文章编号：1001-3806(2014)04-0488-06

球面波照明下傅里叶变换全息多图像加密方法研究

沈学举，刘旭敏，许芹祖，林 超
（军械工程学院，石家庄 050003）

摘要：为了减少加密系统所用模板数，简化隐藏图像对解密过程的影响，采用球面波照明研究了基于傅里叶变换全息的多图像加密隐藏方法，并进行了加密、加密图像隐藏和解密的理论分析和数值模拟，加密图像和原始图像间的相关系数趋于 0，宿主图像和加密图像的叠加系数 $\rho<0.3$ 时，宿主图像和隐藏图像的相关系数趋于 1，解密图像和原始图像间的相关系数趋于 1。结果表明，该加密隐藏方法的加密、解密和隐藏效果良好。

关键词：信息光学；光学图像加密；加密图像隐藏；二值随机相位模板；傅里叶变换全息；球面波照明
中图分类号：O438 **文献标志码**：A **doi**：10.7510/jgjs.issn.1001-3806.2014.04.012

Multiple image encryption based on Fourier transform holography under spherical wave illumination

SHEN Xueju, LIU Xumin, XU Qinzu, LIN Chao
(Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: To reduce the number of binary random phase mask used in an image encryption system and simplify the effect of hidden encryption images on decryption process, an optical multiple-image encryption and hiding scheme was put forward based on Fourier transform holography under spherical wave illumination. Theoretical analysis and numerical simulation of image encryption and hiding encryption image and image decryption were made. The results show that correlation coefficient between encryption image and original image approaches 0, correlation coefficient between host image and hiding encryption image approaches 1 when superposition coefficient ρ between host image and hiding encryption image is less than 0.3, correlation coefficient between decryption image and original image approaches 1. The encryption method can obtain good encryption effect.

Key words: information optics; optical image encryption; hiding encryption image; binary random phase masks; Fourier transform holography; spherical wave illuminating

引 言

近年来，光学信息处理已广泛用于光学图像加密，由于光学信息处理系统固有的高并行性、高处理速度与维度以及多加密参量，极大地增强了加密系统的安全性和有效性，使光学图像加密技术的研究成为了信息安全领域的研究热点[1-15]。在已报道的一些光学图像加密方法[1-3,7-14]中，最基本的是双随机相位加密方法，但在光学实现过程中一般是将随机相位模板(random phase mask, RPM)上载到光路中的空间光调制器上，需要把相位映射或编码为实数，此过程中可实现的相位值的分辨力和范围受限，存在较大误差。为提高编码精度，参考文献[7]中分析了图像加密中二值随机相位模板(binary random phase mask, BRPM)的特性。另外许多研究者利用参量复用技术可实现多幅图像加密，例如角度[8]、波长[9]、位移[10]、偏振[11]、旋转[12]、孔径[13]等复用不仅实现多幅图像加密，且在一定程度上增强抗攻击能力。

为进一步简化加密系统，作者将参考文献[14]中的光学菲涅耳变换换成 4*f* 系统，采用球面波照明，仅在 4*f* 系统的频谱面上置 1 个二值随机相位模板，利用参考光束入射角度复用和计算机处理实现多幅光学图像加密和隐藏。在原理分析的基础上数值模拟了图像的加密、隐藏和解密过程，对加密隐藏效果及其影响因素进行了分析。

作者简介：沈学举(1963-)，教授，博士生导师，主要从事激光技术和光学信息处理方面的教学和科研工作。
E-mail：shxjoptics@aliyun.com

收稿日期：2013-08-14；收到修改稿日期：2013-09-22

1 原理分析

1.1 加密原理分析

单幅图像加密过程示意图如图 1 所示,点光源发出球面波照明输入面上的待加密原始图像,在频谱面上插入 1 个二值随机相位模板,在 4*f* 系统输出面上入射角为 α 的参考光和输出光场干涉由 CCD 记录下干涉场即为全息图。

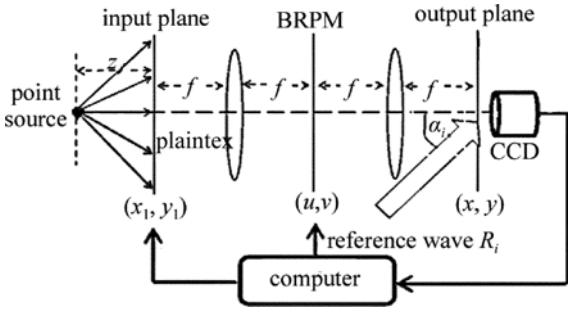

Fig. 1 Sketch map of encryption system

取输入面、输出面和空间频率平面坐标分别为 (x_1,y_1),(x,y) 和 (u,v)。透镜焦距为 f,点光源和输入面之间距离为 z,则球面波在入射面上复振幅分布为:

$$n(x_1,y_1) = \frac{A}{z}\exp\left[\mathrm{i}kz + \frac{\mathrm{i}k(x_1^2+y_1^2)}{2z}\right] \quad (1)$$

式中,A 为距点光源单位距离处球面波的振幅,波数 $k=2\pi/\lambda$,λ 为照明光波长。输出面上干涉场强度分布为:

$$I_1(x,y) = |\mathscr{F}^{-1}\{\mathscr{F}[f_1(x_1,y_1)n(x_1,y_1)]\times b_1(u,v)\} + R_1(x,y)|^2 \quad (2)$$

式中,倾角为 α 的参考平面波在输出面上的复振幅 $R_1(x,y)=\exp(\mathrm{i}kx\sin\alpha)$,$f_1(x_1,y_1)$ 为输入面上待加密原始图像,$b_1(u,v)$ 为频谱面上二值随机相位模板,$\mathscr{F}$ 表示傅里叶变换,$\mathscr{F}^{-1}$ 表示逆傅里叶变换。

挡住参考光和照明球面波分别记录 4*f* 系统输出面上的参考光场和图像的输出光场,其中参考光强度为:

$$|R_1(x,y)|^2 = 1 \quad (3)$$

图像的输出光强度为:

$$|O_1(x,y)|^2 = |\mathscr{F}^{-1}\{\mathscr{F}[f_1(x_1,y_1)n(x_1,y_1)]b_1(u,v)\}|^2 \quad (4)$$

用(2)式减去(3)式和(4)式,得加密图像强度分布为:

$$I_1' = I_1 - |O_1|^2 - |R_1|^2 = O_1R_1^* + O_1^*R_1 \quad (5)$$

式中,* 表示复共轭。

为加密多幅图像,可改变参考光入射角,在 4*f* 系统输出面上分别由 CCD 记录不同入射角的参考光与不同图像在球面波照射下的输出场干涉得到的全息图,采用上述同样的处理得到第 m 幅加密图像为:

$$I_m'(x,y) = I_m(x,y) - |O_m|^2 - |R_m|^2 = O_mR_m^* + O_m^*R_m \quad (6)$$

式中,$|O_m(x,y)|^2 = |\mathscr{F}^{-1}\{\mathscr{F}[f_m(x_1,y_1)n_m(x_1,y_1)]\times b_m(u,v)\}|^2$,$n_m(x_1,y_1)$ 为记录第 m 幅图像时所用的球面波。

$$|R_m(x,y)|^2 = 1 \quad (7)$$

最终得到的含 N 幅图像信息的加密图像为:

$$I_N'(x,y) = \sum_{m=1}^{N}(O_mR_m^* + O_m^*R_m) = \sum_{m=1}^{N}[O_m(x,y)\exp(-\mathrm{i}kx\sin\alpha_m) + O_m^*(x,y)\exp(\mathrm{i}kx\sin\alpha_m)] \quad (8)$$

式中,α_m 为加密第 m 幅图像时的参考光入射角。由于最终的加密图像是强度图像,便于存储和传输。

1.2 解密原理分析

由于解密过程是加密过程的逆过程,解密密钥应为加密时所用二值随机相位模板的共轭,将其称为共轭二值随机相位模板(conjugative binary random phase mask, CBRPM),置于 4*f* 系统的频谱面上。将加密图像置于 4*f* 系统的输入面上,用加密第 m 幅图像时所用的参考光照射加密图像,透过加密图像的光场复振幅为:

$$I_m''(x,y) = R_m(x,y)I_N'(x,y) = O_m(x,y) + O_m^*(x,y)\exp(2\mathrm{i}kx\sin\alpha_m) + \sum_{k=1,k\neq m}^{N}\{O_k\exp[\mathrm{i}kx(\sin\alpha_m-\sin\alpha_k)] + O_k^*\exp[\mathrm{i}kx(\sin\alpha_m+\sin\alpha_k)]\} \quad (9)$$

从(9)式看出,仅第 1 项沿 4*f* 系统光轴方向传输,合理选择不同图像加密时参考光的入射角使其它项对应的光束不能通过 4*f* 系统传输。由于 4*f* 系统频谱面上存在 CBRPM,透过 CBRPM 的场为:

$$\mathscr{F}^{-1}[\mathscr{F}[O_m(x,y)]b_m^*(u,v)] = f_m(x,y)\frac{A}{z_m}\exp\left[\mathrm{i}kz_i + \frac{\mathrm{i}k(x^2+y^2)}{2z_m}\right] \quad (10)$$

式中,$b_m^*(u,v)$ 是解密密钥,可用 CBRPM 表示,z_m 是加密第 m 幅图像时点光源和输入面之间距离。如果原始图像是实图像,解密图像可由 CCD 在 4*f* 系统输出面上探测到。

1.3 加密图像的隐藏

由于加密图像是一幅均匀白噪音图像,传输时会引起攻击者的注意,因此,实际中应将加密图像隐藏在宿主图像中传输。根据上述多幅图像加密原理,利用空域隐藏算法,设宿主图像为 $C(u,v)$,则隐藏后的合成图像为:

$$I_N'''(x,y) = \rho I_N'(x,y) + C(x,y) \quad (11)$$

式中,ρ 为常数。合理选择 ρ 值即可有效隐藏加密图像,同时保证被隐藏加密图像的抗畸变性。

比较(8)式、(9)式和(11)式可以看出,解密时将 $I_N'(x,y)$ 换成 $I_N'''(x,y)$,仅多出一项 $C(x,y) \times \exp(\mathrm{i}kx\sin\alpha_m)$,该项所示的光波沿 α_m 方向传播,而解密出的第 m 幅图像沿光轴方向传播,宿主图像并不影响图像的正常解密,因此,本文中所述的图像加密方法适于空域图像隐藏。

2 数值模拟

为验证所设计系统的可行性,进行了数值模拟。用于加密的 4 幅原始图像如图 2 所示,模拟所用的照明光波波长为 632.8nm,点光源距 4f 系统输入面 0.2m,加密 4 幅图像时选择参考光入射角分别为 π/8,π/4,π/5 和 π/6。设计二值随机相位模板时首先使用 MATLAB 中的随机函数 rand(m,n)生成随机相位矩阵,再根据矩阵元相位值将其转换为相位差为 π 的二值相位矩阵,按(8)式得到的加密图像如图 3 所示,从图 3 看到,加密图像是一幅均匀白噪音图像,视觉上看不到任何原始图像的信息,可将其隐藏于公开的图像中进行传输。

为便于传输加密图像,选择宿主图像如图 4a 所

Fig. 2 Original images
a—Lena b—Babara c—baboon d—peppers

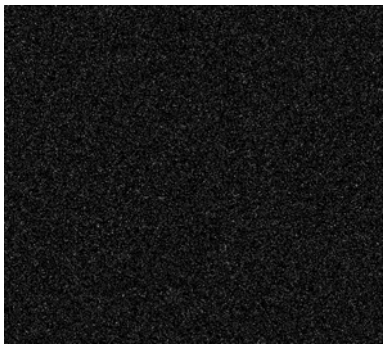

Fig. 3 Encryption image

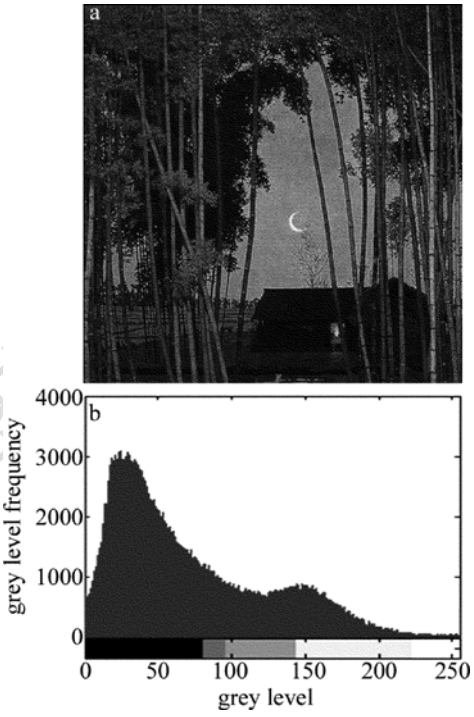

Fig. 4 a—host image b—histogram

示,相应的灰度直方图如图 4b 所示,ρ 分别取为 0.1,0.3 和 0.5,按(11)式模拟得到的隐藏图像和相应的灰度直方图如图 5 所示,计算得到的宿主图像和隐藏图像的相关系数分别为 0.9982,0.9846 和 0.9588。

由图 4、图 5 和不同 ρ 值对应的宿主图像和隐藏图像相关系数可以看出,$\rho < 0.3$ 时,宿主图像和隐藏图像差异很小,传输中很难发现宿主图像中隐藏有加密图像。

为解密出每一个原始图像,用解密模板 CBRPM 替换频谱面上的加密模板 BRPM,用入射角为 α_i 的参考光照明 4f 系统输入面上的隐藏加密图像,在 4f 系统的输出面上用 CCD 可接收到第 i 幅解密图像。使用图 3 所示的加密图像和图 5 所示的隐藏加密图像来解密,其差别仅仅是后者要求照明参考光的强

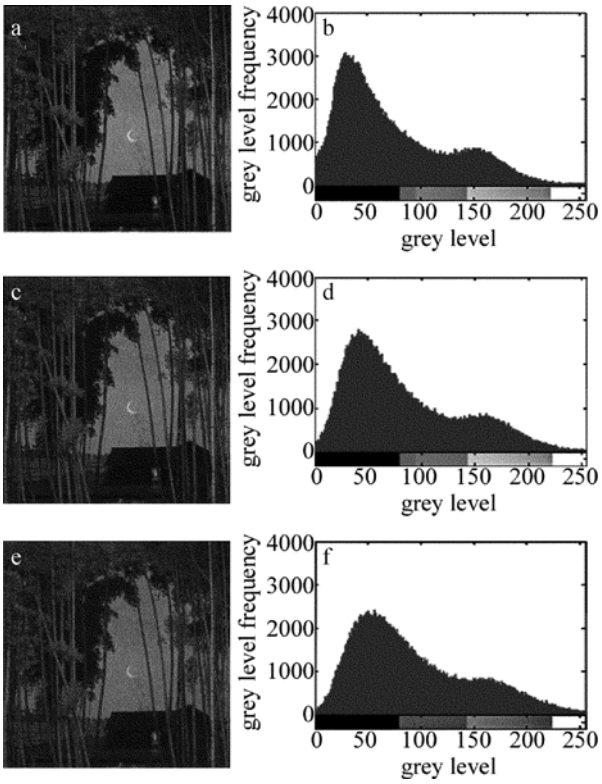

Fig. 5 Hiding image and its histogram
a,b—$\rho=0.1$ c,d—$\rho=0.3$ e,f—$\rho=0.5$

度要强些,ρ 值越小,要求照明参考光的强度越强。由(9)式、(10)式和(11)式计算得到的解密图像如图 6 所示。

Fig. 6 Decryption images
a—Lena b—Babara c—baboon d—peppers

3 加密和解密图像特性分析

通过理论分析和数值模拟可以看出本文中所述的方法利用二值随机相位模板可以实现多图像加密和解密,且加密图像适于空域隐藏传输。为更好地评估该加密方法的加、解密效果,利用相关系数 C、灰度直方图和峰值信噪比(peak signal-to-noise ratio,PSNR)R_{PSNR} 3 个参量[15]进行定量分析评估。灰度直方图给出了一幅图像中的灰度值分布,如果两幅图像的灰度直方图差别很大,可以认为这两幅图像是完全不同的;如果两幅图像的相关系数和峰值信噪比很小,则说明这两幅图像差别很大。利用这 3 个参量可以定量描述加密图像和解密图像的差异,即加密和解密效果。原始图像和加密图像的灰度直方图如图 7 所示,原始图像和加密图像以及解密图像之间的相关系数和峰值信噪比如表 1 所示。

从图 7 看出加密图像和各原始图像的灰度分布完全不同,差异很大,由表 1 中数据看出,加密图像的 C 趋于 0,R_{PSNR} 值也较小,说明加密效果很好,从视觉上加密图像是一幅噪声图像,完全看不出任何原始图像信息。解密图像的 $C=1$,其 R_{PSNR} 值比加密图像大得多,说明解密图像质量很好。

为进一步分析加密效果,用单色平面波照明,仅在图 1 所示的加密系统频谱面上置 1 个二值随机相位模板,数值模拟单幅图像的加、解密图像和加密图像的灰度直方图如图 8 所示。在输入面和频谱面上各置 1 个二值随机相位模板时,数值模拟单幅图像的加、解密图像和加密图像的灰度直方图如图 9 所示。用球面波照明,仅在频谱面上放置二值随机相位模板,数值模拟单幅图像的加、解密图像和加密图像灰度直方图如图 10 所示。模拟所用的照明光波波长为 632.8nm,点光源距 $4f$ 系统输入面 0.2m,加密图像时选择参考光入射角为 $\pi/8$。

在双随机相位光学加密系统中输入面上的随机相位模板在图像加密中主要起扩散作用,使输出的加密图像成为均匀白噪声,不能作为密钥使用,用球面波取代输入面上的随机相位模板,利用球面波的二次相位因子同样起到对加密图像的扩散作用。比较图 8 和图 9 看出,由于图 8 对应的加密系统中输入面上没有随机相位模板,生成的加密图像非均匀白噪音,而图 9 中的加密图像是均匀白噪音,两加密图像的灰度直方图差异较大。比较图 9 和图 10 看出,尽管图 10 对应的加密系统中输入面上也没有随机相位模板,但因采用球面波照明,生成的加密图像和图 9 中的加密图像很接近,都是均匀白噪音,两加密图像的灰度直方图也很接近,表明球面波的二次相位因子在图像加密过程中确实起到了扩散作用。

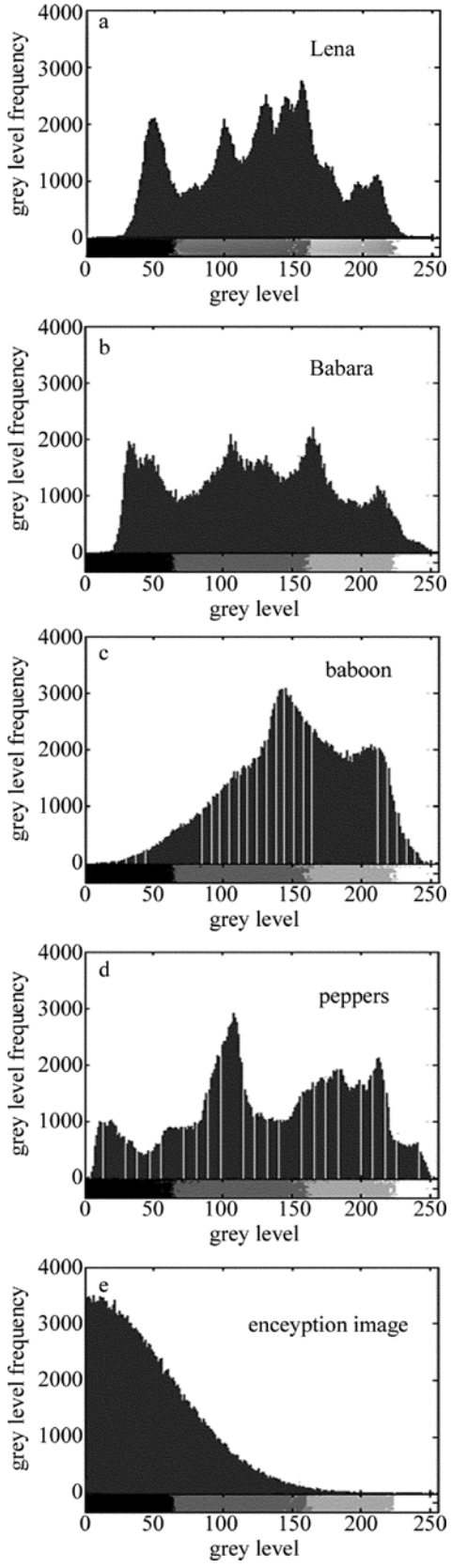

Fig. 7 Histograms of original images and encryption image
a—Lena b—Babara c—baboon d—peppers e—encryption image

Table 1 Correlation coefficient and peak value of signal-to-noise ratio

	encryption image		decryption images	
original images	R_{PSNR}	C	R_{PSNR}	C
Lena	110.371	0.0002	354.221	1.000
Babara	110.200	0.0054	354.694	1.000
baboon	108.683	0.0004	355.832	1.000
peppers	109.207	0.0028	350.632	1.000

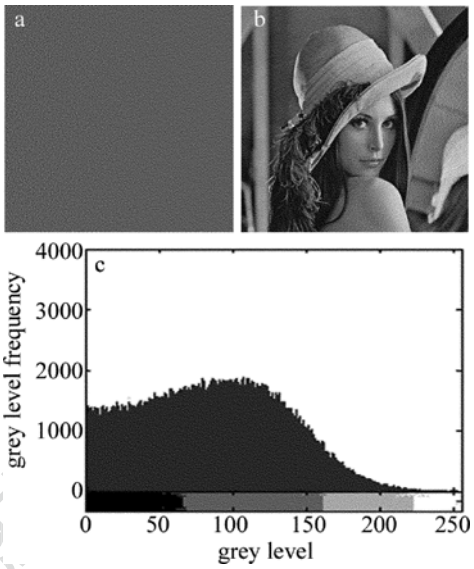

Fig. 8 Encryption image and decryption image and histogram of encryption image accepted by simulation when plane wave illuminating and single random mask were used
a—encryption image b—decryption image c—histogram of encryption image

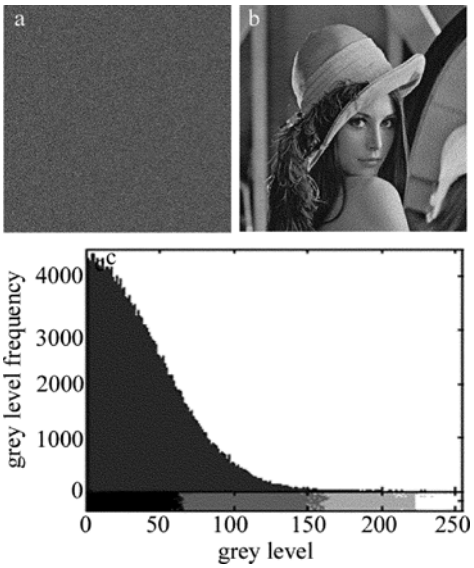

Fig. 9 Encryption image and decryption image and histogram of encryption image accepted by simulation when plane wave illuminating and double random mask were used
a—encryption image b—decryption image c—histogram of encryption image

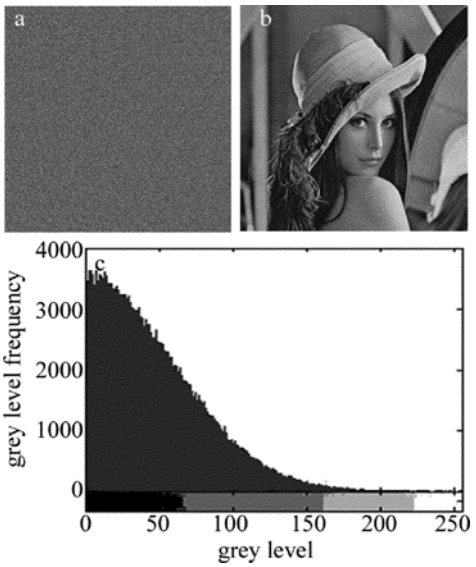

Fig. 10　Encryption image and decryption image and histogram of encryption image accepted by simulation when spherical wave illuminating and single random mask were used
a—encryption image　b—decryption image　c—histogram of encryption image

4　结　论

作者设计了一种多图像加密系统,采用球面波照明,用球面二次相因子取代输入面上的随机相位模板,使加密系统仅使用一个二值随机相位模板,其光学实现结构简单,采用二值随机相位模板,在光学实现过程中将二值随机模板上载到空间光调制器等元件上时可进一步提高相位模板在空间光调制器上的精度,同时利用参考光入射角复用可实现多图像加密。数值模拟加密、解密和隐藏过程以及对解密图像的特性分析表明,图像加密过程中球面波二次相因子在光学图像加密过程中能起到较好的扩散作用。

参　考　文　献

[1] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(3):767-769.
[2] UNNIKRISHNAN G, JOSEPH J. Optical encryption system that uses phase conjugation in a photorefractive crystal[J]. Applied Optics, 1998, 37(18): 8181-8186.
[3] MATOBA O, JAVIDI B. Encrypted optical memory system using three dimensional-keys in the fresnel domain [J]. Optics Letters, 1999, 24(4): 762-764.
[4] XIAO Y L, LIU Q, YUAN Sh, *et al*. Study about decryption based on optical image encryption system in the Fresnel domain [J]. Laser Technology, 2009, 33(4): 433-436 (in Chinese).
[5] LIN Ch ,SHEN X J, YANG Sh X. Simulation analysis of random phase mask with spatial light modulator[J]. Laser Technology, 2013, 37(3): 365-370 (in Chinese).
[6] FENG J B, ZHOU X. Random phase encoding achievement of color images under spotlight illumination [J]. Laser Technology, 2008, 32(6): 621-623 (in Chinese).
[7] LIN Ch, SHEN X J, LI Z. cryptographic analysis on the key space of optical phase encryption algorithm based on the design of discrete random phase mask [J]. Optics and Laser Technology, 2013,49(1):108-117.
[8] MATOBA O, JAVIDI B. Encrypted optical storage with angular multiplexing[J]. Applied Optics, 1999, 38(15): 7288-7293.
[9] SITU G H, ZHANG J. Multiple-image encryption by wavelength multiplexing[J]. Optics Letters, 2005, 30(6): 1306-1308.
[10] BARRERA J, HENAO R. Multiplexing encryption-decryption via lateral shifting of a random phase mask[J]. Optics Communications, 2006, 259(3): 532-536.
[11] BARRERA J, HENAO R. Multiplexing encrypted data by using polarized light [J]. Optics Communications, 2006, 260 (1): 109-112.
[12] RUEDA E, RIOS C. Experimental multiplexing approach via code key rotations under a joint transform correlator scheme[J]. Optics Communications, 2011, 284(7):2500-2504.
[13] BARRERA J, HENAO R. Multiple image encryption using an aperture-modulated optical system[J]. Optics Communications, 2006, 261(1): 29-33.
[14] SHEN X J, LIN Ch, KONG D Zh. Fresnel-transform holographic encryption based on angular ultiplexing and random-amplitude mask[J]. Optical Engineering, 2012, 51(6): 3286-3219.
[15] MUNOZ-RODRIGUEZ J A. Computational cryptography based on trigonometric algorithms and intensity superposition[J]. Imaging Science Journal, 2010, 58(2): 61-80.