

# 新型混沌系统的同步及在图像加密传输中的应用

邵书义, 闵富红, 李登辉, 黄雯迪

(南京师范大学电气与自动化工程学院, 江苏 南京 210042)

**[摘要]** 提出一个新型四维四翼混沌系统, 分析了参数变化时系统动力学行为的特性. 基于分数阶混沌系统稳定性理论, 设计合适的非线性反馈控制器, 实现了初始值不同的整数阶与其分数阶混沌系统之间的同步. 此外, 利用改进的混沌掩盖通信原理, 提出了一种新型图像加密传输方法, 并将以上同步方案应用于图像加密传输中, 在发送端使用整数阶混沌序列对图像加密传送, 从接收端可以无失真地恢复出原始图像. 数值仿真证实了新混沌系统的存在性以及同步控制应用的可行性.

**[关键词]** 混沌系统, 动力学行为, 同步控制, 图像加密传输

**[中图分类号]** TP391.9 **[文献标志码]** A **[文章编号]** 1672-1292(2015)01-0001-07

## The Synchronization for Novel Chaotic System and Its Application in Image Encryption Transmission

Shao Shuyi, Min Fuhong, Li Denghui, Huang Wendi

(School of Electrical and Automation Engineering, Nanjing Normal University, Nanjing 210042, China)

**Abstract:** In this paper, a new four-dimensional four-wing chaotic system is proposed and its dynamic properties are investigated through numerical simulations. The different dynamic behaviors of the new system are analyzed with system parameters changed. Based on the stability theory of fractional-order chaotic system, chaotic synchronization between fractional-order chaotic system and chaotic system of integer orders is successfully completed. Furthermore, the synchronization is applied to a new image encryption transmission. The image can be concealed and recovered. Numerical simulation results prove the feasibility of the proposed method of synchronization application and the existence of the new chaotic system.

**Key words:** chaotic system, dynamical behavior, synchronization control, image encryption transmission

Lorenz 从气象学的对流运动中提出第一个混沌系统后, 从上世纪半叶直到现在, 混沌理论得到了迅速的发展, 并在生物工程和保密通信等工程领域得到了广泛的应用<sup>[1-3]</sup>. 随着人们对混沌系统不断深入的研究, 研究者相继提出了 Lorenz 系统<sup>[4]</sup>、Rössler 系统<sup>[5]</sup>、Chen 系统<sup>[6]</sup>、Lü 系统<sup>[7]</sup>以及连接 Lorenz 系统、Chen 系统和 Lü 系统的统一混沌系统<sup>[8]</sup>. 此外, 近年来更多的新混沌系统不断被发现和提出, 如超混沌系统<sup>[9]</sup>、分数阶混沌系统<sup>[10]</sup>、多翼混沌系统<sup>[11]</sup>等. 新的混沌系统不断被发现和提出, 促使人们对如何利用和控制混沌系统有了更深入的研究.

自从 1990 年 Pecora L M 和 Carroll T L 发表了一篇关于混沌同步的开创性文章<sup>[12]</sup>以来, 混沌同步一直是非线性动力学领域研究的热点. 现有文献中大多数是研究整数阶混沌系统之间的同步或分数阶混沌系统之间的同步, 而对整数阶与分数阶混沌系统之间的同步研究鲜少. 由于整数阶与分数阶混沌系统之间的同步在保密通信和图像加密传输中具有更强的抗破译能力, 大大增强了信息通信安全, 因此, 研究整数阶与分数阶混沌系统之间的同步对混沌保密通信具有重要的意义. 文献[13]提出一种整数阶与分数阶系统同步的通用方法, 并运用该方法实现了整数阶 Lorenz 系统与分数阶 Lorenz 系统之间的同步. 文献[14]利用分数阶系统稳定性理论, 实现了分数阶 Chen 系统和整数阶 Lorenz 系统之间的函数投影同步. 文

收稿日期: 2014-04-16.

基金项目: 国家自然科学基金(51075215、51475246)、江苏省自然科学基金(BK20131402)、教育部留学回国人员科研启动基金(教外司[2012]1707号)、江苏省六大人才高峰资助课题

通讯联系人: 闵富红, 博士, 副教授, 研究方向: 非线性电路与系统. E-mail: minfuhong@njnu.edu.cn

献[15]利用 Lyapunov 稳定性理论和数值微分提出了一种非线性反馈控制器,并实现了分数阶统一系统与整数阶 Chen 系统之间的同步. 文献[16]基于追踪控制思想和线性分数阶系统稳定性理论研究了分数阶 Lü 系统和一种整数阶系统的同步,以及分数阶超混沌 Lorenz 系统和整数阶超混沌 Chen 系统的同步. 可见,上述文献成功实现了整数阶与分数阶混沌系统的同步,但都是在已存在混沌系统的基础上进行分析.

由于混沌信号自身的初值敏感、非周期、类噪声等特性,使得混沌同步的研究为保密通信方案提供了信号隐藏和恢复的可行手段. 文献[17]利用改进的混沌掩盖通信原理将两个同结构 Qi 混沌系统错位投影同步应用于保密通信. 文献[18]在混沌保密通信系统中应用了两个统一混沌系统的自适应投影同步. 而文献[19]研究了两个不同整数阶时延系统的同步在图像加密中的应用,实现了图像的加密与解密. 由于对混沌同步在图像加密传输中的应用研究鲜少,且整数阶与分数阶混沌系统之间的同步在图像加密传输中的应用比整数阶混沌系统之间的同步在图像加密中的应用具有更强的抗破译能力. 因此,本文提出一个新型四翼四维混沌系统,并开展整数阶四翼混沌系统与其分数阶混沌系统之间的同步研究及在图像加密传输中的应用,具有重要的意义.

本文构建了一个新型四维四翼混沌系统,通过分析系统平衡点的稳定性、分岔图和 Lyapunov 指数谱,验证新系统的混沌特性. 利用分数阶混沌系统稳定性理论,设计同步方案,实现初始值不同的整数阶与分数阶混沌系统之间的同步. 然后,提出一种新型图像加密传输方案,并将以上同步应用于该图像加密传输方案,证实了同步方案在图像加密传输中的有效性.

## 1 新型混沌系统的基本分析

### 1.1 数学模型

本文提出的新型四维四翼混沌系统的数学模型为:

$$\begin{cases} dx(t)/dt = -ax(t) + 20y(t)z(t) - w(t), \\ dy(t)/dt = by(t) - 30x(t)z(t), \\ dz(t)/dt = -cz(t) + 40x(t)y(t), \\ dw(t)/dt = -5w(t) - 5x(t)y(t) - 20x(t)z(t). \end{cases} \quad (1)$$

其中,  $a$ 、 $b$  和  $c$  为实常数. 当  $a=30$ 、 $b=5$  和  $c=15$  时,系统存在一个典型的混沌吸引子,如图 1 所示.

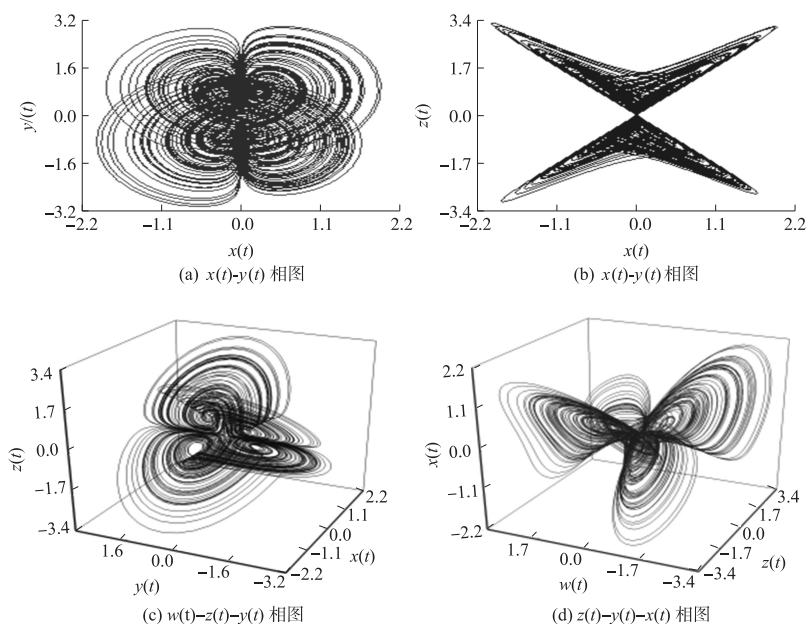


图 1 新系统的混沌吸引子

Fig. 1 The chaotic attractors of the new system

### 1.2 动力学特性分析

在给定参数情况下,可以通过分析系统平衡点的稳定性来判断系统是否满足混沌动力学行为存在的条件. 为了分析系统(1)平衡点的稳定性,令系统(1)方程的右边等于零,即

$$\begin{cases} -ax(t)+20y(t)z(t)-w(t)=0, \\ by(t)-30x(t)z(t)=0, \\ -cz(t)+40x(t)y(t)=0, \\ -5w(t)-5x(t)y(t)-20x(t)z(t)=0. \end{cases} \quad (2)$$

当参数  $a=30$ 、 $b=5$ 、 $c=15$  时,求解方程(2),得到系统的 5 个平衡点,分别为  $P_0(0,0,0,0)$ 、 $P_1(-0.25,-0.734\ 5,0.489\ 7,0.306\ 1)$ 、 $P_2(-0.25,0.765\ 8,-0.510\ 5,-0.319\ 1)$ 、 $P_3(0.25,0.716\ 4,0.477\ 6,-0.656\ 7)$  和  $P_4(0.25,-0.785\ 2,-0.523\ 4,0.719\ 7)$ 。

在平衡点  $P_0(0,0,0,0)$  处,将系统(1)线性化得到 Jacobi 矩阵  $J_0$  为

$$J_0 = \begin{bmatrix} -a & 20z(t) & 20y(t) & -1 \\ -30z(t) & b & -30x(t) & 0 \\ 40y(t) & 40x(t) & -c & 0 \\ -20z(t)-5y(t) & -5x(t) & -20x(t) & -5 \end{bmatrix} = \begin{bmatrix} -30 & 0 & 0 & -1 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & -15 & 0 \\ 0 & 0 & 0 & -5 \end{bmatrix}, \quad (3)$$

其特征方程为

$$|\lambda I - J_0| = 0. \quad (4)$$

解得式(4)的特征值为  $\lambda_1=-30$ 、 $\lambda_2=5$ 、 $\lambda_3=-15$ 、 $\lambda_4=-5$ 。由于特征值  $\lambda_1$ 、 $\lambda_3$ 、 $\lambda_4$  为负实数,而  $\lambda_2$  为正实数,因此平衡点  $P_0(0,0,0,0)$  是一个不稳定的鞍点。在平衡点  $P_1$ 、 $P_2$ 、 $P_3$  和  $P_4$  处,采用同样的方法求得平衡点  $P_1$  对应的特征值为  $\lambda'_1=2.182\ 2+13.677\ 8i$ 、 $\lambda'_2=2.182\ 2-13.677\ 8i$ 、 $\lambda'_3=-44.161\ 4$ 、 $\lambda'_4=-5.203$ ,平衡点  $P_2$  对应的特征值为  $\lambda''_1=2.364\ 5+14.390\ 7i$ 、 $\lambda''_2=2.364\ 5-14.390\ 7i$ 、 $\lambda''_3=-44.918\ 7$ 、 $\lambda''_4=-4.810\ 4$ ,平衡点  $P_3$  对应的特征值为  $\lambda'''_1=2.081\ 2+13.413\ 5i$ 、 $\lambda'''_2=-43.835\ 1$ 、 $\lambda'''_3=2.081\ 2-13.413\ 5i$ 、 $\lambda'''_4=-5.327\ 4$ ,平衡点  $P_4$  对应的特征值为  $\lambda''''_1=-45.272\ 9$ 、 $\lambda''''_2=2.489\ 7+14.667\ 0i$ 、 $\lambda''''_3=2.489\ 7-14.667\ 0i$ 、 $\lambda''''_4=-4.706\ 5$ 。其中, $\lambda'_1$ 、 $\lambda'_2$ 、 $\lambda''_1$ 、 $\lambda''_2$ 、 $\lambda'''_1$ 、 $\lambda'''_2$ 、 $\lambda''''_2$ 、 $\lambda''''_3$  为正实部的共轭复根,其余的特征值为负实数。因此,平衡点  $P_1$ 、 $P_2$ 、 $P_3$  和  $P_4$  为不稳定的鞍焦点。根据上述分析的平衡点稳定性可知,系统(1)的 5 个平衡点都是不稳定的,满足该系统存在混沌特性的条件。

随着四维四翼系统参数的改变,系统平衡点的稳定性将会发生变化,从而系统会处于不同的运动状态。通过对 Lyapunov 指数谱(LE 谱)和分岔图的分析,可直观地表明系统随参数变化时,系统运动状态的变化情况。以下只讨论系统随参数  $b$  变化时的动力学行为。

固定参数  $a=30$  和  $c=15$ ,改变参数  $b$ ,使  $b \in (0,18)$ 。当  $b \in (0,18)$  变化时,系统关于  $y(t)$  的分岔以及系统的 LE 谱如图 2 所示,其中图 2(a)是状态变量  $y(t)$  随参数  $b$  变化的分岔图,图 2(b)是系统随参数  $b$  变化的 LE 谱。从图 2 可清晰地看出,当  $b \in (0.4,10)$  和  $b \in (12.2,4.6)$  时,系统处于混沌运动状态,此时系统的最大 LE 大于零。对于  $b \in (0,0.32)$  和  $b \in (14.87,18)$ ,此时系统处于周期运动状态;当  $a \geq 18$  时,系统将趋于稳定点,此时系统的最大 LE 小于零。根据如图 3 所示的 2 个局部放大分岔图可知,系统(1)在  $b=10.33$  和  $b=11.72$  附近出现倍周期分岔(PDB);在图 3(b)中,在  $b=13.96$  和  $b=15.06$  附近出现倍周期分岔。

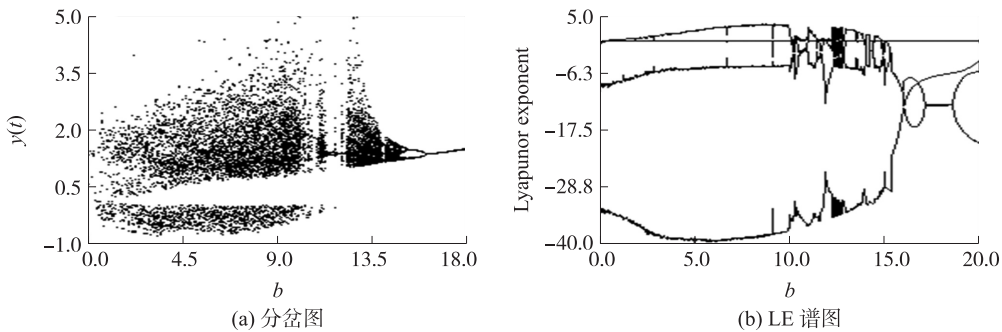


图 2 系统的分岔图与 LE 谱图

Fig. 2 The bifurcation diagram and Lyapunov exponent spectrum of the new system

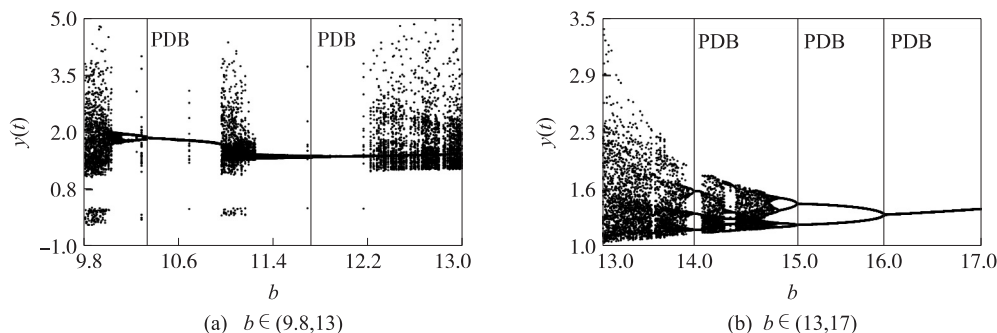


图 3 系统的局部分岔图

 Fig. 3 The bifurcation diagram for  $b \in (9.8, 13)$  and  $b \in (13, 17)$ 

## 2 整数阶与分数阶混沌的非线性反馈同步

以下将设计合适的非线性控制器,研究整数阶四翼混沌系统与分数阶四翼混沌系统的同步及应用.以系统(1)作为驱动系统,响应系统设为:

$$\begin{cases} {}_0D_t^\alpha y_1(t) = -ay_1(t) + 20y_2(t)y_3(t) - y_4(t) + u_1(t), \\ {}_0D_t^\alpha y_2(t) = by_2(t) - 30y_1(t)y_3(t) + u_2(t), \\ {}_0D_t^\alpha y_3(t) = -cy_3(t) + 40y_1(t)y_2(t) + u_3(t), \\ {}_0D_t^\alpha y_4(t) = -5y_4(t) - 5y_1(t)y_2(t) - 20y_1(t)y_3(t) + u_4(t). \end{cases} \quad (5)$$

其中,  $u_1(t)$ 、 $u_2(t)$ 、 $u_3(t)$ 、 $u_4(t)$  为控制器. 定义同步误差为

$$\begin{cases} e_1(t) = y_1(t) - x_1(t), \\ e_2(t) = y_2(t) - x_2(t), \\ e_3(t) = y_3(t) - x_3(t), \\ e_4(t) = y_4(t) - x_4(t). \end{cases} \quad (6)$$

设计的控制器  $u_1(t)$ 、 $u_2(t)$ 、 $u_3(t)$ 、 $u_4(t)$  为

$$\begin{cases} u_1(t) = {}_0D_t^{-(1-\alpha)}(- (a+10)y_1(t) + 20x_2(t)x_3(t) - y_4(t) + 10x_1(t)) + ay_1(t) - 20y_2(t)y_3(t) + y_4(t), \\ u_2(t) = {}_0D_t^{-(1-\alpha)}(- (b-10)y_2(t) - 30x_1(t)x_3(t) + 10x_2(t)) - by_2(t) + 30y_1(t)y_3(t), \\ u_3(t) = {}_0D_t^{-(1-\alpha)}(- (c+10)y_3(t) + 40x_1(t)x_2(t) + 10x_3(t)) + cy_3(t) - 40y_1(t)y_2(t), \\ u_4(t) = {}_0D_t^{-(1-\alpha)}(- (5+10)y_4(t) - 5x_1(t)x_2(t) - 20x_1(t)x_3(t) + 10x_4(t)) + 5y_4(t) + 5y_1(t)y_2(t) + 20y_1(t)y_3(t). \end{cases} \quad (7)$$

则误差系统可表示为

$$\dot{\mathbf{e}} = \mathbf{Q} \times [e_1, e_2, e_3, e_4]^T = \begin{bmatrix} -(a+10) & 0 & 0 & -1 \\ 0 & (b-10) & 0 & 0 \\ 0 & 0 & -(c+10) & 0 \\ 0 & 0 & 0 & -(5+10) \end{bmatrix} \times \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix}. \quad (8)$$

当参数  $a=30$ 、 $b=5$  和  $c=15$  时,分数阶响应系统(5)存在四翼混沌运动特性. 根据误差系统方程(8)可得,矩阵  $\mathbf{Q}$  的特征值分别为  $\lambda_1=-40$ 、 $\lambda_2=-5$ 、 $\lambda_3=-25$ 、 $\lambda_4=-15$ ,均满足  $\lambda_m < 0$  ( $m=1, 2, 3, 4$ ),即误差系统(8)将趋于稳定,对于整数阶混沌系统(1)与分数阶混沌系统(5)将实现同步.

以  $\alpha=0.91$ ,  $1-\alpha=0.09$  为例,利用数值仿真分析整数阶与分数阶四翼混沌系统的同步. 令  $[x_1(0), x_2(0), x_3(0), x_4(0)]^T = [15, 5, 7, 3]^T$  为系统初始值,响应系统初始值为  $[y_1(0), y_2(0), y_3(0), y_4(0)]^T = [-17, -18, -13, 11.5]^T$ . 仿真结果如图 4 和图 5 所示,图 4 表示驱动系统和响应系统的状态向量时序图,图 5 表示同步的误差响应曲线. 可见,驱动系统与响应系统的演化趋于一致,且同步误差在 1 s 左右收敛于 0,从而实现了整数阶与分数阶四翼混沌系统的同步.



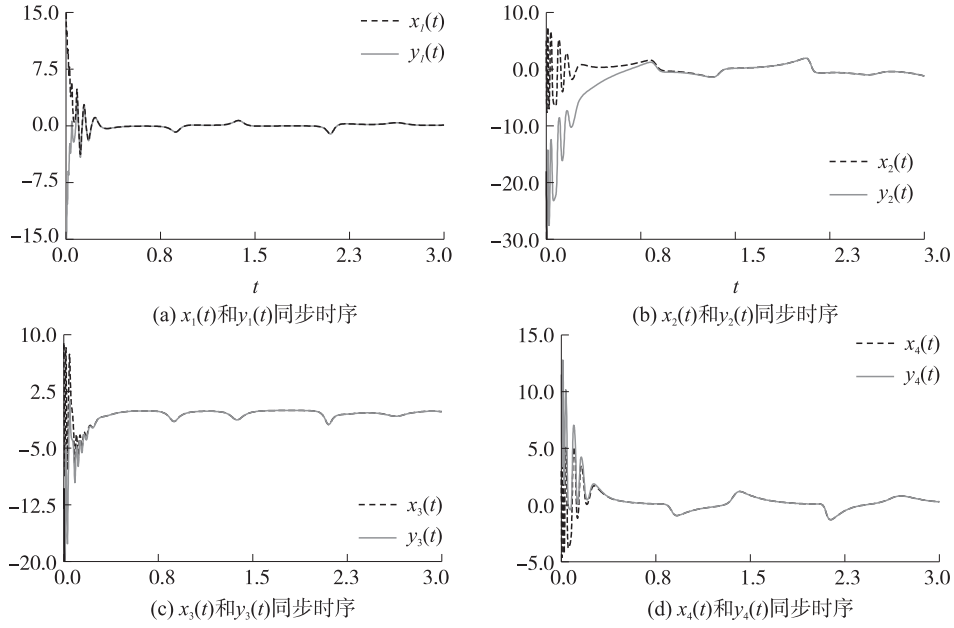


图4 同步时序图

Fig. 4 The time-histories of synchronization

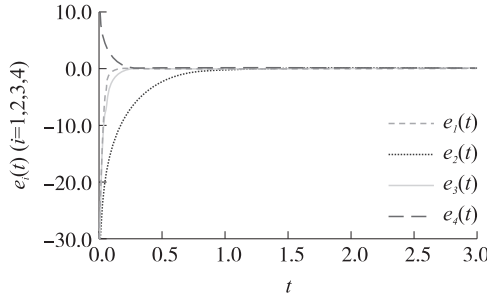


图5 同步误差响应曲线

Fig. 5 The error curves of synchronization

### 3 同步在图像加密传输中的应用

混沌信号的非周期性、类噪声、长期不可预见性及对初始条件的极端敏感性,使其在保密通信领域显示出卓越的优越性. 混沌同步的实现,保证了混沌保密通信的实时性,因此混沌同步在保密通信及信息安全等领域具有很高的实用价值. 在以往文献中,大多数是将整数阶系统的同步应用到图像加密中,对整数阶与分数阶系统同步在图像加密中的应用研究很少,然而将整数阶与分数阶混沌系统的同步应用到保密通信中,具有更强的抗破译能力.

本文结合像素值置换和像素位置置乱两种加密方法以及整数阶与分数阶四翼混沌系统的同步,提出一种新的图像加密传输方案,如图6所示. 该方案能够实现数字图像在发送端的完全加密与接受端的无失真解密,从而达到数字图像保密传输功能. 这里以大小为  $M \times N$  ( $M$  为图像的行像素数,  $N$  为图像的列像素数) 的图像作为加密传输与解密测试图像,如图7(a)所示. 从驱动系统产生的4组混沌序列中,取每组一部分序列组成长度为  $M \times N$  的序列,结合图像像素值置换和像素位置置乱两种加密方法(两种加密算法所取的序列段不同)实现对图像的加密,如图7(c)所示. 最后,取响应系统产生的4组混沌序列中每组一部分序列(序列段同加密步骤所取的序列段)组成长度为  $M \times N$  的序列,并利用像素值逆置换和像素位置逆置乱两种解密算法完成加密图像的解密,如图7(e)所示.

接着,对原始图像、加密后的图像及解密后的图像分别绘制直方图,如图7(b)、(d)和(f)所示. 可见,加密后图像直方图上的像素值分布均匀,已完全没有原始图像的统计特征,而解密后图像直方图上的像素值分布已恢复到原始图像的统计特征. 该图像加密传输方案有效地完成了数字图像的传输加密,且在解

密端不失真地恢复,说明整数阶四翼混沌系统与分数阶四翼混沌系统同步方案的有效性.

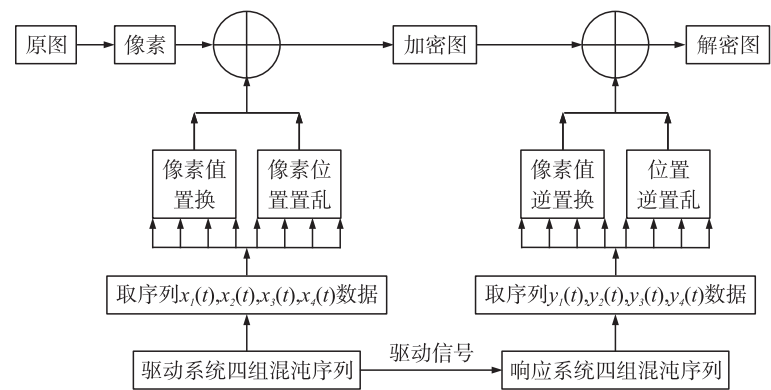


图 6 新型图像加密传输与解密方案

Fig. 6 The method of a new image encryption transmission

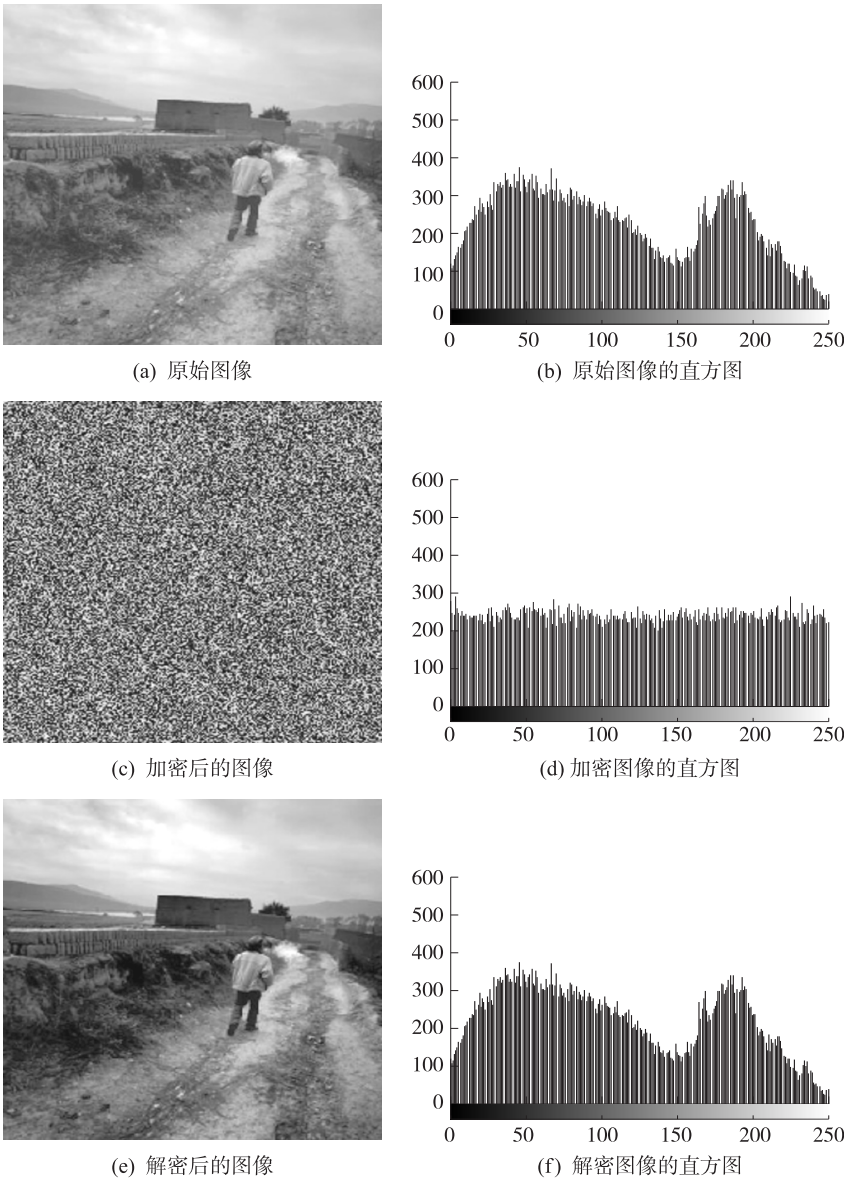


图 7 加密与解密图

Fig. 7 The figures of encryption and decode

## 4 结论

本文提出了一个新型四翼四维混沌系统,重点分析了系统的动力学行为,验证了系统丰富的混沌特性. 另外,构造合适的控制器,实现了整数阶四翼混沌系统与分数阶四翼混沌系统的同步. 最后,提出新型图像加密传输方案,并将新型混沌系统的同步应用到图像加密传输中,该方案实现了很好的效果,表明同步方案在图像加密传输中的有效性和可行性. 这为进一步研究不同维混沌系统以及不同阶次的分数阶混沌系统的同步控制及其在保密通信中的应用打下了基础.

### [参考文献](References)

- [1] Jovic B. Synchronization Techniques for Chaotic Communication Systems[M]. Berlin:Springer-Verlag, 2011:135-168.
- [2] 刘锋,陈小钊,穆肇骊,等. 混沌系统的反馈同步及其在保密通讯中的应用[J]. 电子学报,2000,28(8):46-48.  
Liu Feng, Chen Xiaozhao, Mu Zhaoli, et al. Feedback synchronization of chaotic system with application to secure communications[J]. Acta Electronica Sinica, 2000, 28(8):46-48. (in Chinese).
- [3] 邵书义, 闵富红, 马美玲, 等. 分数阶 Chua's 系统错位同步无感模块化电路实现及应用[J]. 物理学报, 2013, 62(13):130504.  
Shao Shuyi, Min Fuhong, Ma Meiling, et al. Non-inductive modular circuit of dislocated synchronization of fractional-order Chua's system and its application[J]. Acta Phys Sin, 2013, 62(13):130504. (in Chinese).
- [4] Lorenz E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(5):130-141.
- [5] Rössler O E. An equation for continuous chaos[J]. Physics Letters A, 1976, 57(5):397-398.
- [6] Chen G R, Ueta T. Yet another chaotic attractor[J]. International Journal of Bifurcation and Chaos, 1999, 9(7):1 465-1 466.
- [7] Lü J H, Chen G R. A new chaotic attractor coined[J]. International Journal of Bifurcation and Chaos, 2002, 3(12):659-661.
- [8] Lü J H, Chen G R, Cheng D Z, et al. Bridge the gap between the Lorenz system and the Chen system[J]. International Journal of Bifurcation and Chaos, 2002, 12(12):2 917-2 926.
- [9] 唐良瑞, 李静, 樊冰. 一个新四维自治超混沌系统及其电路实现[J]. 物理学报, 2009, 58(3):1 446-1 455.  
Tang Liangrui, Li Jing, Fan Bing. A new four-dimensional hyperchaotic system and its circuit simulation[J]. Acta Phys Sin, 2009, 58(3):1 446-1 455. (in Chinese).
- [10] Lu J G, Chen G R. A note on the fractional-order Chen system[J]. Chaos, Solitons and Fractals, 2006, 27(2006):685-688.
- [11] 罗明伟, 罗小华, 李华春. 一类四维多翼混沌系统及其电路实现[J]. 物理学报, 2013, 62(2):020512.  
Luo Mingwei, Luo Xiaohua, Li Huachun. A family of four-dimensional multi-wing chaotic system and its circuit implementation[J]. Acta Phys Sin, 2013, 62(2):020512. (in Chinese)
- [12] Pecora L M, Carroll T L. Synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(8):821-824.
- [13] Si G Q, Sun Z Y. A general method for synchronizing an integer-order chaotic system and a fractional-order chaotic system[J]. Chin Phys B, 2011, 20(8):080505.
- [14] Zhou P, Cao Y X. Function projective synchronization between fractional-order chaotic systems and integer-order chaotic systems[J]. Chin Phys B, 2010, 19(10):100507.
- [15] Jia L X, Dai H, Hui M. Nonlinear feedback synchronization control between fractional-order and integer-order chaotic systems[J]. Chin Phys B, 2010, 19(11):100509.
- [16] Yang L X, He W S, Liu X J. Synchronization between a fractional-order system and an integer order system[J]. Computers and Mathematics with Applications, 2011, 62(2011):4 708-4 716.
- [17] 闵富红, 王恩荣. 超混沌 Qi 系统的错位投影同步及其在保密通信中的应用[J]. 物理学报, 2010, 59(11):7 657-7 662.  
Min Fuhong, Wang Enrong. Dislocated projective synchronization of Qi hyper-chaotic system and its application to secure communication[J]. Acta Phys Sin, 2010, 59(11):7 657-7 662. (in Chinese).
- [18] Hu M F, Xu Z Y. Adaptive projective synchronization of unified chaotic systems and its application to secure communication[J]. Chinese Physics, 2007, 16(11):3 231-3 237.
- [19] Banerjee S, Ghosh D, Ray A, et al. Synchronization between two different time-delayed systems and image encryption[J]. A Letters Journal Exploring the Frontiers of Physics, 2008, 81(2):20006.

[责任编辑:严海琳]