

基于离散忆阻器的复值混沌系统动力学分析 及其在双图像加密中的应用*

邓全利¹⁾ 王春华^{1)2)†} 杨港¹⁾

1) (湖南大学信息科学与工程学院, 长沙 410082)

2) (湖南大学大湾区创新研究院, 广州 511300)

(2025年9月10日收到; 2025年10月13日收到修改稿)

设计新型混沌系统能够丰富加密系统的候选资源, 是基于混沌加密安全性的重要途径. 离散忆阻器因其固有的非线性特性与电路友好特性, 为构建新型混沌系统提供了有效途径. 然而, 其在复值离散混沌系统中的应用仍有待探索. 为此, 本文构建了一种基于离散忆阻器的复高斯混沌模型, 其中忆阻器由复数模长驱动. 通过李雅普诺夫指数、分岔图和相图等数值仿真分析, 验证了该系统具有增强的混沌特性. 同时, 在FPGA数字平台上实现了该模型的硬件部署, 证明其硬件可行性. 基于该模型生成的复值混沌序列, 本文进一步设计了一种双图像加密方案, 将两幅图像视为复数矩阵的实部和虚部, 通过混沌序列进行置乱和扩散操作. 仿真结果表明, 该加密方案具有高安全性, 能够抵抗多种攻击.

关键词: 离散忆阻器, 复值混沌, FPGA, 双图像加密

DOI: 10.7498/aps.75.20251242

CSTR: 32037.14.aps.75.20251242

1 引言

随着云计算、物联网和智能监控等技术的广泛应用, 敏感信息的保护已经成为关键性议题^[1-3]. 在各种数据形式中, 图像因其丰富的视觉信息承载能力以及在医疗影像、军事通信和社交媒体等领域的广泛应用, 成为至关重要的信息载体^[4-6]. 因此, 确保图像数据的机密性和完整性, 防止未授权访问和恶意攻击具有重要意义. 传统加密方法 (如 AES 和 DES) 虽然对文本数据有效, 但由于其计算复杂性及对特定图像攻击缺乏鲁棒性, 往往难以有效保障图像数据安全^[7]. 相比之下, 基于混沌系统的加密技术凭借混沌系统固有的特性, 包括对初始条件的敏感性、遍历性和伪随机性, 成为一种具有前景的图像加密方案. 现有研究提出了诸多利用经典离

散时间混沌映射 (如 Logistic, Tent 和 Hénon 等) 或连续时间混沌系统 (如 Lorenz, Chen 和 Chua 等) 的方案来生成加密所需的伪随机序列^[8-10]. 然而, 尽管取得了这些进展, 现有混沌图像加密方案仍面临着重大挑战, 如部分常用离散时间混沌映射存在密钥空间有限、混沌行为退化或抗密码分析攻击能力弱等问题; 而连续时间系统虽然能够提供更强的复杂性, 却通常需要采用特定的微分方程求解算法, 增加了计算资源的消耗, 这对实际应用构成了关键制约^[11-13].

为了应对这些局限性, 复数域的混沌现象逐渐受到关注, 复值混沌系统固有的多维特性为产生更加丰富的动力学行为以及提升加密系统的安全性提供了新途径. 这一新兴领域研究取得了瞩目的进展: 例如, Zhang 等^[14] 利用复数域多值函数构建了一种新型一维离散系统, 对其李雅普诺夫指数进行

* 国家自然科学基金 (批准号: 62571183, 62271197) 和广东省基础与应用基础研究基金 (批准号: 2024A1515011910) 资助的课题.

† 通信作者. E-mail: wch1227164@hnu.edu.cn

理论分析证明了该系统的复杂动力学特性; Hua 等^[15]设计了一种耦合二维复值离散系统, 并通过数值仿真验证了所设计系统的复杂性, 揭示了其相较于实数域混沌系统的优越性; Yao 等^[16]基于复参数帕斯卡矩阵设计了一种 N 维离散系统, 通过实验验证了该系统具有更高的混沌鲁棒性. 此外, 国外学者也在此领域做出了重要贡献. 例如, Rani 和 Agarwal^[17]对广义复值 Logistic 映射中的复杂分形行为进行了分析, 探究了复值 Logistic 混沌系统受初始值影响下的边界行为; Ayubi 等^[18]采用复折叠变换的方式提出了一种二维混沌系统, 并成功将其应用于视频水印, 展现了其在信息安全性领域的应用价值. 然而当前研究主要集中于通过数学分析的方式设计复数域混沌映射模型, 未将混沌系统与物理背景相结合, 特别是基于新型电子元件模型 (如忆阻器) 构建复值混沌系统的研究尚未得到充分关注.

忆阻器作为新型电子元件, 凭借其独特的非线性和非易失性, 已被广泛应用于非易失性存储器^[19]、存内计算^[20]以及非线性电路设计^[21]等领域. 近期提出的离散忆阻器模型因其具有计算高效性并且与以数字形式实现的加密算法高度契合, 进一步加速了忆阻器在混沌加密系统中的应用. 例如, Bao 等^[22]基于离散忆阻 Hopfield 神经网络开发的基于忆阻状态图像加密方案, 在资源受限场景中展现出良好的加密性能; Gao 等^[23]设计的双忆阻器立方映射在图像加密中表现出强扩散与混淆特性, 能够有效抵抗密码分析攻击. 国外学者在该领域研究中也取得了丰硕的成果, 如 Qurashi 等^[24]利用离散忆阻器设计了新型的神经元模型, 并分析了该模型在分数阶差分下的复杂动力学行为, 证明了该离散忆阻神经元模型具有较高的熵, 增强了混沌行为的不可预测性; Almatroud 等^[25]利用离散忆阻器构建了一个新型的 Grassi-Miller 混沌系统, 通过分析发现该系统为无平衡点型混沌系统且具有丰富的吸引子共存行为. 现有研究表明, 离散忆阻器混沌系统具有增强的混沌性能, 能够满足密码学应用需求. 然而, 当前研究多局限于实数域. 本文将离散忆阻器引入复值高斯系统, 旨在探索复数域中忆阻混沌系统的特性.

为此, 本文构建了一种新型忆阻器复值高斯混沌系统 (memristive complex-valued Gaussian model, MCVGM), 该系统以复值高斯映射的模长

作为忆阻器的输入变量, 并将忆阻器的输出反馈到复变量系统中. 采用李雅普诺夫指数、分岔图以及相轨迹等多种方式, 系统性地分析了所提出模型的动力学行为特性. 同时基于 FPGA 平台设计了 MCVGM 的数字化实现方案, 通过电路实验验证了模型的有效性. 此外, 充分利用复数运算特性, 创新性地设计了一种双图像加密方案, 将两幅图像视为复数矩阵的实部和虚部, 利用复值混沌序列对双图像矩阵进行联合加密操作. 数值仿真结果表明所设计的基于复数混沌序列的加密系统可以展现出良好的安全特性和抗攻击能力.

2 模型描述及动力学行为分析

2.1 系统模型

连续时间忆阻器模型的高计算复杂度成了限制其在诸多计算资源受限场景中应用的重要原因. 通过采用欧拉差分法进行时间离散化处理, 研究人员开发出了离散时间忆阻器模型^[26-28]. 这些模型在有效保持忆阻器核心特性的同时; 显著降低了计算资源开销, 从而为系统分析和硬件实现提供了便利. 本文采用的离散时间忆阻器模型如下:

$$\begin{cases} i_n = \sin(\pi w_n) v_n, \\ w_{n+1} = v_n, \end{cases} \quad (1)$$

其中, v_n , i_n 和 w_n 分别表示采样时刻 n 时忆阻器的输入电压、输出电流以及状态变量. 该模型将正弦函数作为忆导变量的状态调整函数, 因其能够以简洁的数学形式有效地模拟忆阻系统的关键非线性特性, 从而展现出丰富的动力学行为. 忆阻器在施加正弦激励信号 $v_n = A \sin(\omega n)$ 时, 系统会产生压控型磁滞回线. 图 1 展示了 v_n - i_n 平面上依赖于激励信号频率和幅值的磁滞回线特性, 随着激励信号频率的增大, 滞回曲线旁瓣面积逐渐减小, 当频率趋于无穷大时最终收敛为一条单值曲线. 该特性符合判断广义忆阻器的特征, 因此可以使用该模型模拟忆阻器的特性^[29-31].

经典高斯混沌映射是一种离散时间动力学系统, 其数学表达式如下:

$$x_{n+1} = e^{-ax_n^2} + b, \quad (2)$$

其中状态变量 x_n 及控制参数 a, b 均为实数. 具有二次指数的非线性项使得该系统能够呈现出混沌

行为. 经典高斯混沌映射的数学形式简单, 是研究离散非线性的重要模型之一. 然而, 其动力学行为主要受限于少有的几个系统参数, 在复杂性和可调控方面具有局限性. 为突破经典模型的限制, 本文引入离散忆阻器构建新型复数高斯混沌. 这种设计不仅保留了原模型结构简单的特性, 更重要的是利用忆阻器的非线性特性以及复数域的系统扩充, 为生成更复杂的混沌特性提供了基础. 本文构建了如图 2 所示的离散忆阻器复值高斯模型.

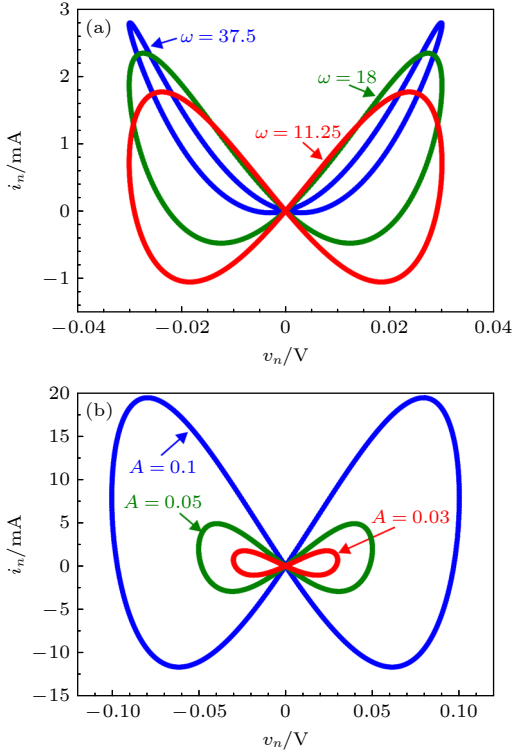


图 1 施加 $v_n = A \sin(\omega n)$ 时忆阻器的磁滞回线 (a) 固定 $A = 0.03$, ω 分别取 11.25, 18, 37.5; (b) 固定 $\omega = 11.25$, A 分别取 0.03, 0.05, 0.1

Fig. 1. Pinched hysteresis loops of the memristor when applying $v_n = A \sin(\omega n)$: (a) Fixed $A = 0.03$, ω selected as 11.25, 18 and 37.5; (b) fixed $\omega = 11.25$, A selected as 0.03, 0.05 and 0.1.

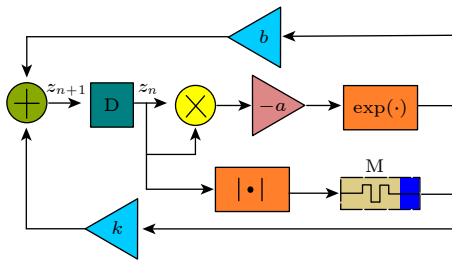


图 2 忆阻器复值高斯混沌系统的构成框图
Fig. 2. Structure diagram of the memristive complex-valued Gaussian map.

该系统包含两个部分: 1) 对 az^2 进行指数映射并通过参数 b 进行幅度缩放 ($a \in \mathbb{R}, b \in \mathbb{C}$); 2) 通过由模长 $|z|$ 驱动的忆阻器进行反馈, 忆阻器的输出由参数 $k \in \mathbb{C}$ 进行调节. 因此, 本文提出的系统模型可数学表述为如下形式:

$$\begin{cases} z[n+1] = be^{-az^2[n]} + k \sin(\pi y[n])|z[n]|, \\ y[n+1] = |z[n]|, \end{cases} \quad (3)$$

其中 $|z| = \sqrt{z_r^2 + z_i^2}$, z_r 和 z_i 分别表示系统状态变量的实部和虚部. 复值参数 k 设置为 $(1 - b_r) + i(1 - b_i)$, 其中 b_r 和 b_i 分别表示参数 b 的实部和虚部. 根据复数运算法则, (3) 式可以等价描述为

$$\begin{cases} z_r[n+1] = E[n][b_r \cos(\phi[n]) + b_i \sin(\phi[n]) \\ \quad + (1 - b_r) \sin(\pi y[n])v[n], \\ z_i[n+1] = E[n][-b_r \sin(\phi[n]) + b_i \cos(\phi[n]) \\ \quad + (1 - b_i) \sin(\pi y[n])v[n], \\ y[n+1] = v[n], \end{cases} \quad (4)$$

其中, $E[n] = e^{-a(z_r^2[n] - z_i^2[n])}$, $\phi[n] = 2az_r[n]z_i[n]$ 和 $v[n] = \sqrt{z_r^2[n] + z_i^2[n]}$ 分别表示指数项、相位角项和模长项.

2.2 动力学行为分析

为探究 MCVGM 的动力学特性, 本研究通过分岔图、李雅普诺夫指数谱、相轨迹和动力学地图分析其参数依赖行为. 所有数值仿真均在 MATLAB 环境中进行, 迭代初始条件设置为 $z[1] = 0.1 + 0.1i$, $y[1] = 0.1$. 李雅普诺夫指数谱采用 QR 分解法计算, 迭代次数为 5×10^4 次. 分岔图通过以小步长变化控制参数生成, 相轨迹则通过舍弃前 10% 迭代数据以消除瞬态效应后的时间序列数据构建.

为探究系统动力学行为对实参数 a 的依赖性, 本研究首先固定复参数 $b = 0.1 + 0.1i$, 令 a 在区间 $[-5, 5]$ 内变化. 图 3 通过数值仿真展示了与 a 相关的动力学行为: 图 3(a) 呈现前两个李雅普诺夫指数的演化规律, 图 3(b) 则展示了状态变量实部 (z_r) 与虚部 (z_i) 的分岔图. 最大李雅普诺夫指数 (LLE) 呈现关于 $a = 0$ 奇对称特性. 且在原点附近具有较宽的正李雅普诺夫参数范围, 表明系统对实数参数 a 的变化具有对称特性. 图 3(b) 中的分岔图揭示了这些动力学机制在状态空间的表现形式: 混沌区间对应 z_r 和 z_i 值的稠密非周期簇集 (如在

$a \in [-1.95, 1.95]$ 等区域尤为明显), 而周期窗口如 $a \in [-3.4, -2.9]$ 则呈现离散的分岔分支.

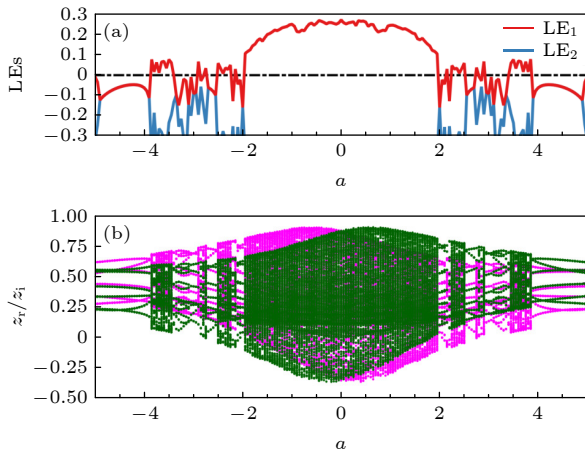


图 3 依赖于实数参数的动力学行为仿真 (a) 前两个李雅普诺夫指数; (b) z_r (绿色) 与 z_i (粉色) 的分岔图
Fig. 3. The real-valued parameter a -dependent dynamical behavior simulations: (a) First two Lyapunov exponents; (b) bifurcation of z_r (green colored) and z_i (pink colored).

在实值高斯映射中, 当 $a < 0$ 时会导致系统呈现指数发散行为. 本文设计的 MCVGM 在 $a = 0$ 处呈现出动力学行为的对称性. 这种对称性源于复动力系统的精确对偶覆盖特性: 变换 $\mathcal{T} : (a, z) \rightarrow (-a, iz)$ 使方程 (3) 保持不变量. 具体而言在 (3) 式中, 非线性项 e^{-az^2} 经变换后为 $e^{-(-a)(iz)^2} = e^{-az^2}$, 而耦合项 $(1 + i - b) \sin(\pi y)|z|$ 在 $z \rightarrow iz$ 作用下保持不变. 因此, 所有动力学机制在 $a = 0$ 两侧呈现镜像对称分布.

为探究复值耦合参数 $b = b_r + ib_i$ 的作用, 本研究固定 $a = 0.2$ 并分析系统随 b_r 和 b_i 变化的动力学行为. 图 4 分别展示了依赖于 b_r 和 b_i 的动力学特性: 当固定 $b_i = 0.1$ 且 b_r 在 $[0, 1]$ 区间变化时, 数值仿真的李雅普诺夫指数和分岔图分别如图 4(a1), (a2) 所示. 图 4(a1) 显示混沌区域主要集中于 $b_r \in [0, 0.62]$ 区间, 其间穿插多个周期窗口, 并在 $b_r \in [0.87, 0.9]$ 处出现 $LLE = 0$ 的准周期区域; 图 4(a2) 的分岔图证实了这些转变, 显示 $b_r < 0.62$ 时出现混沌结构, 超过该阈值后则呈现周期吸引子. 当固定 $b_r = 0.1$ 且 $b_i \in [-0.8, 0.8]$ 变化时, 从图 4(b1) 可观察到 $b_i \in [-0.8, -0.648]$ 处存在 $LLE = 0$ 的准周期区域, 而在 $b_i \in [-0.512, 0.4]$ 区间以混沌行为为主导并嵌入周期窗口; 图 4(b2) 展示的分岔结构与图 4(b1) 的李雅普诺夫指数变化一致, 即系

统在 $b_i \approx -0.648$ 处经历准周期行为向周期窗口的转变, 并在 $[-0.512, 0.4]$ 区间呈现稠密混沌轨迹.

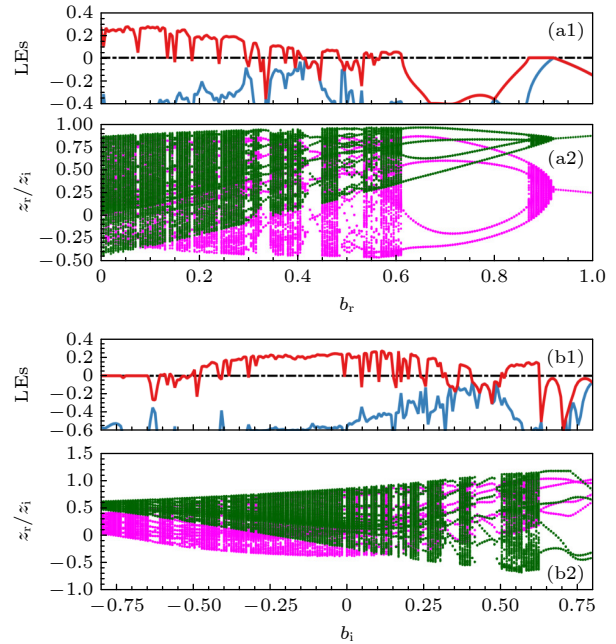


图 4 依赖于耦合参数 b 的动力学行为仿真 (a1), (a2) 固定 $b_i = 0.1$, $b_r \in [0, 1]$; (b1), (b2) 固定 $b_r = 0.1$, $b_i \in [-0.8, 0.8]$
Fig. 4. The coupling parameter b -dependent dynamical behavior simulations: (a1), (a2) $b_r \in [0, 1]$ with $b_i = 0.1$; (b1), (b2) $b_i \in [-0.8, 0.8]$ with $b_r = 0.1$.

基于李雅普诺夫指数与分岔图的参数分析, 本研究进一步选取 b_r 的 4 个典型取值 (0.1, 0.3, 0.4 和 0.9), 在固定 $a = 0.2$ 和 $b_i = 0.1$ 的条件下考察相空间吸引子, 结果如图 5 所示. 以忆阻状态变量 y 为纵坐标、复变量 z 的实部 (红色) 与虚部 (蓝色) 为横坐标绘制的相轨迹, 直接印证了先前识别的动力学机制: 当 b_r 取 0.1 和 0.4 时, 轨迹形成混沌吸引子 (图 5(a), (c)); 而设置 b_r 为 0.3 和 0.9 时, 则分别得到周期吸引子与准周期吸引子.

联合变换 $(a, z) \rightarrow (-a, iz)$ 保持了系统的不变性. 对称性破缺扰动对于全面表征其动力学鲁棒性和参数敏感性至关重要. 下文通过 3 种针对性变换来破坏系统结构的不同方面: 首先, 采用变量旋转 $(a, z) \rightarrow (a, iz)$ 来探究混沌生成对状态变量变换的敏感性; 其次, 通过参数复化 $(a, z) \rightarrow (ia, z)$ 测试系统对复值参数的容忍度; 最后, 利用复共轭变换 $(a, z) \rightarrow (a, \bar{z})$ 通过破坏 z 的解析性来评估时间反演不对称性. 为保证仿真条件的一致性, 本文后续数值分析中统一设定系统的初始值为 $z[1] = 0.1 + 0.1i$, $y[1] = 0.1$.

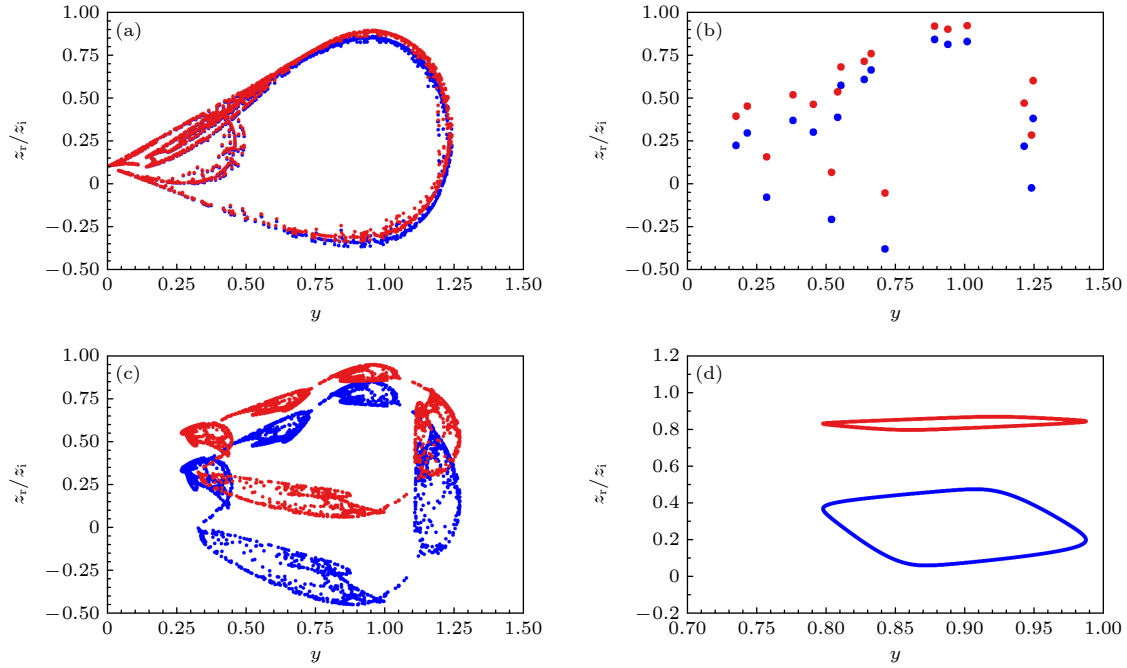


图 5 在 $y-z_r$ (红色) 和 $y-z_i$ (蓝色) 平面上的相图 (a) 混沌吸引子, $b_r = 0.1$; (b) 周期吸引子, $b_r = 0.3$; (c) 混沌吸引子, $b_r = 0.4$; (d) 准周期吸引子, $b_r = 0.9$

Fig. 5. Phase portrait in $y-z_r$ (red) and $y-z_i$ (blue) plane: (a) Chaotic attractor with $b_r = 0.1$; (b) periodic attractor with $b_r = 0.3$; (c) chaotic attractor with $b_r = 0.4$; (d) quasi-periodic attractor with $b_r = 0.9$.

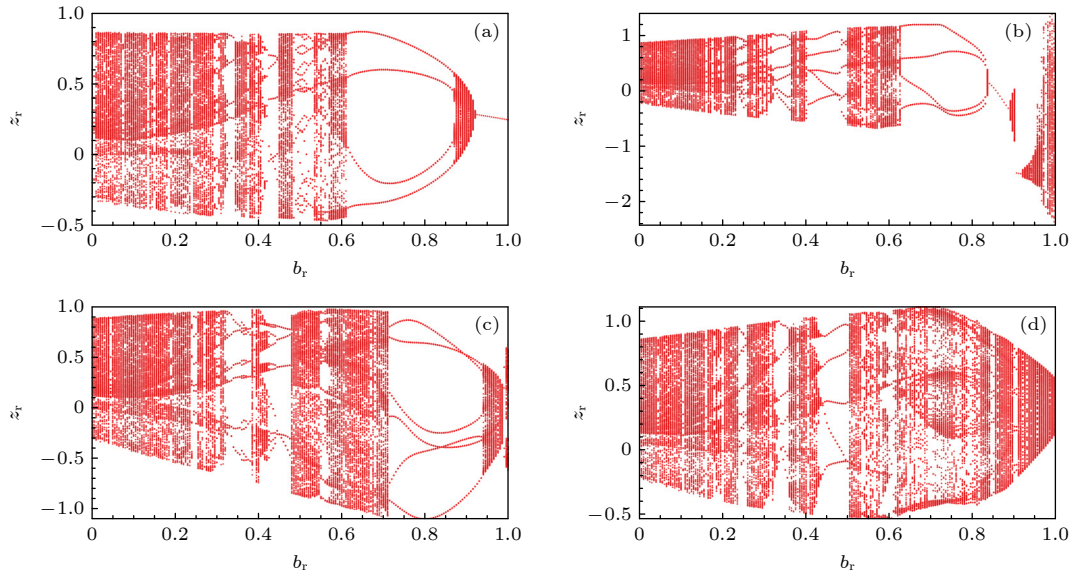


图 6 状态变量的分岔图 (a) 原始系统; (b) 施加变量旋转后; (c) 施加参数复化后; (d) 施加复共轭后

Fig. 6. Bifurcation diagram of z_r : (a) Original system; (b) under variable rotation; (c) under parameter complexification; (d) under complex conjugation.

图 6 中的分岔图展示了对称性破缺变换引发的动力学机制显著改变 (参数固定为 $a = 0.2$ (复化变换时取 $a = 0.2i$) 和 $b_i = 0.1$, 同时令 $b_r \in [0, 1]$ 变化). 原始系统 (图 6(a)) 在 $b_r \in [0, 0.62]$ 区间呈现典型混沌行为, 表现为 z_r 的稠密簇集与周期窗口交错分布; 在变量旋转变换下 ($z \rightarrow iz$, 图 6(b)), 主要

混沌区域破碎为间歇性混沌且周期性显著增强, 而在原周期域 $b_r \in [0.92, 1]$ 意外涌现新混沌带; 参数复化变换 ($a \rightarrow ia$, 图 6(c)) 将混沌范围扩展至 $b_r \in [0, 0.71]$, 但在 $[0.325, 0.385]$ 和 $[0.425, 0.475]$ 区间引入两个清晰的周期窗口, 其分岔转变较基线系统更为平滑; 最显著的改变出现在复共轭变换下

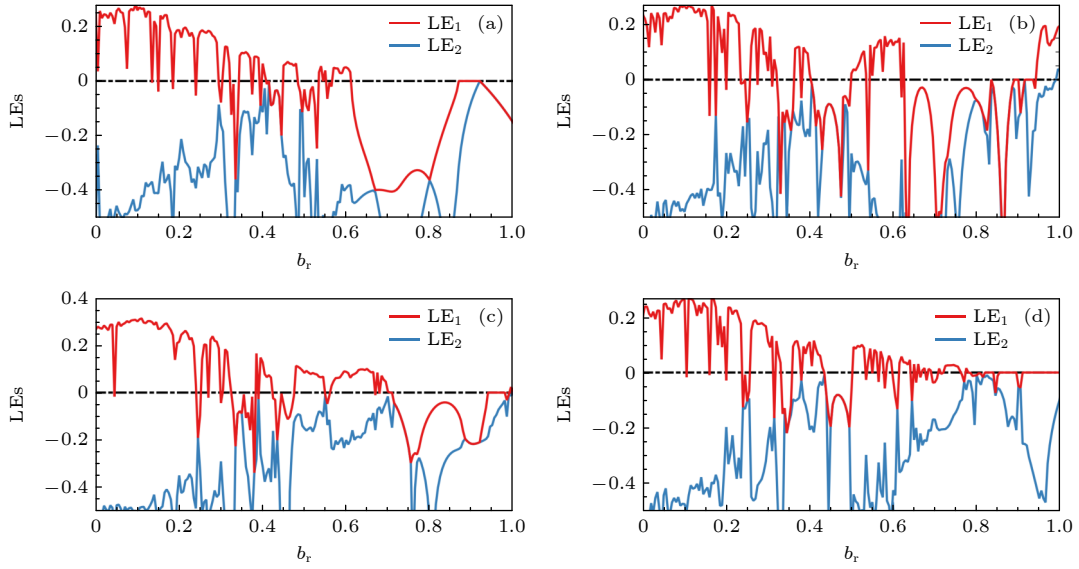


图 7 李雅普诺夫指数 (a) 原始系统; (b) 施加变量旋转后; (c) 施加参数复化后; (d) 施加复共轭后
 Fig. 7. Lyapunov exponents: (a) Original system; (b) under variable rotation; (c) under parameter complexification; (d) under complex conjugation.

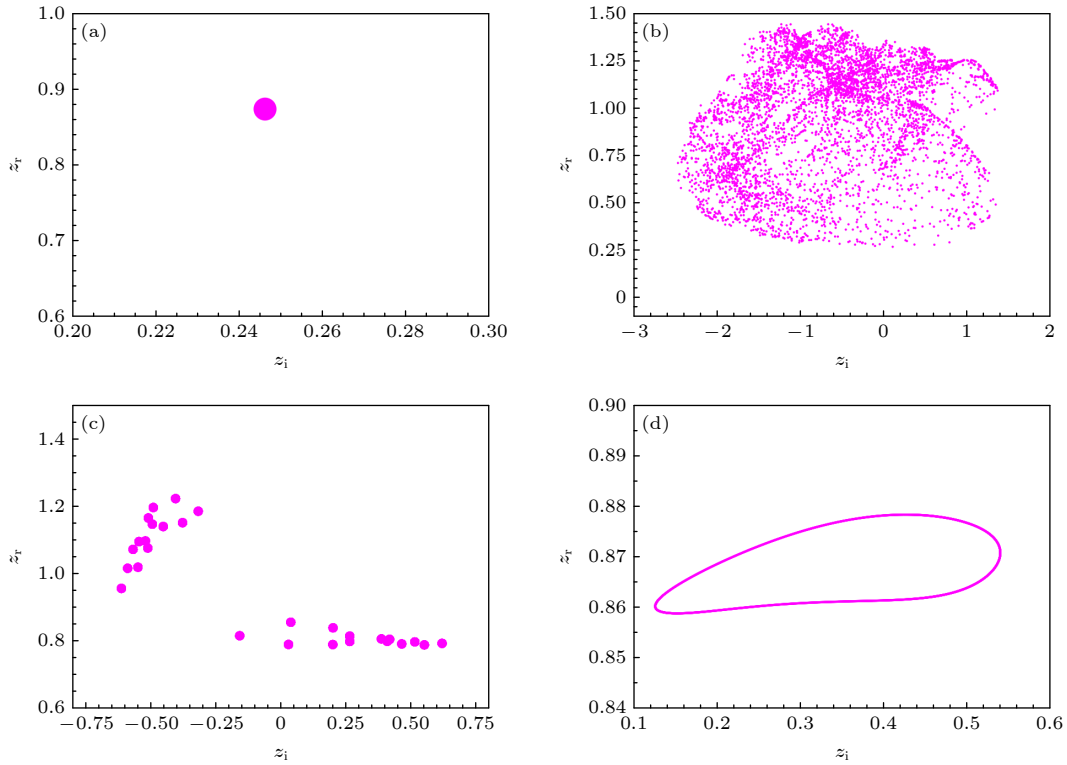


图 8 当 $b_r = 1$ 时的相图 (a) 原始系统; (b) 施加变量旋转后; (c) 施加参数复化后; (d) 施加复共轭后
 Fig. 8. Phase portraits with $b_r = 1$: (a) Original system; (b) under variable rotation; (c) under parameter complexification; (d) under complex conjugation.

($z \rightarrow \bar{z}$, 图 6(d)), 混沌主导区域扩大至 $b_r \in [0, 0.79]$, 原始周期轨道退化为准周期环面, 表现为无清晰分岔边界的增厚轨迹带. 这些变换共同表明: 对称性破缺不仅非均匀地重新分配参数空间中的混沌与周期区域, 还改变了转变阈值并引入新型吸引子,

图 7 中的李雅普诺夫指数谱证实了正指数与观测到的混沌带之间的对应关系.

图 8 中的相空间轨迹进一步阐明了 $b_r = 1$ 时对称性破缺变换下的动力学变异. 原始系统在 z_r - z_i 平面上收敛于稳定不动点 (图 8(a)), 这与图 6(a)

观测到的不动点机制一致; 相比之下, 变量旋转变换破坏该稳定性并生成混沌吸引子 (图 8(b)), 与对应分岔图中涌现的混沌现象相符; 参数复化变换诱发多周期动力学行为 (图 8(c)), 该现象与图 6(c) 识别的周期行为相关联; 复共轭变换则产生极限环 (图 8(d)), 这反映了从图 6(d) 展宽连续带推断出的准周期行为. 这些相空间观测结果定量验证了基于分岔的动力学行为变化, 表明对称性破缺不仅改变系统的参数依赖性, 更从根本上重构了其状态空间中的吸引子拓扑结构.

3 基于 FPGA 平台的硬件实现

基于 FPGA 的数字电路混沌映射实现因其高计算速度、强稳定性以及可灵活调节系统参数与初始条件等优势而备受关注 [32-34]. 本研究实现了所提出 MCVGM 模型 (4) 的 FPGA 硬件平台部署, 其实现流程框图如图 9 所示. 该实现中, 第 n 次迭代的状态变量分别记为 z_n^r , z_n^i 和 y_n : MCVGM 核心模块负责执行模型的迭代运算, 计算结果传输至数据转换模块以准备数模转换器 (DAC) 输出信号. 迭代运算与输出预处理操作在 Xilinx xc7z020c1g400-1 平台上执行, 数字信号通过 AD9767 DAC 转换为模拟信号后由示波器采集.

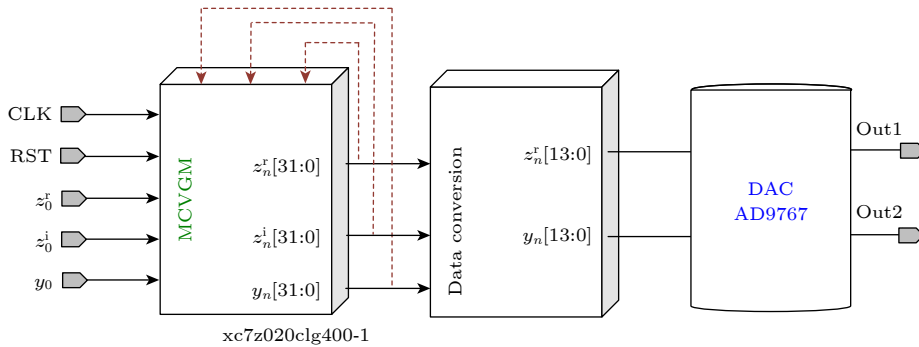


图 9 基于 FPGA 实现 MCVGM 的结构框图

Fig. 9. Block diagram for the FPGA-based implementation of MCVGM.

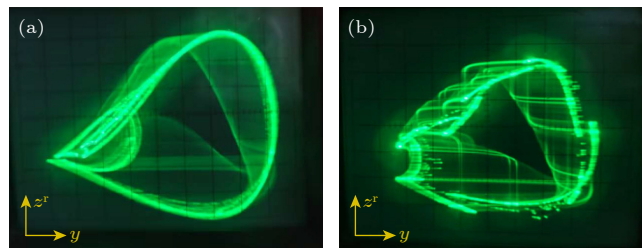


图 10 基于 FPGA 硬件实验产生的混沌吸引子 (a) $b_r = 0.1$; (b) $b_r = 0.4$

Fig. 10. FPGA-based experimental chaotic attractor: (a) $b_r = 0.1$; (b) $b_r = 0.4$.

在基于 FPGA 的设计过程中, 采用 Verilog 硬件描述语言实现算法编码. 为确保精度, 使用包含 1 位符号位、6 位整数位和 25 位小数位的 32 位定点小数格式. 为计算系统中的三角函数与指数项, 采用 CORDIC 算法——该算法通过旋转模式 (计算三角函数) 和双曲模式 (计算指数函数) 协同工作. 其迭代过程定义如下:

$$\begin{cases} u_{i+1} = u_i - \mu\sigma_i v_i 2^{-i}, \\ v_{i+1} = v_i + \sigma_i u_i 2^{-i}, \\ w_{i+1} = w_i - \sigma_i T_i, \end{cases} \quad (5)$$

其中 $\sigma_i = \text{sign}(w_i)$ 决定旋转或双曲缩放方向 ($\mu = 1$ 时用于三角计算, $\mu = -1$ 时用于指数计算), T_i 表示基本角步长——旋转模式下 $T_i = \arctan(2^{-i})$, 双曲模式下 $T_i = \text{arctanh}(2^{-i})$. 为提升计算效率, 基本角步长 T_i 均预计算并存储于查找表 (LUT) 中. 对于三角函数, 最终输出结果为 $\cos(\theta) \approx u_N K_1$ 和 $\sin(\theta) \approx v_N K_1$, 其中 $K_1 = \prod_{i=0}^{N_1} \sqrt{1 + 2^{-2i}}$ 为旋转模式缩放因子; 指数计算最终结果为 $e^z \approx (u_N + v_N) K_2$, 其中 $K_2 = \prod_{i \in S} \sqrt{1 - 2^{-2i}}$ 为双曲模式缩放因子 (S 为选定索引集合).

基于 FPGA 的实验混沌吸引子如图 10 所示 (状态变量初始条件设为 $z_0^r = z_0^i = y_0 = 0.1$, 参数

配置为 $a = 0.2$, $b_1 = 0.1$). 通过示波器采集的 $y-z^r$ 平面硬件相轨迹观测结果与图 5 数值仿真结果高度一致, 这些实验结果既证明了基于 FPGA 数字化实现的可行性与简易性, 也验证了数学模型的正确性.

为评估基于 FPGA 的硬件实现与双精度浮点数仿真之间的一致性, 本文对系统状态变量 (z^r , z^i , y) 的输出误差进行了统计分析. 如图 11 所示, 我们从多个角度对误差分布进行了量化评估. 如图 11(a) 的箱线图显示 3 个变量的误差分布较为集中, 中位数误差与均值接近, 表明误差分布相对对称. 图 11(b) 中的累积分布函数表明, 变量 z^r 和 z^i 约为 90% 的误差样本小于 8×10^{-4} , 表明误差分布具有较好的收敛性. 误差指标对比柱状图如图 11(c), 图中清晰地展示了 3 个状态变量在不同误差指标下的表现. 可以看到, 3 个变量的 MAE, RMSE 和最大误差都维持在相近的数量级, 且 RMSE 值均略大于相应的 MAE 值, 这表明误差分布中存在少量较大误差值, 但整体控制良好. 最大误差均不超过 1.24×10^{-3} , 进一步证明了 FPGA 实现的稳定性. 图 11(d) 进一步证实了误差主要集中在较小的范围内. 同时基于 Kolmogorov-Smirnov

检验的结果显示, 3 个维度的 p 值均大于 0.05(分别为 0.145, 0.356 和 0.131), 无法拒绝两个序列来自同一分布的假设 [35-37]. 这表明 FPGA 实现的混沌序列虽然在数值精度上同双精度仿真相比有些许误差, 但其完整地保持了混沌序列的统计分析特性, 为硬件实现混沌系统在信息安全领域提供了可靠保证.

4 基于复混沌序列的双图像加密系统

双图像加密机制的核心优势在于其内在的交叉混淆特性. 两幅图像在加密过程中相互充当动态随机源, 其像素间的非线性融合能更彻底地破坏各自的统计特征. 这不仅增强了对抗统计分析的能力, 更等效于扩大了系统的有效密钥空间, 从而显著提升了安全性. 本文所提出的系统 (4) 具有对初始条件和控制参数的高度敏感性, 可以为加密系统提供巨大的密钥空间, 确保微小的密钥偏差即可导致解密失败 [38-40]. 同时由该混沌系统产生的混沌序列展现出良好的伪随机性和遍历性, 可以在加密过程中有效破坏明文图像的统计特征. 此外, 系统在相空间中展现的复杂吸引子结构, 反映了其动力

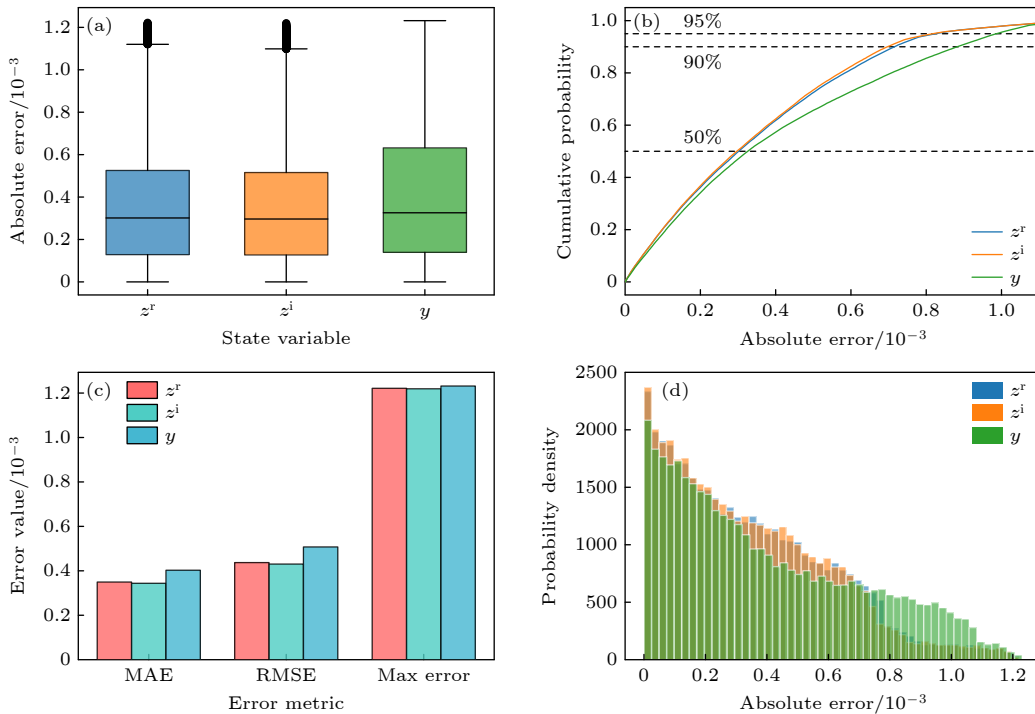


图 11 基于 FPGA 产生混沌序列与数值仿真之间的误差统计 (a) 绝对误差分布; (b) 绝对误差累积分布函数; (c) 误差指标对比; (d) 绝对误差分布直方图

Fig. 11. Error statistics between FPGA-generated chaotic sequence and numerical simulation: (a) Absolute error distribution; (b) cumulative distribution function of absolute errors; (c) comparison of error metrics; (d) histogram of absolute error distribution.

学行为而的复杂性,可以保证所生成的密钥流具有低可预测性.因此,本文提出的系统为视觉数据提供安全高效的保护方案.基于此本文提出了一种新型双图像加密系统(结构如图12所示):该系统将两幅原始图像表示为复数数据的实部与虚部,记作 I ;在复值混沌系统 MCVGM 生成的混沌伪随机数驱动下,加密系统同步执行像素位置与像素值的联合操作,最终将图像转换为类噪声数据 C .具体流程可通过以下步骤描述:

步骤 1 过程始于双图像复数数据预处理.将两幅尺寸为 $M \times N$ 的灰度图像(分别记为 I_r 和 I_i)像素值归一化至 $[0, 1]$ 范围,继而组合成复矩阵 $I = I_r + iI_i$.

步骤 2 设置 MCVGM 参数与初始条件.对 MCVGM 进行 N_0 次预迭代以消除瞬态效应,随后继续迭代 $M \times N$ 次(M 和 N 由复值数据 I 的行列尺寸确定).迭代过程中生成伪随机序列 K_1 , K_2 和 K_3 ,分别用于像素位置置乱与像素值扩散.其中置乱序列 K_1 通过对忆阻状态混沌序列 y 排序拼接获得,具体计算方式为

$$K_1 = [\text{sort}(y(1 : M)) || \text{sort}(y(M + 1 : M + N))], \quad (6)$$

其中 $||$ 表示向量拼接操作.用于与置乱数据执行复值乘法的伪随机序列 K_2 通过对复值混沌序列 z 缩放生成:

$$K_2 = (d_r + id_i) + 0.5z. \quad (7)$$

此处 d_r 和 d_i 为预设系数,缩放操作旨在为后续复值乘法运算提供最佳动态范围.序列 K_3 是尺寸为 $M \times N$ 的复值矩阵,其虚部与实部均约束在 $[0, 255]$ 范围内,通过以下方式计算:

$$K_3^r = \text{mod}(\text{floor}((z_r + 1) \times 10^{12}), 256),$$

$$K_3^i = \text{mod}(\text{floor}((z_i + 1) \times 10^{12}), 256), \quad (8)$$

其中 $K_3 = K_3^r + iK_3^i$.

步骤 3 复值矩阵 I 通过两阶段置乱过程使用序列 K_1 进行位置置乱.先对行元素操作,再对列元素处理.所得密文数据 P 计算公式如下:

$$P^t = I(K_1^m(m), n),$$

$$P = P^t(m, K_1^n(n)), \quad (9)$$

其中 P^t 表示对矩阵 I 执行行置乱后的中间结果, K_1^m 和 K_1^n 分别表示从 K_1 的前 M 个元素和剩余 N 个元素提取的行、列置换索引.矩阵 I 的每个元素 $I(m, n)$ 都是一个复数,其实部和虚部分别源自

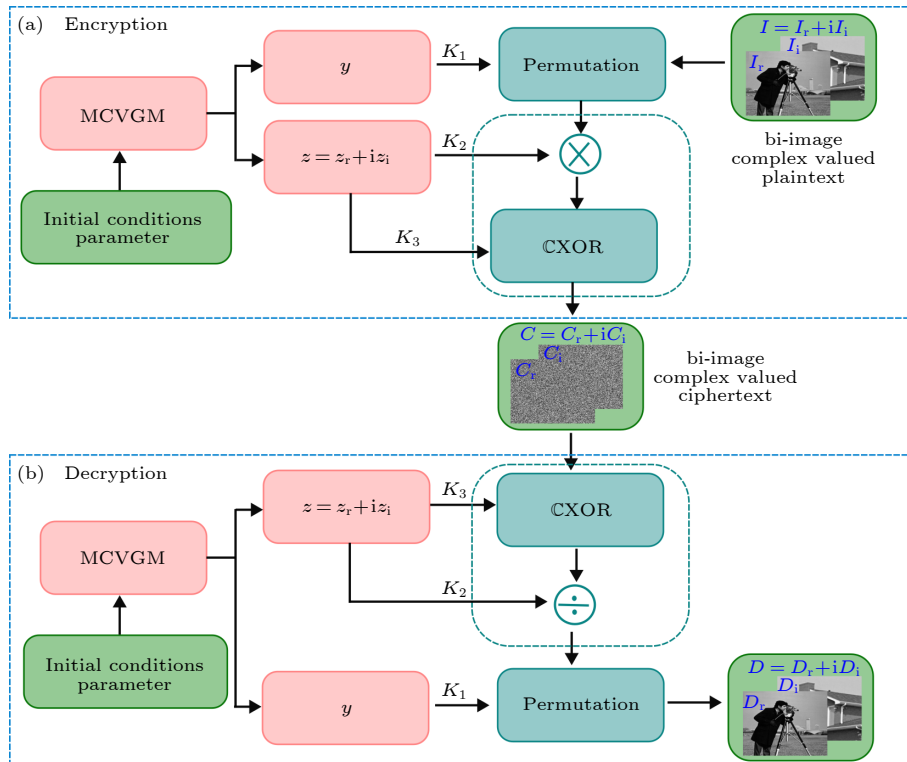


图 12 双图像复值加密系统流程图

Fig. 12. Flowchart of the dual-image complex-valued encryption system.

不同的明文图像. 矩阵 I 元素位置的重排列意味着隶属于同一复数的实部和虚部 (即两幅图像的配对像素) 在置乱过程中始终保持绑定关系, 经历完全一致的坐标变换. 因此, 通过单次对复数矩阵 I 的置换操作, 即可同步完成两幅图像所有像素位置的关联置乱.

步骤 4 通过置乱数据 P 与伪随机序列 K_2 之间的复值乘法运算修改像素值, 变换后的数据 Q 由下式获得:

$$Q = P \otimes K_2. \quad (10)$$

此处 \otimes 表示逐元素复值乘法运算. 该运算在矩阵的每个对应位置 (m, n) 上对立执行标准复数乘法. 令 $P(m, n) = p_r + ip_i$ 和 $K_2(m, n) = k_r^2 + ik_i^2$, 则输出 $Q(m, n)$ 的实部 q_r 和虚部 q_i 表示为

$$\begin{aligned} q_r &= p_r \cdot k_r^2 - p_i \cdot k_i^2, \\ q_i &= p_r \cdot k_i^2 + p_i \cdot k_r^2. \end{aligned} \quad (11)$$

此过程对每个复数元素的实部与虚部进行交叉融合, 实现了像素值的非线性变换, 从而完成两幅图像的信息同步扩散.

步骤 5 完成复值乘法像素值扩散后, 将 Q 的实部与虚部缩放为 8 位整数. 随后通过复值按位异或 (CXOR) 运算与 K_3 进行进一步像素值扩散, 其定义为

$$C = Q \text{CXOR} K_3 = (Q^r \oplus K_3^r) + i(Q^i \oplus K_3^i), \quad (12)$$

其中, \oplus 表示逐元素异或操作. 在该复值按位异或运算中, 将一个复数 $Q(m, n) = q_r + iq_i$ 与 $K_3(m, n) = k_r^3 + ik_i^3$ 的运算解耦为对实部通道和虚部通道的并行且独立操作, 即

$$\begin{aligned} C_r &= q_r \oplus k_r^3, \\ C_i &= q_i \oplus k_i^3. \end{aligned} \quad (13)$$

最终结果为 $C = (q_r \oplus k_r^3) + i(q_i \oplus k_i^3)$. 此操作以极低的计算复杂度, 高效地破坏了前后像素值间的线性关系, 实现了对两幅图像像素值的最终混淆.

经过上述像素位置置乱、基于复值乘法的像素值扩散以及基于 CXOR 的像素值扩散后, 最终获得密文图像 C . 解密过程完全逆序执行加密操作: 首先对密文图像执行与伪随机矩阵 K_3 的 CXOR 运算; 随后将数据归一化至 $[0, 1]$ 范围; 接着使用复值矩阵 K_2 对数据进行复除法运算以逆转先前乘法步骤; 最后利用序列 K_1 实施逆置换恢复原始像素位

置, 从而重建解密后的双图像 D .

在 MATLAB 2024a 环境中对所设计的加密系统进行数值仿真以评估所提加密方案的性能. 混沌系统参数配置为 $a = 0.2$, $b = 0.1 + 0.1i$, 初始条件设为 $z_0 = 0.1 + 0.1i$ 和 $y_0 = 0.1$. 为消除瞬态效应进行 $N_0 = 1000$ 次预迭代, 生成 K_2 所用的复值缩放因子设置为 $d = 5 + 0.5i$. 实验采用标准 256×256 灰度测试图像构建复值矩阵: 通过随机组合构建 4 组不同的复图像对 (I_1 — I_4)——分别将 Cameraman, Pepper, Butterfly 和 Parrot 图像设为实部, House, Starfish, Aircraft 和 Lena 图像作为对应虚部. 接下来对该加密系统从像素直方图、密钥空间、密钥敏感性等多个方面进行性能分析.

1) 像素直方图分析 图像像素值分布是关键特征, 而直方图是可视化该特征的重要工具. 有效的加密方案应产生具有近乎均匀像素分布的密文图像, 以增强抗统计攻击能力. 如图 13 所示, 加密双图像的直方图中红色曲线代表实部, 绿色曲线对应虚部. 统计分析证实两部分均呈现近似均匀分布, 表明该加密算法有效掩盖了统计模式, 从而增强了抗统计密码分析的安全性.

2) 密钥空间分析 为抵抗暴力攻击, 加密方案必须具有足够大的密钥空间. 本复值双图像加密方案中, 参数 a , b_r , b_i 及初始条件 z_{r0} , z_{i0} 和 y_0 共同构成随机序列生成的密钥. 假设浮点数据精度为 10^{16} , 总密钥空间计算为 $(10^{16})^6 = 10^{96} \approx 2^{318}$. 该值显著超过公认安全阈值 2^{100} , 表明该密码系统具有强大的抗暴力攻击能力.

3) 密钥敏感性分析 密钥敏感性原则要求密钥的微小变化应导致解密图像无法呈现原始明文的任何可识别信息. 图 14 所示的仿真结果对比了使用正确密钥的成功解密与初始条件 z_0 存在微小扰动 (10^{-16}) 时的失败解密尝试, 证实即使密钥发生极小变化也无法从密文图像恢复原始图像, 从而证明了该密码系统的高密钥敏感性.

4) 像素相关性分析 相邻像素的相关系数可通过下式计算:

$$\rho_{xy} = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}}, \quad (14)$$

其中 $E(x) = \frac{1}{N} \sum_{i=1}^N x_i$, $E(y) = \frac{1}{N} \sum_{i=1}^N y_i$. 典型

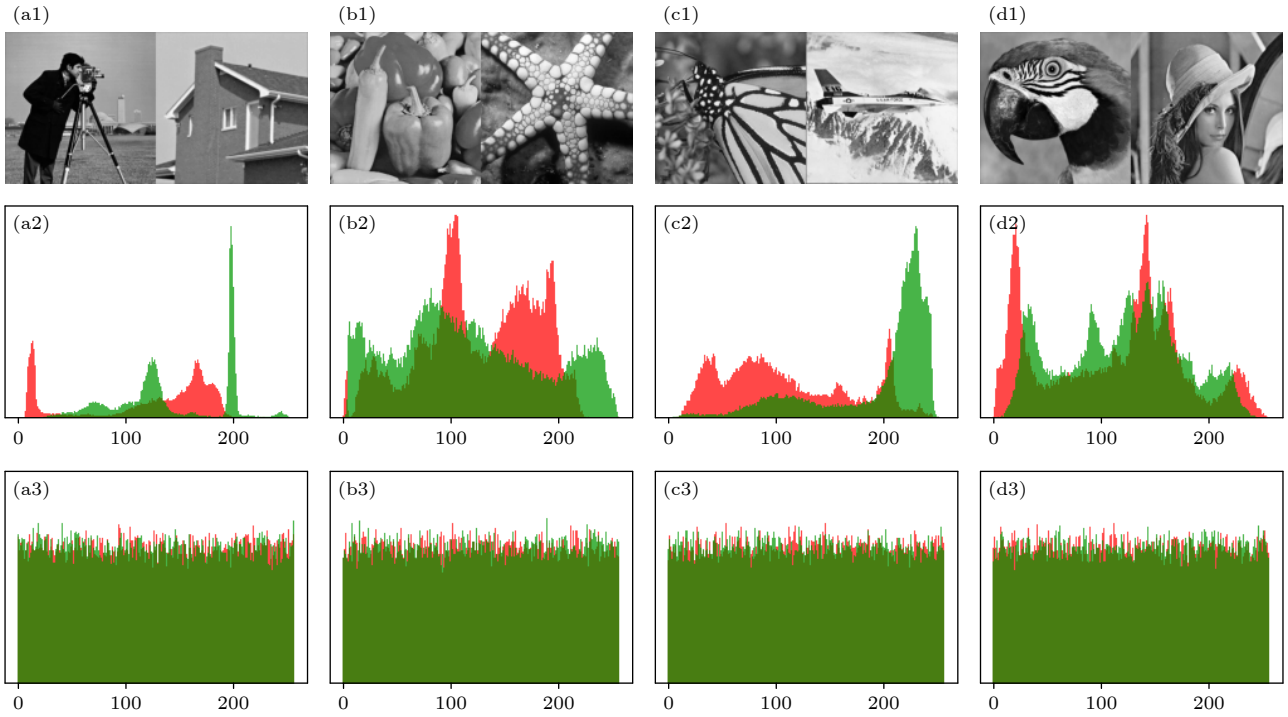


图 13 像素直方图测试 (a1)–(d1) 原始图像; (a2)–(d2) 原始图像的像素直方图; (a3)–(d3) 加密图像的像素直方图
 Fig. 13. Histogram test of cryptosystem: (a1)–(d1) Original image; (a2)–(d2) histogram of original image; (a3)–(d3) histogram of encrypted image.

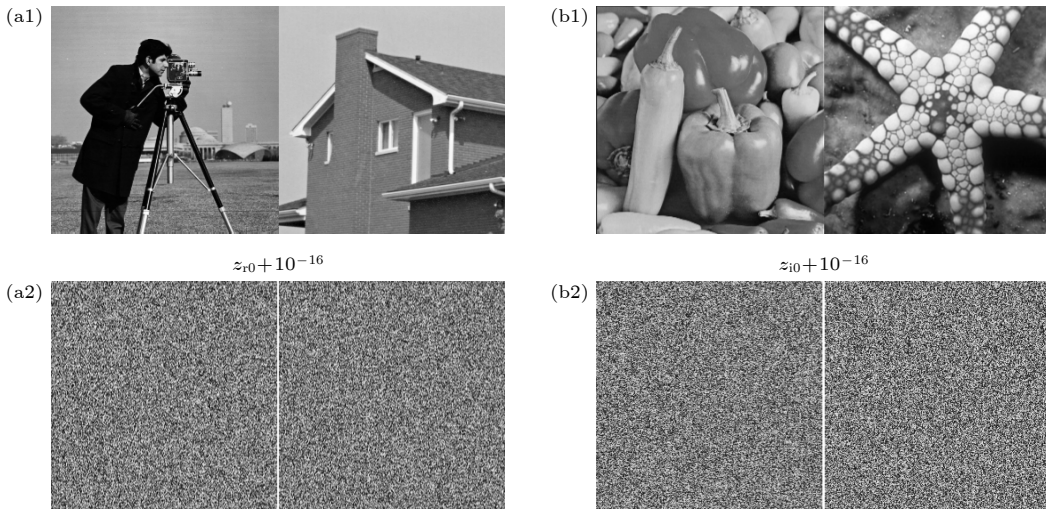


图 14 解密结果 (a1), (b1) 使用正确密钥得到的还原图像; (a2), (b2) 初始条件 z_0 仅有微小偏差时的解密图像
 Fig. 14. Decrypted images: (a1), (b1) With correct secret keys; (a2), (b2) with tiny variation in the initial condition z_0 .

明文图像中, 相邻像素在所有空间方向上均呈现高相关系数 (常接近 1), 而安全加密方案应显著降低此类相关性, 使密文图像相关系数趋近于零. 例如图 15 展示了原始图像 I_1 与其加密图像的相关性分布: 图中红色表示加密图像实部, 绿色表示虚部. 显然加密后任意方向上相邻像素间均无显著相关性, 证实了加密算法在消除像素关联性方面的有效性.

表 1 汇总了加密前后相关系数的计算结果. 可

以明显看出: 原始图像的相关系数接近 1, 而加密图像的系数趋近于 0, 这表明该方案在消除相邻像素相关性方面具有优异性能.

5) 信息熵分析 信息熵是量化信号源不确定性及测量其平均信息量的基本指标. 对于 8 位灰度图像, 信息熵定义为

$$H = - \sum_{i=0}^{255} p(x_i) \log_2(p(x_i)), \quad (15)$$

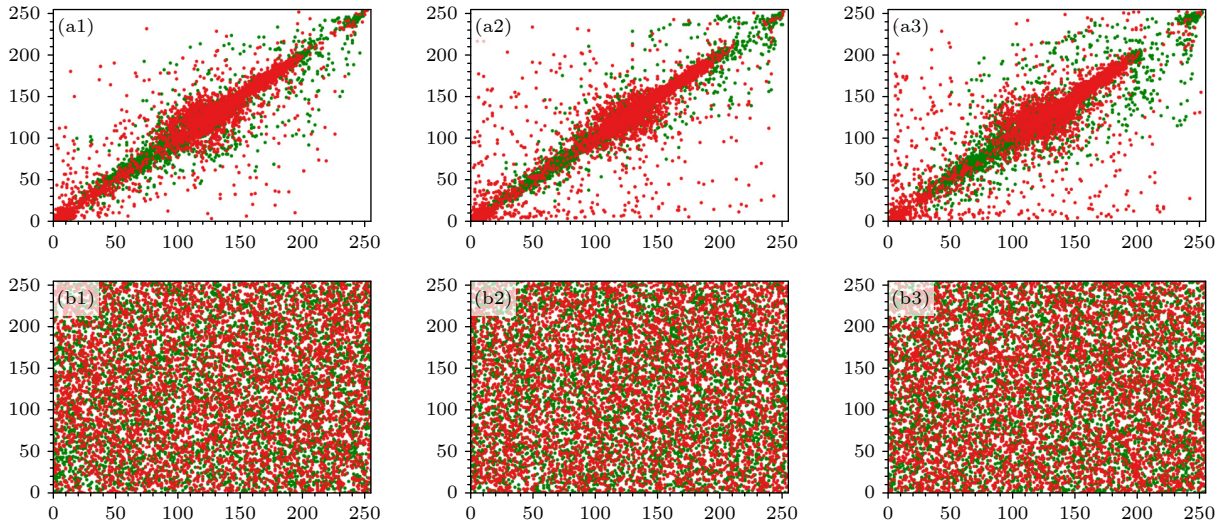


图 15 图像的像素相关性分布 (a1) 水平方向, (a2) 垂直方向, (a3) 对角方向的原始图像; (b1) 水平方向, (b2) 垂直方向, (b3) 对角方向的加密图像

Fig. 15. Distribution of pixel correlations in images: Original image in (a1) horizontal direction, (a2) vertical direction, (a3) diagonal direction; encrypted image in (b1) horizontal direction, (b2) vertical direction, (b3) diagonal direction.

表 1 原始图像和加密图像的相关性系数

Table 1. Correlation coefficients of original and encrypted images.

图像	原始图像	原始图像			加密图像		
		H	V	D	H	V	D
I1	Cameraman	0.9576	0.9259	0.9147	0.0015	0.0027	-0.0034
	House	0.9669	0.9460	0.9779	0.0012	-0.0021	0.0011
I2	Pepper	0.9439	0.9585	0.9106	-0.0092	0.0071	-0.0099
	Starfish	0.9630	0.9357	0.8983	-0.0016	0.0037	-0.0055
I3	Butterfly	0.9310	0.9388	0.9017	0.0080	-0.0011	0.0008
	Aircraft	0.9037	0.9122	0.8427	0.0023	-0.0088	0.0014
I4	Parrot	0.9406	0.9532	0.9199	0.0037	0.0093	-0.0074
	Lena	0.9716	0.9437	0.9240	0.0019	-0.0010	0.0092

其中 $p(x_i)$ 表示像素 x_i 在图像中出现的概率. 有效的加密算法应使密文图像熵值接近理想值 8, 表明其具有高随机性与不可预测性. 表 2 对比了原始明文图像与加密图像的信息熵, 结果表明所设计的加密方案显著提升了原始图像的熵值, 使其接近类随机图像水平, 从而增强了抗统计攻击的安全性.

表 2 原始图像和加密图像的信息熵

Table 2. Information entropy of original and encrypted images.

图像	原始图像	加密图像	
I1	Cameraman	7.0875	7.9987
	House	6.7152	7.9989
I2	Pepper	7.5498	7.9983
	Starfish	7.6959	7.9979
I3	Butterfly	7.6420	7.9991
	Aircraft	6.9593	7.9989
I4	Parrot	7.6624	7.9986
	Lena	7.6591	7.9979

6) 数据丢失与噪声攻击分析 数字图像在传输过程中常易受噪声干扰与部分数据丢失的影响, 因此理想的图像加密方案应对此类扰动具有强鲁棒性, 确保在噪声或损坏条件下仍能实现可靠解密. 为评估鲁棒性, 对密文图像 I_1 进行了 30% 区域数据丢失和 30% 强度的椒盐噪声测试, 结果如图 16 所示. 尽管解密图像部分像素值发生变化, 但原始明文的基本内容仍保持视觉可识别性. 这些结果证实: 即使存在显著数据丢失与噪声污染, 所提加密方法仍能保持令人满意的解密质量与结构可恢复性.

为了评估本加密方案的安全性, 我们将其在密钥空间、密钥敏感性、信息熵以及相邻像素相关性的指标上同近期发表文献进行对比, 结果如表 3 所示. 综合分析表明, 本方案在多个指标维度上展现出显著优势. 在抗暴力攻击方面, 本方案的密钥空

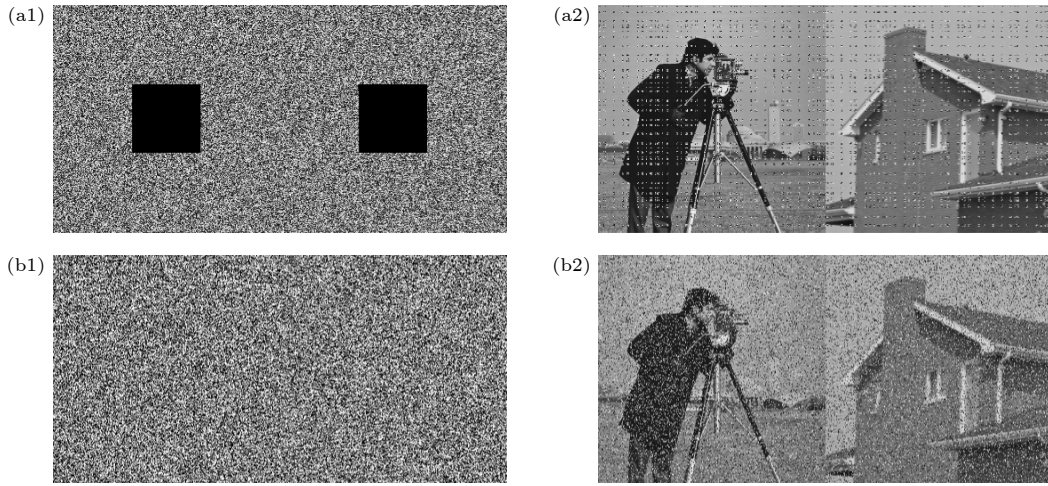


图 16 数据丢失与噪声攻击测试结果 (a1) 图像 I_1 密文遭受 30% 数据丢失后的图像; (a2) 从数据丢失后的密文恢复出的图像; (b1) 图像 I_1 密文添加强度为 30% 的椒盐噪声后的图像; (b2) 从被添加噪声后的密文中恢复的图像

Fig. 16. Test results of data loss and noise attacks: (a1) Ciphertext images of I_1 with 30% loss; (a2) recovered images from ciphertext after data loss; (b1) ciphertext images of I_1 with 30% intensity of pepper and salt noise; (b2) recovered images from the ciphertext after adding noise.

间为 2^{318} 虽低于文献 [41], 但已远超出计算安全阈值, 并显著高于文献 [42, 43], 具备抵御暴力攻击的充足能力. 在系统敏感性方面, 本方案的密钥灵敏度为 10^{-16} 优于对比文献, 这得益于复值混沌系统对初始条件极微小的变化也极为灵敏. 在统计特性方面, 本方案加密图像的信息熵相较于对比文献更接近于理想值, 表明其密文像素分布具有更好的随机效果. 同时, 其像素相关性系数优于多数对比方案, 印证了所提出复值混沌序列在破坏图像统计特性上的高效性. 综上所述, 这些量化对比有力地证明了本方案在密钥敏感性、统计随机性等关键指标上的优势.

表 3 与现有加密方案安全性能对比

Table 3. Comparison of security performance with existing encryption schemes.

安全指标	文献[42]	文献[43]	文献[41]	本文
密钥空间	2^{256}	2^{260}	2^{627}	2^{318}
密钥敏感性	—	10^{-13}	10^{-14}	10^{-16}
信息熵	7.9944	7.9969	7.9915	7.9979
相关性系数	0.0011	0.0043	0.0118	0.0040

5 总结与展望

本文提出并分析了一种新型离散忆阻复值高斯映射, 以填补复域离散忆阻混沌系统研究空白. 通过引入由复变量幅值驱动的离散忆阻器, 所构建系统展现出显著增强的复杂混沌动力学特性, 该特性

通过李雅普诺夫指数谱、分岔图和相轨迹等数值分析得到全面验证. 所提出的 MCVGM 系统在 FPGA 平台上成功进行了数字化实现, 证实了其硬件应用的可行性. 基于复数运算固有特性, 进一步设计了一种安全高效的双图像加密方案: 通过将两幅图像视为复矩阵的实部与虚部, 并采用复值混沌序列实现同步置乱与扩散, 该方案展现出优异的加密性能. 结果表明, 所提出的基于 MCVGM 的加密框架具有强安全性、高敏感度和抗攻击能力, 为现代图像加密需求提供了有前景的解决方案. 本文虽然为复数域忆阻混沌系统的设计与实现奠定了基础, 但基于现有成果仍有可深入探索的研究. 在系统构建层面, 可将本文中的单忆阻器扩展为包含多个忆阻器或忆阻器与其他经典混沌映射的高维架构, 从而进一步提升系统的动力学复杂特性. 在此基础上, 开发硬件友好的轻量化混沌加密方案, 节约资源消耗, 并探索其在物联网等领域的应用.

参考文献

- [1] Zhou S, Yin Y L, Wang S Y, Zhang Y Q 2024 *Acta Phys. Sin.* **73** 210501 (in Chinese) [周双, 尹彦力, 王诗雨, 张盈谦 2024 *物理学报* **73** 210501]
- [2] Bao H, Wang R M, Tang H G, Chen M, Bao B C 2025 *IEEE Internet Things J.* **12** 20902
- [3] Deng Q L, Wang C H, Sun Y C, Yang G 2025 *IEEE Trans. Cybern.* **55** 3926
- [4] Lai Q, Wang J, Huang D X 2025 *Acta Phys. Sin.* **74** 200501 (in Chinese) [赖强, 王君, 黄大勋 2025 *物理学报* **74** 200501]
- [5] Deng Q L, Wang C H, Yang G, Luo D W 2025 *IEEE Internet*

- Things J.* **12** 25559
- [6] Yu F, He S Q, Yao W, Cai S, Xu Q 2025 *IEEE Trans. Comput. Aid. Des.* **44** 1
- [7] Zhou L L, Lin Z Q, Tan F, Chen P Y 2025 *Expert Syst. Appl.* **281** 127475
- [8] Luo D W, Wang C H, Liang J H, Deng Q L 2025 *Nonlinear Dyn.* **113** 29983
- [9] Chen W, Wang Y C, Shi C, Shen G L, Li M Y, Liu Y, Hei X H 2025 *Neural Netw.* **191** 107799
- [10] Li H D, Min F H 2025 *IEEE Int. Things J.* **12** 29018
- [11] Bao H, Fan Z, Hua Z Y, Zhang Y Z, Xu Q, Bao B C 2025 *Expert Syst. Appl.* **290** 128448
- [12] Wang X, Du J R, Li Z J, Ma M L, Li C L 2024 *Acta Phys. Sin.* **73** 110503 (in Chinese) [王璇, 杜健嵘, 李志军, 马铭磷, 李春来 2024 物理学报 **73** 110503]
- [13] Yu F, Tan B H, He T, He S Q, Huang Y Y, Cai S, Lin H R 2025 *Mathematics* **13** 726
- [14] Zhang Y X, Hua Z Y, Bao H, Huang H J 2024 *IEEE Trans. Circuits Syst. I* **71** 2783
- [15] Hua Z Y, Yao J H, Zhang Y X, Bao H, Yi S 2025 *IEEE Trans. Ind. Inf.* **21** 85
- [16] Yao J H, Zhang Y X, Bao H, Hua Z Y 2025 *Chaos Soliton. Fract.* **197** 116453
- [17] Rani M, Agarwal R 2009 *Chaos Soliton. Fract.* **42** 447
- [18] Ayubi P, Barani M J, Valandar M Y, Irani B Y, Sadigh R S M 2021 *Artif. Intell. Rev.* **54** 1237
- [19] Yu Y J, Ren S G, Yang L, Li Y, Miao X S 2025 *Sci. China Inf. Sci.* **68** 139402
- [20] Deng Q L, Wang C H, Sun Y C, Xu C, Lin H R, Deng Z K 2025 *IEEE Trans. Comput. Aid. Des.* **44** 4701
- [21] Zhang X, Li C B, Moroz I, Huang K, Liu Z H 2025 *Nonlinear Dyn.* **113** 15487
- [22] Bao H, Fan J H, Hua Z Y, Xu Q, Bao B C 2025 *IEEE Internet Things J.* **12** 31843
- [23] Gao S, Ho-Ching-Iu H, Erkan U, Simsek C, Toktas A, Cao Y H, Wu R, Mou J, Li Q, Wang C P 2025 *IEEE Trans. Circuits Syst. Video Technol.* **35** 7706
- [24] Al Qurashi M, Asif Q U A, Chu Y M, Rashid S, Elagan S K 2023 *Results Phys.* **51** 106627
- [25] Almatroud A O, Grassi G, Khennaoui A A, Abbes A, Onanmas A, Alshammari S, Albosaily S 2024 *Alexandria Eng. J.* **93** 1
- [26] Li H D, Min F H 2025 *IEEE Trans. Circuits Syst. I* **72** 4820
- [27] Wang C H, Li Y F, Yang G, Deng Q L 2025 *Mathematics* **13** 1600
- [28] Yu F, Zhang S K, Su D, Wu Y Y, Yumba Musoya G, Yin H G 2025 *Fractal Fractional* **9** 115
- [29] Deng Q L, Wang C H, Sun Y C, Yang G 2025 *IEEE Trans. Circuits Syst. I* **72** 300
- [30] Luo D W, Wang C H, Deng Q L, Yang G 2025 *Nonlinear Dyn.* **113** 28381
- [31] Fan C L, Ding Q 2025 *Chaos Soliton. Fract.* **191** 115905
- [32] Zhang S, He D Z, Li Y X, Lu D R, Li C B 2025 *IEEE Trans. Autom. Sci. Eng.* **22** 17828
- [33] Yu F, Su D, He S Q, Wu Y Y, Zhang S K, Yin H G 2025 *Chin. Phys. B* **34** 050502
- [34] Zhang H W, Fu C L, Pan Z P, Ding D W, Wang J, Yang Z L, Liu T 2024 *Acta Phys. Sin.* **73** 180501 (in Chinese) [张红伟, 付常磊, 潘志鹏, 丁大为, 王金, 杨宗立, 刘涛 2024 物理学报 **73** 180501]
- [35] Lai Q, Qin M H 2025 *J. Electron. Inf. Technol.* **47** 3262 (in Chinese) [赖强, 秦铭宏 2025 电子信息学报 **47** 3262]
- [36] Lai Q, Qin M H 2025 *J. Guizhou Norm. Univ. (Nat. Sci.)* **43** 1 (in Chinese) [赖强, 秦铭宏 2025 贵州师范大学学报(自然科学版) **43** 1]
- [37] Lai Q, Wang J 2024 *Acta Phys. Sin.* **73** 180503 (in Chinese) [赖强, 王君 2024 物理学报 **73** 180503]
- [38] Yu F, Yumba Musoya G, Guo R, Ying Z, Xu J, Yao W, Jin J, Lin H 2025 *Axioms* **14** 638
- [39] Zhao Q H, Bao H, Zhang X, Wu H G, Bao B C 2024 *Chaos Soliton. Fract.* **182** 114769
- [40] An X L, Liu S Y, Li X, Zhang J G, Li X Y 2024 *Expert Syst. Appl.* **243** 122899
- [41] An T, Gao T, Chen T, Jiang D 2025 *Complex Intell. Syst.* **11** 319
- [42] Zhong Y M, Lai Q, Zhu C K, Qin M H 2026 *Comput. Stand. Interfaces* **95** 104051
- [43] Zhao Y, Zheng M, Zhang Y, Yuan M, Zhou H 2024 *Nonlinear Dyn.* **112** 19515

Discrete memristor-based complex-valued chaotic system dynamic analysis and its application in dual-image encryption*

DENG Quanli¹⁾ WANG Chunhua^{1)2)†} YANG Gang¹⁾

1) (*College of Information Science and Engineering, Hunan University, Changsha 410082, China*)

2) (*Greater Bay Area Institute for Innovation, Hunan University, Guangzhou 511300, China*)

(Received 10 September 2025; revised manuscript received 13 October 2025)

Abstract

The exploration of complex-valued chaos not only provides a feasible approach for practical applications such as image encryption, but also has great potential in simulating wave phenomena and quantum inspired process. In order to bridge it with nonlinear circuit components, we introduce a novel complex-valued chaotic system by embedding a discrete memristor into a complex Gaussian map. The memristor, a component with inherent physical memory, is uniquely driven by the modulus of the complex state variable, which is a key physical quantity often related to energy or amplitude in wave systems. This coupling induces complex nonlinear dynamics, which are physically characterized through Lyapunov exponents and bifurcation analysis, revealing an enhanced and more robust chaotic regime. The physical feasibility of this system is demonstrated by its successful hardware realization on an FPGA platform. To demonstrate its potential applications, we leverage the complex chaotic flows of the system to engineer a dual-image encryption scheme, where the encryption process is explained as a physical diffusion and scrambling of information represented by a complex matrix. Our results verify that this approach not only yields a cryptosystem with high security but also provides a link between complex chaos and information security applications.

Keywords: discrete memristor, complex-valued chaos, FPGA implementation, dual-image encryption

DOI: [10.7498/aps.75.20251242](https://doi.org/10.7498/aps.75.20251242)

CSTR: [32037.14.aps.75.20251242](https://cstr.cn/32037.14.aps.75.20251242)

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62571183, 62271197) and the Basic and Applied Basic Research Foundation of Guangdong Province, China (Grant No. 2024A1515011910).

† Corresponding author. E-mail: wch1227164@hnu.edu.cn



基于离散忆阻器的复值混沌系统动力学分析及其在双图像加密中的应用

邓全利 王春华 杨港

Discrete memristor-based complex-valued chaotic system dynamic analysis and its application in dual-image encryption

DENG Quanli WANG Chunhua YANG Gang

引用信息 Citation: *Acta Physica Sinica*, 75, 010003 (2026) DOI: 10.7498/aps.75.20251242

CSTR: 32037.14.aps.75.20251242

在线阅读 View online: <https://doi.org/10.7498/aps.75.20251242>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

离散忆阻混沌系统的Simulink建模及其动力学特性分析

Simulink modeling and dynamic characteristics of discrete memristor chaotic system

物理学报. 2022, 71(3): 030501 <https://doi.org/10.7498/aps.71.20211549>

一个具有超级多稳定性的忆阻混沌系统的分析与FPGA实现

Analysis and FPGA implementation of memristor chaotic system with extreme multistability

物理学报. 2022, 71(24): 240502 <https://doi.org/10.7498/aps.71.20221423>

基于深度学习的新混沌信号及其在图像加密中的应用

A new chaotic signal based on deep learning and its application in image encryption

物理学报. 2021, 70(23): 230502 <https://doi.org/10.7498/aps.70.20210561>

具有多种共存现象的新型忆阻混沌系统的周期轨道分析及DSP实现

Periodic orbit analysis and DSP implementation of a novel memristor-based chaotic system with multiple coexisting phenomena

物理学报. 2025, 74(24): 240502 <https://doi.org/10.7498/aps.74.20251102>

n 维离散超混沌系统及其在音频加密中的应用

An n -dimensional discrete hyperchaotic system and its application in audio encryption

物理学报. 2024, 73(21): 210501 <https://doi.org/10.7498/aps.73.20241028>

分数阶忆阻Henon映射的可控多稳定性及其视频加密应用

Controllable multistability of fractional-order memristive Henon map and its application in video encryption

物理学报. 2024, 73(18): 180501 <https://doi.org/10.7498/aps.73.20240942>