文章编号：0253-2239(2008)supplement2-0117-04

光学图像加密与多参数加权类分数傅里叶变换

张海莹[1] 冉启文[1,2] 张 晋[2]

([1] 哈尔滨工业大学航天学院，黑龙江 哈尔滨 150001
[2] 哈尔滨工业大学理学研究中心，黑龙江 哈尔滨 150001)

摘要 为了提高图像加密的安全性，提出了一种多参数加权类分数傅里叶变换。此类多参数加权类分数傅里叶变换是 C. C. Shih 提出的四项加权类分数傅里叶变换的一种扩展，除了分数阶数，还有四个在四项加权系数之中的自由参数，称其为向量参数。同时给出此多参数加权类分数傅里叶变换的离散形式，并把这种算法应用到光学图像加密中。此算法在应用一次二维分数傅里叶变换可以有十个密键：一类为阶数参数；另一类为向量参数，因此这种加密算法在增加了安全性的同时，加密过程的复杂度降低。数值仿真验证了此算法的有效性和可靠性。

关键词 图像处理；光学图像加密；分数傅里叶变换；信息安全

中图分类号 TP751.2 **文献标识码** A **doi**：10.3788/AOS200828s2.0117

Optical Image Encryption and Multiple Parameter Weighted Fractional Fourier Transform

Zhang Haiying[1] Ran Qiwen[1,2] Zhang Jin[2]

([1] *School of Astronautics, Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*
[2] *Science Research Center, Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*)

Abstract In order to increase the security of the image encryption, the weighted fractional Fourier transform with dilation parameter (PWFRFT) is proposed. This PWFRFT is an extension of four-item weighted fractional Fourier transform (FRFT) defined by C. C. Shih. It owns four free parameters, which is called the vector parameter here, in the weight coefficients besides the order of the fractional Fourier transform. A novel optical image encryption algorithm is presented by the PWFRFT. The method owns ten secret keys when two-dimensional PWFRFT is operated one time: one kind is the order parameter and other kind is the vector parameter. Therefore, the new encryption method makes the security of image information better and the encryption process simpler. Digital simulations are presented to verify the validity and efficiency of the algorithm.

Key words image processing; optical image encryption; fractional Fourier transform; information security

1 引 言

分数傅里叶变换(FRFT)是傅里叶变换的一种扩展[1~3]，在这里傅里叶变换被称为经典的 FT，它是信号处理最经常使用的工具之一。作为光学信息处理的基本工具，分数傅里叶变换最近被引入散射光学[4~6]和众所周知的光栅光学[7~8]。由于互联网的开放性，信息安全变得越来越重要，图像加密也就得到了重视。2000 年，应用分数傅里叶变换的图像加密文献首次出现[9]，这里是以分数傅里叶变换的阶数为密键的。随后，为了增加安全性和可靠性，文献[10]提出了应用多次分数傅里叶变换进行加密，以获得更多的密键，同时这种方法的计算复杂度增加了。文献[11～13]同样利用分数傅里叶变换的叠加，在增加安全性的同时也增大了算法的复杂度。

基金项目：国家自然科学基金(10374023)资助项目。

作者简介：张海莹(1977－)，女，博士研究生，讲师，主要从事傅里叶光学和图像处理方面的研究。
E-mail：zhyhit0452@163.com

导师简介：冉启文(1966－)，男，博士，教授，主要从事小波变换与分数傅里叶变换方面的研究。
E-mail：qiwenran@hit.edu.cn

本文提出了一种多参数加权类分数傅里叶变换，具有阶数参数和四个在四项加权的系数中的自由参数，称这里的自由参数为向量参数。这种多参数加权类分数傅里叶变换应用于图像加密时，不仅分数傅里叶变换的阶数可以作为密键，而且向量参数也可以作为密键。也就是说，应用一次一维多参数加权类分数傅里叶变换就可以获得五个密键。本文使用二维多参数加权类分数傅里叶变换，应用一次变换可以有十个密键，使图像加密的安全性和可靠性增强，同时算法的复杂度降低。

2 连续多参数加权类分数傅里叶变换

1995 年，C. C. Shih[1] 提出了一种分数化经典傅里叶变换的方法，是一种新的分数傅里叶变换定义形式，称之为加权类分数傅里叶变换（WFRFT）。定义 α 阶多参数加权类分数傅里叶变换是 WFRFT 的扩展，记为 $\boldsymbol{F}^{\alpha}$

$$\boldsymbol{F}^{\alpha}=\sum_{l=0}^{3}p_l(\alpha)f_l, \tag{1}$$

这里 $f_{4L+l}(x)=(\boldsymbol{F}^{4L+l}f)(x)=f_l(x)$，$p_l(\alpha)$ 是 $f_l(l=0,1,2,3)$ 的系数。这里的系数 $p_l(\alpha)$ 与 WFRFT 的系数是不同的

$$p_l(\alpha)=\left(\frac{1}{4}\right)\sum_{k=0}^{3}\mathrm{e}^{-2\pi\mathrm{i}[\alpha(k+4n_k)-lk]/4},(l=0,1,2,3), \tag{2}$$

这里 $\boldsymbol{N}=(n_0,n_1,n_2,n_3)\in\boldsymbol{Z}\times\boldsymbol{Z}\times\boldsymbol{Z}\times\boldsymbol{Z}=\boldsymbol{Z}^4$ 是一个有四个整数元的向量，并且对于 $0\leqslant m,l\leqslant 3$，$\alpha,\beta\in\boldsymbol{R}$，$p_l(\alpha)$ 具有下列特性：

① 连续性：对任意的实数 α，$p_l(\alpha)$ 是连续的；

② 边界性：$p_l(m)=\delta(m-l)$；

③ 周期性：$p_l(\alpha)=p_l(\alpha+4)$；

④ 可加性：$p_l(\alpha+\beta)=\sum_{\substack{0\leqslant m,n\leqslant 3\\ m+n\equiv l \bmod(4)}}p_m(\alpha)p_n(\beta),\ (l=0,1,2,3)$

把(2)式代入(1)式，得到多参数加权类分数傅里叶变换的一般形式

$$\boldsymbol{F}_{\mathrm{N}}^{\alpha}=\left(\frac{1}{4}\right)\sum_{l=0}^{3}\sum_{k=0}^{3}\mathrm{e}^{-2\pi\mathrm{i}[\alpha(k+4n_k)-lk]/4}\boldsymbol{F}^{l} \tag{3}$$

3 光学图像加密

把多参数加权类分数傅里叶变换应用于光学图像加密。具体过程如下：首先读入原始图像；然后进行二维多参数加权类分数傅里叶变换；完成图像加密。根据多参数加权类分数傅里叶变换的可加性，解密过程只需使用多参数加权类分数傅里叶变换的逆变换，完成对加密图像的解密图像恢复。由于多参数加权类分数傅里叶变换除了阶数参数之外，还有一组向量参数可以作为密键，这样应用一次二维离散多参数加权类分数傅里叶变换可以有 10 个密键，从而使图像加密的安全性增加且复杂度降低。

这里 $f_l(l=0,1,2,3)$ 是函数 f 的分数傅里叶变换，图像加密过程可以用一个示意性的迭代装置，即光电混合系统来说明。位于透镜的左边平面的是空间光调制器（SLM），SLM 可以显示振幅和相位用来显示函数 f_{l-1} 的第 l 次叠加。透镜右端的接收面可由一个电荷耦合装置（CCD）记录全息图，导入计算机。通过计算机的后加工，f_{l-1} 的振幅和相位在空间光调制器上得到恢复和显示，经过叠加之后，所有的基函数都得到了，如图 1 所示。

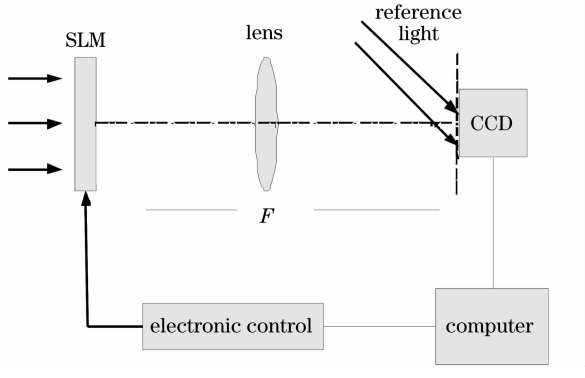


图 1 基于多参数加权类分数傅里叶变换的光学图像加密和解密系统

Fig. 1 Optical setup of the image encryption and decryption system based on multiple parameter weighted fractional Fourier transform

由于多参数分数傅里叶变换有向量参数可以作为密键，这样经过加密，密键为 (α,β,N_l,N_r)，有 10 个密键，其中 $\alpha,\beta\in\boldsymbol{R}$，$N_l=(n_{l0},n_{l1},n_{l2},n_{l3})$，$N_r=(n_{r0},n_{r1},n_{r2},n_{r3})\in\boldsymbol{Z}\times\boldsymbol{Z}\times\boldsymbol{Z}\times\boldsymbol{Z}=\boldsymbol{Z}^4$。解密键为 $(-\alpha,-\beta,N_l,N_r)$，所以想要得到原始图像需要得到 10 个参数，大大提高了加密的性能。

4 仿 真

4.1 加 密

用数字仿真来证实应用多参数加权类分数傅里叶变换的图像加密的有效性和可靠性。图 2(a) 为原始图像，图 2(b) 为加密图像，密键为 (−3.1623，−3.3166，[9,4,16,20]，[8,3,17,13])。从加密图像可以看出，经过一次多参数加权类分数傅里叶变

换之后，由 8 个整数密键，2 个实数密键加密的图像，在视觉上没有原图像的任何信息。这 10 个密键中的 8 个整数是任意取得的，2 个实数也是随机产生的，所以具有很好的安全性。

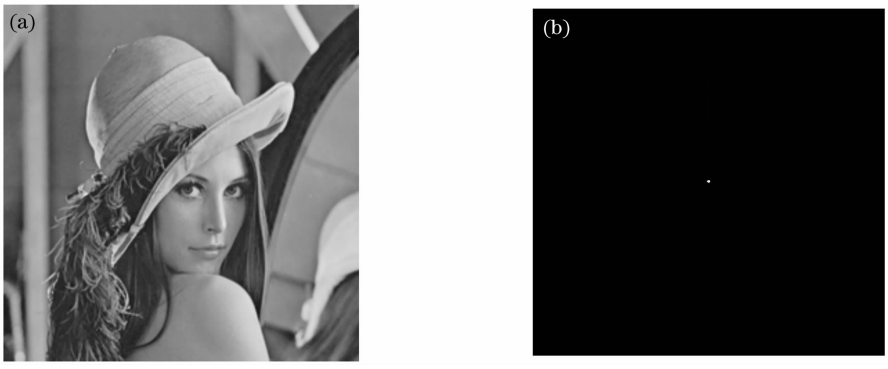
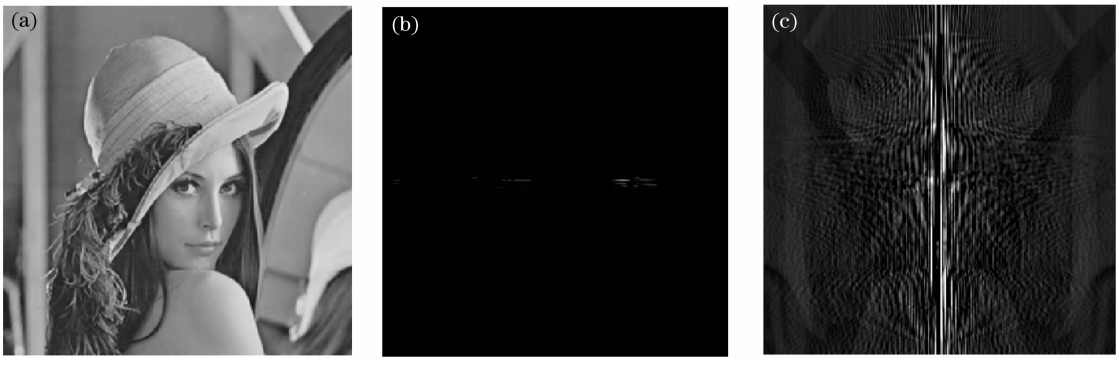


图 2　图像加密计算机仿真。(a) 原始图像；(b) 加密图像

Fig. 2　Computer simulations of encryption. (a) the original image; (b) encryption image

4.2　解　密

图 3(a)为利用正确的解密键(3.1623,3.3166,[9,4,16,20],[8,3,17,13])解密图像得到的结果，可以得到清晰的原图像，说明了这种方法的可靠性。图 3(b)为利用错误的解密键(3,3.3166,[9,4,16,20],[8,3,17,13])解密图像得到的结果，可以看到即使得到 9 个正确的解密键，而只有一个阶数参数的解密键偏差很小的情况下，仍然得不到原图像的任何信息，说明了这种方法的安全性很好。图 3(c)为利用错误的解密键(3.1623,3.3166,[9,4,16,20],[48,3,17,43])解密图像得到的结果，由图中可见，向量参数对于解密过程也起了相当大的作用，当向量参数中的两个元素是未知时，仍然不能得到原图像的任何信息，进一步说时了这种加密方法的安全性很高。



3　解密图像。(a) 正确的密键；(b) (3,3.3166,[9,4,16,20],[8,3,17,13])；(c) (3.1623,3.3166,[9,4,16,20],[48,3,17,43])

Fig. 3　Decryption image with keys. (a) correct keys; (b) incorrect keys (3,3.3166,[9,4,16,20],[8,3,17,13]); (c) incorrect keys (3.1623,3.3166,[9,4,16,20],[48,3,17,43])

4.3　误差分析

图 4(a)表示当阶数参数 α 变化时，加密图像和原始图像的均方误差，可以看到纵轴的均方误差达到了 10^4 量级，进一步说明这种加密方法的可靠性。图 4(b)为向量参数变化时，解密的均方误差。向量参数共有八个，以 m_{r3} 和 n_{l4} 为例，通过三维的图像来说明向量参数对于图像加密的影响。由图中可以看出，向量参数对于图像恢复的影响很大，这一点通过纵坐标的均方误差可以看出。作为加密图像的另一类参数密键，向量参数提高了图像加密的安全性和可靠性，使得应用多参数加权类分数傅里叶变换进行图像加密具有更加明显的优越性。

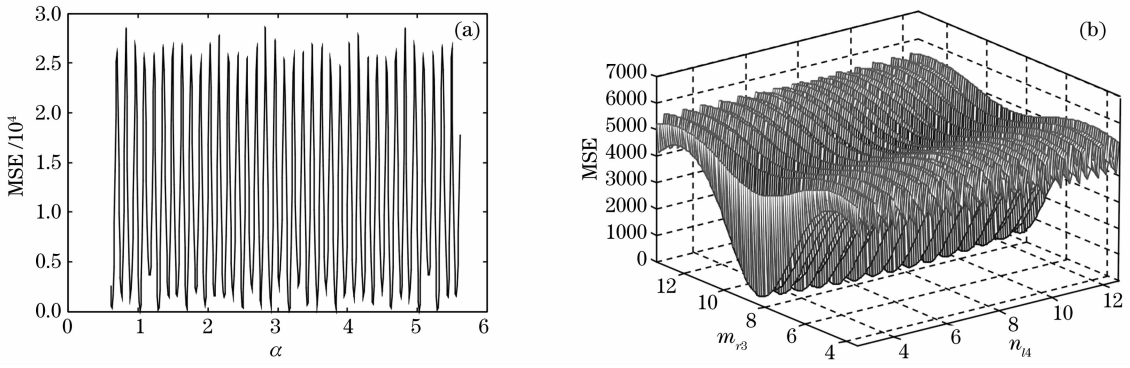


图 4 MSE 随着阶数参数密键的变化(a)和向量的参数密键变化(b)

Fig. 4 MSE changing with the order parameter (a); and the vector parameter (b)

5 结 论

提出了一种多参数加权类分数傅里叶变换,具有阶数参数和向量参数。当八个向量参数均取零时,这种变换退化为标准加权类分数傅里叶变换。同时基于多参数加权类分数傅里叶变换提出一种新的图像加密方法,这种加密方法一次变换可以有十个密键。而以往应用的分数傅里叶变换加密的方法,一次分数傅里叶变换只能得到一个或两个密键,为了得到更多的密键,只能多次应用分数傅里叶变换,在增加安全性的同时大大增加了复杂度。基于多参数加权类分数傅里叶变换提出一种新的图像加密方法,应用简单且复杂度较低,并且提高了图像加密的安全性和可靠性。

参 考 文 献

1 C. C. Shih. Fractionalization of Fourier transform[J]. *Opt. Commun.*, 1995, **11**(8): 495～498

2 V. Namias. The fractional order Fourier transform and its applications to quantum mechanics[J]. *Inst. Math. Appl.*, 1980, **25**: 241～265

3 C. McBride, F. H. Kerr. On Namias's fractional Fourier transform[J]. *IMA J. Appl. Math.*, 1987, **39**: 159～175

4 A. W. Lohmann. Image rotation, wigner rotation, and the fractional Fourier transform[J]. *J. Opt. Soc. Am. A.*, 1993, **10**(10): 2181～2186

5 L. M. Bernardo, O. D. D. Soares. Fractional Fourier transforms and imaging[J]. *J. Opt. Soc. Am. A.*, 1994, **11**(10): 2622～2626

6 M. Ozaktas, D. Mendlovic. Fractional Fourier optics[J]. *J. Opt. Soc. Am. A.*, 1995, **12**(4): 743～751

7 H. M. Ozaktas, D. Mendlovic. Fractional Fourier transforms and their optical implementation: II[J]. *J. Opt. Soc. Am. A.*, 1993, **10**(12): 2522～2531

8 Yue Huimin, Su Xiangyu, Li Zeren. Improved fast Fourier transform profilometry based on composite grating [J]. *Acta Optica Sinica*, 2005, **25**(6): 767～771
岳慧敏, 苏显渝, 李泽仁. 基于复合光栅的快速傅里叶变换轮廓术[J]. 光学学报, 2005, **25**(6): 767～771

9 B. H. Zhu, S. T. Liu, Q. W. Ran. Optical image encryption based on multi-fractional Fourier transforms[J]. *Opt. Lett.*, 2000, **25**(16): 1159～1161

10 S. Liu, L. Yu, B. Zhu. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering[J]. *Opt. Commun.*, 2001. **187**: 57～63

11 Y. Zhang, C. H. Zheng, N. Tanno. Optical encryption based on iterative fractional Fourier transform[J]. *Opt. Commun.*, 2002, **202**: 277～285

12 B. Hennelly, J. T. Sheridan. Fractional Fourier transform-based image encryption: phase retrieval algorithm [J]. *Opt. Commmun.*, 2003, **226**: 60～81

13 X. Wang, D. Zhao, L. Chen. Image encryption based on extended fractional Fourier transform and digital holography technique[J]. *Opt. Commun.*, 2006, **260**: 449～453