离散Arnold变换改进及其在图像置乱加密中的应用*

吴成茂†

(西安邮电大学电子工程学院, 西安 710121)

(2013 年 12 月 3 日收到; 2014 年 1 月 23 日收到修改稿)

为了改善传统二维 Arnold 变换用于图像置乱加密的效果, 提出了离散 Arnold 变换的改进方法, 并将其用于图像置乱加密测试研究. 该方法利用现有离散标准映射的构造思想, 将传统离散二维 Arnold 变换表达式中第一个变换表达式所对应变换结果非线性融入第二个变换表达式, 实现经典离散二维 Arnold 变换的非线性去拟仿射化修改, 以便快速改善图像置乱加密效果. 数学证明改进方法不再保持现有离散二维 Arnold 变换所具有的拟仿射不变性, 但是改进变换仍是一种具有周期性的可逆映射, 将其用于图像置乱加密时, 利用其周期性或逆变换能恢复置乱前原图像. 大量实验结果表明, 本文所建议的改进方法是有效的, 相比现有的离散 Arnold 变换更具有实用价值意义.

关键词: 图像置乱, Arnold 变换, 可逆映射, 置乱效果

PACS: 05.45.Gg **DOI:** 10.7498/aps.63.090504

1 引 言

Arnold 变换是一种从环面到自身的混沌映射, 又简称为 Cat 映射 [1]. 它具有优美的数学性质 [2]: 1) 可逆的; 2) 保面积的; 3) 唯一双曲不动点; 4) 环面上的周期轨道点集合是稠密的; 5) 拓扑可迁移性; 6) 遍历和混合性; 7) Anosov 微分同胚的, 特别是具有结构稳定性. 针对传统 Arnold 变换是一种连续映射不便于处理离散问题的需要, 于是 Dyson 等人 [3] 首次提出了离散型 Arnold 变换并研究其周期性及其周期上界, 后来仍有大量文献不断探讨其周期性质 [4−8]. 从数论角度看, 离散型 Arnold 变换的本质是整数域上的单模数线性同余方程组, 其解或逆变换已得到深入讨论 [9−13]. 针对 Arnold 变换具有良好的混沌动力学特性, 已广泛应用于图像信息安全保护、最优化问题求解、控制等众多领域, 其中我国学者齐东旭等人 [14−15] 率先提出 Arnold 变换或单模数线性同余方程组用于图像加密、信息隐藏等研究, 引起了众多从事图像信息安全保护学者的高度重视, 现今已涌现大量文献 [16−20] 探讨 Arnold 变换在图像置乱加密中的应用. 针对传统 Arnold 变换的变换矩阵系数是固定不变的缺陷, 马在光等人 [21] 提出了二维广义参数型 Arnold 变换并用于图像置乱加密. Chen 等人 [16] 提出利用二维广义 Arnold 变换构造三维 Arnold 变换. 赵亮等人 [22] 提出一种 Z 矩阵映射的三维 Arnold 变换.Yang 等人 [23] 提出了任意高维 Arnold 变换矩阵的 A 型和 B 型矩阵但缺乏灵活性. 李用江等人 [24,25] 探讨了等差序列构造广义高维 Arnold 变换矩阵的方法. 李用江和李昌利等人 [25] 又进一步提出了 Fibonacci 序列、Dirichlet 序列, 以及二者相结合构造广义 Arnold 变换矩阵的一般方法, 甚至其逆矩阵求解方法也在其博士论文中进行了详细讨论 [26]. Fransson [27] 提出了利用广义 Fibonacci 序列构造 Arnold 变换矩阵的一般方法. 最近, Wu 等人 [28] 提出了一种三维广义 Arnold 变换矩阵构

* 国家自然科学基金 (批准号: 90607008, 61073106) 和陕西省教育厅科研计划专项 (批准号:2013JK1129) 资助的课题.

† 通讯作者. E-mail: wuchengmao123@sohu.com

造方法, 甚至可推广至高维 Arnold 变换. 这些构造方法为广义 Arnold 变换理论的发展和实际置乱加密应用起到非常重要的作用, 但它们对现有 Arnold 变换本身的安全性并没有实质性的改善, 因 Arnold 变换本身是一种拟仿射变换, 具有线性密码学特性, 导致其安全性较差 [29,30], 特别是广义 Arnold 变换对零向量 $(0,0,\cdots,0)$ 置乱后并不发生改变, 很容易受到安全攻击, 于是将 Arnold 变换进行适当修改可获取安全性更高的改进形式 [31,32]. 另外,Arnold 变换本身用于图像置乱时因其周期短且置乱后图像存在明显的纹理效果等不足, 这方面的问题未引起学者们的高度重视. 因此, 本文将对现有 Arnold 变换表达式中引入非线性量, 一方面是改善该变换本身所具有的拟仿射特性的不足并延长其周期, 另一方面提高该变换的扩散能力, 并改善图像置乱效果所具有的明显纹理特性. 大量实验结果表明, 本文所建议的改进 Arnold 变换方法是有效的.

2 Arnold 变换理论

Arnold 变换又称为猫映射, 它是由俄国数学家 Arnold 引入的, 因常采用一张猫脸演示而得名, 其具体变换表达式为

$$\begin{aligned} x_{n+1} &= (x_n + y_n) \bmod 1, \\ y_{n+1} &= (x_n + 2y_n) \bmod 1, \end{aligned} \tag{1}$$

其中 mod1 表示只取小数部分, 即 $x \bmod 1 = x - \lfloor x \rfloor$. 因此, (x_n, y_n) 的相空间被限制在单位正方形 $[0,1]\times[0,1]$ 内, 将其采用矩阵形式可描述为

$$\begin{aligned} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \\ &= \boldsymbol{C} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1, \end{aligned} \tag{2}$$

其中 $\boldsymbol{C} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ 是变换矩阵, 其行列式值为 1. 因此, 该映射是一个保面积且没有吸引子的一一映射, 单位正方形内任意一点唯一变换到单位正方形内的另一点. 该猫映射具有非常典型的产生混沌运动的两个因素是拉伸 (乘以矩阵 $\boldsymbol{C}$ 使 x, y 的值变大) 和折叠 (取模 mol1 使 x, y 又折回单位矩形内). 事实上猫映射确实是混沌映射. 两个 Lyapunov 指数分别为 $\ln(0.5(3+\sqrt{5}))$ 和 $\ln(0.5(3-\sqrt{5}))$, 即通过计算矩阵 $\boldsymbol{C}$ 的两个特征值所获得的.

从几何方面考虑可将其相空间从 $[0,1]\times[0,1]$ 推广至 $\{0,1,\cdots,N-1\}\times\{0,1,\cdots,N-1\}$, 于是获得离散化的猫映射表达式为

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N. \tag{3}$$

由于离散化的猫映射状态空间是有限的, 可能不再具有良好的混沌特性; 但从几何上看仍具有猫映射的拉伸和折叠性质, 这就导致相邻的两点 (i,j) 和 $(i,j+1)$ 经多次离散变换迭代后不再相邻, 表明了该变换具有一定的初始值敏感性. 利用这一点性质, 可以打乱一幅图像相邻像素的位置, 使得从图像中无法获取原图像相关信息, 从而达到保密图像信息的目的.

离散猫映射 (3) 式存在一个不动点是 $(0,0)$, 这将导致该变换存在严重的安全隐患. 另外, 该离散变换存在一定的周期性, 且随参数 N 变化导致其周期有显著差别, 鲍江宏 [33] 详细探讨了其周期与参数 N 选取之间的关系. 离散猫映射 (3) 式用于图像置乱加密因缺乏一定参数 N 选取导致其加密安全性弱, 甚至加密结果存在唯一性, 不符合传统密码学基本要求. 为此, 许多学者探讨离散猫映射 (3) 式中的变换矩阵 $\boldsymbol{C}$ 的构造问题和约束条件等, 现已形成较为完善的广义 Arnold 变换理论.

3 广义 Arnold 变换方法

为了提高离散 Arnold 变换用于图像置乱的灵活和安全性, 对其变换矩阵 $\boldsymbol{C}$ 各元素参数化并满足一定约束条件时, 则获得如下广义 Arnold 变换为

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N, \tag{4}$$

其中参数 a, b, c, $d \in G$ 且 $\gcd(ad-bc, N) = 1$.

针对广义 Arnold 变换 (4) 式, 若 $a = 1$, $d = 1+bc$, 或 $a = 1+bc$, $d = 1$, 或 $b = 1$, $c = ad-1$, 或 $b = ad-1$, $c = 1$ 时, 则获得典型广义 Arnold 变换 [21]. 将 (4) 式转化为方程组形式为

$$\begin{aligned} x_{n+1} &= (ax_n + by_n) \bmod N, \\ y_{n+1} &= (cx_n + dy_n) \bmod N, \end{aligned} \tag{5}$$

可进一步转化为等价形式

$$x_{n+1} = ax_n + by_n - l_1 N, \tag{6}$$

$$y_{n+1} = cx_n + dy_n - l_2 N, \tag{7}$$

其中 l_1, l_2 是整数. 利用解线性方程组的消元法解方程组 (6) 式和 (7) 式时, 则获得广义 Arnold 变换的反变换表达式为

$$\begin{aligned}\begin{pmatrix} x_n \\ y_n \end{pmatrix} &= [ad-bc]_N^{-1} \begin{pmatrix} d & (N-b) \\ (N-c) & a \end{pmatrix} \\ &\quad \times \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \bmod N \\ &= [ad-bc]_N^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \bmod N, \end{aligned} \tag{8}$$

其中 $[ad-bc]_N^{-1}$ 是正整数且使得

$$((ad-bc)\,[ad-bc]_N^{-1}) \bmod N = 1.$$

另外, 针对整数型方程组 (6) 和 (7) 式, 可以得到类似传统克莱姆法则的求解法为 [34]

$$\begin{aligned} x_n &= \left(\left[\begin{vmatrix} a & b \\ c & d \end{vmatrix} \right]_N^{-1} \cdot \begin{vmatrix} x_{n+1} & b \\ y_{n+1} & d \end{vmatrix} \right) \bmod N, \\ y_n &= \left(\left[\begin{vmatrix} a & b \\ c & d \end{vmatrix} \right]_N^{-1} \cdot \begin{vmatrix} a & x_{n+1} \\ c & y_{n+1} \end{vmatrix} \right) \bmod N. \end{aligned} \tag{9}$$

通过矩阵运算法, 可判定反变换 (8) 和 (9) 式是等价的. 将反变换 (8) 式可用于置乱后图像的快速复原, 相比利用其周期性恢复原图像更快, 特别有利于视频图像置乱与恢复的快速需要. 另外, 张涛等人 [9] 所给出 Arnold 反变换算法仅是反变换 (8) 式的一种特例.

针对二维广义 Arnold 变换表达式仅适合两变量的平面图像像素位置置乱的不足, Chen 等人 [16] 提出了广义二维 Arnold 变换构造广义三维 Arnold 变换方法, 但其构造所得矩阵显得非常复杂, 于是已涌现大量文献探讨广义三维 Arnold 变换矩阵构造法 [22−28], 这为广义三维 Arnold 变换应用提供了一定依据. 一般而言, 广义三维 Arnold 变换可描述为

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \bmod N, \tag{10}$$

其中矩阵 $\boldsymbol{C} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ 称为变换矩阵且满足约束条件为

1) 参数 $a, b, \cdots, f$ 应为整数值;

2) 变换矩阵 $\boldsymbol{C}$ 的行列式值满足

$$\gcd(\det \boldsymbol{C}, N) = 1.$$

正是由于约束条件 $\gcd(\det \boldsymbol{C}, N) = 1$ 使得广义三维 Arnold 变换具有周期性、保面积性和可逆性. 该变换周期特性的研究还未引起学者们的高度重视, 其逆变换的研究主要针对特殊变换矩阵有一定探讨和应用 [22,24−26,32]. 针对广义三维 Arnold 变换的一般情形, 周利敏 [12] 提出了较为复杂的消元法获取其相应的逆变换结果, 但不便于理论分析和实际应用, 于是本文仍给出类似传统克莱姆法则的求解法, 其具体表达式为

$$\begin{aligned} x_n &= \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} x_{n+1} & b & c \\ y_{n+1} & e & f \\ z_{n+1} & h & i \end{vmatrix} \right) \bmod N, \\ y_n &= \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} a & x_{n+1} & c \\ d & y_{n+1} & f \\ g & z_{n+1} & i \end{vmatrix} \right) \bmod N, \\ y_n &= \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} a & b & x_{n+1} \\ d & e & y_{n+1} \\ g & h & z_{n+1} \end{vmatrix} \right) \bmod N, \end{aligned} \tag{11}$$

其中 $[\det \boldsymbol{C}]_N^{-1} \in \{1, 2, \cdots, N-1\}$ 且

$$([\det \boldsymbol{C}]_N^{-1} \cdot \det \boldsymbol{C}) \bmod N = 1.$$

同理, 针对任意广义高维 Arnold 变换, 可得到类似传统克莱姆法则的求逆变换方法, 相比现有特殊高维变换矩阵求逆变换表达式 [15,23,32] 更具有一定的普适性; 同时, 本文方法便于计算机编程快速实现.

4 广义 Arnold 变换的改进方法

无论是二维广义 Arnold 变换, 还是高维广义 Arnold 变换, 它们的数学本质都是一类拟仿射变换, 具有线性密码学特性, 导致其安全性差和置乱加密效果难以令人满意, 于是本文提出一类改进方法.

为了提出广义 Arnold 变换的改进, 先回顾离散标准映射的构造思想, 然后提出本文所建议的改进型广义 Arnold 变换构造法.

在混沌动力学中,有一类映射称为标准映射[35,36], 即

$$\begin{aligned} s_1(x,y) &= (x+y) \bmod 2\pi, \\ s_2(x,y) &= (y-k\sin(x+y)) \bmod 2\pi, \end{aligned} \tag{12}$$

其中 k 为一正常数,很容易将表达式(12)推广至一般情形为

$$\begin{aligned} s_1(x,y) &= (x+f(y)) \bmod 2\pi, \\ s_2(x,y) &= (y+g(s_1)) \bmod 2\pi. \end{aligned} \tag{13}$$

为了图像位置置乱及其像素值大小加密, 可将表达式(13)离散为

$$\begin{aligned} x_{n+1} &= (x_n+f(y_n)) \bmod N, \\ y_{n+1} &= (y_n+g(x_{n+1})) \bmod N. \end{aligned} \tag{14}$$

它与传统密码学中的分组密码Feistel结构[37]具有惊人的相似, 这将促使利用离散标准映射的构造思想来改进广义Arnold变换,其详细构造过程如下:

针对广义二维Arnold变换(4)式, 其改进表达式为

$$\begin{aligned} x_{n+1} &= (ax_n+by_n) \bmod N, \\ y_{n+1} &= (cx_n+dy_n+ef(x_{n+1})) \bmod N. \end{aligned} \tag{15}$$

或者

$$\begin{aligned} y_{n+1} &= (cx_n+dy_n) \bmod N, \\ x_{n+1} &= (ax_n+by_n+ef(y_{n+1})) \bmod N, \end{aligned} \tag{16}$$

其中参数 a, b, c, d, $e \in G$ 且 $\gcd(ad-bc,N)=1$, 函数 $f(x_{n+1})$ 或 $f(y_{n+1})$ 都是变量 x_{n+1} 或 y_{n+1} 的非线性函数. 典型函数选取方式如下:

1) $f(x_{n+1})=(x_{n+1})^2+1$;

2) $f(x_{n+1})=(x_{n+1})^3+1$;

3) $f(x_{n+1})=(x_{n+1})^4+(x_{n+1})^2+1$.

特别地,若参数 e 选取为0时,改进的广义Arnold变换退化为现有的广义Arnold变换.因此,现有广义Arnold变换是本文所建议新的改进变换表达式特例.

另外,为了进一步增强本文所建议的改进广义Arnold变换的灵活型和安全性,可将(15)和(16)式相结合得到一种复合变换表达式为

$$\begin{aligned} x_n^* &= (ax_n+by_n) \bmod N, \\ y_n^* &= (cx_n+dy_n+ef(x_n^*)) \bmod N, \\ y_{n+1} &= (cx_n^*+dy_n^*) \bmod N, \\ x_{n+1} &= (cx_n^*+dy_n^*+ef(y_{n+1})) \bmod N. \end{aligned} \tag{17}$$

无论是(15)和(16)式, 还是(17)式, 这些修改形式并未改变置乱变换本身,它们仍是具有周期的可逆映射, 但是其周期大小可能发生了改变. 以变换(15)式为例,下面详细探讨其逆变换求解方法.

针对变换(15)式, 将其转化去除模运算的表达式为

$$\begin{aligned} x_{n+1} &= ax_n+by_n-l_1N, \\ y_{n+1} &= cx_n+dy_n+ef(x_{n+1})-l_2N, \end{aligned} \tag{18}$$

其中 $\exists l_1,l_2 \in G$ 使得(18)式成立. 于是获得其逆变换表达式为

$$\begin{aligned} x_n &= \left([ad-bc]_N^{-1} \begin{vmatrix} x_{n+1} & b \\ y_{n+1}-ef(x_{n+1}) & d \end{vmatrix} \right) \bmod N, \\ y_n &= \left([ad-bc]_N^{-1} \begin{vmatrix} a & x_{n+1} \\ c & y_{n+1}-ef(x_{n+1}) \end{vmatrix} \right) \bmod N. \end{aligned} \tag{19}$$

但它与(9)式并没有本质区别, 将其用于图像像素位置置乱将能加速改善置乱效果同时降低其置乱结果的纹理特性.

同理, 针对广义三维Arnold变换(10)式, 可获得提高其安全性的改进型变换表达式为

$$\begin{aligned} x_{n+1} &= (ax_n+by_n+cz_n) \bmod N, \\ y_{n+1} &= (dx_n+ey_n+fz_n+jG_1(x_{n+1})) \bmod N, \\ z_{n+1} &= (gx_n+hy_n+iz_n+kG_2(y_{n+1})) \bmod N, \end{aligned} \tag{20}$$

其中参数 a, b, $\cdots$, j, k 是整数, 且满足约束条件为

1) 矩阵 $\boldsymbol{C}=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ 是非奇异的;

2) $\gcd(\det \boldsymbol{C},N)=1$.

函数 $G_r(x)(r=1,2)$ 是非线性函数, 如 $G_r(x)=x^2+1$ 或 $x^4+x^3+x^2+1$ 等.

该变换(20)式仍是一种可逆映射, 其相应的逆变换表达式为

$$x_n = \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} x_{n+1} & b & c \\ y_{n+1}-jG_1(x_{n+1}) & e & f \\ z_{n+1}-kG_2(y_{n+1}) & h & i \end{vmatrix} \right) \bmod N,$$

$$y_n = \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} a & x_{n+1} & c \\ d & y_{n+1}-jG_1(x_{n+1}) & f \\ g & z_{n+1}-kG_2(y_{n+1}) & i \end{vmatrix} \right) \bmod N,$$

$$y_n = \left([\det \boldsymbol{C}]_N^{-1} \cdot \begin{vmatrix} a & b & x_{n+1} \\ d & e & y_{n+1} - jG_1(x_{n+1}) \\ g & h & z_{n+1} - kG_2(y_{n+1}) \end{vmatrix} \right) \bmod N. \tag{21}$$

同理, 可将改进型广义三维 Arnold 变换推广至任意高维 Arnold 变换, 本文省略其讨论.

5 改进广义 Arnold 变换性质研究

限于篇幅有限, 本文以改进广义二维 Arnold 变换为例, 探讨该类变换所具有的数学性质.

针对改进型广义二维 Arnold 变换 (15) 式, 将其转化为

$$\begin{aligned} x_{n+1} &= ax_n + by_n - l_1 N, \\ y_{n+1} &= cx_n + dy_n + ef(x_{n+1}) - l_2 N, \end{aligned} \tag{22}$$

其中存在 $l_1,\ l_2 \in \{0, 1, \cdots, N-1\}$ 且 $\gcd(ad - bc, N) = 1$. 若选取函数 $f(x) = x^2 + 1$, 则 (22) 式简化为

$$\begin{aligned} x_{n+1} &= ax_n + by_n - l_1 N, \\ y_{n+1} &= cx_n + dy_n + e(x_{n+1}^2 + 1) - l_2 N. \end{aligned} \tag{23}$$

进一步可整理为

$$\begin{aligned} x_{n+1} &= ax_n + by_n - l_1 N, \\ y_{n+1} &= (c - 2eal_1 N)x_n + ea^2 x_n^2 + (d - 2ebl_1 N)y_n \\ &\quad + eb^2 y_n^2 + 2eabx_n y_n + e - l_2 N. \end{aligned} \tag{24}$$

很显然, 变换 (24) 式因具有非线性项, 导致该变换不再是一种拟仿射变换, 将其用于图像置乱加密时不再具有传统线性密码学特性, 因而具有一定程度抵抗差分攻击的能力.

为了证明 (15) 式是一一可逆映射, 该证明可分两步完成: 其一是证明 (15) 式是单值映射; 其二是证明 (15) 式的逆变换是单值映射. 限于篇幅有限仅给出第一步的证明过程.

证明 将 (15) 式转化为二元函数表达式为

$$\begin{aligned} s_1(x, y) &= (ax + by) \bmod N, \\ s_2(x, y) &= (cx + dy + ef(s_1(x, y))) \bmod N. \end{aligned} \tag{25}$$

假设二元组 (x_1, y_1) 和 (x_2, y_2) 经二元函数 (25) 式都映射为相等值, 即 $(s_1(x_1, y_1), s_2(x_1, y_1)) = (s_1(x_2, y_2), s_2(x_2, y_2))$, 于是有

$$s_1(x_1, y_1) = (ax_1 + by_1) \bmod N, \tag{26}$$

$$s_1(x_2, y_2) = (ax_2 + by_2) \bmod N, \tag{27}$$

$$s_2(x_1, y_1) = (cx_1 + dy_1 + ef(s_1(x_1, y_1))) \bmod N, \tag{28}$$

$$s_2(x_2, y_2) = (cx_2 + dy_2 + ef(s_1(x_2, y_2))) \bmod N. \tag{29}$$

利用 $s_1(x_1, y_1) = s_1(x_2, y_2)$ 和 $s_2(x_1, y_1) = s_2(x_2, y_2)$, 将 (26) 至 (29) 式简化为

$$\begin{aligned} 0 &= (a(x_1 - x_2) + b(y_1 - y_2)) \bmod N, \\ 0 &= (c(x_1 - x_2) + d(y_1 - y_2)) \bmod N. \end{aligned} \tag{30}$$

再此考虑到 $\gcd(ad - bc, N) = 1$, 于是有

$$\begin{aligned} (x_1 - x_2) &\bmod N = 0, \\ (y_1 - y_2) &\bmod N = 0. \end{aligned}$$

又因 $x_1,\ x_2,\ y_1,\ y_2 \in \{0, 1, \cdots, N-1\}$, 于是有 $x_1 = x_2$ 和 $y_1 = y_2$ 成立. 因此, (15) 式是单值映射. 同理, 针对 (15) 式的逆变换表达式可证明仍是单值映射. 综合上述两方面可判断 (15) 式可逆一一映射.

另外, 根据有限整数域上的可逆变换一定存在变换周期的判定定理 [38], 可得知变换 (15) 式仍是一种具有周期的可逆一一映射. 同理, 任何改进的高维广义 Arnold 变换也具有周期性.

6 改进广义 Arnold 变换图像加密算法

离散二位 Arnold 变换及其改进型 Arnold 变换主要用于图像像素位置置乱, 打乱图像相邻像素并使其像素空间分布尽可能均匀. 齐东旭 [14] 探讨了高维 Arnold 变换用于图像像素值大小加密的算法, 即

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \bmod 256, \tag{31}$$

其中 $x_i (i = 1, 2, \cdots, n)$ 是被加密图像某行或列的像素值, $x_i'\ (i = 1, 2, \cdots, n)$ 是加密后图像某行或列的像素值, 变换系数矩阵 $\boldsymbol{A} = (a_{ij})_{n \times n}$ 满足约束条件 $\gcd(\det A, 256) = 1$. 该种图像加密方法由于其变换本身具有线性密码特性且缺乏抵抗差分密码

等攻击能力. 于是提出如下新的典型图像像素加密方法, 即

$$x'_j=\begin{cases}\left(\sum\limits_{i=1}^{n}x_i\right) \bmod 256, & j=1,\\ \left(\sum\limits_{i=1}^{n}x_i+x_j+f(x'_{j-1})\right) \bmod 256, & \\ \qquad 2\leqslant j\leqslant n,\end{cases} \tag{32}$$

或者

$$x'_j=\begin{cases}\left(\sum\limits_{i=1}^{n}x_i\right) \bmod 256, & j=1,\\ \left(\sum\limits_{i=1}^{j-1}ix_i+j\sum\limits_{i=j}^{n}x_i+f(x'_{j-1})\right) \bmod 256, & \\ \qquad 2\leqslant j\leqslant n,\end{cases} \tag{33}$$

其中非线性函数

$$f(x)=x^r+d,\quad r\in\{2,3,4,5,6,7\},$$
$$d\in\{1,2,\cdots,255\}.$$

它们是经典高维 Arnold 变换

$$\begin{pmatrix}x'_1\\x'_2\\\vdots\\x'_n\end{pmatrix}=\begin{pmatrix}1&1&\cdots&1\\1&2&\cdots&1\\\vdots&\vdots&\ddots&\vdots\\1&1&\cdots&n\end{pmatrix}\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} \bmod 256$$

和

$$\begin{pmatrix}x'_1\\x'_2\\\vdots\\x'_n\end{pmatrix}=\begin{pmatrix}1&1&\cdots&1\\1&2&\cdots&2\\\vdots&\vdots&\ddots&\vdots\\1&2&\cdots&n\end{pmatrix}\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} \bmod 256$$

采用本文建议的非线性变换构造法得到的.

针对大小为 $n\times n$ 的灰度图像

$$G=\{g(i,j)|0\leqslant g(i,j)\leqslant 255, i,j=1,2,\cdots,n\},$$

利用改进 Arnold 变换执行像素值大小加密需两步完成, 其一是将图像逐行执行改进 Arnold 变换加密; 其二是将加密后图像逐列执行 Arnold 变换加密. 这种行列两遍加密的目的是增强像素加密扩散能力. 其详细的加密算法如下:

步骤 1 任意给定的外部密钥为 32 位二进制整数 Key.

步骤 2 计算图像平均灰度值所对应的最小整数

$$\mathrm{Ag}=\left\lfloor\frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}g(i,j)\right\rfloor.$$

步骤 3 利用外部密钥 Key 和图像平均灰度值整数 Ag 构造 Logistic 混沌映射的初始值 $y(0)$ 和参数 μ 为

$$y(0)=\sqrt{(\mathrm{key}\times\mathrm{Ag})/2^{40}},$$
$$\mu=3.6+0.39\times(\bmod(\mathrm{key},256))\oplus\mathrm{Ag})/256.$$

步骤 4 Logistic 混沌映射 $y(k+1)=\mu y(k)(1-y(k)), k=0,1,\cdots$ 迭代 1000 次所产生随机值丢掉, 然后产生随机值并整数化为 $id(k)=\bmod(\lfloor y(k)\times 2^{32}\rfloor,256)$ $(k=1001,1002,\cdots)$ 作为图像加密 (32) 或 (33) 式所对应函数 $f(x)$ 中参数 d 的随机取值, 并使得不同位置像素加密时所对应的 d 取值尽可能随机化.

步骤 5 首先对灰度图像逐行读取加密的方法描述如下:

读取任意行像素灰度值并求和 $S_i=\sum\limits_{j=1}^{n}g(i,j)$, 采用 (32) 式的加密结果为

$$g'(i,j)=\begin{cases}\bmod(S_i+id(1000+(i-1)n+1),256), & j=1,\\ \bmod(S_i+g(i,j)+(g'(i,j-1))^r+id(1000+(i-1)n+j),256), & 1<j\leqslant n.\end{cases}$$

采用 (33) 式的加密结果为

$$g'(i,j)=\begin{cases}\bmod(S_i+id(1000+(i-1)n+1),256), & j=1,\\ \bmod\left(S_i+\sum\limits_{l=2}^{j}(l-1)\cdot g(i,l)+\sum\limits_{l=j+1}^{n}(j-1)\cdot g(i,l)\right. & \\ \qquad \left.+(g'(i,j-1))^r+id(1000+(i-1)n+j),256\right), & 1<j\leqslant n.\end{cases}$$

其次, 对逐行加密结果逐列读取加密的方法描述如下:

读取任意列像素灰度值并求和 $S'_j=\sum_{i=1}^{n}g'(i,j)$, 采用 (32) 式的加密结果为

$$g''(i,j)=\begin{cases}\mathrm{mod}(S'_j+id(1000+(j-1)n+1),256), & i=1,\\ \mathrm{mod}(S'_j+g'(i,j)+(g''(i-1,j))^r+id(1000+(j-1)n+i),256), & 1<i\leqslant n.\end{cases}$$

采用 (33) 式的加密结果为

$$g''(i,j)=\begin{cases}\mathrm{mod}(S'_j+id(1000+(i-1)n+1),256), & i=1,\\ \mathrm{mod}\Big(S'_j+\sum_{l=2}^{i}(l-1)\cdot g(l,j)+\sum_{l=i+1}^{n}(i-1)\cdot g'(l,j)\\ \quad +(g''(i-1,j))^r+id(1000+(j-1)n+i),256\Big), & 1<i\leqslant n.\end{cases}$$

步骤 6 输出加密灰度图像并结束.

另外, 上述图像逐行逐列加密时, 加密过程中不同行列组间相互影响较小, 导致加密过程中像素扩散能力非常有限, 于是利用现代分组密码和流密码相融合的思想 [39,40], 提出基于高维 Arnold 变换与其改进所对应的分组反馈链式流密码加密算法, 可以克服分组加密和序列加密各自的不足, 提高算法抗选择明文等攻击. 其关键部分描述如下:

首先读取任意行像素灰度值并求和 $S=\sum_{j=1}^{n}g(i,j)$, 采用 (32) 式的加密结果为

$$g'(i,j)=\begin{cases}\mathrm{mod}(C_{i-1}+S_i+id(1000+(i-1)n+1),256), & j=1,\\ \mathrm{mod}(C_{i-1}+S_i+g(i,j)+(g'(i,j-1))^r+id(1000+(i-1)n+j),256), & 1<j\leqslant n.\end{cases}$$

采用 (33) 式的加密结果为

$$g'(i,j)=\begin{cases}\mathrm{mod}(C_{i-1}+S_i+id(1000+(i-1)n+1),256), & j=1\\ \mathrm{mod}\Big(C_{i-1}+S_i+\sum_{l=2}^{j}(l-1)\cdot g(i,l)+\sum_{l=j+1}^{n}(j-1)\cdot g(i,l)\\ \quad +(g'(i,j-1))^r+id(1000+(i-1)n+j),256\Big), & 1<j\leqslant n,\end{cases}$$

$$C_i=\mathrm{mod}\Big(\sum_{j=1}^{n}g'(i,j)\times g'(i,j),256\Big).$$

其次, 对逐行加密结果逐列读取加密描述为

读取任意列像素灰度值并求和 $S'=\sum_{j=1}^{n}g'(i,j)$, 采用 (32) 式的加密结果为

$$g''(i,j)=\begin{cases}\mathrm{mod}(C'_{j-1}+S'_j+id(1000+(j-1)n+1),256), & i=1,\\ \mathrm{mod}(C'_{j-1}+S'_j+g'(i,j)+(g''(i-1,j))^r+id(1000+(j-1)n+i),256), & 1<i\leqslant n,\end{cases}$$

$$C'_j=\mathrm{mod}\Big(\sum_{i=1}^{n}g''(i,j)\times g''(i,j),256\Big).$$

采用 (33) 式的加密结果为

$$g''(i,j)=\begin{cases}\mathrm{mod}(C'_{j-1}+S'_j+id(1000+(i-1)n+1),256), & i=1,\\ \mathrm{mod}\Big(C'_{j-1}+S'_j+\sum_{l=2}^{i}(l-1)\cdot g(l,j)+\sum_{l=i+1}^{n}(i-1)\cdot g'(l,j)\\ +(g''(i-1,j))^r+id(1000+(j-1)n+i),256\Big), & 1<i\leqslant n,\end{cases}$$

$$C'_j = \mathrm{mod}\left(\sum_{i=1}^{n} g''(i,j) \times g''(i,j), 256\right),$$

其中 $C_0 = \mathrm{mod}(\mathrm{Key}, 256) \oplus ((\mathrm{Key} - \mathrm{mod}(\mathrm{key}, 256))/256)$, $C'_0 = C_n$.

其解密算法利用到高维 Arnold 变换和其改进 Arnold 变换的逆变换; 同时解密过程与加密顺序刚好相反, 限于篇幅省略讨论.

7 实验结果及其分析

针对改进型广义 Arnold 变换, 本文将从该变换用于图像像素位置置乱的有效性和合理性, 置乱周期, 以及改进型高维广义 Arnold 变换用于图像像素值大小加密和安全性等方面进行测试, 并与传统 Arnold 变换及其高维 Arnold 变换置乱加密测试结果进行比较分析.

7.1 改进广义 Arnold 变换置乱测试与分析

针对大小为 256×256 的黑白二值图像, 采用标准 Arnold 变换 (3) 式以及其相应的改进型 Arnold 变换 (15) 式 (其中 $a = b = c = e = 1$, $d = 2$, 函数 $f(x) = x^4 + 1$) 为例, 验证本文所建议方法的有效性和可行性.

从图 1 和图 2 所示的置乱结果来看, 本文所建议的改进 Arnold 变换置乱效率高且置乱结果纹理特征明显降低, 甚至置乱 4 次几乎没有明显纹理特征信息, 其像素空间非常均匀. 因此, 本文方法相比传统 Arnold 变换用于图像置乱更有优越性.

为了从理论上解释本文构造的改进 Arnold 变换置乱的有效性, 本文首先引入 Jonathan 等人 [41] 关于分组密码中 Feistel 网络的置乱结果判定定理, 其详细描述如下:

定理 1 使用伪随机轮函数, 第 1 轮 Feistel 迭代所产生的置乱结果不是伪随机的.

定理 2 使用伪随机轮函数, 第 2 轮 Feistel 迭代所产生的置乱结果是伪随机的.

定理 3 使用伪随机轮函数, 第 3 轮 Feistel 迭代所产生的置乱结果不是强伪随机的.

定理 4 使用伪随机轮函数, 第 4 轮 Feistel 迭代所产生的置乱结果是一个强伪随机的.

因本文所构造的改进 Arnold 变换借鉴了传统标准混沌映射的构造思想, 且标准混沌映射又具有 Feistel 网络相似结构, 这就导致采用本文建议置乱变换对图像置乱 4 次能保证获得相对满意的置乱效果. 为了进一步证实本文置乱方法的有效性, 下面给出离散标准映射

$$x_{n+1} = (x_n + y_n) \bmod N,$$
$$y_{n+1} = (y_n - 2f(x_{n+1})) \bmod N,$$

这里, 选取 $f(x) = x^4$, 对上述二值黑白图像置乱的置乱结果.

从图 1、图 2 和图 3 所示的置乱测试结果来看, 本文所建议的置乱效果比离散标准映射好, 但离散标准映射置乱效果好于 Arnold 变换结果. 综合上述 3 类置乱方法结果来看, 本文所建议改进 Arnold 变换是可行的.

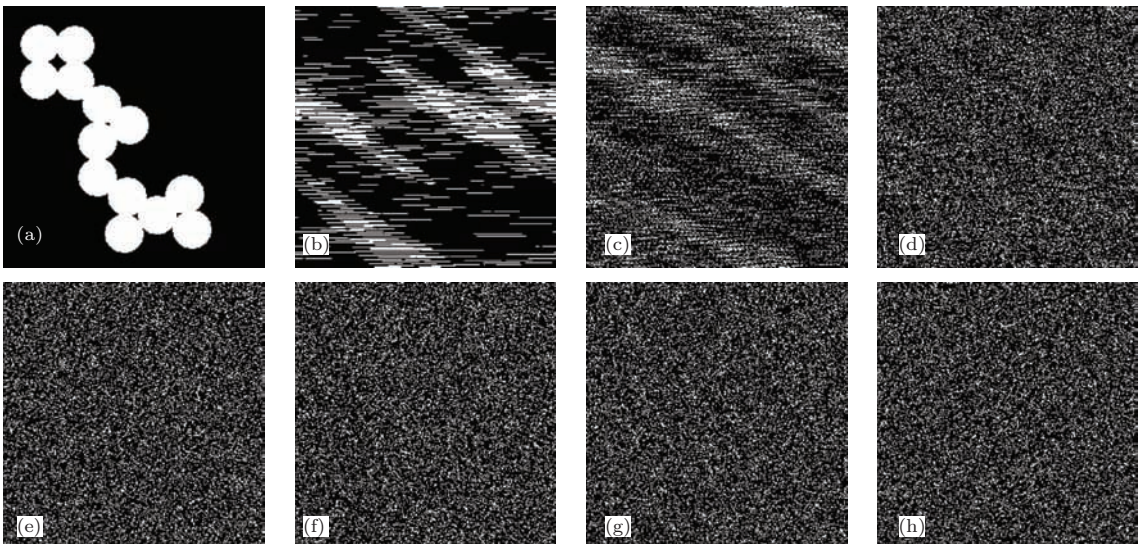

图 1 二值圆饼图像及本文建议方法置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

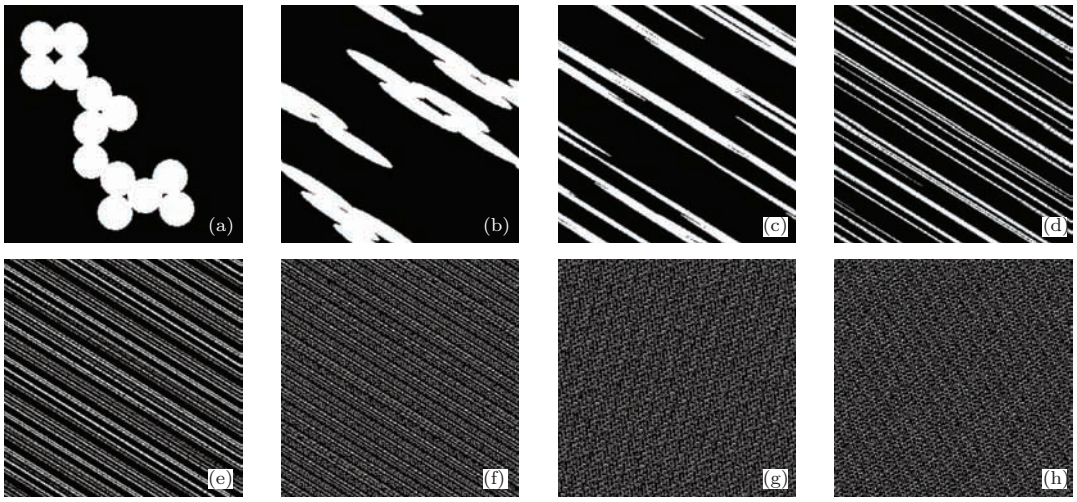

图 2 二值圆饼图像及标准 Arnold 变换置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

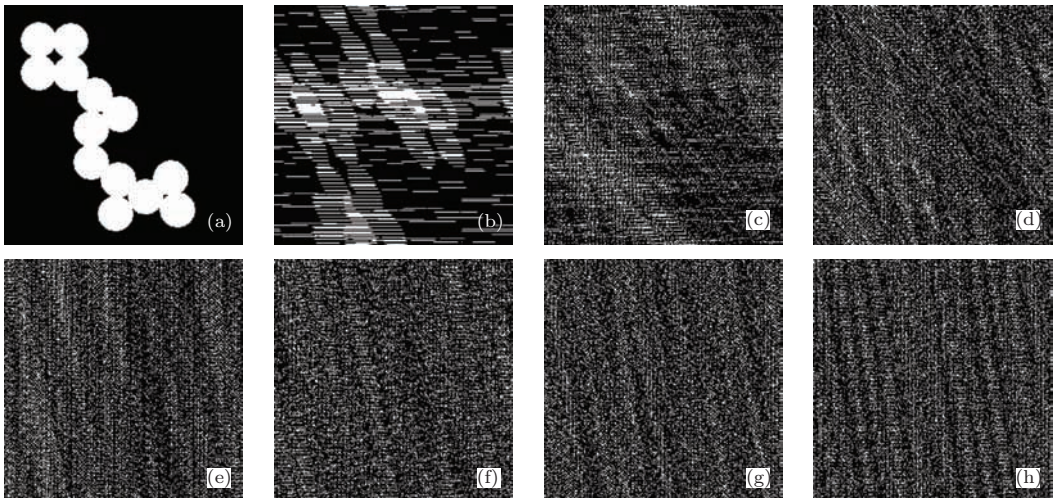

图 3 二值圆饼图像及离散标准映射置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

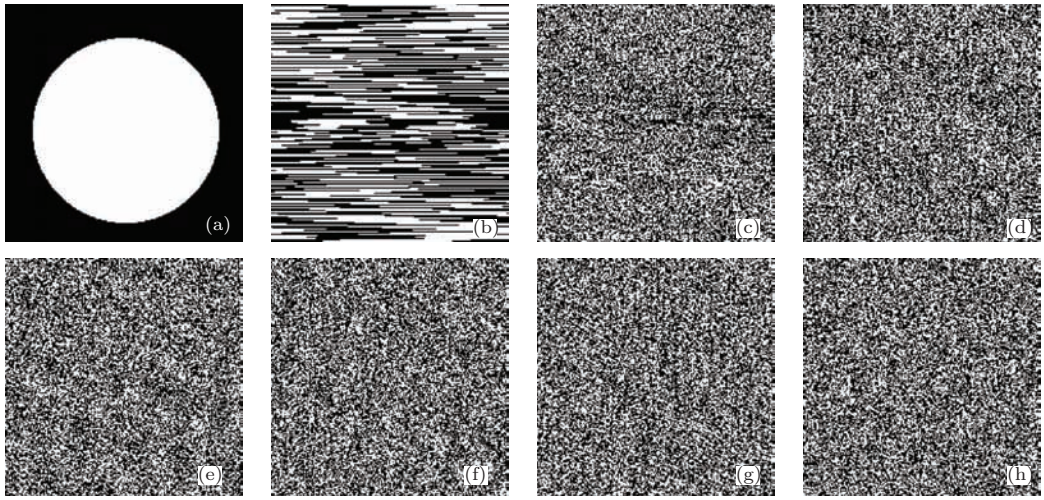

图 4 二值圆状图像及本文建议方法置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

为了证实本文所建议的改进Arnold变换法所具有的普适性,下面图4和图5给出大小为 180×180 的人造二值黑白圆状图像的采用两种方法所获得置乱结果.

从图4和图5所示的圆状图像采用两种方法置乱0至7次结果来看,本文所建议的方法明显好于标准Arnold 变换置乱结果且纹理特征非常弱.

针对大小为 256×256 的标准Lena灰度图像,采用标准Arnold变换(3)式以及本文所建议的改进型Arnold变换(15)式 (其中 $a = b = c = e = 1$, $d = 2$, 函数 $f(x) = x^2 + 1$) 为例,验证本文所建议方法的有效性和可行性.

从图6和图7所示的著名标准Lena灰度图像采用两种不同方法置乱结果来看,本文所建议的改进型Arnold 变换是有效的,其置乱结果中纹理特征弱且像素空间分布无论是整体还是局部都是均匀的,然而传统Arnold变换存在明显纹理特性且像素整体空间分布均匀但局部不均匀.这表明传统Arnold变换改变像素空间分布能力弱,然而本文所建议的改进Arnold变换从整体和局部两方面考虑了改善像素空间分布均匀性的能力,更有利于图像信息安全保护等需要.

针对大小为 256×256 的黑白二值棋盘图像,采用标准Arnold变换(3)式以及其相应的本文所建议的改进型Arnold变换(15)式 (其中 $a = b = c = e = 1$, $d = 2$, 函数 $f(x) = x^3 + 1$) 为例, 验证本文所建议方法的有效性和可行性.

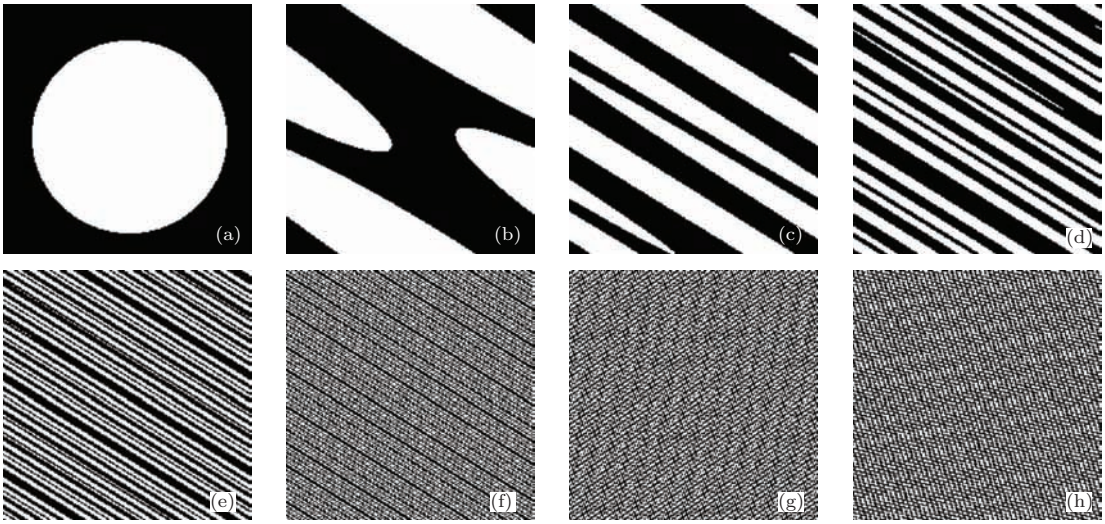

图5 二值圆状图像及标准 Arnold 变换置乱 1 至 7 次结果, (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

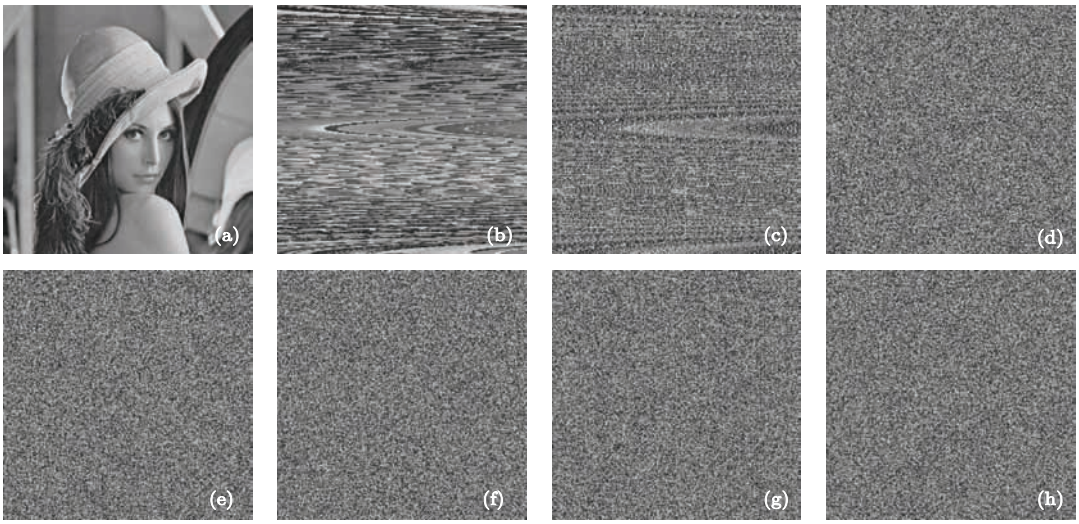

图6 Lena 图像及采用本文建议方法置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

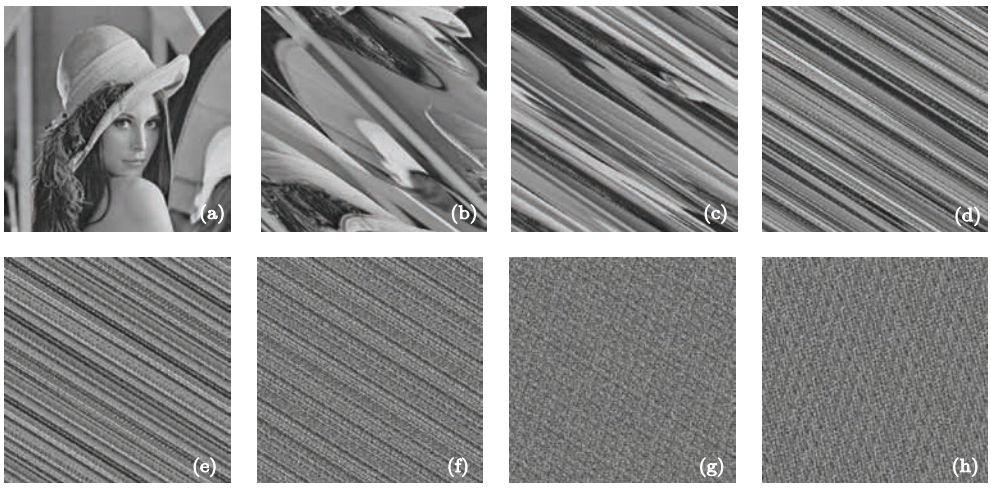

图 7 Lena 图像采用及标准 Arnold 变换置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

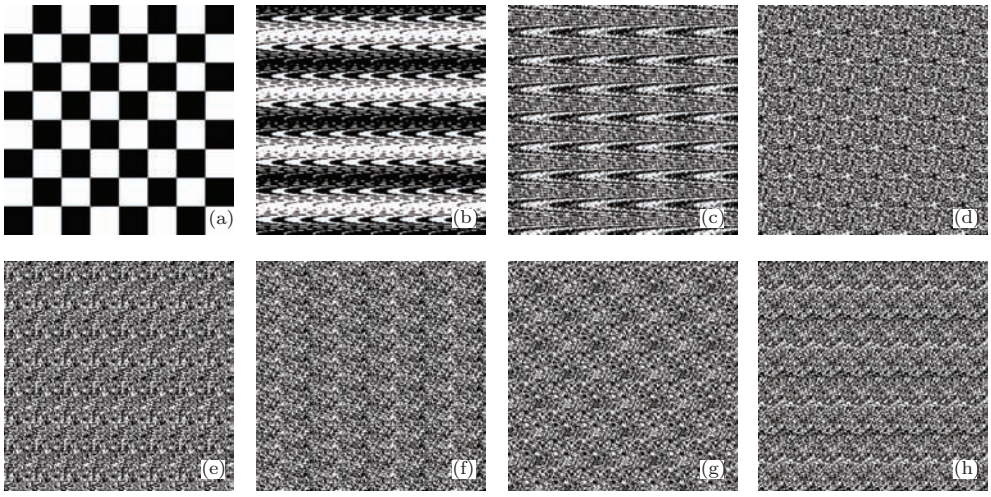

图 8 Lena 图像及采用本文建议方法置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

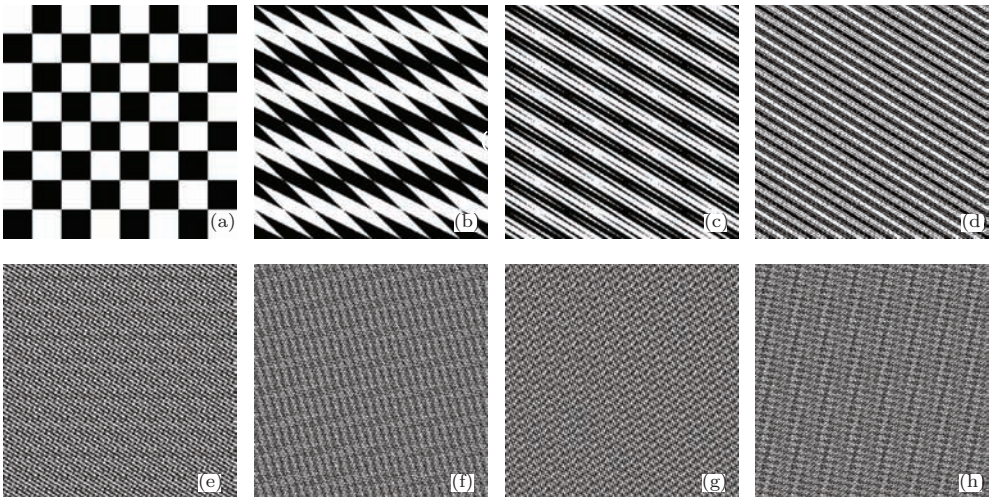

图 9 Lena 图像及采用标准 Arnold 变换置乱 1 至 7 次结果 (a) 原始图; (b) 置乱 1 次; (c) 置乱 2 次; (d) 置乱 3 次; (e) 置乱 4 次; (f) 置乱 5 次; (g) 置乱 6 次; (h) 置乱 7 次

从图8和图9所示的两种置乱方法所得结果来看, 本文所建议的改进型Arnold变换是可行且有效的, 相比传统Arnold变换置乱图像能获得较弱的纹理信息, 以便从视觉感知角度获取原图像信息更具有迷惑性.

总之, 从上述典型二值黑白图像及标准Lena灰度图像的置乱测试结果及其比较分析来看, 本文所建议的改进型Arnold变换是可行且有效的, 甚至更具有推广实用价值意义.

7.2 改进广义Arnold变换置乱周期测试与分析

无论是传统标准Arnold变换, 还是本文所建议的改进型Arnold变换, 其本质都是可逆一一映射, 这就导致有限域上的置乱存在周期. 迄今, 已有大量文献探讨Arnold变换的周期性, 并获得有一定理论价值的成果. 为此, 本文将探讨改进型Arnold变换的周期, 为其广泛应用于图像加密和水印等场合提供一定理论支撑.

针对Arnold变换(3)式, 将其置乱周期采用函数$T(N)$表示, 而其改进型Arnold变换式

$$x_{n+1} = (x_n + y_n) \bmod N,$$
$$y_{n+1} = (x_n + 2y_n + x_{n+1}^4 + 1) \bmod N$$

的周期采用函数$T_1^*(N)$表示. 下面测试其周期随参数N变化的详细情况如表1所示.

从表1所示的测试结果来看, 本文所建议的改进型Arnold变换对于大多数参数N的置乱周期大大延长, 特别是若参数N是质数时, 其置乱周期有了非常显著的增大.

表1 标准Arnold变换及其改进型Arnold变换的周期

Arnold变换				改进型Arnold变换			
N	$T(N)$	N	$T(N)$	$T_1^*(N)$	$T_1^*(N)$	$T_1^*(N)$	$T_1^*(N)$
2	3	11	5	2	4	11	51660
3	4	12	12	3	15	12	60
4	3	13	14	4	12	13	$> 3.0 \times 10^7$
5	10	14	24	5	84	14	420
6	12	15	20	6	60	15	420
7	8	16	12	7	210	16	12
8	6	17	18	8	12	17	$> 3.0 \times 10^7$
9	12	18	12	9	90	18	180
10	30	19	9	10	84	19	$> 3.0 \times 10^7$

针对Arnold变换(3)式, 鲍江宏[33]获得其周期计算判定定理为

定理5 如果N是大于5的素数, 则有

1) 如果N能表示成$10m \pm 3$的形式, 则其周期$T(N) = N + 1$;

2) 如果能表示成$10m \pm 1$的形式, 则其周期$T(N) = (N - 1)/2$.

定理6 如果N是合数, 则有

1) 如果$N = p \cdot q (p \neq q)$且$(p, q) = 1$, 则其周期$T(N)$是$T(p)$和$T(q)$的最小公倍数, 即$T(N) = lcm(T(p), T(q))$;

2) 如果N的标准分解形式是p^2 (p是素数且$p \neq 2$), 则其周期$T(N) = p \cdot T(p)$.

但是, 这两个判定定理并不适合改进型Arnold变换的周期值大小判定. 通过表1所示的部分测试结果来看, 改进型Arnold变换周期存在显著特点是若模参数N是偶数时, 则其变换周期$T^*(N)$是偶数.

针对Arnold变换(3)式, 将其置乱周期采用函数$T(N)$表示, 而其改进型Arnold变换式

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + y_{n+1}^4 + 1) \bmod N$$

的周期采用函数$T_2^*(N)$表示, 通过实验测试发现$T_2^*(N) = T_1^*(N)$, 这表明这两种改进型Arnold变换周期相同. 另外, 无论是

$$x_{n+1} = (x_n + y_n) \bmod N,$$
$$y_{n+1} = (x_n + 2y_n + e(x_{n+1}^4 + 1)) \bmod N,$$

还是

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + e(y_{n+1}^4 + 1)) \bmod N,$$

它们的置乱周期 $T_i^*(e,N)$ $(i = 1,2)$ 不仅与参数 N 有关, 而且与参数 e 有一定关系, 甚至具有一定的对称性 $T_i^*(e,N) = T_i^*(N-e,N)$ $(i = 1,2)$, $e \in [1,2,\cdots,N-1]$. 下面仅需测试参数 e 的部分取值情况: 1) 若参数 N 是偶数, 则选取参数 e 的范围为 $[1,2,\cdots,N/2]$; 2) 若参数 N 是奇数, 则选取参数 e 的范围为 $[1,2,\cdots,(N-1)/2]$. 其详细测试结果如下:

若 $N = 2$ 时, 其 $T_1^*(1,2) = 4$;

若 $N = 3$ 时, 有 $T_1^*(1,3) = 15$;

若 $N = 4$ 时, 有 $T_1^*(1,4) = 12$, $T_1^*(2,4) = 6$;

若 $N = 5$ 时, 有 $T_1^*(1,5) = 84$, $T_1^*(2,5) = 84$;

若 $N = 6$ 时, 有 $T_1^*(1,6) = 60$, $T_1^*(2,6) = 15$, $T_1^*(3,6) = 4$;

若 $N = 7$ 时, 有 $T_1^*(1,7) = 210$, $T_1^*(2,7) = 84$, $T_1^*(3,7) = 2508$;

若 $N = 8$ 时, 有 $T_1^*(1,8) = 12$, $T_1^*(2,8) = 12$, $T_1^*(3,8) = 12, T_1^*(4,8) = 3$;

若 $N = 9$ 时, 有 $T_1^*(1,9) = 90$, $T_1^*(2,9) = 90$, $T_1^*(3,9) = 12$, $T_1^*(4,9) = 90$;

若 $N = 10$ 时, 有 $T_1^*(1,10) = 84$, $T_1^*(2,10) = 84$, $T_1^*(3,10) = 84$, $T_1^*(4,10) = 84$, $T_1^*(5,10) = 20$.

从上述部分测试结果来看, 参数 e 的取值变化对置乱变换周期具有一定影响. 大多数情况下, 参数 e 选取较小或较大的值可能获得更长的置乱周期值.

针对本文建议的改进型 Arnold 变换

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + y_{n+1}^2 + 1) \bmod N,$$

将其置乱周期记为 $T_3^*(N)$, 其详细测试结果如表 2 所示.

从表 2 和表 1 所示的两种改进型 Arnold 变换置乱周期测试结果来看, 它们所对应的置乱周期并不完全相同, 且存在相同的置乱周期部分没有一定规律可循.

针对本文建议的改进型 Arnold 变换

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + e(y_{n+1}^2 + 1)) \bmod N$$

和

$$x_{n+1} = (x_n + y_n) \bmod N,$$
$$y_{n+1} = (x_n + 2y_n + e(x_{n+1}^2 + 1)) \bmod N$$

而言, 这二者的置乱周期随参数 e 和参数 N 变化通过测试发现也是相同的且满足 $T_3^*(e,N) = T_3^*(N-e,N)$, $e \in [1,2,\cdots,N-1]$, 于是本文仅探讨其参数 e 对置乱变换周期 $T_3^*(e,N)$ 影响的测试.

若 $N = 2$ 时, 其 $T_3^*(1,2) = 4$;

若 $N = 3$ 时, 有 $T_3^*(1,3) = 15$;

若 $N = 4$ 时, 有 $T_3^*(1,4) = 12$, $T_3^*(2,4) = 6$;

若 $N = 5$ 时, 有 $T_3^*(1,5) = 210$, $T_3^*(2,5) = 308$;

若 $N = 6$ 时, 有 $T_3^*(1,6) = 60$, $T_3^*(2,6) = 15$, $T_3^*(3,6) = 4$;

若 $N = 7$ 时, 有 $T_3^*(1,7) = 120$, $T_3^*(2,7) = 16380$, $T_3^*(3,7) = 2730$;

若 $N = 8$ 时, 有 $T_3^*(1,8) = 12$, $T_3^*(2,8) = 12$, $T_3^*(3,8) = 12$, $T_3^*(4,8) = 3$;

若 $N = 9$ 时, 有 $T_3^*(1,9) = 90$, $T_3^*(2,9) = 90$, $T_3^*(3,9) = 12$, $T_3^*(4,9) = 90$;

若 $N = 10$ 时, 有 $T_3^*(1,10) = 420$, $T_3^*(2,10) = 924$, $T_3^*(3,10) = 308$, $T_4^*(4,10) = 210$, $T_5^*(5,10) = 20$.

从上述部分测试结果来看, 参数的取值变化对置乱变换周期具有一定影响. 大多数情况下, 参数 e 选取较小或较大的值 (即从 $1,2,\cdots,N-1$ 的两端选取) 可能获得更长的置乱周期值. 另外, 从上述实验测试结果来看, 两种改进型 Arnold 变换

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + e(y_{n+1}^4 + 1)) \bmod N$$

表 2 改进型 Arnold 变换周期 $T_3^*(N)$ 值

N	2	3	4	5	6	7	8	9	10	11	12
$T_3^*(N)$	4	15	12	210	60	120	12	90	420	34320	60
N	13	14	15	16	17	18	19	20	21	22	
$T_3^*(N)$	4084080	120	210	12	$> 3.0 \times 10^7$	180	$> 3.0 \times 10^7$	420	120	34320	

表 3 改进型 Arnold 变换周期 $T_5^*(N)$ 值

N	2	3	4	5	6	7	8	9	10	11	12
$T_5^*(N)$	4	6	12	60	12	3120	24	12	60	1053360	12
N	13	14	15	16	17	18	19	20	21	22	
$T_5^*(N)$	13104	3120	60	24	637560	12	$> 3.0 \times 10^7$	60	3120	1053360	

和

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + y_n + e(y_{n+1}^2 + 1)) \bmod N$$

的置乱周期 $T_1^*(e,N)$ 和 $T_2^*(e,N)$ 随参数 e 的变化也是不完全相同的.

针对改进型 Arnold 变换

$$x_{n+1} = (x_n + y_n) \bmod N,$$
$$y_{n+1} = (x_n + y_n + x_{n+1}^3 + 1) \bmod N,$$

将其置乱周期记为 $T_5^*(N)$, 它与置乱变换

$$y_{n+1} = (x_n + 2y_n) \bmod N,$$
$$x_{n+1} = (x_n + 2y_n + y_{n+1}^3 + 1) \bmod N$$

的置乱周期 $T_6^*(N)$ 通过仿真测试表明是相同的, 于是文中仅给出的测试结果如表 3 所示.

从表 1、表 2 和表 3 所示的 3 种改进型 Arnold 变换置乱周期测试结果来看, 它们所对应的置乱周期并不完全相同, 且存在相同的置乱周期部分但没有一定规律可循.

针对大小为 256×256 的灰度图像而言, 采用传统 Arnold 变换置乱时, 其置乱周期为 192. 若采用本文所建议的改进 Arnold 变换

$$x_{n+1} = (x_n + y_n) \bmod 256,$$
$$y_{n+1} = (x_n + 2y_n + x_{n+1}^k + 1) \bmod 256$$

所获得置乱周期情况如下:

1) 若 $k = 2$ 时, 该改进型 Arnold 变换的置乱周期为 192;

2) 若 $k = 3$ 时, 该改进型 Arnold 变换的置乱周期为 384;

3) 若 $k = 4$ 时, 该改进型 Arnold 变换的置乱周期为 96;

4) 若 $k = 5$ 时, 该改进型 Arnold 变换的置乱周期为 192;

5) 若 $k = 6$ 时, 该改进型 Arnold 变换的置乱周期为 192.

从上述测试结果来看, 其参数 k 对其置乱周期有一定影响. 若考虑到运算复杂性和周期长短两方面因素, 一般应用时可选取参数 k 为 3.

7.3 改进高维 Arnold 变换图像加密测试及其安全性分析

将改进高维 Arnold 变换式 (32) 或 (33) 用于图像像素值大小加密时, 综合考虑选取非线性函数 $f(x) = x^r + d$ 中的参数 r 为 3, 参数 d 由外部密钥、图像平均灰度信息和 Logistic 混沌映射共同产生的离散随机整数确定, 可以有效避免穷举攻击、选择明文攻击、差分攻击加密结果的可能性. 下面给出传统高维 Arnold 变换 (其中变换矩阵采用 A 型 Arnold 系数矩阵) 和本文改进高维 A 型 Arnold 变换 (32) 式对二值黑白图像和灰度图像进行逐行再逐列加密, 其详细结果如图 10 和图 11 所示. 针对采用灰度级出现次数统计 (即 1 维直方图) 的均匀性来评价图像加密效果的不足, 本文引入像素与其相邻像素所对应联合空间统计量 (即共生直方图) 的均匀程度来反映图像加密效果真实情况, 即

水平方向共生直方图为

$$Co_0(i,j) = \sum_{x=1}^{n-1}\sum_{j=1}^{n} \delta(g(x,y) - i)\delta(g(x+1,y) - j),$$
$$i,j = 0,1,\cdots,255.$$

垂直方向共生直方图为

$$Co_2(i,j) = \sum_{x=1}^{n-1}\sum_{j=1}^{n} \delta(g(x,y) - i)\delta(g(x,y+1) - j),$$
$$i,j = 0,1,\cdots,255.$$

该共生直方图所对应的信息熵大小度量其二维直方图分布的均匀性程度, 即

$$H(Co_l) = -\sum_{i=0}^{255}\sum_{j=0}^{255} \frac{Co_l(i,j)}{n(n-1)} \ln\left(\frac{Co_l(i,j)}{n(n-1)}\right),$$
$$l = 1,2.$$

该值越大, 则对应像素空间分布越均匀. 其加密详细结果共生直方图熵值如表 4 所示.

另外, 针对二值摄影师黑白图像, 本文采用齐东旭 [14] 高维 Arnold 变换和本文所建议的改进型 Arnold 变换 (33) 式对其逐行逐列加密, 其结果如图 12 和图 13 所示.

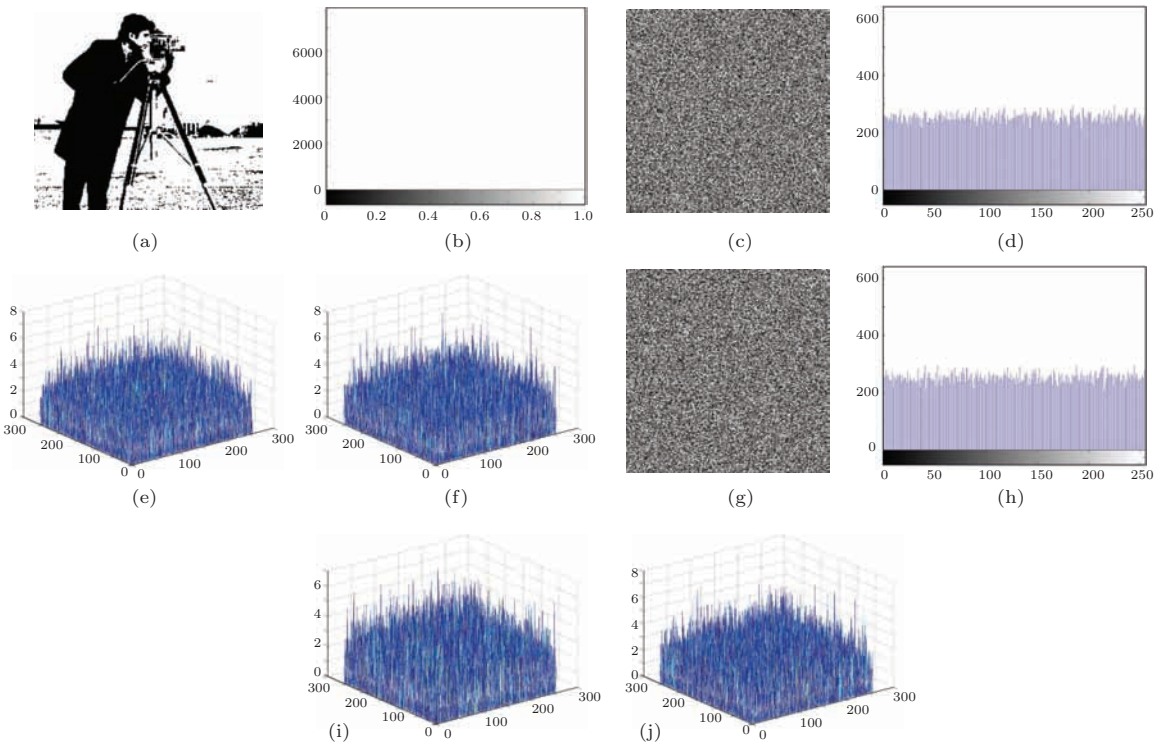

图 10 二值图像及改进 Arnold 变换 (32) 式加密结果 (a) 二值图像; (b) 1 维直方图; (c) 逐行加密结果; (d) 逐行加密结果 1 维直方图; (e) 逐行加密结果水平方向共生直方图; (f) 逐行加密结果垂直方向共生直方图; (g) 逐行逐列加密结果; (h) 逐行逐列加密结果 1 维直方图; (i) 逐行逐列加密结果水平方向共生直方图; (j) 逐行逐列加密结果垂直方向共生直方图

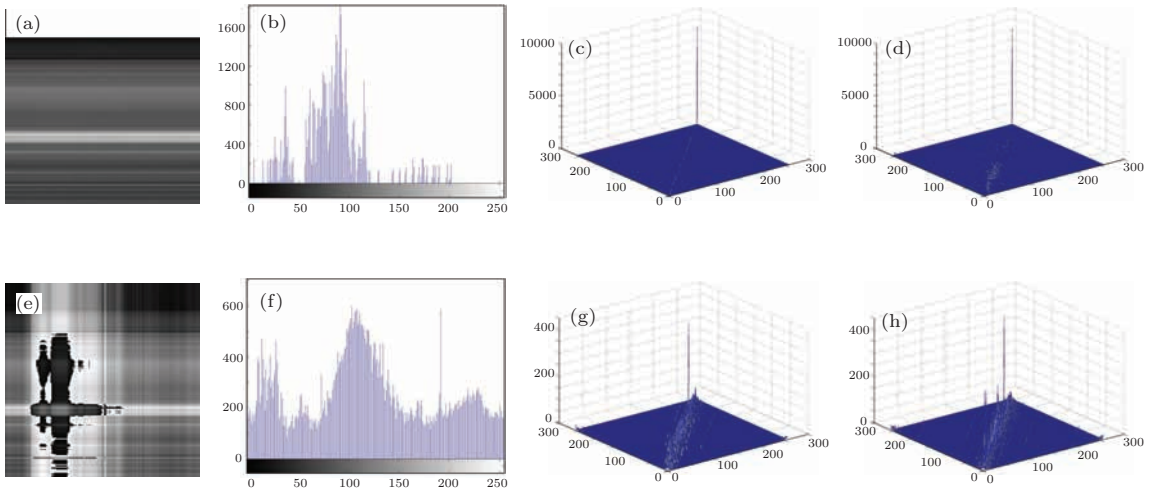

图 11 二值摄影师图像及 A 型 Arnold 变换加密结果 (a) 逐行加密结果; (b) 逐行加密结果 1 维直方图; (c) 逐行加密结果水平方向共生直方图;(d) 逐行加密结果垂直方向共生直方图; (e) 逐行逐列加密结果; (f) 逐行逐列加密结果 1 维直方图; (g) 逐行逐列加密结果水平方向共生直方图; (h) 逐行逐列加密结果垂直方向共生直方图

从图 10 至图 13 所示的二值黑白摄影师图像加密结果, 以及表 4 所对应的加密结果共生直方图熵值来看, 本文所建议的改进型高维 Arnold 变换 (32) 或 (33) 式所加密图像 1 维直方图以及其水平方向邻域像素水平共生直方图的统计分布均较为均匀. 但是, 采用高维 A 型 Arnold 变换以及高维标准 Arnold 变换对二值黑白摄影师图像片加密结果有很大差异性, 其中高维 A 型 Arnold 变换无法实现二值黑白图像加密, 其加密结果 1 维直方图和水平邻域像素共生直方图的统计分布与均匀分

布相差甚远; 高维标准 Arnold 变换对二值黑白摄影师图像加密结果的 1 维直方图呈明显均匀分布, 但其水平邻域像素共生直方图的统计分布与均匀分布相差一定距离. 因此, 本文所建议的改进型高维 Arnold 变换加密算法有利于二值黑白图像加密的需要.

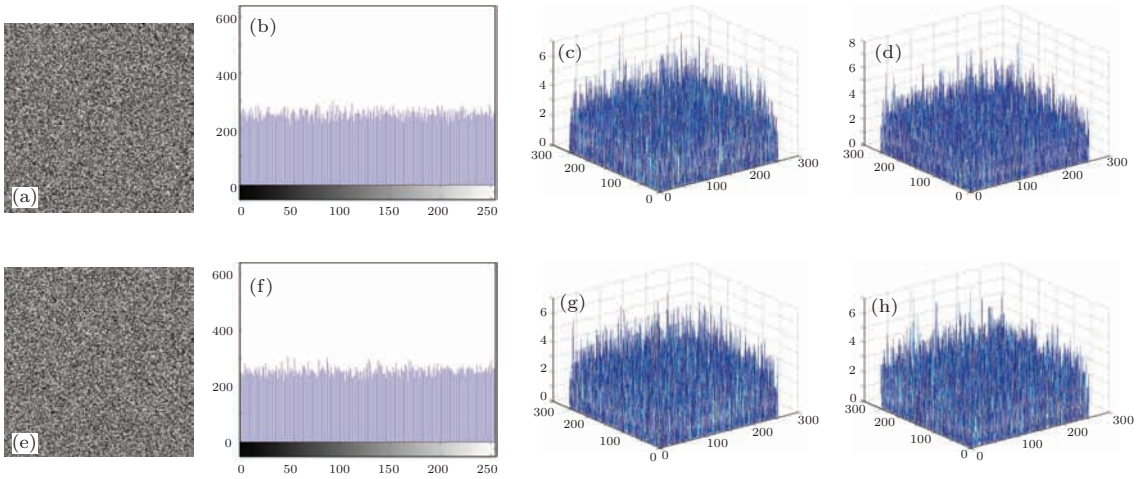

图 12 二值摄影师图像及改进高维标准 Arnold 变换加密结果 (a) 逐行加密结果;(b) 逐行加密结果 1 维直方图;(c) 逐行加密结果水平方向共生直方图; (d) 逐行加密结果垂直方向共生直方图; (e) 逐行逐列加密结果; (f) 逐行逐列加密结果 1 维直方图; (g) 逐行逐列加密结果水平方向共生直方图; (h) 逐行逐列加密结果垂直方向共生直方图

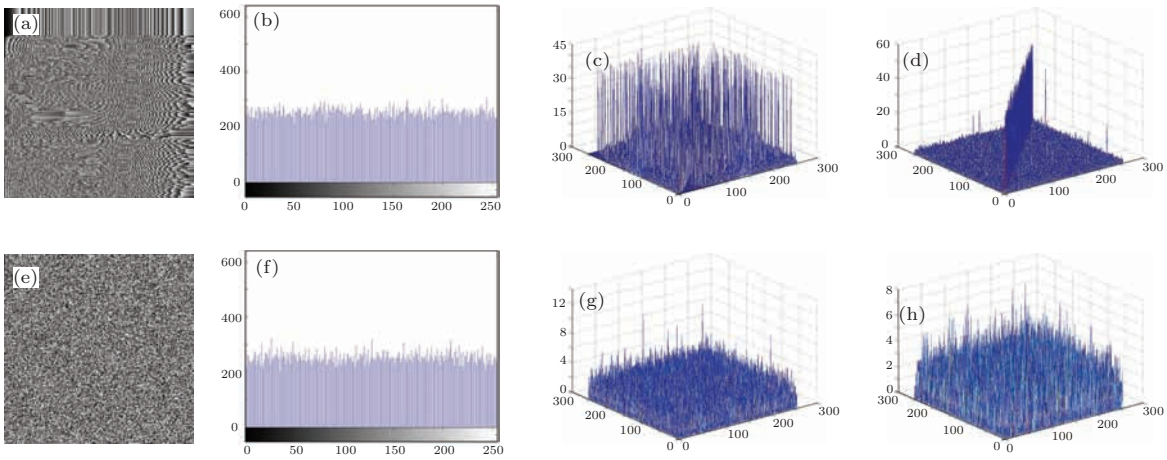

图 13 二值摄影师图像及高维标准 Arnold 变换加密结果 (a) 逐行加密结果;(b) 逐行加密结果 1 维直方图; (c) 逐行加密结果水平方向共生直方图; (d) 逐行加密结果垂直方向共生直方图; (e) 逐行逐列加密结果; (f) 逐行逐列加密结果 1 维直方图; (g) 逐行逐列加密结果水平方向共生直方图; (h) 逐行逐列加密结果垂直方向共生直方图

表 4 二值摄影师图像加密相邻像素共生直方图熵值

加密方法	逐行加密		逐行逐列加密	
	水平方向	垂直方向	水平方向	垂直方向
A 型高维 Arnold 变换	4.4445	5.4897	8.1572	8.1501
本文改进 A 型高维 Arnold 变换	10.5180	10.5170	10.5120	10.5096
标准高维 Arnold 变换	9.8576	10.0110	10.5028	10.5122
本文改进标准高维 Arnold 变换	10.5146	10.5173	10.5179	10.5141

下面给出分组密码与流密码相结合的反馈链式逐行逐列加密算法对二值黑白棋盘图像的加密结果, 其中分组加密算法中使用的改进型高维标准 Arnold 变换并融入反馈流信息 C_i 或 C'_i, 随机参数 $id(i)$ 或 $id(j)$ 采用外部密钥和图像灰度统计信息控制 Logistic 混沌映射产生所得. 图像中各个像素不是独立的其相关性很大这说明大块区域中的灰度值相差不大. 图像加密的目标之一就是减少相邻像

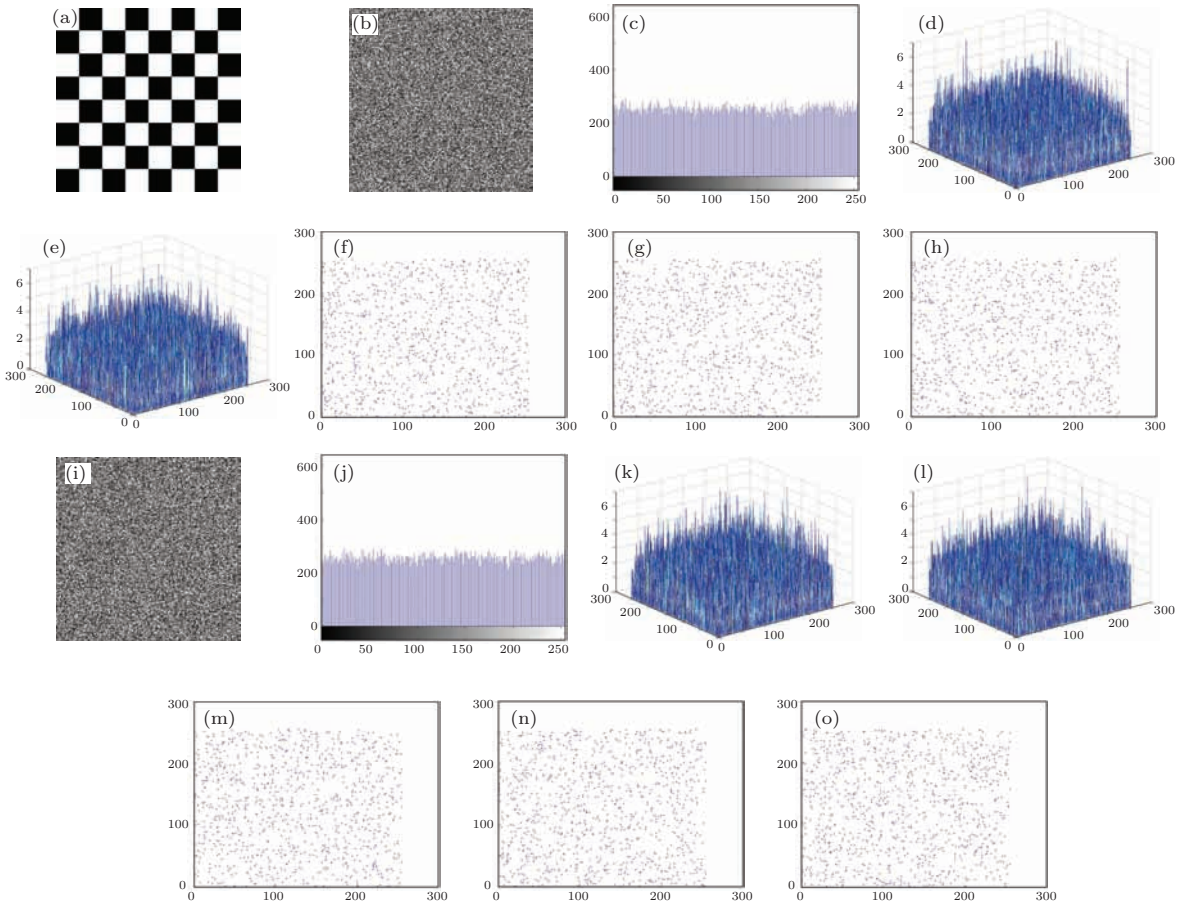

图 14 分组反馈链式流密码改进高维标准 Arnold 变换加密结果 (a) 原图像; (b) 逐行加密结果; (c) 逐行加密 1 维直方图; (d) 逐行加密结果水平方向共生直方图; (e) 逐行加密结果垂直方向共生直方图; (f) 逐行加密结果水平方向相邻像素分布图;(g) 逐行加密结果垂直方向相邻像素分布图; (h) 逐行加密结果对角线方向相邻像素分布图; (i) 逐行逐列加密结果; (j) 逐行逐列加密 1 维直方图; (k) 逐行逐列加密水平方向共生直方图; (l) 逐行逐列加密垂直方向共生直方图; (m) 逐行逐列加密水平方向相邻像素分布图; (n) 逐行逐列加密垂直方向相邻像素分布图; (o) 逐行逐列加密对角线方向相邻像素分布图

素之间的相关性, 主要包括水平像素、垂直像素和对角线像素间的相关性. 很显然, 相关性越小, 则说明图像加密效果好且安全性越高.

表 5 棋盘图像加密前后相邻像素相关系数值 (随机选取 1000 对)

	水平方向	垂直方向	对角线方向
原图像	0.9750	0.9712	0.9483
逐行加密后图像	0.7583	0.7381	0.7361
逐行逐列加密后图像	0.7430	0.7577	0.7544

表 6 棋盘图像加密后相邻像素共生直方图熵值

	水平方向 共生直方图	垂直方向 共生直方图
原始图像	0.8189	0.8189
逐行加密后图像	10.5098	10.5174
逐行逐列加密后图像	10.5152	10.5151

从图 14 所示的加密结果, 以及表 4 和表 5 所示的相邻像素相关性值和共生矩阵熵值来看, 本文所建议的分组反馈链式流密码结构加密算法是有效的, 特别分组之间的反馈信息具有较强的非线性特性, 导致其加密算法相比文献 [15] 加密算法具有较高的安全性能. 另外, 由于本文所建议的加密算法其密钥由外部密钥 (密钥空间大小为 2^{32}) 和图像统计信息共同决定 Logistic 混沌映射初始参数 x_0 和映射参数 μ, 其加密结果安全性不仅与改进型 Arnold 变换紧密相关, 而且与 Logistic 混沌映射产生的随机序列值相关. 因此, 本文加密方法首先能够抵抗统计、选择明文、选择密文等攻击 [42−44], 以及若外部密钥参数变化导致 Logistic 映射的参数和初始值发生变化, 从而使得该加密算法对密钥参数具有一定的敏感性; 一旦外部密钥发生错误是无法正确解密图像.

下面将继续探讨该加密算法的抗差分攻击能

力或密钥敏感性. 像素数变化率 R_{NPC} 和归一化平均变化强度 I_{UAC} 是衡量图像加密算法抵抗差分攻击和密钥敏感性的重要指标.

$$R_{\mathrm{NPC}} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\delta\left(g_1''(i,j) - g_2''(i,j)\right),$$

$$I_{\mathrm{UAC}} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|g_1''(i,j) - g_2''(i,j)\right|}{255},$$

其中 $g_1''(i,j)(1 \leqslant i \leqslant M,\ \ 1 \leqslant j \leqslant N)$ 是原图像 $G = \{g(i,j)|1 \leqslant i \leqslant M,\ \ 1 \leqslant j \leqslant N\}$ 所对应的加密结果, $g_2''(i,j)(1 \leqslant i \leqslant M,\ \ 1 \leqslant j \leqslant N)$ 是原图像 $G = \{g(i,j)|1 \leqslant i \leqslant M,\ \ 1 \leqslant j \leqslant N\}$ 改变某位置像素所对应图像 G_1 的加密结果.

若图像的某个像素值的改变可以很大程度地改变加密图像, 则说明该算法具有较强的抵抗差分攻击能力. 针对本文所建议的基于改进型 Arnold 变换 (32) 式或 (33) 式所对应的分组反馈链式流密码算法, 采用二值黑白棋盘图像为例, 将其像素位置为 (100,100) 处的像素若为 0 变成 255(若为 255 变成 0) 再实现前后两幅图像逐行逐列加密, 其加密测试差分攻击能力如表 7 所示, 表明该类分组反馈链式流密码算法能够有效地抵御差分攻击. 另外, 保持原始二值黑白图像不变, 将该加密算法所对应的外部数字密钥值相差为 1 的改变, 将导致对同幅图像加密结果相差很大, 其加密测试密钥敏感性结果如表 7 所示, 这表明该加密算法对密钥参数变化具有较高的敏感特性.

表 7 分组反馈链式流密码算法抗差分攻击和密钥敏感性的测试结果

	抗差分攻击能力		密钥敏感性能力	
	R_{NPC}/%	I_{UAC}/%	R_{NPC}/%	I_{UAC}/%
(32) 式	99.63	33.39	99.58	33.48
(33) 式	99.64	33.34	99.63	33.47

从上述加密算法测试结果及其安全性分析来看, 本文所建议的图像加密算法相比现有 Arnold 变换用于图像加密和水印等信息安全保护需要更具有普适性, 特别有利于现代军事战场数据链系统高安全信息保护需要.

本文建议了 Arnold 变换的非仿射改进形式, 将其用于图像像素位置置乱和像素值大小加密具有一定的理论和实用价值意义; 但是, 从图像加密方法的发展趋势来看, 单一加密方法难以满足高安全性信息保护需要, 于是探索多种加密方法相融合的高安全性图像加密算法已成为当前图像密码算法设计中的热点课题. 针对 Sun 等人 [45] 提出的高维 Lorenz 混沌和 Arnold 变换相结合的高维混沌加密算法安全性弱的不足, 可将其 Arnold 变换采用本文所建议的改进型 Arnold 变换替代, 进一步混淆密文图像和明文图像的关联性, 以便满足高安全性图像加密和传输的需要. 为了进一步提高本文所建议的图像像素值大小加密算法的抗差分攻击、选择明文攻击、已知明文攻击和生日攻击等要求, 可将 Wang 等人 [46] 提出的延时分数阶 Logistic 混沌映射取代本文加密算法中所使用的经典 Logistic 混沌映射, 从而获取高安全性能的改进高维 Arnold 变换加密算法. 针对遍历矩阵和空间暂态混沌相结合的图像加密算法 [47], 其遍历矩阵的构造与加密外部密钥和明文图像之间缺乏紧密联系, 导致其加密算法的抗选择明文攻击等能力弱, 于是将该算法中的遍历矩阵采用外部密钥和明文图像统计量融合控制的改进 Arnold 变换替代, 提高该自适应加密算法的密钥敏感性、抗典型攻击的能力. 最近, Li 团队 [48] 对广义猫映射、单向耦合映射格子和分组交替密码 Feistel 结构相融合的图像加密算法 [49] 采用差分法攻击, 发现仅需利用少量明文信息在较少循环次数下能获得等价密钥, 从而证实该复合加密算法存在严重安全隐患. 为了提高基于交替结构的混沌加密算法的安全性, 特别是将本文所建议的改进型广义二维 Arnold 变换用于图像像素位置置乱, 并将改进型高维 Arnold 变换加密方法和分组密码 Feistel 结构相结合来改善该类加密算法抗差分攻击、选择明文攻击等能力; 同时, 提高该类加密算法的外部密钥敏感性和密钥空间大小, 以达到增强该类算法的普适性能力.

8 结 论

针对传统离散 Arnold 变换是一种拟仿射变换, 将其用于图像像素位置置乱和像素值大小加密结果的视觉效果和安全性存在难以令人满意的缺陷, 提出了非线性去仿射构造法并获得一种崭新的可逆变换方法, 并将传统 Arnold 变换视为本文建议变换的特例. 将本文所建议的改进型 Arnold 变换用于图像像素位置置乱能获得纹理特性较弱的置乱效果且置乱周期有了明显增长, 特别是对于模参数为素数时其置乱周期有了显著的延长; 将其用于图像像素值大小置乱加密能获得相比传统高维 Arnold

变换更好的加密效果, 以及其灰度级和邻域灰度级对统计特性完全呈现均匀分布.

另外, 本文存在的不足是未从理论上证明变换(15)和(16)式的置乱周期的相等性问题, 这将是下一步将要研究的重要内容.

参考文献

[1] Arnold V I, Avez A 1968 *Ergodic Problems in Classical Mechanics* (New York: Benjamin) p286

[2] Franks J 1977 *Am. J. Math* **99** 1089

[3] Dyson F J, Falk H 1992 *Amer. Math Mon.* **99** 603

[4] Behrends E, Fiedler B 1998 *Ergod. theor. Dyn. Systems* **18** 331

[5] Li P, Xu J W 2005 *J. Cent. South Univ. Technol.* **12** 278

[6] Chen F, Wong K W, Liao X F, Xiang T 2012 *IEEE Trans. Inform. Theory* **58** 445

[7] Bao J H, Yang Q G 2012 *Nonlinear Dyn.* **70** 1365

[8] Chen F, Wong K W, Liao X F, Xiang T 2013 *IEEE Trans. Inform. Theory* **59** 3249

[9] Kong T, Zhang D 2004 *J. Software* **15** 1558 (in Chinese) [张涛, 张亶 2004 软件学报 **15** 1558]

[10] Huang W B, Zhang D Dong G C 2008 *Appl. Math. J. Chin. Univ.* **23** 99 (in Chinese) [黄外斌, 张亶, 董光昌 2008 高校应用数学学报 **23** 99]

[11] Shao L P, Qin Z, Heng X C, Gao H J 2008 *Acta Electron. Sin.* **36** 1355 (in Chinese) [邵利平, 覃征, 衡星辰, 高洪江 2008 电子学报 **36** 1355]

[12] Zhou L M 2010 *M.S. Dissertation* (Ganzhou: Gannan Normal University) (in Chinese) [周利敏 2010 硕士论文 (赣州: 赣南师范学院)]

[13] Pan C D, Pan C B 1998 *Simple Number Theory* (Beijing: Beijing University Press) p136 (in Chinese) [潘承洞, 潘承彪 1998 简明数论 (北京: 北京大学出版社) 第136页]

[14] Qi D X 1999 *J. North Chin. Uinv. Technol.* **11** 24 (in Chinese) [齐东旭 1999 北方工业大学学报 **11** 24]

[15] Qi D X, Zou J C, Han X Y 2000 *Sci. Chin.* (Ser. E) **43** 304

[16] Chen G, Mao Y B, Chui C K 2004 *Chaos, Soliton Fract.* **21** 749

[17] Deng X, Zhao D 2011 *Opt. Commun.* **284** 5623

[18] Liu Z, Gong M, Dou Y, Liu E, Ashfag M, Dai J, Liu S 2011 *Opt. Laser Engin.* **50** 246

[19] Kanso K, Chebleh M 2012 *Commun. Nonlinear Sci. Numer. Simul.* **17** 2943

[20] Ye G D, Wong K W 2012 *Nonlinear Dyn.* **69** 2079

[21] Ma Z G, Qiu Y S 2003 *J. Chin. Inst. Telecom.* **24** 51 (in Chinese) [马在光, 丘水生 2003 通信学报 **24** 51]

[22] Zhao L, Liao X F, Xiang T, Xiao D 2010 *Acta phys. Sin.* **59** 1507 (in Chinese) [赵亮, 廖晓峰, 向涛, 肖迪 2010 物理学报 **59** 1507]

[23] Yang L Z, Chen K F 2004 *Sci. Chin.* (Ser. F) **32** 151

[24] Li Y J, Ge J H, Li C L, Sun Z L 2010 *J. Univ. Sci. Technol.* **32** 1630 (in Chinese) [李用江, 葛建华, 李昌利, 孙志林 2010 北京科技大学学报 **32** 1630]

[25] Li Y J, Li C L, Ge J H, Sun Z L 2010 *Comput. Sci.* **37** 278 (in Chinese) [李用江, 李昌利, 葛建华, 孙志林 2010 计算机科学 **37** 278]

[26] Li Y J 2011 *Ph. D. Dissertation* (Xian: Xidian University) (in Chinese) [李用江 2011 博士论文 (西安: 西安电子科技大学)]

[27] Fransson J 2013 *B. S. Dissertation* (Smaland: Linnaeus University)

[28] Wu Y, Agaian S, Noonan J P 2012 *IEEE Sign. Process. Lett.* (received)

[29] Guo J S, Jin C H 2003 *J. Chin. inst. telecom.* **26** 131 (in Chinese) [郭建胜, 金辰辉 2003 通信学报 **26** 131]

[30] Liu T, Min L Q 2011 *J. Wuhan Univ. (Nat. Sci. Ed.)* **57** 444 (in Chinese) [刘婷, 闵乐泉 2011 武汉大学学报 (理科版) **57** 444]

[31] Zhang Q, Shen M F, Zhai Y K 2007 *J. Data Acq. Process.* **22** 292 (in Chinese) [张琼, 沈民奋, 翟懿奎 2007 数据采集与处理 **22** 292]

[32] Guan J, Ding Z Y, Duan X F 2013 *J. Guilin Univ. Electron. Technol.* **33** 152 (in Chinese) [关健, 丁振亚, 段雪峰 2013 桂林电子科技大学学报 **33** 152]

[33] Bao J H 2010 *Ph. D. Dissertation* (Guangzhou: South China University of technology) (in Chinese) [鲍江宏 2010 博士论文 (广州: 华南理工大学)]

[34] Rosen K H (translated by Xiao H G) 2009 *Elementary Number Theory and Its Application* (5th Ed.) (Beijing: China Machine Press) p133 (in Chinese) [罗申 KH 著 (夏洪刚译)2009 初等数论及其应用 (第5版) (北京: 机械工业出版社) 第133页]

[35] Gelfreich V 2000 *Phys. D* **136** 266

[36] Li C G, Han Z Z, Zhang H R 2003 *Chin. J. Comput.* **26** 465 (in Chinese)[李昌刚, 韩正之, 张浩然 2003 计算机学报 **26** 465]

[37] Chee S, Lee S, Park C, Sung S H 1999 *Electron. Lett.* **35** 707

[38] Shao L P, Qin Z, Gao H J, Heng X C 2007 *Acta Electron. Sin.* **35** 1290 (in Chinese)[邵利平, 覃征, 高洪江, 衡星辰 2007 电子学报 **35** 1290]

[39] Wu C K, Wang X M 1995 *J. Xidian Univ.* **22** 94 (in Chinese) [武传坤, 王新梅 1995 西安电子科技大学学报 **22** 94]

[40] Du Y Z, Ju Y, Wu W 2005 *J. Hefei Univ. Technol.* (Nat. Ed.) **28** 592 (in Chinese) [杜奕智, 琚耀, 吴伟 2005 合肥工业大学学报 (自然科学版) **28** 592]

[41] Jonathan K, Yehuda L (translated by Ren W) 2011 *Introduction to modern cryptography: Principles and Protocols* (Beijing: National Defense Industry Press) p138 (in Chinese) [乔纳森卡茨, 耶胡达林德尔著 (任伟译)2011 现代密码学—原理与协议 (北京: 国防工业出版社) 第138页]

[42] Peng F, Qiu S S, Long M 2005 *J. South Chin. Univ. Technol.* (Nat. Sci. Ed.) **33** 20 (in Chinese) [彭飞, 丘水生, 龙敏 2005 华南理工大学学报 (自然科学版) **33** 20]

[43] Xu S J, Wang J Z 2008 *Acta Phys. Sin.* **57** 37 (in Chinese)[徐淑奖, 王继志 2008 物理学报 **57** 37]

[44] Wang J, Jiang G P 2011 *Acta Phys. Sin.* **60** 060503 (in Chinese)[王静, 蒋国平 2011 物理学报 **60** 060503]

[45] Sun F Y, Liu S T, Lü Z W 2007 *Chin. Phys.* **16** 3616

[46] Wang Z, Huang X, Li N, Song X N 2012 *Chin. Phys. B* **21** 050506

[47] Luo Y L, Du M H 2013 *Chin. Phys. B* **22** 080503

[48] Zhang L Y, Li C Q, Wong K K, Shu S, Chen G R 2012 *J. Syst. Software* **85** 2077

[49] Zhang Y W, Wang Y M, Shen Y B 2007 *Sci. Chin.(Ser. F)* **50** 334

An improved discrete arnold transform and its application in image scrambling and encryption*

Wu Cheng-Mao†

(*School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*)

(Received 3 December 2013; revised manuscript received 23 January 2014)

Abstract

To improve the image scrambling and encryption effect in traditional two-dimensional discrete Arnold transform, a new nonlinear transform for image scrambling is proposed which improves the classical discrete Arnold transform with quasi-affine properties, and can be applied in image scrambling and encryption researching. This method first makes good use of the construction thought in classical discrete standard map, and embeds the nonlinear expressions of output results of one congruence equation for classical two-dimensional discrete Arnold transform into the input item of the other congruence equation for two-dimensional discrete Arnold transform. Then a new transform with good nonlinear characteristics is constructed on the basis of classical two-dimensional discrete Arnold transform in order to quickly improve the scrambling effect of the gray image. In the end, through mathematical proof it is shown that the proposed transform no longer has the quasi-affine invariance properties in the existing two-dimensional discrete Arnold transform, but it is still a reversible mapping with periodic properties; and when it is applied in image scrambling encryption, the original image can be restored from the scrambling and encryption in gray image for its periodic properties or inverse transform. Some experimental results show that the proposed nonlinear transform is effective, and can obtain better scrambling and encryption quality than the existing discrete two-dimensional Arnold transform, meanwhile it is more practical than the standard Arnold transform in view of security.

Keywords: image scrambling, Arnold transform, invertible map, scrambling effect

PACS: 05.45.Gg **DOI:** 10.7498/aps.63.090504

* Project supported by the National Natural Science Foundation of China (Grant Nos. 90607008, 61073106), and the Scientific Research Project of the Education Department of Shaanxi Province, China (Grant No. 2013JK1129).

† Corresponding author. E-mail: wuchengmao123@sohu.com