基于空域-分频域混合编码的光学图像加密

方靖岳[1],周 朴[2],康 强[1]

(1.国防科技大学 理学院 应用物理系, 湖南 长沙 410073;
2.国防科技大学 光电科学与工程学院, 湖南 长沙 410073)

摘要:为了提高现有光学安全系统的安全性能,首次提出"空域-分频域(分数傅里叶域)"混合编码的光学图像加密方法。该方法对图像分别进行一次菲涅耳变换和分数傅里叶变换,并在图像的菲涅耳域和分数傅里叶域上分别利用随机相位版施行相位编码。在加密过程中,上述两次变换的参数均可以设计成密钥,波长因子也可以引入加密过程,这样系统密钥被设计在两个不同的变换域上,提高了系统的安全性能。计算机仿真试验表明,该加密方法能够成功实现图像的加密和解密,系统对密钥参数十分敏感,非授权认证方在不知道密钥参数的情况下几乎不可能对加密图像正确解密。

关键词:信息光学; 光学安全; 光学加密

中图分类号:O438 **文献标识码**: A **文章编号**:1007-2276(2005)03-0345-03

Encrypting optical image based on compound encoding on space-fractional domain

FANG Jing-yue[1], ZHOU Pu[2], KANG Qiang[1]

(1.Department of Applied Physics, Institute of Science, National University of Defence Technology, Changsha 410073, China;
2.College of Optoelectronic Sicence and Engineering, National University of Defence Technology, Changsha 410073, China)

Abstract: For the improvement of security capability of existing optical security system, a novel method for encrypting optical image using encoding on both space domain and fractional Fourier domain is presented. In this paper, image is Fresnel transformed and Fractional Fourier transformed successively, and phase encoding is implemented in both Fresnel domain and Fractional Fourier domain. The parameters in two transform can be designed as keys, and the wavelength-key can also be introduced into the encryption process successfully, then the keys of the security system are set on different domains, which can improve the security capability of the system. Computer simulation indicates that the method proposed in this paper can encrypt and decrypt image successfully, and the decrypted results are very sensitive to the keys, people unauthorized can hardly decrypt the image correctly without knowing them.

Key words: Information optics; Optical security; Optical encryption

收稿日期:2004-06-08; **修订日期**:2004-08-10

作者简介:方靖岳(1983-),男,湖南湘潭人,硕士生,主要从事紫外光谱、信息光学等方面的研究。

0 引 言

光学图像加密以其高度的并行性、密钥的多维性、极高的空间分辨率等突出优点已经成为国内外的研究热点，自从 1995 年 Bahram Javidi 等人提出利用随机相位编码进行光学加密的理论以来[1]，关于这个领域的研究已经得到越来越多人的重视。目前有很多用于光学图像加密的方法[1~15]，其中双相位编码技术的应用最为广泛[1, 5~15]。人们对光学图像在空域[10]、频域[1]和分频域[11~15](分数傅里叶域)上的编码技术进行了深入的研究，但将编码密钥分别设置在空域和分频域上的光学图像加密方法还没有相关报道。本文利用光学菲涅耳变换和分数傅里叶变换，在光学图像的空域和分频域上分别施行相位编码，并且将波长因子[3]成功引入加密过程，这样将图像加密的五重密钥安置在不同的变换域上，便于加密方法的光学实现，使得系统的保密性能得到提高。

1 加密方法

1.1 本文算法涉及的光学变换

如图 1 所示，菲涅耳变换定义为：

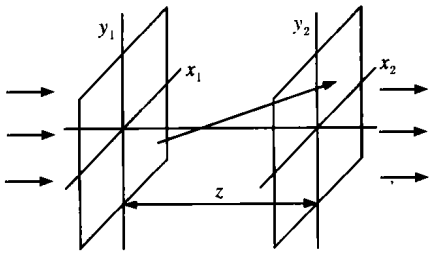

图 1 菲涅耳变换示意图

Fig 1 Fresnel transform

$$E_2(x_2,y_2)=F[E_1(x_1,y_1),z]=\frac{1}{i\lambda z}\exp(ikz)\exp\left[\frac{i\pi}{\lambda z}\left(x_2^2+y_2^2\right)\right]\times\iint E_1(x_1,y_1)\exp\left[\frac{i\pi}{\lambda z}\left(x_1^2+y_1^2\right)\right]\times\exp\left[\frac{-i2\pi}{\lambda z}(x_1x_2+y_1y_2)\right]\mathrm{d}x_1\mathrm{d}y_1 \quad (1)$$

式中 F 表示菲涅耳变换；z 为光的传输距离；λ 为光波波长；k 为波数。

菲涅耳逆变换可以用以下形式描述：

$$E_1(x_1,y_1)=F^{-1}[E_2(x_2,y_2),-z]=\frac{1}{-i\lambda z}\exp(-ikz)\exp\left[\frac{-i\pi}{\lambda z}\left(x_1^2+y_1^2\right)\right]\times\iint E_2(x_2,y_2)\exp\left[-\frac{i\pi}{\lambda z}\left(x_2^2+y_2^2\right)\right]\times\exp\left[\frac{i2\pi}{\lambda z}(x_1x_2+y_1y_2)\right]\mathrm{d}x_2\mathrm{d}y_2 \quad (2)$$

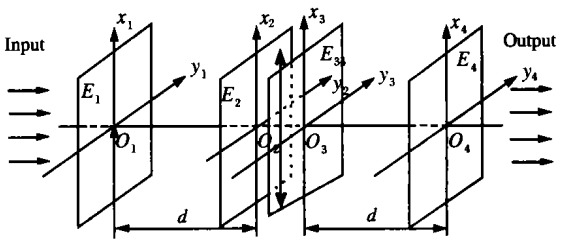

图 2 实现分数傅里叶变换的光学系统

Fig.2 Optical system to implement fractional Fourier transform

分数傅里叶变换作为一种新的信号表征方式，已经在信息加密、信息隐藏、模式识别等领域得到了广泛的应用，它可以通过简单的光学系统实现，如图 2 所示，可以定义为：

$$E_4(x_4,y_4)=F_f^{\varphi}[E_1(x_1,y_1)=\iint E_1(x_1,y_1)\times\exp\left[\frac{i\pi}{\lambda f_s\tan\varphi}\left(x_1^2+y_1^2+x_4^2+y_4^2\right)\right]\times\exp\left[\frac{-i2\pi}{\lambda f_s\sin\varphi}(x_1x_4+y_1y_4)\right]\mathrm{d}x_1\mathrm{d}y_1 \quad (3)$$

式中 f_s 是分数傅里叶变换的族参数；φ 是分数傅里叶变换的阶数，其中 $d=f\times(1-\cos\varphi)$，分数傅里叶逆变换只需将公式(3)中的 φ 替换成 $-\varphi$ 即可。

1.2 加密方法

空域-分频域混合编码的光学图像加密方法是将随机相位掩模版分别设置在菲涅耳衍射区（空域）和分数傅里叶变换面上(分频域)，其光学实现方法如图 3 所示。

设待加密图像为 $E_1(x_1,y_1)$，随机相位版分别为

$M_1(x,y)$,$M_2(\alpha,\beta)$,它们是服从高斯分布的白噪声。

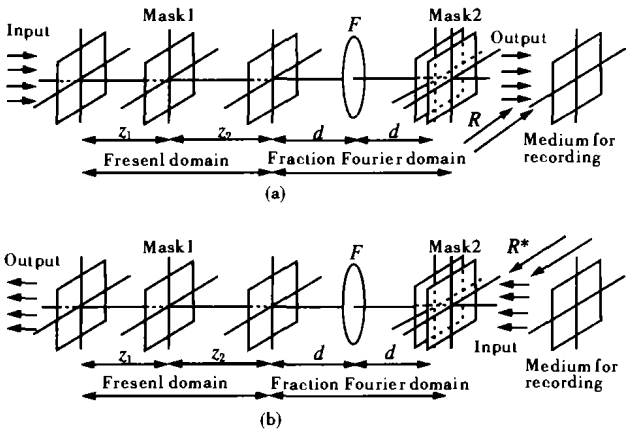

图 3　系统加密、解密过程

Fig.3　Diagram for encrypting and decrypting

光学图像的加密过程(如图 3 所示)可以表示为:

(1) 经菲涅耳变换到达 Mask 1 的前表面,此时光场的复振幅分布为:

$$E_2(x_2,y_2)=F[E_1(x_1,y_1),z_1]$$

(2) 在 Mask 1 的后表面上用随机相位版 M_1 对 E_2 进行相位掩模,光场复振幅分布变为:

$$E_3(x_3,y_3)=E_2(x_2,y_2)\times M_1(x_2,y_2)$$

(3) 继续传播到达实现分数傅里叶变换的光学基本单元前表面,此时复振幅分布为:

$$E_4(x_4,y_4)=F[E_3(x_3,y_3),z_2]$$

(4) 在实现分数傅里叶变换的光学基本单元的后表面上用随机相位版 M_2 对 E_4 进行相位掩模,光场复振幅分布为:

$$E_5(x_5,y_5)=F_f^{\varphi}[E_4(x_4,y_4)]\times M_2(x_5,y_5)$$

采用光学记录介质或数字记录设备记录 E_5,即得经空域-分频域混合编码的加密图像。除了两个随机相位版 M_1,M_2 具有加密作用外,上述加密过程中的参数 z_1,z_2,f,φ 以及光波波长 λ 均可设置为不同变换域上的密钥。由于上述参数类型不同,又在不同的变换域上发挥作用,因此极大地提高了保密性能。

为了从 E_5 中解密出原始光学图像,首先制作解密相位版 $M_3=(\alpha,\beta)$,$M_4(x,y)$,其中 $M_3=M_2^*$,$M_4=M_1^*$,然后只需执行上述步骤的逆过程即可,这在光学上可以用共轭光照射记录介质来实现,即:

$$E_4'=F_f^{-\varphi}(E_5)\times M_3$$
$$E_3'=F^{-1}(E_4',-z_2)$$
$$E_2'=E_3'\times M_4$$
$$E_1'=F^{-1}(E_2',-z_1)$$

E_1'就是解密后的图像,从加密、解密的过程可知,它与 E_1 完全一致。

2　仿真实验

为了检验本文提出的空域-分频域混合编码的光学图像加密方法的有效性,进行了计算机仿真实验。

待加密的图像是一幅 256×256 的灰度图,如图 4(a)所示,随机相位版是服从高斯分布的白噪声,由随机函数产生。对该图像实行空域-分频域混合编码,加密参数 z_1,z_2,f,φ,λ 分别设为:0.1π,0.1,0.2,0.3,632.8×10^{-9},得到经过加密的图像。

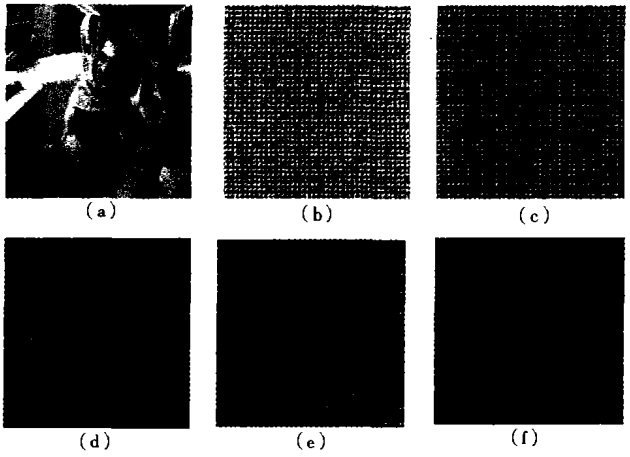

图4　密钥参数不同情形下的解密结果

Fig.4　Images decrypted using different keys

在密钥参数完全正确的情况下,能正确解密得到与原始图像一样的图像。当密钥参数不正确,或是随机相位版没有准确复位,都得不到正确的解密结果,如图 4(b)~(f)所示。图 4(b)~(e)是密钥参数 z_1,z_2,f,φ 分别偏差为 0.001 m 的解密效果,图 4(f)是激光波长为 514 nm 时的解密效果。　(下转第 372 页)

优点,可以提供快速和准确的 LD 驱动。

参考文献:

[1] 滕明,闫丽丽.选择电源改进激光二极管性能[J].红外与激光技术,1994,23(4):58-61.

[2] 邹文栋,高益庆.单片机控制的半导体激光驱动电源[J].激光杂志,2002,23(4): 70-71.

[3] 刘奎学,尹裕,解澎. 高精度电流、温度控制器在半导体激光器中的应用[J].电子工业专用设备,2002,31(3):167-170.

[4] 王明生, 张娜,单江东,等.半导体激光器驱动与控制系统的分析与设计[J].吉林大学学报 (理学版),2002, 41(2):206-208.

[5] 史全林,辛德胜,张剑家,等.连续半导体激光器驱动电源[J].长春光学精密机械学院学报,2001,24(1):12-15.

[6] 许文海,杨明伟,唐文彦.一种多功能半导体激光器驱动电源的研制[J].红外与激光工程,2004,34(5):465-468.

(上接第 347 页)

从图 4 可以看出,本文提出的加密方法将五重密钥安置在不同的变换域上,只要一个密钥参数与正确参数有很小的偏差,都不能得到正确的解密结果,因而有着极强的保密性能。

3 总 结

本文首次采用空域-分频域混合编码的方法,对光学图像在不同变换域上实行编码,并将波长因子引入加密过程,成功实现了光学图像的加密和解密。尽管加密过程公开,但本文提出的方法在不同变换域上设置密钥,使得系统保密性能得到了极大的提高。该方法可广泛用于光学安全等相关领域,具有广阔的应用前景。

参考文献:

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

[2] Bahram Javidi,Takanori Nomura. Secure information by use of digital holography[J].Optics Letter,2000,25(1):28-30.

[3] Peng X,Yu L F,Cai L L.Double-lock for image encryption with virtual optical wavelength[J].Opt Express,2002,10(1):41-45.

[4] Tan Xiao-di,Osamu Matoba,Yoshiko Okada-Shudo,et al. Secure optical memory system with polarization encryption[J]. App Opt, 2001,40(14):2310-2315.

[5] Tan Xiao-di ,Osamu Matoba,Tsutomu Shimura,et al.Secure optical storage that use fully phase encryption [J]. App Opt,2000,39(35): 6689-6694.

[6] Heanue J F,Bashaw M C,Hesselink L.Encrypted holographic data storage based on orthogonal-phase-code multiplexing[J].App Opt, 1995,34(26):6012-6015.

[7] Paul C Mogensen, Jesper Glckstad. Phase-only optical encryption [J].Opt Lett, 2000,25(8):566-568.

[8] Su Wei-chia,Sun Ching-cherng,Chen Yu-cheng,et al.Dupication of phase key for random-phase-encrypted volume holograms[J]. App Opt,2004,43(8):1728-1733.

[9] Seo Dong-hoan,Kim Soo-joong.Interferometric phase-only optical encryption system that uses a reference wave[J]. Opt Lett, 2003, 28(5):304-306.

[10] Osamu Matoba,Bahram Javidi.Encrypted optical memory system using three-dimensional keys in the Fresnel domain[J].Opt Lett, 1999,24(11):762-764.

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

[12] Gopinathan Unnikrishnan, Joby Joseph, Kehar Singh. Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system[J].App Opt,2001,40(2):299-306.

[13] Hennelly B,Sheridan J T. Optical image encryption by random shifting in fractional Fourier domains[J].Opt Lett, 2003,28(4): 269-271.

[14] 于力,朱邦和,刘邦田.用于光学图像加密的分数傅里叶变换双相位编码[J].光子学报,2001,30(7):904-907.

[15] 苏显渝,李继陶.信息光学[M].北京:科学出版社,1999.