doi:10.3969/j.issn.1672-1292.2016.01.013

基于交叠成像技术的彩色图像加密算法研究

韩庭晶,王 亮,袁操今,聂守平,冯少彤,姚丽莉,姜志俊,周 意,强俊杰

(南京师范大学江苏省光电技术重点实验室,江苏 南京 210023)

[摘要] 本文研究了基于交叠成像技术的彩色图像加密算法,利用正弦组合光栅将彩色图像编码为灰度图像,结合交叠成像技术与双随机相位加密技术对图像进行加密,从而实现彩色图像的加密.该加密系统不仅扩大了密钥的空间,提升了系统的安全性,而且具有较强的抗剪切和抗噪声能力.该加密系统实验装置简单,实用性较强.模拟的实验结果验证了该系统的有效性.

[关键词] 交叠成像,双随机相位,彩色图像

[中图分类号]TP391.9 [文献标志码]A [文章编号]1672-1292(2016)01-0076-08

Color Image Encryption Algorithm Based on Ptychography Technology

Han Tingjing,Wang Liang,Yuan Caojin,Nie Shouping,Feng Shaotong,
Yao Lili,Jiang Zhijun,Zhou Yi,Qiang Junjie

(Key Laboratory for Opto-Electronic Technology of Jiangsu Province,Nanjing Normal University,Nanjing 210023,China)

Abstract: Color image encryption algorithm based on ptychography technology is researched in this paper. In order to encrypt the color image, we use sinusoidal combinational grating to encode color image into gray image, and then the gray image is encrypted by ptychography and double random phase encoding. The encryption system not only enlarges the key spaces and enhances system security, but also the resistance of shear and noise performance are strong. The encryption system is simpler and more practical. The simulation proves the validity of the encryption system.

Key words: ptychography, double random phase, color image

交叠成像是在远场衍射下利用空间局域的平行照明光对待测物体进行二维扫描,并用CCD记录一系列衍射强度图,通过迭代运算,最终快速稳定地恢复物体的振幅和相位信息的一项技术[1-4],该技术在2004年由英国谢菲尔德大学的Rodenburg教授提出.它不依赖高质量高品质的透镜,避免了透镜像差对系统分辨力的影响,理论上突破了瑞利判据下的分辨率限制,可以达到光学衍射极限.此外,它还具有收敛速度快、成像视场大等优点.目前该技术已成功应用在超分辨成像[5]、三维物体成像[6]、光学测量[7]、图像处理[8]等领域.在图像加密领域中,以光信息处理为核心的光学图像加密系统具有高并行性、高速率、高存储等特点,越来越受到国内外专家的关注.最经典的光学图像加密算法是Refregier和Javidi提出的双随机相位光学加密方法[9],但加密后的结果为复振幅形式.近年来,Chen[10]等人提出了基于多光束干涉和矢量合成实现图像的加密,Li Jun[11]等人提出了二步正交相移数字全息方法对图像加密,这些方法虽然克服了加密结果为复振幅形式,但采用的光学干涉系统对装置的稳定性要求非常高,给记录带来了严重不便.Chen W[12]等人提出了基于衍射成像的加密系统,王志鹏[13]等人提出了基于相位恢复算法的单强度记录光学加密系统,这类基于衍射的装置系统避免了干涉装置稳定性的问题,将衍射强度作为密文,系统的安全性也进一步提高.以上是关于灰度图像的加密算法.在彩色图像的加密中,Zhao D M[14-15]等人提出了基于波分复用和无透镜菲涅尔变换全息的光学彩色图像加密技术,Abuturab M R[16]等人提出了基于

收稿日期:2015-08-02.

基金项目:国家自然科学基金(61377003、61275133)、南京师范大学高层次人才科研启动项目(184080H20162)、南京师范大学青年领军人才培养项目(184080H20178).

通讯联系人:袁操今,博士,副教授,研究方向:光学工程.E-mail: optyuan@163.com

Hartly 和 Gyrator 域变换的彩色图像加密技术,这类加密方法都是采用对彩色图像的 3 个分量分别加密的方法来实现彩色图像的加密,实验系统较复杂,增加了实验成本 . 杨晓萍[17]等人提出了基于双相位编码的单通道彩色图像加密方法,周南润[18]等人提出了三相位编码的单通道彩色图像加密方法,这类方法将彩色图像的 3 个通道转化为单通道处理,加密密钥有限,得到的密文易被破解 . 最近,史祎诗[19-20]等人将交叠成像技术应用于图像加密领域,但仅局限于研究灰度图像 . 然而,生活中大多物体都呈现彩色,且彩色图像将不同的色彩和亮度组合起来包含丰富的信息,因此彩色图像的加密已成为信息安全领域重要的研究分支 .

针对彩色图像加密问题,本文首先利用正弦组合光栅将一幅彩色图像的三通道编码[21-22]成一个通道,得到一幅灰度图像,然后引入交叠成像技术和双随机相位加密技术对其编码加密,从而实现了彩色图像的加密 . 同时,本文还对加密图像进行剪切攻击和噪声攻击模拟实验,模拟实验结果表明该加密系统具有较强的鲁棒性 . 该加密系统不仅扩大了密钥的空间,提升了系统的安全性,而且具有较强的抗剪切和抗噪声能力,实验装置简单,实用性较强 . 模拟的实验结果验证了该系统的有效性 .

1　基本原理

利用正弦组合光栅对彩色图像进行调制,调制后的灰度图像即后续待加密图像,它包含了原彩色图像的红、绿、蓝信息 . 加密系统光路如图 1 所示,其中 P_i 表示第 i 个局域平行照明光的复振幅分布,M_1 和 M_2 为随机相位板,FL_1 和 FL_2 为傅里叶变换透镜,$T(x,y)$ 表示待加密图像,CCD 为电荷耦合元件,PC 为计算机 .

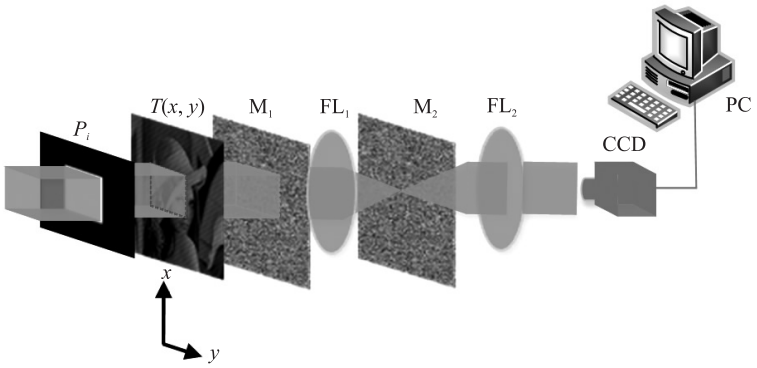


图 1　加密系统光路图

Fig.1　Schematic of optical image encryption system

在加密过程中,经过方孔后形成的空间局域平行光以固定的步长对灰度图像进行二维扫描,即灰度图像函数和方孔函数相乘,然后与一个随机相位板作用进行傅里叶变换,得到在频谱平面上的频谱,再将其与另一个随机相位板作用进行傅里叶变换,用 CCD 记录在衍射平面上的衍射斑,继续以一定的步长移动方孔,重复上述过程,用 CCD 依次记录在衍射平面上的一系列衍射斑,最终将灰度图加密成一系列稳定的白噪声图像 . 扫描时应保证灰度图像的相邻扫描部分有一定面积的重叠,这种重叠[23-24]不仅可以提高成像恢复质量,还可提高收敛速度,排除不必要的误差,对交叠成像技术起关键作用 . 上述加密过程可表示为:

$$ID_i=\left|F\left\{F\left\{P_i\cdot T(x,y)\cdot\exp\left[\mathrm{j}M_1\right]\right\}\cdot\exp\left[\mathrm{j}M_2\right]\right\}\right|^2\quad(i=1,2,3\cdots).\tag{1}$$

其中,算符 F 表示傅里叶变换 .

假设灰度图像 $T(x,y)$ 为随机分布函数 $T_{g,1}(x,y)$,则可按图 2 流程实现解密:

计算出第 i 个局域平行照明光照明随机分布函数 $T_{g,i}(x,y)$ 后在输出平面上的复振幅 $\Psi_{i,g}(x,y)$. 该过程可表示为:

$$\Psi_{i,g}(x,y)=F\left\{F\left\{P_i\cdot T_{i,g}(x,y)\cdot\exp\left[\mathrm{j}M_1\right]\right\}\cdot\exp\left[\mathrm{j}M_2\right]\right\}\quad(i=1,2,3\cdots).\tag{2}$$

将复振幅 $\Psi_{i,g}(x,y)$ 的振幅用加密图 ID_i 替换,相位保留不变,得到新的复振幅 $\Psi_{i,c}(x,y)$,可表示为:

$$\Psi_{i,c}(x,y)=\left[ID_i\right]^{1/2}\cdot\left[\Psi_{i,g}(x,y)/\Psi_{i,g}(x,y)\right]\quad(i=1,2,3\cdots).\ (3)$$

将新的复振幅 $\Psi_{i,c}(x,y)$ 逆傅里叶变换到输入图像平面上,得到复函数 $T_{i,g,N}$,表示为:

$$T_{i,g,N}=F^{-1}\left\{F^{-1}\left\{\Psi_{i,c}(x,y)\right\}\cdot\exp\left[-\mathrm{j}M_2\right]\right\}\cdot\exp\left[-\mathrm{j}M_1\right]\quad(i=1,2,3\cdots).\ (4)$$

其中,F^{-1}表示逆傅里叶变化.

对复函数 $T_{i,g,N}$ 进行更新,得到一次迭代后的分布函数,表示为:

$$T_{g,(i+1)}=T_{g,i}+\chi P_i\left(T_{i,g,N}-T_{g,i}\cdot P_i\right)/(P_i^2+\sigma)\quad(i=1,2,3\cdots),\ (5)$$

其中,σ 为常数,为了避免出现分母为 0 的无意义情况;χ 是一个反馈参数,一般取值为 0.5~1.

逐次移动局域平行光,并将上一个循环中更新后的样品分布函数 $T_{g,(i+1)}$ 作为下一个循环样品分布函数的初始值 $T_{g,i}$,当相对误差值($\mathrm{Error}=\dfrac{\sum\left[\left|T'(x,y)\right|-\left|T(x,y)\right|\right]^2}{\sum\left|T(x,y)\right|^2}$,其中,$T(x,y)$ 为原图像,$T'(x,y)$ 为解密图像)达到某一值后退出循环,得到解密后的图像 $T'(x,y)$.

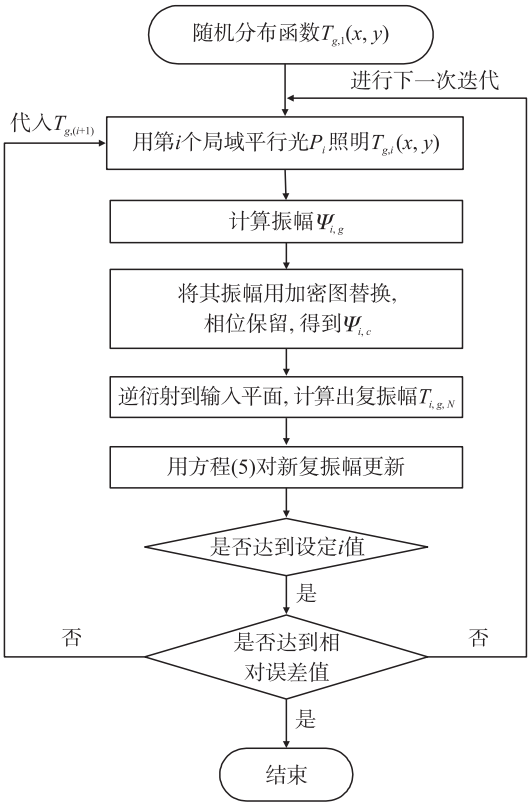


图2　解密算法流程图

Fig.2　Flow chart of optical image decryption

由于双随机相位板中的两个相位因子是随机的,且该系统中方孔的大小、移动步长都可作为加密的密钥,提升了系统的安全性.将解密后得到的图像 $T'(x,y)$ 作为输入图像,首先对图像 $T'(x,y)$ 进行傅里叶变换后会得到图像的多个级频谱,然后将空间滤波器放置在图像 $T'(x,y)$ 对应的一级频谱上,再进行反向傅里叶变换,最后恢复出彩色图像 $f'(x,y)$.

2　模拟结果及分析

利用上述方法对彩色图像进行模拟,图 3(a)为输入的一幅大小为 512×512 像素的彩色图像,图 3(b)为经过正弦组合光栅调制后得到的灰度图像.

(a) 彩色原图　　(b) 正弦组合光栅调制图像

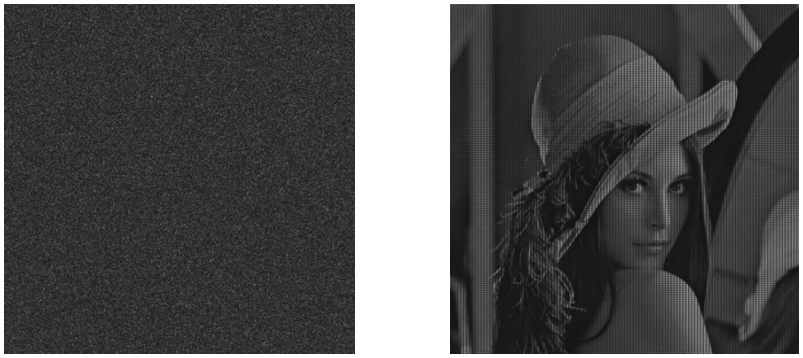
图3　彩色原图及正弦组合光栅调制图像

Fig.3　Original color image and the modulated image with sinusoidal combinatorial grating

通过交叠成像技术和双随机相位加密技术对灰度图像加密,图 4(a)为交叠成像中所需移动的方孔,其大小为 256 像素×256 像素,图 4(b)为局域平行光以步长为 128 像素移动 2×2 个矩阵位置对应的照明区域,相邻两个方孔的重叠率为 50%(本文移动 3×3 个矩阵位置). 图 4(c)为对灰度图像扫描后得到的其中一幅加密图像.将孔的大小、扫描步长作为密钥,用正确的密钥即大小为 256 像素、扫描步长为 128 像

素的方孔对图像解密后得到解密图如图 4(d)所示 .

(a) 方孔　(b) 扫描区域



(c) 加密图　(d) 用正确的密钥所得解密图

图 4　方孔、扫描区域、加密图及用正确的密钥所得解密图

Fig.4　The square probe, the scanned area, the encryption image and decryption image with right keys

对解密后的灰度图像进行傅里叶变换,利用它的一级频谱来解码操作,解码后的彩色图像如图 5(a)所示 . 利用一级频谱解码得到的彩色图像基本恢复了原来彩色图像的颜色特征,用均方差(MSE)来评价彩色图像恢复质量的标准,均方差的定义为:

$$\mathrm{MSE}=\frac{1}{3\times M\times N}\sum_{c\in\{\mathrm{R,G,B}\}}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\mathrm{image}_c(x,y)-\tilde{\mathrm{image}}_c(x,y)\right|^2, \tag{6}$$

其中, $M\times N$ 为图像的大小, $c\in\{\mathrm{R,G,B}\}$ 为彩色图像的红绿蓝通道, $\mathrm{image}_c(x,y)$ 表示彩色原图像, $\tilde{\mathrm{image}}_c(x,y)$ 表示恢复后的彩色图像 .MSE 越接近于 0,表明恢复图像质量越高 . 模拟结果表明,一级频谱解码后的彩色图像 MSE 为 0.014 0.

(a) 一级频谱解码后的彩色图像　(b) 融合零级频谱解码后的彩色图像

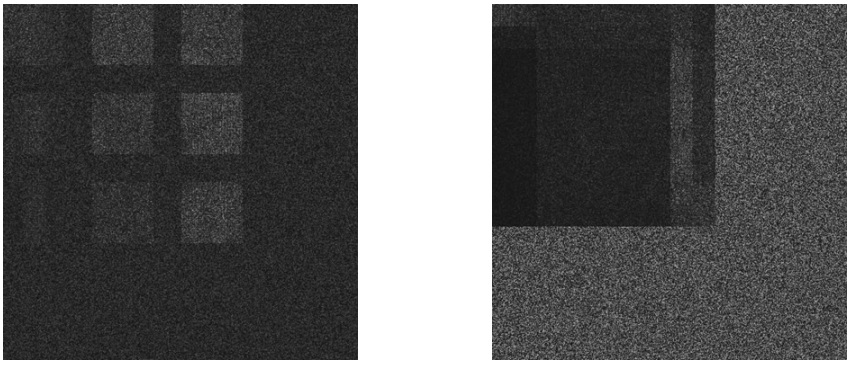
图 5　一级频谱解码及融合零级频谱解码后的彩色图像

Fig.5　The color image of one-order spectrum decoding and fusing zero-order spectrum decoding

从视觉效果上,跟原图相比,亮度降低,空间分辨率也降低,原因是图像的高频信息以及零级频谱中包含有原来彩色图像的强度信息丢失,因此可通过融合零级频谱解码的方法来提高图像的质量 . 本文采

用的方法为先将一级频谱解码后的彩色图像由 RGB 色彩空间转化至 HSI 色彩空间,然后将零级频谱解码后的灰度图像代替其中的 I 分量,再将替换后的 HSI 色彩空间转化至 RGB 色彩空间[25],即可得到融合零级频谱后的解码图像,如图 5(b)所示,解码的彩色图像 MSE 为 0.004 0,图像的质量得到明显改善 .

若将方孔的大小改为 44×44 像素,解密后的结果如图 6(a)所示 . 若将方孔移动的步长改为 32 像素,解密后的结果如图 6(b)所示 .



(a) 用错误的方孔大小解密图像　　(b) 用错误的步长解密图像

图6　用错误的密钥解密图

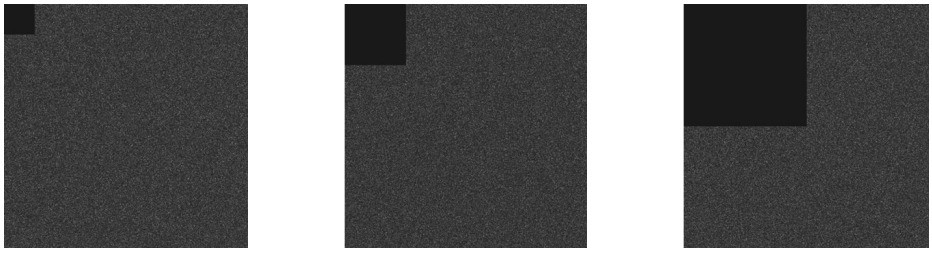
Fig.6　The decryption image with wrong keys

由图 6 可以看出,利用交叠成像技术对图像进行加密,移动方孔的步长不对应以及方孔的大小不对应不能解密出加密后的图像 . 因此用交叠成像技术可以增加加密的密钥,保证光学系统的安全性 .

3　对加密系统的鲁棒性能分析

3.1　抗剪切性能分析

利用上述算法对彩色图像进行加密,然后对加密图像进行如图 7 所示的一定程度的剪切,对剪切图像进行解密,解密结果如图 8 所示 . 从图 8 可以看出,即使图像受到 25%剪切,解密算法仍然能够恢复出原始图像,说明该加密系统可有效抗剪切攻击[26].



(a) 1/16　　(b) 1/8　　(c) 1/4

图7　不同的剪切比例

Fig.7　Different shear proportions

(a) 剪切1/16所对应的解密图　　(b) 剪切1/8所对应的解密图　　(c) 剪切1/4所对应的解密图

图8　在不同的剪切比例下所恢复的图像

Fig.8　The recovered image in different shear proportions

为了评价在不同的剪切比例下彩色原图像的恢复效果,计算彩色原图与恢复图像的均方差如表 1 所示 .

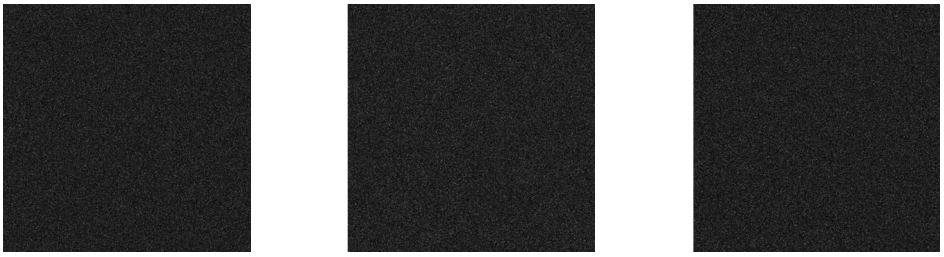
表1　在不同剪切比例下恢复的图像与彩色原图的均方差值

Table 1　The value of MSE between the recovered image and the original image in different shear proportions

评价标准	剪切区域		
	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{4}$
MSE	0.005 9	0.007 5	0.027 0

3.2　抗噪声性能分析

利用上述算法对彩色图像进行加密,然后对加密图像中加入不同取值范围的随机噪声 . 图 9 为加入不同取值范围随机噪声的加密图,图 10 为加入不同取值范围的随机噪声后的解密图 . 从图 10 中可以看出,当加密图像受到不同取值范围随机噪声的影响后,该图像解密算法能基本恢复出原始图像且基本不会影响图像整体视觉效果 . 结果表明,该解密系统可以抵抗不同程度的随机噪声攻击,具有较强的鲁棒性 .



(a) 随机噪声强度范围[0,0.1]　(b) 随机噪声强度范围[0,1]　(c)随机噪声强度范围[0,10]

图9　加入不同取值范围的噪声

Fig.9　Add the different limits of noise

(a) 加入[0,0.1]随机噪声的解密图　(b) 加入[0,1]随机噪声的解密图　(c) 加入[0,10]随机噪声的解密图

图10　加入不同取值范围的噪声后所恢复的图像

Fig.10　The recovered image at different limits of noise

为了评价在不同取值范围的噪声下彩色原图像的恢复效果,计算恢复图像与彩色原图的均方差如表 2 所示 .

表2　在不同取值范围的噪声下恢复的图像与彩色原图的均方差值

Table 2　The value of MSE between the recovered image and the original image at different limits of noise

评价标准	噪声强度范围		
	[0,0.1]	[0,1]	[0,10]
MSE	0.004 0	0.004 1	0.004 8

4　结论

本文利用正弦组合光栅和基于交叠成像技术的双随机相位加密方法,实现了彩色图像的加密与解密过程 . 模拟实验表明,交叠成像中方孔的大小以及移动的步长可以作为图像加密中的密钥,因此该加密系统增大了密钥的空间,提升了系统的安全性 . 通过对该加密系统的抗剪切性能和抗噪声性能进行定性分析,表明该加密系统具有较强的抗攻击性 . 与彩色图像多通道加密相比,本加密系统实验装置简单,简化了实验系统,降低了实验成本,提高了系统的实用性 . 理论分析和模拟实验结果证明了该系统的有效性 .

[参考文献](References)

[1] THIBAULT P, DIEROLF M, BUNK O, et al. Probe retrieval in ptychographic coherent diffractive imaging[J]. Ultramicroscopy, 2009, 109(4): 338-343.

[2] 刘诚,潘兴臣,朱健强 . 基于光栅分光法的相干衍射成像[J]. 物理学报,2013,62(18):184204.
LIU C, PAN X C, ZHU J Q. Coherent diffractive imaging based on the multiple beam illumination with cross grating[J]. Acta Phys Sin, 2013, 62(18): 184204.(in Chinese)

[3] RODENBURG J M, FAULKNER H M L. A phase retrieval algorithm for shifting illumination[J]. Applied physics letters, 2004, 85(20): 4 795-4 797.

[4] FAULKNER H M L, RODENBURG J M. Movable aperture lensless transmission microscopy: a novel phase retrieval algorithm[J]. Physical review letters, 2004, 93(2): 023903.

[5] MAIDEN A M, HUMPHRY M J, ZHANG F, et al. Superresolution imaging via ptychography[J]. JOSA A, 2011, 28(4): 604-612.

[6] GODDEN T M, SUMAN R, HUMPHRY M J, et al. Ptychographic microscope for three-dimensional imaging[J]. Opt Express, 2014, 22(10): 12513.

[7] CLAUS D, ROBINSON D J, CHETWYND D G, et al. Dual wavelength optical metrology using ptychography[J]. Journal of optics, 2013, 15(3): 035702.

[8] BATEY D J, CLAUS D, RODENBURG J M. Information multiplexing in ptychography[J]. Ultramicroscopy, 2014, 138: 13-21.

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

[10] CHEN L, LIU J, WEN J, et al. A new optical image encryption method based on multi-beams interference and vector composition[J]. Optics & laser technology, 2015, 69: 80-86.

[11] LI J, LI H, LI J, et al. Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography [J]. Optics communications, 2015, 344: 166-171.

[12] CHEN W, CHEN X, ANAND A, et al. Optical encryption using multiple intensity samplings in the axial domain[J]. JOSA A, 2013, 30(5): 806-812.

[13] QIN Y, GONG Q, WANG Z. Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme[J]. Optics express, 2014, 22(18): 21 790-21 799.

[14] CHEN L, ZHAO D. Color information processing(coding and synthesis)with fractional Fourier transforms and digital holography[J]. Optics express, 2007, 15(24): 16 080-16 089.

[15] GE F, CHEN L, ZHAO D. A half-blind color image hiding and encryption method in fractional Fourier domains[J]. Optics communications, 2008, 281(17): 4 254-4 260.

[16] ABUTURAB M R. An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform [J]. Optics and lasers in engineering, 2015, 69: 49-57.

[17] 杨晓萍,高丽娟,王晓雷,等 . 基于双相位编码的单通道彩色图像加密[J]. 物理学报,2009,58(3):1 662-1 667.
YANG X P, GAO L J, WANG X L, et al. Single channel encryption of color image based on double phase encoding[J]. Acta Phys Sin, 2009, 58(3): 1 662-1 667.(in Chinese)

[18] 董太继,周南润 . 单通道彩色图像加密方案[J]. 光电子·激光,2010,21(10):1 542-1 546.
DONG T J, ZHOU N R.An encryption scheme for single channel color images[J].Journal of optoelectronics·laser, 2010, 21(10): 1 542-1 546.(in Chinese)

[19] SHI Y, LI T, WANG Y, et al. Optical image encryption via ptychography[J]. Optics letters, 2013, 38(9): 1 425-1 427.

[20] RAWAT N, SHI Y, KIM B, et al. Sparse-based multispectral image encryption via ptychography[J]. Optics communications, 2015, 356: 296-305.

[21] 秦怡,郑长波 . 基于双随机相位编码的彩色图像加密技术[J]. 光子学报,2012,41(3):326-329.
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)

[22] 张煜东,吴乐南 . 基于分割的彩色图像编码[J]. 中国科学(F 辑:信息科学),2009,39(4):405-415.

ZHANG Y D, WU L N. Color image coding based on segmentation[J]. China science(Series F: Information Sciences), 2009, 39(4): 405-415.(in Chinese)

[23] BUNK O, DIEROLF M, KYNDE S, et al. Influence of the overlap parameter on the convergence of the ptychographical iterative engine[J]. Ultramicroscopy, 2008, 108(5): 481-487.

[24] 王雅丽,史祎诗,李拓,等 . 可见光域叠层成像中照明光束的关键参量研究[J]. 物理学报,2013,62(6):064206.
WANG Y L, SHI Y S, LI T, et al. Research on the key parameters of illuminating beam for imaging via ptychography in visible light band[J]. Acta Phys Sin, 2013, 62(6): 064206.(in Chinese)

[25] ALFALOU A, BROSSEAU C, ABDALLAH N, et al. Simultaneous fusion, compression, and encryption of multiple images[J]. Optics express, 2011, 19(24): 24 023-24 029.

[26] 张煜东,吴乐南,王水花 . 一种基于光全息的图像混合加密算法[J]. 计算机工程与应用,2011,47(20):201-205.
ZHANG Y D, WU L N, WANG S H. Hybrid image encryption method based on hologram[J]. Computer engineering and applications, 2011, 47(20): 201-205.(in Chinese)

[责任编辑:严海琳]