

【电子与信息科学 / Electronics and Information Science】

## 图像 Arnold 变换中的准对称性问题与半周期现象

李雄军, 廖日军, 李金龙, 冼建标, 徐健杰, 黄培, 何小雨

深圳大学物理科学与技术学院, 深圳 518060

**摘要:** 从广义 Arnold 变换的周期性及标准 Arnold 变换与 Fibonacci 的关系出发, 推导  $k$  步 Arnold 变换的一次性等效变换矩阵, 特别是半周期处的一次性变换矩阵, 并分析其特点, 证明图像经广义 Arnold 变换位置置乱后在置乱周期内呈现图像置乱度的准对称性, 讨论当置乱周期为偶数时的半周期现象和置乱周期为奇数时的各种不同情况. 研究表明, 无论置乱周期为奇数还是偶数, 图像乱度存在前半周期和后半周期的准对称性; 对偶数周期情况, 标准 Arnold 变换下, 在置乱次数等于周期的一半时, 一次性置乱变换矩阵为单位矩阵的整数倍; 半周期处置乱图像更易呈现与原图相似的结构或内容信息; 对于某些维数的图像, 半周期处的一次性置乱变换为负的单位矩阵, 此时图像为原图的水平加垂直镜像图像; 广义 Arnold 变换下, 偶数置乱周期变换的半周期处的一次性变换矩阵可能是标准 Arnold 变换的结果, 或在此基础上叠加了一个位移量为图像维数一半的水平或垂直平移, 因而仍然存在较明显的半周期现象. 对于奇数周期, 半周期现象虽然存在但一般不如偶数周期情况明显, 更不易出现镜像或提前恢复原图的情况. 该研究可用于指导图像加密预处理中置乱次数选择和置乱乱度计算方法的评价与比较.

**关键词:** 计算机应用; Arnold 变换; 准对称性; 置乱变换; 置乱度; 半周期现象; Fibonacci 变换; 图像加密

中图分类号: U 491.1      文献标志码: A      doi: 10.3724/SP.J.1249.2015.06551

## Quasi-symmetry and the half-cycle phenomenon in scrambling degrees for images with pixel locations scrambled by Arnold transformation

Li Xiongjun<sup>†</sup>, Liao Rijun, Li Jinlong, Xian Jianbiao,  
Xu Jianjie, Huang Pei, and He Xiaoyu

College of Physics Science and Technology, Shenzhen University, Shenzhen 518060, P. R. China

**Abstract:** By referring to the periodicity of the general Arnold transformation and the relationship between standard Arnold transformation and Fibonacci transformation, we deduce the equivalent one-step transformation matrix for  $k$  times of Arnold transformation with pixel position scrambled, especially the one at the half-cycle of the scrambling period. We analyze their characteristics and provide a proof of the quasi-symmetry in scrambling degrees for images

**Received:** 2015-10-22; **Accepted:** 2015-10-31

**Foundation:** University Student's Innovation and Entrepreneurship Training Program Foundation of Shenzhen University (201510590079); 2015 Foundation for College Students' Science and Technology Innovation Training Program ("Climbing" Program) of Guangdong Province (201510590079)

<sup>†</sup> **Corresponding author:** Associate professor Li Xiongjun. E-mail: lixj@szu.edu.cn

**Citation:** Li Xiongjun, Liao Rijun, Li Jinlong, et al. Quasi-symmetry and the half-cycle phenomenon in scrambling degrees for images with pixel locations scrambled by Arnold transformation [J]. Journal of Shenzhen University Science and Engineering, 2015, 32(6): 551-562. (in Chinese)



in one cycle. We discuss the half-cycle effect in scrambling degrees in scrambled images with even and odd scrambling periods respectively. Results show that there exists a quasi-symmetry in scrambling performance between the two half cycles regardless of the period being even or odd. In a standard Arnold transformation with a commonly even period, the one-step transform is equivalent to a simple scaling matrix transform which leads to the scrambled image at the half period with an obvious lower scrambling degree, where being the minus unitary matrix as a special case results in the scrambled image being the horizontal mirror image with an overlying vertical mirror image of the original image. For any general Arnold transformation with an even scrambling period, the one-step transformation at half cycle may be the same as the one-step transform for standard Arnold transform or with a translation of half of the image dimension superimposed, thus leading to a little less salient half-cycle phenomenon. For an Arnold transformation with an odd scrambling period, no such situation happens in general unless for images with very special contents and structure. The results can be applied in choice of scrambling time for the pre-processing in image encryption and the evaluation and comparison of image scrambling degree criteria.

**Key words:** computer application; Arnold transformation; quasi-symmetry; scrambling transform; scrambling degree; half-cycle phenomenon; Fibonacci transformation; image encryption

Arnold 变换因其简捷、周期性和非线性<sup>[1-5]</sup>, 一直是图像加密、信息隐藏和数字版权保护中普遍采用的置乱技术之一<sup>[6-8]</sup>. 由于置乱效果的好坏直接关系到后续加密或隐藏处理的加密性、隐蔽性及抗检测性, 因此, 针对图像置乱度评价和影响置乱效果的因素分析的研究具有重要意义. 近年来, 图像乱度评价准则与置乱度计算方法引起了学者的广泛关注<sup>[9-17]</sup>, 而影响图像置乱效果的因素分析并未受到足够重视. 实践证明, Arnold 置乱变换的效果不仅与原图结构内容有关, 且与置乱变换参数和置乱次数密切相关. 如图 1 所示, 包括灰度图像和二值图像在内的图像, 经标准 Arnold 变换位置置乱后, 在整个变换周期内, 其置乱图像的乱度呈现前半周期和后半周期之间一定的对称性 (非严格对称, 即准对称性), 且在半周期处, 置乱图像与原图有较大相似性. 对有一定规则性且乱度较低的原图, 随着变换次数增加, 图像乱度虽然有所波动, 但总体趋势是越来越乱, 当置乱次数  $k$  接近半周期次数时, 图像乱度又明显下降, 甚至隐约可见原图的信息; 继续置乱, 图像乱度又会增加并伴随轻微波动, 当置乱次数接近置乱周期次时乱度明显下降, 直到等于置乱周期时恢复为原图. 标准 Arnold 变换的这种俗称“半周期”现象已被普遍察觉, 并依图像内容结构的不同和置乱变换周期的不同, 出现明显程度或强或弱的变化. 那么, 广义 Arnold 变换是否具有与标准 Arnold 变换同样的准对称性和半周期现象? 能否从数学上严格证明准对称性呢? 排

除原图对置乱图像乱度的影响, 图像乱度与变换参数和置乱次数之间是否存在更明显和直接的关系? 当置乱周期为偶数或奇数时, 半周期现象在明显程度上有何不同? 目前, 这些问题都没有很好的解释, 这也带来了 Arnold 变换在乱度研究和图像加密应用中的局限性: 在图像乱度研究领域, Arnold 变换一个变换周期内的置乱图像常常被用来定性测试某置乱度指标的合理性. 但一般只限于标准 Arnold 变换, 并且只考察图像乱度大概趋势的反映. 由于半周期现象的明显程度与所选原图及置乱周期有关, 使这样的测试带有一定主观性和片面性. 在图像加密和信息隐藏领域, 选择置乱次数时人们往往会首先人为确定变换参数 (最典型的是直接采用标准 Arnold 变换), 然后常用两种方法确定置乱次数: 一是依据经验或对原图进行置乱测试, 依据视觉观察结果来选择, 其缺点是此选择存在一定主观性和随意性, 且结果依赖于原图, 一旦原图改变则必须重新测试; 二是采用某种乱度指标随时计算置乱图像的置乱度来选择置乱次数. 虽然这种方法能实现置乱过程中自动选择乱度较高的置乱次数, 但由于至今尚无一种普遍适用且与人类视觉效果吻合的图像乱度评价方法, 影响了结果的可靠性.

鉴于以上理论和应用两方面的原因, 本研究从 Arnold 变换及其与 Fibonacci 数列的关系入手, 分置乱周期为奇数和偶数两种情况, 来深入探讨这些问题, 并讨论此结论在应用方面的启示.

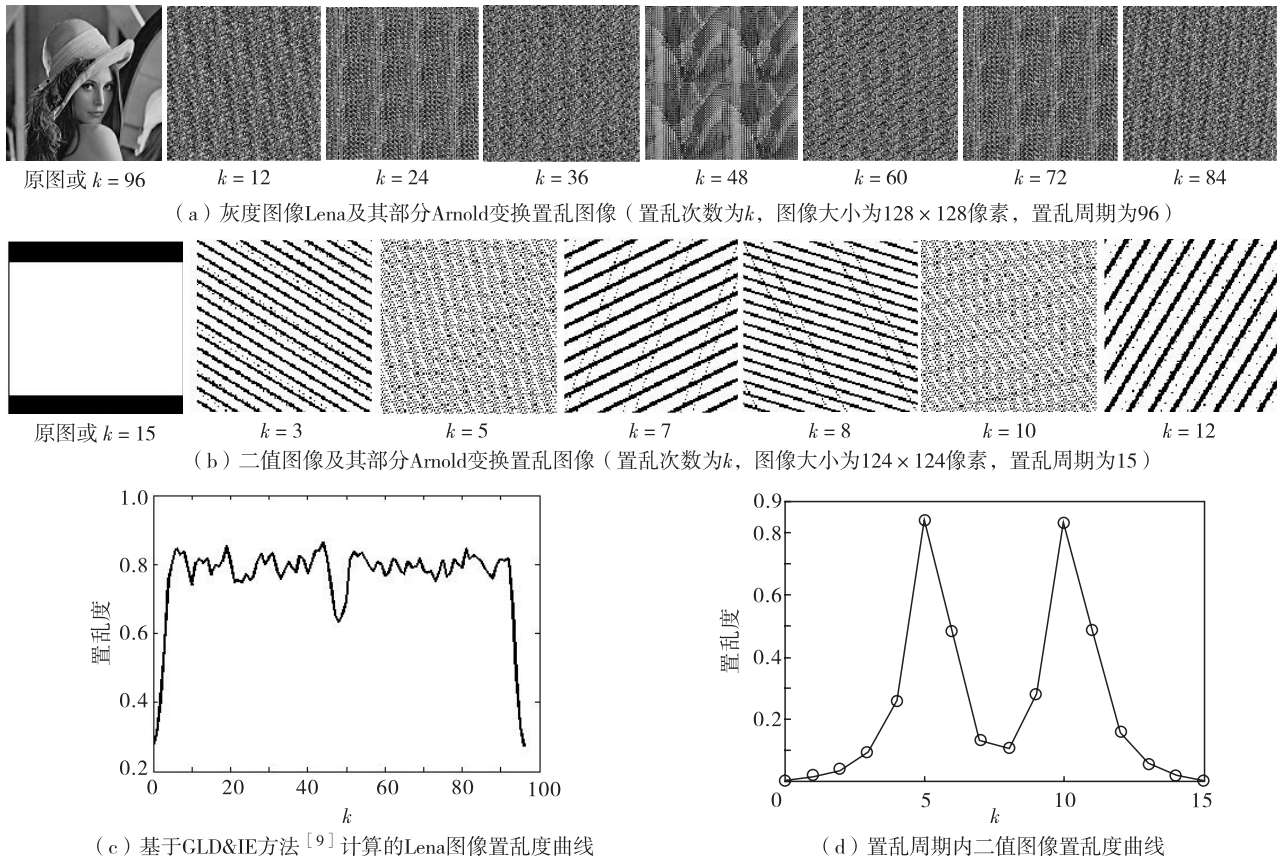


图 1 图像经 Arnold 变换置乱情况

Fig. 1 Images scrambled by Arnold transformation and their scrambling degree curves during a scrambling cycle

# 1 准对称性问题

## 1.1 基本概念

### 1.1.1 广义 Arnold 变换与标准 Arnold 变换

大小为  $N \times N$  的图像经 Arnold 变换后, 位置置乱可表示为

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (1)$$

其中,  $x, y, x_1, y_1 \in [0, N - 1], (x, y)$  和  $(x_1, y_1)$  分别为原图像坐标和对应的置乱图像坐标.

广义 Arnold 变换形式为

$$A = \begin{bmatrix} 1 & b \\ c & 1 + bc \end{bmatrix}$$

其中,  $b$  和  $c$  为整数. 满足  $A$  的行列式值  $\det A = |A| = 1$ . 当  $b = c = 1$ , 即为 Arnold 变换的标准形式<sup>[1]</sup>为

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

### 1.1.2 一次性等效变换矩阵

对原图进行  $k$  次 Arnold 变换后, 有

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = A^k \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (2)$$

其中,  $(x_k, y_k)$  是像素  $(x, y)$  经整数  $k$  次 Arnold 变换后的新坐标,  $k \in [1, N]$ . 若存在  $A_k$ , 对所有  $(x, y)$  图像坐标满足

$$\begin{aligned} A_k \begin{bmatrix} x \\ y \end{bmatrix} \bmod N &= \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \\ &A^k \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \end{aligned} \quad (3)$$

其中,  $a_k, b_k, c_k, d_k \in [0, N - 1]$  的整数, 则称  $A_k$  为对维数为  $N \times N$  的图像进行  $k$  次 Arnold 变换的一次性等效变换矩阵<sup>[18]</sup>. 那么

$$A_k = \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix} = A^k \bmod N \quad (4)$$

为求取任意次置乱变换的一次性等效变换的公式. 同时, 求  $A_k$  时要注意, 计算矩阵乘方时要及时取模, 以免元素太大而溢出, 造成结果错误<sup>[18]</sup>.

### 1.1.3 模 $N$ 逆矩阵

设  $I$  为单位矩阵, 对变换矩阵  $T$  和  $R$ , 若

$$TR \bmod N = RT \bmod N = I \quad (5)$$

则称  $T$  和  $R$  互为模  $N$  逆矩阵.

### 1.2 准对称性的推导

依据式(1)至式(3), 由  $\det A_k \bmod N = \det A^k \bmod N = (\det A)^k \bmod N = 1$  可得

$$(a_k d_k - b_k c_k) \bmod N = 1 \quad (6)$$

由于

$$\begin{aligned} A_k &= A^k \bmod N = A^{k-m} A^m \bmod N = \\ &= \begin{bmatrix} a_{k-m} & b_{k-m} \\ c_{k-m} & d_{k-m} \end{bmatrix} \begin{bmatrix} a_m & b_m \\ c_m & d_m \end{bmatrix} \bmod N = \\ &= \begin{bmatrix} a_{k-m} a_m + b_{k-m} c_m & a_{k-m} b_m + b_{k-m} d_m \\ c_{k-m} a_m + d_{k-m} c_m & c_{k-m} b_m + d_{k-m} d_m \end{bmatrix} \bmod N \end{aligned} \quad (7)$$

当  $k = m_N$ , 其中  $m_N$  为置乱周期, 满足

$$A_{m_N} = A^{m_N} \bmod N = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (8)$$

原图经  $m_N$  次置乱后恢复为原图, 对照式(7)与式(8), 则有

$$(a_{m_N-m} a_m + b_{m_N-m} c_m) \bmod N = 1 \quad (9)$$

$$(a_{m_N-m} b_m + b_{m_N-m} d_m) \bmod N = 0 \quad (10)$$

$$(c_{m_N-m} a_m + d_{m_N-m} c_m) \bmod N = 0 \quad (11)$$

$$(c_{m_N-m} b_m + d_{m_N-m} d_m) \bmod N = 1 \quad (12)$$

将式(9)两边分别乘以  $d_m$  和  $b_m$ , 得

$$(a_{m_N-m} a_m d_m + b_{m_N-m} c_m d_m) \bmod N = d_m \quad (13)$$

$$(a_{m_N-m} a_m b_m + b_{m_N-m} c_m b_m) \bmod N = b_m \quad (14)$$

由式(10)移项得

$$(b_{m_N-m} d_m) \bmod N = (-a_{m_N-m} b_m) \bmod N \quad (15)$$

将(15)式分别代入式(13)和式(14), 可得

$$\begin{cases} a_{m_N-m} (a_m d_m - b_m c_m) \bmod N = d_m \\ b_{m_N-m} (-a_m d_m + b_m c_m) \bmod N = b_m \end{cases} \quad (16)$$

根据式(6)得到  $(a_m d_m - b_m c_m) \bmod N = 1$ , 则有

$$\begin{cases} a_{m_N-m} = d_m \\ b_{m_N-m} = (-b_m) \bmod N \end{cases} \quad (17)$$

类似地, 由式(11)和式(12)可得

$$c_{m_N-m} = (-c_m) \bmod N \quad (18)$$

式(17)至式(18)的结论对于标准 Arnold 变换和广义 Arnold 变换都成立.

设大小为  $N \times N$  的原图像  $I$  上的某个像素  $(x, y)$ , 分别经  $m$  次和  $m_N - m$  次 Arnold 变换后, 得到置乱图像  $I'$  和  $I''$  上对应像素的位置  $(x', y')$  和  $(x'', y'')$  分别为

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A_m \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (19)$$

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = A_{m_N-m} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (20)$$

则对应的一次性等效变换矩阵为  $A_m = \begin{bmatrix} a_m & b_m \\ c_m & d_m \end{bmatrix}$  和

$$\begin{aligned} A_{m_N-m} &= \begin{bmatrix} a_{m_N-m} & b_{m_N-m} \\ c_{m_N-m} & d_{m_N-m} \end{bmatrix} = \begin{bmatrix} d_m & -b_m \\ -c_m & a_m \end{bmatrix} \bmod N = \\ &= R_m \bmod N \end{aligned} \quad (21)$$

其中,  $R_m$  为  $A_m$  的逆变换,

$$R_m = (A_m)^{-1} = \begin{bmatrix} d_m & -b_m \\ -c_m & a_m \end{bmatrix} \quad (22)$$

则有

$$\begin{aligned} A_m A_{m_N-m} \bmod N &= R_m A_m \bmod N = A_m R_m \bmod N = \\ &= \begin{bmatrix} a_m & b_m \\ c_m & d_m \end{bmatrix} \begin{bmatrix} d_m & -b_m \\ -c_m & a_m \end{bmatrix} \bmod N = \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \quad (23)$$

显然,  $A_m$  与  $A_{m_N-m} (R_m)$  互为模  $N$  逆矩阵.

式(21)说明, 原图经  $m_N - m$  次 Arnold 正变换与原图经  $m$  次 Arnold 逆变换是等效的. 式(23)反映了原图经  $m$  次 Arnold 正变换的一次性等效变换  $A_m$  与原图经  $m$  次 Arnold 逆变换的一次性等效变换

$R_m$  之间的准对称关系.

若将式(19)和式(20)两边分别乘以  $R_m$  和  $A_m$ , 则可得

$$\begin{bmatrix} x \\ y \end{bmatrix} = R_m \begin{bmatrix} x' \\ y' \end{bmatrix} \pmod N \quad (24)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = R_m \begin{bmatrix} x'' \\ y'' \end{bmatrix} \pmod N \quad (25)$$

图 2 用示意图方式对准对称性做出解释, 其中  $k$  为置乱次数.

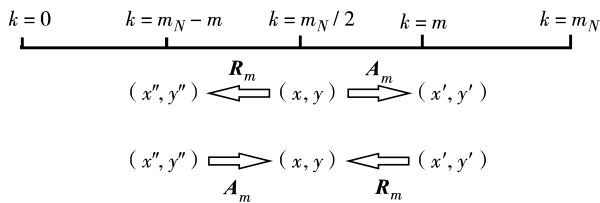


图 2 准对称性解释示意图

Fig. 2 Schematic sketch for explanation of quasi-symmetry

由图 2 可见,  $A_m$  与  $A_{m_N-m}$  使原图同一像素被映射到不同位置上, 但置乱后的位置不是毫无关联, 而是通过这两个互为模  $N$  逆变换矩阵呈现一定对称相关性.

通过比较两个坐标乘积  $x'y'$  与  $x''y''$  还发现, 若

$$(a_m + d_m)(b_m + c_m)(x^2 + y^2) \pmod N = 0 \quad (26)$$

成立, 则存在  $x'y' = x''y''$ , 使得置乱图像  $I'$  和  $I''$  上的像素  $(x', y')$  和  $(x'', y'')$  存在更密切的对应关系.

以上证明在置乱周期内, 经广义 Arnold 变换 (包括标准 Arnold 变换在内), 进行像素位置置乱的图像在图像乱度上存在准对称性.

## 2 半周期现象讨论

### 2.1 置乱周期为偶数时的情况

若周期  $m_N$  为偶数, 则半周期  $s = m_N/2$  为整数. 在  $m = s$  时, 由式(16)得  $a_s = d_s$ . 由式(17)得  $b_s = -b_s \pmod N$ , 那么, 若  $N$  为奇数, 则唯一解  $b_s = 0$ ; 若  $N$  是偶数, 则  $b_s = 0$  或  $N/2$ . 同理, 由式(18)可得, 若  $N$  是奇数, 有  $c_s = 0$ ; 若  $N$  是偶数,  $c_s = 0$  或  $N/2$ . 因此, 原图被广义 Arnold 变换位置置乱半

周期次的一次性变换矩阵有 4 种可能的形式, 即

$$\text{I 类 } A_{s1} = A^s \pmod N = \begin{bmatrix} a_s & 0 \\ 0 & a_s \end{bmatrix} \quad (27)$$

$$\text{II 类 } A_{s2} = A^s \pmod N = \begin{bmatrix} a_s & N/2 \\ 0 & a_s \end{bmatrix} \quad (28)$$

$$\text{III 类 } A_{s3} = A^s \pmod N = \begin{bmatrix} a_s & 0 \\ N/2 & a_s \end{bmatrix} \quad (29)$$

$$\text{IV 类 } A_{s4} = A^s \pmod N = \begin{bmatrix} a_s & N/2 \\ N/2 & a_s \end{bmatrix} \quad (30)$$

式(27)至式(29)同时必须满足

$$a_s^2 \pmod N = 1, \quad a_s \in [1, N-1] \quad (31)$$

式(31)可等效为

$$(a_s + 1)(a_s - 1) \pmod N = 0, \quad a_s \in [1, N-1] \quad (32)$$

式(30)同时需满足

$$(a_s + N/2)(a_s - N/2) \pmod N = 1, \quad a_s \in [1, N-1] \quad (33)$$

下面针对以上 4 类  $A_s$ , 分析原图图像像素  $(x, y)$  被置乱到置乱图像像素  $(x_s, y_s)$  的具体情况. 首先, 对于 I 类情况有

$$\begin{bmatrix} x_s \\ y_s \end{bmatrix} = A_{s1} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = \begin{bmatrix} a_s & 0 \\ 0 & a_s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = a_s \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = \begin{bmatrix} a_s x \\ a_s y \end{bmatrix} \pmod N \quad (34)$$

式(27)说明, 半周期处的  $A_s$  是单位矩阵的整数倍, 相当于把图像在模  $N$  内进行拉伸, 使置乱图像与原图有较大相似性. 同时, 原图对角线和反对角线的点被映射到置乱图像上的对角线和反对角线上. 关于  $x$  轴、 $y$  轴或原点对称的原图图像像素映射到置乱图像后, 仍关于  $x$  轴、 $y$  轴或原点对称. 因此, 当原图乱度较低时, 半周期处的置乱图像便相应呈现较低乱度.

对于 II、III 和 IV 类的  $A_s$  有

$$\begin{bmatrix} x_s \\ y_s \end{bmatrix} = A_{s2} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = \begin{bmatrix} a_s & N/2 \\ 0 & a_s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N = \begin{bmatrix} a_s x + (N/2)y \\ a_s y \end{bmatrix} \pmod N \quad (35)$$

$$\begin{bmatrix} x_s \\ y_s \end{bmatrix} = A_{s3} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} a_s & 0 \\ N/2 & a_s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} a_s x \\ (N/2)x + a_s y \end{bmatrix} \bmod N \quad (36)$$

$$\begin{bmatrix} x_s \\ y_s \end{bmatrix} = A_{s4} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} a_s & N/2 \\ N/2 & a_s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} a_s x + (N/2)y \\ (N/2)x + a_s y \end{bmatrix} \bmod N \quad (37)$$

式(35)说明, 经  $A_s$  置乱后坐标在 I 类情况的拉伸变换基础上, 对原图奇数列的像素, 其变换后的横坐标还叠加  $N/2$  (若  $y \leq N/2$ ) 或  $-N/2$  (若  $y > N/2$ ) 的平移. 同理, 式(36)说明, 置乱后坐标在 I 类拉伸变换基础上, 对原图奇数行的像素其纵坐标还要叠加  $N/2$  ( $x \leq N/2$ ) 或  $-N/2$  ( $x > N/2$ ) 的平移量. 式(37)说明, 置乱后坐标在 I 类拉伸变换的基础上, 对原图奇数行和/或奇数列的像素其纵坐标和/或横坐标都要分别叠加  $N/2$  或  $-N/2$  的平移量. 以上 3 种情况, 虽然会使置乱图像与原图的相似性不如 I 类情况, 但因为坐标变换都只是多了固定的  $N/2$  或  $-N/2$  平移量, 所以与半周期处附件其他置乱图像比较, 在半周期处置乱图像仍呈现相对较大的与原图的相似性.

进一步讨论 I 类情况的两个  $A_s$  特例.

1)  $a_s = N - 1$  的情况.

$$A_s = \begin{bmatrix} N-1 & 0 \\ 0 & N-1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \bmod N = - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \quad (38)$$

此时,  $A_s$  实质上是将原图像进行了水平镜像加垂直镜像变换.

由于满足式(27)和式(31)的解  $a_s$  并非唯一, 当  $N$  是素数时, 解得  $a_s = N - 1$ , 式(34)恒成立; 当  $N$  为非素数时, 式(34)也可能成立. 此时, 原图置乱半周期次后得到水平加垂直镜像图像, 暴露了原图信息.

2) 对某些为 4 的倍数的  $N$ , 当  $a_s = N/2 + 1$  时的情况.

当  $N$  为 4 的倍数时,  $N/2$  是偶数. 当  $a_s = N/2 + 1$  时, 因为  $(a_s + 1) \bmod 2 = 0$ ,  $(a_s - 1) \times \bmod(N/2) = 0$ , 使式(32)成立.

因此, 由  $A_s = \begin{bmatrix} N/2 + 1 & 0 \\ 0 & N/2 + 1 \end{bmatrix}$  得

$$\begin{cases} x_s = [(N/2)x + x] \bmod N \\ y_s = [(N/2)y + y] \bmod N \end{cases} \quad (39)$$

对  $x$  和  $y$  的奇数和偶数情况分别有 4 种解的形式, 即

1)  $x$  和  $y$  都为奇数

$$\begin{cases} x_s = \begin{cases} x + N/2, & x < N/2 \\ x - N/2, & x \geq N/2 \end{cases} \\ y_s = \begin{cases} y + N/2, & y < N/2 \\ y - N/2, & y \geq N/2 \end{cases} \end{cases} \quad (40)$$

2)  $x$  奇数,  $y$  为偶数

$$\begin{cases} x_s = \begin{cases} x + N/2, & x < N/2 \\ x - N/2, & x \geq N/2 \end{cases} \\ y_s = y \end{cases} \quad (41)$$

3)  $x$  偶数,  $y$  为奇数

$$\begin{cases} x_s = x \\ y_s = \begin{cases} y + N/2, & y < N/2 \\ y - N/2, & y \geq N/2 \end{cases} \end{cases} \quad (42)$$

4)  $x$  和  $y$  都为偶数

$$\begin{cases} x_s = x \\ y_s = y \end{cases} \quad (43)$$

如果原图由 4 个大小为原图 1/4, 内容完全相同的图像上下左右拼接而成, 即

$$I(x, y) = \begin{cases} I(x + \frac{N}{2}, y + \frac{N}{2}), & x, y < \frac{N}{2} \\ I(x - \frac{N}{2}, y), & x \geq \frac{N}{2}, y < \frac{N}{2} \\ I(x, y - \frac{N}{2}), & x < \frac{N}{2}, y \geq \frac{N}{2} \\ I(x - \frac{N}{2}, y - \frac{N}{2}), & x, y \geq \frac{N}{2} \end{cases}$$

则在置乱变换半周期处有  $I(x_s, y_s) \equiv I(x, y)$ , 即置乱图像提前恢复为原图, 使该图像置乱周期为置乱变换周期的 1/2. 这进一步说明, 文献[6]提出的置乱图像置乱周期与置乱变换周期是两个不同概念的结论, 适用于包括二值图像在内的所有图像.

所以, 当置乱周期为偶数时, 不管原图结构内

容如何,该图像经过广义 Arnold 变换(包括标准 Arnold 变换)置乱半周期次后,置乱图像与原图有较大相似性,呈现较明显的半周期现象.置乱变换周期除了与变换本身的参数有关外,还与图像维数  $N$  有关.但事实上,置乱周期为偶数的情况更普遍,因此半周期现象也很普遍.

### 2.2 置乱周期为奇数时的情况

当周期  $m_N$  为奇数时,设  $s = [m_N/2]$ ,符号  $[ ]$  表示取整,则  $m_N - [m_N/2] = s + 1$ .此时,半周期处对应着两个变换矩阵  $A_s$  和  $A_{s+1}$ .当  $m = s$  时,由式(17)至式(19)可得  $a_{s+1} = d_s$ ;  $b_{s+1} = (-b_s) \bmod N$ ;  $c_{s+1} = (-c_s) \bmod N$ .当  $m = s + 1$  时,由式(16)得  $a_s = d_{s+1}$ .因此,置乱周期中的最中间的两个一次

性广义 Arnold 变换矩阵为  $A_s \begin{bmatrix} a_s & b_s \\ c_s & d_s \end{bmatrix}$  和

$$A_{s+1} = \begin{bmatrix} a_{s+1} & b_{s+1} \\ c_{s+1} & d_{s+1} \end{bmatrix} = \begin{bmatrix} d_s & -b_s \\ -c_s & a_s \end{bmatrix} \bmod N \quad (44)$$

$$A_s A_{s+1} \bmod N = A_{s+1} A_s \bmod N = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (45)$$

说明  $A_s$  和  $A_{s+1}$  具备准对称性关系,对应置乱周期里呈准对称性的两个置乱图像.虽然  $A_s$  和  $A_{s+1}$  不完全相同,但有一定相关性,使对应的置乱图像亦有一定相似性.

因  $A_{s+1} = AA_s \bmod N$ , 有

$$\begin{bmatrix} 1 & b \\ c & 1 + bc \end{bmatrix} \begin{bmatrix} a_s & b_s \\ c_s & d_s \end{bmatrix} \bmod N = \begin{bmatrix} d_s & -b_s \\ -c_s & a_s \end{bmatrix} \bmod N \quad (46)$$

从而有

$$d_s = (a_s + bc_s) \bmod N \quad (47)$$

$$(-b_s) \bmod N = (b_s + bd_s) \bmod N \quad (48)$$

$$(-c_s) \bmod N = [ca_s + (1 + bc)c_s] \bmod N \quad (49)$$

$$a_s = [cb_s + (1 + bc)d_s] \bmod N \quad (50)$$

由式(47)至式(50)解得

$$\begin{cases} a_s = [-(2 + bc)b_s/b] \bmod N \\ c_s = (cb_s/b) \bmod N \\ d_s = (-2b_s/b) \bmod N \end{cases} \quad (51)$$

考虑到  $\det A_s \bmod N = 1$ , 因此得到

$$\begin{cases} A_s = \begin{bmatrix} -(2 + bc)b_s/b & b_s \\ cb_s/b & -2b_s/b \end{bmatrix} \bmod N \\ A_{s+1} = \begin{bmatrix} -(2 + bc)b_s/b & b_s \\ cb_s/b & -2b_s/b \end{bmatrix} \bmod N \\ [(4 + bc)b_s^2/b^2] \bmod N = 1 \end{cases} \quad (52)$$

显然,  $b_s \neq 0$ . 将式(52)与偶数置乱周期的式(27)至式(30)中任一公式比较可知,偶数变换周期的半周期处一次性变换矩阵相对简单得多,置乱过程中像素横坐标  $x$  和纵坐标  $y$  交错影响小;相比之下,奇数周期的半周期处的一次性变换矩阵有  $A_s$  和  $A_{s+1}$  两个,只有当变换参数  $b = c$  时,它们才为对称阵,且变换过程中像素横坐标  $x$  和纵坐标  $y$  同时对变换坐标交错产生影响,使置乱图像相对较乱;因  $b_s \neq 0$ ,则  $A_s$  和  $A_{s+1}$  两者对任何原图都不会出现类似偶数变换周期时的 I 类  $A_s$  的形式,使半周期处的置乱图像一般不会出现为原图或其镜像的情况.

### 2.3 标准 Arnold 变换下的半周期现象

标准 Arnold 变换与 Fibonacci 变换关系<sup>[3-5]</sup>为  $A^m = Q^{2m} = \begin{bmatrix} F_{2m-1} & F_{2m} \\ F_{2m} & F_{2m+1} \end{bmatrix}$ . Fibonacci 数列  $F_0 = 0, F_1 = F_2 = 1, F_3 = F_1 + F_2, \dots, F_{m+1} = F_m + F_{m-1}, \dots, F_{2m+1} = F_{2m} + F_{2m-1}$ , 其中,  $Q = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$  称为 Fibonacci 变换矩阵,那么,

$$\begin{aligned} A_m &= \begin{bmatrix} a_m & b_m \\ c_m & d_m \end{bmatrix} = A^m \bmod N = \\ Q^{2m} \bmod N &= \begin{bmatrix} F_{2m-1} & F_{2m} \\ F_{2m} & F_{2m+1} \end{bmatrix} \bmod N \end{aligned} \quad (53)$$

因此有

$$b_m = c_m = (d_m - a_m) \bmod N \quad (54)$$

$$b_m^2 = (a_m d_m - 1) \bmod N \quad (55)$$

对于标准 Arnold 变换,置乱周期内任意次 Arnold 变换所对应的一次性等效变换矩阵可写成

$$\begin{cases} A_m = \begin{bmatrix} a_m & d_m - a_m \\ d_m - a_m & d_m \end{bmatrix} \bmod N \\ (a_m^2 + d_m^2 - 3a_m d_m + 1) \bmod N = 0 \end{cases} \quad (56)$$

因此对于  $m_N$  为偶数时,在半周期处  $m = s$ ,由式(16)可得  $a_s = d_s$ .对于标准 Arnold 变换的  $b_s = c_s$ ,

由式(54)得  $b_s = c_s = 0$ . 那么, 式(27)至式(30)这 4 类情况只剩下 I 类, 即标准 Arnold 变换下偶数置乱周期情况的半周期处对应的一次性等效变换为

$$\begin{cases} A_s = A^s \bmod N = \begin{bmatrix} a_s & 0 \\ 0 & a_s \end{bmatrix} \\ a_s^2 \bmod N = 1, \quad a_s \in [1, N-1] \end{cases} \quad (57)$$

进一步推导当  $m_N$  为奇数时, 标准 Arnold 变换下半周期处  $A_s$  和  $A_{s+1}$  的具体形式.

对于标准 Arnold 变换, 把  $b = c = 1$  代入式(52), 得

$$A_s = \begin{bmatrix} -3b_s & b_s \\ b_s & -2b_s \end{bmatrix} \bmod N \quad (58)$$

$$A_{s+1} = \begin{bmatrix} -2b_s & -b_s \\ -b_s & -3b_s \end{bmatrix} \bmod N \quad (59)$$

$$5b^2 \bmod N = 1, \quad b_s \in [1, N-1] \quad (60)$$

由式(60)求  $b_s$ , 即可得到奇数置乱周期里半周期处的两个一次性等效变换矩阵.

从式(58)至式(60)可得, 在标准 Arnold 变换下, 奇数置乱周期的半周期处, 一次性变换矩阵的形式与广义 Arnold 变换下的结论类似, 即与偶数置乱周期的情况相比, 奇数置乱周期的半周期处的置乱图像与原图的相似性小得多.

奇数置乱周期的半周期处也常见乱度有一定下降趋势的半周期现象, 甚至对于对称性强或某种结构的原图, 类似图 1 (b) 的情况, 也会出现置乱图像乱度显著下降的情况. 产生此现象的原因有两方面: ① 在整个置乱周期内, 乱度较低的原图逐步被置乱成较乱的图像, 最后又回到原图. 鉴于存在前述所说的准对称性, 使半周期处往往成为分水岭; ② 置乱图像的最终乱度不仅与变换矩阵有关, 而且与原始图像的结构内容关系密切. 在原图乱度较低的大前提下, 与原图结构与内容有一定相似性, 则乱度较低; 但图像乱度较低并非完全等效与原图相似. 然而, 从一次性变换矩阵的形式可见, 奇数周期与原图的相似度不如偶数周期情况下的明显.

### 3 实验与讨论

表 1 给出不同情况下置乱变换参数与特性对

照. 由表 1 可见, Arnold 变换周期的和奇偶性由变换参数和被置乱图像维数大小共同决定; Arnold 变换的一次性等效置乱变换不仅与置乱次数和置乱周期有关, 还与图像大小有关.

表 1 典型 Arnold 变换参数与特性  
Table 1 Some typical Arnold transforms for scrambling and their characteristics

$N$	变换参数	变换类型	变换周期	半周期处 $A_s$	$A_s$ 类型
29	$b = c = 1$	标准	7	$\begin{bmatrix} 5 & 8 \\ 8 & 13 \end{bmatrix}$	奇数周期
41	$b = c = 1$	标准	20	$\begin{bmatrix} 40 & 0 \\ 0 & 40 \end{bmatrix}$	I 类
64	$b = c = 1$	标准	48	$\begin{bmatrix} 33 & 0 \\ 0 & 33 \end{bmatrix}$	I 类
64	$b = 3, c = 2$	广义	16	$\begin{bmatrix} 33 & 32 \\ 0 & 33 \end{bmatrix}$	II 类
122	$b = c = 1$	标准	30	$\begin{bmatrix} 121 & 0 \\ 0 & 121 \end{bmatrix}$	I 类
122	$b = 2, c = 3$	广义	12	$\begin{bmatrix} 121 & 0 \\ 0 & 121 \end{bmatrix}$	I 类
124	$b = c = 1$	标准	15	$\begin{bmatrix} 109 & 5 \\ 5 & 114 \end{bmatrix}$	奇数周期
124	$b = 2, c = 3$	广义	8	$\begin{bmatrix} 61 & 0 \\ 0 & 61 \end{bmatrix}$	I 类
128	$b = c = 1$	标准	96	$\begin{bmatrix} 65 & 0 \\ 0 & 65 \end{bmatrix}$	I 类
128	$b = 2, c = 1$	广义	64	$\begin{bmatrix} 65 & 0 \\ 64 & 65 \end{bmatrix}$	III 类
256	$b = c = 1$	标准	192	$\begin{bmatrix} 129 & 0 \\ 0 & 129 \end{bmatrix}$	I 类

通过改变图像维数和内容、置乱变换参数并进行大量实验, 验证了前述准对称性和半周期现象的结论. 下面给出 3 个有代表性的实验结果. 实验中的原图 (包括大小和内容) 与置乱变换及其参数作为实验条件, 置乱图评价指标仍采用文献[9]介绍的基于灰度差和信息熵的 GLD&IE 法.

实例 1 原图为 4 个完全相同的由  $128 \times 128$  的 baboon 图像压缩到  $64 \times 64$  后拼接而成 (如图 3 (a)),  $N = 128$ , 采用标准 Arnold 变换, 并设  $b = 1, c = 1$ .



由表 1 可查得, 置乱周期  $m_N = 96$ , 半周期处一次性变换矩阵  $A_s$  的参数  $a_s = 65 = N/2 + 1$ . 与图 1 (a) 比较, 此测试只改变了原图, 二者从置乱图像和置乱度曲线均可见标准 Arnold 变换下当置乱周期为偶数时出现比较明显的准对称性与半周期现象. 图 1 (a) 的半周期处隐约可见原图, 而实例 1 的半周期处 ( $k = 48$ ) 置乱图像恢复为原图 (图 3

(b)), 使图像置乱周期为置乱变换周期 96 的一半. 此时出现最明显的半周期现象, 从置乱度曲线 (如图 3 (c)) 和置乱图像还可以看到置乱周期的 1/4 处新的明显类似半周期性现象.

**实例 2** 将大小为  $256 \times 256$  的 Lena 图像缩放成  $122 \times 122$  ( $N = 122$ ) 的图像作为原图 (图 4 (a)), 采用广义 Arnold 变换, 并设  $b = 2, c = 3$ .

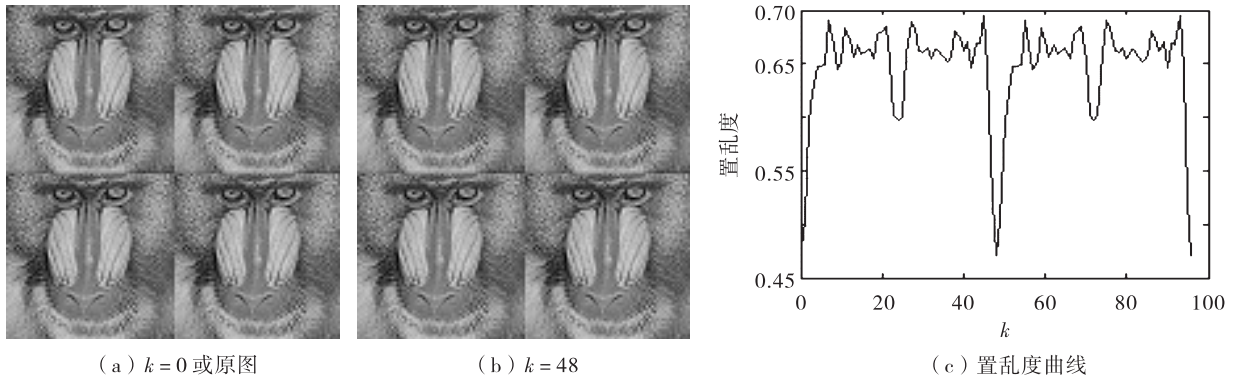


图 3 图像在半周期处恢复原图的特例 ( $b = c = 1, N = 128, m_N = 96$ )

Fig. 3 Image recovery at the half scrambling cycle for the original image with specific symmetry

( $b = c = 1, N = 128, m_N = 96$ )

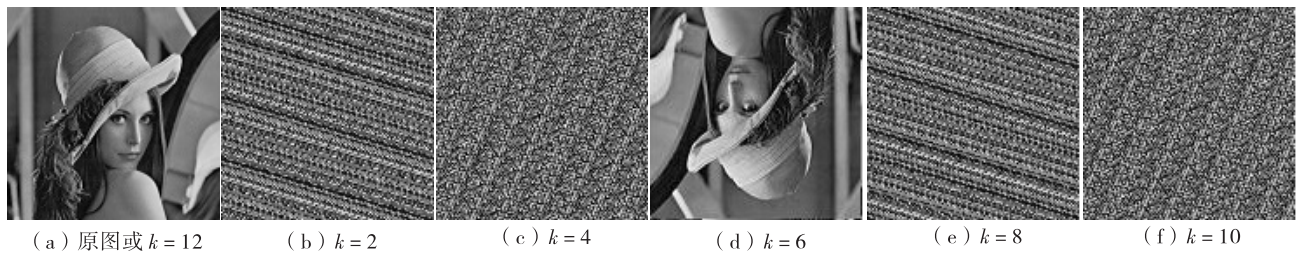


图 4 实例 2 的部分置乱图像 ( $b = 2, c = 3$ , 图像大小为  $122 \times 122, m_N = 12$ )

Fig. 4 Some scrambled images by a general Arnold transformation with  $b=2$  and  $c=3$  for Test 2 ( $N = 122, m_N = 12$ )

由表 1 可查得, 置乱周期  $m_N = 12$ , 其半周期处一次性变换矩阵  $A_s$  的参数  $a_s = 121$ . 图 4 给出了整个置乱周期内的部分置乱图像. 图 5 为对应的置乱度曲线. 从置乱图像和置乱度曲线均可见: 广义 Arnold 变换下, 偶数周期情况下, 同样能观察到准对称性和明显的半周期现象. 而且由于  $a_s = 121 = N - 1$ , 在半周期处出现了原图的水平加垂直镜像图像.

**实例 3** 将大小为  $256 \times 256$  的 Lena 图像缩放大小为  $124 \times 124$  ( $N = 124$ ) 的图像作为原图 (图 6 (a)), 采用标准 Arnold 变换, 并设  $b = 1, c = 1$ .

由表 1 可查得, 标准 Arnold 变换下  $N = 124$

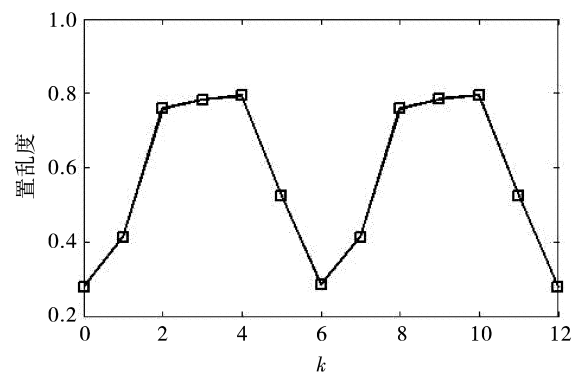


图 5 实例 2 的置乱度曲线

Fig. 5 The scrambling degree curve for Test 2

时, 置乱周期  $m_N = 15$ , 为奇数. 除了原图内容不同外, 实例 3 的其他实验参数与图 1 (b) 的相同. 其半周期处的一次性变换矩阵可从式 (60) 求得. 式 (60) 又可写作

$$5b_s^2 = rN + 1, \quad r, b_s \in [0, N - 1] \quad (61)$$

满足式 (61) 的解为  $r = 1, b_s = 5$ . 由此可得

$$A_s = \begin{bmatrix} -15 & 5 \\ 5 & -10 \end{bmatrix} \bmod N = \begin{bmatrix} 109 & 5 \\ 5 & 114 \end{bmatrix} \quad (62)$$

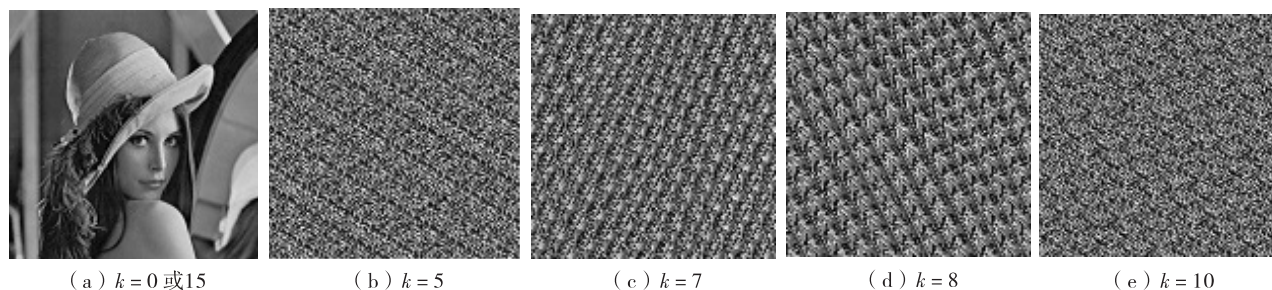


图 6 实例 3 的部分置乱结果和置乱曲线 ( $b = c = 1, N = 124, m_N = 15$ )

Fig. 6 Some scrambled images for Test 3 ( $b = c = 1, N = 124, m_N = 15$ )

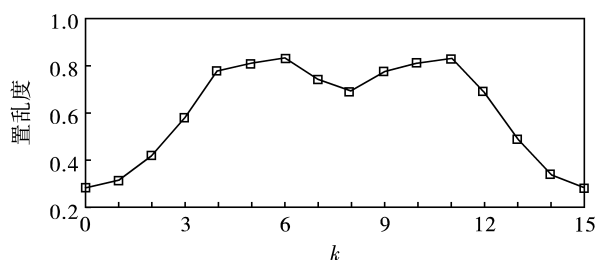


图 7 实例 3 的置乱度曲线

Fig. 7 The scrambling degree curve for Test 3

对图 1 (b) 对应的置乱度曲线, 即图 1 (d), 同样可见半周期性现象, 分析原因我们认为: 由于原图具有强对称性而且是二值图像, 虽然置乱图像与原图相似性不太强, 但乱度度较低, 在整个置乱周期内半周期处成为乱度由高到低再由低到高的分水岭, 与视觉评判结果基本吻合, 说明该乱度评价指标设置合理. 这也表明, 置乱图像乱度由一次性等效置乱变换和原图内容两者共同

与 Matlab 计算结果吻合.

图 6 和图 7 分别给出实例 3 的部分置乱结果和置乱度曲线, 同样可见准对称性和半周期现象. 但如果将实例 3 与图 1 (a) 实验比较可发现, 二者原图内容结构基本一致而图像大小稍有偏差, 置乱变换相同, 置乱周期差异大而且奇偶有别. 结果半周期现象的显著性差异较大, 偶数变换周期下的半周期现象明显得多.

决定.

为了定量比较奇数周期和偶数周期下半周期现象的显著性, 表 2 给出了关键次数置乱情况对照表, 并特别定义一个半周期现象显著性指标

$$r_s = (SD_m - SD) / (SD - SD_0) \quad (63)$$

其中,  $SD_0$  为原图像乱度;  $SD$  为半周期处图像乱度, 置乱周期内最乱图像乱度  $SD_m$ . 对于奇数周期情况, 取半周期处两幅置乱图像中较乱的那幅图像乱度作为  $SD$  来计算.  $r_s$  越大, 说明半周期现象越显著; 反之亦然. 极限状态时,  $SD = SD_0$ , 则  $r_s = \infty$ , 对应半周期处置乱图像恢复为原图或为原图镜像.

从表 2 可见, 当两幅内容基本相同而图像维数稍有不同的原图经标准 Arnold 变换时, 出现偶数置乱周期情况的  $r_s$  大于出现奇数置乱周期情况的  $r_s$ , 前者的半周期现象更明显. 这与理论分析结果吻合.

表 2 乱度对照表与半周期显著性

Table 2 Contrast of scrambling degrees and salience test of the half-cycle phenomenon for Fig. 1 (a) and Fig. 5

图像	$N \times N$	$m_N$	$SD_0$	$SD$	$SD_m$	$r_s$
图 1 (a)	$128 \times 128$	96	0.274 6	$SD = 0.655 7 (k = 48)$	0.864 2	0.547 1
图 5	$124 \times 124$	15	0.278 8	$SD = 0.736 8 (k = 7); SD = 0.688 4 (k = 8)$	0.829 0	0.343 3

以上实验说明,在图像乱度指标的评价方法上,除了与分析人类视觉评判结果的吻合程度作为依据外,Arnold 变换图像也可成为图像乱度计算方法或指标的性能评价与测试数据.乱度曲线能否反映 Arnold 变换的准对称性和半周期现象可成为乱度指标评判的重要依据.在评判过程中,为消除评判结果对所选被置乱图像的依赖性,让结果更客观可靠,建议首先选择偶数置乱周期的置乱变换一周期内的置乱图像进行测试,但要避开在半周期处恢复为原图或产生镜像的情况,考察乱度指标对准对称性和较明显的半周期现象的检测能力.然后用奇数周期的置乱变换图像来测试,考察乱度检测灵敏度.经以上测试,若乱度指标技能反映准对称性,且能检测到半周期现象,说明该乱度指标具有一定合理性;否则,存在不合理性.

在多种乱度计算指标的性能比较上,可采用类似表 2 对图 1(a)与图 6 对照的方法.首先取某偶数置乱周期的 Arnold 变换置乱同一原图,分别计算不同乱度评价方法的半周期现象显著性指标  $r_s$ ,  $r_c$ . 越高,说明该乱度指标对图像乱度检测越灵敏.如果偶数周期情况下的  $r_s$  指标差别不大,再取内容相同但维数稍有不同的具有奇数变换周期的 Arnold 置乱变换图像进行计算,进一步考察各乱度指标对半周期现象的灵敏度.以上方法不依赖原图内容与结构,可避免选择特定结构和内容图像作为原图而对评判结果造成影响,克服了传统视觉吻合程度的主观性(因人而异)和模糊性,为乱度评价指标评判与比较提供一种比较客观的定量方法.

同时,Arnold 置乱变换是图像加密或信息隐藏的预处理中常见的方法,其置乱效果,直接关系后续加密或隐藏处理的加密性、隐蔽性以及抗检测性能.而不同置乱变换置乱效果不同,即使同一置乱变换,置乱次数不同置乱效果也不一样.本文研究的一次性变换求取方法和有关半周期现象的讨论,通过对一次性置乱变换的形式分析可以指导置乱次数的选择.

## 结 语

图像经多步置乱变换的效果可通过对一次性等效变换的形式分析基本得出.本研究从 Arnold 变换的周期性出发,证明了包括广义 Arnold 变换在内的

准对称性,推导和分析了广义 Arnold 变换下置乱周期为偶数和奇数时的半周期处的一次性置乱变换矩阵及其置乱特征,深入讨论了半周期现象的不同表现.研究发现,在原图乱度较低的大前提下,无论是广义 Arnold 变换,还是标准 Arnold 变换,都会出现程度不同的“半周期”现象;偶数置乱周期情况与奇数置乱周期比较,前者的半周期处的置乱图像与原图更相似,一般半周期现象更明显,甚至会出现原图镜像甚至恢复为原图的现象.以上结论既可通过计算一次性变换矩阵来指导加密处理置乱次数的选择,且可用于图像乱度评价方法的评估测试与比较,通过乱度算法对准对称性以及半周期现象的检测能力与敏感性,判断乱度评价方法的合理性与性能优劣.

**基金项目:**广东省“攀登计划”资助项目(201560020006);深圳大学大学生创新创业训练计划资助项目(201510590079)

**作者简介:**李雄军(1966—),女(汉族),湖南省双峰县人,深圳大学副教授、博士. E-mail:lixj@szu.edu.cn

**引 文:**李雄军,廖日军,李金龙,等.图像 Arnold 变换中的准对称性问题与半周期现象[J].深圳大学学报理工版,2015,32(6):551-562.

## 参考文献 / References:

- [1] Arnold V J, Aves A. Ergodic problems of classical mechanics, mathematical Physics monograph series [M]. New York (USA): W A Benjamin Inc, 1968.
- [2] Li Xiongjun. A generalized matrix-based scrambling transformation and its properties [C]// Proceedings of the 9th International Conference for Young Computer Scientists. Huangshan (China): IEEE, 2008: 1429-1434.
- [3] Zou Jiancheng, Tie Xiaoyun. Arnold transformation of digital image with two dimensions and its periodicity [J]. Journal of North China University of Technology, 2000, 12(1): 10-14. (in Chinese)  
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): 10-14.
- [4] Mao Leibo. Research on Arnold transformation algorithm and anti-Arnold transformation algorithm [J]. Journal of Chongqing Technology and Business University Natural Science Edition, 2012, 29(3): 16-21. (in Chinese)  
毛雷波. Arnold 变换及其逆变换 [J]. 重庆工商大学学报自然科学版, 2012, 29(3): 16-21.
- [5] Wu Faen, Zou Jiancheng. Some necessary conditions for

- the periodicity of Arnold transformation of digital image with two dimensions [J]. *Journal of North China University of Technology*, 2001, 125(6): 66-69. (in Chinese)  
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]. *北方工业大学学报*, 2001, 125(6): 66-69.
- [ 6 ] Wu Chengmao. An improved discrete arnold transform and its application in image scrambling and encryption [J]. *Acta Physica Sinica*, 2014, 63(9): 90504-1-090504-20. (in Chinese)  
吴成茂. 离散 Arnold 变换改进及其在图像置乱加密中的应用 [J]. *物理学报*, 2014, 63(9): 90504-1-090504-20.
- [ 7 ] Radharani S, Valarmathi M L. Content based image watermarking scheme using block SVD and Arnold transform [C]// *International Conference on Electronics and Communication Systems (ICECS)*. Coimbatore (India): IEEE, 2014: 1-4.
- [ 8 ] Mehta R, Vishwakarma V P, Rajpal N. Lagrangian support vector regression based image watermarking in wavelet domain [C]// *The 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*. Noida (India): IEEE, 2015: 854-859.
- [ 9 ] Li Xiongjun. A new measure of image scrambling degree based on grey level difference and information entropy [C]// *Proceedings of International Conference on Computational Intelligence and Security*. Washington D C: IEEE, 2008, 1: 350-354.
- [10] Wang Xinxin, Bu Ting. An evaluation algorithm of image scrambling degree based on the image area [J]. *Journal of Anhui University Natural Science Edition*, 2011, 35(4): 48-52. (in Chinese)  
王新新, 布挺. 基于图像表面积的置乱程度评价算法 [J]. *安徽大学学报自然科学版*, 2011, 35(4): 48-52.
- [11] Xu Jiangfeng, Yang You. Analysis of scrambling performance of encrypted image [J]. *Computer Science*, 2006, 33(3): 110-113. (in Chinese)  
徐江峰, 杨有. 加密图像之乱性能表面积的置乱性能分析 [J]. *计算机科学*, 2006, 33(3): 110-113.
- [12] Tan Yongjie, Hu Haizhi. A survey of assessment of image scrambling degree [J]. *Computer and Digital Engineering*, 2012, 40(4): 93-95. (in Chinese)  
谭永杰, 胡海芝. 图像置乱效果评价算法综述 [J]. *计算机与数字工程*, 2012, 40(4): 93-95.
- [13] Huang Liangyong, Xiao Degui. The best image scrambling degree of binary image based on Arnold transform [J]. *Journal of Computer Applications*, 2009, 29(2): 474-476. (in Chinese)  
黄良永, 肖德贵. 二值图像 Arnold 变换的最佳置乱度 [J]. *计算机应用*, 2009, 29(2): 474-476.
- [14] Feng Xingang, Zhou Quan. A novel scrambling degree rule of digital image based on center of mass [J]. *Journal of Electronics & Information Technology*, 2008, 30(11): 2684-2687. (in Chinese)  
冯新岗, 周诠. 基于质心的数字图像置乱度衡量准则 [J]. *电子与信息学报*, 2008, 30(11): 2684-2687.
- [15] Huang Xing, Zhang Minrui. Study on the image scrambling extent [J]. *Geomatics and Information Science of Wuhan University*, 2008, 33(5): 465-468. (in Chinese)  
黄兴, 张敏瑞. 图像置乱程度的研究 [J]. *武汉大学学报信息科学版*, 2008, 33(5): 465-468.
- [16] Guo Linqin. On the image scrambling and scrambling degree [J]. *Journal of Xi'an University of Arts and Science Natural Science Edition*, 2013, 16(3): 49-52. (in Chinese)  
郭琳琴. 图像置乱及置乱度评价方法综述 [J]. *西安文理学院学报自然科学版*, 2013, 16(3): 49-52.
- [17] Yang Xiyang, Li Zhiwei. Image scrambling measurement based on chi-square statistic [J]. *Journal of Xiamen University Natural Science*, 2010, 49(6): 778-781. (in Chinese)  
杨昔阳, 李志伟. 置乱均匀性的优度拟合统计分析 [J]. *厦门大学学报自然科学版*, 2010, 49(6): 778-781.
- [18] Liao Rijun, Li Xiongjun, Xu Jianjie, et al. Discussions on applications of Arnold transformation in binary image scrambling [J]. *Journal of Shenzhen University Science and Engineering*, 2015, 32(4): 428-433. (in Chinese)  
廖日军, 李雄军, 徐健杰, 等. Arnold 变换在二值图像置乱应用中若干问题讨论 [J]. *深圳大学学报理工版*, 2015, 32(4): 428-433.

【中文责编: 英子; 英文责编: 雨辰】