文章编号：1001-3806(2018)05-0655-04

基于光栅滤波器的新型光学图像加密技术

李盛林[1,2]，王华英[3]

(1. 广东开放大学 工程技术系，广州 510091；2. 广东理工职业学院 工程技术系，广州 510091；3. 河北工程大学 数理科学与工程学院，邯郸 056038)

摘要：为了提高干涉加密技术的光学处理速度和光学实现的可行性，基于干涉原理的加密技术的思想，结合光栅滤波器的图像处理方法，研究了基于光栅滤波器的 4*f* 系统双图像光学加密技术。该技术利用已成熟的基于光栅滤波的图像相加减 4*f* 系统，将两个待加密图像转化为两个实值的白噪声，理论模拟验证了该方法的可行性和有效性。结果表明，该方法简单实用，易于光学实现并具有很高的安全性。

关键词：信息光学；光学密钥；图像加密；光栅滤波器；干涉

中图分类号：TN911.73　　**文献标志码**：A　　**doi**：10.7510/jgjs.issn.1001-3806.2018.05.014

New optical image encryption technology based on grating filter

LI Shenglin [1,2], *WANG Huaying* [3]

(1. Engineering Technology Department, Open University of Guangdong, Guangzhou 510091, China; 2. Engineering Technology Department, Guangdong Polytechnic Institute, Guangzhou 510091, China; 3. School of Mathematics & Physics, Hebei University of Engineering, Handan 056000, China)

Abstract: In order to improve optical processing speed and the feasibility of optical realization in interference encryption technology, based on the idea of interference encryption principle and image processing method of grating filter, 4*f* system double image optical encryption technology based on grating filter was designed. The mature image additiion and subtraction 4*f* system based on grating filtering was used to transform two encrypting images into two real values of white noise. The feasibility and effectiveness of the method were verified by theoretical simulation. The results show that the method is simple, practical, safe and easy to implement.

Key words: information optics; optical encryption; image encryption; grating filter; interference

引　言

近年来，计算机和通信技术不断快速发展，图像信息的安全已成为严重的社会问题。由于光的波长短、信息容量大，同时又具有振幅、相位、波长、偏振等多种属性，是多维的信息载体，并且光学图像信息处理技术本身具有高速度、并行性的特点，被认为是下一代广泛应用的密钥技术[1-7]。1995 年，REFREGIER 提出了经典的双随机相位编码光学加密系统[8]，此后一系列其衍生出来的光学加密系统得到广泛研究。最近 JAVIDI[9] 等人对光学图像加密的研究进展做了详细和深入的分析，因为解密时随机相位的单个像素与单个像素的精确对准问题对实验装置和系统搭建要求太高，制约了光学图像加密技术的实验研究发展，这也是当前光学图像加密主要集中于数字系统和混合光学数字系统的原因。这些加密系统包括基于分数傅里叶变换的加密方法[10]、基于菲涅耳变换的加密方法[11]、利用离轴数字全息的加密系统[12]等大量改进的加密系统。但是这些系统难以抵御目前日益高明的攻击手段[13-14]。所以其它更加复杂的加密手段也被不断地研究和改进，包括基于小波变换的加密系统[15]，利用相衬技术的全相位加密系统[16]、利用平面集成微光学器件加密系统[17]、偏振编码加密系统[18]、虚拟光学加密技术[19]等。然而，这些方法也具有较严重的缺陷，加密过程需要用计算机完成大量迭代运算，影响加密系统的处理速度。2008 年，ZHANG 等人提出了基于干涉原理的简单易行的加密方法[20]。该算法利用干涉原理的逆过程，解析地产生 2 个随机相位板，并将原

作者简介：李盛林(1976-)，男，硕士，讲师，现主要从事图像处理、电子系统设计方面的研究。

E-mail：slli@gdrtvu.edu.cn

收稿日期：2017-11-09；收到修改稿日期：2018-01-02

始图像隐藏于这两个纯随机相位板中。但是该方法存在固有的“轮廓像”问题,即在附加参量已知的情况下,使用其中任意一个随机相位板进行衍射均可以获取原始图像的轮廓,而这个轮廓提供了关于原始图像的足够信息。同时由于菲涅耳衍射场的场分布位置和大小与作为密钥的衍射距离有关,并且随机相位板的密钥空间非常大,所以该方法在光学上很难实现。作者将基于干涉原理的加密技术思想引入图像加减的 4*f* 系统,提高了安全性的同时,降低了光学实现的难度。

本文中将图像加减的 4*f* 系统与基于干涉原理的图像加密方法结合,设计了基于正弦光栅的 4*f* 图像加密系统,成功地实现了图像的加密和解密,具有极高的安全性。该方法克服了基于干涉原理的加密方法中,两束解密光束需要精确对准的问题,因为基于光栅的图像相加的技术已非常成熟[21]。本文中使用计算机模拟验证了系统的性能,结果显示,任何一个密钥错误都将导致解密失败。解密过程对系统的附加参量特别敏感,因而极大地提升了系统的密钥空间。

1 加密过程

加密过程中,将两个待加密的图像加密成两个均匀的白噪声。待加密的图像为非负分布 $o(x,y)$,首先给予待加密图像初始随机相位 $P_1(x,y)=\exp[\mathrm{i}2\pi\times r(x,y)]$,其中,$r(x,y)$ 表示 0 ~ 1 的随机分布数值。同时也作为加密密钥。相应的复振幅表达为:

$$O_1(x,y)=o(x,y)P_1(x,y) \tag{1}$$

根据作者的设计思想,令上述复振幅是由两个具有随机相位分布的复光场的傅里叶变换场的相干叠加产生,即:

$$O_1(x,y)=\mathscr{F}[A(\varepsilon,\eta)P_2(\varepsilon,\eta)]+\mathscr{F}[B(\varepsilon,\eta)P_2(\varepsilon,\eta)] \tag{2}$$

式中,$\mathscr{F}$ 表示傅里叶变换,$A(\varepsilon,\eta)$ 和 $B(\varepsilon,\eta)$ 是频谱面上的振幅,$P_2(\varepsilon,\eta)$ 为相位。第 2 步是将频谱面上的 $A(\varepsilon,\eta)$ 和 $B(\varepsilon,\eta)$ 经过随机相位板 $P_3(\varepsilon,\eta)=\exp[\mathrm{i}2\pi\times r(\varepsilon,\eta)]$ 进行加密,获得最终的加密图像 $o_1'(x_1,y_1)$ 和 $o_2'(x_1,y_1)$:

$$o_1'(x_1,y_1)R_1(x_1,y_1)=\mathscr{F}[o_1(\varepsilon,\eta)]=\mathscr{F}[A(\varepsilon,\eta)P_3(\varepsilon,\eta)] \tag{3}$$

$$o_2'(x_1,y_1)R_2(x_1,y_1)=\mathscr{F}[o_2(\varepsilon,\eta)]=\mathscr{F}[B(\varepsilon,\eta)P_3(\varepsilon,\eta)] \tag{4}$$

所以,$o_1'(x_1,y_1)$ 和 $o_2'(x_1,y_1)$ 就是包含待加密图像信息的两个白噪声振幅,即完成了加密过程;而 $R_1(x_1,y_1)$ 和 $R_2(x_1,y_1)$ 将作为解密的密钥。整个加密过程不需要任何迭代运算。

2 解密过程

解密系统如图 1 所示。它是一个在频谱面放置全息光栅的 4*f* 系统。将获得的两个包含带加密图像信息的白噪声 $o_1'(x_1,y_1)$ 和 $o_2'(x_1,y_1)$ 放置在 4*f* 系统的输入面 Σ 上,两者的间距为 $2b$,同时在输入面上放置解密密钥,分别为 $R_1(x_1,y_1)$ 和 $R_2(x_1,y_1)$。

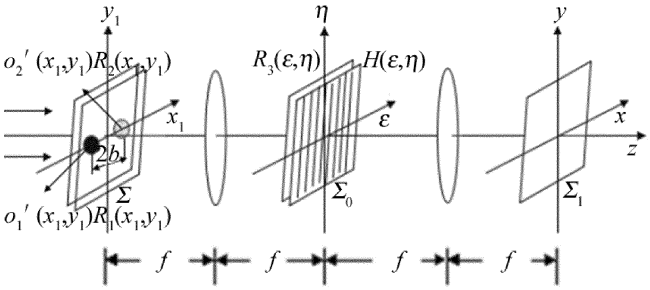

Fig. 1 Schematic diagram of decryption system

根据图 1 所示,首先在输入面 Σ 上获得 $o_1'(x_1,y_1)R_1(x_1,y_1)$ 和 $o_2'(x_1,y_1)R_2(x_1,y_1)$。经过傅里叶变换,在频谱面 Σ_0 上获得:

$$g(\varepsilon,\eta)=\mathscr{F}[o_1'(x_1+b,y_1)R_1(x_1+b,y_1)+o_2'(x_1,y_1)R_2(x_1+b,y_1)]=o_1(\varepsilon,\eta)\exp[\mathrm{i}2\pi b\varepsilon]+o_2(\varepsilon,\eta)\exp[\mathrm{i}2\pi b\varepsilon] \tag{5}$$

在频谱面 Σ_0 上,放置相位密钥 $R_3(\varepsilon,\eta)$ 和一个全息光栅,该全息光栅的透过率函数为:

$$H(\varepsilon,\eta)=\frac{1}{2}+\frac{1}{4}\exp[\mathrm{i}(2\pi\varepsilon_0\varepsilon)]+\frac{1}{4}\exp[\mathrm{i}(-2\pi\varepsilon_0\varepsilon)] \tag{6}$$

式中,ε_0 为全息光栅的空间频率。在解密过程中,在频谱面上放置的解密密钥为:

$$R_3(\varepsilon,\eta)=P_3{}^*(\varepsilon,\eta)\times P_2(\varepsilon,\eta) \tag{7}$$

式中,* 表示共轭。在频谱面 Σ_1 上,经过相位板 $R_3(\varepsilon,\eta)$ 和全息光栅后,为了获得解密图像,光栅的参量 ε_0 和 b 满足 $b=\lambda f\varepsilon_0$,其中,λ 为照射波长,f 为透镜焦距。然后光场分布为:

$$g_1(\varepsilon,\eta)=g(\varepsilon,\eta)R_3(\varepsilon,\eta)H(\varepsilon,\eta)=\frac{1}{2}g(\varepsilon,\eta)R_3(\varepsilon,\eta)+\frac{1}{4}\exp[\mathrm{i}(2\pi\varepsilon_0\varepsilon)]\times o_1(\varepsilon,\eta)\exp[-\mathrm{i}2\pi b\varepsilon]+\frac{1}{4}\exp[\mathrm{i}(-2\pi\varepsilon_0\varepsilon)]\times o_1(\varepsilon,\eta)\exp[\mathrm{i}2\pi b\varepsilon]+\frac{1}{4}\exp[\mathrm{i}(2\pi\varepsilon_0\varepsilon)]\times o_1(\varepsilon,\eta)\exp[\mathrm{i}2\pi b\varepsilon]+\frac{1}{4}\exp[\mathrm{i}(-2\pi\varepsilon_0\varepsilon)]\times$$

$$o_1(\varepsilon,\eta)\exp[-\mathrm{i}2\pi b\varepsilon] \tag{8}$$

此后,(8)式的光场再经过一次傅里叶变换便获得输出,如下式所示:

$$\mathscr{F}[g_1(\varepsilon,\eta)] = \frac{1}{2}o(x,y)P_1(x,y) + \frac{1}{4}o_1'(x-b,y)R_1(x-b,y) * \mathscr{F}[R_3(\varepsilon,\eta)] + \frac{1}{4}o_2'(x+b,y)R_2(x+b,y) * \mathscr{F}[R_3(\varepsilon,\eta)] + \frac{1}{4}o_1'(x-2b,y)R_1(x-2b,y) * \mathscr{F}[R_3(\varepsilon,\eta)] + \frac{1}{4}o_2'(x+2b,y)R_2(x+2b,y) * \mathscr{F}[R_3(\varepsilon,\eta)] \tag{9}$$

式中,* 表示卷积。由(9)式可见,在输出面上一共获得 5 项输出,分别对应于(8)式中的每一项的傅里叶变换;并且它们的位置分别是(0,0),(b,0),(−b,0),(2b,0),(−2b,0)。其中位于中心的图像为 $o(x,y)\times P(x,y)$,取振幅即为原始图像,因此完成了解密过程。

最终的加密图像为两个实值的平稳白噪声,利于保存和传输,因此该方法的加密信息不需要全息存储;解密过程对系统的附加参量敏感,这些系统参量也可作为密钥。

3　模拟实验和结果分析

采用计算机对所提出的方法进行了模拟验证和分析。待加密图像如图 2a 所示。像素为 256 × 256,图像的大小为 3cm × 3cm。实验中选用的激光波长为 633nm,频谱面上的光栅的空间频率 $\varepsilon_0 = 10/\mathrm{mm}$,透镜的焦距为 0.2m。因此根据上面的分析,解密中输入平面的两幅图的距离 b 应为 1.27mm。首先,根据第 1 节中描述的加密过程,获得了两个白噪声如图 2b 和图 2c 所示,可见已经完全隐藏了待加密图像的信息和特征。随后,利用全部正确的密钥,包括相位板 R_1,R_2 和 R_3,光栅的透过率函数 H,波长 λ,光场常数 ε_0 和两个加密图像的距离 2b,可获得的解密图像如图 2d 所示,可见当作者的密钥都正确时,能够很好地还原原始图像。若采用错误的密钥,如仅有密钥 R_1 错误而其它密钥全部正确的情况下,所获得的解密结果图 2e 所示;而若仅有密钥 R_2 错误而其它密钥全部正确的情况下,所获得的解密结果图如图 2f 所示;若仅有密钥 R_3 错误而其它密钥全部正确的情况下,所获得的解密结果图如图 2g 所示。可见在上述 3 种情况下的解密结果类似白噪声,完全得不到原始图像的有效信息。由此可知,相位密钥 R_1,R_2 和 R_3 均能够分别独立地保证该加密方法的安全性。

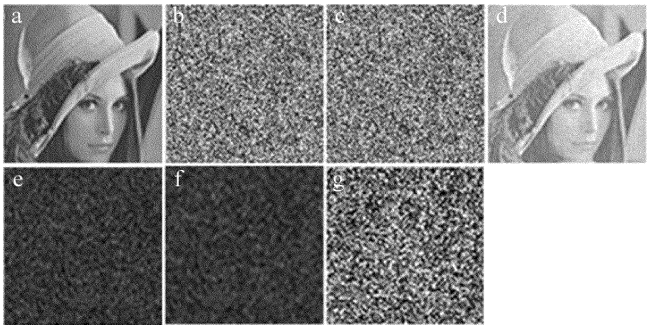

Fig. 2　a—the image to be encrypted　b—the encrypted image o_1　c—the encrypted image o_2　d—decryption result with correct key　e—decryption result with wrong key R_1　f—decryption result with wrong key R_2　g—decryption result with wrong key R_3

为了定量比较解密图像与原始图像的相似性,作者采用解密图像和原图像均方误差 R_e 进行评价:

$$R_e = \frac{\sum_{n=1}^{N}\sum_{m=1}^{N}\left|\,|o'(m,n)| - |o(m,n)|\,\right|^2}{\sum_{n=1}^{N}\sum_{m=1}^{N}|o(m,n)|^2} \tag{10}$$

式中,$N\times N$ 为图像的像素点数,在这里是 256 × 256,$o(m,n)$和$o'(m,n)$分别表示原图像和解密图像的振幅,将图 2a 和图 2d 中的振幅数据带入该公式得到相应的数值为2.21×10^{-1},是一个很小的值。而当密钥错误时,将图 2e、图 2f 和图 2g 中的振幅数据分别带入(10)式所得到的 R_e 值分别为 0.41,0.42 和 0.45,这表明重构结果与原始结果无关联。

此外,该图像加密系统对参量 b 和 f 的敏感性进

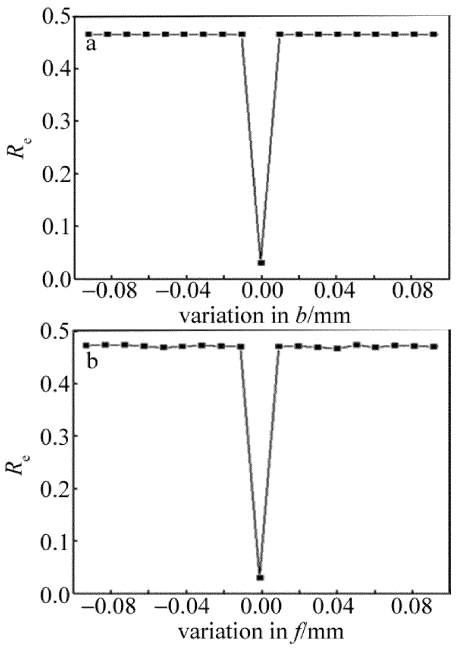

Fig. 3　The curve of R_e with the change of b and f

行了测试和计算,如图 3 所示。图 3a 和图 3b 中分别为图像距离 b 和透镜焦距 f 与正确值有差别时,解密图像和原图像均方误差 R_e 的变化曲线。

由图 3 可见,图像距离 b 和透镜焦距 f 距正确值有微小变化时,R_e 迅速增大,所以这些系统参量能够增强该系统的安全性。

4 结 论

结合图像加减的 4f 系统与基于干涉原理的图像加密技术,设计了基于全息正光栅的 4f 图像加密系统。该方法将原始图像最终加密成两个实值的白噪声,并在频谱面放有全息光栅的 4f 系统中完成解密。计算机模拟结果表明,利用全部正确的密钥才能够获得较好的解密结果;除了设计的密钥外,解密结果对系统中的其它参量,包括输入面白噪声间距、波长、光栅载频等参量,也非常敏感,这均表明该方法具有很高的安全性。该方法克服了基于干涉原理的加密方法中两束解密光束需要精确对准的弊端,同时降低了光学实现的难度。该加密技术在图像信息的加密、存储和传输中有重要的意义。

参 考 文 献

[1] MATOBA O, JAVIDI B. Encrypted optical storage with wavelength-key and random phase codes [J]. Applied Optics, 1999, 38(32): 6785-6790.

[2] MATOBA O, JAVIDI B. The keys to holographic data security[J]. IEEE Circuits and Devices Magazine, 2000, 16(5):8-15.

[3] XU G X, XU Sh Q, GUO X J, *et al*. Image compression-encryption algorithm combined DCT transform with DNA operation[J]. Laser Technology, 2015, 39(6):460-463(in Chinese).

[4] PAN T G, LI D Y. A novel image encryption using Arnold cat[J]. International Journal of Security and its Application, 2013, 7(5): 377-386.

[5] XI S X, WANG X L, SONG L P, *et al*. Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram[J]. Optics Express, 2017, 25(7):8212-8222.

[6] XIAO Y L, LIU Q, YUAN Sh. Research on optical images encryption system based on fresnel zone[J]. Laser Technology, 2009, 33(4): 433-436(in Chinese).

[7] ZHANG H Zh, YAO M, LEI P. Research of image processing method of far-field laser spots[J]. Laser Technology, 2013, 37(4):460-463 (in Chinese).

[8] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7):767-769.

[9] JAVIDI B, CARNICER A, YAMAGUCHI M, *et al*. Roadmap on optical security[J]. Journal of Optics, 2016, 18(8):083001.

[10] UNNIKRISHNAN G, SINGH K. Double random fractional Fourier domain encoding for optical security [J]. Optical Engineering, 2000, 39(11):2853-2859.

[11] MATOBA O, JAVIDI B. Encrypted optical storage with wavelength-key and random phase codes [J]. Applied Optics, 1999, 38(32): 6785-6790.

[12] GOODMAN J W, LAWRENCE R W. Digital image formation from electronically detected holograms [J]. Applied Physics Letters, 1967, 11(3):77-79.

[13] 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]. Optics Letters, 2005, 30 (13):1644-1646.

[14] FRAUEL Y, CASTRO A, NAUGHTON T J, *et al*. Resistance of the double random phase encryption against various attacks[J]. Optics Express, 2007, 15(16):10253-10265.

[15] CHEN L F, ZHAO D M. Optical image encryption based on fractional wavelet transform[J]. Optical Communications, 2005, 254 (4/6):361-367.

[16] GLUCKSTAD J, MOGENSEN P C. Phase-only optical encryption [J]. Optics Letters, 2000, 25(8):566-568.

[17] DARIA V R, SINZINGER S, GLUCKSTAD J. Phase-only optical decryption in a planar integratedmicro-optics system[J]. Optcal Engineering, 2004, 43(10):2223-2227.

[18] MOGENSEN P C, GLUCKSTAD J. A phase-based optical encryption system with polarisation encoding[J]. Optical Communications, 2000, 173(1/6):177-183.

[19] PENG X, CUI Z, TAN T. Information encryption with virtual-optics imaging system[J]. Optical Communications, 2002, 212(4/6): 235-242.

[20] ZHANG Y, WANG B. Optical image encryption based on interference[J]. Optics Letters, 2008, 33(21):2443-2445.

[21] JABLOWSKI D P, LEE S H. Restoration of degraded images by compo site gratings in a coherent optical prcessor[J]. Applied Optics, 1973, 2(7):1703-1712.