第 37 卷 第 5 期
2013 年 9 月

激 光 技 术
LASER TECHNOLOGY

Vol. 37, No. 5
September, 2013

文章编号：1001-3806(2013)05-0577-05

基于球面波照射的非对称光学图像加密

丁湘陵
（怀化学院 物理与信息工程系，怀化 418008）

摘要：为了克服基于相位截断傅里叶变换的非对称光学图像加密系统不能抵御已知明文攻击的缺陷，采用球面波的自带因子扰乱输入图像空间信息的方法实现图像的加解密，并通过理论分析和实验仿真进行了研究。结果表明，该方法既能抵御已知明文攻击和保持非线性特性，又能获得原系统加解密图像的效果，同时还能减少相位掩膜数量，简化系统设置。这一结果对于改进基于相位截断傅里叶变换的非对称光学图像加密系统的安全性是有帮助的。

关键词：信息光学；图像加密；球面波；已知明文攻击；非线性特性
中图分类号：TN911.73　　**文献标识码**：A　　**doi**：10.7510/jgjs.issn.1001-3806.2013.05.004

Asymmetric optical image cryptosystem based on spherical wave illumination

DING Xiang-ling
(Department of Physics and Information Engineering, Huaihua College, Huaihua 418008, China)

Abstract: In order to overcome the known plaintext attack which the asymmetric optical image cryptosystem based on phase-truncated Fourier transforms can not resist, an encryption method based on phase-truncated Fourier transforms was proposed by employing the phase factor of the spherical wave under the spherical wave illumination. The theoretical analysis and experiment results indicate that the proposed encryption method can maintain the asymmetric characteristic of the cryptosystem and avoid various types of the currently existing attacks, especially the known plaintext attack, which the asymmetric cryptosystem based on phase-truncated Fourier transforms can not resist. The results are helpful for the security improvement of the asymmetric optical image cryptosystem based on phase-truncated Fourier transform.

Key words: information optics; image encryption; spherical wave; known plaintext attack; asymmetric characteristic

引　言

伴随着计算机软硬件技术的快速发展和网络的广泛使用，信息安全问题变得越来越严峻。近年来，光学加密技术由于具有并行的内在特性和光学信号处理的多维特性，在某种意义上比数字方法更具有优越性，因而探索和开发光学加密技术具有更高的学术价值和应用价值。当前讨论最多的是基于 1995 年 REFREGIER 和 JAVIDI 提出的双随机相位编码加密(double random phase encoding, DRPE)技术[1]，例如分数傅里叶变换系统、扩展分数傅里叶变换系统和菲涅耳衍射系统等[2-10]。然而，这些基于 DRPE 的加密技术都是通过在加密过程中增加一系列额外的密钥来提供更多的信息安全，例如 DENG 等人提出利用球面波照射双随机相位加密系统使得球面波的波长和半径成为加密系统的额外密钥来提供更高的安全性[7-10]，但是，该方案依然基于 DRPE 加密技术，由此，它们特有的线性特性导致其不能抵抗某种特定的攻击，例如已知明文攻击或选择明文攻击等[11-14]。从加密学观点看，基于 DRPE 技术提出的加密方法[2-10]都是加密密钥和解密密钥相同的对称加密系统，在网络环境下对称加密系统容易遭受一些安全问题，例如密钥的安全分发和管理。同样，DENG 等人提出的使用球面波照射双随机相位加密技术仍然是对称加密系统，虽然该加密技术增加球面波的波长和半径作为加密密钥，但是在解密过程中依然需要球面波的波长和半径[7-10]，在网络环境下同样也容易遭受对称加密系统所遭受的安全问题。为了克服对称加密系统所具有的这些

基金项目：怀化市创新团队基金资助项目(2012-16)
作者简介：丁湘陵(1981-)，男，讲师，硕士，主要从事信息光学的研究。
E-mail：dingxl1981@163.com
收稿日期：2013-01-04；收到修改稿日期：2013-01-21

情况,WANG 等人提出基于相位截断傅里叶变换(phase-truncated Fourier transform, PTFT)的非对称加密系统[14]成为讨论的热点。该系统依然采用 4*f* 系统来实现:加密过程中通过使用相位截断处理和两个公开的随机相位掩膜产生具有实值和白噪声特性的密文;在解密过程中,使用在加密过程中利用振幅截断处理非线性产生的两个与加密密钥完全不同的解密密钥恢复原文[15]。尽管相位截断的非线性操作使得基于 PTFT 的非对称加密系统具有很强的健壮性,但是,当加密密钥作为公钥加密不同明文时,发现基于相位截断傅里叶变换的非对称加密系统不能抵御已知明文攻击。由此,提高基于相位截断傅里叶变换的非对称加密系统的安全性就势在必行。虽然可以通过采用不同的随机相位掩膜加密不同的明文来抵御已知明文攻击,但是,相位掩膜的制作过程非常复杂,针对这种情况,作者提出利用不同的球面波在输入平面和傅里叶平面照射来加密不同的明文抵御已知明文攻击,既能抵御已知明文攻击,又能获得同样的加密效果和省掉输入面的随机相位掩膜,同时,在实际操作中还能减少光能的损失和相应的噪声。

1 基于相位截断傅里叶变换的非对称加密系统

基于相位截断傅里叶变换的非对称加密系统[15]利用 4*f* 系统来实现。加密时,输入图像 $P(x,y)$ 在空域受到随机相位掩膜 $R_1(x,y)$(输入平面密钥)的调制,经过傅里叶变换,再经过非线性的相位截断操作后,在频域被随机相位掩膜 $R_2(u,v)$(频谱面密钥)滤波,经过逆傅里叶变换和非线性的相位截断操作后,在输出平面上得到密文,表示为:

$$\psi(x,y) = \mathrm{T}\{\mathscr{F}^{-1}[\mathrm{T}\{\mathscr{F}[P(x,y)\cdot R_1(x,y)]\}\cdot R_2(u,v)]\} \tag{1}$$

式中,$\psi(x,y)$ 表示频域密文,$R_1(x,y)$ 和 $R_2(u,v)$ 分别定义为 $\exp[\mathrm{i}2\pi b(x,y)]$ 和 $\exp[\mathrm{i}2\pi n(u,v)]$,$b(x,y)$ 和 $n(u,v)$ 是均匀分布在[0,1]上的两个独立噪声序列,T,$\mathscr{F}$ 和 $\mathscr{F}^{-1}$ 分别表示相位截断操作、傅里叶变换和傅里叶逆变换。其两个解密密钥 $W_1(x,y)$ 和 $W_2(u,v)$ 在加密过程中产生,产生过程如下:

$$W_2(u,v) = \mathrm{R}\{\mathscr{F}[P(x,y)\cdot R_1(x,y)]\} \tag{2}$$

$$W_1(x,y) = \mathrm{R}\{\mathscr{F}^{-1}[\mathrm{T}\{\mathscr{F}[P(x,y)\cdot R_1(x,y)]\cdot R_2(u,v)]\} \tag{3}$$

式中,R 表示振幅截断操作。

解密时将密文 $\psi(x,y)$ 置于 4*f* 系统的输入平面,在空域受到解密密钥 $W_1(x,y)$ 调制,经傅里叶变换和相位截断操作后,在频谱平面上用解密密钥 $W_2(u,v)$ 滤波,再经逆傅里叶变换和相位截断操作,即可恢复出明文 $P(x,y)$,产生过程如下:

$$P(x,y) = \mathrm{T}\{\mathscr{F}^{-1}[\mathrm{T}\{\mathscr{F}[\psi(x,y)\cdot W_1(x,y)]\}\cdot W_2(u,v)]\} \tag{4}$$

通过分析(2)式和(3)式,解密密钥与原始图像 $P(x,y)$ 和两个相位掩膜 $R_1(x,y)$ 和 $R_2(u,v)$ 相关。因此,任意选择的随机相位掩膜或者密钥都可能导致错误的解密。但是,使用公开的随机相位掩膜($R_1(x,y)$ 和 $R_2(u,v)$)和任意给定的明文-密文对,根据已知明文攻击原理,发现使用任意给定的明文-密文对获得的解密密钥去解密某个待解密的密文能获得原文。由此,作者从安全性的角度对其进行改进,利用不同的球面波照射输入平面和傅里叶平面加密不同的明文抵御已知明文攻击,既能获得原非对称加密系统同样的图像加解密效果,又能省去输入平面处的相位掩膜。

2 球面波照射下的非对称加密系统

作者提出的球面波照射下的非对称加密系统流程如图 1 所示,图中⊗表示乘法操作。首先,输入的图像 $P(x,y)$ 被球面波 $S_1(x,y)$ 照射,在紧靠输入平面后面得到的复振幅分布为 $P(x,y)\cdot S_1(x,y)$,其中,$S_1(x,y)$ 为球面波,其表达式表示为:

$$S_1(x,y) = C\exp\left[-\frac{\mathrm{i}k}{2z}(x^2+y^2)\right] \tag{5}$$

式中,C,$k=\dfrac{2\pi}{\lambda}$ 和 z 分别表示为一个无关紧要的可以忽略的系数、波数和球面波半径。由于 $S_1(x,y)$ 和随机相位掩膜 $R_1(x,y)$ 一样也是相位函数,因此它也具有扰乱输入图像空间信息的作用,这样用球面波照射输入图像所获得的效果与使用平行光照射

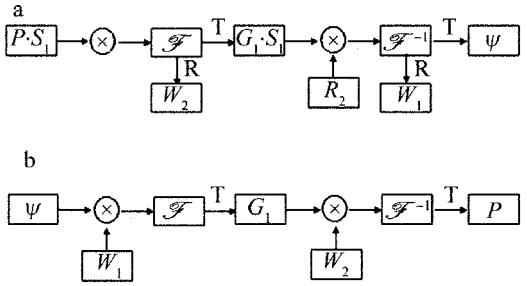

Fig. 1 Flowchart of the asymmetric cryptosystem based on spherical wave illumination
a—encryption process b—decryption process

输入图像再通过随机相位掩膜 $R_1(x,y)$ 调制产生的效果一样[7]。由此,就可以使用球面波本身所携带的相位因子来代替随机相位掩膜 $R_1(x,y)$,这样做不仅不会影响图像的解密,还能使得对于不同的明文,采用不同的球面波照射,既避免了已知明文攻击,又在输入平面省掉了一块随机相位掩膜。这样,输入图像在空域内被球面波 $S_1(x,y)$ 所调制,完成空间域的编码,即:

$$S_m(x,y) = P(x,y) \cdot S_1(x,y) \tag{6}$$

然后对调制后的物面波函数 $S_m(x,y)$ 进行傅里叶变换和相位截断操作得到:

$$G_1(u,v) = \mathrm{T}\{\mathscr{F}[S_m(x,y)]\} \tag{7}$$

最后,在频谱面上依然用同样的球面波照射,并用一个随机相位掩膜 $R_2(u,v)$ 对其滤波,再进行一次傅里叶逆变换和相位截断操作,得到最后的加密图像:

$$\psi(x,y) = \mathrm{T}\{\mathscr{F}[G_1(u,v) \cdot S_2(u,v) \cdot R_2(u,v)]\} \tag{8}$$

式中,$S_2(u,v)$ 的定义如(5)式所示,$R_2(u,v)$ 为 $\exp[\mathrm{j}\varphi(u,v)]$,$\varphi(u,v)$ 表示均匀分布在 $(0,2\pi)$ 的彼此独立的随机函数,(u,v) 为频率域坐标。同时,两个解密密钥在加密过程中通过振幅截断操作获得:

$$W_1(x,y) = \mathrm{R}\{\mathscr{F}^{-1}[G_1(u,v) \cdot S_2(u,v) \cdot R_2(u,v)]\} \tag{9}$$

$$W_2(u,v) = \mathrm{R}\{\mathscr{F}[S_m(x,y)]\} \tag{10}$$

解密过程如图 1b 所示,将密文 $\psi(x,y)$ 置于输入面,使用解密密钥 $W_1(x,y)$ 对其滤波,经过傅里叶变换和相位截断操作得到:

$$\mathrm{T}\{\mathscr{F}[\psi(x,y) \cdot W_1(x,y)]\} = G_1(u,v) \tag{11}$$

再对 $G_1(u,v)$ 使用解密密钥 $W_2(u,v)$ 对其滤波,经过傅里叶逆变换和相位截断操作得到原图像,过程为:

$$\mathrm{T}\{\mathscr{F}^{-1}[G_1(u,v) \cdot W_2(u,v)]\} = P(x,y) \tag{12}$$

从(11)式和(12)式可以很容易发现:由于使用非线性的相位截断操作,在解密过程中,对于获得正确的解密结果并不需要球面波 $S_1(x,y)$ 与加密密钥 $R_2(u,v)$。同时,在整个加密过程中,作者仅仅改变照明方式,由平行光改为球面波照射,且在输入面省略一块随机相位掩膜,而解密过程与原基于 PTFT 的加密系统的解密过程一样。由此,通过对于不同的明文使用不同的球面波照射(通过更改球面波的半径或波长)既能避免被已知明文攻击,又能保持非对称加密系统所具有的非线性特性,还能在实际操作中减少光能的损失和相应的噪声。

3 计算机仿真实验

为了验证方法的可行性,作者进行了仿真实验,并对两种方法所获得的结果进行了比较,见图 2。实验中,采用波长为 600nm 的会聚球面波来照射,

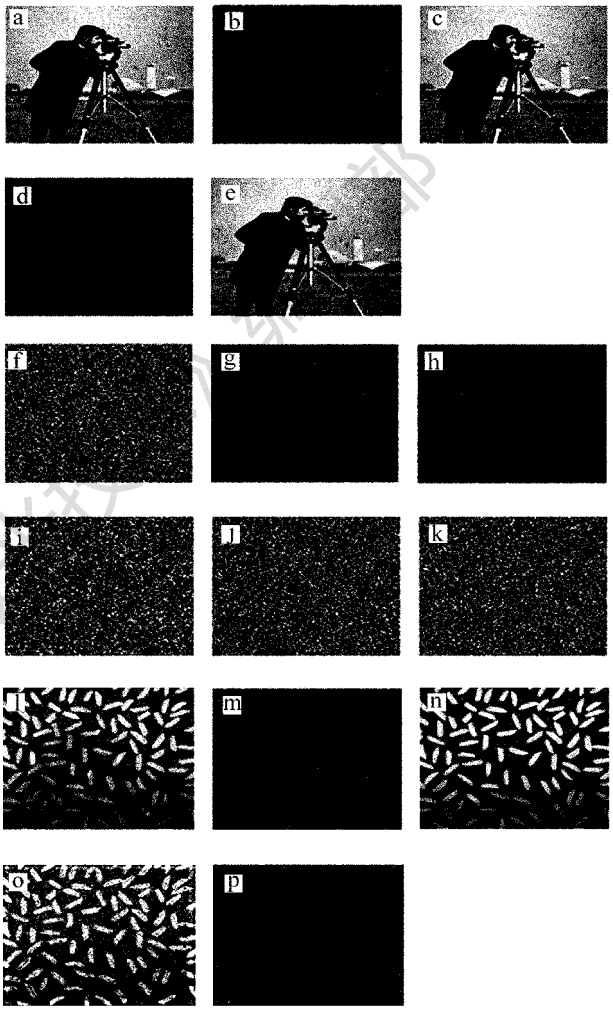

Fig. 2 Computer simulation results

a—original image b—encryption image of the PTFT-based asymmetric cryptosystem c—decryption image of the PTFT-based asymmetric cryptosystem d—encryption image of the asymmetric cryptosystem based on spherical wave illumination e—decryption image of the asymmetric cryptosystem based on spherical wave illumination f—no keys of the PTFT-based asymmetric cryptosystem g—arbitrary phase mask of the PTFT-based asymmetric cryptosystem h—encryption keys of the PTFT-based asymmetric cryptosystem i—no keys of the asymmetric cryptosystem based on spherical wave illumination j—arbitrary phase mask of the asymmetric cryptosystem based on spherical wave illumination k—encryption keys of the asymmetric cryptosystem based on spherical wave illumination l—chosen plaintext attack of the PTFT-based asymmetric cryptosystem m—procession result of Fig. 2l n—chosen plaintext o—chosen plaintext attack of the asymmetric cryptosystem based on spherical wave illumination p—procession result of Fig. 2o

球面波的半径为 4cm,取图像的尺度为 2cm × 2cm,像素为 256 × 256,在 MATLAB 7.0 下仿真。图 2a 为原始图像。图 2b ~ 图 2e 分别是对基于 PTFT 的非对称加密系统和基于球面波照射的非对称加密系统对灰度图像进行加密和解密所得的仿真结果。分别对比图 2b、图 2d 和图 2c、图 2e 可以看出,用球面波自带的相位因子取代输入面密钥 $R_1(x,y)$ 及频谱面密钥 $R_2(u,v)$ 结合进行图像加密和解密的效果与基于 PTFT 的非对称加密系统加密和解密效果一样。

图 2f ~ 图 2k 证明基于球面波照射的非对称加密系统与基于 PTFT 的非对称加密系统同样能抵御无密钥解密、任选随机相位解密和加密密钥解密。图 2f ~ 图 2h 分别显示基于 PTFT 的非对称加密系统抵御无密钥解密、任选随机相位解密和加密密钥解密的仿真结果;图 2i ~ 图 2k 分别显示基于球面波照射的非对称加密系统抵御无密钥解密、任选随机相位解密和加密密钥解密的仿真结果。

图 2l ~ 图 2p 是基于 PTFT 的非对称加密系统和基于球面波照射的非对称加密系统进行已知明文攻击的仿真结果。图 2l 显示基于 PTFT 的非对称加密系统进行已知明文攻击的仿真结果;图 2m 是图 2l 使用数字方法(盲去卷积)处理后的解密结果;图 2n 是已知的明文;图 2o 显示基于球面波照射的非对称加密系统进行已知明文攻击的仿真结果;图 2p 是图 2o 经过与图 2m 同样的处理技术处理后的解密结果。从图 2l 和图 2m 可以很明显地得到基于 PTFT 的非对称加密系统不能抵御已知明文攻击,而图 2o 和图 2p 证明了基于球面波照射的非对称加密系统虽然只使用了一块相位掩膜 $R_2(u,v)$,但是由于采用球面波照射,球面波的相位因子替代输入面的随机相位掩膜,扰乱输入图像的空间信息,却能很好地抵御已知明文攻击。

从图 2l ~ 图 2p 的仿真结果可以很显然地得出:在不知道球面波任何信息的情况下是无法使用已知明文攻击获得明文的。但是,攻击者在已知加密算法和公钥的情况下,可能通过任意选择球面波使用已知明文攻击原理来恢复明文。因此,有必要研究波长和半径的变化对攻击结果的灵敏度问题。为了进一步说明波长和半径的变化对攻击结果的灵敏度,使用均方误差(mean-square error,MSE)来说明:

$$E_{\mathrm{MSE}} = \frac{1}{L}\sum_{i=1}^{L}(f_i - |f_i'|)^2 \qquad (13)$$

式中,L 表示图像中像素点的总个数,f_i 和 f_i' 分别表示图像中的某个像素点灰度值和对应的恢复结果值。首先,为了说明波长的灵敏度问题,作者仅仅修改球面波的波长从 −4nm 到 4nm,步长 $\Delta\lambda$ = 0.5nm,而保持球面波的半径不变(即球面波半径为 4cm)。原始图像与攻击结果间的 MSE 与波长的变化关系如图 3a 所示。图 3a 显示攻击结果对于波长的变化非常敏感。同样,为了说明半径的灵敏度问题,作者也仅仅修改球面波的半径从 −100μm到 100μm,步长 Δz = 1μm,而保持球面波的波长不变(即球面波波长为 600nm)。原始图像与攻击结果间的 MSE 与半径的变化关系如图 3b 所示。图 3b 显示 MSE 随着 $|z|$ 的增加而增加。由上面的结果可知,攻击者即使任意选择球面波也无法恢复原文。

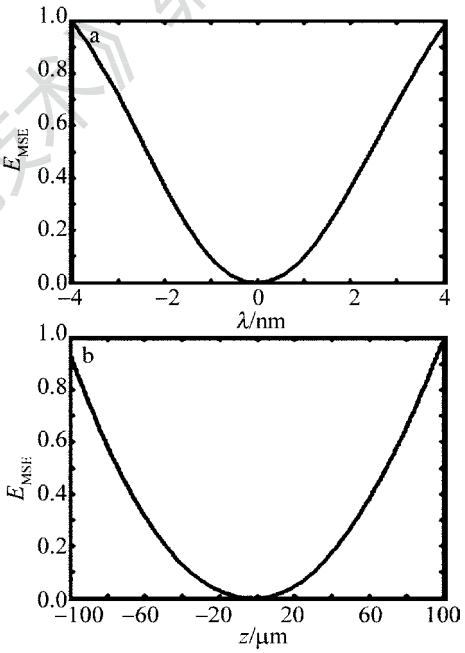

Fig. 3 a—E_{MSE} variation versus wavelength λ b—E_{MSE} variation versus displacement z

4 结 论

根据新提出的非对称加密系统 PTFT 不能抵抗已知明文攻击的情况出发,结合球面波的自带相位因子,提出用球面波的相位因子替代 $R_1(x,y)$ 进行图像加密,实验结果和安全性分析表明,基于球面波照射的非对称加密系统在保留了原基于 PTFT 的非对称加密系统优点的同时,克服其被已知明文攻击破解的缺陷,取得了良好的加密效果。相对于原 PTFT 系统而言,在安全性上有明显改善。因此,系统在图像加密应用中将具有良好应用前景。

参 考 文 献

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

[2] SITU G H, ZHANG J J. Double random phase encoding in the Fresnel domain[J]. Optics Letters,2004,29(14):1584-1586.

[3] LIN R, LIU Q N, ZHANG C L. A new fast algorithm for gyrator transform[J]. Laser Technology, 2012, 33(1): 50-53 (in Chinese).

[4] NISHCHAL N K, JOSEPH J, SIGN H K. Optical encryption using cascaded extended fractional Fourier transform[J]. Optical Memory & Neural Networks,2003,12(2): 139-145.

[5] HWANG H E, CHANG H T, LIE W N. Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems[J]. Optics Express, 2009,17(16):13700-13710.

[6] HENNELLY B, SHERIDANJ T. Optical image encryption by random shifting in fractional Fourier domains[J]. Optics Letters, 2003,28(4): 269-271.

[7] DENG X P. Optical image encryption using double phase mask based on spherical wave illumination[J]. Laser Technology, 2006,30(4):442-444(in Chinese).

[8] DENG X P, XIANG G X, WANG Sh F. Optical image encryption using only one random phase mask based on spherical wave illumination[J]. Laser Journal,2005,26(5): 52-53(in Chinese).

[9] DENG X P, ZOU K. Optical image encryption using one random phase mask based on spotlight illumination in the Fresnel domain [J]. Laser Technology,2006,30(3):327-328(in Chinese).

[10] DENG X P. Optical image encryption based on asymmetric abnormal Fourier transform[J]. Journal of Applied Optics,2007,28(3):262-264(in Chinese).

[11] PENG X, ZHANG P, WEI H Zh, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. Optics Letters,2006,31(8):1044-1046.

[12] PENG X, WEI H Zh, ZHANG P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain [J]. Optics Letters,2006,31(8):3261-3263.

[13] GOPINATHAN U, MONAGHAN D S, NAUGHTON T J, *et al*. A known-plaintext heuristic attack on the Fourier plane encryption [J]. Optics Express,2006,14(8):3181-3186.

[14] FRAUEL Y, CASTRO A, NAUGHTON T J, *et al*. Resistance of the double random phase encryption against various attacks[J]. Optics Express,2007,15(16):10253-10265.

[15] WANG Q, PENG X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Letters, 2010, 35(2): 118-120.