基于排序变换的混沌图像置乱算法

刘向东[1] 焉德军[1] 朱志良[2] 王光兴[2]
[1](大连民族学院非线性信息技术研究所, 大连 116600) [2](东北大学信息科学与工程学院, 沈阳 110004)

摘 要 为了更好地利用混沌进行图像保密, 基于排序变换设计了一个混沌图像置乱算法, 新算法不经过量化, 而是直接通过混沌序列的排序变换来得到图像置换的地址码, 这就有效地避免了量化必须已知混沌轨道分布密度函数的要求, 同时也降低了算法的时间复杂度。由于排序变换的强不规则性, 因此使新的混沌图像置乱算法具有较强的安全保密性能。通过对新算法的置乱性能进行的实验分析结果表明, 新算法不仅具有良好的置乱性能, 而且可以有效地保障加密图像的安全。

关键词 混沌序列 置乱 排序变换
中图法分类号: TP309 TN918 文献标识码: A 文章编号: 1006-8961(2005)05-0656-05

Chaotic Picture Scrambling Algorithm Based on Sort Transfomation

LIU Xiang-dong[1], YAN De-jun[1], ZHU Zhi-liang[2], WANG Guang-xing[2]
[1](*The Research Institute of Nonlinear Information Technology, Dalian Nationalities University, Dalian* 116600)
[2](*College of Information Science & Engineering, Northeastern University, Shenyang* 110004)

Abstract This paper proposes an algorithm of chaotic images scrambling based on the sort transformation. The new algorithm obtains the address codes of the images transposition by the sort transformation of the chaotic sequence and does not need the quantification. The probability density function of the chaotic orbits must be known by the method of quantification. The new algorithm, however, overcomes this disadvantage, which not only facilitates the choice of chaotic systems but also reduces the time complexity of traversing the images scrambling quantified by chaos. As a result, it increases the speed of scrambling images. Due to the strong irregularity of sort transformation, the new chaotic images scrambling algorithm possesses high-level security. The paper 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 and guarantees the security of the encrypted images effectively.

Keywords chaos sequence; permutation network; sort transformation

1 引 言

图像置乱技术既是一种常用的图像加密方法, 又可作为进一步隐藏图像信息的预处理手段, 是信息保密安全重要的研究课题[1]。图像置乱目前主要有基于图像像素点坐标的空间域置换、频域置换和基于图像色度域的置换。图像置乱的要求是置乱后的图像应具有较低的可懂度, 并能抗一定程度的破译攻击, 而解密后图像又能准确表达原始图像的内容[1,2]。在大量不同的图像置乱算法[2~4]中, 基于混沌的图像置乱技术, 由于具有充分大的密码空间及较高的保密性能, 正成为图像置乱技术的热点方法[5,6]。文献[7]研究了采用 1维混沌映射的空间域图像置乱加密算法, 文献[8, 9]分别提出采用参数化 2维混沌映射的空间域图像置乱算法, 文献[9]研究了通过利用混沌映射构造空间域置换矩阵和色度域置换矩阵来进行置乱的图像加密算法。

基金项目: 国家自然科学基金项目(60473108); 辽宁省自然科学基金项目(20040948)
收稿日期: 2004-07-02; 改回日期: 2004-12-14

第一作者简介: 刘向东(1967~), 男。2000年获东北大学信息科学与工程学院博士学位, 现为大连民族学院计算机科学与工程系教授。主要研究领域为混沌分形信号处理、计算机图形、图像处理。E-mail: liuxd@dlnu.edu.cn

目前应用混沌的图像置乱方案一般都是先通过计算混沌模拟序列, 再对其进行多值量化来生成置换地址码。由于对混沌模拟序列进行量化要求对混沌轨道的概率分布有相当的了解, 而这正是混沌研究的一个仍未解决的难题, 并且易受量化精度的影响, 因此多值量化所得置换地址码很难完全保持混沌固有的特性。另外, 由于置换地址码的特殊要求, 要求必须遍历所有置换地址, 而为能遍历所有的地址, 算法不得不经历许多不能生成置换地址码的迭代, 这就增加了算法的时间复杂度。本文提出的置乱算法, 其置换地址码的产生则不需对混沌实值序列进行量化, 而是通过排序变换直接由混沌模拟序列来产生。该方法不需对轨道分布具有先验知识, 即可以选用任何一个混沌模型, 这就极大地扩展了算法的密码空间。本文算法不仅大大减少了混沌映射迭代次数, 并能很好地利用混沌的特性, 同时由于排序变换的强不规则性, 也增加了破译置乱图像的难度。

2　基于排序变换的混沌图像置乱算法

对于一个数字灰度图像 $\boldsymbol{I}$, 其大小为 $M\times N$, 可以利用任一混沌迭代

$$x_{n+1}=f(x_n)\quad x_i\in \boldsymbol{A} \tag{1}$$

来产生混沌实值序列, 然后通过下面描述的置乱算法即可对图像 $\boldsymbol{I}$逐行进行置乱和解密。

2.1　置乱算法

置乱算法步骤如下:

(1) 给定迭代初始值 x_1(相当于密钥);

(2) 经 $N-1$次混沌迭代运算得到混沌实值序列 $\{x_1, x_2, \cdots, x_N\}$;

(3) 通过排序变换, 将实值序列集合 $\{x_1, x_2, \cdots, x_N\}$中的 N 个值由小到大排序, 形成有序序列 $\{\hat{x_1}, \hat{x_2}, \cdots, \hat{x_N}\}$;

(4) 确定混沌实值序列 $\{x_1, x_2, \cdots, x_N\}$中的每个 x_i 在有序序列 $\{\hat{x_1}, \hat{x_2}, \cdots, \hat{x_N}\}$中的位置编号, 形成置换地址集合 $\boldsymbol{T}=\{t_1, t_2, \cdots, t_N\}$, 其中 $t_i\in \boldsymbol{T}$, $i=1, 2, \cdots, N$;

(5) 按置换地址集合 $\{t_1, t_2, \cdots, t_N\}$对图像的第 1行像素进行置换, 同时将其第 i列像素置换至第 t_i 列, $i=1, 2, \cdots, N$;

(6) 置 $x_1=x_N$, 对 2到 M行, 重复步骤(2)到步骤(5)。

2.2　解密算法

对给定的密钥(迭代初始值 x_1), 可采用类似置乱的步骤, 即只需将其步骤(5)改为: 按置换地址集合 $\{t_1, t_2, \cdots, t_N\}$对图像的第 1行像素进行置换, 同时将其第 t_i 列像素置换至第 i列($i=1, 2, \cdots, N$)即可实现图像的解密。

3　基于排序变换的混沌图像置乱性能

本文采用 1维 Logistic映射

$$x_{n+1}=1-2x_n^2\quad x\in[-1, 1] \tag{2}$$

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 $\boldsymbol{I}$ 大小取为 256×256pixels

基于排序变换的混沌图像置乱性能如下:

(1) 时间复杂度

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

$$\rho(x)=\frac{1}{\pi\sqrt{1-x^2}}\quad x\in[-1, 1] \tag{3}$$

易知, 各划分点为

$$L_k=-\cos(k\pi/256)\quad k=0, 1, 2, \cdots, 256 \tag{4}$$

若随机选取 50000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　随机选取 50000个初值, 遍历 256个地址码所需迭代次数

Tab. 1　Iterative steps for 1000 initial points to ergod the 256 addresses

最大迭代次数	最小迭代次数	平均迭代次数
2294	1252	1660.2

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)置乱变换的不动点

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 50000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 基于排序变换的混沌图像行置乱变换不动点统计结果

Tab. 2 Statistical results of the number of fixed points of chaotic picture row scrambling algorithm

不动点最多所占比例(%)	不动点最少所占比例(%)	不动点平均所占比例(%)
0.45	0.38	0.40

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。

(3)置乱移动平均距离

置乱移动平均距离定义为

$$D=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{(w-i)^2+(v-j)^2} \quad (5)$$

其中,(i, j)和(w, v)分别代表原图像像素点的坐标和其置乱后的坐标。置换移动平均距离越大,说明经置乱后像素点总体的位移越大,其与原图像相关性越差,置乱效率越高。表 3是对 256×256pixels大小的灰度图像,采用随机选取的 50000个初值,通过基于排序变换的图像混沌行置乱算法构造的置乱变换的平均移动距离的统计分析结果。

表 3 基于排序变换的混沌图像行置乱变换平均移动距离统计结果

Tab. 3 Statistical results of average shifting distance of chaotic picture row scrambling algorithm

置换移动平均距离最大值	置换移动平均距离最小值	置换移动平均距离平均值
85.5290	85.0698	85.2564

由表 3可以看出,基于排序变换的图像混沌行置乱后的平均移动距离基本稳定在 $256/3\approx 85.3333$pixels,而这也是完全随机行置乱平均移动距离的期望值[10]。这说明基于排序变换的混沌置乱具有良好的随机性与保密性。

(4)自然序

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 4是对 256×256pixels大小的灰度图像,采用随机选取的 50000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 3×3方阵内自然序点出现比例的统计分析结果。

表 4 基于排序变换的混沌图像行置乱变换自然序点统计结果

Tab. 4 Statistical results of natural order numbers of chaotic picture row scrambling algorithm

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
0.0663	0.05754	0.0610

从表 4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 3×3方阵内出现的自然序个数比例在 6%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。

(5)汉明相关性

由于本文算法是逐行生成置换地址码的行置换算法,因此需进一步研究各行置换地址码的汉明相关性。

记$\{t_1, t_2, \cdots, t_N\}$和$\{s_1, s_2, \cdots, s_N\}$是长度为$N$的两个不同行的置换码,它们的汉明相关为$H=\sum_{i=1}^{N}\delta(t_i, s_i)$,其中,$\delta(a, b)=\begin{cases}1 & a=b\\ 0 & a\neq b\end{cases}$

汉明相关描述了不同行置换的相似程度,即汉明相关值越大,其各行置换的相似性越强,置乱的效果就越差。表 5是对 256×256pixels大小的灰度图像,采用随机选取的 50000个初值,通过基于排序变换的图像混沌行置乱算法构造的行置乱变换,其各行与其他各行进行汉明相关的统计分析结果。

表 5 基于排序变换的混沌图像行置乱变换汉明相关统计结果

Tab. 5 Statistical results of Hamming correlation coefficient of chaotic picture row scrambling algorithm

汉明相关最大	汉明相关最小	汉明相关平均
254	235	245.8562

从表 5可以看出,基于排序变换的图像混沌行置乱变换不同行的汉明相关性很小,任意 2行置乱码相同的地址码个数平均不到 1个。

4 计算机模拟结果

图 1是利用基于排序变换的混沌图像行置乱算法来对 256× 256pixels大小的 Lena灰度图像进行置乱和解密后的图像。实验采用 Logistic映射, 其置乱密钥初值为 0.7, 图 1(a)是 Lena原图, 图 1(b)是用基于排序变换的混沌图像行置乱算法对其置乱后的图像, 由该图可以看出, 置乱后的图像已不能看出原图像的任何轮廓, 图 1(c)是解密密钥与加密密钥稍有不同的解密结果图像, 解密密钥取初值 0. 700000 01, 结果表明, 只要密钥稍略有不同, 就无法解密出原图像, 使得用枚举搜索很难对置乱图像进行解密。图 1(d)为密钥正确时解密出的图像, 由该图可见, 解密图像和原图像完全相同。

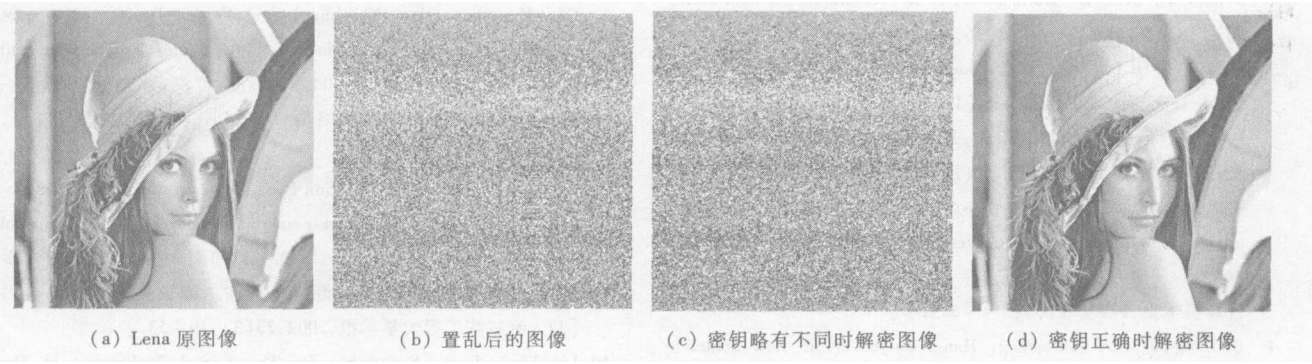

图 1　基于排序变换的混沌图像行置乱算法加密、解密实验结果

Fig 1　Experimental results of chaotic picture row scrambling algorithm based on sort transformation

基于图像行或列置乱的置乱算法在图像比较简单、具有大量相同色调块时, 由于容易让攻击者判断出采用的置乱方式, 因而降低了置乱的安全性。虽然本文主要讨论的是基于图像行置乱的置乱算法, 但该算法很容易修改成为列置乱算法, 而且经过行、列置乱的复合置乱还可进一步增强算法的保密性能。图 2展示了行、列复合置乱的效果, 其中, 图 2(a)是一个较简单的 256× 256pixels大小的 Tiger灰度图像, 图 2(b)、(c)是对该图像分别进行行、列置乱后的图像, 由该两图可见, 图像上均具有明显的条纹结构。图 2(d)是对该图像进行行、列复合置乱后解密的图像, 该图像上已看不出任何结构特征。另外, 本文提出的基于排序的混沌图像置乱算法也很容易推广到彩色图像及色彩域上进行置乱, 并且可以在空间域及色彩域上联合使用, 以增强保密效果。

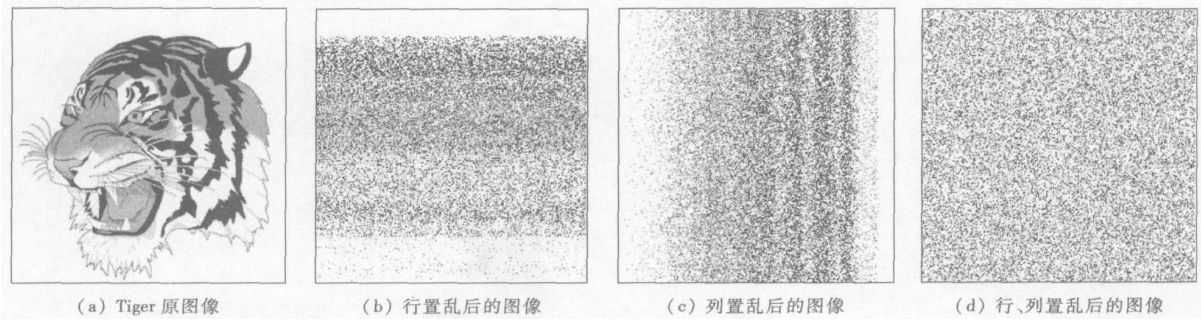

图 2　基于排序变换的混沌图像行、列复合置乱算法实验结果

Fig 2　Experimental results of the chaotic picture row, line and their combination scrambling algorithm based on sort transformation

5 结　论

本文提出一种基于排序变换的混沌图像置乱算法, 该算法克服了普通混沌量化图像置乱算法时间复杂度较高和需要对混沌轨道的概率分布有先验知识等缺陷, 这不仅方便了混沌置乱算法混沌系统的选择, 而且在置乱的速度上也有了很大提高。另外,

由于排序变换的强不规则性,还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和足够大的密钥量。通过对新算法置乱性能的统计分析结果表明,该算法不仅具有良好的置乱性能,还可以有效地保障加密图像的安全。

参考文献(References)

1 BenderW, GruhlD, MorimotoN, *et al*. Techniques for data hiding [J]. IBM Systems Journal, 1996, **35**(3&4): 313~335.

2 Ding Wei, Qi Dong-xu. Digital image transformation and information hiding and disguising technology[J]. Chinese Journal of Computers, 1998, **21**(9): 838~843. [丁玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, **21**(9): 838~843.]

3 Wu Min-sheng, Wang Jie-sheng, Liu Sheng-quan. Permutation transformation of image[J]. Chinese Journal of Computers, 1998, **21**(6): 514~519. [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.]

4 Qi Dong-xu, Zou Jian-cheng, Han Xiao-you, *et al*. New Scramble Transformation and Application in Information Hiding[J]. Chinese Science(E), 2000, **30**(5): 440~447. [齐东旭, 邹建成, 韩效宥. 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), 2000, **30**(5): 440~447.]

5 Matthews R. On the derivation of a 'chaotic' encryption algorithm [J]. Cryptogia, 1989, **13**(1): 29~42.

6 Li Chang-gang, Han Zheng-zhi, Zhang Hao-ran. An image encryption algrithm based on random key and "qusi-standard map" [J]. Chinese Journal of Computers, 2003, **26**(4): 465~470. [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.]

7 Sun Xia, Yi Kai-xiang, Sun You-xian. New image encryption algorithm based on chaos system [J]. Journal of Computer-Aided Design & Computer Graphics, 2002, **14**(2): 1~4. [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): 1~4.]

8 Qin Hong-lei, Hao Yan-ling, Sun Feng. Design of picture permutation network on chaos[J]. Computer Engineering and Application, 2002, **38**(7): 104~106. [秦红磊, 郝燕玲, 孙枫. 一种基于混沌的图像置乱网络的设计[J]. 计算机工程与应用, 2002, **38**(7): 104~106.]

9 Xu Yao-quan, Qin Hong-lei, Sun Feng, *et al*. Application of logistic-map chaos sequence to planar permutation network[J]. Journal of Harbin Engineering University, 2002, **23**(3): 49~53. [徐耀群, 秦红磊, 孙枫等. LogisticMap混沌序列在二维置换网络中的应用[J]. 哈尔滨工程大学学报, 2002, **23**(3): 49~53.]

10 Liu Xiang-dong. Researches for The Kernel Techniques of The Chaotic Secret Multiple Address Communication Systems[D]. Post Doctor Report of Northeastern University, 2002, 51~52. [刘向东. 混沌保密多址通信系统关键技术的研究[D]. 沈阳: 东北大学, 2002, 51~52.]