一种基于混沌的图像置乱算法*)

邓绍江　张岱固　濮忠良
(重庆大学计算机学院　重庆 400044)

摘　要　本文提出了一种新的基于混沌系统的数字图像置乱算法，并将其应用于图像加密。该算法用 Logistic 映射产生的混沌序列值，离散化后构造出对换规则矩阵和横向、纵向移动量矩阵，通过遍历图像中的每个像素点，根据规则和图像中的另一像素点进行对换置乱。实验结果分析表明，该算法具有很好的置乱效果，有较好的加密效率和安全性。

关键词　混沌，图像置乱，图像加密

Digital Image Scrambling Algorithm Based on Chaotic System

DENG Shao-jiang　ZHANG Dai-gu　PU Zhong-liang
(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract　A new digital image scrambling algorithm based on chaotic system is presented in this paper for image encryption. The chaotic sequence generated by Logistic-ma Pis discretized to generate the matrixes which control the rules of exchange and the displacement distance both in horizontal and vertical direction. By traversing each pixel in image, each pixel is exchanged with another pixel in the image following the rules. Simulation experimental result shows that this algorithm has good scrambling performance, high efficiency and security.

Keywords　Chaotic, Image scrambling, Image encryption

1　引言

随着信息化进程的加速发展，特别是互联网和多媒体技术的高速发展，图像信息隐藏作为人们备受关注的研究方向已经取得了很大的进展[1]。数字图像隐藏包含数字图像分存技术、数字水印技术、图像加密技术等等。图像置乱技术就是一种重要的图像加密技术[2]，它的作用就是将图像信元的次序打乱，消除信元流中的各个图像信息间的相关性，实现图像的保密。图像置乱可分为基于图像位置空间、基于图像色彩空间和基于图像频域空间的置乱。目前，常见的数字图像置乱技术主要有基于 Arnold 变换[3,4]、幻方[5]、骑士巡游置乱变换[6]、Hilbert 曲线、Conway 游戏、Tangram 算法、IFS 模型、Fibonacci 变换、Gray 码变换、广义 Gray 变换等方法。虽然这些方法能很好地隐藏图像，达到保密目的。但是，它们对图像大小有限制，变化少，容易被破解。

混沌[7,8]是确定系统中出现的一种类随机现象，它具有良好的伪随机性、统计学和拓扑学特性，它对初始条件极其敏感，且其迭代轨迹在一定程度上不可预测，但只要系统参数及其初始条件相同，就能重构混沌。鉴于此基于混沌的图像置乱算法[9]于是纷纷被提出，本文也是利用混沌系统以上特性，提出了一种新的数字图像置乱算法。实验证明，该算法复杂性高，保密性好。

2　Logistic 映射简介

Logistic 映射是目前被广泛应用的一种混沌动力系统，其数学表达式为：

$$x_{n+1}=f(x_n)=\lambda x_n(1-x_n) \tag{1}$$

其中 λ 为常数，$x_n\in(0,1)$，$n\in N$，当 $3.569945<\lambda\leqslant 4$ 时，映射(1)处于混沌状态，(1)式迭代得到在(0,1)上的伪随机序列 $\{x_k\}_{k=0}^{\infty}$。

3　置乱算法描述

算法设计思想：先后按行和按列遍历每个像素点，使其与图像中随机的任意另一个像素点进行对换。此过程中通过 Logistic 映射产生混沌序列值，将其离散化后生成与原图像等大的矩阵 D,A,O，其中 D 矩阵中的值用来控制像素点对换规则，A,O 矩阵中的值用来控制像素点横向和纵向的移动距离。通过两轮对每个像素点的对换实现图像的置乱。

算法的具体描述如下：

对任意一个数字图像 $I(m\times n)$，设图像像素点的位置用 (i,j) 表示，其中 $i\in\{0,1,\cdots,m-1\}$，$j\in\{0,1,\cdots,n-1\}$。

分别取图像宽度的位长 l 和长度的位长 s，$l=\lceil\log_2 m\rceil$，$s=\lceil\log_2 n\rceil$。其中运算符⌈⌉是表示向上取整运算。

3.1　加密算法

1. 以 k_0 为初始值(同时也作为解密算法的密钥)，通过 Logistic 映射迭代产生混沌序列值。取迭代 10000 次甚至更加后的 $6mn$ 个迭代值 $X=\{x_0,x_1,\cdots,x_{6mn-1}\}$。

2. 从 X 序列中分别取 x_{6t}，x_{6t+1}(其中 $t=0,1,\cdots,mn-1$)，分别构造与图像 I 等大的矩阵 D1$(m\times n)$、D2$(m\times n)$，使得

D1$(i,j)=\lfloor 4x_{6t}\rfloor$(其中 $t=i\times n+j$)；

D2$(i,j)=\lfloor 4x_{6t+1}\rfloor$(其中 $t=i\times n+j$)；

其中运算符⌊⌋是向下取整运算，这样 D1(i,j)，D2$(i,j)\in\{0,1,2,3\}$。

3. 从 X 序列中分别取 x_{6t+2}，x_{6t+3}，x_{6t+4}，x_{6t+5}(其中 $t=0,1,\cdots,mn-1$)，分别构造与图像 I 等大的矩阵 A1$(m\times n)$，

*)国家自然科学基金(60703035)，重庆市自然科学基金(2006BB2227)。**邓绍江**　副教授，博士，主要研究领域为信息安全、混沌理论；**张岱固**　硕士研究生，主要研究领域为信息安全；**濮忠良**　硕士研究生，主要研究领域为信息安全。

$O1(m\times n)$,$A2(m\times n)$,$O2(m\times n)$,使得

$A1(i,j)=\lfloor 2^s\times x_{6t+2}\rfloor$ (其中 $t=i\times n+j$);

$O1(i,j)=\lfloor 2^t\times x_{6t+3}\rfloor$ (其中 $t=i\times n+j$);

$A2(i,j)=\lfloor 2^s\times x_{6t+4}\rfloor$ (其中 $t=i\times n+j$);

$O2(i,j)=\lfloor 2^t\times x_{6t+5}\rfloor$ (其中 $t=i\times n+j$);

这样 $A1(i,j)$、$A2(i,j)\in\{0,1,\cdots,2^s-1\}$; $O1(i,j)$、$O2(i,j)\in\{0,1,\cdots,2^t-1\}$。

4. 以行为主序,按升序遍历像素点,对换像素点。即从第一行起至第 m 行,对任意行 i,从 $I(i,1)$到 $I(i,n)$,每个像素点分别与图像 I 中的一个像素点 $I(p,q)$交换,$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}[(i-A1(i,j))\bmod n]+1, & D1(i,j)=0,1\\ [(i+A1(i,j))\bmod n]+1, & D1(i,j)=2,3\end{cases}$$

$$q=\begin{cases}[(j-O1(i,j))\bmod m]+1, & D1(i,j)=0,3\\ [(j+O1(i,j))\bmod m]+1, & D1(i,j)=1,2\end{cases}$$

5. 以列为主序,按降序遍历像素点,对换像素点。即从第 n 列起至第一列,对任意列 j,从 $I(m,j)$到 $I(1,j)$,每个像素点分别与图像 I 中的一个像素点 $I(p,q)$交换,$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}[(i-A2(i,j))\bmod n]+1, & D2(i,j)=0,3\\ [(i+A2(i,j))\bmod n]+1, & D2(i,j)=1,2\end{cases}$$

$$q=\begin{cases}[(j-O2(i,j))\bmod m]+1, & D2(i,j)=2,3\\ [(j+O2(i,j))\bmod m]+1, & D2(i,j)=0,1\end{cases}$$

3.2 解密算法

1. 前三步同加密算法的第 1,2,3 步

2. 以列为主序,按升序遍历像素点,对换像素点。即从第一列起至第 n 列,对任意列 j,从 $I(1,j)$到 $I(m,j)$,每个像素点分别与图像 I 中的一个像素点 $I(p,q)$交换,$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}[(i-A2(i,j))\bmod n]+1, & D2(i,j)=0,3\\ [(i+A2(i,j))\bmod n]+1, & D2(i,j)=1,2\end{cases}$$

$$q=\begin{cases}[(j-O2(i,j))\bmod m]+1, & D2(i,j)=2,3\\ [(j+O2(i,j))\bmod m]+1, & D2(i,j)=0,1\end{cases}$$

3. 以行为主序,按降序遍历像素点,对换像素点。即从第 m 行起至第一行,对任意行 i,从 $I(i,n)$到 $I(i,1)$,每个像素点分别与图像 I 中的一个像素点 $I(p,q)$交换,$I(i,j)\Leftrightarrow I(p,q)$。其中

$$p=\begin{cases}[(i-A1(i,j))\bmod n]+1, & D1(i,j)=0,1\\ [(i+A1(i,j))\bmod n]+1, & D1(i,j)=2,3\end{cases}$$

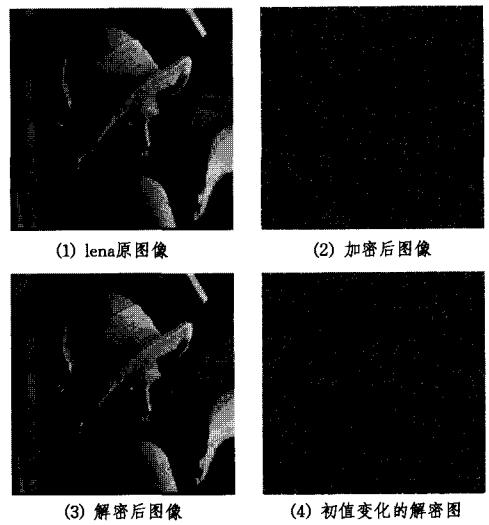
$$q=\begin{cases}[(j-O1(i,j))\bmod m]+1, & D1(i,j)=0,3\\ [(j+O1(i,j))\bmod m]+1, & D1(i,j)=1,2\end{cases}$$

4 实验结果

取密钥初值 $k_0=0.8112$,Logistic 映射中取 $\lambda=3.8104$,用本文置乱算法对图像进行加密,其加密结果均能得到类似于噪声的均匀图像,且完全不能从加密图像中识别原图像的几乎任何信息。

解密过程则刚好是加密的逆过程,在得到正确的密钥前提下,对已加密图像执行解密算法,便能得到解密图像。在解密过程中,若初始值(密钥)发生极其细微的变化,例如 $k_0=0.81120001$,解密后的图像则不能恢复到原图像,且与原图像差异巨大,依然是类似于噪声的均匀图像,完全不能获得原图像的几乎任何信息。

图 1 是 256×256pixels 大小的灰度图像 lena. bmp 的实验数据,(1)为原图(2)加密后的图像(3)解密后的图像(4)初始值细微变化后的解密图像。



(1) lena原图像　(2) 加密后图像

(3) 解密后图像　(4) 初值变化的解密图

图 1　lena 图像实验结果

5 算法性能分析

5.1 置乱后的不动点

所谓不动点,即原图像 I 中像素点 $I(i,j)$经过置乱变换之后,若其在图像中的相对位置(i,j)没发生变化,则称此像素点为不动点。从加密的角度来讲,不动点的数目越少,置乱的效果就越好,保密性能也就越高,反之不动点的数目越多性能越差。

表 1 是随机选取 1000 个初值 k_0,运用本文描述的置乱算法对 256×256pixels 大小的灰度图像 lena. bmp 进行加密,用 matlab 模拟图像置乱实验测试得到的图像不动点统计分析的结果。

表 1　用置乱算法加密后图像不动点统计结果

	平均值	最大值	最小值
不动点个数	3.8	8	0
不动点所占比例	0.0058%	0.0122%	0.0%

5.2 置乱后的平均移动距离

置乱后的平均移动距离定义为:

$$\bar{d}=\frac{1}{mn}\sum_{i=1}^{n}\sum_{j=1}^{m}\sqrt{(i'-i)^2+(j'-j)^2}$$

其中(i,j)、(i',j')分别是某个像素点在原图像中的坐标和在置乱后图像中的坐标。平均移动距离越大,说明置乱后像素点的总体的位移越大,与原图像的相关性越差,置乱效果就越好,保密性能也就越高,反之平均移动距离越小性能越差。

表 2 是随机选取 1000 个初值 k_0,运用本文描述的置乱算法对 256×256pixels 大小的灰度图像 lena. bmp 进行加密,用 matlab 模拟图像置乱实验测试得到的图像置乱后的平均移动距离的结果。

表 2　用置乱算法加密后图像平均移动距离的统计结果

	平均值	最大值	最小值
平均移动距离	133.3728	133.8923	133.1109

从本文置乱算法描述中的加密过程第 4、5 步可以看出,原图像中任意一点 $I(i,j)$,在每一步的交换过程中,点 $I(p,q)$

的 $p\in\{0,1,\cdots,m-1\}$、$q\in\{0,1,\cdots,n-1\}$，且 p,q 能取到属于其中的任意值，故每一次交换 $I(i,j)$ 均能和图像中包括自己在内的任意一点交换。若算法中 p 取 $\{0,1,\cdots,m-1\}$ 中任意值，q 取 $\{0,1,\cdots,n-1\}$ 中任意值的概率相等，这样加密就能具有很好的抗统计特性，不利于统计分析破密。这种情况下，置乱后的平均移动距离即为图像中任意两点的距离的数学期望。即

$$\bar{l}=E(l)=(\sum_{i=0}^{255}\sum_{j=0}^{255}(\sum_{i'=0}^{255}\sum_{j'=0}^{255}\sqrt{(i'-i)^2+(j'-j)^2}))/256^4=133.4788$$

从模拟实验测试得到的图像置乱后的平均移动距离的结果可以看出，每次置乱之后像素点的平均移动距离均非常接近期望值 133.4788。由此说明，本文提出的置乱算法具有良好的随机性和保密性，能很好地抵抗分析统计。

5.3 置乱后的自然序

所谓自然序，即在原图像中相邻的像素点，置乱之后虽然它们在图像中的坐标发生了变化，但它们却仍然相邻，即它们的相对位置未发生变化，则称之为自然序。从加密的角度来讲，自然序数目越少，置乱的效果就越好，保密性能也就越高，反之，自然序数目越多，性能越差。

表 3 是随机选取 1000 个初值 k_0，运用本文描述的置乱算法对 256×256pixels 大小的灰度图像 lena、bmp 进行加密，用 matlab 模拟图像置乱实验测试，分别以 2×2pixels，3×3pixels 为分块大小统计得到的图像自然序统计分析的结果。

表 3 用置乱算法加密后图像自然序统计结果

	平均值	最大值	最小值
2×2 自然序数	0.0050	3	0
3×3 自然序数	0	0	0

从表 3 可见，以 2×2pixels 为分块大小的自然序最大值为 3，而平均值仅仅为 0.005，即说明每次加密在 2×2pixels 大小范围内自然序极少；而以 3×3pixels 为分块大小的自然序均为 0，则说明在长与宽都大于或等于 3pixels 大小的分块下，图像的自然序均将肯定为 0，实验结果证明此算法在自然序上具有良好的统计特性。

5.4 置乱后行、列的汉明相关性

序列 $X=\{x_0,x_1,\cdots,x_{n-1}\}$，$Y=\{y_0,y_1,\cdots,y_{n-1}\}$，则 X，Y 之间的汉明相关函数[10]为：

$$H_{XY}(\tau)=\sum_{i=0}^{n-1}h(x_i,y_{(i+\tau)\bmod n}),0<\tau<n-1$$

其中 $h(x_i,y_{(i+\tau)\bmod n})=\begin{cases}1,x_i=y_{(i+n)\bmod n}\\0,x_i\neq y_{(i+\tau)\bmod n}\end{cases}$

根据定义，在 X 序列中的一个序列值在 Y 序列中与其相等的值的数目的平均值为 $H_{XY}(\tau)/n$。汉明相关就描述了序列 X 与序列 Y 的相似程度，即汉明相关值越大，两个序列 X，Y 的相似度越高。对加密图像，可分别按行序和列序统计任意行和任意列的汉明相关特性，若汉明相关值越高，说明行相似性越低，置乱效果越好，保密性能也就越高。反之汉明相关值越高，性能越差。

表 4 是随机选取 1000 个初值 k_0，运用本文描述的置乱算法对 256×256pixels 大小的灰度图像 lena.bmp 进行加密，用 matlab 模拟图像置乱实验测试，得到的图像任意两行和任意两列的汉明相关值的平均值 $H_{XY}(\tau)/n$ 统计分析的结果。

表 4 用置乱算法加密后汉明相关的统计结果

	平均值	最大值	最小值
任意两行 $H_{XY}(\tau)/n$	0.7968	0.8026	0.7918
任意两列 $H_{XY}(\tau)/n$	0.7974	0.8021	0.7942

从表 4 可见，任意一个像素点，在除自身所在的行和列以外的任意行或列中，与其像素值相同的点的个数约 0.8 个，说明行间、列间的汉明相关度非常低。

5.5 时间复杂度分析

从算法分析，生成矩阵 $D1(i,j)$，$D2(i,j)$，$A1(i,j)$，$O1(i,j)$，$A2(i,j)$，$O2(i,j)$ 时 Logistic 映射迭代次数为 $10000+6mn$ 次；加密与解密的过程分别遍历了每个像素点 2 次，遍历过程中每个像素点都和另外的某个像素点对换（temp=I(i,j)；I(i,j)=I(p,q)；I(p,q)=temp），每次对换计算 3 次，总共运算次数为 $2\times3mn$。故算法在时间复杂度上的度量为 $O(n^2)$。

对 256×256pixels 大小的灰度图像 lena.bmp 进行加密，从模拟实验测试得到的加密平均时间约为 2～3s，具有很快的加密速度。

结束语 本文在混沌系统良好的密码学特性基础上，提出了一种针对像素点对换的数字图像置乱算法。算法中，对换规则中的关键矩阵 D,A,O 均由 Logistic 映射产生，这很好地增加了算法对混沌映射初始值的依赖，使得初值敏感性提高，加密的复杂度成倍提高，用穷举法攻击几乎不可实现，难于破解；算法具有很好的安全保密性能和足够大的密钥空间；从加密时间来看，本算法下的图像加密速度快，能很好地满足加密需要。通过反复测试与分析，本文所述算法下的图像置乱加密具有加密快、安全性高等众多特点，具有很好的加密表现。

参 考 文 献

[1] Wu M, Liu B. Data hiding in image and video: Part I—Fundamental issues and solutions [J]. IEEE Trans On Image Processing, 2003, 12(6): 685-694

[2] 李昌刚，韩正之，张浩然. 图像加密技术综述[J]. 计算机研究与发展，2002，39(10)：1317-1324

[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)：338-340

[4] 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

[5] 李国富. 基于正交拉丁方的数字图像置乱方法[J]. 北方工业大学学报，2001，13(1)：14-16

[6] 柏森，曹长修，曹龙汉. 基于骑士巡游变换的图像细节隐藏技术[J]. 中国图像图形学报，2001，6(11)：1096-1100

[7] Dachselt F, Schwarz W. Chaos and Cryptography [J]. IEEE Trans Circuits Syst I, 2001, 48(12): 1498-1509

[8] Li Shujun, Mou Xuanqin, Cai Yuanlong. Improving security of a chaotic encryption approach[J]. Physics Letters A, 2001, 290(11): 127-133

[9] 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]. 中国图象图形学报，2005，10(5)：656-660

[10] 凌聪，孙松庚. 用于跳频码分多址通信的混沌跳频序列[J]. 电子学报，1999，27(1)：67-69