Arnold 型置乱变换周期分析*

黎 罗 罗
（中山大学数学与计算科学学院，广东 广州 510275）

摘 要：Arnold 变换是通信安全中数字图像置乱技术之一。在一定条件下，Arnold 型置乱变换具有周期性，使得通信双方可以随机控制图像传输中变换的次数。为统一地分析各类 Arnold 型变换的周期性，首先建立整数矩阵模算术的基本法则，然后证明模 N 的 Arnold 型变换的周期等于以 N 的两两互素的因数为模的变换的周期之最小公倍数。问题于是归结为模是素数及其幂的情形。最后导出模取素数之不同的幂时相应变换周期间的关系，引入周期特征码的概念，获得对各类 Arnold 型置乱变换的周期的统一、规整而简洁的理解与把握。

关键词：数字图像置乱；Arnold 变换；信息隐藏；周期特征码
中图分类号：TP391 文献标识码：A 文章编号：0529-6579（2005）02-0001-04

图像信息安全问题已经成为人们关注的热点。对于图像信息，传统保密学尚缺少足够的研究；普遍认为，针对大幅图像的信息隐蔽问题，置乱技术是基础性的工作。为了隐蔽数字图像信息，或作为隐蔽的预处理，文 [1－7] 等提出用 Arnold、Fibonacci-Q 变换等对图像进行置乱变换的技术，即对 N 阶数字图像，采用 Arnold 矩阵（或 Fibonacci-Q 矩阵等）$\boldsymbol{A}$，借助变换 $\boldsymbol{x}' \equiv \boldsymbol{A}\boldsymbol{x} \pmod N$（矩阵或向量的同余规定为对应的元素同余），改变图像灰度值的布局，从而达到信息隐蔽的目的。上述变换在很一般的条件下呈现周期现象。（变换的周期指的是使 $\boldsymbol{A}^d \equiv \boldsymbol{I} \pmod N$ 成立的最小正整数 d，其中 $\boldsymbol{I}$ 表示单位矩阵）。该项技术所用变换的周期无疑对信息隐蔽及攻击双方都有至关重要的意义，所以文[1－5] 均以之作为重要论题叙述，并通过计算实验列出在若干不同 N 值时置乱变换的周期值。数据表明变换周期随 N 的变化呈强烈的非线性。

上述置乱技术与 Hill 密码相比更强调周期的讨论。笔者未见文献中对这一问题作统一分析。本文将从揭示貌似杂乱无章的周期变化背后的规律，所得结论有普遍意义；实践上，N 的素分解的密钥掌握者可有针对性地压缩确定变换周期的工作量。

1 矩阵同余关系的基本性质

设 N 为大于 1 的整数，记整数集合 $Z_N = \{0, 1, \cdots, N-1\}$，又 $\boldsymbol{A} = (a_{ij})$ 为 n 阶整数矩阵，$\boldsymbol{x} = (x_1, \cdots, x_n)^{\mathrm{T}}$ 为整数向量，$x_i \in Z_N$。规定变换

$$\boldsymbol{x}' \equiv \boldsymbol{A}\boldsymbol{x} \pmod N \tag{1}$$

文献 [1，2] 已经指出如下结果。

定理 1 下面 3 个命题等价：①行列式 $|\boldsymbol{A}|$ 与 N 互素；②变换式（1）有周期；③矩阵 $\boldsymbol{A}$ 有唯一的模 N 下的逆：$\boldsymbol{A}^{-1}\boldsymbol{A} \equiv \boldsymbol{A}\boldsymbol{A}^{-1} \equiv \boldsymbol{1} \pmod N$。

下文采用记号 $m \perp n$ 表示整数 m，n 互素。另外，变换式（1）的周期称为 $\boldsymbol{A}$ 关于模 N（或在模 N 下）的周期，记为 $\delta_N(\boldsymbol{A})$。

性质 1 矩阵在模 N 下的同余关系是等价关系（即有反身性，对称性和传递性）；

性质 2 若 $\boldsymbol{A} \equiv \boldsymbol{B} \pmod N$，$\boldsymbol{C} \equiv \boldsymbol{D} \pmod N$，则 $\boldsymbol{A}+\boldsymbol{C} \equiv \boldsymbol{B}+\boldsymbol{D} \pmod N$；

性质 3 若 $\boldsymbol{A} \equiv \boldsymbol{B} \pmod N$，$\boldsymbol{C} \equiv \boldsymbol{D} \pmod N$，则 $\boldsymbol{A}\boldsymbol{C} \equiv \boldsymbol{B}\boldsymbol{D} \pmod N$。

证明 设 $\boldsymbol{U} = \boldsymbol{A}\boldsymbol{C} = (u_{i,j})$，$\boldsymbol{V} = \boldsymbol{B}\boldsymbol{D} = (v_{i,j})$。于是可证 $u_{ij} \equiv v_{ij} \pmod N$。证毕。

性质 4 若 $\boldsymbol{B}\boldsymbol{C} \equiv \boldsymbol{O} \pmod N$，$|\boldsymbol{C}| \perp N$，则必有 $\boldsymbol{B} \equiv \boldsymbol{O} \pmod N$（$\boldsymbol{O}$ 表示零矩阵）。

证明 用定理 1 及性质 3。

性质 5 若则 $\boldsymbol{A} \equiv \boldsymbol{B} \pmod N$ 则 $\boldsymbol{A}\boldsymbol{B} \equiv \boldsymbol{B}\boldsymbol{A} \pmod N$。

证明 用性质 1 与 3。

性质 6 若 $\boldsymbol{A} \equiv \boldsymbol{B} \pmod N$，则行列式 $|\boldsymbol{A}| \equiv |\boldsymbol{B}| \pmod N$。

性质 7 若 $\boldsymbol{A} \equiv \boldsymbol{O} \pmod M$，$\boldsymbol{B} \equiv \boldsymbol{O} \pmod N$ 则 $\boldsymbol{A}\boldsymbol{B} \equiv \boldsymbol{O} \pmod{MN}$。

性质 8 若 $\boldsymbol{A}^m \equiv \boldsymbol{I} \pmod N$，则 $\delta_N(\boldsymbol{A}) \mid m$

* 收稿日期：2004－04－20
基金项目：国家自然科学基金资助项目（60373082）
作者简介：黎罗罗（1945 年生），男，教授；E-mail：lnslll@zsu.edu.cn

（用 $k \mid m$ 表示 k 整除 m）。

证明 用数论中典型的整除性证法，但须借助定理 1 及性质 3。证毕。

性质 9 若 $\boldsymbol{A} \equiv \boldsymbol{B} \pmod N$ 且行列式 $|\boldsymbol{A}| \perp N$，则 $|\boldsymbol{B}| \perp N$ 且 $\delta_N(\boldsymbol{B}) = \delta_N(\boldsymbol{A})$。

证明 记 $\delta = \delta_N(\boldsymbol{A})$。由性质 3，$\boldsymbol{A}^{\delta} \equiv \boldsymbol{B}^{\delta} \equiv \boldsymbol{I} \pmod N$，可见 $\boldsymbol{B}$ 有周期，$|\boldsymbol{B}| \perp N$；由性质 8，$\delta_N(\boldsymbol{B}) \mid \delta$，即 $\delta_N(\boldsymbol{B}) \mid \delta_N(\boldsymbol{A})$. 同理证 $\delta_N(\boldsymbol{A}) \mid \delta_N(\boldsymbol{B})$，故 $\delta_N(\boldsymbol{B}) = \delta_N(\boldsymbol{A})$。证毕。

2 置乱变换周期分析

引理 1 设整数 $s \geqslant 2$，若 $\boldsymbol{BC} \equiv \boldsymbol{O} \pmod{N^{s+1+l}}$，$\boldsymbol{B} \equiv \boldsymbol{O} \pmod{N^{1+l}}$，$\boldsymbol{C} \equiv N\boldsymbol{I} \pmod{N^s}$，则必有 $\boldsymbol{B} \equiv \boldsymbol{O} \pmod{N^{s+l}}$，其中 $l = 1, 2, \cdots$。

证明 用反证法。设 $\boldsymbol{B}$ 的元素 $b_{rt} \not\equiv 0 \pmod{N^{s+l}}$，考虑矩阵 $\boldsymbol{V} = \boldsymbol{BC}$ 的元素 v_{rt}。由 $n^s \mid c_{jt}$（$j \neq t$）及 $N^{1+l} \mid b_{rj}$ 知 $v_{rt} = \sum_{j=1}^{n} b_{rj} c_{jt} \equiv b_{rt} c_{tt} \pmod{N^{s+1+l}}$，所以 $b_{rt} c_{tt} \equiv 0 \pmod{N^{s+1+l}}$。$\boldsymbol{C}$ 的对角元 $c_{tt} = hN$，$h \perp N$，于是 $N^{s+1+l} \mid b_{rt} c_{tt}$ 导致 $N^{s+l} \mid b_{rt}$，这与反证法的假设矛盾。证毕。

引理 2 设 $N \perp\!\!\!\perp |\boldsymbol{A}|$，$k \mid N$ 则

（1）$k \perp\!\!\!\perp |\boldsymbol{A}|$；

（2）$\delta_k(\boldsymbol{A}) \mid \delta_N(\boldsymbol{A})$。

证明

（1）显然。

（2）记 $\delta_k = \delta_k(\boldsymbol{A})$，$\delta_N = \delta_N(\boldsymbol{A})$。由 $\boldsymbol{A}^{\delta_N} \equiv \boldsymbol{I} \pmod N$，知 $\boldsymbol{A}^{\delta_N} \equiv \boldsymbol{I} \pmod k$，从而由性质 8 知 $\delta_k \mid \delta_N$。证毕。

引理 3 若将 $N = m^j$ 时变换式（1）的周期记为 α_j，则同时成立 $\alpha_j \mid \alpha_{j+1}$ 及 $\alpha_{j+1} \mid m\alpha_j$。

证明 因为

$$\boldsymbol{A}^{\alpha_j} \equiv \boldsymbol{I} \pmod{m^j} \tag{2}$$

故对 $k = 0, 1, 2, \cdots, m-1$（用性质 3）均有

$$(\boldsymbol{A}^{\alpha_j})^k \equiv \boldsymbol{I} \pmod{m^j} \tag{3}$$

其中规定 $\boldsymbol{A}^0 \equiv \boldsymbol{I}$。将式（3）中 m 个式子相加，得（见性质 2）

$$\boldsymbol{A}^{(m-1)a_j} + \cdots + \boldsymbol{A}^{2\alpha_j} + \boldsymbol{A}^{\alpha_j} + \boldsymbol{I} \equiv m\boldsymbol{I} \pmod{m^j}$$

可见

$$\boldsymbol{A}^{(m-1)a_j} + \cdots + \boldsymbol{A}^{2\alpha_j} + \boldsymbol{A}^{\alpha_j} + \boldsymbol{I} \equiv \boldsymbol{O} \pmod m \tag{4}$$

由式（2）、（4）可见

$$\boldsymbol{A}^{m\alpha_j} - \boldsymbol{I} = (\boldsymbol{A}_j^{\alpha} - \boldsymbol{I})(\boldsymbol{A}^{(m-1)a_j} + \cdots + \boldsymbol{A}^{2\alpha_j} + \boldsymbol{A}^{\alpha_j} + \boldsymbol{I} \equiv \boldsymbol{O} \pmod{m^{j+1}})$$

即 $\boldsymbol{A}^{m\alpha_j} \equiv \boldsymbol{I} \pmod{m^{j+1}}$。可见 $\alpha_{j+1} \mid m\alpha_j$。另方面显然 $\boldsymbol{A}^{\alpha_{j+1}} \equiv \boldsymbol{I} \pmod{m^j}$ 故由性质 8 得 $\alpha_j \mid \alpha_{j+1}$。证毕。

引理 4 设 $N \perp |\boldsymbol{A}|$，$k \perp |\boldsymbol{A}|$，且 $k \perp N$，于是

（1）$kN \perp |\boldsymbol{A}|$；

（2）$\delta_{kN}(\boldsymbol{A}) = [\delta_k(\boldsymbol{A}), \delta_N(\boldsymbol{A})]$。（用 $[m_1, m_2, \cdots, m_s]$ 记 $m_1, m_2, \cdots, m_s$ 的最小公倍数）。

证明 （1）因为 $|\boldsymbol{A}|$ 与 k，N 均互素，故 $|\boldsymbol{A}|$ 与 kN 互素，（1）得证。记 $\delta_k = \delta_k(\boldsymbol{A})$，$\delta_N = \delta_N(\boldsymbol{A})$，$\delta = \delta_{kN}(\boldsymbol{A})$，$\eta = [\delta_k(\boldsymbol{A}), \delta_N(\boldsymbol{A})]$。由引理 2 之（2），$\delta_k \mid \delta$，$\delta_N \mid \delta$ 从而 $\eta \mid \delta$ 另方面，显然 $\boldsymbol{A}^{\eta} \equiv \boldsymbol{I} \pmod k$，$\boldsymbol{A}^{\eta} \equiv \boldsymbol{I} \pmod N$，即 $\boldsymbol{A}^{\eta} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod k$，$\boldsymbol{A}^{\eta} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod N$，由 $k \perp N$ 知 $\boldsymbol{A}^{\eta} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod{kN}$，即 $\boldsymbol{A}^{\eta} \equiv \boldsymbol{I} \pmod{kN}$，可见 $\delta \mid \eta$。证得 $\delta = \eta$。证毕。

推广引理 4 的结果可得

引理 5 若 $m_1, m_2, \cdots, m_s$ 两两互素，且 $m_i \perp |\boldsymbol{A}|$（$i = 1, 2, \cdots, s$）。记 $\delta_i = \delta_{m_i}(\boldsymbol{A})$，$N = m_1 m_2 \cdots m_s$。于是

（1）$N \perp |\boldsymbol{A}|$；

（2）$\delta_N(\boldsymbol{A}) = [\delta_1, \delta_2, \cdots, \delta_s]$。

现在可以着手对变换式（1）的周期作进一步分析。已知有如下基本结果[8]。

算术基本定理 任一正整数 $N > 1$ 均可分解为若干个素数及其幂的乘积：

$$N = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} \tag{5}$$

其中，p_j 为互不相等的素数，整数 $n_j \geqslant 1$。

由引理 5 有以下定理。

定理 2 设 $N \perp\!\!\!\perp |\boldsymbol{A}|$，且 N 的素数分解如（5）式，则 $\delta_N(\boldsymbol{A})$ 是 δ_1，δ_2，$\cdots$，δ_s 的最小公倍数：$\delta_N(\boldsymbol{A}) = [\delta_1, \delta_2, \cdots, \delta_s]$，其中 δ_j 是 $\boldsymbol{A}$ 在模 $p_j^{n_j}$ 下的周期：即 δ_j 是使 $\boldsymbol{A}^d \equiv \boldsymbol{I} \pmod{p_j^{n_j}}$ 成立的最小正整数 d。

因此，变换式（1）的周期（如果存在的话）问题归结为：对给定的矩阵 $\boldsymbol{A}$，就素数 p 及幂 j，求 $\boldsymbol{A}$ 关于模 p^j 的周期的问题. 以下记这个周期为 β_j。称序列 $L_p(\boldsymbol{A}) = \{\beta_1, \beta_2, \cdots\}$ 为 $\boldsymbol{A}$ 关于素数 p 的周期序列。对该序列的 β_j 成立如下周期递推定理 3 与定理 4：

定理 3 $\beta_{j+1} = \beta_j$ 或 $\beta_{j+1} = p\beta_j$ 二者必居其一。

证明 在引理 3 中取 $m = p$，于是同时有 $\beta_j \mid \beta_{j+1}$ 及 $\beta_{j+1} \mid p\beta_j$，注意到 p 是素数，故知结论成立。

进一步有

定理 4 设 $s \geqslant 2$。

（1）若 $\boldsymbol{A}^{\beta_1} \equiv \boldsymbol{I} \pmod{p^s}$ 但 $\boldsymbol{A}^{\beta_1} \not\equiv \boldsymbol{I} \pmod$

p^{s+1}）则

$$\beta_s = \beta_{s-1} = \cdots = \beta_1 \tag{6}$$

$\beta_{s+1} = p\beta_s = p\beta_1$, $\beta_{s+2} = p\beta_{s+1} = p^2\beta_1$, …, 即

$$\beta_{s+j} = p\beta_{s+j-1} = p^j\beta_1 \tag{7}$$

（2）若 $\boldsymbol{A}^{\beta_1} \not\equiv \boldsymbol{I} \pmod{p^2}$, 但 $\boldsymbol{A}^{\beta_2} \equiv \boldsymbol{I} \pmod{p^s}$ 而 $\boldsymbol{A}^{\beta_2} \not\equiv \boldsymbol{I} \pmod{p^{s+1}}$ 则

$$\beta_2 = p\beta_1 \tag{8}$$

$$\beta_s = \beta_{s-1} = \cdots = \beta_2 \tag{9}$$

$$\beta_{s+1} = p\beta_s,\ \beta_{s+2} = p\beta_{s+1},\ \cdots,$$

即

$$\beta_{s+j} = p^j\beta_2 \tag{10}$$

证明　由

$$\boldsymbol{A}^{\beta_1} \equiv \boldsymbol{I} \pmod{p^s}$$

知　　$\boldsymbol{A}^{\beta_1} \equiv \boldsymbol{I} \pmod{p^j}\ (1 \leqslant j \leqslant s)$

所以　　$\beta_j \mid \beta_1,\ 1 \leqslant j \leqslant s$

但由定理 3（或性质 8）的结论知 $\beta_1 \mid \beta_j$。故

$$\beta_s = \beta_{s-1} = \cdots = \beta_1$$

此为结论（6）。由定理 3 知 $\beta_{s+1} = \beta_s$ 或 $\beta_{s+1} = p\beta_s$。但若 $\beta_{s+1} = \beta_s$ 则导致 $\beta_{s+1} = \beta_s = \cdots = \beta_1$。这与 $\boldsymbol{A}^{\beta_1} \not\equiv \boldsymbol{I} \pmod{p^{s+1}}$ 矛盾。所以 $\beta_{s+1} = p\beta_s$。已经知道 $\beta_{s+2} = \beta_{s+1}$ 或 $\beta_{s+2} = p\beta_{s+1}$ 二者居其一。下面用反证法证明 $\beta_{s+2} = \beta_{s+1}$ 不成立。因为若 $\beta_{s+2} = \beta_{s+1}$ 则由

$$\boldsymbol{A}^{\beta_{s+2}} \equiv \boldsymbol{I} \pmod{p^{s+2}}$$

得

$$\boldsymbol{A}^{\beta_{s+1}} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod{p^{s+2}}$$

又由已证之 $\beta_{s+1} = p\beta_s$ 得

$$\boldsymbol{A}^{p\beta_s} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod{p^{s+2}}$$

即

$$(\boldsymbol{A}^{\beta_s} - \boldsymbol{I})\left(\sum_{k=0}^{p-1}\boldsymbol{A}^{k\beta_s}\right) \equiv \boldsymbol{O} \pmod{p^{s+2}}$$

与引理 3 证明过程相仿，求和式 $\sum_{k=0}^{p-1}\boldsymbol{A}^{k\beta_s}$ 中每一项满足

$$\boldsymbol{A}^{k\beta_s} \equiv \boldsymbol{I} \pmod{p^s}\ (k = 0, 1, 2, \cdots, p-1)$$

从而

$$\sum_{k=0}^{p-1}\boldsymbol{A}^{k\beta_s} \equiv p\boldsymbol{I} \pmod{p^s}$$

将 $\sum_{k=0}^{p-1}\boldsymbol{A}^{k\beta_s}$ 看作引理 1（取 $N = p$, $l = 1$）中的 $\boldsymbol{C}$, $(\boldsymbol{A}^{\beta_s} - \boldsymbol{I})$ 看作引理 1 中的 $\boldsymbol{B}$，则得

$$\boldsymbol{A}^{\beta_s} - \boldsymbol{I} \equiv \boldsymbol{O} \pmod{p^{s+1}}$$

从而 $\beta_{s+1} \mid \beta_s$。此与先前所得 $\beta_{s+1} = p\beta_s$ 矛盾。这就证明了 $\beta_{s+2} = p\beta_{s+1}$。类似地，可证

$$\beta_{s+3} = p\beta_{s+2},\ \cdots,\ \beta_{s+j} = p\beta_{s+j-1} = \cdots = p^j\beta_1$$

定理结论（1）证毕。

（2）因 $\beta_2 \neq \beta_1$，故（8）式成立。仿（1）中式（6）的证明知式（9）成立。式（10）的证明与（7）相仿。证毕。

推论　对固定的素数 p，矩阵 $\boldsymbol{A}$ 的周期序列 $L_p(\boldsymbol{A})$ 取下列 2 种可能的模式之一：

（1）存在 $s \geqslant 2$，使得

$$\beta_1 = \beta_2 = \cdots = \beta_s,\ \beta_{s+j} = p^j\beta_2,\ j = 1, 2, \cdots$$

（2）存在 $s \geqslant 2$，使得

$$p\beta_1 = \beta_2 = \cdots = \beta_s,\ \beta_{s+j} = p^j\beta_2,\ j = 1, 2, \cdots$$

3　周期特征码

定理 5　设 p 为素数，$\boldsymbol{A}$ 为整数矩阵，且 $|\boldsymbol{A}| \perp p$，则对于 $j = 1, 2, \cdots$，无穷个变换

$$\boldsymbol{x}' \equiv \boldsymbol{A}\boldsymbol{x} \pmod{p^j} \tag{11}$$

的周期均可由 3 个数 β_1，β_2，t 完全确定，其中 β_1，β_2 是 $L_p(\boldsymbol{A})$ 的前 2 个数，t 是使得 $\beta_{2+t} = p\beta_2$ 的整数。

上述 3 个数与素数 p 及矩阵 $\boldsymbol{A}$ 有关，记为 $l_p(\boldsymbol{A}) = [\beta_1, \beta_2; t]$，称之为变换系列（11）的周期特征码。它由 3 个分量组成。由周期递推关系定理，式（11）中任一变换的周期信息已压缩在周期特征码中。

现就文献中常见置乱变换给出若干周期特征码及其应用例子如下：

（1）2 维 Arnold 变换矩阵[11] 关于头 3 个素数的周期特征码与周期序列

$l_2(\text{Arnold-2}) = [3, 3; 1]$，于是

$L_2(\text{Arnold-2}) = \{3, 3, 6, 12, 24, \cdots\}$

$l_3(\text{Arnold-2}) = [4, 12; 1]$，于是

$L_3(\text{Arnold-2}) = \{4, 12, 36, 108, 324, \cdots\}$

$l_5(\text{Arnold-2}) = [10, 50; 1]$，于是

$L_5(\text{Arnold-2}) = \{10, 50, 250, 1\,250, 6\,250, \cdots\}$

（2）3 维 Arnold 变换矩阵 [1]　关于头 3 个素数的周期特征码与周期序列

$l_2(\text{Arnold-3}) = [7, 7; 1]$，于是

$L_2(\text{Arnold-3}) = \{7, 7, 14, 28, 56, \cdots\}$

$l_3(\text{Arnold-3}) = [13, 39; 1]$，于是

$L_3(\text{Arnold-3}) = \{13, 39, 117, 351, 1\,053, \cdots\}$

$l_5(\text{Arnold-3}) = [31, 155; 1]$，于是

$L_5(\text{Arnold-3}) = \{31, 155, 775, 3\,875, 19\,375, \cdots\}$

（3）3 维 Fibonacci Q 变换矩阵[13] 关于头 3 个素数的周期特征码与周期序列

$l_2(\text{FQ-3}) = [7, 14; 1]$，于是

$L_2(\text{FQ-3}) = \{7, 14, 28, 56, 112, \cdots\}$

l_3(FQ-3) = [8, 24; 1]，于是

L_3(FQ-3) = {8, 24, 72, 216, 648, …}

l_5(FQ-3) = [31, 155; 1]，于是

L_5(FQ-3) = {31, 155, 775, 3 875, 19 375, …}

（4）2 维 AF 变换矩阵[3] 关于头 3 个素数的周期特征码与周期序列

l_2(AF-2) = [1, 2; 1]，于是

L_2(AF-2) = {1, 2, 4, 8, 16, …}

l_3(AF-2) = [3, 9; 1]，于是

L_2(AF-2) = {3, 9, 27, 81, 243, …}

l_5(AF-2) = [5, 25; 1]，于是

L_5(AF-2) = {5, 25, 125, 625, 3 125, …}

例如，若置乱变换（1）以整数 $N=810\,000=2^4\times3^4\times5^4$ 为模，则

2 维 Arnold 变换的周期为

[12, 108, 1 250] = 67 500

显然，求最小公倍数[12, 108, 1 250] 归结为与素数 2，3，5 相应的各周期特征码的第 1 或第 2 个分量的素分解。类似地，

3 维 Arnold 变换的周期为

[28, 351, 3 875] = 38 083 500;

3 维 Fibonacci-Q 变换的周期为

[56, 216, 3 875] = 5 859 000;

2 维 AF 变换的周期为

[8, 81, 625] = 405 000。

本文从理论上揭示了以 Arnold 变换为代表的置乱变换（1）的周期的内在规律. 整数的素分解式（5）在密码学理论中是典型陷门单向的，在取得素数分解的密钥后，置乱变换（1）的周期归结为有针对性和相对简单得多的周期特征码问题。

参考文献：

[1] QI D X, ZHOU J CH, HAN X Y. 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] 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.

[3] QI D X, WANG D SH, YANG D L. Matrix transformation of digital image and its periodicity[J]. Progress in Natural Science, 2001, 11(7): 542－549.

[4] 齐东旭. 矩阵变换及其在图像信息隐蔽中的应用研究[J]. 北方工业大学学报, 1999, 11(1): 24－28.

[5] 王道顺, 杨地莲, 齐东旭. 数字图像的两类非线性变换及其周期性[J]. 计算机辅助设计与图形学学报, 2001, 13(9): 828－833.

[6] 朱桂斌, 曹长修, 胡中豫, 等. 基于仿射变换的数字图像置乱加密算法[J]. 计算机辅助设计与图形学学报, 2003, 15(6): 711－715.

[7] 齐东旭. 分形及其计算机生成[M]. 北京: 科学出版社, 1994.

[8] 潘承洞, 潘承彪. 简明数论[M]. 北京: 北京大学出版社, 1998.

On Periods of Arnold-type Transformations

LI Luo-huo

(School of Mathematics and Scientific Computation, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Arnold transformation is one of the techniques for scrambling digital images for the sake of communication security. Under certain conditions Arnold transformation $\boldsymbol{A}$ modulo N possesses periodicity by which the encoder and decoder can control randomly the number of the transformations in the image transportation. To study periodicity of Arnold-type transformations, basic modular arithmetic properties of integer matrices are firstly established. A theorem is secondly obtained to show that the periodicity of $\boldsymbol{A}$ modulo N equals the least common multiple of all those moduloes mutually prime factors of N. Thus the periodicity analysis can be reduced to transformation modulo prime numbers (and their powers). Finally formulas for periodicity of transformation modulo powers of prime number are proved and the concept of period character code is introduced by which an elegant and concise method to calculate the period of Arnold-type scrambling transformation is obtained.

Key words: digital image scrambling; Arnold transformation; information hiding; period character code