文章编号:1671-4598(2014)07-2157-03　　中图分类号:TP391　　文献标识码:A

基于改进 Logistic 混沌映射的数字图像加密算法研究

徐　兵[1]，袁　立[2]
(1. 重庆三峡学院，重庆　404000；2. 重庆师范大学 计算机与信息科学学院，重庆　401331)

摘要：混沌序列具有伪随机性、遍历性、对初始条件极其敏感性以及具备白噪声的统计特性等特点；文章利用 Logistic 混沌映射的改进算法产生的混沌序列所具有的这些特性，对数字图像进行空域像素进行位置置乱，然后对置乱后的图像序列按照一定的方法进行异或处理得到加密图像；实验在图像的竖直、水平、对角线方向，随机选择像素点，利用其灰度值，图像像素个数，计算数学期望，方差，协方差，相关系数；结果表明文章算法扰乱了图像像素间的相关性，使得加密图像能够抵抗明文统计的攻击，且密钥空间大，运算速度快，具有非常好的加密效果。

关键词：数字图像加密；Logistic 映射；混沌序列；置乱；异或

Research on Image Encryption Algorithm Logistic Chaotic Based on an Improved Digital Mapping

Xu Bing[1]，Yuan Li[2]
(1. Chongqing Three Gorges University，Chongqing　404000，China；
2. College of Computer and Information Science，Chongqing Normal University，Chongqing　401331，China)

Abstract：Chaotic sequence has a pseudo—random ergodic，which is extremely sensitive to initial conditions as well as with the statistical properties of white noise characteristics. This paper use the characteristics of the improved algorithm Logistic chaotic map chaotic sequence generated by these characteristics，making airspace pixels for digital image and scrambling for position，and then getting the scrambling image sequence according to a certain method or process which is encrypted exclusive image. Experiments on image vertical，horizontal，diagonal，randomly selecting pixel，using the gray value，image pixel number，and calculating mathematical expectation，variance，covariance，correlation coefficient. Results showing that：the proposed algorithm disrupts the correlation between the image pixels，which made the encrypted image can resist plaintext attack statistics，and the key space is large with a fast operation speed，also with a very good effect of encryption.

Keywords：digital image encryption；logistic map；chaotic sequence；scrambling；XOR

0　引言

数字图像通常以二维序列来表示，它要比文本文件大得多，并且数字图像由于人类视觉系统的特性往往允许图像的内容有缺损。用传统的加密技术对数字图像这样的大数据进行加密，其加密时间会很长、安全性低、效果不理想，有很大的局限性。图像加密的基本思想是对原始图像信息进行混淆，可分为置乱图像位置的加密方式[3]、置乱图像像素值的加密方式[4]和两者相互结合的加密方式[5-6]。

近年来，混沌理论以其对初值极其敏感性、伪随机、非线性等特性受到人们的广泛研究和应用，用混沌理论的方法来加密数字图像已成为一个很热的研究方向[1-12]。

本文提出一种基于 Logistic 混沌映射的数字图像加密新算法，首先该文利用 Logistic 混沌映射的改进算法产生的混沌序列对数字图像进行空域像素进行位置置乱，然后对置乱后的图像序列按照一定的方法进行异或处理得到加密图像。通过实验证明，该加密算法具有极好的加密性能。

收稿日期:2014-03-13；　**修回日期**:2014-04-21。
基金项目:重庆市教育委员会科学基金资助项目(KJ131115)。
作者简介:徐　兵(1976-)，男，重庆垫江人，硕士，副教授，主要从事计算机网络、计算机应用、数据挖掘方向的研究。

1　混沌系统

1.1　Logistic 混沌系统算法

混沌现象指的是在非线性动力系统中出现的类似随机的过程。这种过程具有无周期性，不收敛和对初始值极其敏感的特性[7]。混沌是非线性动力系统的固有特性，是非线性系统普遍存在的现象。从时域上看，混沌映射得到的序列很像随机序列，之间的相关性较弱，具备白噪声的统计特性，则可以用来产生伪随机码。原理上只要将迭代次数增加，伪随机码的周期能够很长，这样可以十分简单的产生长码。由于上述特点，混沌加密技术被应用于图像加密当中。目前，用于图像加密的混沌系统大致有 3 种：一维的 Logistic 映射[9]，二维的 Henon 映射[5,8]，三维的 Lorenz 映射[6]。Logistic 映射是一个很简单但是具有重要意义的非线性迭代方程。它能产生完全随机的、对初值和参量 μ 的动态变化非常敏感的随机序列。其方程如下：

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

其中：x_n 为映射变量，u 为分枝参数（系统混沌参数），它们的取值范围分别为：$0<x_n<1$，$0<u\leqslant 4$。当 $0<u<3.569\,945\,972\ldots$ 时，该系统因从稳定状态到分叉而产生倍周期，$3.569\,945\,972\ldots<u\leqslant 4$ 时，该系统进入混沌状态。混沌动力学的研究表明，即使 Logistic 映射处于混沌状态，其区域情况也相当复杂，因此使用 Logistic 映射置乱图像效果很好。由于能使

Logistic映射进入混沌状态时的 u 在范围 3.569 945 972... $< u \leqslant 4$ 内，且 u 的值取为4，即混沌迭代方程为 $x_{n+1}=4x_n(1-x_n)$ 时，能产生最佳混沌效果。但是这样参数 u 就为常数，失去了一定的加密安全性，为此可以用一个值域上限和值域下限都接近4的表达式代替式（1）中的系统参数（分枝参数）u。这样通过改进的Logistic映射既能产生极佳的混沌效果，又由于参数的在不停的无周期性的变化，能进一步增加加密图像的安全性，使加密后的图像更加不易被破解。基于上述思想，将Logistic映射方程改进为如下方程：

$$x_{n+1}=\left[3.569\ 945\ 973+(4-3.569\ 945\ 973)*\sin\left(\frac{\pi}{2}x_n\right)\right]x_n(1-x_n) \tag{2}$$

其中：x_n 为映射变量，在正弦中表示弧度，x_n 的取值范围为：$0<x_n<1$。以下证明函数

$$y=3.569\ 945\ 973+(4-3.569\ 945\ 973)*\sin\left(\frac{\pi}{2}x\right) \tag{3}$$

自变量 x 的取值范围为 $0<x<1$ 时，y 的值域范围为 $3.569\ 945\ 973<y<4$。

对式（1）进行一定变化后来可得Logistic映射的另一种表达形式，如下所示：

$$x_{n+1}=1-vx_n^2 \tag{4}$$

其中：x_n 为映射变量，v 为映射参量，x_n 和 v 的取值范围分别为：$-1<x_n<1$，$0<v\leqslant 2$。根据式（4）可知，当 $x\in(0,1)$ 时，函数 $y=\left|1-\frac{2}{2-x}x^2\right|$ 的值域为 $[0,1)$。

通过计算当 $x=\frac{\sqrt{17}-1}{4}$ 时，$y=\left|1-\frac{2}{2-x}x^2\right|=0$。可以用如下式（5）对初始值进行处理，使得图像加密效果更佳，能够增大破解的难度。

$$x_{n+1}=\left|1-\frac{2}{2-x_n}x_n^2\right| \tag{5}$$

x_n 取值范围为：$0<x_n<1$。由于当 $x=\frac{\sqrt{17}-1}{4}$ 时，$y=\left|1-\frac{2}{2-x}x^2\right|=0$。如果初始值为 $\frac{\sqrt{17}-1}{4}$ 或者在对初始值处理过程中出现 x_n $\frac{\sqrt{17}-1}{4}$，那么采用 $x_n=\frac{\sqrt{17}-1}{4}+0.01*\frac{\sqrt{17}-1}{4}$ 处理后继续用式（5）进行初始值处理。

1.2 基于改进的Logistic混沌映射算法

1.2.1 算法原理

首先根据式（5）将初始值进行迭代 S 次处理。接着将处理后的初始值 x_0^* 根据式（3）进行迭代，迭代次数为需要加密的图像像素大小，生成混沌序列。然后将生成的混沌序列整数化，使之生成置乱矩阵 $\boldsymbol{I}$。最后对矩阵 $\boldsymbol{I}$ 进行按位行异或处理，生成加密图像。

1.2.2 具体算法描述

数字图像相邻像素间的相关性非常强，而相关性强的加密图像是很容易被破解的，为此在对数字图像加密时要扰乱像素间的高度相关性。设原始图像为 I，大小为 $M*N$，各像素灰度值为 $I(i,j)$，$i=0,1,\cdots,M-1$，$j=0,1,\cdots,N-1$；标志数组 flag[]，元素个数为 $M*N$，初始值全为0。mod(x,y) 表示 x 对 y 取余，round(x) 是取靠近 x 的整数。图像的加密过程具体如下：

步骤1：根据式（5）将初始值 x_0^* 迭代 S 次后得到处理后的初始值 x_0。如果初始值为 $\frac{\sqrt{17}-1}{4}$ 或者在对初始值处理过程中出现 $x_n=\frac{\sqrt{17}-1}{4}$，那么采用 $x_n=\frac{\sqrt{17}-1}{4}+0.01*\frac{\sqrt{17}-1}{4}$ 处理后继续用式（5）进行初始值处理。

步骤2：根据式（3）将 x_0 迭代300次后所得的值赋给 x_0。

步骤3：根据式（3）将 x_0 迭代一次得到 x_1，对 x_1 做 $round(x_1*M*N)$ 处理得到 V。如果 $flag[V]=0$，进行步骤3操作；如果 $flag[V]=1$，进行步骤4操作后，如果 $flag[V]=0$，进行步骤3操作；如果 $flag[V]=1$，重复进行步骤4和步骤3操作。

步骤4：对 V 做如下处理：

$$\begin{cases} n=\mathrm{mod}(V,N) \\ m=round(\frac{V}{M}) \\ flag[V]=1 \end{cases} \tag{6}$$

很明显，$m\in[0,M-1]$，$n\in[0,N-1]$。

步骤5：根据式（3）将 x_1 迭代一次得到 x_2；根据公式 $v=round(x_2*M*N)$ 得到 V。

步骤6：用 m 和 n 作为置乱矩阵的行地址和列地址，对原始图像进行位置置乱。(m,n) 表示原始图像像素点 (i,j) 经过位置置乱后的坐标值，$I(i,j)$ 对应置乱后图像的像素点 $I(m,n)$，即 $I(m,n)=I(i,j)$。

步骤7：重复 $M*N$ 次步骤2和步骤7，最后得到置乱后的加密图像为 $I(m,n)$，$m=0,1,\cdots,M-1$，$n=0,1,\cdots,N-1$，其图像矩阵为 $\boldsymbol{G}$。

步骤8：将图像矩阵 $\boldsymbol{G}$ 的奇数行中的元素与偶数行中在同一列的元素按位异或后放入对应的奇数行。如果总行数为奇数，则最后一行不做任何操作。这样得到的矩阵记为矩阵 $\boldsymbol{H}$。

步骤9：将矩阵 $\boldsymbol{H}$ 的奇数列中的元素与偶数列中在同一行的元素按位异或后放入对应的奇数列。如果总列数为奇数，则最后一列不做任何操作。这样得到的矩阵记为矩阵 $\boldsymbol{L}$，通过矩阵 $\boldsymbol{L}$ 得到最终加密图像。

图像解密算法是图像加密算法的逆过程，加密算法是先进行像素位置置乱后进行像素值替换；解密算法只需要输入正确的初始值 x_0^*、初始迭代次数S，利用式（3）、式（5）和式（6）先进行像素值替换后进行像素位置置乱。按照这样的解密操作即可解密出原始图像 I。

2 实验结果与分析

实验选取大小为 $256*256$ 的经典Lena图像作为实验图片进行了仿真实验。实验采用Matlab7.0作为仿真实验软件。

2.1 直方图分析

Lena原图像如图1所示。Lena原图像直方图如图2所示。实验中选取混沌映射的初始值为 $x_0^*=0.479\ 322\ 222\ 222\ 222$，初始迭代次数 $S=5\ 000$，加密图像如图3所示，其加密图像直方图如图4所示。通过图2和图4对比可以看出，原始Lena图像对的灰度直方图分布不均，而通过本文算法加密后图像灰度直方图分布均匀，这可以有效地抵抗已知密文攻击与统计攻击。

图 1　Lena 原始图像

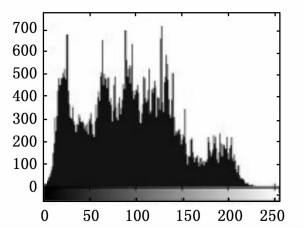

图 2　Lena 图像直方图

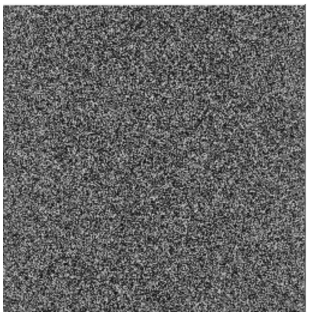

图 3　Lena 加密图像

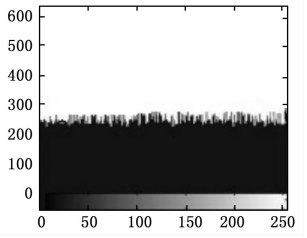

图 4　Lena 加密图像直方图

2.2　密钥敏感性实验

该文加密算法的密钥由 2 个参数组成即初始值 x_0^* 和初始迭代次数 S，加密过程的 2 个参数可以生成各种混沌序列，具有很好加密效果。对图 3 所示的加密图像使用正确解密密钥后的图像如图 5 所示。实验选取 x_0^* ＝0.479 322 222 222 223，初始迭代次数 S＝5 000，即使初始迭代次数 S 正确，但初始值相差 0.000 000 000 000 001 也不能解密出正确图像，解密效果如图 6 所示。实验选取 x_0^* ＝0.479 322 222 222 222，初始迭代 S＝5 001 次，即初始值正确，初始迭代次数相差一次也不能解密出正确图像。我们选取 x_0^* ＝0.479 322 222 222 223，初始迭代 S＝5001 次。这说明采用该加密方法的密图可以完全依赖密钥而不依赖于算法，其加密效果很好，能够很好的抵抗明文统计的攻击。

图 5　正确解密图像图

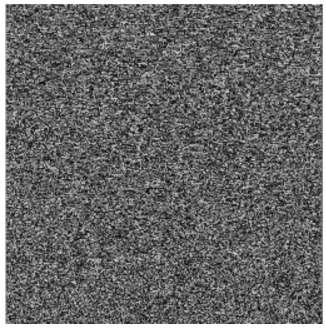

图 6　错误初始值解密图像

2.3　相邻像素点的相关性

实验在图像的竖直、水平、对角线方向上随机选择 3 000 对相邻的像素点，进行了相关性分析。加密图像与原始图像相比加密图像相邻元素的灰度值相差越大，表明它的相关性越小，从而加密效果也就越好，作为一个图像加密的衡量指标，用式（7）～（10）能够计算相关系数。

$$E(x)=\frac{1}{K}\sum_{i=1}^{K}x_i \tag{7}$$

$$D(x)=\frac{1}{K}\sum_{i=1}^{N}(x_i-E(x_i))^2 \tag{8}$$

$$\mathrm{cov}(x,y)=\frac{1}{K}\sum_{i=1}^{N}(x_i-E(x_i))(y_i-E(y_i)) \tag{9}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

其中：x 和 y 表示图像像素的灰度值；k 表示图像像素个数；E（x）表示 x 的数学期望；D（x）表示 x 的方差；cov（x，y）表示 x，y 的协方差；r_{xy} 表示相关系数。能够看出，Lena 原始图像的相邻像素的相关性是极高的，相关系数接近于 1，而加密图像的相邻像素相关性非常小，相关系数接近 0，说明原始图像的统计特性已被很好的扩散到随机的加密图像中。

3　结束语

由于计算机网络传递信息方便和快捷，因此越来越多的数字图像信息通过网络来传输。但是，传输的信息可能被非法浏览、查看、篡改、破坏等。为了防止这些事情的发生，计算机信息安全技术已经成为一个重要发展方向，保证数字图像储存和传输安全已经成为计算机信息安全的一个重要课题。该文将混沌系统理论引入数字图像加密算法中，充分利用混沌系统具有运算速度快、初始条件的敏感性和具备白噪声的统计特性等很多特性，对图像置乱算法进行了改进，方法简单易行，可靠性和保密性很高。通过实验分析表明，本文算法对明文和密钥均极端敏感，且密钥空间大，用于数字图像加密，能取得非常好的加密效果。

参考文献：

[1] 文昌辞，王　沁，苗晓宁，等. 数字图像加密综述 [J]. 计算机科学，2012，39 (12)：6－9.

[2] 王琳娟. 基于 Logistic 映射的多重图像加密技术 [J]. 科学技术与工程，2011，11 (2)：1818－1821.

[3] 樊春霞，姜长生. 基于标准混沌映射的图像加密/解密算法 [J]. 哈尔滨工业大学学报，2006，38 (1)：119－122.

[4] 贺　超，赵春喜. 基于混沌的图像加密隐藏方法 [J]. 长春理工大学学报，2008，31 (2)：115－117.

[5] 郑　凡，田小建，范文华，等. 基于 Henon 映射的数字图像加密 [J]. 北京邮电大学学报，2008，31 (1)：66－70.

[6] 卢辉斌，刘海莺. 基于耦合混沌系统的彩色图像加密算法 [J]. 计算机应用，2010，30 (7)：1812－1817.

[7] 张云鹏，左　飞，翟正军. 基于混沌的数字图像加密综述 [J]. 计算机工程与设计，2011，32 (2)：463－465.

[8] 张　瀚，王秀峰，李朝晖. 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)：2137－2141.

[9] Zhang J. Image encryption scheme based on cat map and Lu chaotic map [J]. Chinese Journal of Electron Devices，2007，30 (1)：155－157.

[10] Zhu C X. New image encryption algorithm based on combined multidimensional chaotic systems [J]. Computer Engineering，2007，33 (2)：142－144.

[11] 张定会，许赛赛，等. 彩色数字图像的小波变换和混沌序列加密 [J]. 计算机测量与控制，2011，19 (6)，1417－1419.

[12] 江　平，张定会. 彩色数字图像的超混沌 Lorenz 系统加密 [J]. 计算机测量与控制，2013，21 (3)，782－784.