齐鲁工业大学学报 第40卷 第4期 2026年8月出版
JOURNAL OF QILU UNIVERSITY OF TECHNOLOGY Vol.40 No.4 Aug.2026
DOI:10.16442/j.cnki.qlgydxxb.2026.04.005 【机电与信息工程】

基于忆阻器的复 Lorenz 系统及其在图像加密的应用

孙文靓,郑洪晖,刘 赛,庄新晨,姜翠美*
齐鲁工业大学(山东省科学院) 数学与统计学院,山东 济南 250353

摘要:基于三次非线性忆阻器,本文建立了一个新的复混沌系统,通过耗散性、初值敏感性、平衡点的稳定性研究、分岔图、Lyapunov 指数谱、时序图、相图等数值仿真以及 0-1 测试进行了动力学分析,证明了忆阻复 Lorenz 系统有优越的混沌特性,可为加密应用提供增强的安全保障。利用新系统生成的混沌时间序列,本文采用置乱-扩散算法对灰色图像进行加密。通过对加密方案的安全性分析,本文得出以下结论:本方案采用的密钥空间设计满足密码学安全需求,加密后图像灰度直方图呈现均匀分布特征,相邻像素间的相关系数显著降低趋近于零,信息熵接近于理论最大值 8,系统对差分攻击具有强鲁棒性。

关键词:忆阻器;复混沌系统;动力学分析;图像加密;加密算法
中图分类号:O174 **文献标志码**:A **文章编号**:2097-2792(2026)04-38-14

Memristor-based complex Lorenz system and its application in image encryption

SUN Wenjing, ZHENG Honghui, LIU Sai, ZHUANG Xinchen, JIANG Cuimei*
School of Mathematics and Statistics, Qilu University of Technology
(Shandong Academy of Sciences), Jinan 250353, China

Abstract: Based on a cubic nonlinear memristor, a novel complex chaotic system is proposed. Through dynamical analysis including dissipativity, sensitivity to initial conditions, stability of equilibrium points, bifurcation diagrams, Lyapunov exponent spectra, time series, phase portraits, and 0-1 tests, it is demonstrated that superior chaotic characteristics are exhibited by the memristive complex Lorenz system, which provides enhanced security for cryptographic applications. The encryptionof grayscale images isperformedusing a novel scrambling-diffusionalgorithmthat harnesses the chaotic time series producedby aninnovative system. Through security analysis of the image encryption scheme, the following conclusions are obtained: the key space designadoptedinthis scheme isdesignedtomeet cryptographic securityrequirements; the histogram of the encrypted image exhibits a uniform distribution; the correlation coefficients between adjacent pixels are significantly reduced and approach zero; the information entropy is close to the theoretical maximum of 8; and the system demonstrates strong robustness against differential attacks.

Key words: memristor; complex chaotic systems; dynamical analysis; image encryption; encryption algorithm

收稿日期:2025-06-01 **网络出版时间**:2026-08-31
基金项目:山东省中小企业创新能力提升项目(2024TSGC0645)
作者简介:孙文靓,本科生;研究方向:非线性系统研究
* **通信作者**:姜翠美,博士、副教授;研究方向:非线性系统研究;jiangcuimei2004@163.com

忆阻器作为 4 个基本电路元件之一,它通过表示出磁通量与电荷间的动态关系来实现对电路状态的记忆功能。这种兼具非线性特征与记忆特性的电路元件,在混沌电路研究领域展现出独特优势。目前忆阻器的数学模型主要包含 3 种典型形式:Chua 提出的分段线性模型[1]、基于单调二次或三次函数的光滑模型[2],以及 HP 实验室开发的离子迁移模型[3]。忆阻器的多维度研究价值集中体现为:既可作为人工神经网络突触仿生的理想器件[4],又能基于其交叉阵列结构实现图像处理功能[5]。这些应用推动忆阻器的研究向多学科交叉领域深化发展。

忆阻器的引入更是为混沌系统提供了更高的灵活性和丰富的动力学行为[6-7]。近几年,忆阻实混沌系统引起了广大学者的研究[8-9],例如,忆阻器混沌在语音保密通信的应用[10-11]和图像加密中的应用[12-14]。与实混沌系统相比,复混沌系统因状态变量虚部的存在使系统的动力学行为更加复杂,在动态复杂度、抗干扰能力和功能扩展性上远超普通混沌系统,被广泛应用于物理、电子信息等领域[15-16],将在安全加密、智能优化、复杂系统控制等领域引发技术革命[17-18],特别在加密通信中,复混沌增加了传输信息的内容和保密效果[19],成为非线性科学迈向工程实践的重要桥梁。

然而,基于忆阻器的复混沌动力学研究不多,其在图像加密领域的应用还需要进一步拓展研究与应用。

另外,数字媒体技术的快速发展加剧了图像作为信息载体在互联网中的安全性问题。混沌系统因其丰富的混沌性和类噪声特性,成为图像加密的理想工具[20]。现有研究仍面临两大核心问题:混沌系统受限于数值精度效应,长期迭代易使动力学特性退化;传统“置乱-扩散”架构[21]中,位置置乱的周期性与扩散环节的线性依赖使得加密系统易受统计攻击与暴力破解威胁。为解决上述问题,本文将基于忆阻器构建一个新的复 Lorenz 系统,通过数值仿真分析系统的动力学特性后,利用系统生成的混沌序列作为伪随机序列设计图像加密算法,并进行密钥敏感性分析等安全评估。

1　模型建立与动力学分析

1.1　模型建立

复 Lorenz 系统[22]为:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = bx_1 - x_1x_3 - x_2 \\ \dot{x} = -cx_3 + \dfrac{1}{2}(\bar{x}_1x_2 + x_1\bar{x}_2) \end{cases}, \tag{1}$$

在本文中使用的忆阻器物理模型是光滑三次非线性模型[2],该模型使用三次多项式函数来描述电阻值随电压或电荷变化的关系,其磁控型表达式为:

$$q(\varphi) = \alpha\varphi + \beta\varphi^3, \tag{2}$$

其中 α 和 β 是两个常数参数。

现在复 Lorenz 系统(1)中加入一个光滑三次非线性忆阻器,建立了一个新的复混沌系统,其具体形式如下:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = bx_1 - x_1x_3 - x_2 - w(x_3)x_1 \\ \dot{x} = -cx_3 + \dfrac{1}{2}(\bar{x}_1x_2 + x_1\bar{x}_2) \end{cases}, \tag{3}$$

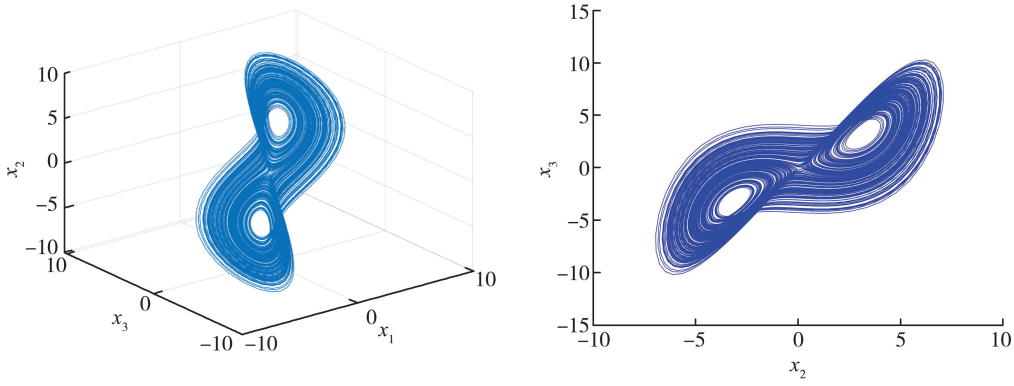
其中 $\omega(x_3) = \alpha + 3\beta x_3^{\,2}$。

分离系统(3)中每个变量的实数和虚数,可得:

$$\begin{cases}\dot{x}_1=a(x_3-x_1)\\ \dot{x}_2=a(x_4-x_2)\\ \dot{x}_3=bx_1-x_3-x_1x_5-\omega(x_5)x_1\\ \dot{x}_4=bx_2-x_4-x_2x_5-\omega(x_5)x_2\\ \dot{x}_5=x_1x_3+x_2x_4-cx_5\end{cases}, \tag{4}$$

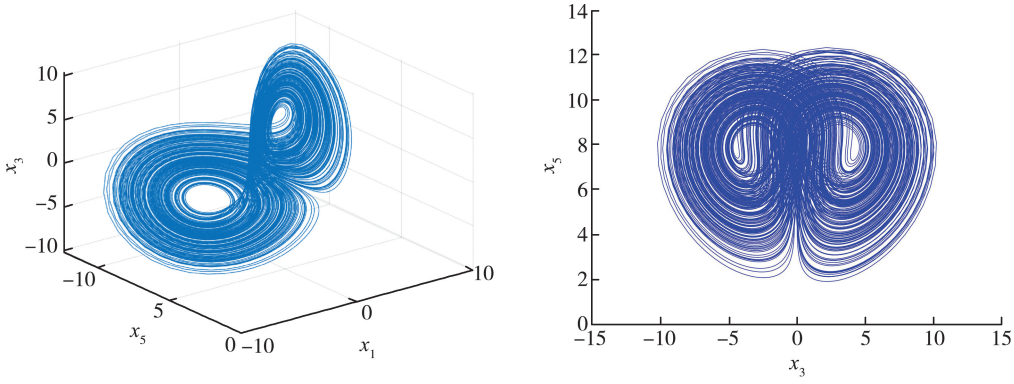
其中 $\omega(x_5)=\alpha+3\beta x_5^{\,2}$。

当参数为 $a=10,b=28,c=8/3,\alpha=0.2,\beta=0.1$ 时，初值为[0.1,0.1,0.1,0.1,0.1]，系统(4)展现出明显的混沌特征，如图 1~3。



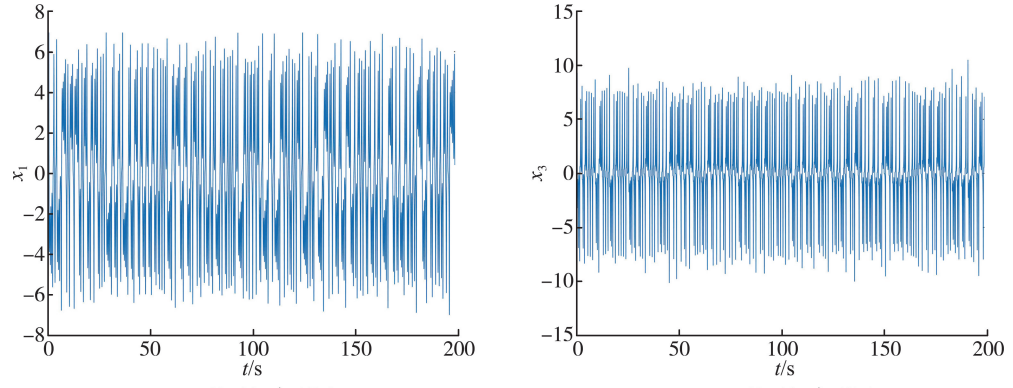
(a) 系统(4)的混沌吸引子　　(b) (a)中吸引子中的二维相图

图 1　系统(4)x_1、x_2、x_3 的混沌吸引子及其二维相图



(a) 系统(4)的混沌吸引子　　(b) (a)中吸引子中的二维相图

图 2　系统(4)x_1、x_3、x_5 的混沌吸引子及其二维相图



(a) x_1的时间序列图　　(b) x_3的时间序列图

图 3　x_1、x_3 的时间序列图

1.2　动力学分析

1.2.1　耗散性

系统的耗散度可表示为

$$\Delta V=\sum_{k=1}^{5}\frac{\partial \dot{x}_k}{\partial x_k}=-a-a-1-1-c=-2a-c-2。$$

当$-2a-c-2<0$时,系统是耗散的,

$$\frac{\mathrm{d}V}{\mathrm{d}t}=(-2a-c-2)\rightarrow V=V_0\mathrm{e}^{(-2a-c-2)t}。$$

系统(4)的轨迹最终收敛至零体积极限集且稳定于吸引子,证明系统(4)存在吸引子。

1.2.2　李雅普诺夫指数

系统(4)的 Jacobian 矩阵为:

$$\boldsymbol{J}=\begin{pmatrix}-a & 0 & a & 0 & 0\\ 0 & -a & 0 & a & 0\\ b-x_5-\alpha-3\beta x_5^{\ 2} & 0 & -1 & 0 & -x_1-6\beta x_1x_5\\ 0 & b-x_5-\alpha-3\beta x_5^{\ 2} & 0 & -1 & -x_2-6\beta x_2x_5\\ x_3 & x_4 & x_1 & x_2 & -c\end{pmatrix}。$$

根据 Wolf 算法,计算可得到系统(4)在参数 $a=10,b=28,c=8/3,\alpha=0.2,\beta=0.1$ 和初值 $\boldsymbol{x}_0=(0.1,0.1,0.1,0.1,0.1)$下的 Lyapunov 指数分别为:

$$\lambda_1=1.008\ 609,\lambda_2=0.067\ 718,\lambda_3=-0.021\ 638,\lambda_4=-11.005\ 480,\lambda_5=-14.739\ 60。$$

如图 4,可以得到系统(4)的分数维数为:

$$D=l+\frac{1}{|\lambda_{l+1}|}\sum_{k=1}^{l}\lambda_k=3+\frac{\lambda_1+\lambda_2+\lambda_3}{|\lambda_4|}=3.095\ 83。$$

由此可得系统(4)具有大于 0 的 Lyapunov 指数,其维数为分数维数,即表示系统具有混沌的性质。

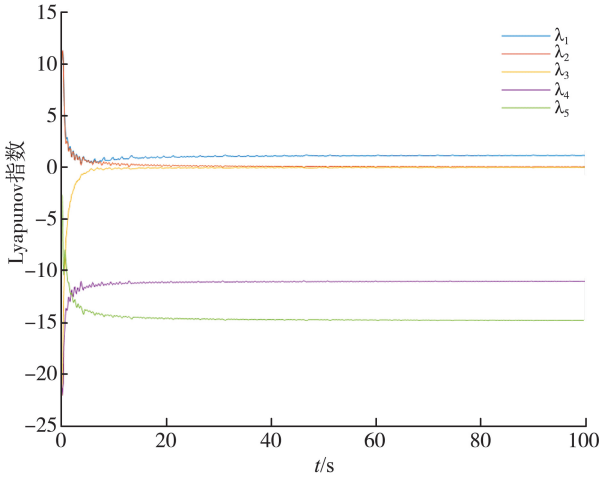
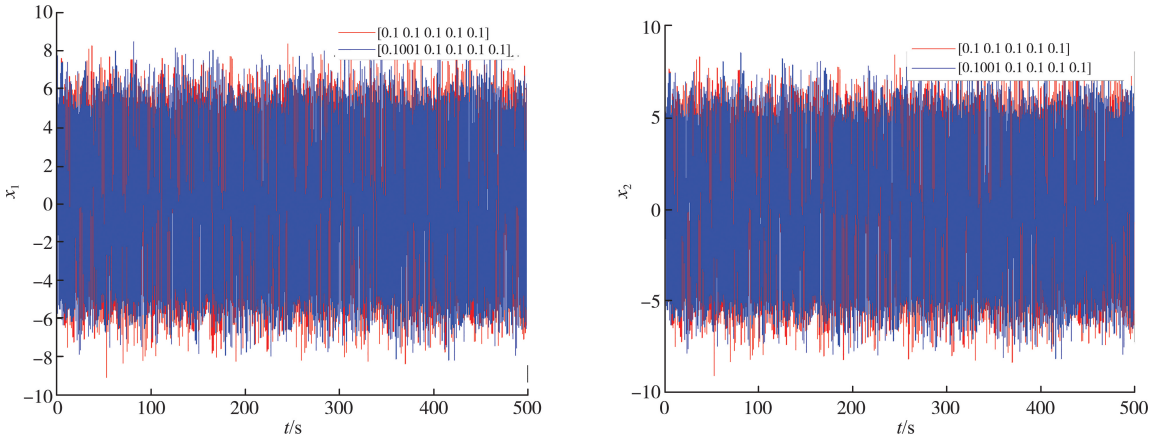


图 4　系统(4)的 Lyapunov 指数

1.2.3　初值敏感性

在不改变系统(4)参数的条件下,仅将状态变量 x_1(或 x_2)的初始值从 0.1 微调至 0.100 1(如图 5 所示)。尽管初始值的变化幅度仅为 0.01%,但系统状态却产生了显著偏差,这表明系统(4)对初始条件具有初值敏感性。



(a) 只改变初始值 x_1　　(b) 只改变初始值 x_2

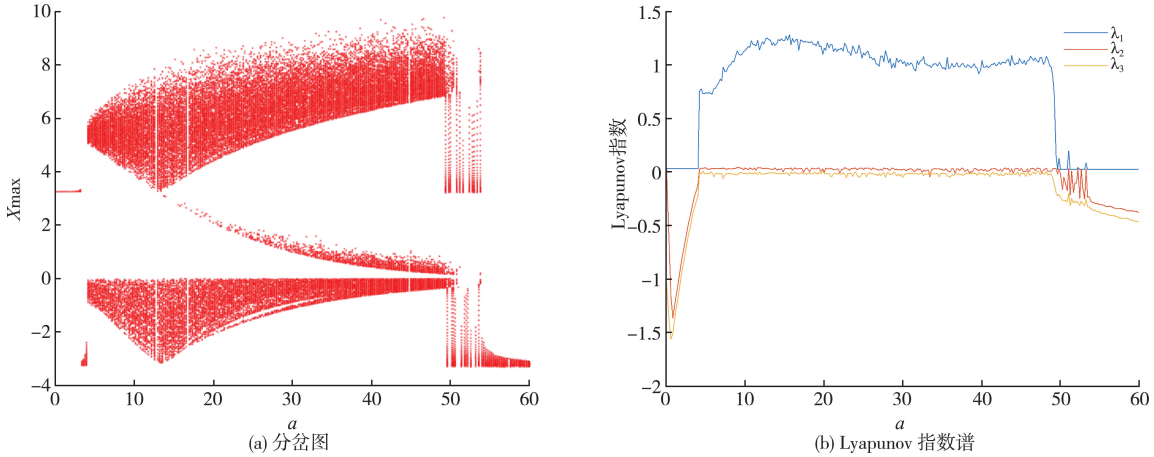
图 5　系统的初值敏感性

1.2.4　随参数变化的动力学分析

下面的数值仿真中，系统初值选为[0.1,0.1,0.1,0.1,0.1]。

(1)参数 a 的改变

系统(4)的其它参数为 $b=28,c=8/3,\alpha=0.2,\beta=0.1$。参数 $a\in[0,60]$的分岔图与 Lyapunov 指数谱，如图 6 显示。由于 λ_4、λ_5 数值相较于 λ_1、λ_2、λ_3 过小故不显示，Lyapunov 指数谱只显示随参数 a 递增变化的 λ_1、λ_2、λ_3。当 $a\in[0,4)$时，系统处于周期一的状态；当 $a\in[4,49.2)$时，系统是混沌的。

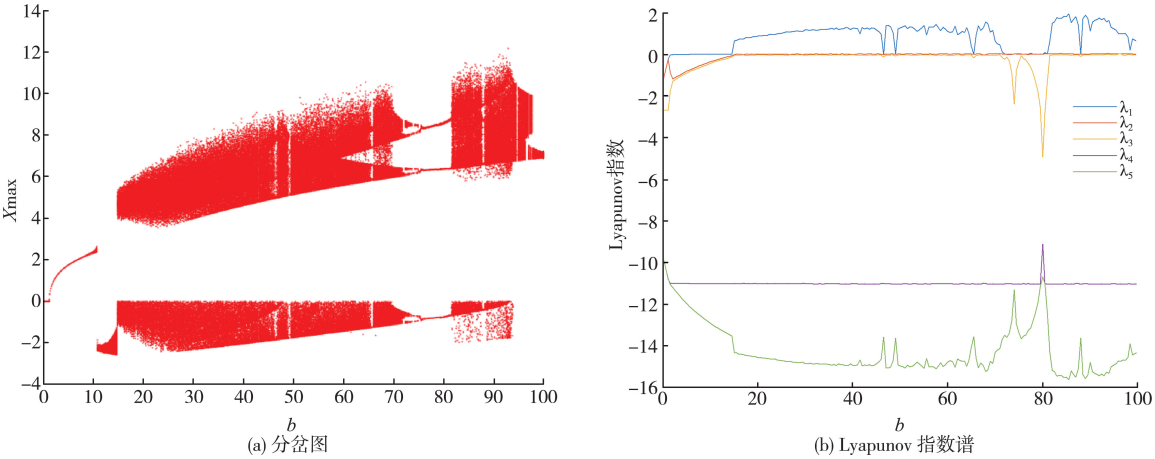


(a) 分岔图　　(b) Lyapunov 指数谱

图 6　随参数 a 变化的分岔图和 Lyapunov 指数谱

(2)参数 b 的改变

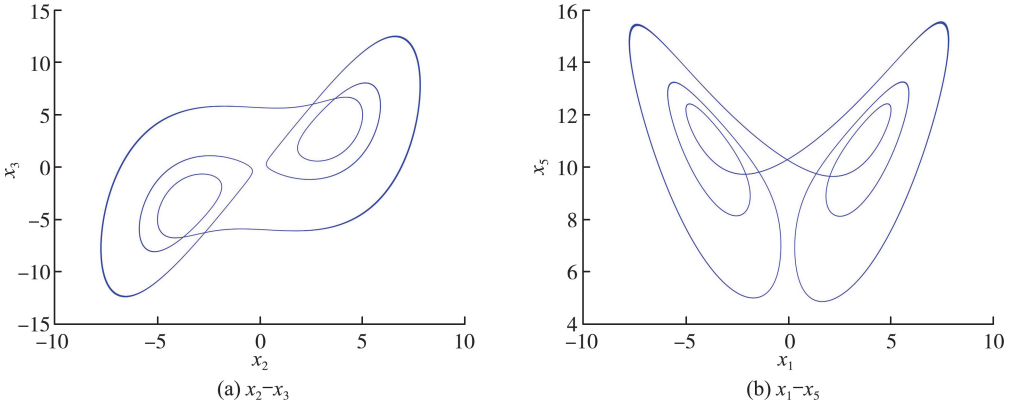
系统(4)的其它参数为 $a=10,c=8/3,\alpha=0.2,\beta=0.1$。参数 $b\in[0,100]$的 Lyapunov 指数谱与分岔图，如图 7 显示。当 $b\in[0,10)$时，系统呈现周期一行为。当 $b\in[14.5,72)$，系统处于混沌态。当 $b\in[72,81)$时，系统此时出现了逆二倍周期分岔现象，当 $b\in[81,95)$时，系统再次进入混沌态，表现为非周期或噪声状模式。



(a) 分岔图　　(b) Lyapunov 指数谱

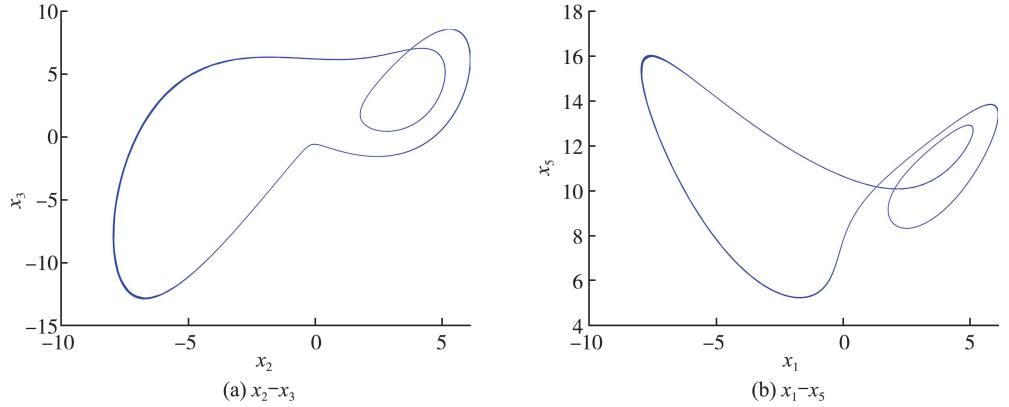
图 7　随参数 b 变化的分岔图和 Lyapunov 指数谱

当参数 $b=46.4$，$b=49.295$，$b=79.2$ 和 $b=88.001$ 时，系统(4)出现了周期性窗口，此吸引子对应的相图，如图 8～11 所示。



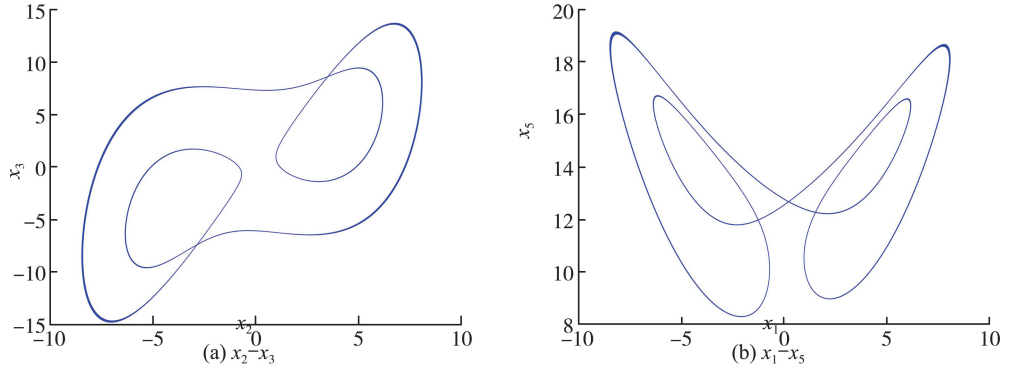
(a) x_2–x_3　　(b) x_1–x_5

图 8　当 $b=46.4$ 时，系统(4)吸引子的相图



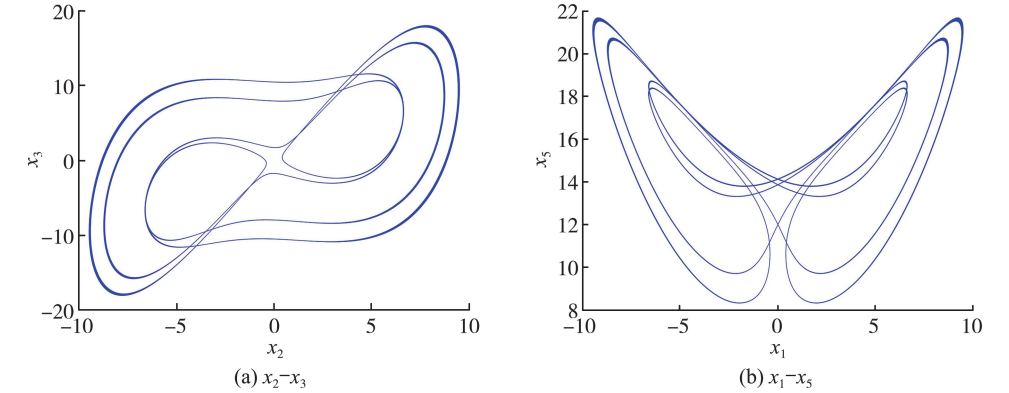
(a) x_2–x_3　　(b) x_1–x_5

图 9　当 $b=49.295$ 时，系统(4)吸引子的相图



(a) x_2–x_3　　(b) x_1–x_5

图 10　当 $b=79.2$ 时，系统(4)吸引子的相图

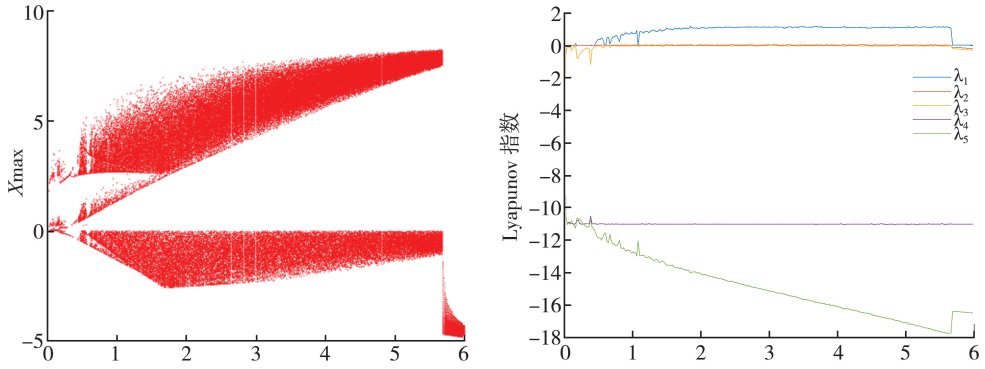


(a) x_2–x_3　　(b) x_1–x_5

图 11　当 $b=88.001$ 时，系统(4)吸引子的相图

(3)参数 c 的改变

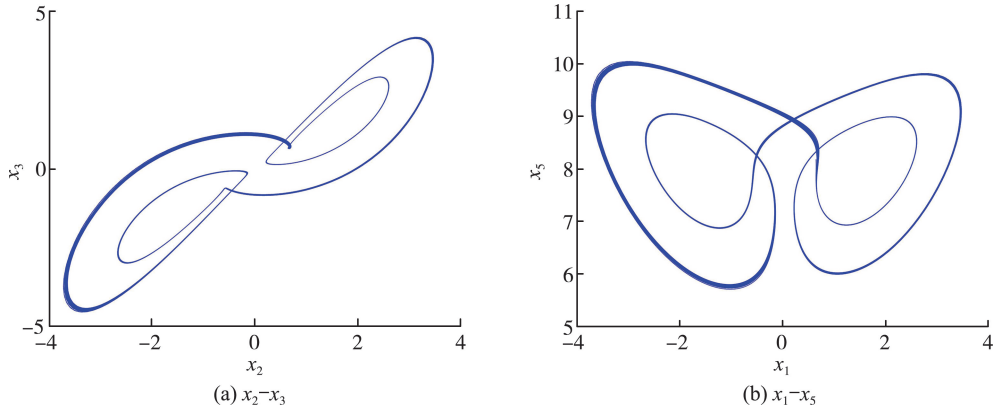
系统(4)的其它参数为 $a=10,b=28,\alpha=0.2,\beta=0.1$。图 12 显示了参数 $c\in[0,6]$ 的分岔图与 Lyapunov 指数谱。当 $c\in[0,0.5)$ 时,系统处于周期状态,当 $c\in[0.5,5.7)$ 时,系统处于混沌状态。



(a) 分岔图　　(b) Lyapunov 指数谱

图 12　随参数 c 变化的分岔图和 Lyapunov 指数谱

当 $c=0.6$ 时,处于周期窗口的吸引子对应的相图,如图 13 所示。

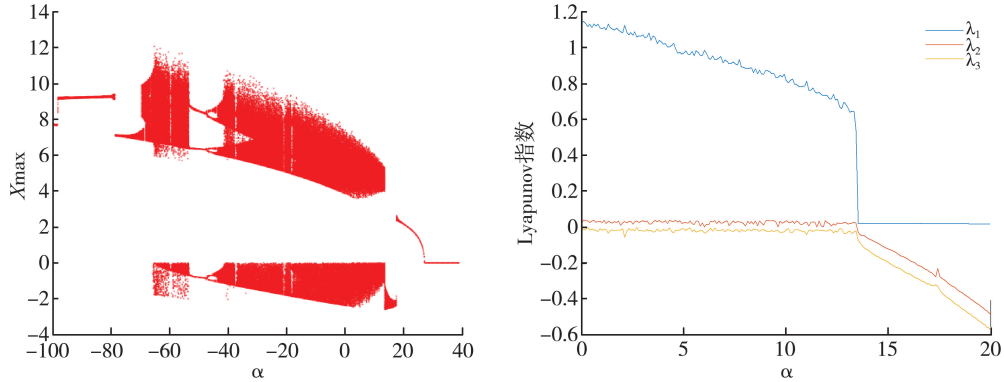


(a) x_2-x_3　　(b) x_1-x_5

图 13　当 $c=0.6$ 时,系统(4)吸引子的相图

(4)忆阻参数 α 的改变

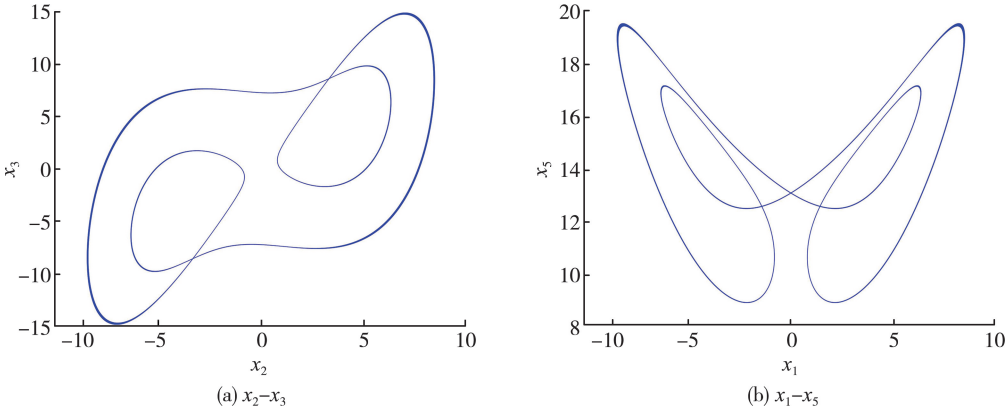
系统(4)的其它参数为 $a=10,b=28,c=8/3,\beta=0.1$。图 14 显示了参数 α 在$[-100,40]$变化的分岔图与 Lyapunov 指数谱。当 $\alpha\in[-100,-65)$时,系统是周期的;当 $\alpha\in[-65,-54)$时,系统是混沌的;当 $\alpha\in[-54,-46)$时,系统处于周期 3 状态;当 $\alpha\in[-46,-43)$时系统处于周期 6 状态;当 $\alpha\in[-43,13.5)$时,系统是混沌的;当 $\alpha\in[13.5,40)$时,系统出现逆二倍周期现象。



(a) 分岔图　　(b) Lyapunov 指数谱

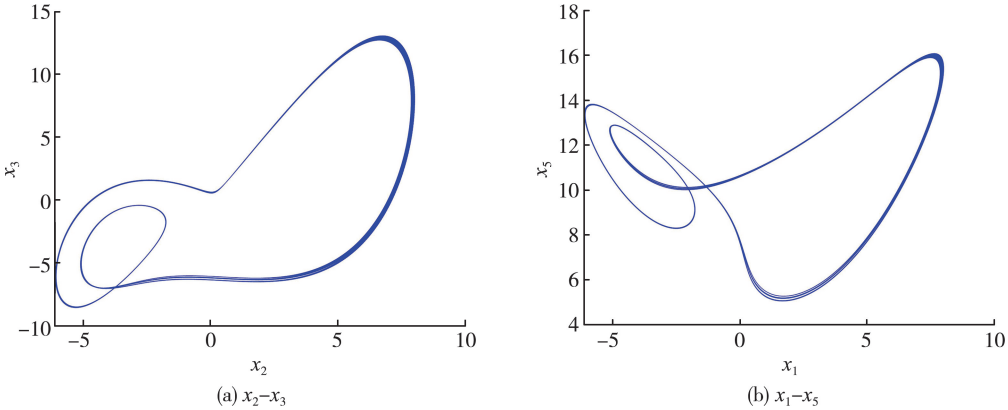
图 14　随参数 α 变化的分岔图和 Lyapunov 指数谱

当 $\alpha=-60$,$\alpha=-20.9$ 时,系统(4)出现了周期窗口,处于周期窗口的吸引子对应的二维相图如图 15~16 所示。



(a) x_2–x_3　　(b) x_1–x_5

图 15　当 $\alpha=-60$ 时,系统(4)吸引子的相图



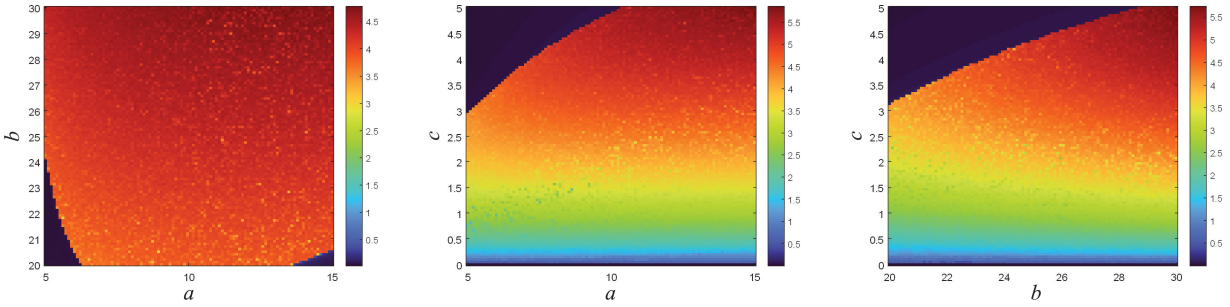
(a) x_2–x_3　　(b) x_1–x_5

图 16　当 $\alpha=-20.9$ 时,系统(4)吸引子的相图

(5)随双参数的变化

图 17 展示了系统(4)在不同参数组合下的双参数分岔图,其中颜色刻度表示系统状态变量在稳态阶段的标准差大小。标准差越大,意味着系统的动力学响应幅度越高,通常指示复杂周期或混沌行为;相反,标准差接近零(图中呈现为黑色区域)则对应系统进入稳定平衡态或低幅度的周期运动。(a)在 a-b 平面中,左下角的黑色区域表明当 a 与 b 均处于较低值时,系统动力学受到显著抑制,趋于稳定平衡状态;随着 a 与 b 的增大,黑色区域逐渐消失,标准差快速升高,系统由稳定态过渡到周期及混沌态。(b)在 a-c 平面中,低 c 值区域(特别是 $c<1$)出现连续分布的黑色稳定区,即使 a 较大,系统仍表现出低幅度振荡或稳定平衡,说明 c 对稳定性的增强作用较为显著;而当 c 超过一定阈值时,黑色区域被高标准差区取代,系统呈现复杂振荡甚至混沌特性。(c)在 b-c 平面中,低 b 或低 c 的组合对应大面积黑色稳定区,表明任一参数较小都能有效抑制系统振荡幅度,使其处于稳定态;而当 b 与 c 同时增大时,黑色区域消失,标准差显著上升,系统进入高非线性混沌状态。

总体来看,系统在不同参数组合下展现出由稳定平衡态、低阶周期运动到高幅度混沌振荡的多种动力学模式,形成了丰富而复杂的动力学特性。这些结果不仅揭示了参数 a、b、c 对系统行为的显著影响及其耦合效应,也为深入研究该系统的非线性机理与控制策略提供了重要参考。



(a) 参数$a-b$ (b) 参数$a-c$ (c) 参数$b-c$

图 17 系统(4)的双参数分岔图

1.2.5 平衡点的稳定性

求解方程组 $\dot{x}_1=0,\dot{x}_2=0,\dot{x}_3=0,\dot{x}_4=0$ 和 $\dot{x}_5=0$,可得到系统(4)的平衡点。当 $x_5>0$ 时,故有:

$$\boldsymbol{E}_0=(0,0,0,0,0),$$

$$\boldsymbol{E}_\theta=(\sin\theta,r\cos\theta,r\sin\theta,r\cos\theta,x_5),$$

其中 $r=\pm\sqrt{c\left(\sqrt{\frac{b-\alpha-1}{3\beta}+\frac{1}{36\beta^2}}-\frac{1}{6\beta}\right)}$,$x_5=\sqrt{\frac{b-\alpha-1}{3\beta}+\frac{1}{36\beta^2}}-\frac{1}{6\beta}$。

下面讨论平衡点 $\boldsymbol{E}_0=(0,0,0,0,0)$ 的稳定性。系统(4)在 $\boldsymbol{E}_0$ 的 Jacobian 矩阵为

$$\boldsymbol{J}_{\boldsymbol{E}_0}=\begin{pmatrix}-a & 0 & a & 0 & 0\\ 0 & -a & 0 & a & 0\\ b-\alpha & 0 & -1 & 0 & 0\\ 0 & b-\alpha & 0 & -1 & 0\\ 0 & 0 & 0 & 0 & -c\end{pmatrix},$$

从而可得到矩阵 $\boldsymbol{J}_{\boldsymbol{E}_0}$的特征方程为

$$(\lambda+c)(\lambda^2+(a+1)\lambda+a+a(\alpha-b))^2=0。$$

根据 Routh-Hurwitz[23] 判断定理,其特征值满足 $\mathrm{Re}[\lambda]<0$,平衡点稳定。因此,当 $c>0$ 和$(a-1)^2>4a(\alpha-b)$时,$\boldsymbol{E}_0$ 是稳定的,否则 $\boldsymbol{E}_0$ 不稳定。此外,可以分析平衡点 $\boldsymbol{E}_\theta$ 的稳定性。

1.2.6 0-1 测试

设 $x(j)(j=1,2,\cdots,N)$ 为离散时间序列,选取 c 为区间$(0,\pi)$的随机常数,定义函数 $p(n)$ 与 $q(n)$ 为:

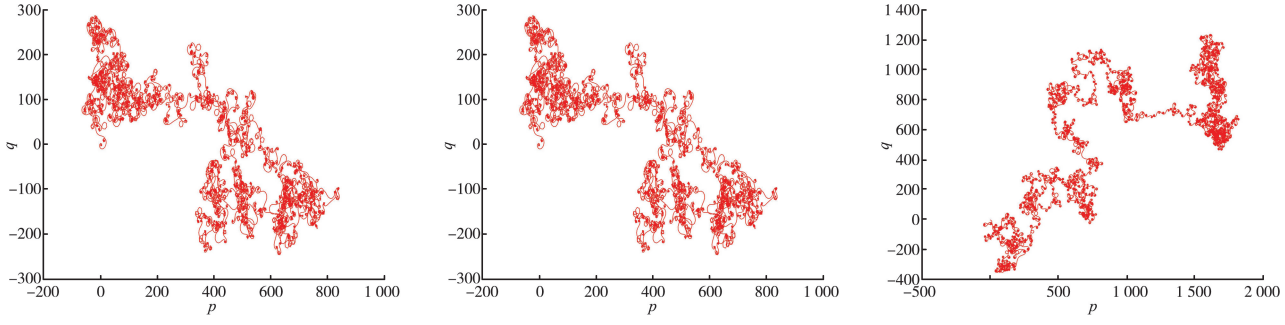
$$p(n)=\sum_{j=1}^{n}x(j)\cos(\theta(j)),n=1,2,\cdots,N,$$

$$q(n)=\sum_{j=1}^{n}x(j)\sin(\theta(j)),n=1,2,\cdots,N,$$

$$\theta(n)=jc+\sum_{j=1}^{j}x(j),j=1,2,\cdots,n,$$

如果函数 $p(n)$ 与 $q(n)$ 的轨迹表现为不规则运动,那么可表明系统是混沌的。如不是,则系统为非混沌。

分别针对状态变量 x_3、x_4 和 x_5 进行仿真测试,系统初值为$[0.1,0.1,0.1,0.1,0.1]$,得到 $p(n)$ 与 $q(n)$ 的轨迹,如图 18,结果表明轨迹呈现不规则的运动,即可说明系统(4)是混沌的。



(a) x_3 (b) x_4 (c) x_5

图 18 $p(n)-q(n)$ 运动轨迹图

1.2.7　庞加莱截面

庞加莱截面[24]的截点分布特征可用于识别系统的动力学行为。若截面呈现离散点集,表明系统处于周期状态;而当截面分布呈现无规则密集点集且具有分形特征时,系统表现为混沌态。

从图 19 可得出,系统(4)在 x_1-x_2、x_1-x_3、x_1-x_5 以及 x_3-x_5 方向上的庞加莱截面中,都出现了成无规则密集点集且具有分形特征,表明系统(4)表现为混沌态。

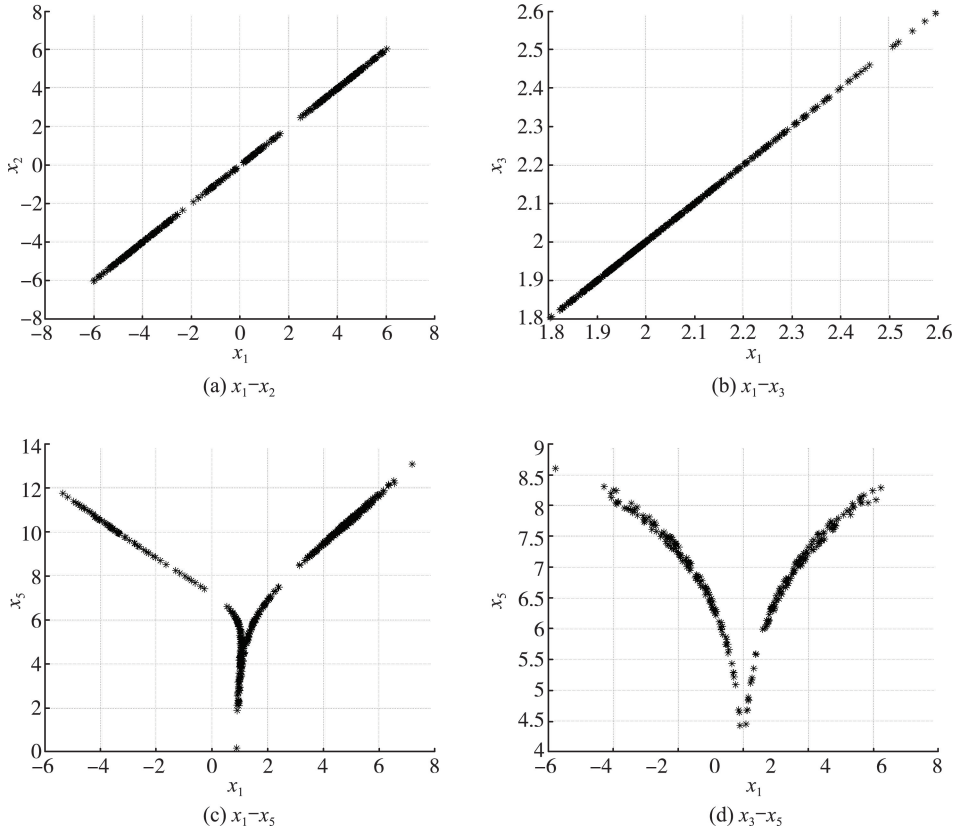


图 19　庞加莱截面图

2　图像加密

在新复混沌系统的基础上,本文提出一种融合“置乱-扩散”双阶段的加密方案,旨在实现高效且鲁棒的图像保护。下面将系统性地探讨加密算法的设计原理、实现流程与性能验证。

2.1　图像加密实现

图像加密的具体方案如下:

首先,将具有 $M\times N$ 像素的明文图像按行展开为一维行向量 $\boldsymbol{\alpha}$。对系统(4)生成的混沌序列进行如下处理:

(1)去除重复值形成初始序列 B;

(2)将原混沌序列中未被包含在 B 中的数值追加至 B 末尾;

(3)对 B 执行 m 次无重复位置置乱,每次通过交换第 i 个与第 $MN-i+1$ 个元素实现。最终完成基于伪随机序列的图像置乱操作。

对经过 m 轮置乱的图像进行基于有限域 $GF(2^{17})$ 的扩散处理,但因为 $GF(2^{17})$ 有限域运算中,以 0 作为乘数会导致信息的损失,所以不能直接将 $GF(2^{17})$ 域上的乘法运算应用于扩散算法中。

扩散算法[25]的具体过程如下：

$$\begin{cases} C_{i,H}=C_{i-1,H}\times S_{i,H}\times P_{i,H} \\ C_{i,L}=C_{i-1,L}\times S_{i,L}\times P_{i,L} \\ C_i=C_{i-H}\times 16+C_{i,L} \end{cases}, \tag{5}$$

$$\begin{cases} C_{i,H}=C_{i+1,H}\times S_{i,H}\times P_{i,H} \\ C_{i,L}=C_{i+1,L}\times S_{i,L}\times P_{i,L} \\ C_i=C_{i-H}\times 16+C_{i,L} \end{cases}, \tag{6}$$

其中 $\boldsymbol{C}$ 和 $\boldsymbol{S}$ 是密码向量，P 是明文图像。扩散时，借助于式(5)，而式(6)是扩散的逆运算。

算法流程图，如图 20 所示：

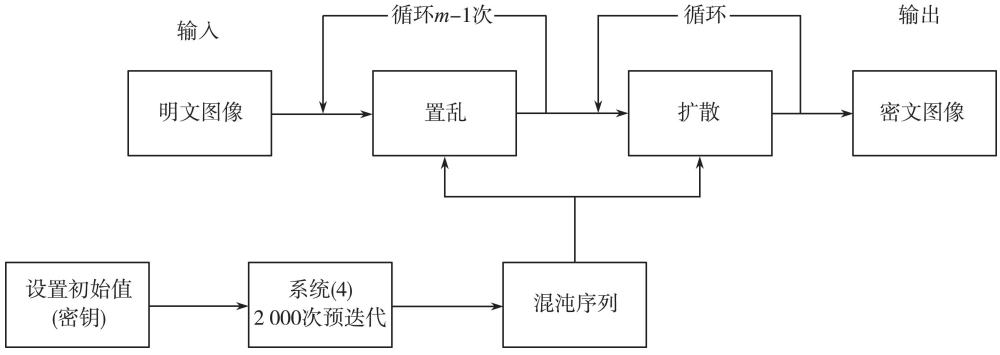


图 20　加密算法的实现过程

2.2　效果展示

使用上述加密算法，实现图像加密，对比结果如图 21 所示，系统(4)对明文图像加密效果好。根据上述执行扩散与置乱的逆运算，利用相同初始参数再生混沌序列，可无损还原恢复明文图像，如图 22，结果表明该加密算法能够满足加密需求且具有可逆性。

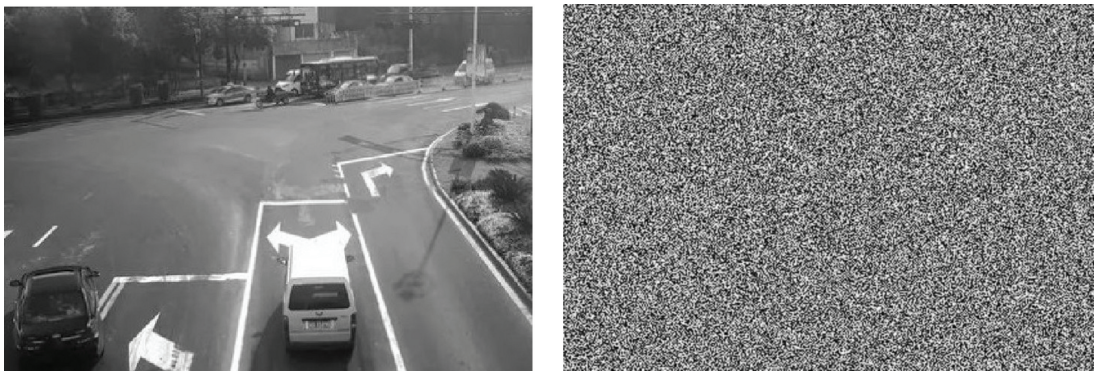


图 21　明文图像与置乱—扩散后的图像对比



图 22　扩散后的密文图像与解密结果图的对比

2.3　安全性分析

为更好地分析该加密算法的性能,下面进行了一系列图像加密性能分析。

2.3.1　密钥空间分析

在 64 位计算机系统中使用精度为小数点后 4 位的浮点数时,该加密算法的密钥空间至少为 $2^{120}>2^{100}$ 符合标准加密规范要求[26]。

2.3.2　直方图分析与卡方检验

如图 23,通过原始图像、密文图像及解密图像的直方图对比,加密算法改变了图像的统计特性,密文直方图图像呈现均匀化分布特征,该加密算法能够很好地抵抗直方图攻击[27]。而解密过程能够准确重构原始图像,解密直方图与明文直方图高度相同。这充分验证了加解密过程的可逆性以及加密算法的抗统计分析能力。

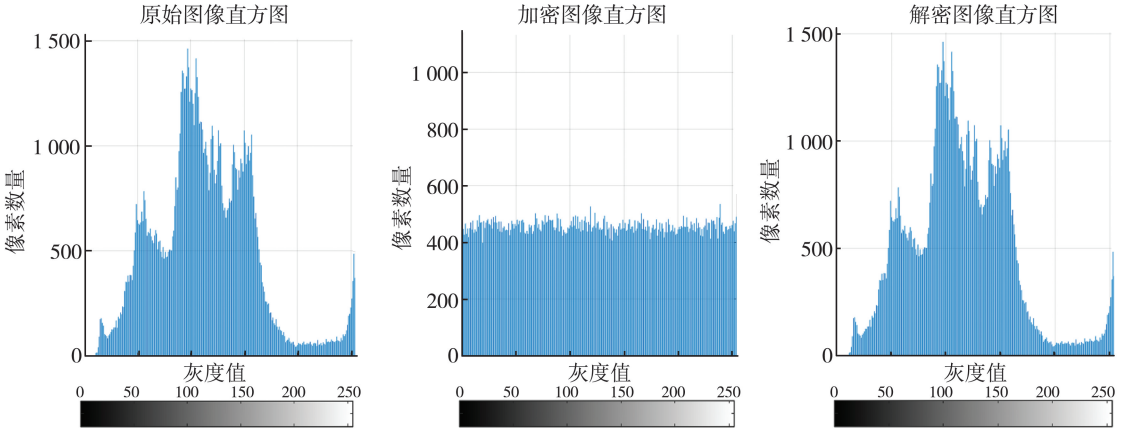


图 23　加密前、加密后以及解密后直方图

2.3.3　相邻像素的相关性分析

相关性测试[28]是指相邻像素点之间的相关程度,这里所做的相关性测试看的是水平,垂直,正对角(右上位置),这 4 个方向上的相关情况。相关系数计算公式如下:

$$C_r=\frac{N\sum_{i=0}^{N}x_iy_i-(\sum_{i=0}^{N}x_i)(\sum_{i=0}^{N}y_i)}{\sqrt{(N\sum_{i=0}^{N}x_i^2-(\sum_{i=0}^{N}x_i)^2)(N\sum_{i=0}^{N}y_i^2-(\sum_{i=0}^{N}y_i)^2)}},\tag{7}$$

其中 N 是选取的相邻像素组的数目,x 和 y 代表两个相邻图像像素的取值。从图像中随机抽取 2 000 对相邻像素,计算其相关系数,结果如表 1 相邻像素的相关系数所示。分析结果表明原始图像的相邻像素相关系数接近 1,而密文图像的相关系数则趋近于 0,该加密过程有效破坏了原图像的统计特性,实现了良好的图像加密效果。

表 1　相邻像素的相关系数

方向	相关系数		
	原始图像(明文)	加密图像(密文)	解密图像
水平	0.964	−0.001	0.964
垂直	0.958	−0.003	0.958
对角	0.938	−0.000	0.938

2.3.4　信息熵分析

信息熵[29],即平均信息量,定义:$H(x)=-\sum_{i=1}^{n}p(x_i)\log_2 p(x_i)$,其中 $p(x_i)$ 表示符号 x_i 在消息中出现的

概率。用信息熵的量值来衡量图像加密后信息的不确定程度,即信息熵越大,信息量越大,说明不确定程度越大,故安全性越高。在灰度图像中,最大信息熵为 8。经过 Matlab 数值仿真计算,加密后的信息熵别为7.998 5。

2.3.5 密钥敏感性分析

对密钥敏感性进行具体实验分析,采用标准灰度测试图像,通过数值仿真计算在 5 个扰动参数下对应的像素变化率(Number of Pixels Change Rate,N_{PCR})和统一的平均变化强度(Unified Average Changing Intensity,I_{UAC})[30],此时系统参数为 $a=10$,$b=28$,$c=8/3$,$\alpha=0.2$,$\beta=0.1$,设定扰动强度为 $\Delta=10^{-10}$,测试结果如表 2 所示。

对表2 的 N_{PCR}、I_{UAC}相关数值分析可得,所有扰动参数的 N_{PCR}值均高于99.610 0%,其中 x_2 的像素变化率最高(99.632 3%),系统偏差小于 0.03%,满足抗差分攻击的要求。I_{UAC}值分布在 33.33%~33.58%之间,与理论理想值33.463 5%的偏差小于0.14%。其中,x_5 的 I_{UAC}值最高(33.580 0%),表明其非线性反馈机制对像素值强度变化具有放大效应。

表 2 N_{PCR}、I_{UAC}相关数值

扰动参数	N_{PCR}/%	I_{UAC}/%
x_1	99.620 1	33.332 9
x_2	99.630 7	33.534 6
x_3	99.632 3	33.492 9
x_4	99.615 5	33.375 8
x_5	99.618 5	33.580 0

3 结 论

通过将忆阻器引入复 Lorenz 系统,本文建立了新型忆阻复混沌模型。利用耗散性、平衡点稳定性、初值敏感性、分岔图、相图、庞加莱截面、Lyapunov 指数和 0-1 测试等,本文对新系统进行了动力学分析,结果显示该系统具有混沌特性。基于新复混沌系统生成高熵伪随机序列,本文利用“置乱-扩散”,设计了图像加密方案,加密后的图像直方图分布均匀,密钥敏感性显著且信息熵接近理想值 8,该方案能够有效减小相关系数,对密文攻击模式有很好的抵御效能。本研究不仅提出了一个具有实用价值的忆阻复混沌系统,更为实现轻量级、高安全性的图像加密提供了切实可行的解决方案,在信息安全领域具有重要的应用前景。

参考文献:

[1] Chua L.Memristor-the missing circuit element[J].IEEE Transactions on Circuit Theory,1971,18(5):507-519.

[2] 欧青立,赵平荣,游淼.基于三次非线性忆阻器的有源低通滤波器[J].应用科技,2014(5):6-10.

[3] Muthuswamy B.Implementing memristor based chaotic circuits[J].International Journal of Bifurcation and Chaos,2010,20(5):1335-1350.

[4] 王国权,刘亮.忆阻器应用于人工神经网络的前景与展望[J].中国新技术新产品,2009(6):18-19.

[5] 胡小方,段书凯,王丽丹,等.忆阻器交叉阵列及在图像处理中的应用[J].中国科学(信息科学),2011,41(4):500-512.

[6] Chen Lijuan, Yu Mingchu, Luo Jinnan, et al. Dynamic analysis and FPGA implementation of a new linear memristor-based hyperchaotic system with strong complexity[J].Mathematics,2024,12(12):1891.

[7] Zhang Jie, Cheng Nana, Zuo Jiangang, et al. Design, analysis and application of Non-Hamiltonian conservative chaotic system based on memristor[J].Integration,2025,100:102307.

[8] Xie Xianyang, Wen Shiping, Feng Yuming, et al.Three-stage-impulse control of memristor-based Chen Hyper-chaotic system[J].

Mathematics,2022,10(23):4560.
[9] 张贵重,全旭,刘嵩.一个具有超级多稳定性的忆阻混沌系统的分析与 FPGA 实现[J].物理学报,2022,71(24):149-158.
[10] 刘威.忆阻器在混沌及语音保密通信中的应用研究[D].杭州:杭州电子科技大学,2015.
[11] 闵国旗,王丽丹,段书凯.离子迁移忆阻混沌电路及其在语音保密通信中的应用[J].物理学报,2015,64(21):251-263.
[12] Wang Zhulin,Min Fuhong,Wang Enrong.A new hyperchaotic circuit with two memristors and its application in image encryption[J].AIP Advances,2016,6(9):095316.
[13] 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.
[14] 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.
[15] Yang Feifei,Mou Jun,Yan Huizhen,et al.Dynamical analysis of a novel complex chaotic system and application in image diffusion[J].IEEE Access,2019,7:118188-118202.
[16] 肖成龙,孙颖,林邦姜,等.基于神经网络与复合离散混沌系统的双重加密方法[J].电子与信息学报,2020,42(3):687-694.
[17] 张芳芳,张帅虎,马凤英,等.复混沌系统的稳态控制[J].控制理论与应用,2023,40(4):744-752.
[18] 赵云,李晓明,刘振盛.基于优化协调复合混沌密码系统的广域海量信息加密方法[J].电力系统自动化,2013,37(6):69-76.
[19] 杨文涛,叶欢,李子龙,等.基于一类复混沌系统的图像加密研究[J].齐鲁工业大学学报,2021,35(6):73-80.
[20] 孙鑫,易开祥,孙优贤.基于混沌系统的图像加密算法[J].计算机辅助设计与图形学学报,2002,14(2):136-139.
[21] 舒永录,张玉书,肖迪,等.基于置乱扩散同步实现的图像加密算法[J].兰州大学学报(自然科学版),2012,48(2):113-116.
[22] Fowler A C,McGuinness M J.On the nature of the torus in the complex Lorenz equations[J].SIAM Journal on Applied Mathematics,1984,44(4):681-700.
[23] Wang Xingyuan,He Yijie,Wang Mingjun.Chaos control of a fractional order modified coupled dynamos system[J].Nonlinear Analysis:Theory,Methods & Applications,2009,71(12):6126-6134.
[24] 张识,王攀,张瑞浩,等.选取任意庞加莱截面的新方法[J].物理学报,2020,69(4):58-67.
[25] Zhang Jie,Yang Jing,Xu Longhao,et al.The circuit realization of a fifth-order multi-wing chaotic system and its application in image encryption[J].International Journal of Circuit Theory and Applications,2023,51(3):1168-1186.
[26] 王宏达.基于 DNA 和元胞自动机的新型图像加密算法[J].电子科技,2019,32(4):39-43.
[27] 李贤丽,王壮,于婷婷,等.一个新超混沌系统及其图像加密的应用[J].自动化与仪器仪表,2023(5):45-50.
[28] 周连兵,周湘贞,崔学荣.基于双重二维混沌映射的压缩图像加密方案[J].计算机科学,2022,49(8):344-349.
[29] 王越,安新磊,施倩倩,等.基于一个四维超混沌系统的图像加密算法[J].计算机仿真,2024,41(4):237-244.
[30] AlShaikh M,Alkhalifah A M,Alamri S.Improved resilience of image encryption based on hybrid TEA and RSA techniques[J].Computer Systems Science and Engineering,2025,49(1):353-376.

(责任编辑:王亚宾;校　对:孙洪清)