文章编号：1001-3806(2009)04-0433-04

# 基于菲涅耳域光学图像加密系统的解密研究

肖永亮[1]，刘 强[1]，袁 胜[1]，周 昕[1]*，赵晓军[1]，杨泽后[2]，陈 涌[2]，周鼎富[2]
（1. 四川大学 电子信息学院，成都 610064；2. 西南技术物理研究所，成都 610041）

**摘要**：为了研究菲涅耳域光学图像加密系统的解密过程，提出了一种根据对称图像加密密文恢复原图像的方法。采用密文全息的逆菲涅耳变换重构出频谱强度，用CCD接收后送入计算机，根据离散菲涅耳变换的相关和复卷积的性质，对其系数进行分类和排列，可以恢复出入射光波，即可恢复原图像。并研究了对称偏差对解密图像质量的影响。结果表明，此方法可以通过离散菲涅耳衍射解密出原对称图像。

**关键词**：信息光学；双随机加密；菲涅耳衍射；自相关；复卷积；对称图像
**中图分类号**：O438 **文献标识码**：A **doi**：10.3969/j.issn.1001-3806.2009.04.029

# Study about decryption based on optical image encryption system in the Fresnel domain

*XIAO Yong-liang*[1], *LIU Qiang*[1], *YUAN Sheng*[1], *ZHOU Xin*[1], *ZHAO Xiao-jun*[1], *YANG Ze-hou*[2], *CHEN Yong*[2], *ZHOU Ding-fu*[2]
(1. School of Electronics and Information, Sichuan University, Chengdu 610064, China; 2. Southwest Institute of Technical Physics, Chengdu 610041, China)

**Abstract**: A method was proposed to decrypt the original image from an only ciphertext encrypted from a symmetrical image. Through inverse Fresnel transform of the ciphertext holograph, the intensity of the frequency spectrum can be received by CCD and sent into a computer. According to the characteristics of autocorrelation and complex-convolution in discrete Fresnel transform, the coefficients are classified and ranked, so that the input light wave can be recovered and the original image can be obtained. The effect of the symmetrical deviation on the quality of the decrypted image was also studied. The investigation indicates that the original image can be decrypted by means of discrete Fresnel diffraction.

**Key words**: information optics; dual-random encryption; Fresnel diffraction; autocorrelation; complex-convolution; symmetrical image



## 引 言

近年来，大量的光学信息处理技术用于信息安全领域。其中REFREGIER和JAVIDI于1995年提出的双随机相位编码的方法最具代表性[1]，且完全可以用光学实现，因而受到人们的广泛关注。随后，SITU[2]等人提出了菲涅耳域的双随机相位编码，UNNIKRISHNAN[3]等人提出了基于分数傅里叶变换的双随机相位编码技术，进一步增加了密钥的维度和系统可行性[4]，推动了双随机相位编码的研究。但是，由于双随机相位编码系统的线性性质，为安全性留下了极大的隐患。CARNICER[5]等人通过“选择密文攻击”的方法可以分析得到双随机相位编码加密系统的频谱面密钥，PENG[6]对傅里叶域的双随机相位编码实施了“已知明文攻击”，和“唯密文攻击”[7]，并获得成功，还有很多攻击方法，例如相位恢复算法[8]、遗传算法[9]等。傅里叶域的攻击已经取得了一定的成果。对于菲涅耳域，“选择明文攻击”也获得成功，但是需要多个明文作为数据源。本文中提出一种基于菲涅耳域的图像恢复方法，根据密文能够重构出频谱面的谱强度，然后再使用文中的重构算法可以恢复出入射平面振幅和相位。此方法在一定程度上属于“部分唯密文攻击”，只需要截获密文，绕过了相位板，攻击过程没有使用傅里叶变换，收敛速度很快。

## 1 菲涅耳域的对称图像双随机相位加密系统的解密分析

### 1.1 菲涅耳域的双随机相位加密系统

此加密系统装置见图1，3块平面板从左到右分别代表输入面，变换平面和输出面。$\exp[j2\pi\phi(x,y)]$和

作者简介：肖永亮(1982-)，男，硕士研究生，研究方向为光学信息处理。
* 通讯联系人。E-mail：zhoxn@21cn.com
收稿日期：2008-06-03；收到修改稿日期：2008-10-30

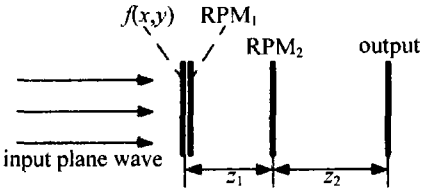


Fig. 1 Optical setup of the optical encryption system in Fresnel domain

$\exp[j2\pi\varphi(\alpha,\beta)]$是两个随机相位板，$\phi(x,y)$和$\varphi(\alpha,\beta)$是均匀分布在[0,1]上的两个独立的白噪声序列，$z_1$和$z_2$是平面板之间的距离。当系统被波长为$\lambda$的平面光波垂直照射时，在输出面得到加密图像$g(x,y)$。加密时，输入信号$f(x,y)$受到第1个相位板$RPM_1$的调制，经过距离$z_1$，到达相位板$RPM_2$。在菲涅耳近似的情况下，复振幅$u(\alpha,\beta)$可以表示为[2]：

$$u(\alpha,\beta) = F_F\{f(x,y)\exp[j2\pi\phi(x,y)];z_1\} \quad (1)$$

式中，$F_F$表示菲涅耳衍射。然后，经过距离$z_2$，经菲涅耳变换在输出平面得到的加密图像为：

$$g(x,y) = F_F\{u(\alpha,\beta)\exp[j2\pi\varphi(\alpha,\beta)];z_2\} \quad (2)$$

解密时，由于逆菲涅耳变换在光学上不存在[10]，取$g(x,y)$的共轭来实现解密。解密的装置与加密的装置一样，只是方向相反。$g^*(x,y)$经过两次菲涅耳变换后得到原图像：

$$f(x,y)\exp[j2\pi\phi(x,y)] = F_F\{F_F[g^*(x,y);z_2]\exp[j2\pi\varphi(\alpha,\beta)];z_1\} \quad (3)$$

由于$f(x,y)$是实函数，所以能够用CCD获得图像的光强$|f(x,y)|^2$。这说明解密过程中输入平面密钥不起作用。

### 1.2 菲涅耳域双随机光学加密系统的图像恢复

通常假定密码分析者具备所使用的密码系统的完全知识，这个假定称作Kerchoffs条件假设[11]，密码系统的安全性必须要建立在此假设基础上。在本文中，假定攻击者有机会使用解密机，便可以知道加密系统的部分参量，如$z_1$，$z_2$，$\lambda$，再通过特定的算法重构原来的信息。假设攻击者已经知道了在菲涅耳域中由强度恢复输入平面信息的算法。那么，通过接收到的密文$g(x,y)$，在不知道密钥即两个随机相位板的情况下就可以重构出原图像。首先，利用逆菲涅耳衍射获得变换平面强度，用CCD接收，其强度表示如下：

$$|v(\alpha,\beta)|^2 = |u(\alpha,\beta)\exp[j2\pi\varphi(\alpha,\beta)]|^2 = |u(\alpha,\beta)|^2 \quad (4)$$

然后，使用该算法$\Gamma$：

$$\Gamma[|u(\alpha,\beta)|^2] = f(x,y)\exp[j2\pi\phi(x,y)] \quad (5)$$

便可以提取自己需要的图像信息。所以，菲涅耳域的对称图像双随机加密图像的恢复问题转化为寻找算法$\Gamma$的问题。

### 1.3 基于菲涅耳域光强的对称信号重构算法

近期，HWANG和HAN[12]提出了仅由菲涅耳域的光强重构出对称信号（振幅和相位）的算法。根据离散菲涅耳变换的相关性质和复卷积性质，由计算机控制，恢复信号。由于CCD摄取的图像被离散化，而且满足Nyquist取样定理[13]，因此可以定义离散菲涅耳变换：

$$\delta F_F[f(m\delta x_0)] = \delta x_0 \sum_{m=-N/2}^{N/2-1} k(m,n,z)f(m\delta x_0) \quad (6)$$

其中：

$$k(m,n,z) = \frac{\exp(j2\pi z/\lambda)}{\sqrt{j\lambda z}}\exp\left[\frac{j\pi}{\lambda z}(m\delta x_0 - n\delta x_p)^2\right] \quad (7)$$

式中，$n$代表样本数，$\delta x_0$和$\delta x_p$是样本间隔，$m=-N/2,\cdots,N/2-1$，$N$是整数。用$R(k)$表示(6)式的自相关，如果自相关的延迟$k=N-1$，根据下式可以得到：

$$f^*\left(-\frac{N}{2}\right)f\left(\frac{N}{2}-1\right) = R(N-1)\exp\left[\frac{j\pi N(N-1)(\delta x_0)^2}{\lambda z}\right] \quad (8)$$

用$R'(k)$表示复卷积，如果复卷积中的$k=-N+1$：

$$f^*(-N/2)f(-N/2+1)\exp\left[\frac{j\pi N(-N+1)(\delta x_0)^2}{\lambda z}\right] + f^*(-N/2+1)f(-N/2)\times\exp\left[\frac{j\pi(N-2)(-N+1)(\delta x_0)^2}{\lambda z}\right] = R'(-N+1) \quad (9)$$

根据HWANG和HAN的对称信号重构算法理论[12]，通过将具有不同延迟的无相位的因子进行分类和排列，对比其系数，发现自相关和复卷积的这些因子具有递归性，可以重建$f(x)$的每一个离散值，在重构过程中，用到了图像的对称性：

$$f(-N/2+i) = f(N/2-i),(i=1,2,\cdots,N/2) \quad (10)$$

算法递归的初值可以从(8)式和(9)式获得，此递归进行到$k=N-(N/2+1)$截止。这时，每一个具有不同延迟无相位的因子得到确切值。最后，将已知的两个因子$f^*(-N/2)f(0)$和$f^*(0)f(-N/2-1)$相乘并运用(8)式得到：

$$[f^*(-N/2)f(0)]\times[f^*(0)f(N/2-1)] = |f(0)^2|R(N-1)\exp\left[\frac{j\pi N(N-1)(\delta x_0)^2}{\lambda z}\right] \quad (11)$$

$f(0)$的值可以获得。按(8)式、(9)式进行递归，可以得到所有的序列。因此，信号$f(m)$被恢复，$m=-N/2,-N/2+2,\cdots,N/2-1$。

## 2 数值模拟及讨论

在菲涅耳加密系统中，$\delta x_p$由入射光波波长$\lambda$和

传输距离 $z$ 决定，作者已经假定有机会使用解密机，便可以获得 $\delta x_p$。图 2 是利用 MATLAB7.0 仿真软件采用基于快速傅里叶变换的角谱传播算法[14]计算的结果。此角谱算法是将输入函数的傅里叶谱和传递函数

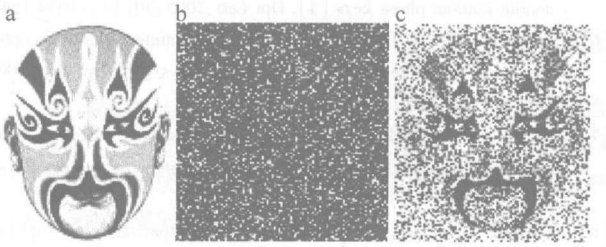


Fig. 2　The results of angular spectrum propagation algorithm based on the fast Fourier transform
a—symmetrical original image　b—encrypted image　c—decrypted image

的谱相乘，然后再做逆傅里叶变换。图 2a 是一幅对称脸谱图像，经过菲涅耳域的双随机相位加密后，得到加密图像，见图 2b。利用上面所讨论的算法，在没有密钥的情况下进行解密，得到解密图像，见图 2c。如图 2c 所示，解密图像的质量不是很好，出现了较大的失真和噪声，但图像的基本特征还是可以辨清的。出现这种情况的原因可以追溯到攻击的整个过程。由重构算法可知，初值 $f^*(-N/2)f(-N/2)$，$f^*(-N/2)\times f(N/2-1)$ 影响后面一系列因子的值，而初值是直接与谱强度 $\sum_{-N}^{N-1}|F^z(n)|^2$ 有关的，用 CCD 探测的谱强度采用灰度图记录，灰度图通常为量化整数。因此，灰度图记录为量化的整数，与记录的谱强度本身有一定的偏差，在进行计算机模拟时，灰度图的像素值发生一定的截断，导致具有不同延迟无相位的因子与理想值的偏差，其结果就是图像出现噪声。

假设对称像素值发生偏差 $\sigma_i$，对称关系应该修正为：

$$f(-N/2+i)+\sigma_i=f(N/2-i) \tag{12}$$

由于重构像素值时采用 $f(0)$ 为始态，讨论偏差对 $f(0)$ 的影响，将(12)式代入(11)式，可以得到对称偏差值 $\sigma$ 对重构像素值 $\hat{f}(0)$ 的影响：

$$\hat{f}(0)=f(0)\sqrt{1+\frac{\sigma}{f(N/2-1)}} \tag{13}$$

对于任意对称图像来说，$\sigma$ 和 $f(N/2-1)$ 都是变量，其变化规律见图 3，图 3a 中的曲线表明：当 $f(N/2-1)$ 越小时，$\hat{f}(0)$ 的偏差越大，且像素值对称偏差对于 $\hat{f}(0)$ 的影响不是简单的线形叠加的关系，而是典型的乘性噪声，这使图像表现出来的噪声更加复杂化。由于其它位置的像素值都是由 $\hat{f}(0)$ 作为始态递归而成，再加上其它对称位置也可能存在像素值的偏差，因而每一个像素值都存在一个乘性噪声。所以 图 2c 中原来像素值为 255 的位置也引入乘性噪声。图 3b 表明：不管

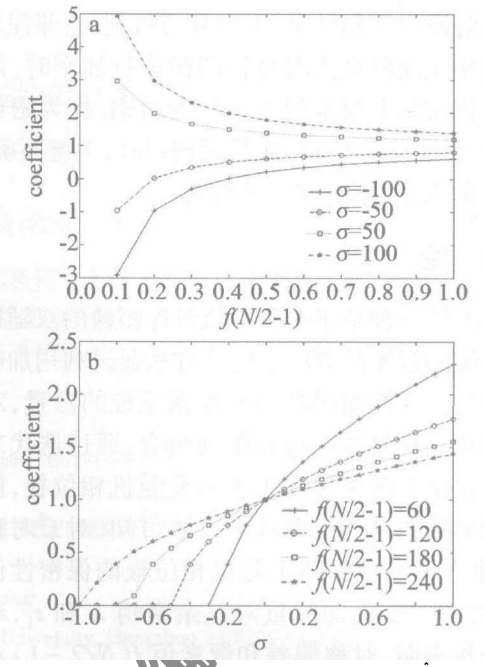


Fig. 3　The influence of $\sigma$ and $f(N/2-1)$ on $\hat{f}(0)$

对称偏差 $\sigma$ 是多少，只要 $f(N/2-1)$ 的值低于 $0.1\times 255=25.5$ 时，解密质量会产生严重的影响。

采用 Photoshop 产生的标准对称图像进行仿真，其结果如图 4 所示，其效果有明显改善。一般采用信噪

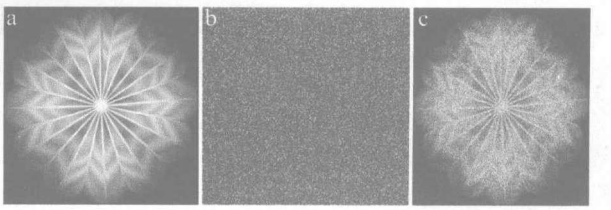


Fig. 4　The simulation results of standard symmetrical images prodaced by Photoshop
a—symmetrical original image　b—encrypted image　c—decrypted image

($D_{SNR}$)来比评价图像改变前后的像质差异程度[15]：

$$D_{SNR}=10\lg\left\{\frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[f(x,y)]^2}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[\hat{f}(x,y)-f(x,y)]^2}\right\} \tag{14}$$

$D_{SNR}$ 反映的是差异的相对程度。计算得到重构图像图 2c 的信噪比为 8.48dB，图 4c 的信噪比为15.36dB。对非对称图像 LENA 加密后进行重构，如图 5 所示，加

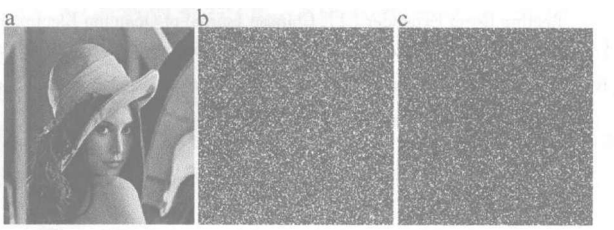


Fig. 5　The reconstruction results of LENA encrypted asymmetric image
a—unsymmetrical image　b—encrypted image　c—decrypted image

密的图像为图 5b，解密结果图 5c 的信噪比为 -20.73dB。结果表明，此算法只适合于对称图像。

由上述解密过程和结果,可以分析得到,在菲涅耳域采用双随相位加密算法对对称图像进行加密时,两个随机相位板实际上根本就不能作为密钥,作为密钥的只有 $z_1$,$z_2$ 和 $\lambda$ 了。所以,在分配密钥时,关键要确保 $z_1$,$z_2$ 和 $\lambda$ 的安全,不被攻击者截获。

## 3 结 论

提出了一种基于菲涅耳域对称图像的双随机光学加密系统的解密的方法。这种方法通过利用加密图像逆变换后在变换面的光强和加密系统的参量,对离散值的自相关和复卷积进行排列组合,通过迭代来重构图像。在整个解密过程中不需要随机相位板,就可以重构出对称图像。根据这个算法可知,对于对称图像而言,菲涅耳域中的两个随机相位板的保密性已经失效,这提醒了要更加注重对其余密钥 $\lambda$ 和 $z_1$,$z_2$ 的保护。分析表明,对称偏差和像素值 $f(N/2-1)$ 对图像恢复质量有影响。

### 参 考 文 献


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

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

[3] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random encoding in the fractional Fourier [J]. Opt Lett, 2000, 25(12): 887-889.

[4] ZHOU X, YUAN S, WANG S W, *et al*. Affine cryptosystem of double-random-phase encryption based on the fractional Fourier transform [J]. Appl Opt, 2006, 45(33): 8434-8439.

[5] CARNICER A, MONTES-USATEGUI M, ARCOS S, *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.

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

[7] 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).

[8] FIENUP J R. Phase retrieval algorithms: a comparison [J]. Appl Opt, 1982, 21(15): 2758-2769.

[9] UNNIKRISHNAN G, MONAGHAN D S, NAUGHTON J T. A known-plaintext heuristic attack on the Fourier plane encryption algorithm [J]. Optics Express, 2006, 14(8): 3181-3186.

[10] YU F T S, JUTAUMULIA S. Optical signal processing computing and neural networks [M]. New York: Wiley-Interscience, 1992: 1-432.

[11] GARRETT P. Introduction to cryptology [M]. Beijing: Science Press, 1999: 4 (in Chinese).

[12] HWANG H E, HAN P. Signal reconstruction algorithm based on a single intensity in the Fresnel domain [J]. Optics Express, 2007, 15(7): 3766-3776.

[13] CONG W X, CHEN N X, GU B Y. Phase retrieval in the Fresnel transforms system: a recursive algorithm [J]. J O S A, 1999, A16(7): 1827-1830.

[14] GOODMAN J W. Introduction to fourier optics [M]. New York: McGraw-Hill, 1968: 1-441.

[15] GOUDAI F, JAVIDI B, REFREGIER P. Influence of a perturbation in a double phase-encoding system [J]. J O S A, 1998, A15(10): 2629-2637.




(上接第 428 页)


[2] SUN N Ch, CHENG J, DAI M, *et al*. Problem of engineering application for laser expansion telescope [J]. Laser Technology, 1996, 20(3): 191-192 (in Chinese).

[3] XIN W J, GAO M, DU Y J. Lens design for multi-wavelength laser beam expander [J]. Optical Instruments, 2007, 29(3): 31-34 (in Chinese).

[4] GUO Sh F, LU Q Sh, YIN Y, *et al*. Theoretical study on damage thresholds for elastic stress fracture in laser-irradiated optical glass [J]. Infrared and Laser Engineering, 2004, 33(2): 133-137 (in Chinese).

[5] KONG X L, HAO P M, ZHOU Sh K, *et al*. Study on Aspherical Reflecting Beam Expander [J]. Chinese Journal of Quantum Electronics, 2001, 18(s1): 40-44 (in Chinese).

[6] ZHANG Y M. Geometrical optics [M]. Tianjing: Engineering Industry Publishing Company, 1987: 78-79 (in Chinese).

[7] YUAN L, PAN B Zh, HAO P M, *et al*. Study of the laser beam-expander optical system with large aperture and non-curvature of field [J]. Laser & Infrared, 2007, 37(7): 672-675 (in Chinese).

[8] YUAN X C. Optical design [M]. Beijing: Science Press, 1983: 223-224 (in Chinese).

[9] HUANG J, REN H, LÜ H B, *et al*. Comparison of damage action of fused silica at different laser wavelength [J]. Optics & Optoelectronic Technology, 2007, 5(6): 5-8 (in Chinese).

[10] ZHANG J, XIAO L, ZHAO J J. Study of thermal and mechanical damage in ZF2 glass induced by high-power laser [J]. Science Technology and Engineering, 2007, 7(16): 3990-3994 (in Chinese).

[11] LI Sh X, ZHENG L N. Optical design manual [M]. Beijing: University of Science & Technology Beijing Press, 1990: 135-136 (in Chinese).