DOI: 10.16452/j.cnki.sdkjzk.2023.04.013 文章编号:1672-3767(2023)04-0113-14

具有隐藏吸引子的新四维混沌系统的共存现象及图像加密

颜闽秀[1,2],张 萍[1]

(1. 沈阳化工大学 信息工程学院,辽宁 沈阳 110142;
2. 工业环境-资源协同控制与优化技术辽宁省高校重点实验室,辽宁 沈阳 110142)

摘 要:提出具有隐藏吸引子的新四维复杂混沌系统,系统在不同初始条件下产生不同类型的吸引子,且存在共存现象。对系统进行复杂度分析,发现该系统复杂度较高;设计图像置乱加密算法,利用隐藏吸引子混沌系统产生的混沌序列对图像进行置乱和扩散,对比发现隐藏型混沌系统的保密性强,并验证了加密算法的可实现性。该系统通过了 NIST 标准测试中的 15 项指标,验证系统具有随机性。通过电路设计,证明系统在实际应用中具有可行性。

关键词:混沌系统;隐藏吸引子;共存现象;复杂度分析;图像加密;随机性测试;电路设计

中图分类号:O414.5;TP309.7 **文献标志码**:A

Coexistence and image encryption of a new four-dimensional chaotic system with hidden attractors

YAN Minxiu[1,2], ZHANG Ping[1]

(1. College of Information Engineering, Shenyang University of Chemical Technology, Shenyang 110142, China;
2. Key Laboratory for Industrial Environment-Resources Cooperative Control and Optimization Technology, Shenyang 110142, China)

Abstract: This paper proposed a new four-dimensional complex chaotic system with hidden attractors, which, under different initial conditions, produces different attractor types that coexist. The complexity analysis showed that the system had relatively higher complexity. An image scrambling encryption algorithm was designed and the images were scrambled and diffused by using the chaotic sequence generated by the hidden attractor chaotic system. A comparison with traditional chaotic system shows that the hidden chaotic system has strong secrecy. The achievability of the encryption algorithm was then verified. The system has passed 15 indicators in the NIST standard test, which proves that the system is random. Finally, the feasibility of the system in practical applications was testified through circuit design.

Key words: chaotic system; hidden attractors; coexistence; complexity analysis; image encryption; randomness test; circuit design

自 1963 年著名的 Lorenz 混沌系统[1]建立以来,对混沌的研究迅速开展起来,并取得一些重要的成果,主要应用于图像加密[2-3]、通信加密[4-5]、生物医疗[6]等方面。根据平衡点类型,系统产生吸引子可以分为自激吸引子和隐藏吸引子[7],而隐藏吸引子的数学定义,在 2013 年[8]才首次被提出。隐藏吸引子通常存在于无平衡点、唯一稳定平衡点或无限平衡点等[9]非线性混沌系统当中。Zhang 等[10]在经典混沌系统的基础上

收稿日期:2021-12-27

基金项目:国家科技部中国-马其顿政府间科技合作项目(国科外[2019]22;6-8)

作者简介:颜闽秀(1972—),女,福建仙游人,副教授,博士,主要研究方向为复杂系统控制. E-mail:yanminxiu@syuct.edu.cn
张 萍(1997—),女,辽宁鞍山人,硕士研究生,主要研究方向为混沌系统.

引入状态反馈控制器,构建了具有隐藏吸引子的混沌系统,动态分析发现,隐藏型混沌系统具有复杂的动力学行为;Wang 等[11]提出一个简单的三维自治系统,该系统仅有一个稳定平衡点,具有隐藏混沌吸引子系统的特性。与有自激吸引子的混沌系统相比,具有隐藏吸引子的混沌系统复杂度更高,并且能够避免一般混沌系统所具有的局限性和缺陷。由于在实际工程应用中具有重要作用,因此研究人员更加注重对隐藏吸引子的研究[12-14]。

吸引子共存[15]是一种非常复杂且有趣的现象,同时含有隐藏吸引子的共存现象也值得探究。Fang 等[16]提出具有隐藏吸引子的分数阶混沌系统,并分析了其共存现象;Al-Hayali 等[17]基于 Sprott S 系统提出一个四维混沌系统,该系统不具有平衡点,不同参数时李雅普诺夫指数和为整数,此时具有保守吸引子;Li 等[18]研究了一种具有共存的隐藏吸引子的分数阶混沌系统,并设计了电路。在探索混沌系统复杂的动力学特性时,进行复杂度分析尤为必要。随着科学技术的发展,对于数字图像安全性的探究逐渐增多,图像加密已经成为一项广泛应用的技术,而混沌系统具有对初始值敏感性、随机性等显著特征,因此非常适合应用在数字图像加密中[19]。Wang 等[20]将隐藏型混沌系统应用于图像加密算法中,具有较强的安全性能。Patro 等[21]提出利用线性混沌映射交叉耦合的图像加密算法,避免了单一映射的缺点。设计实用且可靠的图像加密算法,并利用电路设计[22]验证是否具有应用的可能,具有一定的实用价值。

本研究设计了一个结构简单的新四维混沌系统,该系统不存在平衡点,却表现出复杂的动力学特性。首先,通过对其耗散性、李雅普诺夫指数和维数分析验证该系统的动态行为,改变参数值和初始条件,系统的吸引子类型也会相应改变,并且在给定不同初始值和参数的情况下,系统能够产生不同状态的隐藏吸引子共存,复杂度分析发现该系统具有极高的复杂度;然后,设计了图像加密算法,实验证明,基于隐藏吸引子混沌系统的加密算法具有很强的安全性能,利用混沌序列的不均匀性可为信息安全领域提供理论支撑;最后,随机特性测试表明,P-value 均大于 0.01,说明该系统的混沌序列具有随机性;利用 Multisim 进行电路仿真,仿真结果与 Matlab 运行结果一致,说明该系统具有可行性。

1 系统模型及动力学特性分析

1.1 系统模型

基于三维 Lü 混沌系统[23],构造一个新的四维混沌系统:

$$\begin{cases}\dot{x}=y-ax,\\ \dot{y}=bz-xz,\\ \dot{z}=xy-xw,\\ \dot{w}=-x+c。\end{cases} \tag{1}$$

式中:x、y、z、w 为状态变量,a、b、c 为参数值。

1.2 平衡点

为计算系统的平衡点,令

$$\begin{cases}y-ax=0,\\ bz-xz=0,\\ xy-xw=0,\\ -x+c=0。\end{cases} \tag{2}$$

根据式(2)显然可得,当 $c\neq 0$ 时,系统没有平衡点,此时该系统所产生的吸引子均为隐藏吸引子。当参数值 $a=10$、$b=3$、$c=12$,初始值为(1,1,1,1)时,系统的混沌吸引子如图 1 所示。可以看出,隐藏混沌吸引子不具有平衡点,却能产生混沌行为,其运动轨迹复杂,具有复杂的折叠性、重复性和延伸性结构,但又是有界的。

1.3 动力学特性分析

对系统进行耗散度分析,有

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

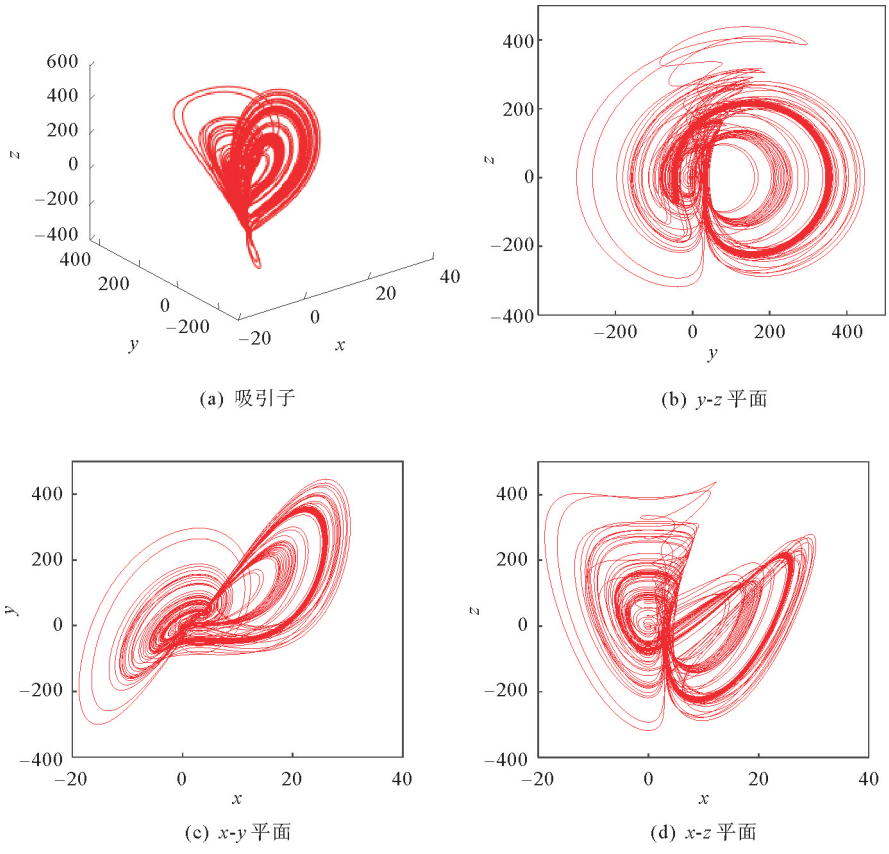


图 1 系统的吸引子相图

Fig. 1 Attractor phase diagram of the system

当 $a>0$ 时，$\nabla V<0$，因此系统是耗散的，并且以指数形式收敛。分析李雅普诺夫指数(如图 2)可得，$LE_1=0.58$，$LE_2=0$，$LE_3=0$，$LE_4=-10.56$，则李雅普诺夫维数为：

$$D_{LE}=j+\sum_{i=1}^{j}\lambda_{LE_i}/|\lambda_{LE_{(j+1)}}|=$$
$$3+(LE_1+LE_2+LE_3)/|LE_4|=3.05\ 。\qquad(4)$$

由图 2 可以看出，系统有一个正数、两个零、一个负数的李雅普诺夫指数，说明系统具有混沌特性。同时，由于李雅普诺夫维数是分数，说明隐藏型系统具有混沌特性。由于参数及初始值的波动对系统具有一定影响，同时该系统具有复杂的动力学特性，因此根据参数的不同取值可得系统吸引子类型，如表 1。

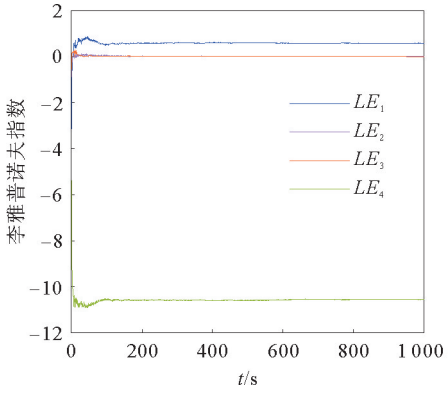


图 2 李雅普诺夫指数图

Fig. 2 Lyapunov exponent diagram

表 1 系统不同类型的吸引子

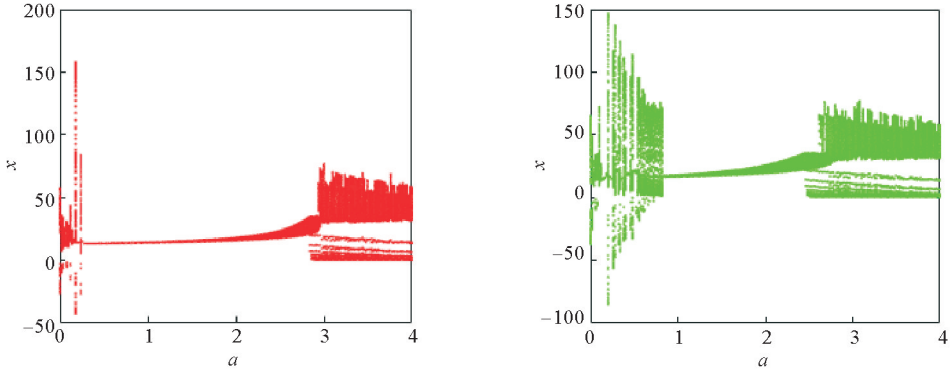
Table 1 Attractor types of the system

参数值	初始值	李雅普诺夫指数	吸引子类型
$a=2,b=2,c=10$	(1,1,1,1)	$LE_1=0,LE_2=-0.11,LE_3=-0.30,LE_4=-1.59$	极限环
$a=0.2,b=0.3,c=12$	(1,1,1,1)	$LE_1=0,LE_2=0,LE_3=-0.09,LE_4=-0.10$	二维环面
$a=10,b=3,c=5$	(1,−1,1,1)	$LE_1=0.63,LE_2=0,LE_3=-0.02,LE_4=-10.61$	隐藏混沌吸引子
$a=10,b=2,c=12$	(1,1,1,1)	$LE_1=0.56,LE_2=0.02,LE_3=0,LE_4=-10.58$	隐藏超混沌吸引子

2 隐藏吸引子的共存现象

隐藏吸引子的共存在非线性系统中是一种复杂现象,一般在系统存在对称性的情况下产生,而该系统不存在对称性,却能产生共存现象,是极为少见的。

情况Ⅰ。固定参数 $b=0.3$,$c=12$,令 a 为变量,$a\in[0,4]$,得到关于初始值(1,1,1,1)和初始值(−1,−1,−1,−1)的分岔图,如图 3 所示。取初始值为(1,1,1,1)时关于 a 的李雅普诺夫指数如图 4 所示。



(a) 初始值为(1,1,1,1)的分岔图　(b) 初始值为(−1,−1,−1,−1)的分岔图

图 3 情况Ⅰ的分岔图

Fig. 3 Bifurcation diagram for Case Ⅰ

通过图 3 可以看出,系统存在共存现象,给定不同的初始值系统具有不同的混沌特性,对比分析可以发现隐藏型混沌系统具有共存现象。当 $a\in[0.32,2.06]$ 时,分析图 4 可知,系统呈周期状态;当 $a\in[0,0.32]\cup[2.06,4]$ 时,最大李雅普诺夫指数为正,说明系统是混沌状态。

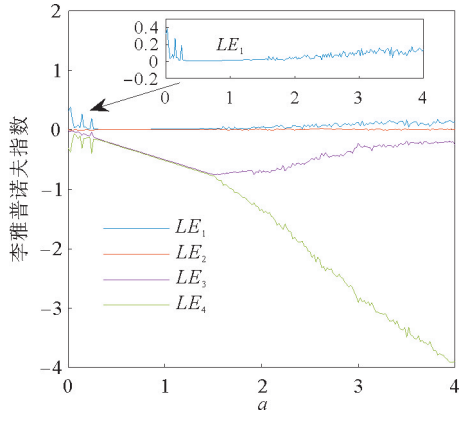
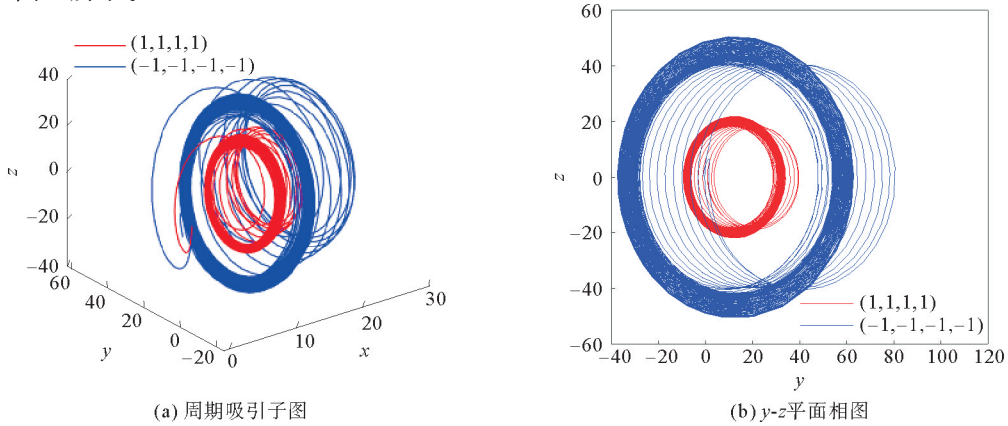


图 4 情况Ⅰ的李雅普诺夫指数图

Fig. 4 Lyapunov exponent graph for Case Ⅰ

为使共存现象清晰展示,取 $a=1$,产生如图 5 的周期与周期共存状态的相图。由图 5 可以看出,在给定参数 $a=1$,$b=0.3$,$c=12$ 以及不同初始值的情况下,出现两个环形的周期吸引子共存的现象。

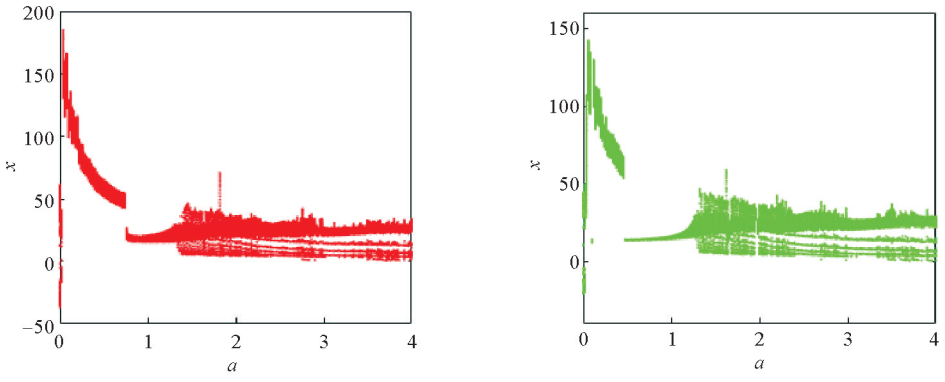
情况Ⅱ。固定参数 $b=2$,$c=12$,令 a 为变量,$a\in[0,4]$,得到关于初始值(1,1,1,1)和(−1,−1,−1,−1)的分岔图,如图 6 所示。取初始值为(1,1,1,1)时关于 a 的李雅普诺夫指数如图 7 所示。



(a) 周期吸引子图　(b) y-z平面相图

图 5 周期与周期吸引子共存

Fig. 5 Coexistence of cycle and cycle attractor



(a) 初始值为(1,1,1,1)的分岔图　　(b) 初始值为(−1,−1,−1,−1)的分岔图

图 6　情况Ⅱ的分岔图

Fig. 6　Bifurcation diagram for Case Ⅱ

由图 6 可以看出,改变参数值得到的分岔图不同,但同样存在共存现象。由图 7 可以看出,当 $a \in [0.78,1.54] \cup [3.06,3.26]$ 时,系统做周期运动;当 $a \in [0,0.78] \cup [1.54,3.06] \cup [3.26,4]$ 时,系统做混沌运动;当 $a=3.2$ 时,出现隐藏混沌吸引子与隐藏混沌吸引子共存现象,两个混沌吸引子结构相似但运动轨迹不同,如图 8 所示。

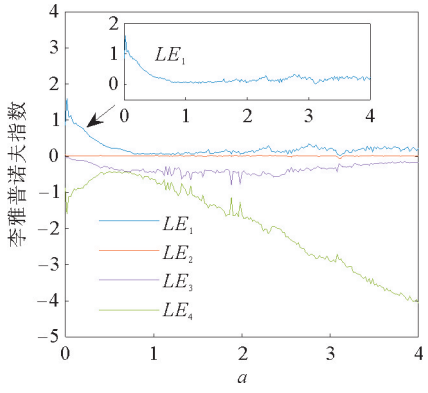
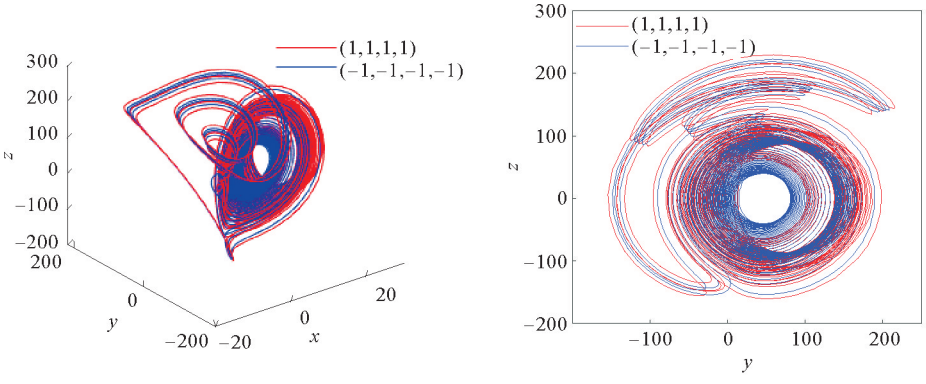


图 7　情况Ⅱ的李雅普诺夫指数图

Fig. 7　Lyapunov exponent graph for Case Ⅱ

情况Ⅲ。固定参数 $b=3$,$c=12$,令 a 为变量,$a \in [0,3]$,给定初始值分别为(1,1,1,1)和(1,−1,1,−1),可以得到分岔图如图 9 所示。取初始值为(1,1,1,1)时,关于 a 的李雅普诺夫指数如图 10 所示。

由图 9 可以看出,系统具有复杂多变的动力学行为,当系统选取不同的初始值时,分岔图中的密集点分布存在明显的差异,说明系统具有共存现象。对比图 9 与图 10 可知,隐藏型混沌系统具有复杂的共存特性。

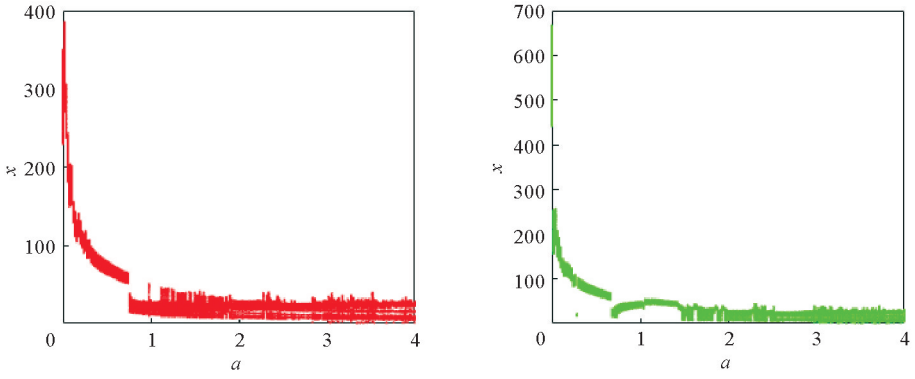


(a) 混沌吸引子图　　(b) y-z平面相图

图 8　混沌与混沌吸引子共存

Fig. 8　Coexistence of chaos and chaotic attractor

为进一步探究系统吸引子共存的具体情况,分别取 $a=0.5$、$a=2.8$,产生如图 11、图 12 所示的混沌吸引子与混沌吸引子共存现象。由图 11 和图 12 可以看出,当 $a=0.5$ 时,混沌吸引子成“薯片状”共存;当 $a=2.8$ 时,混沌吸引子成“花状”共存。



(a) 初始值为(1,1,1,1)的分岔图　　(b) 初始值为(−1,−1,−1,−1)的分岔图

图 9　情况 Ⅲ 的分岔图

Fig. 9　Bifurcation diagram for Case Ⅲ

由上述分岔图可知,系统具有复杂的混沌特性,通过对 a 的不同取值可以得到不同形状的混沌吸引子共存现象。

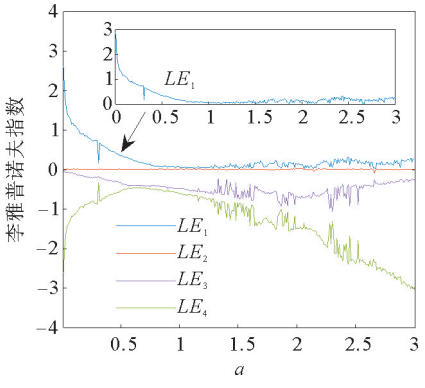


图 10　情况 Ⅲ 的李雅普诺夫指数图

Fig. 10　Lyapunov exponent graph for Case Ⅲ

3　复杂度分析

相对普通混沌系统,具有隐藏混沌吸引子的系统更具复杂性,利用谱熵(spectral entropy,SE)和 C_0 复杂度算法证明系统结构复杂程度较高,如图 13、图 14。

C_0 算法保留了系统不规则的部分,由图 13 可以看出,C_0 的值均大于 0.52,即在序列当中不规则部分较大,说明序列的复杂度高。与传统混沌系统对比可知,经典 Bao 混沌系统 C_0 的值最大为 0.4,因此隐藏吸引子的复杂程度相对较高。分析 SE 复杂度图像可以看出,谱熵值整体大于 0.9,序列振幅明显,测量值较高,因此系统的复杂程度较高。经典 Bao 混沌系统最大谱熵值在 0.75 左右,Rössler 混沌系统最大谱熵值在 0.3 左右[24]。综上可知,具有隐藏吸引子的混沌系统复杂度较高。

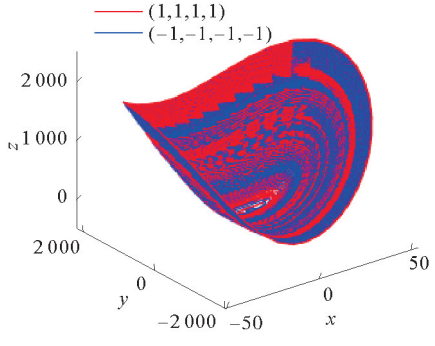


图 11　$a=0.5$ 时的共存混沌吸引子图

Fig. 11　Coexisting chaotic attractor graph when $a=0.5$

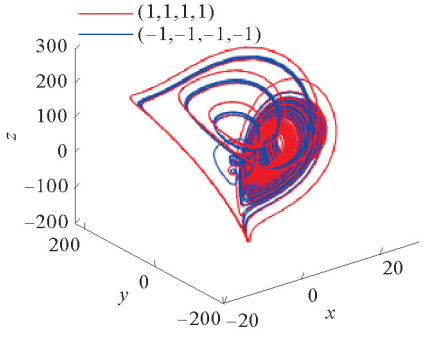


图 12　$a=2.8$ 时的共存混沌吸引子图

Fig. 12　Coexisting chaotic attractor graph when $a=2.8$

4　图像加密

基于隐藏吸引子的混沌系统设计图像加密系统,结构如图 15 所示。该图像加密系统主要包含四部分,分别为基于具有隐藏吸引子的混沌系统(1)(式(1))的密码生成模块、明文无关的顺向扩散模块、明文关联的

图像置乱模块、明文无关的逆向扩散模块。

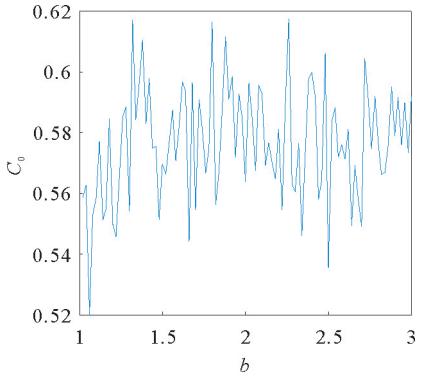


图 13　C_0 复杂度

Fig. 13　C_0 complexity

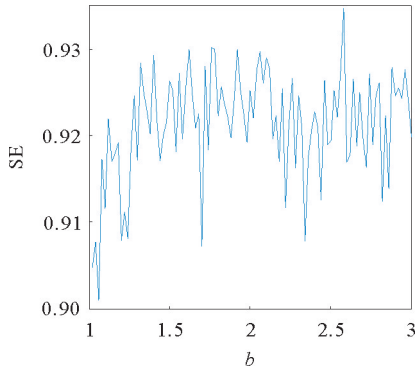


图 14　SE 复杂度

Fig. 14　SE complexity

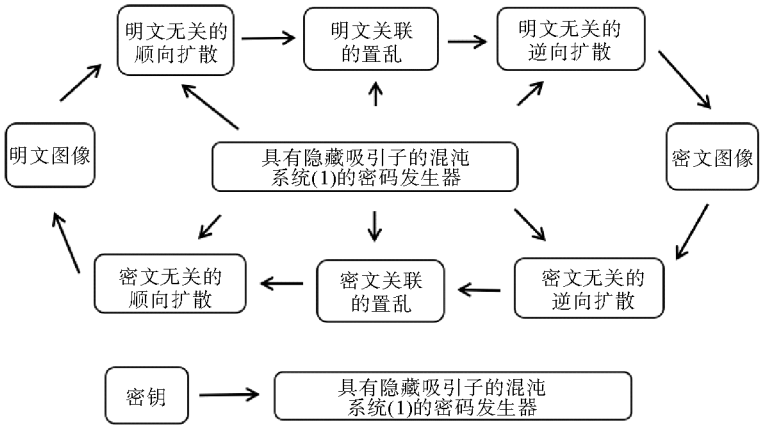


图 15　基于隐藏吸引子的图像加密系统结构图

Fig. 15　Structure diagram of image encrgption system based on hidden attractor

给定密钥为 $K=\{a_0,b_0,c_0,d_0,r_1,r_2,r_3,r_4\}$,其中 a_0、b_0、c_0、d_0 为系统的初始条件,r_1、r_2、r_3、r_4 为[0,255]中的 4 个随机整数。用 $\boldsymbol{P}$ 表示明文图像,大小为 $M\times N$ 。利用混沌密码发生器产生与明文图像 $\boldsymbol{P}$ 大小相等的随机矩阵,记为 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{D}$。将这 4 个矩阵分别用于扩散模块和置乱模块中。具体步骤为:

1) 将$\{a_0,b_0,c_0,d_0\}$作为系统的初始条件,利用龙格-库塔法迭代 $r_1+r_2+r_3+r_4+MN$ 次,跳过过渡状态值,因此得到状态变量序列长度为 MN,该状态变量序列可记为$\{x_i\}$,$i=1,2,\cdots,MN$ 。

2) 由序列$\{x_i\}$,$i=1,2,\cdots,MN$,根据式(5)得到随机矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{D}$。

$$\begin{cases}\boldsymbol{A}(u,v)=\mathrm{mod}(\mathrm{floor}(\dfrac{r_1+1}{r_1+r_3+2}x_{(u-1)\times N+v})\times 10^{14},256),\\ \boldsymbol{B}(u,v)=\mathrm{mod}(\mathrm{floor}(\dfrac{r_2+1}{r_2+r_4+2}x_{(u-1)\times N+v})\times 10^{13},256),\\ \boldsymbol{C}(u,v)=\mathrm{mod}(\mathrm{floor}(\dfrac{r_1+1}{r_1+r_4+2}x_{(u-1)\times N+v})\times 10^{12},L),\\ \boldsymbol{D}(u,v)=\mathrm{mod}(\mathrm{floor}(\dfrac{r_2+1}{r_2+r_3+2}x_{(u-1)\times N+v})\times 10^{11},L)。\end{cases}\tag{5}$$

式中:$L=\max(M,N)$;$u=1,2,\cdots,M$;$v=1,2,\cdots,N$;$\mathrm{floor}(t)$ 是返回小于等于 t 的最大整数。

接下来,通过顺向扩散模块将明文图像 $\boldsymbol{P}$ 转换为矩阵 $\boldsymbol{T}$。

3) 将 $\boldsymbol{P}(1,j)$ 转化为 $\boldsymbol{T}(1,j)$, $j=1,2,\cdots,N$ 。

$$\boldsymbol{T}(1,1)=\mathrm{mod}(P(1,1)+\boldsymbol{A}(1,1)+r_1+r_3,256), \tag{6}$$

$$\boldsymbol{T}(1,j)=\mathrm{mod}(P(1,j)+\boldsymbol{A}(1,j)+\boldsymbol{T}(1,j-1),256)。 \tag{7}$$

4) 将 $\boldsymbol{P}(i,1)$ 转化为 $\boldsymbol{T}(i,1)$, $i=2,3,\cdots,M$ 。

$$\boldsymbol{T}(i,1)=\mathrm{mod}(P(i,1)+\boldsymbol{A}(i,1)+\boldsymbol{T}(i-1,1),256)。 \tag{8}$$

5) 将 $\boldsymbol{P}(i,j)$ 转化为 $\boldsymbol{T}(i,j)$, $i=2,3,\cdots,M$, $j=1,2,\cdots,N$,

$$\boldsymbol{T}(i,j)=\mathrm{mod}(P(i,1)+\boldsymbol{A}(i-1,j)+\boldsymbol{T}(i,j-1)+T(i-1,j),256)。 \tag{9}$$

然后,通过对像素点 $\boldsymbol{T}(i,j)$, $i=2,3,\cdots,M$, $j=1,2,\cdots,N$ 与 $\boldsymbol{T}(m,n)$ 置换位置对矩阵 $\boldsymbol{T}$ 进行置乱。

6) 计算 $\boldsymbol{T}(i,j)$ 所在行的全部元素(不含 $\boldsymbol{T}(i,j)$)的和,记为 s_{ri},

$$s_{ri}=sum(\boldsymbol{T}(i,1:N))-\boldsymbol{T}(i,j)。 \tag{10}$$

7) 计算 $\boldsymbol{T}(i,j)$ 所在列的全部元素(不含 $\boldsymbol{T}(i,j)$)的和,记为 s_{ci},

$$s_{ci}=sum(\boldsymbol{T}(1:M,j))-\boldsymbol{T}(i,j)。 \tag{11}$$

8) 计算 m、n 的值

$$\begin{cases} m=\mathrm{mod}(s_{ri}+C(i,j),M)+1, \\ n=\mathrm{mod}(s_{ci}+D(i,j),N)+1。 \end{cases} \tag{12}$$

9) 当 $m=i$ 或者 $n=j$ 时, $\boldsymbol{T}(i,j)$ 与 $\boldsymbol{T}(m,n)$ 位置是相同的。反之,两者根据循环置换位置。最后,将由 $\boldsymbol{T}$ 置乱得到的图像命名为 $\boldsymbol{S}$,通过逆向扩散模块将 $\boldsymbol{S}$ 转化为矩阵密文图像 $\boldsymbol{J}$。

10) 将 $\boldsymbol{S}(M,j)$ 转化为 $\boldsymbol{J}(M,j)$, $j=N,N-1,\cdots,2,1$,

$$\boldsymbol{J}(M,N)=\mathrm{mod}(\boldsymbol{S}(M,N)+\boldsymbol{B}(M,N)+r_2+r_4,256)\ , \tag{13}$$

$$\boldsymbol{J}(M,j)=\mathrm{mod}(\boldsymbol{S}(M,j)+\boldsymbol{B}(M,j)+\boldsymbol{J}(M,j+1),256), j=N-1,N-2,\cdots 3,2\ 。 \tag{14}$$

11) 将 $\boldsymbol{S}(i,N)$ 转化为 $\boldsymbol{J}(i,N)$, $i=M,M-1,\cdots,2,1$,

$$\boldsymbol{J}(i,N)=\mathrm{mod}(\boldsymbol{S}(i,N)+\boldsymbol{B}(i,N)+\boldsymbol{J}(i+1,N),256)。 \tag{15}$$

12) 将 $\boldsymbol{S}(i,j)$ 转化为 $\boldsymbol{J}(i,j)$, $i=M,M-1,\cdots,2,1$, $j=N,N-1,\cdots,2,1$,

$$\boldsymbol{J}(i,j)=\mathrm{mod}(\boldsymbol{S}(i,j)+\boldsymbol{J}(i+1,j)+\boldsymbol{J}(i,j+1)+\boldsymbol{B}(i,j),256)。 \tag{16}$$

通过扩散处理之后可得到密文图像 $\boldsymbol{J}$。

以上是图像加密的全部过程,而解密过程就是加密过程的逆过程。解密步骤的置乱和扩散的步骤与加密步骤完全相同,过程相反,此处不再过多赘述。

5 仿真实验与性能分析

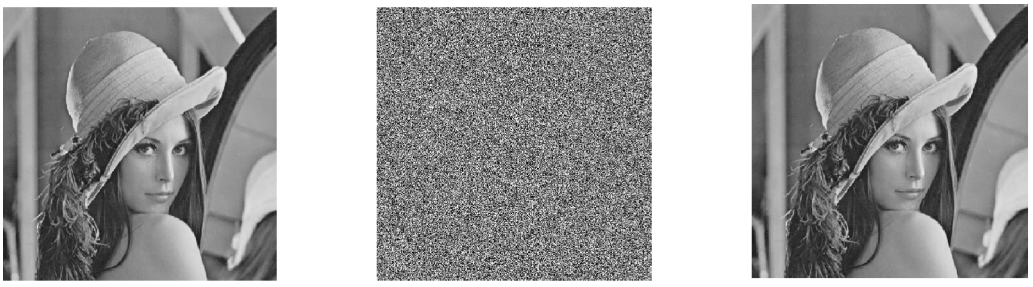
5.1 加密与解密

密钥是加密性能好坏以及是否足够安全的一个非常直观的体现,这里给定密钥为 $K=\{a_0,b_0,c_0,d_0,r_1,r_2,r_3,r_4\}$,同时给定系统(1)的参数值 $a=10$, $b=3$, $c=12$,密钥选取 $a_0,b_0,c_0,d_0\in[-40,40]$,步长为 $1/l$, $l=10^{15}$,因此密钥空间为 $2.814\ 7\times10^{66}$,远大于 2^{100}。

仿真使用计算机配置:CPU 为 Intel(R) Core(TM)i5-9300H 2.40 GHz,RAM 为 8.00 GB,64 位操作系统。在 Matlab R2019b 中编写并运行加密解密算法过程,选用经典 Lena 图像进行仿真。同时,选取一组密钥 $K_1=\{5.490\ 1,5.578\ 7,-4.108\ 6,9.411\ 9,99,245,66,138,3\}$,可得如图 16 的图像加密和解密图。由图 16 可以看出,加密解密前后图像完全相同,说明具有良好的加密和解密效果,并且具有可实现性。

5.2 直方图和信息熵

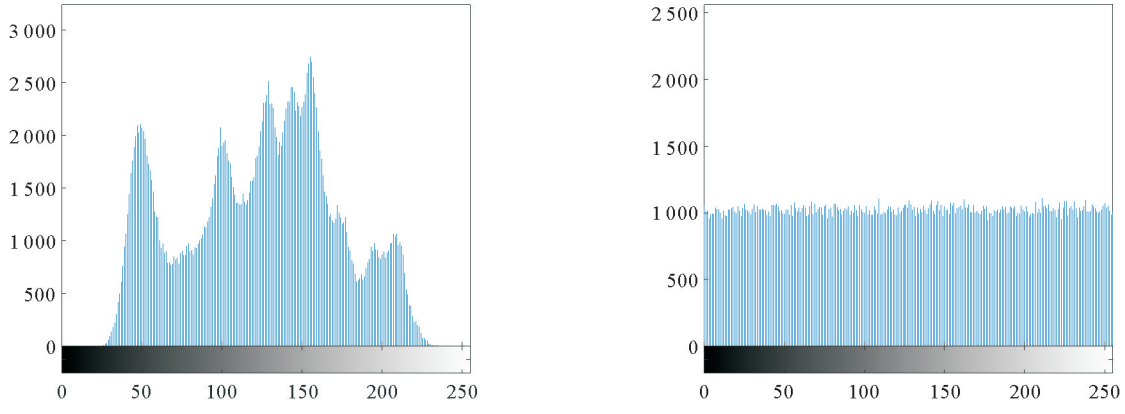
图 17 为明文与密文的直方图。当直方图分布均匀平稳时,可视信息较少,信息熵较大,安全性能高,保密性较强,此时攻击者难以获取图像的特征。由图 17 可看出,加密后直方图相对平稳,计算明文的信息熵为 7.445 1,密文的信息熵为 7.999 3,信息熵较高,说明保密性能较好。



(a) 明文图　(b) 加密图　(c) 解密图

图 16　图像的加密与解密

Fig. 16　Image encryption and decryption



(a) 明文直方图　(b) 密文直方图

图 17　明文与密文的直方图

Fig. 17　Histogram of plain text and cipher text

5.3　密钥的敏感性

为验证密钥的敏感性,选取 8 组密钥进行实验操作,并取其平均值,密钥敏感性分析结果如表 2。表 2 中,NPCR 为像素数变化率(number of pixels change rate),UACI 为统一平均变化强度(unitied average changing intensity),BACI 为块平均变化强度(block average changing intensity)。由表 2 可知,对比文献[21],实验值几乎接近于理论值,说明密钥敏感性较强,系统抵抗差分攻击性强,安全性能高。

以上为定量分析得到的结论,接下来进行定性分析。对密钥进行微小的改变,观察加密解密过程的变化,进一步分析密钥的敏感性。给定密钥 K_c = {3.363 0,−1.323 1,−3.099 7,−1.921 8,196,39,204,89,3},对 K_c 进行微小改变,得到 K_n = {3.363 0 + 1/l,−1.323 1,−3.099 7,−1.921 8,196,39,204,89,3}。根据这两组密钥进行加密解密分析,得到密钥敏感性性能测试结果如图 18。分析图 18 可知,尽管密钥进行了微小的改变,却不能解密出原图像,只有正确的密钥才能解密,验证了密钥的敏感性。

表 2　密钥敏感性性能分析结果

Table 2　Key sensitivity performance analysis results

指标	实验值	理论值
NPCR	99.606 9	99.609 4
UACI	33.483 3	33.463 5
BACI	26.753 8	26.771 2

表 3　相邻像素相关测试系数

Table 3　Adjacent pixel correlation test coefficient

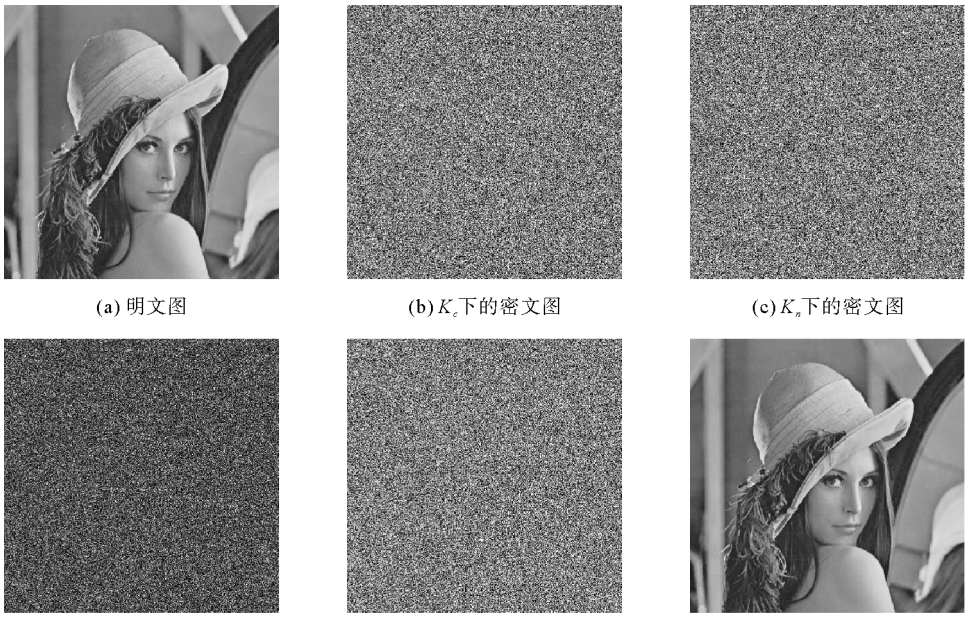
图像	水平方向	垂直方向	对角方向
明文	0.984 9	0.967 8	0.971 9
密文	0.017 0	0.002 4	−0.010 7

5.4　系统相关性分析

一般来说,明文图像有很强的相关性,若经过安全性较强的保密处理之后,图像相邻像素相关性应当较弱。为验证这一理论,首先进行定量分析,在水平、垂直、对角方向上分别取 10 000 对相邻像素点,相邻

像素相关测试系数如表 3。通过测试仿真可得到如图 19 所示的相邻像素间的相关性。

分析表 3 和图 19 可得,明文图像相关性均在 0.9 以上,相关性较强,而通过加密过程处理之后,图像相关性几乎接近于 0,说明加密操作的安全性强,证明该算法具有可实现性。

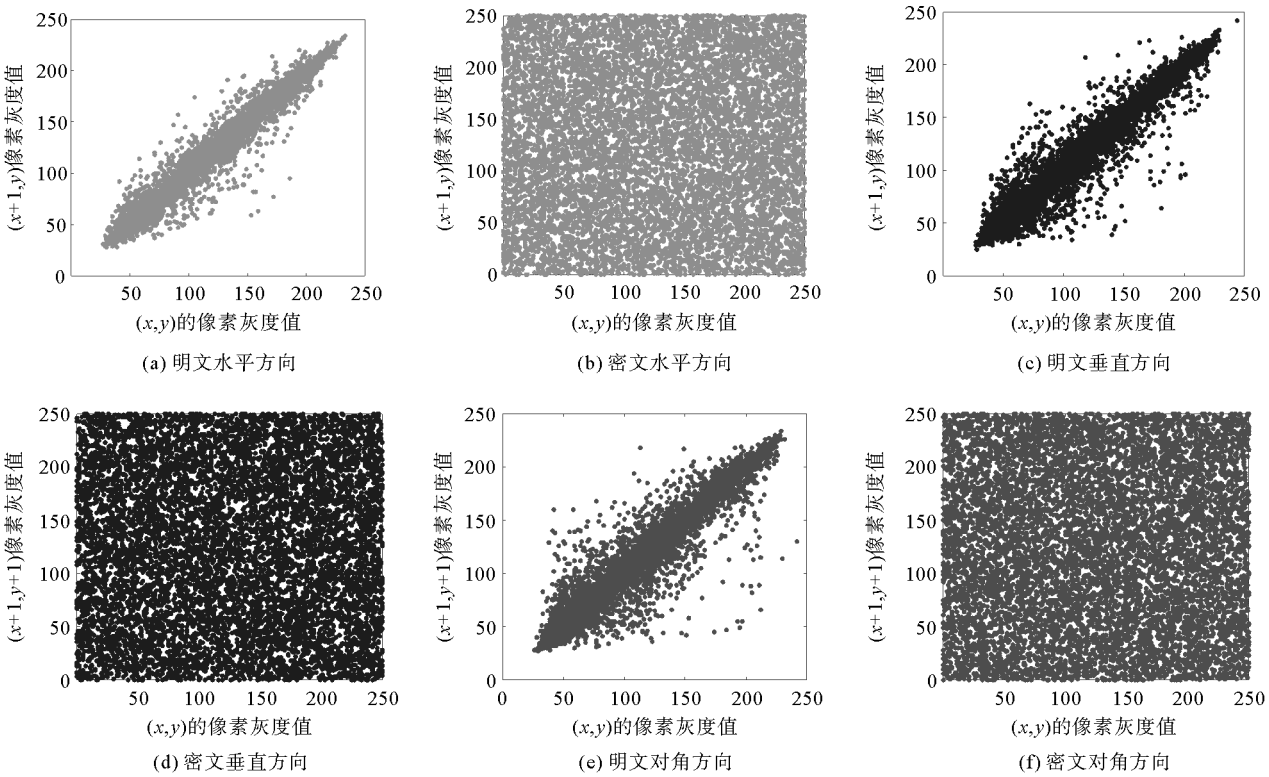


(a) 明文图 (b) K_c下的密文图 (c) K_n下的密文图

(d) 作差图 (e) K_n下的解密图 (f) K_c下的解密图

图 18 密钥敏感性性能测试结果

Fig. 18 Key sensitivity performance test analysis results



(a) 明文水平方向 (b) 密文水平方向 (c) 明文垂直方向

(d) 密文垂直方向 (e) 明文对角方向 (f) 密文对角方向

图 19 相邻像素间的相关性

Fig. 19 Correlation between adjacent pixels

6 随机性测试

为验证具有隐藏吸引子的新四维混沌系统的混沌序列伪随机性,使用四阶 Rugge-Kutta 法将系统进行离散化,按照 NIST(national institute of standards and technology)标准,利用 SP800-22 Revla 标准评估中给出的 15 种测试方法检验系统的比特序列的随机特性。在 15 个检验指标中,每项检验指标都会产生 P-value,通过 P-value 是否大于 0.01 判断系统是否具有随机性。若 P-value 大于等于 0.01,即可认为序列具有随机性,反之不具有随机性。由于 SP800-22 Revla 标准评估中建议测试比特序列长度为 $10^3 \sim 10^7$,这里给定长度 n 为 10^6,定义测试序列为 S,同时给定 $(x_0, y_0, z_0, w_0, a, b, c)=(10,10,10,10,10,3,12)$,由此可得表 4 的测试结果。由表 4 可以看出,P-value 值结果均大于 0.01,可以判定混沌系统产生的比特序列具有随机性。

表 4 随机性测试结果

Table 4 Randomness test results

序号	测试方法	P-value
1	Frequency	0.201 2
2	Block Frequency	0.885 5
3	Runs	0.890 5
4	Longest Run	0.435 7
5	Rank	0.026 5
6	FFT	0.895 4
7	Non-overlapping Template	0.288 9
8	Overlapping Template	0.540 5
9	Universal	0.211 9
10	Linear Complexity	0.152 8
11	Serial	0.474 2
12	Approximate Entropy	0.204 8
13	Cumulative Sums	0.999 8
14	Random Excursions	[0.140 5,0.499 5,0.485 5,0.478 2,0.683 4,0.408 1,0.136 5,0.833 0]
15	Random Excursions Variant	[0.287 7,0.311 9,0.317 4,0.452 1,0.563 2,0.285 6,0.048 9,0.031 7,0.250 3, 0.349 7,0.228 7,0.264 7,0.299 1,0.431 9,0.568 8,0.452 6,0.257 7,0.172 0]

7 电路实现

利用 Multisim 设计混沌系统的仿真电路,进一步判断混沌系统是否具有可实现性。由图 1 可看出,系统的吸引子状态在较大峰值范围内变化。较大的峰值变化范围对系统的硬件实现难度较大。以运算放大器 LM324m 为例,需要通过一定的变化使系统的峰值缩小到工作范围之内。

本研究的电路搭建主要使用 LM324m 运算放大器、电阻、电容和增益为 1 的乘法器等元器件。对原系统进行坐标尺度变换,令 $x'=\frac{x}{10}, y'=\frac{y}{30}, z'=\frac{z}{40}, w'=\frac{w}{20}$ 并代入系统(1)中。根据混沌系统、电路仿真图以及相应的电路理论知识可得:

$$\begin{cases}\dfrac{\mathrm{d}x'}{\mathrm{d}t}=\dfrac{R_3}{3C_1R_2R_4}y'-\dfrac{1}{C_1R_1}x',\\ \dfrac{\mathrm{d}y'}{\mathrm{d}t}=\dfrac{3R_6}{4C_2R_5R_7}z'-\dfrac{3}{40C_2R_8}x'z',\\ \dfrac{\mathrm{d}z'}{\mathrm{d}t}=\dfrac{2R_{10}}{15C_3R_9R_{11}}x'y'-\dfrac{1}{5C_3R_{12}}x'w',\\ \dfrac{\mathrm{d}w'}{\mathrm{d}t}=-\dfrac{2}{C_4R_{13}}x'+\dfrac{20V_1R_{15}}{C_4R_{14}R_{16}}。\end{cases}\tag{17}$$

根据混沌系统(1)和式(17),可得:

$$\begin{cases}\dfrac{R_3}{3C_1R_2R_4}=1,\ \dfrac{1}{C_1R_1}=10;\\ \dfrac{3R_6}{4C_2R_5R_7}=3,\ \dfrac{3}{40C_2R_8}=1;\\ \dfrac{2R_{10}}{15C_3R_9R_{11}}=1,\ \dfrac{1}{5C_3R_{12}}=1;\\ \dfrac{2}{C_4R_{13}}=1,\ \dfrac{20V_1R_{15}}{C_4R_{14}R_{16}}=12。\end{cases}\tag{18}$$

计算可得,$R_1=100\ \mathrm{k\Omega}$,$R_2=10\ \mathrm{k\Omega}$,$R_3=3\ \mathrm{k\Omega}$,$R_4=R_5=R_7=R_{11}=100\ \mathrm{k\Omega}$,$R_6=4\ \mathrm{k\Omega}$,$R_8=75\ \mathrm{k\Omega}$,$R_9=20\ \mathrm{k\Omega}$,$R_{10}=15\ \mathrm{k\Omega}$,$R_{12}=200\ \mathrm{k\Omega}$,$R_{13}=2\ 000\ \mathrm{k\Omega}$,$R_{14}=50\ \mathrm{k\Omega}$,$R_{15}=3\ \mathrm{k\Omega}$,$R_{16}=100\ \mathrm{k\Omega}$,$V_1=1\ \mathrm{V}$,$C_1=C_2=C_3=C_4=1\ \mu\mathrm{F}$。搭建电路设计仿真图如图 20 所示,其仿真结果如图 21 所示。

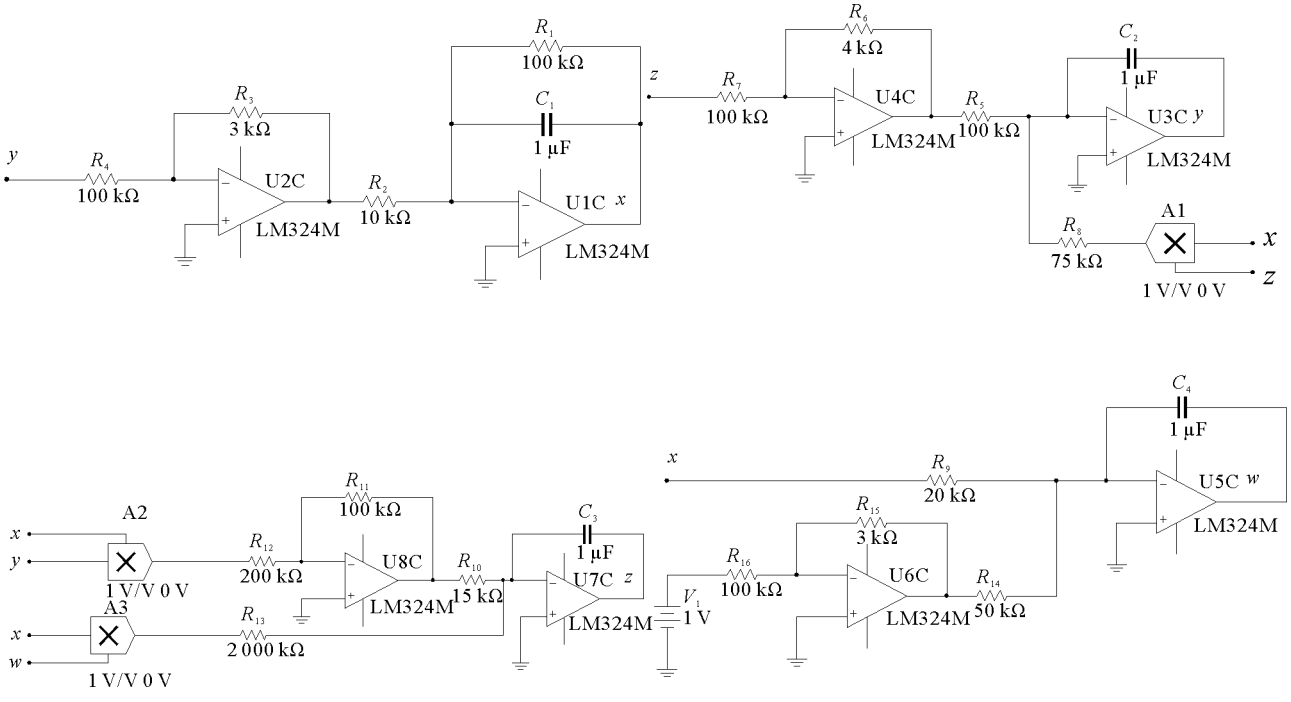
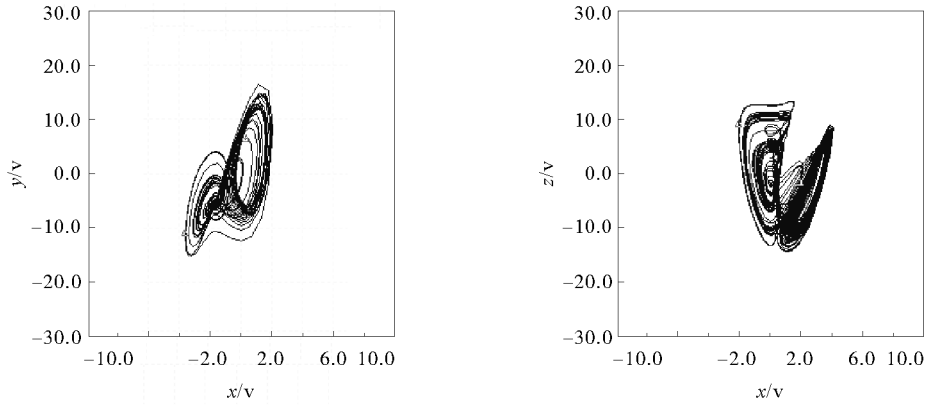


图 20 电路设计仿真图

Fig. 20 Circuit design simulation diagram

从图 21 可以看出,所得吸引子相图与 Matlab 中所得相图基本一致,混沌吸引子存在的峰值范围符合电路元器件的要求,表明该混沌系统在实际生产生活中具有可实现性。



(a) x-y相图　　(b) x-z相图

图 21　电路仿真吸引子相图

Fig. 21　Circuit simulation attractor phase diagram

8　结论

本研究构造了一个新的四维混沌系统,该系统没有平衡点即可产生隐藏吸引子,具有丰富的动力学特性,改变其参数值能够产生不同的隐藏吸引子共存现象。通过 SE 和 C_0 算法进行复杂度分析表明,该系统的 C_0 复杂度均高于 0.52,SE 复杂度均高于 0.9,总体复杂度较高;设计了图像加密算法,通过性能分析发现,该加密算法可以更好地抵抗攻击,具有良好的保密性能和可实现性。系统通过了 NIST 标准测试中的 15 项指标,表明混沌系统具有随机性。最后,通过电路仿真验证了其可实现性。

参考文献:

[1] LORENZ E N. Deterministic non-periodic flow[J]. Journal of the Atmospheric Sciences,1963,20(2):130-141.

[2] YILDIRIM M,KACAR F. Chaotic circuit with OTA based memristor on image cryptology[J/OL]. AEU:International Journal of Electronics and Communications,2020,127(1). DOI:10.1016/j.aeue.2020.153490.

[3] YAN M X,XU H. The multi-scroll hyper-chaotic coexistence attractors and its application[J/OL]. Signal Processing Image Communication,2021,95. DOI:10.1016/j.image.2021.116210.

[4] XIU C B,ZHOU R X,LIU Y X. New chaotic memristive cellular neural network and its application in secure communication system[J/OL]. Chaos,Solitons and Fractals,2020(141). DOI:10.1016/j.chaos.2020.110316.

[5] XIU C,ZHOU R,ZHAO S,et al. Memristive hyperchaos secure communication based on sliding mode control[J]. Nonlinear Dynamics,2021,(4):1-17.

[6] MARTINES-ARANO H,VIDALES-HURTADO M A,PALACIOS-BARRETO S,et al. Sequential photodamage driven by chaotic systems in NiO thin films and fluorescent human cells[J/OL]. Processes,2020,8(11). DOI:10.4319/lo.2013.58.2.0489.

[7] YANG L B,YANG Q G,CHEN G R. Hidden attractors,singularly degenerate heteroclinic orbits,multistability and physical realization of a new 6D hyperchaotic system[J]. Communications in Nonlinear Science and Numerical Simulation,2020,90:10-17.

[8] LEONOV G A,KUZNETSOV N V. Hidden attractors in dynamical systems:From hidden oscillations in Hilbert-Kolmogorov Aizerman,and Kalman problems to hidden chaotic attractor in Chua circuits[J]. International Journal of Bifurcation and Chaos,2013,23(1):285-303.

[9] JAFARI S,SPROTT J C,NAZARIMEHR F. Recent new examples of hidden attractors[J]. The European Physical Journal Special Topics,2015,224(8):331-343.

[10] ZHANG S,ZENG Y C,LI Z J,et al. Generating one to four-wing hidden attractors in a novel 4D no-equilibrium chaotic system with extreme multistability[J]. Chaos,2018,28(1):1-9.

[11] WANG X,CHEN G R. A chaotic system with only one stable equilibrium[J]. Communications in Nonlinear Science and Numerical Simulation,2011,17(3):429-436.

[12] JIA H Y,SHI W X,WANG L,et al. Energy analysis of Sprott:A system and generation of a new Hamiltonian conservative chaotic system with coexisting hidden attractors[J]. Chaos,Solitons and Fractals:the interdisciplinary journal of Nonlinear Science,and Nonequilibrium and Complex Phenomena,2020,133:85-96.

[13] LAI Q,WAN Z Q,KUATE P D K. Modelling and circuit realisation of a new no-equilibrium chaotic system with hidden attractor and coexisting attractors[J]. Electronics Letters,2020,56(20):529-538.

[14] JIN X,DUAN X T,JIN H,et al. A novel hybrid secure image encryption based on the shuffle algorithm and the hidden attractor chaos system[J]. Entropy,2020,22(6):1-18.

[15] 鲜永菊,莫运辉,徐昌彪,等. 具有多种吸引子共存类型的新型四维混沌系统[J]. 华南理工大学学报(自然科学版),2020,48(3):32-43.
XIAN Yongju,MO Yunhui,XU Changbiao,et al. New four-dimensional chaotic system with multiple types of coexistence of attractor[J]. Journal of South China University of Technology (Natural Science Edition),2020,48(3):32-43.

[16] FANG S Y,LI Z J,ZHANG X,et al. Hidden extreme multistability in a novel no-equilibrium fractional-order chaotic system and its synchronization control[J]. Brazilian Journal of Physics,2019,49(6):846-858.

[17] AL-HAYALI M A, AL-AZZAWI F S. A 4D hyperchaotic Sprott S system with multistability and hidden attractors [J/OL]. Journal of Physics:Conference Series,2021,1879(3). DOI:10.1088/1742-6596/1879/3/032031.

[18] LI X,LI Z J. Hidden extreme multistability generated from a fractional-order chaotic system[J]. Indian Journal of Physics,2019,93(12):856-866.

[19] LIU J Y,YANG D D,ZHOU H B,et al. A digital image encryption algorithm based on bit-planes and an improved logistic map[J]. Multimedia Tools and Applications,2018,77(8):10217-10233.

[20] WANG S C,WANG C H,XU C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm[J]. Optics and Lasers in Engineering,2020,128:1299-1308.

[21] PATRO K A K,SONI A,NETAM P K,et al. Multiple grayscale image encryption using cross-coupled chaotic maps[J]. Journal of Information Security and Applications,2020,52:28-36.

[22] 王忠林,姚福安,李祥峰. 基于 FPGA 的一个超混沌系统设计与电路实现[J]. 山东大学学报(理学版),2008,43(12):93-96.
WANG Zhonglin,YAO Fuan,LI Xiangfeng. Design and realization of a hyperchaotic system based FPGA[J]. Journal of Shandong University (Natural Science),2008,43(12):93-96.

[23] LÜ J H,CHEN G R. A new chaotic attractor coined[J]. International Journal of Bifurcation and Chaos,2002,12(3):659-661.

[24] 叶晓林,牟俊,王智森,等. 基于 SE 和 C_0 算法的连续混沌系统复杂度分析[J]. 大连工业大学学报,2018,37(1):67-72.
YE Xiaolin,MU Jun,WANG Zhisen,et al. Analysis of continuous chaotic complexity based on SE and C_0 algorithm[J]. Journal of Dalian Polytechnic University,2018,37(1):67-72.

(责任编辑:傅 游)