简化Lorenz多涡卷混沌吸引子的设计与应用*

艾星星[1)] 孙克辉[1)2)†] 贺少波[1)] 王会海[1)]

1)(中南大学物理与电子学院, 长沙 410083)

2)(新疆大学物理科学与技术学院, 乌鲁木齐 830046)

(2014年1月17日收到; 2014年2月28日收到修改稿)

将简化Lorenz系统线性化成两个线性系统, 采用控制方法得到两涡卷混沌系统, 通过扩展两涡卷混沌系统的指标2鞍焦点, 设计了多涡卷混沌吸引子. 利用相图、分岔图、Poincaré 截面和最大Lyapunov 指数等方法, 分析了该多涡卷混沌系统的动力学特性. 设计了多涡卷混沌吸引子的模拟电路, 并进行了仿真, 数值仿真与电路仿真相一致. 将多涡卷混沌系统应用于图像加密, 设计了多涡卷混沌与高级加密标准(AES)的改进混合加密算法, 并分析了其加密性能. 结果表明, 基于多涡卷混沌系统的改进混合加密算法具有更高的安全性.

关键词: 混沌, 多涡卷吸引子, 简化Lorenz系统, 图像加密

PACS: 05.45.Ac, 05.45.Gg **DOI:** 10.7498/aps.63.120511

1 引 言

自1963年Lorenz提出Lorenz混沌系统, 开启了混沌研究热潮的序幕. 为了更好地应用于保密通信, 人们致力于构造性能更优的混沌系统. 多涡卷混沌系统具有更加复杂的动力学行为, 因此, 多涡卷混沌吸引子的研究正成为混沌领域的研究热点. 在该领域, 人们先后提出了用分段线性、阶梯波、符号函数和延迟微分方程等来产生多涡卷混沌吸引子的方法[1−13]. 近年来, 采用新型控制方法来构造复杂吸引子受到广泛的关注[14−17], 如分段线性控制[14], 反馈控制[15−17]等得到多涡卷混沌吸引子. 此外, 人们提出了多种基于Lorenz 系统族的多翅膀构造方法[18−21], 却鲜有在Lorenz系统族中得到多涡卷吸引子模型的报道. 因此, 研究基于Lorenz系统族的多涡卷混沌吸引子的设计方法具有理论意义与应用价值. 随着多媒体信息技术的飞速发展, 信息安全越来越重要. 对于图像加密, 人们提出了许多传统的加密算法, 如数据加密算法(DES)和高级加密标准(AES)等. 传统加密的主要优势在于具有成熟的密钥空间设计技术, 主要缺点在于明文密文对惟一对应从而可能被破译. 为了提高安全性能, 将混沌技术应用于加密算法中具有很好的应用前景[22−24]. 相比于单一的加密算法, 混沌加密与传统加密算法相结合的混合加密算法具有更好的安全性能[25,26]. 文献[25] 在AES的基础上, 提出将混沌序列作为AES的基密钥对信号进行加密的混合加密算法, 得到了很好的加密效果. 文献[26]提出先对信号混沌加密, 然后再进行AES加密的混合加密算法, 比单一的加密算法具有更好的加密效果. 混合加密算法既利用了传统加密技术的成熟性, 同时又将混沌的良好随机性应用到加密中, 提高了系统的安全性.

本文以单参数简化Lorenz系统[27]为模型, 研究多涡卷混沌系统的设计与应用问题. 首先给出设计原理, 然后通过线性化简化Lorenz系统得到两个线性化系统; 通过设计合适的控制器, 在线性化系统的基础上得到两涡卷和多涡卷混沌吸引子, 并进行了性能分析; 设计相应的混沌电路并进行仿真,

* 国家自然科学基金(批准号: 61161006, 61073187)和中央高校基本科研业务费(批准号: 72150050650)资助的课题.

† 通讯作者. E-mail: kehui@csu.edu.cn

最后将多涡卷混沌系统应用于图像加密.

2 两涡卷混沌吸引子的设计

2.1 设计原理

若一个三维系统具有两个指标2鞍焦点, 则将系统在两个指标2鞍焦点处进行线性化, 得到两个线性化系统, 因线性化系统是由原系统的雅可比矩阵在两个指标2鞍焦点处得到的, 容易验证两线性化系统的平衡点为(0,0,0), 并且平衡点的特征值与原来的鞍焦点相同, 所以线性化后的平衡点也为指标2鞍焦点. 通过设计控制器将两平衡点移位, 并连接组合在一起, 理论上便能形成具有两个指标2鞍焦点的混沌系统. 在此基础上, 通过设计控制器可得到具有多个指标2鞍焦点的混沌系统, 从而得到多涡卷混沌吸引子.

2.2 简化Lorenz多涡卷混沌吸引子的设计

单参数简化Lorenz系统的数学模型为[27]

$$\begin{cases} \dot{x} = 10(y - x), \\ \dot{y} = (24 - 4c)x - xz + cy, \\ \dot{z} = xy - 8z/3, \end{cases} \tag{1}$$

其中, c是系统参数, 当参数$c \in [-1.59,\ 7.75]$时, 系统出现混沌态. 易求得系统有三个平衡点分别是

$$S_0 = (0, 0, 0),$$
$$S_1 = (\sqrt{64-8c}, \sqrt{64-8c}, 24 - 3c),$$
$$S_2 = (-\sqrt{64-8c}, -\sqrt{64-8c}, 24 - 3c).$$

将系统(1)在平衡点S_1处线性化可得

$$\begin{bmatrix} \dot{x}_1 \\ \dot{y}_1 \\ \dot{z}_1 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ -c & c & -\sqrt{64-8c} \\ \sqrt{64-8c} & \sqrt{64-8c} & -8/3 \end{bmatrix} \times \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix} = \boldsymbol{J}_1 \boldsymbol{X}_1, \tag{2}$$

类似地, 将系统(1)在平衡点S_2处线性化得

$$\begin{bmatrix} \dot{x}_2 \\ \dot{y}_2 \\ \dot{z}_2 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ -c & c & \sqrt{64-8c} \\ -\sqrt{64-8c} & -\sqrt{64-8c} & -8/3 \end{bmatrix} \times \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix} = \boldsymbol{J}_2 \boldsymbol{X}_2, \tag{3}$$

显然$O_1 = O_2 = (0, 0, 0)$是系统(2)和(3)的平衡点. 并且相对应的特征值均为$\lambda_1 = -13.5458$, $\lambda_{2,3} = 0.1645 \pm 10.0481\mathrm{i}$, 因此$O_1$, O_2都是指标2鞍焦点. 与之相对应的特征向量分别为

$$\begin{cases} \boldsymbol{V}_1 = \begin{bmatrix} -0.8555 \\ 0.3033 \\ 0.4197 \end{bmatrix}, \\ \boldsymbol{V}_{2,3} = \begin{bmatrix} 0.2693 \pm 0.2967\mathrm{i} \\ -0.0244 \pm 0.5722\mathrm{i} \\ 0.7152 \end{bmatrix}, \end{cases} \tag{4}$$

$$\begin{cases} \boldsymbol{V}_1' = \begin{bmatrix} -0.8555 \\ 0.3033 \\ -0.4197 \end{bmatrix}, \\ \boldsymbol{V}_{2,3}' = \begin{bmatrix} -0.2693 \mp 0.2967\mathrm{i} \\ 0.0244 \mp 0.5722\mathrm{i} \\ 0.7152 \end{bmatrix}, \end{cases} \tag{5}$$

实特征值λ_1对应一维稳定的特征空间为$E^S(O_1)$, 即

$$E^S(O_1) : \frac{x}{0.8555} = \frac{y}{0.3033} = \frac{z}{0.4197}, \tag{6}$$

它是空间直线方程, 方向矢量为(8555, 3033, 4197), 而两个复特征值对应两个特征矢量为共轭的复值矢量, 根据线性代数理论, 可由其实部和虚部张成一个特征平面$E^U(O_1)$, 即

$$E^U(O_1) : -0.4092x + 0.2122y + 0.1613z = 0. \tag{7}$$

同样地, 可得到$E^S(O_2)$和$E^U(O_2)$

$$E^S(O_2) : \frac{x}{-0.8555} = \frac{y}{0.3033} = \frac{z}{-0.4197}, \tag{8}$$

$$E^U(O_2) : -0.4092x + 0.2122y - 0.1613z = 0. \tag{9}$$

在系统(2)与系统(3)的基础上, 设计一个合适的控制器, 将系统(2)与系统(3)连接在一起, 从而形成一个异宿轨道. 理论上可得到一个两涡卷的混沌吸引子. 令该转换平面为$S = \{(x, y, z)|x = 0\}$, 控制器为$U = F(x, y, z)$, 即

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix}=\begin{bmatrix}-10 & 10 & 0\\ -c & c & -\sqrt{64-8c}\\ \sqrt{64-8c} & \sqrt{64-8c} & -8/3\end{bmatrix}\left[\begin{pmatrix}x\\ y\\ z\end{pmatrix}-U\right]\quad (x>0), \tag{10a}$$

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix}=\begin{bmatrix}-10 & 10 & 0\\ -c & c & -\sqrt{64-8c}\\ -\sqrt{64-8c} & -\sqrt{64-8c} & -8/3\end{bmatrix}\left[\begin{pmatrix}x\\ y\\ z\end{pmatrix}-U\right]\quad (x<0), \tag{10b}$$

系统 (10) 的平衡点分别在平面的两侧, 其中平衡点 P_1 在平面 $S=\{(x,y,z)|x=0\}$ 上面, P_2 在平面 $S=\{(x,y,z)|x=0\}$ 下面, 且 P_1, P_2 对应的一维稳定特征空间与特征平面分别为

$$\begin{cases}E^S(P_1):\dfrac{x-x_1}{0.8555}=\dfrac{y-y_1}{0.3033}=\dfrac{z-z_1}{0.4197},\\ E^U(P_1):-0.4092(x-x_1)+0.2122(y-y_1)+0.1613(z-z_1)=0,\end{cases} \tag{11}$$

$$\begin{cases}E^S(P_2):\dfrac{x-x_1}{-0.8555}=\dfrac{y-y_1}{0.3033}=\dfrac{z-z_1}{-0.4197},\\ E^U(P_2):-0.4092(x-x_1)+0.2122(y-y_1)-0.1613(z-z_1)=0.\end{cases} \tag{12}$$

$E^S(P_1)$ 与平面 S 相交于一个点 Q_1, $E^S(P_2)$ 与平面 S 相交于一个点 Q_2; $E^U(P_1)$ 与平面 S 相交于一条线 L_1; $E^U(P_2)$ 与平面 S 相交于一条线 L_2. 如果 Q_1 位于 L_2, Q_2 位于 L_1, 则存在一个异宿轨道将平衡点 P_1 和 P_2 连接在一起, 图 1 为异宿轨道示意图, 这样就能得到一个两涡卷混沌吸引子.

设 $U=[x_0\mathrm{sgn}(x),\ y_0\mathrm{sgn}(y),\ z_0\mathrm{sgn}(z)]^{\mathrm{T}}$, 其中 $x_0=1$, $y_0=0.8$, $z_0=0$, 控制器的参数并不惟一, 是通过反复实验验证得到, 并且混沌系统对控制器的参数具有敏感性. 代入系统 (10) 可得

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix}=\begin{bmatrix}-10 & 10 & 0\\ -c & c & -\mathrm{sgn}(x)\sqrt{64-8c}\\ \mathrm{sgn}(x)\sqrt{64-8c} & \mathrm{sgn}(x)\sqrt{64-8c} & -8/3\end{bmatrix}\begin{bmatrix}x-x_0\mathrm{sgn}(x)\\ y-y_0\mathrm{sgn}(y)\\ z-z_0\mathrm{sgn}(z)\end{bmatrix}. \tag{13}$$

系统 (13) 的三维吸引子相图如图 2 所示, 其中系统参数 $c=-1.5$. 可见系统 (13) 能够得到两涡卷吸引子, 并且存在键带, 键带是涡卷系统独有的, 通过键带将两个涡卷连在一起, 从而形成两涡卷混沌吸引子, 同时验证了系统 (13) 具有异宿轨道.

2.3 两涡卷混沌系统的特性分析

$x_0=1$, $y_0=0.8$, $z_0=0$, 初始值为 (2, 1, 1), 在 Matlab 中计算出系统 (13) 的分岔图如图 3 所示, 其中 $c\in[-2,\ 2]$, 步长为 0.005. 通过图示可得, 在

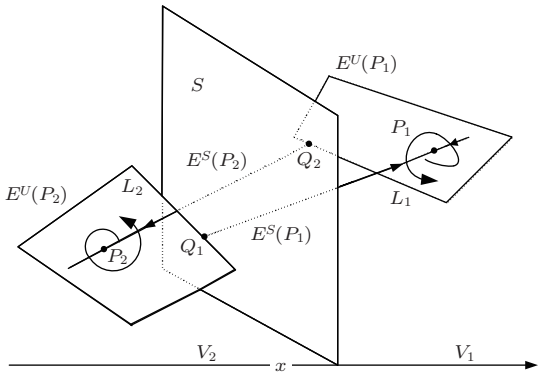

图 1 异宿轨道示意图

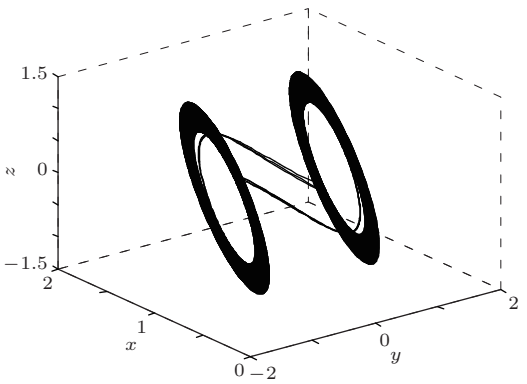

图 2 系统 (13) 的三维吸引子相图

参数$c = -1.5$时系统处于混沌状态. 图4为系统的最大Lyapunov指数, 可见系统在$c = -1.58$时进入混沌状态, 与分岔图相一致. 选取平面$S_p = \{(x, y, z)|z = 0\}$, 给出系统的Poincaré 截面如图5所示, 所有的点密集分布在两条并行的直线上, 这也证明系统处于两涡卷混沌状态.

3 多涡卷混沌吸引子设计与电路仿真

3.1 多涡卷混沌吸引子模型

与两涡卷系统设计相类似, 设计合适的控制器从而得到多涡卷混沌吸引子. 多涡卷混沌系统模型为

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix} = \begin{bmatrix}-10 & 10 & 0\\ -c & c & -T\sqrt{64-8c}\\ T\sqrt{64-8c} & T\sqrt{64-8c} & -8/3\end{bmatrix}\left[\begin{pmatrix}x\\ y\\ z\end{pmatrix} - U'\right], \tag{14}$$

其中

$$T(x, y, z) = \mathrm{sgn}(x) + \sum_{m=1}^{M}(-1)^m[\mathrm{sgn}(x + 2mx_0) + \mathrm{sgn}(x - 2mx_0)], \tag{15}$$

$$U'(x, y, z) = \begin{bmatrix} x_0\mathrm{sgn}(x) + \sum\limits_{m=1}^{M}[\mathrm{sgn}(x + 2mx_0) + \mathrm{sgn}(x - 2mx_0)]\\ y_0\mathrm{sgn}(y) + \sum\limits_{m=1}^{M}[\mathrm{sgn}(y + 2my_0) + \mathrm{sgn}(y - 2my_0)]\\ z_0\mathrm{sgn}(z) + \sum\limits_{n=1}^{N}[\mathrm{sgn}(z + 2nz_0) + \mathrm{sgn}(z - 2nz_0)]\end{bmatrix}. \tag{16}$$

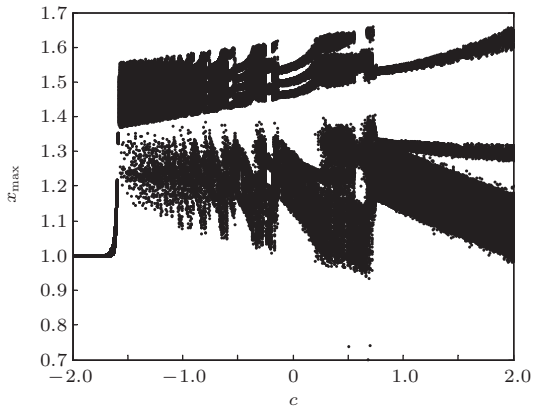

图3 系统(13)的分岔图

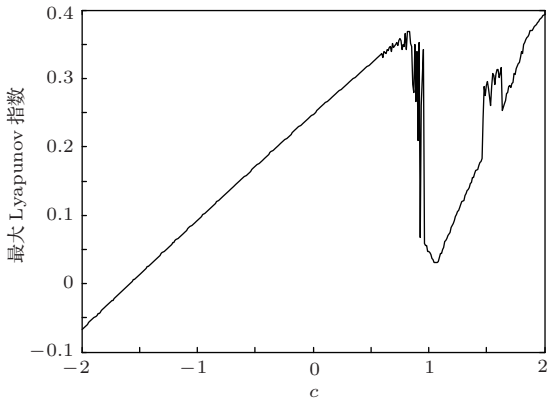

图4 系统(13)的最大Lyapunov指数

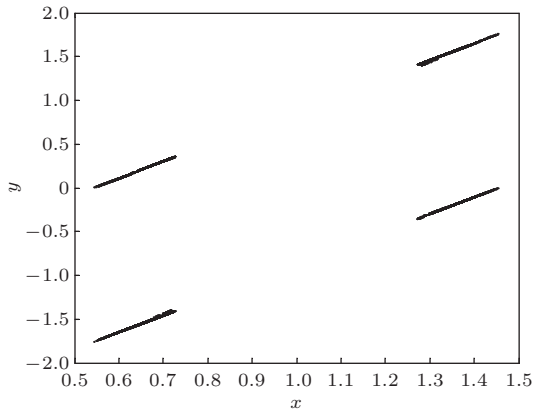

图5 系统(13)的Poincaré 截面

当$z_0 = 0$时, 系统(14)能产生$2M + 2$个涡卷, 当$z_0 \neq 0$时, 系统(14)能产生网格$(2M + 2) \times (2N + 2)$个涡卷. 初始值取(0.3, 0.1, 0.1), 步长为0.01, 当$c = -1.5$, $x_0 = 1$, $y_0 = 0.8$, $z_0 = 0$, $M = 2$, $N = 0$时, 系统(14)的吸引子相图如图6(a)所示, $M = 3$, $N = 0$时, 系统(14)的吸引子相图如图6(b)所示; 当$c = -0.55$, $x_0 = 1$, $y_0 = 0.8$, $z_0 = 1.05$, $M = 0$, $N = 1$时, 系统(14)的吸引子相图如图6(c)所示, $M = 3$, $N = 1$时, 系统(14)的吸引子相图如图6(d)所示. 可见多涡卷

吸引子相图的大小一致, 设计方法正确. 值得一提的是控制器的参数选取并不惟一, 是通过反复实验验证得到的, 并且混沌系统对控制器的参数具有敏感性.

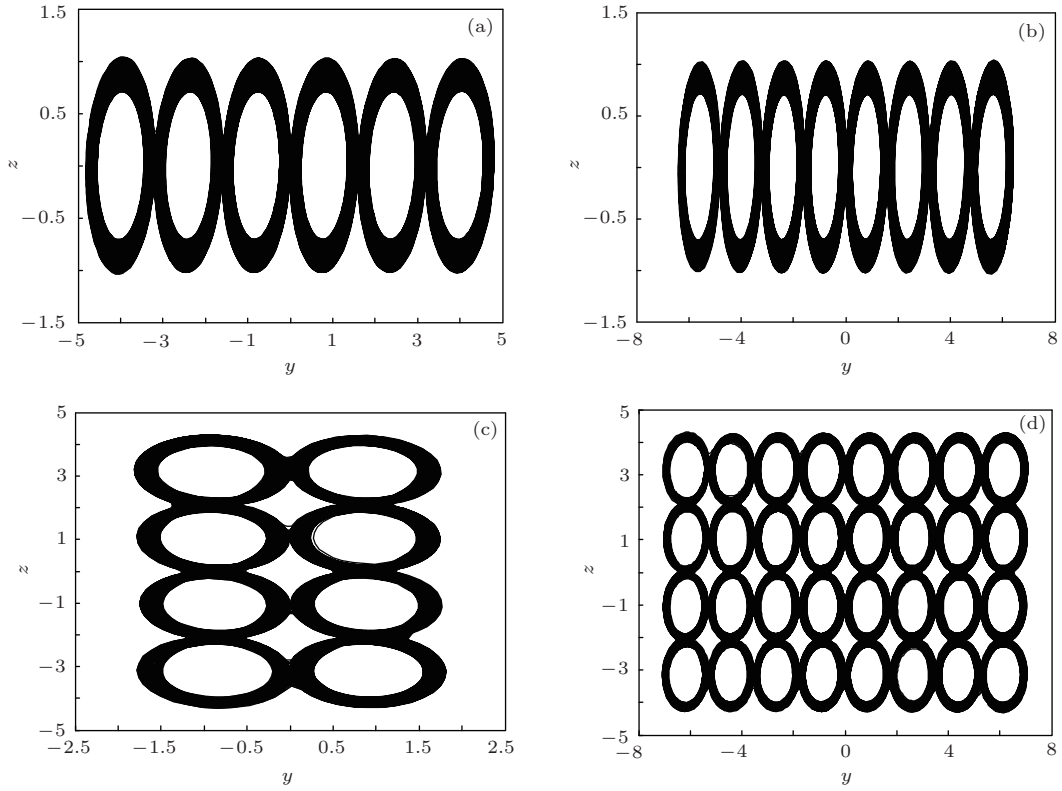

图 6 多涡卷吸引子相图 (a) 6 × 1 涡卷吸引子; (b) 8 × 1 涡卷吸引子; (c) 2 × 4 涡卷吸引子; (d) 8 × 4 涡卷吸引子

3.2 多涡卷混沌吸引子电路仿真

在 Multisim 软件中, 采用模块化方法设计了多涡卷混沌系统的电路, 根据 (14), (15), (16) 式进行电路设计. 为了防止中间变量超出运算放大器的线性动态范围, 首先将系统变量缩小 1/100, 得到系统方程为

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix}=\begin{bmatrix}-10 & 10 & 0\\ -c & c & -T'\sqrt{64-8c}\\ T'\sqrt{64-8c} & T'\sqrt{64-8c} & -8/3\end{bmatrix}\left[\begin{pmatrix}x\\ y\\ z\end{pmatrix}-\frac{U''}{100}\right], \tag{17}$$

$$T'(x,y,z)=\operatorname{sgn}(100x)+\sum_{m=1}^{M}(-1)^m[\operatorname{sgn}(100x+2mx_0)+\operatorname{sgn}(100x-2mx_0)], \tag{18}$$

$$U''(x,y,z)=\begin{bmatrix}x_0\operatorname{sgn}(100x)+\sum\limits_{m=1}^{M}[\operatorname{sgn}(100x+2mx_0)+\operatorname{sgn}(100x-2mx_0)]\\ y_0\operatorname{sgn}(100y)+\sum\limits_{m=1}^{M}[\operatorname{sgn}(100y+2my_0)+\operatorname{sgn}(100y-2my_0)]\\ z_0\operatorname{sgn}(100z)+\sum\limits_{n=1}^{N}[\operatorname{sgn}(100z+2nz_0)+\operatorname{sgn}(100z-2nz_0)]\end{bmatrix}. \tag{19}$$

根据方程得到系统的电路图如图 7 所示, 图中模块 X_1, X_2, X_3, X_4 为实现 T' 和 U'' 的电路模块. 根据图 7 可得电路状态方程为

$$\begin{cases} \dot{x} = \dfrac{1}{R_1C_1}\left[-\dfrac{R_8}{R_4}x - \dfrac{R_8}{R_5}u_2 + \dfrac{R_8}{R_6}y + \dfrac{R_8}{R_7}u_1\right], \\ \dot{y} = \dfrac{1}{R_2C_2}\left[-\dfrac{R_9}{R_{10}}\sqrt{64-8c}Tz - \dfrac{R_9}{R_{11}}y - \dfrac{R_9}{R_{12}}u_1 + \dfrac{R_9}{R_{13}}\sqrt{64-8c}Tu_3 + \dfrac{R_9}{R_{14}}y + \dfrac{R_9}{R_{15}}u_2\right], \\ \dot{z} = \dfrac{1}{R_3C_3}\left[\dfrac{R_{16}}{R_{17}}\sqrt{64-8c}T\left(x+y-\dfrac{u_1}{100}-\dfrac{u_2}{100}\right) + \dfrac{R_{16}}{R_{18}}u_3 - \dfrac{R_{16}}{R_{19}}z\right]. \end{cases} \tag{20}$$

与系统方程对比可得

$$C_1 = C_2 = C_3 = 100\ \text{nF},$$
$$R_1 = R_2 = R_3 = 1000\ \text{k}\Omega,$$
$$R_4 = R_6 = R_{11} = R_{14} = 10\ \text{k}\Omega,$$
$$R_5 = R_7 = R_{12} = R_{15} = 1000\ \text{k}\Omega,$$
$$R_8 = 10\ \text{k}\Omega, \quad R_9 = R_{10} = 0.55\ \text{k}\Omega,$$
$$R_{13} = 55\ \text{k}\Omega, \quad R_{16} = R_{17} = 0.8\ \text{k}\Omega,$$
$$R_{18} = 300\ \text{k}\Omega, \quad R_{19} = 3\ \text{k}\Omega.$$

图 8 为实现 2×4 网格多涡卷吸引子的 T' 和 U'' 电路图. 2×4 网格多涡卷吸引子电路仿真如图 9 所示, 可见, 电路仿真与数值仿真相一致. 实际中, 可修改模块 T' 和 u'' 的电路设计来控制涡卷的数目.

4 改进型多涡卷混沌-AES混合加密算法

4.1 加密算法

将混沌技术应用于加密算法中有利于提高加密系统的安全性能. 文献 [26] 将多涡卷混沌加密技术与 AES 加密技术结合在一起, 其加密原理如图 10 所示. 但该文献中对混沌序列的量化方法仅为简单地将三维数据整合然后对 256 取模, 相比于离散混沌系统, 连续混沌系统的混沌序列的随机性与复杂性并不是很好 [23], 所以直接将连续混沌系统的混沌序列简单地应用于加密中不能够充分地利用混沌系统的良好随机性能, 要得到具有良好随机性能的序列, 量化算法的设计非常重要 [24]. 在

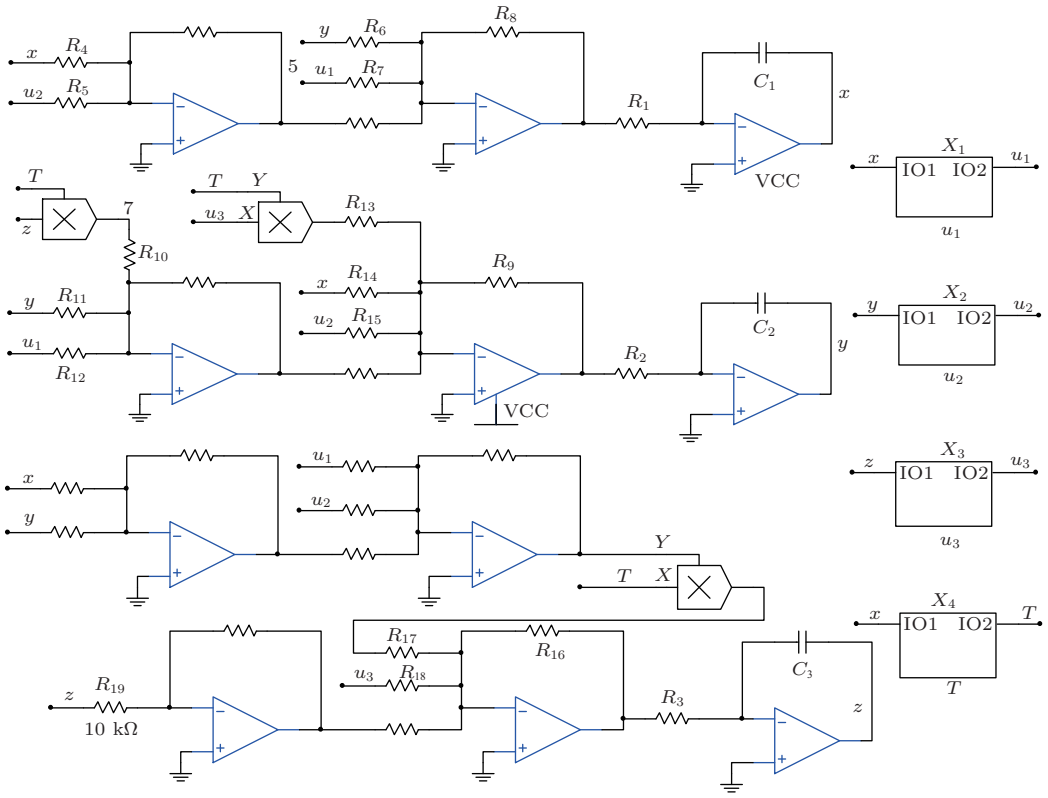

图 7 多涡卷混沌系统电路图

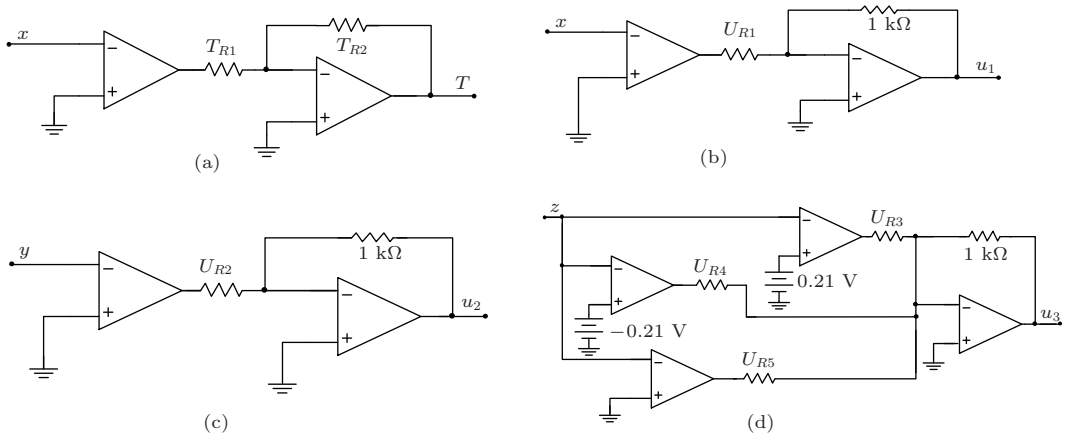

图 8 模块电路图 (a) T' 模块; (b) u_1 模块; (c) u_2 模块; (c) u_3 模块; (图中 $T_{R1} = U_{R1} = U_{R3} = U_{R4} = 14.28\ \text{k}\Omega$, $T_{R2} = 8.27\ \text{k}\Omega$, $U_{R2} = 17.85\ \text{k}\Omega$, $U_{R5} = 13.60\ \text{k}\Omega$)

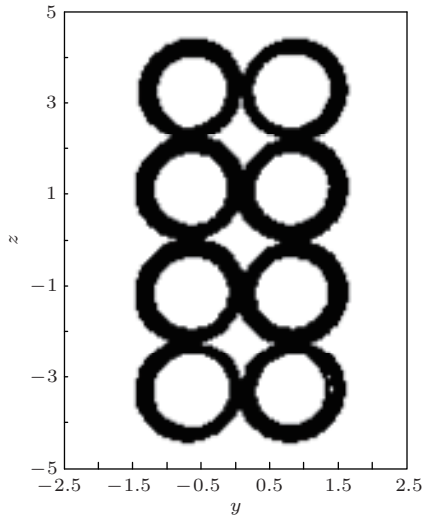

图 9 电路仿真图

此, 提出一种新的量化方法对该加密算法进行改进. 量化算法为: 首先将混沌序列 x_i 转化为IEEE-754标准的32 bit二进制序列, 记为 $\{X_i^j | j = 1, 2, \cdots, 32\}$, 因为连续混沌序列中相邻的两个数值的变化不是很大, 相关性比较强, 所以为了得到随机性良好的混沌序列, 舍去32 bit中的符号位、指数位的前4位和尾数位的后15位, 即选取第6位到第17位来生成混沌序列, 处理方法为

$$K_i^j = X_i^{j+5} \oplus X_i^{j+9} \oplus X_i^{j+13} \quad (1 \leqslant j \leqslant 4), \quad (21)$$

通过一个混沌数值可以得到4 bit二进制伪随机序列, 从而得到一串伪随机序列 K_i^j, 每8 bit一组转换成0—255的整数序列 x_j. 通过该算法, 两个混沌数值 x_i 便能得到一个数值, 原文献中需要三个混沌数值 x_i 才能得到一个数值, 所以改进量化算法对混沌序列的利用效率更高. 值得一提的是改进量化算法也能应用于混沌伪随机序列发生器, 并且该算法基于IEEE-754标准, 工程实用性好.

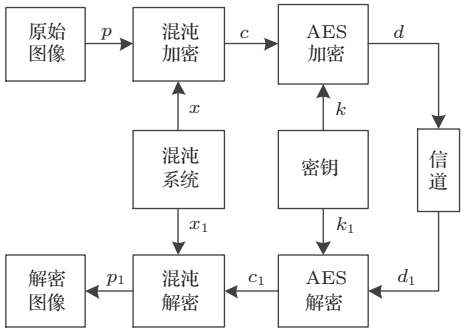

图 10 混合加密原理框图

改进混合加密主要步骤为:

1) 利用多涡卷混沌系统, 得到混沌序列 x_i, 通过改进量化算法得到0—255之间的整数序列 x_j, 由 x_j 构成的密钥对原始信息 p 进行加密, $c = p \oplus x$;

2) 利用密钥 k 对密文 c 进行AES加密得到密文 d;

3) 密文 d 经信道传输, 接收信号 d_1, $d_1 = d$;

4) 首先对 d_1 进行AES解密, 在解密密钥 k_1 下得到解密密文 c_1;

5) 密文 c_1 经混沌解密得到原始信息.

通过改进混合加密, 将明文先通过混沌加密, 由于混沌信号具有不可预测性, 之后再进行AES加密, 密文 c 和密文 d 具有惟一对应性, 但是密文 c 是原始信息 p 通过混沌加密得到, 混沌信号具有不可预测性与随机性, 所以密文 d 与信息 p 没有惟一对应性, 大大增大了加密的安全性, 克服了AES明文密文对惟一对应的缺点.

4.2 加密性能分析

混沌加密效果图如图11所示. 其中图11 (d)为初始值相差10^{-5}的解密效果图, 可见通过改进混合加密算法能够正确解密加密图像, 而且若初始值有很微小的变化都会导致解密失败, 说明该算法对密钥具有高度的敏感性, 安全性高.

加密前后图像的灰度直方图分布比较如图12所示. 可见, 加密前图像呈现出非均匀分布, 加密后密文空间呈现均匀分布, 可防止统计攻击, 安全性强. 数字图像中的相邻像素之间不是互相独立的, 相关性大, 图像加密目标之一便是减小图像相邻像素的相关性, 主要包括水平像素、垂直像素和对角像素之间的相关性, 相关性越小, 图像加密效果越好, 安全性越高. 图13为水平方向与垂直方向上原始图像和改进混合加密图像相邻像素的相关性. 可见, 原始图像像素间的相关性呈现明显的线性关系, 而改进混合加密图像像素间的相关性呈现随机的对应关系.

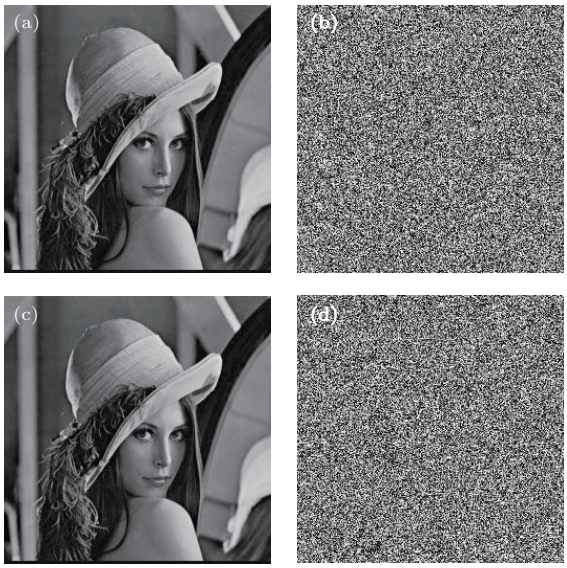

图11 改进混合加解密效果图 (a) 原图; (b) 加密后的图; (c) 正确解密图; (d) 错误解密图

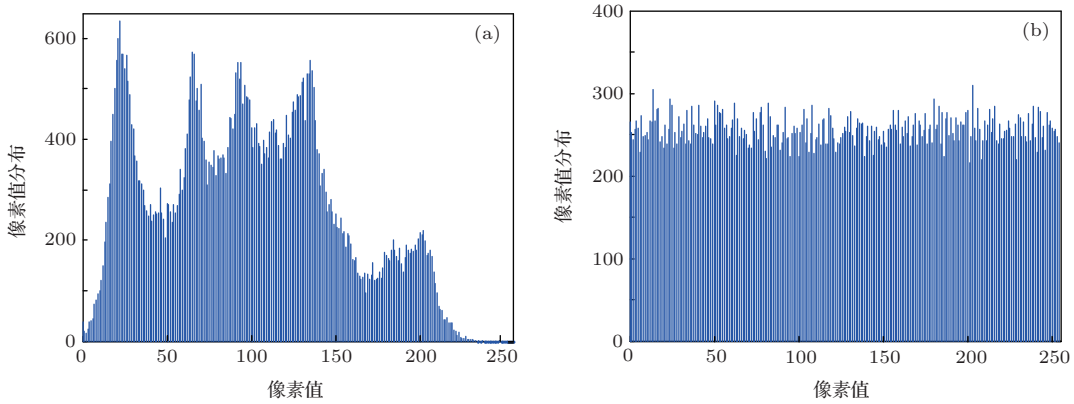

图12 直方图分布比较 (a) 原图的分布图; (b) 加密后的分布图

为了定量分析其抗统计分析能力, 计算相邻像素的相关系数ρ_{xy}, 其表达式为

$$\rho_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}, \tag{22}$$

其中

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

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

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

相关系数ρ_{xy}表征两个相邻像素之间的相关性, 相关系数越大, 相关性越强. 以网格8×4涡卷为例, 计算相邻像素之间的相关系数如表1所示, 可见改进混沌加密的水平相邻像素和垂直相邻像素的相关系数比原文献中提出的混沌加密算法计算出来的相关系数要低一个数量级, 说明通过改进之后混沌序列的随机性更好. 改进混合加密后水平相邻像素的相关系数比AES加密的低一个数量级, 比改进混沌加密的要低两个数量级, 垂直相邻像素和对角相邻像素的相关系数与AES加密和改进混沌加密的相关系数处于同一个数量级, 可见改进混合加密后的效果比单独加密要好. 表2为不同涡卷数目的改进混合加密相关性比较, 可见, 网格多涡卷混沌系统的加密效果要比单方向多涡卷混沌系统的加密效果好.

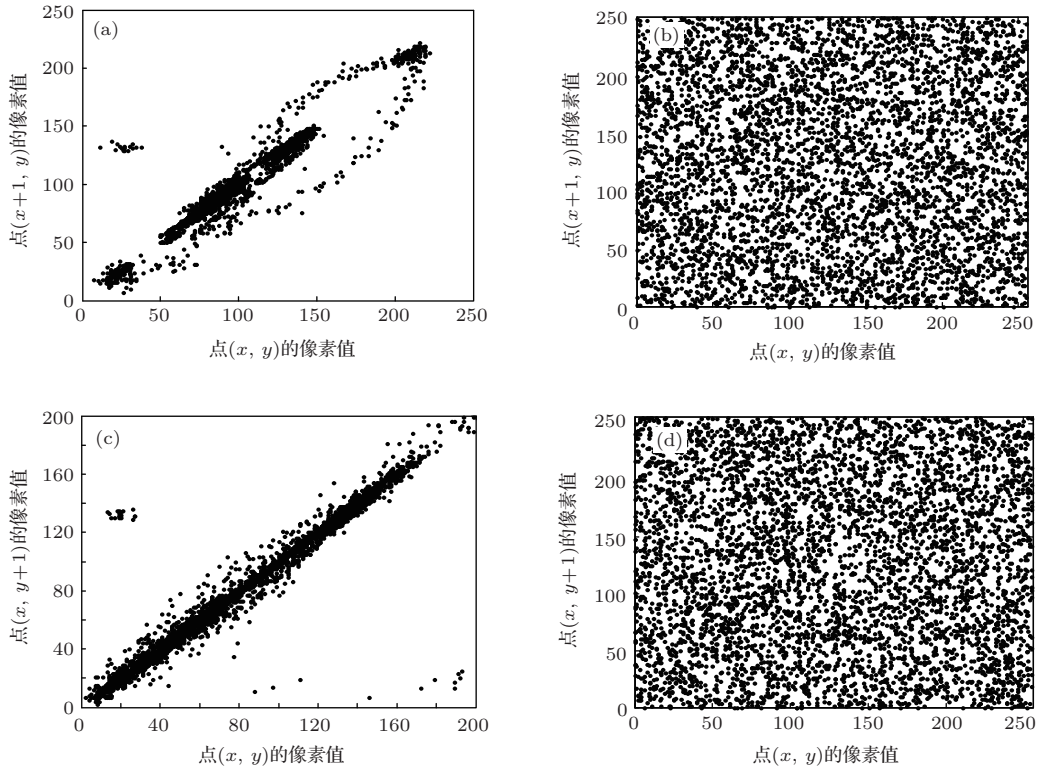

图 13 相邻像素相关性 (a) 原始图像水平方向; (b) 改进混合加密图像水平方向; (c) 原始图像垂直方向; (d) 改进混合加密图像垂直方向

表 1 相邻像素的相关性比较

像素关系	原始图	原混沌加密	改进混沌加密	AES 加密	改进混合加密
水平	0.9416	0.2100	0.0470	0.0019	−0.0004
垂直	0.9659	−0.0145	0.0034	0.0024	0.0079
对角	0.9237	−0.0072	0.0075	0.0019	0.0044

表 2 改进混合加密后的相关性比较

涡卷系统	水平相邻	垂直相邻	对角相邻
2 涡卷	0.0057	0.0061	0.0031
4 涡卷	0.0059	0.0031	−0.0022
6 涡卷	−0.0051	−0.0003	0.0028
8 涡卷	−0.0011	0.0095	0.0048
2 × 4 涡卷	0.0018	0.0016	0.0067
4 × 4 涡卷	−0.0045	0.0010	0.0005
6 × 4 涡卷	−0.0059	0.0001	0.0008
8 × 4 涡卷	0.0004	0.0079	0.0044

5 结 论

采用理论分析和仿真方法, 研究了基于简化 Lorenz 系统的多涡卷混沌吸引子设计问题, 并将其应用于混沌图像加密中. 得到如下结论: 1) 通过设计合适的控制器, 得到了多涡卷混沌吸引子; 2) 多涡卷混沌系统具有丰富的动力学行为; 3) 数值仿真与电路仿真结果一致, 表明了多涡卷吸引子设计的正确性和物理可实现性; 4) 改进的混合加密算法的加密效果比原算法和单一加密算法的加密效果好; 基于网格多涡卷混沌系统的加密效果比基于单方向多涡卷混沌系统的加密效果优.

参考文献

[1] Yu S M 2005 *Acta Phys. Sin.* **54** 1500 (in Chinese) [禹思敏 2005 物理学报 **54** 1500]

[2] Maksuanpan S, San U W 2013 *Knowledge and Smart Technology* **5** 134

[3] Zhang C X, Yu S M 2009 *Acta Phys. Sin.* **58** 120 (in Chinese) [张朝霞, 禹思敏 2009 物理学报 **58** 120]

[4] Trejo G R, Tlelo C E, Jimenez F 2012 *Commun. Nonlinear Sci. Numerical Simulat.* **17** 4328

[5] Chen L, Peng H J, Wang D S 2008 *Acta Phys. Sin.* **57** 3337 (in Chinese) [谌龙, 彭海军, 王德石 2008 物理学报 **57** 3337]
[6] Bao B C, Xu Q, Xu Y M, Wang X F 2001 *J. Circ. Syst.* **16** 69 (in Chinese) [包伯成, 徐强, 徐煜明, 汪小锋 2001 电路与系统学报 **16** 69]
[7] Mustafa T, Hidayet O 2010 *Expert Syst. Appl.* **37** 8667
[8] Yu S M, Lü J H, Chen G R 2007 *Phys. Lett. A* **364** 244
[9] Sanchez-Lopez C 2011 *Appl. Math. Computat.* **217** 4350
[10] Xu F, Yu P 2010 *Math. Anal. Appl.* **362** 252
[11] Li G L, Chen X Y 2009 *Commun. Nonlinear Sci. Numerical Simul.* **14** 194
[12] Liu C X, Yi J, Xi X C 2012 *Proced. Engineer.* **29** 957
[13] Luo X H, Tu Z W, Liu X R, Cai C, Liang Y L, Gong P 2010 *Chin. Phys. B* **19** 070510
[14] Mao W, Guang H, Li L H 2010 *Systems and Control in Aeronautics and Astoinautics 3rd International Symposium on IEEE* Harbin, China, June 8–10, 2010 p289
[15] Xi H L, Yu S M, Zhang Z X 2010 *Chaos Fractals Theories and Applictaions, 2010 International Workshop on IEEE* Kunming, China, October 29–31, 2010 p92
[16] Gui Z, Wu X, Chen Y 2013 *Int. J. Mod. Phys. B* **27** 1350007
[17] Liu X, Shen X, Zhang H 2012 *Int. J. Bifurc. Chaos Appl. Sci. Engineer.* **22** 1250033
[18] Yu S M, Lü J H, Chen G R 2011 *Circuits and Systems IEEE International Symposium on IEEE* Rio de Janeiro, Brazil, May 15–18, 2011 p1335
[19] Yu S M, Lu J H 2012 *Circ. Syst.* **59** 1015
[20] Kais B, Abdessattar C, Ahmed T 2011 *Chaos Solition. Fract.* **44** 79
[21] Lu J H, Yu X H, Chen G R 2003 *Circ. Syst.* **50** 198
[22] Zhao P T, Liu G, Wang M H, Peng J L 2012 *Biomed. Engineer. Inform.* **5** 186
[23] Sun K H, He S B, Zhu C X, He Y 2013 *Acta Elect. Sin.* **9** 1765 (in Chinese) [孙克辉, 贺少波, 朱从旭, 何毅 2013 电子学报 **9** 1765]
[24] Sheng L Y, Xiao Y Y, Sheng Z 2008 *Acta Phys. Sin.* **57** 4007 (in Chinese) [盛利元, 肖燕予, 盛喆 2008 物理学报 **57** 4007]
[25] Wang C L, Wang G Y, Sun Y, Chen W 2011 *Proceedings-4th International Workshop on Chaos-Fractals Theories and Applications* China, October 19–21, 2011 p183
[26] Lin Y, Wang C H, Xu H 2012 *Acta Phys. Sin.* **61** 73 (in Chinese) [林愿, 王春华, 徐浩 2012 物理学报 **61** 73]
[27] Sun K H, Sprott J C 2009 *Int. J. Bifurc. Chaos* **19** 1357

Design and application of multi-scroll chaotic attractors based on simplified Lorenz system*

Ai Xing-Xing[1)] Sun Ke-Hui[1)2)†] He Shao-Bo[1)] Wang Hui-Hai[1)]

1) (*School of Physics and Electronics, Central South University, Changsha 410083, China*)

2) (*School of Physics Science and Technology, Xinjiang University, Urumqi 830046, China*)

(Received 17 January 2014; revised manuscript received 28 February 2014)

Abstract

Two linear systems are obtained by employing linearization technique in a simplified Lorenz system, and a two-scroll chaotic attractor is generated via the control method. Multi-scroll chaotic attractors are generated by extending the saddle-focus equilibrium points with index 2. Dynamic characteristics of the multi-scroll chaotic system are analyzed by observing the phase diagrams, bifurcation diagrams, Poincaré sections and calculating the largest Lyapunov exponent. A circuit for the multi-scroll attractor is designed and simulated. The numerical simulation result and the circuit simulation result are consistent with each other. To apply the multi-scroll chaotic systems to image encryption, an improved hybrid encryption algorithm is designed based on the multi-scroll chaotic system and advanced encryption standard (AES), and its encryption performances are analyzed. The results show that the improved hybrid encryption has a higher security.

Keywords: chaos, multi-scroll attractor, simplified Lorenz system, image encryption

PACS: 05.45.Ac, 05.45.Gg **DOI:** 10.7498/aps.63.120511

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61161006, 61073187) and the Fundamental Research Fund for the Central Universities, China (Grant No. 72150050650).

† Corresponding author. E-mail: kehui@csu.edu.cn