文章编号:1672 - 058X(2012)03 - 0016 - 06

Arnold 变换及其逆变换研究*

毛雷波
(重庆师范大学 数学学院,重庆 401331)

摘 要:Arnold 变换由于具有周期性,被广泛地应用于图像加密. 但在利用其周期性进行解密时,有时会比较费时,因此提出了一种 Arnold 逆变换算法;在此基础上,将其拓展到非方阵图像,即一般的矩形图像上,扩展了其在图像加密上的应用范围;最后在理论上将二维推广到 n 维 Arnold 变换及逆变换.

关键词:数字图像;图像置乱;置乱恢复;Arnold 变换;Arnold 逆变换
中图分类号:TP391 **文献标志码**:A

图像作为人类认识和描述世界的一种基本方法,应用非常广泛,从古老的壁画、象形文字到现代的数字化视频,图像一直伴随着人类历史的发展[1]. 但是随着计算机网络和多媒体技术的迅速发展,人们越来越多的在互联网上传输图像、视频等多媒体信息,开展如远程教学、网络办公等网络业务. 许多重要的图像信息也会在互联网上传播,如:病人病例、设计图纸、电子政务[2]、军事资料等,这些数据在网络传输时一旦被非法获取,则会泄露个人隐私,严重的甚至会影响国家安全,数字图像的安全保障问题日益凸显出来. 这些重要的图像数据在互联网上传播时必须要进行有效的加密[3],图像置乱技术作为图像信息的一种加密算法应运而生.

图像置乱就是把一幅给定的数字图像变成一幅杂乱无章的图像,这样其所要表达的真实信息就无法直观地得到,即使计算各种可能的组合也势必会花费巨大代价. 但如果知道了置乱的方法和所采用的参数即密钥,只要进行逆置乱变换,即可恢复原始图像. 因此,它既可以作为一种独立的图像加密技术,又可以用作数字图像水印、分存的预处理和后处理过程[4].

图像置乱主要有位置置乱和灰度置乱两种. 位置置乱即通过某种算法改变图像中各像素点的位置以达到图像加密的目的. 灰度置乱就是通过改变各个像素点的灰度值来实现图像的加密[5]. 目前常用的图像置乱方法有:Arnold 变换、幻方变换、分形 Hilbert 曲线、Tangram 算法、Conway 游戏、IFS 模型、Gray 码变换和广义 Gray 码变换、正交拉丁方、仿射变换、骑士巡游等. Arnold 变换由于算法简单、置乱效果显著且具有周期性,在图像信息隐藏方面得到了很好的应用.

收稿日期:2011 - 09 - 03;**修回日期**:2011 - 09 - 20.
* **基金项目**:重庆市自然科学基金(CSTC,2011BB2116).
作者简介:毛雷波(1986-),男,山西晋城人,硕士研究生,从事智能计算及模式识别研究.

1　Arnold 变换及其逆变换

1.1　Arnold 变换

Arnold 变换是 V. J. Arnold 在遍历理论的研究中提出的一种变换,俗称猫脸变换(Cat Mapping)[6,7],假设在平面上的单位正方形内绘制一个猫脸图像,通过如下变换:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\quad 1) \tag{1}$$

这个猫脸图像会由清晰变为模糊,这就是 Arnold 变换[1]. 但是当具体到数字图像上,需要将式(1)中的二维 Arnold 变换改写为[8]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\quad N) \quad x,y \in \{1,2,\cdots,N\} \tag{2}$$

其中,(x,y)是像素在原图像中的坐标,(x',y')是变换后该像素在新图像中的坐标,N 是图像矩阵的阶数,即图像的大小,一般指正方形图像.

当对一幅图像进行 Arnold 变换时,就是把图像的像素点位置按照公式(2)进行移动,得到一个相对原图像混乱的图像. 对一幅图像进行一次 Arnold 变换,就相当于对该图像进行了一次置乱. 通常这一过程需要反复迭代多次才能达到满意的效果.

利用 Arnold 变换对图像进行置乱,使有意义的数字图像变成象白噪声一样的无意义图像,实现了信息的初步隐藏,并且置乱次数可以为水印系统提供密钥,从而增强了系统的安全性和保密性.

1.2　Arnold 变换的周期性及置乱恢复

Arnold 变换可以看作是裁剪和拼接的过程,通过这一过程,将数字图像矩阵中的像素重新排列,达到置乱的目的. 由于离散数字图像是有限点集,对图像反复进行 Arnold 变换,迭代到一定步数时,必然会恢复原图,即 Arnold 变换具有周期性. 利用这一周期特性可以实现逆置乱,表 1 是在不同阶数 N 下 Arnold 变换的周期[9]. 可以观察得出,Arnold 变换的周期性与图像大小有关,但并不成正比.

表 1　不同阶数 N 下 Arnold 变换的周期 T_N

N	2	3	4	5	6	8	10	12	25	50	64	128	256	512
T_N	3	4	3	10	12	6	30	12	50	150	48	96	192	384

前面通过研究 Arnold 变换的周期性,已经得出了这样的结论:对于 $N \times N$ 的数字图像,只要满足 N 为非 1 正整数,其 Arnold 变换均具有周期. 用 T_N 代表 $N \times N$ 的数字图像的 Arnold 变换周期. 若要对一幅进行过 $t(t \in [1,T_N])$次 Arnold 置乱变换的数字图像进行恢复,只需对其继续进行$(T_N - t)$次 Arnold 置乱,即可得到与原图一模一样的图像;推广到任意置乱次数 n,则需要继续进行$(T_N - n \mathrm{mod} T_N)$次 Arnold 置乱变换.

简单举个例子,如图 1,对于 256 × 256 的 lena 数字图像,其置乱周期 $T_{256} = 192$,也就是说原图经过 192 次 Arnold 变换后会变回原图. 利用 Arnold 置乱的周期性,对 Arnold 置乱 50 次后的图像,只需再进行(192 − 50)次即 142 次 Arnold 变换,便可恢复出原图;对置乱 300 次后的图像,需要继续进行置乱变换的次数为 192 − (300mod192) = 84 次.

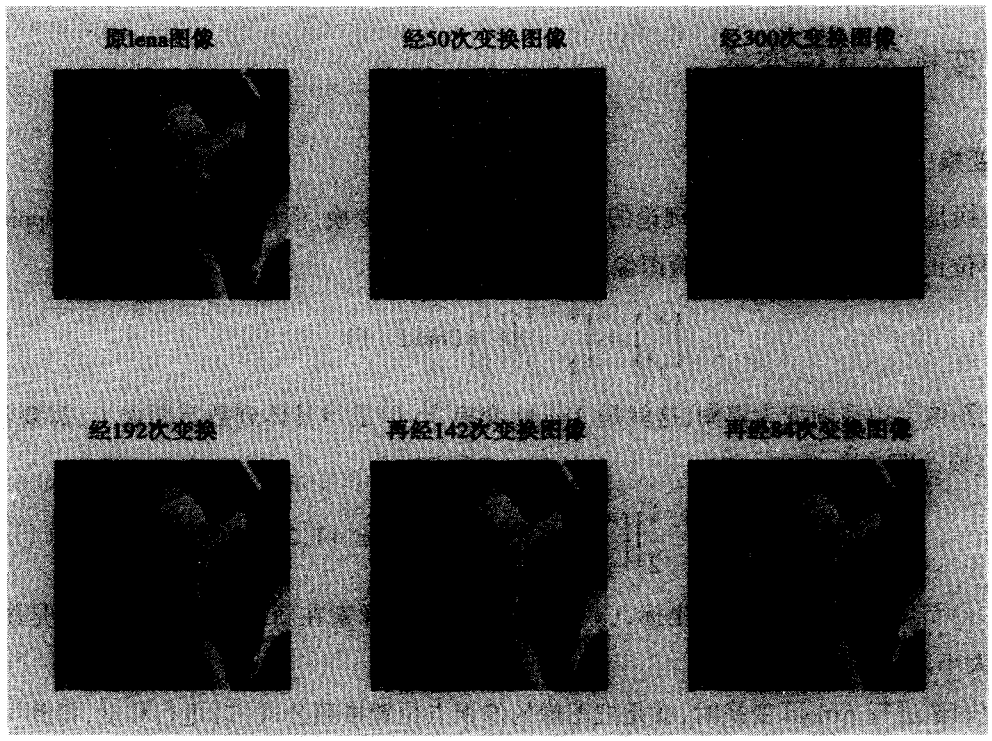

图1 lena图像经Arnold变换效果图(列对比)

1.3 Arnold逆变换

Arnold变换是一种简便的图像置乱方法,它的周期性是一个很好的性质,当反复利用Arnold变换,在某一个变换后,就能恢复成原图. Arnold变换的周期性与图像大小有关,但并不成正比,因而在进行Arnold变换时,首先需要检测图像大小及置乱周期,而且在处理较大的图像时,利用周期性来恢复原图,势必会花费较长的时间. 在实际中,将Arnold变换应用于数字图像水印时,应尽量减少它的时间和空间上的复杂度,这时,就只能考虑阶数小一点的图像,这就会限制水印图像的选择. 于是,提出了一种Arnold变换的逆变换.

由于Arnold变换具有很好的代数结构,因而可以通过求Arnold变换的反函数来进行Arnold逆变换. 对式(2)中的Arnold变换定义方程进行推导,在已知(x',y')和N的情况下,求出(x,y). 式(2)等价为:

$$\begin{cases} x' = (x+y)\ (\mathrm{mod}\ N) \\ y' = (x+2y)\ (\mathrm{mod}\ N) \end{cases} \tag{3}$$

用数学函数的知识解这个方程组,会得到一些二元一次方程组,解之取解集的并集,得到Arnold变换的逆变换[8,10]. 但是这种方法讨论起来比较麻烦,可以用Arnold变换的变换矩阵的逆矩阵来作为Arnold逆变换的变换矩阵,可以不用计算图像的大小和变换周期,大大节约了计算成本,只要知道变换的密钥,即变换次数,就可以利用Arnold逆变换变换同样的次数恢复出原图像.

对于Arnold变换的变换矩阵$A=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$,如果用其逆矩阵$A^{-1}=\begin{bmatrix}2 & -1\\ -1 & 1\end{bmatrix}$来代替,即使用如下变换:

$$\begin{bmatrix}x'\\ y'\end{bmatrix}=\begin{bmatrix}2 & -1\\ -1 & 1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}(\mathrm{mod}\quad N),x,y\in\{1,2,\cdots,N\} \tag{4}$$

变换(4)与变换(2)有相同的周期,称之为Arnold逆变换.

由Arnold逆变换的定义知道,当得到一幅经过n步Arnold变换的图像时,便可以利用Arnold逆变换迭

代 n 步使一副置乱的图像恢复原图,而无需计算图像的大小及图像 Arnold 变换的周期. 如图 2,lena 图像经 48 次 Arnold 变换后的图像再经 48 次的 Arnold 逆变换后恢复原图像.

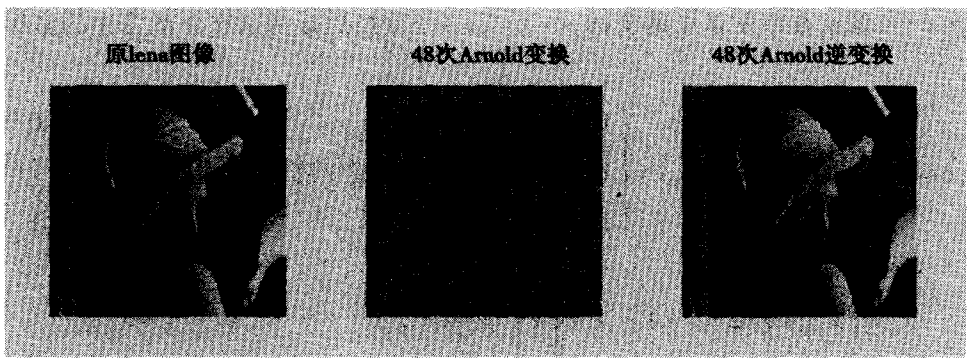

图 2　Arnold 变换与 Arnold 逆变换效果图

1.4　Arnold 变换扩展:非方阵变换(矩形变换)

一般都是对正方形图像进行 Arnold 变换,现在把它推广到 $m \times n$ 的矩形图像上,即图像的长度和宽度不相等[10]. 如图 3 (该图像为 175 ×256):

图 3　长度和宽度不相等的矩形图像

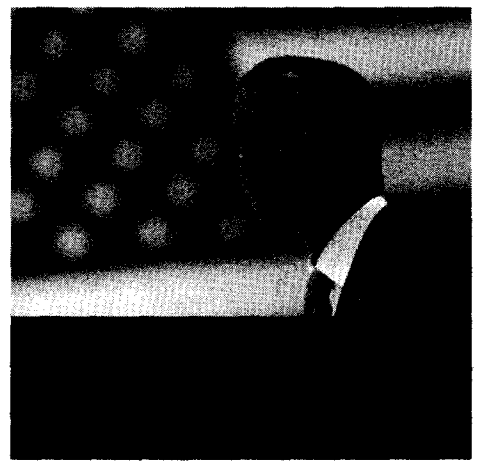

图 4　对长度和宽度不等的矩形图像扩充为方形图像

此时,对图像进行的 Arnold 变换就非一一映射,因此不可逆,就不能运用周期性和 Arnold 逆变换重新得到原始图像. 将矩形图像以它的长或宽作为新图像的边长扩充正方形图像,长度大于宽度则以长度为边长进行扩充,宽度大于长度则以宽度作为边长进行扩充. 对灰度图像进行扩充时,可以在图像上下或左右任意扩充,可以是全白色或全黑色,只要扩充的像素灰度值在 0 ~ 255 之间都是允许的[10]. 如图 4,在图像的下方扩充图像,当图像被扩充为正方形图像时,对其进行的 Arnold 变换和 Arnold 逆变换就和正方形图像是一样的,扩充部分对 Arnold 变换和 Arnold 逆变换毫无影响.

2　n 维 Arnold 变换及其逆变换

定义三维的 Arnold 变换如下[11]:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} (\mathrm{mod}\ \ N), x,y,z \in \{1,2,\cdots,N\} \tag{5}$$

其中,(x,y,z)是像素在原图像中的坐标,(x',y',z')是变换后该像素在新图像中的坐标,N是图像的阶数.

对于三维 Arnold 变换的变换矩阵 $A=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix}$,如果用其逆矩阵 $A^{-1}=\begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix}$来代替,即使用如下变换:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} (\mathrm{mod}\ \ N), x,y,z \in \{1,2,\cdots,N\} \tag{6}$$

易知,变换(6)与变换(5)有相同的周期,称之为三维 Arnold 逆变换.

在三维的 RGB 空间中,有如下的三维 Arnold 逆变换[12]:

$$\begin{bmatrix} r' \\ g' \\ b' \end{bmatrix} = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} (\mathrm{mod}\ \ 256), r,g,b \in \{1,2,\cdots,256\} \tag{7}$$

对于 n 维 Arnold 变换和 n 维 Arnold 逆变换,分别给出以下定义[12,13]:

$$\begin{bmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_{n-1} \\ x'_n \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 & 1 \\ 1 & 2 & \cdots & \cdots & 2 & 2 \\ \vdots & \vdots & \cdots & \cdots & \vdots & \vdots \\ 1 & 2 & \cdots & \cdots & n-1 & n-1 \\ 1 & 2 & \cdots & \cdots & n-1 & n \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} (\mathrm{mod}\ N), x_1,x_2,\cdots,x_{n-1} \in \{1,2,\cdots,N\} \tag{8}$$

$$\begin{bmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_{n-1} \\ x'_n \end{bmatrix} = \begin{bmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & 0 \\ & -1 & \ddots & \ddots & \\ & & \ddots & 2 & -1 \\ & 0 & & -1 & 2 & -1 \\ & & & & -1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} (\mathrm{mod}\ N), x_1,x_2,\cdots,x_{n-1} \in \{1,2,\cdots,N\} \tag{9}$$

其中,$(x_1,x_2,\cdots,x_n)$是像素在原图像中的坐标,$(x'_1,x'_2,\cdots,x'_n)$是变换后该像素在新图像中的坐标,N是数字图像矩阵的阶数. 分别称式(8)和(9)为 n 维 Arnold 变换和 n 维 Arnold 逆变换. 对于给定的正整数 N,当 $N\geqslant 2$ 时,有 n 维 Arnold 变换和 n 维 Arnold 逆变换的周期 $T_N \leqslant \frac{1}{2}N^n$.

3 结束语

着重介绍了二维 Arnold 变换及其逆变换的算法,并通过实验数据对二维 Arnold 变换及其逆变换的周期

性理论进行解释论证,给出了非方形矩阵的图像进行扩充至方形的处理,最后,对二维 Arnold 变换及其逆变换在理论上进行了推广. 实验证明,二维 Arnold 逆变换在进行图像复原时具有一定的有效性,在很大程度上,节约了时间和空间. 不足是三维乃至 n 维 Arnold 变换及其逆变换仍需要继续研究,做出实验结果以验证 Arnold 逆变换的有效性.

参考文献:

[1] 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,1999,11(1):338-341

[2] 王行荣,临官春. 信息隐藏技术应用研究[J]. 重庆工商大学学报:自然科学版,2010(1):79-83

[3] 黄仿元. 基于 Arnold 变换的图像置乱算法及实现[J]. 贵州大学学报:自然科学版,2008,25(3):276-279

[4] 吴玲玲,张建伟,葛琪. Arnold 变换及其逆变换[J]. 微计算机信息(嵌入式与 SOC),2010,26(5-2):206-208

[5] 任洪娥,尚振伟,张健. 一种基于 Arnold 变换的数字图像加密算法[J]. 光学技术,2009,35(3):384-390

[6] ARNOLD V J,AVEZ A. Ergodic Problems of Classica Mechanics,Mathematical Physics Monograph Series[M]. New York:W A Ben-jamin Inc,1968

[7] 齐东旭. 分形及其计算机生成[M]. 北京:科学出版社,1994

[8] 张俊萍,谭月辉,梁欣,等. Arnold 变换的置乱恢复研究[J]. 军械工程学院学报,2006,18(4):52-55

[9] 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

[10] 孔涛,张亶. Arnold 反变换的一种新算法[J]. 软件学报,2004,15(10):1558-1564

[11] 齐东旭,邹建成,韩效宥. 一种新的置乱变换及其在图像信息影藏中的应用[J]. 中国科学(E 辑),2000,30(5):440-448

[12] 邹玮刚,刘辉. 基于三维 Arnold 逆变换的数字图像置乱技术及其周期性[J]. 江西理工大学学报,2007,28(6):36-38

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

Research on Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm

MAO Lei-bo

(School of Mathematics,Chongqing Normal University,Chongqing 401331,China)

Abstract: Arnold transform, due to its periodicity, is widely used in image encryption, however, it is quite time-consuming when the periodicity of the transform is used in decryption, as a result, anti-Arnold transform algorithm is presented, and based on this, the algorithm is extended into non-square matrix image, general rectangular image, therefore, its application range in image encryption is expanded. Finally, 2-dimensional Arnold transform is extended to n-dimensional Arnold transform and anti-Arnold transform in theory.

Key words: digital image; image scrambling; scrambling resumption; Arnold transformation; anti-Arnold transformation

责任编辑:李翠薇