doi:10.3788/gzxb20124101.0072

基于两步正交相移干涉的振幅图像光学加密技术

曾大奎,马利红,刘健,金伟民

(浙江师范大学 信息光学研究所,浙江 金华 321004)

摘 要:提出一种基于两步正交相移干涉的光学图像加密技术.这种相移干涉数字全息只要记录两幅干涉图,不需要记录物光波和参考光波的强度信息,就可以再现没有零级像和共轭像的再现像.物光波对应的光路经过两次菲涅尔变换,并结合双随机相位编码.参考光分别引入 0 和 π/2 相位,用数字化记录介质记录两幅数字全息图作为加密图像.解密时只要获得正确的密钥,经过简单的计算就可以重建清晰的原始图像.模拟实验验证了它的可行性和有效性,分析了抗裁剪和噪音的鲁棒性.

关键词:加密;相移干涉;数字全息;菲涅尔变换;随机相位

中图分类号:O438 **文献标识码**:A **文章编号**:1004-4213(2012)01-0072-5

0 引言

在信息安全理论与技术的研究中,基于光学理论和手段的图像加密技术[1]是一个重要的分支.自从 1995 年 Philippe Refregier 和 Bahram Javidi 提出双随机相位加密技术[2]以来,许多学者提出了改进的方法.在系统结构方面,采用了傅里叶变换[3-5]、菲涅尔变换[6]、分数傅里叶变换[7-9]、小波变换[10-11]、联合变换相关器[12-13]干涉[14-16]等;在加密方法方面,有双随机相位加密[2]、相位恢复算法[17-19]、像素置乱[20]、衍射光学元件[21]等;在记录方式上,有卤化银全息干板、光折变晶体、CCD 等.由于 CCD 记录方式的数字全息具有实时记录、数字存储和传输等优点,解密再现可以是电子或光电方式,使光学加密技术更好地与数字信号处理和通讯系统相兼容,而被广泛应用[22].数字全息和相移干涉技术相结合后,在保留原物体信息的基础上,很好地去除了零级像和共轭像,可以获得更理想的再现像.现有的相移干涉光学加密技术一般采用四步或三步相移干涉[23-24].近些年提出的广义两步相移干涉方法[25-26],虽然相移的步长可以是 0 到 π 范围内的任意值,但需要记录物光波和参考光波的强度,记录次数并没有减少.为了减少记录次数及数值处理过程,文献[27]提出了仅记录两幅干涉图就可以恢复物光场的方法.这种方法仅需记录两幅干涉图,不需要记录物光波和参考光波的强度,就可以再现没有零级像和共轭像的再现像,记录次数只有两次,是最为简单的相移干涉方法.

本文在基于两步正交相移干涉的基础上,结合菲涅尔域的双随机相位编码方法,对光学图像进行了加密.通过模拟实验证明,该方法不仅减少了系统的运算和存储量,而且提高了信息传输效率.

1 加密解密的原理

1.1 只有两步的正交相移干涉数字全息

在全息图记录平面上,假设物光波复振幅为 O,参考光波是平面波,振幅为 R.参考光分别引入 0 和 π/2 相位.被 CCD 记录的两个正交相移同轴全息图的光强分布表示为

$$I_{H_1}=|R+O|^2=I_0+R^*O+RO^* \tag{1}$$

$$I_{H_2}=|R\exp^{j\pi/2}+O|^2=I_0-jR^*O+jRO^* \tag{2}$$

式中 I_0 表示零级光波或直流项

$$I_0=|R|^2+|O|^2 \tag{3}$$

如果构建一个复合全息图 H_{PHS}

$$H_{PHS}=(I_{H_1}-I_0)+j(I_{H_2}-I_0)=2R^*O \tag{4}$$

即获得没有零级光波和共轭光波的全息图.

因为没有记录物光波和参考光波的强度,只能从两个正交相移干涉图 I_{H_1} 和 I_{H_2} 中获得 I_0.

只要参考光强度达到一定值,满足

$$A=\frac{2R}{\max(|O|)+\min(|O|)}\geqslant 1 \tag{5}$$

基金项目:浙江省自然科学基金(No. Y1080944)资助

第一作者:曾大奎(1973—),男,硕士研究生,主要研究方向为光学信息处理. Email:524752919@qq.com

导师(通讯作者):金伟民(1965—),男,教授,主要研究方向为光学信息处理. Email:jhjinwm@163.com

收稿日期:2011-09-20;**修回日期**:2011-10-17

的要求，可以按照表达式

$$I_0=(2R^2+I_{H_1}+I_{H_2})/2-[(2R^2+I_{H_1}+I_{H_2})^2-2(I_{H_1}^2+I_{H_2}^2+4R^4)]^{1/2}/2 \quad (6)$$

计算 I_0. 选取各种可能的 R 值，按照式(4)和(6)再现的光波表示为 E_R. 从 I_{H_1} 直接再现的光波为 E_T. 通过计算 E_R 和 E_T 相关值，找出相关峰，对应的 R 值确定为最终实际再现的 R 值大小. 再根据式(4)和(6)，可以得到与原始图像非常接近的再现像.

1.2　加密过程

本文加密过程光路如图 1. 图中，HWP 为半波片，PBS 为偏振分束器，M 为反射镜，QWP 为四分之一波片，BS 为分束器，PM_1、PM_2 为相位掩模板，BE 为扩束器.

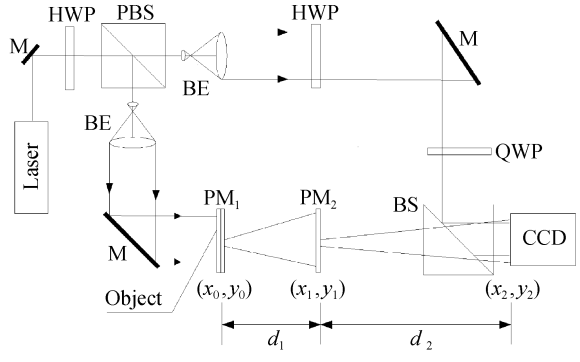


图 1　加密过程光路

Fig. 1　Optical setup for image encryption

假设两个随机相位板 PM_1 和 PM_2 的复振幅透过率分别可以表示为 $\exp[j2\pi\phi_1(x,y)]$ 和 $\exp[j2\pi\phi_2(x,y)]$，其中 $\phi_1(x,y)$ 和 $\phi_2(x,y)$ 分别代表两个在[0,1]之间随机分布的白噪音. 输入平面 (x_0,y_0) 与变换平面 (x_1,y_1) 之间的距离为 d_1，变换平面 (x_1,y_1) 与记录平面 (x_2,y_2) 之间的距离为 d_2，记录平面的物光波复振幅场可以表示为

$$U(x_2,y_2)=\mathrm{FrT}_{d_2}\{\mathrm{FrT}_{d_1}\{O(x_0,y_0)\cdot \exp[j2\pi\phi_1(x_0,y_0)]\}\exp[j2\pi\phi_2(x_1,y_1)]\} \quad (7)$$

式中 FrT 表示菲涅尔变换. 对平面波参考光引入相位分别为 0 和 $\pi/2$，用 CCD 记录得到两幅干涉图 I_{H_1} 和 I_{H_2}. 它们可以当作加密后的非负图像通过网络或者其他方式传送给信息的接收方，两个随机相位板 PM_1、PM_2 以及 d_1、d_2、λ 等都可以视为密钥.

1.3　解密过程

接受方得到所有密钥后，原来被隐藏的振幅图像 $O(x_0,y_0)$ 的解密步骤为：

1)选取各种可能的 R 值，按照式(4)和(6)获得取各种 R 值所对应的再现光波 E_R.

2)从 I_{H_1} 直接再现获得光波 E_T，$E_T=I_{H_1}-I_0=R^*O+RO^*$. 其中，$I_0=\frac{1}{M\times N}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1}[I_{H_1}(k\Delta x,l\Delta y)]$，全息图的像素为 $M\times N$，Δx、Δy 分别表示 CCD 在水平和垂直方向相邻像素的间距[28]. 虽然 E_T 中含有物光波的共轭项，但毕竟包含了物光波的正确信息，用它作为目标图像与 E_R 相关运算，可以确定 R 值的大小.

3)计算 E_R 和 E_T 的相关值，画出相关值随 R 值的变化曲线. 找出相关峰，因为相关峰所对应的 E_R 与 E_T 最为接近，所以与相关峰所对应的 R 值确定为最终实际再现的 R 值大小[27].

4)按照式(6)计算得到 I_0.

5)根据式(4)计算得到

$$H_{PHS}=(I_{H_1}-I_0)+j(I_{H_2}-I_0)=2R^*U(x_2,y_2) \quad (8)$$

6)计算得

$$U(x_2,y_2)=H_{PHS}/2R^* \quad (9)$$

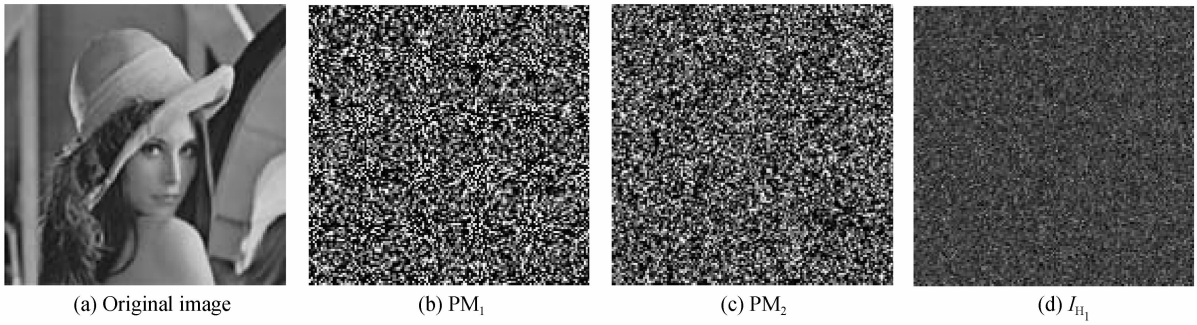
7)通过两次逆菲涅尔变换恢复出原输入平面 (x_0,y_0) 上的物光场复振幅. 由于光学上无法实现逆菲涅尔变换，取 $U(x_2,y_2)$ 的复共轭对 $U^*(x_2,y_2)$ 菲涅尔变换，然后乘以 PM_2；再进行一次菲涅尔变换，乘以 PM_1，得到光场复振幅的复共轭[6].

$$O^*(x_0,y_0)=\mathrm{FrT}_{d_1}\{\mathrm{FrT}_{d_2}[U^*(x_2,y_2)]\cdot \exp[j2\pi\phi_2(x_1,y_1)]\}\exp[j2\pi\phi_1(x_0,y_0)] \quad (10)$$

而：$|O^*(x_0,y_0)|^2=|O(x_0,y_0)|^2$，原图像得到恢复.

2　实验与分析

为了验证该加密系统的可行性，本文进行了数值模拟实验. 选取了灰度级为 256、像素为 256×256 的‘Lena’图像作为待加密的振幅物体，如图 2(a). 系统参量 $\lambda=632.8$ nm，$d_1=110$ mm，$d_2=245$ mm. 选取 $A=3$.



(a) Original image　(b) PM_1　(c) PM_2　(d) I_{H_1}

图 2 加密、解密过程中得到的图像

Fig. 2 Encryption and decryption of images obtained in the course

本文验证了当所有密钥都正确使用时，该加密系统的可行性. 图 2(b)和(c)分别表示随机相位板 PM_1 和 PM_2；干涉图 I_{H_1} 和 I_{H_2} 分别如图 2(d)、(e)；图 2(f)给出了正确解密后的振幅图像，很明显，解密图像可以成功恢复，没有任何噪音影响.

如果待加密的是图像函数是复数，当密钥 PM_1、PM_2 不正确时，不能得到原始图像. 如果待加密的是振幅图像，图像函数是正的实函数，密钥 PM_1 的相位函数 $\exp[j2\pi\psi_1(x,y)]$ 可以通过光强敏感的探测器消除. 图 2(g)表示随机相位板 PM_2 不正确时的解密图像.

当系统参量 d_1、d_2、λ 有微小变化时，将影响解密图像的质量，严重的话，将不能恢复原始图像. 因此，系统参量也可以作为密钥. 为了评价解密图像的质量，用解密图像与原始图像之间的相关系数(Correlation Coefficient，CC)或均方差(Mean Square Error，MSE)来衡量. 相关系数表示为

$$\mathrm{CC}=\Big[\sum_{M=1}^{M}\sum_{N=1}^{N}(O'_{(M,N)}-\overline{O'_{(M,N)}})(O_{(M,N)}-\overline{O_{(M,N)}})\Big]\Big/\Big[\Big(\sum_{M=1}^{M}\sum_{N=1}^{N}(O'_{(M,N)}-\overline{O'_{(M,N)}})^2\Big)\cdot\Big(\sum_{M=1}^{M}\sum_{N=1}^{N}(O_{(M,N)}-\overline{O_{(M,N)}})^2\Big)\Big]^{1/2} \tag{11}$$

式中

$$\overline{O_{(M,N)}}=\frac{1}{M\times N}\sum_{M=1}^{M}\sum_{N=1}^{N}O_{(M,N)} \tag{12}$$

$$\overline{O'_{(M,N)}}=\frac{1}{M\times N}\sum_{M=1}^{M}\sum_{N=1}^{N}O'_{(M,N)} \tag{13}$$

$M\times N$ 为图像的像素数，O 表示原始图像，O' 表示解密图像.

均方差表示为

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{M=1}^{M}\sum_{N=1}^{N}|O'_{(M,N)}-O_{(M,N)}|^2 \tag{14}$$

图 3(a)绘制了解密图像的相关系数 CC 与波长误差之间的关系曲线；图 3(b)绘制了解密图像的相关系数 CC 与衍射距离 d_1、d_2 误差之间的关系曲线. 不难看出，曲线具有一定的对称性，随着波长误差的增大，相关系数 CC 显著下降. 当波长的相对误差达到 2.14%时，此时相关系数 CC 为 0.15，均方差为 0.09，解密出的图像将变成噪音图像. 相关系数 CC 与两个距离参量之间的关系曲线有一定的差异，距离记录平面较近的参量 d_2 比与之较远的参量 d_1 有更高的灵敏度. 当衍射距离 d_2 有 1.91%的相对误差时，其恢复的图像已变为噪音图像，此时相关系数为 0.15，均方差为 0.09；当衍射距离 d_1 达到 18.01%的相对误差时，其恢复的图像变为噪音图像，此时相关系数为 0.15，均方差为 0.09.

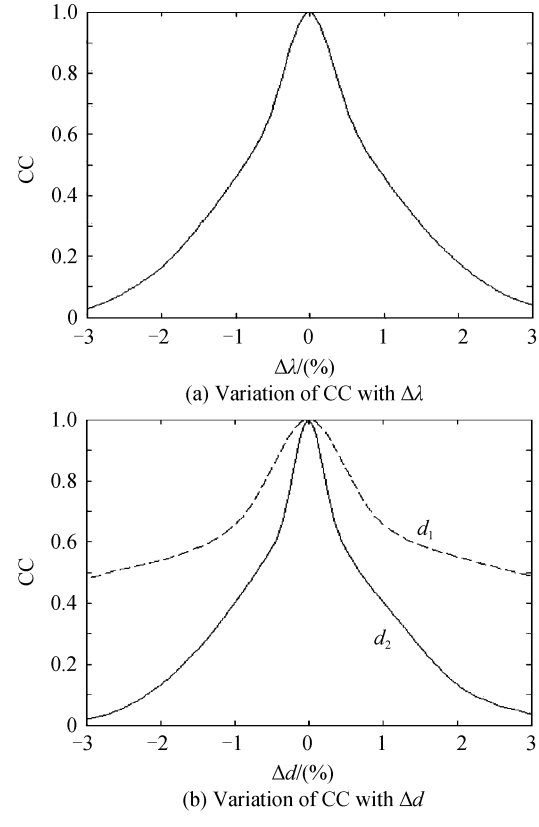


图 3 相关系数 CC 与波长误差、衍射距离误差之间关系

Fig. 3 The relation of correlation coefficient versus the wavelength error and the diffraction distance error

对该加密系统抗裁剪和噪音攻击的鲁棒性的分析. 图 4(a)给出了其中一幅干涉图 I_{H_1} 被裁剪 1.56%后的结果，利用一套被1.56%裁剪攻击后的干涉图解密出的振幅图像如图 4(b). 图 4(c)表示某

一幅干涉图 I_{H_1} 被零均值、标准差为 0.01 的加性高斯白噪音攻击后的结果，利用这一套被噪音攻击后的干涉图解密出的振幅图像如图 4(d). 在裁剪和噪音攻击两种情况下，虽然恢复后的图像均受到了一定噪音的影响，但振幅图像的基本信息都可以成功辨别，表明该振幅图像加密系统具有一定的抗裁剪和噪音攻击的鲁棒性. 与其它系统相比，抗裁剪的鲁棒性不够理想.

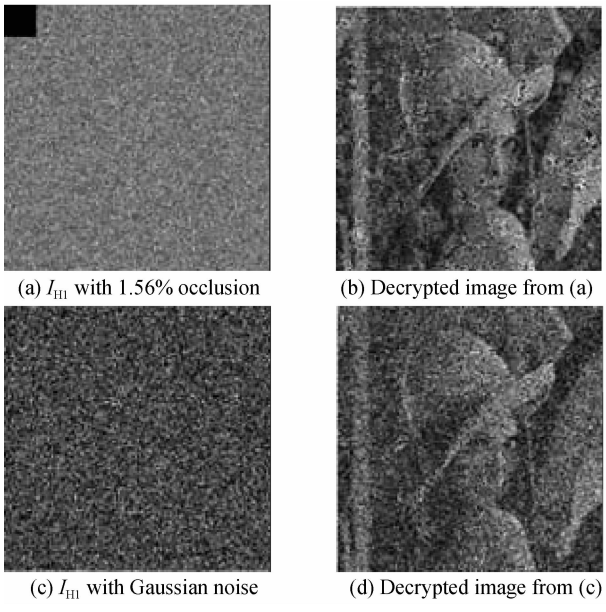


图 4　抗裁剪和噪音攻击的鲁棒性

Fig. 4　The robustness against occlusion and noise attacking

3　结论

本文成功地将两步正交相移干涉应用于光学图像的加密，仅记录两幅全息图，而不需要记录物光波和参考光波的强度信息. 由于记录次数的减少，简化了实验操作步骤，降低了计算量和存储量，并提高了信息的传输效率. 模拟实验验证了该方法的可行性. 研究结果表明，在各个密钥正确的情况下，可以重建清晰的原图像，但是密钥一旦错误，重建图像就会受到影响或不能恢复. 在保持了双随机相位编码方法安全性的同时，还增加了系统参量密钥，进一步提高了系统的安全性. 通过鲁棒性分析，该加密系统具有一定的抗裁剪和噪音攻击的能力，与其它系统相比，抗裁剪的鲁棒性不是很好.

参考文献

[1] DENG Xiao-peng. Optical encryption based on public key distribution system[J]. *Acta Photonica Sinica*, 2010, **39**(7): 1263-1267.
邓晓鹏. 基于公匙密匙分配体制的光学加密系统[J]. 光子学报, 2010, **39**(7): 1263-1267.

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

[3] SINGH M, KUMAR A. Optical encryption and decryption using a sandwich random phase diffuser in the Fourier plane [J]. *Optical Engineering*, 2007, **46**(5): 055201.

[4] ZHANG Yan, WANG Bo. Optical image encryption based on interference[J]. *Optics Letters*, 2008, **33**(21): 2443-2445.

[5] QIN Wan, PENG Xiang. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Letters*, 2010, **35**(2): 118-120.

[6] SI-TU Guo-hai, ZHANG Jing-juan. Double random-phase encoding in the Fresnel domain[J]. *Optics Letters*, 2004, **29**(14): 1584-1586.

[7] TAO R, LANG J, WANG Y. Optical image encryption based on the multiple parameter fractional Fourier transform[J]. *Optics Letters*, 2008, **33**(6): 581-583.

[8] HENNELLY B M, SHERIDAN J T. Optical image encryption by random shifting in fractional Fourier domains [J]. *Optics Letters*, 2003, **28**(4): 269-271.

[9] JIA Li-juan, LIU Zheng-jun. Double image encryption algorithm based on random fractional Fourier transform[J]. *Acta Photonica Sinica*, 2009, **38**(4): 1020-1024.
贾丽娟，刘正君. 基于随机分数傅里叶变换的双图像加密算法[J]. 光子学报, 2009, **38**(4): 1020-1024.

[10] DANG P P, CHAU P M. Image encryption for secure Internet multimedia applications[J]. *IEEE Transactions on Consumer Electronics*, 2000, **46**(3): 395-403.

[11] CHEN Lin-fei, ZHAO Dao-mu. Optical image encryption based on fractional wavelet transform [J]. *Optics Communications*, 2005, **254**(4-6): 361-367.

[12] LU Ding, JIN Wei-min. Color image encryption based on joint fractional Fourier transform correlator [J]. *Optical Engineering*, 2011, **50**(6): 8201-8207.

[13] MELA C L, IEMI C. Optical encryption using phase-shifting interferometry in a joint transform correlatorr[J]. *Optics Letters*, 2006, **31**(17): 2562-2564.

[14] ZHANG Yan, WANG Bo. Optical image encryption based on interference[J]. *Optics Letters*, 2008, **33**(21): 2443-2445.

[15] ZHU Nan, WANG Yong-tian, LIU Juan, *et al*. Optical image encryption based on interference of polarized light[J]. *Optics Express*, 2009, **17**(16): 13418-13424.

[16] NIU Chun-hui, WANG Xiao-ling, LV Nai-guang, *et al*. An encryption method with multiple encrypted keys based on interference principle[J]. *Optics Express*, 2010, **18**(8): 7827-7834.

[17] HWANG H E, CHANG H T, LIE W N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain[J]. *Optics Letters*, 2009, **34**(24): 3917-3919.

[18] LU Ding, JIN Wei-min. Fully phase color image encryption based on joint fractional Fourier transform correlator and phase retrieval algorithm[J]. *Chinese Optics Letters*, 2011, **9**(2): 34-36.

[19] LU Ding, JIN Wei-min. Color image encryption based on joint fractional Fourier transform correlator and phase retrieval algorithm[C]. *SPIE*, 2010, **7851**: 785101-785109.

[20] LU Hong-qiang, ZHAO Jian-lin, FAN Qi, *et al*. Iterative double random phase encryption based on pixel scrambling technology[J]. *Acta Photonica Sinica*, 2005, **34**(7): 1069-1073.
陆红强，赵建林，范琦，等. 基于像素置乱技术的多重双随机相位加密法[J]. 光子学报, 2005, **34**(7): 1069-1073.

[21] JOHNSON E G, BRASHER J D. Phase encryption of biometrics in diffractive optical elements[J]. *Optics Letters*, 1996, **21**(16): 1271-1273.

[22] GIL S K, JEON S H, KIM N, *et al*. Successive encryption

and transmission with phase-shifting digital holography[C]. *SPIE*, 2006, **6136**: 613615-1-2613615-8.

[23] WANG Xiao-gang, ZHAO Dao-mu. Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry[J]. *Optics Communications*, 2006, **268**(2): 240-244.

[24] HE Ming-zhao, CAI Lv-zhong, LIU Qing, *et al*. Phase-only encryption and watermarking based on phase-shifting interferometry[J]. *Appled Optics*, 2005, **44**(13): 2600-2606.

[25] MENG Xiang-feng, CAI Lv-zhong, XU Xian-feng, *et al*. Two-step phase-shifting interferometry and its application in image encryption[J]. *Optics Letters*, 2006, **31**(10): 1414-1416.

[26] LI Hui-juan. Image encryption based on gyrator transform and two-step phase-shifting interferometry[J]. *Optics and Lasers in Engineering*, 2009, **47**(1): 40-50.

[27] LIU J P, POON T C. Two-step-only quadrature phase-shifting digital holography[J]. *Optics Letters*, 2009, **34**(3): 250-252.

[28] SCHNARS U, JÜPTNER W P O. Digital recording and numerical reconstruction of holograms[J]. *Measurement Science and Technology*, 2002, **13**(9): R85-R101.

Amplitude Image Optical Encryption Based on Two-step-only Quadrature Phase-shifting Interferometry

ZENG Da-kui, MA Li-hong, LIU Jian, JIN Wei-min

(*Institute of information Optics, Zhejiang Normal University, Jinhua, Zhejiang* 321004, *China*)

Abstract: A novel optical image encryption is proposed based on two-step-only quadrature phase-shifting interferometry. Only two interferograms are needed to reconstruct a zero-order-and twin-image-free hologram in this phase-shifting digital holography interference. Such technique precludes the need from recording either the reference wave or the object wave intensity. The object wavefront propagates with two Fresnel transforms in the light path, combined with the double random phase encoding. The following is that introducing zero and $\pi/2$ phase into reference waves respectively and recording two digital holograms as encrypted image. As long as the correct key is given in the decryption, a clear original image can be reconstructed by a simple calculation. The feasibility and its robustness against occlusion and noise attacks are verified by a series of numerical simulations.

Key words: Encryption; Phase-shifting interferometry; Digital holography; The Fresnel transform; Random phase