Arnold 反变换的规范表达式及多维推广①

赵海英[1,2]　孙凤玉[3]　(1.北京科技大学 信息工程学院 北京 100083; 2. 新疆师范大学 数理学院 乌鲁木齐 830054; 3. 北京科技大学 应用科学学院 北京 100083)

摘　要: Arnold 变换具有周期性，广泛应用于图像加密方面，其正变换具有规范的表达式，但 Arnold 的反变换却没有一个规范表达式，因此论文提出一种 Arnold 反变换的规范表达式对各类 Arnold 正反变换进行形式上的统一，规整而简洁化，并在多维上进行推广。

关键词: Arnold 变换；周期性；规范表达式；多维推广

Arnold Inverse Transformation's Normative Expression and Multi-Dimension Extend

ZHAO Hai-Ying[1,2], SUN Feng-Yu[3] (1. School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China; 2. College of Maths-Physics and Information Sciences, Xinjiang Normal University Urumqi, China; 3. School of Applied Science, University of Science and Technology Beijing, China)

Abstract: The periodicity of the Arnold transformation is widely used in image encryption aspect. This transformation is provided with normative expression, but its inverse transformation does not. In this paper, a new normative expression which enable all kinds of Arnold transformation and its inverse transformation formally unify is proposed, in good order and concise, and extend it on multidimensional space as well..

Keywords: Arnold transformation; periodicity; normative expression; multi-dimension extend

Arnold 变换是 V.J. Arnold 在遍历理论的研究中提出的，将其应用在数字图像上，可通过像素坐标的改变而转换图像灰度值的布局，把数字图像看做一个矩阵，那么反复使用这种变换则使矩阵中的元素排列，“混乱不堪“，若将变换作用于图像，则会使图像变得”无法相认“，但是，随着迭代的进行，最终会出现一幅与原图像一模一样的图像，原因就在 Arnold 变换所具有性质，其变换具有一定的周期性。其周期性与图像的阶数有关，但并不成比例[1]。为了统一分析各类 Arnold 型变换的周期性，北方工业大学齐东旭教授的研究梯队给出了一系列的推广及应用[2-5]，然而 Arnold 型变换的时间和计算量较大，尤其在对变换中某一幅图像进行演化求周期，困难很大，促使我们去寻找 Arnold 的反变换，浙江大学的张涛博士给出了 Arnold 反变换的一种新算法，但没有给出 Arnold 反变换的规范表达式。

本论文基于 Arnold 正变换的表达，推证出了一套 Arnold 反变换的规范式，并对规范的反变换表达式进行了多维推广。

1　关于Arnold变换及其周期

Arnold 变换是 Arnold V.J 为了研究遍历理论而提出的一种非线性变换[5]。是一个迭代计算，假设我们的画面是一个单位正方形，(x,y)为该正方形上的点，将(x,y)变换到同一个正方形的另外一点(x',y')的变换。

① 基金项目:国家自然科学基金(60863010)资助和新疆自然科学基金项目(2010211a19)
收稿时间:2010-04-04;收到修改稿时间:2010-05-08

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod} \quad 1) \tag{1}$$

其中(mod 1)表示模 1 运算，式(1)就是 Arnold 变换。

对于 N 阶图像方阵来说，Arnold 变换的计算是按照(mod N)进行的，于是式(1)改写成如下的形式:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod} \quad N) \quad x, y \in \{0,1,2,\mathbf{L},N-1\} \tag{2}$$

注：称 A=$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ 为 Arnold 变换矩阵，N 为数字图像矩阵形式的阶数。

我们根据式(2)给出迭代公式:

$$P_{ij}^{n+1} = AP_{ij}^{n} (\text{mod} \ \ N) \quad n = 0,1,2,..... \tag{3}$$

其中

$$P_{ij}^{n} = (i,j)^{T}, i, j \in \{0,1,2,.....,N-1\} \tag{4}$$

式(3)，(4)中 P 的上标代表迭代次数

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灰度图像的灰度值布局。经 Arnold 变换后的图像会变的“混乱“，对混乱的图像继续迭代若干次后，一定会出现与原图像相同的一幅图像，这个过程就反映出 Arnold 变换具有周期的特性。式(2)给出了点的位置变化，当计算出新点P_{ij}^{n+1}之后，立即将原P_{ij}^{n}处的信息(灰色，颜色，饱和度)移植过来，在遍历了原来图像的所有点之后，下一副新的图像就生成了。

2 Arnold反变换的算法推导过程

Arnold 变换的定义为(2)其中(x,y)原图像的像素点，坐标位置(x', y')是变换后新图像的像素点位置，N 是图像阶数。

下面推导正方形图像(N×N)Arnold 反变换的规范定义表达式其中和 N 是已知，(x,y)是未知的量。由(2)可得:

$$\begin{cases} x' = (x + y)(\text{mod} \quad x) \\ y' = (x + 2y)(\text{mod} \quad N) \end{cases} \tag{5}$$

即存在$\exists p, q \in z$ (z 为整数)s.t.

$$\begin{cases} x + y = np + x' \\ x + 2y = nq + y' \end{cases} \tag{6}$$

并且有:

$0 \leqslant x, y, x', y' \leqslant N-1$ (7)

由(7)可知:

$$\begin{cases} 0 \le x + y \le 2N - 2 \\ 0 \le x + 2y \le 3N - 3 \end{cases} \tag{8}$$

由(7)、(8)及不等式性质，有:

$$\begin{cases} 0 \le x + y - x' \le 2N - 2 \\ 0 \le x + 2y - y' \le 3N - 3 \end{cases} \tag{9}$$

即:

$$\begin{cases} 0 \le Np \le 2N - 2 \\ 0 \le Nq \le 3N - 3 \end{cases} \tag{10}$$

所以 P 只能取 0 和 1，而 q 只能取 0，1，2 下面我们充分利用条件来具体确定 p 和 q 的值。

第 1 中情况:

当 p=0 时，由式(6)得$x + y = x'$，

所以 $0 \leqslant x + y = x' \leqslant N-1$,进一步由不等式性质和式(7)得到：$0 \leqslant x + y + y \leqslant 2N-2$ 又因为$x + 2y = Nq + y'$并且 $0 \leqslant y' \leqslant N-1$。

所以 q 只能取 0 和 1，不能取 2。所以得到两个方程组，它们分别是:

$$\begin{cases} x + y = x' \\ x + 2y = y' \end{cases} \tag{11}$$

$$\begin{cases} x + y = x' \\ x + y = N + y' \end{cases} \tag{12}$$

我们把(11)、(12)写成行列式形式可得

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{11*}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} + \begin{pmatrix} -N \\ N \end{pmatrix} \tag{12*}$$

第 2 种情况:

当 p=1 时，由式(6)得$x + y = N + x'$ 所以

$N \leqslant N + x' = x + y \leqslant 2N-1$

由(7)进一步得到，$N \leqslant x+y+y \leqslant 3N-2$

又因为$x + 2y = Nq + y'$且$0 \leqslant y' \leqslant N-1$,所以 q 只能取 1 和 2 不能取 0，因此又得到两个方程组，它们分别是:

$$\begin{cases} x + y = N + x' \\ x + 2y = N + y' \end{cases} \tag{13}$$

$$\begin{cases} x+y=N+x' \\ x+2y=2N+y' \end{cases} \quad (14)$$

我们把(13)、(14)写成行列式形式，可得：

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}+\begin{pmatrix} N \\ 0 \end{pmatrix} \quad (13^*)$$

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}+\begin{pmatrix} 0 \\ N \end{pmatrix} \quad (14^*)$$

所以两种情况解集的并(即$11^*\sim14^*$)就是所求的反变换我们可以发现$11^*\sim14^*$可归纳为：

$$\begin{pmatrix} x \\ y \end{pmatrix}=B\begin{pmatrix} x' \\ y' \end{pmatrix}+b$$

其中 $B=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$　$b=\begin{pmatrix} b^1 \\ b_2 \end{pmatrix}$

我们可以把($11^*\sim14^*$)写成一个通式：

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}(\text{mod}\quad N) \quad (15)$$

此式即为 Arnold 反变换规范定义，可以发现(15)式与(2)式$\begin{pmatrix} x' \\ y' \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}(\text{mod}\quad N)$极其相似，形式上完全一致，且$\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1}$因此，(15)就是我们给出的 Arnold 反变换的规范表达式。

3　实验验证

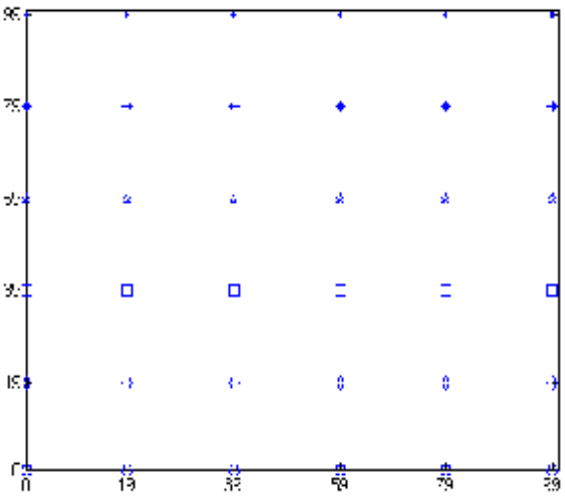

图 1　Arnold 变换前像素位置

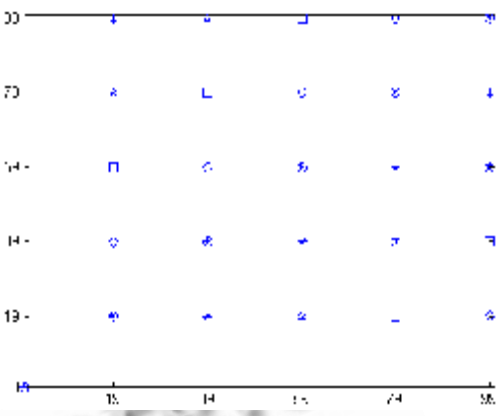

图 2　Arnold 变换后像素位置

在图 1 中我们以一个 100×100 大小图像为例(N=100),为了表示清楚我们把不同水平线上的一部分像素点用不同符号表示出来，从图 2 中可以看出经过 Arnold 变换之后这部分像素点位置的变化。

表 1　部分像素点的变换情况(变换前)

x'	0	19	39	59	79	99
y'	99	99	99	99	99	99

表 2　部分像素点变换情况(变换后)

x'	99	18	38	58	78	98
y'	98	17	37	57	77	97

4　Arnold反变换的推广

定义三维 Arnold 变换[7]形式如下：

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}(\text{mod}\quad N)$$

其中 (x,y,z) 是原三维图像的像素点，(x',y',z')是变换后新三维图像的像素点，N 是图像阶数。

可仿照(15)式得到

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{pmatrix}^{-1}=\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}=B$$

即：

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}(\text{mod}\quad N) \quad (*)$$

(下转第 136 页)

(上接第 224 页)

而如果按照以前的方法(张涛[6])只能得到 $\prod_{i=1}^{m} C_{\sum_{k=0}^{i-1}(m-k)}^{1}$ 方程，无法得到 Arnold 反变换多维规范定义式(*)。

5 小结

在图像置乱技术中，Arnold 变换具有良好特性，但由于 Arnold 变换的周期性与图像阶有关，其置乱的程度与 Arnold 的变换矩阵有关，对于一幅较大的置乱图像，若想利用其周期性来恢复原图，需要很长时间[7]。通过 Arnold 反变换可以对 Arnold 变换后的任意时刻图像进行恢复，但反变换解的并集很庞大、不规范，为了节省变换时间，统一变换形式提出一套 Arnold 反变换的规范表达式，降低了 Arnold 变换应用的难度，提高了人们对各类 Arnold 变换的理解和把握。最后又把二维 Arnold 反变换推广到三维反变换，并给出其规范表达式。

参考文献

1 Arnold VI, Avez A, Ergodic problems of clssical Mechanics, Mathematic physic monograph series. New York: Benjamin W.A. INC, 1968.

2 丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术. 计算机学报, 1998,21(9):838－843.

3 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藏中的应用.中国科学(E 辑), 2000,30(5):440－447.

4 赵慧. n 维 Arnold 变换及其周期性.北方工业大学学报, 2002,14(1):21－25.

5 齐东旭.分形及其计算机生成.北京:科学出版社, 1994.

6 张涛等. Arnold 反变换的一种新算法.软件学报, 2004,15(10):1558－1564.

7 QI DX, WANG DSH, YANG DL. Matrix transformation of disital image and its periodicity. Progress in Natural Science, 2001,11(7):542－549.