物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

一种基于双光束干涉和非线性相关的身份认证方法

何江涛　何文奇　廖美华　卢大江　彭翔

Identity authentication based on two-beam interference and nonlinear correlation

He Jiang-Tao　He Wen-Qi　Liao Mei-Hua　Lu Da-Jiang　Peng Xiang

引用信息 Citation: Acta Physica Sinica, 66, 044202 (2017)　DOI: 10.7498/aps.66.044202
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.044202
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I4

一种基于双光束干涉和非线性相关的身份认证方法*

何江涛 何文奇† 廖美华 卢大江 彭翔‡

(深圳大学光电工程学院, 光电子器件与系统教育部/广东省重点实验室, 深圳 518060)

(2016 年 9 月 7 日收到; 2016 年 11 月 28 日收到修改稿)

提出了一种基于双光束干涉结构和非线性相关算法的身份认证方法. 该方法在传统双光束干涉加密结构中引入基于“随机二值振幅分布”的相位恢复技术, 将多幅图像分别编码至对应的稀疏相位分布, 并通过叠加复用技术和非线性相关算法, 实现了多级别的身份认证功能. 其认证过程中不同级别用户所持有的相位密钥是一个稀疏相位分布, 数据量更小, 便于存储和传输. 此外, 认证时的输出图像虽然含有标准参考图像的核心信息却具有视觉上的不可分辨性, 降低了信息泄露的风险. 理论分析和数值仿真结果都证实了该方案的有效性和可行性.

关键词: 光学信息安全, 非线性相关, 身份认证, 相位恢复

PACS: 42.25.Hz, 42.30.Rx, 42.79.Hp **DOI:** 10.7498/aps.66.044202

1 引 言

近二十年来, 光学信息安全技术由于其高速并行的数据处理能力、多维度的设计自由度等固有优势而被广泛研究. 最具代表性的工作是由 Refragier 和 Javidi 在 1995 年提出的基于 $4f$ 光学相关器的双随机相位编码图像加密技术 [1]. 双随机相位编码一直是该领域的研究热点, 研究者们先后在此基础上提出了一系列相关的衍生技术 [2−5]. 此外, 一些基于其他光学结构或原理的新型光学信息安全技术也不断涌现, 涉及的典型技术手段主要有: 双光束干涉 [6]、计算鬼成像 [7]、光子计数 [8]、叠层成像 [9]、压缩感知等 [10]. 其中, 2008 年由首都师范大学 Zhang 和 Wang [6] 提出的基于双光束干涉结构的光学图像加密技术, 由于其工作原理清晰, 系统结构简单及加密算法简易高效而受到研究者们的持续关注. 但后续研究表明, 这个系统存在固有的“ 轮廓复现”问题, 即仅用其中任意一个随机相位掩膜进行衍射成像时, 在输出面即可观察到初始图像的模糊轮廓, 使得系统存在信息泄露的安全隐患. 研究者们针对此问题也提出了一些安全性增强的改进方案, 例如: 随机交换两个相位掩膜上部分对应位置的像素值 [11]、引入 Jigsaw 等非线性变换 [12]、增加随机相位扰动次数 [13,14] 等. 然而, 上述改进方案中, 通常又面临设计复杂、实现困难等新问题, 且部分改进方案并未完全消除影像问题.

其实, 这种基于双光束干涉的加密系统更适合被理解为一种认证系统. 早在 20 世纪 90 年代, Javidi 和 Horner [15] 就提出了基于随机相位编码和非线性联合变换相关的光学认证技术. 近些年来, 陆续报道了一系列利用光学结构和原理的认证/识别技术 [16−19]. 2011 年, Pérez-Cabré 等 [8] 提出了一种基于光子计数的光学认证方法, 该方法利用光子计数手段对双随机相位编码系统的密文进

* 国家自然科学基金 (批准号: 61377017, 61307003)、中德合作项目 (批准号: GZ 760)、深圳大学自然科学基金 (批准号: 2016028) 和深圳市科技计划项目 (批准号: JCYJ20160520164642478) 资助的课题.

† 通信作者. E-mail: he.wenqi@qq.com

‡ 通信作者. E-mail: xpeng@szu.edu.cn

行稀疏化表达, 并将其作为安全认证系统的“锁”固定在系统中, 合法用户通过“密钥”对“锁”进行解密操作, 可得到视觉上不可分辨的伪噪声分布, 但通过计算该分布与标准参考图像的非线性相关值, 便可判断出“密钥”的正确性, 从而达到对用户进行身份认证的目的. 由于认证过程中解密操作所得的输出图像是伪噪声分布, 而不是原始明文本身, 在一定程度上提高了系统的安全性. 随后, Chen 等[20]提出用随机二值振幅掩膜的方式来替代光子计数手段, 以完成对密文的稀疏化表达. 此后, 相继提出了一系列涉及稀疏化表达策略的认证方案[21−26].

鉴于稀疏化表达在光学认证领域中固有的优点, 本文将其应用到最近在本领域颇受关注的双光束干涉结构中, 并结合一种修正的相位恢复算法, 提出了一种基于双光束干涉和非线性相关的新型身份认证方案. 在认证系统设计的过程中, 引入随机二值振幅分布函数作为相位恢复算法中的约束, 得到一系列稀疏相位分布, 并将其按照约定进行叠加复用操作以获得不同级别的相位密钥. 由于该认证方案采用了双光束干涉的双密钥认证结构, 且输出图像为视觉上不可分辨的伪噪声分布, 在一定程度上能够有效地降低相位密钥被伪造的风险. 后文将详细描述所提出认证系统的设计过程和认证过程, 并给出相应的仿真实验结果和分析.

2 认证系统理论分析

2.1 非线性相关算法简介

非线性相关算法是一种用来比较两幅图像之间相关性的算法, 与传统线性相关算法的不同在于: 前者相对于后者具有更高的峰值强度、更大的峰值旁瓣比、更窄的自相关带宽、更好的互相关敏感度及对目标图像位置无限制等优势, 而且前者能有效地判断出两幅视觉上无关联的图像之间的相关性. 自从1989年 Javidi[27]将非线性相关概念引入基于联合变换相关器的图像识别系统以来, 非线性相关算法被广泛用于与稀疏表达相结合的识别/认证系统中. 非线性相关算法的计算过程为: 第一步, 对待测图像 $u(\mu,\nu)$ 进行傅里叶变换, 并用非线性强度参数 k 对所得频谱的振幅部分 $|F_u(\mu,\nu)|$ 进行非线性调制, 相位部分保持不变, 调制后的频谱记为 $|F_u(\mu,\nu)|^k\exp[\mathrm{i}\psi_{F_u}(\mu,\nu)]$; 第二步, 对标准参考图像 $o(\mu,\nu)$ 进行同样的处理, 并对获得的调制频谱取复共轭, 得 $|F_o^*(\mu,\nu)|^k\exp[-\mathrm{i}\psi_{F_o}(\mu,\nu)]$; 第三步, 将上述两个调制后的频谱相乘, 并对其乘积进行傅里叶逆变换即可得到两幅图像的非线性相关分布 $nc(x,y)$, 其数学表达式可写为

$$nc(x,y)=\mathrm{IFT}\{|F_u(\mu,\nu)F_o^*(\mu,\nu)|^k \times\exp[\mathrm{i}(\psi_{F_u}(\mu,\nu)-\psi_{F_o}(\mu,\nu))]\},\quad(1)$$

其中, $\mathrm{IFT}\{*\}$ 表示傅里叶逆变换; k 表示所取的非线性强度值, 取值为 $[0,1]$ 之间的实数, $k=0$ 时, 相当于相位提取, $k=1$ 时, 相当于线性匹配滤波器. 显然, 参数 k 定义了非线性强度, 改变 k 会产生具有不同特性的相关信号, k 值越小, 对应的非线性变换强度越大, 高频成分越突出, 处理器对比较对象的差异更敏感.

非线性相关分布通常用“相关峰”来评估, 其定义为输出分布的最大强度峰值和总能量之比, 反映了输出相关峰的尖锐度与高度, 本文正是采取了此参数来评估所得的非线性相关分布, 从而达到身份认证的目的.

2.2 认证系统设计过程

所提出的身份认证方案以经典的双光束干涉光学结构为基础, 如图1所示. 系统的设计过程如下: 第一步, 选取 M 幅图像 $(O_m(x,y),m=1,2,3,\cdots,M)$, 并将它们全部存储在系统内置的数据库中, 作为认证过程中的标准参考图像; 第二步, 随机选定一个纯相位分布函数 $P(x,y)$, 将其固定在双光束干涉结构的参考臂中作为“相位锁”;

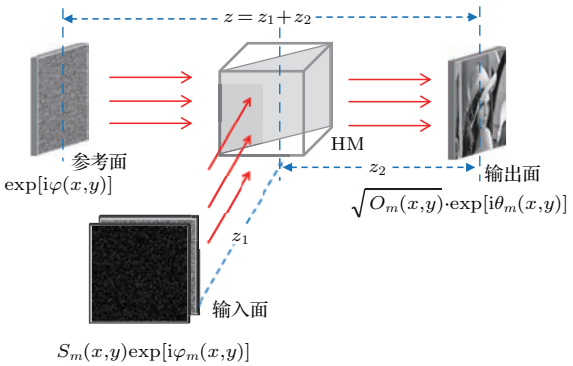


图1 双光束干涉结构示意图

Fig. 1. The schematic diagram of the two-beam interference setup.

第三步, 通过一种修正的迭代相位恢复算法, 将全部M幅标准参考图像$(O_m(x,y), m = 1,2,3,\cdots,M)$分别编码至输入面对应的"稀疏相位分布" $(P_m(x,y), m = 1,2,3,\cdots,M)$中, 再将其按照约定的认证规则进行简单的叠加复用操作以获得不同授权等级的相位密钥$(T_n(x,y), n = 1,2,\cdots,M)$. 接下来, 我们以第$m$幅标准参考图像$O_m(x,y)$为例来详细描述以上过程.

在修正的迭代相位恢复算法中, 标准参考图像、随机二值振幅分布以及"相位锁"分别作为输出面、输入面以及参考面的约束, 并以此估算输入面的"稀疏相位分布", 如图2所示.

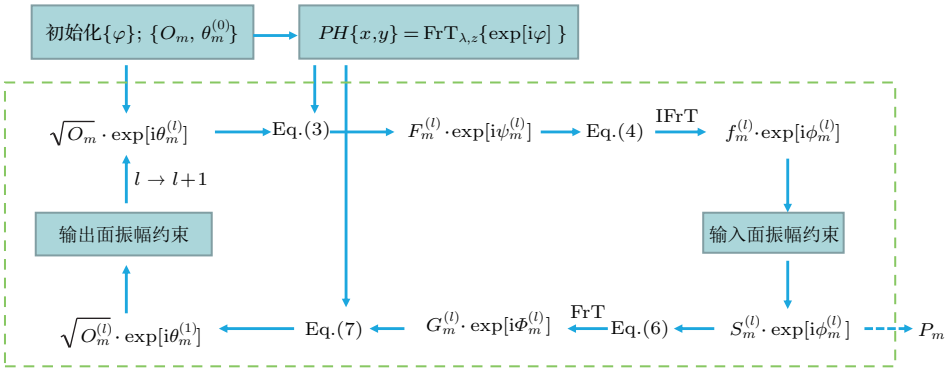


图2 修正的相位恢复算法流程图

Fig. 2. Flowchart of the proposed modified phase retrieval algorithm.

具体迭代过程如下.

1) 由随机数产生器生成一个随机二值振幅分布$S_m(x,y)$, 其有效像素点(即像素值为1的点)占总像素点的百分比为事先设定.

2) 由随机数产生器生成一个均匀分布在区间$[0,2\pi]$上的随机数矩阵$\boldsymbol{\varphi}(x,y)$, 并由此构建出"相位锁"$P(x,y) = \exp[\mathrm{i}\varphi(x,y)]$, 其菲涅耳衍射分布可表示为

$$PH(x,y) = \mathrm{FrT}_{\lambda,z}\{\exp[\mathrm{i}\varphi(x,y)]\}, \tag{2}$$

其中, 算符$\mathrm{FrT}_{\lambda,z}\{*\}$表示入射波长和衍射距离分别为$\lambda$和$z$的菲涅耳衍射.

3) 初始化输出面的相位分布函数$\exp[\mathrm{i}\theta_m^{(0)}(x,y)]$, 其中, $\theta_m^{(0)}(x,y)$在区间$[0,2\pi]$中随机选取. 对其施加"输出面约束"(即标准参考图像$O_m(x,y)$), 构造出的复振幅分布函数$\sqrt{O_m(x,y)}\exp[\mathrm{i}\theta_m^{(0)}(x,y)]$作为输出面的迭代初始值.

4) 假设经过$l-1$次迭代后, 我们获得经过"输出面约束"的复振幅分布函数$\sqrt{O_m(x,y)}\exp[\mathrm{i}\theta_m^{(l)}(x,y)]$, 然后, 利用步骤2)中所得的$PH(x,y)$可计算出一个新的输出面复振幅分布:

$$\begin{aligned} &F_m^{(l)}(x,y)\exp[\mathrm{i}\psi_m^{(l)}(x,y)] \\ &= \sqrt{O_m(x,y)}\exp[\mathrm{i}\theta_m^{(l)}(x,y)] - PH(x,y). \end{aligned} \tag{3}$$

5) 对步骤4)所得的$F_m^{(l)}(x,y)\exp[\mathrm{i}\psi_m^{(l)}(x,y)]$直接进行逆菲涅耳衍射运算, 可得到其对应于输入面的复振幅分布$f_m^{(l)}(x,y)\exp[\mathrm{i}\phi_m^{(l)}(x,y)]$, 其运算过程表示为

$$\begin{aligned} &f_m^{(l)}(x,y)\exp[\mathrm{i}\phi_m^{(l)}(x,y)] \\ &= \mathrm{IFrT}_{\lambda,z}\{F_m^{(l)}(x,y)\exp[\mathrm{i}\psi_m^{(l)}(x,y)]\}, \end{aligned} \tag{4}$$

其中, 算符$\mathrm{IFrT}_{\lambda,z}\{*\}$表示入射波长和衍射距离分别为$\lambda$和$z$的逆菲涅耳衍射.

6) 利用步骤1)给出的随机二值振幅分布$S_m(x,y)$对步骤5)所得的输入面复振幅分布$f_m^{(l)}(x,y)\exp[\mathrm{i}\phi_m^{(l)}(x,y)]$施加"输入面约束", 即得输入面"稀疏相位分布"的一个估计值$S_m(x,y)\exp[\mathrm{i}\phi_m^{(l)}(x,y)]$, 并将其记为$P_m^{(l)}(x,y)$, 且有关系式如下:

$$\begin{aligned} &P_m^{(l)}(x,y) \\ &= \begin{cases} \exp[\mathrm{i}\phi_m^{(l)}(x,y)] & S_m(x,y) = 1, \\ 0 & S_m(x,y) = 0. \end{cases} \end{aligned} \tag{5}$$

7) 计算步骤6)中所得"稀疏相位分布"估计值$P_m^{(l)}(x,y)$的菲涅耳衍射分布

$$\sqrt{G_m^{(l)}(x,y)}\exp[\mathrm{i}\Phi_m^{(l)}(x,y)],$$

并将其结果与"相位锁"在输出面的固定偏置$PH(x,y)$相加, 在输出面即可获得二者的干涉场

分布 $\sqrt{O_m^{(l)}(x,y)}\exp[\mathrm{i}\theta_m^{(l)}(x,y)]$:

$$G_m^{(l)}(x,y)\exp[\mathrm{i}\Phi_m^{(l)}(x,y)] = \mathrm{FrT}_{\lambda,z}\{S_m(x,y)\exp[\mathrm{i}\phi_m^{(l)}(x,y)]\}, \tag{6}$$

$$\sqrt{O_m^{(l)}(x,y)}\exp[\mathrm{i}\theta_m^{(l)}(x,y)] = G_m^{(l)}(x,y)\exp[\mathrm{i}\Phi_m^{(l)}(x,y)] + PH(x,y). \tag{7}$$

8) 利用非线性相关算法比较步骤7) 所得干涉场强度分布 $O_m^{(l)}(x,y)$ 和标准参考图像 $O_m(x,y)$ 的相似程度. 当相关峰值达到预先设定的阈值, 或迭代次数达到预设值时, 迭代算法停止, 此时的"稀疏相位分布"估计值 $P_m^{(l)}(x,y)$ 作为最终的"稀疏相位分布" $P_m(x,y)$. 若不满足迭代终止条件, 则用标准参考图像 $O_m(x,y)$ 对上述输出面干涉场分布函数 $\sqrt{O_m^{(l)}(x,y)}\exp[\mathrm{i}\theta_m^{(l)}(x,y)]$ 施加振幅约束, 获得的复振幅分布函数 $\sqrt{O_m(x,y)}\exp[\mathrm{i}\theta_m^{(l+1)}(x,y)], \theta_m^{(l+1)}(x,y) = \theta_m^{(l)}(x,y)$ 作为输出面的新复振幅估计值, 进行下一轮迭代.

重复步骤4)—8) 直到满足迭代终止条件. 对所有 M 幅标准参考图像分别应用同样的编码方案, 可获得相应的 M 个稀疏纯相位分布 $(P_m(x,y), m = 1,2,\cdots,M)$.

在进一步设计相位密钥之前, 先介绍本认证方案的分级规则: 根据访问系统资源的权限大小, 将授权用户分为 M 级, 最高级别的授权用户必须通过所有 M 幅标准参考图像的认证, 第二级授权用户须通过前 $M-1$ 幅标准参考图像的认证, 最低级别的授权用户, 仅需通过第一幅标准参考图像的认证. 按照上述分级身份认证规则, 我们将以上获得的 M 个"稀疏相位分布" $(P_m(x,y), m = 1,2,\cdots,M)$ 进行叠加, 即可获得对应的 M 个相位密钥 $(T_n(x,y), n = 1,2,\cdots,M)$, 并将其分配给不同授权级别的用户. 对应的数学表达式可表示为

$$T_n = \sum_{m=1}^{n} P_m \quad n \leqslant M. \tag{8}$$

为了更清晰直观地表示该相位密钥叠加复用过程, 复用示意图如图3所示.

在所有 M 幅标准参考图像循环迭代编码过程中, 由于相位锁和系统结构参数是固定的, 因此认证过程中不同级别的授权用户所得的输出图像均含有不同程度的串扰信息. 而在本方案中, 由于随机二值振幅分布的引入, 输出图像为视觉上不可分辨的伪噪声分布, 一定程度的串扰反而可以进一步增强输出图像不可视化的程度, 有利于系统的安全. 对于随机二值振幅分布函数的设计, 需尽可能使各个稀疏相位分布有效值的位置均不相同, 避免叠加复用过程中认证密钥里有效值的重叠, 降低认证过程中的串扰影响. 由(8)式可知, 最高级别用户的相位密钥中的稀疏相位分布函数含有最多的有效像素点, 其相互之间的串扰最为严重. 对此, 一方面, 每个稀疏相位分布函数所含的有效像素点应该相对最多, 才能保证其认证结果能从含有串扰的输出图像中被识别出来; 另一方面, 若每个稀疏相位分布函数所含的有效像素点过多, 又会导致低级别用户的输出图像含有过多的有效认证信息, 从而带来信息泄漏的安全隐患. 因此, 在设计过程中要平衡好二者之间的关系, 即合理选择随机二值振幅分布函数中有效像素点的比例.

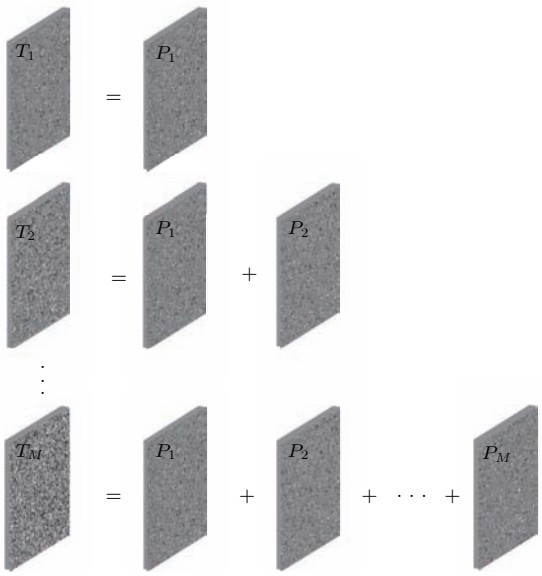


图3 相位密钥复用示意图

Fig. 3. The multiplexing schematic diagram of the phase key.

2.3 用户分级认证过程

本方案涉及的认证过程可利用如图4所示的光电混合系统来完成. 用户进行身份认证时, 认证流程如下: 第一步, 由于系统的相位锁 $P(x,y)$ 已固定在认证系统中 (SLM1), 用户只需将个人的相位密钥 $T_n(x,y)$ 加载至系统的指定位置 (SLM2); 第二步, 用两束相干平面波分别垂直照射于SLM1和SLM2, 再各自经由半透半反镜重新合成一束, 一起

在自由空间传播一段距离后, 在输出面相互干涉, 干涉后形成的强度分布就是用于实现认证的输出图像$U_n(x,y)$, 用电荷耦合器(CCD)等强度探测器就可以直接记录; 第三步, 利用非线性相关算法计算输出图像$U_n(x,y)$和各个对应的标准参考图像$(O_m(x,y), m=1,2,3,\cdots,M)$的非线性相关分布, 如果计算所得的前$n$个非线性相关分布均有明显的非线性相关峰, 则通过身份认证, 可授予该用户第n级别的系统访问权限, 如果前n个非线性相关分布中某一个或多个非线性相关分布没有显著的相关峰, 而是噪声背景分布, 则不能通过身份认证, 拒绝该用户访问第n级系统资源.

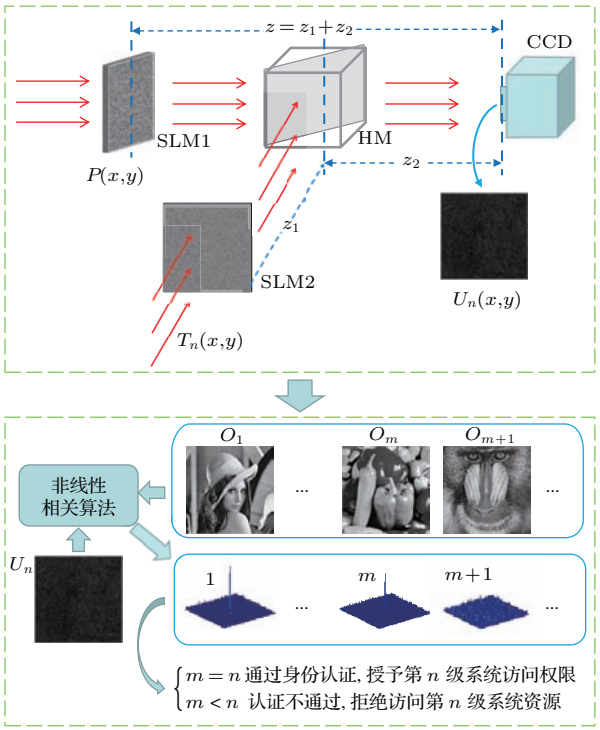


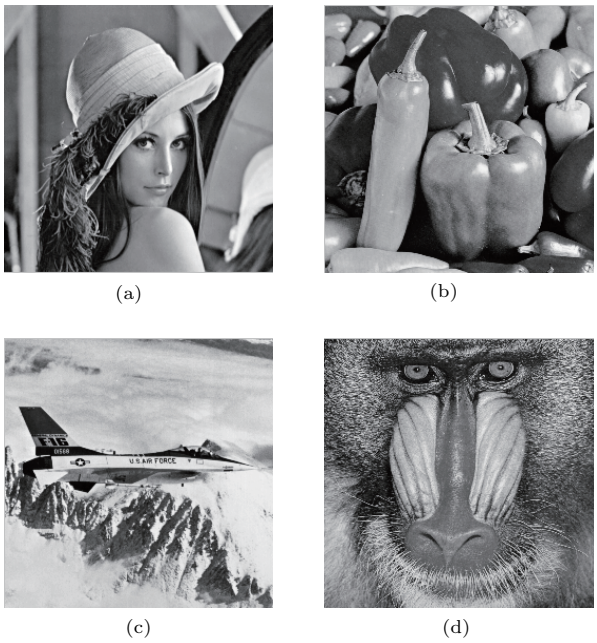
图4 光学认证系统示意图

Fig. 4. The schematic diagram of the proposed optical authentication system.

3 仿真实验与分析

我们在Matlab R2013b的环境下, 对上述方案进行仿真实验认证. 首先给定四幅标准参考图像("Lena", "peppers", "airplane", "baboon"), 如图5所示. 图片大小为256 × 256像素, 像素尺寸为5 mm × 5 mm. 其他系统结构参数为: 照明波长为532 nm, 菲涅耳衍射距离为300 mm.

系统的"相位锁"和作为输入面约束的随机二值振幅分布均由计算机随机生成, 分别如图6(a)和图6(b)—(e)所示. 初始化迭代过程中四个标准参考图像对应的输出面初始相位分布函数、尺寸参数和标准参考图像一致. 其中, 四个随机二值振幅分布有效像素点比例均为15%, 且有效值位置互不重合, 图6(d)的插图显示了其左上角35 × 35像素区域的放大图.



(a) (b) (c) (d)

图5 四幅标准参考图像 (a) Lena; (b) peppers; (c) airplane; (d) baboon

Fig. 5. Four standard reference images: (a) Lena; (b) peppers; (c) airplane; (d) baboon.

根据本文2.2节中提出的修正的相位恢复算法, 对四幅标准参考图像分别进行编码, 最终分别得到与其对应的稀疏相位分布(图7(a)—(d)所示).

对以上四个稀疏相位分布按预定的认证标准((8)式)进行叠加复用, 获得四个不同级别的相位分布函数如图8(a)—(d)所示, 并将其作为"相位密钥"分发给4个不同授权级别的用户, 最高级用户为第四级用户, 依次类推, 最低级用户为第一级用户. 当四个不同授权级别的用户访问该身份认证系统时, 根据2.3节所述的认证流程, 得到四幅相应的输出图像, 如图8(e)—(h)所示. 显然, 这四幅输出图像为视觉上不可分辨的伪噪声分布, 降低了标准参考图像泄漏的风险.

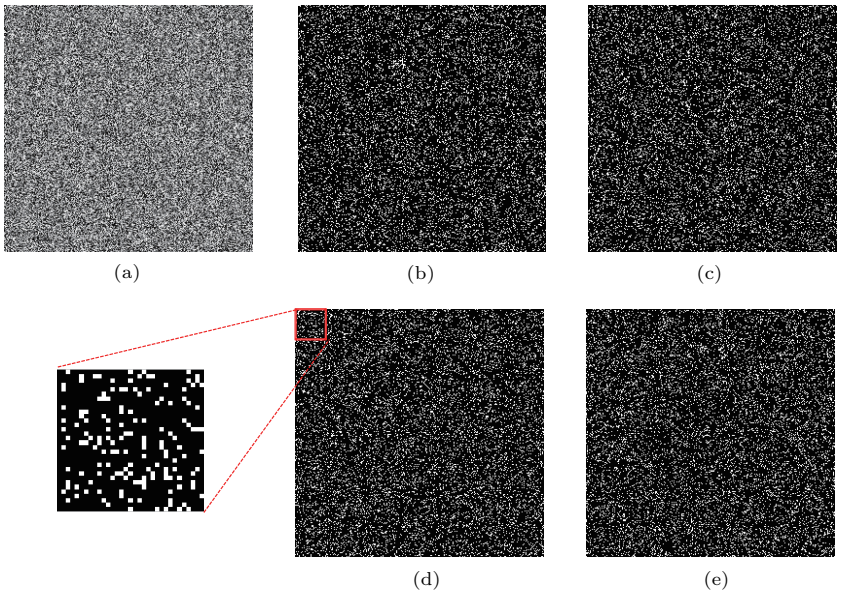


图 6 初始随机分布 (a) 系统锁; (b)—(e) 对应于图 5 (a)—(d) 的随机二值振幅分布; 插图是 (d) 中所标注区域的放大图

Fig. 6. The initial random distribution: (a) System lock; (b)–(e) random binary amplitude distribution corresponding to Fig. 5. (a)–(d); the inset figure is an enlarged version of the marked region in (d).

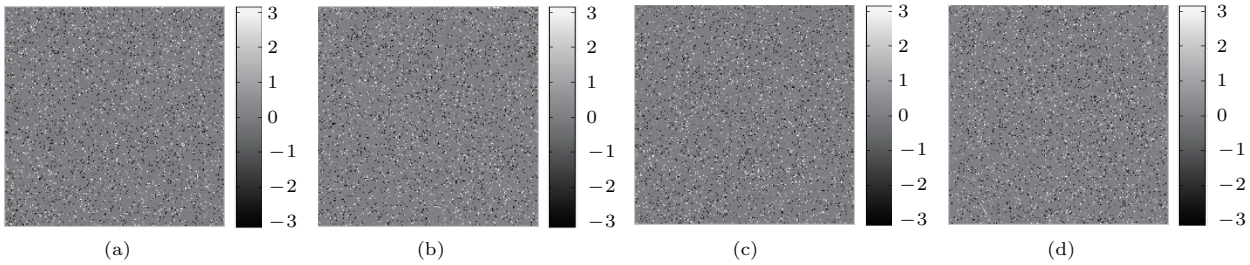


图 7 (a)—(d) 分别对应于图 5 (a)—(d) 编码获得的稀疏纯相位分布 (相角部分)

Fig. 7. The corresponding sparse phase-only distributions (phase angles) generated by encoding Fig. 5. (a)–(d), respectively.

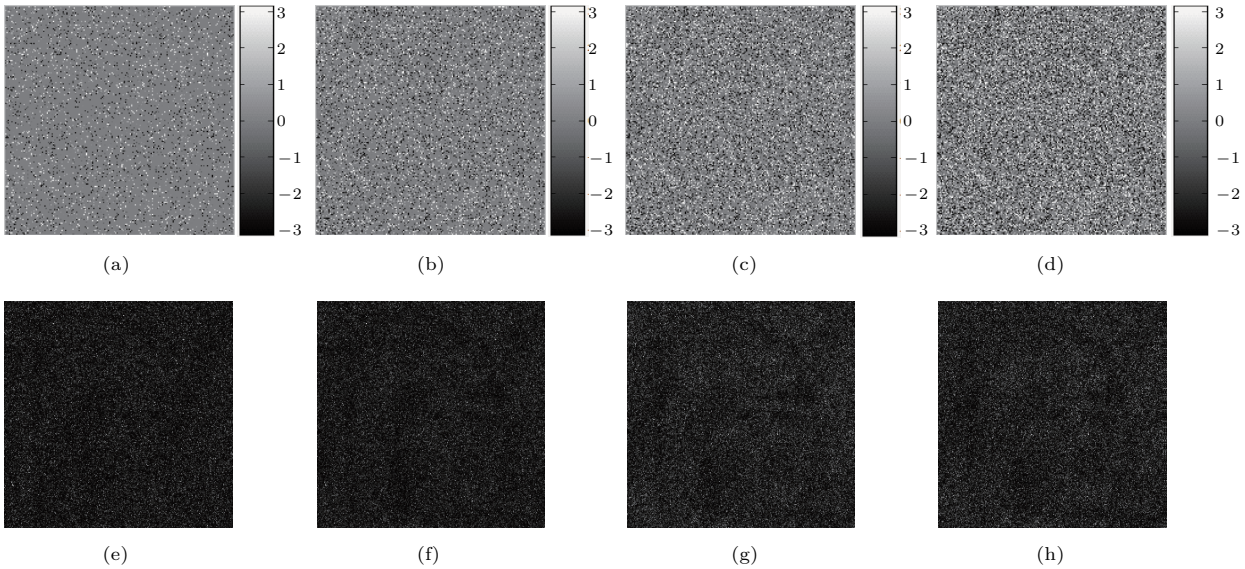


图 8 不同授权级别用户的相位密钥 (a) 第一级; (b) 第二级; (c) 第三级; (d) 第四级; (e)—(h) 分别对应于 (a)—(d) 的输出图像

Fig. 8. The phase keys corresponding to users with different authorization level: (a) First level; (b) second level; (c) third level; (d) fourth level; (e)–(h) the output images corresponding to (a)–(d), respectively.

接下来, 将上述获得的输出图像分别与认证系统内置数据库中的标准参考图像进行非线性相关比较, 其分级认证结果如图9所示, 其中, U_1—U_4分别表示认证密钥T_1—T_4对应的输出图像, O_1—O_4表示内置数据库的标准参考图像. 根据认证标准可知, 如果某来访用户的输出图像(如U_4), 与四幅标准参考图像均可产生显著的非线性相关峰, 则可授予其最高级别的访问权限; 如果来访用户的输出图像(如U_1)仅能与第一幅标准参考图像产生非线性相关峰, 则仅能获得最低级别的访问权限. 高级别用户可以通过所有低级别用户的认证, 但是低级别用户不能通过高级别用户的认证.

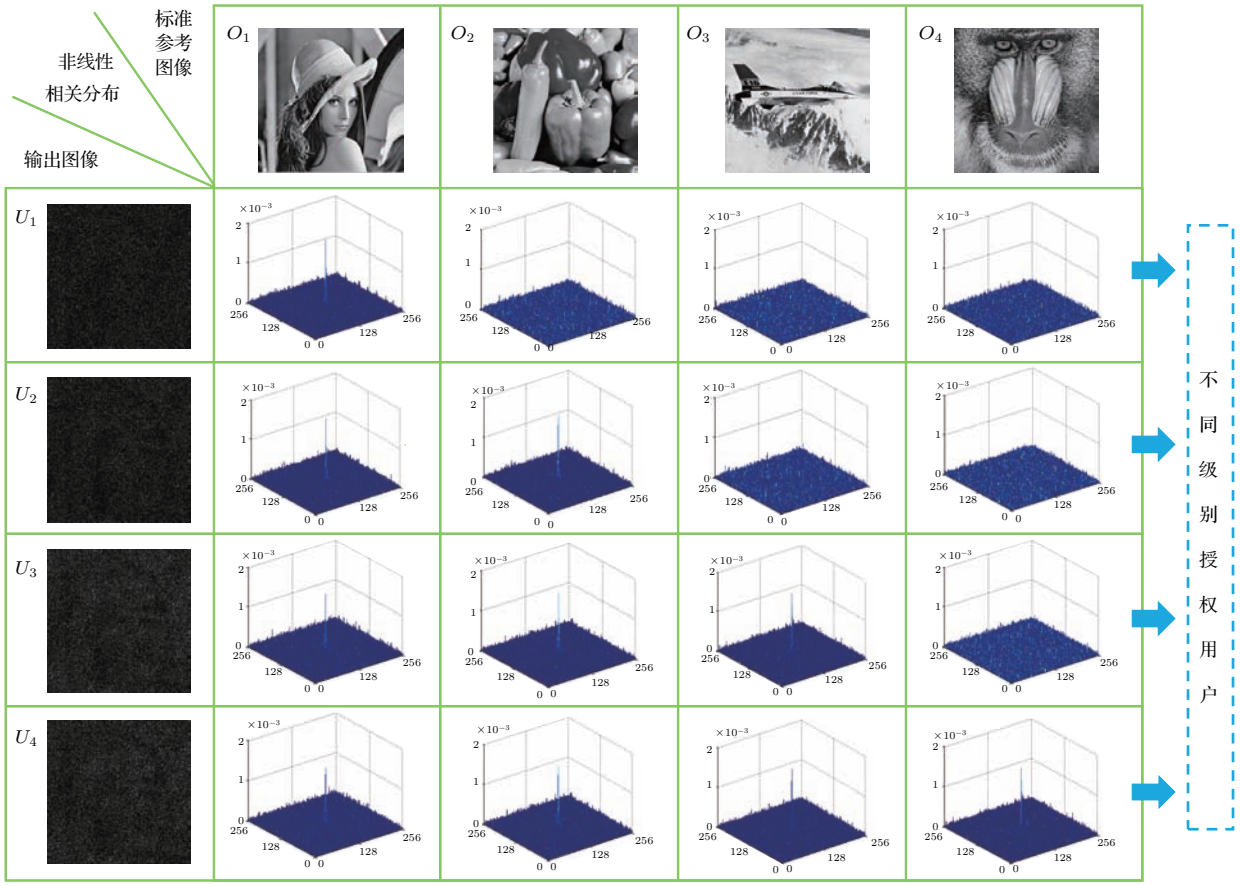


图9 分级认证结果

Fig. 9. Multi-level authentication results.

此外, 由于相位密钥在分发和保存的过程中可能存在数据丢失、噪声污染以及恶意伪造等情况, 因此我们对系统分别进行抗噪声、抗剪切和抗伪造的系统鲁棒性测试, 不失一般性, 这里仅对最低级别授权用户的"相位密钥"进行测试.

首先进行的是抗噪声测试, 图10(a)表示最低级别授权用户的相位密钥被信噪比为10 dB的高斯白噪声污染后的分布图, 图10(b)给出了对应的输出面图像, 其与标准参考图像进行非线性相关运算得到的非线性相关分布如图10(c)所示, 图10(d)给出了认证时非线性相关峰值与"加性高斯白噪声"信噪比的关系曲线. 从图10(d)的内插图可以看出当信噪比为5 dB时, 仍然能得到明显的非线性相关峰, 通过身份认证. 分析表明该系统能够有效地抵抗高斯白噪声.

然后对系统进行抗剪切测试, 图11(a)显示的是剪切比为25%的相位密钥(25%的像素点值置为0, 其他保持不变), 对应的输出图像如图11(b)所示, 图11(c)为相对应的非线性相关分布, 图11(d)则表示了非线性相关峰值与相位密钥剪切比的关系曲线, 并由内插图分布可知, 当相位密钥被剪切掉40%时仍能通过认证. 以上数值仿真结果表明, 该系统对数据丢失具有一定的鲁棒性.

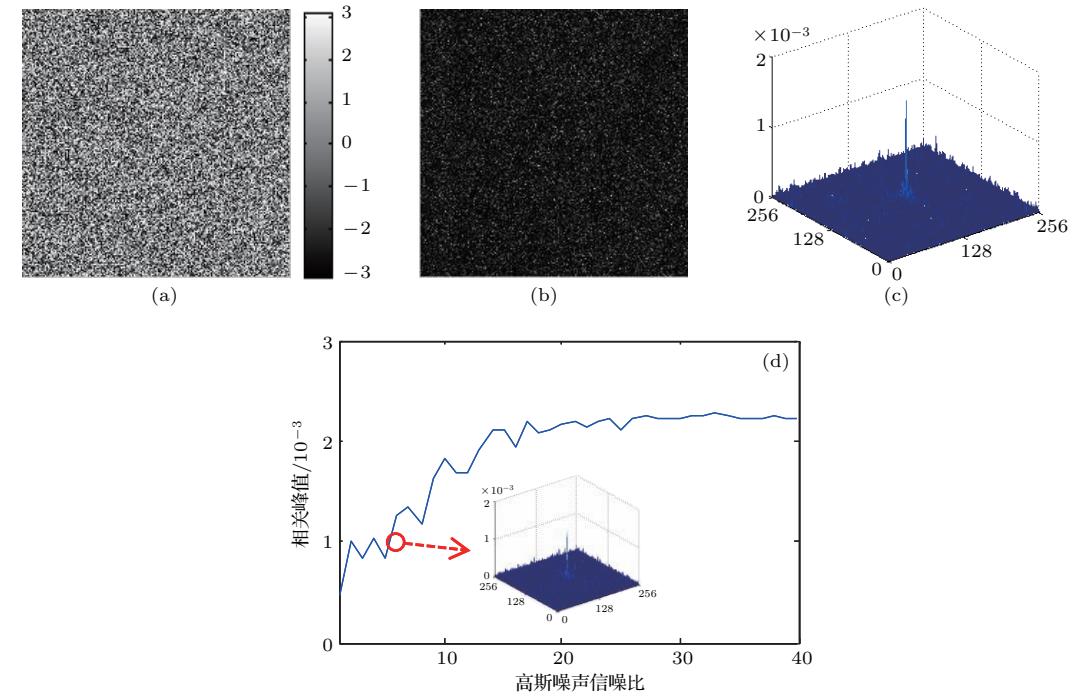


图 10 系统的加性高斯白噪声鲁棒性分析 (a) 信噪比为 10 dB 的相位密钥; (b) 对应的输出图像; (d) 对应的非线性相关分布; (c) 非线性相关峰值与信噪比的关系曲线, 内插图是信噪比为 5 dB 的非线性相关分布

Fig. 10. Robustness analysis of additive white Gaussian noise: (a) Phase key with noise-to-signal ratio of 10 dB; (b) the corresponding output image; (c) the corresponding nonlinear correlation distribution; (d) relationship between nonlinear peak-to-correlation value and signal-to-noise ratio, the inset image is a nonlinear correlation distribution with 5 dB signal-to-noise ratio.

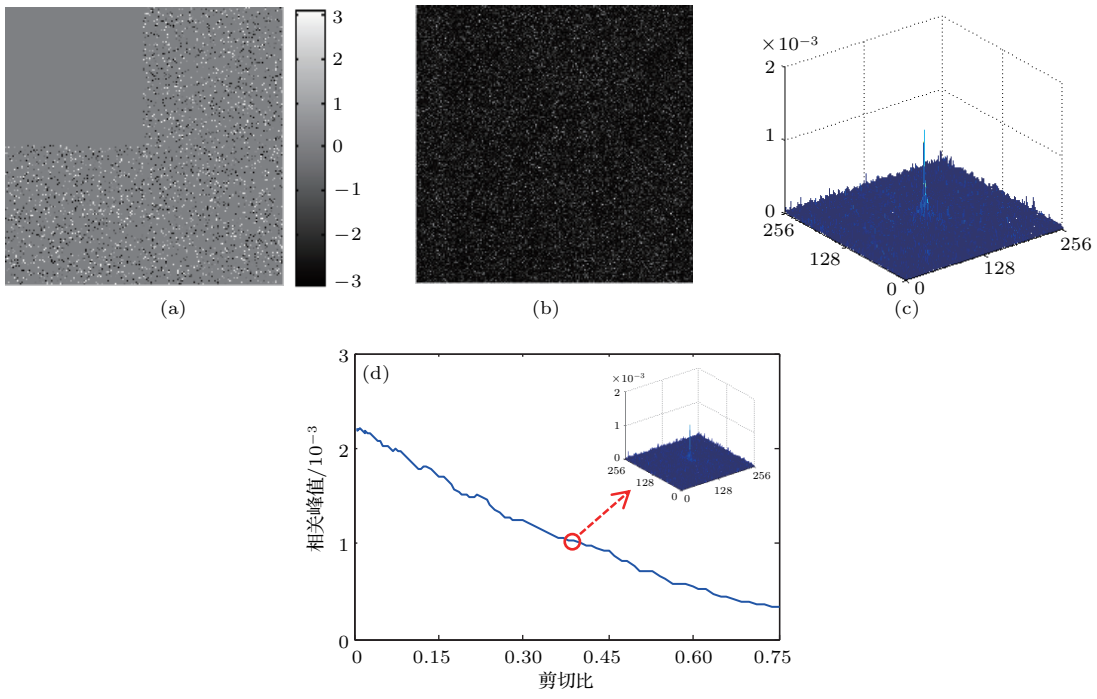


图 11 系统抗剪切鲁棒性分析 (a) 剪切 25% 的相位密钥; (b) 对应的输出图像; (c) 对应的非线性相关分布; (d) 非线性相关峰值与剪切比的关系曲线, 内插图表示密钥剪切 40% 时的非线性相关分布

Fig. 11. Robustness analysis of occlusion: (a) Phase key with 25% occluded; (b) the corresponding output image; (c) the corresponding nonlinear correlation distribution; (d) relationship between nonlinear peak-to-correlation value and occlusion ratio, the inset image is nonlinear correlation distribution when 40% of the phase key is occluded.

最后对系统进行抗伪造测试. 我们选取1000个经过不同的随机二值振幅分布函数调制的随机相位分布函数, 将其视为1000个伪造密钥. 其中, 所选定的1000个随机二值振幅分布函数的有效像素点比例均为15%, 位置随机给定. 图12 (a) 表示的是其中任意一个伪造密钥输入认证系统后所得非线性相关分布, 图12 (b) 给出了所有1000个伪造密钥对应的认证输出的非线性相关峰值. 仿真结果表明, 伪造密钥所得的非线性相关分布没有明显的峰值, 且其相关峰值均比正确密钥所得的相关峰值小约一个数量级. 因此本方案具有一定的抗伪造密钥攻击的能力.

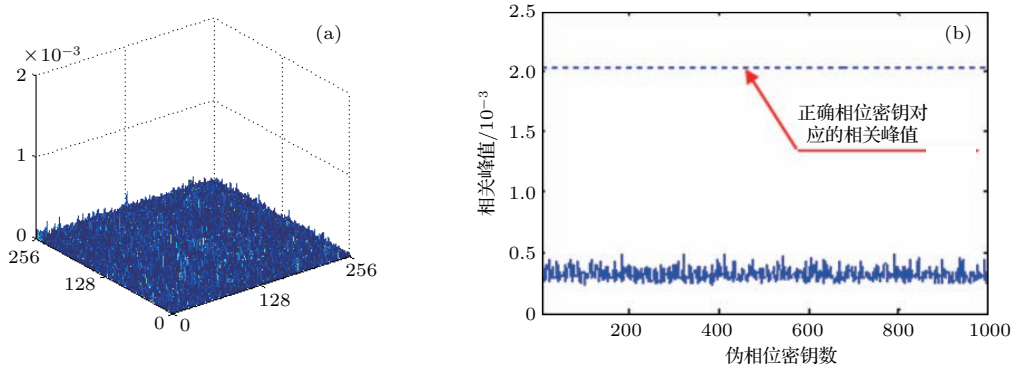


图12 (a) 对应于随机相位密钥的非线性相关分布; (b) 对应于不同随机相位密钥的非线性相关峰值的统计分布

Fig. 12. (a) The nonlinear correlation distribution corresponding to random phase key; (b) the statistical distribution of peak-to-correlation value versus number of fake random phase keys.

此外, 根据2.2节的分析可知, 应该合理选择随机二值振幅分布函数的有效像素点比例, 使得各个级别的授权用户均能顺利通过身份认证. 在此, 我们以最低级别授权用户为例来分析比例选取对身份认证过程的影响, 并选用符号R来表示随机二值振幅分布函数$S_1(x,y)$的有效像素点比例. 当R分别取值为5%, 15%, 25%, 35%时对应的输出图像如图13 (a)—(d) 所示, 将其分别与标准参考图像$O_1(x,y)$进行非线性相关计算, 获得的非线性相关分布如图13 (e)—(h) 所示.

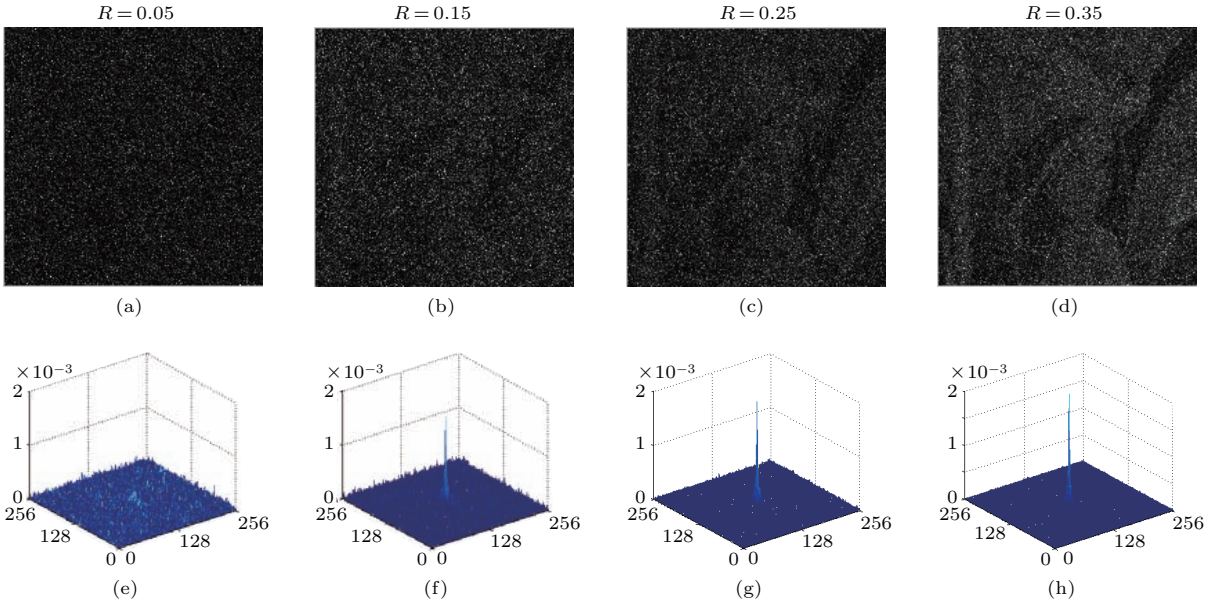


图13 不同稀疏比例的认证结果 (a) $R=0.05$; (b) $R=0.15$; (c) $R=0.25$; (d) $R=0.35$; (e)—(h) 为对应于 (a)—(d) 的非线性相关分布

Fig. 13. Authentication results of different sparse ratios: (a) $R=0.05$; (b) $R=0.15$; (c) $R=0.25$; (d) $R=0.35$; (e)–(h) nonlinear correlation distributions corresponding to (a)–(d).

仿真结果表明, 当R取值为5%时, 认证过程中输出图像是视觉上不可分辨的伪噪声分布, 对应的非线性相关分布为没有显著相关峰的背景噪声分布, 不能通过身份认证. 随着R值逐渐增大, 非线性相关分布峰值越来越好, 但是输出图像的影像效果也越来越明显, 因而会降低系统的安全性. 根据上述测试结果, 在本方案中所选用的R值为0.15.

4 总 结

本文提出了一种基于双光束干涉结构和非线性相关算法的光学身份认证方案. 主要原理是将各个标准参考图像利用所提出的修正的相位恢复算法编码至相对应的稀疏相位分布函数中, 再对其叠加复用获得不同授权等级的相位密钥, 从而达到分级身份认证目的. 该认证方案的主要特点有: 稀疏的相位密钥所含数据量少, 便于携带; 相位信息由于不能被CCD等强度探测器探测到, 具有相对较高的安全性; 认证过程中的输出图像为视觉上不可分辨的伪噪声分布, 进一步增强了系统的安全性. 数值仿真结果表明了该方案的可行性、有效性以及可靠性.

参考文献

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767

[2] Situ G H, Zhang J J 2004 *Opt. Lett.* **29** 1584

[3] Peng X, Zhang P, Wei H Z, Yu B 2006 *Acta Phys. Sin.* **55** 1130 (in Chinese) [彭翔, 张鹏, 位恒政, 于斌 2006 物理学报 **55** 1130]

[4] Liu Z J, Guo Q, Xu L, Ahmad M A, Liu S T 2010 *Opt. Express* **18** 12033

[5] Qin W, Peng X 2010 *Opt. Lett.* **35** 118

[6] Zhang Y, Wang B 2008 *Opt. Lett.* **33** 2443

[7] Clemente P, Duran V, Torres-Company V, Tajahuerce E, Lancis J 2010 *Opt. Lett.* **35** 2391

[8] Pérez-Cabré E, Cho M, Javidi B 2011 *Opt. Lett.* **36** 22

[9] Shi Y S, Li T, Wang Y L, Gao Q K, Zhang S G, Li H F 2013 *Opt. Lett.* **38** 1425

[10] Zhou N R, Zhang A D, Zheng F, Gong L H 2014 *Opt. Laser Technol.* **62** 152

[11] Zhang Y, Wang B, Dong Z L 2009 *J. Opt. A: Pure Appl. Opt.* **11** 125406

[12] Kumar P, Joseph J, Singh K 2011 *Appl. Opt.* **50** 1805

[13] Niu C H, Wang X L, Lü N G, Zhou Z H, Li X Y 2010 *Opt. Express* **18** 7827

[14] Wang X G, Zhao D M 2012 *Appl. Opt.* **51** 686

[15] Javidi B, Horner J L 1994 *Opt. Eng.* **33** 1752

[16] Wang R K, Watson I A, Chatwin C 1996 *Opt. Eng.* **35** 2464

[17] He W Q, Peng X, Meng X F, Liu X L 2013 *Acta. Phys. Sin.* **62** 064205 (in Chinese) [何文奇, 彭翔, 孟祥锋, 刘晓利 2013 物理学报 **62** 064205]

[18] Liu W, Liu Z J, Liu S T 2015 *Appl. Opt.* **54** 1802

[19] Shi X Y, Chen Z Y, Zhao D M, Mao H D, Chen L F 2015 *Appl. Opt.* **54** 3197

[20] Chen W, Chen X D, Stern A, Javidi B 2013 *IEEE Photon. J.* **5** 6900113

[21] Gong Q, Liu X Y, Li G Q, Qin Y 2013 *Appl. Opt.* **52** 7486

[22] Chen W, Chen X D 2014 *Opt. Commun.* **318** 128

[23] Wang X G, Chen W, Chen X D 2015 *IEEE Photon. J.* **7** 7800310

[24] Pan X M, Meng X F, Yang X L, Wang Y R, Peng X, He W Q, Dong G Y, Chen H Y 2015 *Acta. Phys. Sin.* **64** 110701 (in Chinese) [潘雪梅, 孟祥锋, 杨修伦, 王玉荣, 彭翔, 何文奇, 董国艳, 陈红艺 2015 物理学报 **64** 110701]

[25] Wang X G, Chen W, Mei S T, Chen X D 2015 *Sci. Rep.* **5** 15668

[26] Wang Q, Alfalou A, Brosseau C 2016 *Opt. Commun.* **372** 144

[27] Javidi B 1989 *Appl. Opt.* **28** 2358

Identity authentication based on two-beam interference and nonlinear correlation*

He Jiang-Tao He Wen-Qi† Liao Mei-Hua Lu Da-Jiang Peng Xiang‡

(*College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, Shenzhen University, Shenzhen 518060, China*)

(Received 7 September 2016; revised manuscript received 28 November 2016)

Abstract

In this paper, a new approach to identity authentication is proposed, which takes advantage of the two-beam interference setup and the nonlinear correlation technique. According to the traditional two-beam interference encryption/decryption structure, we design a modified iterative phase retrieval algorithm (MIPRA), which takes the random binary amplitudes as the constraints at the input plane to encode different images (standard reference images) into a set of sparse phase distributions. In the MIPRA, a given random phase distribution serves as a system lock, and it is placed at one of the arms of the two-beam interference setup and keeps unchanged in the whole iterative phase retrieval algorithm but equivalently provides a fixed shifting vector toward the output complex amplitude field. While the peak-to-correlation value (between the output intensity and the original image) reaches a presetting threshold value, or the iterative numer of time reaches a presetting maximum value, the MIPRA stops. Here, the phase lock is assumed to be the same for all the users and thus it is placed and fixed in the system, while the calculated phase distributions vary from the MIPRA to different binary constraints, which are related to different users. Meanwhile, we also study an extension version of the proposed method. By using a superposition multiplexing technique and a nonlinear correlation technique, we can realize a function of hierarchical authentication for various kinds of users through a similar but more smart decision strategy. For example, we adopt the MIPRA four times with different constraints (random binary amplitude distribution) to obtain four phase distributions, the sum of them will be regarded as a final phase key and is designed to the user with the highest privilege. He is then able to pass all the authentication process for each standard reference image with his multiplexed phase key, that is to say, there are obvious peaks in all the nonlinear correlation maps between all the output images and the corresponding standard reference images. In a similar way, the user with the lowest privilege can only pass one authentication process. Compared with the previous identity authentication methods in the optical security area, the phase key for each user, no matter what level he belongs to, is easy to be stored and transmitted because its distinguishing feature of sparsity. It is worthwhile to note that the cross-talk between different output images are very low and will has no effect on the authentication decision since we deliberately assemble all the binary distributions, which act as constraints at the input plane in the MIPRA. Moreover, the output results are all noise-like distributions, which makes it nearly impossible for any potential intruders to find any clues of the original standard reference images. However, on the other hand, with the nonlinear correlation technique, we can easily extract enough information from these noise-like output results to authorize any users, usually we can obtain an obvious peak at

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61377017, 61307003), the Sino-German Center for Research Promotion (Grant No. GZ 760), the Natural Science Foundation of Shenzhen University, China (Grant No. 2016028), and the Science and Technology Innovation Commission of Shenzhen, China (Grant No. JCYJ20160520164642478).

† Corresponding author. E-mail: he.wenqi@qq.com

‡ Corresponding author. E-mail: xpeng@szu.edu.cn

the center of the correlation results but there is no peak if we adopt the traditional correlation algorithms. This feature helps reduce the risk of information leakage, thereby providing an additional protection layer. Also, weinvestigate the robustness properties by taking the sparsity ratio, Gaussian noise, and shear/occluded attack into consideration. Some previous tests alsoindicated that our scheme can resist the attack employing incorrect random phase keys. Theoretical analysis and a series simulation results are provided to verify the feasibility and effectiveness of the proposed scheme.

Keywords: optical information security, nonlinear correlation, identify authentication, phase retrieval

PACS: 42.25.Hz, 42.30.Rx, 42.79.Hp **DOI:** 10.7498/aps.66.044202