文章编号：2095-2163(2023)02-0081-06 中图分类号：TP309.7 文献标志码：A

基于螺旋光栅相位和分数 Fourier 的光学图像加密算法

车 凯[1,2]，王海翔[1]，白林亭[1,2]，文鹏程[1]，杨芷柔[1]，赵洪东[3]
（1 中航工业西安航空计算技术研究所，西安 710065；2 西北工业大学 计算机学院，西安 710072；
3 哈尔滨工业大学 计算学部，哈尔滨 150001）

摘 要：针对传统图像加密算法鲁棒性不足的问题，本文提出了一种基于螺旋光栅相位和分数 Fourier 的光学图像加密算法。该算法在密码学及利用分数傅里叶变换频域处理算法进行图像加密的基础上，引入了错位光栅生成的涡旋光束，作为部分加密密钥的思想。首先，利用螺旋相位变换自行设计加密图像的螺旋相位，作为一种加密密钥；其次，使用计算全息法模拟生成的涡旋光束，作为另一种加密密钥；最后，将上述两种密钥组合，生成最终的加密密钥，并利用分数傅里叶变换进行光学图像加密。经统计直方图分析、信息熵分析、差异性分析和抗噪声攻击能力分析等实验结果表明，本算法具有很好的鲁棒性和安全性。

关键词：光学图像加密；螺旋相位变换；涡旋光束；分数傅里叶变换

Optical image encryption algorithm based on spiral grating phase and fractional Fourier

CHE Kai[1,2], WANG Haixiang[1], BAI Linting[1,2], WEN Pengcheng[1], YANG Zhirou[1], ZHAO Hongdong[3]
(1 Xi′an Aeronautics Computing Technique Research Institute, AVIC, Xi′an 710065, China;
2 School of Computer Science, Northwestern Polytechnical University, Xi′an 710072, China;
3 Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China)

【Abstract】 To deal with the problem of insufficient robustness of traditional image encryption algorithms, an optical image encryption algorithm based on spiral grating phase and fractional Fourier is proposed. Based on cryptography and optical image encryption by the frequency-domain algorithm of fractional Fourier transform, the idea that the vortex beam generated by dislocation grating is used as the partial encryption key is introduced in this algorithm. Firstly, the spiral phase of the encrypted image is designed as an encryption key. Secondly, the vortex beam generated by computational holography is used as another encryption key. Finally, the two keys are combined to generate the final encryption key, and the fractional Fourier transform is used to encrypt the image. The experiments of statistical histogram analysis, information entropy analysis, difference analysis and anti-noise capability analysis show that this algorithm has good robustness and security.

【Key words】 optical image encryption; spiral phase transform; vortex beam; fractional Fourier transform

0 引 言

随着大数据时代的来临，图片数据存储量越来越大，原始的图像置乱加密的方法，已不能满足高效加密的需求。当前不仅需要的是安全性较高的加密方法，且实际场景应用要求加密系统在保证足够安全的前提下，对性能提出了要确保时效性较高、抵抗攻击的鲁棒性能要好、图像密钥占据空间要小、密文图像与明文图像的相似度小等众多要求[1-2]。

目前，在图像加密技术中，较为流行的方法主要分为两大类：混沌加密和光学加密[3]。混沌加密技术主要是利用复杂的相空间等特征，对图像像素及其值进行改变。虽然此类方法的加密效果较好，但混沌系统的周期性会造成加密安全性的缺失。为解决混沌加密安全性的问题，光学加密技术相继被提出，该技术具有效率高、存储量大、并行度高以及密钥维度多等特性。自 1995 年后，随着 Refregier 等人[4]提出经典的双随机相位编码光学加密系统后，一系列的光学加密方法相继被提出。2017 年，Kumar[5]等人提出了一种新的非线性光学图像加密

基金项目：国防科技创新特区项目(20-163-01-ZT-004-102-01)。
作者简介：车 凯(1987-)，男，博士，工程师，主要研究方向：机器学习、信息处理。
通讯作者：车 凯 Email：chekai@hit.edu.cn
收稿日期：2022-12-21

技术,使用螺旋相位变换(SPT),采用随机相位掩码(RPM)调制,使得图像以距离 z 进行菲涅耳传播,以达到加密的效果。但是,复杂的菲涅耳变换会增加计算的难度。同年,Kumar 等[6]又提出了利用小波变换替换分数傅里叶变换,并分析了不同融合方法的优缺点。2018 年,Khurana M[7]提出了一种基于混合结构相位掩模(HSPM)的旋转变换(GT)域双图像加密方法,使光学图像加密方法鲁棒性得到提升。

为了同时提高鲁棒性和加密效率,本文在使用螺旋相位作为部分密钥的基础上,引入错位光栅生成的涡旋光束作为部分密钥,提出了一种基于螺旋光栅相位和分数 Fourier 的光学图像加密算法。利用计算全息法设计位错光栅并生成涡旋光束,然后与自主设计的螺旋相位结合形成加密密钥,使用分数傅里叶变换对图像进行加密。经统计直方图、信息熵、差异性和抗噪声攻击能力等实验分析,表明该方法具有很好的鲁棒性和安全性。

1 基于螺旋光栅相位和分数 Fourier 的光学图像加密算法

1.1 螺旋相位变换(SPT)

在螺旋相位变换中,二维符号函数 $\mathrm{sgn}(\mu,\nu)$ 也被称为螺旋相位函数(SPF),用于二维 Hilbert 变换[8-9]。二维符号函数可以定义为空间频率中的纯 SPF:

$$\mathrm{SPF}=\mathrm{sgn}(\mu,\nu)=\frac{\mu+\nu}{\sqrt{\mu^2+\nu^2}}=\exp\{i\varphi(\mu,\nu)\} \quad (1)$$

其中,相位 $\varphi(\mu,\nu)$ 是频率空间中的极坐标角。SPF 函数未在原点处定义,其在原点处的值可以是 0 或 1,这些值指向奇点。

在此情况下,通过引入参数 q 来修改 SPM 函数。q 是奇点的数量或 SPF 的阶,对应于 SPF 值未定义的点(即 0 或 1)。修改后的 SPF 可改写为

$$\mathrm{SPF}=\exp\{iq\varphi(\mu,\nu)\} \quad (2)$$

因此,对于特定阶的 SPF,二维信号的 SPT 可以表示为

$$\mathrm{SPF}\{f(x,y)\}=\mathrm{IFT}\{\mathrm{SPF}.\mathrm{FT}\{f(x,y)\}\} \quad (3)$$

其中,FT 和 IFT 分别表示二维傅里叶正变换和反变换。

SPT 的逆为

$$\mathrm{ISPF}\{f(x,y)\}=\mathrm{IFT}\{conj(\mathrm{SPF}).\mathrm{FT}\{f(x,y)\}\} \quad (4)$$

其中,$conj(\,)$ 表示共轭复数。

1.2 计算全息法生成涡旋光束

涡旋光束是一种具有螺旋状相位波前的光束,且在传播方向上,光束中心强度或轴向强度为 0,又被称为暗中空光束[10]。涡旋光束具有暗斑尺寸极小、光强呈环状分布和传播不变性等独特的物理特性,因此涡旋光束被广泛地应用在光学计算、物理数学和信息处理等方面。

通常,涡旋光束的获取有多种方法,如:计算全息法、几何光学法和中空波导法等[11]。以上方法中,基于计算全息法适用范围广,能够便捷地生成不同阶的涡旋光束。

假设:$E_1\exp(i\varphi_1)$ 和 $E_2\exp(i\varphi_2)$ 分别表示两个光束的波函数,当两束光发生干涉时,产生的干涉光强则为

$$I=E_1^2+E_2^2+2E_1E_2\cos(\varphi_1-\varphi_2) \quad (5)$$

其中,$2E_1E_2\cos(\varphi_1-\varphi_2)$ 表示干涉光强的空间分布特性,通常选择其作为光栅透过率函数来产生光栅。将 $E_1\exp(i\varphi_1)$ 作为参考光束,通过照射光栅,光束 $E_2\exp(i\varphi_2)$ 能够在透射光束中再现,即为全息术的原理。

计算全息法就是基于全息术原理,利用已有光束来获取所需的具有某种特性的光束。由于光栅的种类可以不同,透射光束也就不同,造成了透射光束的多样性和不确定性,这正是生成密钥所需要考虑的形式之一。因此,本文选择计算全息法产生的涡旋光束相位作为密钥的一部分。

1.3 分数傅里叶变换

分数傅里叶变换是 1980 年 Namias[12]为求解偏微分方程而引入量子力学。1993 年,Mendlovic 等[13]人通过研究光在二次梯度折射率介质中的传播,给出了分数阶傅里叶变换级数形式的表达式。同年,Lonmann 用 Wigner 相空间旋转的概念,给出了分数傅里叶变换的积分形式表达式[14]。

设 $f(x)$ 为输入信号,则其 P 阶分数傅里叶变换定义为

$$f_p(x_p)=C_p\exp\left(\mathrm{j}\pi\frac{x_p^2}{\tan\varphi}\right)\int_{-\infty}^{+\infty}f(x)\exp\left(\mathrm{j}\pi\frac{x^2}{\tan\varphi}\right)\exp\left(-\mathrm{j}2\pi\frac{xx_p}{\sin\varphi}\right)dx \quad (6)$$

其中,常数 $C_p=\dfrac{\exp\{-j[\frac{\pi\mathrm{sgn}(\sin\varphi)}{4}-\frac{\varphi}{2}]\}}{\sqrt{|\sin\varphi|}}$;

$P(0<|p|<2)$ 为分数阶;$\varphi=p\times\dfrac{\pi}{2}$。特别是当 $p=1$ 时,分数傅里叶变换转化为传统的傅里叶变换。

验证得:$f_2[f(x)]=f(-x)$、$f_4[f(x)]=f(-x)$。其物理意义相当于对原函数进行 2 次连

续 $\frac{\pi}{2}$ 旋转，得到相对于 y 轴翻转的函数图像；则表示对其进行 4 次连续 $\frac{\pi}{2}$ 的旋转，所得图像与原函数完全相同。

1.4　加密算法的实现

加密流程如图 1 所示，其实现的具体步骤如下：

Step 1　将原彩色图像转化为灰度图像，再将灰度图像转换为 double 值；

Step 2　利用 SPT 自行设计一个螺旋相位，记为 p1；

Step 3　利用计算全息法模拟错位光栅产生的涡旋光束相位，记为 p2；

Step 4　将 p1 和 p2 组成密钥 p；

Step 5　利用密钥 p，采用分数傅里叶变换对 double 值图像进行处理，即得到加密图像。

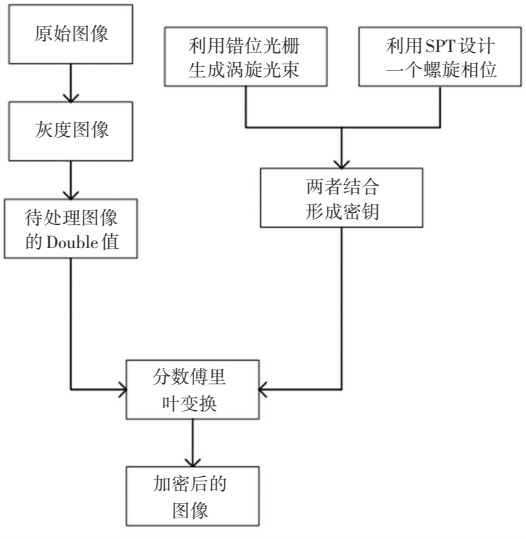

图 1　加密计算流程图

Fig. 1　Flowchart of the encryption process

与之对应的解密过程为：利用相同参数的加密密钥图像，输入加密参数相反数，对加密图像进行分数傅里叶变换，即可以得到加密之前的灰度图像。还可恢复原来色彩，得到原始彩色图像。具体解密流程如图 2 所示。

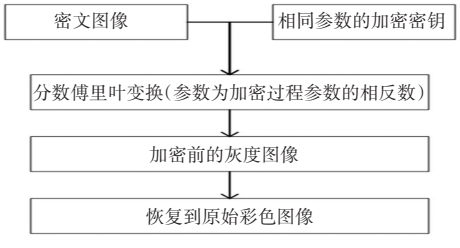

图 2　解密计算流程图

Fig. 2　Flowchart of the decryption process

2　实验仿真与算法性能分析

仿真实验选取大小为 512 * 512 的“Lena”彩色图像。首先，采用本文提出的加密算法进行实验；其次，以统计直方图、信息熵、差异性和抗干扰能力等评价指标与其它加密算法进行比较。实验表明，本文提出的加密算法具有很好的安全性和有效性。

2.1　加密实验

在不进行任何攻击测试的前提下，测试了加密的全过程，实验结果如图 3 所示。

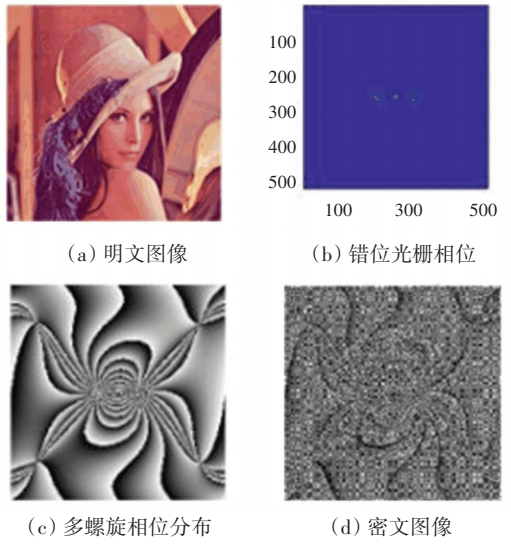

图 3　无攻击情况下的加密过程

Fig. 3　Encryption process without attack

其中，加密处理结果的放大效果如图 4 所示。

图 4　放大后的加密结果

Fig. 4　Enlarged encryption result

2.2　算法安全性及性能分析

2.2.1　统计直方图分析

首先，对明文图像和密文图像的统计直方图进行了对比，实验结果如图 5 所示；其次，为了对比明文图像与解密图像的差异性，对两者进行了统计分析，实验结果见图 6；最后，对经典的混沌加密算法、块置乱加密算法、像素置乱加密算法和 CaTmap 加

密算法的实验结果进行了统计图分析,实验结果如图 7~图 10 所示。

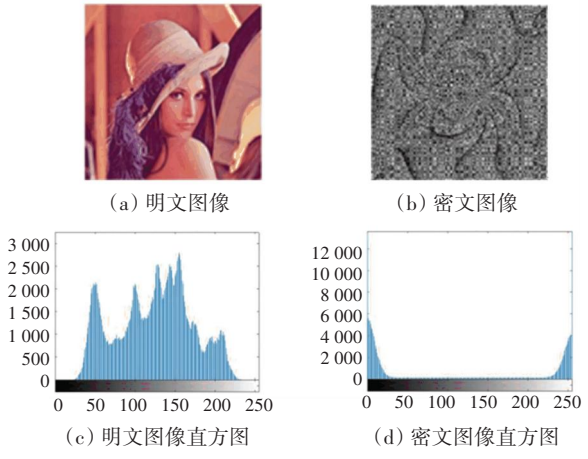

图 5 本文方法的明文和密文图像直方图

Fig. 5 Histogram of plaintext and ciphertext images with our method

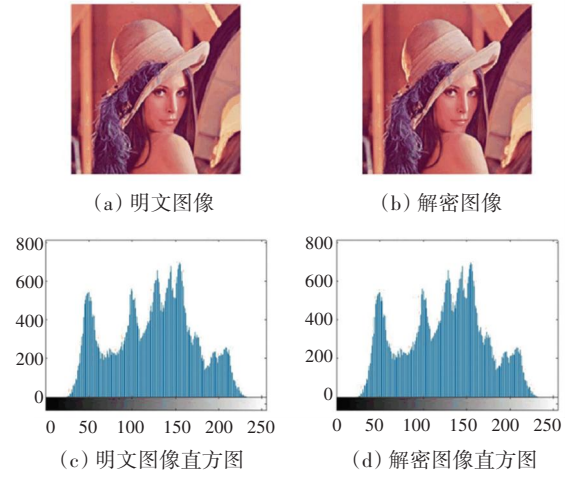

图 6 本文方法的明文和解密图像直方图

Fig. 6 Histogram of plaintext and decrypted images with our method

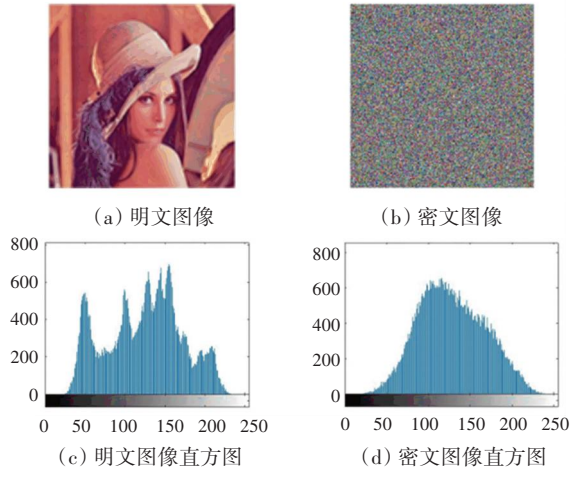

图 7 混沌加密算法的明文和密文图像直方图

Fig. 7 Histogram of plaintext and ciphertext images with chaos encryption algorithm

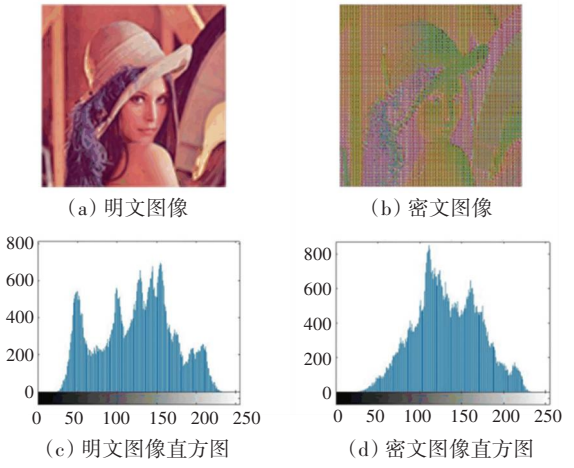

图 8 块置乱加密算法的明文和密文图像直方图

Fig. 8 Histogram of plaintext and ciphertext images with block scrambling encryption algorithm

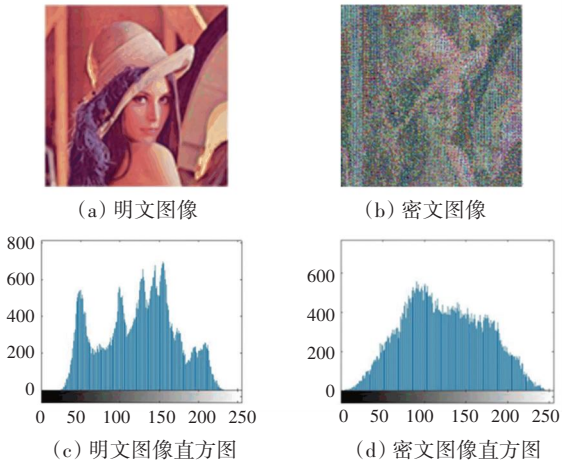

图 9 像素置乱加密算法的明文和密文图像直方图

Fig. 9 Histogram of plaintext and ciphertext images with pixel scrambling encryption algorithm

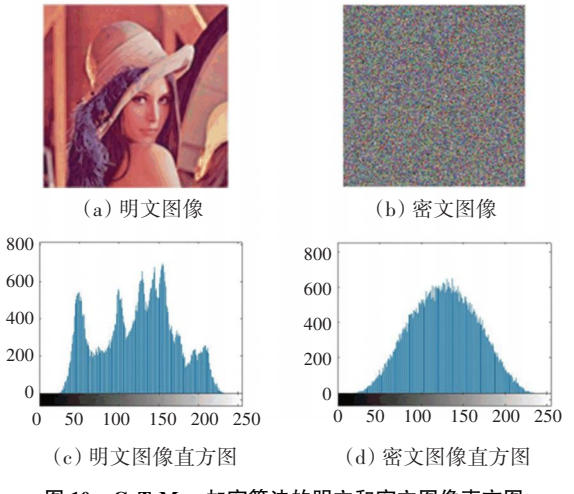

图 10 CaT Map 加密算法的明文和密文图像直方图

Fig. 10 Histogram of plaintext and ciphertext images with CaT Map encryption algorithm

由多组实验对比可以看出，本论文提出的加密算法在统计规律上，停留在像素值为 0～35 和 220～155这个区域，这是由于图像的加密算法中的密钥造成的。从密文图片可见，整体可以看出融合密钥的纹理信息，这也从侧面说明了统计图的结果。

2.2.2　信息熵分析

信息熵表示信息的混乱程度，图像的信息熵越接近理想值，则表示其信息越混乱，也说明其加密效果越好[15]。通常，加密图像信息熵的理想值为 8。本文所提算法加密后图像的信息熵为 7.995 85。

设图像 m 的信息熵为 $H(m)$，其定义为

$$H(m) = -\sum_{i=0}^{2N-1} p(m_i)\log_2\frac{1}{p(m_i)} \tag{7}$$

其中，$p(m_i)$ 表示信息值 m_i 出现的概率。

2.2.3　差异攻击分析

当明文图像中的微小变化在密文像素中产生巨大差异时，图像加密方法对于差分攻击具有较强的抵抗力。这种类型的分析通过像素变化率（NPCR）和均匀变化强度（UACI）来度量。本文方法与 Jan Sher Khan[16] 的方法在 NPCR 和 UACI 上进行了对比，实验结果见表 1。结果表明，本文方法具有良好的差异攻击性。

表 1　NPCR 和 UACI 测试数值的对比结果

Tab. 1　Test results of NPCR and UACI for images

指标	本文算法		Jan Sher Khan 的方法	
	彩色图片	灰度图片	彩色图片	灰度图片
NPCR	99.941 2	99.609 3	99.230 4	99.154 7
UACI	44.983	33.463 5	33.034 1	33.207 2

2.2.4　噪声攻击分析

为了验证加密算法在抵抗密文攻击时的鲁棒性，本文验证了抗噪声干扰的能力。在密文图像中加入高斯噪声。

$$G' = G(1 + K\sigma) \tag{8}$$

其中，G 和 G' 分别表示密文图像和攻击后的图像；K 表示噪声强度系数；σ 表示加入的随机噪声。

图 11 为加入不同噪声后灰度图像的解密结果。Lena 的解密图像能够被识别出来，当 $K = 0.6$ 时，解密图像仍能够被识别出来，表明该加密算法对噪声攻击具有较强的鲁棒性。

（a）$K = 0.1$　　（b）$K = 0.3$　　（c）$K = 0.6$

图 11　Lena 解密图像

Fig. 11　Decrypted images of images Lena

3　结束语

本文提出了一种基于螺旋光栅相位和分数 Fourier 的光学图像加密算法。该方法的密钥融合了螺旋相位和错位光栅生成的涡旋光束，在利用分数傅里叶变换对图像进行加密处理。仿真实验从统计直方图分析、信息熵分析、差异性分析和抗噪声攻击能力分析等方面进行验证，实验结果表明该方法具有很好的加密效果、鲁棒性和安全性。

参考文献

[1] LIU X, CAO Y, LU P, et al. Optical image encryption technique based on compressed sensing and Arnold transformation[J].Optik, 2013, 124(24): 6590-6593.

[2] ENAYATIFAR R , ABDULLAH A H, ISNIN I F , et al. Image encryption using a synchronous permutation-diffusion technique [J]. Optics & Lasers in Engineering, 2017, 90(3):146-154.

[3] SU Y, CHEN T, XIA C, et al. Optical Image Encryption Based on Mixed Chaotic Maps and Single-Shot Digital Holography[J]. 天津大学学报:英文版, 2017, 23(2):8.

[4] REFREGIER P, JAVIDI B. Optical image encryption using input plane and Fourier plane random encoding [C]// Optical Implementation of Information Processing. International Society for Optics and Photonics, 1995,20(7):767-769.

[5] KUMAR R, BHADURI B. Optical image encryption in Fresnel domain using spiral phase transform[J]. Journal of Optics, 2017, 19:095771.

[6] KUMAR R, BHADURI B. Double image encryption in Fresnel domain using wavelet transform, gyrator transform and spiral phase masks[C]// Society of Photo-optical Instrumentation Engineers. Society of Photo - Optical Instrumentation Engineers (SPIE) Conference Series, 2017:110-115.

[7] KHURANA M, SINGH H. Optical image encryption using fresnel zone plate mask based on fast walsh hadamard transform[C]// 2nd International Conference on Condensed Matter and Applied Physics (ICC 2017). American Institute of Physics Conference Series, 2018:140043.

[8] LIN C, SHEN X. Design of reconfigurable and structured spiral phase mask for optical security system [J]. Optics Communications, 2016,370:127-134..

[9] LARKIN K G, BONE D J, OLDFIELD M A. Natural demodulation of two-dimensional fringe patterns. I. General background of the spiral phase quadrature transform[J]. JOSA A, 2001, 18(8): 1862-1870.

（下转第 91 页）