DOI: 10.13382/j.jemi.B2508242

激光混沌系统及抗攻击图像加密算法的协同设计*

杨 阳[1] 摆玉龙[2] 李 艳[1] 张俊芳[1] 万怡华[1]
(1. 宁夏师范大学物理与电子信息工程学院 固原 756000;2. 西北师范大学物理与电子工程学院 兰州 730070)

摘 要:基于经典 Lorenz—Haken 混沌系统构建了一个四维激光混沌系统,并对其非线性动力学特性进行了理论分析与数值验证。通过对 Lyapunov 指数谱、分岔图、Poincaré 截面等多维度分析方法,系统揭示了该混沌系统的平衡点稳定性、非线性演化规律及多稳态共存特性。基于相空间重构与吸引子维度计算,定量表征了系统吸引子的复杂动力学行为,发现其存在双涡卷混沌吸引子的对称现象。为实现理论模型向物理系统的转化,设计并实现了等效模拟电路,实验电路输出信号与数值仿真结果具有高度一致性。在此基础上,提出并设计了一种联合置乱、动态 DNA 编码、逆向级联扩散的三阶段彩色图像加密算法。结果表明,加密图像的信息熵达到 7.999 4,相邻像素相关系数低于 0.003,直方图呈现均匀分布特性,能够抵御裁剪攻击和噪声攻击。理论分析与实验验证表明,该系统在混沌特性与抗攻击能力方面满足信息安全需求,为光通信加密技术提供了新的实现方案。

关键词:四维激光混沌系统;非线性动力学分析;多稳态吸引子;模拟电路实现;抗攻击图像加密
中图分类号:TP309.7;TN918;O415.5 **文献标识码**:A **国家标准学科分类代码**:520.63;120.30

Co-design of laser chaotic system and anti-attack image encryption algorithm

Yang Yang[1] Bai Yulong[2] Li Yan[1] Zhang Junfang[1] Wan Yihua[1]
(1. School of Physics and Electronic Information Engineering, Ningxia Normal University, Guyuan 756000, China;
2. College of Physics and Electronic Engineering, Northwest Normal University, Lanzhou 730070, China)

Abstract: Based on the classical Lorenz-Haken chaotic system, a four-dimensional laser chaotic system is constructed, and its nonlinear dynamical characteristics are theoretically analyzed and numerically verified. Through multi-dimensional analytical methods, including Lyapunov exponent spectra, bifurcation diagrams, and Poincaré sections, the equilibrium point stability, nonlinear evolution mechanisms, and multi-stability coexistence characteristics of the chaotic system are systematically revealed. Based on phase space reconstruction and attractor dimension calculations, the complex dynamical behaviors of the system's attractor are quantitatively characterized, revealing the symmetric dual-vortex chaotic attractor. To bridge the theoretical model with physical implementation, an equivalent analog circuit is designed and experimentally validated, demonstrating high consistency between the circuit output signals and numerical simulation results. Building on this foundation, a three-stage color image encryption algorithm combining position scrambling, dynamic DNA encoding, and reverse cascaded diffusion is proposed. The results show that the encrypted image achieves an information entropy of 7.999 4, adjacent pixel correlation coefficients below 0.003, and a uniform histogram distribution, demonstrating strong resistance to cropping and noise attacks. Theoretical analysis and experimental verification confirm that the system meets the requirements for information security in terms of chaotic characteristics and anti-attack capabilities, providing a new implementation scheme for optical communication encryption technologies.

Keywords: four-dimensional laser chaotic system; nonlinear dynamics analysis; multistable attractors; analog circuit implementation; anti-attack image encryption

收稿日期: 2025-03-19 Received Date: 2025-03-19
*基金项目:2025 年自治区重点研发计划引才专项(2025BEH04102)项目资助

0　引　言

混沌作为非线性动力学研究的核心领域，其初值敏感性与伪随机特性为信息安全领域提供了重要理论基础[1-4]。自 Lorenz 揭示首个确定性混沌系统以来[5]，混沌系统的维度拓展与工程应用持续推动着非线性科学的发展。当前研究主要聚焦于系统维度与结构创新领域，Liu 等[6]通过符号函数构建三维切换多翼吸引子系统，显著提升了系统的视觉复杂度。然而，这类基于数学构造的系统物理可解释性较弱，硬件实现难度较大。Zhang 等[7]提出无平衡点、多翼隐藏吸引子共存的四维混沌系统，但多稳态演化机制未明确量化。周双等设计的 n 维离散超混沌系统，优势在于实现任意维度扩展，同时也增加了硬件实现的复杂度[8]。物理实现方法探索领域，刘思聪等[9]采用指数-余弦离散映射，其算法效率高适合数字实现，局限在于物理随机性来源受限。王诗楠等[10]开发现场可编程门阵列(FPGA)随机实时建模，验证了电力电子混沌硬件的可行性，但未解决高维系统实现问题。解旭辉等[11]设计模数混合混沌 TRNG，成功融合物理熵源与数字控制，为电路实现提供了参考。安全应用拓展领域，摆玉龙等[12]将多涡卷系统用于图像加密，提升置乱复杂度，但单一置乱存在被统计攻击破解的问题。Dong 等[13]提出 DNA 像素值伪随机替换，优势在于增强扩散效果，但静态编码规则降低非线性强度。何纪辉等[14]开发双混沌动态 DNA 编码，创新性的引入规则动态变化，挑战在于解决多阶段操作级联脆弱性。分别在图像加密[15]、同步控制[16]等领域形成系列成果。值得注意的是，在激光混沌研究领域，Haken[17]于 1975 年首次建立激光混沌模型，开辟了光物理与非线性科学的交叉研究方向。相较于传统电子混沌[18]，激光混沌系统因其物理可解释性强、硬件易实现等优势[19]，在高速密钥分发[20]等方面展现出独特价值。最新进展包括，Atsushi 团队[21]实现基于激光混沌的 Gb/s 级安全通信，证明了激光混沌系统的高速适用性。Yang 等[22]构建四维激光混沌系统并深入分析了其密码学特性，标志着激光混沌系统向更高维度和更深层次安全应用迈出了重要一步。然而，现有研究仍存在如下 3 方面局限：系统维度多局限于三维，制约复杂动力学特性的开发；吸引子共存机制与多稳态演化规律尚未明晰；加密算法普遍采用单一置乱策略，难以抵御联合攻击。

针对上述挑战，本文提出一种基于四维激光混沌系统的抗攻击图像加密新方法。核心研究思路与技术要素在于建立具有双参数调制机制的四维激光混沌模型，显著提升系统维度并产生丰富的多涡卷吸引子。通过 Lyapunov 指数谱与分岔分析揭示其多稳态演化机制；设计多涡卷吸引子的模拟电路实现方案，完成理论模型向物理系统的有效映射；构建联合置乱、动态 DNA 编码、逆向级联扩散三阶段加密架构，显著提升算法抵御复杂联合攻击的能力，突破安全瓶颈。

1　四维激光混沌系统

1.1　激光混沌系统

Haken 在非线性光学领域取得突破性进展，其通过严格理论推导证实，单模激光器的 Maxwell-Bloch 方程在特定参数域内可退化为类 Lorenz 系统，由此奠定激光混沌的理论基础。该发现建立了光物理系统与经典混沌理论的内在关联，其规范化动力学方程表述为：

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = rx - y - xz \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

1.2　四维激光混沌系统

基于 Lorenz-Haken 激光动力学方程，通过引入线性耦合项与参数调制机制，构建具有双曲平衡点的四维混沌系统，其非线性微分方程组表述为：

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -by + xz - zw \\ \dot{z} = c - xy \\ \dot{w} = dyw \end{cases} \tag{2}$$

式中：x、y、z、w 是系统变量；a、b、c、d 是系统参数。当选取系统参数 $a = 5, b = 0.5, c = 20, d = -0.4$，并给定初始条件(1,2,3,4)时，相空间轨迹呈现典型的双涡卷混沌吸引子特征，如图 1 所示。

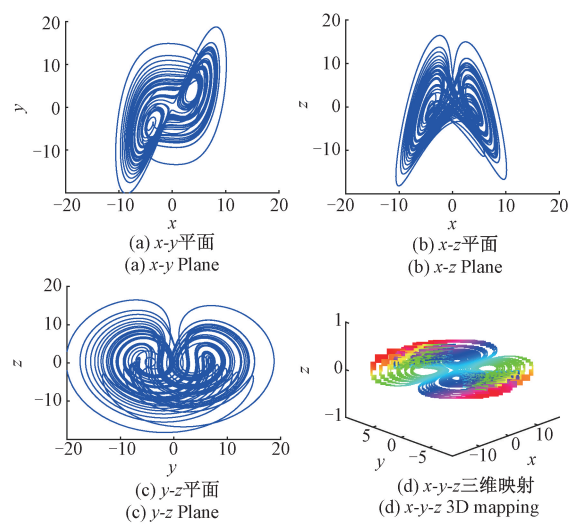


图 1　混沌吸引子相图

Fig. 1　Chaotic attractors phase diagram

2　动力学特性分析

2.1　平衡点与稳定性分析

系统的耗散特性可通过相空间散度分析进行量化。根据 Liouville 定理，系统的散度表达式为：

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -(a + b - d) \tag{3}$$

通过计算 $\nabla V = -5.9 < 0$，表明系统具有全局耗散性。此时相空间体积元 $V(t)$ 随时间演化满足指数收缩律 $V(t) = V(0) \cdot e(\nabla V)$，当 $t \to +\infty$ 时，$V(t) \to 0$，系统轨迹将收敛至一个零体积的吸引子集，证实了系统存在混沌吸引子。为分析系统的平衡点特性，令式(2)中 $\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0$，得到不随时间变化的系统动态平衡点 $S_1(-2, -2, 0.5, 0)$、$S_2(2, 2, 0.5, 0)$。为分析平衡点的稳定性，计算系统在平衡点处的雅可比矩阵为：

$$\boldsymbol{J} = \begin{bmatrix} -a & a & 0 & 0 \\ z & -b & x-w & -z \\ -y & -x & 0 & 0 \\ 0 & ew & 0 & ey \end{bmatrix} \tag{4}$$

通过求解特征方程 $\det(\boldsymbol{J} - \lambda \boldsymbol{I})$，可获得特征值为 $\lambda_1 = 3.869\ 0$，$\lambda_2 = -7.016\ 9$，$\lambda_3 = -0.500\ 0$，$\lambda_4 = -2.652\ 1$，存在负的特征值，为不稳定的鞍点，满足产生混沌的必要条件。

2.2　参数对系统的影响

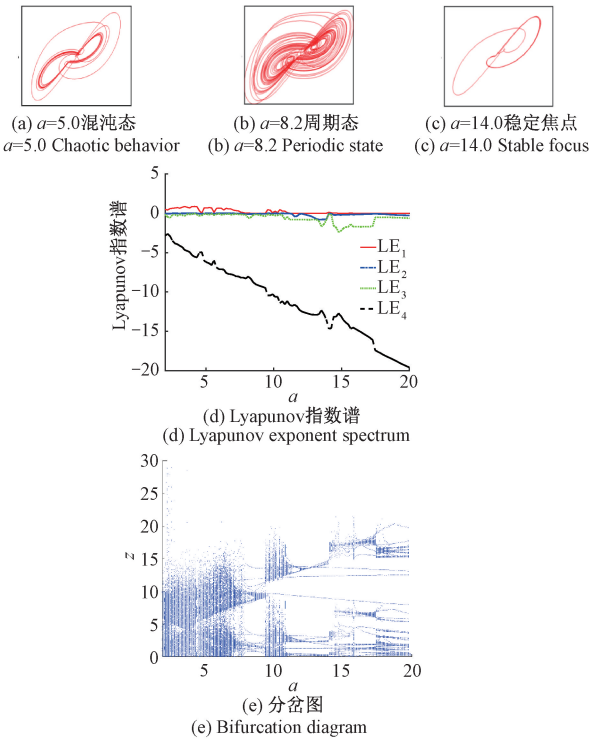
参数的变化直接影响混沌系统的稳定性，同时也会导致吸引子的拓扑结构发生变化。

以参数 a 为例，固定参数 $b = 0.5$，$c = 20$，$d = -0.4$，初始条件为 (1,2,3,4)，通过连续变参数法研究系统演化规律。当 $a = 5.0$ 时，最大 Lyapunov 指数(maximum Lyapunov exponent，MLE)为 0.167 大于 0，相空间轨迹呈现双涡卷混沌吸引子，如图 2(a)、(d)所示。当 $a = 8.2$ 时，$MLE = 0.150$，系统经逆倍周期分岔进入周期态，如图 2(b)所示。当 $a = 14.0$ 时，吸引子退化为稳定焦点，如图 2(c)所示。分岔图定量揭示参数 $a \in [2, 20]$ 区间的周期窗口与混沌带交替现象，如图 2(e)所示，符合 Shilnikov 同宿轨理论预测。

参数 b 的调控效应如图 3 所示。当 $b = 0.50$ 时，系统处于混沌态，$MLE = 1.672$；当 $b = 2.50$ 时，发生 Hopf 分岔进入周期态；当 $b = 1.24$ 时，出现阵发混沌现象。这种参数敏感性为加密系统密钥空间设计提供了理论依据。

2.3　多稳态吸引子共存

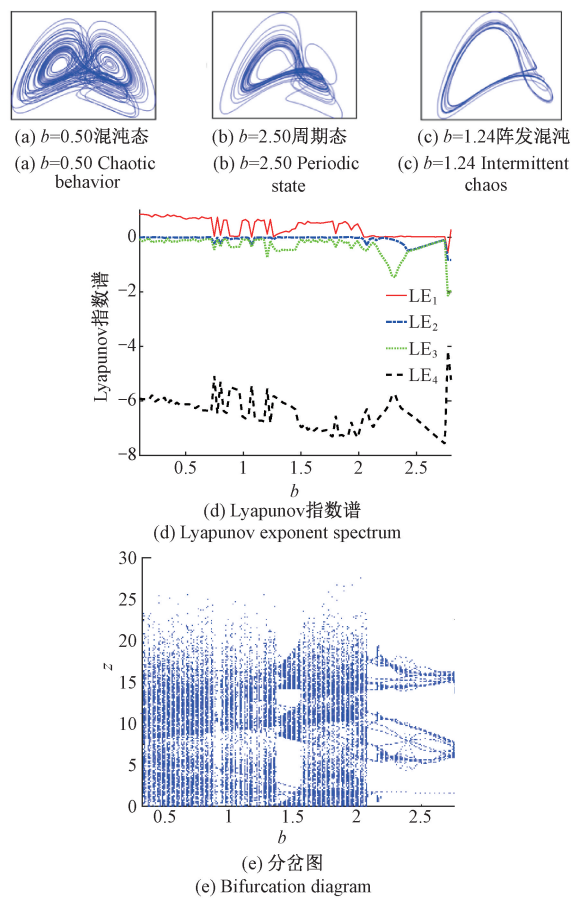
共存吸引子表明在参数固定的情况下，不同初始条件的吸引子运动轨迹所对应的收敛域不同。混沌系统初始状态的微小变化会导致吸引子状态产生巨大差异，从



(a) a=5.0混沌态　(b) a=8.2周期态　(c) a=14.0稳定焦点
(a) a=5.0 Chaotic behavior　(b) a=8.2 Periodic state　(c) a=14.0 Stable focus
(d) Lyapunov指数谱
(d) Lyapunov exponent spectrum
(e) 分岔图
(e) Bifurcation diagram

图 2　参数 a 动力学演化

Fig. 2　Dynamical evolution of parameter a



(a) b=0.50混沌态　(b) b=2.50周期态　(c) b=1.24阵发混沌
(a) b=0.50 Chaotic behavior　(b) b=2.50 Periodic state　(c) b=1.24 Intermittent chaos
(d) Lyapunov指数谱
(d) Lyapunov exponent spectrum
(e) 分岔图
(e) Bifurcation diagram

图 3　参数 b 动力学演化

Fig. 3　Dynamical evolution of parameter b

而增强了系统的随机性和复杂性，这对于加密领域具有积极意义。在固定参数下，选取两组对称初始值(1,2,3,4)和(1,−2,3,−4)，数值仿真获得两类拓扑异构的吸引子。如图 4 所示，蓝色表示初始值(1,2,3,4)生成顺时针旋转的双涡卷吸引子，红色表示初始值(1,−2,3,−4)产生逆时针旋转的折叠吸引子。

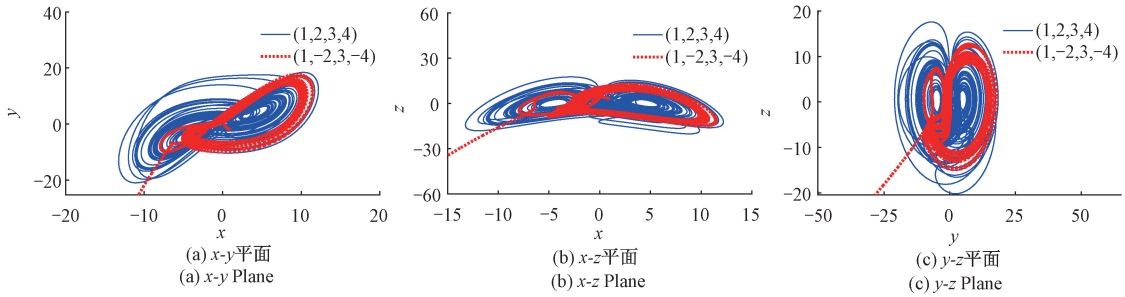


图 4　多稳态吸引子相图

Fig. 4　Phase portrait of multistable attractors

2.4　偏置控制与吸引子迁移

偏置增强是在系统中引入增压控制器，使得吸引子能够在系统空间中移动而不改变系统的初始值。可以在不改变系统初始值的情况下在系统空间中移动，偏置增压可以有效地丰富系统的动态特性。为增强系统可控性，引入偏置控制器 (m,n) 重构动力学方程为：

$$\begin{cases}\dot{x}=a((y+m)-x)\\ \dot{y}=-b(y+m)+x(z+n)-(z+n)w\\ \dot{z}=c-x(y+m)\\ \dot{w}=d(y+m)w\end{cases}\tag{5}$$

理论分析表明，控制器 (m,n) 通过平移平衡点位置实现吸引子迁移。如图 5 所示，当 m 和 n 发生改变时，系统的吸引子沿着 y 轴与 z 轴上下移动。当 $m=30$，$n=30$ 时，吸引子沿着 y 轴和 z 轴的负方向移动；当 $m=-30$，$n=-30$ 时，吸引子沿着 z 轴的正方向移动。迁移过程保持吸引子拓扑结构不变，满足同步控制对参数鲁棒性的要求。

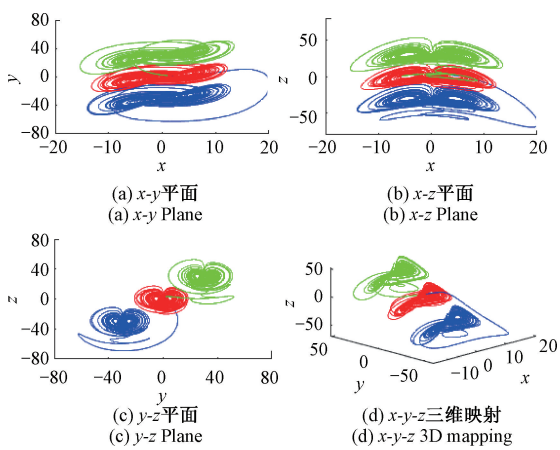


图 5　偏移增量吸引子相图

Fig. 5　Phase portrait of attractors with offset increment

2.5　混沌特性验证

采用 Poincaré 截面与 0−1 测试联合验证混沌特性。Poincaré 截面可以清晰地区分周期性和非周期性。在多维相空间中选择某一截面，如果呈现连续的直线或密集点，则表明系统处于混沌状态。在 $z=0$ 和 $y=0$ 截面观测到非周期点集，分形维数 $D=1.23$，如图 6(a)、图 6(b)所示。0−1 测试通过观察 p 平面上的轨迹来确定状态，轨迹扩散系数 $K=0.98$，满足混沌判据 $K\approx 1$，如图 6(c)所示。功率谱呈现连续宽带特征，衰减指数 $\gamma=-2.1$，如图 6(d)所示。

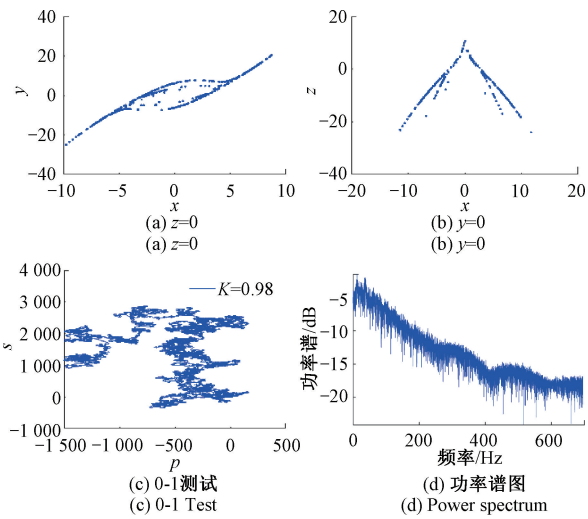


图 6　Poincaré 截面、0−1 测试和功率谱图

Fig. 6　Poincaré section diagram, 0−1 test and power spectrum

2.6　复杂度量化分析

混沌系统的复杂度评估是衡量其密码学适用性的关键指标。采用谱熵(spectral entropy, SE)与组合复杂度(composite complexity, CO)双指标量化体系。复杂度越大，表明混沌序列的随机性和复杂度越高，适用于保密通信。谱熵值越大表示序列的频谱结构越复杂，复杂度

越高。在参数空间 $a \in [0,10]$ 内，进行遍历计算，如图 7(a)、(b)所示。当 $a = 5.0$ 时系统处于混沌状态，此时 $SE = 0.92$，$CO = 0.78$，显著高于 $a = 8.2$ 时，$SE = 0.15$，$CO = 0.03$ 的周期态和 $a = 14.0$，$SE = 0.08$，$CO = 0.01$ 的稳定态。进一步构建复杂度混沌图，通过伪彩色编码揭示参数敏感区，如图 7(c)、(d)所示，深色区域为 $a \in [4.5,6.2]$，对应 $SE > 0.9$ 且 $CO > 0.85$，为最优加密参数域。

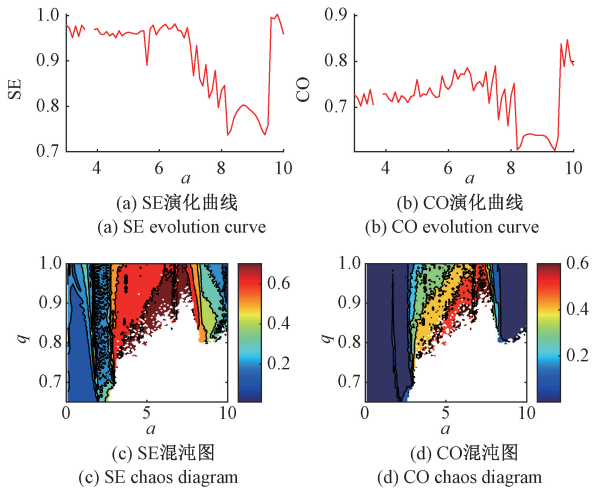


图 7　随 a 变化的 SE 与 CO 复杂度

Fig. 7　SE and CO complexity as functions of parameter a

3　混沌系统的电路设计

利用电路仿真软件 Multisim 对系统进行了电路设计和仿真，电路如图 8 所示，首先将变量比例压缩到原来的 1/10，并进行时间尺度变换。令 $\tau = \tau_0 t$，$\tau_0 = 1\ 000$，得到：

$$\begin{cases} \dfrac{dx}{dt} = 5\ 000y - 5\ 000x \\ \dfrac{dy}{dt} = -500y + 1\ 000xz - 1\ 000zw \\ \dfrac{dz}{dt} = 20\ 000 - 1\ 000xy \\ \dfrac{dw}{dt} = -400yw \end{cases} \tag{6}$$

根据电路原理得到电路方程如下：

$$\begin{cases} \dfrac{dx}{dt} = -\dfrac{1}{R_1C_1}(-y) - \dfrac{1}{R_2C_1}x \\ \dfrac{dy}{dt} = -\dfrac{1}{R_3C_2}y - \dfrac{1}{R_4C_2}(-x)z - \dfrac{1}{R_5C_2}zw \\ \dfrac{dz}{dt} = -\dfrac{1}{R_6C_3}xy \\ \dfrac{dw}{dt} = -\dfrac{1}{R_7C_4}yw \end{cases} \tag{7}$$

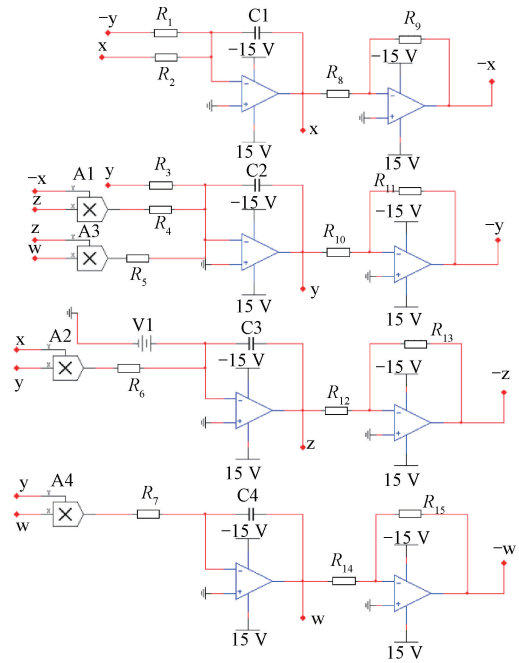


图 8　混沌系统电路原理图

Fig. 8　Schematic diagram of the chaotic system circuit

令 $C_1 = C_2 = C_3 = C_4 = 0.1\ \mu F$，$R_1 = R_2 = 2\ k\Omega$，$R_3 = 20\ k\Omega$，$R_4 = R_5 = R_6 = 10\ k\Omega$，$R_7 = 25\ k\Omega$，其余电阻值为 10 kΩ，图 9 所示为仿真相图，与图 1 中数值仿真结果相吻合，验证了混沌系统的正确性和可行性。

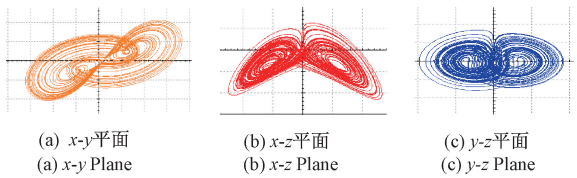


图 9　电路仿真结果

Fig. 9　Circuit simulation results

4　图像加密

4.1　加密算法与步骤

加密算法结合了联合置乱、动态 DNA 编码、逆向级联扩散。扩散的作用是改变像素的值，本文采用的是逆向扩散算法，具体算法原理如下：设 B 为扩散前的图像，C 为扩散后的图像，根据以下公式将 $B(M,j)$ 转换为 $C(M,j)$，$B(i,N)$ 转换为 $C(i,N)$，$B(i,j)$ 转换为 $C(i,j)$。

$$\begin{cases} C(M,N) = (B(M,N) + Y(M,N) + r_1 + r_2) \bmod 256 \\ C(M,j) = (B(M,j) + Y(M,j) + C(M,j+1)) \bmod 256 \\ C(i,N) = (B(i,N) + Y(i,N) + C(i+1,N)) \bmod 256 \\ C(i,j) = (B(i,j) + C(i+1,j) + C(i,j+1) + Y(i,j)) \bmod 256 \end{cases} \tag{8}$$

式中：$j=N-1,N-2,\cdots,2,1$；$i=M-1,M-2,\cdots,2,1$。加密过程如图 10 所示。

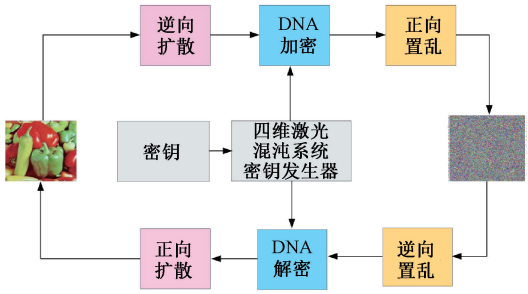


图 10　加密流程图

Fig. 10　Schematic diagram of the Chaotic system circuit

1）设置初始密钥并生成混沌序列。利用 SHA256 函数对明文图像进行计算，得到 32 个十进制数作为初始密钥 $m=\{k_1,k_2,\cdots,k_{32}\}$。根据式(2)计算混沌系统的初始值 x_0,y_0,z_0,w_0 并进行迭代计算，去除前 2 000 项，得到长度为 MN 的混沌序列。

2）对混沌序列进行逆向扩散。$\{X,Y,Z,W\}$ 为扩散前的序列，$\{X',Y',Z',W'\}$ 为扩散后的序列，通过式(9)进行逆向扩散。

$$\begin{cases} X'=X'_{i+1}\oplus X\oplus(X'_{i+1}\oplus X'\oplus X) \\ Y'=Y'_{i+1}\oplus Y\oplus(Y'_{i+1}\oplus Y'\oplus Y) \\ Z'=Z'_{i+1}\oplus Z\oplus(Z'_{i+1}\oplus Z'\oplus Z) \\ W'=W'_{i+1}\oplus W\oplus(W'_{i+1}\oplus W'\oplus W) \end{cases} \tag{9}$$

3）进行 DNA 加密操作。对混沌序列 $\{X',Y',Z',W'\}$ 进行如下处理。其中，序列 W' 用于 DNA 加密操作，$\{X',Y',Z'\}$ 表示 DNA 的 3 种操作，加、减和异或，表达式如下：

$$\begin{cases} X''=\ \mathrm{mod}(floor((60+a\sin(X'))/\pi)\times 65\,536),256) \\ Y''=\ \mathrm{mod}(floor((60+a\sin(Y'))/\pi)\times 65\,536),256) \\ Z''=\ \mathrm{mod}(floor((60+a\sin(Z'))/\pi)\times 65\,536),256) \\ W''=\ \mathrm{mod}(floor((60+a\sin(W'))/\pi)\times 65\,536),3)+1 \end{cases} \tag{10}$$

4）将 W''转换为二进制矩阵 $\boldsymbol{M}$，Y''转换为二进制矩阵 $\boldsymbol{N}$，将 $\boldsymbol{M}$ 与 $\boldsymbol{N}$ 进行异或运算，得到矩阵 $\boldsymbol{P}$。

5）使用序列 $\boldsymbol{P}$ 对整个图像进行无重复的置乱操作，得到加密图像。置乱算法的本质是在不改变像素值的情况下改变像素的位置。对于加密算法，其反向过程即为解密算法。

4.2　加密性能与安全性分析

以标准 Peppers 彩色测试图像为加密对象，通过三通道联合加密实现信息混淆。密文图像呈现视觉白噪声特性，其 RGB 直方图均匀分布，与明文图像的显著聚集特性形成鲜明对比，满足 Kerckhoffs 准则的统计隐蔽性要求，加密后的图像和直方图如图 11 所示。

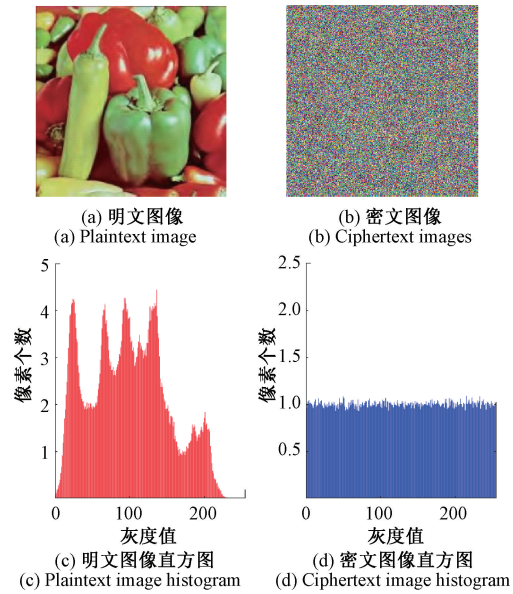


图 11　加密效果与直方图

Fig. 11　Encryption effect and histogram

定义相关系数为：

$$\begin{cases} E(u)=\dfrac{1}{N}\sum_{i=1}^{N}(u_i) \\ D(u)=\dfrac{1}{N}\sum_{i=1}^{N}(u_i-E(u))^2 \\ \mathrm{cov}(u,v)=\dfrac{1}{N}\sum_{i=1}^{N}(u_i-E(u))(v_i-E(v)) \\ \gamma=\dfrac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\ \sqrt{D(v)}} \end{cases} \tag{11}$$

式中：u、v 为相邻像素值；$E(u)$、$D(u)$ 表示数学期望和方差。随机选取 10^4 对相邻像素，分析水平、垂直与对角线方向的统计特性。相邻像素相关性如图 12 所示，明文图像相邻像素在 $y=x$ 对角线附近呈强相关性，而密文像素散点呈均匀分布。相邻像素相关性系数比较如表 1 所示，表 1 数据表明，本文算法相关系数绝对值$|\gamma|<0.003$，优于现有方案，且通过 χ^2 拟合优度检验其显著性水平 $\alpha=0.01$，证明其可有效抵御基于统计分析的已知明文攻击。

表 1　相邻像素相关性系数比较

Table 1　Comparison of correlation coefficients of adjacent pixels

方向	明文图像	密文图像	文献[23]	文献[24]
水平	0.964 7	0.002 2	−0.030 4	0.019 7
垂直	0.942 0	−0.002 1	−0.003 0	−0.000 8
对角线	0.917 0	−0.002 8	0.001 8	−0.002 5

信息熵是衡量信息随机性与不确定性的重要指标，

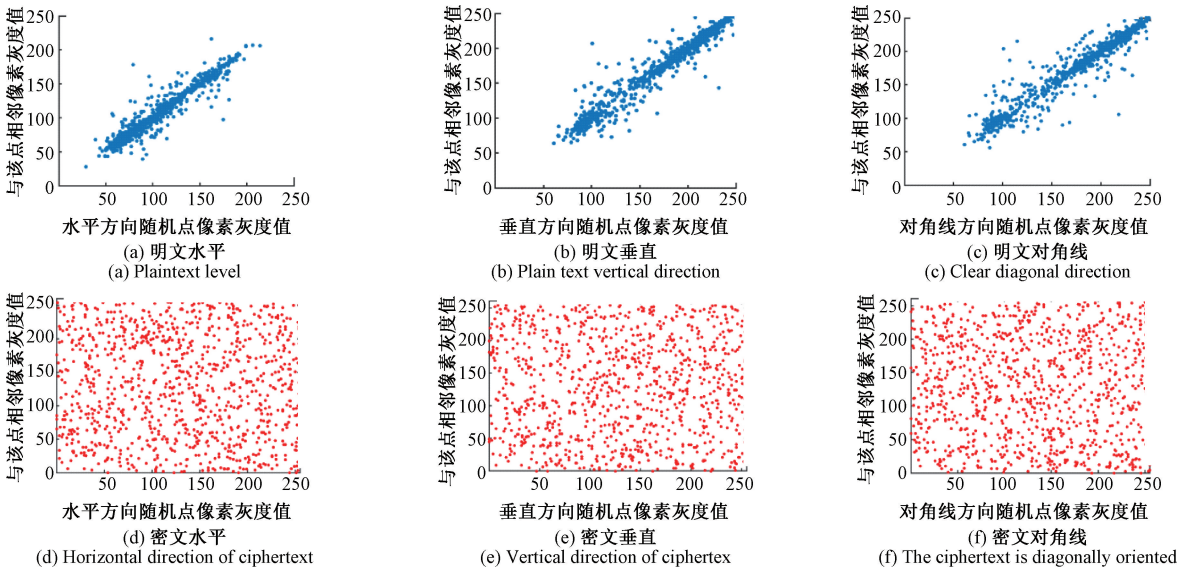


图 12　相邻像素相关性

Fig. 12　Adjacent pixel correlation

其数学定义为：

$$H = -\sum_{i=0}^{2^n-1} p(s_i)\log_2 p(s_i) \tag{12}$$

式中：s_i 是像素值；$p(s_i)$ 是像素值出现的概率。对于具有 256 个状态的标准彩色图像，其理论最大熵值为 8，对应完全均匀的像素分布。本算法对 Peppers 密文图像的 RGB 三通道进行熵值计算，信息熵对比如表 2 所示，结果表明，各通道熵值均达到 $H=7.999\ 4$，与理论最大值的绝对偏差仅为 $\Delta H=0.000\ 6$。通过 χ^2 拟合优度检验其显著性水平 $\alpha=0.05$，表明密文序列满足密码学随机性标准。

表 2　信息熵对比分析

Table 2　Comparative analysis of information entropy

算法	Peppers 密文图像		
	R 通道	G 通道	B 通道
本文	7.999 4	7.999 4	7.999 4
文献[23]	7.999 3	7.997 2	7.996 7
文献[24]	7.999 3	7.996 9	7.996 9
文献[25]	7.999 3	7.999 3	7.999 3

抗攻击鲁棒性分析通过对 Peppers 图像进行噪声和剪切攻击来测试加密算法的性能，这对于衡量加密算法的抗干扰能力非常重要。为评估算法对传输损伤的容错能力，采用峰值信噪比(peak signal to noise ratio，PSNR)与结构相似性指数(structural similarity index，SSIM)定量评估解密质量。抗攻击性能对比如表 3 所示，结果表明，在密文中加入密度为 10%的椒盐噪声，解密图像 $PSNR=32.1$ dB，显著优于文献[23]的 28.4 dB，如图 13(b)、(c)所示。加入均值为 0、方差为 0.2 的加性高斯噪声，解密图像 $SSIM=0.974$，较文献[24]提升 12.3%，如图 13(d)、(e)所示。随机裁剪 25%密文数据，采用压缩感知重构算法恢复，解密图像 $SSIM=0.981$，其重建误差 $\varepsilon=(\|I_{orig}-I_{dec}\|_2)/(\|I_{orig}\|_2)=0.037$，结果表明该算法具有较强的抗干扰、抗丢失能力。

表 3　抗攻击性能对比

Table 3　Attack resistance performance comparison

攻击类型	本文算法(PSNR/SSIM)	文献[23]	文献[24]
椒盐噪声(10%)	32.1 dB/0.962	28.4 dB/0.901	30.7 dB/0.943
高斯噪声($\sigma^2=0.2$)	28.7 dB/0.974	25.1 dB/0.892	27.3 dB/0.926
数据丢失(25%)	/0.981	/0.932	/0.967

5　结　论

基于 Lorenz-Haken 激光动力学方程，提出了一种具有双参数调制的新型四维混沌系统，并系统研究了其在信息安全领域的应用。通过平衡点稳定性分析、Lyapunov 指数谱计算、分岔图与 Poincaré 截面等多维度动力学分析，证实系统具有复杂的混沌行为与多稳态特性。系统在不同初始条件下呈现双涡卷与折叠吸引子的共存现象。为验证系统的物理可实现性，构建等效电路，仿真结果与数值分析结果一致。在此基础上，提出了一种融合动态 DNA 编码、联合置乱与逆向级联扩散的三阶段图像加密算法。通过分析加密前后图像的相关系数、直方图和信息熵，可以证明该算法有良好的加密效果，此外，针对剪切攻击和噪声攻击，对解密图像的影响进行了分析，证实了该算法具有较强的鲁棒性，对保密通信奠定了良好的基础。未来的研究计划包括对加密算法进行优化，实现所提出的图像加密系统的硬件实现，以进一步提

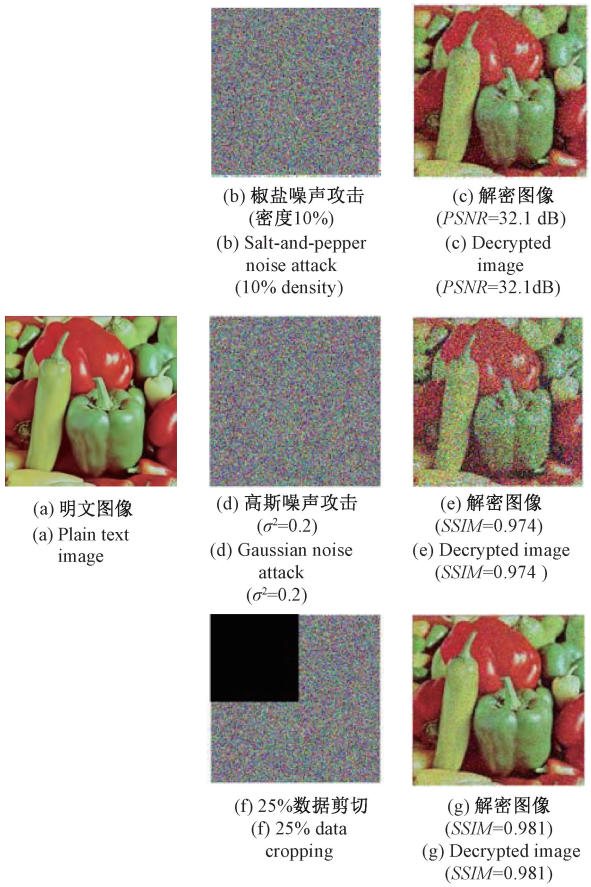


图 13　抗攻击性能分析

Fig. 13　Analysis of attack resistance performance

高加密过程的速度和效率,并增强安全性和抗攻击能力。

参考文献

[1] WANG S M, PENG Q Q, DU B X. Chaotic color image encryption based on 4D chaotic maps and DNA sequence[J]. Optics and Laser Technology, 2022, 148: 107753.

[2] 高志强,陈翰博. 线性化模型下二阶逆变器的混沌控制[J]. 电子测量与仪器学报,2023,37(3):152-160.
GAO ZH Q, CHEN H B. Chaos control of a second-order inverter under linearized model[J]. Journal of Electronic Measurement and Instrumentation, 2023, 37(3): 152-160.

[3] TONG X J, ZHANG M, WANG Z, et al. A fast encryption algorithm of color image based on four-dimensional chaotic system[J]. Journal of Visual Communication and Image Representation, 2015, 33: 219-234.

[4] 马幼捷,王硕,周雪松,等. 基于混沌同步的 Buck 变换器并联均流控制[J]. 电子测量技术,2022,45(5):13-19.
MA Y J, WANG SH, ZHOU X S, et al. Parallel current sharing control for buck converters based on chaotic synchronization[J]. Electronic Measurement Technology, 2022, 45(5): 13-19.

[5] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of The Atmospheric Sciences, 1963, 20(2): 130-141.

[6] LIU J M. A four-wing and double-wing 3D chaotic system based on sign function[J]. Optik, 2014, 125(3): 7089-7095.

[7] ZHANG S, ZENG Y C, LI Z J, et al. Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability[J]. Chaos, 2018, 28(1): 1-9.

[8] 周双,尹彦力,王诗雨,等. n 维离散超混沌系统及其在音频加密中的应用[J]. 物理学报,2024,73(21):41-50.
ZHOU SH, YIN Y L, WANG SH Y, et al. n-Dimensional discrete hyperchaotic system and its application in audio encryption[J]. Acta Physica Sinica, 2024, 73(21): 41-50.

[9] 刘思聪,李春彪,李泳新. 基于指数-余弦离散混沌映射的图像加密算法研究[J]. 电子与信息学报,2022,44(5):1754-1762.
LIU S C, LI CH B, LI Y X. Research on image encryption algorithm based on exponential-cosine discrete chaotic mapping[J]. Journal of Electronics and Information Technology, 2022, 44(5): 1754-1762.

[10] 王诗楠,郭希铮,孙宗辉,等. 基于 FPGA 的电力电子变换器随机实时仿真建模方法[J]. 电力自动化设备,2025,45(2):110-118.
WANG SH N, GUO X ZH, SUN Z H, et al. FPGA-based stochastic real-time simulation modeling method for power electronic converters[J]. Electric Power Automation Equipment, 2025, 45(2): 110-118.

[11] 解旭辉,胡汉平,郑俊,等. 一种面向硬件实现的模数混合混沌真随机数发生器[J]. 密码学报(中英文),2024,11(6):1399-1414.
JIE X H, HU H P, ZHENG J, et al. A mixed analog-digital chaotic true random number generator for hardware implementation[J]. Journal of Cryptologic Research (Chinese & English), 2024, 11(6): 1399-1414.

[12] 摆玉龙,杨阳,唐丽红. 一个新多涡卷混沌系统的设计及在图像加密中的应用[J]. 电子与信息学报,2021,43(2):436-444.
BAI Y L, YANG Y, TANG L H. Design of a new multi-scroll chaotic system and its application in image encryption[J]. Journal of Electronics & Information Technology, 2021, 43(2): 436-444.

[13] DONG W L, LI Q L, TANG Y W, et al. A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme [J]. Optics Communications, 2021, 499: 127211.

[14] 何纪辉,王倩,赵瑛. 基于双混沌系统与 DNA 动态编码的医学图像加密算法[J]. 国外电子测量技术, 2023, 42(8): 124-131.
HE J H, WANG Q, ZHAO Y. Medical image encryption algorithm based on dual chaotic systems and dynamic DNA encoding [J]. Foreign Electronic Measurement Technology, 2023, 42(8): 124-131.

[15] YAN M X, XIE J H. A conservative chaotic system with coexisting chaotic-like attractors and its application in image encryption[J]. Journal of Control and Decision, 2023, 10(2): 237-249.

[16] ZHILENKOV A. Nonsingular integral-type dynamic finite-time synchronization for hyper-chaotic systems[J]. Mathematics, 2021, 10(1): 115.

[17] HAKEN H. Analogy between higher instabilities in fluids and lasers[J]. Physics Letters A, 1975, 53(1): 77-78.

[18] LI C H, LUO G CH, QIN K, et al. An image encryption scheme based on chaotic tent map [J]. Nonlinear Dynamics, 2017, 87(1): 127-133.

[19] WANG J Y, MOU J, XIONG L, et al. Fractional-order design of a novel non-autonomous laser chaotic system with compound nonlinearity and its circuit realization[J]. Chaos, Solitons and Fractals, 2021, 152: 11324.

[20] WU H G, ZHANG Y, BAO H, et al. Initial-offset boosted dynamics in memristor-sine-modulation-based system and its image encryption application[J] AEUE International Journal of Electronics and Communications, 2022, 157: 154440.

[21] YOSHIMURA K, TERAYAMA K, DAVIS P, et al. Secure key distribution using correlated chaos in lasers [J]. Physical Review Letters, 2012, 108(7): 070602.

[22] YANG F F, MOU J, MA C G, et al. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application[J]. Optics and Lasers in Engineering, 2020, 129: 106031.

[23] 方鹏飞,黄陆光,娄苗苗,等. 基于四维超混沌系统的彩色图像加密算法[J]. 计算机工程与设计, 2022, 43(2): 361-369.
FANG P F, HUANG L G, LOU M M, et al. Color image encryption algorithm based on four-dimensional hyperchaotic system [J]. Computer Engineering and Design, 2022, 43(2): 361-369.

[24] 肖嵩,陈哲,杨亚涛,等. 基于混沌理论与 DNA 动态编码的卫星图像加密算法[J]. 电子与信息学报, 2024, 46(3): 1128-1137.
XIAO S, CHEN ZH, YANG Y T, et al. Satellite image encryption algorithm based on Chaos theory and DNA dynamic coding [J]. Journal of Electronics and Information Technology, 2024, 46(3): 1128-1137.

[25] 闫少辉,顾斌贤,宋震龙,等. 基于一种四维忆阻超混沌系统的图像加密算法[J]. 复杂系统与复杂性科学, 2023, 20(2): 43-51.
YAN SH H, GU B X, SONG ZH L, et al. Image encryption algorithm based on a four-dimensional memristor hyperchaotic system[J]. Complex Systems and Complexity Science, 2023, 20(2): 43-51.

作者简介

杨阳(通信作者),2018 年于济南大学获得学士学位,2021 年于西北师范大学获得硕士学位,现为宁夏师范大学讲师,主要研究方向为非线性系统控制及理论。
E-mail: yangyang@ nxnu. edu. cn

Yang Yang (Corresponding author) received her B. Sc. degree from University of Jinan in 2018, and M. Sc. degree from Northwest Normal University in 2021. She is currently a lecturer at Ningxia Normal University. Her main research interests include nonlinear systems control and theory.