

基于随机分数梅林变换的非线性图像加密算法

张文全, 张 烨, 周南润*

(南昌大学 电子信息工程系, 南昌 330031)

(*通信作者电子邮箱 zmr21@163.com)

摘 要: 为了消除线性加密系统的安全隐患, 提出了一种基于随机分数梅林变换的非线性图像加密算法。结合对数—极坐标变换和随机分数傅里叶变换构造了随机分数梅林变换, 随机化过程用到的实对称随机矩阵由线性同余函数生成。输入的实值图像经随机分数梅林变换非线性加密, 得到便于存储和传输的实值密文。该算法增加了线性同余函数的 3 个参数作为密钥, 与分数梅林变换相比, 随机分数梅林变换的分数阶密钥的敏感性更强。数值模拟表明该算法有较强的抗攻击能力, 密钥灵敏度高, 具有良好的安全性。

关键词: 图像加密; 分数梅林变换; 分数傅里叶变换; 线性同余; 非线性加密

中图分类号: TP309.7 **文献标志码:** A

Nonlinear image encryption algorithm based on random fractional Mellin transform

ZHANG Wenquan, ZHANG Ye, ZHOU Nanrun*

(Department of Electronic Information Engineering, Nanchang University, Nanchang Jiangxi 330031, China)

Abstract: A nonlinear image encryption algorithm based on random Fractional Mellin Transform (FrMT) was proposed to get rid of the potential insecurity problem of the linear encryption system. The random FrMT was constructed by combining log-polar transformation with random Fractional Fourier Transform (FrFT), and a real-valued symmetrical random matrix was generated by Linear Congruential Generator (LCG) in randomizing process. The real value input image was encrypted by random FrMT which made the encryption be nonlinear, and the output ciphertext of the FrMT was also real-valued, which was convenient for storage and transmission. The encryption algorithm had three keys that were the parameters of LCG. Compared with FrMT, the fractional order key of random FrMT was more sensitive. The numerical simulation results demonstrate that the encryption algorithm is against common attacks, and sensitive to keys with good security.

Key words: image encryption; Fractional Mellin Transform (FrMT); Fractional Fourier Transform (FrFT); linear congruence; nonlinear encryption

0 引言

近年来, 分数傅里叶变换 (Fractional Fourier Transform, FrFT) 成为图像加密领域的一个重要数学工具。随着对 FrFT 及其应用的深入研究, 衍生出多种新型的分数变换并被应用到图像加密中^[1-6]。文献[1]构造出的随机离散 FrFT 的幅度和相位都是随机化的, 利用随机离散 FrFT 的这一特点进行加密, 可增强算法的安全性。文献[5]针对离散 FrFT 矩阵的不同特征值取不同的分数阶次, 构成多参数离散 FrFT, 其变换核有多个参数, 用在图像加密中可增加密钥数量。但 FrFT 是典型的线性变换, 大部分基于 FrFT 的图像加密系统具有线性属性, 明文、密文、密钥之间的函数关系相对较简单, 无法有效抵抗选择明文攻击、已知明文攻击等常见攻击。

密码系统设计的一个基本准则是尽量引入非线性操作来增强系统的安全性, 文献[7]利用对数的底变换规则将待加密彩色图像的三个分量分别代入随机模板中, 再分别进行基于 FrFT 的随机相位编码实现非线性加密, 文献[8-9]在傅里叶域运用相位截断和振幅保留非线性运算, 移除了加密系统的线性属性, 截断的相位作为解密密钥不同于加密密钥, 属非对称密码系统。这些非线性加密系统有很强的抗攻击能力, 但加密方法复杂。为了消除线性加密系统的安全隐患, 有

必要寻找适合于图像加密的非线性变换。

分数梅林变换 (Fractional Mellin Transform, FrMT) 是输入函数在对数—极坐标下的 FrFT, 其变换具有非线性属性^[10]。本文提出了一种基于随机 FrMT 的非线性图像加密算法。利用线性同余伪随机序列发生器^[11] (Linear Congruential Generator, LCG) 参数的敏感性, 生成实对称随机矩阵随机化离散 FrFT 的核矩阵^[12]。在保持 FrMT 非线性属性的基础上, 与 FrMT 相比, 随机 FrMT 的密钥灵敏度大幅改善。对于实值的输入图像, 本算法输出密文是实值图像, 便于密文的存储与传输。算法的密钥为 FrMT 的分数阶和 LCG 的 3 个参数, LCG 参数增大了算法的密钥空间。数值模拟验证了该加密算法的可行性和有效性。

1 图像加密算法

1.1 分数梅林变换

二维函数 $f(x, y)$ 的分数梅林变换定义为:

$$\text{FrMT}^{(p_1, p_2)}(u, v) = C \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(x, y) x^{-\left(\frac{2\pi i u}{\sin \theta_1} + 1\right)} y^{-\left(\frac{2\pi i v}{\sin \theta_2} + 1\right)} \times \exp \left[\frac{i\pi(u^2 + \ln^2 x)}{\tan \theta_1} + \frac{i\pi(v^2 + \ln^2 y)}{\tan \theta_2} \right] dx dy \quad (1)$$

其中: C 为常数, p_1, p_2 分别为 x, y 方向的变换阶次, $\theta_1 = \frac{p_1 \pi}{2}$

收稿日期: 2013-04-07; 修回日期: 2013-06-09。 基金项目: 国家自然科学基金资助项目 (61262084, 61141007, 61162014, 61210306074)。

作者简介: 张文全 (1969-), 男, 江西南昌人, 实验师, 硕士, 主要研究方向: 图像加密; 张烨 (1965-), 男, 河南洛阳人, 副教授, 博士, 主要研究方向: 信号处理; 周南润 (1976-), 男, 江西吉安人, 教授, 博士, 主要研究方向: 网络与信息安全。

和 $\theta_2 = \frac{p_2 \pi}{2}$ 。分数梅林变换的一种快速实现方法是先将 $f(x, y)$ 由笛卡尔坐标系转换到对数—极坐标中, 再对转换结果实施 FrFT, 即:

$$\text{FrMT}^{(p_1, p_2)}(u, v) = \text{FrFT}^{(p_1, p_2)}(f(\rho, \theta)) \quad (2)$$

对数—极坐标变换定义如下:

$$\begin{cases} \rho = \ln \sqrt{x^2 + y^2} \\ \theta = \tan^{-1} \frac{y}{x} \end{cases} \quad (3)$$

对数—极坐标变换决定了分数梅林变换具有非线性属性。

1.2 数字图像加密过程

根据式(2)的类推, FrMT 的实现可在离散分数傅里叶变换 (Discrete Fractional Transform, DFrFT) 的基础上得到, 即 $\text{FrMT}[f(x, y)] = \text{DFrFT}[f(\rho, \theta)]$ 。图像的加密和解密过程如图1所示。

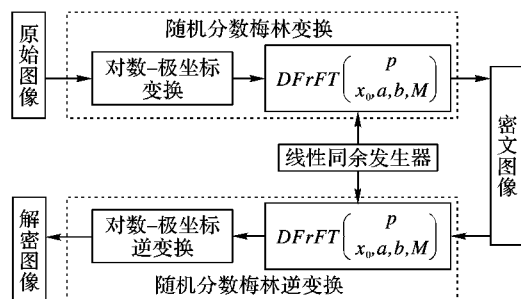


图1 随机分数梅林变换加密/解密示意图

待加密的二维数字图像 A 的 DFrFT 的矩阵形式为

$$\text{DFrFT}^p[A] = H^p A (H^p)^T \quad (4)$$

其中: T 表示矩阵转置, p 是 DFrFT 的分数阶。变换核矩阵 H^p 为

$$H^p = V D^p V^T \quad (5)$$

其中: V 为本征向量矩阵, D^p 为 DFrFT 本征值的对角矩阵, D^p 中的 N 个值为: $\{\exp(-2i\pi np/t) \mid (n = 0, 1, 2, \dots, N-1)\}$, 这里 t 是 DFrFT 的周期, N 是自然整数。

引入 LCG 随机化本征向量 V , 即随机化了 DFrFT 的核矩阵 H^p , LCG 的递推关系为:

$$r_n = x_n/M; x_n = (ax_{n-1} + b) \bmod M \quad (6)$$

其中: $n=1, 2, \dots$; 模数 M 为大的正整数。初值 $x_0 (0 \leq x_0 < M)$, 乘数 $a (0 \leq a < M)$ 和增量 $b (0 \leq b < M)$ 为 LCG 的 3 个参数。利用 LCG 生成的伪随机序列 r_n 重构一个 2 维随机矩阵 R , 并通过计算得到一个实数对称矩阵 S :

$$S = (R + R^T)/2 \quad (7)$$

数值计算矩阵 S 的归一化本征向量, 得到实数的本征向量矩阵 V , S 是对称的随机矩阵, 由它计算得到的本征向量矩阵相互正交, 且具有随机性。矩阵 S 与 H^p 满足乘积交换关系 $H^p S = S H^p$, 它们具有相同的本征向量; 随机化的 V 作为 DFrFT 的本征向量矩阵, 也即随机化了 DFrFT 的核矩阵, 从而得到随机 FrFT。随机 FrFT 有 FrFT 良好的数学性质, 且具有变换谱能量均匀分布和半周期实数化的特点, 这对图像加密来说十分有益。

原始图像通过由对数—极坐标变换和随机 FrFT 构造的随机 FrMT, 完成图像像素值和位置的双重加密, 得到类白噪声的密文, 分数阶 p 和 LCG 的参数 (x_0, a, b) 作为加密算法的密钥。对于实值输入信号, 随机分数傅里叶变换的输出结果

是实值的, 可节省密文的存储空间, 减轻传输负担。密文的解密过程通过随机 FrMT 的逆变换完成。

2 加密算法统计分析

模拟中分数阶 $p = 0.5$, 线性同余函数的参数 $x_0 = 100, a = 16807, b = 7, M = 2^{31} - 1$ 。图2(a)为 255×255 的原始图像 Lena, 图2(b)为加密结果, 是类似于噪声图像的实值信息, 利于密文存储与传输。图2(c)为 Lena 的直方图, 图2(d)是密文的直方图, 相比原图的直方图明显变平滑了, 密码分析者难以通过统计特性获得原始图像的特征。

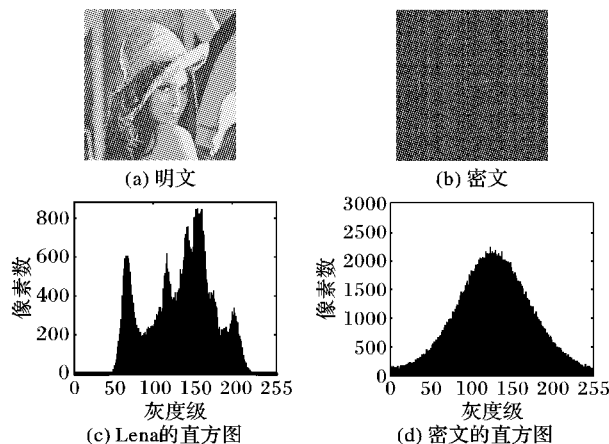


图2 明文 Lena 加密统计分析

为了说明加密算法符合经典密码理论中的混淆与扩散思想, 在密钥相同的条件下, 用本算法加密图3(a)所示的图像 Baboon, 图3(b)为其直方图, 与 Lena 的直方图明显不同, 统计特性完全不同。密文直方图如图3(c), 与图2(d)相比, 对不同统计特性图像加密获得的密文具有相类似的直方图, 加密算法可有效抵抗统计分析攻击。

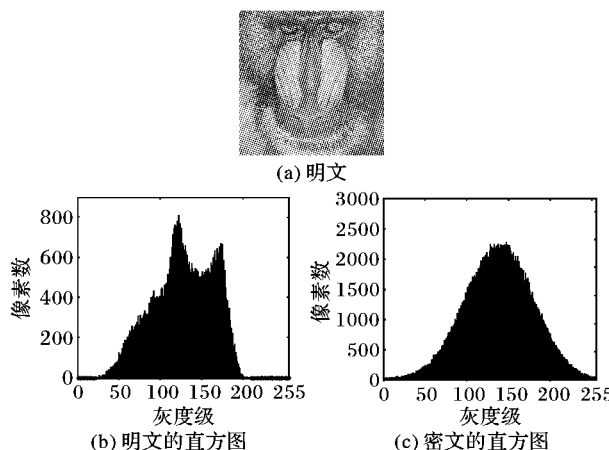


图3 图像 Baboon 加密统计分析

相邻像素的相关性反映像素的扩散程度, 原始图像的水平、垂直和对角方向的相邻像素具有很高的相关性, 安全的加密算法得到的密文相邻像素相关性要尽可能小。表1给出了明文和密文图像在水平、垂直和对角线方向上相邻像素的相关系数。

表1 Lena 图像明文和密文相邻像素的相关系数

方向	明文	密文
水平方向	0.985	0.315
垂直方向	0.921	0.119
对角方向	0.898	0.015

图 4(a)和 4(b)分别为明文和密文在水平方向上相邻像素的相关性分布图。从相关系数表和相关性分布图可知,密文的相关性显著弱于原图的相关性,无法通过相关性分析由少量图像信息恢复明文。

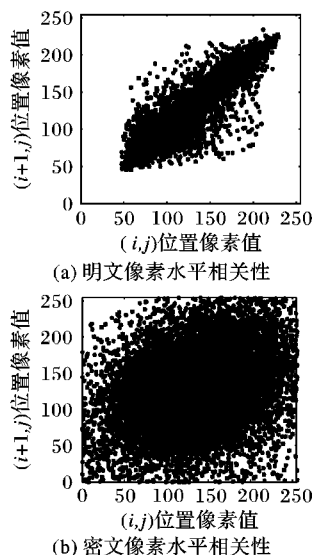


图 4 Lena 图像水平方向上相邻像素的相关性分布布

3 加密算法安全性分析

算法的密钥为 DFrMT 的分数阶和 LCG 的 3 个参数,所有密钥正确时,解密的结果如图 5(a)所示。衡量解密图像和原始图像的相似程度一般采用均方误差 (Mean Square Error, MSE), $MSE = 3000$ 作为阈值,当均方误差低于此阈值时,几乎可以恢复原始图像。均方误差定义为:

$$MSE(h_1, h_2) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N |h_2(i, j) - h_1(i, j)|^2 \quad (8)$$

其中: $M \times N$ 为图像的大小, $h_1(i, j)$ 和 $h_2(i, j)$ 分别代表原图和解密图像的灰度值。

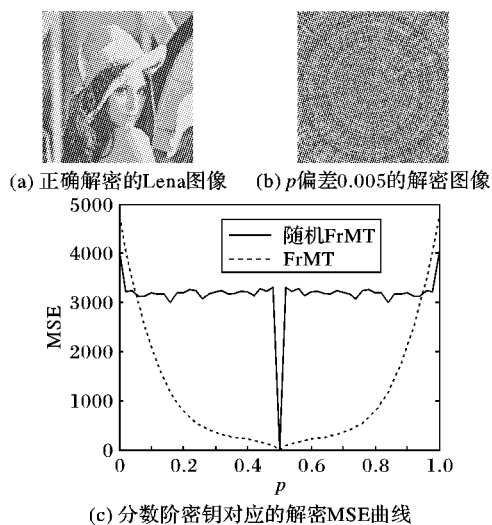


图 5 分数阶密钥安全性分析

图 5(c) 对应 FrMT 和随机 FrMT 计算了分数阶密钥的 MSE,进行了灵敏度对比。当分数阶没有偏差,即 $p = 0.5$ 时, MSE 值为 0。常规 FrMT 的 MSE 曲线 $p = 0.1$ 或 $p = 0.9$ 时,对应的 MSE 值才达到阈值,分数阶灵敏度不高,只能作为辅助密钥,还需设计主密钥达到加密所需的安全指标。随机 FrMT 在 p 有微小偏差时, MSE 曲线迅速上升到 3000 以上。图

5(b) 是 $p = 0.505$ 时对应的解密图像,有相当强的噪声。随机化后 FrMT 的分数阶密钥灵敏度大幅提高,密钥空间巨大,穷举攻击很难成功,完全可以作为加密算法的主要密钥。

为了说明 LCG 参数密钥的安全性,引入偏差量 Δ , 图 6(a)、(b)和(c)表示 3 个参数 x_0 , a 和 b 分别偏差 $\Delta = 1$ 时对应的解密图像, LCG 参数作为密钥的 MSE 曲线如图 6(d)所示,由图可知,任何一个 LCG 参数的偏差量 $|\Delta| \geq 1$ 时, $MSE > 3000$, 3 个参数作为密钥具有几乎相同的高灵敏度,拥有巨大的密钥空间,能有效抵抗穷举攻击。

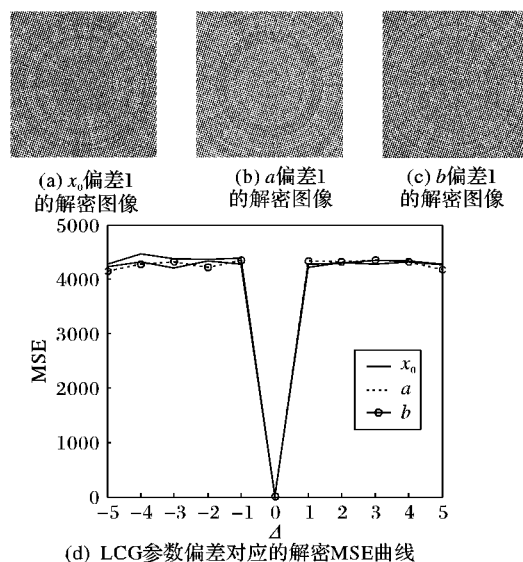


图 6 LCG 参数密钥安全性分析

图像处理和传输过程中会有噪声的影响,所以算法抵抗噪声的鲁棒性很重要。将均值为 0, 方差为 0.1 的高斯噪声 G 加入密文 E , 噪声干扰后加密图像振幅为 E' , 表示为:

$$E' = E(1 + kG) \quad (9)$$

其中 k 是噪声强度的系数。对应 k 的变化,解密图像的 MSE 变化如图 7 所示,高斯噪声强度 $k = 0.5$ 和 $k = 1$ 时,攻击后的解密图像 MSE 值分别为 400 和 1200,两者的值远小于阈值,表明加密算法具有良好的抗噪声攻击能力。

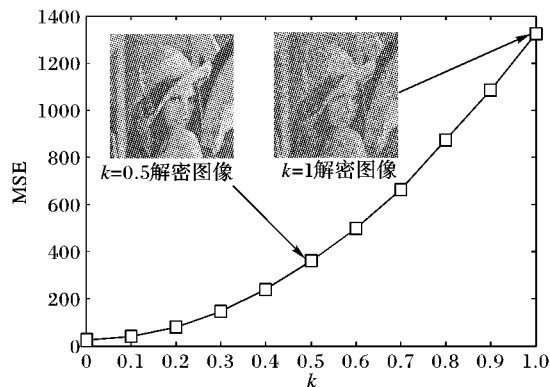


图 7 噪声强度系数 k 的取值在 $[0, 1]$ 内变化时的 MSE 曲线

4 结语

本文基于随机分数梅林变换设计了一种非线性图像加密算法,加密系统满足密码学的混淆和扩散的原则,具有很好的去相关效果。由于随机分数梅林变换的非线性属性,使得加密算法的明文、密文、密钥之间不满足线性关系,攻击者无法对加密系统实施各类已知的基于明文密文对的攻击方法。加

(下转第 2894 页)

结果正好相吻合。

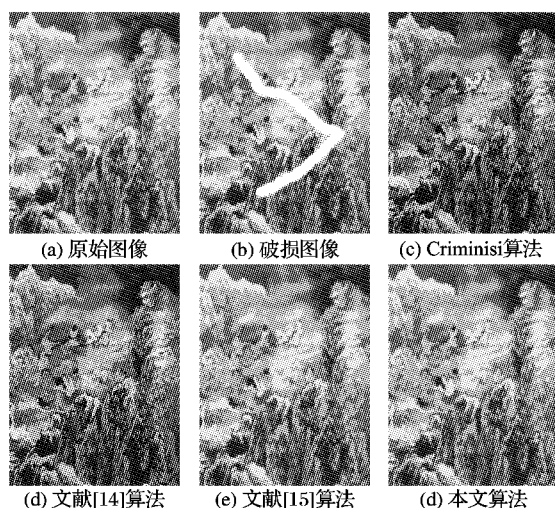


图7 各算法图像修复效果比较三

4 结语

在基于纹理的图像修复算法中,针对模板块尺寸固定的问题,本文提出了基于自适应模板的图像修复算法。该算法根据当前模板块与尺寸扩大后模板块间灰度均值及方差的变化情况来自适应地扩大模板尺寸;同时,根据模板块与样本块之间的匹配情况来自适应地缩小模板块。在自适应确定模板块尺寸的基础上,本文对基于纹理的图像修复算法进行改进并用于实例验证,其结果表明,本文提出的算法在提高图像修复精度的同时,提高了图像修复的效率。

参考文献:

- [1] 张红英,彭启琮. 数字图像修复技术综述[J]. 中国图象图形学报, 2007, 12(1): 1-10.
- [2] 张晴,林家骏. 纹理分布分析的快速图像修复算法[J]. 中国图象图形学报, 2012, 17(1): 0123-0129.
- [3] 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.
- [4] BERTAMLIO M, SAPIRO G, CASELLES V, *et al.* Image inpainting [C]// SIGGRAPH 2000: Proceedings of the 27th Annual Conference on Computer Graphics and Interactive Techniques. New

York: ACM Press, 2000: 417-424.

- [5] CHAN T, SHEN J. Mathematical models for local non-texture inpaintings [J]. SIAM Journal on Applied Mathematics, 2001, 62(3): 1019-1043.
- [6] CRIMINISI A, PEREZ P, TOYAMA K. Region filling and object removal by exemplar-based image inpainting[J]. IEEE Transactions on Image Processing, 2004, 13(9): 1200-1212.
- [7] WU J, RUAN Q. Object removal by cross isophotes exemplar-based inpainting [C]// Proceedings of the 18th International Conference on Pattern Recognition. Washington, DC: IEEE Computer Society, 2006, 3: 810-813.
- [8] 陈卿,王慧琴,吴萌. 基于纹理特征的自适应图像修复算法[J]. 计算机应用, 2011, 31(6): 1572-1574.
- [9] GROVER S, MITTAL A, GUPTA S, *et al.* A unified approach for digital image inpainting using bounded search space [J]. International Journal on Graphics, Vision and Image Processing, 2005, 5(6): 17-24.
- [10] WONG A, ORCHARD J. A nonlocal-means approach to exemplar-based inpainting[C]// ICIP 2008: Proceedings of 15th IEEE International Conference on Image Processing. Piscataway, NJ: IEEE Press, 2008: 2600-2603.
- [11] KOMODAKIS N, TZIRTAS G. Image completion using efficient belief propagation via priority scheduling and dynamic pruning [J]. IEEE Transactions on Image Processing, 2007, 16(11): 2649-2661.
- [12] 葛仕明,程义民,潘浩,等. 基于离散优化的图像修复[J]. 中国科学技术大学学报, 2008, 38(12): 1381-1385.
- [13] KWATRA V, ESSA I, BOBICK A, *et al.* Texture optimization for example-based synthesis [J]. ACM Transactions on Graphics, 2005, 24(3): 795-802.
- [14] ZHOU H L, ZHENG J M. Adaptive patch size determination for patch-based image completion[C]// Proceedings of the 17th IEEE International Conference on Image Processing. Piscataway, NJ: IEEE Press, 2010: 421-424.
- [15] 孟春芝,何凯,焦青兰. 自适应样本块大小的图像修复方法[J]. 中国图象图形学报, 2012, 17(3): 337-341.
- [16] 彭坤杨,董兰芳. 一种基于图像平均灰度值的快速图像修复算法[J]. 中国图象图形学报, 2010, 15(1): 50-55.

(上接第2867页)

密算法获得的加密结果为实值密文,分数阶密钥和线性同余参数密钥具有很高的灵敏度。仿真分析说明了加密算法可抵抗统计分析攻击和噪声攻击。

参考文献:

- [1] PEI S C, HSUE W L. Random discrete fractional Fourier transform [J]. IEEE Signal Processing Letters, 2009, 16(12): 1015-1018.
- [2] GUO Q, LIU Z J, LIU S T. Color image encryption by using Arnold and discrete fractional random transforms in IHS space[J]. Optics and Lasers in Engineering, 2010, 48(12): 1174-1181.
- [3] SINGH N, SINHA A. Chaos based multiple image encryption using multiple canonical transforms [J]. Optics & Laser Technology, 2010, 42(5): 724-731.
- [4] LI X X, ZHAO D M. Optical color image encryption with redefined fractional Hartley transform[J]. Optik, 2010, 121(7): 673-677.
- [5] LANG J, TAO R, WANG Y. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function [J]. Optics Communications, 2010, 283(10): 2092-2096.
- [6] BHATNAGAR G, WU Q M, RAMAN B. Discrete fractional wavelet transform and its application to multiple encryption[J]. Information

Sciences, 2013, 223: 297-316.

- [7] JOSHI M, SHAKHER C, SINGH K. Logarithms-based RGB image encryption in the fractional Fourier domain: A non-linear approach [J]. Optics and Lasers in Engineering, 2009, 47(6): 721-727.
- [8] WANG X G, ZHAO D M. Multiple-image encryption based on non-linear amplitude-truncation and phase-truncation in Fourier domain [J]. Optics Communications, 2011, 284(1): 148-152.
- [9] DENG X P, ZHAO D M. Single-channel color image encryption based on asymmetric cryptosystem [J]. Optics & Laser Technology, 2012, 44(1): 163-140.
- [10] ZHOU N R, WANG Y X, GONG L H. Novel optical image encryption scheme based on fractional Mellin transform [J]. Optics Communications, 2011, 284(12): 3234-3242.
- [11] WIKRAMARATNA R S. Theoretical and empirical convergence results for additive congruential random number generators [J]. Journal of Computational and Applied Mathematics, 2010, 233(9): 2302-2311.
- [12] 张文全,周南润. 基于离散分数随机变换的双彩色图像加密算法[J]. 电子与信息学报, 2012, 34(7): 1727-1734.