文章编号：1001-3806(2014)04-0551-05

基于分数傅里叶变换的双彩色图像加密

王 鹏[1]，袁操今[2*]，王 林[1]，李重光[1]
(1. 昆明理工大学 理学院，昆明 650500；2. 南京师范大学 物理科学与技术学院，南京 210023)

摘要：为了实现单通道双彩色图像的同时加密，首先将两幅待加密的彩色图像转换成索引图像的形式，保留索引图像的颜色映射矩阵，然后仅对数据矩阵采用复数合成、分数傅里叶变换、随机调制实现了双图像的加密。结果表明，只有在使用完全正确密钥的情况下才能恢复出两幅无失真的图像。该算法具有很高的安全性。

关键词：信息光学；彩色图像加密；分数傅里叶变换；索引图像
中图分类号：O438 **文献标志码**：A **doi**：10.7510/jgjs.issn.1001-3806.2014.04.023

Encryption and decryption for double images based on fractional Fourier transformation

WANG Peng[1], *YUAN Caojin*[2], *WANG Lin*[1], *LI Chongguang*[1]
(1. Faculty of Science, Kunming University of Science and Technology, Kunming 650500, China; 2. College of Physics Science and Technology, Nanjing Normal University, Nanjing 210023, China)

Abstract: In order to encrypt double color images in a single channel, firstly, two color images to be encrypted were converted to indexed images instead of RGB model and the color mapping matrix of the index images was reserved. Then, after the logarithm operation, fraction Fourier transformation and random modulation of the data matrix, both the images were encrypted. The theoretical analysis and experiment results indicate that two color images can be retrieved without distortion only when correct keys are used. The algorithm has high security.

Key words: information optics; color image encryption; fractional Fourier transform; indexed image

引 言

随着因特网的迅速发展，用于传输或存储的数字图像也随之大大增多。为保护图像信息，防止非授权用户盗取，需要利用信息安全技术对图像进行加密处理。在信息安全研究中，由于基于信息光学理论的加密技术具有高速、并行性好等特点，现在已经成为了信息安全技术中一个非常重要的分支[1-5]。该理论首先由 JAVIDI 提出，该课题组利用 4*f* 成像系统和双随机相位编码技术[6]，对灰度图像的空间信息和频谱信息做随机调制，从而达到加密的效果。在此基础上，研究人员相继提出了基于菲涅耳变换的加密方法[7]、基于分数傅里叶变换的加密方法[8]、纯相位加密方法[9]等。

由于彩色图像相对于灰度图像，包含更多的信息，可以描述更为丰富的内容，因此对彩色图像的加密更具有现实意义。彩色图像的加密方法众多，大致可分为多通道和单通道两大类。多通道的方法是将彩色图像分解为 *R*，*G* 和 *B* 3 个分量，分别对 3 个分量按照灰度图加密的方法进行加密[10-12]。这类方法相对比较繁琐，实现成本比较高。单通道方法则是将彩色图像转换成索引图像，或是将它的 *R*，*G*，*B* 的 3 个分量编码成 1 个灰度图像，再对它们进行双随机相位加密[13-15]。与三通道的方法相比，该类加密方法比较简单，易于实现。为提高彩色图像的加密效率，ZHANG 等人[16]提出了对两幅彩色图像同时加密的技术，该技术将两幅彩色图像分别转换成索引图像，通过将其中一幅图像的数据矩阵作为振幅，另外一幅图像的数据矩阵则作为相位掩膜，将它们在空域中融合成一幅灰度图像。在解密过程中，由于涉及到相位解包裹问题，恢复原图像经常带

基金项目：国家自然科学基金资助项目(61377003)
作者简介：王 鹏(1987-)，男，硕士研究生，现主要从事图像处理方面的研究。
*通讯联系人。E-mail：optyuan@163.com
收稿日期：2013-08-01；收到修改稿日期：2013-11-06

有误差。JOSHI 等人[17]提出将彩色图像转换成索引图像的形式,在空域中,首先利用余弦函数对随机密钥进行处理,然后使用处理后的随机密钥对数据矩阵进行调制,并以复数的形式合并组成一个复数矩阵。在变换域,该复数矩阵被随机相位掩膜调制,最终实现双彩色图像的同时加密。由于余弦函数具有周期性,因此解密密钥并不是唯一的,降低了加密的安全性。

本文中提出了一种基于分数傅里叶变换的单通道双彩色图像加密方法。将待加密的两幅彩色图像转换成索引图像,在加密过程,对这两索引图像对应的数据矩阵取以随机数组为底的对数,并将得到的两个结果构成一个复数矩阵,再对这个复数矩阵进行第 1 次分数傅里叶变换。然后使用随机相位密钥在变换域中进行调制,调制的结果再进行第 2 次分数傅里叶变换,最终实现了双彩色图像的同时加密。在加密过程中,图像在空域不是受到随机相位掩膜的调制,而是对图像取以随机数组为底的对数,不仅实现了对图像的置乱,而且空域中的随机矩阵也实现了加密的作用。同时该算法能够对两幅彩色图像同时加密,相对于只能对一幅彩色图像加密来说,加密的效率更高。实验也证明了该方法具有很好的加密效果。

1 图像加密及解密原理

1.1 索引图像与三原色图像

三原色图像(red,green,blue,RGB)图像可以分解为红(R)、绿(G)和蓝(B)3 个分量,图像的每个像素点都是用这 3 个分量对应的强度值来描述,如图 1a 所示,右上角方框中的某个像素的 3 个分量的强度值分别是 69,74 和 45。因此,一个 $M\times N$ 大小的图像,若利用 RGB 模型表示,图像矩阵大小就为 $M\times N\times 3$,这不仅大大占用了计算机存储空间,而且分别对 3 层图像进行加密处理,也会使计算量增大。

索引图像则只由两个矩阵构成,分别是颜色映射矩阵和数据矩阵。颜色映射矩阵是 1 个 $m\times 3$ 的矩阵,m 的值取决于调色板的大小(最大为 256),颜色映射矩阵每行的 3 个值分别表示红、绿、蓝 3 个分量的值。数据矩阵则是 1 个 $M\times N$ 的 2 维矩阵。数据矩阵的作用类似于“指针”,指向颜色映射矩阵,如图 1b 所示,同样也是右上角的 1 个像素,在数据矩阵中对应“186”,与颜色映射矩阵中的 3 个数对应。由于整幅图像共用 1 个颜色矩阵,就不需要再

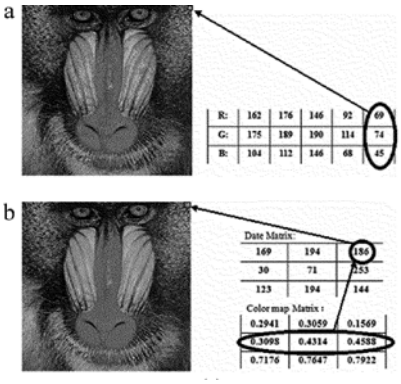

Fig. 1 The difference between the colored image and indexed image
a—typical representation of a colored image b—typical representation of an indexed image

利用一个 3 维数组来描述图像。比起 RGB 模型,索引表示大大节省了计算机存储空间。

1.2 加密过程

加密过程的示意图如图 2a 所示。设待加密的两幅图像分别表示为 p 和 q,将这两幅彩色图像分别转换成像素点数为 $M\times N$ 的数据矩阵 $\boldsymbol{p}_1(x,y)$ 和 $\boldsymbol{q}_1(x,y)$ 以及颜色映射矩阵($\boldsymbol{M}_1$,$\boldsymbol{M}_2$)。

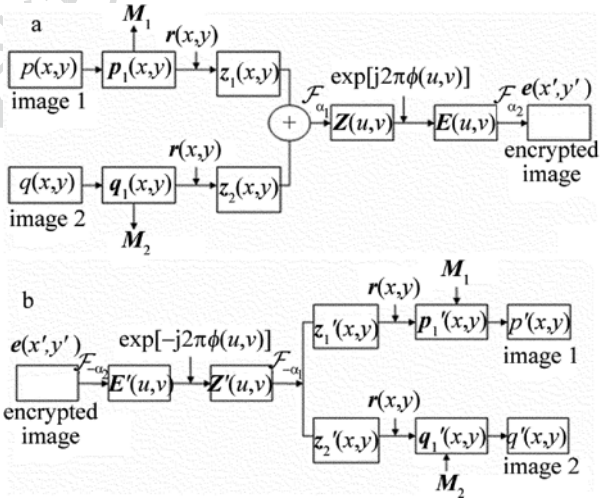

Fig. 2 The encryption and decryption process
a—the algorithm for encryption b—the algorithm for decryption

分别对数据矩阵 $\boldsymbol{p}_1(x,y)$ 和 $\boldsymbol{q}_1(x,y)$ 取以 $\boldsymbol{r}(x,y)$ 为底的对数,$\boldsymbol{r}(x,y)$ 为一个 2 维随机矩阵,其大小为 $M\times N$,得到 $z_1(x,y)$ 和 $z_2(x,y)$,数学上表示为:

$$z_1(x,y)=\log_{\boldsymbol{r}(x,y)}\boldsymbol{p}_1(x,y)=\frac{\ln[\boldsymbol{p}_1(x,y)]}{\ln[\boldsymbol{r}(x,y)]}\quad(1)$$

$$z_2(x,y)=\log_{\boldsymbol{r}(x,y)}\boldsymbol{q}_1(x,y)=\frac{\ln[\boldsymbol{q}_1(x,y)]}{\ln[\boldsymbol{r}(x,y)]}\quad(2)$$

将 $z_1(x,y)$ 和 $z_2(x,y)$ 以复数的形式合在一起,即 $z_1+\mathrm{i}z_2$,并对这个复数矩阵进行 α_1 阶的分数傅里

叶变换,将其计算结果 $\boldsymbol{Z}(u,v)=\mathscr{F}_{\alpha_1}[z_1+\mathrm{i}z_2]$($\mathscr{F}_{\alpha_1}$ 表示 α_1 分数阶的分数傅里叶变换),乘以随机相位掩膜 $\varphi(u,v)=\exp[\mathrm{j}\phi(u,v)]$,其中 $\phi(u,v)$ 为取值在 $-\pi$ 到 π 的随机分布,得到 $\boldsymbol{E}(u,v)=\boldsymbol{Z}(u,v)\times\phi(u,v)$。最后对 $\boldsymbol{E}(u,v)$ 进行 α_2 阶分数傅里叶变换,得到加密后的图像 $\boldsymbol{e}(x',y')$。

解密方法为加密过程的逆过程,其示意图如图 2b 所示。首先对加密后的图像 $\boldsymbol{e}(x',y')$ 进行 $-\alpha_2$ 阶分数傅里叶变换,再乘以相位掩膜的共轭函数 $\varphi^*(u,v)$,得到 $\boldsymbol{Z}'(u,v)$。然后,对 $\boldsymbol{Z}'(u,v)$ 进行 $-\alpha_1$ 阶分数傅里叶变换,并分离出结果的实部和虚部,得到 $z_1'(x',y')$ 和 $z_2'(x',y')$。通过 $\boldsymbol{r}(x,y)$ 可以得到数据矩阵 $\boldsymbol{p}_1'(x,y)$,$\boldsymbol{q}_1'(x,y)$,这个过程的数学表达式为:

$$\boldsymbol{p}_1'(x',y')=z_1'(x',y')\times\ln[\boldsymbol{r}(x,y)] \quad (3)$$

$$\boldsymbol{q}_1'(x',y')=z_2'(x',y')\times\ln[\boldsymbol{r}(x,y)] \quad (4)$$

最后,$\boldsymbol{p}_1'(x,y)$ 和 $\boldsymbol{q}_1'(x,y)$ 与对应的颜色映射矩阵($\boldsymbol{M}_1$,$\boldsymbol{M}_2$)可以恢复出两幅彩色图像。

为客观评价图像的解密效果,利用均方差(mean square error,MSE)来衡量原图像与解密图像的差异,其表达式为:

$$E_{\mathrm{MSE}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|f(i,j)-f_{\mathrm{d}}(i,j)|^2 \quad (5)$$

式中,$f(i,j)$ 和 $f_{\mathrm{d}}(i,j)$ 分别表示原图像和解密图像在 (i,j) 处的灰度值,$M\times N$ 表示图像的尺寸。对于彩色图像,分别计算原图像的 R,G,B 3 个分量与解密图像的 R,G,B 分量之间的均方差,并取其平均值[18],即:

$$E_{\mathrm{MSE}}=\frac{e(r)+e(g)+e(b)}{3} \quad (6)$$

式中,$e(r)$,$e(g)$,$e(b)$ 分别对应于原图像的 R,G,B 与解密图像的 R,G,B 分量之间的均方差。均方差 MSE 的值越小,说明两幅彩色图像越相似。

2 实验模拟的结果及分析

2.1 实验模拟

在计算机模拟仿真中,待加密的两幅彩色图像如图 3a 和图 3b 所示,其像素大小均为 256×256 的 24 位彩色图像。加密过程中使用的随机密钥分别为 $\boldsymbol{r}(x,y)$ 和 $\varphi(u,v)$,如图 3c 和图 3d 所示,除此之外分数阶也可以作为密钥(取 $\alpha_1=\alpha_2=1.2$),利用本文中提出的方法对图 3a 和图 3b 两幅图像加密,得到图 3e 的结果,经过加密处理后,两幅图像已经

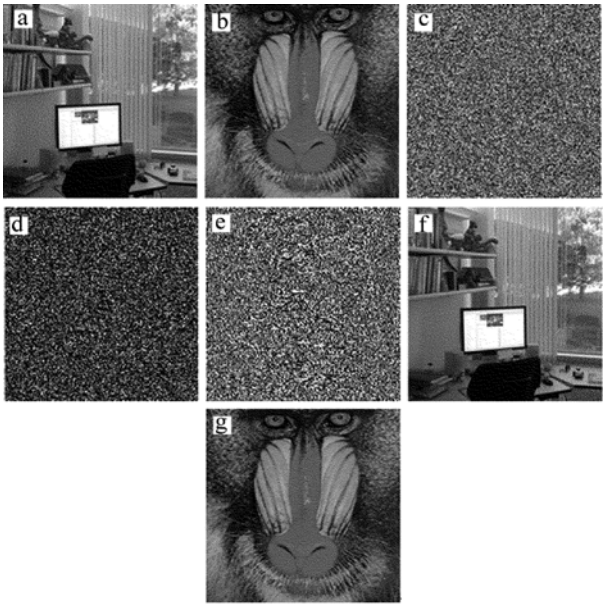

Fig. 3 a—the original color image: office b—the original color image: mandrill c—the 2-D random matrix d—the random phase mask e—encrypted image f—decrypted image of office g—decrypted image of mandrill

加密成一幅稳定的白噪声图像,完全看不出原始图像。利用解密过程,可以获得原图像,如图 3f 和图 3g 所示。从上面的结果可以看出,在视觉上无法区分原彩色图像和解密得到的彩色图像,证明了该加密(解密)算法的可行性。

利用(6)式可计算出两幅解密后的彩色图像与原始彩色图像之间的均方差分别为 4.6403×10^{-4} 和 8.3864×10^{-4}。从客观上也证明了解密出的彩色图像与原始彩色图像差异非常小,可以忽略,认为对应的两幅彩色图像相同。

为进一步验证算法的可行性,选取 100 幅不同的彩色图像作为试验样本。实验中,在试验样本中任意抽取 2 幅图像作为加密图像采用该加密算法进行加密、解密。部分试验结果(从论文篇幅考虑,只列举了两组 4 幅彩色图像的加密(解密)结果)如图 4 所示。“original images”中每组的 2 幅彩色图像作为待加密的原始图像;“encrypted image”是为使用本文中的算法对原始图像的加密结果;“decrypted images”为相应的解密图像;E_{MSE} 表示解密图像与相对应的原始图像之间的均方误差,其结果均小于 10^{-3},可以认为对应两幅图像相同,也进一步证明了该加密算法的普适性。

在相同的计算机配置下(CORE™ i5 处理器,主频 2.5GHz,2G 内存,MATLAB 软件),还模拟了在分数傅里叶变换域多通道的彩色图像加密技术[11],并

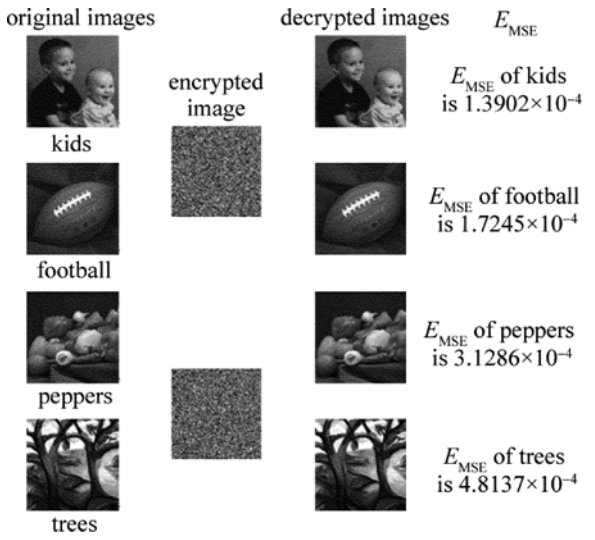

Fig. 4 A part of experimental result

比较了该技术与本文中算法对两幅彩色图像(像素大小为 256 × 256,24 位 bmp 格式)加密所需的时间,其加密时间统计结果依次为 1.967s,0.472s。从该结果看,本文中算法具有更高的加密效率。

2.2 安全分析

2.2.1 分数阶的安全性能 取分数阶在(1.15, 1.24]之间,等间隔 0.005,分别计算对应解密结果的均方差,如图 5 所示,横坐标表示分数阶的取值,纵坐标表示相应解密结果的均方差。从结果上看,仅当分数阶 $\alpha_1 = \alpha_2 = 1.2$ 时,才能正确解密出原彩色图像的信息。而且在 $\alpha_1 = \alpha_2 = 1.2$ 处曲线发生了突变,说明分数阶密钥具有很高的灵敏度,所以在未知分数阶的情况下很难解出正确的结果。

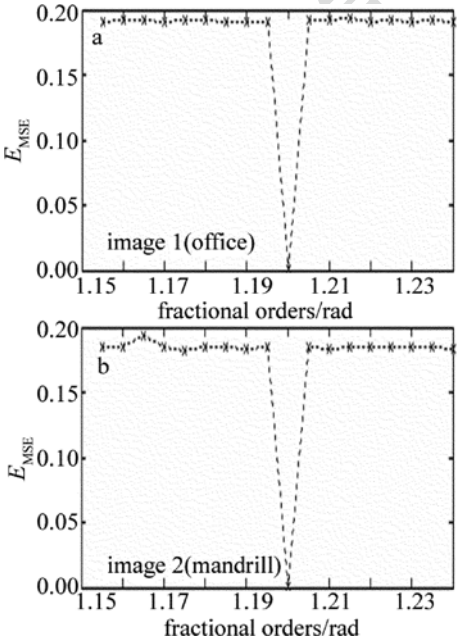

Fig. 5 MSE against variation in fractional orders

2.2.2 随机密钥的安全性能 随机密钥有 $\boldsymbol{r}(x,y)$ 和 $\varphi(u,v)$。其中若密钥 $\boldsymbol{r}(x,y)$ 部分错误的情况下,计算对应的解密图像,如图 6 所示。图 6a、图 6d 分别为错误尺寸为密钥的 1/4 和 1/8,图中黑色部分为密钥的未知或错误部分;图 6b、图 6c 以及图 6e、图 6f 分别对应于使用密钥图 6a 和图 6d 进行解密的结果(图中 E_{MSE} 表示解密图像与原图像之间的 MSE 值)。从结果来看,完全无法分辨出解密结果的图像信息,从而验证了密钥 $\boldsymbol{r}(x,y)$ 具有很高的安全性。

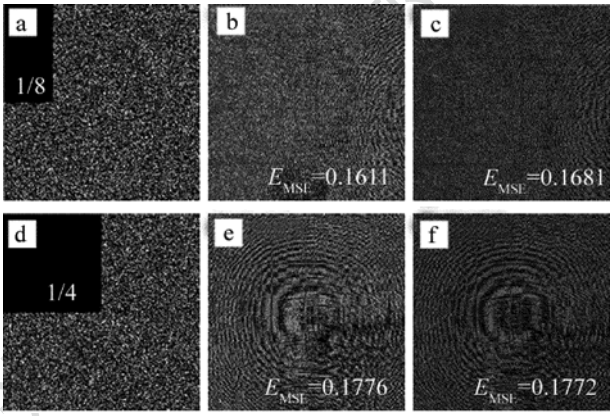

Fig. 6 Security of $\boldsymbol{r}(x,y)$

如果密钥 $\varphi(u,v)$ 部分错误的情况下,解密的结果如图 7 所示。图 7a、图 7d 分别为错误尺寸为密钥的 1/4 和 1/8;图 7b、图 7c、图 7e 和图 7f 分别对应于使用密钥图 7a 和图 7d 进行解密得到的图像。从结果来看,只能获取图像的部分信息,说明密钥 $\varphi(u,v)$ 有一定的安全性能。

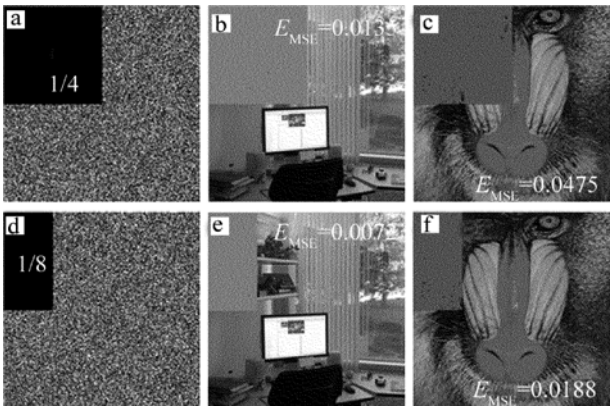

Fig. 7 Security of $\varphi(u,v)$

2.2.3 颜色映射矩阵的安全性能 颜色映射矩阵保存的是彩色图像的颜色信息,加密系统中,颜色映射矩阵也可以作为密钥。在颜色映射矩阵 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 的部分数据错误,其它密钥均正确的情况下,解

密结果如图 8 所示。图 8a 和图 8b 为 20% 的数据错误(实验中,错误数据均设为 0)时的解密结果;图 8c 和图 8d 为 10% 的数据错误时的解密结果。从结果上看,虽然能分辨出图像的基本轮廓,但是图像的颜色发生了严重的畸变,说明颜色映射矩阵有较好的安全性能。

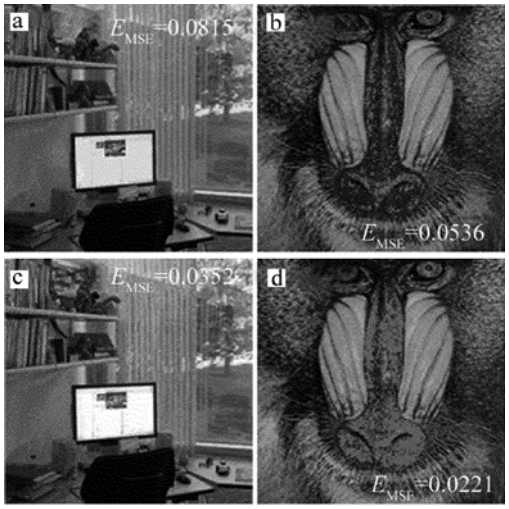

Fig. 8 Security of the color mapping matrix

3 结 论

设计了一种基于分数傅里叶变换单通道的双彩色图像的加密算法。该算法在空域中,将两幅彩色图像表示为索引图像,对相应的数据矩阵分别取以随机数组为底的对数,并将得到的两个结果组合成一个复数矩阵。这个复数矩阵在变换域受到了随机相位密钥的调制,从而实现双彩色图像的同时加密。在该算法中,无论空域中的随机数组还是变换域中的随机相位掩膜,都能很好地起到加密作用,不会因为图像为实数矩阵时,空域中的密钥无法起到加密的作用。除此之外,加密(解密)过程使用的是分数傅里叶变换,该变换的分数阶以及颜色映射矩阵也都可以作为密钥,所以该加密系统具有很好的加密性能。由于该算法对两幅彩色图像同时加密,而且加密系统并没有因此变得复杂,所以该算法对彩色图像加密的效率更高。模拟实验证明了该方法的有效性,并具有很高的安全性。

参 考 文 献

[1] LIU Z, XU L, LIN C, *et al*. Image encryption scheme by using iterative random phase encoding in gyrator transform domains[J]. Optics and Lasers in Engineering, 2011, 49(4): 542-546.

[2] DENG X P, WEN W. Binary image encryption using logic operations based on interferometer [J]. Laser Technology, 2010, 34(3): 401-404(in Chinese)

[3] ZHANG H Z, YAO M, LEI P, *et al*. Research of image processing method of far-field laser spots[J]. Laser Technology, 2013, 37(4):460-463 (in Chinese).

[4] LIN R, LIU Q N, ZHANG C L. A new fast algorithm for gyrator transform[J]. Laser Technology, 2012, 36(1):50-53(in Chinese).

[5] DING X L. Asymmetric optical image cryptosystem based on spherical wave illumination [J]. Laser Technology, 2013, 37(5): 576-581(in Chinese).

[6] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding [J]. Optics Letters, 1995, 20(7): 767-769.

[7] XIAO Y L, ZHOU X, LIU Q, *et al*. An image reconstruction method based on the double- random phase encoding system in the Fresnel domain [J]. Optics and Laser Technology,2009,41(9): 449-453.

[8] BRYAN H, JOHN T S. Fractional Fourier transform-based image encryption: phase retrieval algorithm [J]. Optics Communications, 2003, 226(3):61-80.

[9] TAN X D, OSAMU M, TSUTOMU S, *et al*. Secure optical storage that uses fully phase encryption [J]. Applied Optics, 2000, 39(35):6689-6694.

[10] CHEN L, ZHAO D. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms [J]. Optics Express, 2006, 14(19): 8552-8560.

[11] 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.

[12] JOSHI M, SINGH K. Color image encryption and decryption using fractional Fourier transform [J]. Optics Communications, 2007, 279(1): 35-42.

[13] ZHANG S, KARIM M A. Color image encryption using double random phase encoding[J]. Microwave and Optical Technology Letters, 1999, 21(5): 318-323.

[14] QIN Y, ZHENG C B. Color image encryption based on double random phase encoding [J]. Acta Photonica Sinica, 2012, 41(3):326-329(in Chinese).

[15] LI Zh L, WANG X L, ZHAI H Ch, *et al*. A method of color image single-channel encryption[J]. Acta Physica Sinica, 2009, 58(2):1053-1056(in Chinese).

[16] ZHANG W Q, ZHOU N R. Double-color image encryption based on discrete fractional random transform [J]. Journal of Electronics & Information Technology, 2012, 34(7): 1727-1734(in Chinese).

[17] JOSHI M, SINGH K. Color image encryption and decryption for twin images in fractional Fourier domain [J]. Optics Communications, 2008, 281(23): 5713-5720.

[18] SUI L Sh, GAO B. Color image encryption based on gyrator transform and arnold transform [J]. Optics & Laser Technology, 2013, 48: 530-538.