基于新的五维多环多翼超混沌系统的图像加密算法*

庄志本[1)] 李军[2)] 刘静漪[1)] 陈世强[3)†]

1) (湖北民族大学理学院, 恩施 445000)

2) (湖北民族大学信息工程学院, 恩施 445000)

3) (湖北民族大学新材料与机电工程学院, 恩施 445000)

(2019 年 9 月 5 日收到; 2019 年 11 月 21 日收到修改稿)

本文提出了一种基于新的五维多环多翼超混沌系统的数字图像加密方法. 首先, 将明文图像矩阵和五条混沌序列分别通过 QR 分解法分解成一个正交矩阵和一个上三角矩阵, 将混沌系统产生的五条混沌序列分别通过 LU 分解法分解成一个上三角矩阵和一个下三角矩阵, 分别将两个上三角矩阵和一个下三角矩阵相加, 得到五个离散后的混沌序列; 其次, 将明文图像矩阵分解出来的正交矩阵与五个混沌序列分解出来的五个正交矩阵相乘, 同时把明文图像矩阵分解出来的上三角矩阵中的元素通过混沌序列进行位置乱, 再将操作后的两个矩阵相乘; 最后, 将相乘后的矩阵通过混沌序列进行比特位位置乱, 再用混沌序列与其进行按位“异或”运算, 得到最终加密图像. 理论分析和仿真实验结果表明该算法的密钥空间远大于 10^{200}, 密钥敏感性强, 能够有效地抵御统计分析和灰度值分析的攻击, 对数字图像的加密具有很好的加密效果.

关键词: 五维超混沌系统, 正交分解, 比特位扰乱, 数字图像加密

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.69.20191342

1 引 言

在网络高速发展的今天, 保密通信已成为当今备受关注的一个热门话题, 其中混沌系统和超混沌系统的复杂结构和动力学行为在通信保密中有着很好的应用前景. 因此, 构造出能够产生具有复杂拓扑结构的超混沌系统是非常重要的.

目前, 构造新混沌系统的方法主要有三种, 一是通过引入一些非线性函数来产生多涡卷混沌吸引子[1−4]; 二是在三维混沌系统的基础上, 增加一个新的状态反馈控制器来构造出超混沌系统[5−7], 这就使得到的新混沌系统满足超混沌系统的必要条件. 在构造的过程中, 必须将新增加的控制器反馈到原始的控制器中, 同时将原始控制器反馈到新的控制器中, 这两个操作能够使此系统的四个控制器之间互相影响, 可使得关系更加复杂; 三是通过多个正李氏指数来构造超混沌系统[8]. 1979 年, Rossler 首次提出了超混沌系统, 从此, 专家和学者就相继提出了一些超混沌系统. 2014 年与 2015 年, 彭再平等[6] 和刘杨[7] 分别提出的新的四维超混沌系统结构简单, 动力学特征复杂, 但不具有多环的特征, 且刘杨的系统方程处于混沌状态的参数不够大. 本文提出了一种五维多环多翼超混沌系统, 能够产生明显的多环和多翼, 系统处于混沌状态的参数范围大, 且系统方程结构简单, 没有平衡点.

随着混沌理论及其应用的发展, 专家和学者提出了很多基于混沌的数字图像加密算法. 相对于传

* 湖北民族学院博士启动基金 (批准号: MY2018B014) 和国家自然科学基金 (批准号: 61562025) 资助的课题.

† 通信作者. E-mail: chensq8808@126.com

统的加密算法, 基于混沌的图像加密算法在安全性、抗攻击能力、复杂度等方面都具有很好的特性[9,10]. 因此, 专家和学者提出了许多基于混沌的图像加密算法. 为了提高后续密码系统的安全性, 2016 年, Zhang 等[11] 提出基于 3D 比特位矩阵的混合置换架构; 2018 年, Luo 等[12] 根据密钥和明文图像信息, 设计了一种新颖的并行量化方法. 而在图像的加密过程中, 主要是改变其像素的位置和像素值的大小, 目前主要有三种方法, 一是在比特位上用混沌序列进行行列扰乱, 二是直接对明文图像进行像素位置扰乱和改变像素值的大小[13−15], 三是用可逆矩阵去乘明文图像矩阵. 针对方法一, 2018 年, He 等[16] 提出对比特位高位进行扰乱, Raza 和 Satpute[17] 提出先对高 6 位进行处理, 紧接着再对低 6 位进行扰乱, 但所用的混沌系统都不是超混沌系统, 也不能产生多环; 针对方法三, 2017 年, Ahmad 等[18,19] 提出用正交矩阵去乘以明文图像矩阵, 以达到改变像素值的目的, 但不能很好地克服计算机精度对复杂的混沌动力学特性迅速退化问题. 在本文提出的方案中, 当混沌系统的参数 $f \in (0, 50)$ 时, 混沌系统都处于混沌状态; 将原文图像进行 QR 分解, 分别对正交矩阵 $\boldsymbol{Q}$ 和上三角矩阵 $\boldsymbol{R}$ 进行处理; 同时将混沌系统产生的 5 条混沌序列进行了 QR 分解和 LU 分解处理, 通过这些处理, 增大了穷举攻击的难度, 除穷举之外的一切基于明确的明文密文映射的攻击方法, 对该方法都将失效, 具有较高的安全性.

2 相关知识

2.1 矩阵的一些基本性质及运算规律

设 $\boldsymbol{Q}$ 是一个正交矩阵, $\boldsymbol{P}$ 为与 $\boldsymbol{Q}$ 满足乘法条件的一般矩阵, 那么:

i) $\boldsymbol{Q}$ 的逆一定存在并且有 $\boldsymbol{Q}^{-1} = \boldsymbol{Q}^{\mathrm{T}}$;

ii) $\boldsymbol{Q}^{-1}\boldsymbol{Q} = \boldsymbol{Q}^{\mathrm{T}}\boldsymbol{Q} = \boldsymbol{Q}\boldsymbol{Q}^{-1} = \boldsymbol{Q}\boldsymbol{Q}^{\mathrm{T}} = \boldsymbol{E}$, (其中 $\boldsymbol{E}$ 为单位矩阵);

iii) 如果 $\boldsymbol{A} = \boldsymbol{Q}\boldsymbol{P}$, 那么 $\boldsymbol{P} = \boldsymbol{Q}^{-1}\boldsymbol{A} = \boldsymbol{Q}^{\mathrm{T}}A$;

iv) 如果 $\boldsymbol{Q}_1, \boldsymbol{Q}_2, ..., \boldsymbol{Q}_n$ 都是与 $\boldsymbol{Q}$ 具有相同行列的正交矩阵, 且 $\boldsymbol{A}_1 = \boldsymbol{Q}_1\boldsymbol{Q}_2...\boldsymbol{Q}_n\boldsymbol{P}$, 则 $\boldsymbol{P} = \boldsymbol{Q}_n^{-1}\boldsymbol{Q}_{n-1}^{-1}...\boldsymbol{Q}_1^{-1}\boldsymbol{A}_1$.

2.2 矩形矩阵的正交分解与一般方阵的高斯消去法分解

矩形矩阵的正交分解又称 QR 分解. QR 分解是把一个 $m \times n$ 的矩阵 $\boldsymbol{A}$ 分解成一个正交矩阵 $\boldsymbol{Q}$ 和一个上三角矩阵 $\boldsymbol{R}$. 即设矩阵

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n-1} & a_{2n} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn-1} & a_{mn} \end{bmatrix},$$

通过调用 MATLAB 程序 $[\boldsymbol{Q},\boldsymbol{R}] = \mathrm{qr}(\boldsymbol{A})$, 就可以把矩阵 $\boldsymbol{A}$ 分解成一个正交矩阵

$$\boldsymbol{Q} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mm} \end{bmatrix}$$

和一个上三角矩阵

$$\boldsymbol{R} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n-1} & c_{1n} \\ 0 & c_{22} & c_{23} & \cdots & c_{2n-1} & c_{2n} \\ 0 & 0 & c_{33} & \cdots & c_{3n-1} & c_{3n} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & c_{mn} \end{bmatrix}.$$

很显然矩阵 $\boldsymbol{R}$ 是与矩阵 $\boldsymbol{A}$ 具有相同大小的上三角矩阵, 矩阵 $\boldsymbol{Q}$ 是 $m \times m$ 矩阵, 并且还要满足

$$\boldsymbol{A} = \boldsymbol{Q} \cdot \boldsymbol{R}$$

$$= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n-1} & a_{2n} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn-1} & a_{mn} \end{bmatrix}$$

$$= \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mm} \end{bmatrix}$$

$$\times \begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n-1} & c_{1n} \\ 0 & c_{22} & c_{23} & \cdots & c_{2n-1} & c_{2n} \\ 0 & 0 & c_{33} & \cdots & c_{3n-1} & c_{3n} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & c_{mn} \end{bmatrix}.$$

高斯消去法分解又称 LU 分解. LU 是把任意一个方阵 $\boldsymbol{X}$ 分解成一个下三角矩阵 $\boldsymbol{L}$ 和一个上三角矩阵 $\boldsymbol{U}$. 即设矩阵

$$\boldsymbol{X}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n-1} & a_{2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn-1} & a_{nn} \end{bmatrix},$$

通过调用 MATLAB 程序 $[\boldsymbol{L},\boldsymbol{U}]=\mathrm{lu}(\boldsymbol{X})$, 就可以把矩阵 $\boldsymbol{X}$ 分解成一个下三角矩阵

$$\boldsymbol{L}=\begin{bmatrix} b_{11} & 0 & 0 & \cdots & 0 & 0 \\ b_{21} & b_{22} & 0 & \cdots & 0 & 0 \\ b_{31} & b_{32} & b_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \cdots & b_{nn-1} & b_{nn} \end{bmatrix}$$

和一个上三角矩阵

$$\boldsymbol{U}=\begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n-1} & c_{1n} \\ 0 & c_{22} & c_{23} & \cdots & c_{2n-1} & c_{2n} \\ 0 & 0 & c_{33} & \cdots & c_{3n-1} & c_{3n} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & c_{nn} \end{bmatrix}.$$

很显然矩阵 $\boldsymbol{L}$ 和 $\boldsymbol{U}$ 都与方阵 $\boldsymbol{X}$ 具有相同的大小. 并且满足

$$\begin{aligned}\boldsymbol{X}&=\boldsymbol{L}\cdot\boldsymbol{U}\\ &=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n-1} & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n-1} & a_{2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn-1} & a_{nn} \end{bmatrix}\\ &=\begin{bmatrix} b_{11} & 0 & 0 & \cdots & 0 & 0 \\ b_{21} & b_{22} & 0 & \cdots & 0 & 0 \\ b_{31} & b_{32} & b_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ b_{n1} & b_{n2} & b_{n3} & \cdots & b_{nn-1} & b_{nn} \end{bmatrix}\\ &\quad\times\begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n-1} & c_{1n} \\ 0 & c_{22} & c_{23} & \cdots & c_{2n-1} & c_{2n} \\ 0 & 0 & c_{33} & \cdots & c_{3n-1} & c_{3n} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & c_{nn} \end{bmatrix}.\end{aligned}$$

3 新的五维多环多翼超混沌系统

1994 年, Sprott[20] 总结了许多三维混沌系统, 其 A 系统方程如下:

$$\begin{cases}\dot{x}=y,\\ \dot{y}=-x+yz,\\ \dot{z}=1-y^2.\end{cases}\tag{1}$$

在系统 (1) 的基础上, 我们引入了两个控制器 w,v, 并将原始控制器 y 反馈到新的控制器 w 中, 将原始控制器 z 反馈到新的控制器 v 中, 这两个操作能够使此系统的五个控制器之间互相影响, 可使得关系更加复杂. 新构造出来的五维多环多翼超混沌方程如下:

$$\begin{cases}\dot{x}=ay,\\ \dot{y}=-bx+cyz,\\ \dot{z}=g-dy^2,\\ \dot{w}=ey^3,\\ \dot{v}=fz,\end{cases}\tag{2}$$

方程中的 a, b, c, d, e, f, g 是系统参数, 且均取大于 0 的数.

3.1 Lyapunov 指数谱分析

混沌方程的主要动力学特性可以通过它的 Lyapunov 指数谱来进行分析. 当系统参数 $a=1.5$, $b=c=d=e=f=g=1$ 时, 该系统的 Lyapunov 指数谱如图 1 所示. 从图 1 中可以明显地看出, 该系统有两个 Lyapunov 指数为正, 一个 Lyapunov 指数为零, 还有两个 Lyapunov 指数为负, 因此系统 (2) 处于超混沌状态.

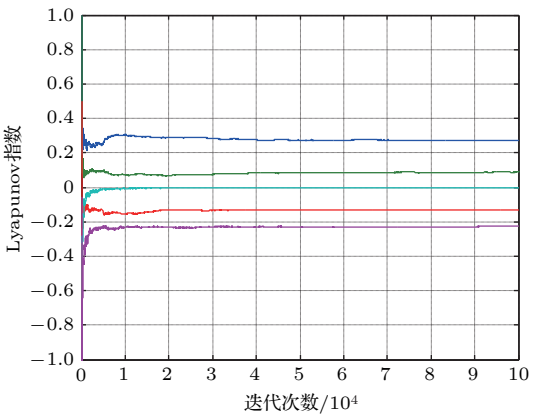

图 1 Lyapunov 指数谱

Fig. 1. Lyapunov exponent diagram.

3.2 平衡点分析

令 $\dot{x}=\dot{y}=\dot{z}=\dot{w}=\dot{v}=0$, 即

$$\begin{cases} ay = 0, \\ -bx + cyz = 0, \\ g - dy^2 = 0, \\ ey^3 = 0, \\ fz = 0, \end{cases} \tag{3}$$

很显然, 无论系统参数a, b, c, d, e, f, g取大于 0 的任何值, 方程 (3) 都没有解, 因此该系统方程无平衡点.

3.3 分岔图分析

方程参数$a = 1.5$, $b = c = d = e = g = 1$, 参数f在变化时, 关于f的分岔图如图 2 所示. 从图 2 中可以看出, 当$f \in (0, 50)$时, 系统 (2) 都是处于混沌状态. 因此, 该系统处于混沌状态的参数动态范围很大.

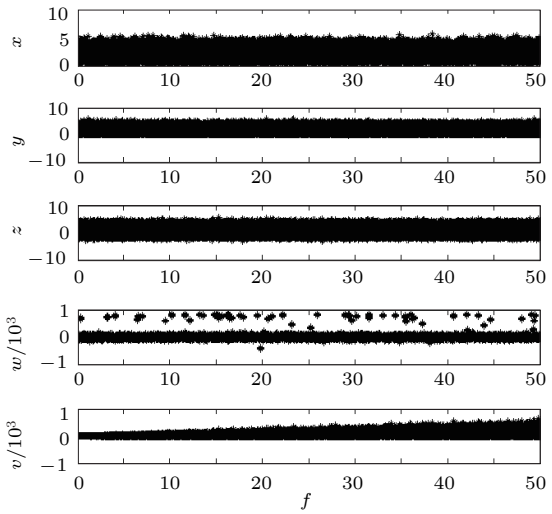

图 2 系统 (2) 随f变化的分岔图

Fig. 2. Bifurcation diagram of system (2) variation with f.

3.4 时间序列图

当系统参数$a = 1.5$, $b = c = d = e = f = g = 1$时, x, y, z, w, v的值随时间t的变化序列图如图 3 所示. 从图 3 中也可以看出, 在系统参数$a = 1.5$, $b = c = d = \ e = f = g = 1$时, 系统 (2) 处于混沌状态.

3.5 五维多环多翼混沌相图

当系统参数$a = 1.5$, $b = c = d = e = f = g = 1$时, 系统 (2) 产生的多环多翼的三维相图如图 4 所示. 方程 (2) 产生的多环多翼的平面相图如图 5 所示. 从图 4 和图 5 可以明显地看出, 该混沌系统能在多个方向上产生多环多翼.

4 算法描述

4.1 加密算法描述

给定一个$M \times N$的灰度图像$\boldsymbol{P}$, 加密步骤如下:

Step1 输入灰度图像$\boldsymbol{P}$, 通过QR分解把$\boldsymbol{P}$分解成一个正交矩阵$\boldsymbol{E}$和一个$M \times N$的上三角矩阵$\boldsymbol{R}$;

Step2 输入超混沌系统的初始值$y_0 = [1, 0.1, 2, 0.5, 0.4]$和步长$l = 0.02$, 求出迭代总时间$T = l \times (P \times P + 250)$. 其中$P = \max(M, N)$;

Step3 调用 ode45 函数, 迭代系统 (3), 产生 5 条混沌序列;

Step4 分别把 5 条混沌序列作如下处理:

$$B = \text{reshape}(y(201 : (200 + M \times N), i), M, N)$$
$$B1(:, :, i) = B, \quad i = 1, 2, 3, 4, 5 \tag{4}$$

其中$y(201 : (200 + M \times N), i)$是把混沌序列$y(i)$的第 201 个值到第$200 + M \times N$ 个值取出来; reshape$(y(201 : (200 + M \times N), i), M, N)$是把取出来的$M \times N$个值转换成$M \times N$矩阵;

Step5 第 4 步中的 5 个$M \times N$矩阵分别通过QR分解, 得到五个正交矩阵$\boldsymbol{E}_1, \boldsymbol{E}_2, \boldsymbol{E}_3, \boldsymbol{E}_4, \boldsymbol{E}_5$和五个上三角矩阵$\boldsymbol{R}_1, \boldsymbol{R}_2, \boldsymbol{R}_3, \boldsymbol{R}_4, \boldsymbol{R}_5$;

Step6 改变初始值y_0, 重复步骤二到步骤五$n(n \geqslant 2)$次, 得到$5n$个正交矩阵和$5n$个上三角矩阵. 分别记为$\boldsymbol{E}_{11}, \boldsymbol{E}_{12}, \boldsymbol{E}_{13}, \boldsymbol{E}_{14}, \boldsymbol{E}_{15}, \boldsymbol{E}_{21}, \cdots, \boldsymbol{E}_{n1}, \boldsymbol{E}_{n2}, \boldsymbol{E}_{n3}, \boldsymbol{E}_{n4}, \boldsymbol{E}_{n5}$;

Step7 第一步中的正交矩阵$\boldsymbol{E}$与第六步中的正交矩阵$\boldsymbol{E}_{11}, \boldsymbol{E}_{12}, \boldsymbol{E}_{13}, \boldsymbol{E}_{14}, \boldsymbol{E}_{15}, \boldsymbol{E}_{21}, \cdots, \boldsymbol{E}_{n1}, \boldsymbol{E}_{n2}, \boldsymbol{E}_{n3}, \boldsymbol{E}_{n4}, \boldsymbol{E}_{n5}$分别相乘, 得到矩阵$\boldsymbol{EE}$; 即$\boldsymbol{EE} = \boldsymbol{E}_{11} \times \boldsymbol{E}_{12} \times \boldsymbol{E}_{13} \times \boldsymbol{E}_{14} \times \boldsymbol{E}_{15} \times \boldsymbol{E}_{21} \times \cdots \times \boldsymbol{E}_{n1} \times \boldsymbol{E}_{n2} \times \boldsymbol{E}_{n3} \times \boldsymbol{E}_{n4} \times \boldsymbol{E}_{n5} \times \boldsymbol{E}$;

Step8 第三步中的五条混沌序列分别作如下处理:

$$B2 = \text{reshape}(y(201 : (200 + P \times P), i1), P, P)$$
$$B3(:, :, i1) = B2, \quad i1 = 1, 2, 3, 4, 5, \tag{5}$$

然后把这五个$P \times P$矩阵分别通过LU分解, 得到五个上三角矩阵$\boldsymbol{L}_1, \boldsymbol{L}_2, \boldsymbol{L}_3, \boldsymbol{L}_4, \boldsymbol{L}_5$ 和五个下三角矩阵$\boldsymbol{U}_1, \boldsymbol{U}_2, \boldsymbol{U}_3, \boldsymbol{U}_4, \boldsymbol{U}_5$;

Step9 $\boldsymbol{L}_1, \boldsymbol{L}_2, \boldsymbol{L}_3, \boldsymbol{L}_4, \boldsymbol{L}_5$与$\boldsymbol{U}_1, \boldsymbol{U}_2, \boldsymbol{U}_3, \boldsymbol{U}_4, \boldsymbol{U}_5$分别对应相加, 即$\boldsymbol{LU}_1 = \boldsymbol{L}_1 + \boldsymbol{U}_1, \boldsymbol{LU}_2 = \boldsymbol{L}_2 + \boldsymbol{U}_2,$

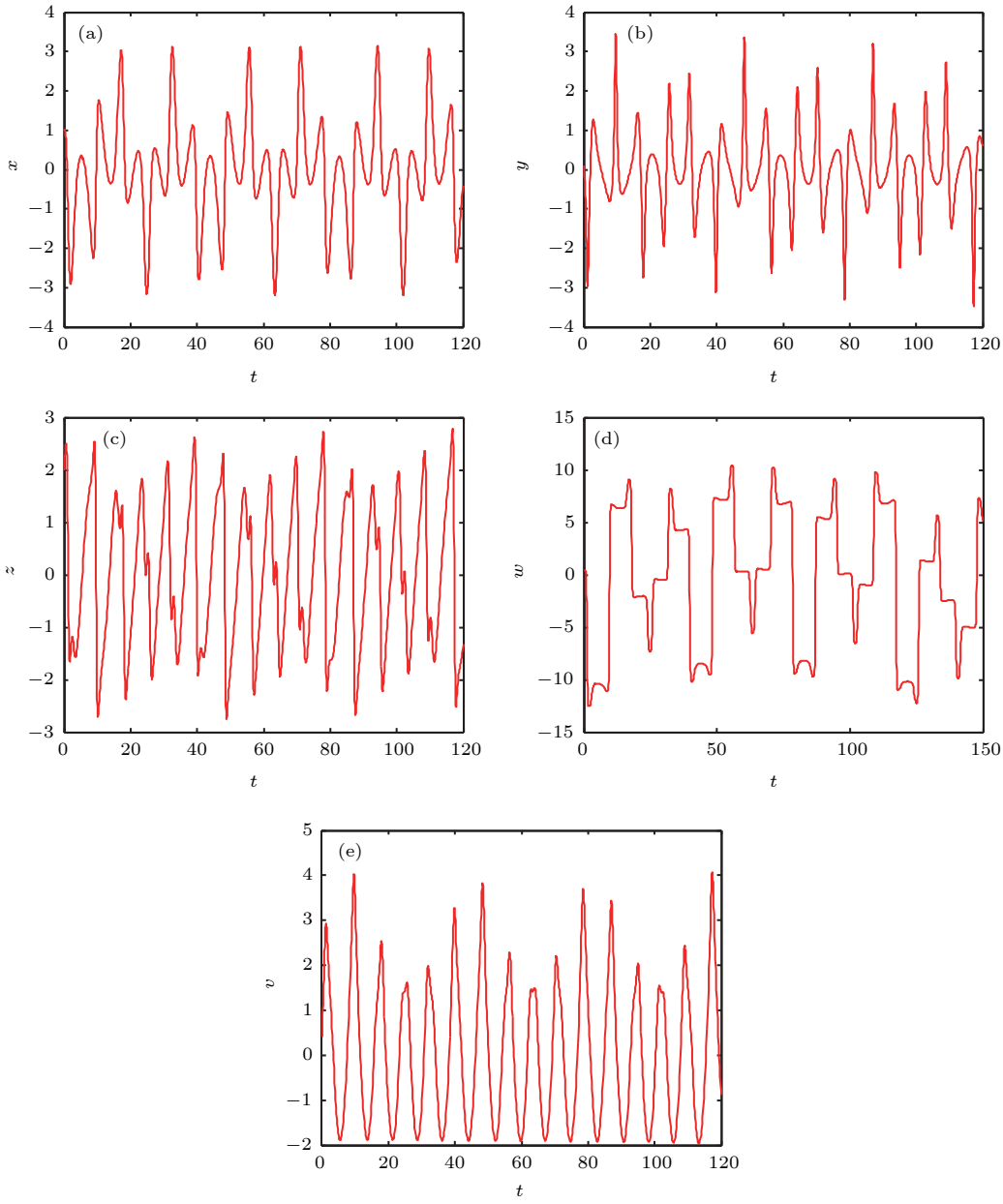

图 3 时间序列图 (a) x-t 时间序列; (b) y-t 时间序列; (c) z-t 时间序列; (d) w-t 时间序列; (e) v-t 时间序列

Fig. 3. Time series diagram: (a) x-t time series; (b) y-t time series; (c) z-t time series; (d) w-t time series; (e) v-t time series.

$\boldsymbol{LU}_3=\boldsymbol{L}_3+\boldsymbol{U}_3$, $\boldsymbol{LU}_4=\boldsymbol{L}_4+\boldsymbol{U}_4$, $\boldsymbol{LU}_5=\boldsymbol{L}_5+\boldsymbol{U}_5$. 然后分别取出 $\boldsymbol{LU}_i(i=1,2,3,4,5)$ 中的前 M 行与前 N 列位置上的元素, 从而得到五个 $M\times N$ 矩阵. 分别记为 $\boldsymbol{MN}_1,\boldsymbol{MN}_2,\boldsymbol{MN}_3,\boldsymbol{MN}_4,\boldsymbol{MN}_5$;

Step10 $\boldsymbol{MN}_1,\boldsymbol{MN}_2,\boldsymbol{MN}_3,\boldsymbol{MN}_4,\boldsymbol{MN}_5$ 与 $\boldsymbol{R}_1,\boldsymbol{R}_2,\boldsymbol{R}_3,\boldsymbol{R}_4,\boldsymbol{R}_5$ $\boldsymbol{R}_2,\boldsymbol{R}_3,\boldsymbol{R}_4,\boldsymbol{R}_5$ 分别对应相加, 即 $\boldsymbol{B}_{41}=\boldsymbol{MN}_1+\boldsymbol{R}_1$, $\boldsymbol{B}_{42}=\boldsymbol{MN}_2+\boldsymbol{R}_2$, $\boldsymbol{B}_{43}=\boldsymbol{MN}_3+\boldsymbol{R}_3$, $\boldsymbol{B}_{44}=\boldsymbol{MN}_4+\boldsymbol{R}_4$, $\boldsymbol{B}_{45}=\boldsymbol{MN}_5+\boldsymbol{R}_5$;

Step11 $\boldsymbol{B}_{41},\boldsymbol{B}_{42},\boldsymbol{B}_{43},\boldsymbol{B}_{44},\boldsymbol{B}_{45}$ 转换成 1 行 $M\times N$ 列的矩阵, 同时把每个矩阵中的所有元素转换成 0—255 之间的整数, 分别得到矩阵 $\boldsymbol{B}_{51},\boldsymbol{B}_{52},\boldsymbol{B}_{53},\boldsymbol{B}_{54},\boldsymbol{B}_{55}$;

Step12 $\boldsymbol{B}_{51},\boldsymbol{B}_{52},\boldsymbol{B}_{53},\boldsymbol{B}_{54},\boldsymbol{B}_{55}$ 作如下处理:

$$\begin{aligned}
&\boldsymbol{B}_{61}(i2)=\boldsymbol{B}_{51}(i2)\oplus\boldsymbol{B}_{52}(i2)\oplus\boldsymbol{B}_{53}(i2)\oplus\boldsymbol{B}_{54}(i2);\\
&\boldsymbol{B}_{62}(i2)=\boldsymbol{B}_{51}(i2)\oplus\boldsymbol{B}_{52}(i2)\oplus\boldsymbol{B}_{53}(i2)\oplus\boldsymbol{B}_{55}(i2);\\
&\boldsymbol{B}_{63}(i2)=\boldsymbol{B}_{51}(i2)\oplus\boldsymbol{B}_{52}(i2)\oplus\boldsymbol{B}_{54}(i2)\oplus\boldsymbol{B}_{55}(i2);\\
&\boldsymbol{B}_{64}(i2)=\boldsymbol{B}_{51}(i2)\oplus\boldsymbol{B}_{53}(i2)\oplus\boldsymbol{B}_{54}(i2)\oplus\boldsymbol{B}_{55}(i2);\\
&\boldsymbol{B}_{65}(i2)=\boldsymbol{B}_{52}(i2)\oplus\boldsymbol{B}_{53}(i2)\oplus\boldsymbol{B}_{54}(i2)\oplus\boldsymbol{B}_{55}(i2);
\end{aligned}\tag{6}$$

其中 $i2=1,2,3,\cdots,M\times N$;

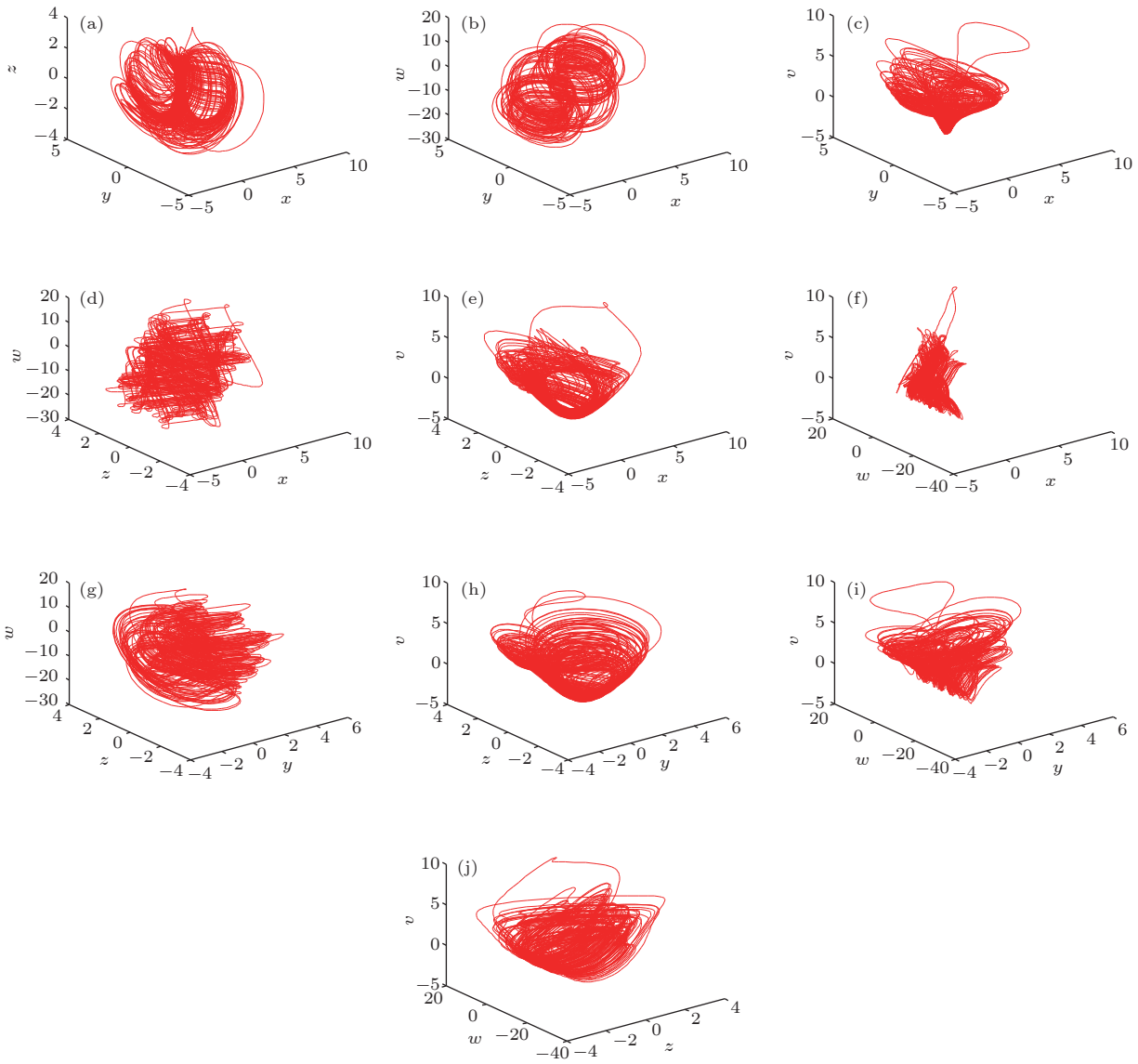

图 4 三维相图 (a) x-y-z 三维图; (b) x-y-w 三维图; (c) x-y-v 三维图; (d) x-z-w 三维图; (e) x-z-v 三维图; (f) x-w-v 三维图; (g) y-z-w 三维图; (h) y-z-v 三维图; (i) y-w-v 三维图; (j) z-w-v 三维图

Fig. 4. Three-dimensional phase diagram: (a) x-y-z Three-dimensional map; (b) x-y-w Three-dimensional map; (c) x-y-v Three-dimensional map; (d) x-z-w Three-dimensional map; (e) x-z-v Three-dimensional map; (f) x-w-v Three-dimensional map; (g) y-z-w Three-dimensional map; (h) y-z-v Three-dimensional map; (i) x-y-z Three-dimensional map; (j) z-w-v Three-dimensional map.

Step13 $\boldsymbol{B}_{61}, \boldsymbol{B}_{62}, \boldsymbol{B}_{63}, \boldsymbol{B}_{64}$作如下处理:

$$\begin{aligned}
&\boldsymbol{B}_{71} = \text{mod}(\text{round}(\boldsymbol{B}_{61}(1:M)\times 10^5), N-1)+1;\\
&\boldsymbol{B}_{72} = \text{mod}(\text{round}(\boldsymbol{B}_{62}(1:N)\times 10^5), M-1)+1;\\
&\boldsymbol{B}_{73} = \text{mod}(\text{round}(\boldsymbol{B}_{63}(1:M\times N)\times 10^{10}), 7)+1;\\
&\boldsymbol{B}_{74} = \text{mod}(\text{round}(\boldsymbol{B}_{64}((\text{end}-7):\text{end})\times 10^{20}),\\
&(M\times N-1))+1; \qquad (7)
\end{aligned}$$

其中 mod 为求模运算, round(f)是对 f 进行靠近取整;

Step14 上三角矩阵 $\boldsymbol{R}$ 的所有行的元素进行扰乱, 扰乱公式如下:

$$\begin{aligned}
&\boldsymbol{RR}(i3,:) = \text{circshift}(\boldsymbol{R}(i3,:), \boldsymbol{B}_{71}(i3), 2);\\
&i3 = 1, 2, ..., M, \qquad (8)
\end{aligned}$$

其中 $\boldsymbol{Z}(i3,:)$是矩阵 $\boldsymbol{Z}$的第 $i3$行的所有列, circshift($\boldsymbol{A}, k, 2$)是把行向量 $\boldsymbol{A}$ 的所有元素按顺时针方向移动 k 个单位;

Step15 将 $\boldsymbol{RR}$ 的所有列的元素进行扰乱, 扰

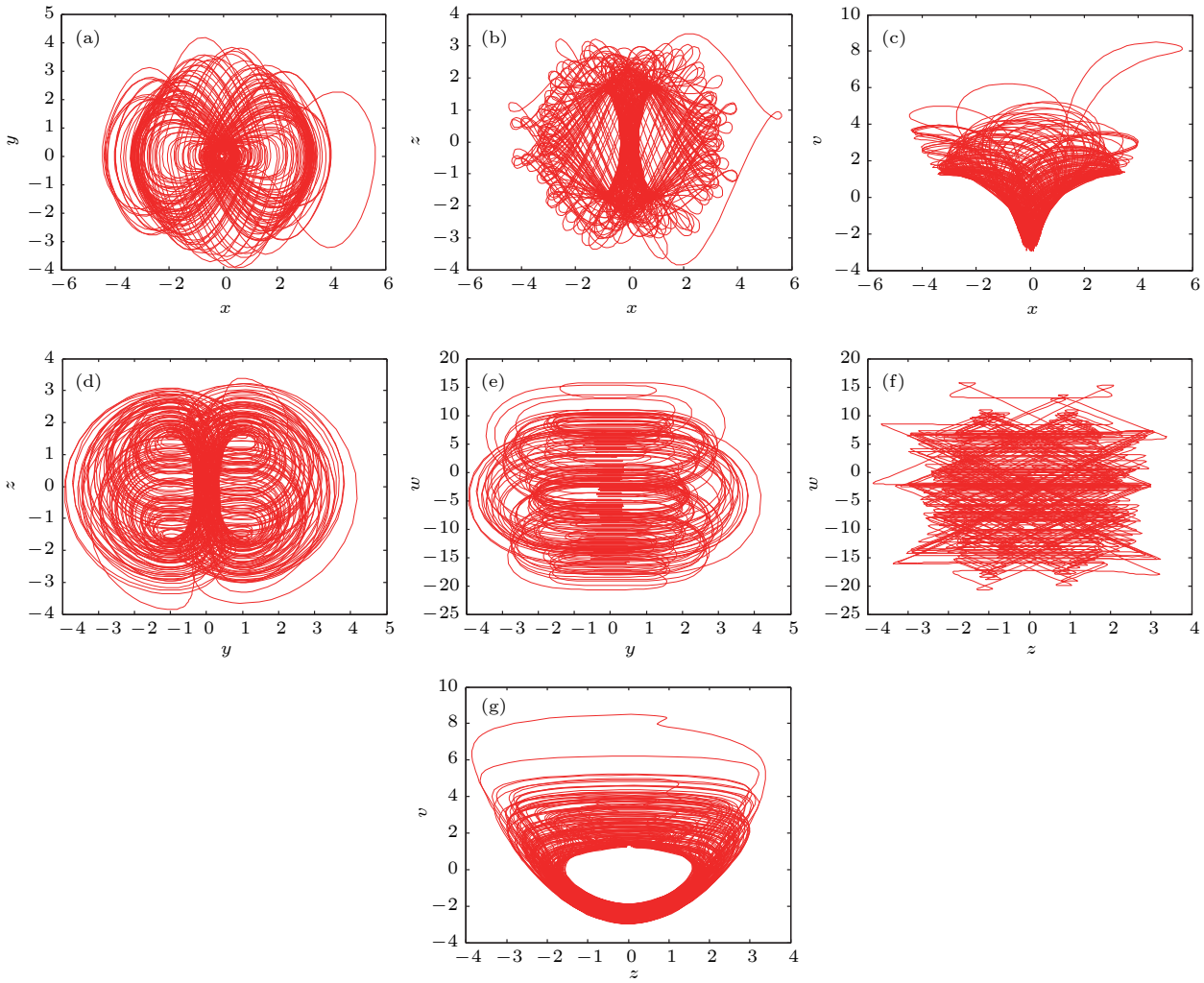

图 5 二维平面相图 (a) x-y 平面; (b) x-z 平面; (c) x-v 平面; (d) y-z 平面; (e) y-w 平面; (f) z-w 平面; (g) z-v 平面

Fig. 5. Two-dimensional plane phase diagram: (a) x-y flat; (b) x-z flat; (c) x-v flat; (d) y-z flat; (e) y-w flat; (f) z-w flat; (g) z-v flat.

乱公式如下:

$$\begin{aligned}&\boldsymbol{RR}_1(:,i4)=\text{circshift}(\boldsymbol{RR}(:,i4),\boldsymbol{B}_{72}(i4),1);\\&i4=1,2,\cdots,N,\end{aligned}\tag{9}$$

其中 $\boldsymbol{Z}(:,i4)$是矩阵 $\boldsymbol{Z}$的第 $i4$列的所有行, circshift$(B,k,1)$是把列向量 $\boldsymbol{B}$ 的所有元素按顺时针方向移动 k 个单位;

Step16 将 $\boldsymbol{EE}$与 $\boldsymbol{RR}_1$相乘, 得到矩阵 $\boldsymbol{EE}_1$, 即 $\boldsymbol{EE}_1=\boldsymbol{EE}\times\boldsymbol{RR}_1$;

Step17 将 $\boldsymbol{EE}_1$转换成 1 行 $M\times N$列的矩阵 $\boldsymbol{EE}_2$, 再把 $\boldsymbol{EE}_2$中的所有元素都映射成 0—255 之间的整数, 映射公式如下:

$$\begin{aligned}&\text{round}\left(\frac{\boldsymbol{EE}_2(i5)-(\min(\boldsymbol{EE}_2)-1)}{\max(\boldsymbol{EE}_2)-(\min(\boldsymbol{EE}_2)-1)}\times 255\right);\\&i5=1,2,\cdots,M\times N;\end{aligned}\tag{10}$$

Step18 第十七步中经过映射公式处理了的 $\boldsymbol{EE}_1$转换成二进制数, 得到矩阵 $\boldsymbol{EE}_2$;

Step19 $\boldsymbol{EE}_2$中的每一行二进制数分别进行扰乱, 得到矩阵 $\boldsymbol{EE}_3$, 扰乱公式如下:

$$\begin{aligned}&\boldsymbol{EE}_3(i6,:)=\text{circshift}(\boldsymbol{EE}_2(i6,:),\boldsymbol{B}_{73}(i6),2);\\&i6=1,2,\cdots,M\times N;\end{aligned}\tag{11}$$

Step20 $\boldsymbol{EE}_3$中的每一列二进制数分别进行扰乱, 得到矩阵 $\boldsymbol{EE}_4$, 扰乱公式如下:

$$\begin{aligned}&\boldsymbol{EE}_4(:,i7)=\text{circshift}(\boldsymbol{EE}_3(:,i7),\boldsymbol{B}_{74}(i7),1);\\&i7=1,2,\cdots,8;\end{aligned}\tag{12}$$

Step21 将 $\boldsymbol{EE}_4$转换成十进制数, 再把已经转换成十进制数的 $\boldsymbol{EE}_4$转换成 1 行 $M\times N$列的矩阵 $\boldsymbol{EE}_5$;

Step22 $\boldsymbol{EE}_5$与 $\boldsymbol{B}_{65}$进行按位"异或"运算, 得

到一个新的序列 $\boldsymbol{EE}_6$, 把 $\boldsymbol{EE}_6$ 转换成 $M \times N$ 的矩阵 $\boldsymbol{EE}_7$, $\boldsymbol{EE}_7$ 为最终的加密图像.

4.2 解密算法描述

Step1 输入图像矩阵 $\boldsymbol{EE}_7$, 同时与 $\boldsymbol{B}_{65}$ 进行按位"异或"运算, 得到一个新的序列 $\boldsymbol{EE}_8$;

Step2 $\boldsymbol{EE}_8$ 转换成二进制数, 然后把行列进行还原, 得到矩阵 $\boldsymbol{EE}_9$;

Step3 $\boldsymbol{EE}_9$ 转换成十进制数, 得到矩阵 $\boldsymbol{EE}_{10}$, 再把 $\boldsymbol{EE}_{10}$ 通过下列公式还原成 $\boldsymbol{EE}_1$,

$$\begin{aligned}\boldsymbol{EE}_1(j) = {} & (\boldsymbol{EE}_{10}(j) \div 255) \times (\max(\boldsymbol{EE}_2) \\ & - (\min(\boldsymbol{EE}_2) - 1)) \\ & + (\min(\boldsymbol{EE}_2) - 1), \end{aligned} \tag{13}$$

其中 $j = 1, 2, \cdots, M \times N$;

Step4 在 $\boldsymbol{EE}_1$ 的左边依次乘上 $\boldsymbol{E}_{11}, \boldsymbol{E}_{12}, \boldsymbol{E}_{13}, \boldsymbol{E}_{14}, \boldsymbol{E}_{15}, \boldsymbol{E}_{21}, \cdots, \boldsymbol{E}_{n1}, \boldsymbol{E}_{n2}, \boldsymbol{E}_{n3}, \boldsymbol{E}_{n4}, \boldsymbol{E}_{n5}, E$ 的逆, 得到矩阵 $\boldsymbol{RR}_1$;

Step5 $\boldsymbol{RR}_1$ 的行列进行还原, 得到矩阵 $\boldsymbol{R}$, 再把矩阵 $\boldsymbol{E}$ 与 $\boldsymbol{R}$ 相乘, 得到解密图像 $\boldsymbol{P}$.

5 实验结果

5.1 实验平台

PC 机配置: Intel(R) Core(TM) i3-4170 CPU @ 3.70 GHz, 内存 4 GB, Windows7 32 位操作系统. 通过 Matlab R2014 a 编写程序实现上述加密算法.

5.2 实验结果

实验选取了经典的 lena, baboon, boat 灰度图像, 其大小均为 512×512. 明文图像、加密图像和解密图像如图 6 所示.

6 安全性分析

6.1 密钥空间分析

决定图像加密算法强度的最重要因素之一是密钥空间的大小. 本文的初始密钥由 y_0 中的五个初

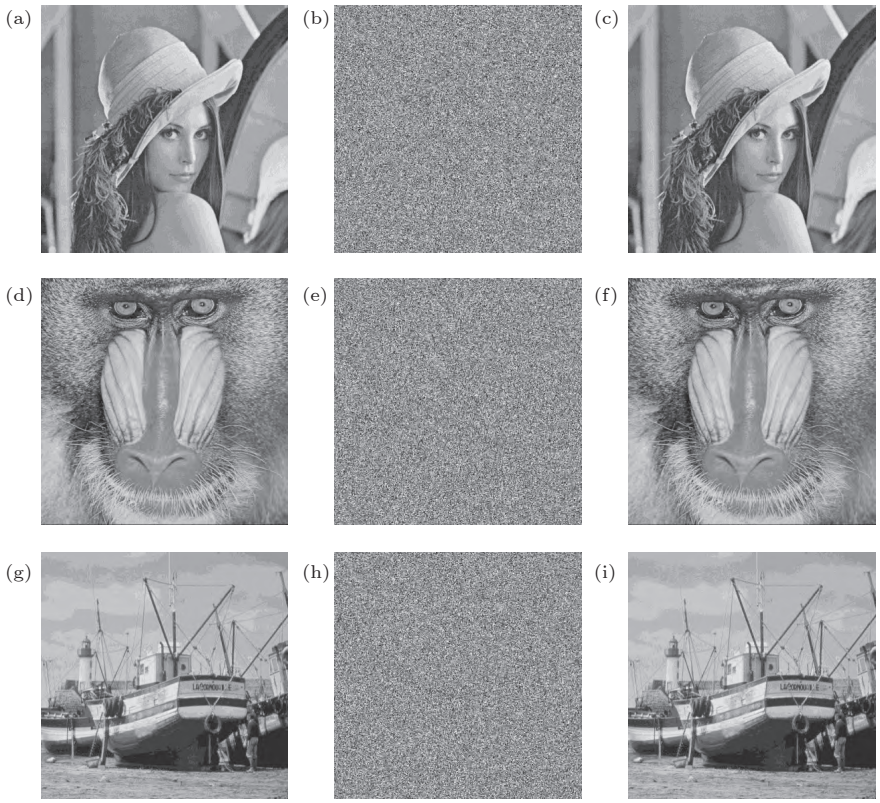

图 6 数字图像加解密实验图 (a) lena 原图; (b) lena 加密图像; (c) lena 解密图像; (d) baboon 原图; (e) baboon 加密图像; (f) baboon 解密图像; (g) boat 原图; (h) boat 加密图像; (i) boat 解密图像

Fig. 6. Digital image encryption and decryption experiment: (a) Original Lena image; (b) encrypted Lena image; (c) decrypted Lena image; (d) original baboon image; (e) encrypted baboon image; (f) decrypted baboon image; (g) original boat image.; (h) encrypted boat image; (i)decrypted boat image.

始值、系统参数a, b, c, d, e, f, g、正交矩阵$\boldsymbol{E}$和原图像的最大值最小值组成, 以计算机精度为10^{-15}计算的话, 本算法的密钥空间远大于$10^{200} > 2^{100}$. 如果一种图像加密算法的密钥空间大于2^{100}, 则它就是安全的[21,22]. 因此本算法是足够安全的.

6.2 直方图分析

直方图可以很好地反映图像像素值的分布情况, 直方图越平坦则像素值分布就越均匀. 图 7 分别是 lena, baboon 和 boat 的原图像直方图和加密后图像的直方图.

6.3 信息熵分析

信息熵是最重要的随意因素之一. 计算公式如下:

$$H(m) = -\sum_{i=1}^{L} p(m_i)\log_2 p(m_i), \tag{14}$$

这里的$p(m_i)$是m_i的机率, L是m_i的总数量. 对于灰度图像来说, 信息熵的最大值为 8. Lena,

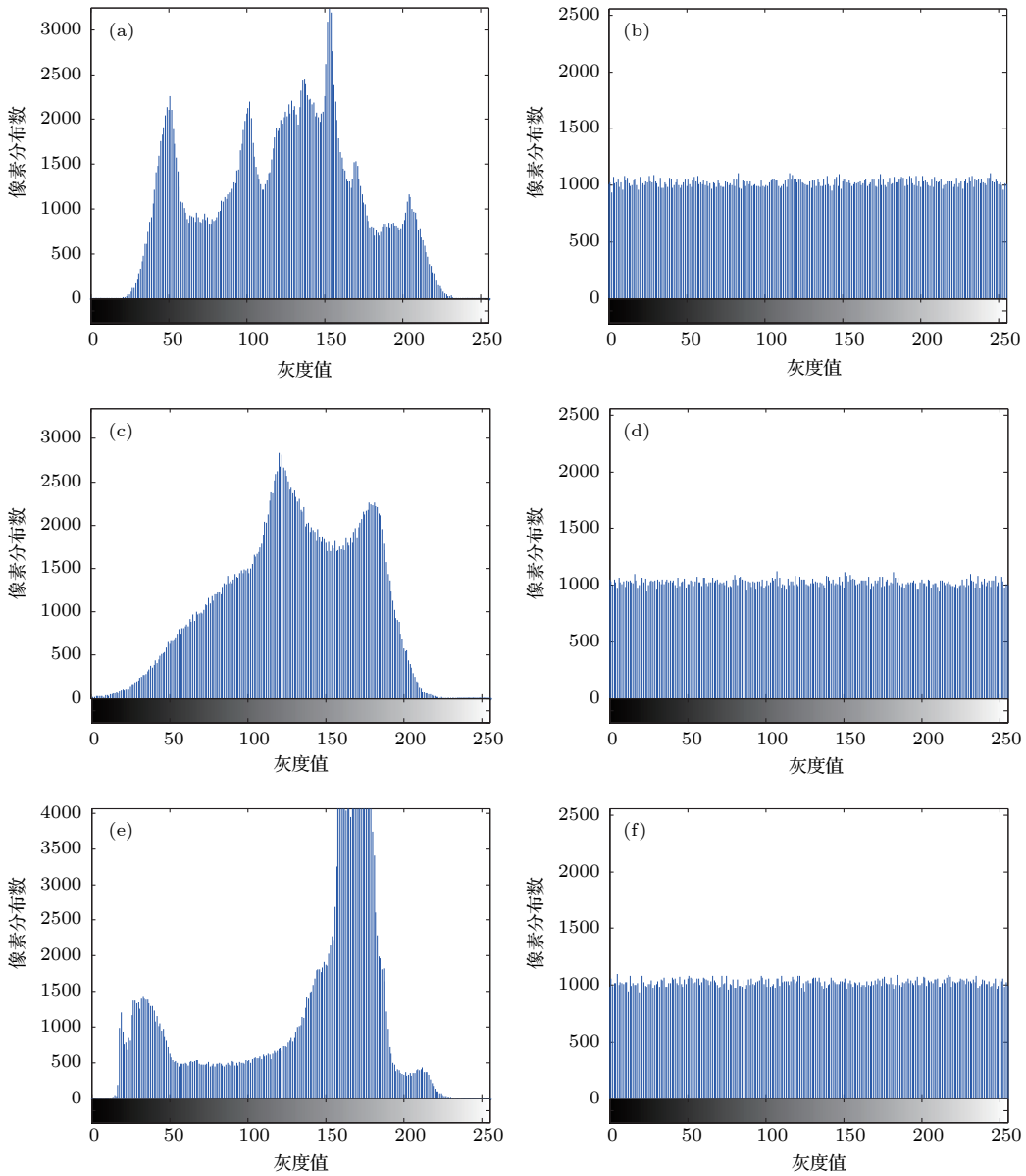

图 7 明文图像和密文图像直方图 (a) lena 明文直方图; (b) lena 密文直方图; (c) baboon 明文直方图; (d) baboon 密文直方图; (e) boat 明文直方图; (f) boat 密文直方图

Fig. 7. Histogram of plaintext and ciphertext images (a) Plaintext Lena image histogram; (b) ciphertext Lena image histogram; (c) plaintext baboon image histogram; (d) ciphertext baboon image histogram; (e) plaintext boat image histogram; (f) ciphertext boat image histogram.

baboon 和 boat 加密前后的信息熵与文献 [11—17] 的测试值如表 1 所列. 仿真实验结果表明本算法具有良好的加密效果.

表 1 明文图像与加密图像的信息熵分析表

Table 1. Information entropy analysis table of plain text and encrypted image.

图像	Lena图像	Baboon图像	Boat图像
原图像	7.4644	7.3713	7.1267
密文图像	7.9994	7.9994	7.9993
文献[11]	7.9992	7.9993	—
文献[12]	7.9994	7.9993	—
文献[13]	7.9971	—	7.9993
文献[14]	7.9960	—	—
文献[15]	7.9993	7.9993	—
文献[16]	7.9993	7.9992	—
文献[17]	7.9974	—	—

6.4 不动点比和灰度平均变化值分析

不动点比为图像加密后灰度值未发生变化的像素点占所有像素点的百分比, 计算公式如 (15) 式所示; 而灰度平均变化值能更好地评价加密图像灰度变化的程度, 计算公式如 (16) 式所示.

$$\mathrm{BD}(\boldsymbol{G},\boldsymbol{C})=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)\times 100\%, \tag{15}$$

其中 $f(i,j)=\begin{cases}1, & g_{ij}=c_{ij}\\ 0, & g_{ij}\neq c_{ij}\end{cases}$. 由 (15) 式计算出本算法的不动点比如表 2 所列.

$$\mathrm{GAVE}(\boldsymbol{C},\boldsymbol{G})=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|c_{ij}-\ g_{ij}|, \tag{16}$$

其中 $\boldsymbol{G}$ 为明文图像, $\boldsymbol{C}$ 为密文图像. 根据 (16) 式计算出本算法的灰度平均变化值如表 3 所列.

表 2 加密图像不动点比分析表

Table 2. Encrypted image fixed point ratio analysis table.

图像	总像素数	不动点数	不动点比
Lena图像	262144	1015	0.39%
Baboon图像	262144	1014	0.39%
Boat图像	262144	999	0.38%

表 3 灰度平均变化值分析表

Table 3. Grayscale average change value analysis table.

图像	Lena图像	Baboon图像	Boat图像
灰度平均变化值	73.1937	70.8589	74.8383

6.5 密钥敏感性分析

密钥的微小改变就会导致密文的极大改变, 这就是密钥敏感性. 实验以经典的 lena 图像为例. 图 8 展示了本算法对初始密钥的敏感性. 图 8(a) 是 lena 的明文图像; 图 8(b) 和图 8(c) 分别是用密钥 $y_0=[1,0.1,2,0.5,0.4]$ 和 $y_1=[1,0.1000000000000001,2,0.5,0.4]$ 加密的密文图像 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$; 图 8(d) 是 $\boldsymbol{Y}_1$ 用 y_0 正确解密的结果图; 图 8(e) 和图 8(f) 是 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$ 分别用错误的密钥 y_1 和 y_0 解密的结果. 图 8 说明尽管密钥 y_0 和 y_1 之间仅有微小的变化, 密文图像 $\boldsymbol{Y}_1$ 和 $\boldsymbol{Y}_2$ 却不能相应的用密钥 y_1 和 y_0 正确解密.

两幅图像之间的差异还可以用像素变化率 (NPCR) 和归一化平均变化强度 (UACI) 来度量. 计算公式分别如下:

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i,j}^{M,N}D\left(i,j\right)\times 100\%, \tag{17}$$

$$\mathrm{UACI}=\frac{\sum_{i,j}^{M,N}\left|C_1\left(i,j\right)-C_2\left(i,j\right)\right|}{M\times N\times 255}\times 100\%, \tag{18}$$

其中 $D\left(i,j\right)=\begin{cases}1, & C_1\left(i,j\right)\neq C_2\left(i,j\right)\\ 0, & C_1\left(i,j\right)=C_2\left(i,j\right)\end{cases}$; M,N 为图像的大小, $C_1\left(i,j\right)$ 和 $C_2\left(i,j\right)$ 分别是两幅图像在 (i,j) 位置上的像素值. NPCR 和 UACI 的值越大, 说明两幅图像之间的差异就越大. 为了更好地评价算法的密钥敏感性, 我们测试了分别用密钥 $y_0=[1,0.1,2,0.5,0.4]$ 和 $y_1=[1,0.1000000000000001,2,0.5,0.4]$ 加密的图像之间的 NPCR 和 UACI 的值, 测试值和文献 [13—16] 的测试值如表 4 所列. 从表 4 可以看出, 测试结果良好, 因此提出的加密算法具有良好的密钥敏感性.

6.6 相邻像素相关性分析

相邻像素的相关性用来评价图像加密算法在消除明文图像相邻像素相关性方面的效果. 本文分别在 lena, baboon 和 boat 的明文图像和密文图像中随机选取了 5000 个相邻像素点, 按 (19)—(22) 式计算明文图像与密文图像在水平方向的相邻像素的相关性系数、垂直方向的相邻像素的相关性系数和对角线方向的相邻像素的相关性系数. 测试结果如表 5 所列. Baboon 明文图像和密文图像在水

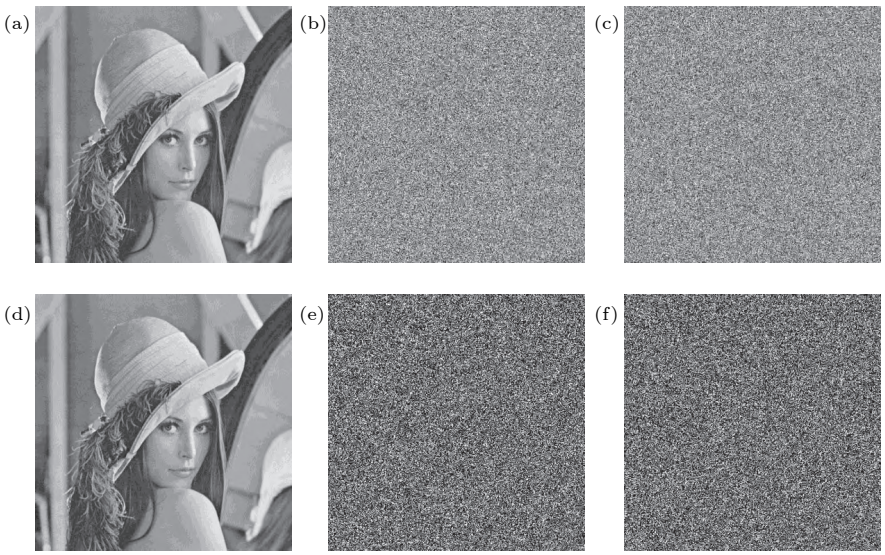

图 8 密钥敏感性测试图 (a) 明文图像; (b) 密文 $\boldsymbol{Y}_1$(密钥为 y_0); (c) 密文 $\boldsymbol{Y}_2$(密钥为 y_1); (d) $\boldsymbol{Y}_1$正确解密结果; (e) $\boldsymbol{Y}_1$用 y_1 错误解密结果; (f) $\boldsymbol{Y}_2$用 y_0 错误解密结果

Fig. 8. Key sensitivity tests: (a) Plain-image; (b) cipher $\boldsymbol{Y}_1$ with key y_0; (c) cipher $\boldsymbol{Y}_2$ with key y_1; (d) right decrypted $\boldsymbol{Y}_1$; (e) decrypted $\boldsymbol{Y}_1$ with y_1; (f) decrypted $\boldsymbol{Y}_2$ with y_0.

表 4 密钥敏感性测试结果表

Table 4. Key sensitivity test result table.

图像	lena图像		baboon图像		boat图像	
指标	NPCR	UACI	NPCR	UACI	NPCR	UACI
本文算法	0.9964	0.3340	0.9962	0.3346	0.9958	0.3344
文献[13]	0.9962	0.3347	—	—	0.9960	0.3340
文献[14]	0.9957	0.3508	—	—	—	—
文献[15]	0.9961	0.3347	0.9961	0.3347	—	—
文献[16]	0.9962	0.3344	0.9961	0.3349	—	—

表 5 明文图像与密文图像相关系数测试结果表

Table 5. Plaintext image and ciphertext image correlation coefficient test result table.

图像	水平方向相关系数		垂直方向相关系数		对角线方向相关系数	
	明文图像	密文图像	明文图像	密文图像	明文图像	密文图像
Lena	0.9762	–0.0084	0.9659	0.0461	0.9468	0.0131
Baboon	0.7204	–0.0050	0.8264	–0.0074	0.7046	–0.0322
boat	0.9621	0.0106	0.8252	0.0087	0.8327	–0.0423

平方向、垂直方向和对角线方向的像素相关性图如图 9 所示.

$$E(u)=\frac{1}{N}\sum_{i=1}^{N}u_i, \tag{19}$$

$$D(u)=\frac{1}{N}\sum_{i=1}^{N}(u_i-E(u))^2, \tag{20}$$

$$\mathrm{Cov}(u,v)=\frac{1}{N}\sum_{i=1}^{N}(u_i-E(u))(v_i-E(v)), \tag{21}$$

$$r_{uv}=\frac{\mathrm{Cov}(u,v)}{\sqrt{D(u)}*\sqrt{D(v)}}. \tag{22}$$

从表 5 中可以看出, 明文图像在三个方向上的相关系数都大于 0.6, 说明明文图像的相邻像素之间的相关性非常强; 而密文图像在三个方向上的相关系数都接近于 0, 说明密文图像的相邻像素之间的相关性已被打破.

从图 9 可以看出, 明文图像的像素点集中分布在对角线附近, 说明明文图像的像素点之间的相关性很强; 而密文图像的像素点分布得比较均匀、散

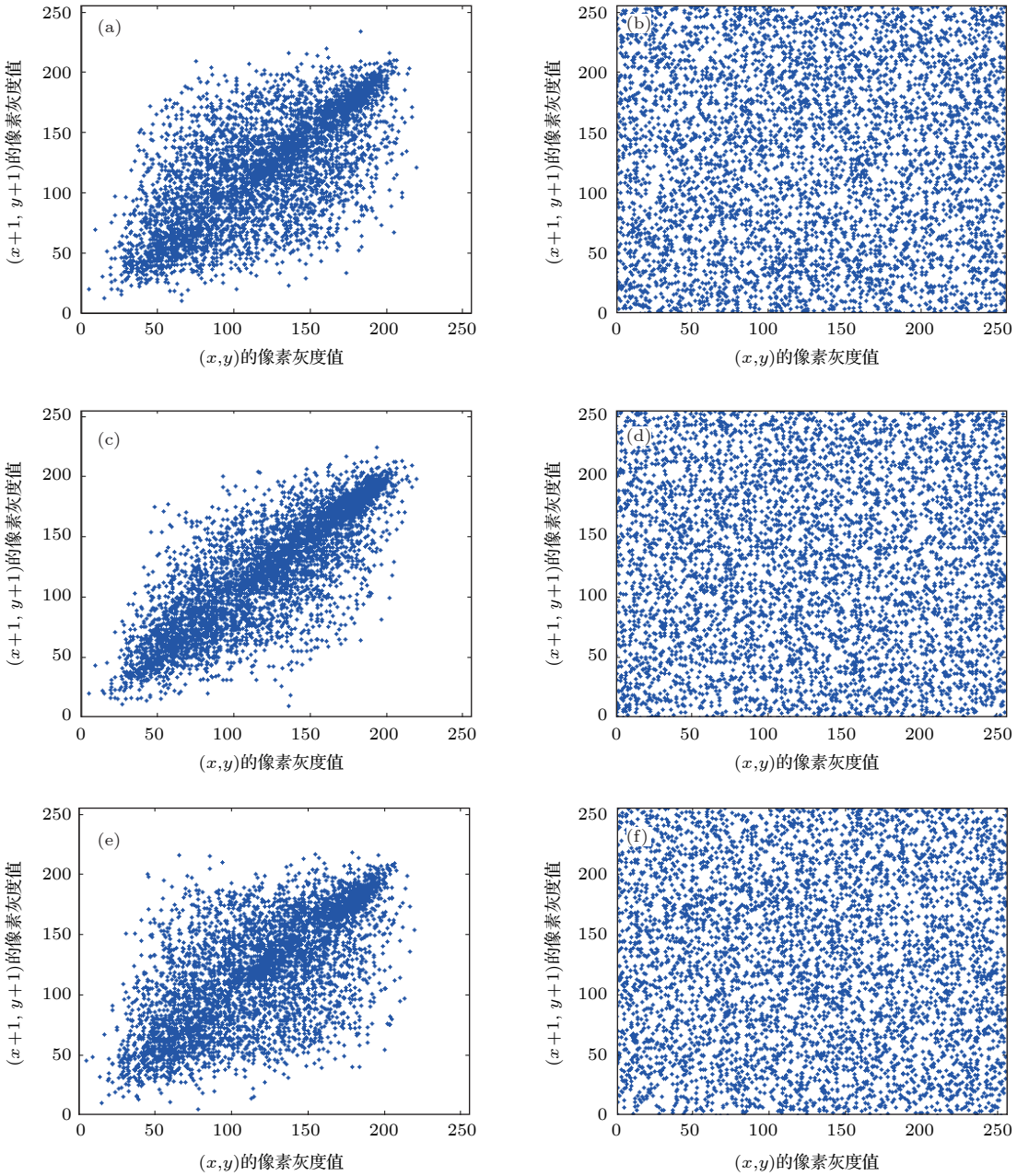

图 9 baboon 图像加密前后三个方向上的相关性分析图 (a), (b) 对角相邻; (c), (d) 水平相邻; (e), (f) 垂直相邻;

Fig. 9. Correlation analysis chart in three directions before and after baboon image encryption: (a), (b) Diagonally adjacent; (c), (d) horizontally adjacent; (e), (f) vertically adjacent.

乱, 说明密文图像的像素之间的相关性已被破坏. 因此提出的算法可以很好地降低图像相邻像素之间的强相关性, 对图像加密具有良好的效果.

6.7 抗剪切能力分析

为测试该算法的抗剪切能力, 我们剪掉 Lena 加密图像中间 60 × 60 大小的图像, 如图 10(b) 所示, 再对剪切过的加密图像进行解密, 解密图像如图 10(d) 所示. 图 10(a) 为原加密图像, 图 10(c) 为原加密图像的解密图像. 对比图 10(c) 和图 10(d) 可以发现, 图 10(d) 中有些点的像素值发生了改变, 但仍然可以显示出明文图像的大致信息. 因此, 加密图像在遭受剪切攻击后仍然具有一定的解密效果.

6.8 抗噪声能力分析

椒盐噪声是图像中常见到的一种噪声, 当影像讯号受到突如其来的强烈干扰、类比数位转换器或

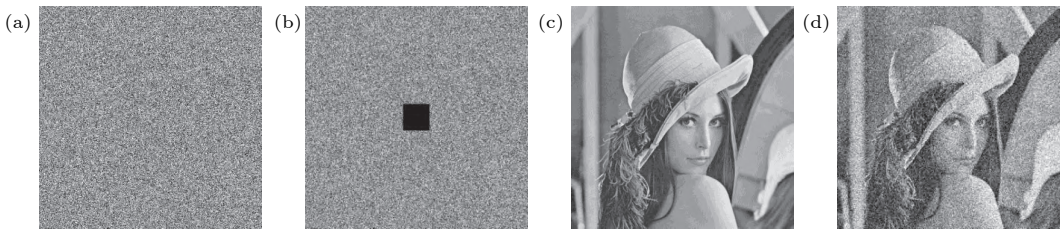

图 10 抗剪切攻击能力分析图 (a) 剪切前密文; (b) 剪切后密文; (c) 剪切前解密; (d) 剪切后解密

Fig. 10. Anti-shear attack capability analysis chart: (a) Ciphertext before cutting; (b) ciphertext after cutting; (c) decrypted image before cutting; (d) decrypted image after cutting.

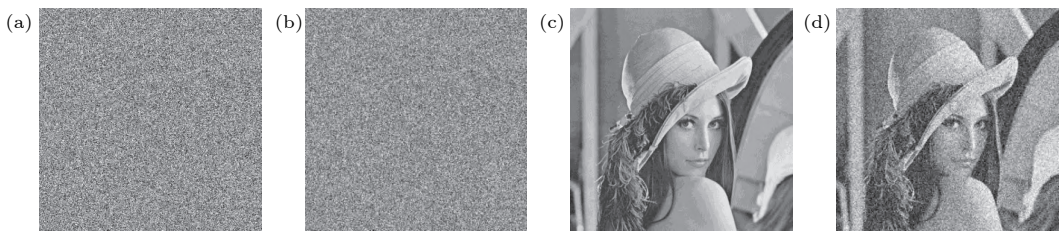

图 11 抗噪声攻击能力分析图 (a) 加噪前密文; (b) 加噪后密文; (c) 加噪前解密; (d) 加噪后解密

Fig. 11. Anti-noise attack capability analysis chart: (a) Ciphertext before adding noise; (b) ciphertext after adding noise; (c) decrypted image before adding noise; (d) decrypted image after adding noise.

位元传输错误等都可能产生椒盐噪声. 为了测试本算法的抗椒盐噪声攻击能力, 我们对 Lena 加密图像加入 1% 的椒盐噪声, 加噪后的加密图像如图 11(b) 所示, 再对加噪后的加密图像进行解密, 解密图像如图 11(d) 所示. 图 11(a) 为原加密图像, 图 11(c) 为原解密图像. 对比图 11(c) 和图 11(d) 可以发现, 图 11(d) 中有些点的像素值发生了改变, 但仍然可以显示出原始明文图像的大致信息. 这说明加密图像在遭受到椒盐噪声攻击后仍然具有一定的解密效果.

7 结 论

本文提出了一种新的五维多环多翼超混沌系统, 该系统结构简单. 对该混沌系统的基本动力学特征进行了理论分析和数值仿真实验, 包括 Lyapunov 指数谱、平衡点、分岔图、时间序列、相图等, 从相图中可以明显看出, 该混沌系统能够在多方向上产生多环多翼, 从分岔图可以看出, 该系统参数的动态范围很广. 同时, 将该五维多环多翼超混沌系统应用于物理混沌加密和代数加密的混合图像加密算法, 并对混合加密系统进行了数值仿真实验, 实验结果验证了该加密方法的正确性. 因此, 本文提出的加密算法在数字图像的保密通信中有很好的应用前景.

参考文献

[1] Wang P, Feng Y, Sun L X, Han F L 2002 *Control Theory & Appl.* **21** 1 (in Chinese) [王平, 冯勇, 孙黎霞, 韩凤玲 2002 控制理论与应用 **21** 1]

[2] Yu S M 2005 *Acta Phys.Sin.* **54** 1500 (in Chinese) [禹思敏 2005 物理学报 **54** 1500]

[3] Karthikeyan R, Serdar C, Peiman N, Abdul J M, Sajad J, Anitha K 2018 *Eur. Phys. J. Plus* **133** 354

[4] Jia M M, Jiang H G, Li W J 2019 *Acta Phys. Sin.* **68** 130503 (in Chinese) [贾美美, 蒋浩刚, 李文静 2019 物理学报 **68** 130503]

[5] Li Y X, Tang W K S, Chen G R 2005 *Int. J. Bifurcation Chaos.* **15** 3367

[6] Peng Z P, Wang C H, Lin Y, Luo X W 2014 *Acta Phys. Sin.* **63** 240506 (in Chinese) [彭再平, 王春华, 林愿, 骆小文 2014 物理学报 **63** 240506]

[7] Liu Y 2015 *Ph. D. Dissertation* (Harbin: Harbin Institute of Technology) (in Chinese) [刘杨 2015 博士学位论文 (哈尔滨: 哈尔滨工业大学)]

[8] Yu S M 2018 *Design Principles and Applications of New Chaotic Circuits and Systems* (Beijing: Science Press) pp139–155 (in Chinese) [禹思敏 2018 新型混沌电路与系统的设计原理及其应用 (北京: 科学出版社) 第139—155页]

[9] Zhang L H, Liao X F, Wang X B 2005 *Chaos, Solitons Fractals* **24** 759

[10] Wong K, Kwor B, Law W 2008 *Phys. Lett. A* **372** 2645

[11] Zhang W, Yu H, Zhao Y L, Zhu Z L 2016 *Signal Process.* **118** 36

[12] Luo Y L, Zhou R L, Liu J X, Gao Y, Ding X M 2018 *Nonlinear Dyn.* **4** 1

[13] Ye G D, Pan C, Huang X L, Mei Q X 2018 *Nonlinear Dyn.* **20** 18

[14] Abanda Y, Tiedeu A 2016 *IET Image Proc.* **10** 742

[15] Zhang Y 2018 *Inf. Sci.* **255** 31145

[16] He Y, Zhang Y Q, Wang X Y 2018 *Neural Comput. Appl.* **10** 1

[17] Raza S F, Satpute V 2018 *Nonlinear Dyn.* **254** 1
[18] Ahmad J, Khan M A, Hwang S O, Khan J S 2017 *Neural Comput. Appl.* **28** 953
[19] Ahmad J, Khan M A, Ahmed F, Khan J S 2018 *Neural Comput. Appl.* **3** 1
[20] Sprott J C 1994 *Phys. Rev. E* **50** 647
[21] Enayatifar R, Abdullah A H, Isnin I F, Altameem A, Lee A 2017 *Opt. Lasers Eng.* **90** 146
[22] Liu H J, Wang X Y, Kadir A 2012 *Appl. Soft Comput.* **12** 1457

Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system*

Zhuang Zhi-Ben [1)] Li Jun [2)] Liu Jing-Yi [1)] Chen Shi-Qiang [3)†]

1) (*School of Science*, *Hubei Mimzu University*, *Enshi* 445000, *China*)

2) (*School of Information Engineering*, *Hubei Minzu University*, *Enshi* 445000, *China*)

3) (*School of Advanced Materials and Mechatronic Engineering*, *Hubei Minzu University*, *Enshi* 445000, *China*)

(Received 5 September 2019; revised manuscript received 21 November 2019)

Abstract

The complex structure of hyperchaos and its complex dynamic behavior have a good application prospect in the fields of image encryption, digital watermarking and information security. Therefore, it has become very important to generate chaotic attractors with multi-vortex and multi-winged multi-rings with complex topologies. In this paper, we propose a new five-dimensional hyperchaotic system capable of generating multi-ring and multi-wing, and carry out theoretical analysis and numerical simulation experiments on some basic dynamic characteristics of the chaotic system. Such as equilibrium point, dissipation, Lyapunov exponent, bifurcation diagram, phase diagram and so on. In the process of encryption, first, we decompose the plaintext image matrix and the five chaotic sequences into an orthogonal matrix and an upper triangular matrix by QR decomposition. The five chaotic sequences generated by the chaotic system are respectively decomposed into an upper triangular matrix and a lower triangular matrix by the LU decomposition method. The upper triangular matrix decomposed by the QR decomposition method and the lower triangular matrix decomposed by the LU decomposition method are respectively added to obtain five discrete chaotic sequences. At the same time, the five discrete chaotic sequences are added to the upper triangular matrix decomposed by the LU decomposition method to obtain the final five discrete chaotic sequences. Secondly, the orthogonal matrix decomposed by the plaintext image matrix is multiplied by five orthogonal matrices decomposed by five chaotic sequences. At the same time, the elements in the upper triangular matrix decomposed by the plaintext image matrix are chaotically arranged by the chaotic sequence, and then the two matrices after the operation are multiplied. Finally, the multiplied matrix is chaotically placed on the bit by a chaotic sequence. Then use the chaotic sequence to perform a bitwise XOR operation to obtain the final encrypted image. The theoretical analysis and simulation results show that the algorithm has large key space and strong key sensitivity. It can effectively resist the attacks of statistical analysis and gray value analysis, and has good encryption effect on digital image encryption. This image encryption algorithm using a combination of conventional encryption and chaotic encryption does not have a defined plaintext ciphertext mapping relationship.

Keywords: five-dimensional hyperchaotic system, orthogonal decomposition, bit disturb, digital image encryption

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.69.20191342

* Project supported by the Doctoral Scientific Research Foundation of Hubei University for Nationalities, China (Grant No. MY2018B014) and the National Natural Science Foundation of China (Grant No. 61562025).

† Corresponding author. E-mail: chensq8808@126.com