

# 一个新多涡卷混沌系统的设计及在图像加密中的应用

摆玉龙 杨阳\* 唐丽红

(西北师范大学物理与电子工程学院 兰州 730070)

**摘要:** 该文提出一种三涡卷混沌系统, 首先对系统的李雅普诺夫指数、分岔图、Poincare截面图、功率谱图及平衡点稳定性等动力学特性进行了理论分析和数值仿真, 结果表明该系统具有良好的动力学特性和丰富的拓扑吸引子。基于电路仿真软件Multisim研制了实验仿真电路, 该电路结构简单、易于实际制作, 且仿真实验与理论分析结论十分吻合, 证实了提出的混沌系统电路在物理上是可以实现的, 从而验证了该混沌系统的混沌产生能力。最后结合DNA算法设计了一种彩色图像加密算法, 利用新系统混沌序列对图像进行加密, 重点分析了加密直方图、相邻像素相关性。结果表明, 新系统对混沌密钥及明文都非常敏感, 密钥空间较大, 提出的混沌系统应用于图像加密具有较高的安全性能。

**关键词:** 图像加密; 三涡卷; 混沌系统; 动力学行为; 电路实现

中图分类号: TN918.4

文献标识码: A

文章编号: 1009-5896(2021)02-0436-09

DOI: 10.11999/JEIT191002

## Design of a Multi-scroll Chaotic System and its Application to Image Encryption

BAI Yulong YANG Yang TANG Lihong

(College of Physics and Electronic Engineering, Northwest Normal University, Lanzhou 730070, China)

**Abstract:** A chaotic system with three scrolls is proposed. The dynamics characteristics of the system, such as Lyapunov index, bifurcation diagram, Poincare cross section diagram, power spectrum and equilibrium stability, are studied by numerical simulation. The analysis results show that the system has good dynamics characteristics and rich topological attractors. In addition, an experimental simulation circuit is developed based on the circuit simulation software Multisim, which has a simple structure and is easy to realize in practice. Moreover, the simulation experiment is very consistent with the theoretical analysis conclusion, confirming that the proposed chaotic system circuit can be realized physically, thus verifying the chaos generation capacity of the chaotic system. Finally, a color image encryption algorithm is designed based on DNA algorithm, and the results show that the system has high security performance. Using the new system chaotic sequence to encrypt image, the encryption histogram and correlation between adjacent pixels are analyzed, results show that the new systems are very sensitive to image key and plaintext, key space is large, chaotic system applied to image encryption has higher safety performance.

**Key words:** Image encryption; Multi-scrolls; Chaotic system; Dynamical behavior; Circuit implementation

### 1 引言

混沌系统是一种非线性动力系统, 具有不规则性、非周期性、不可预测性和对初始条件极其敏感

的特性<sup>[1]</sup>。由于洛伦兹在气象模型中首次观测到混沌现象, 因此混沌现象的产生一直被认为是一种有趣的非线性现象, 对混沌系统已有一些研究。例如 Rossler系统<sup>[2]</sup>, Arneodo系统<sup>[3]</sup>, Chen系统<sup>[4]</sup>等。由于混沌系统在模式识别、神经网络、保密通信、密码学等中应用广泛, 所以混沌系统得到了广泛的关注<sup>[5-10]</sup>, 研究人员不断探索混沌理论在不同的领域中的新应用。一般而言, 涡卷越多, 混沌行为的动力学和拓扑结构就越复杂<sup>[7]</sup>。现有的混沌系统多为单涡卷或双涡卷系统, 它们很少包含3个或更多的涡卷, 即使它们是用非光滑函数而不是光滑非线性

收稿日期: 2019-12-16; 改回日期: 2020-08-29; 网络出版: 2020-12-07

\*通信作者: 杨阳 2442361622@qq.com

基金项目: 国家自然科学基金(41861047, 41461078), 西北师范大学青年教师科研能力提升计划(NWNU-LKQN-17-6)

Foundation Items: The National Natural Science Foundation of China (41861047, 41461078), The Northwest Normal University Young Teachers' Scientific Research Capability Upgrading Program (NWNU-LKQN-17-6)

性项构造的。

随着互联网技术的快速发展，人们交流密切会导致大量的信息泄露，信息安全成为当今社会需要解决的问题。数字图像具有数据量大且像素之间相关性强的特点<sup>[8,9]</sup>，混沌系统具有随机性，因此将混沌系统应用到图像加密中具有一定的优势。在本文中，采用Arnold预处理与DNA加密算法相结合的双重加密，对加密前后图像相邻像素的直方图、相关性等进行了分析。结果表明，本文所提出的混沌系统应用于图像加密具有较高的安全性能。

本文的其余部分按如下结构组织：在第2节介绍一个3维空间三涡卷混沌系统；在第3、第4节将讨论所提出的混沌系统的动力学行为以及稳定性，对李雅普诺夫指数进行数值计算，然后分别对混沌系统的分岔图、庞加莱截面图、频谱图进行分析；电路实现以及仿真结果安排在第5节；第6节对于图像加密进行分析；第7节给出了结论。

## 2 一种新的混沌系统

设计的3维混沌系统，在一定的参数下体现出良好的混沌行为，其数学模型为

$$\left. \begin{aligned} \frac{dx}{dt} &= \alpha(y-x) + \gamma xz \\ \frac{dy}{dt} &= \varepsilon y - xz + x \\ \frac{dz}{dt} &= \beta z - xy - \delta x^2 \end{aligned} \right\} \quad (1)$$

其中， $x, y, z$ 为系统的状态变量， $\alpha = 40, \beta = 0.9, \gamma = 0.5, \delta = 0.6, \varepsilon = 12$ 为系统的参数。当系统的参数为 $\alpha = 40, \beta = 0.9, \gamma = 0.5, \delta = 0.6, \varepsilon = 12$ 时，初

始值为(1,0,0)时，系统式(1)存在复杂的混沌现象，包含着复杂的拉伸和扭曲结构，如图1所示，但是从整体上看系统又是稳定的。

利用4阶龙格库塔算法解方程式(1)，步长设置为0.001。图1(a)、图1(b)、图1(c)分别展示了系统式(1)混沌吸引子在 $(x, y), (x, z)$ 和 $(y, z)$ 3个平面的2维映射图，图1(d)表示的是混沌吸引子的3维映射图。

## 3 多涡卷系统动力学特性分析

### 3.1 Lyapunov指数和维数

Lyapunov指数(LE)可以定量地表征系统的运动状态特性，形象地描述系统相邻轨迹之间彼此吸引和排斥的程度，是刻画混沌系统的一个最重要的物理量。因此利用LE谱能够清晰地观察到当系统的参数发生变化时，系统的运动状态随之发生变化，曲线由上向下依次表示为 $LE_1, LE_2$ 和 $LE_3$ 。当系统参数设置为 $\alpha = 40, \beta = 0.9, \gamma = 0.5, \delta = 0.6, \varepsilon = 12$ 时，计算系统的Lyapunov指数为 $LE_1 = 0.5598, LE_2 = 0.0006, LE_3 = -3.1715$ ，图2给出了在 $\delta = [0.5, 0.8]$ 时该混沌系统随着参数 $\delta$ 发生变化时的曲线，观察曲线可以看出，当 $\delta = [0.5, 0.52]$ 时，只有一个 $LE_1 = 0$ ，其他两个LE指数小于0，表明此区间为周期运动；当 $\delta = [0.5202, 0.5256], [0.5343, 0.5478], [0.5518, 0.6887], [0.6931, 0.7182], [0.7373, 0.7532]$ 时，可以观察到存在正的LE指数，系统处于混沌状态。综合来说， $\delta$ 的变化区间内保持一个正的、一个接近于0、一个负的LE指数，存在混沌吸引子，系统始终处于复杂的混沌状态。

系统的LE维数

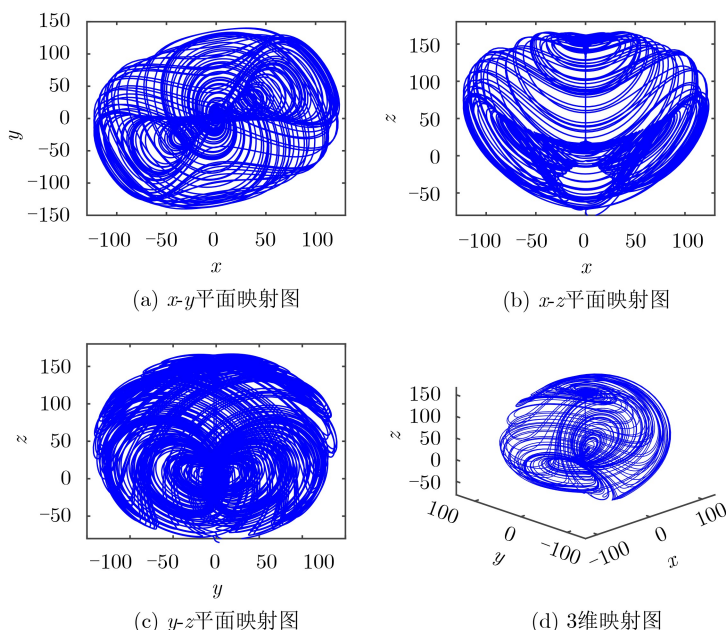


图1 三涡卷混沌系统的相图

$$D_L = j + \frac{1}{|\text{LE}_{j+1}|} \sum_{i=1}^j \text{LE}_i = 2 + \frac{\text{LE}_1 + \text{LE}_2}{\text{LE}_3} = 2.1765 \quad (2)$$

显然系统式(1)的Lyapunov维数是分数维,表示一个奇异吸引子,说明系统是混沌系统,具有复杂的分形结构。

### 3.2 分岔图和庞加莱截面图

分岔是非线性领域一个重要的内容。图3给出了混沌系统的状态变量z随着系统参数δ发生变化的分岔图,可以清晰地观察到系统的周期、倍周期、混沌运动的参数范围等。将其与LE谱进行对比分析之后发现,两者随参数的变化情况基本一致,可以看出混沌系统关于z=0对称。

Poincare截面对于分析多变量的系统很有效果,由于系统是3维的,所以在相空间中应做2维的Poincare截面图,如图4所示利用MATLAB选取x=0, y=0, z=0分别得到y-z, x-z, x-y平面上的Poincare截面,当Poincare截面上只有1个不动点或少数离散点时,运动是周期的;当Poincare截面上是1条封闭的连续曲线时,运动是拟周期的;当Poincare截面上是一段连续曲线或是一些成片的密集点时,运动是混沌的。通过观察截面图,可以验证系统是混沌的<sup>[4]</sup>。

### 3.3 功率谱分析

周期信号的功率谱是离散谱,非周期信号的功效

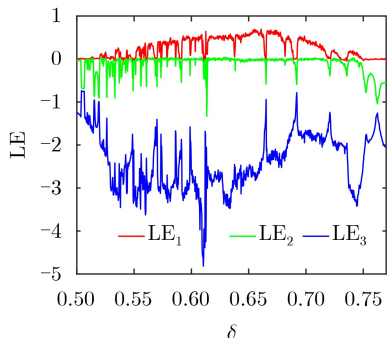


图2 参数δ变化时的Lyapunov指数谱

率谱是连续谱。对于混沌系统来说,产生的混沌信号是非周期信号,所以其功率谱也应为连续谱。由此可见,可以用功率谱来分析区别周期信号和混沌信号。图5给出了系统式(1)的功率谱图,可以观察到是连续谱。

## 4 系统稳定性分析

### 4.1 耗散性

通过式(3)得到系统的散度

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} = \gamma z - \alpha + \varepsilon + \beta \quad (3)$$

系统的散度 $\gamma z - \alpha + \varepsilon + \beta = -27.1 < 0$ ,其中z恒为0,散度小于0,所以系统是耗散的,并且系统以指数形式 $\frac{dv}{dx} = e^{-27.1t}$ 收敛。当 $t \rightarrow \infty$ 时,所有的系统轨线最终将会被限制在一个体积为零的极限点集上,而且它的动力学行为将会被固定在一个吸引子上,这充分证明了吸引子的存在。

### 4.2 平衡点

为求系统平衡点,令非线性混沌系统式(1)方程的右边等于零,得到

$$\left. \begin{aligned} \alpha(y-x) + \gamma xz &= 0 \\ \varepsilon y - xz + x &= 0 \\ \beta z - xy - \delta x^2 &= 0 \end{aligned} \right\} \quad (4)$$

当参数为 $\alpha = 40, \beta = 0.9, \gamma = 0.5, \delta = 0.6, \varepsilon = 12$ ,系统的平衡点集为 $(0, 0, 0), (\pm P, \pm(\alpha - \gamma)PQ,$

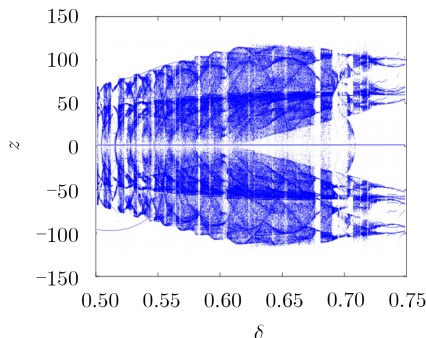


图3 z变量随参数δ变化时的分岔图

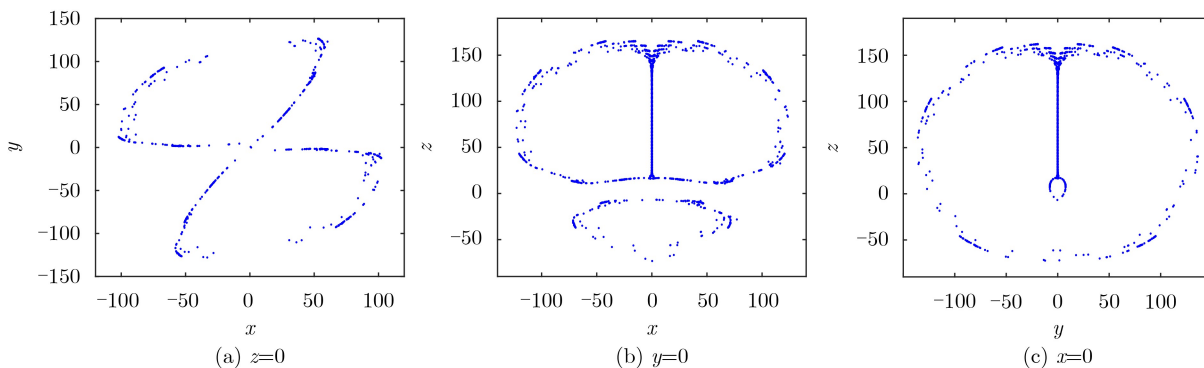


图4 系统式(1)的Poincare截面图

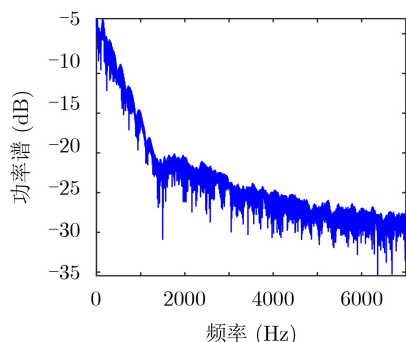


图5 系统的功率谱图

$\alpha(\varepsilon + 1)Q$ , 在平衡点集 $(0, 0, 0)$ 处, 线性化系统<sup>[6]</sup>得到Jacobi矩阵

$$\mathbf{J} = \begin{bmatrix} -\alpha + \gamma z & \alpha & \gamma x \\ -z + 1 & \varepsilon & -x \\ y - 2\delta x & x & \beta \end{bmatrix} \quad (5)$$

令 $\det(\mathbf{J} - \lambda\mathbf{I}) = 0$ , 其 $\mathbf{I}$ 为单位矩阵, 求得系统在平衡点 $(0, 0, 0)$ 处的特征值为 $\lambda_1 = -40.7581$ ,  $\lambda_2 = 12.7581$ ,  $\lambda_3 = 0.9$ , 有两个正的特征值, 一个负的特征值, 说明平衡点 $(0, 0, 0)$ 是不稳定的鞍点。

## 5 电路设计与仿真实验

对系统进行了理论分析和数值仿真之后, 为了进一步验证混沌系统的动力学行为, 本节将在实验上通过设计非线性模拟电路进行验证分析。首先对系统式(1)进行了尺度变换, 令 $\mu = k_a x$ ,  $v = k_a y$ ,  $z = k_a z$ ,  $\tau = k_t t$ ,  $k_a$ 是振幅变换系数,  $k_t$ 是时间变换系数。应用上述变换, 系统式(1)变为

$$\left. \begin{aligned} \frac{\partial \mu}{\partial \tau} &= 4000(\mu - v) + 2000v \\ \frac{\partial v}{\partial \tau} &= 100\mu + 1000v - 4000\mu v \\ \frac{\partial w}{\partial \tau} &= 90w - 2400\mu^2 - 4000\mu w \end{aligned} \right\} \quad (6)$$

其中,  $\mu, v, w$ 是新的状态变量,  $k_a = 0.025$ ,  $k_t = 100$ , 电路原理图如图6所示, 便于系统的电路实现, 运算放大器选用LM358, 乘法器选用AD633JN, 电源选用 $\pm 15V$ 。应用算法方程式(6)变为

$$\left. \begin{aligned} \frac{d\mu C_1}{dt} &= -\frac{1}{R_1 C_1} \mu c_1 + \frac{1}{R_2 C_1} \mu c_2 + \frac{1}{R_3 C_1} \mu c_1 \mu c_3 \\ \frac{d\mu C_2}{dt} &= \frac{1}{R_4 C_2} \mu c_2 + \frac{1}{R_5 C_2} \mu c_2 - \frac{1}{R_6 C_2} \mu c_1 \mu c_3 \\ \frac{d\mu C_3}{dt} &= \frac{1}{R_7 C_3} \mu c_3 + \frac{1}{R_8 C_3} \mu c_1 \mu c_2 + \frac{1}{R_9 C_3} \mu c_1 \mu c_1 \end{aligned} \right\} \quad (7)$$

其中,  $\mu c_1, \mu c_2, \mu c_3$ 分别是通过 $C_1, C_2, C_3$ 的电压。通过对比方程式(6)和方程式(7), 可以得到

$$\left. \begin{aligned} \frac{1}{R_1 C_1} &= \frac{1}{R_2 C_1} = 4000, \frac{1}{10 R_3 C_1} = 2000 \\ \frac{1}{R_4 C_2} &= 100, \frac{1}{R_5 C_2} = 1000, \frac{1}{10 R_6 C_2} = 4000 \\ \frac{1}{R_7 C_3} &= 90, \frac{1}{10 R_8 C_3} = 2400, \frac{1}{10 R_9 C_3} = 4000 \end{aligned} \right\} \quad (8)$$

令 $C_1 = C_2 = C_3 = 0.1$ , 对于方程式(8), 我们取 $R_1 = R_2 = 2.5 \text{ k}\Omega$ ,  $R_3 = 500 \Omega$ ,  $R_4 = 100 \text{ k}\Omega$ ,  $R_5 = 10 \text{ k}\Omega$ ,  $R_6 = R_8 = 250 \Omega$ ,  $R_7 = 110 \text{ k}\Omega$ ,  $R_9 = 417 \text{ k}\Omega$ ,  $R_{10} = R_{11} = R_{12} = R_{14} = R_{15} = 10 \text{ k}\Omega$ 。

通过在Multisim电路仿真软件上进行验证, 得到的相位图如图7所示, 通过比较发现, 理论吸引子和电路吸引子比较相似。因此该混沌系统在数值分析和实验研究方面得到了证实, 存在吸引子。

## 6 在图像加密中的应用

设计新型的图像加密算法<sup>[10]</sup>已经成为现在研究的热点。“置乱”是一种传统的图像加密方法<sup>[11]</sup>, 它有许多的优点但是仍然存在局限性, 1次加密算法被证明是不安全的, 很容易被选择明文攻击所攻破, 因此配合混沌系统和新的算法可以达到更好的加密效果。本文所采用的图像加密算法为双重加密, 以一副大小为 $M \times N$ 的彩色图像为例, 先对原始图像进行Arnold变换置乱进行预处理, 然后对变换后的1次加密图像进行DNA加密运算, 加密流程如图8所示。

### 6.1 预处理

Arnold置乱变换是由Arnold提出的一种置乱方法<sup>[12]</sup>, 该方法最初是对猫脸图像进行操作, 因此也称为猫脸变换, 实质是新旧位置的一一映射, 具体变换矩阵公式为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (9)$$

其中,  $x, y \in \{0, 1, \dots, N-1\}$ 表示的是置乱变换前像素点位置,  $(x', y')$ 表示的是变换后的位置,  $\text{mod}$ 表示模运算,  $N$ 表示正方形图像的边长。Arnold变换多项式公式为

$$\left. \begin{aligned} x' &= (x + y) \pmod{N} \\ y' &= (x + 2y) \pmod{N} \end{aligned} \right\} \quad (10)$$

### 6.2 DNA加密

首先, 利用ode45算法计算混沌系统的初始值并迭代混沌系统, 去除前1500项获得更好的随机性, 得到3个混沌序列 $\{x_i, y_i, z_i\}$ , 其中将 $\{z_i\}$ 混沌序列转化为0~255之间的整数, 然后将其转换为与预处理之后的大小一致的矩阵 $\mathbf{R}$ , 接下来利用大小为 $t \times t$ 的方阵分别对混沌矩阵和置乱矩阵进行均匀分块, 得到的总块数为 $(M/t + N/t) \times 3$ 。设 $I(x, y)$

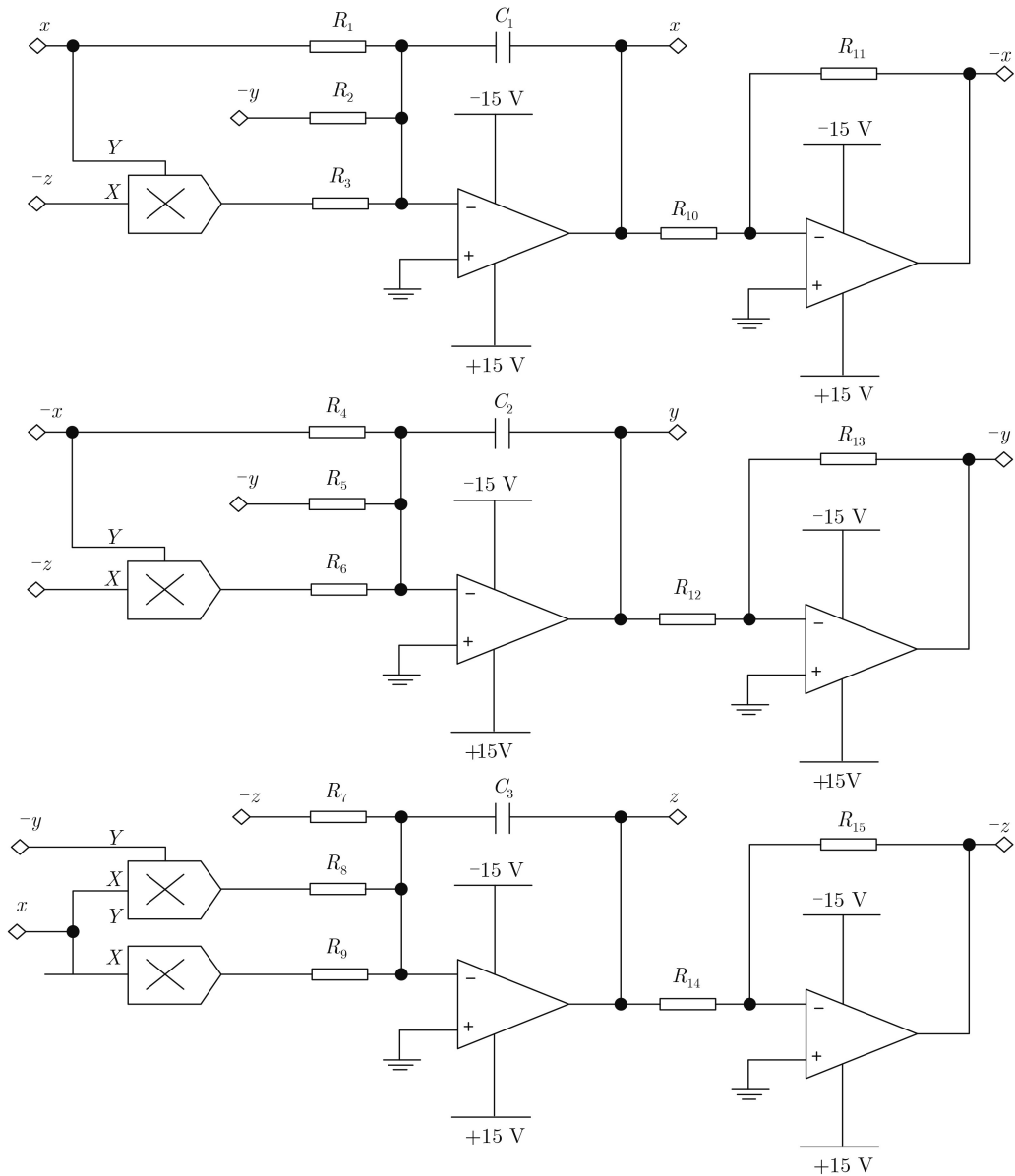
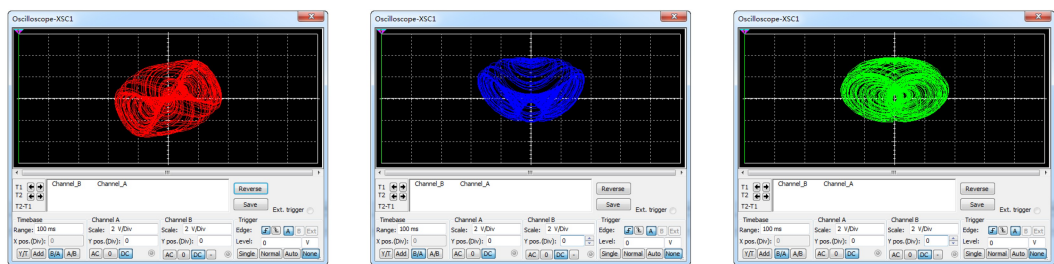


图6 电路原理图



(a)  $x-y$ 平面

(b)  $x-y$ 平面

(c)  $y-z$ 平面

图7 电路实验吸引子相图

为图像在 $(x, y)$ 处的灰度值，将 $I$ 相邻的比特面两两合并得到 $I_1 = \{i_1i_2\}$ ,  $I_2 = \{i_3i_4\}$ ,  $I_3 = \{i_5i_6\}$ ,  $I_4 = \{i_7i_8\}$ 作为混沌系统的初值，最后进行DNA编码。实验结果表明，双重加密在很大程度上提高了加密算法的安全性和效率，图9分别是加密前后的Lena

图像，由图可知，加密图像已看不出原始图像所具有的特征，即没有明显的规律性。

### 6.3 相关性分析

数字图像的各相邻像素间在水平、垂直和对角线方向的相关性很大，接近于1。图像加密的目的

就是要破坏相邻像素之间的相关性，所以下面将通过对比加密前后图像的相邻像素的分布图研究加密效果。相关系数为

$$\left. \begin{aligned} E(x) &= \frac{1}{n} \sum_{i=1}^n x_i \\ D(x) &= \frac{1}{n} \sum_{i=1}^n (x_i - E(x))^2 \\ \text{cov}(x, y) &= \frac{1}{n} \sum_{i=1}^n (x_i - E(x))(y_i - E(y)) \\ \tau &= \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \end{aligned} \right\} \quad (11)$$

其中， $x, y$ 分别表示图像中相邻两个像素点的像素值， $n$ 是像素总数， $E(x)$ 和 $D(x)$ 分别表示所对应的像素的灰度值的期望和方差。

选择大小为 $256 \times 256$ 的明文图像和加密后的密文图像，分别在水平、垂直和对角线3个方向上对明文图像和密文图像的相邻像素进行分析，选取水平方向相关性曲线结果如图10所示，明文图像存在明显的相关性，而对应的密文图像则均匀分布，说明该算法破坏了原始图像的相关特征。图11给出了加密后3个方向3个通道的完整相关性曲线图。

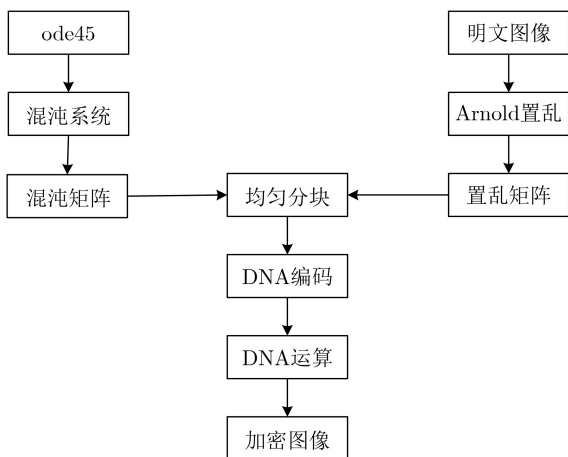


图8 图像加密算法框架图

计算加密前后图像在水平、垂直和对角线3个方向上的相关系数，分别取3个方向上3个通道的平均值，结果见表1。由表可知，明文图像在3个方向上的相关性很强接近于1，而对应的密文图像的像素均匀分布，其相关系数接近于0，与其他加密方法对比后可知，该加密效果非常明显。

### 6.4 灰度直方图

图像的直方图是图像的重要统计特征，图12给出了加密前后图像的直方图，从图中可以看出明文图像的直方图分布不均匀，显示了像素的统计特性；而密文图像的直方图分布较均匀。

### 6.5 信息熵分析

信息熵是衡量信息随机性的度量指标，反映了加密后密文图像的像素值随机分布信息，信息熵为

$$G(s) = - \sum_{i=0}^{2^n-1} p(s_i) \log_2 p(s_i) \quad (12)$$

其中， $p(s_i)$ 表示该像素值在整幅图像中所占的概率， $2^n$ 表示图像中像素值的所有状态。本加密算法中，取3个信道信息熵的平均值，得到的信息熵为7.9995，非常接近理想值8，如表2所示。

## 7 结论

本文设计了一个三涡卷混沌系统，分别分析了三涡卷混沌系统的平衡点性质、Lyapunov指数谱、分岔图、Poincare截面图以及频谱图，充分呈现了系统的混沌特性。然后进行了硬件电路实验，

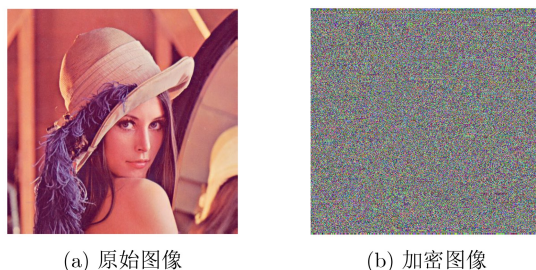


图9 图像加密效果

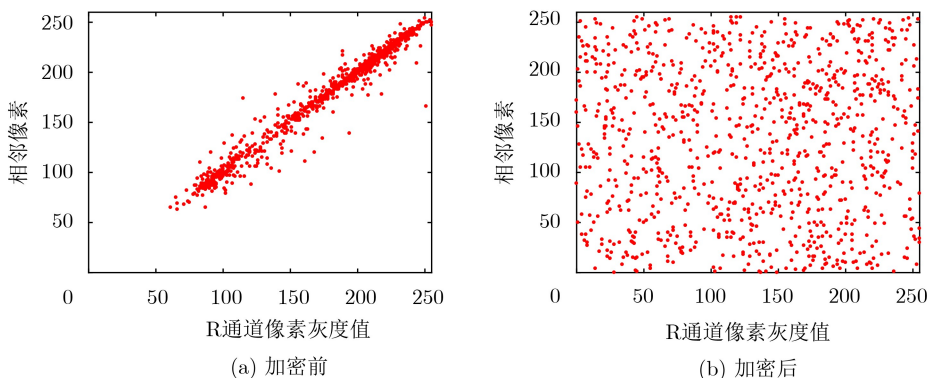


图10 水平方向R通道相邻像素分布

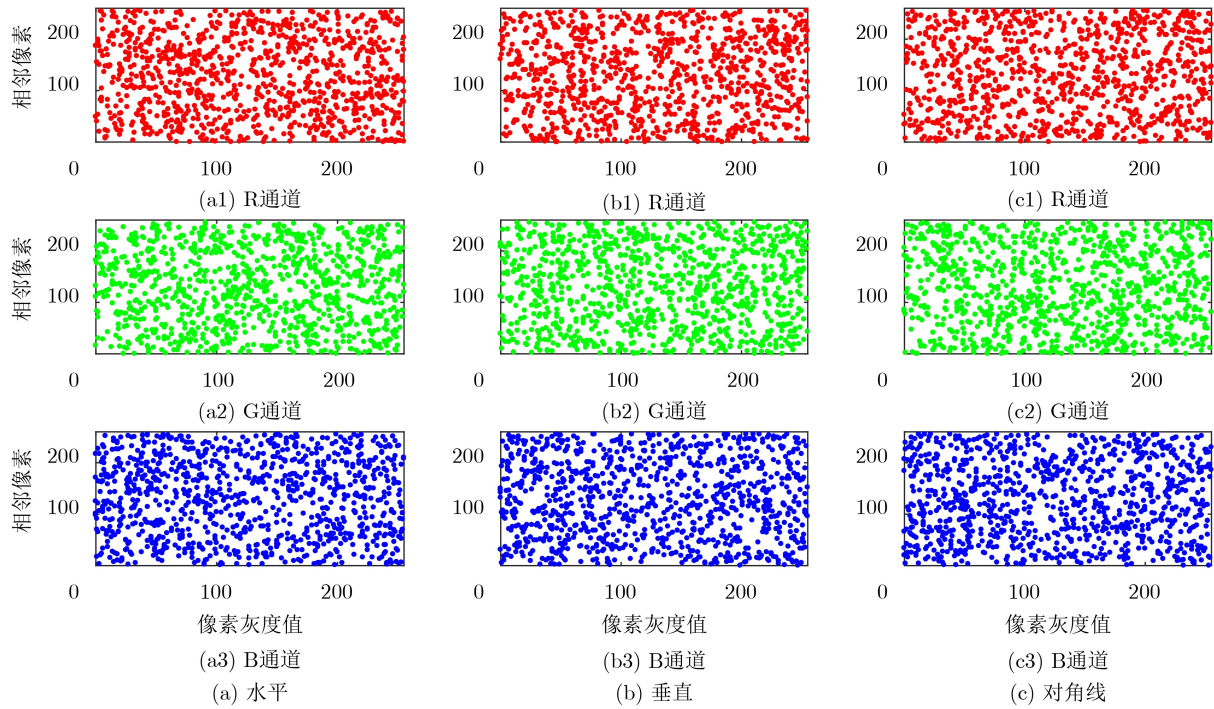
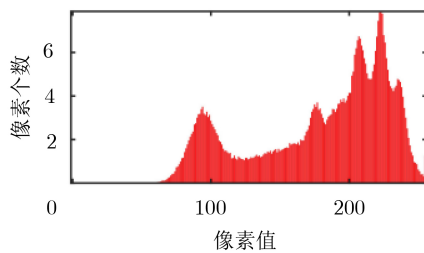


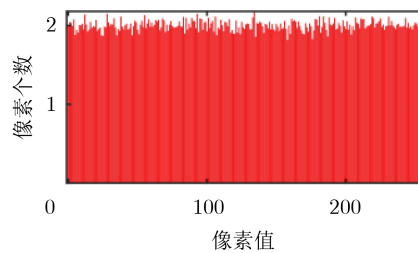
图 11 加密后完整相邻像素分布

表 1 相邻像素在不同方向上的相关系数

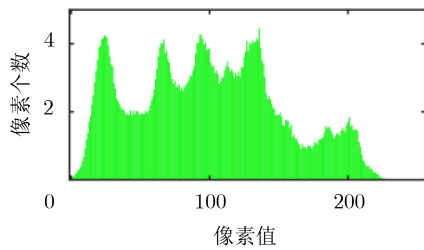
方法	水平相关性	垂直相关性	对角相关性
原始Lena图像	0.9712	0.9782	0.9547
文献[13]	0.0061	0.0153	0.0031
文献[14]	0.0102	0.0214	0.0061
文献[15]	0.0027	0.0152	0.0071
文献[16]	0.0151	0.0011	0.0403
文献[17]	-0.0034	-0.0060	0.0063
文献[18]	0.0029	0.0041	0.0019
本文算法	0.0006	0.0013	-0.0011



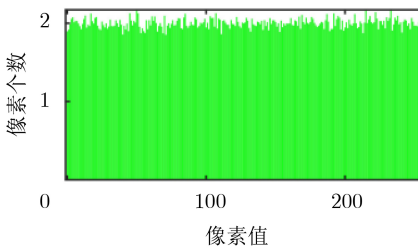
(a1) R通道



(b1) R通道



(a2) G通道



(b2) G通道

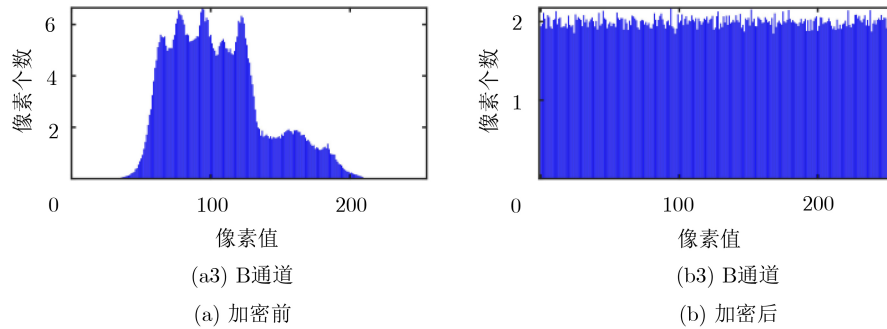


图 12 图像像素分布直方图

表 2 RGB三个通道的信息熵

方法	信息熵
原始Lena图像	6.9951
文献[13]	7.9964
文献[14]	7.9979
文献[18]	7.9983
文献[19]	7.9978
文献[20]	7.9968
本文算法	7.9995

发现电路仿真与数值分析的结果一致，最后将混沌系统与DAN算法相结合设计了图像加密方案，极大地增强了算法的安全性。通过对各性能指标的分析，发现该算法具有较好的加密效果和潜在的应用价值，可广泛应用于保密通信领域。

### 参考文献

- [1] MOOTHATHU T K S. Stronger forms of sensitivity for dynamical systems[J]. *Nonlinearity*, 2007, 20(9): 2115–2126. doi: [10.1088/0951-7715/20/9/006](https://doi.org/10.1088/0951-7715/20/9/006).
- [2] 李志军, 曾以成. 基于文氏振荡器的忆阻混沌电路[J]. *电子与信息学报*, 2014, 36(1): 88–93. doi: [10.3724/SP.J.1146.2013.00332](https://doi.org/10.3724/SP.J.1146.2013.00332).  
LI Zhijun and ZENG Yicheng. A memristor chaotic circuit based on Wien-bridge oscillator[J]. *Journal of Electronics & Information Technology*, 2014, 36(1): 88–93. doi: [10.3724/SP.J.1146.2013.00332](https://doi.org/10.3724/SP.J.1146.2013.00332).
- [3] LÜ Jinhua and CHEN Guanrong. A new chaotic attractor coined[J]. *International Journal of Bifurcation and Chaos*, 2002, 12(3): 659–661. doi: [10.1142/S0218127402004620](https://doi.org/10.1142/S0218127402004620).
- [4] BANERJEE T, BISWAS D, and SARKAR B C. Design and analysis of a first order time-delayed chaotic system[J]. *Nonlinear Dynamics*, 2012, 70(1): 721–734. doi: [10.1007/s11071-012-0490-3](https://doi.org/10.1007/s11071-012-0490-3).
- [5] VAIDYANATHAN S. A new six-term 3-d chaotic system with an exponential nonlinearity[J]. *Far East Journal of Mathematical Sciences*, 2013, 79(1): 135–145.
- [6] 张平伟, 唐国宁, 罗晓曙. 双向耦合混沌系统广义同步[J]. *物理学报*, 2005, 54(8): 3497–3501. doi: [10.3321/j.issn:1000-3290.2005.08.005](https://doi.org/10.3321/j.issn:1000-3290.2005.08.005).  
ZHANG Pingwei, TANG Guoning, and LUO Xiaoshu. Generalized synchronization of bidirectionally coupled chaos systems[J]. *Acta Physica Sinica*, 2005, 54(8): 3497–3501. doi: [10.3321/j.issn:1000-3290.2005.08.005](https://doi.org/10.3321/j.issn:1000-3290.2005.08.005).
- [7] 李付鹏, 刘敬彪, 王光义, 等. 基于混沌集的图像加密算法[J]. *电子与信息学报*, 2020, 42(4): 981–987. doi: [10.11999/JEIT190344](https://doi.org/10.11999/JEIT190344).  
LI Fupeng, LIU Jingbiao, WANG Guangyi, et al. An image encryption algorithm based on chaos set[J]. *Journal of Electronics & Information Technology*, 2020, 42(4): 981–987. doi: [10.11999/JEIT190344](https://doi.org/10.11999/JEIT190344).
- [8] LI Chengqing, LIN Dongdong, and LÜ Jinhua. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits[J]. *IEEE MultiMedia*, 2017, 24(3): 64–71. doi: [10.1109/MMUL.2017.3051512](https://doi.org/10.1109/MMUL.2017.3051512).
- [9] VOLOS C K, KYPRIANIDIS I M, and STOUBOULOS I N. Text encryption scheme realized with a chaotic pseudo-random bit generator[J]. *Journal of Engineering Science and Technology Review*, 2013, 6(4): 9–14. doi: [10.25103/jestr.064.02](https://doi.org/10.25103/jestr.064.02).
- [10] YI Shuang and ZHOU Yicong. Binary-block embedding for reversible data hiding in encrypted images[J]. *Signal Processing*, 2017, 133: 40–51. doi: [10.1016/j.sigpro.2016.10.017](https://doi.org/10.1016/j.sigpro.2016.10.017).
- [11] WANG Xingyuan, LIU Lintao, and ZHANG Yingqian. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. *Optics and Lasers in Engineering*, 2015, 66: 10–18. doi: [10.1016/j.optlaseng.2014.08.005](https://doi.org/10.1016/j.optlaseng.2014.08.005).
- [12] 段欢, 郑紫薇. 基于位平面Arnold置乱变换改进算法[J]. *无线通信技术*, 2018, 27(2): 37–42. doi: [10.3969/j.issn.1003-8329.2018.02.008](https://doi.org/10.3969/j.issn.1003-8329.2018.02.008).  
DUAN Huan and ZHENG Ziwei. Improved algorithm of Arnold scrambling transformation based on bit plane[J]. *Wireless Communication Technology*, 2018, 27(2): 37–42. doi: [10.3969/j.issn.1003-8329.2018.02.008](https://doi.org/10.3969/j.issn.1003-8329.2018.02.008).
- [13] KAMELI MOHAMED F. A parallel block-based encryption

- schema for digital images using reversible cellular automata[J]. *Engineering Science & Technology An International Journal*, 2014, 17(2): 85–94. doi: [10.1016/j.jestch.2014.04.001](https://doi.org/10.1016/j.jestch.2014.04.001).
- [14] 李琳, 孔留勇. 一种基于混沌的新型图像加密算法[J]. 系统仿真学报, 2008, 30(3): 954–961. doi: [10.16182/j.issn1004731x.joss.201803023](https://doi.org/10.16182/j.issn1004731x.joss.201803023).
- LI Lin and KONG Liuyong. A new image encryption algorithm based on chaos[J]. *Journal of System Simulation*, 2008, 30(3): 954–961. doi: [10.16182/j.issn1004731x.joss.201803023](https://doi.org/10.16182/j.issn1004731x.joss.201803023).
- [15] 闵富红, 王珠林, 王恩荣, 等. 新型忆阻器混沌电路及其在图像加密中的应用[J]. 电子与信息学报, 2016, 38(10): 2681–2688. doi: [10.11999/JEIT160178](https://doi.org/10.11999/JEIT160178).
- MIN Fuhong, WANG Zhulin, WANG Enrong, *et al.* New memristor chaotic circuit and its application to image encryption[J]. *Journal of Electronics & Information Technology*, 2016, 38(10): 2681–2688. doi: [10.11999/JEIT160178](https://doi.org/10.11999/JEIT160178).
- [16] 屈双惠, 杨志宏, 容旭巍, 等. 一个新忆阻混沌系统及其在图像加密中的应用[J]. 系统仿真学报, 2019, 31(5): 984–991. doi: [10.16182/j.issn1004731x.joss.17-0170](https://doi.org/10.16182/j.issn1004731x.joss.17-0170).
- QU Shuanghui, YANG Zhihong, RONG Xuwei, *et al.* A new memristor chaotic system and its application in image encryption[J]. *Journal of System Simulation*, 2019, 31(5): 984–991. doi: [10.16182/j.issn1004731x.joss.17-0170](https://doi.org/10.16182/j.issn1004731x.joss.17-0170).
- [17] 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报, 2012, 34(7): 1735–1743. doi: [10.3724/SP.J.1146.2011.01004](https://doi.org/10.3724/SP.J.1146.2011.01004).
- ZHU Congxu, HU Yuping, and SUN Kehui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern[J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1735–1743. doi: [10.3724/SP.J.1146.2011.01004](https://doi.org/10.3724/SP.J.1146.2011.01004).
- [18] ENAYATIFAR R, ABDULL A H, and ISNIN I F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence[J]. *Optics and Lasers in Engineering*, 2014, 56: 83–93. doi: [10.1016/j.optlaseng.2013.12.003](https://doi.org/10.1016/j.optlaseng.2013.12.003).
- [19] PING Ping, XU Feng, and WANG Zhijian. Image encryption based on non-affine and balanced cellular automata[J]. *Signal Processing*, 2014, 105: 419–429. doi: [10.1016/j.sigpro.2014.06.020](https://doi.org/10.1016/j.sigpro.2014.06.020).
- [20] ZHANG Qiang, LIU Lili, and WEI Xiaopeng. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps[J]. *AEU-International Journal of Electronics and Communications*, 2014, 68(3): 186–192. doi: [10.1016/j.aeue.2013.08.007](https://doi.org/10.1016/j.aeue.2013.08.007).
- 摆玉龙: 男, 1973年生, 教授, 博士生导师, 研究方向为控制理论与应用.
- 杨 阳: 女, 1995年生, 硕士生, 研究方向为混沌系统.
- 唐丽红: 女, 1995年生, 硕士生, 研究方向为时间序列与风速预测.
- 责任编辑: 陈 倩