

文章编号:2095-6134(2016)05-0612-06

基于傅里叶叠层成像的光学图像加密^{*}

许文慧¹, 李 拓¹, 史伟诗^{1, 2†}

(1 中国科学院大学, 北京 100049; 2 中国科学院光电研究院, 北京 100094)

(2015 年 9 月 6 日收稿; 2016 年 3 月 26 日收修稿)

Xu W H, Li T, Shi Y S. Optical image encryption based on Fourier ptychography [J]. Journal of University of Chinese Academy of Sciences, 2016, 33(5): 612-617.

摘 要 提出一种基于傅里叶叠层成像的光学图像加密技术. 基于传统的 $4f$ 双随机相位编码系统, 将滤波孔径(探针)紧贴着随机相位掩模板放置在傅里叶频谱面上, 在频域限制不同成分的空间频率信息通过. 该技术采用低数值孔径的透镜和平行光多角度照明, 使装置更加简单. 计算机模拟结果表明, 该技术收敛速度快, 可行性较强, 并具有高鲁棒性、高安全性和高解密质量等优点.

关键词 光学图像加密; 傅里叶叠层成像; 双随机相位编码

中图分类号: O438 文献标志码: A doi: 10. 7523/j. issn. 2095-6134. 2016. 05. 006

Optical image encryption based on Fourier ptychography

XU Wenhui¹, LI Tuo¹, SHI Yishi^{1, 2}

(1 University of Chinese Academy of Sciences, Beijing 100049, China; 2 Academy of Opto-Electronics,

Chinese Academy of Sciences, Beijing 100094, China)

Abstract We propose a method for optical image encryption based on Fourier ptychography (FP). On the basis of $4f$ double random phase encoding system, the filter aperture (probe) is placed at the Fourier plane, so that the object support constraints for phase retrieval of FP are imposed by the confined optical-transfer-functions in the Fourier domain. Furthermore, we adopt the low numerical aperture objective lens and the variable-angle illumination, which simplifies the device effectively. Numerical simulation results show that the method has the merits of high convergence speed, feasibility, robustness, decryption quality, and security.

Key words optical image encryption; Fourier ptychography; double random phase encoding

傅里叶叠层成像是一种能够利用多角度光照明和低数值孔径的物镜重建出具有高分辨率图像的相位恢复技术^[1]. 与传统的叠层成像技术相似, 傅里叶叠层成像利用在频域上形成光谱的叠

层恢复出样本的复振幅分布, 因此也具有收敛速度快和消除解的二义性等优点^[2-4]. 然而, 傅里叶叠层成像并不是用扫描相干衍射的方法, 而是采用合成孔径的概念^[5-6]. 与传统叠层成像相

^{*} 国家自然科学基金(61575197)资助
[†] 通信作者, E-mail: shiyishi@ucas.ac.cn

比,傅里叶叠层成像的受限支撑不是受限的照明光束,而是傅里叶域受限的光学传递函数^[7-12]。除此之外,傅里叶叠层成像系统中由于引入了低数值孔径的透镜,不仅可以扩大视场,提高信噪比和分辨率,而且能降低对光源相干性的要求。并且,傅里叶叠层成像还可以突破物镜本身的限制,在消除透镜带来的像差的同时增加景深^[11]。

光学信息安全技术由于其具有高设计自由度、多加密维度、高鲁棒性、高速并行处理的能力和难以破解等诸多优势,而受到诸多研究学者的关注^[13]。自从 Refregier 和 Javidi^[14] 提出基于双随机相位的加密方法以来,光学图像加密便成为一个研究热点。在此方面,近年来不断有新的进展。Liu 等^[15] 提出一种基于级联分数傅里叶变换的光学图像加密系统,具有良好的安全性; Situ 和 Zhang^[16] 将波长复用技术引入到菲涅尔域的双随机相位加密系统中,完成了多幅图像的加密; Shi 等^[17] 提出一种基于叠层成像的光学图像加密方法,该方法采用的装置简单、适用性强,还能有效地扩大密钥空间以提高系统的安全性。众所周知,图像解密的过程和成像系统中图像恢复的过程相似,鉴于傅里叶叠层成像具有诸多优良性能,于是本文提出一种基于傅里叶叠层成像的光学图像加密技术。该技术是将探针放置在傅里叶频谱面上,采用 LED 阵列进行多角度的平行光源照明,在频域上形成频谱的叠层,“层”与“层”的交叠扩展了频域带宽。模拟仿真结果表明,该技术既保证了加密系统具有较高的安全性,鲁棒性和解密质量,又能简化装置,提高收敛速度。

1 光学图像加密及解密算法

1.1 加密算法

本文提出的基于傅里叶叠层成像的光学图像加密算法是基于传统 $4f$ 双随机相位编码系统来实现的,如图 1 所示。与基于叠层成像的双随机相位光学图像加密系统不同的是,探针紧贴着随机相位板被放在第 1 个透镜的傅里叶频谱面上,这样就避免了照明光源的机械扫描装置。由于傅里叶叠层成像的关键也在于叠层,频谱的某一“层”,也就是频谱受探针限制通过的某一部分,需要与其他“层”发生交叠,因此重构的每“层”频

谱也同时满足其他“层”的频谱约束,最后重构的频谱是所有层的共解,因而提高了迭代速度,增加了重构的准确性。

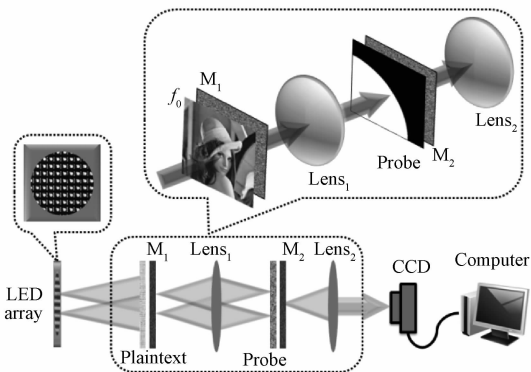


图1 基于傅里叶叠层成像的光学图像加密系统示意图

Fig. 1 Schematic of optical image encryption based on Fourier ptychography

构建如图 2 所示的 4 个不同孔径的探针 K1 为例。其中黑色为完全遮挡光波的部分,白色为完全透过光波的部分。对于本文所采用的 4 个不同的探针,使用一个 $0-1$ 分布的光瞳函数 P_i 来表征,其定义为

$$P_i = \begin{cases} 1 & \text{透光孔径内} \\ 0 & \text{透光孔径外} \end{cases} (i = 1, 2, 3, 4), \quad (1)$$

其中,下标 i 表示第 i 个探针。

加密时,输入的明文 $f_0(x, y)$ 在空域受到随机相位 $M_1: N(x, y) = \exp[jn(x, y)]$ 的调制,在频域先后受到探针: P_i 和随机相位 $M_2: K(\alpha, \beta) = \exp[jk(\alpha, \beta)]$ 的滤波, $n(x, y)$ 和 $k(\alpha, \beta)$ 分别表示 2 个均匀分布于 $[0, 2\pi]$ 的独立随机白噪声序列。加密结果表示如下

$$\psi_i = \left| \frac{FT\{FT[f_0(x, y) \cdot N(x, y)] \cdot P_i\}}{P_i \cdot K(\alpha, \beta)} \right|^2, \quad (2)$$

其中, ψ_i 为相应的衍射图样强度,即为所要加密图像对应的密文。FT 表示傅里叶变换。

1.2 解密算法

由密文和正确的相位密钥,即可采用解密算法恢复出明文信息。从数学的角度来看,该解密算法可以视为傅里叶叠层成像迭代算法的一种特殊形式,并且与传统的叠层成像迭代算法相似。下面简述解密算法:

1) 首先估计输入图像的复振幅为 $f_g(x, y)$, 然后开始进行迭代.

2) 假设进行到第 m 次迭代时, 对于第 i 个探针, 由前面迭代得出的图像复振幅为 $f_{ig}^m(x, y)$. 则基于前面加密算法的推导, 可得到频谱面上的场分布为

$$f_{ig}^m(\alpha, \beta) = FT[f_{ig}^m(x, y) \cdot N(x, y)]. \quad (3)$$

3) 最终输出面上的衍射图样复振幅为

$$D_{ig}^m = FT[f_{ig}^m(\alpha, \beta) \cdot P_i \cdot K(\alpha, \beta)]. \quad (4)$$

4) 用记录的强度图样的平方根值 $(\psi_i)^{\frac{1}{2}}$ 表示像面场分布的振幅, 用方程 (4) 的推导结果表示相位, 则得到新的输出面上的复振幅分布 D_{ig}^m 为

$$D_{ig}^m = (\psi_i)^{\frac{1}{2}} \frac{D_{ig}^m}{|D_{ig}^m|}. \quad (5)$$

5) 原来频谱面场分布对应于通光孔径 P_i 的部分用新的频谱场分布相应部分替换, 得到

$$f_{igs}^m(\alpha, \beta) = f_{ig}^m(\alpha, \beta) \cdot (1 - P_i) + FT^{-1}(D_{ig}^m) \cdot K^*(\alpha, \beta) \cdot P_i, \quad (6)$$

其中, $K^*(\alpha, \beta) = \exp[-jk(\alpha, \beta)]$ 为 M_2 的复共轭.

6) 继续做傅里叶逆变换, 最后再乘 M_1 的复共轭: $N^*(x, y) = \exp[-jn(x, y)]$ 得到重建图像的复振幅分布为

$$f_{igN}^m(x, y) = FT^{-1}[f_{igs}^m(\alpha, \beta)] \cdot N^*(x, y). \quad (7)$$

7) 用 $f_{igN}^m(x, y)$ 作为初始值, 对第 $i + 1$ 个探针所对应的密文 (衍射图样强度测量值), 进行步骤 2) 到 4) 的计算, 以此类推, 直到将 4 个探针对应的密文计算完毕.

8) 计算解密图像和密文的相关系数 Co . Co 是评价 2 个函数相似程度的量化指标, 取值范围为 $[0, 1]$, Co 值越接近于 1, 表明 2 个函数的分布形式越相近. Co 的表达式为

$$Co = \text{cov}(f, f_0) (\sigma_f \cdot \sigma_{f_0})^{-1}. \quad (8)$$

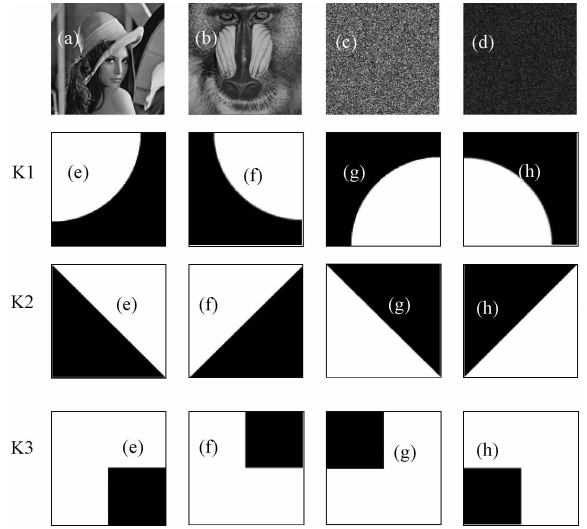
其中, f 和 f_0 分别为解密图像和原始被加密图像的复振幅, $\text{cov}(f, f_0)$ 为 f 和 f_0 的互协方差, σ_f 和 σ_{f_0} 为标准差. 评价解密质量时, 需要分别计算振幅和相位的相关系数值 Co_A 和 Co_ϕ .

9) 如果 Co 达到预期标准, 则此时恢复的复振幅即为所期望得到的解密图像; 如果 Co 未达到

预期标准, 则将此恢复的复振幅作为初始值, 进行下一轮迭代, 即对所有的 P_i 重新进行从步骤 2) 到 8) 的计算. 进行多次迭代, 直至解密出来的图像达到要求.

2 模拟实验与分析

我们进行了一系列的模拟实验来验证本文所提出技术的可行性和有效性. 分别采用均为 256 像素 \times 256 像素的“Lena”和“Baboon”作为样品的振幅和相位信息, 如图 2(a) 和图 2(b) 所示. 选取的 2 块随机相位板 M_1 和 M_2 均匀独立随机分布在 $[0, 2\pi]$ 内, 其中一块如图 2(c) 所示. 图 2(d) 为 4 个探针中的 1 个所对应的衍射图样 (密文). 模拟所采用的探针如图 2 中 K1, K2, K3 所示, 其中图 2(f)、2(g) 和 2(h) 可以看做是由图 2(e) 分别旋转 90° , 180° , 270° 得到的. 模拟所用的处理器为 Intel i7 - 4790 @ 3.60 GHz, 软件为 MATLAB R2014a, 采用探针 K1 模拟重建迭代 50 次所需时间约为 1.85 s, 迭代 30 次所需时间约为 0.94 s.



(a) 振幅; (b) 相位; (c) 随机相位板; (d) 密文.

K1, K2, K3 为模拟所采用的各种不同的探针, 其中 (e) 为 P_1 ; (f) 为 P_2 ; (g) 为 P_3 ; (h) 为 P_4 .

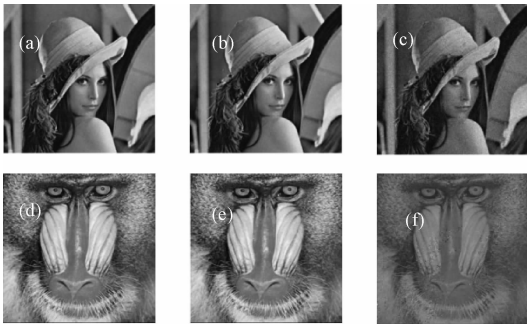
图 2 模拟实验数据

Fig. 2 Data used in simulation

2.1 可行性分析

通过采用探针 K1 进行模拟, 恢复出来的振幅和相位如图 3(a) 和图 3(d) 所示, 在迭代 25 次

时,得到的振幅和相位相关系数 Co 均可达到 0.999. 也就是说,在理想状态下,密文可以快速且无损地解密出来. 此外,为了验证本文所提方案的适用性,采用如图 2 中 K2 和 K3 所示的另外 2 种不同形状的振幅型探针进行加密和解密,其相应的解密结果如图 3(b)、3(e)和图 3(c)、3(f)所示. 由计算结果可知,采用 K2 可以得到和采用 K1 相同的良好效果. 对于采用 K3,在迭代 35 次之后,得到的振幅 Co 可达到 0.93,相位 Co 可达到 0.97. 由此可见,本文提出的加密方案具有很强的可行性.



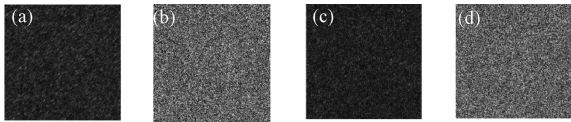
(a)和(d) K1;(b)和(e) K2;(c)和(f) K3.

图 3 不同探针对应的解密结果

Fig.3 Decrypted results with different probes

2.2 安全性分析

为了验证探针也可以作为密钥,于是采用正确的随机相位板和错误的探针来进行模拟实验. 图 4 为模拟实验解密出来的振幅和相位,其中图 4(a)和 4(b)为在解密时将相应加密时采用的探针 K1 的顺序置乱而解密出来的图像,图 4(c)和 4(d)为采用和加密过程不同的探针解密出来的图像. 模拟结果表明,使用错误的探针不能解密出预期的图像. 也就是说,探针也可作为一种新的密钥,这进一步提高了加密系统的安全性.



(a),(b)为将探针 K1 的顺序置乱解密出来的振幅和相位;
(c),(d)为采用和加密过程不同的探针解密出来的振幅和相位.

图 4 错误探针对应的解密结果

Fig.4 Decrypted images with wrong probes

2.3 鲁棒性分析

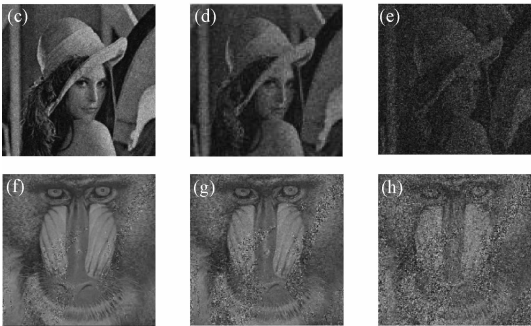
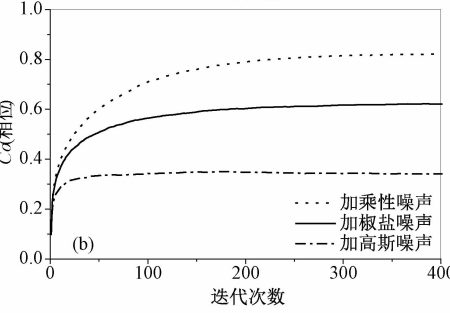
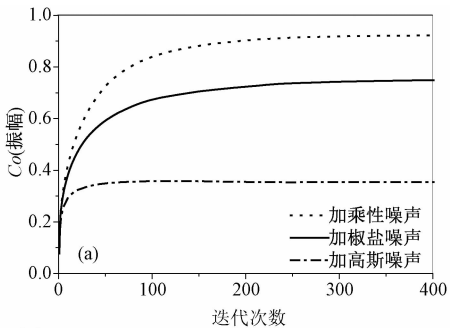
为验证本文加密技术的鲁棒性,分别对密文

进行加噪声和剪切操作. 模拟采用的均为振幅型探针. 模拟结果表明该技术具有很强的抵抗加噪声和剪切攻击的能力.

2.3.1 抗噪声能力分析

首先分析本算法对抗各类噪声的有效性. 我们分别模拟乘性噪声、椒盐噪声和高斯噪声对解密质量的影响.

模拟采用的高斯噪声的均值为 0,方差为 0.01,椒盐噪声和乘性噪声的密度均为 0.01. 图 5(a)和 5(b)分别是解密之后的图像和原图像之间关于振幅和相位的相关系数 Co 随迭代次数的变化曲线. 由图 5(c),5(f)和 5(d),5(g)可以看出本算法能够很好地抵抗乘性噪声和椒盐噪声.



(a) 振幅相关系数 Co ;(b) 相位相关系数 Co ;(c)和(f)对应于添加乘性噪声;(d)和(g)对应于添加椒盐噪声;(e)和(h)对应于添加高斯噪声.

图 5 添加不同噪声情况下解密出来的振幅和相位分布及其相应的 Co 值随迭代次数的变化

Fig.5 Decrypted results under the attacks of divers noises

相对而言,本算法对于高斯噪声的抵抗能力较差,但是对密文添加了上述高斯噪声后,仍能恢复出具有一定识别度的图像. 这些结果表明,本文提出的加密技术能够抵抗一定的噪声攻击.

2.3.2 抗剪切能力分析

为增加密文被攻击的随机性,分别从密文中心截去占密文 5%、11%、20%、30%、45% 和 60% 的圆形部分,如图 6(a) — 图 6(f) 所示. 相应的解

密出来的结果如图 6(g) 和 6(h) 所示. 此外,图 6(g) 和 6(h) 还分别示出了在迭代 30 次左右时振幅和相位 Co 值随剪切面积的变化曲线. 由图 6(g) 和 6(h) 可以直观地看出当密文被剪切 30% 时,振幅和相位 Co 值都能达到 0.5 以上,具有较高的解密质量;当密文被剪切大约 60% 时,解密出来的振幅和相位仍具有一定的可辨识度. 由此可见,本文所提出的方法具有很强的抗剪切攻击能力.

3 结论

本文将傅里叶叠层成像用于双随机相位光学图像加密系统. 一方面,置于傅里叶频谱面上的滤波孔径可以作为新的密钥,显著增大了系统的密钥空间. 另一方面,该技术采用平行光多角度照明,降低了对光源相干性的要求,能够简化实验装置. 模拟结果表明,该技术的收敛速度快,并且具有较强的可行性和较高的鲁棒性. 此外,该技术还可以用来对三维图像进行加密和隐藏,具有广阔的应用前景.

参考文献

[1] Zheng G, Horstmeyer R, Yang C. Wide-field, high-resolution Fourier ptychographic microscopy[J]. Nat Photonics, 2013, 7 (9) : 739-745.

[2] Ou X, Horstmeyer R, Yang C, et al. Quantitative phase imaging via Fourier ptychographic microscopy[J]. Opt Lett, 2013, 38 (22) : 4 845-4 848.

[3] Faulkner H M L, Rodenburg J M. Movable aperture lensless transmission microscopy: A novel phase retrieval algorithm [J]. Phys Rev Lett, 2004, 93 (2) : 023903.

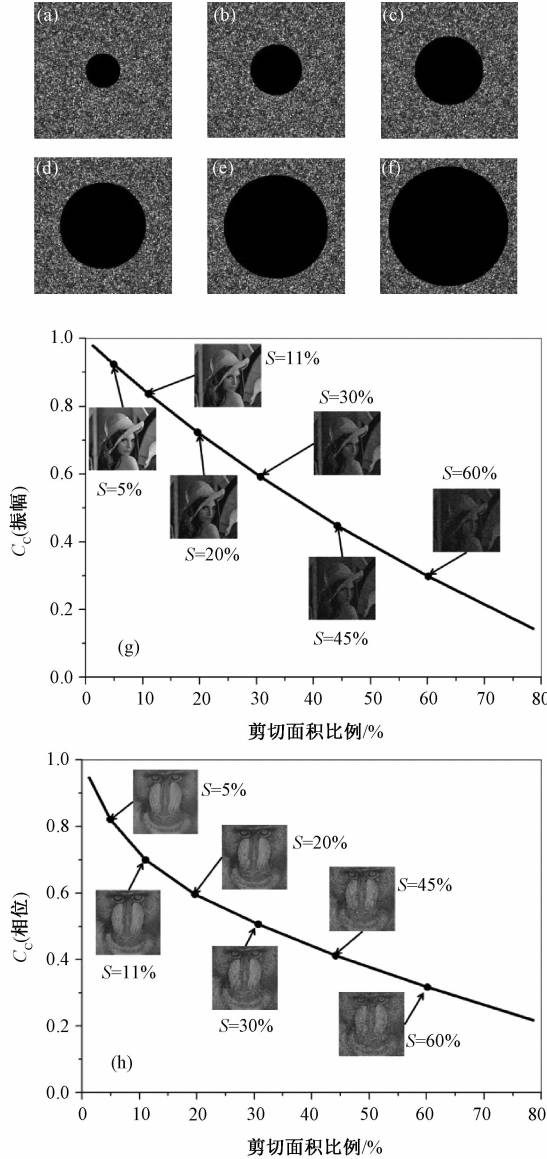
[4] Zheng G, Ou X, Horstmeyer R, et al. Fourier ptychographic microscopy: a gigapixel superscope for biomedicine[J]. Opt Photon News, 2014, 25 (4) : 26-33.

[5] Garc 1' a J, Zalevsky Z, Fixler D. Synthetic aperture superresolution by speckle pattern projection[J]. Opt Exp, 2005, 13 (16) : 6 073-6 078.

[6] Alexandrov S A, Hillman T R, Gutzler T, et al. Synthetic aperture Fourier holographic optical microscopy [J]. Phys Rev Lett, 2006, 97 (16) : 168102.

[7] Guizar - Sicairos M, Fienup J R. Phase retrieval with transverse translation diversity: a nonlinear optimization approach[J]. Opt Exp, 2008, 16(10) : 7 264-7 278.

[8] Hoppe W, Strube G. Diffraction in inhomogeneous primary



(a) 5%; (b) 11%; (c) 20%; (d) 30%; (e) 45%; (f) 60%;
(g) 振幅分布情况; (h) 相位分布情况.

图 6 不同剪切面积的密文以及相应的重建图像的 Co 值
Fig. 6 Ciphertexts at different occlusion percentages and relationship between values of Co and occlusion percentages

- wave fields. 2. Optical experiments for phase determination of lattice interferences[J]. *Acta Crystallogr*,1969, A 25 : 502-507.
- [9] Shi Y S, Wang Y L, Zhang S G. Generalized ptychography with diverse probes[J]. *Chin Phys Lett*, 2013, 30 (5) : 054203.
- [10] Dong S, Shiradkar R, Nanda P, et al. Spectral multiplexing and coherent-state decomposition in Fourier ptychographic imaging[J]. *Biomed Opt Express*, 2014, 5 (6) : 1 757-1 767.
- [11] Zheng G. Fourier ptychographic imaging[J]. *IEEE Photonics Journal*,2014,6 (2) :0701207.
- [12] Horstmeyer R, Yang C. A phase space model of Fourier ptychographic microscopy[J]. *Opt Exp*,2014,22 (1) : 338-358.
- [13] Javidi B. Securing information with optical technologies[J]. *Physics Today*,1997,50 (3) : 27 – 32.
- [14] Refregier P,Javidi B. Optical image encryption based on input plane and Fourier plane random encoding [J]. *Opt Lett*, 1995,20 (7) : 767 – 769.
- [15] Liu S, Yu L, Zhu B. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering[J]. *Opt Commun*,2001,187 (1) : 57 – 63.
- [16] Situ G H, Zhang J J. Multiple -image encryption based on wavelength multiplexing [J]. *Opt Lett*, 2005 , 30 (11) : 1 306 – 1 308.
- [17] Shi Y S, Li T, Wang Y L, et al. Optical image encryption via ptychography[J]. *Opt Lett*,2013,38 (9) : 1 425 – 1 427.