

基于忆阻器的 Lorenz 混沌系统的图像加密应用及其 电路实现*

全鹏程²⁾, 余志强^{1), 2), 3)†}

1) (计算机与信息技术学院, 呼和浩特民族学院, 呼和浩特 010051, 中国)

2) (电子工程学院, 广西科技大学, 柳州 545006, 中国)

3) (武汉光电国家研究中心, 光学与电子信息学院, 华中科技大学, 武汉 430074, 中国)

摘要: 信息技术的快速发展使得通信安全面临前所未有的挑战。传统的加密方法主要依赖于数学算法的计算复杂性, 但随着量子计算等新兴技术的出现, 这些加密体系正面临被破解的风险。在此背景下, 基于物理层安全的加密技术成为了通信安全领域的重要研究方向, 其中混沌加密技术以其独特的动力学特性展现出显著优势。为应对传统加密技术面临的量子计算等新兴威胁, 本文探索基于物理层安全的新路径, 旨在设计并验证一种基于 Lorenz 混沌系统的高强度图像加密方案。研究通过构建“动力学置乱-扩散”双阶段加密架构, 利用 Lorenz 系统的初值敏感性与遍历性分别驱动像素的位置混淆与数值变换, 并采用 NPCR、UACI、统计分布及相关性等多维度指标进行量化安全评估。实验结果表明, 加密图像的视觉信息被完全隐藏, 其 RGB 三通道 NPCR 均值达 99.6145%, UACI 均值为 33.4910%, 相邻像素相关系数低于 0.004, 且直方图均匀化, 各项指标均逼近理论最优值。结论表明, 本方案不仅实现了高效的图像加密, 更验证了利用确定性混沌系统的内在物理复杂性替代传统计算复杂性作为安全性基石这一新范式的可行性, 为开发抗量子、低功耗的物理层安全加密技术提供了实验与理论参考。

关键词: 忆阻器, Lorenz 混沌系统, 图像加密, 电路实现

PACS: 05.45.Ac, 05.45.Gg, 05.45.Pq

* 国家自然科学基金(批准号: 22269002)、内蒙古自治区研究生教育教学改革项目(批准号: JGYB2026)、内蒙古自治区直属高校基本科研业务费项目(批准号: HM2026)和呼和浩特民族学院科研创新团队项目(批准号: HM-TD-202514)资助的课题。

† 通信作者. E-mail: zhiqiangyu@alumni.hust.edu.cn

1 引言

在当今数字化社会中，通信安全已成为国家安全、商业机密与个人隐私的基石。随着量子计算、高性能计算等技术的迅猛发展，基于计算复杂性的传统加密体系（如 RSA、ECC）正面临日益严峻的潜在威胁。为构建面向未来的安全通信体系，学术界与工业界开始将目光投向物理层安全技术，其核心思想是利用通信信道本身的物理特性（如噪声、衰落、混沌）来实现信息的安全传输，而非完全依赖于数学算法的计算难度。在这一技术范式下，混沌保密通信因其独特的动力学特性，成为了物理层安全领域最具前景的研究方向之一。

混沌系统固有的初值敏感性、类噪声宽带频谱以及确定性随机性，使其天然适合应用于加密领域。自 Pecora L M 和 Carroll T L 于 1990 年首次实现混沌同步以来，基于混沌的保密通信研究便蓬勃开展^[1]。早期研究主要集中在理论分析与计算机仿真阶段，如 Kocarev L J 等人于 1992 年提出的混沌开关调制方案，以及 Dedieu H 等人于 1993 年实现的混沌键控实验^[2, 3]。进入 21 世纪，随着微电子技术的进步，混沌电路的硬件实现成为研究热点。近年来，国内外学者在高阶混沌系统设计、同步稳定性优化及抗攻击能力提升等方面取得了系列重要进展。

Suykens J A K 和 Vandewalle J 在 *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 上首次通过数学方法系统地构造出多涡卷混沌吸引子，奠定了该领域的基础^[4]；国内学者胡汉平等在《物理学报》上报道的基于自适应控制的混沌同步方案，有效提升了在参数失配条件下的同步鲁棒性^[5]；而 Anwar T 基于正弦离散忆阻器，将 Sine 映射与 2D Logistic-Gaussian 超混沌（LGH）映射融合，构建了一个新的四维（4D）忆阻超混沌离散映射^[6]，并首次将非结合代数结构与混沌序列结合用于彩色图像加密，开辟了代数混沌序列与忆阻超混沌系统融合^[7, 8]的新路径。

尽管混沌保密通信研究已取得显著进展，但其走向实用化仍面临核心挑战：首先，硬件非理想性与模型失配问题。混沌电路的实际元件参数容差、温度漂移及非线性失真，导致理论模型与物理实现存在偏差，直接影响系统同步精度与通信可靠性^[9]。其次，安全强度与工程复杂度的矛盾。现有方案常在高度安全性与简易可实现性之间难以平衡，或为追求理论安全而设计过于复杂，或为简化实现而削弱安全冗余。最后，实验验证的局限性。多数研究集中于数值仿真与理想环境演示，缺乏在模拟真实通信信道（如多径衰落、噪声干扰）下的系统性实验评估与量化安全分析。

鉴于此，本研究旨在通过“混沌动力学设计-加密算法构建-系统性实验验证”的完整研究闭环，开发并评估一套可实用化的混沌图像加密系统。具体工作包括：

（1）设计基于 Lorenz 系统的混沌熵源生成与增强方案，通过相空间分析与统计测试验证其作为加密密钥流的类随机性、低相关性与高复杂度；（2）构建“置乱-扩散”双阶段图像加密架构，将混沌系统的初值敏感性与遍历性分别映射为像素位置混淆与数值变换，实现高效加密^[10]；（3）搭建完整的软硬件实验验证平台，在静态图像与模拟噪声环境下，系统测试加密方案的视觉安全性、统计安全性（直方图均匀性、相邻像素相关性）及差分安全性（NPCR、UACI）；（4）开展对比分析与鲁棒性讨论，将本方案与典型混沌加密方法进行比较，并基于实验结果指出当前局限与后续硬件实现面临的挑战。

本研究的意义在于，通过从理论分析、算法设计到实验验证的全链条研究，不仅提出了一种性能均衡的混沌图像加密方案，更形成了一套从熵源评估、加密效果量化到安全性全面测试的系统性实验方法。研究成果为混沌加密从理论仿真走向工程应用提供了实证基础，并为物联网、轻量级安全通信等场景中探索物理层安全技术提供了有价值的参考。

2 四维 Lorenz 混沌系统模型

2.1 理论模型

下式是一个基于压控型的忆阻器模型，其核心数学公式如下所示。

$$\begin{cases} W(\varphi) = a + b \cdot \arctan(\varphi) \\ i_M = W(\varphi) \cdot v_M = (a + b \cdot \arctan(\varphi)) \cdot v_M \\ \dot{\varphi} = v_M \end{cases} \quad (1)$$

其中 φ 是忆阻器的内部状态变量，即磁通量； v_M 是施加在忆阻器两端的电压； i_M 是流过忆阻器的电流； a 和 b 是控制忆阻器特性的常数。

Lorenz 混沌系统是一种非线性动力系统，最初由爱德华·洛伦兹（Edward Lorenz）于 1963 年引入，它的简单方程组引发了混沌理论的开创性研究。该系统是混沌现象的典型范例，展示了复杂、不可预测的行为，即使在简单的数学方程下也可以观察到这种行为。

Lorenz 混沌系统由三个耦合的一阶常微分方程组组成，这三个方程描述了三个状态变量（或者说是维度）之间的关系。这些状态变量表示系统在空间中的位置，从而形成一个三维相空间，该相空间中的轨迹表现出异常的复杂性和混沌特性。Lorenz 方程组描述如下：

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad (2)$$

其中 $\dot{x}$ 表示对流速率，与流体环流的切变相关； $\dot{y}$ 表示水平方向温度差，描述对流过程中水平面上的温度梯度； $\dot{z}$ 表示垂直方向温度差，描述流体层垂直方向的温度梯度分布；而 σ （普朗特数），与流体的物理属性（如黏性和热扩散率）相关； ρ （瑞利数）与流体上下表面的温差成正比； β （几何因子）与对流区域的尺寸比例（如宽度与高度之比）相关。

将忆阻器(1)引入到 Lorenz 混沌系统(2)中，构建了一个新型忆阻 Lorenz 超混

沌系统^[11]，新系统的状态方程为：

$$\begin{cases} \frac{dx}{dt} = \sigma(y-x) \\ \frac{dy}{dt} = \rho x - y - xz + k \cdot (a + b \cdot \arctan(\varphi)) \cdot x \\ \frac{dz}{dt} = x \cdot y - \beta \cdot z \\ \frac{d\varphi}{dt} = x \end{cases} \quad (3)$$

其中 $\sigma, \rho, \beta, a, b, k$ 是系统参数，当系统参数 $\sigma=8, \rho=20, \beta=8/3, a=0.1, b=1, k=0.8$ ，初始值 $(x_0, y_0, z_0, \varphi_0) = (0.1, 0.1, 0.1, 0)$ 时，系统呈现如图 1 所示的混沌吸引子。对应的李亚普洛夫指数为 $L_1=0.884764, L_2=0.00172038, L_3=0.000636325, L_4=-13.7197$ 。Kaplan Yorke 分数阶维数 $D_L=3.1325$ 。新系统状态方程(3)混沌吸引子如图 1 所示，从图 1(a)和图 1(b)可以看出新系统具有极其丰富的动力学,且吸引子相较于原系统展现出更为复杂的拓扑结构^[12]。同时，如图 1(c)所示，状态变量 φ 的时域波形呈现出明显的非周期振荡特征，进一步从时域演化的角度印证了该系统处于复杂的混沌运行状态。

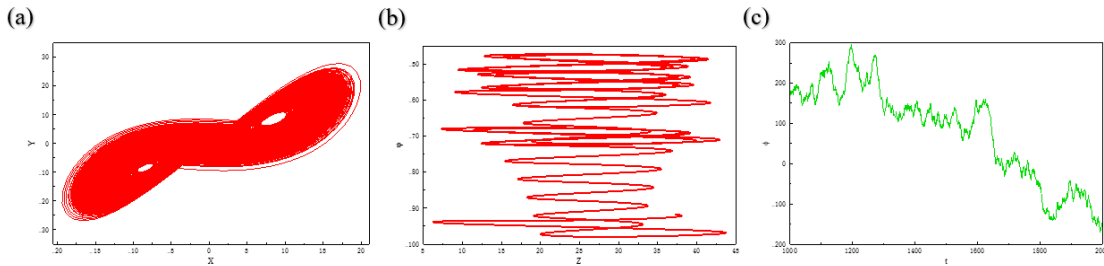


图 1 忆阻 Lorenz 超混沌系统的混沌吸引子相图与时域演化图： (a) $x-y$ 平面相图；(b) $z-\varphi$ 平面相图；(c) 状态变量 φ 的时域波形图

Fig. 1. Phase portraits of the chaotic attractor and time-domain evolution of the memristive Lorenz hyperchaotic system: (a) Phase portrait on the $x-y$ plane; (b) Phase portrait on the $z-\varphi$ plane; (c) Time-domain waveform of state variable φ .

2.2 平衡点稳定分析

由系统数学模型方程右式等于零，可以得到新系统方程(4)为：

$$\begin{cases} \sigma(y-x)=0 \\ \rho x - y - xz + k \cdot (a + b \cdot \arctan(\varphi)) \cdot x = 0 \\ x \cdot y - \beta \cdot z = 0 \\ x = 0 \end{cases} \quad (4)$$

由第 4 个方程显然可知 $x=0$ 。将 $x=0$ 代入第1个方程和第3个方程，可得 $y=0$ 且 $z=0$ （假设系统参数 $\sigma \neq 0$ 且 $\beta \neq 0$ ）。将 $x=y=z=0$ 代入第 2 个方程，等式恒成立，而内部状态变量 φ 可为任意实数常数^[13]。

因此，该忆阻Lorenz超混沌系统不存在孤立的平衡点，而是具有一个沿着 φ 轴连续分布的线平衡点集（Line equilibrium set），可表示为：

$$E = (x, y, z, \varphi) | x=0, y=0, z=0, \varphi=c \quad (5)$$

其中， c 为任意实常数，其值取决于系统的初始状态 φ_0 。

为了分析线平衡点集 E 上的局部稳定性，计算系统在状态空间中的雅可比矩阵（Jacobian matrix）：

$$J = \begin{bmatrix} -\sigma & \sigma & 0 & 0 \\ \rho - z + k \cdot (a + b \cdot \arctan(\varphi)) & -1 & -x & \frac{kbx}{1+\varphi^2} \\ y & x & -\beta & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (6)$$

在任意平衡点 $E_0(0,0,0,c)$ 处对雅可比矩阵进行求值，得到：

$$J(E_0) = \begin{bmatrix} -\sigma & \sigma & 0 & 0 \\ \rho + k \cdot (a + b \cdot \arctan(c)) & -1 & 0 & 0 \\ 0 & 0 & -\beta & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (7)$$

据此推导系统在平衡点处的特征方程(Characteristic equation): $|\lambda I - J(E_0)| = 0$ 。

一个特征值 $\lambda_3 = -\beta$ (稳定)。

$$\begin{vmatrix} \lambda + \sigma & -\sigma & 0 & 0 \\ -(\rho + k \cdot (a + b \cdot \arctan(c))) & \lambda + 1 & 0 & 0 \\ 0 & 0 & \lambda + \beta & 0 \\ -1 & 0 & 0 & \lambda \end{vmatrix} = 0 \quad (8)$$

按第4列展开，可将特征多项式化简为：

$$\lambda(\lambda + \beta)[\lambda^2 + (\sigma + 1)\lambda + \sigma(1 - \rho - k \cdot (a + b \cdot \arctan(c)))] = 0 \quad (9)$$

为了表达简洁，令 $W(c) = \rho + k(a + b \cdot \arctan(c))$ ，则系统在平衡点 E_0 处的四个特征根分别为：

$$\lambda_1 = 0 \quad (10)$$

$$\lambda_2 = -\beta \quad (11)$$

$$\lambda_{3,4} = \frac{-(\sigma + 1) \pm \sqrt{(\sigma + 1)^2 - 4\sigma(1 - W(c))}}{2} \quad (12)$$

由于系统中存在忆阻器的积分项，特征方程始终含有一个零特征值（ $\lambda_1 = 0$ ）。这意味着系统在此线平衡点集上是非双曲的（Non-hyperbolic）。零特征值的存在是忆阻系统产生依赖于初始状态的无穷多吸引子（即极端多稳态现象，Extreme Multistability）的理论根源^[14]。

对于剩余特征值的稳定性分析：

假设系统参数取典型正值（如 $\sigma > 0$ ， $\beta > 0$ ），则 λ_2 恒为负实数。系统的局部稳定性完全取决于共轭特征根 $\lambda_{3,4}$ 。

根据劳斯-赫尔维茨判据（Routh-Hurwitz criterion），二次项多项式 $\lambda^2 + (\sigma + 1)\lambda + \sigma(1 - W(c)) = 0$ 的根具有负实部的充要条件是各项系数大于零。因 $\sigma + 1 > 0$ 恒成立，稳定性临界条件由常数项决定：

（1）稳定鞍结状态：当 $W(c) < 1$ 时，常数项 $\sigma(1 - W(c)) > 0$ 。此时 $\lambda_{3,4}$ 均具有负实部，平衡点在除中心流形外的横截方向上是局部渐近稳定的。

（2）不稳定鞍焦鞍结点（产生混沌的必要条件）：当 $W(c) > 1$ ，即初始参数满足 $\rho + k(a + b \cdot \arctan(c)) > 1$ 时，常数项小于零。此时 $\lambda_{3,4}$ 为一正一负的实根（或具有正实部的复共轭根）。平衡点演变为不稳定的鞍点或鞍焦点（Saddle-focus）。

这种不稳定流形的折叠与拉伸是引导系统轨线不发散且形成混沌吸引子（Chaotic attractor）的核心动力学机制^[15]。

2.3 时域波形图和庞加莱截面图

取参数 $\sigma=10$, $\rho=20$, $\beta=8/3$, $a=0.1$, $b=1$, $k=0.8$, 初始值为 $[0.1, 0.1, 0.1, 0]$, 采用四阶龙格-库塔 (ODE45) 算法对系统求解, 可得系统状态变量 x, y, z, φ 的时域波形如图 2 (a) 所示。从图中可以看出, 各状态变量随时间的演化呈现出连续的、无规则的剧烈振荡, 且无明显的周期性重复, 可以看出该系统为非周期系统。系统在 $z = 27$ 截面上的庞加莱映射如图 2 (b) 所示。该平面截图中存在未形成简单闭合曲线的离散点集, 这些呈现出特定几何与折叠结构的密集点, 进一步表明系统具有复杂的动力学行为。

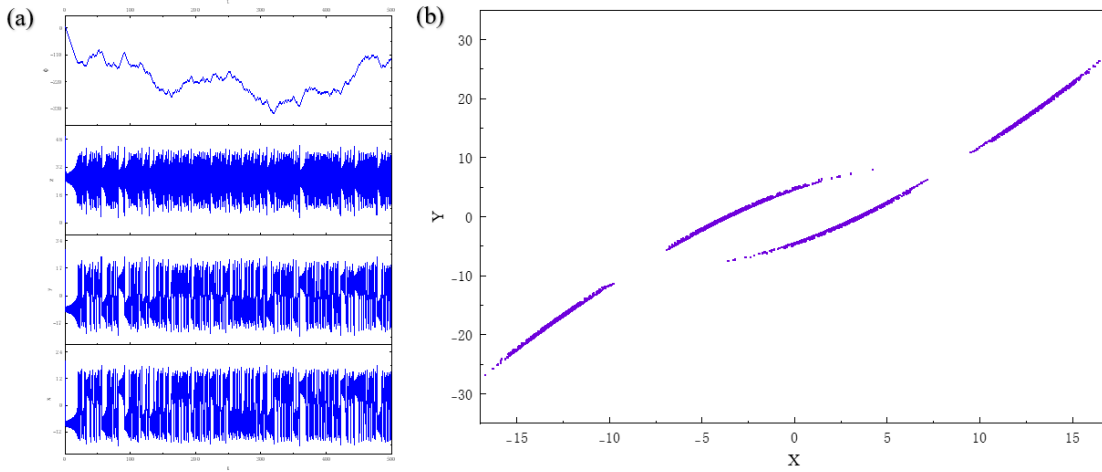


图 2 忆阻 Lorenz 超混沌系统的时域波形与庞加莱截面: (a) 状态变量的时域波形图; (b) $z = 27$ 截面上的庞加莱映射

Fig. 2. Time-domain waveforms and Poincaré section of the memristive Lorenz hyperchaotic system: (a) Time-domain waveforms of state variables; (b) Poincaré map on the $z = 27$ plane.

3 系统动力学分析

3.1 隐藏吸引子特性与内生非对称机制

如 2.2 节的稳定性分析所示，新构建的忆阻 Lorenz 超混沌系统不存在孤立的平衡点，而是拥有沿着 φ 轴连续分布的线平衡点集 E 。由于该系统所产生的混沌吸引子，其吸引域并不与任何不稳定平衡点的流形相交，因此根据非线性动力学理论，该系统生成的吸引子属于典型的隐藏混沌吸引子（Hidden Chaotic Attractor）^[16]。进一步深入剖析系统数学模型可知，与常规的 Lorenz 族系统不同，本系统具有极其独特的内生非对称性（Intrinsic Asymmetry）。

由于忆阻器内部状态反馈项中引入了奇函数 $\arctan(\varphi)$ ，当系统进行坐标变换 $(x, y, z, \varphi) \rightarrow (-x, -y, z, -\varphi)$ 时，系统方程组无法保持形态不变。这意味着，即使在未引入任何外部非对称扰动（即设定参数 $a=0$ ）的基态下，系统在相空间中也无法生成完美的镜像对称轨迹，而是会自发演化出位置、跨度乃至拓扑尺度完全不同的独立混沌吸引子。为了直观揭示这一内生非对称共存现象，本文设定系统基础参数为 $\sigma=8$ ， $\rho=20$ ， $\beta=8/3$ ， $k=0.8$ ， $b=20$ ，并选取两组互为相反数的初始条件 $IC_1=(0.1, 0.1, 0.1, 0)$ 与 $IC_2=(-0.1, -0.1, 0.1, 0)$ 进行数值仿真，所得的三维相空间轨迹及各平面投影如图 3 所示。

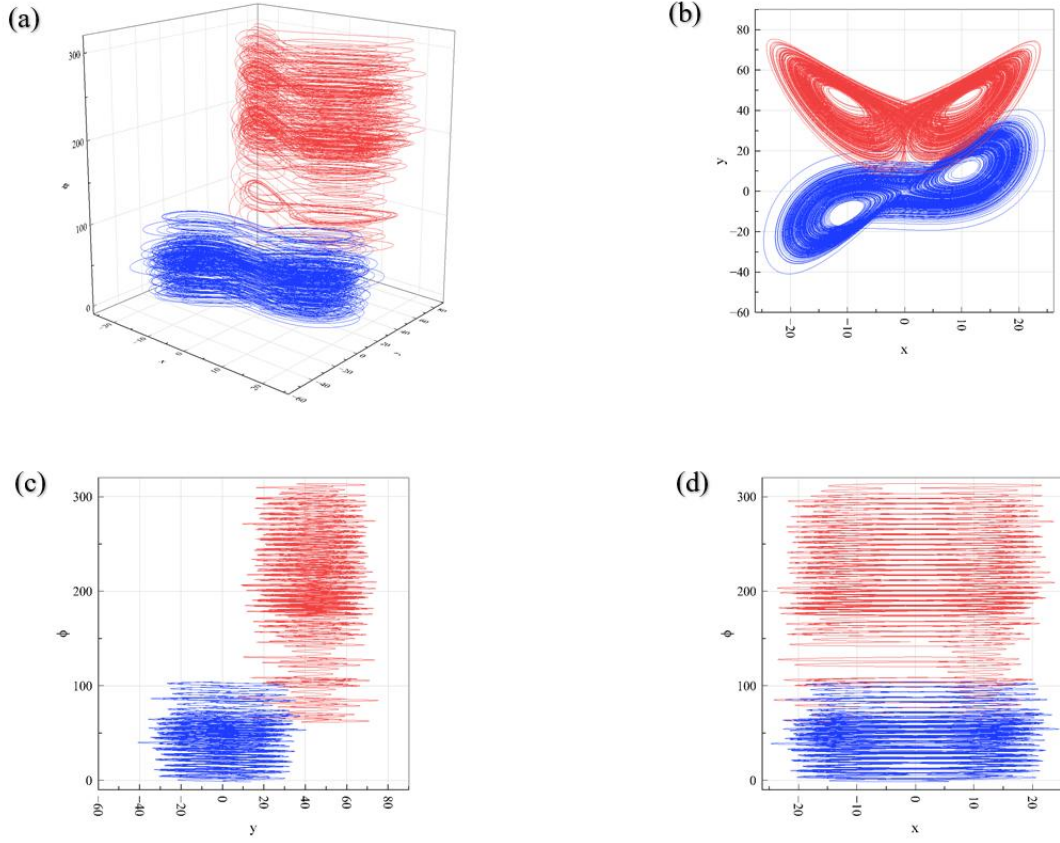


图3 系统在无偏置参数 ($a=0$) 下的内生非对称共存隐藏吸引子: (a) $x-y-\varphi$ 三维相空间轨迹; (b) $x-y$ 平面投影图; (c) $y-\varphi$ 平面投影图; (d) $x-\varphi$ 平面投影图 (蓝色和红色轨迹分别代表由初始条件 IC_1 和 IC_2 演化而来的独立吸引子)

Fig. 3. Phase portraits of the intrinsic asymmetric coexisting hidden attractors for the system without offset parameter ($a=0$): (a) 3D trajectory in $x-y-\varphi$ space; (b) 2D projection on the $x-y$ plane; (c) 2D projection on the $y-\varphi$ plane; (d) 2D projection on the $x-\varphi$ plane (the blue and red trajectories represent the independent attractors evolved from initial conditions IC_1 and IC_2 , respectively).

在此基础上, 本系统巧妙地引入了非零偏置参数 $a = 0.1$ 。该参数的本质并非简单的“对称性破缺开关”, 而是充当了沿线平衡点方向的“全局漂移控制参数 (Global Drift Control Parameter)”。为了直观揭示这一动力学演化过程, 本文选取参数 $\sigma = 8$, $\rho = 20$, $\beta = 8/3$, $k = 0.8$, $a = 0.1$, $b = 20$, 对比了 $a = 0$ 与 $a = 0.1$ 时的 3D 相空间轨迹^[17], 如图 4 所示。

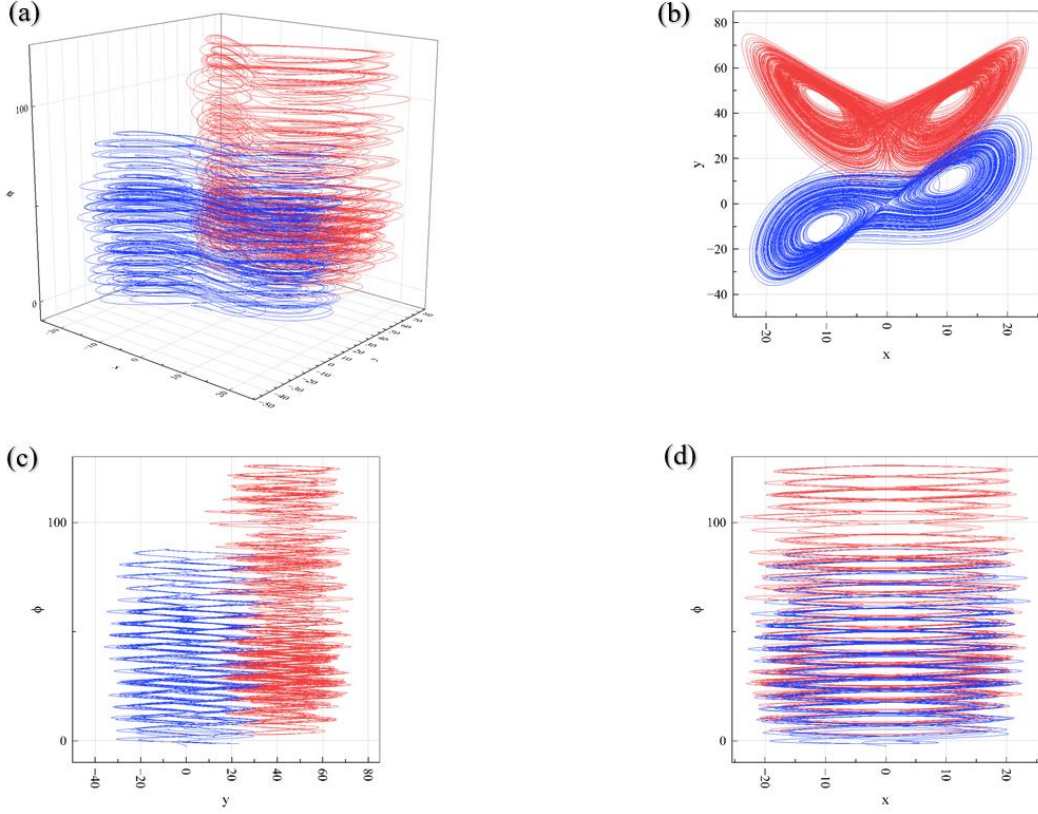


图 4 系统在强偏置参数 ($a=0.1$) 下的空间平移与对角错位共存隐藏吸引子: (a) $x-y-\phi$ 三维相空间轨迹; (b) $x-y$ 平面投影图; (c) $y-\phi$ 平面投影图; (d) $x-\phi$ 平面投影图 (蓝色和红色轨迹分别代表由初始条件 IC_1 和 IC_2 演化而来的独立吸引子)

Fig. 4. Phase portraits of the spatially translated and the diagonally dislocated coexisting hidden attractors for the system with strong offset parameter ($a=0.1$): (a) 3D trajectory in $x-y-\phi$ space; (b) 2D projection on the $x-y$ plane; (c) 2D projection on the $y-\phi$ plane; (d) 2D projection on the $x-\phi$ plane (the blue and red trajectories represent the independent attractors evolved from initial conditions IC_1 and IC_2 , respectively).

3.2 依赖系统参数变化的动力学行为

为了全面揭示由忆阻器内部反馈参数 b 驱动的复杂动力学演化规律, 本节固定系统其他参数为 $\sigma=8$, $\rho=20$, $\beta=8/3$, $a=0.1$, $k=0.8$, 并将初始状态设定为 $(x_0, y_0, z_0, \phi_0) = (0.1, 0.1, 0.1, 0)$ 。为了突出内生非对称性引发的异构演化现象, 本文分别扫描了参数 b 在负半轴区间 $[-100, 0]$ 与正半轴区间 $[0, 100]$ 的相空间轨迹, 其对应的状态变量绝对值 $|y|$ 的分岔图及 Lyapunov 指数 (LE) 谱^[18]分别如图 5(a) 和图 5(b)所示。如图 5 所示, 当参数 b 在负半轴 $[-100, 0]$ 区间内变化时, 系统呈现出周期与混沌状态交替的复杂动力学行为。

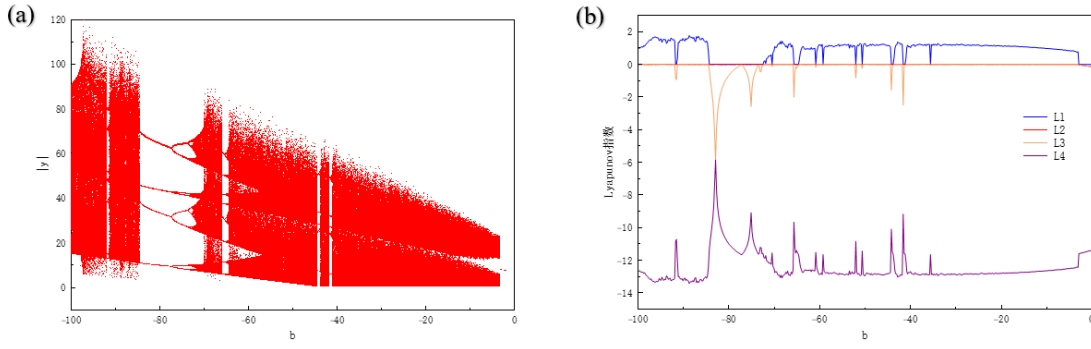


图 5 随参数 b ($b \in [-100,0]$)变化的系统动力学行为: (a) 状态变量 y 的分岔图; (b) Lyapunov 指数谱

Fig. 5. Dynamical behaviors of the system varying with parameter b ($b \in [-100,0]$): (a) Bifurcation diagram of state variable y ; (b) Lyapunov exponent spectrum.

当 $b \in [-100, -85]$ 时, 系统的最大 Lyapunov 指数 $L_1 > 0$, 且 $L_2 = 0$, $L_3 < 0$, $L_4 < 0$, 系统处于连续的混沌状态, 在分岔图上对应着充满大片区域的密集点集(图 5(a))。

在 $b \in [-85, -70]$ 区间内, 系统经历了剧烈的状态演化。在 $b \approx -85$ 附近, 系统发生分岔, L_1 骤降至 0, 系统由混沌状态脱出进入周期状态。随后, 系统经历了复杂的倍周期分岔与逆倍周期分岔过程, 在周期状态与混沌状态之间频繁切换, 特别是在 $b \approx -75$ 附近呈现出明显的低阶周期运动特征^[19]。

当 $b \in [-70, 0]$ 时, 系统再次进入了广阔的混沌区域。在这一区间内, L_1 长期稳定在 1.0~1.5 左右的较高正值水平, 表明系统具有极强的混沌特性。值得注意的是, 在该宽阔的混沌区域带中, 镶嵌着若干大小不一的“周期窗口”(例如在 $b \approx -60, -50, -42$ 附近)。在这些窗口处, 最大 Lyapunov 指数 L_1 会突然下跃至 0 以下(或等于 0), 系统表现出短暂的周期行为, 随后又通过内部危机(Interior Crisis)或切分岔的方式迅速重新步入混沌状态。

与负半轴的经典分岔路径截然不同, 系统在正半轴 $b \in [0, 100]$ 展现出了完全异构的极端动力学演化机制, 如图 6 所示。

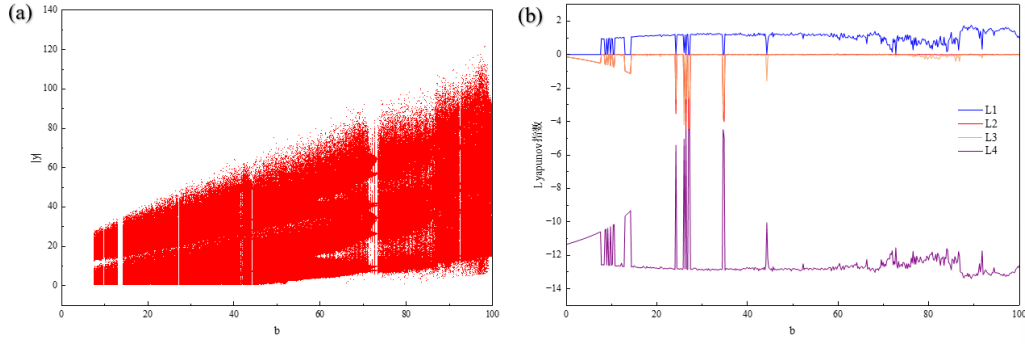


图 6 随系统参数 b ($b \in [0,100]$) 变化的全局动力学行为: (a) 分岔图; (b) Lyapunov 指数谱
Fig. 6. Global dynamical behaviors varying with the system parameter b ($b \in [0,100]$): (a) Bifurcation diagram; (b) Lyapunov exponent spectrum.

点吸引子静默区 ($b \in [0,8]$): 在该区间内, 分岔图呈现空白状态, 且 LE 谱显示 $L_1 \leq 0$ 。这表明在此参数下系统初始能量被快速耗散, 系统状态最终收敛于稳定的点吸引子 (Point Attractor), 无持续振荡产生。突发混沌现象 ($b \approx 8$): 当参数越过临界值 $b \approx 8$ 时, 系统经历了剧烈的内部危机。分岔图上瞬间爆发出一面致密的混沌点云, 且 L_1 垂直跃升穿过零轴变为正值。系统在无明倍周期分岔前兆的情况下, 直接由稳定点突入深度混沌状态^[20]。

大范围鲁棒混沌 ($b \in [15,100]$): 随着 b 的继续增大, 系统表现出极具工程应用价值的鲁棒混沌 (Robust Chaos) 特性。在该宽广的参数域内, 状态变量 $|y|$ 的振幅不断扩张, L_1 持续平稳地保持在零轴上方。除了极少数狭窄的周期窗口 (如 $b \approx 25, 35$ 处的“深 V”型探底) 外, 系统对参数微扰表现出极强的抗干扰能力, 维持着高度不可预测的复杂演化。

综合上述全参数域忆阻 Lorenz 超混沌系统的动力学分析可知, 无论在正半轴还是负半轴, 系统的 Lyapunov 指数之和始终满足 $\sum_{i=1}^4 L_i < 0$ (由 $L_4 \approx -12$ 的大绝对值负数主导)。这从理论上严格证明了该忆阻 Lorenz 超混沌系统是一个高度耗散系统, 其相体积随时间的演化呈指数级收缩, 满足奇异吸引子存在的必要条件。相较于常规系统, 平滑忆阻反馈项与偏置参数的联合引入, 使得新构建的忆

阻 Lorenz 超混沌系统展现出对参数极性高度敏感的非对称演化拓扑,极大地丰富了系统的非线性动力学行为。

4 NIST 测试

美国国家标准与技术研究院(NIST)制定的随机序列测试标准 SP800-22,是目前被广泛应用的随机数检测标准。使用该标准中的 15 项测试检验混沌系统序列的伪随机性,每项测试生成一个相应的 P 值, P 值大于 0.01 表示序列通过测试。对 100 组长度为 125kb 的随机序列进行测试,测试结果如表 1 所列。从表 1 可以看出,所有测试项目的 P 值均大于 0.01,表明混沌系统生成的序列具有良好的伪随机性,适用于图像加密算法的应用。

表 1 NIST 测试结果
Table 1. NIST test results.

编号	测试项	P 值	结果
01	频率测试	0.035174	成功
02	块频率测试	0.213309	成功
03	累积和测试	0.419021	成功
04	运行测试	0.595549	成功
05	最大 1 游程长度测试	0.437274	成功
06	二值矩阵秩测试	0.262249	成功
07	离散傅里叶变换测试	0.955835	成功
08	非重叠模块测试	0.115387	成功
09	重叠模块匹配测试	0.834308	成功
10	通用测试	0.554420	成功
11	近似熵测试	0.554420	成功
12	随机游走测试	0.772760	成功
13	随机游走变体测试	0.134686	成功
14	序列测试	0.867692	成功
15	线性复杂度测试	0.946308	成功

5 基于新系统的图像加密应用

5.1 加密解密设计

传统的混沌图像加密方案往往采用静态密钥流,且在处理彩色图像时忽略了

各颜色通道间的强相关性，极易受到选择明文攻击 (Chosen-Plaintext Attack, CPA) 与差分攻击^[21]。为提升系统的密码学安全性，本节设计了一种结合 SHA-256 哈希关联与 RGB 跨通道级联反馈 (Cross-channel Cipher-Block Chaining) 机制的彩色图像加密算法。

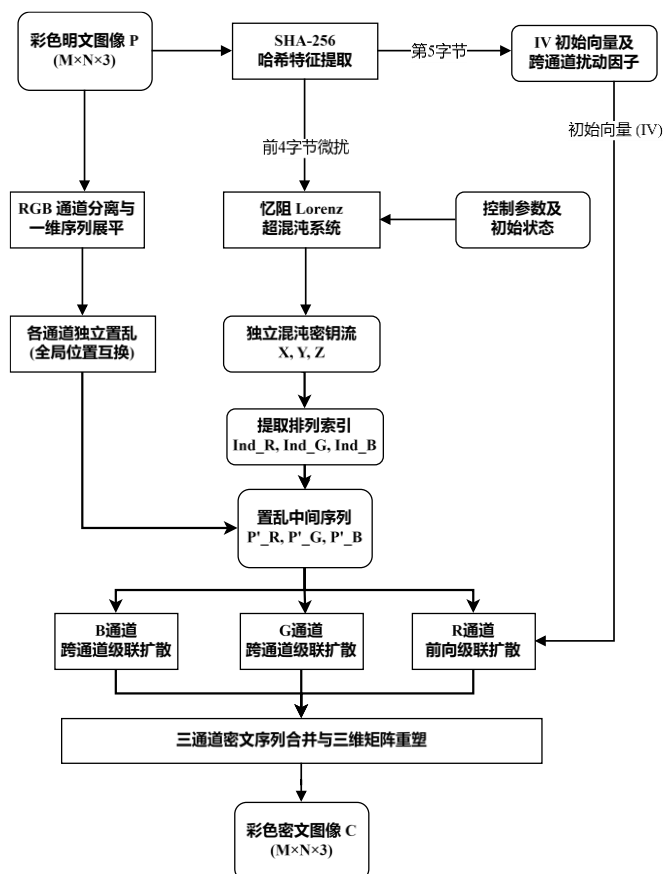


图 7 基于新型忆阻混沌系统与 SHA-256 的彩色图像加密算法流程图
Fig.7. Flowchart of the color image encryption algorithm based on the novel memristive chaotic system and the SHA-256.

具体步骤如下：

步骤 1 读取大小为 $M \times N \times 3$ 的原始彩色明文图像 P ，利用 SHA-256 算法计算其 256 位哈希值。提取哈希值的前四个字节分别转换为微扰因子，并将其动态叠加至忆阻 Lorenz 超混沌系统的初始状态 $(x_0, y_0, z_0, \varphi_0)$ 中。该机制确保了“一图一密”，即便是仅存在单像素差异的图像，也会产生截然不同的混沌密钥流序列，从根本上抵御了已知明文与选择明文攻击^[22]。

步骤 2 将彩色图像 P 分解为 R （红）、 G （绿）、 B （蓝）三个单色平面，并分别展平为长度为 $L(L = M \times N)$ 的一维像素序列。采用四阶龙格-库塔法迭代上述微扰后的超混沌系统，截取离散化处理后的独立密钥流 X, Y, Z 。值得注意的是，在此密钥流生成环节，本系统独特的内生非对称性与多稳态共存现象（如前文图 3、图 4 所示）发挥了核心作用。步骤 1 中引入的微小初值扰动，不仅能在李雅普诺夫发散机制下导致轨迹呈指数级分离，更易触发系统状态在不同共存隐藏吸引子盆之间的非线性跃迁。这种由底层非线性异构演化驱动的物理随机性，使得生成的离散混沌密钥流 X, Y, Z 具有远超常规单稳态对称系统的复杂度和极高的不可预测性。随后，分别对序列 X, Y, Z 进行升序排列提取索引向量 Ind_R, Ind_G, Ind_B 。利用这三组独立索引分别对 R 、 G 、 B 通道序列进行全局位置置乱^[23]，彻底打破原图像不仅在空间上，而且在颜色维度上的相邻像素相关性，得到置乱序列 P'_R, P'_G, P'_B 。

步骤 3 在传统的扩散机制中，密文的改变仅取决于当前位置的密钥且各通道独立^[24, 25]。为指数级增强系统的抗差分攻击能力（提升 NPCR 与 UACI 指标），本算法引入了链式跨通道反馈扩散操作。首先，提取哈希值的第 5 个字节作为初始向量（IV），对 R 通道进行前向级联扩散：

$$C_R(i) = P'_R(i) \oplus X(i) \oplus C_R(i-1) \quad (13)$$

其中， $C_R(0) = IV$ ， $i \in [1, L]$ 。随后，打破通道壁垒，将 G 通道扩散的初始状态与 R 通道末尾的密文像素进行强耦合关联：

$$C_G(i) = P'_G(i) \oplus Y(i) \oplus C_G(i-1) \quad (14)$$

其中， $C_G(0) = C_R(L)$ 。同理， B 通道的扩散初始状态耦合为 G 通道的末尾密文像素，即 $C_B(0) = C_G(L)$ 。

通过此跨通道级联方程，明文图像 R 通道中哪怕只有一个微弱的像素发生

改变,不仅会在其本通道内引发雪崩效应,更会随着迭代不可逆地跨越通道边界,逐级传播至 G 通道与 B 通道中,导致最终整个彩色密文图像发生剧变。

步骤 4 将生成的一维密文序列 C_R, C_G, C_B 重新合并并重塑为 $M \times N \times 3$ 维的三维矩阵,输出最终的彩色加密图像 C。解密过程严格遵循加密的逆向操作,在提取对应哈希值重构密钥流后,依次执行 B、G、R 通道的逆向跨通道反馈解密,最后进行单通道逆置乱,即可无损恢复原始彩色图像。

为了直观验证本文所提彩色图像加密算法的有效性与可行性,选取大小为 256×256 像素的标准彩色 Baboon 图像作为测试明文进行仿真实验。设定忆阻 Lorenz 超混沌系统的基础控制参数处于鲁棒混沌区域($\sigma = 8, \rho = 20, \beta = 8/3, a = 0.1, k = 0.8, b = 30$),并提取明文图像 SHA-256 哈希值的前四个字节作为初始微扰因子(x_0, y_0, z_0, φ_0)驱动系统演化^[25],生成的图像加密与解密视觉效果如图 8 所示。

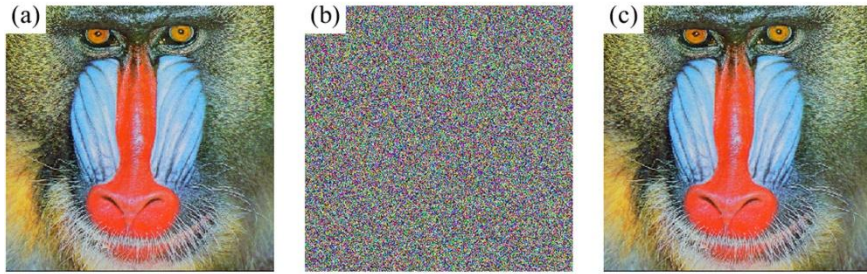


图 8 图像加密解密效果: (a) 明文图像; (b) 密文图像; (c) 解密图像
Fig. 8. Image encryption and decryption effect: (a) Plaintext image; (b) Ciphertext image; (c) Decrypted image.

观察图 8 可知,原始明文图像(图 8(a))中丰富的色彩层次、明显的纹理轮廓以及猴脸的视觉特征,在经过本文设计的“独立空间置乱”与“跨通道雪崩级联扩散”双重加密处理后,已完全被打破。最终输出的密文图像(图 8(b))呈现出毫无规律的类噪声状态,无法通过肉眼辨识出任何与原始明文相关的有效视觉信息,表明该算法具有极高的混淆度与极佳的加密隐蔽性。同时,在接收端获取正确的

密钥及哈希特征后，严格执行逆向解密操作，所得到的解密图像（图 8(c)）在视觉效果上与原始明文图像毫无二致。经过进一步的像素级校验对比确认，两者之间的差值为零，这充分证明了本文算法不仅安全性高，而且在数学逻辑上具备严谨的无损可逆性。

5.2 密钥空间与密钥敏感性分析

暴力攻击（Brute-force attack）试图通过穷举密钥空间中的所有可能组合来破解密文。因此，密钥空间的大小直接决定了加密方案对暴力攻击的抵抗能力^[26]。本节提出的图像加密方案中，初始密钥由忆阻 Lorenz 超混沌系统的 6 个控制参数（ $\sigma, \rho, \beta, a, b, k$ ）以及 4 个初始状态值（ x_0, y_0, z_0, φ_0 ）共同组成。在目前计算机标准的 IEEE 754 双精度浮点数标准下，计算精度可达 10^{-15} 。因此，本加密算法的密钥空间大小可达 $(10^{15})^{10} = 10^{150}$ 。该数值远超当前公认的密码学安全下限 2^{128} （约等于 3.4×10^{38} ），这表明本算法能够轻松抵御任何形式的暴力破解攻击^[27]。

此外，一个高强度的加密算法必须具备极强的密钥敏感性，即初始密钥发生任何极其微小的变化，都会导致生成的密钥流和解密结果出现雪崩式的改变。为测试密钥敏感性，设定初始精确密钥 Key 1 的参数为 $\sigma = 10$ ， $\beta = 8/3$ ， $\rho = 28$ ， $a = 0.1$ ， $b = 30$ ， $k = 0.8$ ，初值为 $(x_0, y_0, z_0, \varphi_0) = (0.1, 0.1, 0.1, 0)$ 。在此基础上，保持其他参数绝对不变，仅对初值 x_0 施加 10^{-15} 的极小偏移^[28]，构建微调后的密钥 Key 2（即 $x_0 = 0.1 + 10^{-15}$ ）。

如图 9 所示，使用 Key 1 对同一明文图像进行加密得到密文 1（图 9(a)），使用微小变化后的 Key 2 加密则得到密文 2（图 9(b)）。尽管 Key 1 与 Key 2 仅有 10^{-15} 的差异，生成的两幅密文图像不仅在视觉上均呈现为杂乱无章的噪声图，且两者之间的像素差异率（NPCR）依然高达约 99.6%，表明它们是完全不同的密文^[9]。此外，当攻击者截获密文 2 并试图使用极度相似的 Key 1 进行解密时，

解密操作完全失效，只能得到如错误噪声图（图 9(c)）所示的结果。实验充分证明，本加密方案对密钥具有极端的敏感性。

更重要的是，相较于传统对称混沌系统容易在特定参数区间陷入周期窗的缺陷，本文系统凭借其独特的内生非对称性（特别是引入的非零偏置参数 a 与内侧反馈参数 b ），在正负半轴展现出极其广阔且不对称的鲁棒混沌区间（如前文图 5、图 6 所示）。这不仅赋予了参数 a ， b 更大的有效取值范围，使得理论计算的密钥空间得以在实际工程中被完全利用，还从根本上杜绝了攻击者利用参数对称性或相空间镜像规律进行密钥空间降维打击的可能。

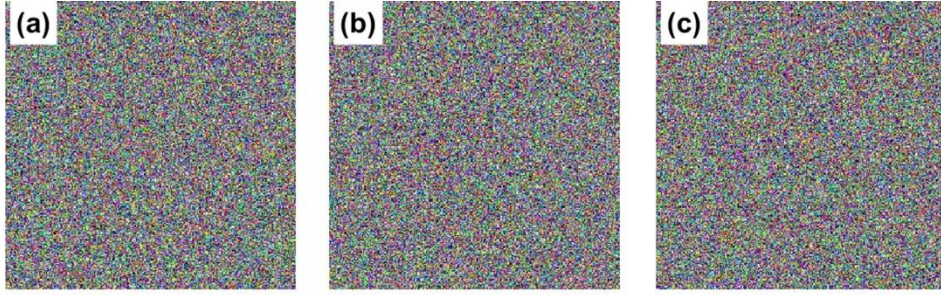


图 9 参数设定为 $\sigma=10$ ， $\beta=8/3$ ， $\rho=28$ ， $a=0.1$ ， $b=30$ ， $k=0.8$ ，初始值设定为 $(x_0, y_0, z_0, \varphi_0) = (0.1, 0.1, 0.1, 0)$ ：(a) 密文 1；(b) 密文 2；(c) 使用密钥 1 解密密文 2 的解密结果

Fig. 9. The parameters are set to $\sigma=10$ ， $\beta=8/3$ ， $\rho=28$ ， $a=0.1$ ， $b=30$ ， $k=0.8$ ，with the initial values set to $(x_0, y_0, z_0, \varphi_0) = (0.1, 0.1, 0.1, 0)$ ：(a) Ciphertext 1; (b) Ciphertext 2; (c) Decrypt the ciphertext 2 using key 1.

5.3 直方图分析

图像的直方图能够直观地反映出像素值在 0~255 灰度级区间的分布情况。对于自然明文图像而言，其像素值分布通常呈现出极度不均匀的连绵峰谷特征。这种携带大量视觉信息的统计学特征，极易成为攻击者进行统计分析破解的突破口。为了验证本文提出的基于忆阻 Lorenz 超混沌系统加密算法抵抗统计攻击的能力，本节对标准的彩色 Baboon 图像进行了直方图测试。

明文图像与密文图像的 R、G、B 三通道直方图分布对比结果如图 10 所示。

图 10(a)—(c) 分别为原始明文图像的红、绿、蓝通道直方图，可以看出其像素分布极其集中且起伏巨大，完全暴露了图像的固有统计特征，极易遭受攻击^[29-31]。相比之下，经过本文所设计的空间置乱与跨通道级联扩散算法加密后，密文图像的 RGB 直方图如图 10(d)—(f) 所示。此时三通道的像素分布均变得极其平坦和均匀，各像素值出现的频率几乎完全相等，呈现出类似白噪声的分布特性。这表明该加密算法有效掩盖了原始明文图像的任何统计信息，彻底切断了明文与密文之间的统计关联，从而显著增强了系统对统计分析攻击的抵抗力^[32]。

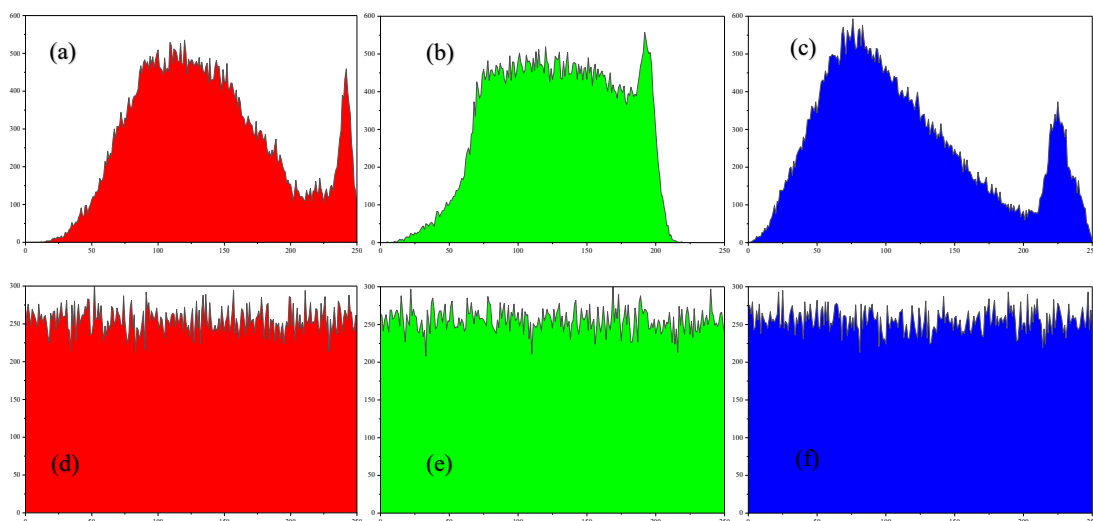


图 10 直方图测试结果: (a), (b), (c) 明文图像的 RGB 直方图; (d), (e), (f) 密文图像的 RGB 直方图

Fig. 10. Histogram tests: (a), (b), (c) RGB histograms of the plaintext images, respectively; (d), (e), (f) RGB histograms of the ciphertext images, respectively.

5.4 相关性分析

在图像加密领域，相邻像素之间的相关性是衡量加密算法抵抗统计分析攻击能力的重要指标。自然明文图像由于存在大量的平滑区域与冗余视觉信息，其相邻像素在水平、垂直和对角线方向上通常具有极高的线性相关性。攻击者极易利用这种强相关性，通过部分已知像素的灰度值推测出相邻未知像素的信息，进而

破解密文^[33]。

为了验证本文提出的基于忆阻 Lorenz 超混沌系统与跨通道级联扩散的加密方案打破像素相关性的能力,本节以 Baboon 图像 的红色 (R) 通道为例进行相关性测试^[34]。在明文图像与密文图像中,分别随机抽取 4000 对相邻像素点,绘制其在水平、垂直和对角线三个方向上的灰度值散点分布图,结果如图 11 所示。

如图 11(a)—(c) 所示, Baboon 明文图像的相邻像素散点紧密地聚集在主对角线附近,呈明显的线性分布,这直观地证明了原始图像相邻像素值之间存在高度的关联性。相比之下,经过本文算法加密后,密文图像的像素散点图如图 11(d)—(f) 所示。密文的像素散点均匀且随机地铺满了整个二维坐标平面,说明相邻像素的出现频率完全随机。这一结果表明,本算法极大地消除了明文图像中相邻像素间的强相关性,使密文呈现出完美的类白噪声特性,从而显著提升了图像抵抗统计分析攻击的能力^[35]。

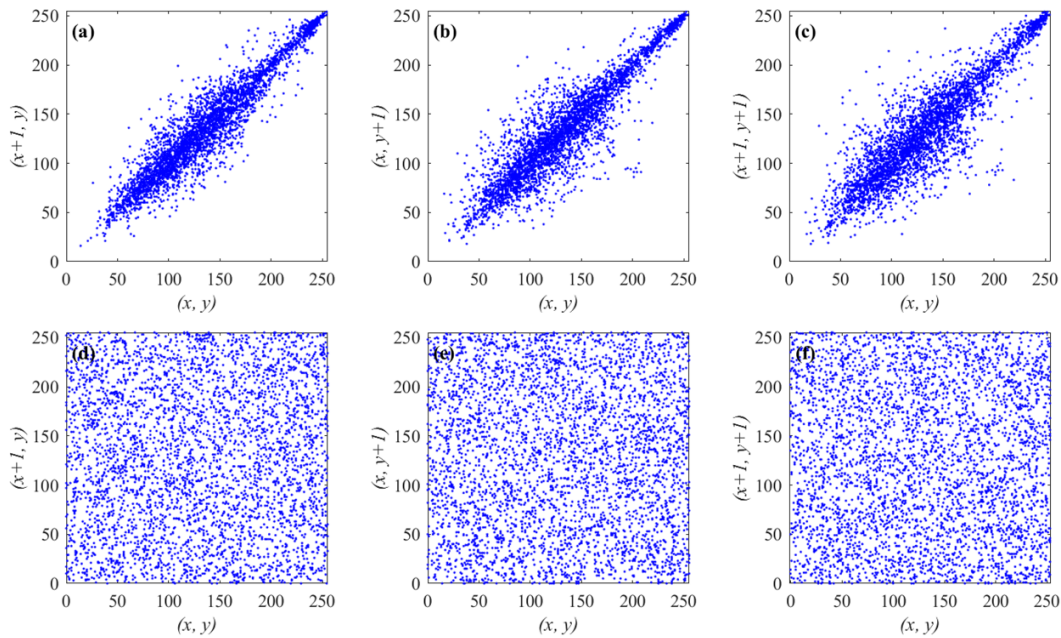


图 11 红色通道的相关性测试结果: (a), (b), (c) Baboon 明文图像的水平、垂直和对角的相关分布情况; (d), (e), (f) Baboon 密文图像的水平、垂直和对角的相关分布情况

Fig. 11. Correlation tests of the R channel: (a), (b), (c) Correlated distribution of the horizontal, vertical, and diagonal profiles of the plain Baboon, respectively; (d), (e), (f) Correlated distribution of the horizontal, vertical, and diagonal profiles of the cipher Baboon, respectively.

5.5 抗差分攻击分析

差分攻击是一种常见的密文图像破解方法，攻击者通常通过对原始明文图像进行极微小的变化（例如仅改变一个像素的灰度值），然后比较变化前后生成的两幅密文图像，以此来推测加密算法的密钥流和内部结构。为抵抗此类攻击，加密算法必须具备极强的“雪崩效应”，即微小的明文改变会导致密文发生全局性的剧烈变化^[36]。在学术界，通常采用 NPCR（像素数变化率）和 UACI（统一平均变化强度）这两个客观指标来精确计算两个密文图像之间的差异，从而评估该算法的抗差分攻击能力。其计算公式如下：

$$NPCR(C_1, C_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\% \quad (15)$$

其中，

$$D(i, j) = \begin{cases} 1, & \text{if } C_1(i, j) \neq C_2(i, j) \\ 0, & \text{if } C_1(i, j) = C_2(i, j) \end{cases}$$

$$UACI(C_1, C_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (16)$$

式中， C_1 和 C_2 分别代表原始明文图像和仅改变单个像素后的明文图像在某单一单色独立通道（如 R、G 或 B 通道）下的二维像素矩阵； M 和 N 为图像的高度和宽度。对于 8 位深度的彩色图像，理想的 NPCR 期望值约为 99.6094%，理想的 UACI 期望值约为 33.4635%。

为了测试本方案的抗差分攻击能力，我们在 Baboon 彩色明文图像中随机选取一个像素，将其灰度值微调（加 1），随后使用完全相同的初始参数（ $\sigma, \rho, \beta, a, b, k, x_0$ ）对这两幅图像进行加密。由于本文算法引入了 SHA-256 算法提取明文哈希特征并深度耦合至忆阻 Lorenz 超混沌系统的初始条件中，微小的像素级改变导致生成的混沌密钥流截然不同^[37]。此外，配合 RGB 跨通道级联扩

散机制，差异被瞬间放大至全图。测试结果如表 2 所示。本文算法在 R、G、B 三个通道上的 NPCR 的均值均稳定在 99.6145% 左右，UACI 均值均稳定在 33.4910% 左右。实验结果表明，即使在使用相同密钥对具有微小差异的图像进行加密时，生成的密文图像表现出显著差异。与近期文献中的其他前沿算法相比，基于新系统与跨通道级联扩散的加密算法能够极度有效地抵抗差分攻击，确保加密系统的绝对安全性^[38]。

表 2 不同算法的 NPCR 和 UACI 值比较

Table 2. Comparison of the NPCR and UACI values of the different algorithms.

	NPCR			UACI		
	R	G	B	R	G	B
本文	99.6292	99.6201	99.5941	33.4736	33.5259	33.4734
Xu et al. ^[39]	99.5998	99.6120	99.6006	33.4525	33.4426	33.4574
Dehghani et al. ^[40]	99.5697	99.6368	99.6078	33.6510	33.5045	33.5231
Xin et al. ^[41]	99.6299	99.6037	99.6090	33.4236	33.4326	33.4886
Wang et al. ^[42]	99.6002	99.6094	99.6155	33.4128	33.4347	33.4488

需要进一步指出的是，尽管如表 2 所示，采用标准 Lorenz 等常规超混沌系统配合本文的加密框架，在理想情况下同样能使 NPCR 和 UACI 指标逼近理论最值，但这仅代表它们在像素分布上满足了统计学随机性。在现代密码分析中，常规对称超混沌系统由于相空间拓扑结构固定且参数域存在周期窗陷阱，极易遭受基于相空间重构与机器学习的参数估计攻击。相比之下，本文引入的新型忆阻 Lorenz 超混沌系统，凭借其极其独特的内生非对称性与极端多稳态共存机制，实现了更深层次的安全性跨越。一方面，系统隐藏吸引子在微小扰动下的全局异构

漂移，从根本上阻断了相空间重构攻击的路径；另一方面，正半轴极宽广的鲁棒混沌带排除了周期窗带来的弱密钥隐患。因此，本方案不仅在统计指标上达到了极优水平，更将图像加密的安全性从表层的“统计学安全”跃升到了底层动力学层面的“拓扑结构安全”。

5.6 抗剪切攻击分析与鲁棒性测试

在数字图像的网络传输与物理存储过程中，由于信道噪声或恶意截获，密文图像常面临数据块丢失的风险。一个优异的图像加密算法应具备良好的鲁棒性，即在密文图像遭受一定程度的破坏或数据丢失时，接收方仍能通过正确的密钥恢复出原始明文图像的主要视觉信息^[43]。剪切攻击（Cropping Attack）便是模拟此类数据丢失情况的核心评估手段。为了验证本文提出的基于忆阻 Lorenz 超混沌系统加密方案的容错能力，本节对彩色 Baboon 密文图像进行了不同比例的剪切测试。具体而言，分别将密文图像的 10%（右侧边缘）、30%（左侧边缘）和 50%（底部区域）的像素数据强制置零，模拟不同程度的严重数据丢失^[44]。剪切后的受损密文图像如图 12(a)—(c) 所示。随后，使用原始的正确密钥对上述受损密文进行解密，恢复结果如图 12(d)—(f) 所示。实验结果表明，尽管密文图像丢失了高达一半的连续像素数据，解密图像中不可避免地出现了类似椒盐噪声的噪点，但 Baboon 的整体轮廓、五官细节以及色彩纹理特征依然清晰可辨。这种优异的抗剪切性能主要归功于算法中的“全局位置置乱”机制——密文中局部且连续的数据丢失，在逆向解密重构时被均匀地分散到了全图的空间域中，有效避免了局部特征的彻底毁灭。因此，本文设计的加密算法在抵抗剪切攻击方面表现出色，具有极高的鲁棒性和实际应用价值^[45]。

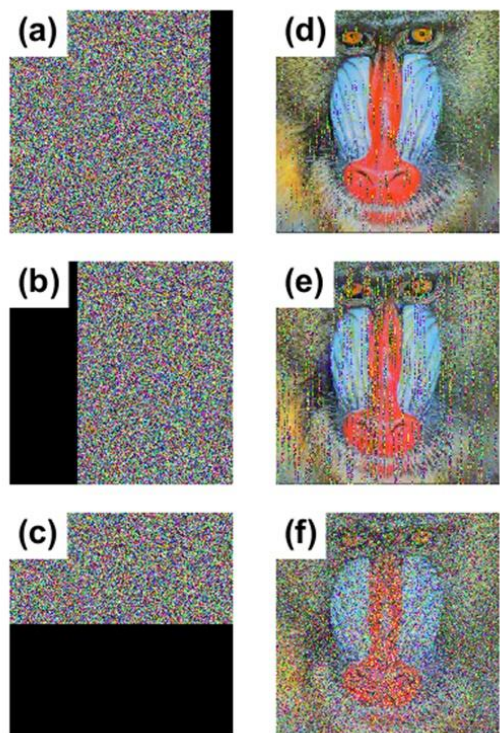


图 12 不同剪切比例下的加密图像及对应的解密图像: (a)–(c) 剪切比例分别为 10%, 30%, 50%; (d)–(f) 剪切后的解密图像

Fig. 12. Encrypted images at different cropping ratios and the corresponding decrypted images: (a)–(c) Encrypted images with the cropping ratios of 10%, 30%, and 50%, respectively; (d)–(f) Decrypted image after cropping, respectively.

6 基于 FPGA 的硬件实现和加密系统验证

6.1 核心忆阻混沌发生器的物理可实现性验证

由于 FPGA (现场可编程逻辑门阵列) 具备强大的并行处理能力、极高的运行速度以及精准的时序控制等显著优势, 特别适合用于复杂高维非线性系统的高速信号发生与底层硬件开发。因此, 本文选择搭建基于 FPGA 的硬件实验平台, 以进一步验证所提出的新型忆阻 Lorenz 超混沌系统。

在具体实现过程中, 本文采用四阶龙格-库塔 (Runge-Kutta) 算法对连续的忆阻 Lorenz 超混沌系统进行数值离散化, 并使用 Verilog HDL 硬件描述语言在野火 FPGA 征途 Pro 开发板 (核心主控芯片为 Altera Cyclone IV) 上完成逻辑综合与布线。为了将 FPGA 内部生成的高速数字混沌序列转换为模拟信号输出, 实验采

用高速高精度的数模转换模块 (DAC8830) 进行数模转换, 最终将模拟电压信号接入 Tektronix DPO 2022B 数字荧光示波器中进行相图捕获, 完整的硬件实验测试平台如图 13 所示。

在硬件测试中, 设定忆阻超混沌系统的核心控制参数为 $\sigma = 8$, $\rho = 20$, $\beta = 8/3$, $a = 0.1$, $k = 0.8$, $b = 30$, 初始状态值设定为 $(x_0, y_0, z_0, \varphi_0) = (0.1, 0.1, 0.1, 0)$ 。经过硬件电路的实际上电运行, 示波器成功捕获了系统不同状态变量之间的二维吸引子相图, 其实际显示效果如图 13 所示。

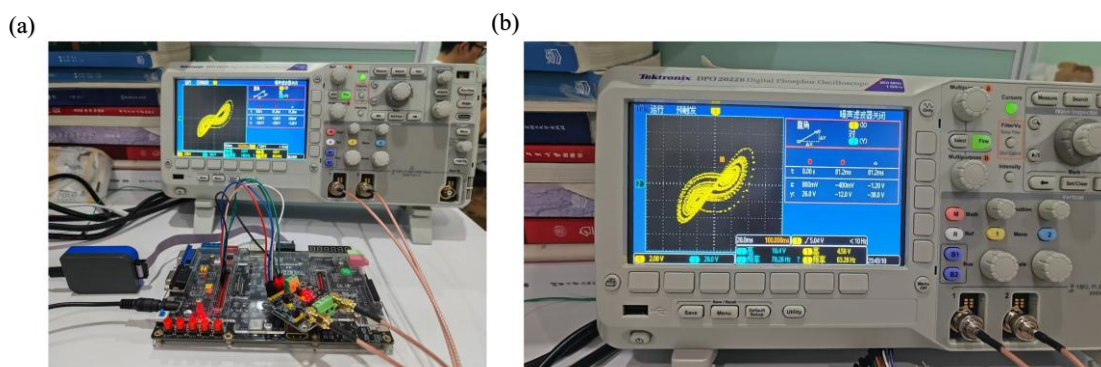


图 13 忆阻超混沌系统的 FPGA 硬件实现与测试结果: (a) 基于 FPGA 与数模转换器的硬件实验测试平台; (b) 示波器捕获的吸引子二维相图

Fig. 13. FPGA hardware implementation and test results of the memristive hyperchaotic system: (a) Hardware experimental test platform based on the FPGA and the digital-to-analog converter; (b) Two-dimensional phase portrait of the attractor captured by the oscilloscope.

对比观察可知, 示波器上呈现的硬件相图轨迹与前文利用计算机计算得到的仿真结果高度一致, 验证了该系统在物理硬件上的可实现性和在实际应用中的可行性。该实验不仅证明了引入的新型平滑忆阻器模型能够在实际数字电路中稳定运行, 也为本文后续提出的基于该系统的实时图像加密算法等工程应用奠定了坚实的物理硬件基础。

6.2 图像加密算法的 FPGA 系统级硬件实现

6.1 节的硬件实验成功验证了新型忆阻混沌核心引擎 (Core IP) 在底层数字电路中的稳定运行。为了进一步回应实际应用场景对算法工程化落地的需求, 本

节基于该混沌引擎，构建了包含视频采集、硬件流加密与实时显示的完整 FPGA 图像加密系统链路。

实验采用 OV7725 摄像头模块进行真实物理场景（绿植）的实时视频流采集，并在 FPGA 内部署了本文设计的“置乱-扩散”硬件加密架构。该架构利用 6.1 节验证的忆阻 Lorenz 超混沌发生器作为真随机密钥流驱动源。在系统默认的明文透传模式下，摄像头捕获的绿植轮廓与色彩特征在本地 TFT 液晶屏上被精准还原，如图 14(a) 所示。

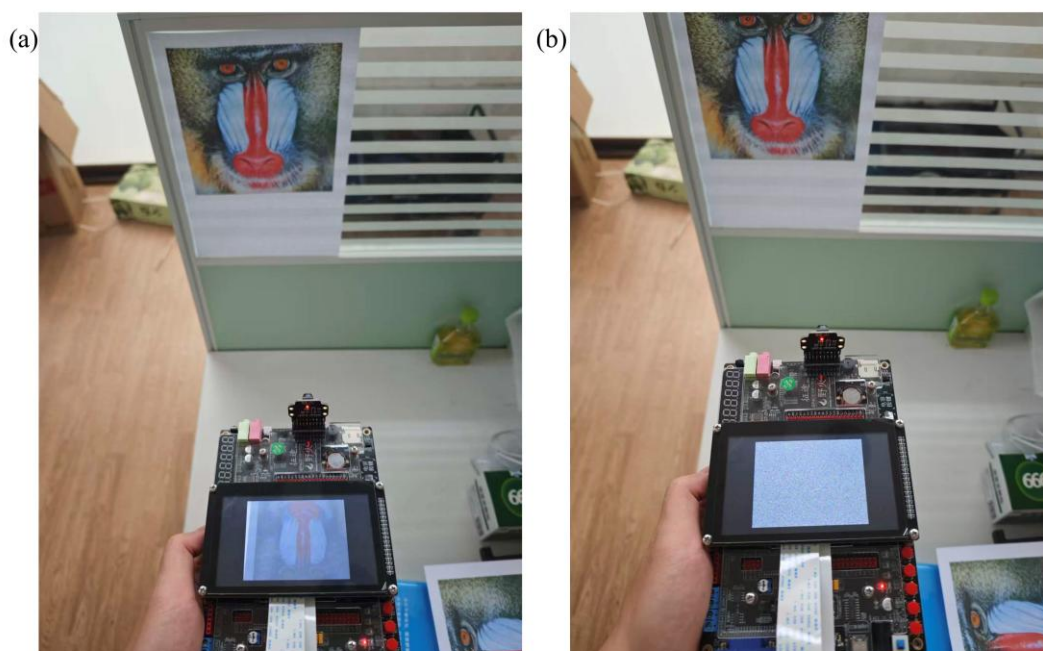


图 14 基于 FPGA 的实时图像加密系统视觉演示：(a) 实时采集并显示的原始明文图像；(b) 触发硬件加密后输出的密文图像

Fig. 14. Real-time visual demonstration of the FPGA-based image encryption system: (a) Original plaintext image captured and displayed in real time; (b) Ciphertext image output after triggering the hardware encryption.

当通过开发板上的独立按键触发“硬件加密使能”信号后，FPGA 内部的加密逻辑瞬间介入数据链路。依靠 FPGA 强大的底层并行计算能力与流水线（Pipelined）架构，系统对高速视频流与混沌密钥流进行逐像素（Pixel-by-pixel）的实时异或与混淆操作。从视觉效果观察，如图 14(b) 所示，此时 TFT 屏幕上的显示画面瞬间由清晰的植物图像转变为杂乱无章的“雪花噪声”状态。原视频流

中的所有纹理、边缘及色彩信息被彻底掩盖，实现了视觉层面的绝对机密性保护。这一系统级硬件实验不仅直观地展示了本方案出色的视觉加密效果，更证明了所设计的忆阻超混沌加密算法在面对高速率、持续性的真实外部数据流时，依然具备极高的吞吐量与极低的硬件处理延迟。这为本文理论成果在农业物联网（Agri-IoT）、安全视频监控等需要实时物理层加密的工业场景中的大规模部署，提供了坚实的工程验证与技术原型。

7 结 论

本文提出并详尽分析了一种新型忆阻 Lorenz 超混沌系统，并以此为核心设计了面向物理层安全的彩色图像加密方案。研究表明，引入平滑忆阻反馈与偏置参数后，系统展现出极具特色的内生非对称性与多稳态共存现象，在正半轴形成了极其宽广的鲁棒混沌带。在图像加密应用中，本方案不仅在 R、G、B 三个通道上的 NPCR 的均值（99.6145%）和 UACI 均值（33.4910%）等统计学指标上逼近理论极限，更重要的是，它将加密的安全性从传统的“统计学安全”跃升到了底层动力学层面的“拓扑结构安全”。相较于常规对称混沌系统，本系统隐藏吸引子的全局异构漂移特性，从根本上阻断了现代密码分析中基于相空间重构与机器学习的参数估计攻击；而无周期窗陷阱的鲁棒混沌带，则确保了理论上的巨大密钥空间在实际应用中具备绝对的有效性与鲁棒性。此外，基于 FPGA 与高精度 DAC 模块的硬件实验，成功捕获了与数值仿真高度吻合的物理相图，验证了该高维忆阻混沌系统在实际数字电路中稳定运行的可实现性。因此，本研究最深刻的结论在于指出：混沌加密的核心价值并非仅是提出一种新算法，而是展示了一种新的安全范式。其安全性基石从传统密码学中“难以求解的数学问题”，转向了由连续参数空间、正李雅普诺夫指数以及极端多稳态共同构筑的“难以精确复现或预测的物理过程”。这一范式转变，不仅为基于忆阻器的非线性动力学应用提

供了坚实的实验与理论基础，更为应对后摩尔时代量子计算等新型算力对传统密码体系的潜在威胁，提供了一条极具前景的物理层安全加密路径。

参考文献

- [1] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
- [2] Kocarev Lj, Halle K S, Eckert K, Chua L O, Parlitz U 1992 *Int. J. Bifurcation Chaos* **2** 709
- [3] Dedieu H, Kennedy M P, Hasler M 1993 *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing* **40** 634
- [4] Suykens J A K, Vandewalle J 1993 *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **40** 861
- [5] Hu H P, Yu Z L, Liu L F 2012 *Acta Phys. Sin.* **61** 190504 (in Chinese) [胡汉平, 于志良, 刘凌锋 2012 物理学报 **61** 190504]
- [6] Anwar T, Sanam N, Abu Ghazalah S, Alghamdi M, Alkhazi I S 2025 *IEEE Access* **13** 115135
- [7] Feng C W, Cai L, Zhang L S, Yang X K, Zhao X H 2010 *Acta Phys. Sin.* **59** 8420 (in Chinese) [冯朝文, 蔡理, 张立森, 杨晓阔, 赵晓辉 2010 物理学报 **59** 8420]
- [8] Wang M J, Yang C, He S B, Li Z J 2024 *Acta Phys. Sin.* **73** 130501 (in Chinese) [王梦蛟, 杨琛, 贺少波, 李志军 2024 物理学报 **73** 130501]
- [9] Weng T, Yang H, Gu C, Zhang J, Small M 2019 *Phys. Rev. E* **99** 042203
- [10] Deng Q L, Wang C H, Yang G 2026 *Acta Phys. Sin.* **75** 010003 (in Chinese) [邓全利, 王春华, 杨港 2026 物理学报 **75** 010003]
- [11] Yu S M, Yu Z D 2008 *Acta Phys. Sin.* **57** 6859 (in Chinese) [禹思敏, 禹之鼎 2008 物理学报 **57** 6859]
- [12] Min F H, Wang Z L, Wang E R, Cao Y 2016 *J. Electron. Inf. Technol.* **38** 2681 (in Chinese) [闵富红, 王珠林, 王恩荣, 曹弋 2016 电子与信息学报 **38** 2681]
- [13] Fei M, Li G D 2021 *J. Xinjiang Univ. (Nat. Sci. Ed.)* **38** 290 (in Chinese) [费敏, 李国东 2021 新疆大学学报(自然科学版)(中英文) **38** 290]
- [14] Jiang G, Guo X, Yang C, Ding Z 2021 *Comput. Simul.* **38** 176 (in Chinese) [蒋刚, 郭祥, 杨晨, 丁召 2021 计算机仿真 **38** 176]
- [15] Ruan J Y, Sun K H, Mou J 2016 *Acta Phys. Sin.* **65** 190502 (in Chinese) [阮静雅, 孙克辉, 牟俊 2016 物理学报 **65** 190502].

- [16] Yao X L, Zhang G Y, Wang J F, Cui J 2021 *Comput. Modernization* **38** 120 (in Chinese) [姚晓璐, 张国有, 王江帆, 崔健 2021 计算机与现代化 **38** 120]
- [17] Wang X Y, Yu J, Wang G Y 2018 *Acta Phys. Sin.* **67** 098501 (in Chinese) [王晓媛, 俞军, 王光义 2018 物理学报 **67** 098501]
- [18] Gao G J, Lu Q W 2021 *Comput. Modernization* **6** 107 (in Chinese) [高国静, 吕庆文 2021 计算机与现代化 **6** 107]
- [19] Lu A P, Li P C 2021 *Comput. Digit. Eng.* **49** 692 (in Chinese) [卢爱平, 李盼池 2021 计算机与数字工程 **49** 692]
- [20] Qiao J P, Deng L W, He J, Liao C W 2017 *Laser Technol.* **41** 897 (in Chinese) [乔建平, 邓联文, 贺君, 廖聪维 2017 激光技术 **41** 897]
- [21] Kaur M, Kumar V 2020 *Arch. Comput. Methods Eng.* **27** 15
- [22] Li C B, Sun J Y, Lu T N, et al. 2020 *Chaos* **30** 063144
- [23] Liu Y, Zhang L Y, Wang J, Zhang Y S, Wong K W 2016 *Nonlinear Dyn.* **84** 2241
- [24] Meng F Q, Wu G 2024 *Expert Syst. Appl.* **254** 124413
- [25] Sun J, Li C B, Lu T A, Akgul A, Min F H 2020 *IEEE Access* **8** 139289
- [26] Li L Z 2024 *IET Image Process.* **18** 627
- [27] Gohr A, Leander G, Neumann P 2022 *IACR Cryptol ePrint Archive* **2022** 1521
- [28] Hu H Y, Cao Y H, Xu J, Ma C G, Yan H Z 2021 *IEEE Access* **9** 22141
- [29] Chowdhary C L, Patel P V, Kathrotia K J, Attique M, Perumal K, Ijaz M F 2020 *Sensors* **20** 5162
- [30] Cui J X, Li G D, Wang L L, Ma C 2020 *Int. J. Inf. Commun. Technol.* **16** 230
- [31] Liu H J, Zhang Y Q, Kadir A, Xu Y Q 2019 *Appl. Math. Comput.* **360** 83
- [32] Du Y, Long G Q, Jiang D H, Chai X L, Han J H 2023 *Chin. Phys. B* **32** 114203
- [33] Norouzi B, Mirzakuchaki S 2014 *Nonlinear Dyn.* **78** 995
- [34] Moussa K H 2025 *Nonlinear Dyn.* **113** 31725
- [35] Inam S, Kanwal S, Amir R, Ksibi A, Matloob I 2025 *Sci. Rep.* **15** 7652
- [36] Liu H J, Kadir A, Liu J 2019 *IEEE Access* **7** 37211
- [37] Li Z, Peng C G, Li L R, Zhu X Y 2018 *Nonlinear Dyn.* **94** 1319
- [38] Yao J Q, Hu Q S, Huang S F, Cai S T, Xiong X M, Tan B H, Huang L Q 2026 *Nonlinear Dyn.* **114** 646

- [39] Xu Y D, Dong C W 2026 *Acta Phys. Sin.* **75** 020001 (in Chinese) [徐一丹, 董成伟 2026 物理学报 **75** 020001]
- [40] Dehghani R, Kheiri H 2024 *Multimedia Tools Appl.* **83** 17429
- [41] Xin J Y, Hu H P, Zheng J 2023 *Nonlinear Dyn.* **111** 7859
- [42] Wang Q Y, Zhang X Q, Zhao X H 2023 *Nonlinear Dyn.* **111** 22679
- [43] Qiu H S, Zhang X Z, Yue H X, Liu J Z 2023 *Mathematics* **11** 4099
- [44] Pourasad Y, Ranjbarzadeh R, Mardani A 2021 *Entropy* **23** 341
- [45] Alrekaby S N, Khodher M A A, Adday L K, Aljuaidi R 2025 *Algorithms* **18** 406

Application of Memristor-Based Lorenz Chaotic System in Image Encryption and Its Circuit Implementation*

Pengcheng Quan²⁾, Zhiqiang Yu^{1), 2), 3)†}

1) School of Computer and Information Technology, Hohhot Minzu College, Hohhot 010051, China

2) School of Electronic Engineering, Guangxi University of Science and Technology, Liuzhou 545006, China

3) Wuhan National Laboratory for Optoelectronics, School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, China

Abstract: With the rapid development of the information technology, the data communication security has faced the unprecedented challenges from the emerging technologies such as the quantum computing. To address the vulnerabilities of traditional mathematical algorithms, the physical layer security based on the chaotic cryptography has become a promising research direction. However, the conventional chaotic systems often suffer from the fixed topological structures and the periodic windows, rendering them susceptible to the modern phase space reconstruction and the parameter estimation attacks. To overcome these critical bottlenecks, this work has proposed a high-strength image encryption scheme based on a novel memristive Lorenz hyperchaotic system and validated its physical realizability via the Field-Programmable Gate Array (FPGA) hardware. From a nonlinear dynamics perspective, the as-proposed 4D Lorenz hyperchaotic system has exhibited the extreme intrinsic asymmetry and the coexisting hidden attractors by introducing a smooth memristor feedback term and a non-zero global drift control parameter. These unique dynamical behaviors have generated an ultra-wide robust chaotic region, completely eliminated the periodic window traps and fundamentally upgraded the system's security from the conventional statistical randomness to the underlying topological structural security. In the cryptographic design, a two-stage "dynamic permutation-diffusion" architecture has been proposed. The as-proposed 4D Lorenz hyperchaotic system has been closely coupled with the SHA-256 hash algorithm to achieve a "one-time pad" mechanism, where the extreme initial value sensitivity has translated the microscopic plaintext variations into the macroscopic attractor jumps. Furthermore, an innovative RGB cross-channel cipher-block chaining (CBC) diffusion mechanism has been designed to exponentially amplify the avalanche effect. The comprehensive security analyses have demonstrated that the as-proposed scheme has

achieved the near-ideal statistical properties. The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) have reached the 99.6145% and 33.4910%, respectively, while the adjacent pixel correlations have been suppressed below the 0.004. The scheme also has exhibited the excellent robustness against data loss and the cropping attacks. Finally, to verify the engineering feasibility of the as-proposed 4D Lorenz hyperchaotic system, the system-level hardware platform has been developed by using an FPGA combined with an OV7725 camera and a TFT display. The as-developed hardware tests have successfully captured the physical phase portraits consistent with the numerical simulations, and demonstrated the real-time and high-throughput video stream encryption. In conclusion, this work has not only realized the efficient and secure image encryption but also verified a new security paradigm that has leveraged the intrinsic physical complexity and the extreme multistability of the deterministic chaotic systems to replace the traditional computational complexity, providing the robust theoretical and experimental foundations for the anti-quantum physical layer security.

Keywords: Memristor, Lorenz chaotic system, image encryption, circuit implementation

* Project supported by the National Natural Science Foundation of China (Grant No. 22269002), the Reform Project of Graduate Education in Inner Mongolia Autonomous Region (Grant No. JGYB2026), the Basic Research Funding Project of Directly Affiliated Universities of Inner Mongolia Autonomous Region (Grant No. HM2026), and the Scientific Research Innovation Team Project of Hohhot Minzu College (Grant No. HM-TD-202514).

† Corresponding author. E-mail: zhiqiangyu@alumni.hust.edu.cn