

文章编号: 1001-9081(2013)04-1043-04

doi: 10.3724/SP.J.1087.2013.01043

基于分数阶陈氏混沌系统的图像加密算法

王雅庆^{1*}, 周尚波^{1,2}

(1. 重庆大学 计算机学院, 重庆 400044; 2. 重庆市计算机网络与通信技术重点实验室, 重庆 400030)

(* 通信作者电子邮箱 wangyaqing@cqu.edu.cn)

摘要: 由于分数阶混沌动力学系统比整数阶系统具有更复杂的动力学特性, 且能为图像加密方案提供更多的自由度, 基于分数阶陈氏混沌系统, 提出了一种图像加密方法。在发送端, 驱动系统产生混沌信号, 利用混沌信号扰乱明文图像的像素位置, 将扰乱后的图像掩盖在混沌信号中, 得到传输的密文图像。在接收端, 通过同步系统去掩盖, 进行像素位置扰乱的逆操作, 恢复明文图像。最后对提出的加密算法进行了安全性分析。实验结果表明, 该加密算法安全性高, 具有良好的研究价值和应用前景。

关键词: 分数阶陈氏系统; 混沌; 同步; 图像加密; 安全性

中图分类号: TP309; TP391.41 **文献标志码:**A

Image encryption algorithm based on fractional-order Chen chaotic system

WANG Yaqing^{1*}, ZHOU Shangbo^{1,2}

(1. Department of Computer Science, Chongqing University, Chongqing 400044, China;

2. Chongqing Key Laboratory of Computer Network and Communication Technology, Chongqing 400030, China)

Abstract: In this paper, a new image encryption algorithm was presented based on the fractional-order Chen chaotic system, for fractional-order chaotic dynamical systems have more complex dynamical behaviors than those of integer-order systems and can provide more freedom for image encryption schemes. In the transmitter, the positions of the image pixels were scrambled by the chaotic signal generated by the driving system firstly. Then the disturbed image was embedded into the chaotic signal and the encrypted image for transmission was obtained. In the receiver, the chaotic signal was removed by the synchronization system. Then the inverse process of pixel scrambling was carried out and the original image was recovered. The security of the proposed algorithm was analyzed in the end. The experimental results demonstrate that the encryption algorithm is of high security and has good research value and application prospects.

Key words: fractional-order Chen's chaotic system; chaos; synchronization; image encryption; security

0 引言

自1990年Pecora和Carroll^[1]提出混沌同步理论以来, 混沌同步引起了人们的极大关注。近年来, 将混沌同步应用于保密通信逐渐成为一个研究热点^[2-7]。研究表明, 低维混沌系统存在密钥空间小、安全性不高的缺陷, 而高维混沌系统具有更高的复杂性、随机性和不可预测性, 能更好地抵抗相空间重构等破译方法的攻击^[8]。因此, 高维混沌系统在保密通信中具有更广阔的应用前景。

陈氏系统是一个三维的混沌系统, 比Lorenz吸引子具有复杂的拓扑结构, 对保密通信有更好的隐蔽性。其同步问题也备受研究者的关注^[9-10]。随着人们对分数阶混沌系统的深入研究, 已构造分数阶陈氏系统及其混沌同步系统^[11-13]。分数阶混沌动力学系统比整数阶系统具有更为复杂、丰富的动力学特性, 以及具有随机性和不可预测性增加的优点; 而且, 分数阶系统还能为加密系统提供更多的密钥参数, 增大密钥空间, 从而提高系统的安全性。因此, 将分数阶陈氏系统应用于保密通信极具研究价值。

目前, 基于混沌同步的保密通信系统主要用于加密正弦信号、余弦信号、简单的混合信号以及文本信息^[2-5, 14-15]。由于图像信号和一般信号有很多不同, 如数据量大, 相邻像素相关性强, 将混沌同步应用于图像加密的研究还比较

少^[16-18], 而且往往缺乏安全性分析^[16-17]。文献[18]提出了一种双通道的图像保密通信方案, 然而双通道增加了系统开销。本文采用单通道保密通信方案, 将分数阶陈氏混沌系统应用于图像加密, 并分析了加密算法的安全性。

1 分数阶陈氏混沌系统

1.1 分数阶陈氏系统

分数阶陈氏系统的数学模型^[11]如下:

$$\begin{cases} \frac{d^\alpha x}{dt^\alpha} = a(y - x) \\ \frac{d^\beta y}{dt^\beta} = (c - a)x - xz + cy \\ \frac{d^\gamma z}{dt^\gamma} = xy - bz \end{cases} \quad (1)$$

其中: $(x, y, z) \in \mathbb{R}^3$ 为系统的状态; $a > 0, b > 0, c > 0$ 为系统的参数; α, β, γ 为分数阶数。该模型可用分数阶微积分的Grunwald-Letnikov定义进行数值求解。

分数阶微积分的Grunwald-Letnikov定义^[19]为:

$${}_a D_t^\nu f(x) = \lim_{h \rightarrow 0} \frac{1}{h^\nu} \sum_{j=0}^{\lfloor (t-a)/h \rfloor} (-1)^j \frac{\Gamma(\nu+1)}{j! \Gamma(\nu-j+1)} f(x-jh); \nu > 0 \quad (2)$$

收稿日期: 2012-09-04; 修回日期: 2012-10-29。

基金项目: 国家自然科学基金资助项目(60873200, 61174025); 中央高校基本科研业务费资助项目(CDJXS10181132)。

作者简介: 王雅庆(1987-), 女, 湖北天门人, 硕士研究生, 主要研究方向: 图像处理、信息安全; 周尚波(1963-), 男, 广西宁明人, 教授, 博士, 主要研究方向: 混沌及其控制、图像处理、信息安全、物理工程计算、计算机仿真。

其中: a 和 t 分别为积分的下限和上限, v 为分数阶数, h 是积分时间步长,符号 $[x]$ 表示取出变量 x 的整数部分。其数学表达式如式(3)所示:

$${}_a D_t^\alpha f(t) = \lim_{h \rightarrow 0} h^{-\alpha} \sum_{j=0}^{[(t-a)/h]} (-1)^j \binom{\alpha}{j} f(t-jh) \quad (3)$$

其中: $\binom{\alpha}{j} = \frac{\alpha(\alpha-1)\cdots(\alpha-j+1)}{j!}$ 。

化简式(3)可得式(4):

$${}_0 D_t^\alpha y(t_m) = h^{-\alpha} \sum_{j=0}^m \omega_j^{(\alpha)} y_{m-j} \quad (4)$$

其中: $\omega_j^{(\alpha)} = (-1)^j \binom{\alpha}{j}; j = 0, 1, 2, \dots$ 。

根据式(4),式(1)可转化为:

$$\begin{cases} h^{-\alpha} \sum_{j=0}^m \omega_j^{(\alpha)} x_{m-j} = a(y_m - x_m) \\ h^{-\beta} \sum_{j=0}^m \omega_j^{(\beta)} y_{m-j} = (c-a)x_m - x_m z_m + cy_m \\ h^{-\gamma} \sum_{j=0}^m \omega_j^{(\gamma)} z_{m-j} = x_m y_m - bz_m \end{cases} \quad (5)$$

简化式(5)得:

$$\begin{cases} x_m = (ah^\alpha y_m - \sum_{j=1}^m \omega_j^{(\alpha)} x_{m-j}) / (1 + ah^\alpha) \\ y_m = (h^\beta(c - a - z_m)x_m - \sum_{j=1}^m \omega_j^{(\beta)} y_{m-j}) / (1 - ch^\beta) \\ z_m = (h^\gamma x_m y_m - \sum_{j=1}^m \omega_j^{(\gamma)} z_{m-j}) / (1 + bh^\gamma) \end{cases} \quad (6)$$

其中: x_m, y_m, z_m 是隐含显示的。利用迭代算法将它们显含表示为:

$$\begin{cases} x_m^{(l)} = (ah^\alpha y_m^{(l-1)} - \sum_{j=1}^m \omega_j^{(\alpha)} x_{m-j}^{(l-1)}) / (1 + ah^\alpha) \\ y_m^{(l)} = (h^\beta(c - a - z_m^{(l-1)})x_m^{(l-1)} - \sum_{j=1}^m \omega_j^{(\beta)} y_{m-j}^{(l-1)}) / (1 - ch^\beta) \\ z_m^{(l)} = (h^\gamma x_m^{(l-1)} y_m^{(l-1)} - \sum_{j=1}^m \omega_j^{(\gamma)} z_{m-j}^{(l-1)}) / (1 + bh^\gamma) \end{cases} \quad (7)$$

其中: l 表示迭代次数,当 $|x_m^{(l)} - x_m^{(l-1)}| < \delta, |y_m^{(l)} - y_m^{(l-1)}| < \delta, |z_m^{(l)} - z_m^{(l-1)}| < \delta$ (δ 很小,例如 $\delta = 10^{-5}$),就可以认为: $x_m^{(l)} = x_m^{(l-1)}, y_m^{(l)} = y_m^{(l-1)}, z_m^{(l)} = z_m^{(l-1)}$ 。

在Matlab仿真实验中,取步长 $h = 0.001, a = 35, b = 3, c = 28$, 初始条件 $(x_0, y_0, z_0) = (1, 1, 1)$, 阶数 $(\alpha, \beta, \gamma) = (0.97, 0.96, 0.95)$, 系统出现混沌现象。分数阶陈氏系统的混沌吸引子如图1所示。

1.2 分数阶陈氏系统的混沌同步

PC(Pecora-Carroll)同步方法^[1]是用一个混沌系统的输出作为信号去驱动另一个混沌系统实现这两个混沌系统的同步。针对分数阶陈氏混沌系统,以 y 作为驱动变量,驱动系统如式(8)所示。

$$\begin{cases} \frac{dx}{dt^\alpha} = a(y - x) \\ \frac{dy}{dt^\beta} = (c - a)x - xz + cy \\ \frac{dz}{dt^\gamma} = xy - bz \end{cases} \quad (8)$$

相应的响应系统可设计为:

$$\begin{cases} \frac{dx_2}{dt^\alpha} = a(y - x_2) \\ \frac{dy}{dt^\gamma} = x_2 y - bz_2 \end{cases} \quad (9)$$

仿真参数设置同系统(1),响应系统的初始条件设置为 $(x_{20}, z_{20}) = (2, 2)$ 。响应系统也出现混沌现象,混沌吸引子如图2所示,变量 x_2 与 z_2 随时间变化的波形图如图3所示。驱动系统相应分量与响应系统的相图和同步误差图如图4~5所示,可以看出经过一段短时的演化后,响应系统与驱动系统能够较好地同步。

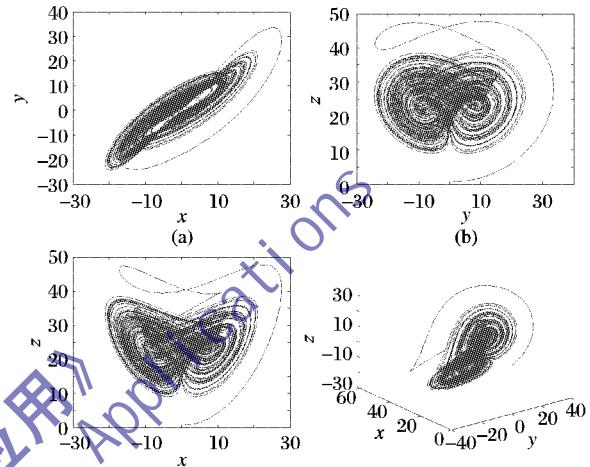


图1 分数阶陈氏系统的混沌吸引子

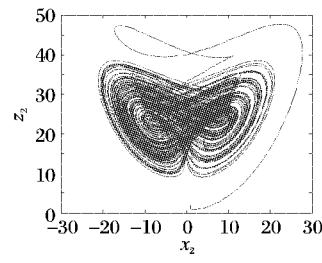


图2 响应系统的混沌吸引子

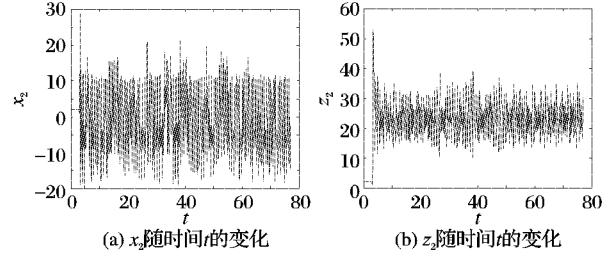


图3 响应系统的波形图

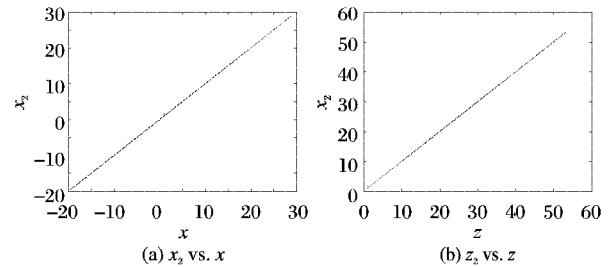


图4 驱动系统相应分量与响应系统的相图

2 基于陈氏混沌的图像加密

基于分数阶陈氏混沌系统及其同步系统,本文提出一种

图像加密算法。加密过程主要包括两个步骤:混沌置乱和混沌掩盖。解密过程则是其逆过程,即混沌去掩盖和混沌逆置乱。整个加解密流程如图6所示。

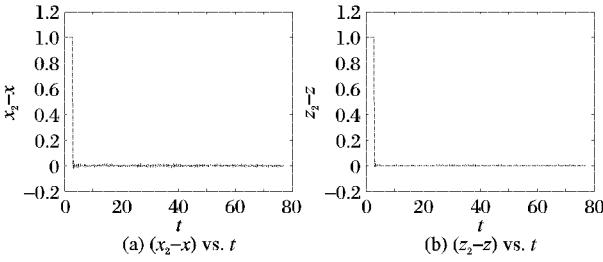


图5 驱动系统相应分量与响应系统的同步误差

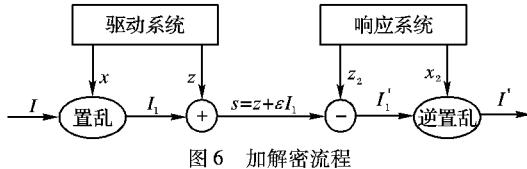


图6 加解密流程

2.1 加密过程

在发送端,驱动系统产生混沌信号 x 和 z 。先利用混沌信号 x 对图像 I 进行置乱,扰乱其像素的空间位置。再将扰乱后的图像 I_1 掩盖在混沌信号 z 中,即得到密文图像 s 。具体过程如下:

1) 混沌置乱。

设图像的大小为 $H \times W$,将其按行先序转化为一维序列 L , L 的长度为 $N = H \times W$ 。由于响应系统与驱动系统要经过一段短暂停后才同步,本文在混沌信号的中间部分取长为 N 的混沌序列 Q ,并将 Q 进行排序,得到 Q_{sort} 。再用得到的 Q_{sort} 对序列 L 进行置乱得到序列 L' ,规则为: $L'(i) = L(Q_{\text{sort}}(i))$, $i = 1, 2, \dots, N$ 。这样就得到了像素位置置乱的图像 I_1 。

2) 混沌掩盖。

为了更好地将图像信息隐藏在类噪声的混沌信号中,先将图像乘以一个较小的系数 ε ($0 < \varepsilon < 0.5$),以降低图像的幅度信息。然后从混沌信号的中间某点开始,将二维矩阵 εI_1 转化成一维序列掩盖在其中,得到密文图像,即 $s = z + \varepsilon I_1$ 。

取 $\varepsilon = 0.02$,对标准 bmp 测试图像 fishingboat (如图7(a))进行加密,得到密文图像(如图7(c))。图7(b)是上一步混沌置乱后得到的图像。从密文图像完全看不到任何有关明文图像的信息,经加密后明文信息得到了较好的隐藏。



图7 图像加密过程

2.2 解密过程

在接收端,响应系统产生混沌信号 x_2 和 z_2 。先用混沌信号 z_2 对密文图像 s 去掩盖,得到 I_1' ,即 $I_1' = (s - z_2)/\varepsilon$ 。然后用混沌信号 x_2 对图像 I_1' 进行逆置乱得到恢复的图像 I' 。具体过程与加密过程类似,此处不再赘述。解密过程如图8所示,恢复的图像与原图像基本一致。

3 安全性分析

作为一个图像加密系统,其安全性是不容忽视的。如果只是纯粹地先隐藏原图像信息,再通过一些操作恢复原图像,如文献[16-17],这只是编码系统,而不是密码系统。本章

从统计特性和密钥两方面来对算法安全性进行分析。

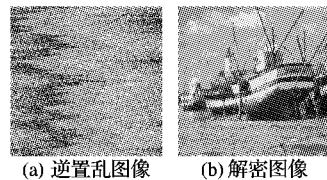


图8 图像解密过程

3.1 统计特性分析

3.1.1 直方图分析

直方图反映了图像最基本的统计特征。由于将图像信息掩盖在混沌信号中时,对图像进行了乘以系数 ε 的操作,仿真实验中 ε 取 0.02,所以密文图像的像素值在 [0, 1] 范围内。从图9可以看出,密文直方图与明文直方图有很大的不同,原图的真实分布已较好地被掩盖,攻击者很难从密文直方图得到破译明文的有用信息。

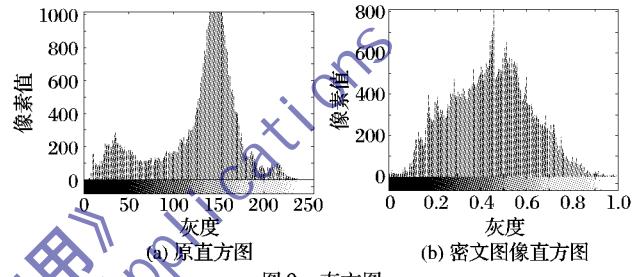


图9 直方图

3.1.2 相邻像素的相关性分析

直方图能反映图像像素的灰度分布情况,但不能反映图像像素的位置信息。通常原始图像的相邻像素是有一定的相关性的,为了抵抗统计攻击,必须降低相邻像素间的相关性。对于加密后的图像,相邻像素的相关性越小说明置乱效果越好。为了测试原图像和密文图像的相邻像素的相关性,分别在水平、竖直和对角方向各随机选取 1000 对相邻像素点,计算其相关系数。设表示两个相邻像素的灰度值,则相关系数的计算公式如下:

$$\begin{cases} r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \\ E(x) = \frac{1}{N} \sum_{i=1}^N x_i \\ D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \end{cases} \quad (10)$$

从表1可以看出,原图像的相邻像素相关系数较大,加密后的图像相关性明显降低,能有效地抵抗统计分析。

表1 原图像与密文图像相邻像素的相关性比较

图像	水平方向	竖直方向	对角方向
原图像	0.9237	0.9146	0.9051
密文图像	0.0152	0.0104	0.0283

3.2 密钥空间的大小与敏感性分析

本算法的参数比较多,根据算法结构,系统的密钥可考虑参数 $(\alpha, \gamma, a, b, \varepsilon)$ 。经实验证,解密系统对参数 ε 不敏感,加密密钥中取 $\varepsilon = 0.02$,当使用 $\varepsilon = 0.2$ 解密时仍能得到原图的大致信息,如图10(a)所示,因此 ε 不适合作为密钥。系统的密钥可选为 (α, γ, a, b) ,各个密钥参数相互独立。其中,分数阶陈氏混沌系统的阶数取值范围为 $0 < \alpha < 1, 0 < \gamma <$

1, 参数满足 $a > 0, b > 0$ 即可, 当然实际的电路系统实现中 a, b 不可能无限大, 不妨取 $0 < a, b < 100$ 。根据计算机双精度浮点数的精度, 本文取 8 字节、15 位有效数字进行分析, 那么 α, γ 分别有大约 10^{14} 种取值可能, 而 a, b 的取值可能则多达 10^{15} 的数量级。设尝试一次破解所需时间的数量级为秒, 则穷举破解所需时间约为 $(10^{14} \times 10^{14} \times 10^{15} \times 10^{15}) / (3.15 \times 10^7) \approx 3.17 \times 10^{50}$ 年, 这个密钥空间比文献[20]中加密算法的密钥空间还要大。理论上讲这是一个非常大的密钥空间, 足以抵抗穷举攻击。

一个良好的加密算法不仅要有较大的密钥空间, 而且还要对密钥参数敏感, 以抵抗差分攻击。在加解密测试中, 本文使用的密钥是 $(0.97, 0.95, 35, 3)$ 。为了验证解密算法对密钥的敏感程度, 使用一些错误密钥来对密文图像进行解密。从图 10 可看出, 解密算法对密钥参数非常敏感, 即使单个密钥参数只有 0.001 的偏差, 也会导致完全不同的解密结果。

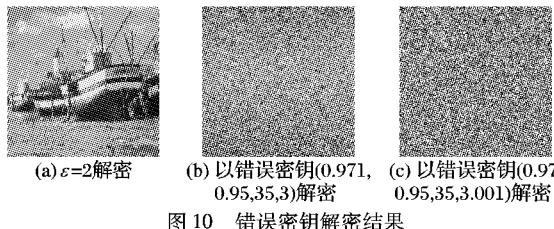


图 10 错误密钥解密结果

为了更加准确地说明错误密钥解密得到的图像与原图差别很大, 使用均方误差(Mean Square Error, MSE)作为衡量解密图像质量的客观指标。MSE 的计算公式^[21]如下:

$$MSE = \frac{1}{NM} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - H(i, j)]^2 \quad (11)$$

其中 $I(i, j)$ 和 $H(i, j)$ 分别表示原图像和解密图像的像素点灰度值。当单个密钥参数与正确密钥出现不同偏差时, 计算解密图像与原图的 MSE, 画出密钥参数 a 的 MSE 曲线, 如图 11。从图 11 中可以看出: 当密钥参数与正确密钥一致时, 解密图像与原图像的 MSE 为 0; 随着偏差的增加, MSE 迅速增大, 即解密图像与原图像的差异明显增大。与文献[21]相比, 本算法的 MSE 值更大, 即算法对密钥更敏感。

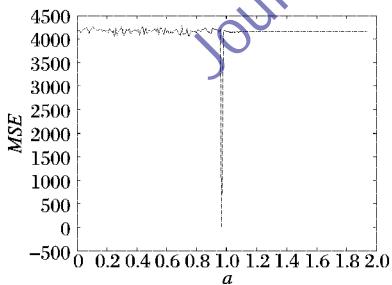


图 11 单个密钥的 MSE 图

4 结语

基于分数阶陈氏混沌系统及其同步系统, 本文提出了一种图像加密算法。本算法既将混沌同步保密通信系统应用于图像加密, 而且也很好地利用了混沌系统产生的混沌信号来进行图像像素位置的置乱, 从而提高加密系统的安全性。实验结果表明, 该算法具有较高的安全性, 能抵抗统计攻击和差分攻击。由于混沌系统需要一定的同步时间, 所以加密时不宜选取混沌序列的初始部分。探索同步速度更快、结构更复杂的混沌系统, 设计更加安全高效的图像加密算法将是下一

步努力的方向。

参考文献:

- [1] PECORA L, CARROLL T. Synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(8): 821–824.
- [2] 高铁杠, 陈增强, 袁著祉. 混沌系统的混合同步及其在安全通信中的应用[J]. 通信学报, 2005, 26(3): 21–24.
- [3] 汪学兵, 张林华, 李传东. 混沌同步及其在保密通信中的应用[J]. 计算机应用研究, 2007, 24(5): 127–129, 132.
- [4] NANA B, WOAFOL P, DOMNGANG S. Chaotic synchronization with experimental application to secure communications[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(5): 2266–2276.
- [5] 徐进, 翡艳, 崔宝同. 时滞混沌系统的同步与反同步及其在保密通信中的应用[J]. 计算机应用, 2010, 30(9): 2413–2416.
- [6] WANG H, ZHU X J, GAO S W, et al. Singular observer approach for chaotic synchronization and private communication[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(3): 1517–1523.
- [7] MATA - MACHUCA J L, MARTINEZ - GUERRA R, AGUILAR - LÓPEZ R, et al. A chaotic system in synchronization and secure communications[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(4): 1706–1713.
- [8] TANG G P, LIAO X F, CHEN Y. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons & Fractals, 2005, 23(2): 413–419.
- [9] 关新平, 范正平, 彭海朋, 等. 陈氏混沌系统的自适应控制[J]. 物理学报, 2003, 50(11): 2108–2111.
- [10] 吴先用, 关治洪, 吴正平. 陈氏混沌系统的全局同步与自适应同步[J]. 华中科技大学学报: 自然科学版, 2007, 35(12): 24–27.
- [11] LI C P, PENG G J. Chaos in Chen's system with a fractional order [J]. Chaos, Solitons & Fractals, 2004, 22(2): 443–450.
- [12] LI C G, CHEN G R. Chaos in the fractional order Chen system and its control[J]. Chaos, Solitons & Fractals, 2004, 22(3): 549–554.
- [13] ZHU H, ZHOU S B, HE Z S. Chaos synchronization of the fractional-order Chen's system[J]. Chaos, Solitons & Fractals, 2009, 41(5): 2733–2740.
- [14] BOWONG S. Stability analysis for the synchronization of chaotic systems with different order: application to secure communications [J]. Physics Letters A, 2004, 326(1/2): 102–113.
- [15] 王震, 孙卫. 分数阶混沌系统同步及其保密通信[J]. 计算机应用研究, 2012, 29(6): 2221–2223, 2261.
- [16] GÁMEZ-GUZMÁN L, CRUZ-HERMÁNEZ C, LÓPEZ-GUTIÉRREZ R M, et al. Synchronization of Chua's circuits with multi-scroll attractors: application to communication[J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(6): 2765–2775.
- [17] SMAOUI N, KAROUMA A, ZRIBI M. Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(8): 3279–3293.
- [18] 潘勃, 李骞, 冯金富, 等. 一种新的离散混沌同步保密通信方案[J]. 计算机应用, 2010, 30(1): 198–202.
- [19] KENNETH S M, BERTRAM R. An introduction to the fractional calculus and fractional differential equations[M]. [S. l.]: Wiley-Interscience, 1993.
- [20] 杨倬, 冯久超, 方勇. 一种基于混沌和分数阶傅里叶变换的图像加密算法[J]. 计算机科学, 2008, 35(9): 239–240, 273.
- [21] 辛怡, 陶然, 王越. 基于分数阶 Fourier 变换的数字图像实值加密方法[J]. 光学技术, 2008, 34(4): 498–502, 508.