

# 基于三维空间正交偏振态复用的光学认证技术研究

林 超<sup>1</sup> 沈学举<sup>1</sup> 雷 鸣<sup>2</sup> 窦帅风<sup>1</sup> 邹 效<sup>3</sup>

<sup>1</sup>军械工程学院电子与光学工程系,河北 石家庄 050003

<sup>2</sup>中国国防科技信息中心,北京 100138

<sup>3</sup>总装备部重庆军代局驻北碚军代室,重庆 400700

**摘要** 为提高光学认证技术的安全性及实用性,提出了基于三维空间正交偏振态复用的光学多级安全认证方法。用所设计的多衍射平面多信号窗口相位恢复算法,生成两个相位模板,使由认证图像分割得到的子块图像分布于其三维菲涅耳衍射场的特定位置。一个相位模板作为系统锁,另一个作为认证密钥。用正交偏振光分别照明两相位模板,实现了三维空间衍射场内不同位置强度分布和偏振态分布的控制。只有同时具备认证密钥和三维空间正交偏振态映射密钥,才能恢复认证图像,模拟及实验结果与认证图像的相关系数分别为0.93和0.79,表明该系统结构紧凑、安全等级高,可以实现分级认证。

**关键词** 傅里叶光学; 光学数据处理; 光学安全认证; 相位恢复算法; 正交偏振态复用

中图分类号 O438; TP751 文献标识码 A

doi: 10.3788/AOS201636.0307001

## Optical Security Validation Based on Orthogonal Polarization Multiplexing in Three-Dimensional Space

Lin Chao<sup>1</sup> Shen Xueju<sup>1</sup> Lei Ming<sup>2</sup> Dou Shuaifeng<sup>1</sup> Zou Xiao<sup>3</sup>

<sup>1</sup>Department of Opto-Electronics Engineering, Ordnance Engineering College of PLA, Shijiazhuang, Hebei 050003, China

<sup>2</sup>China Defense Science & Technology Information Center, Beijing 100138, China

<sup>3</sup>Military Representatives Office of Beibei District, Military Representatives Bureau of General Armament Department, Chongqing 400700, China

**Abstract** To enhance the security level and practicality of optical validation technique, an optical multiple-level security validation method is proposed based on the multiplexing of orthogonal polarization states in three-dimensional space. Two phase-only masks are generated by adopting the designed multiple diffractive planes and multiple signal windows phase retrieval algorithm, in order to reproduce Fresnel diffraction field with all of the subblocks which are obtained by the partition of the validated image distributed in specific locations in three-dimensional space. One of the two phase-only masks is taken as the system lock. The other one is acted as the security validation key. The two phase-only masks are illuminated by orthogonal polarized respectively. The control of both intensity distributions and polarization distributions in different place are achieved in three-dimensional space. Only when both the security validation key and the three-dimensional orthogonal polarization map key are obtained, the validated image is retrieved. The correlation coefficients between the verification image and simulation or experimental results are 0.93 and 0.79 respectively, which shows the proposed system is a quite compact setup, with both high security level and multiple-level validation functionality.

收稿日期: 2015-09-05; 收到修改稿日期: 2015-11-10

基金项目: 河北省自然科学基金(F2014506004)

作者简介: 林 超(1987—),男,博士研究生,主要从事光电信息处理方面的研究。E-mail: vestigelinchao@163.com

导师简介: 沈学举(1963—),男,博士,教授,主要从事光电信息处理及激光技术方面的研究。

E-mail: shxjoptics@aliyun.com(通信联系人)

**Key words** Fourier optics; data processing by optical means; optical security validation; phase retrieval algorithm; orthogonal polarization multiplexing

**OCIS codes** 070.4560; 060.4785; 260.5430

## 1 引 言

由于光波的固有属性,使光学加密、解密和认证具有处理速度快、编码维度多等优点。双随机相位编码(DRPE)方法的提出在加密和认证领域掀起了一股研究热潮<sup>[1-2]</sup>。光学密码编码学从线性、对称加密算法的研究<sup>[3]</sup>,演化到非线性、非对称加密方法的探索<sup>[4-5]</sup>,使光学加密技术的安全性得到很大提高。然而,随着光学密码分析学的深入研究,DRPE暴露出了很多安全隐患。例如,通过已知明文攻击或唯密文攻击<sup>[6-7]</sup>,可以获得加密系统的密钥。各种新的光学加密和认证方法的提出,在丰富其研究内容的同时,也不断地提高其安全性<sup>[8-12]</sup>。然而,随着光电器件性能的提高,传统的认证全息图容易被复制,造成安全隐患。由于相位信息的不易探测性,基于纯相位编码的安全认证技术得到广泛关注<sup>[13]</sup>,在信用卡或护照认证、高强度门禁系统、数据库访问权限控制等领域有潜在应用前景。但是,由于相干光学信息系统对元件的空间对准精度要求很高且容错能力较低,现有加密和认证方案在光学实现方面进展较为缓慢<sup>[14-15]</sup>,其实用化仍面临挑战。

基于双光束干涉的光学加密及认证方法具有系统结构简单,对空间对准精度要求不高,易于光学实现等优点<sup>[16]</sup>。其加密过程是基于复振幅平面中的矢量分解,生成一对纯相位模板,其中一个纯相位模板作为加密图像,另一个作为密钥。其解密过程是基于菲涅耳域中的双光束干涉<sup>[17-18]</sup>。然而,由于两个纯相位模板是线性地提取自原始图像,存在相互依赖关系,攻击者只需获得其中一个相位模板,就可以恢复出原始图像的轮廓信息<sup>[19]</sup>,这在光学认证中是一个安全隐患。并且,对干涉加密方法的碰撞攻击的研究表明,存在多对密钥,可以认证出同一图像<sup>[20]</sup>。因此,干涉加密的应用受到限制。为解决上述问题并提高干涉加密方法的安全性。研究者提出了多种改进方法。例如,三光束相干叠加<sup>[21]</sup>,分数阶傅里叶变换域干涉加密<sup>[22]</sup>等。虽然提高了安全性,但也使系统结构趋于复杂,其实用性有待进一步提高。

针对上述问题,本文提出了基于双光束正交偏振态复用的光学认证方法。充分利用光波的振幅、相位和偏振态以及菲涅耳衍射距离,实现多密钥维度光学安全认证。同时,所设计的认证系统基于正交偏振光的非相干叠加,可明显降低相干噪声的影响和光学系统的调试难度。在具有较高安全性的同时降低了系统复杂度。在理论分析和数值模拟的基础上,进行了实验验证,展示了该方法的优点,对于光学安全认证技术的实用化有一定价值。

## 2 原 理

### 2.1 编码过程

系统的编码算法采用计算机实现,认证过程采用光学硬件实现。编码过程分为两个步骤:

1) 待认证图像的预处理。将待认证图像分解为互补的两个子图像,将子图像分割为若干子块图像。为防止攻击者穷举搜索获取各子块图像信息,引入一幅独立于认证图像的错误认证图像来混淆攻击者。将错误认证图像和待认证图像按上述方式采用相同的分割方法进行分解和分块,将两图像的子块图像随机组合,生成两幅含错误子块图像的合成子图像。如图1所示,用  $P_1$  表示待认证图像,  $P_2$  表示错误认证图像,  $P_{1_i}$  和  $P_{1_k}$  分别表示  $P_1$  的两个互补子图像的第  $i$  和第  $k$  个子块图像,  $P_{2_i}$  和  $P_{2_k}$  分别表示  $P_2$  的两个互补子图像的第  $i$  和第  $k$  个子块图像。假设  $P_1$  和  $P_2$  均被分割为  $3 \times 3$  个子块,则认证图像的振幅分布可表示为

$$P_1 = \sum_{i=1}^{i_{\max}} P_{1_i} + \sum_{k=1}^{k_{\max}} P_{1_k} = (\sum_{i=1}^{i_{\max}} P_{1_i} + \sum_{k=1}^{k_{\max}} P_{2_k}) + (\sum_{k=1}^{k_{\max}} P_{1_k} + \sum_{i=1}^{i_{\max}} P_{2_i}) - P_2 = P_3 + P_4 - P_2, \quad (1)$$

式中  $P_2 = \sum_{i=1}^{i_{\max}} P_{2_i} + \sum_{k=1}^{k_{\max}} P_{2_k}$ ,  $P_3 = \sum_{i=1}^{i_{\max}} P_{1_i} + \sum_{k=1}^{k_{\max}} P_{2_k}$ ,  $P_4 = \sum_{k=1}^{k_{\max}} P_{1_k} + \sum_{i=1}^{i_{\max}} P_{2_i}$ ,  $i_{\max}$  和  $k_{\max}$  分别表示  $P_1$  或  $P_2$  两互补子图中的子块图像最大个数,假设子块个数为9时,满足  $i_{\max} + k_{\max} = 9$ 。  $P_3$  和  $P_4$  表示加入了错误子块后的合成子图像振幅分布,即由  $P_1$  的某一子图像和与其互补的  $P_2$  的子图像组成的合成图像振幅分布。

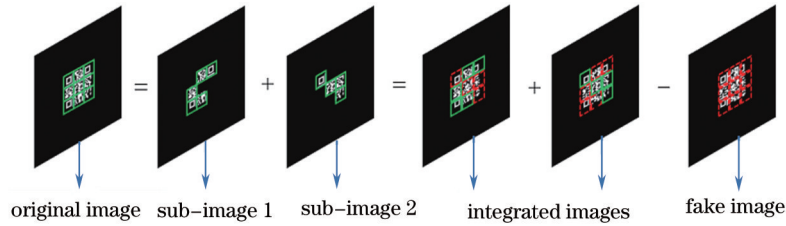


图1 图像分解和分块预处理

Fig.1 Preprocessing procedure of image decomposition and partitioning

图1绿色实线框表示待认证图像的分块,红色虚线框表示错误认证图像的分块。原则上说,任意规则或不规则的图像分割方法均可以用来预处理待认证图像。

2) 认证密钥的生成。用所设计的多平面多信号窗口(MP-MSW)相位恢复算法,将加入错误子块后的子图1和2编码成两个纯相位函数,使其菲涅耳衍射图样在三维空间呈现出预定的强度分布。由于采用了分块预处理方法,可以有效防止只用一个纯相位函数恢复出认证图像的轮廓信息。结合正交偏振态复用,可以进一步提高系统的安全性。本质上说,基于三维空间正交偏振态复用的光学认证技术是通过优化特定的矢量光束,生成具有特定强度和偏振态空间分布的三维菲涅耳衍射场。

取方位为  $\theta$  的正交线偏光作为正交基,待优化的矢量光束表示为

$$E(x,y) = \exp[j\delta_+(x,y)] \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix} + \exp[j\delta_-(x,y)] \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix}, \quad (2)$$

式中  $(x,y)$  表示空间位置坐标,  $j$  为虚数单位,  $\delta_+(x,y)$  及  $\delta_-(x,y)$  为待优化的两个纯相位函数。根据 MP-MSW 相位恢复算法<sup>[23]</sup>,迭代算法开始时,分别赋予两个纯相位函数一组均匀分布于  $(0,2\pi)$  的随机相位值。分别计算两个纯相位函数的菲涅耳衍射场。需要注意的是,严格地说,对于矢量光束,需要采用矢量形式的衍射积分计算方法。然而,在本文实验条件下,由于系统的菲涅耳数满足  $F = a^2/(\lambda z) > 1$ ,式中  $a$  为系统衍射孔径的直径,  $\lambda$  为照明光波长,  $z$  为菲涅耳衍射距离。因此,采用标量菲涅耳衍射积分能够得到足够精确的衍射场的复振幅分布。设  $E_+(x,y) = \exp[j\delta_+(x,y)]$ ,  $E_-(x,y) = \exp[j\delta_-(x,y)]$ , 则光束传播到距纯相位模板所在平面距离为  $z_m$  的菲涅耳衍射场复振幅为

$$\begin{cases} O_{m+}^{(n)}(u,v) = F_{z_m} [E_+^{(n)}(x,y)] \\ O_{m-}^{(n)}(u,v) = F_{z_m} [E_-^{(n)}(x,y)] \end{cases}, \quad (3)$$

式中  $z_m$  表示一系列菲涅耳衍射平面距离纯相位模板所在平面的距离 ( $z_0 = 0$  位于纯相位模板所在平面),  $(u,v)$  表示菲涅耳衍射域的空间位置坐标,  $F[\cdot]$  表示菲涅耳衍射积分算符,上标  $n$  表示迭代次数 ( $n=1,2,3,\dots$ )。当待认证图像被分割成  $3 \times 3$  个子块时,  $m$  是最大值为9的正整数,即9个子块分别位于不同距离的衍射平面处。为了减少衍射投影效应的影响,在计算时保证各个子块在纵向位置上不共轴,满足分区复用条件。

由于具有正交偏振态的两束光均在一系列相同的菲涅耳衍射距离处成像,因此,需要在每个菲涅耳衍射平面上进行多信号窗口的振幅约束,可以描述为

$$\begin{cases} \overline{O_{m+}^{(n)}(u,v)} = f_{\text{FMSWAC}_+} [O_{m+}^{(n)}(u,v)] \\ \overline{O_{m-}^{(n)}(u,v)} = f_{\text{FMSWAC}_-} [O_{m-}^{(n)}(u,v)] \end{cases}, \quad (4)$$

式中  $f_{\text{FMSWAC}[\cdot]}$  表示菲涅耳衍射平面多信号窗口振幅约束(FMSWAC),定义为

$$f_{\text{FMSWAC}} [O_m^{(n)}(u,v)] = \begin{cases} \Omega P_m(u,v), (u,v) \in S \\ |O_m^{(n)}(u,v)|, (u,v) \notin S \end{cases}, \quad (5)$$

式中  $P_m(u,v)$  或  $P_n(u,v)$  表示在预定信号窗口处想要得到的认证图像某一子块的振幅分布,  $\Omega$  表示迭代算法计算得到的信号窗口处所有像素点振幅之和与想要得到的某一子块在信号窗口处所有像素点振幅之和的比值,  $S$  表示多信号窗口支撑的空间区域,即衍射平面内的包含特定子块的窗口。

对施加了振幅约束后的衍射场分布进行逆菲涅耳变换,得到纯相位模板所在平面的复振幅分布为

$$\begin{cases} E_{m+}^{(n)}(x,y) = f_{\text{Fres}_{-z_m}}[\overline{O_{m+}^{(n)}(u,v)}] \\ E_{m-}^{(n)}(x,y) = f_{\text{Fres}_{-z_m}}[\overline{O_{m-}^{(n)}(u,v)}] \end{cases} \quad (6)$$

在该平面,施加均匀振幅分布约束,即将振幅归一化,只保留相位分量。得到经过  $n$  次迭代后的优化的纯相位函数的相位分布为

$$\begin{cases} E_+^{(n)}(x,y) = f_{\text{UAC}}[E_{m+}^{(n)}(x,y)] \\ E_-^{(n)}(x,y) = f_{\text{UAC}}[E_{m-}^{(n)}(x,y)] \end{cases} \quad (7)$$

式中  $f_{\text{UAC}}[\cdot]$  表示均匀振幅分布约束(UAC)。

在迭代过程中,当  $n=1$  时,从  $z_0$  平面到  $z_1$  平面, (2)~(7)式运行一个子循环,得到两个初步优化后的纯相位分布函数。以这两个纯相位函数作为输入,从  $z_0$  到  $z_m$  平面反复运行 (2)~(7)式,直到  $m$  达到最大值。至此,一个完整的循环结束。设  $n=n+1$ ,进行下一个循环计算,直到预先设定的循环次数完成,或者,(4)式和(5)式设定的约束精度达到预定值,该 MP-MSW 相位恢复算法结束,得到最终的优化后的纯相位函数。将其中任意一个纯相位函数作为系统锁,另一个作为认证密钥。

## 2.2 认证过程

认证系统的原理示意图如图 2 所示。图中,认证系统的核心为一个矢量光束生成器,它由两个反射型相位液晶(LCD)空间光调制器(SLM)组成,分别加载系统锁和认证密钥。在 LCD 前表面一定距离处分别放置透光轴方向相互正交的线偏振片(LP)。当用准直单色光照明时,通过消偏振分光棱镜(NPBS)将两个 LCD 的衍射场进行偏振合成,在不同的菲涅耳衍射距离处用电荷耦合器件(CCD)探测强度分布。CCD 前放置一检偏器,用于区分同一衍射距离处不同衍射图案的不同偏振态。在认证密钥正确的前提下,只有当 CCD 在正确的菲涅耳衍射距离处探测到正确偏振态的子块的强度分布时,待认证图像的子块才能全部记录下来,通过后续的子块提取、去噪和重构操作,获得正确的认证图像。在这一过程中,菲涅耳衍射距离密钥和正交偏振映射密钥共同组成了一个三维空间正交偏振态认证密钥。如图 3 所示,只有在正确的衍射距离处选择了正确的偏振态,才能获得正确认证图像的子块强度信息,否则,只能获得噪声或者错误认证图像的子块信息。

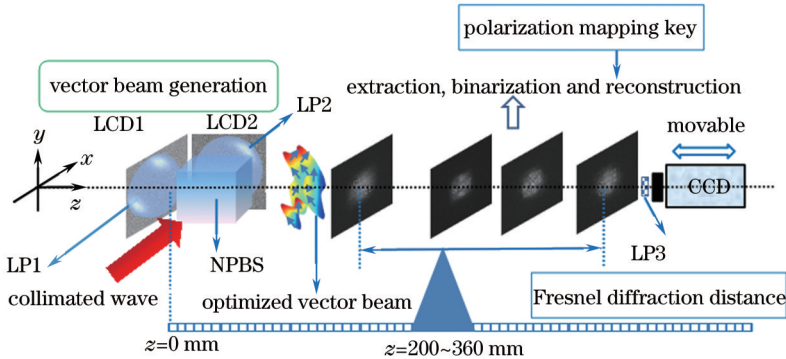


图 2 认证系统示意图

Fig.2 Schematic diagram of validated system

将该系统用于光学分级安全认证可以分为以下几个步骤:

- 1) 授权用户将自己所持有的纯相位认证模板插入系统中或加载到 LCD 上。
- 2) 在认证密钥正确的条件下,授权用户还被要求输入一个认证密码,该密码通过数字电路编码后可以驱动伺服机构使 CCD 及检偏器分别进行轴向移动和旋转,用来探测待认证图像的子块。
- 3) 不同级别的授权用户拥有不同长度的认证密码,一定长度的认证密码可以驱动 CCD 和检偏器探测到认证图像的部分或全部子块。实现了不同用户的分等级安全认证。
- 4) 将探测得到的认证图像子块与存储的正确子块进行比较,根据预先设定的识别阈值,由系统来判断是否通过认证,从而授予或者否决一定等级的系统(例如数据库)使用权限。

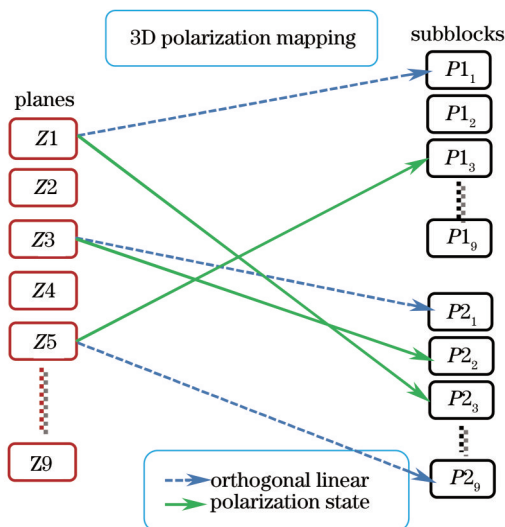


图3 三维空间正交偏振态映射  
Fig.3 Orthogonal polarization mapping in 3D space

### 3 结果及讨论

#### 3.1 数值仿真

基于 Matlab 7.01 平台,对编码和认证过程进行了数值模拟分析。为了消除各个子块的边缘信息对认证图像重构的影响,分别选取一个二维码图像和一个二值符号图像作为待认证图像,如图 4(a)、(c)所示。选取另外两个图像作为错误认证图像,如图 4(b)、(d)所示。图 4(a)、(b)分别编码了一组文字信息,即 3D Polarization Multiplexing 以及 QR Code Block Security。二维码具有较强的对于信息丢失或污损的容错能力,待认证文字信息可以被无损恢复,且其传播和使用途径广泛,因此具有一定的实用价值。

在 SLM 和 CCD 等硬件参数给定的条件下,数值模拟中设定的系统参数如下:为方便光路调校并与 SLM 和 CCD 器件的参数进行匹配,菲涅耳衍射距离范围为 200 ~ 360 mm,且分块个数为 9 个,为得到区分度较好的子块采集图像,每一个菲涅耳衍射平面间隔选为 20 mm。波长设为 632.8 nm,菲涅耳采样间隔设为实验中所使用的 LCD 的像素间隔 12.3 μm,MP-MSW 相位恢复算法迭代次数设置为 50。



图 4 (a)、(b) 待认证图像; (c)、(d) 错误认证图像

Fig.4 (a)、(b) Images before validation; (c)、(d) images with wrong validation

在上述条件下,对于二维码图像,数值模拟结果如图 5 所示。其中,图 5(a)、(b)表示经过预处理后的图像,图 5(c)、(d)表示优化得到的两个纯相位分布函数。假设 CCD 前没有放置检偏器,图 5(e)、(f)表示在不同菲涅耳衍射距离处计算得到的子块强度分布,衍射距离分别为 260 mm 和 360 mm。在相位模板认证密钥和三维正交偏振复用认证密钥均正确的条件下,经过去噪处理并重构的认证图像如图 5(g)所示。图 5(h)为用二维码扫描软件 Scan Life 扫描得到的正确认证信息。

在相同的数值模拟参数条件下,对二值符号图像的数值模拟结果如图 6 所示。其中,图 6(a)、(b)表示优化得到的两个纯相位分布函数。假设 CCD 前放置检偏器,图 6(c)、(d)表示在菲涅耳衍射距离为 260 mm 处计算得到的强度分布,检偏器透光轴方位相互正交。在相位模板认证密钥和三维正交偏振复用认证密钥均正确的条件下,重构的认证图像如图 6(e)所示。

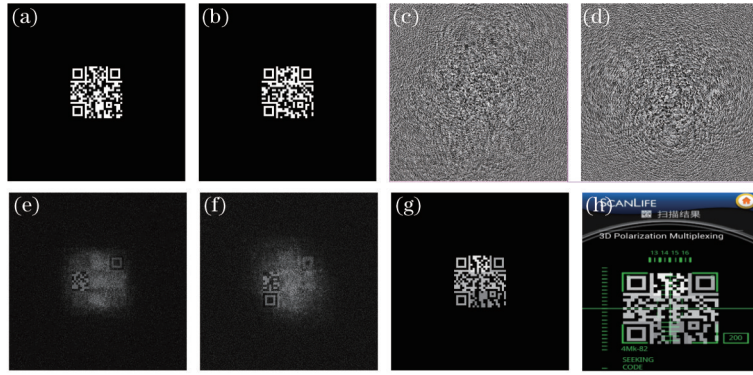


图5 二维码图像的数值模拟结果。(a)、(b) 预处理之后的子图；(c)、(d) 优化后的纯相位模板；(e)、(f) 在两个菲涅耳衍射距离处的衍射图样；(g) 重构的认证图像；(h) 对重构二维码的扫描

Fig.5 Numerical simulation results of QR code images. (a)、(b) Sub-images after preprocessing; (c)、(d) pure phase template after optimization; (e)、(f) diffraction patterns in two Fresnel diffraction distances; (g) reconstructed validation image; (h) scan result of reconstructed QR code

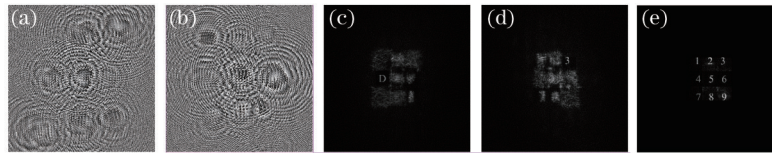


图6 二值符号图像的数值模拟结果。(a)、(b) 优化后的纯相位模板；(c)、(d) 在同一菲涅耳衍射距离处正交偏振态的衍射图样；(e) 重构的认证图像

Fig.6 Numerical simulation results of binary symbol images. (a)、(b) pure phase template after optimization; (c)、(d) diffraction patterns in same Fresnel diffraction distance with orthogonal polarization states; (e) reconstructed validation image

采用相关系数(CC)来定量评价重构图像和原始图像之间的相似程度,进一步说明了本文方法的有效性。其定义为

$$c = \frac{\sum_{k_x=1}^M \sum_{k_y=1}^N | [f(k_x, k_y) - \overline{f(k_x, k_y)}] [I(k_x, k_y) - \overline{I(k_x, k_y)}] |}{\sqrt{\sum_{k_x=1}^M \sum_{k_y=1}^N [f(k_x, k_y) - \overline{f(k_x, k_y)}]^2} \sqrt{\sum_{k_x=1}^M \sum_{k_y=1}^N [I(k_x, k_y) - \overline{I(k_x, k_y)}]^2}}, \quad (8)$$

式中  $k_x$  和  $k_y$  表示像素的位置,  $f$  和  $I$  表示原始图像和重构图像的振幅分布,  $M$  和  $N$  表示像素总数,  $c$  的最大值为1,且数值越大,两图像相似程度越高。计算得到的图6(e)和图4(c),图5(g)和图4(a)之间的相关系数分别为0.93和0.98,表明重构图像和原始图像相似程度较高。对基本编码和认证过程的数值模拟结果初步表明了本文方法的有效性。

为了进一步说明该认证方法的容错能力和密钥敏感性,考虑认证密钥错误的情况下,系统的认证结果。以二维码图像认证为例,在错误的菲涅耳衍射距离处计算得到的衍射图样强度分布如图7(a)、(b)所示,

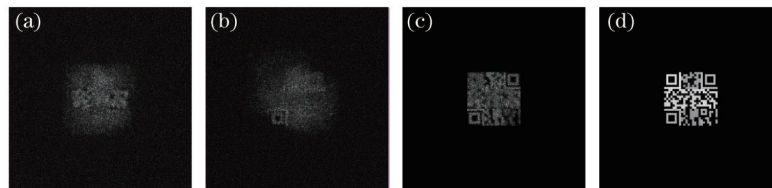


图7 二维码图像的错误认证结果。(a)、(b) 错误菲涅耳衍射距离处的强度分布；(c)菲涅耳衍射距离密钥错误时的重构图像；(d) 正交偏振映射密钥错误时的认证图像

Fig.7 Wrong validation results of QR code images. (a)、(b) Intensity distributions of diffracted patterns in wrong Fresnel diffraction distances; (c) reconstructed image with wrong Fresnel diffraction distance key; (d) validation image with wrong orthogonal polarization mapping key

错误距离分别为 250 mm 和 380 mm,假设偏振映射密钥正确,则重构的认证图像如图 7(c)所示。虽然二维码图像的定位区勉强能被识别,但是核心的数据区被严重污染,因而其编码的信息无法有效恢复。当菲涅耳衍射距离密钥正确,而正交偏振映射密钥错误时,重构得到的错误认证图像如图 7(d)所示。由于其中某一子块信息被错误认证图像的子块替代,导致该二维码信息也无法被有效读出。

数值模拟结果表明所提出的方法充分利用了矢量光束的多参量特性,使光学认证系统同时具备相位模板认证密钥和三维空间正交偏振映射认证密钥,因而安全性较高。另外,在实际应用中,可以根据需求,改变系统的识别阈值,实现对密钥敏感性和系统容错能力的控制和优化。

### 3.2 实验研究

用光学硬件搭建认证系统,如图 8 所示。图 8(a)展示了实验系统的全貌,图 8(b)为系统的核心部分,即矢量光束生成器。实验采用两个相位型硅基液晶(LCOS)SLM,分辨率为 1280 pixel × 1024 pixel,像素间距为 12.3 μm。CCD 分辨率为 1280 pixel × 1024 pixel,像素尺寸 10 μm。照明光源为波长 632.8nm 的 He-Ne 激光器。其中一台计算机同时控制一个 SLM 和 CCD,另一台计算机单独控制另一个 SLM。MP-MSW 相位恢复算法参数与数值模拟参数一致。实验对二值符号图像的认证过程进行了验证,将图 6(a)和(b)分别作为系统锁和认证密钥加载到 SLM 上,通过一个在三维空间位置可调的底座控制 CCD 的位置探测认证图像的子块,结合三维正交偏振复用密钥,可以重构出正确的认证图像。

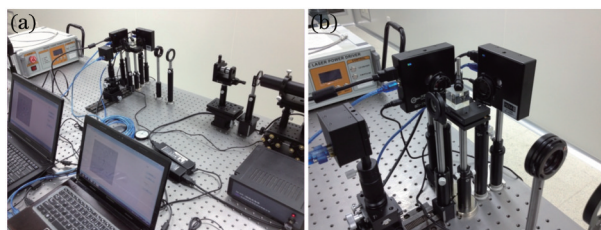


图 8 三维偏振复用光学安全认证实验系统。(a) 系统结构; (b) 核心组件-矢量光束生成器

Fig.8 Experimental system of 3D polarization multiplexing optical validation. (a) System structure; (b) core component-vector beam generator

图 9(a)~(h)分别展示了在一系列菲涅耳衍射距离为 200、260、320、360 mm 处,检偏器透光轴取向正交时探测的强度分布,原始符号的轮廓信息能够被人眼识别。在实际系统设计中,通过设计特定的比较器或采用光学相关器,可以更精确地识别出所有的符号。根据正确的三维偏振映射密钥合成后的正确认证图像如图 10(a)所示,对采集得到的子图像进行缩放和亮度调节后计算重构图像与原始认证图像的相关系数为 0.79。图 10(b)~(d)还展示了当衍射距离密钥错误时采集到的强度分布,可以看出,待认证图像中包含的符号轮廓信息很难被识别出,说明了本文方法有较高的安全性。

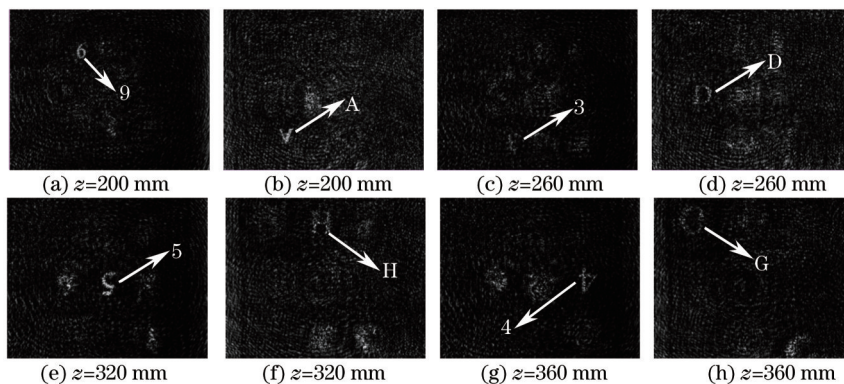


图 9 在不同衍射距离和检偏器透光轴正交取向向下 CCD 采集的强度分布

Fig.9 Captured intensity distribution of images by CCD under various diffraction distances and orthogonal orientations of analyzer

实验结果表明,所提出的光学认证方法不仅具有较高的安全性,而且,由于采用了正交偏振态强度叠加的认证原理,还具有受相干噪声影响小,系统结构稳定,对空间对准精度要求低,光学调试方便等优点。

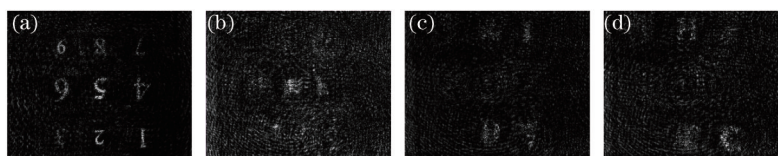


图 10 (a) 重构的认证图像; (b)  $z=230$  mm 处错误认证图像子块; (c)  $z=290$  mm 处错误认证图像子块;  
(d)  $z=330$  mm 处错误认证图像子块

Fig.10 (a) Reconstructed validation image; (b) wrong validation image sub-block at  $z=230$  mm;  
(c) wrong validation image sub-block at  $z=290$  mm; (d) wrong validation image sub-block at  $z=330$  mm

## 4 结 论

提出了一种基于三维空间正交偏振态复用的光学认证方法。该方法基于多平面多信号窗口相位恢复算法优化一束矢量光,实现了在三维空间对强度和偏振态分布的独立控制。数值模拟和光学实验结果表明了该方法具有多重密钥维度,包括相位模板认证密钥、菲涅耳衍射距离密钥和正交偏振映射密钥,有效地提高了系统抵抗暴力攻击的能力。由于预处理算法的引入,能有效防止轮廓信息的泄露。另外,该方法还有易于光学实现,受相干噪声影响小等优点,对光学安全认证技术的实用化具有潜在价值。

## 参 考 文 献

- 1 Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Opt Lett, 1995, 20(7): 767-769.
- 2 Javidi B, Horner J L. Optical pattern recognition for validation and security verification[J]. Opt Eng, 1994, 33(6): 1752-1756.
- 3 Chen W, Javidi B, Chen X. Advances in optical security systems[J]. Adv Opt Photon, 2014, 6(2): 120-155.
- 4 Shen X, Lin C, Zou X, *et al.* Nonlinear optical cryptosystem based on joint Fresnel transform under vector wave illumination [J]. Journal of Optics, 2015, 17(5): 055701.
- 5 Qin W, Peng X. Asymmetric cryptosystem based on phase truncated Fourier transforms[J]. Opt Lett, 2010, 35(2): 118-120.
- 6 Wei Hengzheng, Peng Xiang. Known-plaintext attack on optical cryptosystem based on project-onto-constraint-sets algorithm and a 4f correlator[J]. Acta Optica Sinica, 2008, 28(3): 429-434.  
位恒政, 彭翔. 约束集投影算法和4f相关器的光学密码系统的已知明文攻击[J]. 光学学报, 2008, 28(3): 429-434.
- 7 Peng Xiang, Tang Hongqiao, Tian Jindong. Ciphertext-only attack on double random phase encoding optical encryption system[J]. Acta Physica Sinica, 2007, 56(5): 2629-2636.  
彭翔, 汤红乔, 田劲东. 双随机相位编码光学加密系统的唯密文攻击[J]. 物理学报, 2007, 56(5): 2629-2636.
- 8 Wang Hongjuan, Wang Zhipeng, Zhang Yingying, *et al.* Using QR codes in multi-image optical interference encryption system to reconstruct high quality original information[J]. Acta Optica Sinica, 2014, 34(9): 0907001.  
王红娟, 王志鹏, 张颖颖, 等. 利用QR码在光学干涉多图像加密系统中实现信息高质量恢复[J]. 光学学报, 2014, 34(9): 0907001.
- 9 Liu Zhen, Bai Taotao, Lu Peng. Encrypted holographic watermarking technology with decrypted image superposed no noise [J]. Acta Optica Sinica, 2015, 35(2): 0209002.  
刘真, 白韬韬, 卢鹏. 一种解密图像无背景噪声的加密全息数字水印技术[J]. 光学学报, 2015, 35(2): 0209002.
- 10 Hou Junfeng, Huang Sujuan, Situ Guohai. Nonlinear optical image encryption[J]. Acta Optica Sinica, 2015, 35(8): 0807001.  
侯俊峰, 黄素娟, 司徒国海. 非线性光学图像加密[J]. 光学学报, 2015, 35(8): 0807001.
- 11 Wang Hongjuan, Wang Zhipeng, Hai Tao, *et al.* Lossless binary image reconstruction in diffractive encryption system with redundant data[J]. Chinese J Lasers, 2015, 42(7): 0709002.  
王红娟, 王志鹏, 海涛, 等. 利用冗余数据在衍射加密系统中实现二值图像无损恢复[J]. 中国激光, 2015, 42(7): 0709002.
- 12 Shen Xueju, Liu Xumin, Cai Ning. Nonlinear image encryption system based on JTC and its removing noise and resisting attack properties research[J]. Chinese J Lasers, 2015, 42(7): 0709003.  
沈学举, 刘旭敏, 蔡宁. 非线性JTC光学图像加密系统及其消噪声和抗攻击特性研究[J]. 中国激光, 2015, 42(7): 0709003.
- 13 Volodin B L, Kippelen B, Meerholz K, *et al.* A polymeric optical pattern-recognition system for security verification[J]. Nature, 1996, 383(5): 58-60.
- 14 Weng D, Zhu N, Wang Y, *et al.* Experimental verification of optical image encryption based on interference[J]. Opt Commun, 2015, 330(1): 1-5.



- 2011, 284(10-11): 2485-2487.
- 15 Barrera J F, Agudelo A M, Torroba R. Experimental QR code optical encryption: noise-free data recovering[J]. Opt Lett, 2014, 39(10): 3074-3077.
- 16 Zhang Y, Wang B. Optical image encryption based on interference[J]. Opt Lett, 2008, 33(21): 2443-2445.
- 17 Wang B, Zhang Y. Double images hiding based on optical interference[J]. Opt Commun, 2009, 282(17): 3439-3443.
- 18 Chen W, Chen X, Sheppard C J R. Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution[J]. Journal of Optics, 2012, 14(7): 075402.
- 19 Wang X, Zhao D. Optical image hiding with silhouette removal based on the optical interference principle[J]. Appl Opt, 2012, 51(6): 686-691.
- 20 He W, Peng X, Meng X, *et al.*. Collision in optical image encryption based on interference and a method for avoiding this security leak[J]. Optics & Laser Technology, 2013, 47(1): 31-36.
- 21 Niu C, Wang X, Lü N, *et al.*. An encryption method with multiple encrypted keys based on interference principle[J]. Opt Express, 2010, 18(8): 7827-7834.
- 22 Chen W, Chen X. Security-enhanced interference-based optical image encryption[J]. Opt Commun, 2013, 286(1): 123-129.
- 23 Ying C, Pang H, Fan C, *et al.*. New method for the design of a phase-only computer hologram for multiplane reconstruction [J]. Opt Eng, 2011, 50(5): 055802.

栏目编辑: 张 雁