物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

一种新型的四维多翼超混沌吸引子及其在图像加密中的研究

彭再平　王春华　林愿　骆小文

A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption

Peng Zai-Ping　Wang Chun-Hua　Lin Yuan　Luo Xiao-Wen

引用信息 Citation: Acta Physica Sinica, **63**, 240506 (2014)　DOI: 10.7498/aps.63.240506
在线阅读 View online: http://dx.doi.org/10.7498/aps.63.240506
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2014/V63/I24

一种新型的四维多翼超混沌吸引子及其在图像加密中的研究*

彭再平 王春华† 林愿 骆小文

(湖南大学信息科学与工程学院, 长沙 410082)

(2014 年 5 月 28 日收到; 2014 年 8 月 10 日收到修改稿)

提出了一种新的能产生多翼混沌吸引子的四维混沌系统, 该系统在不同的参数条件下能产生混沌、超混沌吸引子. 然后对此混沌系统的一些基本的动力学特性进行了理论分析和数值仿真, 如平衡点、Poincaré 映射、耗散性、功率谱、Lyapunov 指数谱、分岔图等. 同时设计了一个模拟振荡电路实现四翼超混沌吸引子, 硬件电路模拟实验结果与数值仿真结果相一致. 最后将此四维多翼超混沌系统用于物理混沌加密和高级加密标准加密级联的混合图像加密算法, 这种利用物理混沌不可预测性的混合加密系统, 不存在确定的明文密文映射关系, 且密文统计特性也比其他加密系统要好.

关键词: 四维混沌系统, 高级加密标准, 物理混沌, 混合加密系统

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.63.240506

1 引 言

在非线性电路中产生各种不同类型并适合保密通信的混沌与超混沌信号是近年来物理学和信息科学界所关注的热门话题, 混沌吸引子的复杂结构及其复杂的动力学行为, 在生物学、电子工程学、数字水印、保密通信和信息处理学等领域有着很好的应用前景[1−6]. 因此, 产生具有复杂拓扑结构的多涡卷和多翼混沌吸引子已经变得非常重要.

目前, 一方面是通过使用一些非线性函数来产生多涡卷混沌吸引子, 另一方面是利用光滑自治系统来构建多翼混沌吸引子. 1993 年, Miranda 和 Stone[7] 首次提出了在 Lorenz 系统中产生环状多翼混沌吸引子. 2007 年, 王繁珍等提出了一个三翼或四翼的混沌系统. 2008 年, Grassi[8] 通过耦合几个混沌系统, 可以产生四翼和八翼混沌吸引子. 2012 年, 周欣等[9] 提出了一种网格多翼的混沌系统. 虽然人们已经能很容易地构造出多翼混沌系统, 但是对于多翼超混沌吸引子的构造和研究还是很少. 且多翼超混沌吸引子的拓扑结构更加复杂, 具有丰富的动力学特性, 因此, 研究多翼超混沌系统具有重要的应用价值. 1979 年, Rössler 最先提出超混沌系统. 从那时起, 一些超混沌系统相继被提出. 仓诗建等提出了一个四维非自治超混沌系统, 但是该系统包含了一个驱动信号, 该驱动信号引入了时间 t, 因此分析和计算都不方便. Qi 等[10] 提出了一个新的四维超混沌系统, 但是该超混沌结构简单, 包含四个非线性项, 且四翼形式并不明显. 本文提出了一种新型的四维多翼超混沌系统, 能产生明显的两翼混沌吸引子、四翼超混沌吸引子, 系统参数的动态范围广, 而且该系统仅包含三个光滑的非线性项, 只有五个平衡点, 系统结构简单, 电路易于实现, 只需要三个模拟乘法器.

近年来, 随着混沌理论与应用的发展, 很多基于混沌系统的图像加密算法方案被提出, 基于混沌系统的图像加密方案在安全性、计算能力、复杂度等方面都表现出了优良的特性[11−13]. 但是, 采用单一的混沌去进行图像加密面临的问题是: 当用数字计算机实现时, 由于有限精度效应, 其复杂的混沌动力学特性退化迅速. 因此, 采用轨道简单的混沌系统组成的密码直接加密明文, 能够从混沌轨道

* 国家自然科学基金 (批准号: 61274020) 资助的课题.

† 通讯作者. E-mail: wch1227164@sina.com

中提取有效的信息来破解密码[14]. 为了克服采用单一的混沌进行图像加密的缺陷, 一些采用常规加密和混沌加密相混合的图像加密算法被提出. 2009年晋建秀和丘水生[15]提出采用物理实现装置所产生的物理混沌加密与DES加密级联来实现混合图像加密, 但采用的是普通的Lorenz物理混沌、Chua物理混沌等, 动力学特征不够复杂, 而且高级加密标准(AES)的128位密钥比DES的56位密钥强1024倍, 相比之下, AES比DES的加密效率更高. 2012年, 林愿等[16]提出了基于CCII的多涡卷物理混沌加密与AES加密的混合加密系统, 但是该加密系统采用的物理混沌不是超混沌吸引子, 动力学特性不够复杂. 本文提出了一种新的加密方案, 采用四维超混沌系统产生的四翼超混沌吸引子, 用于物理混沌加密与AES 加密的混合加密算法. 该加密算法是将常规加密和混沌加密相混合, 除了穷举攻击之外一切基于确定的明文密文映射关系的攻击方法, 对该方案都将失效, 因此系统具有较高的安全性.

2 一种新型的四维多翼超混沌系统

通过在三维自治混沌系统的基础上引入一个非线性状态反馈控制器u, 构建了一个新型的四维多翼超混沌系统, 它的数学表达式描述为

$$\begin{cases} \dot{x} = ax - yz, \\ \dot{y} = by + xz - cu, \\ \dot{z} = xy - dz, \\ \dot{u} = y + eu, \end{cases} \tag{1}$$

其中, a, b, c, d, e为系统参数; 且均为实常数; x, y, z是状态变量; u是状态反馈控制器.

3 系统的动力学分析

3.1 对称性与耗散性

在系统(1)中可以看出, 该混沌系统具有x轴的对称性, 其对称性可以从$(x, y, z, u) \to (x, -y, -z, -u)$的坐标变换不变性得到. 另外, 由于

$$\begin{aligned} \nabla V &= \partial\dot{x}/\partial x + \partial\dot{y}/\partial y + \partial\dot{z}/\partial z + \partial\dot{u}/\partial u \\ &= a + b - d + e, \end{aligned} \tag{2}$$

所以当$a + b - d + e < 0$时, 则系统(1)是耗散的, 且以指数形式收敛

$$\frac{\mathrm{d}V}{\mathrm{d}t} = \mathrm{e}^{-(d-a-b-e)t}, \tag{3}$$

显然, 体积元V_0在t时刻收缩为体积元$V_0\,\mathrm{e}^{-(d-a-b-e)t}$, 即当$t \to \infty$时, 包含系统轨线的每个体积元以指数率$a + b - d + e$收缩到零. 因此, 所有系统轨线最终会被限制在一个体积元为零的集合上, 而且它的渐进动力学行为固定在一个吸引子上.

3.2 平衡点

令$\dot{x} = \dot{y} = \dot{z} = 0$, 即

$$\begin{cases} ax - yz = 0, \\ by + xz - cu = 0, \\ xy - dz = 0, \\ y + eu = 0. \end{cases} \tag{4}$$

当$a = 3$, $b = -8$, $c = 5$, $d = 5$, $e = 0.5$时, 解方程(4), 得系统(1)有5个平衡点, $\boldsymbol{S}_0 = [0, 0, 0, 0]$, $\boldsymbol{S}_1 = [-9.48,\ 3.87, -7.35,\ 7.74]$, $\boldsymbol{S}_2 = [9.48,\ 3.87,\ 7.35,\ 7.74]$, $\boldsymbol{S}_3 = [-9.48, -3.87,\ 7.35,\ -7.74]$, $\boldsymbol{S}_4 = [9.48,\ -3.87,\ -7.35, -7.74]$. 根据每一个平衡点所对应的雅克比矩阵, 计算相应的特征值, 相关结果在表1中列出. 根据平衡点与稳定性的关系, 平衡点$\boldsymbol{S}_0$是渐近稳定的鞍点, 其他四个平衡点$\boldsymbol{S}_1$, $\boldsymbol{S}_2$, $\boldsymbol{S}_3$, $\boldsymbol{S}_4$是渐近稳定的鞍焦点.

3.3 Poincaré 映射和功率谱

Poincaré 映射能够反映混沌的分岔和可折叠特性, 系统(1)在不同平面的Poincaré 映射如图1所示. 可以很清晰地看出有很多可折叠的枝节, 由此可知系统具有丰富的动力学特性. 图2是

表1 各个平衡点分别对应的特征值

$\boldsymbol{S}_0$	$\boldsymbol{S}_1$	$\boldsymbol{S}_2$	$\boldsymbol{S}_3$	$\boldsymbol{S}_4$
−1.2396	−15.4892	−15.4892	−14.5743	−14.5743
−7.2604	2.7428 + 7.9125i	2.7428 + 7.9125i	2.0372 + 3.9249i	2.0372 + 3.9249i
3	2.7428 − 7.9125i	2.7428 − 7.9125i	2.0372 − 3.9249i	2.0372 − 3.9249i
−5	−0.4965	−0.4965	−0.0002	−0.0002

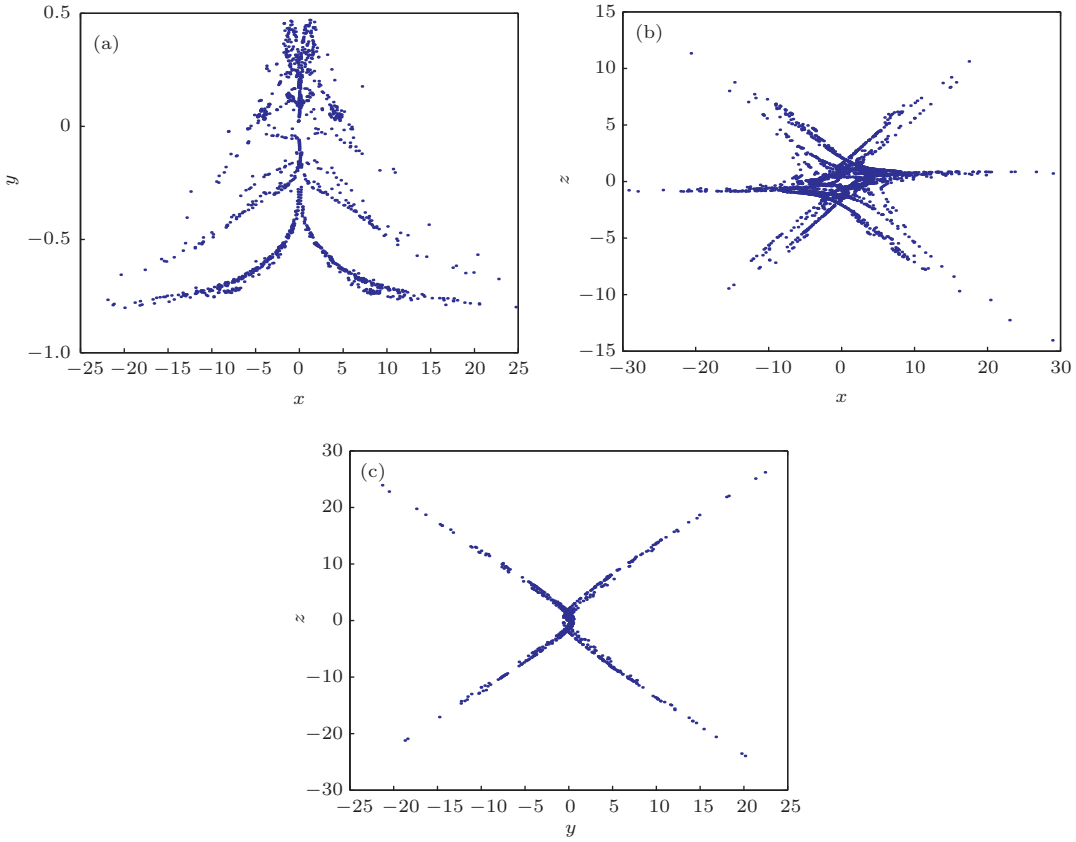

图 1 Poincaré 映射 (a) x-y 截面; (b) x-z 截面; (c) y-z 截面

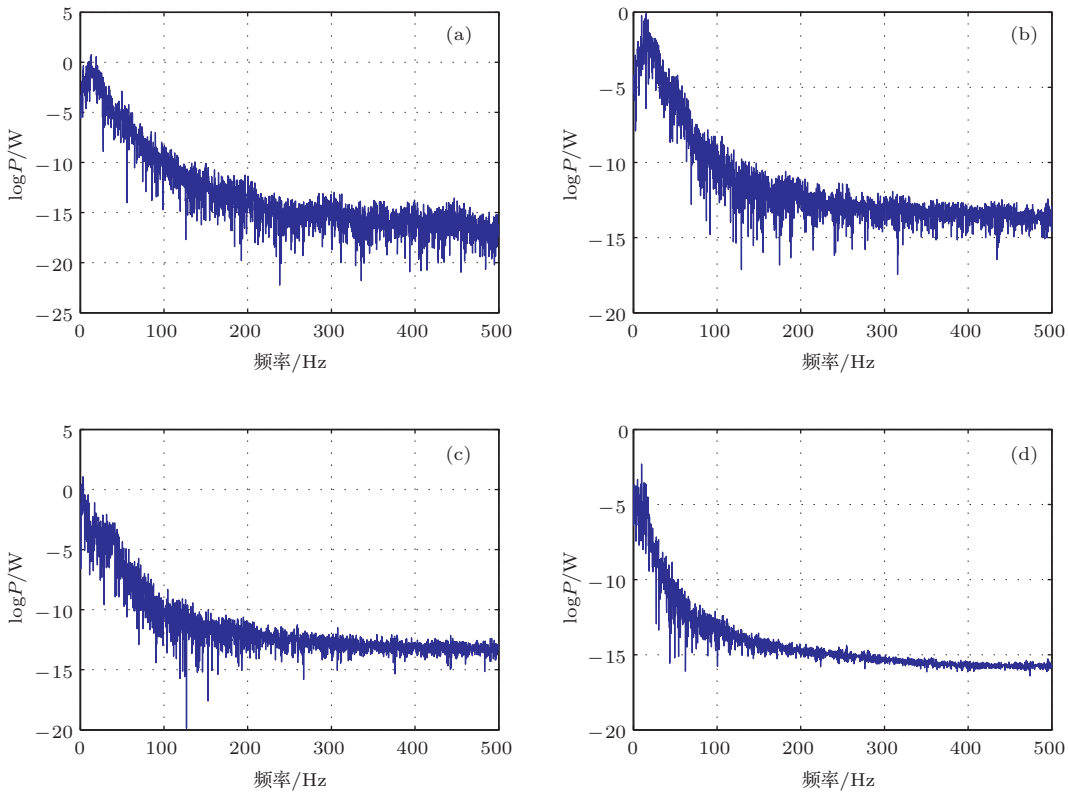

图 2 功率谱 (a) x; (b) y; (c) z; (d) u

系统 (1) 的功率谱, 从中可以看出存在连续的宽频带功率 P 谱特性.

3.4 Lyapunov 指数谱与分岔图

系统的主要动力学特性也可以通过其 Lyapunov 指数谱和分岔图进行分析. 当系统参数 $a = 3$, $b = -8$, $d = 5$, $e = 0.5$, 而系统参数 c 变化时, 即可得到随着 c 变化的 Lyapunov 指数谱如图 3 所示. 从图中可以很明显地看出, 系统有两个大于零的 Lyapunov 指数, 因此该系统处于超混沌系统.

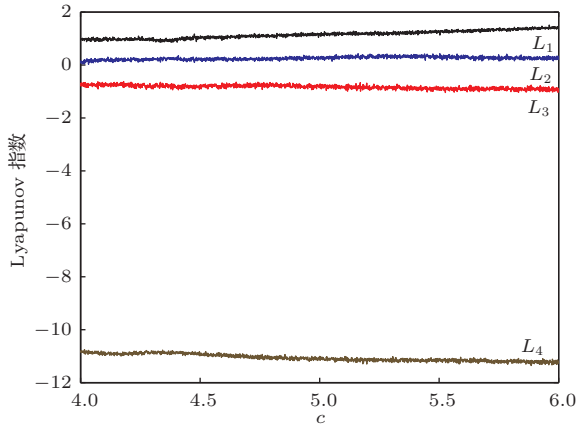

图 3 (网刊彩色) 随 c 变化的 Lyapunov 指数谱

当系统参数 $a = 3$, $b = -8$, $d = 5$, $e = 0.5$, 而参数 c 是变化的, 相应的关于变量 c 的分岔图如图 4 所示. 在图中可以清晰地看出, 在 [0, 15] 区间里, 随着 c 的增加, 系统 (1) 出现倍周期分岔现象.

4 四维多翼混沌吸引子相图

当 $a = 3$, $b = -8$, $c = 5$, $d = 5$, $e = 0.5$ 时, 该四维超混沌系统的四个 Lyapunov 指数分别为 $LE_1 = 1.23$, $LE_2 = 0.32$, $LE_3 = -0.81$, $LE_4 = -11.04$. 容易看出, 系统 (1) 有两个 Lyapunov 指数, $LE_1 = 1.23 > 0$, $LE_2 = 0.32 > 0$, 所以系统处于超混沌状态. 系统 (1) 能够产生四翼超混沌吸引子, 在各个相平面的四翼超混沌吸引子如图 5 所示.

当 $a = 3$, $b = -8$, $c = -3$, $d = 5$, $e = 0.6$ 时, 系统 (1) 能够产生两翼混沌吸引子, 在各个相平面的两翼混子吸引子如图 6 所示.

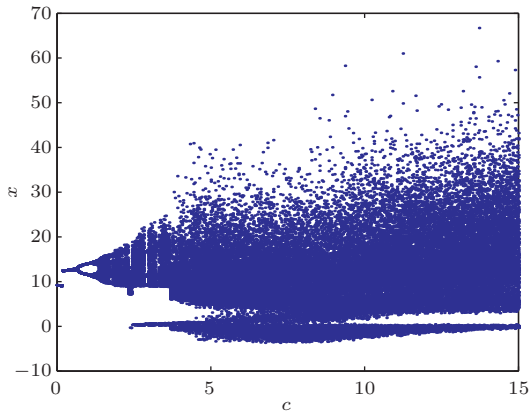

图 4 系统 (1) 随 c 变化的分岔图

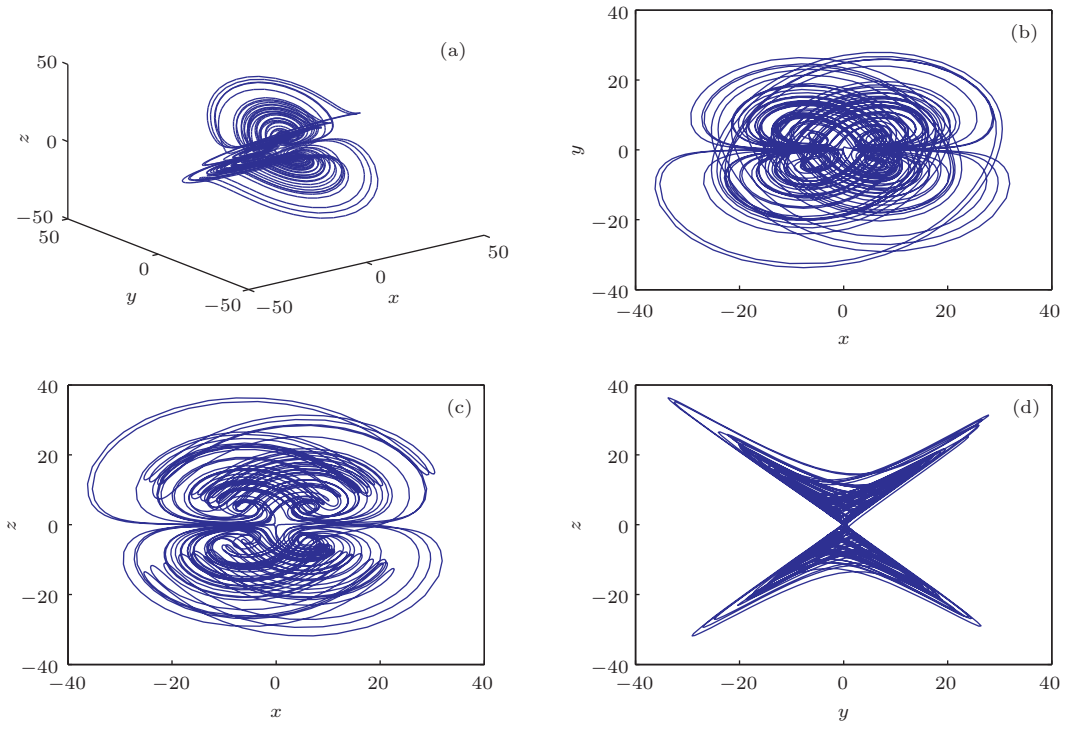

图 5 四翼超混沌吸引子相图 (a) x-y-z 三维图; (b) x-y 平面; (c) x-z 平面; (d) y-z 平面

5 电路设计和实验结果

为了证明系统(1)的四翼超混沌特性, 本节设计了一个模拟电路如图7所示, 该电路主要由运算放大器TL082CD构成的反相加法器、积分器、反相器、乘法器AD633组成. 其中, 运算放大器TL082CD的电源电压 $E = \pm 10$ V 乘法器AD633的增益是0.1. 此电路结构简单, 只需三个乘法器, 相比于其他文献所用的乘法器更少、更易于实现.

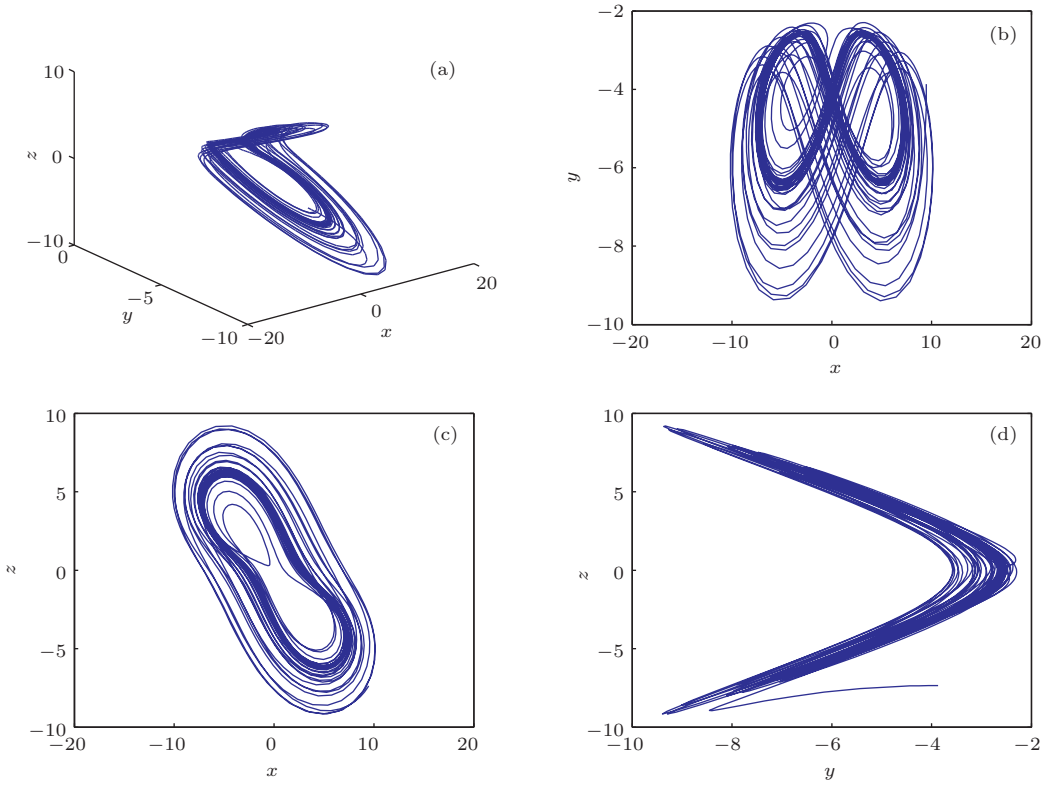

图6 两翼混沌吸引子相图 (a) x-y-z 三维图; (b) x-y 平面; (c) x-z 平面; (d) y-z 平面

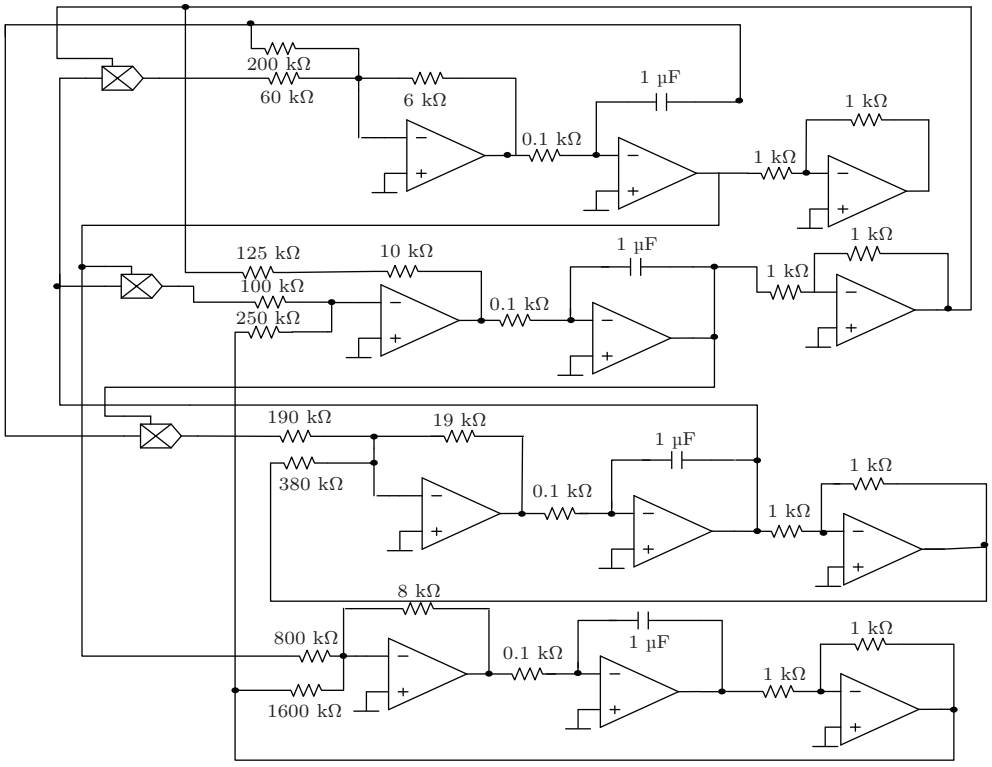

图7 四翼四维超混沌系统电路图

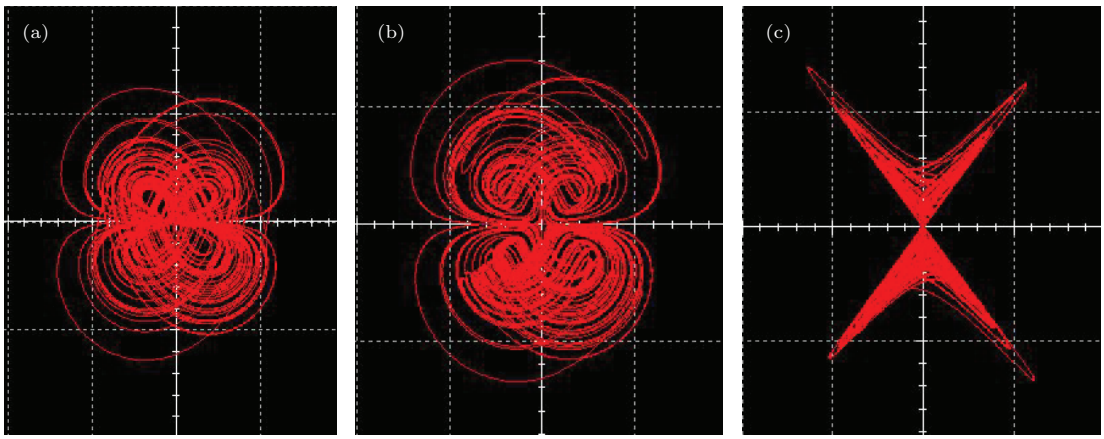

图 8 (网刊彩色) 四翼超混沌吸引子电路实验结果 (a) x-y 平面; (b) x-z 平面; (c) y-z 平面

该电路实验结果在各个平面的投影如图 8 所示, 在示波器上观察到, 该四翼超混沌吸引子在各个平面上的电路实验结果与数值仿真结果相一致.

6 四翼超混沌系统在混合图像加密中的研究

6.1 混合图像加密原理

混沌系统的主要特征有初值敏感性、类随机性和不可预测性, 这几个特征是其被应用于密码学最根本的原因. 混沌加密系统的主要优点是能够利用混沌信号的不可预测性特征, 主要缺点是密钥空间的设计问题没有解决. 而常规的加密系统的主要优点是具有成熟的密钥空间设计技术, 主要缺点是惟一对应的明文密文而被破译的可能性很大. 因此, 本文由混沌加密器和常规加密器相结合组成混合加密系统, 从而使得这两种加密器的优点可以互补, 混合加密系统的抗攻击能力明显高于任一单级加密器.

提出的基于四维超混沌系统产生的四翼超混沌吸引子, 用于物理混沌加密和 AES 加密的混合图像加密算法的方案原理如图 9 所示.

混合加密算法的主要步骤如下.

1) 混沌电路产生的连续四翼超混沌信号经采样得到序列 x_i, x_i 经过变换得到 x_j, $x_j = \mathrm{round}[c(x_{1i}^2+x_{2i}^2+x_{3i}^2)^{1/2}+d]\mathrm{mod}256$ 表示 $c(x_{1i}^2+x_{2i}^2+x_{3i}^2)^{1/2}+d$ 对 255 取整后再取余, $c=3000$, $d=127$. 由 x_j 构成的密钥流 x 对原始信息 p 加密, 得到加密密文 c, 其中 $c=p\oplus x$.

2) 密文 c 经过常规加密技术 AES 在密钥 k 下得到加密密文 d.

3) 加密密文 d 经过信道传送到接收端, 接收端收到信号 $\widehat{d}$, $d=\widehat{d}$.

4) 接收端首先是对 $\widehat{d}$ 进行解密, 在解密密钥 $\widehat{k}$ 解密下得到解密密文 $\widehat{c}$.

5) $\widehat{c}$ 经过混沌解密密钥 $\widehat{x}$, 得到恢复信息流 $\widehat{p}$.

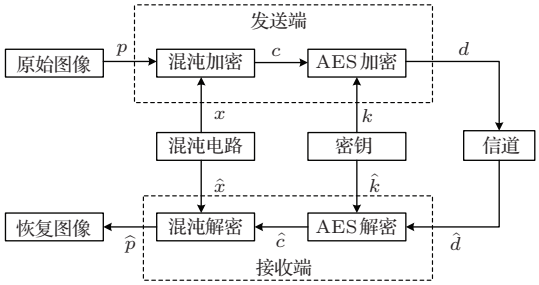

图 9 混合图像加密方案原理框图

6.2 算法仿真结果

仿真过程采用 Matlab 7.11 实现, 同时选取 256×256 的 Lena 灰度图作为初始图像, 如图 10 (a) 所示, 混沌加密信号采用四翼超混沌信号.

6.3 灰度直方图分析

图 11 所示为原始图像和混合加密图像的灰度直方图. 从直观上可以看出, 混合加密图像的灰度均匀性明显优于原始图像, 且密文的像素值在 [0, 255] 范围内取值的概率均等, 如此可以防止密文的灰度统计特性.

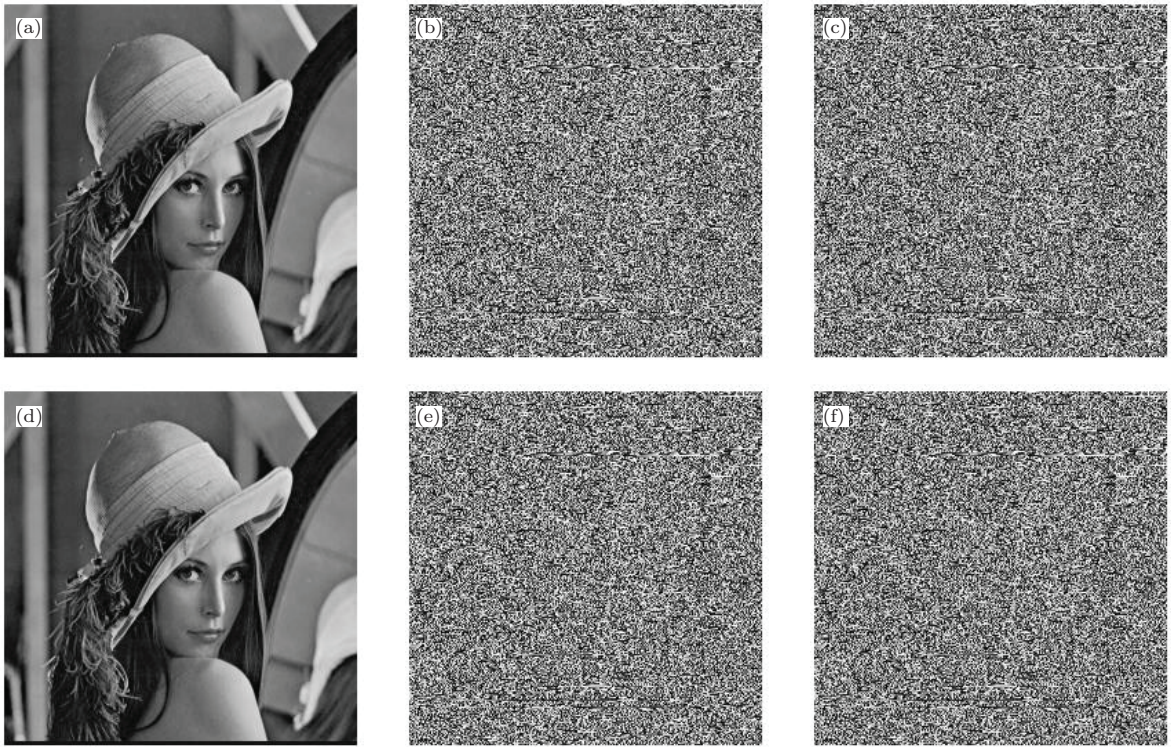

图 10 仿真结果 (a) 原始图像; (b) 单级四翼超混沌加密; (c) 四翼超混沌 -AES 混合加密; (d) 正确解密图像; (e) 单级 AES 加密; (f) 错误解密图像

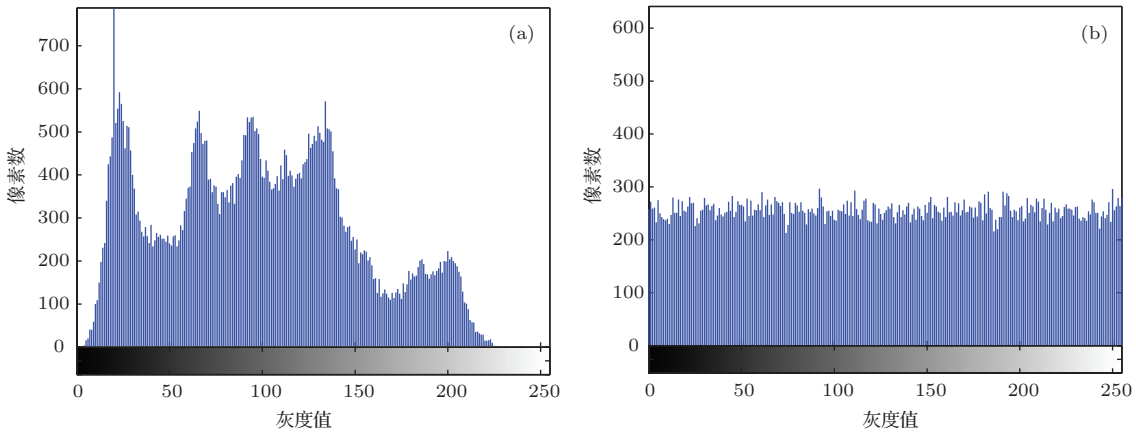

图 11 原始图像及混合加密图像灰度直方图 (a) 原始图像; (b) 混合加密图像

6.4 相邻像素的相关系数

数字图像中各个像素之间的相关性很大, 这就说明在大块区域中, 灰度值可能会出现均匀分布的情况, 因此灰度直方图并不能完全描述混沌加密方案的安全性. 进行图像加密的目标之一是为了减少图像相邻像素的相关性.

为了能够定量比较混合加密图像和原始图像像素的相关性, 本文选取计算整幅图像的相关系数.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(X))^2, \tag{6}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_j - E(y)), \tag{7}$$

$$\rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\cdot D(y)}}, \tag{8}$$

其中 x 和 y 分别表示图像中相邻两个像素点的像素值, ρ_{xy} 为相邻两个像素点的相关系数.

图 12 是原始图像与经过四翼超混沌 -AES 混合加密后的图像相邻像素在对角、水平和垂直方向的相关性. 表 2 中的数据定量地反映了原始

图像的相邻像素高度相关, 而密文图像的相邻像素基本上不相关, 这说明了原始图像的统计相关性已被扩散到随机的密文中, 从而验证了该算法的正确性. 四翼超混沌-AES混合加密图像与单级AES加密的相关系数相比总体上也有一定的改善.

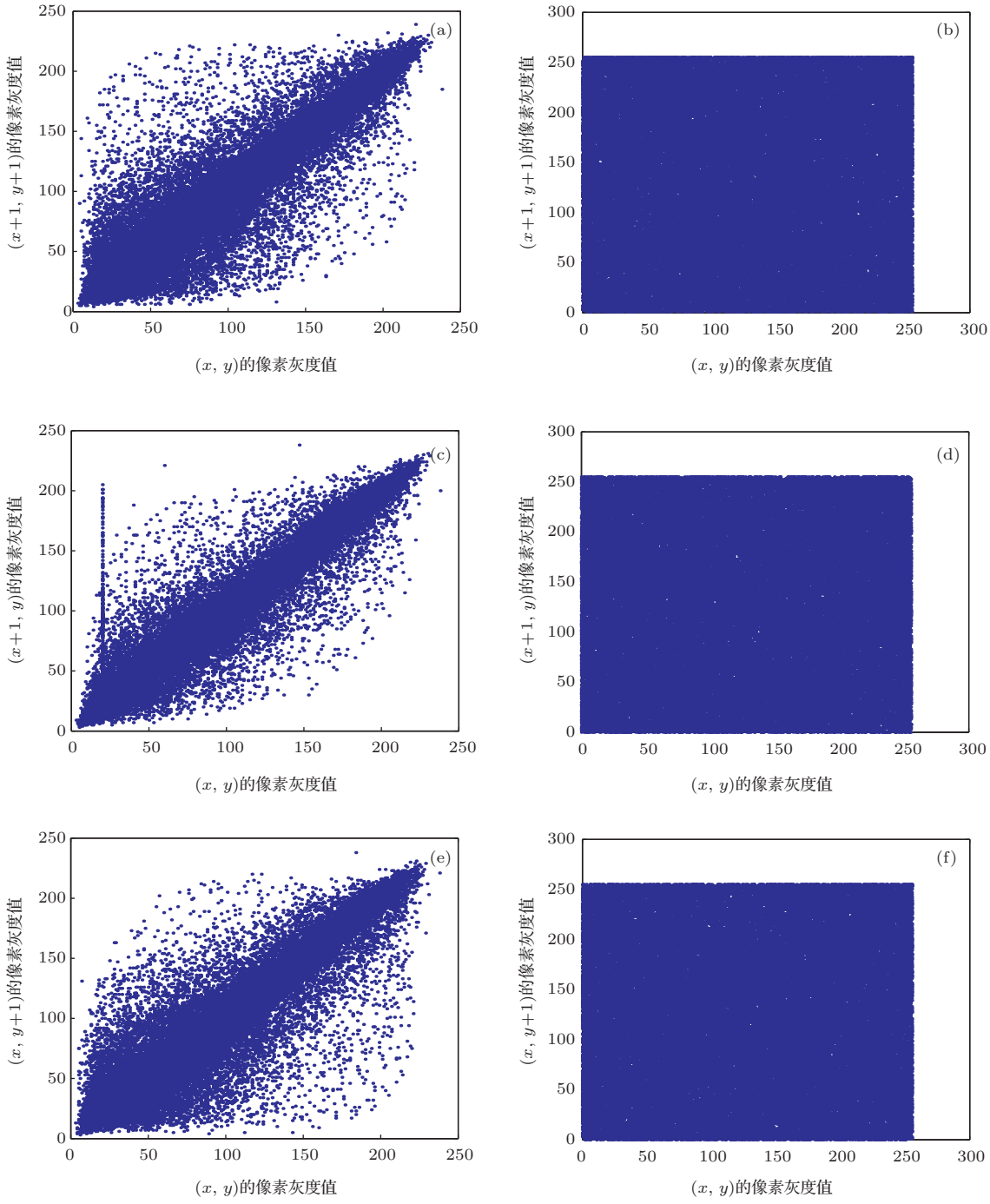

图 12 相邻像素相关性比较 (a) 和 (b) 对角相邻; (c) 和 (d) 水平相邻; (e) 和 (f) 垂直相邻

表3列出了四翼超混沌-AES与其他基于混沌系统的混合加密方法的相邻像素相关系数. 从表3中可以看出, 经过四翼超混沌-AES混合加密后的图像各方向相关系数均小于其他基于混沌系统的混合加密后的图像各方向的相关系数. 所以本文采用的四翼超混沌-AES混合加密明显优于其他基于混沌系统的混合加密方法.

表 2 原始图像与密文图像的相关系数比较

像素关系	原始图像	四翼超混沌-AES 加密	单级 AES 加密
对角相邻	0.9147	0.0018	−0.0019
水平相邻	0.9649	0.0013	−0.0022
垂直相邻	0.9412	0.0020	0.0021

表 3 四翼超混沌 -AES 加密与算法 Lorenz-DES 加密、物理 Chua-DES 加密、多涡卷混沌 (2 × 2)-AES 加密密文的相关系数比较

像素关系	原始图像	四翼超混沌 -AES 加密	算法 Lorenz-DES 加密	物理 Chua-DES 加密	多涡卷混沌 (2 × 2)-AES 加密
对角相邻	0.9147	0.0018	0.0051	0.0082	0.0019
水平相邻	0.9649	0.0013	0.0050	0.0057	0.0020
垂直相邻	0.9412	0.0020	0.0046	0.0020	−0.0031

7 结 论

本文提出了一种新型的四维多翼超混沌系统, 该系统结构简单, 电路易于实现. 分析了混沌系统的基本动力学特性, 包括平衡点、Lyapunov 指数谱、分岔图、Poincaré 映射、功率谱等. 在理论分析的基础上, 运用模拟器件运算放大器 TL082CD 和乘法器 AD633 设计了超混沌电路, 电路实验结果与数值模拟结果的一致性证实了该方法的可行性. 同时, 将此四维多翼超混沌系统应用于物理混沌加密和高级加密标准加密的混合图像加密算法, 并对混合加密系统进行了数值仿真, 仿真结果验证了该混合加密算法的正确性. 因此, 本文提出的四维多翼超混沌系统在工程实践中有很好的应用前景, 特别是保密通信和信息安全等领域有潜在的应用价值.

参考文献

[1] Weiss J N, Garfinkel A, Spano M L 1994 *J. Clin. Invest.* **93** 1355

[2] Elwakil A S, Kennedy M P 1999 *Microelectronics J.* **30** 739

[3] Suzuki T, Saito T 1994 *IEEE Trans. Circuits Syst. I* **41** 876

[4] Gao T, Chen Z 2008 *Phys. Lett. A* **372** 394

[5] Chen G, Mao Y, Chui C K 2004 *Chaos Soliton. Fract.* **21** 749

[6] Pareek N K, Patidar V, Sud K K 2006 *Image. Vision Comput.* **24** 926

[7] Miranda R, Stone E 1993 *Phys. Lett. A* **178** 105

[8] Grassi G 2008 *Chin. Phys. B* **17** 3247

[9] Zhou X, Wang C H, Guo X R 2012 *Acta Phys. Sin.* **61** 200506 (in Chinese) [周欣, 王春华, 郭小蓉 2012 物理学报 **61** 200506]

[10] Qi G, van Wyk M A, van Wyk B J, Chen G R 2009 *Chaos Soliton. Fract.* **40** 2544

[11] Guan Z H, Huang F J, Guan W J 2005 *Phys. Lett. A* **346** 153

[12] Zhang L H, Liao X F, Wang X B 2005 *Chaos Soliton. Fract.* **24** 759

[13] Wong K, Kwor B, Law W 2008 *Phys. Lett. A* **372** 2645

[14] Ashraf A Z, Abdulnasser A R 2011 *Commun. Nonlinear Sci. Numer. Simulat.* **16** 3721

[15] Jin J X, Qiu S S 2010 *Acta Phys. Sin.* **59** 792 (in Chinese) [晋建秀, 丘水生 2010 物理学报 **59** 792]

[16] Lin Y, Wang C H, Xu H 2012 *Acta Phys. Sin.* **61** 240503 (in Chinese) [林愿, 王春华, 徐浩 2012 物理学报 **61** 240503]

A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption*

Peng Zai-Ping Wang Chun-Hua† Lin Yuan Luo Xiao-Wen

(*College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*)

(Received 28 May 2014; revised manuscript received 10 August 2014)

Abstract

In this paper, a novel four-dimensional chaotic system for generating multi-wing chaotic attractors is proposed, and chaotic and hyper-chaotic attractors are generated in different parameters. Besides, basic dynamical properties of the chaotic system, such as equilibrium point Poincaré mapping, dissipativity, power spectrum, Lyapunov exponent spectrum, bifurcation diagram are studied numerically and theoretically. An analog oscillator circuit is designed for implementing the four-wing hyper-chaotic attractors, and the hardware circuit experimental results are shown to be in good agreement with the numerical simulation results. Finally, the four-wing hyper-chaotic system is used for hybrid image encryption of physical chaos encryption and advanced encryption standard encryption algorithm. Because physical chaos is adopted in this system, there does not exist a definitive relationship between plaintexts and ciphertexts. And the statistical characteristics of ciphertexts should be better than those of any other encryption system.

Keywords: four-dimensional chaotic system, advanced encryption standard, physical chaos, hybrid encryption system

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.63.240506

* Project supported by the National Natural Science Foundation of China (Grant No. 61274020).

† Corresponding author. E-mail: wch1227164@sina.com