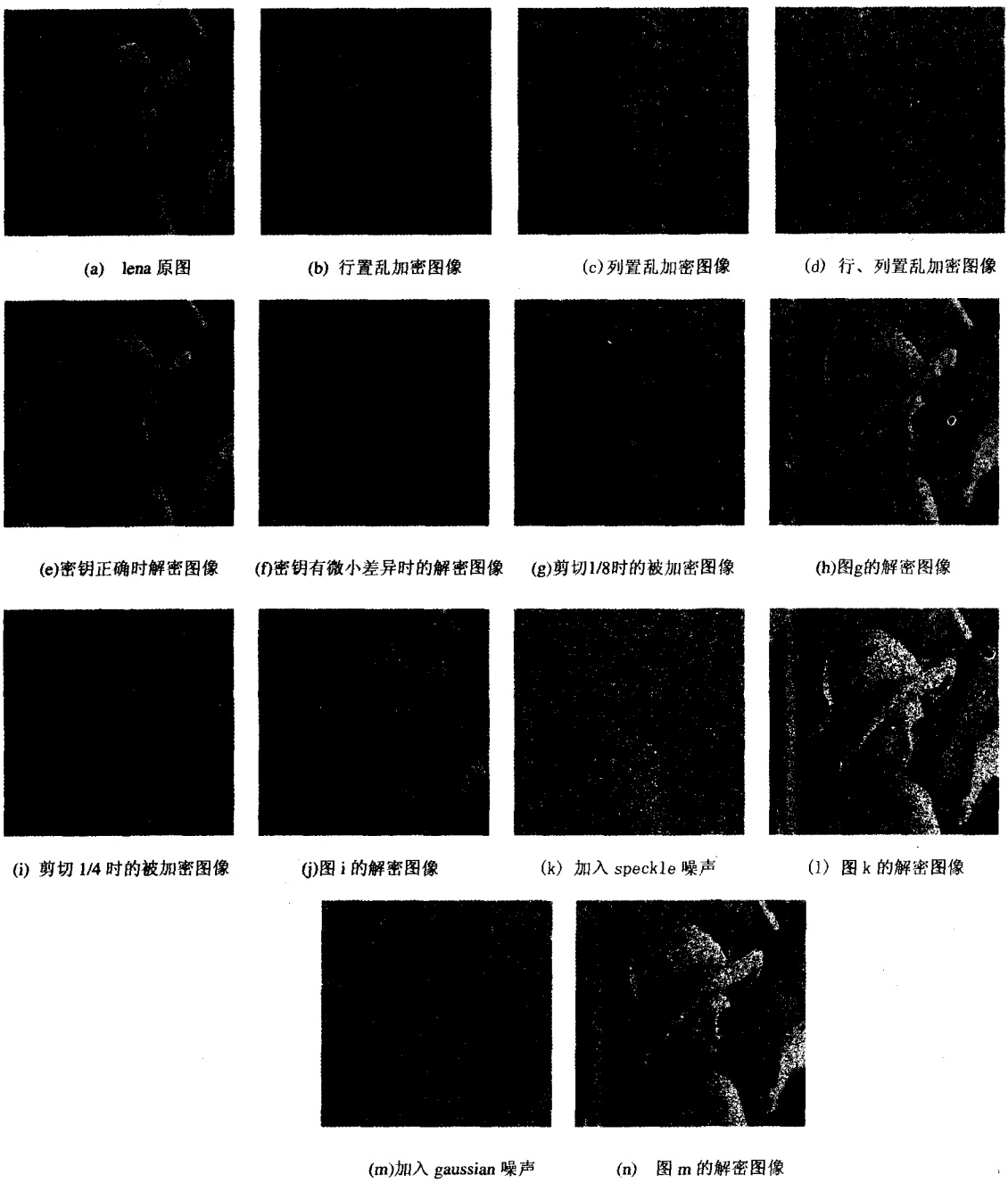
[5] 柏　森,曹长修.一种新的数字图像置乱隐藏算法[J].计算机工程,2001,27(11):18－19.

[6] 吴旻升,王介生,刘慎权.图像的排列变换[J].计算机学报,1998,21(6):514－519.

[7] 文志强,李陶深,张增芳.一种新的基于混沌序列的图像加密技术[J].计算机工程,2004.30:12－14.

[8] 尹显东,姚　军,李在铭,等.基于混沌序列的频域图像加密技术研究[J].计算机工程与应用,2004(34):12－14.

[9] 唐国坪,廖晓峰.基于混沌映射的抗剪切鲁棒水印算法



(a) lena 原图 (b) 行置乱加密图像 (c)列置乱加密图像 (d) 行、列置乱加密图像

(e)密钥正确时解密图像 (f)密钥有微小差异时的解密图像 (g)剪切1/8时的被加密图像 (h)图g的解密图像

(i) 剪切 1/4 时的被加密图像 (j)图 i 的解密图像 (k) 加入 speckle 噪声 (l) 图 k 的解密图像

(m)加入 gaussian 噪声 (n) 图 m 的解密图像

图 1 仿真结果

[J].计算机工程,2005,31(9):34-36.

[10] 王 毅.基于混沌序列的图像加密研究[J].计算机工程与应用,2002(20):99-102.

[11] 易开祥,孙 鑫,石教英.一种基于混沌序列的图像加密算法[J].计算机辅助设计与图形学学报,2000, 12(9):672-676.

[12] 齐东旭,邹建成.一类新的置乱变换及其在图像信息隐蔽中的应用[J].中国科学(E辑),2000,30(5):440-447.

[13] 孙 鑫,易开祥,孙优贤.基于混沌系统的图像加密算法[J].计算机辅助设计与图形学学报,2002,14(2):136-139.

[14] 刘向东,焉德军,朱志良,等.基于排序变换的混沌图像置乱算法[J].中国图像图形学,2005,10(5):656-660.

(上接第 26 页)

mune System[J]. Evolutionary Computation,2000,8(4):443-473.

[2] Forrest S, Perleson A, Allen L, et al. Self-Nonself discrimination in a computer[C]// In: Proceedings of IEEE Symposium on Research in Security and Privacy. Oakland, USA:[s. n.],2002:202-212.

[3] Zhang Jian. An Anomaly Detection Method Based on Fuzzy Judgment[J]. Journal of Computer Research and Development,2003,40(6):776-783.

[4] Hofmeyr S. An immunological model of distributed detection and its application to computer security[D]. New Mexico: Dept of Computer Science, University of New Mexico, 1999.