基于双随机相位编码的非线性双图像加密方法

陈翼翔[1] 汪小刚[2]

([1] 浙江传媒学院电子信息学院, 浙江 杭州 310018
[2] 浙江农林大学理学院, 浙江 临安 311300)

摘要 提出了一种基于双随机相位编码技术的非线性双图像加密方法,并分析了其安全性。在该方法中,加密过程和解密过程以及加密密钥和解密密钥均不相同。加密过程具有非线性,解密过程则是线性的。将两幅待加密图像复合为复振幅图像,并利用双随机相位编码技术和切相傅里叶变换进行加密,加密过程中生成两个解密密钥,解密过程则在经典的基于 $4f$ 系统的双随机相位编码系统中完成。相比经典的双随机相位加密技术和基于切相傅里叶变换的单图像加密技术,该加密方法的安全性更高,它能够抵御最近提出的基于两步振幅-相位恢复算法的特定攻击。理论分析和仿真实验结果都证明了此加密方法的可行性和安全性。

关键词 图像处理;傅里叶光学;双随机相位编码;非线性加密;振幅-相位恢复算法

中图分类号 O438 **文献标识码** A **doi**: 10.3788/AOS201434.0710001

Nonlinear Double Images Encryption Based on Double Random Phase Encoding

Chen Yixiang[1] Wang Xiaogang[2]

([1] *School of Electronic Information, Zhejiang University of Media and Communications, Hangzhou, Zhejiang* 310018, *China*
[2] *School of Sciences, Zhejiang Agriculture and Forestry University, Lin'an, Zhejiang* 311300, *China*)

Abstract A new method of image encryption and decryption is proposed, where the encryption process is different from the decryption and the encryption keys are also different from the decryption keys. The encryption is nonlinear for the sake of security enhancement while the decryption is linear. Two original images are combined as a complex amplitude image and encrypted based on classical double random phase encoding (DRPE) and phase-truncated Fourier transform (PTFT). Two private keys are generated in the encryption process and the decryption can be performed by the double random phase encoding scheme. Compared with the classical DRPE and PTFT-based single-image encryption, the proposed method is more secure and has resistance against on the specific attack that is based on two-step amplitude-phase retrieval algorithm. Numerical simulations are carried out to demonstrate the validity and security of the proposed scheme.

Key words image processing; Fourier optics; double random phase encoding; nonlinear encryption; amplitude-phase retrieval

OCIS codes 100.2000; 100.2960; 100.4998

1 引 言

1995 年,美国 Connecticut 大学的学者 Refregier 等[1]提出的基于 $4f$ 系统的双随机相位编码技术是光学理论在信息安全领域的重大运用。在该技术的基础上,许多研究人员展开了多方面的深入研究,提出了大量新的图像加密方法[2-12]。但随着研究的深入,科研人员发现目前大多数光学图像加密技术,尤其是以双随机相位编码为典型代表的

收稿日期: 2014-01-21; **收到修改稿日期**: 2014-03-05

基金项目: 国家自然科学基金(61205006)、浙江省高等学校访问学者专业发展项目(FX2013103)、浙江传媒学院校级科研项目(ZC12XJY003)

作者简介: 陈翼翔(1979—),男,博士,讲师,主要从事激光光学和光信息安全等方面的研究。

E-mail: chenyix1979@163.com

对称光学加密体制(加密过程与解密过程、加密密钥与解密密钥均相同)由于存在着线性这一性质,系统的安全性存在极大的隐患[13-15]。2005 年,Carniecer 等[13]提出了一种针对双随机相位编码系统的选择密文攻击方法,破解了解密密钥;2006 年,Peng 等[14-15]提出了选择明文攻击和已知明文攻击的方法,破解了双随机相位加密系统。鉴于此,2008 年,Cai 等[16]提出了在双随机相位编码系统的频域增加振幅板的改进方案,用以抵御已知明文攻击。然而,该方法并没有从本质上改变加密系统的对称性,对于其他攻击方案,其安全性仍待检验。2012 年,He 等[17]构造了一种结合选择明文和已知明文的两步攻击方法破解了该系统。2010 年,Qin 等[18]提出了一种基于切相傅里叶变换的光学非线性密码系统。该加密系统去除了经典双随机相位编码系统的线性特点,有效地抵制了暴力攻击、选择明文等多种攻击,显示出了比传统的基于双随机加密的对称加密方法更高的安全性。然而,最近的研究发现基于切相傅里叶变换的单图像加密系统也存在安全隐患,当系统中的两个加密密钥作为公开密钥时,利用基于两步迭代振幅-相位恢复算法的特定攻击方法可以同时破解出原始信息和两个解密密钥[19]。

本文提出了一种基于双随机相位编码技术的非线性双图像加密方法。该方法的加密过程是非线性的,而解密过程则是线性的。在加密过程中,先将两幅待加密图像复合为复振幅图像,接着利用双随机相位编码技术和切相傅里叶变换进行加密。两个解密密钥在加密过程中生成,解密过程则在经典的基于 $4f$ 系统的双随机相位编码系统中完成。研究表明,该双图像加密方法除了能够抵抗暴力攻击、选择明文攻击之外,还能够抵御基于两步振幅-相位恢复算法的特定攻击。

2　加密方法的基本原理及安全性分析

2.1　图像的加密过程

基于经典的双随机相位加密的图像加密方法由于加密系统的线性和对称性,安全性存在问题,在加密过程中引入非线性,可以提高系统的安全性。双图像的加密过程如图 1 所示,$f_1(x,y)$ 和 $f_2(x,y)$ 表示待加密的两幅原始图像,$R_1(x,y)$、$R_2(u,v)$ 是作为公开密钥的两块随机相位板。其中,(x,y)、(u,v) 分别表示空间域的坐标和傅里叶频谱域的坐标。光学上,可以通过计算机控制的空间光调制器进行调制,使两幅图像先复合为复振幅信息,即

$$I(x,y)=f_1(x,y)\exp[2\pi i f_2(x,y)], \quad (1)$$

式中 $I(x,y)$ 代表加密系统中的输入信息。

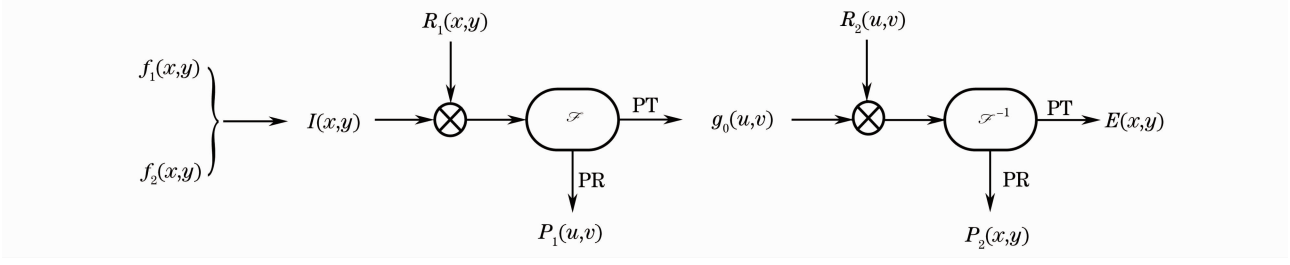

图 1　非线性加密过程流程图

Fig. 1　Flowchart of the nonlinear encryption process

$I(x,y)$ 与 $R_1(x,y)$ 相乘后进行一次傅里叶变换,理论上,可以利用数字全息技术得到变换后的复振幅分布,其振幅信息 $g_0(u,v)$ 和相位信息 $P_1(u,v)$ 可以分别表示成

$$g_0(u,v)=\mathrm{PT}\{\mathcal{F}[I(x,y)R_1(x,y)]\}, \quad (2)$$

$$P_1(u,v)=\mathrm{AT}\{\mathcal{F}[I(x,y)R_1(x,y)]\}, \quad (3)$$

式中 PT{ }代表相位切除运算或取振幅运算,即除去复振幅的相位信息而只保留振幅信息。AT{ }代表取相位运算,即除去复振幅的振幅信息而只保留相位信息。$\mathcal{F}[\ ]$代表傅里叶变换。振幅信息 $g_0(u,v)$ 与 $R_2(u,v)$ 相乘后进行一次逆傅里叶变换。类似地,变换后得到的复振幅信息的相位和振幅信息分别可以表示成

$$P_2(x,y)=\mathrm{AT}\{\mathcal{F}^{-1}[g_0(u,v)R_2(u,v)]\}, \quad (4)$$

$$E(x,y)=\mathrm{PT}\{\mathcal{F}^{-1}[g_0(u,v)R_2(u,v)]\}, \quad (5)$$

式中 $\mathcal{F}^{-1}[\ ]$代表逆傅里叶变换。

在该加密系统中,$E(x,y)$、$P_2(x,y)$ 分别作为加密结果和解密密钥加以保存,而另一个解密密钥是对 $P_1(u,v)$ 进行调制的结果。两个解密密钥分别可以表示为

$$K_1(x,y)=P_2(x,y), \quad (6)$$

$$K_2(u,v)=P_1(u,v)R_2^*(u,v), \quad (7)$$

式中 * 为复共轭运算。

2.2 解密过程

解密过程在经典的基于 $4f$ 系统的双随机相位编码系统中完成。如图 2 所示，密文 $E(x,y)$ 与私有密钥 $K_1(x,y)$ 相乘后进行一次傅里叶变换，由(4)～(6)式可知变换的结果为 $g_0(u,v)R_2(u,v)$。接着，$g_0(u,v)R_2(u,v)$ 与私有密钥 $K_2(u,v)$ 相乘后进行一次逆傅里叶变换，由(2)式、(3)式、(7)式容易证明：$\mathscr{F}^{-1}[g_0(u,v)R_2(u,v)K_2(u,v)] = I(x,y)R_1(x,y)$，利用公有密钥 $R_1(x,y)$，可以恢复出 $I(x,y)$，最后由(1)式可分别得到原始图像 $f_1(x,y)$ 和 $f_2(x,y)$。本加密系统的结构特点是加密过程非线性，而解密过程是线性的。因此，加密过程更适合采用数字方式，而解密过程则可通过光学方式或数字方式加以实现。

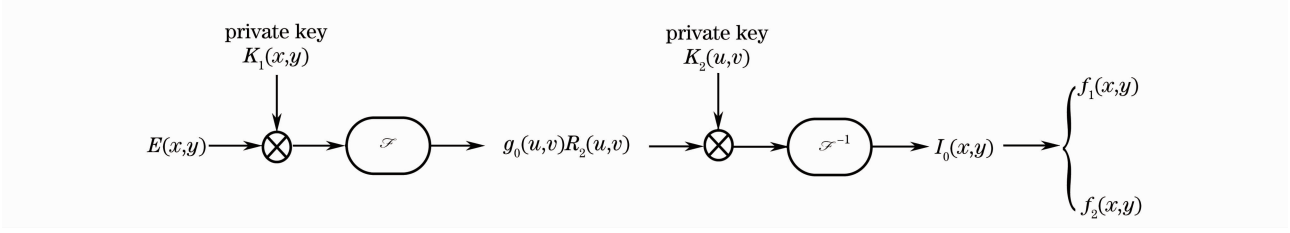

图 2 解密过程流程图

Fig. 2 Flowchart of the decryption process

2.3 安全性分析

本文提出的双图像加密方法的加密过程具有非线性。已经证明，基于双随机相位编码技术的非线性图像加密系统可以抵抗暴力攻击、选择明文攻击等在内的多种攻击方法[18]。因此，相比传统的基于双随机相位编码的对称加密方法，本文提出的双图像加密方法具有更高的安全性。但是需要指出的是，最近的研究表明，基于切相傅里叶变换的非线性单图像加密系统并不能抵御基于两步振幅-相位恢复算法的特定攻击[19]。特定攻击可以分为两步：1) 利用 $R_2(u,v)$ 和 $E(x,y)$ 通过迭代运算得到 $g_0(u,v)$ 的近似值 $g_0'(u,v)$；2) 利用 $R_1(x,y)$ 和 $g_0'(u,v)$，再次利用迭代振幅-相位恢复算法得到原始图像的近似值。不过由于本文提出的双图像加密方法中的输入信息为复振幅信息，因此，采用特定攻击方法进行攻击时，在步骤 2) 的迭代运算中作为限定值的 $R_1(x,y)$ 并不能真正代表输入面上的真实相位，错误的相位限定值将导致攻击的失败。所以，本文提出的非线性图像加密方法不仅实现了双图像的加密，而且具备了抵御特定攻击的能力。

3 仿真实验及结果

本文在 Matlab R2009b 软件平台上，验证了双图像加密方法的可行性和安全性。选择大小均为 256 pixel×256 pixel 的两幅原始图像“Lena”和“Rice”，分别如图 3(a)、(b)所示。仿真中两幅待加密图像均作归一化处理。根据加密流程图(图 1)所示，在两个相互统计独立的随机相位板的作用下，加密的结果如图 3(c)所示。两个私有密钥 K_1，K_2 的相位分布则如图 3(d)、(e)所示。

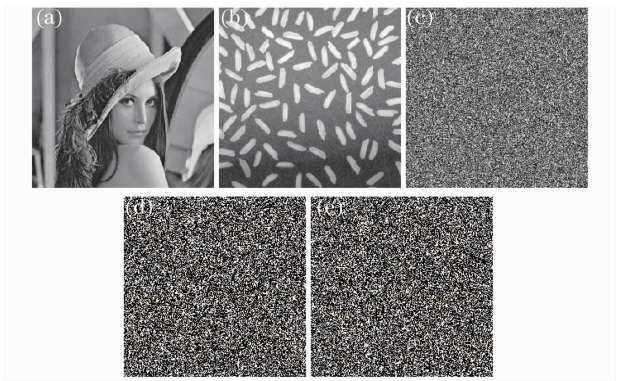

图 3 (a)原始图像 Lena；(b)原始图像 Rice；(c)密文；(d)私有密钥 K_1；(e)私有密钥 K_2

Fig. 3 (a) Primary image of Lena; (b) primary image of Rice; (c) encrypted image; (d) private key K_1; (e) private key K_2

使用均方误差函数(MSE，f_{MSE})衡量两幅图像品质上的差异，假设 f、f' 分别代表原始图像和恢复图像，则两者间的 MSE 可以表示为

$$f_{\mathrm{MSE}}(f,f') = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|f(i,j)-f'(i,j)|^2, \tag{8}$$

式中 M，N 表示图像的尺寸，$f(i,j)$ 和 $f'(i,j)$ 分别表示两幅振幅图像在像素点(i,j)的值。通过 MSE 也可以反映攻击者所进行的迭代运算的收敛性。

根据解密流程图(图 2)所示，正确使用上述两个密钥进行解密得到的结果分别如图 4(a)、(b)所示，它们对应的 MSE 值分别为 8.7365×10^{-32} 和

3.0518×10^{-5}。可以看出，两幅原始图像得到了非常好的恢复。

图 4　(a)原始图像 Lena 的恢复结果；(b)原始图像 Rice 的恢复结果

Fig. 4　(a) Decrypted result of Lena; (b) decrypted result of Rice

当解密密钥 K_1 出错而 K_2 正确的情况下得到的对应原始图像“Lena”和“Rice”的解密结果分别如图 5(a)、(b)所示；当解密密钥 K_2 出错而 K_1 正确的情况下对应原始图像“Lena”和“Rice”的解密结果分别如图 5(c)、(d)所示。仿真实验结果表明该加密系统具有抵抗暴力攻击的能力。

接下来研究系统对基于迭代振幅－相位恢复算法的特定攻击的抵御能力。攻击的步骤 1)中得到的振幅分布 $g_0'(u,v)$ 与 $g_0(u,v)$ 两者之间的 MSE 与迭代运算次数的关系如图 6 所示，迭代次数在 240 次以上，MSE 值基本保持不变；从特定攻击的步骤 2)中得到的攻击结果与输入信息 $I(x,y)$ 的振幅部分(原始图像 Lena)两者之间的 MSE 值与迭代运算次数的关系如图 7(a)所示。说明迭代次数越多，破解的图像质量越差。

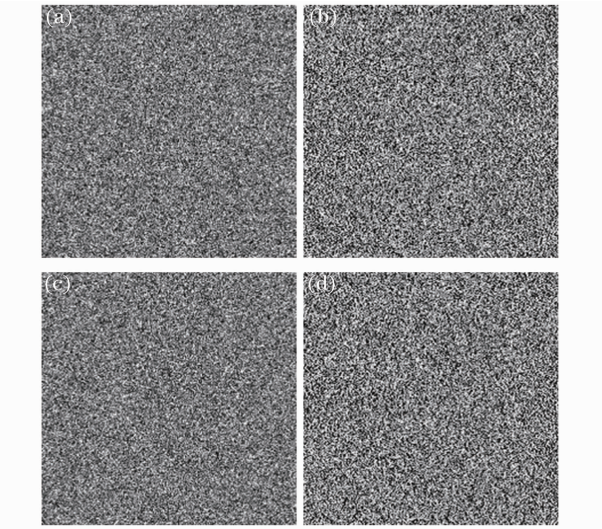

图 5　使用不正确的解密密钥所对应的结果。(a) K_1 错误时 Lena 的恢复结果；(b) K_1 错误时 Rice 的恢复结果；(a) K_2 错误时 Lena 的恢复结果；(b) K_2 错误时 Rice 的恢复结果

Fig. 5　Incorrectly decrypted results. (a) Decrypted result of Lena by using incorrect key of K_1; (b) decrypted result of Rice by using incorrect key of K_1; (c) decrypted result of Lena by using incorrect key of K_2; (d) decrypted result of Rice by using incorrect key of K_2

当特定攻击的步骤 1)的迭代次数设定为 300 次，步骤 2)采用不同的迭代次数时，最终得到的解

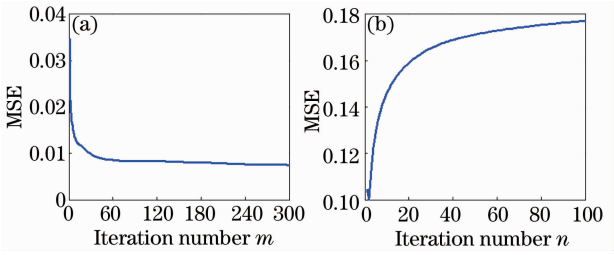

图 6　特定攻击两个步骤中得到的 MSE 与迭代次数的关系图。(a)步骤 1)；(b)步骤 2)

Fig. 6　Behavior of mean square error (MSE) versus number of iterations in (a) step 1) and (b) step 2)

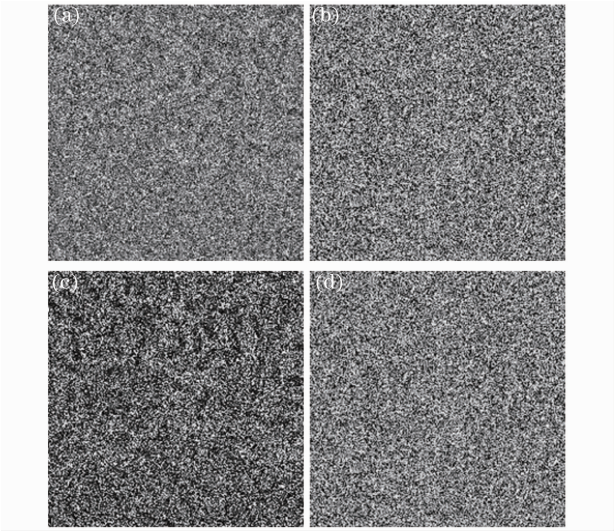

图 7　特定攻击的结果。(a)迭代次数分别为 $m=300$，$n=2$ 时对应于 Lena 的解密结果；(b)迭代次数分别为 $m=300$，$n=2$ 时对应于 Rice 的解密结果；(c)迭代次数分别为 $m=300$，$n=100$ 时对应于 Lena 的解密结果；(d)迭代次数分别为 $m=300$，$n=100$ 时对应于 Rice 的解密结果

Fig. 7　Recovered images with respect to different numbers of iterations. (a) $m=300$, $n=2$ (for the decryption of Lena); (b) $m=300$, $n=2$ (for the decryption of Rice); (c) $m=300$, $n=100$ (for the decryption of Lena); (d) $m=300$, $n=100$ (for the decryption of Rice)

密图像如图 7 所示。当步骤 2)中的迭代次数 $n=2$ 时，对应于 Lena 和 Rice 的解密结果分别如图 7(a)，(b)所示；当步骤 2)中的迭代次数 $n=100$ 时，对应于 Lena 和 Rice 的解密结果则分别如图 7(c)，(d)所示。由图 6 和图 7 可见，本文提出的加密方法能有效地抵御基于迭代振幅-相位恢复算法的特定攻击。

4 结 论

提出了一种基于双随机相位编码技术和切相傅里叶变换的非线性双图像加密方法。不同于经典的双随机相位编码技术，该双图像加密方法的加密过程是非线性的，而解密过程则是线性的。两个不同于加密密钥的解密密钥在加密过程中生成。仿真实验表明该方法能够抵御包括基于迭代振幅-相位恢复算法的特定攻击在内的多种攻击。

参 考 文 献

1 P Refregier, B Javidi. Optical image encryption based on input plane and Fourier plane random encoding [J]. Opt Lett, 1995, 20(7): 767－769.

2 G Unnikrishnan, J Joseph, K Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. Opt Lett, 2000, 25(12): 887－889.

3 Shutian Liu, Li Yu, Banghe Zhu. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering [J]. Opt Commun, 2001, 187(1-3): 57－63.

4 Guohai Situ, Jingjuan Zhang. Double random-phase encoding in the Fresnel domain [J]. Opt Lett, 2004, 29(14): 1584－1586.

5 Yu Bin, Peng Xiang. Optical image encryption based on cascaded phase retrieval algorithm [J]. Acta Optica Sinica, 2005, 25(7): 881－884.
于 斌，彭 翔. 基于级联相位恢复算法的光学图像加密[J]. 光学学报，2005，27(7)：881－884.

6 Zhengjun Liu, Shutian Liu. Random fractional Fourier transform [J]. Opt Lett, 2007, 32(15): 20881－2090.

7 Ran Tao, Jun Lang, Yue Wang. Optical image encryption based on the multiple-parameter fractional Fourier transform [J]. Opt Lett, 2008, 33(6): 581－583.

8 Shi Yishi, Zhang Jingjuan. Research on the phase retrieval algorithm used for multiple-image encryption with region multiplexing [J]. Acta Optica Sinica, 2009, 29(10): 2705－2708.
史祎诗，张静娟. 相位恢复算法用于分区复用多图像加密的研究[J]. 光学学报，2009，29(10)：2705－2708.

9 Jia Lijuan, Liu Zhengjun. Double image encryption algorithm based on random fractional Fourier transform [J]. Acta Photonica Sinica, 2009, 38(4): 1020－1024.
贾丽娟，刘正君. 基于随机分数傅里叶变换的双图像加密算法[J]. 光子学报，2009，38(4)：1020－1024.

10 Xiangfeng Meng, Luzhong Cai, Xianfeng Xu, *et al*.. Full-phase image encryption by two-step phase-shifting interferometry [J]. Optik, 2008, 119(9): 434－440.

11 Zhengjun Liu, Lie Xu, Chuang Lin, *et al*.. Image encryption by encoding with a nonuniform optical beam in gyrator transform domains [J]. Appl Opt, 2010, 49(29): 5632－5637.

12 Linfei Chen, Daomu Zhao, Fan Ge. Image encryption based on singular value decomposition and Arnold transform in fractional domain [J]. Opt Commun, 2013, 291: 98－103.

13 A Carnicer, M Montes-Usategui, S Arcos, *et al*.. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys [J]. Opt Lett, 2005, 30(13): 1644－1646.

14 Xiang Peng, Peng Zhang, Hengzheng Wei, *et al*.. Known-plaintext attack on optical encryption based on double random phase keys [J]. Opt Lett, 2006, 31(8): 1044－1046.

15 Wei Hengzheng, Peng Xiang, Zhang Peng, *et al*.. Chosen plaintext attack on double phase encoding encryption technique [J]. Acta Optica Sinica, 2007, 27(5): 824－829.
位恒政，彭 翔，张 鹏，等. 双随机相位加密系统的选择明文攻击[J]. 光学学报，2007，27(5)：824－829.

16 X C Cheng, L Z Cai, Y R Wang, *et al*.. Security enhancement of double-random phase encryption by amplitude modulation [J]. Opt Lett, 2008, 33(14): 1575－1577.

17 Wenqi He, Xiang Peng, Xiangfeng Meng. A hybrid strategy for cryptanalysis of optical encryption based on double-random phase-amplitude encoding [J]. Opt & Laser Technol, 2012, 44(5): 1203－1206.

18 Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. Opt Lett, 2010, 35(2): 118－120.

19 Xiaogang Wang, Daomu Zhao. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms [J]. Opt Commun, 2012, 285(6): 1078－1081.

栏目编辑：张浩佳