计算 Arnold 变换周期的新算法

孙燮华[1],章仁江[2]
(1.中国计量学院 计算机系,浙江 杭州 310018;
2.中国计量学院 数学系,浙江 杭州 310018)

摘 要:Arnold 变换的周期在图像置乱、图像水印和信息隐藏中具有重要的应用。为了更有效地进行图像置乱等操作,同时,为了进行 Arnold 变换在图像置乱等安全性的研究,需要更深入和全面地研究 Arnold 变换的周期及其规律性。为寻找更快地计算 Arnold 变换周期的新算法,应用迭代 Arnold 变换矩阵与 Fibonacci 序列之间的关系,建立了通过 Fibonacci 数特征计算 Arnold 周期的定理。根据该定理,提出了快速计算 Arnold 变换周期的新算法。实验结果表明,新算法与原算法相比在计算 Arnold 变换周期方面,速度有了很大提高。因此,新算法适用于快速计算 Arnold 变换的周期和用于图像置乱等操作。另一方面,所建立的定理在理论上也是有价值的。

关键词:Arnold 变换;Fibonacci 序列;周期
中图分类号:TN919.31 **文献标识码**:A **文章编号**:1673-629X(2008)11-0066-03

A New Algorithm for Calculating Period of Arnold Transformation

SUN Xie-hua[1], ZHANG Ren-jiang[2]
(1. Department of Computer, China Jiliang University, Hangzhou 310018, China;
2. Department of Mathematics, China Jiliang University, Hangzhou 310018, China)

Abstract: The period of Arnold transformation has some important applications in image scrambling, watermarking and information covering. In order to process image scrambling etc. more efficiently, meanwhile, to research the security of image scrambling using Arnold transformation, the period and its rules need to be studied deeply. The aim of this paper is to find new fast algorithm computing period of Arnold transformation. Using the relationship between iterative Arnold transformation matrix and Fibonacci sequence, a theorem for finding period of Arnold transformation matrix from the characteristics of Fibonacci numbers is established. According to this theorem, a new algorithm for fast computing the period of Arnold transformation is proposed. The results of experiments show that the new algorithm for calculating the period is much faster than old algorithms. Hence, the new algorithm is very useful for fast computing periods of Arnold transformations. On the other hand, the established theorem is valuable in theory.

Key words: Arnold transformation; Fibonacci sequence; period

在一幅灰度数字图像中,各点的灰度值是其坐标 (x, y) 的函数 $f(x,y)$。因此,一幅数字图像对应一个图像矩阵,矩阵的每个元素所在的行与列就是图像显示在屏幕上诸像素点的坐标,元素的数值就是该像素的灰度值。近年来,许多基于几何变换的置乱方法被提出并得到应用,Arnold 变换就是其中的一种基于像素几何位置变换的置乱方法。20 世纪 90 年代末,齐东旭等人[1]对 Arnold 变换及其在图像信息隐蔽和图像置乱技术中的应用作了大量的工作。例如齐东旭、邹建成等人给出了矩阵变换模周期存在的条件,研究了 Fibonacci-Q 矩阵变换的周期和 Arnold 变换周期之间的关系等,文献[2~5]研究了 Arnold 变换的周期性及计算 Arnold 变换的最小周期的算法。但是到目前为止,人们仍然没有很好地解决快速、有效地计算 Arnold 的周期等问题[5]。

文中进一步研究了 Arnold 变换周期的性质。给出计算 Arnold 变换周期的新算法,实验结果表明该算法优于已有的一些算法。

收稿日期:2008-03-08
基金项目:浙江省自然科学基金资助项目(Y607034)
作者简介:孙燮华(1945-),男,浙江嘉兴人,教授,CCF 会员,研究领域为图形与图像处理,模式识别,算法分析。

1 关于 Arnold 变换

二维 Arnold 变换是 V.I. Arnold 在研究环面上的

自同态时所提出的。设 M 是光滑流形环面 $\{(x, y)\bmod 1\}$。M 上的一个自同态 φ 定义如下:

$$\varphi(x,y) = (x + y, x + 2y)(\bmod 1)$$

这里(mod 1)表示单位正方形区域($0 \leqslant x, y \leqslant 1$)上的模 1 运算。显然,映射 φ 导出覆盖平面(x,y)上的一个线性映射,其变换矩阵是 $\bar{\varphi} = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$。将这种变换应用于正方数字图像 NXN,可以引入关于数字图像 Arnold 变换的概念。

定义 1　设$(x,y)^{\mathrm{T}}$为正方数字图像 NXN 上的点,称将点$(x,y)^{\mathrm{T}}$变到另一幅图像上点$(x',y')^{\mathrm{T}}$的变换

$$\begin{pmatrix}x'\\ y'\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} \quad (\bmod N) \qquad (1)$$

为二维 Arnold 变换,简称 Arnold 变换,其中,$x, y \in \{0, 1, \cdots, N-1\}$

称 $\boldsymbol{A} = \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$为 Arnold 变换矩阵,$N$ 为数字图像矩阵的阶。

将 Arnold 变换应用在数字图像上,可以通过像素坐标的改变而改变图像灰度值的布局,经 Arnold 变换后的图像会变得"混乱不堪",这就是图像置乱的概念,参见图 1。

对置乱的图像继续使用 Arnold 变换,一定会出现一幅与原图相同的图像,这就是 Arnold 变换周期的概念。

定义 2　设数字图像矩阵 $\boldsymbol{P} = (P_n)$ 的阶为 N,$\boldsymbol{P}$ 有 N^2 个元素。对给定的正整数 N,Arnold 变换周期 m_N 是指使得图像矩阵 $\boldsymbol{P}$ 经一系列 Arnold 变换后回复到 $\boldsymbol{P}$ 的最小自然数。

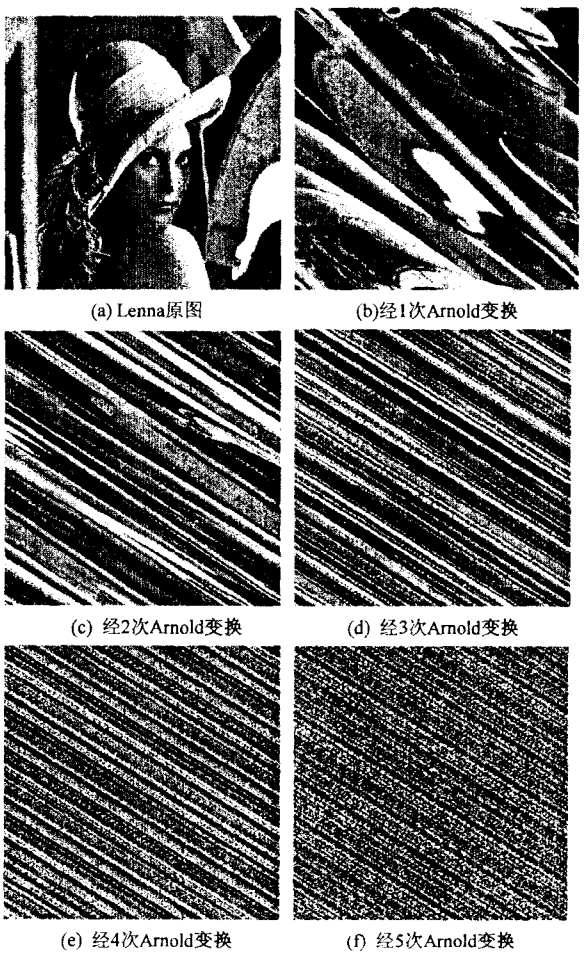
设点$(x_1,y_1)^{\mathrm{T}}$经一次 Arnold 变换变到点$(x_2, y_2)^{\mathrm{T}}$,再经一次 Arnold 变换变到点$(x_3,y_3)^{\mathrm{T}}$,以此类推,如果当变换到点$(x_m,y_m)^{\mathrm{T}}$时,再经一次 Arnold 变换又回到点$(x_1,y_1)^{\mathrm{T}}$。称这 m 个点$(x_i,y_i)^{\mathrm{T}}(i = 1,2, \cdots, m)$构成模 N 下 Arnold 变换的一个 m - 轨道,用记号$\{(x_1,y_1)^{\mathrm{T}},(x_2,y_2)^{\mathrm{T}},\cdots,(x_m,y_m)^{\mathrm{T}}\}$表示,并称 m 为该 m - 轨道的长度。

对于给定的自然数 N,Arnold 变换的周期实际上就是图像矩阵 $\boldsymbol{P}$ 中 N^2 个点$(x,y)^{\mathrm{T}}$所在的所有轨道长度的最小公倍数。

F. J. Dyson 和 H. Falk 证明了关于 Arnold 变换的周期估计定理。

定理 A　对于给定的正整数 N,当 $N > 2$ 时,周期 m_N 满足不等式

$$m_N \leqslant N^2/2$$



(a) Lenna原图　(b)经1次Arnold变换　(c) 经2次Arnold变换　(d) 经3次Arnold变换　(e) 经4次Arnold变换　(f) 经5次Arnold变换

图 1　Lenna 图的各次 Arnold 置乱

表 1 给出了模 N 的 Arnold 变换的各个周期。

表 1　不同阶数 N 下 Arnold 变换周期

N	2	3	4	5	6	7	8	9	10	11	12
m_N	3	4	3	10	12	8	6	12	30	5	12
N	13	14	15	16	17	18	19	20	21	22	23
m_N	14	24	20	12	18	12	9	30	8	15	24
N	25	50	60	100	120	125	128	256	480	512	1024
m_N	50	150	60	150	60	250	96	192	120	384	768

2　计算 Arnold 变换周期的算法

定理 B[2]　对于给定的自然数 $N > 2$,Arnold 变换(1.1)的周期 m_N 即为数字矩阵 $\boldsymbol{P}$ 中元素(1,1)所属轨道的长度,即 m_N 是使下式成立的最小自然数 n:

$$\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}^n = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad (\bmod N) \qquad (2)$$

根据定理 B,用 Matlab 的编程语言,算法的主要部分代码如下:

```
n=1;
x=1;y=1;
%tic %计时开始
flag=0;
while flag==0
```

```
  xn=x+y;
  yn=x+2*y;
    if (mod(xn,N)==1 & mod(yn,N)==1)
      Period=n;
      flag=1;
  end
  x=mod(xn,N);
  y=mod(yn,N);
  n=n+1;
end
%toc %计时开始
```

3 计算 Arnold 变换周期的新算法

称 $f_1=1, f_2=1, f_{n+2}=f_{n+1}+f_n$ 为 Fibonacci 序列。下面的定理给出了 Arnold 变换与 Fibonacci 序列的关系(参见文献[4])。

定理 3.1 对 n 次 Arnold 变换矩阵 $\boldsymbol{A}^n$,成立如下公式:

$$\boldsymbol{A}^n=\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}^n=\begin{pmatrix}f_{2n-1} & f_{2n}\\ f_{2n} & f_{2n+1}\end{pmatrix}(n=1,2,\cdots) \tag{3}$$

下面是文中的定理。

定理 3.2 Arnold 变换的周期 m_N 等于 Fibonacci 序列中第 1 次出现

$$f_{2n-1}=1, f_{2n}=0(\mathrm{mod}\ N) \tag{4}$$

时的 n。

证明:由式(2)和(3)得

$$\begin{pmatrix}f_{2n-1} & f_{2n}\\ f_{2n} & f_{2n+1}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}(\mathrm{mod}\ N) \tag{5}$$

应用定理 B,式(5)表明,Arnold 变换的周期 m_N 是 Fibonacci 序列中第 1 次出现

$$f_{2n-1}=1, f_{2n}=0, f_{2n+1}=1(\mathrm{mod}\ N)$$

时的 n。由

$$f_{2n+1}=f_{2n-1}+f_{2n}$$

可知,当式(4)成立时,必成立 $f_{2n+1}=1(\mathrm{mod}\ N)$ 由此证明了定理 3.2。

应用定理 3.2,得到计算 Arnold 变换周期的新算法。新算法与原算法的不同之处,在于新算法不用 Arnold 变换,仅仅通过取模的 Fibonacci 序列就能获得其周期,新算法不用语句

$$yn=x+2*y$$

从而大大地减少了乘法次数,提高了运算速度。

下面是用 Matlab 编写的源程序:

```
%ArnoldPeriod.m
%作者 孙燮华,2006.10.31
n=1;x=1;y=1;
%tic %计时开始
flag=0; %while 循环标志
while flag==0
  xn=x+y; %计算下一个 Fibonacci 数
  yn=y+xn; %计算下一个 Fibonacci 数
  xn_modN=mod(xn,N);
  yn_modN=mod(yn,N);
    if (xn_modN==1 & yn_modN==0)
    Period=n+1;
    flag=1; %while 循环结束
  end
  x=xn_modN;
  y=yn_modN;
  n=n+1;
end
%toc%计时结束
```

4 实验结果

下面是在同一台计算机上,相同运行环境下计算 Arnold 变换周期的速度比较。表 2 的数据表明,新算法比原算法的计算速度上有了很大的提高。

表 2 原算法与新算法的速度比较

(时间单位:秒)

N	256	1024	65536	100000	200000
原算法速度	0.01	0.02	0.611	0.841	1.612
新算法速度	0.00	0.00	0.030	0.050	0.120

5 结束语

文中使用了不同的思想方法,提出了快速计算 Arnold 变换周期的新算法。实验结果表明新算法比原算法在计算速度上有了很大的提高。该算法在研究 Arnold 变换周期中,不仅具有实用意义,而且在理论上也是有意义的。

参考文献:

[1] Qi Dongxu, Zou Jiancheng, Ha Xiaoyou. A new class of scrambling transformation and its application in the image information covering[J]. Science in China(Series E),2000,43(3):304-312.

[2] 邹建成,铁小匀.数字图像的二维 Arnold 变换及其周期性[J].北方工业大学学报,2000,12(1):1014-1032.

[3] 孙 伟.关于 Arnold 变换的周期性[J].北方工业大学学报,1999,11(1):29-32.

[4] 吴发恩,邹建成.数字图像二维 Arnold 变换周期的一组必要条件[J].北方交通大学学报,2001,25(6):66-69.

[5] 李 兵,徐家伟.Arnold 变换的周期及其应用[J].中山大学学报,2004,43(增 2):139-142.