文章编号: 1001-3806(2006)03-0327-02

点源照射的单随机相位菲涅耳域光学图像加密

邓晓鹏[1], 邹 凯[2]
(1. 怀化学院 物理电子科学技术系, 怀化 418008; 2 泸州医学院 物理系, 泸州 646000)

摘要: 为了简化系统设置, 根据双随机相位编码加密方法中两块相位掩模的作用, 提出用点光源照射系统, 结合球面波的相位因子, 实现了只用一块相位掩模在菲涅耳域进行图像加密。理论分析和计算机仿真实验结果表明, 该方法不仅能获得与双随机相位编码加密技术一样的效果和安全性能, 而且还能减少相位掩模数量, 简化系统设置, 增强了该方法的实用性。

关键词: 傅里叶光学与光信号处理; 图像加密; 双随机相位掩模; 点光源; 单随机相位掩模; 菲涅耳域
中图分类号: TN911 73 文献标识码: A

Optical image encryption using one random phase mask based on spotlight illumination in the Fresnel domain

DENG Xiao-peng[1], *ZOU Kai*[2]
(1. Department of Physical Electronics, University of Huaihua, Huaihua 418008, China; 2. Department of Physics, Luzhou Medical College, Luzhou 646000, China)

Abstract In connection with the function of double random phase, a simple encryption method is proposed. The characteristic of this method is under the spotlight illumination, one random phase mask and the phase factor of spherical wave are used to realize image encryption in the Fresnel domain. Theoretical analysis and computer simulation indicate that the effect and security of the proposed technique is the same as that of classic technique, and that the system is simplified and practicability is reinforced.

Key words Fourier optics and optical signal processing; image encryption; double random-phase mask; spotlight; only-one random-phase mask; Fresnel domain

引 言

光学信息处理系统具有高处理速度、高并行度、高加密维度、能快速实现卷积和相关运算等特点, 在某种意义上比数字方法更具优越性, 因而探索和开发光学信息安全系统具有很高的学术和应用价值。目前讨论较多的是双随机相位编码加密技术[1]。该技术是采用 4*f*系统来实现的: 把两块统计无关的随机相位掩模(random-phase mask, RPM)分别置于 4*f*系统的输入平面和傅里叶频谱平面, 分别对原图像 $f(x, y)$的空间信息和频谱信息作随机编码, 达到加密的目的。由于该技术具有较高的安全性能, 引起了世界上许多国家科研人员的兴趣和注意[2~9]。为了简化系统设置, 减少系统元件所引起的相干噪声和光能损耗, SITU 和 ZHANG 把该技术利用于菲涅耳域进行图像加密[4], 该方法无须透镜直接在菲涅耳域内进行, 加密时, 仅仅需要两块随机相位掩模, 大大简化了系统的硬件设置。对于双随机相位加密技术, 两块随机相位掩模是缺一不可的, 对于正的实函数图像 $f(x, y)$来说, 虽然在解密时只需要 RPM_2 或者是它的复共轭作为解密密匙, 不需要用到第 1块相位掩模 RPM_1 就可在输出平面用 CCD 探测到解密图像, 但是, 没有第 1块相位掩模 RPM_1 在加密阶段所起扰乱空间信息的作用, 加密的图像很容易用错误的密钥盲解密[1]。针对这些情况, 在保证一定安全性能的条件下, 作者提出只用 1块相位掩模, 利用球面波的相位因子替代第 1块相位掩模 RPM_1 对图像进行加密, 既能获得同样的效果和安全性能, 又能省掉 1块相位掩模, 进一步减少了系统元件, 从而达到在实际操作中减少相应的光能损失和相干噪声的目的。

1 基于菲涅耳域的双随机相位图像加密

菲涅耳域双随机相位加密技术是通过如图 1所示的系统来实现的[4]。加密时, 在输入端, 用平行光照射, 输入的原始图像 $f(x, y)$首先被随机相位掩模函数 $\exp[\mathrm{j}n(x, y)]$所调制, 完成第 1次编码, 即:

作者简介: 邓晓鹏(1972-), 男, 硕士, 讲师, 主要从事信息光学的研究。
E-mail: dxpzqh@tom.com
收稿日期: 2005-03-14; 收到修改稿日期: 2005-09-14

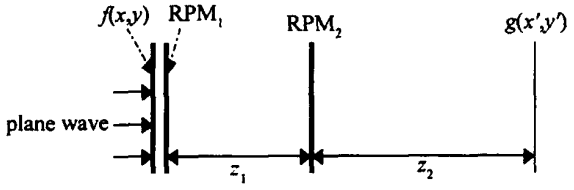

Fig. 1 Optical setup of double random-phase encoding in the Fresnel domain

$$f_1(x, y) = f(x, y)\exp[j n(x, y)] \quad (1)$$

然后对调制后的函数 $f_1(x, y)$进行距离为 z_1 菲涅耳变换,在中间平面上用另一个随机相位函数 $\exp[jb(\xi, \eta)]$对其第 2次编码,再进行一次距离为 z_2 菲涅耳变换,得到最后的加密图像,其结果可表示为:

$$g(x', y') = \mathrm{FrT}\{\mathrm{FrT}[f_1(x, y); z_1]\exp[jb(\xi, \eta)]; z_2\} \quad (2)$$

式中, $\mathrm{FrT}\{; z\}$代表距离为 z的菲涅耳变换, $n(x, y)$和 $b(\xi, \eta)$分别代表均匀分布在 $[0, 2\pi]$的彼此独立的随机函数。

根据光路的可逆性,对加密图像进行解密是上述过程的一个逆过程。将加密图像的共轭 $g(x', y')^*$ 从原系统的输出面输入,经距离为 z_2 菲涅耳变换后,在中间平面经相位函数 $\exp[jb(\xi, \eta)]$滤波,再进行一次距离为 z_1 菲涅耳变换,得到最后输出结果为:

$$f'(x, y) = \mathrm{FrT}\{\mathrm{FrT}[g(x', y')^*; z_2] \times \exp[jb(\xi, \eta)]; z_1\} \quad (3)$$

如果 $f(x, y)$是正的实函数,则 $|f'(x, y)| = f(x, y)$,这样可以用 CCD来接收解密图像。

2 点源照射的单随机相位菲涅耳域图像加密

当用平面观察屏接收由点光源发出的发散球面波的波前时,往往采用二次曲面近似[5],这样在某平面上的发散球面波可用下面的式子来表示:

$$U(x, y) = \frac{A}{z}\exp\left[jkz + \frac{jk}{2z}(x^2 + y^2)\right] \quad (4)$$

式中, A表示为光振幅, z为点源到观察屏的距离, k为波矢的模, j为单位虚数。从上述表达式可以看出,如果忽略与 x和 y无关的常数项的话,它是一个相位函数,如果用它来照射一幅图像 $f(x, y)$,在紧靠图像平面的后面所得的复振幅分布,与用平行光照射 $U(x, y)\cdot f(x, y)$所得的复振幅分布一样。这样改用点光源照射图 1所示的加密系统时,就相当于该加密系统在平行光照射下,对 $f(x, y)\cdot U(x, y)$进行加密。由于 $U(x, y)$和 RPM_1一样也是相位函数,因此它也具有扰乱 $f(x, y)$的空间信息的作用,这样在点光源照射下,就可以省掉 RPM_1,而用点光源本身所携带的相位因子来代替 RPM_1,从而达到只用 1块相位掩模进行图像加密的目的,这样做并不会影响系统的安全性能和图像的解密,因为对于 $f(x, y)$是正的实函数来说, RPM_1仅仅在加密阶段起扰乱 $f(x, y)$的空间信息的作用,对于用 CCD探测解密图像没有任何影响。图 2是在点光源发散球面波照射下的菲涅耳域单随机相位编码加密的示意图。

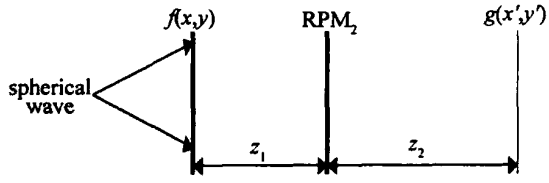

Fig. 2 Optical setup of one random-phase encoding based on spotlight illumination in the Fresnel domain

从图 2中可以看出,用球面波照射 $f(x, y)$就相当于用平行光照射 $f(x, y)\cdot U(x, y)$,它们的唯一区别就是第 1块相位掩模不同。因此,解密过程的操作与双随机相位解密方法一样。

3 计算机仿真实验

为了验证该替代方案的可行性,进行了计算机仿真实验,并对两种方法所获得结果进行了对比。由于菲涅耳衍射可以看成是一个卷积过程,所以,仍然可以采用快速傅里叶算法来进行计算。在仿真时,采用波长为 600nm的发散球面波来照射,球面波的半径为 5cm,衍射距离 z_1 和 z_2分别为 2cm和 3cm,取图像的尺度为 2cm × 2cm,像素为 256 × 256。图 3是对灰度图像进行加密和解密所得的仿真结果。图 4证明该方法具有与双随机相位加密技术同样的抗盲解密性,图 4a是在平行光照射下只用 RPM_2进行加密的盲解密图像;图 4b是在平行光照射下双随机相位加密的盲解密图像;图 4c在球面波照射下只用 RPM_2进行加密的盲解密图像。

对比图 3中各图形可以看出,用点光源自带的相位因子完全可以取代 RPM_1与 RPM_2结合进行图像加密,其效果与双随机相位掩模加密和解密效果一样。

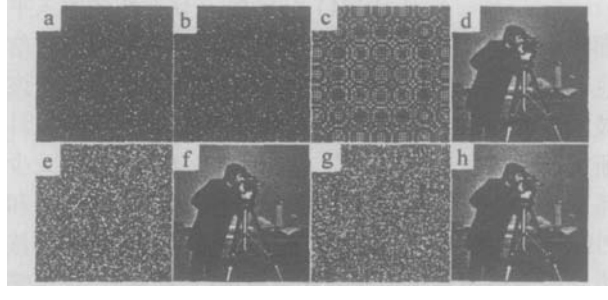

Fig. 3 Computer simulation results

a— random phase RPM_1 b— random phase RPM_2 c— phase of the spherical wave d— input image e— encrypted image of double random phase under the plane wave illumination f— decrypted image of double random phase under the plane wave illumination g— enerypted image of one random phase under the spotlight illumination h— decrypted image of one random phase under the spotlight illumination

(下转第 33页)

有明显差别,和理论计算一样,在反射率为 90%时有比较高的效率。在实验当中,改变二极管激光器冷却水温度 15℃ ~ 30℃,即改变抽运波长,输出没有明显改变。

3 结 论

报道了 LD侧面抽运铒玻璃激光的初步研究成果。实验结果表明,和闪光灯抽运方式相比, LD抽运提高了转化效率和重复频率,且系统稳定,受到较少干扰。由于抽运耦合系统和铒玻璃材料本身的质量原因导致激光效率较低。铒玻璃材料的物理性质决定了该类激光器只适合小能量、低重频运转。对铒玻璃材料和抽运方式的改进工作正在进行当中。下一步将就铒玻璃调 Q 技术做一些研究。

参 考 文 献

[1] FROMZEL V, KUCHMA I, LUNTER S *et al*. Efficiency and tuning of the erbium-doped glass lasers [J]. SPIE, 1991, 1839: 166~ 172.

[2] HAMLIN S J, MERS J D, MERS M J. High repetition rate *Q*-switched erbium glass lasers [J]. SPIE, 1981, 1419: 100.

[3] ANSILE B J. A review of the fabrication and properties of erbium doped fibers for optical waveguides [J]. IEEE Journal of Lightwave Technology, 1991, 9(2): 220.

[4] LAPORTA P, TECCHEO S, LONGHI S *et al*. Erbium-ytterbium microlasers: optical properties and lasing characteristics [J]. Optical Materials, 1999, 11(3): 269~ 288.

[5] WU R K, MYERS J D, MYERS M J *et al*. Diode pumped miniature eye-safe laser *Q*-switched by U^{+2}: CaF_2 and Co^{+2}: $MgAl_2O_4$ [J]. SPIE, 2002, 4630: 94~ 95.

[6] LU Zh P, HU L L, DAI Sh X *et al*. LD pumped Er, Yb codoped phosphate glass laser [J]. Chinese Journal Luminescence, 2002, 22(9): 1129~ 1131(in Chinese).

[7] KOECHNER W. Solid-state laser engineering [M]. Beijing: Science Press, 2002: 58(in Chinese).

[8] LEVOSHKIN A, MONTAGNE J E. Efficient diode pumping for *Q*-switched Yb, Er: glass lasers [J]. Appl Opt, 2001, 40(18): 3023~ 3032.

[9] ALEKSEEV N E, GAPONTSEV V P, ZHABOTINSKII L M E *et al*. Laser phosphate glasses [M]. Moscow: Moscow Nauka Publishing House, 1983: 25.

[10] YANAGISAWA T, ASAKA K, HAMAZU K *et al*. 11mJ, 15Hz single-frequency diode pumped *Q*-switched Er, Yb: phosphate glass laser [J]. Opt Lett, 2001, 26(16): 1262~ 1264.

[11] BOUTCHNKOW V, KUCHMA I, LEVOSHKIN A *et al*. High efficiency diode pumped *Q*-switched Yb: Er: glass laser [J]. Opt Commun, 2002, 173: 383~ 388.

[12] WU R K, MYERS J D, MYERS M J *et al*. Fluorescence lifetime and 980nm pump energy transfer dynamics in erbium and ytterbium codoped phosphate laser glasses [J]. SPIE, 2003, 4968: 11~ 17.

(上接第 328页)

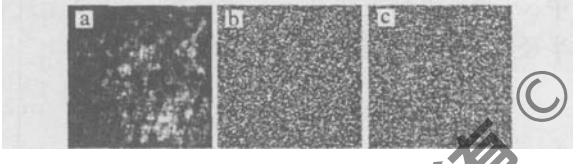

Fig. 4 Decrypted image with the incorrect key code

另外从图 4可以看出,当用平行光照射且只用 1块相位掩模 RPM_2 而不用 RPM_1 进行加密时,其抗盲解密性差,如图 4a所示;图 4b是在平行光照射下双随机相位掩模加密的盲解密图,由于存在 RPM_1 对空间信息的扰乱作用,所以它具有很好的抗盲解密性;图 4c是在点源照射下的单随机相位加密的盲解密图,虽然它只用 1块相位掩模 RPM_2 没用 RPM_1 进行加密,但是由于是采用点源照射,球面波的自带相位因子替代了 RPM_1 扰乱空间信息的作用,因此也具有很好的抗盲解密性。

4 结 论

根据双随机相位编码加密方法中两块相位掩模的作用,结合球面波的相位因子特性,提出用球面波自带的相位因子替代 RPM_1 进行图像加密,实现了只用 1块相位掩模在菲涅耳域对图像进行加密。理论分析和计算机仿真实验结果表明:该方法不仅能获得与双随机相位编码加密技术一样的效果和安全性能,而且还能减少相位掩模数量,简化系统设置。在实际操作中,这些特点对减少因透过相位掩模造成一些相应的相干噪声和光能损失有很大的帮助。

参 考 文 献

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

[2] NOMURA T, JAVIDI B. Optical encryption using a joint transform correlator architecture [J]. Opt Engng, 2000, 39(8): 2031~ 2035.

[3] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption using double random phase encoding in the fractional Fourier domain [J]. Opt Lett, 1995, 20(12): 887~ 889.

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

[5] WANG Sh F, ZHU Zh Q. Principle of modern optics [M]. Chengdu: University of Electronic Science and Technology of China Press, 1998: 117~ 118(in Chinese).

[6] ABOOKASIS D, JAVIDI B. Security optical systems based on a joint transform correlator with significant output images [J]. Opt Engng, 2001, 40(8): 1584~ 1589.

[7] WANG R K K, CHATWIN C. Random phase encoding for optical security [J]. Opt Engng, 1996, 35(9): 2464~ 2469.

[8] NISHCHAL N K, SINGH K. Fully phas-based encryption using fractional order Fourier domain random phase encoding: error analysis [J]. Opt Engng, 2004, 43(10): 2266~ 2273.

[9] NISHCHAL N K, JOSEPH J. Fully phase-encrypted memory using cascaded extended fractional Fourier transform [DB/OL]. http://elsevier.lib.tsinghua.edu.cn/cgi-bin/, 2004-02-16.