基于四维超混沌系统的图像加密算法设计

夏 磊
安徽理工大学 电气与信息工程学院,安徽 淮南 232001

摘 要:目的 针对构造具有混沌特性的复杂四维超混沌系统以及提高图像数据保护的安全问题,提出在经典系统 Lü 基础之上,引入一个状态反馈控制器构建只有一个平衡点的四维超混沌系统,通过理论分析四维超混沌系统的动力学特性并设计超混沌加密算法以保护图像加密后的数据安全性。**方法** 利用 Matlab 软件对该超混沌系统进行数值仿真,如系统耗散性和平衡点稳定性、Lyapunov 指数谱和分岔图、Poincare 截面;同时设计了四维超混沌系统的模拟电路,通过基本的电路元件,以运算放大电路为基础搭建超混沌系统的模拟电路模型;最后将四维超混沌系统与置乱-扩散算法相结合,利用超混沌系统混沌序列的复杂性和伪随机性设计了一种高效且安全的四维超混沌图像加密算法,通过 Matlab 软件对明文和密文图像进行直方图、相邻像素相关性、信息熵和抗攻击性分析。**结果** 仿真数据表明:该四维超混沌系统具有周期、混沌、超混沌吸引子的复杂混沌行为,同时利用 Multisim 软件验证电路实现的准确性和物理可实现性。图像加密实验数据表明:该超系统对混沌密钥和明文非常敏感,超混沌加密算法的安全性更高,同时在保证安全性的前提之下,可以有效抵御统计攻击和差分攻击,也加快了图像解密和加密的速度。**结论** 实验结论表明:该四维超混沌系统在不同参数下可以表现出复杂的动力学特性,利用超混沌系统产生的混沌序列设计的混沌加密算法安全性很高。

关键词:超混沌系统;Lyapunov 指数;电路仿真;图像加密
中图分类号:O415.5;TP309.7 **文献标识码:**A doi:10.16055/j.issn.1672-058X.2024.0005.004

Design of Image Encryption Algorithm Based on Four-dimensional Hyperchaotic System

XIA Lei
School of Electrical and Information Engineering, Anhui University of Science & Technology, Anhui Huainan 232001, China

Abstract: Objective To construct a complex four-dimensional hyperchaotic system with chaotic characteristics and to improve the security of image data protection, a four-dimensional hyperchaotic system with only one equilibrium point by introducing a state feedback controller based on the classical system Lü was proposed and constructed. The dynamics of the four-dimensional hyperchaotic system was analyzed theoretically, and a hyperchaotic encryption algorithm to protect the data security after image encryption was designed. **Methods** Numerical simulations of this hyperchaotic system, such as system dissipation and equilibrium point stability, Lyapunov exponential spectrum and bifurcation diagram, and Poincare cross-section, were performed using Matlab software. Meanwhile, the simulation circuit of the four-dimensional hyperchaotic system was designed, and the simulation circuit model of the hyperchaotic system was built based on the operational amplifier circuit through the basic circuit components. Finally, the four-dimensional hyperchaotic system is combined with the dislocation-diffusion algorithm to design an efficient and secure four-dimensional hyperchaotic image encryption algorithm by using the complexity and pseudo-randomness of the chaotic sequence of the hyperchaotic system, and the histogram, adjacent pixel correlation, information entropy and attack resistance of plaintext and ciphertext images were analyzed by Matlab software. **Results** Simulation data showed that this four-dimensional hyperchaotic system has

收稿日期:2023-03-05 **修回日期:**2023-05-18 **文章编号:**1672-058X(2024)05-0028-10
作者简介:夏磊(1998—),男,安徽合肥人,硕士研究生,从事混沌电路系统研究.
引用格式:夏磊. 基于四维超混沌系统的图像加密算法设计[J]. 重庆工商大学学报(自然科学版),2024,41(5):28—37.
XIA Lei. Design of image encryption algorithm based on four-dimensional hyperchaotic system[J]. Journal of Chongqing Technology and Business University (Natural Science Edition), 2024, 41(5): 28—37.

complex chaotic behavior with periodic, chaotic, and hyperchaotic attractors, while Multisim software was used to verify the accuracy and physical realizability of the circuit implementation. The experimental data of image encryption show that the super system is very sensitive to chaotic keys and plaintexts, and the hyperchaotic encryption algorithm is more secure. Meanwhile, it can effectively resist statistical and differential attacks under the premise of ensuring security, and it also speeds up image decryption and encryption. **Conclusion** The experimental conclusion shows that this four-dimensional hyperchaotic system can exhibit complex dynamics under different parameters, and the chaotic encryption algorithm designed by using the chaotic sequence generated by the hyperchaotic system has high security.

Keywords: hyperchaotic system; Lyapunov exponent; circuit simulation; image encryption

1 引　言

混沌是一种特殊的动态行为,指非线性系统动力学中因初始条件极其敏感导致的复杂运动模式。尽管这种运动状态是确定的,但系统的微小变化足以导致其呈现出看似随机的行为。Lorenz[1]在研究气象中的流体现象时,结合动力系统理论中的空间位置、速度与时间变化之间的关系构建出了一个三维动力系统,即 Lorenz 系统。学者 Rossler[2]基于 Lorenz 混沌系统,引入多个非线性项,构建一种新的混沌系统,通过实验验证发现该系统在两个方向上产生了不稳定的混沌吸引子,并将这种产生新混沌现象的系统命名为超混沌系统。由一组状态参数演化而成的普通混沌系统,随着时间的推移会呈现出不可预测的状态,而超混沌系统则进一步增加了系统的复杂性和随机性。与普通的混沌系统相比,相当于进行了多次混沌处理,从而该超混沌系统的输出信号特征更加复杂和难以预测,在实际应用中更能满足通信保密、图像加密等领域的需求[3-4]。

近几十年来,超混沌系统的研究和构造一直备受关注。Liu 等[5]提出以符号函数为基础建立三维混沌系统,设置不同的参数,可以观察到双翼和四翼的混沌吸引子;Jian 等[6]在三维自治混沌系统中加入忆阻器和交叉积项,使得新超混沌系统拥有了一个具有线平衡点的四涡卷吸引子;欧斌等[7]提出利用共轭 Lorenz 系统的反馈控制技术获得 2 个非线性项四维超混沌系统,验证系统的 Hopf 分叉并研究超混沌系统的动力学特征;牛亚星等[8]提出利用反馈控制器构建 Shil'nikov 型超混沌系统,验证混沌吸引子的最终有界性。经过对已有研究的总结,可以看到超混沌系统在研究和应用方面越来越广泛。然而如何构建结构简单、混沌特性复杂的超混沌系统,仍然是研究者需要面对和解决的一个重要挑战。因此,为了进一步提高超混沌系统的安全性和可靠性,需要深入研究和探索超混沌系统的结构与生成方法。

图像加密的信息安全一直以来都是非线性科学领域研究的热点内容。随着计算机技术的不断发展进步和攻击手段的日益复杂多样化,传统的图像加密算法已经难以满足当今信息安全的保护需求。因此,如何提高图像加密算法的安全性和实用性成为一个亟待解决的问题。Hussainl 等[9]提出在切比雪夫混沌映射的基础之上,结合多个混沌 S 盒设计出图像加密算法,但是由于加密算法本身存在一些安全缺陷,导致算法加密后的密文图像无法抵抗选择的明文攻击,导致加密效果不是很好;Liu 等[10]提出在正弦逻辑映射中与平面排列相结合,设计了一种新的量子图像加密算法,该加密算法的密文图像有着很高的信息熵,但是应对高裁剪攻击时,算法的加密弊端就显现出来了,密文图像很容易被破解;Elamir 等[11]提出将 DNA 计算编码与混沌映射规则组合成的混沌密钥加密算法,但是由于混沌维数比较低,密钥空间较小,所以导致该算法易受到攻击,安全性不高;陈宝文等[12]提出将混沌系统产生的混沌系列与 Arnold 算法相结合设计图像加密算法,利用混沌序列进行线性扩散,完成图像的加密,但是该算法没有消除置乱的周期性,会导致加密效果不好;李付鹏等[13]提出将 Tent 映射与置乱算法相结合用于图像加密,通过混沌序列对图像置乱得到密文图像,而该算法只是将像素点重新排列来加密,没有进行扩散处理,导致图像加密后相关性之间的特征没有改变,容易被破解。

针对上述超混沌系统构造问题以及图像加密中出现的问题,本文提出一种新的四维超混沌系统,以 Lü 系统为基础,引入状态反馈控制器,对原有的基础方程进行优化,设计出四维超混沌系统。在固定其余参数,改变一个初始参数的条件下,系统会表现出周期、混沌、超混沌的丰富混沌特性,相较于一般的高维混沌系统,该系统的方程结构简单且有复杂的动力学特性,也易于实际电路的搭建。同时基于置乱-扩散算法的基础,将超混沌系统生成的复杂性极高的超混沌序列加入算法中,设计了一种高度安全的超混沌图像加密算法。在该算法中,混沌序列与置乱和扩散过程相结合,增大了密钥空间,加强了原有加密算法的抗攻击性和不可预测性,有效地保证了密文图像的安全性和完整性。在第三、第四节中,对四维超系统混沌动力学行为

进行了深入分析,首先分析了平衡点的个数以及稳定性、耗散性、Lyapunov 指数及维数,通过绘制 Poincaré 截面图进行进一步研究,并通过改变系统参数,分析在不同参数下的混沌特性,验证该系统具有丰富的动力学特性。第五节中,利用基本的电路元件在 Multisim 搭建出其相应的电路模型,验证该系统的准确性。第六节中,将新系统与加密算法相结合应用到图像加密上,测试加密性能。

2 新四维超混沌电路模型

经典 Lü 系统的代数方程是 Lorenz 系统和 Chen 系统之间的转换系统,可描述为式(1):

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

式(1)中,a、b、c 为实参数,当 $a=36$,$b=3$,$c=20$ 时,系统处于混沌状态。结合经典的 Lü 系统,在式(1)的基础之上引入状态变量控制器 $\dot{w}$,构造四维超混沌系统。相较于三维混沌系统,四维超混沌系统包含 4 个状态变量,在更多的系统参数调控下,使得其具有更高的系统复杂性。由于四维超混沌系统的状态空间更大,可以产生更加复杂的混沌序列,使得混沌系统在图像加密领域应用更加广泛,四维超混沌系统表达式如式(2):

$$\begin{cases}\dot{x}=a(y-x)+w\\ \dot{y}=bx-xz+cy\\ \dot{z}=xy-dz\\ \dot{w}=-ex\end{cases} \tag{2}$$

式(2)中,x、y、z、w 为状态变量,a、b、c、d、e 为系统的参数,当 $a=30$,$b=35$,$c=7$,$d=9$,$e=0.4$ 时,处于混沌状态,可得到该超混沌系统的相轨图如图 1 所示。

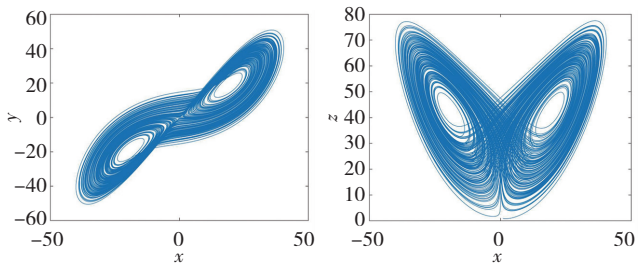


图 1 $x-y$ 平面和 $x-z$ 平面超混沌相轨图

Fig. 1 Hyperchaotic phase track diagram in $x-y$ plane and $x-z$ plane

3 新超混沌系统的动力学分析

3.1 耗散性

当系统式(2)取 $a=30$,$b=35$,$c=7$,$d=9$,$e=0.4$ 时,代入式(3):

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

由式(3)可得 $a-c+d>0$ 时,系统为耗散系统,当 $\nabla V<0$ 时,系统式(2)是耗散的。

3.2 平衡性和稳定性分析

为了计算系统的平衡点,将系统左侧等于 0 可得式(4):

$$\begin{cases}0=a(y-x)+w\\ 0=bx-xz+cy\\ 0=xy-dz\\ 0=-ex\end{cases} \tag{4}$$

由式(4)可解得系统具有唯一的平衡点 $S_0=(0,0,0,0)$,在所构造系统的平衡点处对其线性化,可以得到 Jacobin 矩阵式(5):

$$\boldsymbol{J}_0=\begin{pmatrix}-a & a & 0 & 1\\ b & c & 0 & 0\\ 0 & 0 & -d & 0\\ -e & 0 & 0 & 0\end{pmatrix} \tag{5}$$

根据式(5),可以得到系统的特征方程如式(6)所示:

$$(\lambda+d)(\lambda^3+(a-c)\lambda^2-(ac+ab-d)\lambda-ec)=0 \tag{6}$$

令 $P_1=a-c$,$P_2=-(ab+ac-e)$,$P_3=-ec$,可得方程式(7):

$$\lambda^3+P_1\lambda^2+P_2\lambda+P_3=0 \tag{7}$$

由劳斯-赫尔维茨(Routh-Hurwitz)判据可知,仅当 $P_1>0$,$P_2>0$,$P_3>0$,$P_1P_2-P_3>0$ 时,该平衡点是稳定的。将上述参数代入不等式可知,系统式(2)在平衡点处是不稳定的。

3.3 Lyapunov 指数及维数

Lyapunov 表示吸引子在相邻轨道沿该系统方向平均发散或收敛的快慢,是判断混沌的有效工具。Lyapunov 指数的计算采用著名的 wolf 算法,通过对系统的初始状态进行扰动,根据扰动向量在时间演化中的变化量,构造一种矩阵来描述扰动向量之间的关系,并从中计算出 Lyapunov 指数。代入系统式(2)参数,设置初值为(1, 1, 1, 1),可以计算出 Lyapunov 分别为 2.065 4、0.015 1、−0.039 4、−34.041 2。

同时,该四维超混沌系统的维数计算结果为分数,表明该系统是混沌系统,如式(8):

$$\boldsymbol{D}_L=j+\frac{1}{|L_{j+1}|}\sum_{i=1}^{j}L_i=3.059\ 9 \tag{8}$$

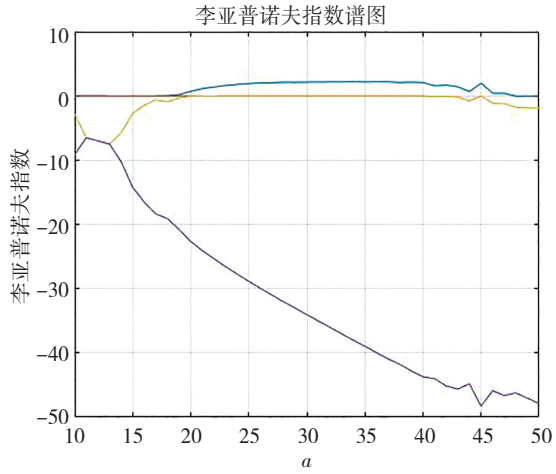
4 系统参数的影响

超混沌系统的演化过程是非常敏感的,当系统的参数值发生改变时,会影响系统平衡点的稳定性,进而导致系统的动力学特性发生改变。

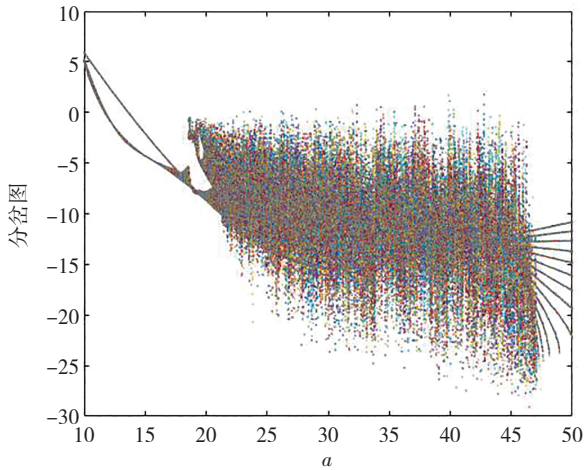
4.1　参数变化对系统的影响

随着参数的改变,系统的稳定性也会发生变化。为了更好地观察和分析系统的状态变化,可以利用 Lyapunov 指数谱及分岔图进行研究。其中,根据 Lyapunov 指数谱,以 0 为基准,根据系统数值大于或小于 0 的个数可以判定系统的稳定状态。而分岔图呈现了系统的混沌特性和周期。通过这两个工具可以更好地了解系统的动态变化,这对更好地研究超混沌系统的运动特性非常有帮助。

固定参数 $b=35$,$c=7$,$d=9$,$e=0.4$,改变参数 a,如图 2 所示。当 $a\in(10,\ 22.8)$ 时,Lyapunov 指数大于 0 的数只有一个,系统处于混沌状态;当 $a\in(22.81,\ 40)$ 时,Lyapunov 指数大于 0 的数有两个,系统处于超混沌状态;$a\in(40,\ 48)$ 时,Lyapunov 指数大于 0 的数只有一个,系统处于混沌状态;$a\in(48,\ 50)$ 时,Lyapunov 指数不会大于 0,系统处于周期态。



(a) Lyapunov 指数谱

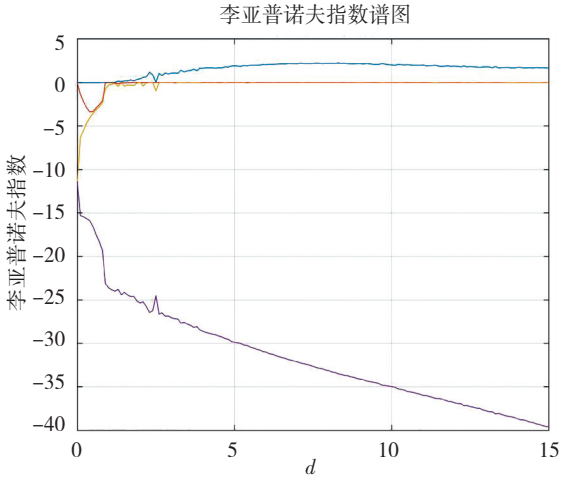


(b) 分岔图

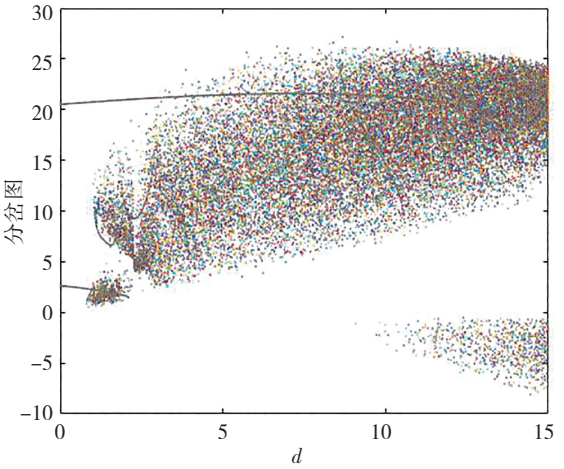
图 2　系统式(2)在参数 a 的 Lyapunov 指数谱和分岔图

Fig. 2　Lyapunov exponential spectrum and bifurcation plot of system (2) with parameter a

固定参数 $a=30$,$b=35$,$c=7$,$e=0.4$,改变参数 d,如图 3 所示。当 $d\in(0,\ 1.2)$ 时,Lyapunov 指数都不大于 0,系统处于周期态;当 $d\in(1.2,\ 2.19)$ 时,Lyapunov 指数大于 0 的数只有一个,系统处于混沌状态;当 $d\in(2.19,\ 2.24)$ 时,Lyapunov 指数大于 0 的数有两个,系统处于超混沌状态;当 $d\in(2.24,\ 2.58)$ 时,Lyapunov 指数不会大于 0,系统处于周期态;当 $d\in(2.58,\ 15)$ 时,系统处于超混沌和混沌相互转化的状态。



(a) Lyapunov 指数谱



(b) 分岔图

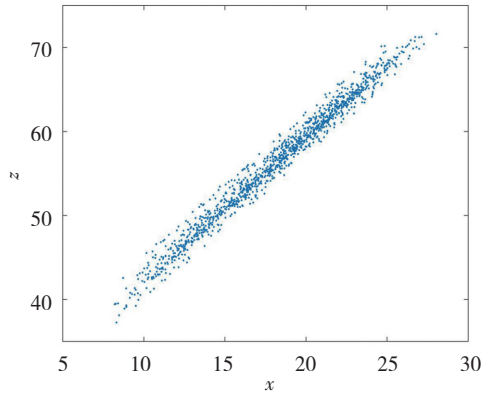
图 3　系统式(2)在参数 d 的 Lyapunov 指数谱和分岔图

Fig. 3　Lyapunov exponential spectrum and bifurcation plot of system (2) with parameter d

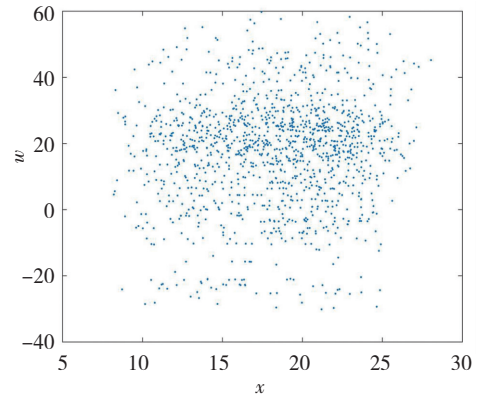
4.2　Poincaré 截面图

Poincaré 截面是一种有效区分系统运动状态的方法,通过观察相空间上截点的分布情况,来判断系统运动的性质。当 $a=30$,$b=35$,$c=7$,$d=9$,$e=0.4$ 时,观察超混沌系统在截面 $y=2$ 上不同平面的映射结果,仿真如图 4 所示。图 4 中截点的分布是成片的密集点,由此可判断系统是超混沌的。同时为了表示状态变量在时间轴上的变化情况,根据初始参数,设系统初始值为 $(1,\ 1,\ 1,\ 1)$,状态变量 $x(t)$ 和 $y(t)$ 的时域波形仿真如图 5 所示。可以观察到状态变量 $x(t)$ 在 $(0,\ 60)$ 范围

内趋于平稳,在(60, 110)范围内有波动,在(110, 160)范围内趋于稳定,在(160, 200)范围内波动明显。可以观察到$y(t)$在(0, 75)范围内有波动,在(75, 120)范围趋于稳定,在(120, 200)范围内波动明显。



(a) x–z 平面



(b) x–w 平面

图 4 超混沌系统的 Poincaré 截面

Fig. 4 Poincaré cross sections for hyperchaotic systems

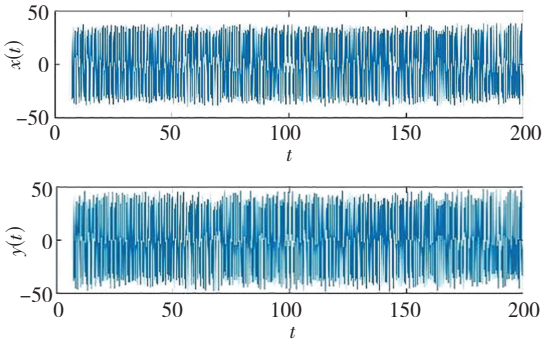


图 5 $x(t)$和$y(t)$超混沌系统时序图

Fig. 5 Timing diagrams for $x(t)$ and $y(t)$ in the hyperchaotic system

5 仿真电路分析

本文通过模拟电路仿真分析可以观察所提出超混沌系统的复杂动力学行为。电路由运算放大器、乘法器、电阻、电容组成,利用 Multisim 软件实现该混沌系统电路模拟。由于运算放大器的输出信号在达到一定的电压或电流值后会饱和,影响系统的动态范围,为了避免这个问题,采用变量代换的方法进行时间尺度的转换。

令 $\tau=\tau_0 t$,其中 $\tau_0=100\ \mu s$,为时间尺度转换因子,参数 $a=30, b=35, c=7, d=9, e=0.4$,则系统式(2)可以表示为式(9):

$$\begin{cases}\dot{x}=-3\ 000x+3\ 000y+100w\\ \dot{y}=3\ 500x-10\ 000xz+700z\\ \dot{z}=10\ 000xy-900z\\ \dot{w}=-40x\end{cases} \tag{9}$$

同时可以设计出电路原理图如图 6 所示,从而推导出电路方程式(10),可计算出电阻、电容的值如下:

$C_1=C_2=C_3=C_4=100$ NF, $R_1=R_2=3.33$ KΩ

$R_3=100$ KΩ, $R_4=2.86$ KΩ, $R_5=14.29$ KΩ

$R_6=R_8=100$ KΩ, $R_7=11.11$ KΩ

$R_9=250$ KΩ, $R_{10}=R_{11}=10$ KΩ

$R_{12}=R_{13}=R_{14}=R_{15}=10$ KΩ

$$\begin{cases}\dfrac{dx}{dt}=-\dfrac{1}{R_1C_1}x+\dfrac{1}{R_2C_1}y+\dfrac{1}{R_3C_1}w\\ \dfrac{dy}{dt}=-\dfrac{1}{R_4C_2}x+\dfrac{1}{R_5C_2}z-\dfrac{1}{R_6C_2}xz\\ \dfrac{dz}{dt}=-\dfrac{1}{R_7C_3}z+\dfrac{1}{R_8C_3}xy\\ \dfrac{dw}{dt}=-\dfrac{1}{R_9C_4}x\end{cases} \tag{10}$$

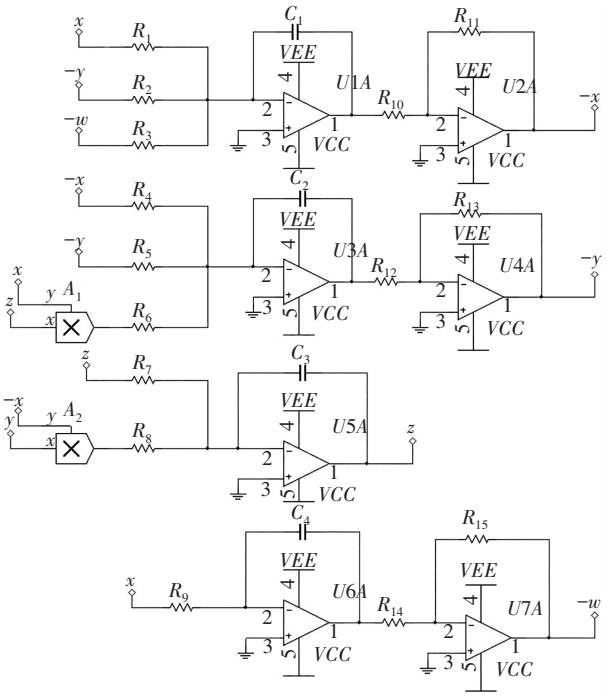
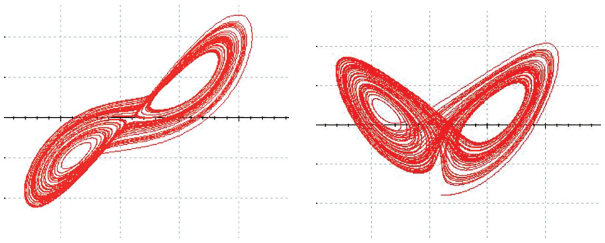


图 6 电路原理图

Fig. 6 Schematic diagram of circuits

将观察到的软件 Multisim 模拟电路中示波器的图

像与数值仿真结果与图 1 进行对比,可知两个图像是一样的,如图 7 所示。证明系统搭建的电路是准确且可以物理实现的。



(a) x-y 平面　　(b) x-z 平面

图 7　电路仿真图

Fig. 7　Circuit simulation diagrams

6　图像加密算法设计

6.1　加密算法原理

四维超混沌图像加密算法是在置乱和扩散的框架体系中完成的,其中置乱算法采用无重复置乱算法,扩散算法采用加取模运算。混沌密钥主要由一组二进制位(比特)或其他数据格式组成,在确定初始值(1, 1, 1, 1)的情况下,通过归一化处理将实数值序列映射在[0, 1]区间内,再进行二值化处理,将归一化实数进行取整,形成一个只包含 0 和 1 的 329 个字符串的不规则排序比特序列。

加密的主要思路:首先使用四阶龙格-库塔法将混沌微分方程转化为差分方程,通过多次迭代计算,得到混沌序列的数字输出,从而得到适合图像加密的超混沌系统混沌伪随机序列 S_1 和 S_2。S_1 序列用于图像加密中的置乱过程,得到密文图像 A,再经过结合 S_2 序列的扩散得到最终的密文图像 B。

Step1　在置乱过程中,将图像由二维矩阵转换为一维向量,借助超混沌系统产生长度为 $M\times N$ 的伪随机序列 S_1,然后 S_1 中重复出现的伪随机数只保留一个,将集合 $i=\{1, 2, \cdots, MN\}$ 中没有出现在 S_1 中的数值按由小到大的顺序添加到 S_1 的末尾,这就避免了图像经历过多次交换位置后回到原位,最后将 $B(S_i)$ 与 $B(S_{MN-i+1})$ 交换位置,完成置乱得到中间密文图像 A。

Step2　扩散过程包含前向扩散和后向扩散。其中,将中间密文图像 A 作为前向扩散加密的输入明文图像,采用加取模运算,借助超混沌系统的伪混沌序列 S_2,将该明文图像分散到 S_2 序列中,可以实现对明文的扩散,如式(11):

$$C_i=(C_{i-1}+S_i+P_i)\bmod 256 \tag{11}$$

式(11)中,C_i 是密文图像,S_i 是混沌序列,P_i 是明文图像。在该扩散算法中,中间密文图像 A 就是 P_i。由于前向扩散会使得中间密文图像的信息分布不均匀,所以需要利用后向扩散使得明文图像的每一点像素信息都扩散到每个密文像素点,如式(12):

$$C_i=(C_{i+1}+S_i+P_i)\bmod 256 \tag{12}$$

Step3　最后将加密后的密文图像再由一维向量转换为二维矩阵,从而得到最终加密后的密文图像 C。

解密算法是对上述算法的逆过程,具体步骤如下:

Step1　采用逆后向扩散算法,i 从 MN 到 1,密文图像 C,混沌序列 S_2 即为式(13)中的 S,P 为中间图像,算法计算为式(13):

$$P_i=(2\times 256+C_i-C_{i+1}-S_i)\bmod 256 \tag{13}$$

Step2　逆前向扩散算法,i 从 1 到 MN,密文图像 C 为式(13)中的中间图像 P,混沌序列 S_1 即为式(14)中的 S,P 为经过逆扩散过程的图像。算法计算如式(14):

$$P_i=(2\times 256+C_i-C_{i-1}-S_i)\bmod 256 \tag{14}$$

Step3　逆置乱算法。以从后向前的顺序置乱密文图像,再将得到的图像由一维向量转为二维矩阵,就得到还原后的灰度图像。

相较于传统的置乱-扩散算法,该算法中加入不可预测性的混沌序列可以使加密数据具有高维和高熵的特性,从而加强了加密算法的复杂度,即使在传输过程中部分数据被窃取,也不会对加密数据的整体性造成影响,因此可以有效抵御攻击,从而提高加密算法的安全性。

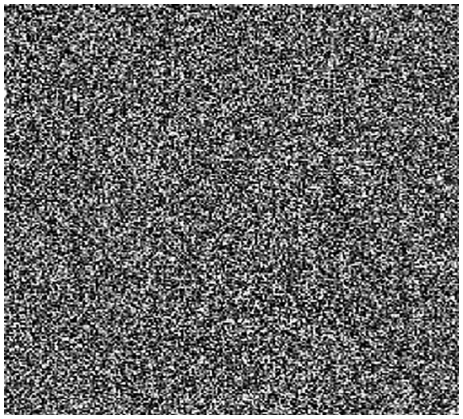
6.2　密钥空间

以超混沌系统的初始值作为密钥,即 $K=\{x_0, y_0, z_0, w_0\}$,其中,$x_0\in(-40, 40)$,$y_0\in(-40, 40)$,$z_0\in(1, 81)$,$w_0\in(-250, 250)$,初始值的精度为 10^{-13},从而可计算出该密钥空间的大小 $S=2.56\times 10^{60}\approx 2^{200}$,数值远大于 2^{128},可知该密钥空间足够大,可以有效抵御暴力攻击。

6.3　实验结果分析

本文选择 256×256 的 Lena 图像作为明文图像,设置参数 $a=30$,$b=35$,$c=7$,$d=9$,$e=0.4$,步长为 0.001,初值(1, 1, 1, 1),利用 Matlab 软件进行实验仿真,结果如图 8 所示。

(a) Lena 原图



(b) Lena 加密图像

(c) Lena 解密图像

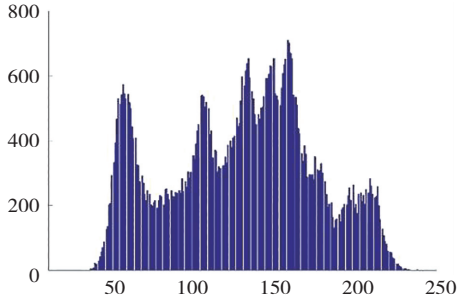
图 8 图像加密和解密仿真图

Fig. 8 Simulation diagrams of image encryption and decryption

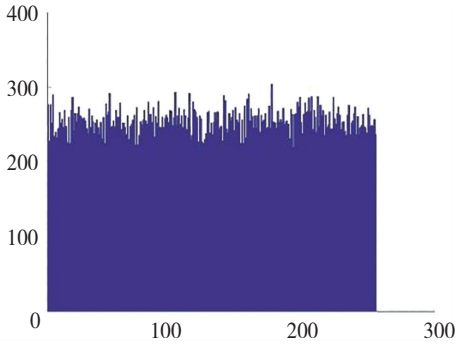
6.4 安全性分析

6.4.1 直方图

直方图是一种对数字图像定性分析的重要方法,利用超混沌系统加密算法对明文图像的像素值进行混淆并扩散,从而使得像素点的分布变得随机,使得像素值在不同位置上出现的频率均匀分布,减小频率的波动。以曲线形式表示该图像整体像素值的分布情况,绘制 Lena 图像的直方图如图 9 所示。明文图像的直方图分布呈现高低起伏的状态,而密文图像呈现随机噪音的形式,其直方图分布更加均匀,很明显加密后的像素值频率没有明显波动,说明加密后有效隐藏了原始图像的信息,保障了信息安全。



(a) Lena 明文图像直方图



(b) Lena 密文图像直方图

图 9 直方图分析

Fig. 9 Histogram analysis

6.4.2 相关性分析

相关性分析可以用来衡量超混沌系统加密算法的安全性和有效性。普通图像中相邻像素的像素值相差不是很大,一般变化范围比较小,分布相对集中,容易受到差分攻击。而密码图像的像素则分布均匀。因此,为了抵御统计学攻击加强图像的安全性,在加密过程中,应该尽可能消除相邻像素之间的相关性来增强图像加密的安全性。此外,可以通过相关系数来定性分析像素之间的关联性。从明文图像和密文图像中选取 2 000 对相邻像素点,图 10 为选取的像素点与相邻像素点的相关性测试结果:明文图像的像素点之间相关性比较强,相关系数数值较大,而加密之后像素点之间强相关性被破坏,相关系数的值接近 0,相关性非常弱。

相关系数可以通过式(15)计算出来:

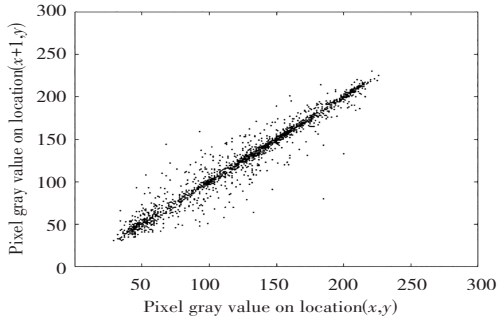
$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))$$

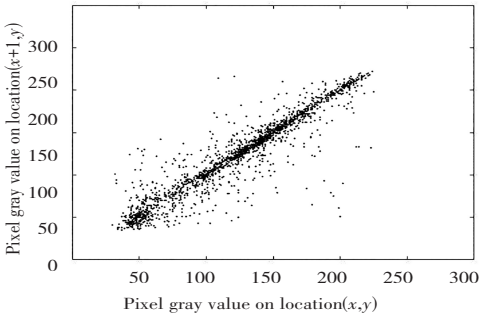
$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{15}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

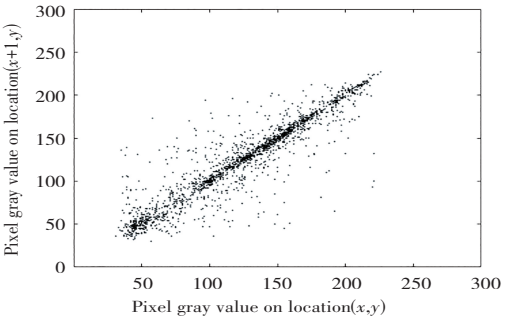
其中,x,y 为相邻像素位置的像素值,N 为像素点的个数,系数的绝对值越大则相关性就越强。从图 10 可以观察到明文图像像素点在各个方向上都集中在 $y=x$ 附近,相关系数大,相邻像素值差距非常小,而经过算法加密后的密文图像中的像素点相差很大且接近于均匀分布,相关系数小,可以很好地隐藏明文图像中的信息。表 1 给出了密文图像的相关系数结果以及比对。可以观察出加密后的图像相邻像素的相关系数与其他文献相比更小,表明该算法加密后的图像具有更高的安全性。



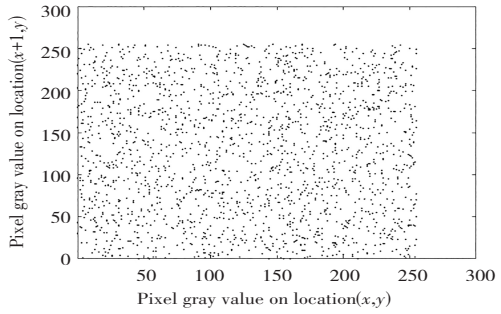
(a) 明文水平



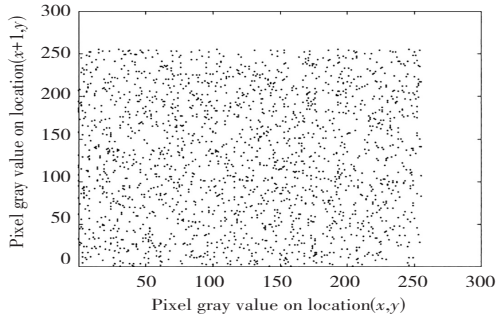
(b) 明文垂直



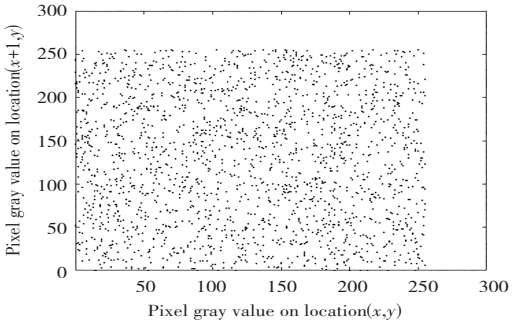
(c) 明文对角



(d) 密文水平



(e) 密文垂直



(f) 密文对角

图 10　相邻像素相关性分布图

Fig. 10　Distribution map of adjacent pixel correlation

表 1　相邻像素相关性

Table 1　Dependencies of adjacent pixels

方　向	明　文	密　文	文献[12]	文献[14]
水平	0.970 3	0.010 4	−0.010 7	−0.014 7
垂直	0.951 5	0.002 8	−0.055 1	0.004 5
对角	0.936 8	−0.028 2	0.039 8	0.008 8

6.4.3　信息熵

信息熵是量化图像不确定度和混乱程度的度量指标。图像的复杂度和随机性随着信息熵增大而增强,该图像的可视信息就越少,图像的安全性就越高,计算式(16)为

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{16}$$

式(16)中,L 是图像的灰数等级,$p(i)$ 表示灰度值 i 出现的概率。

从表 2 中可以看到:对比文献中的信息熵,该超混沌算法的信息熵更加接近理论值 8,说明该算法具有更高的随机性。

表 2　信息熵对比

Table 2　Comparison of information entropies

算　法	本　文	文献[15]	文献[16]	文献[17]
信息熵	7.997 4	7.989 7	7.997 0	7.996 9

6.4.4　差分攻击分析

明文对密文的敏感性反映了算法抗差分攻击性。差分攻击是针对使用同一种密钥加密不同的明文图像算法分析,通过采用不同的明文图像加密后的密文图像进行差分攻击分析,统计不同密文图像之间的规律,寻找密文之间的相关性,从而破解某加密算法的加密密钥,找到明密文图像之间的关系。这里采取两幅图像 P_1 和 P_2,二者的大小都为 $M\times N$,利用像素数变化率(NPCR)和统一平均变化强度(UACI)两个指标来进行抗差分攻击分析,NPCR 和 UACI 的计算为式(17)、式(18):

$$NPCR(P_1,P_2)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|\operatorname{Sign}(P_1(i,j)-P_2(i,j))|\times 100\%}{MN}$$

$$\operatorname{Sign}(x)=\begin{cases}1, x>0\\0, x=0\\-1, x<0\end{cases} \tag{17}$$

$$UACI(P_1,P_2)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|P_1(i,j)-P_2(i,j)|\times 100\%}{255-0} \tag{18}$$

当加密后密文图像的 NPCR 和 UACI 值与其理论值越靠近时,表明该加密算法对差分攻击具有更强的抵抗力,其安全性也就越好。在对 Lena 图像进行加密后,将其与文献中的结果进行对比,具体见表 3。可发现 NPCR 和 UACI 的值均大于对比的文献,说明经过该算法加密的图像抗攻击性更高,有效保护了图像的安全性。

表 3 NPCR 和 UACI

Table 3 NPCR and UACI

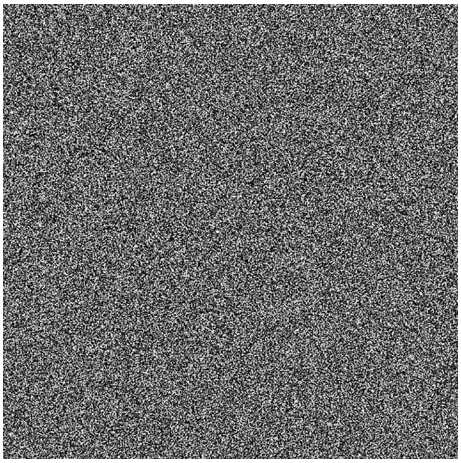
图 像	NPCP	UACI
Lena	99.59	33.51
文献[12]	98.50	33.08
文献[13]	99.39	31.37

6.4.5 密钥敏感性

密钥敏感性是指密钥在加密过程中,即使发生微小的改变也会对加密的结果产生巨大的影响。首先,在正确密钥的情况下,加密得到密文图像后,改变混沌系统的初始值 x_0,使得 $x_0=0+10^{-13}$,利用修改之后的初始值进行解密,如图 11 所示。

图 11 结果显示:即使密钥的数量级相差非常小,解密也无法得到正确的图像,表明该算法的密钥敏感性很高。

(a) Lena 明文图像



(b) Lena 错误的解密图像

图 11 密钥敏感性测试

Fig. 11 Key sensitivity test

7 结论与讨论

本文采用状态变量反馈法构造了超混沌系统,基于 Lü 基础引入了状态反馈控制器,构建了只有一个平衡点的四维超混沌系统,通过理论仿真分析了超混沌系统的耗散性和平衡点稳定性、Lyapunov 指数谱和分岔图、Poincare 截面,数据表明该四维超混沌系统具有周期、混沌、超混沌吸引子的复杂混沌行为。通过在基本运算放大电路上成功搭建四维超混沌系统的电路模型,并使用 Multisim 仿真软件验证该电路模型的准确性,提高了超混沌的物理可实现性。不难发现,将状态变量反馈法与混沌系统结合生成超混沌系统的方法非常简单,同时得到的动力学系统的混沌特征也非常丰富,增加了混沌系统的不可预测性。最后将四维超混沌电路应用在图像加密方面分析,分析直方图、相邻像素相关性、信息熵和抗攻击性以及测试其加密性能。同时,还通过与其他文献进行对比来验证四维超混沌系统的安全性水平。该研究提供了超混沌系统在图像加密中的新思路,进一步推进了四维超混沌系统在该领域的理论认识,并为图像加密的实际应用提供了有价值的研究方向。

参考文献(References):

[1] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(1): 130—141.

[2] ROSSLER O E. An equation for continuous chaos [J]. Physics Letters A, 1976, 57(5): 397—398.

[3] WANG X Y, DU X H. Chaotic image encryption method based on improved zigzag permutation and DNA rules[J]. Multimedia Tools and Applications, 2022, 81(30): 43777—43803.

[4] CUI S Y, ZHANG J Z. Chaotic secure communication based on single feedback phase modulation and channel transmission[J]. IEEE Photonics Journal, 2019, 11(5): 1—8.

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

[6] JIAN M, CHEN Z, WANG Z, et al. A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium[J]. Nonlinear Dynamics, 2015, 81(3): 1275—1288.

[7] 欧斌, 杨启贵. 基于共轭 Lorenz 系统的新四维超混沌系统研究[J]. 重庆工商大学学报(自然科学版), 2019, 36(3): 52—58.
OU Bin, YANG Qi-gui. Research on a new four dimensional Hyperchaotic system based on conjugate Lorenz System[J]. Journal of Chongqing Technology and Business University (Natural Science Edition), 2019, 36(3): 52—58.

[8] 牛亚星, 杨启贵. 一类非 Shil' nikov 型四维超混沌系统的最终有界[J]. 重庆工商大学学报(自然科学版), 2020, 37(4): 20—27.
NIU Ya-xing, YANG Qi-gui. The ultimate boundedness of a class of non Shil' nikov type four dimensional hyperchaotic systems[J]. Journal of Chongqing Technology and Business University (Natural Science Edition), 2020, 37 (4): 20—27.

[9] HUSSAIN I, ANEES A, ALKHALDI A H, et al. Image encryption based on Chebyshev chaotic map and S-8 S-boxes[J]. Optica Applicata, 2019, 49(2): 317—330.

[10] LIU X B, XIAO D, LIU C. Quantum image encryption algorithm based on bit-plane permutation and sine logistic map[J]. Quantum Information Processing, 2020, 19(8): 325—328.

[11] ELAMIR M M, AL-ATABANY W I, MABROUK M S. Hybrid image encryption scheme for secure E-health systems[J]. Network Modeling Analysis in Health Informatics and Bioinformatics, 2021, 10(1): 1727—1744.

[12] 陈宝文, 陈彦安. 基于 Arnold 变换与混沌系统的位级图像加密[J]. 信息通信, 2020, 214(10): 36—39.
CHEN Bao-wen, CHEN Yan-an. Bit-level image encryption based on Arnold transform and chaotic system[J]. Information and Communication, 2020, 214(10): 36—39.

[13] 李付鹏, 刘敬彪, 王康泰. 基于 Tent 映射的图像加密算法及其实验研究[J]. 杭州电子科技大学学报(自然科学版), 2020, 40(3): 38—43.
LI Fu-peng, LIU Jing-biao, Wang Kang-tai. Image encryption algorithm based on Tent mapping and its experimental research[J]. Journal of Hangzhou University of Electronic Science and Technology (Natural Science Edition), 2020, 40(3): 38—43.

[14] 胡春杰, 黄启胜, 陈翠, 等. 结合多混沌映射与 DNA 的彩色图像加密算法[J]. 计算机系统应用, 2019, 28(12): 189—194.
HU Chun-jie, HUANG Qi-sheng, CHEN Cui, et al. A color image encryption algorithm combining multi chaos mapping and DNA[J]. Computer System Applications, 2019, 28 (12): 189—194.

[15] 张勋才, 刘奕杉, 崔光照. 基于 DNA 编码和超混沌系统的图像加密算法[J]. 计算机应用研究, 2019, 36(4): 1139—1143.
ZHANG Xun-cai, LIU Yi-shan, CUI Guang-zhao. Image encryption algorithm based on DNA encoding and hyperchaotic system[J]. Computer Application Research, 2019, 36 (4): 1139—1143.

[16] 赵洪祥, 谢淑翠, 张建中, 等. 基于改进型 Henon 映射的快速图像加密算法[J]. 计算机应用研究, 2020, 37(12): 3726—3730.
ZHAO Hong-xiang, XIE Shu-cui, ZHANG Jian-zhong, et al. A fast image encryption algorithm based on improved Henon mapping[J]. Computer Application Research, 2020, 37(12): 3726—3730.

[17] ZAHRA P, HADI S, MOUSA S. A new secure and sensitive image encryption scheme based on new substitution with chaotic function[J]. Multimedia Tools and Applications, 2016, 75(17): 10631—10648.

责任编辑:李翠薇