文章编号: 1001-3806(2006)04-0442-03

球面波照射的双随机相位掩模光学图像加密

邓晓鹏
(怀化学院 物理电子科学技术系, 怀化 418008)

摘要: 正的实函数图像通过双随机相位编码加密以后,在解密过程中,用光强探测器接收解密图像时,位于空域的第 1块相位掩模不起密匙作用。针对这个缺点,在不增加系统元件的基础上,提出用球面波照射加密系统,并把待加密图像与第 1块相位掩模分开。这样既能使第 1块相位掩模起到密匙作用,其位置又能额外提供一重密匙。计算机仿真结果证明了其可行性。

关键词: 傅里叶光学与信号处理; 图像加密; 双随机相位掩模; 球面波; 4f系统
中图分类号: TN911.73 文献标识码: A

Optical image encryption using double phase mask based on spherical wave illumination

DENG Xiao-peng
(Department of Physical Electronics, University of Huaihua, Huaihua 418008, China)

Abstract For the positive real function image encoded by double random-phase, the first random-phase mask placed in the blank can not serve as the key when the decrypted image is detected by intensity detector in the decrypting process. In connection with the defects, an improved encryption system illuminated with spherical wave is proposed. The input image is not nestled closely to the first random-phase mask, so the first random-phase mask can be used as the key for positive function image and the position of the first random-phase mask provides an additional key. Computer simulation indicates the feasibility of the proposed technique.

Key words Fourier optics and optical signal processing; image encoding; double random-phase mask; spherical wave; 4f-system

引 言

由于光学系统具有高处理速度和高并行性度,使它在信息安全领域显示出巨大的潜力。目前讨论较多的是双随机相位编码加密技术[1-4]。该技术是采用 4f系统来实现的: 把两块统计无关的随机相位掩模 RPM_1 和 RPM_2 分别置于 4f系统的输入平面和傅里叶频谱平面,分别对待加密图像 $f(x, y)$的空间信息和频谱信息作随机编码,达到加密目的。由于一般的图像都是正的实函数,因此,解密时只用到 RPM_2 的复共轭作为解密密匙,在输出平面用 CCD就可探测到解密图像,而 RPM_1 没起到密匙的作用,这样在一定程度上降低了系统的安全性能。针对这个缺点, NISHCHAL 等提出纯位相编码方法,该方法在加密前需要先把实值图像通过空间光调制器转换成纯位相图像,解密后又要把纯位相图像转换成实值图像[5,6],显得比较麻烦。作者提出利用球面波照射系统,把待加密图像与 RPM_1 分开,并移至透镜焦距以外进行加密,既能使 RPM_1 起到密匙的作用,又能额外增加一重密匙。

1 基于球面波照射的双随机相位掩模光学图像加密

当用会聚的球面波照射一幅图像 $f(x, y)$时,在紧靠图像后表面的振幅分布为: $f(x, y)\cdot Q(x, y)$,其中, $Q(x, y)$为会聚球面波的二次曲面近似表达式[8],它与用平行光照射 $f(x, y)\cdot Q(x, y)$所获得的复振幅分布一样。针对这个特点,设计了如图 1所示的光学加密

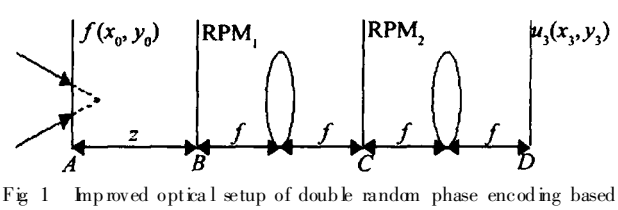

Fig. 1 Improved optical setup of double random phase encoding based on spotlight illumination

系统,该加密系统是在 4f系统的基础上把待加密图像与 RPM_1 分开,并移至透镜焦距以外,同时采用会聚球面波照射进行图像加密。为了便于分析,把图 1所示的光学加密系统转化成如图 2所示的光学加密系统。

作者简介: 邓晓鹏(1972-),男,硕士,讲师,主要从事信息光学研究。
E-mail: dxpzqh@tom.com

收稿日期: 2005-06-16;收到修改稿日期: 2005-09-20

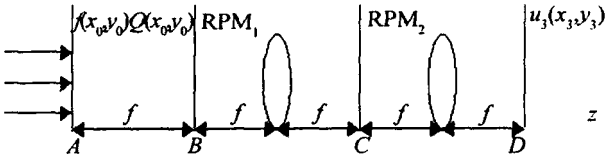

Fig 2 Equivalent fig to Fig 1

从输出角度来说, 图 1与图 2所示情形是等价的。可以把图 2所示的系统分为两部分, 第 1部分为 *AB* 段, 第 2部分为 *BD* 段。对于 *AB* 段, 它相当于一个双相位菲涅耳域图像加密系统[7], 作为编码相位掩模的分别是 $Q(x_0, y_0)$和 RPM$_1$。而 *BD* 段就是一个双随机相位编码加密系统[1], 只不过是它的输入函数不是待加密图像, 而是通过菲涅耳域加密以后的输出图像。解密时必须注意: 由于该系统的输入相对于输出不具有对称性, 再加上光学上不存在菲涅耳逆变换, 所以在解密时保持原系统设置不变, 而采用 $u_3(x_3, y_3)$的复共轭作为输入函数从图 2的 *D* 端输入来恢复原图像[7]。用 CCD 接收解密图像的位置不再是 *B* 处所在的平面, 而是 *A* 处所在的平面, 这样 RPM$_1$ 和距离 *z* 都起到密匙的作用, 从而在不增加系统元件的情况下, 比传统的双随机相位光学图像加密技术多出了二重密匙, 大大地提高了系统的安全性能。

下面用数学公式具体分析其加密和解密过程。令 *A*, *B*, *C*, *D*, 所处平面的坐标系分别为 (x_0, y_0), (x_1, y_1), (x_2, y_2), (x_3, y_3), 随机相位函数分别为 $\exp[\mathrm{j}\phi_1(x_1, y_1)]$和 $\exp[\mathrm{j}\phi_2(x_2, y_2)]$, 其中 ϕ_1、ϕ_2 表示 0~ 1的相互独立随机分布函数。球面波的复振幅的二次曲面近似表达式为[8]:

$$Q(x, y) = A\exp[-\mathrm{j}kz - \mathrm{j}k(x^2 + y^2)/2z]/z \quad (1)$$

式中, *A* 为球面波的振幅, *z* 为球面波的传播距离, *k* 为波矢, j为虚数单位。

在菲涅耳近似的条件下, 菲涅耳衍射的表达式为:

$$U(x, y) = \iint f(x_0, y_0)h(x_0, y_0; x, y; z, \lambda)\,\mathrm{d}x_0\,\mathrm{d}y_0 \quad (2)$$

式中,

$$h(x_0, y_0; x, y; z, \lambda) = \frac{1}{\mathrm{j}z\lambda} \times \exp\left\{\frac{2\pi\mathrm{j}z}{\lambda} + \frac{\mathrm{j}\pi}{z\lambda}[(x - x_0)^2 + (y - y_0)^2]\right\} \quad (3)$$

为脉冲响应函数, λ为波长, *z* 为光波的传播距离。为了简单起见, 把 (2)式写成如下形式:

$$U(x, y) = \mathrm{FrT}[f(x_0, y_0)] \quad (4)$$

式中, FrT表示菲涅耳变换, 这样加密过程可表示成如下几步。

(1)菲涅耳衍射:

$$u_1(x_1, y_1) = \mathrm{FrT}[f(x_0, y_0)Q(x_0, y_0)] \quad (5)$$

(2)空域编码:

$$u_1(x_1, y_1)\exp[\mathrm{j}\phi_1(x_1, y_1)] \quad (6)$$

(3)傅里叶变换:

$$u_2(x_2, y_2) = \mathcal{F}\{u_1(x_1, y_1)\exp[\mathrm{j}\phi_1(x_1, y_1)]\} \quad (7)$$

(4)频域编码:

$$u_2(x_2, y_2)\exp[\mathrm{j}\phi_2(x_2, y_2)] \quad (8)$$

(5)傅里叶变换:

$$u_3(x_3, y_3) = \mathcal{F}\{u_2(x_2, y_2)\exp[\mathrm{j}\phi_2(x_2, y_2)]\} \quad (9)$$

$u_3(x_3, y_3)$为最后的加密图像。解密时, 由于在光学上不存在菲涅耳逆变换, 所以要用 $u_3(x_3, y_3)$的复共轭 $u_3^*(x_3, y_3)$作为解密系统的输入函数, 解密系统设置与加密系统设置一样, 仅仅改变光线的传输方向, 即从图 1所示的 *D* 端输入, *A* 端输出。具体可表示如下。

(1)傅里叶逆变换:

$$g_2(x_2, y_2) = \mathcal{F}^{-1}[u_3^*(x_3, y_3)] \quad (10)$$

(2)频域解码:

$$g_2(x_2, y_2)\exp[\mathrm{j}\phi_2(x_2, y_2)] \quad (11)$$

(3)傅里叶逆变换:

$$g_1(x_1, y_1) = \mathcal{F}^{-1}\{g_2(x_2, y_2)\exp[\mathrm{j}\phi_2(x_2, y_2)]\} \quad (12)$$

(4)空域解码:

$$g_1(x_1, y_1)\exp[\mathrm{j}\phi_1(x_1, y_1)] \quad (13)$$

(5)菲涅耳衍射:

$$g_0(x_0, y_0) = \mathrm{FrT}\{g_1(x_1, y_1)\exp[\mathrm{j}\phi_1(x_1, y_1)]\} \quad (14)$$

$g_0(x_0, y_0)$是解密图像, 由于 $f(x_0, y_0)$为正的实函数, 可用 CCD 接收 $g_0(x_0, y_0)$的光强获得 $f(x_0, y_0)$的信息。另外, 从上面的解密过程可以看出, 在该方法中, RPM$_1$ 对图像的解密是不可缺少的, 同时, 在解密过程中, 由于还要经过距离为 *z* 的菲涅耳衍射, 故 *z* 也提供了一重密匙[7]。这样, 该方法在不增加系统元件的基础上比原方法多出了二重密匙, 大大地提高了系统的安全性能。

2 计算机仿真实验

为了证明该方法的可行性, 作者进行了仿真实验。在仿真实验中, 为了满足近轴条件、抽样定理、以及能够利用快速傅里叶变换进行计算[2], 采用波长为 600nm、半径为 10cm 的会聚球面波照射, 待加密图像是像素为 128 × 128的灰度图像, 镶嵌在像素为 256 × 256, 实际尺寸大小为 4mm × 4mm 的方框中。相位掩模的尺寸为 4mm × 4mm, 衍射距离 *z* = 30mm。图 3是对该图像进行加密和解密所得的仿真结果。

由图 3可知, 理论分析与仿真实验结果完全一致。采用该方法不仅能获得很好的加密和解密效果, 而且使第 1块随机相位掩模对正的实函数图像也能起到密匙作用, 同时根据图 3h可知, 在其它密匙正确的情况下, 如果解密时的衍射距离 *z* 和加密时的衍射距离不相等的话, 不能恢复原图像, 这样该系统比原系统多出了一重密匙, 大大提高了系统的安全性能。

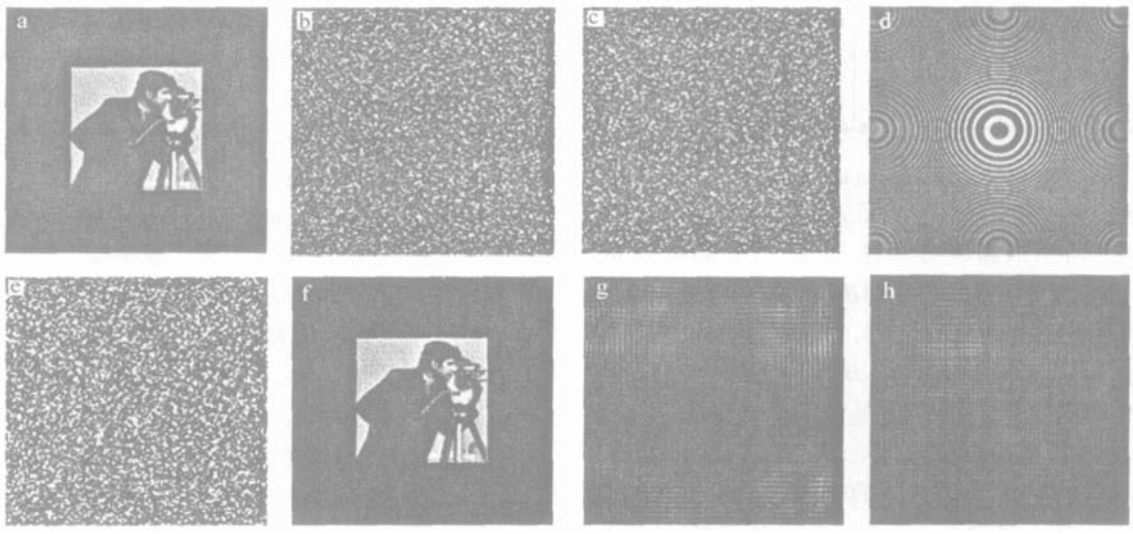

Fig. 3 Computer simulation results

a— input image b— random phase RPM_1 c— random phase RPM_2 d— phase of the spherical wave e— encrypted image f— decrypted image with the correct key code g— decrypted image in the plane of RPM_1 with the correct key code h— decrypted image in the plane of $z=29$mm with the correct other key code

3 结 论

针对双随机相位编码加密技术的缺点,即在解密过程中,当用光强探测器接受解密图像时, RPM_1 对正的实函数图像不起密匙作用,提出了一种球面波照射的改进型双随机相位光学图像加密方法,并进行了计算机仿真。仿真结果表明,该方法不仅能克服上述缺点,而且在不增加系统元件的基础上多获得一重密匙,提高了系统的安全性能。

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] 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.

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

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

[5] 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.

[6] NISHCHAL N K, JOSEPH J. Fully phase-encrypted memory using cascaded extended fractional fractional Fourier transform [DB/OL]. http://elsevier.lib.tsinghua.edu.cn/cgi-bin, 2004-02-16/2005-09-19.

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

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

(上接第 441页)

参 考 文 献

[1] LIU S H. New development of fiber laser [J]. Optoelectronic Technology & Information, 2003, 16(1): 1~8 (in Chinese).

[2] LIU A P, UEDA K. The absorption characteristics of circular, offset and rectangular double-clad fibers [J]. Opt Commun, 1996, 132: 511~518.

[3] LOU Q H, WANG P Y, ZHOU J. Development of double-clad fiber laser [J]. Proc SPIE, 2002, 4914: 136~141.

[4] PASK H M, ARCHAMBAULT J L, HANNA D C. Operation of cladding-pumped Yb^{3+}-doped silica fiber lasers in 1μm region [J]. Electron Lett, 1994, 30(11): 863~865.

[5] KOSINSKI G S, INNISS D. High-power fiber lasers [A]. Tech incal Digest of Lasers and Electro-optics [C]. San Francisco: CLEO, 1998: 78.

[6] DOMINIC V, MacCORMACK S, WAARTS R. 110W fiber laser [J]. Electon Lett, 1999, 35(14): 1158~1160.

[7] THIEME J. World premiere of super power fiber laser at opening of test center aluminum alloy welding (centrAl) in bremen [EB/OL]. http://www.ipgphotonics.com/html/288_jpg_installs_world_s_first_17_kilowatt_fiber_laser.cfm, 2005-04-11.

[8] LÜK Ch, LIU W W, LI Y G *et al*. High power Yb-doped double-clad fiber laser [J]. Chinese Journal of Lasers, 2000, 27(8): 775 (in Chinese).

[9] NING D, WANG W T, RUAN L *et al*. Fabrication and lasing properties of Yb^{3+}-doped double-clad silica fiber [J]. Chinese Journal of Lasers, 2000, A27(11): 987~991 (in Chinese).

[10] LOU Q H, ZHOU J, ZHU J Q *et al*. 100W Yb-doped double-clad fiber laser [J]. Chinese Journal of Lasers, 2003, A30(12): 1064 (in Chinese).

[11] LOU Q H, ZHOU J, ZHU J Q *et al*. 440W Yb-doped fiber laser with a double-clad fiber made in China [J]. Chinese Journal of Lasers, 2005, 32(1): 20 (in Chinese).

[12] WEI W L, OU P, YAN P *et al*. Side-pumping coupler technology for double-clad fiber [J]. Laser Technology, 2004, 28(2): 116~120 (in Chinese).

[13] RUAN Sh Ch, SU H X, FENG M *et al*. Yb^{3+}-doped double clad fiber laser with a output power of 8.6W [J]. Acta Photonica Sinaca, 2003, 32(5): 523~524 (in Chinese).

[14] ZHANG J, PANG Y Zh, HU G J *et al*. Output characteristics of Yb^{3+} doped double-clad fiber grating laser [J]. Laser Technology, 2004, 28(2): 173~176 (in Chinese).

[15] ZHOU Y H, LIAO J H, MENG H Y *et al*. The technological progress of endovascular stents [J]. Journal of South China Normal University (Natural Science Edition), 2005(2): 136~142 (in Chinese).