文章编号：1001-3806(2014)04-0561-04

非对称光学图像加密系统的已知公钥攻击

丁湘陵，袁 倩，张乐冰
（怀化学院 物理与信息工程系，怀化 418008）

摘要：为了破解基于相位截断傅里叶变换的非对称光学图像加密系统，提出一种已知公钥的攻击方法，并通过理论分析和实验仿真进行了研究。结果表明，在已知公钥的攻击下，攻击者可通过获取通用解密密钥恢复基于相位截断傅里叶变换的非对称光学图像加密系统的明文，并取得了较好的破解效果。在整个攻击的实施过程中，除了公开的加密密钥，无需额外的资源，同时攻击难度大大降低，因此更具实际意义。

关键词：信息光学；光学信息安全；非对称光学图像加密；密码分析学；已知公钥攻击
中图分类号：TN911.73 **文献标志码**：A **doi**：10.7510/jgjs.issn.1001-3806.2014.04.025

Known-public key attack on asymmetric optical image cryptosystem

DING Xiangling, *YUAN Qian*, *ZHANG Lebing*
(Department of Physics and Information Engineering, Huaihua College, Huaihua 418008, China)

Abstract: In order to break the asymmetric optical image cryptosystem based on phase-truncated Fourier transforms, known-public key attack method was proposed. Through theoretical analysis and experimental simulation, an attacker can get the general decryption key, recover the plaintext of asymmetric optical image encryption system based on phase truncation Fourier transform and achieve the good crack effect under the known public key attack. During the whole attack process, the method needs anything except for the public keys and the difficulty of implementation is also reduced. The results show this method has the practical significance.

Key words: information optics; optical information security; asymmetric optical image encryption; cryptanalysis; known-public key attack

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，由于光学加密技术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和应用价值。当前讨论最多的都是基于 1995 年 REFREGIER 和 JAVIDI 提出的双随机相位编码加密技术[1]（double random phase encoding technique, DRPE），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[2-7]。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。但是，它们依然基于 DRPE 加密技术，因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，选择明文攻击或唯密文攻击等[8-11]。从加密学观点看，基于 DRPE 技术提出的加密方法[2-7]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。为了克服这种情况，2010 年 WANG 和 PENG 等人利用相位截断的非线性操作改变 DRPE 的线性特性，并提出基于相位截断傅里叶变换（phase-truncated Fourier transform, PTFT）的非对称光学图像加密系统[12]。在该系统的加密过程中，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，使用两个加密过程中利用振幅截断处理非线性产生的与加密密钥完全不同的解密

资助项目：湖南省教育厅一般项目资助项目(13C715)；怀化市创新型人才团队项目资助项目(2012-16；2013-3)

作者简介：丁湘陵(1981-)，男，硕士，讲师，主要研究方向为信息光学、数字图像处理、软件形式化方法。
E-mail：dingxl1981@163.com

收稿日期：2013-08-19；收到修改稿日期：2013-09-27

密钥来恢复原文[12-13]。尽管相位截断的非线性操作使得基于 PTFT 的非对称光学图像加密系统具有很强的健壮性,可是 WANG 和 ZHAO 等人通过“特殊攻击”的办法可以分析得到非对称光学图像加密系统的明文和解密密钥[14]。“特殊攻击”需要攻击者首先截获密文,再在攻击实施过程中使用傅里叶迭代算法恢复明文和解密密钥,难度较大且复杂。

本文中通过分析非对称光学图像加密系统的安全性提出一种已知公钥的攻击方法。相对于 WANG 和 ZHAO 等人提出的基于傅里叶迭代算法的“特殊攻击”[14],本文中所提出的攻击方法仅仅只需要公开的加密密钥,从而获得非对称光学图像加密系统的通用解密密钥,再利用该通用解密密钥破解非对称光学图像加密系统,恢复明文。整个攻击过程实施的难度大大降低,除了公开的加密密钥,无需额外的资源。

1 非对称光学图像加密系统的已知公钥攻击

1.1 非对称光学图像加密系统

基于相位截断傅里叶变换的非对称光学图像加密系统也同样利用 4f 系统来实现。在加密过程中,输入图像 $f(x,y)$ 首先在空间域受到随机相位掩膜 $R_1(x,y)$(输入平面密钥)的调制;调制后的图像经过傅里叶变换和非线性的相位截断操作后,在频率域被随机相位掩膜 $R_2(u,v)$(频谱面密钥)滤波;滤波后的图像经过傅里叶逆变换和非线性的相位截断操作后,在输出平面上得到密文。整个加密过程表示为:

$$s_1(u,v) = \mathrm{PT}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\} \quad (1)$$

$$s(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}[s_1(u,v)\cdot R_2(u,v)]\} \quad (2)$$

式中,$f(x,y)$,$s_1(u,v)$ 和 $s(x,y)$ 分别表示输入图像、傅里叶平面的光强分布和密文,$R_1(x,y)$ 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,PT{},$\mathscr{F}${} 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。

在加密过程中同时也会产生两个解密密钥 $W_1(x,y)$ 和 $W_2(u,v)$,产生过程如下:

$$W_2(u,v) = \mathrm{PR}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\} \quad (3)$$

$$W_1(x,y) = \mathrm{PR}\{\mathscr{F}^{-1}[\mathrm{PT}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\}\cdot R_2(u,v)]\} \quad (4)$$

式中,PR{} 表示振幅截断操作。

解密过程中,首先将密文 $s(x,y)$ 置于非对称光学图像加密系统的输入平面,在空间域受到解密密钥 $W_1(x,y)$ 的调制;调制后的密文经过傅里叶变换和相位截断操作后,在频率域用解密密钥 $W_2(u,v)$ 滤波;滤波后的结果再经傅里叶逆变换和相位截断操作,就能恢复出明文 $f(x,y)$。整个解密过程产生如下:

$$s_1(u,v) = \mathrm{PT}\{\mathscr{F}[s(x,y)\cdot W_1(x,y)]\} \quad (5)$$

$$f(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}[s_1(u,v)\cdot W_2(u,v)]\} \quad (6)$$

1.2 非对称光学图像加密系统的已知公钥攻击

在对密码系统进行安全性分析时,通常认为攻击者已经截获所需的密文,同时知晓密码系统加密、解密算法的整个工作原理[15]。下面利用本文中提出的已知公钥攻击方法来分析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。假定攻击者已经获取公钥 $R_1(x,y)$ 和 $R_2(u,v)$,并且选择一幅幅值全为 1 的实值图像,攻击过程由如下两个步骤组成。

1.2.1 *利用已知公钥获得通用解密密钥* 在已知公钥($R_1(x,y)$ 和 $R_2(u,v)$)的条件下,攻击者利用一幅幅值全为 1 的原始实值图像 $c(x,y)$,对 $c(x,y)$ 使用已知公钥($R_1(x,y)$ 和 $R_2(u,v)$)在空间域调制和频率域滤波,利用振幅截断操作获取通用解密密钥,步骤如下:

$$U_1(x,y) = \mathrm{PR}\{\mathscr{F}^{-1}[\mathrm{PT}\{\mathscr{F}[R_1(x,y)]\}\cdot R_2(u,v)]\} \quad (7)$$

$$U_2(u,v) = \mathrm{PR}\{\mathscr{F}[c(x,y)\cdot R_1(x,y)]\} = \mathrm{PR}\{\mathscr{F}[R_1(x,y)]\} \quad (8)$$

式中,$R_1(x,y)$ 定义为 $\exp[\mathrm{i}2\pi b(x,y)]$,$R_2(u,v)$ 定义为 $\exp[\mathrm{i}2\pi n(u,v)]$,$b(x,y)$ 和 $n(u,v)$ 是均匀分布在[0,1]上的两个独立噪声序列。

1.2.2 *利用通用解密密钥获得明文* 由第 1.2.1 节中得到,通过利用(7)式和(8)式能获取进行解密所需的通用解密密钥 $U_1(x,y)$ 和 $U_2(u,v)$。而本文中所提出的攻击方法就是在解密过程中将通用解密密钥 $U_1(x,y)$ 和 $U_2(u,v)$ 分别替换(5)式和(6)式中的解密密钥 $W_1(x,y)$ 和 $W_2(u,v)$,而解密过程不作任何改变。破解过程如下:

$$s_1'(u,v) = \mathrm{PT}\{\mathscr{F}[s(x,y)\cdot U_1(x,y)]\} = \mathrm{PT}\{\mathscr{F}\{\mathscr{F}^{-1}[s_1(u,v)\cdot R_2(u,v)]\cdot B_1(x,y)\}\} \quad (9)$$

$$f'(x,y) = \mathrm{PT}\{\mathscr{F}^{-1}[s_1(u,v)\cdot U_2(u,v)]\} =$$

$$\mathrm{PT}\{\mathscr{F}^{-1}\{\mathscr{F}[f(x,y)\cdot R_1(x,y)]\cdot B_2(u,v)\}\} \tag{10}$$

式中，$B_1(x,y)$和$B_2(u,v)$为模糊因子，表示如下：

$$B_1(x,y)=\frac{W_1(x,y)}{U_1(x,y)}=\frac{\mathrm{PR}\{\mathscr{F}^{-1}[R_2(u,v)]\}}{\mathrm{PR}\{\mathscr{F}^{-1}[s_1(u,v)]\otimes\mathscr{F}^{-1}[R_2(u,v)]\}} \tag{11}$$

$$B_2(u,v)=\frac{W_2(u,v)}{U_2(u,v)}=\frac{\mathrm{PR}\{\mathscr{F}[R_1(x,y)]\}}{\mathrm{PR}\{\mathscr{F}[f(x,y)]\otimes\mathscr{F}[R_1(x,y)]\}} \tag{12}$$

式中，⊗表示卷积操作。从(11)式和(12)式可以发现，如果傅里叶平面的光强分布$s_1(u,v)$和输入图像$f(x,y)$具有大量低频分量，$\mathscr{F}^{-1}[s_1(u,v)]$和$\mathscr{F}[f(x,y)]$的取值范围将很窄，从而使得$B_1(x,y)$和$B_2(u,v)$趋向于1。由此可见，破解效果的好坏主要由傅里叶平面的光强分布$s_1(u,v)$和输入图像$f(x,y)$的频率分布来决定，当输入图像为实值图像且具有大量低频分量时，将能得到更好的破解效果。

2　实验仿真

为验证本文中提出的已知公钥攻击方法的有效性，在 MATLAB 7.0 环境下进行仿真。首先利用已经公开的用于加密的两块随机相位掩膜$R_1(x,y)$和$R_2(u,v)$(如图 1a 和图 1b 所示)，应用相位截断操作获得通用解密密钥；然后利用通用解密密钥和非对称光学图像加密系统的解密过程解密截获的密文，从而得到明文。图 2a 是灰度实值明文图像，图 2b 是图 2a 加密后的密文，图 2c 是使用本文中所提方法破解后的结果。图 3a 是二值明文图像，图 3b 是图 3a 加密后的密文，图 3c 是使用本文中所提方法破解后的结果。图 4a 是通过低频滤波处理的具有大量低频分量的灰度实值明文图像，图 4b 是图 4a 加密后的密文，图 4c 是使用本文中所提方法破解后的结果。由图 2 ~ 图 4 可知，无论明文图像是否具有大量低频分量，本文中提出的已知公钥攻击方法都能获得较好的破解效果。

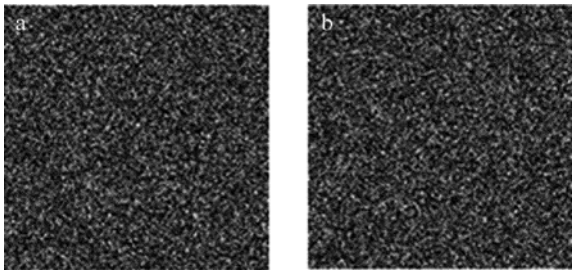

Fig. 1　Two public random phase masks of asymmetric optical cryptosystem
a—$R_1(x,y)$　b—$R_2(u,v)$

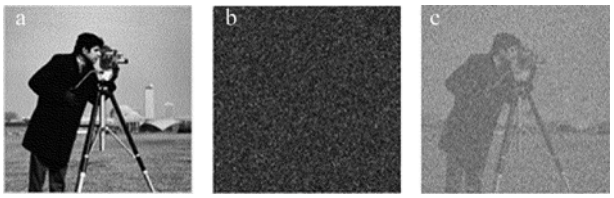

Fig. 2　The simulation results of gray-plaintext image
a—original cameraman image　b—encrypted cameraman image　c—the result of the known-public key attack

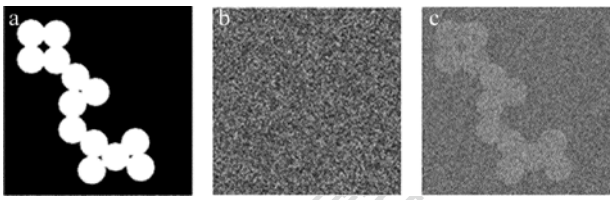

Fig. 3　The simulation results of binary-plaintext image
a—original circle image　b—encrypted circle image　c—the result of the known-public key attack

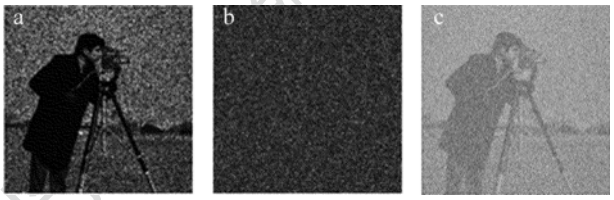

Fig. 4　The simulation results of filtered-plaintext image
a—filtered-plaintext image　b—encrypted image　c—the result of the known-public key attack

为进一步说明本文中所提攻击方法的破解效果，引入归一化均方误差(normalized mean square error, NMSE)N和图像逼真度(image fidelity, IF)I来评价破解结果的质量。分别定义如下：

$$N=\frac{\sum_{i=1}^{L}(\psi_i-|\psi_i'|)^2}{\sum_{i=1}^{L}\psi_i^2} \tag{13}$$

$$I=1-N \tag{14}$$

式中，ψ_i和ψ_i'分别表示图像中的某个像素点灰度值和对应的破解结果值，L表示图像中具有的像素总数。由(13)式和(14)式可知，归一化均方误差值越小，破解图像与原始图像的差异就越小，图像逼真度值就越高。根据(13)式和(14)式对灰度图像、二值图像和通过低频滤波处理的具有大量低频分量的灰度实值明文图像进行 NMSE 和 IF 值计算，计算结果见表 1。

从表 1 可以看出，使用已知公钥攻击方法得到

Table 1 Calculation results

	NMSE	IF
gray image	0.1714	0.8286
binary image	0.9891	0.0109
filtered image	0.0428	0.9572

的解密结果,灰度图像的解密效果比二值图像解密效果更好。主要的原因在于灰度图像的模糊因子 $B_1(x,y)$ 和 $B_2(u,v)$ 的平均结果分别为 2.9172 和 2.6137;二值图像的模糊因子 $B_1(x,y)$ 和 $B_2(u,v)$ 的平均结果分别为 6.4703 和 8.5429;而通过低频滤波处理的具有大量低频分量的灰度实值明文图像的模糊因子 $B_1(x,y)$ 和 $B_2(u,v)$ 的平均结果分别为 0.9804 和 0.9171。由此可得,模糊因子值越逼近 1,破解效果越好,仿真结果与理论推导一致。

3 结 论

阐述了基于相位截断傅里叶变换的非对称光学图像加密系统的已知密钥攻击方法的理论推导过程,虽然推导出的通用解密密钥与真实密钥相差一个模糊因子,但如果输入图像是实值图像且具有大量低频分量,其模糊因子基本上逼近 1,从而可以达到较好的破解效果。通过模拟实验证明,虽然相位截断的非线性操作使得基于 PTFT 的非对称光学图像加密系统具有很强的健壮性,但是,一旦将加密密钥公布出来,通过使用已知公钥攻击方法依然能恢复原图像,所以其安全性并没有提高。同时,与特殊攻击方法相比,本文中提出的已知密钥攻击方法只需要公开的加密密钥,无需额外的资源,因此更具实际意义。

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, 36(1):50-53(in Chinese).

[4] WANG X G, ZHAO D M, CHEN L F. Image encryption based on extended fractional Fourier transform and digital holography technique[J]. Optics Communications, 2006, 260(2): 449-453.

[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] DENG X P, ZHAO D M. Multiple-image encryption using phase retrieve algorithm and inter-modulation in Fourier domain[J]. Optics and Laser Technology, 2012, 44(2):374-377.

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

[8] PENG X, WEI H Zh, ZHANG P. Chosen plaintext attack on double random-phase encoding in the Fresnel domain [J]. Acta Physica Sinica,2007, 56(7):3924-3930 (in Chinese).

[9] PENG X, ZHANG P, WEI H Zh, *et al*. Known-plaintext attack on double phase encoding encryption technique [J]. Acta Physica Sinica, 2006, 55(3):1130-1136 (in Chinese).

[10] WEI H Zh, PENG X, ZHANG P, *et al*. Chosen-Plaintext attack on double phase encoding encryption technique [J]. Acta Optica Sinica,2007,27(5):824-829 (in Chinese).

[11] PENG X, TANG H Q, TIAN J D. Ciphertext-only attack on double random phase encoding optical encryption system [J]. Acta Physica Sinica,2007, 56(5):2629-2636 (in Chinese).

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

[13] DING X L. Asymmetric optifcal image cryptosystem based on spherical wave illumination[J]. Laser Technology,2013,37(5): 577-581 (in Chinese).

[14] WANG X G, ZHAO D M. A specific attack on the asymmetric cryptosystem based on the phase-truncated Fourier trans-forms [J]. Optics Communications, 2012,285(6):1078-1081.

[15] STALLINGS W. Cryptography and network security: principles and practice [M]. 2nd ed. Upper Saddle River, New Jersey, USA: Prentice Hall, 1999:24-26.