Modeling and Simulation 建模与仿真, 2023, 12(5), 4716-4731
Published Online September 2023 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2023.125430

Hans汉斯

基于忆阻隐藏超混沌系统的图像加密算法研究

聂　浩，陆安江*

贵州大学大数据与信息工程学院，贵州　贵阳

收稿日期：2023年7月27日；录用日期：2023年9月13日；发布日期：2023年9月20日

摘　要

针对传统超混沌Lorenz系统应用于图像加密时，存在密钥空间小、安全性不高等问题，本文在lv混沌系统的基础上，通过添加磁控忆阻器，提出一种具有稳定平衡点的四维忆阻超混沌系统，并应用于图像加密。通过相图、Lyapunov指数、分岔图等仿真分析，发现所构建的混沌系统具有稳定平衡点，并且随参数的变化，系统表现出周期－混沌－拟周期－超混沌的丰富动力学行为。通过模块化电路仿真设计，验证了混沌系统的物理可实现性。利用该混沌系统生成六个伪随机矩阵，先对明文图像进行扩散，然后通过置乱降低相邻像素点的相关性，再对置乱图像从最后一个像素点向前扩散，通过两次扩散和一次置乱，最终实现对明文图像加密。由直方图、密钥空间等仿真结果表明，使用新忆阻超混沌系统的图像加密算法比传统超混沌Lorenz算法密钥空间提高了2^{34}，密文的信息熵为7.9993，接近理论值，相邻像素点的相关性与超混沌Lorenz算法相比有数量级的降低，能抵御穷举攻击和差分攻击等常见的攻击方式，具有更高的安全性。

关键词

超混沌，忆阻器，稳定平衡点，图像加密，电路

Research on Image Encryption Algorithm Based on Memristor Hidden Hyperchaotic System

Hao Nie, Anjiang Lu*

College of Big Date and Information Engineering, Guizhou University, Guiyang Guizhou

Received: Jul. 27th, 2023; accepted: Sep. 13th, 2023; published: Sep. 20th, 2023

*通讯作者。

文章引用: 聂浩, 陆安江. 基于忆阻隐藏超混沌系统的图像加密算法研究[J]. 建模与仿真, 2023, 12(5): 4716-4731.
DOI: 10.12677/mos.2023.125430

Abstract

Traditional hyperchaotic Lorenz system is applied to image encryption, but the disadvantages of traditional algorithm are small key space and low security, to solve this problem, in this paper, based on the lv chaotic system, a four-dimensional memristor hyperchaotic system with stable equilibrium point is proposed by adding a magnetron memristor, and it is applied to image encryption. Through the analysis of phase diagram, Lyapunov exponent and bifurcation diagram, it is found that the new chaotic system has a stable equilibrium point, and with the change of parameters, the system shows a rich dynamic behavior, such as periodic, chaotic, quasi-periodic and hyperchaotic. The physical realizability of the chaotic system is verified by a modular circuit simulation design. Firstly, the plaintext image was diffused, and then the correlation of adjacent pixels was reduced by scrambling. Secondly, the scrambled image was diffused again forward from the last pixel. Finally, the plaintext image was encrypted by twice diffusion and once scrambling. The simulation results of histogram and key space show that the key space of the image encryption algorithm using the new memristor hyperchaotic system is 2^{34} higher than that of the traditional hyperchaotic Lorenz algorithm, the information entropy of the ciphertext is 7.9993, which is close to the theoretical value, and the correlation between adjacent pixels is orders of magnitude lower than that of the hyperchaotic Lorenz algorithm. It can resist the common attack methods such as exhaustive attack and differential attack, and has higher security.

Keywords

Hyperchaos, Memristor, Stable Equilibrium Point, Image Encryption, Circuit

1. 引言

随着通信技术的发展，通信的传输内容不再局限于单一的文本和语音消息，更多的是内容丰富、信息量大的图像信息[1]。由于图像数据量大、冗余度高，在图像的传输过程中，极易受到攻击和窃取，传统图像加密算法的安全性已经不能满足现今的传输需求。

由于混沌系统具有遍历性、伪随机性、初值敏感性等[2]，能产生随机性强且难以预测的混沌序列，因此在图像加密方面具有独特的优势。2016 年 Zhou [3]等人提出了一种基于超混沌系统和二维压缩感知的图像压缩加密方案，但由于采用的是低维的混沌系统，导致其密钥空间较小仅为 2149，容易被暴力破解。

2021 年，张雷[4]等人提出了一种结合 S 盒与混沌映射的图像加密算法，但仍采用经典的 Logistic 混沌映射和超混沌 chen 映射，并未使用新的混沌系统。现在，越来越多的学者结合 DNA 编码，提出新的图像加密算法。2017 年 Wang [5]等人通过扫描平面图像，对图像中的特定行采用混沌映射控制的 DNA 编码，最终生成密钥图像。但现有 DNA 图像加密算法，多数借助混沌系统打乱 DNA 编码，然后通过对行、列或像素点进行置换，从而实现图像加密。然而 Wei [6]等人指出，仅通过置换算法和 DNA 编码实现图像加密的安全性较低。

自忆阻器被发现以来[7] [8]，由于其具有良好的非线性特性和记忆性，在混沌电路、神经网络、类脑计算等方面得到应用。包伯成[9]等人通过将蔡氏电路中的非线性电阻替换成理想的忆阻器模型，发现了

具有极端多稳定性的忆阻电路。Ding [10]等人用通量控制忆阻器来模拟电磁感应效应，并结合 PWL 函数模拟双曲正切函数的特性，建立了一个双神经元的忆阻 PWL-HNN 模型。文献[11] [12] [13]通过添加或替换电路中的非线性器件构造了许多具有丰富动力学行为的混沌系统。虽然忆阻器具有广泛的应用前景，但在图像加密领域，使用含忆阻混沌系统的加密算法并不多见。

针对低维混沌系统密钥空间小，传统加密算法安全性低等缺点，本文在 lv 混沌系统的基础上，将磁控忆阻器作为负反馈项添加到原系统，构建了一个含忆阻的新四维混沌系统。分析了系统的耗散性、Lyapunov 指数和维数、分岔图等，并通过电路仿真软件，对系统电路进行仿真。最后借助该混沌系统生成伪随机序列，对明文图像进行两次扩散和一次置乱，实现对图像的加密。结果表明，使用本文混沌系统构建的图像加密算法密钥空间比低维混沌系统有较大的提升，并且加密效率高，有较高的安全性。

2. 四维忆阻混沌系统构建

吕金虎[14]等人提出了一个新的三维混沌系统，式(1)是 lv 混沌系统的数学模型：

$$\begin{cases} \dot{x} = a\left(y - x\right) \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

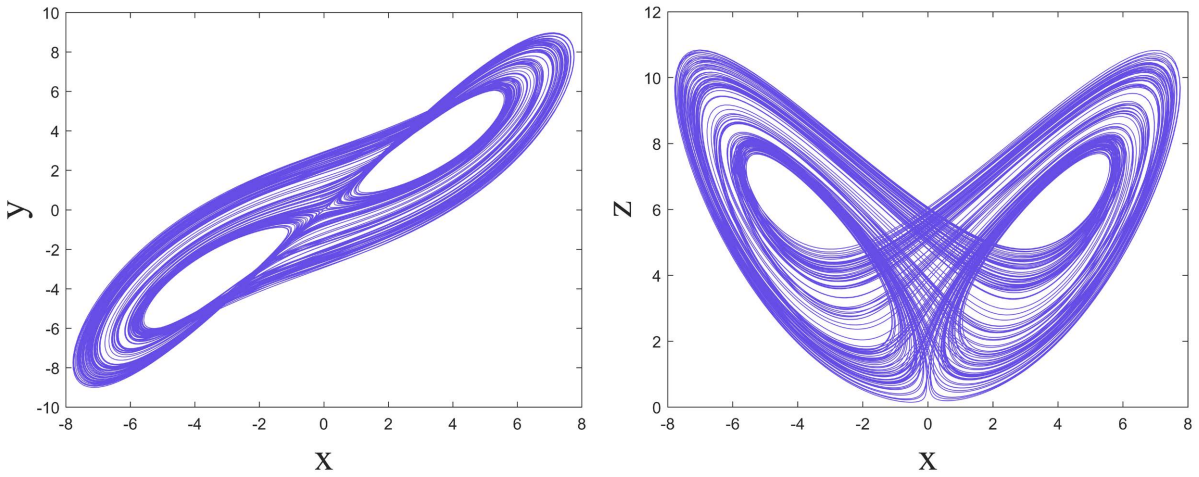
在 lv 系统的基础上，通过添加式(2)的磁控忆阻器作为负反馈项到式(1)中，从而构建新的四维混沌系统，其中 m 和 n 为忆阻器状态参数。

$$W\left(\varphi\right) = m + n\varphi^2 \tag{2}$$

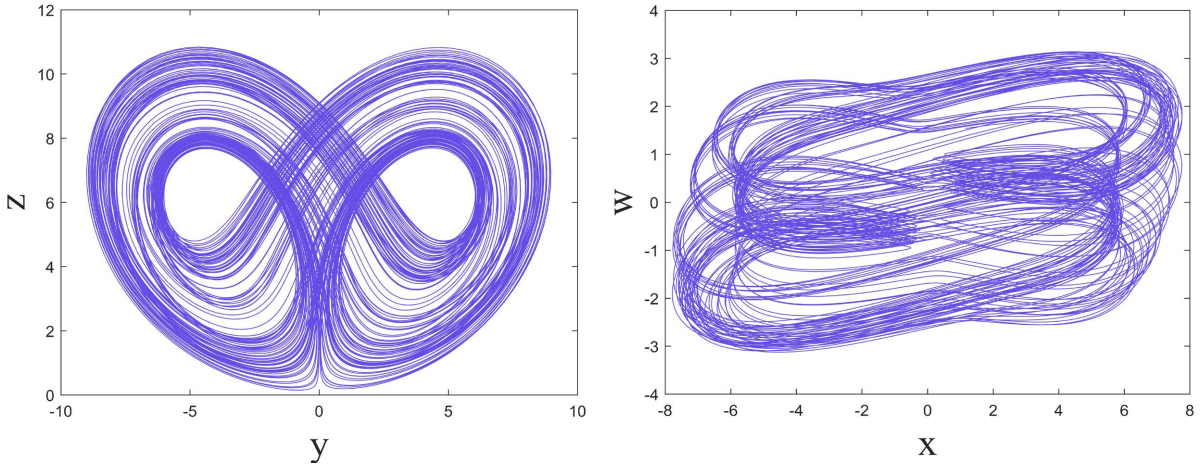
式(3)为新系统的数学模型，式中 x，y，z，w 是系统的四个状态变量。a、b、c、e 为系统参数。

$$\begin{cases} \dot{x} = a\left(y - x\right) \\ \dot{y} = -xz + cy - W\left(\varphi\right)y \\ \dot{z} = xy - bz \\ \dot{w} = eyz - x \end{cases} \tag{3}$$

使用龙格－库塔方法[10]对式(3)进行仿真，设置系统参数 $a = 9$，$b = 3$，$c = 6$，$m = 0.5$，$n = 0.1$，$e = 0.3$ 仿真步长为 0.01，仿真时间为 4000 秒，状态变量的初值 $\left(x_0, y_0, z_0, w_0\right) = \left(1, 0, 1, 0\right)$，系统的相图如图 1 所示。从相图中可以看出，新系统呈现双涡卷吸引子。



(a) (b)



(c) (d)

Figure 1. Phase portraits of chaotic attractor (a) x-y plane; (b) x-z plane; (c) y-z plane; (d) x-w plane
图 1. 混沌吸引子各平面相图(a) x-y 平面；(b) x-z 平面；(c) y-z 平面；(d) x-w 平面

3. 系统非线性特性分析

3.1. 耗散性分析

对新的系统(3)进行耗散性分析

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -5.5 - 0.1w^2 \tag{4}$$

无论 w 取何值，$\nabla V < 0$，因此系统(2)是耗散的，且以指数 $\mathrm{d}V/\mathrm{d}t = \mathrm{e}^{\left(-5.5-0.1w^2\right)t}$ 的速率收敛，当 $t \to \infty$ 时，系统中的任一体积元将收敛到 0。

3.2. 平衡点及稳定性分析

固定系统参数不变，令新系统的左边等于 0，即式(5)：

$$\begin{cases} 0 = a(y - x) \\ 0 = -xz + cy - W(\phi)y \\ 0 = xy - bz \\ 0 = eyz - x \end{cases} \tag{5}$$

通过求解，可得该混沌系统共有 4 个平衡点：$S_1 = (0,0,0,\alpha)$，$S_2 = \left(\sqrt{b/e}, \sqrt{b/e}, 1/e, \sqrt{(ce - me - 1)/ne}\right)$，$S_3 = \left(-\sqrt{b/e}, \sqrt{b/e}, 1/e, \sqrt{(ce - me - 1)/ne}\right)$，$S_4 = \left(-\sqrt{b/e}, \sqrt{b/e}, 1/e, -\sqrt{(ce - me - 1)/ne}\right)$。

其中 α 为任意实数，因此 S_1 为线平衡点，在平衡点处对系统(2)线性化，得到系统的 Jacobi 矩阵如下：

$$\begin{bmatrix} -a & a & 0 & 0 \\ -z & c - \left(m + nw^2\right) & -x & -2nwy \\ y & x & -b & 0 \\ -1 & ez & ey & 0 \end{bmatrix} \tag{6}$$

对于线平衡点 S_1，其特征方程如式(7)所示：

$$\lambda(\lambda + a)(\lambda + b)\left[\lambda - c + w(\phi)\right] \tag{7}$$

四个特征根分别为 $\lambda_1=0$，$\lambda_2=-a$，$\lambda_3=-b$，$\lambda_4=c-W(\alpha)$，带入参数后求得 $\lambda_1=0$，$\lambda_2=-9$，$\lambda_3=-b$，$\lambda_4=5.5-0.1\alpha^2$，$\lambda_4$ 的值与 α 有关，当 $\alpha>\sqrt{55}\cup\alpha<-\sqrt{55}$ 时，$\lambda_4=5.5-0.1\alpha^2>0$，此时稳定点的类型为指标 1 的鞍点。当 $\alpha>\sqrt{55}$ 或 $\alpha<-\sqrt{55}$ 时，此时稳定点的类型为稳定结点。

平衡点 S_1~S_4 的特征根如表 1 所示：

Table 1. Characteristic roots and types of equilibrium points
表 1. 各平衡点的特征根与平衡点类型

平衡点	特征根	平衡点类型
S_1	0，−9，−3，$5.5-0.1\alpha^2$	$-\sqrt{55}<\alpha<\sqrt{55}$ 指标 1 鞍点。$\alpha>\sqrt{55}$ 和 $\alpha<-\sqrt{55}$ 稳定结点
S_2	7.752，0.008 + 4.779i，−0.898，−0.008 − 4.779i	稳定焦点
S_3	8.378，−0.564 + 4.719i，0.840，−0.564 − 4.719i	指标 1 鞍焦点
S_4	−7.752，−0.008 + 4.779i，−0.008 − 4.779i，−0.898	稳定焦点

3.3. 动力学分析

3.3.1. 初值敏感性

对于系统(3)，为分析系统对初值的敏感性，对初值 y_0 添加微小扰动，并观察新初值下状态变量的动态轨迹。从图 2 中可以看出，状态变量在 7 秒后动态轨迹不再重合，随着时间推移，不同初值下的轨迹差异逐渐变大，说明系统的初值敏感性较好。

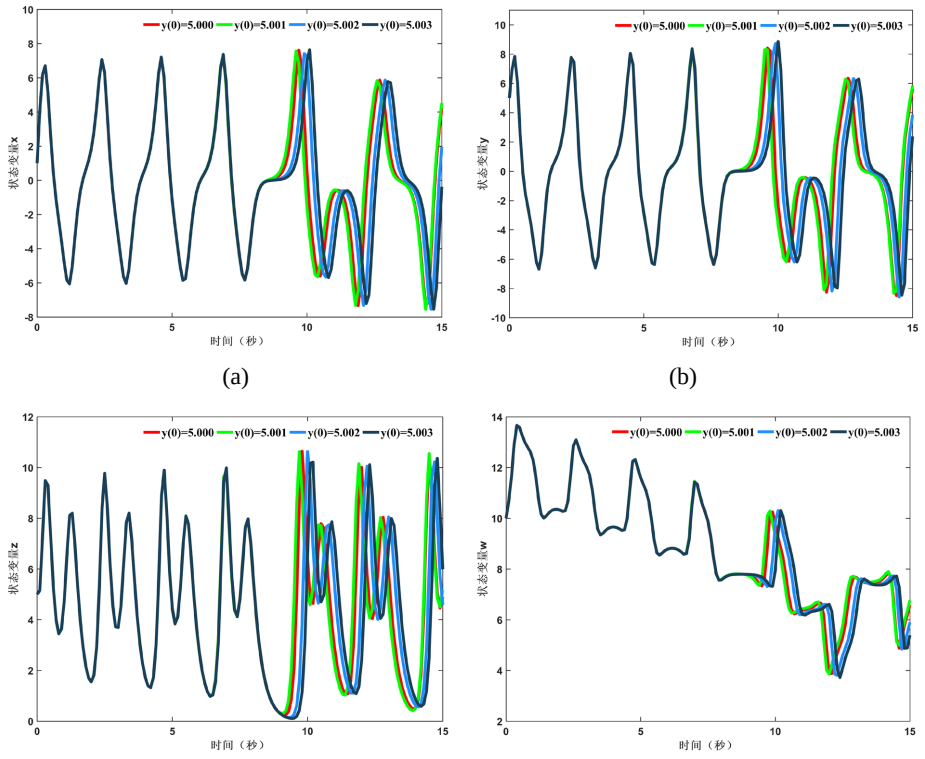


Figure 2. Dynamic trajectory of state variable when initial value changes slightly (a) Variable x; (b) Variable y; (c) Variable z; (d) Variable w
图 2. 初值微小变化时状态变量动态轨迹 (a) 变量 x；(b) 变量 y；(c) 变量 z；(d) 变量 w

3.3.2. 李雅普诺夫指数和维数

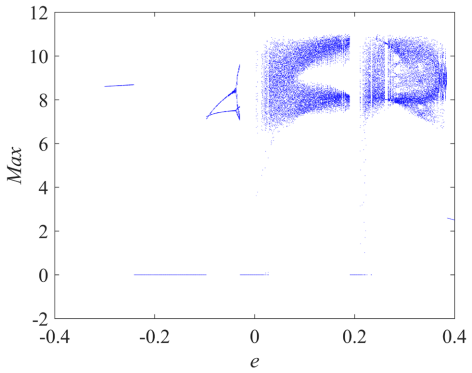
固定系统参数和系统初值不变，利用 Wolf [10]算法求得系统的 4 个李雅普诺夫(Lyapunov Exponent, LE)指数分别为：$LE_1=0.0703$，$LE_2=-0.0027$，$LE_3=0.0144$，$LE_4=-6.7741$。系统具有两个大于 0 的 Lyapunov 指数 LE_1 和 LE_3，系统表现出超混沌状态。系统的分数维如式(8)所示：

$$D_L=3+\frac{\sum_{i=1}^{3}L_i}{|L_4|}=3.0121 \tag{8}$$

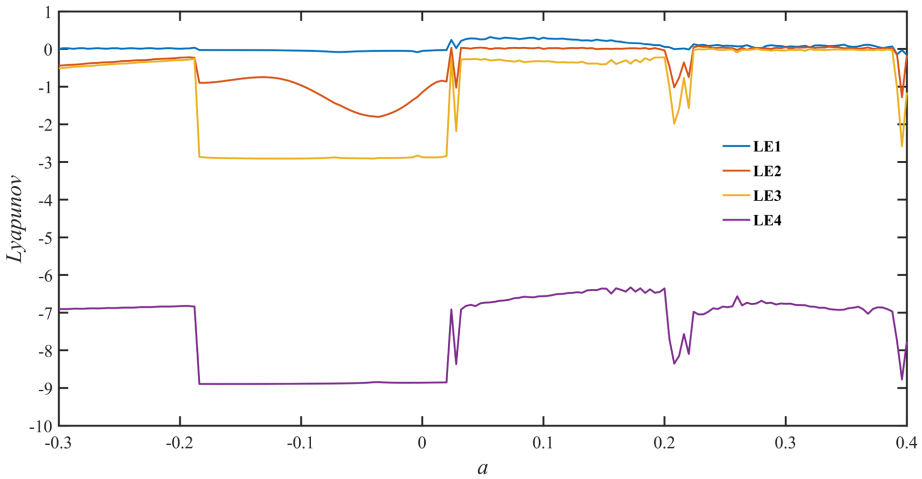
3.3.3. 随参数 e 分岔图

为分析系统随参数 e 变化的系统特征，设置系统(2)初值$(x_0,y_0,z_0,w_0)=(1,0,1,0)$，固定其他参数不变，通过仿真得到系统在参数 e 变化下的分岔图以及 Lyapunov 指数图。可以观察到随参数 e 的变化，系统由周期进入混沌的路径。当 $e=[0,0.38]$ 时，最大的 LE 指数大于 0，说明系统处于混沌状态。其中 $e=[0.24,0.36)$ 时，LE_1 和 LE_2 均大于 0，此时系统处于超混沌状态，当 $e=[-0.24,0.09]$ 和 $e=[0.38,0.40)$ 时，4 个 LE 指数均小于 0，混沌状态消失。

下面在固定参数 $a=9,b=3,c=6,m=0.5,n=0.1$ 条件下，讨论系统(2)随参数 e 变化的系统特征。



(a)

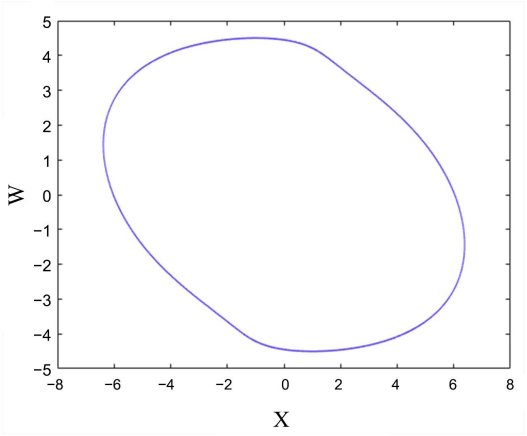


(b)

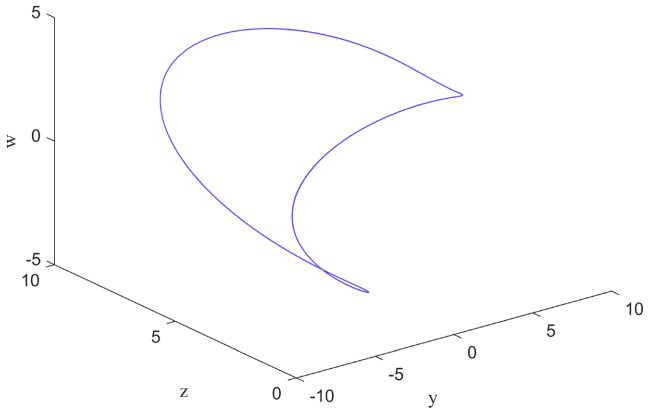
Figure 3. Chaotic dynamics varying with parameterse (a) Bifurcation diagram; (b) Lyapunov exponential spectra

图 3. 随参数 e 变化的混沌动力学 (a) 分岔图；(b) Lyapunov 指数图

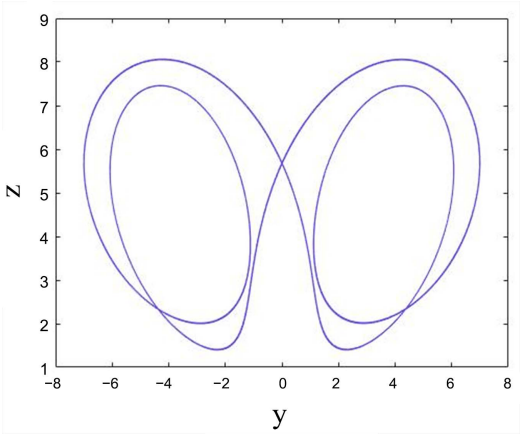
固定其他系统参数不变，取参数 $e=-0.27$ 时，通过观察图 3 的分岔图及 Lyapunov 指数图并结合图 4(a)和图 4(b)可知，在此参数下，系统为周期一状态。取参数 $e=-0.1$。从图 3 以及图 4(c)和图 4(d)可知，在此参数下，系统处于周期二状态。取参数 $e=0.05$，从图 3 以及图 4(e)和图 4(f)可知，在此参数下，系统处于混沌态。取参数 $e=0.2$，从图 3 以及图 4(g)和图 4(h)可知，在此参数下，系统为拟周期态。取参数 $e=0.32$，从图 3 以及图 4(i)和图 4(j)可知，系统为超混沌态。



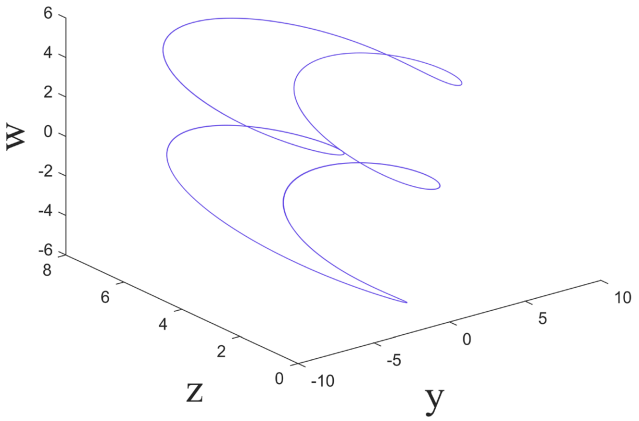
(a)



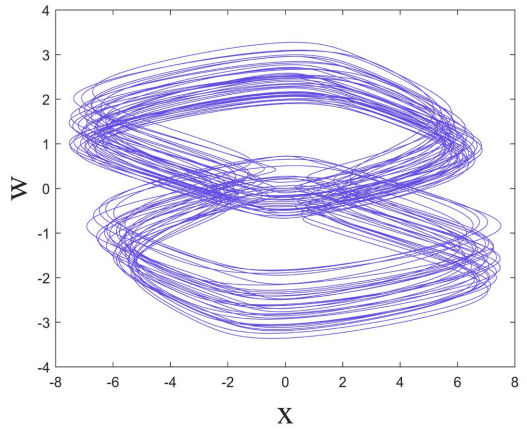
(b)



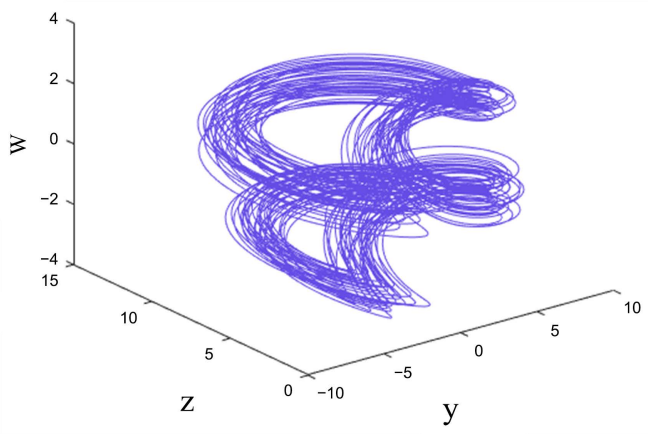
(c)



(d)



(e)



(f)

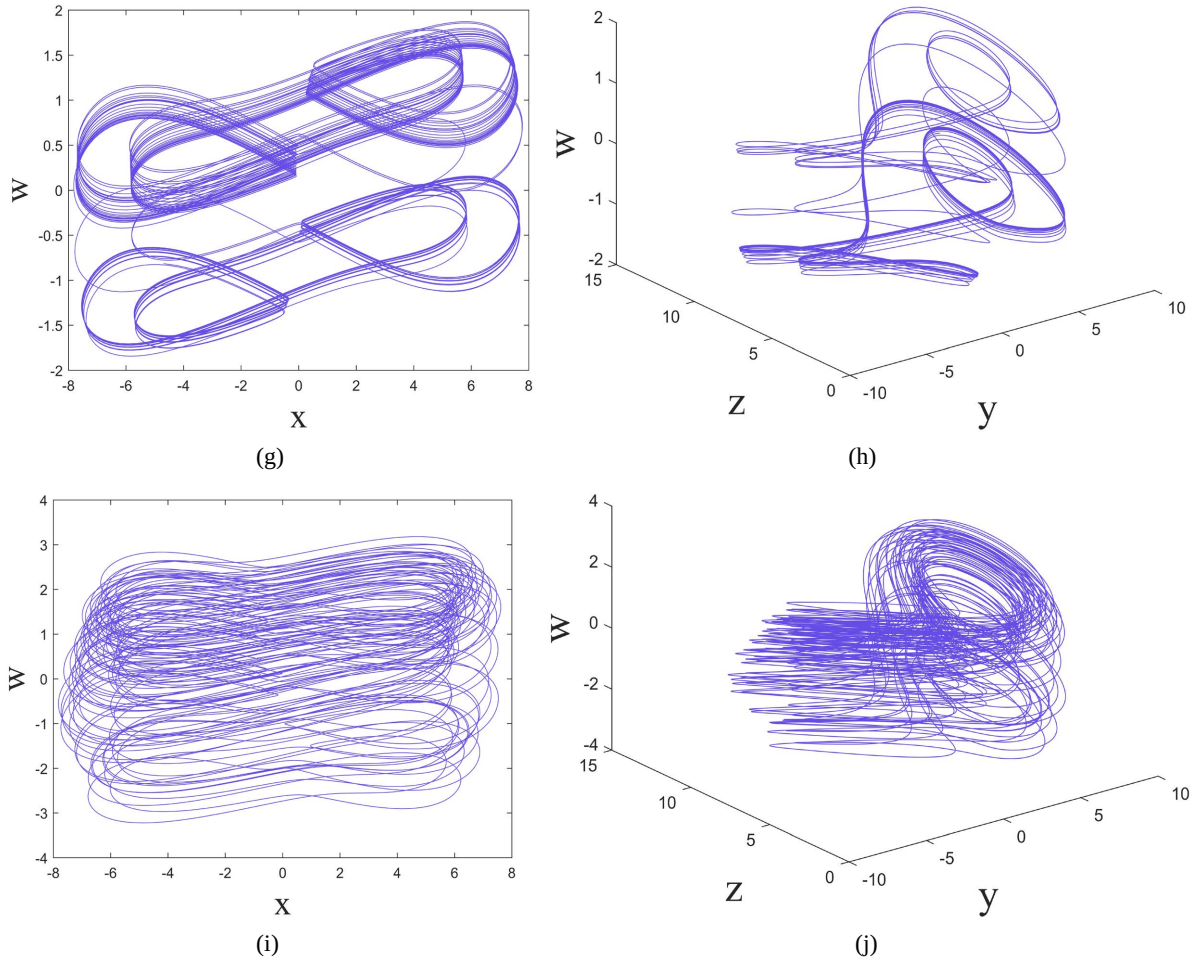


Figure 4. System phase diagram with parameter e (a) $e=-0.27$ x-w plane; (b) $e=-0.27$ y-z-w plane; (c) $e=-0.1$ x-w plane; (d) $e=-0.1$ y-z-w plane; (e) $e=0.05$ x-w plane; (f) $e=0.05$ y-z-w plane; (g) $e=0.2$ x-w plane; (h) $e=0.2$ y-z-w plane; (i) $e=0.32$ x-w plane; (j) $e=0.32$ y-z-w plane

图 4. 随参数 e 变化的系统相图 (a) $e=-0.27$ x-w 平面；(b) $e=-0.27$ y-z-w 平面；(c) $e=-0.1$ x-w 平面；(d) $e=-0.1$ y-z-w 平面；(e) $e=0.05$ x-w 平面；(f) $e=0.05$ y-z-w 平面；(g) $e=0.2$ x-w 平面；(h) $e=0.2$ y-z-w 平面；(i) $e=0.32$ x-w 平面；(j) $e=0.32$ y-z-w 平面

4. 电路实现与仿真

为验证所设计混沌系统的电路可行性，选用电阻、电容、乘法器和 TL082CP 运算放大器等电路元件，在版本为 14.0 的 Multisim 软件中进行仿真。对原系统进行压缩变换，令 $x=2x$，$y=2y$，$z=2z$，$w=w$，将系统转化为式(9)：

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t}=9\left(y-x\right) \\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=-2xz+6y-\left(0.5+0.1\varphi^{2}\right)y \\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=2xy-3z \\ \dfrac{\mathrm{d}w}{\mathrm{d}t}=1.2yz\text{-}2x \end{cases} \tag{9}$$

对系统进行时间尺度变换，使电路参数能更好的与系统匹配，令 $\tau=\tau_0 t$，其中尺度变换因子 $\tau_0=1000$，则系统经过时间尺度变换可转化为式(10)：

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=9000\left(y-x\right)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=-2000xz+6000y-1000\left(0.5+0.1\varphi^2\right)y\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=2000xy-3000z\\ \dfrac{\mathrm{d}u}{\mathrm{d}t}=1200yz\text{-}2000x\end{cases}\tag{10}$$

根据基尔霍夫定律得到式(10)的电路方程为：

$$\begin{cases}\dfrac{\mathrm{d}x}{\mathrm{d}t}=-\dfrac{1}{R_{17}C_1}x-\dfrac{1}{R_{18}C_1}\left(-y\right)\\ \dfrac{\mathrm{d}y}{\mathrm{d}t}=-\dfrac{1}{R_{21}C_2}xz-\dfrac{1}{R_{22}C_2}\left(-y\right)-\dfrac{\left(-0.5-0.1\varphi^2\right)}{R_{23}C_2}\left(-y\right)\\ \dfrac{\mathrm{d}z}{\mathrm{d}t}=-\dfrac{1}{R_{28}C_3}z-\dfrac{1}{R_{29}C_3}\left(-xy\right)\\ \dfrac{\mathrm{d}w}{\mathrm{d}t}=-\dfrac{1}{R_3C_4}x-\dfrac{1}{R_4C_4}\left(-yz\right)\end{cases}\tag{11}$$

其中 $C_1=C_2=C_3=C_4$，均为 10 nF，$R_{19}=R_{20}=R_1=R_2=R_5=R_6=R_7=10$ KΩ，选择系统参数 $a=9$，$b=3$，$c=6$，$m=0.5$，$n=0.1$，$e=0.3$ 时，可求得 $R_{17}=R_{18}=11.1$ kΩ，$R_{21}=R_{29}=5$ kΩ，$R_{22}=16.7$ kΩ，$R_{23}=10$ kΩ，$R_{28}=33.3$ kΩ，$R_3=50$ kΩ，$R_4=8.3$ kΩ。

系统的电路模型如图 5 所示：

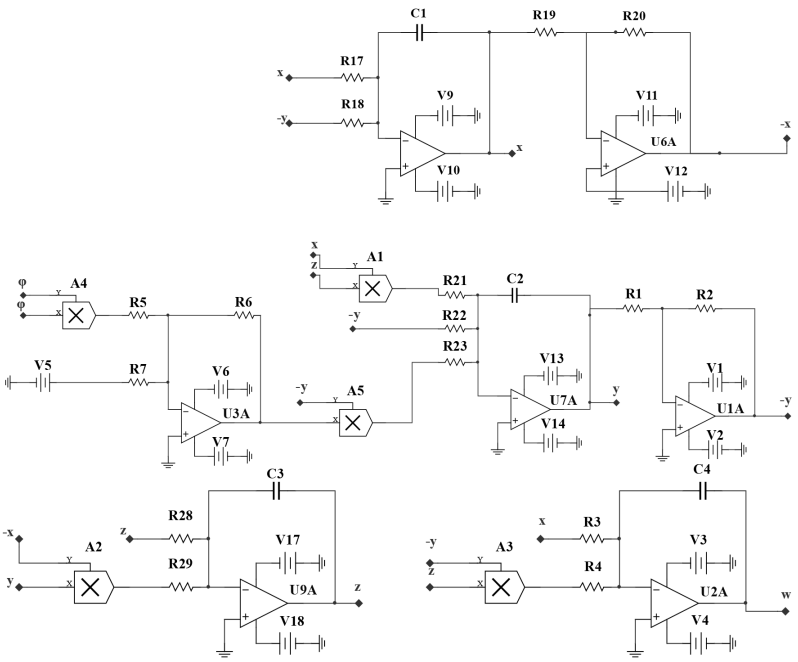


Figure 5. System circuit
图 5. 系统电路

通过模块化设计并在 Multisim 软件上进行仿真验证，从示波器观察到的相图如图 6 所示。电路仿真结果与 Matlab 数值仿真结果相一致，从而证明系统的物理可实现性。

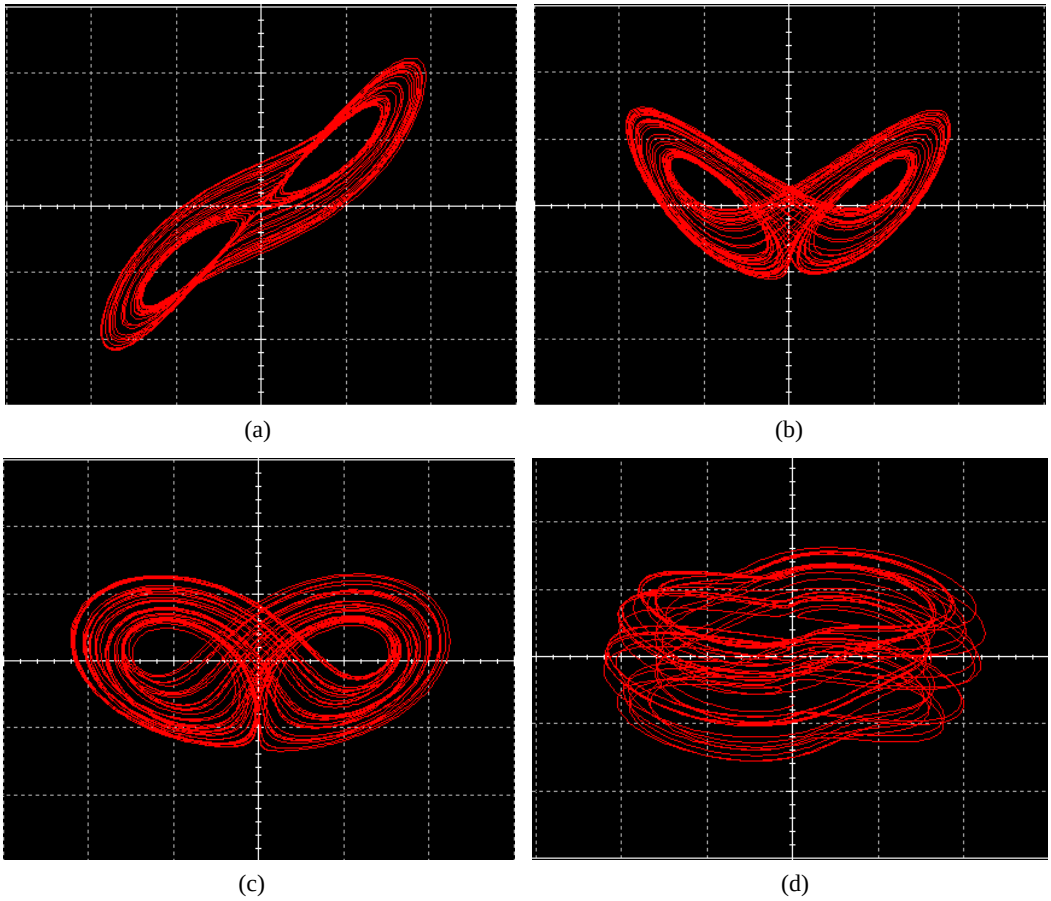


Figure 6. Circuit Simulation result (a) x-y plane; (b) x-z plane; (c) y-z plane; (d) x-w plane
图 6. 电路仿真结果(a) x-y 相图；(b) x-z 相图；(c) y-z 相图；(d) x-w 相图

5. 新混沌系统在图像加密中的应用

采用明文关联的置乱加密算法[15]，将所设计的混沌系统应用到图像加密中，加密过程如图 7 所示。

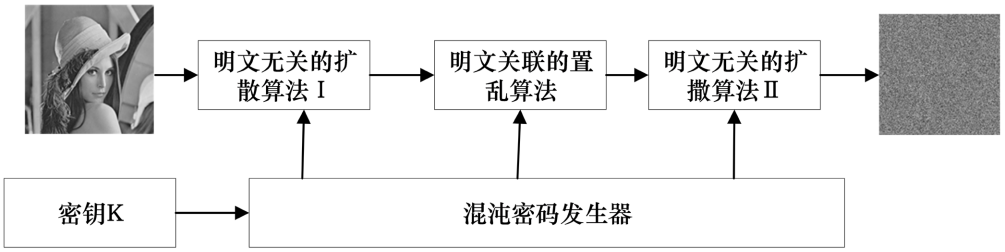


Figure 7. Encryption algorithm
图 7. 加密算法

明文图像经过混沌密码发生器与密钥结合，最终生成密文图像。在混沌密码发生器中，明文图像经过两次扩散和一次置乱，其中置乱算法与明文相关联。

5.1. 混沌密码发生器

通过本文设计的混沌系统来生成 6 个大小为 $M\times N$ 的伪随机矩阵 X、Y、Z、W、U 和 V。密钥 $K=\{x_0,y_0,z_0,w_0,a_1,a_2\}$，其中 x_0、y_0、z_0、w_0 是混沌系统的状态初值，a_1，a_2 是随机数。设置混沌系统的状态初值为密钥 K 中的 x_0、y_0、z_0、w_0，经过 a_1+a_2 次迭代，从而跳过混沌系统的过渡态，然后继续迭代 MN 次，得到 $\{x_i\}$、$\{y_i\}$、$\{z_i\}$、$\{w_i\}$ 4 个伪随机矩阵，最后通过式(12)生成 X、Y、Z、W、U 和 V 共 6 个矩阵。式中 $k=1,2,\cdots,M$，$l=1,2,\cdots,N$。

$$\begin{aligned}
X(k,l)&=floor\left(\left(x_{(k-1)\times N+l}+100 \bmod 1\right)\times 10^{13}\right)\bmod 2^L\\
Y(k,l)&=floor\left(\left(y_{(k-1)\times N+l}+100 \bmod 1\right)\times 10^{13}\right)\bmod 2^L\\
Z(k,l)&=\left(floor\left(z_{(k-1)\times N+l}\times 10^{13}\right)\bmod M\right)+1\\
W(k,l)&=\left(floor\left(\left(w_{(k-1)\times N+l}+100 \bmod 1\right)\times 10^{12}\right)\bmod N\right)+1\\
U(k,l)&=\left(floor\left(\left(x_{(k-1)\times N+l}+y_{(k-1)\times N+l}+100 \bmod 1\right)\times 10^{12}\right)\bmod M\right)+1\\
V(k,l)&=\left(floor\left(\left(z_{(k-1)\times N+l}+w_{(k-1)\times N+l}+100 \bmod 1\right)\times 10^{12}\right)\bmod N\right)+1
\end{aligned}\tag{12}$$

5.2. 加密算法

明文图像 P 的大小为 $M\times N$，借助密码发生器生成的伪随机矩阵 X，将明文图像转换为新的矩阵 $A(i,j)$

$$A(i,j)=P(i,j)+X(i,j)+a_1 \bmod 2^L \tag{13}$$

其中 $i=1$，$j=1$，a_1 是密码发生器中用来跳过混沌系统过渡态的随机数。

步骤一：令 $j=j+1$

$$A(i,j)=P(i,j)+A(i,j-1)+X(i,j)\bmod 2^L \tag{14}$$

将 $P(i,j)$ 转换为 $A(i,j)$，若 $j<N$，则重复步骤一，否则令 $j=1$，$i=i+1$，当 $i\le M$ 时

$$A(i,j)=P(i,j)+sum(A(i-1),1\ to\ N)+X(i,j)\bmod 2^L \tag{15}$$

直到 $i>M$ 时，完成明文图像的第一次扩散得到新的图像 A。

为了抹除图像中相邻像素点的相关性，对扩散后的图像 A 进行置乱，得到置乱后的图像 B。置乱过程如下：

$$m=(U(i,j)+sum\left(A\left(Z(i,j),1\ to\ N\right)\bmod M\right)+1 \tag{16}$$

$$n=\left(V(i,j)+sum\left(A(1\text{ to }M),W(i,j)\right)\bmod N\right)+1 \tag{17}$$

如果 $m=i$ 或 $Z(i,j)$，$n=j$ 或 $W(i,j)$，$Z(i,j)=i$，$W(i,j)=j$ 时原像素点位置不变。否则 $A(i,j)$ 与 $A(m,n)$ 互换位置。对图像 A 中的像素点，按从左到右、从上到下的顺序遍历置乱步骤，最终得到新的置乱图像 B。

步骤三：借助矩阵 Y 对置乱图像 B 中的像素点进行扩散，其扩散过程为从最后一个像素点向前进行扩散，从而将图像 B 转换为矩阵 C，扩散过程如下：

Step1：令 $i=M$，$j=N$，将 $B(i,j)$ 转换为 $C(i,j)$。

$$C(i,j)=B(i,j)+Y(i,j)+r_2 \bmod 2^L \tag{18}$$

Step2：令 $j=j-1$，将 $B(i,j)$ 转换为 $C(i,j)$

$$C(i,j)=B(i,j)+C(i,j+1)+Y(i,j)\bmod 2^L \tag{19}$$

若 $j>1$，重复 Step2。否则 $j=N$， $i=i-1$。如果 $i\geq 1$

$$C(i,j)=B(i,j)+sum\left(C(i+1,1\text{ to }N)\right)+Y(i,j)\bmod 2^L \tag{20}$$

并重复 Step2。当 $i=0$ 时，完成对图像 B 的扩散，此时的矩阵 $C(i,j)$ 即为密文图像。

6. 图像加解密仿真及安全性能分析

6.1. 图像加解密仿真结果

使用分辨率为 512 × 512 的 Lena 和 Baboon 图像进行图像加解密仿真实验，混沌系统为与电路仿真系统一致的系统(2)。为不失一般性，设置密钥 K = [13 48.58 −15.11 22 98 456]对图像进行加密，算法仿真结果如图 8 所示。

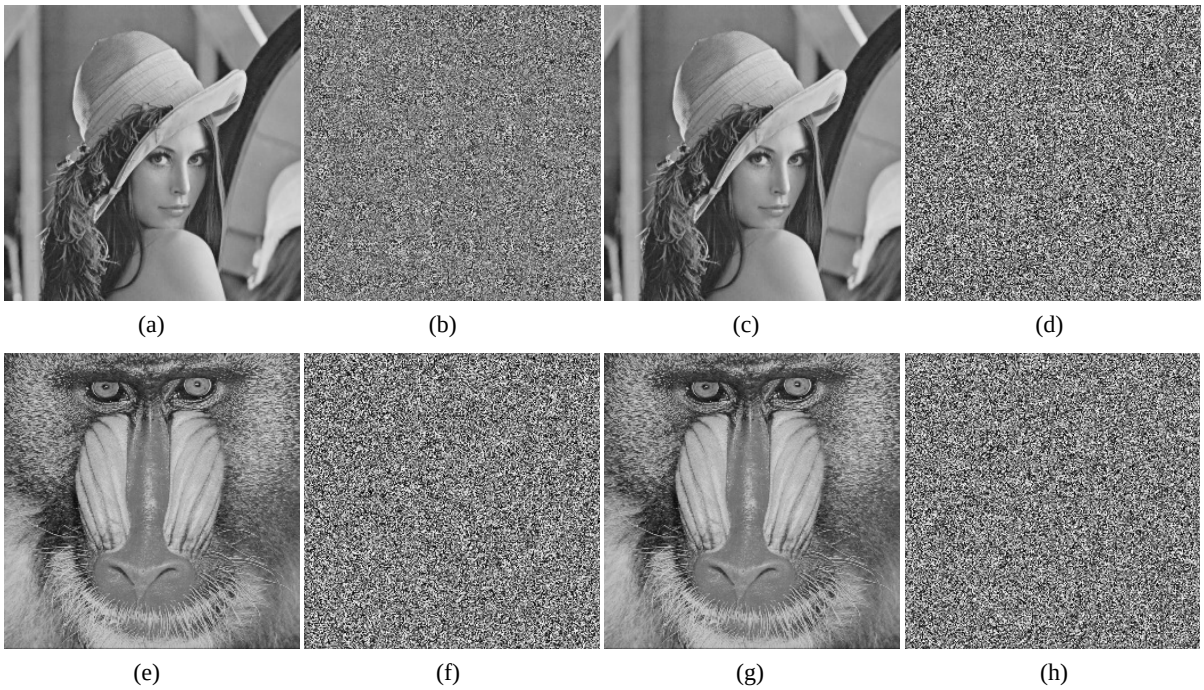
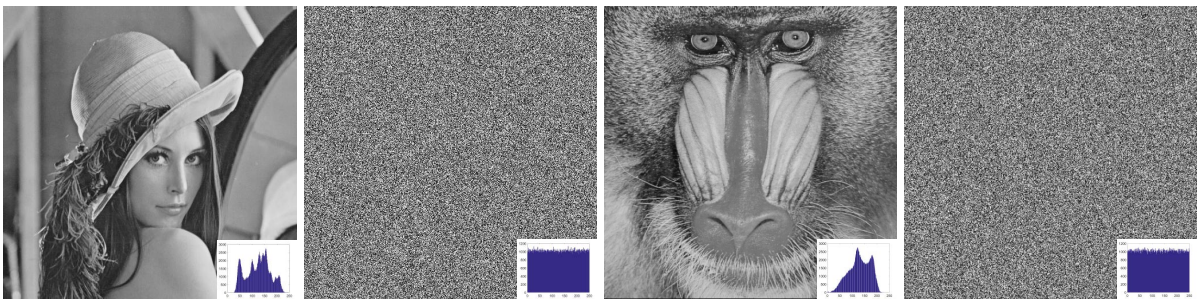


Figure 8. Algorithm simulation result (a) Lena; (b) cryptograph; (c) Correct decryption; (d) Error decryption; (e) Baboon; (b) cryptograph; (g) Correct decryption; (h) Error decryption

图 8. 算法仿真结果(a) Lena 原图；(b) Lena 密文；(c) 正确解密；(d) 错误解密；(e) Baboon 原图；(f) Baboon 密文；(g) 正确解密；(h) 错误解密

6.2. 直方图分析

像灰度级像素的数目通常用直方图来描述[16]。如果攻击者窃取了密文图像，就有可能通过分析密文图像的直方图来提取密文图像中的信息。因此，良好的加密算法，密文的直方图应均匀分布。图 9 显示了原图像与密文的分布直方图，从图中可以看出，与原图像直方图相比较，加密图像的直方图分布均匀，绝大部分统计信息被抹除，从而使得加密图像能有效地抵抗统计攻击。



(a) (b) (c) (d)

Figure 9. Original image and Ciphertext histogram (a) Lena original image; (b) Ciphertext histogram; (c) Baboonoriginal image; (d) Ciphertext histogram
图 9. 原图与密文直方图(a) Lena；(b) 密文直方图；(c) Baboon；(d) 密文直方图

6.3. 信息熵分析

信息熵[17]反映了图像信息的不确定性，信息熵越大，图像的信息量越大，所含的可获得信息越少，计算公式如式(21)所示。

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{21}$$

其中 $p(i)$ 表示灰度值 i 出现的概率，L 表示图像的灰度等级，对于灰度等级为 256 的灰度随机图像，信息熵的理论值为 8，越接近理论值，图像的可视信息越少，表 2 给出了不同算法的信息熵。

Table 2. Information entropy of different algorithms
表 2. 不同算法的信息熵

数量	信息熵
Lena	7.9993
Baboon	7.9994
超混沌 Lorenz	7.9992
文献[18]	7.9975
文献[19]	7.9560
文献[20]	7.9992
文献[21]	7.9993

从表 2 中可以看出，本文算法的信息熵接近于理论值，优于超混沌 Lorenz 加密算法，且优于文献[15]所使用的 DNA 加密算法。

6.4. 密钥空间分析

通常密钥空间越大，抵御穷举攻击的能力越强，加密图像的安全性越好[20]。本文的密钥 K = [13 48.58 −15.11 22 98 456]，x_0、y_0、z_0、w_0 是混沌系统的初值，精度均可达到 10^{-15}，a_1，a_2 是跳过混沌过渡态的迭代次数，值为 0 到 2048，步长为 1 的整数。因此密钥空间的容量可达到 2^{147} 远大于 2^{100}，能有效抵御穷举攻击。表 3 给出了不同算法的密钥空间。

Table 3. Key Spaces for different algorithms
表 3. 不同算法的密钥空间

	信息熵
本文	$\mathbf{2^{247}}$
超混沌 Lorenz	2^{213}
文献[1]	2^{169}
文献[21]	2^{128}
文献[22]	2^{136}

从表 3 中可以看出，本文的密钥空间比传统超混沌 Lorenz 算法提升了 2^{34}，优于文献 18 中的神经网络算法。

6.5. 相关系数分析

明文图像相邻的像素点通常具有很强的相关性，而加密图像水平、垂直、对角方向上相邻像素点间的相关性理论上为 0，也即各像素点间不具有相关性。统计本文与其他文献中 Lena 图像与加密图像在不同方向上的相关性，结果如表 4 所示。

Table 4. Plaintext and ciphertext pixel correlation
表 4. 明文与密文像素相关性

	水平	垂直	对角
Lena 明文	0.9847	0.9721	0.9632
本文密文	−0.0032	0.0037	−0.0009
超混沌 Lorenz	0.0212	0.0244	0.0193
文献[1]	0.0072	0.0055	−0.0008
文献[19]	0.0241	−0.0412	−0.0050
文献[23]	0.0029	0.0080	−0.0003

从表 4 中可以看出，本文相邻系数相关性的表现比传统超混沌 Lorenz 算法有较大的提升。

6.6. 差分攻击分析

差分攻击是一种选择明文攻击，通过分析明文图像差对密文图像差的影响，从而获取加密密钥的一种攻击方式。往往通过定量分析像素改变率(NPCR) [22]和归一化像素平均变化强度(UACI) [22]来度量图像加密算法对差分攻击的抵抗能力。

对于两幅随机图像，同一位置像素点不相同的概率为 99.61%，由于像素点位置的任意性，NPCR 的理论值为 99.61%。由于 NPCR 衡量图像差异性时较为片面，通常还需结合 UACI 共同分析，UACI 通过计算相应位置的像素变化强度来评价图像的差异性，其理论值约为 33.46%。公式如下：

$$NPCR\left(P_1,P_2\right)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}D\left(i,j\right) \tag{22}$$

$$UACI\left(P_1,P_2\right)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\left(\frac{\left|P_1\left(i,j\right)-P_2\left(i,j\right)\right|}{255}\right) \tag{23}$$

式中，P_1，P_2 是两幅大小为 $M\times N$ 的图像，当 $P_1\left(i,j\right)=P_2\left(i,j\right)$ 时，$D\left(i,j\right)=0$，否则 $D\left(i,j\right)=1$。本文通

过加密 Lena 图和改变任一像素点后的 Lena 图，得到两幅加密图像。重复一百次实验，并计算 NPCR 和 UACI 的平均值，如表 5 所示。

Table 5. Average NPCR and UACI of ciphertext images with different algorithms
表 5. 不同算法密文图像平均 NPCR 和 UACI

	NPCR/%	UACI/%
本文 Lena	99.61	33.46
超混沌 Lorenz	99.60	33.44
文献[24]	99.57	33.35
文献[25]	99.61	33.46

可以看出，本文算法的 NPCR 值和 UACI 值十分接近理论值，能有效抵御攻击。

7. 结论

本文通过添加忆阻器构建超混沌系统的方式，将磁控忆阻器添加到 lv 系统中，构建了一个新的具有丰富动力学行为和稳定平衡点的四维忆阻超混沌系统。此外，针对图像安全问题，将该系统与明文关联的图像加密算法结合，对明文像素点进行扩散，置乱再扩散，最终实现图像加密。最后，通过计算密钥空间大小，发现与传统超混沌 Lorenz 系统相比，密钥空间提高了 2^{34}，像素点的相关系数有数量级的降低，安全性得到提高，可广泛应用于图像加密领域。

基金项目

贵州省自然科学基金项目(黔科合基础-ZK [2023]一般 055)；贵州大学人才基金(贵大人基合 201615 号)。

参考文献

[1] Zang, H.Y., Tai, M.D. and Wei, X.Y. (2022) Image Encryption Schemes Based on a Class of Uniformly Distributed Chaotic Systems. *Mathematics*, **10**, Article 1027. https://doi.org/10.3390/math10071027

[2] Zhou, S. and Wang, X.Y. (2021) Simple Estimation Method for the Largest Lyapunov Exponent of Continuous Fractional-Order Differential Equations. *Physica A*: *Statistical Mechanics and Its Applications*, **563**, Article ID: 125478. https://doi.org/10.1016/j.physa.2020.125478

[3] Zhou, S. (2016) Image Compression—Encryption Scheme Based on Hyper-Chaotic System and 2D Compressive Sensing. *Optics & Laser Technology*, **82**, 121-133. https://doi.org/10.1016/j.optlastec.2016.02.018

[4] 张雷, 陈川, 谭淇匀, 等. 结合 S 盒与混沌映射的图像加密算法[J]. 北京邮电大学学报, 2021, 44(6): 40-47.

[5] Wang, X.Y. and Liu, C.M. (2017) A Novel and Effective Image Encryption Algorithm Based on Chaos and DNA Encoding. *Multimedia Tools and Applications*, **76**, 6229-6245. https://doi.org/10.1007/s11042-016-3311-8

[6] Wei, F. and Gang, H.Y. (2018) Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling. *IEEE Photonics Journal*, **10**, 1-15.

[7] Chua, L.O. (1971) Memristor—The Missing Circuit Element. *IEEE Transactions on Circuit Theory*, **18**, 507-519. https://doi.org/10.1109/TCT.1971.1083337

[8] Chua, L.O. and Kang, S.M. (1976) Memristive Devices and Systems. *Proceedings of the IEEE*, **64**, 209-223. https://doi.org/10.1109/PROC.1976.10092

[9] Bao, B.C., Xu, Q., Bao, H. and Chen, M. (2016) Extreme Multistability in a Memristive Circuit. *Electronics Letters*, **52**, 1008-1010. https://doi.org/10.1049/el.2016.0563

[10] 孙夏晨, 明鹏, 李文石. 基于比特全置乱的超混沌图像加密算法[J]. 电子测量技术, 2021, 44(12): 128-132.

[11] Messadi, M., Kemih, K., Moysis, L. and Volos, C. (2023) A New 4D Memristor Chaotic System: Analysis and Imple-

mentation. *Integration*, **88**, 91-100. https://doi.org/10.1016/j.vlsi.2022.09.004

[12] Guo, Y.T., Yao, Z., Xu, Y. and Ma, J. (2022) Control the Stability in Chaotic Circuit Coupled by Memristor in Different Branch Circuits. *AEU—International Journal of Electronics and Communications*, **145**, Article ID: 154074. https://doi.org/10.1016/j.aeue.2021.154074

[13] Hua, M.J., Wu, H.G., Xu, Q., *et al*. (2021) Asymmetric Memristive Chua's Chaotic Circuits. *International Journal of Electronics*, **108**, 1106-1123. https://doi.org/10.1080/00207217.2020.1819440

[14] LÜ, J. and Chen, G. (2002) A New Chaotic Attractor Coined. *International Journal of Bifurcation and Chaos*, **12**, 659-661. https://doi.org/10.1142/S0218127402004620

[15] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社, 2016: 149-159.

[16] Zhang, X.C., Wu, T., Wang, Y.F., Jiang, L.Y. and Niu, Y. (2021) A Novel Chaotic Image Encryption Algorithm Based on Latin Square and Random Shift. *Computational Intelligence and Neuroscience*, **2021**, Article ID: 2091053. https://doi.org/10.1155/2021/2091053

[17] Chen, C., Zhang, H.Y. and Wu, B. (2022) Image Encryption Based on Arnod Transform and Fractional Chaotic. *Symmetry*, **14**, Article 174. https://doi.org/10.3390/sym14010174

[18] Song, C.Y. and Qiao, Y.L. (2015) A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. *Entropy*, **17**, 6954-6968. https://doi.org/10.3390/e17106954

[19] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I. and Zengin, A. (2017) Secure Image Encryption Algorithm Design Using a Novel Chaos Based S-Box. *Chaos, Solitons and Fractals*, **95**, 92-101. https://doi.org/10.1016/j.chaos.2016.12.018

[20] Zhang, Y. (2018) The Unified Image Encryption Algorithm Based on Chaos and Cubic S-Box. *Information Sciences*, **450**, 361-377. https://doi.org/10.1016/j.ins.2018.03.055

[21] Wang, X.Y. and Li, Z.M. (2019) A Color Image Encryption Algorithm Based on Hopfield Chaotic Neural Network. *Optics and Lasers in Engineering*, **115**, 107-118. https://doi.org/10.1016/j.optlaseng.2018.11.010

[22] Tu, G.Y., Liao, X.F. and Xiang, T. (2013) Cryptanalysis of a Color Image Encryption Algorithm Based on Chaos. *Optik*, **124**, 5411-5415. https://doi.org/10.1016/j.ijleo.2013.03.113

[23] Zou, C.Y., Wang, X.Y. and Li, H.F. (2021) Image Encryption Algorithm with Matrix Semi-Tensor Product. *Nonlinear Dynamics*, **105**, 859-876.

[24] Ghazvini, M., Mirzadi, M. and Parvar, N. (2020) A Modified Method for Image Encryption Based on Chaotic Map and Genetic Algorithm. *Multimedia Tools and Applications*, **79**, 26927-26950.

[25] Li, M., Wang, M.D., Fan, H.J., An, K. and Liu, G.Q. (2022) A Novel Plaintext-Related Chaotic Image Encryption Scheme with No Additional Plaintext Information. *Chaos, Solitons and Fractals*, **158**, Article ID: 111989. https://doi.org/10.1016/j.chaos.2022.111989