文章编号:1000－2367(2015)01－0165－06 DOI:10.16366/j.cnki.1000－2367.2015.01.031

四维混沌与分数傅里叶变换的图像加密方案

苏 婷,董胜伟,吕志伟

(安阳工学院 数理学院,河南 安阳 455000)

摘 要:将四维超混沌系统和标准加权类分数傅里叶变换理论相结合,提出了一种数字图像加密双重方案.对图像进行三基色分层标准加权类分数傅里叶变换,利用超四维混沌序列对变换结果进行置乱操作,将置乱后的 3 层数据融合得到加密图像仿真结果表明,加密后的图像灰度分布均衡,相邻像素的相关系数高度不相关,并且加密图像对秘钥高度敏感,具有较好抗攻击性、鲁棒性.

关键词:超混沌系统;标准加权类;分数傅里叶变换;图像加密;信息安全

中图分类号:TP391.9 **文献标志码**:A

随着网络技术和信息技术的飞速发展,数字图像成为一种表达信息的方式,但在其传播的过程中,由于安全或敏感因素不能直接传送,需要对其进行加密处理,因此数字图像加密方案已经成为信息安全中的一个重要的研究领域,其方案所涉及的数学理论和算法是其实现的基础,故对其数学方法和理论的研究至关重要,数字图像与普通文本信息相比,具有数据信息量大、像素间相关性强和冗余度高等特点,因此传统的加密方法只能借鉴,不能照搬.到目前为止,图像加密的研究主要集中在空间域、变换域和混沌系统[1－10]但是单纯地使用某一种加密方案存在系统结构简单,参数与变量少、密钥空间小等缺点.四维以上的高维超混沌系统具有 4 个以上不变量和两个正的李雅普诺夫指数,密钥空间更大,非线性系统行为更复杂,更适合数字图像加密[8];标准加权类分数傅里叶变换[9]既包含时域上的信息又包含频域上的信息,因此借助于这两种方法的数字图像加密方法有很广泛的应用价值,而计算机性能的提高为算法的实现提供了技术保障.

本文是在文献[8]提出的四维超混沌系统加密方法的基础上,提出了一种基于四维超混沌系统和加权分数傅里叶变换相结合的新的图像加密方法.该方法的密钥不仅有混沌参数和初始值,还有分数傅里叶变换的阶数,大大增加了密钥的空间,破解数字图像的难度加大.最后,从灰度直方图分析、相邻像素相关性分析、密钥的敏感性分析几个方面对算法的安全性能进行了分析,数值结果表明该方法可以有效抵御统计、穷举、差分等多种攻击,有很好的安全性.

1 双重图像加密方法的理论基础

1.1 四维超混沌系统

四维超混沌系统描述如下:

$$\begin{cases}\dfrac{\mathrm{d}x_1}{\mathrm{d}t}=a(x_2-x_2),\\ \dfrac{\mathrm{d}x_2}{\mathrm{d}t}=bx_1+cx_2-x_1x_3+x_4,\\ \dfrac{\mathrm{d}x_3}{\mathrm{d}t}=x_2^2-dx_3,\\ \dfrac{\mathrm{d}x_4}{\mathrm{d}t}=-ex_2,\end{cases}\tag{1}$$

收稿日期:2014-06-19

基金项目:河南省青年骨干教师基金(2011GGJS-213)

作者简介:苏 婷(1980－),女,河南许昌人,安阳工学院讲师,研究方向为信息安全、图像处理等,E-mail:suting0374@163.com.

其中 a,b,c,d,e 是系统控制参数，$x=[x_1,x_2,x_3,x_4]$ 表示超混沌系统状态量. 当控制参数在 $a=27.5,b=3,c=19.3,d=2.9,e=3.3$ 条件下，任给一组超混沌系统状态的初始值 $x_0=[x_1(0),x_2(0),x_3(0),x_4(0)]$ 作为原始密钥，(1) 式有两个正的李雅普诺夫指数，处于超混沌状态[3] 根据四阶龙格 —— 库塔算法对(1) 式进行迭代，产生 4 组原始超混沌序列，但该混沌序列并不适合直接用于图像加密，并且与明文图像不存在关联，因此需对其进行优化改造处理.

1.2 标准加权类分数傅里叶变换

标准加权类分数傅里叶变换是在 C. C. Shis 定义的加权类分数傅里叶变换的基础上衍生而来的. 主要研究其定义的加权类分数傅里叶变换的扩展形式，其定义如下[12]：

$$F^{\alpha}[f(x)]=F^{\alpha}(m,M)[f(x)]=\sum_{l=0}^{M-1}A_l(\alpha,m)f_l(x), \tag{2}$$

表达式中的加权系数表示为

$$A_l(\alpha,m)=\frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{-\frac{2\pi i}{M}[\alpha(k+m_kM)-kl]\right\}, \tag{3}$$

其中 $\alpha\in\mathbf{R}^p$ 为分数傅里叶变换的阶数，$m=(m_0,m_1,\cdots,m_{M-1})\in z^M$，$f_l(x)$ 为 $f(x)$ 的 l 次傅里叶变换.

加权类分数傅里叶变换满足下面的 4 个性质：

1) 连续性：对于 $L^2(\mathbf{R})$ 内的两个函数 $f(x),g(x)$，当 $\int_{-\infty}^{+\infty}\|f(x)-g(x)\|^2\mathrm{d}x\to 0$，有 $F^{\alpha}(f(x))\to F^{\alpha}(g(x))$；

2) 线性性质：$F^{\alpha}[af(x)+bg(x)]=aF^{\alpha}[f(x)]+bF^{\alpha}[g(x)]$；

3) 阶数可加性和交换性：$F^{\alpha+\beta}[f(x)]=F^{\alpha}[f(x)]F^{\beta}[f(x)]=F^{\beta}[f(x)]F^{\alpha}[f(x)]=F^{\beta+\alpha}[f(x)]$；

4) 酉性：$F^{\alpha}\cdot(F^{\bar{\alpha}})^H=I$，$I$ 是单位矩阵，H 表示共轭转置.

2 双重图像加密算法

2.1 双重图像加密算法

1) 对原始图像进行预处理，用 p 表示原始图像，其大小为 $M\times N$，R,G,B 分别表示其三基色平面分层矩阵；2) 对 R,G,B 进行二维离散标准加权类分数傅里叶变换，即 $Q_1=F^{\alpha}(R)F^{\alpha}$，$Q_2=F^{\alpha}(G)F^{\alpha}$，$Q_3=F^{\alpha}(B)F^{\alpha}$，$F^{\alpha}$ 是 $X\times X$ 的离散实向量加权酉变换矩阵；3) 分层混沌置乱. 设该混沌系统产生的 4 组原始超混沌序列为 $\{x_j(i)\}(j=1,2,3,4;i=1,2,\cdots,L/4)$，$L$ 为待加密图像像素数目总和为防止混沌迭代暂态效应影响，已舍弃前面次迭代结果将超混沌序列各元素按(4) 式改造为[0,225] 范围内的整数，式中 floor 表示负方向取整，mod 表示取余，S 为待加密图像各像素灰度值总和其中将 y_j 放大倍数进行运算(如 $r(x)$ 倍)，可增强原始图像像素对密钥的敏感性. 将改造得到的序列值按(5) 式组合得到长度为 L 的密钥序列 k_1(灰度置换密钥序列)；根据 k_1 按(6) 式进行得到二值密钥序列 k_2(分离置乱密钥序列)

$$x_j=\mathrm{mod}(\mathrm{floor}((|x_j|-\mathrm{floor}(|x_j|))\times 10^{14}+S\times 10^6),256), \tag{4}$$

$$k_1=\{x_1(1),\cdots,x_1(L/4),\cdots,x_j(L/4)\},j=1,2,3,4, \tag{5}$$

$$k_2=\begin{cases}0,k_1(i)>127.5,\\1,k_1(i)<127.5,\end{cases} \tag{6}$$

该序列满足理想随机序列，因为具有均值为零、自相关为冲激函数、互相关性为零 3 个特点.

分别对 Q_1,Q_2,Q_3 的置乱，Q_1 的置乱方法如下.

1) 若 $k_2(i)=0$，将 $Q_1(i)$ 像素存入序列 p_{1r}；若 $k_2(i)=1$，将 $Q_1(i)$ 像素存入序列 p_{2r}.

2) 将 p_{1r},p_{2r} 连接组合，并按行扫描成与原始图像等大的矩阵 P_1，假设 p_{1r},p_{2r} 连接点为 L_0，L_0 即为序列 p_{1r} 长度，可将 L_0 作为密钥进行保存，按照上面的置乱方法再分别对 G_2,G_3 进行置乱操作，所得到的矩阵分别为 P_2,P_3，因为混沌置乱所产生的混沌序列是相同的，故作为密钥的 L_0 是相同的.

3) 3 层融合，将置乱后的 P_1,P_2,P_3 融合，得到加密后的密图 M.

具体的加密过程可以用图 1 表示解密过程通过分层置乱和分层加权分数傅里叶逆变换实现

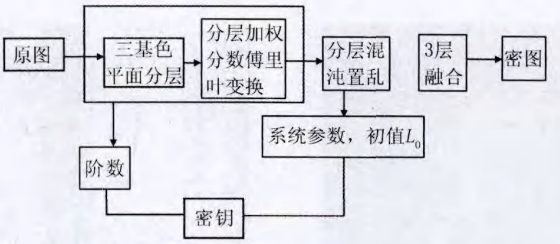


图1 加密方案图解过程

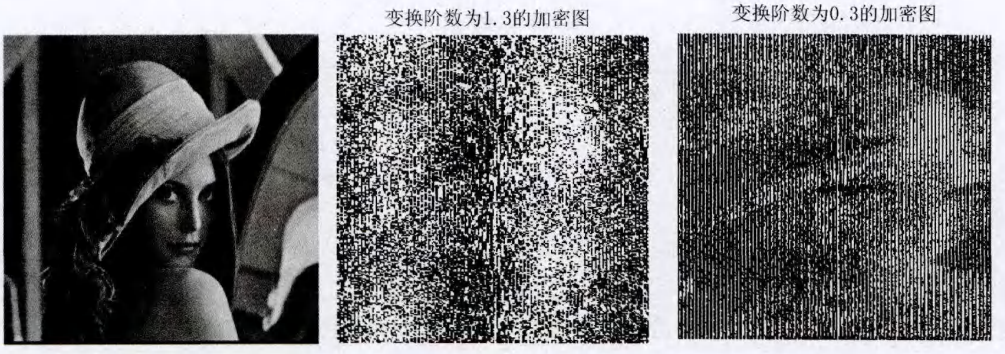
2.2 双重图像加密算法复杂度分析

利用 Matlab 软件中求解微分方程的 ode45 函数可以很快生成四维超混沌序列，分数傅里叶变换和逆变换的数值算法则以快速分数傅里叶变换为基础，利用文献[12]的算法，其复杂度和快速傅里叶变换的一样，计算量没有显著增加，借助于 Matlab 软件图像的加密结果和解密结果均可表示为三维实值矩阵，节省了存贮空间，大大提高了加密和解密的效率.

3 数值仿真及性能分析

3.1 加密算法仿真

选用大小为 256×256 的 lena.bmp 为原始图像，标准加权分数傅里叶变换的阶数选用 0.3 和 1.3，混沌系统中的参数和 4 个初始值分别为 $a=27.5, b=3, c=19.3, d=2.9, e=3.3$ 和[0.5, 0.5, 0.3, 0.5]，$L_0=32\ 887$，其中 L_0 只要选取相当大就行，它是其中的一个密钥，仿真后的效果如图 2 所示.



(a) 原始图像　　(b) 阶数为1.3　　(c) 阶数为0.3

图2 双重加密原图与加密图的对比

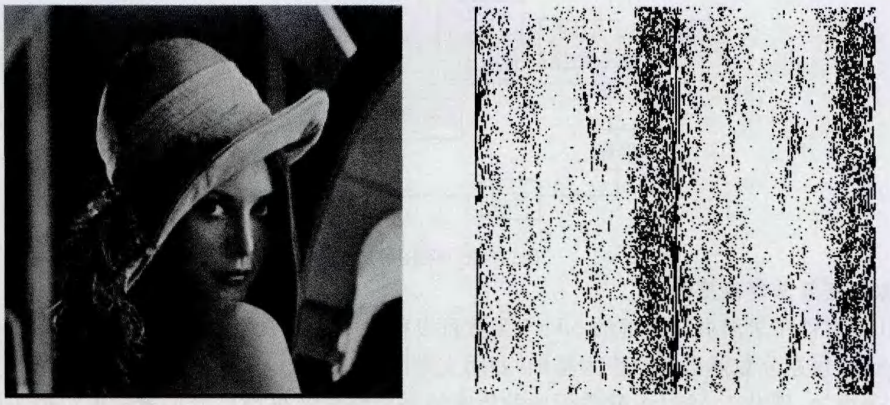
从视觉上看，无论选择哪个阶数进行加密，加密后的图像完全不带有原始图像的信息，从而有较好的加密效果.

3.2 均方误差(MSE)分析(密钥的敏感性分析)

像素大小为 $N\times M$ 图像的均方误差(MSE)定义为：

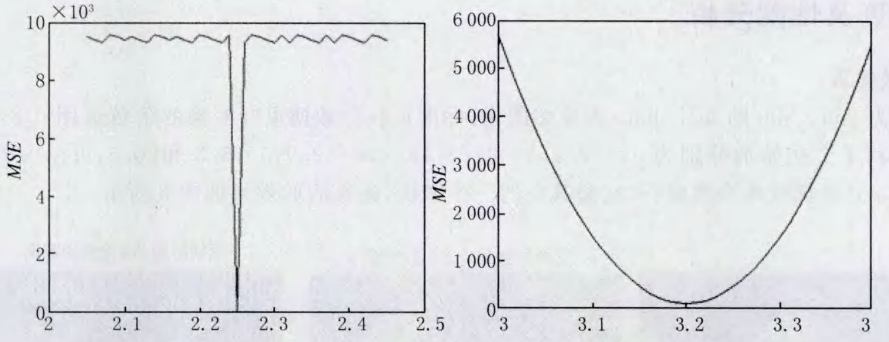
$$\mathrm{MSE}=\|p-\omega\|^2=\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}|p(i,j)-\omega(i,j)|^2, \tag{7}$$

p 为原始图像，ω 为解密图像，在不知道解密键的情况下，MSE 的大小可以表示解密以后的图像与原始图像的近似程度，当 MSE = 0 时，说明推测的解密键与真正的解密键是一致的，当 MSE ≠ 0 时，表示推测的解密键与正确的解密键不一致，无法正确解密图像. 其值越大说明通过解密键解密的图像与加密前的图像的信息差别越大. 从图 3 和图 4 可以看出，由密键的微小变化所引起的解密图像与原始图像的 MSE 数值差别巨大，由此可见加密图像对密键极为敏感.



(a) 正确解密图像 (b) 错误解密图像

图3 正确解密与错误解密图像对比



(a) 混沌参数b变化 (b) 变换阶数变化

图4 单个解密键变化的加密方案的MSE

3.3 灰度直方图分析

统计一幅图像中各个灰度出现的概率二维直方图中,横坐标表示图像中像素点的灰度级,纵坐标表示灰度级上各个像素点出现的概率,从图 5 可以看出,加密后的密图灰度直方图分布较原始图片均匀,并且与原始图像的灰度分布没有相似性,从加密后的灰度直方图很难得到原始图片的正确信息.

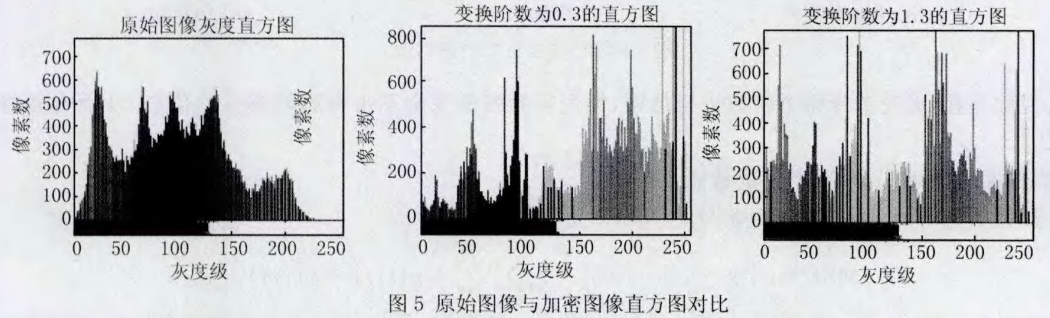


图 5 原始图像与加密图像直方图对比

3.4 相邻像素点间相关性分析

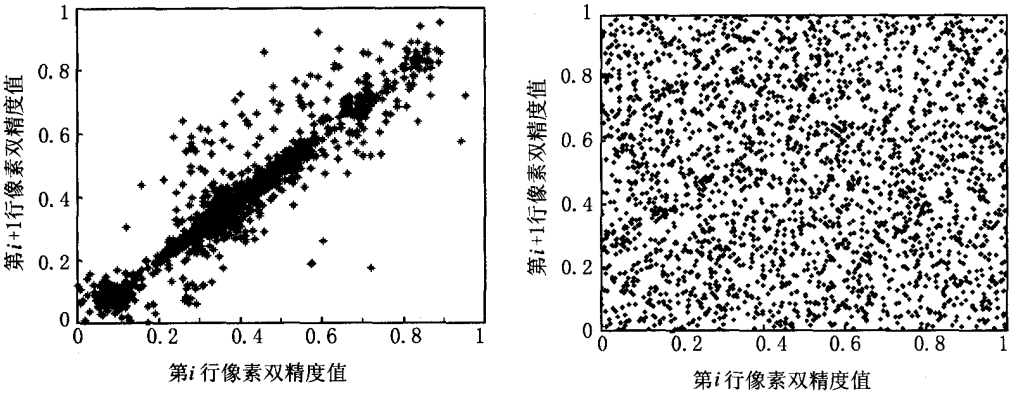
对于一般的数字图像,其水平方向、垂直方向和对角线方向上相邻像素之间的相关性往往非常大,利用这个特点可以由统计特性获得原始图像的有关信息.为防止统计分析攻击,经过加密后图像相邻像素之间的相关性比较低.从原始图像中抽取水平方向上的相邻像素双精度值,并通过下式计算其相关系数:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \tag{8}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2, \tag{9}$$

$$conv(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)], \tag{10}$$

(x_i,y_i) 表示一对相邻像素灰度值；N 表示进行相关系数计算的相邻像素对的数量，相邻两个像素相关系数表示为 $r_{x,y}=\frac{conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$. 用同样的方法，可以计算出垂直方向和对角线方向上相邻像素之间的相关系数. 选取原始图像和加密图像所有相邻像素对（包括水平、垂直、对角方向）进行相关性分析，计算其平均值，所得结果和文献[3]中的计算结果对比见图 6 和表 1，从表 1 中可以看出加密后图像各个方向的相关系数结果明显偏小，接近于 0，并且数值上比文献[9]中的加密方法的效果更好一些.



（a）原始图像前20行像素的结果　　（b）加密图像前20行像素的结果

图6水平方向相关性对比图

表 1　相邻像素相关性分析结果对比表

像素关系	水平方向	垂直方向	对角线方向
原始图像	0.976 1	0.952 3	0.939 4
本文方法加密图像	0.064 9	0.017 4	0.046 6
文献[9]方法加密图像	0.315	0.119	0.015

4　结　语

本文基于四维超混沌系统和标准加权分数傅里叶变换结合的双重加密方案对原始图像先进行三基色分层，对每层进行标准加权分数傅里叶变换，然后对四维超混沌系统的 4 个序列进行改造处理，根据分离置乱密键序列在 3 层图像分数傅里叶变换域进行分离置乱操作，降低图像的相关性，最后再把 3 个基色平面合成，最终得到加密图像. 此外，分别从秘钥敏感性、直方图和图像相邻像素的相关性 3 个方面进行了仿真结果表明，结合混沌置乱的敏感性和分数傅里叶变换加密方法的鲁棒性得到的双重加密方法，有更强的抗攻击能力，信息的安全性更高，有进一步推广应用的价值.

参　考　文　献

[1]　于万波. 基于 Matlab 的图像处理[M]. 北京：清华大学出版社，2008：120-125.

[2]　陈　帅，钟先信，石军锋，等. 基于离散数字混沌序列的图像加密[J]. 电子与信息学报，2007，29(4)：898-900.

[3]　周庆，胡　月，廖晓峰. 一种自适应的图像加密算法的分析及改进[J]. 电子学报，2009，37(12)：2730-2734.

[4]　Langu J，Tao R，Wang Y. Image encryption based on the multiple-parameter discrete frational Fourier transform and chaos function[J]. Opt Commun，2010，283：2092-2096.

[5] 刘建明,鲁东明. 采用加权优化的图像修复[J]. 中国图象图形学报,2011,16(4):528-532.

[6] Patidar V,Pareek N K,Pumhit G,et al. A robust and secure chaotic standard map based pseudorandom per-mutation-substitution scheme for image encryption[J]. Optics Communications,2011,284(19):4331-4339.

[7] 张晓强,王蒙蒙,朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学,2012,34(5):1-6.

[8] 钟厚桥,李建民,林振荣,等. 基于超混沌序列的图像加密方案[J]. 计算机应用研究,2013,30(10):3110-3113.

[9] 张文全,张 烨,周南润基于随机分数梅林变换的非线性图像加密算法[J]. 计算机应用,2013,33(10):2865-2894.

[10] 王俊珺,苏利萍. 一种新的基于双向分数傅里叶变换和 RGB 映射图像保护算法[J]. 计算机应用与软件,2013,30(8):232-235.

[11] Almeida L B. The fractional Fourier transform and time-frequency representations[J]. IEEE Trans Signal Processing,1994,42:3084-3091.

[12] MEI Lin,ZHANG QinYu,SHA XueJun, et al. Digital computation of the weighted-type fractional Fourier transform[J]. SCIENCE CHINA (Information Science),2013,56(7):1-12.

Image Encryption Method Based on Hyper-chaos System of 4-D and Fractional Fourier transform

SU Ting,DONG Shengwei,LYU Zhiwei

(Mathematics and Physics College,Anyang Institute of Technology,Anyang 455000,China)

Abstract: An image encryption algorithm based on hyper-chaos system of 4-d and standard weighted fractional fourier transform was proposed. Firstly, do fractional fourier transform of the image about the three colors layered, then transform the results using 4-D hyper-chaos system, lastly the encrypted image was obtained after three layers of data fusion. The numerical simulation results demonstrate that the encryption algorithm is against common attacks, the correlation coefficients of adjacent pixels is higher irrelevance, has larger key space and sensitive to keys with good security.

Keywords: hyper-chaos system; standard weighted class; fractional Fourier transform; image encryption; information security