一种基于双光束干涉的分级身份认证方法*

何文奇[1)†] 彭翔[1)‡] 孟祥锋[2)] 刘晓利[1)]

1) (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)

2) (山东大学信息科学与工程学院光学系, 山东省激光技术与应用重点实验室, 济南 250100)

(2012 年 8 月 24 日 收到; 2012 年 9 月 20 日 收到修改稿)

提出一种基于双光束干涉的分级身份认证方法. 本方法通过同时验证用户的 “口令” 和 “相位钥” 以实现对用户身份的双重安全认证. 它不仅可以判断某个用户是否合法, 还能鉴别出其相应的身份级别, 从而确定并授予其相应的系统访问权限. 认证过程的核心功能组件是一个基于干涉的光学装置, 用户 “口令” 控制的 “相位锁” 和用户携带的 “相位钥” 被分别加载至此装置中的两个空间光调制器 (spatial light modulator, SLM), 两束相干光分别经过这两个 SLMs 的调制后, 在输出面得到一幅干涉图, 它被传送至计算机并与系统数据库中的 “认证图像” 进行匹配, 以完成身份的鉴别. 系统的设计则是一个逆向的迭代求解问题, 本文根据事先给定的某个用户的身份级别 (对应着某个认证图像) 和随机给定的 “相位锁”, 利用一种修正的相位恢复算法确定出其对应的 “相位钥”. 理论分析和仿真实验都证明了此方案是可行而有效的.

关键词: 干涉, 傅里叶光学, 相位恢复, 身份认证

PACS: 42.25.Hz, 42.30.Kq, 42.30.Rx, 42.82.Fv **DOI:** 10.7498/aps.62.064205

1 引 言

近年来, 基于光学信息安全的相关理论与技术受到越来越多国内外研究者们的关注, 其主要优势体现在: 固有的并行数据处理能力, 多维的设计自由度以及较高的鲁棒性. 这门结合了信息光学、通信理论以及计算机科学的交叉学科, 在国际上被认为是一种新一代的信息安全理论与技术. 值得指出的是, 由于受限于目前各种光学元器件的实际精度以及人为操作带来的误差, 相关的研究大多都还处于理论研究和仿真验证的摸索阶段, 但众多研究者们对其未来仍旧充满了信心. 1995 年, 美国学者 Refregier 和 Javidi [1] 首次在国际上提出了一种基于 “双随机相位编码” 的光学图像加密技术, 这一工作一直被认为是光学信息安全领域的奠基性工作. 时至今日, 一系列与之相关的理论与技术已经在世界范围内被广泛地研究并得到长足的发展, 其中具有代表性的工作涵盖了光学安全认证、光学生物特征识别、光学密码编码、光学密码分析以及光学数字水印等诸多方面 [2−16]. 其中 2008 年首都师范大学的 Zhang 和 Wang [17] 提出的基于干涉原理的光学图像加密技术就是一个典型而有趣的衍生工作, 该方法利用解析和推导的方法, 将一幅有意义的明文图像加密成两个纯相位的呈噪声状态分布的掩模, 从而实现了对明文图像的加密功能; 2009 年, Wang 和 Zhang [18] 进一步将此方法拓展至 “双图” 加密的情形, 并通过引入针对相位掩模的置换操作发展出一种安全性能更高的改进方案; 随后, 北京理工大学的 Zhu 等 [19] 利用偏振光的干涉原理, 将一幅有意义的明文图像编码至单个 “偏振可选的衍射光学元器件” 以实现加密功能; 2010 年, 印度理工大学的 Kumar 等 [20] 引入 “收敛的随机照射光” 替换 Zhang 等 [21] 的原始方案中的 “平面入射光”, 从而增强了系统的安全强度; 随后, 新

* 国家自然科学基金 (批准号: 61171073, 61275014, 61201355, 60907005)、中德科学中心中德合作研究项目 (项目号: GZ760)、山东省自然科学基金 (批准号: ZR2011FQ011)、山东省科技计划项目 (批准号: 2011GGH20119)、山东省优秀中青年科学家科研奖励基金项目 (批准号: BS2011DX023)、深圳市科技研发资金项目 (批准号: 0014632063100426032) 和山东大学自主创新项目 (批准号: 2010TB019) 资助的课题.

† 通讯作者. E-mail: hewenqi@outlook.com

‡ 通讯作者. E-mail: xpeng@szu.edu.cn

加坡国立大学的 Tay 等 [21] 将 Zhang 等的原始方案推广至彩色图像加密领域; 2011 年, 印度理工大学的 Kumar 等 [22] 和北京理工大学的 Weng 等 [23] 分别从现实的光学实验的角度验证了基于干涉原理的图像加密方案的可行性; 随后, 哈尔滨工业大学的刘树田课题组提出了一种基于迈克耳孙干涉仪的 "类序列密码" 的图像加密方案 [24]; 2012 年, 浙江大学的赵道木课题组提出了一种基于干涉原理的图像隐藏技术, 并通过增加一个随机掩模密钥有效地降低了其存在的安全隐患 [25].

实际上, 从密码学的角度来看, 我们认为上述基于干涉原理的光学图像加密技术更像是一个认证技术或者说更容易应用于身份认证领域. 在此理解的基础上, 我们利用 Zhang 和 Wang[17] 提出的原始方案中的双光束干涉结构, 再结合修正的相位恢复算法, 提出一种能够实现多级身份认证的双重安全强度的方案. 同时, 我们提供了一系列仿真实验及其结果以证明此方案的可行性和有效性.

2 方案原理

本节将着重从 "用户认证过程" 和 "系统设计过程" 这两个方面对本方案的工作原理进行阐述. 由于前者相对于后者更直观明了, 下边将首先介绍用户认证的过程, 再介绍系统设计的过程.

2.1 用户认证过程

当用户试图访问系统资源时, 首先需要通过身份认证, 其具体步骤如下 (如图 1): 第 1 步, 用户输入其私有的 "口令", 确定后, 系统自动将此口令与系统内置的 "口令数据库" 进行匹配, 匹配成功后, 系统会将与之对应的一个纯相位掩模 (phase-only mask, POM), 后面也称为 "相位锁", 加载到用于进行认证的双光束干涉装置中的 SLM_1 上 (如图 1 中第 3 步所示); 第 2 步, 用户将自身携带的另一个纯相位掩模, 后面也称为 "相位钥", 通过系统外部设备加载到用于进行认证的双光束干涉装置中的 SLM_2 上; 第 3 步, 两束相干的平面波平行照射 SLM_1 和 SLM_2, 它们分别经过相位锁和相位钥的 "调制" 后, 再一起通过一个 "半反半透" 的光学棱镜 (half mirror, HM), 最后在输出面处发生干涉并得到一幅干涉图, 其强度 (输出图像) 被一个电荷耦合器件 (charge coupled device, CCD) 记录并存储下来, 其具体数学表述为

$$\begin{aligned}&\exp(\mathrm{j}\psi_1(x,y))*h(x,y,l)\\&+\exp(\mathrm{j}\psi_\mathrm{k}(x,y))*h(x,y,l)\\=&O(x,y)\cdot\exp(\mathrm{j}\varphi_O(x,y)),\end{aligned}\tag{1}$$

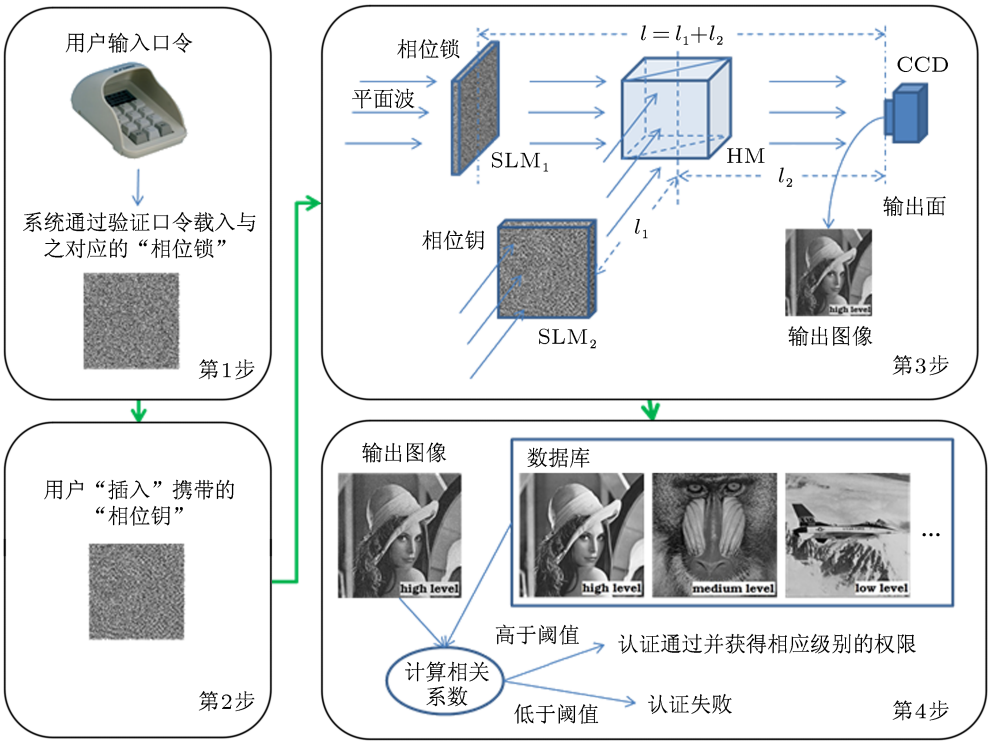

图 1 用户认证的流程图

其中, 符号 "*" 代表卷积运算, $h(x,y,l)$ 表示距离为 l 的菲涅耳衍射的脉冲响应, $\psi_{\mathrm{l}}(x,y)$ 和 $\psi_{\mathrm{k}}(x,y)$ 分别是相位锁和相位钥的分布函数, $O(x,y)$ 是干涉图的振幅分布函数, 而 $\varphi_O(x,y)$ 是输出面处的相位分布函数; 第 4 步, 将第 3 步记录的输出图像与系统内置数据库中的标准 "认证图像" 进行逐一比对, 通过分别计算它们之间的相关系数 (correlation coefficient, CC) 实现对用户身份的最终鉴别和认证, 如果输出图像与数据库中的某个标准认证图像之间的相关系数高于事先设定的阈值 (譬如 0.95), 系统就视为认证通过, 并授予该用户相应级别的系统访问权限, 如果输出图像与数据库中每个标准认证图像之间的相关系数都低于阈值, 系统就视为认证失败, 表示该用户不是授权的合法用户, 并拒绝其访问系统资源.

为了更直观地描述本方法的分级身份认证功能, 我们给出如图 2 所示的一个功能图: 不同级别的用户被分在不同的用户组 (A 组, B 组, C 组, ……, K 组), 每个用户组 (级别组) 中都有数量不等的若干用户 (譬如, B 组中有 m 个用户, C 组中有 n 个用户), 且每个用户都有一个不同的 "口令" 和一个不同的 "相位钥". 特别需要指出的是: 同一个用户组中的所有用户, 在访问系统进行认证时, 所得到的输出图像都能与系统内置数据库中的同一个标准 "认证图像" 成功匹配, 从而获得相同级别的系统访问权限.

2.2 系统设计过程

在进行具体设计之前, 需要根据实际情况对用户进行分级: 将所有合法用户分成若干个不同级别的用户组 (每个用户组里可以有数量不等的用户), 同时确定与每个用户组相对应的标准 "认证图像", 并将它们存储在系统内置的数据库中. 譬如, 图 2 中右侧的三幅标准认证图像分别对应三个不同级别的用户组. 接下来, 我们拟以图 2 中提到的 "C 组" 为例, 介绍系统设计的大致流程, 如图 3 所示: 第 1 步, 随机选择 n 个口令 (口令 C_1, 口令 C_2, ⋯, 口令 C_n); 第 2 步, 再随机生成 n 个相位锁 (相位锁 C_1, 相位锁 C_2, ⋯, 相位锁 C_n) 并将其与第 1 步中的 n 个口令一一关联对应起来, 然后将它们全部一起存入系统数据库中; 第 3 步, 根据 C 组的级别, 调用与其对应的标准认证图像 ("Airplane") 和第 2 步随机生成的 n 个不同的相位锁, 利用修正的相位恢复算法, 分别逐一确定出 n 个相对应的相位钥 (相位钥 C_1, 相位钥 C_2,⋯, 相位钥 C_n,), 从而完成对 C 组的认证设计. 此时, 将这 n 个 "口令" 和 n 个 "相位钥" 分别配发给 C 组中的 n 个用户, 他们便可以利用图 1 所示的步骤进行身份认证并获取相应的系统访问权限.

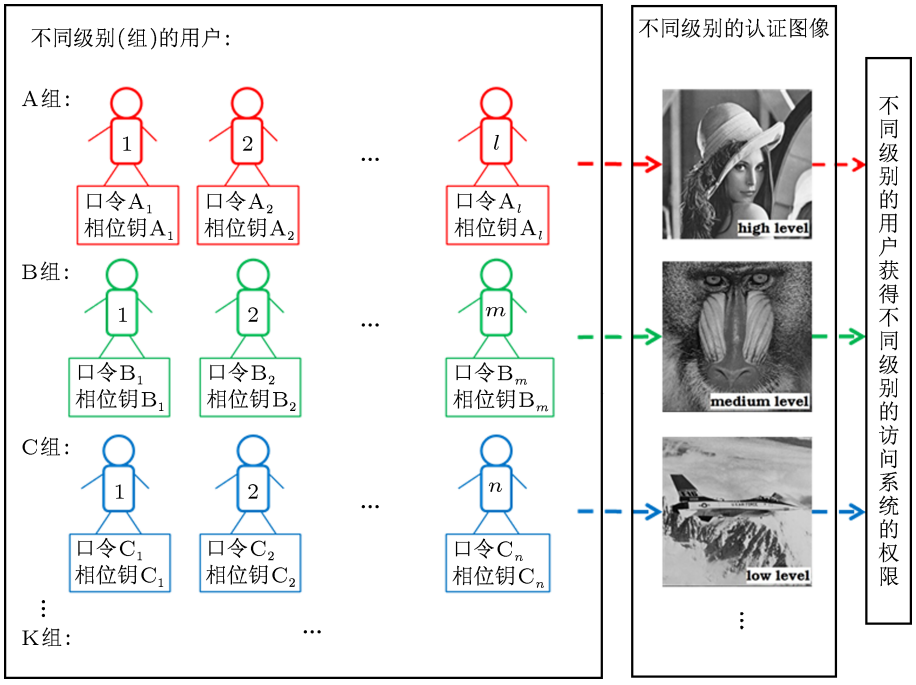

图 2 分级身份认证功能图

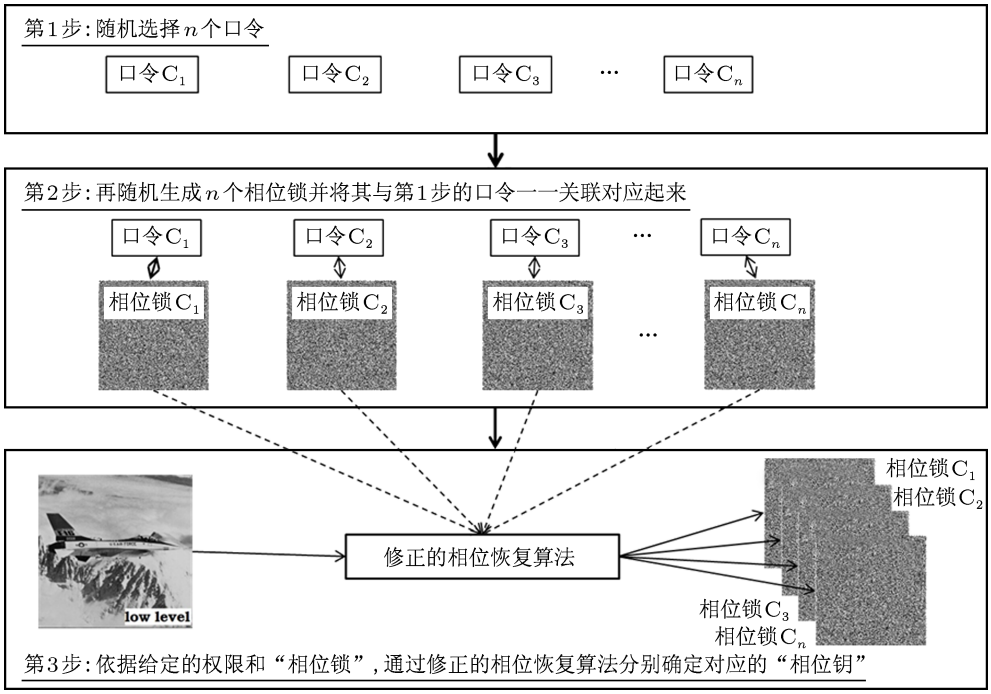

图 3 系统设计流程图 (以图 2 中的 C 组为例)

上述系统设计过程中, 需要进一步描述的关键技术是第 3 步中涉及的“修正的相位恢复技术”. 相位恢复技术是一常见的解决“逆向问题”的迭代算法, 其通常可以被描述为: 已知输出面约束 (目标图像) 和输入面约束 (输入面的振幅分布), 通过循环迭代的算法, 估算出输入面相位分布的过程. 本方案涉及的“修正的相位恢复”技术中, 引入了一个固定的平移矢量, 其算法问题可以描述为: 已知输出面约束 (某个标准的认证图像), 输入面约束 (单位矩阵或者说“去除振幅”操作) 以及一个固定的平移矢量 (相位锁的菲涅耳衍射谱), 需要通过迭代的算法, 估算出输入面的相位分布 (相位钥). 下边将详细描述利用修正的相位恢复算法估算相位钥的过程.

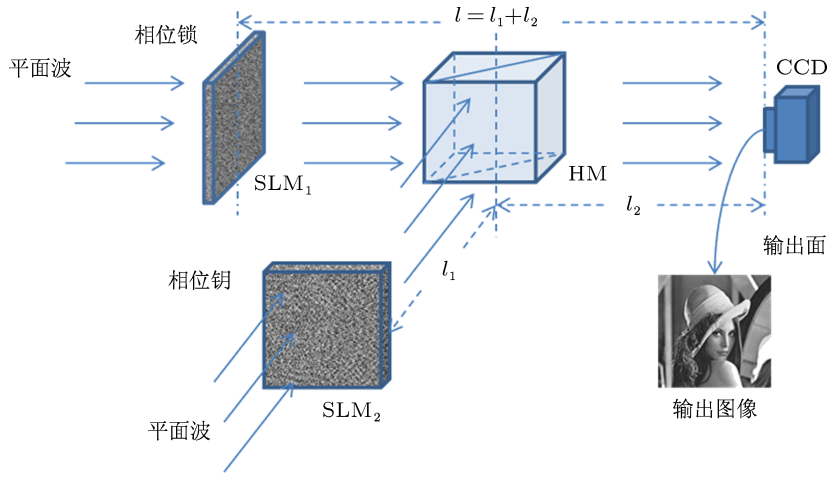

图 4 双光束干涉结构示意图

图 4 是一个双光束干涉结构示意图 (也即图 1 中第 3 步所示), 也是此修正相位恢复技术的作用载体. 我们的目的就是利用给定的相位锁 (加载在 SLM_1 上) 和期望出现在输出面的某个标准认证图像, 确定出相位钥的估算值. 而当用户使用此估算的相位钥和正确的相位锁 (通过口令控制) 在进行

认证时, 所得到的输出图像与标准认证图像的相关系数高于阈值, 通过认证并获得相应的访问权限. 为了便于描述整个算法过程, 将 (1) 式写为

$$L(x,y)+K(x,y)\exp(\mathrm{j}\varphi_K(x,y)) =O(x,y)\cdot\exp(\mathrm{j}\varphi_O(x,y)), \tag{2}$$

其中 $L(x,y)$ 和 $K(x,y)\exp(\mathrm{j}\varphi_K(x,y))$ 分别是相位锁 $\exp(\mathrm{j}\psi_\mathrm{l}(x,y))$ 和相位钥 $\exp(\mathrm{j}\psi_\mathrm{k}(x,y))$ 的菲涅耳衍射分布, $O(x,y)\cdot\exp(\mathrm{j}\varphi_O(x,y))$ 是输出面处的干涉复分布场. 对 (2) 式移项后再两边同时进行一次傅里叶变换并经过一个简单的推导可以得到:

$$\exp(\mathrm{j}\psi_\mathrm{k}(x,y)) =F^{-1}\left\{\frac{F\{O(x,y)\cdot\exp(\mathrm{j}\phi_O(x,y))-L(x,y)\}}{F\{h(x,y,l)\}}\right\}. \tag{3}$$

其中算符 $F\{\cdot\}$ 和 $F^{-1}\{\cdot\}$ 分别表示傅里叶变换和逆傅里叶变换. 通过对 (3) 式的分析, 可以将拟解决的问题重新表述为: 已知输入面为纯相位分布 (SLM_2 处, 振幅约束为单位矩阵), 且给定目标图像 $O(x,y)$(输出面处, 振幅约束为某个标准认证图像) 和一个固定的平移矢量 $L(x,y)$ (相位锁在输出面处的菲涅耳衍射谱), 求输入面的相位分布 (即相位钥 $\exp(\mathrm{j}\psi_\mathrm{k}(x,y))$), 这可看作是一个修正的 “双强度约束” 的相位恢复问题. 具体而言, 我们试图通过这个迭代算法, 确定相位钥的估算值, 使得其输出的图像与给定的标准认证图像之间的相关系数足够高 (譬如高于 0.95). 这里, 相关系数的定义如下:

$$CC=\left[\sum\sum(O(x,y)-\bar{O}(x,y))(O'(x,y)-\bar{O}'(x,y))\right] \times\left[\sqrt{\sum\sum(O(x,y)-\bar{O}(x,y))^2}\right. \times\left.\sqrt{\sum\sum(O'(x,y)-\bar{O}'(x,y))^2}\right]^{-1}, \tag{4}$$

其中 $\bar{O}(x,y)$ 和 $\bar{O}'(x,y)$ 分别表示给定的标准认证图像和实际的输出图像中像素值的平均值. 假设此迭代算法进行到了第 m 次循环, 接下来的迭代过程可以表示为 (为方便起见, 忽略了坐标系标注)

$$\left|K^{(m)}\right|\exp(\mathrm{j}\varphi_K^{(m)}) =O\exp(\mathrm{j}\varphi_O^{(m)})-L, \tag{5a}$$

$$\exp(\mathrm{j}\psi_\mathrm{k}^{(m)}) =\mathrm{phase}\left\{F^{-1}\left\{\frac{F\{|K^{(m)}|\exp(\mathrm{j}\varphi_K^{(m)})\}}{F\{h(x,y,l)\}}\right\}\right\}, \tag{5b}$$

$$\left|K^{(m+1)}\right|\exp(\mathrm{j}\varphi_K^{(m+1)}) =\exp(\mathrm{j}\psi_\mathrm{k}^{(m)})*h(x,y,l), \tag{5c}$$

$$\left|O^{(m+1)}\right|\exp(\mathrm{j}\varphi_O^{(m+1)}) =\left|K^{(m+1)}\right|\exp(\mathrm{j}\varphi_K^{(m+1)})+L, \tag{5d}$$

其中上标 “(m)” 表示迭代次数, 算符 $\mathrm{phase}\{\cdot\}$ 表示取相位操作. 图 5 描述了整个迭代过程的流程, 其亦可概括成下面的几个步骤: 1) 利用初始化的参数 (相位锁 ψ_l, 给定的标准认证图像 O 以及其伴随的初始相位项 φ_O), 根据 (5a) 式计算出相位钥在输出面处的菲涅耳衍射复分布场; 2) 根据 (5b) 式, 利用 1) 中的结果, 计算得到第一个相位钥的估计值, $\exp(\mathrm{j}\psi_\mathrm{k}^{(1)})$; 3) 根据 (5c) 式, 再一次计算出 2) 中所得相位钥估计值的菲涅耳衍射复分布场, $\left|K^{(2)}\right|\exp(\mathrm{j}\varphi_K^{(2)})$; 4) 根据 (5d) 式, 引入固定的平移矢量 L, 构造出输出面处新的复分布 $\left|O^{(2)}\right|\exp(\mathrm{j}\varphi_O^{(2)})$; 5) 计算 4) 中所得输出面处的振幅, $\left|O^{(2)}\right|$ 和给定的标准认证图像 O 之间的相关系数, 如果其值不小于

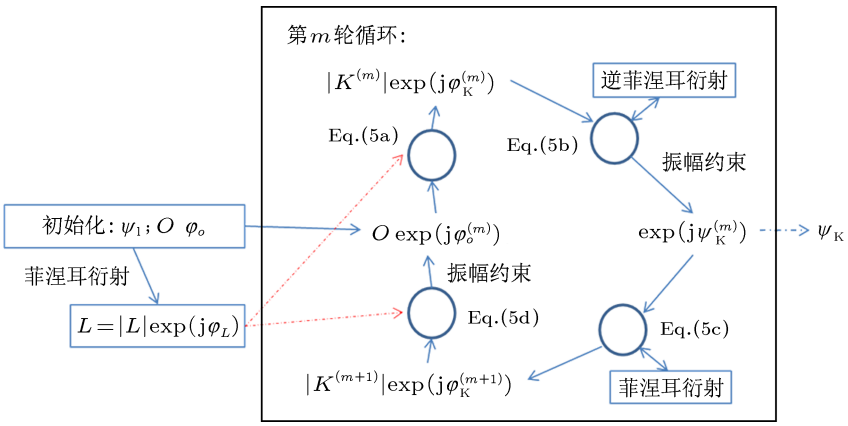

图 5 修正的相位恢复算法流程图

给定的阈值, 譬如 0.95, 我们就停止该迭代算法, 如果小于给定的阈值 0.95, 我们需要将 $\left|O^{(2)}\right|$ 替换成 O, 然后重复上述的步骤 1)—5), 直到输出面图像 (即输出面处复分布的振幅部分) 与给定的标准认证图像之间的相关系数大于事先设定的阈值. 迭代停止, 此时的相位钥估计值就是最终确定的相位钥.

3 仿真实验及结果

我们在 Matlab R2010a 软件仿真平台上, 验证了上述基于双光束干涉的多级身份认证方案的可行性.

首先, 假设某系统需要授权一个合法的 “高级用户”, 其具体操作过程为: 该用户选择一个口令, 系统则同时随机生成一个相位锁并将其与该口令关联起来, 然后一起存入系统. 调出系统数据库中对应高级别用户的标准认证图像 (Lena), 结合修正的相位恢复算法 (这里, 设定迭代停止条件为: 输出图像与标准认证图像的相关系数不低于 0.97), 确定出相位钥. 仿真结果如图 6 和图 7.

其次, 假设系统需要继续授权 2 个 “中级别用户” 和 3 个 “低级别用户”. 经过类似上述的操作步骤, 得到的结果如图 8, 其具体的相关数据如表 1.

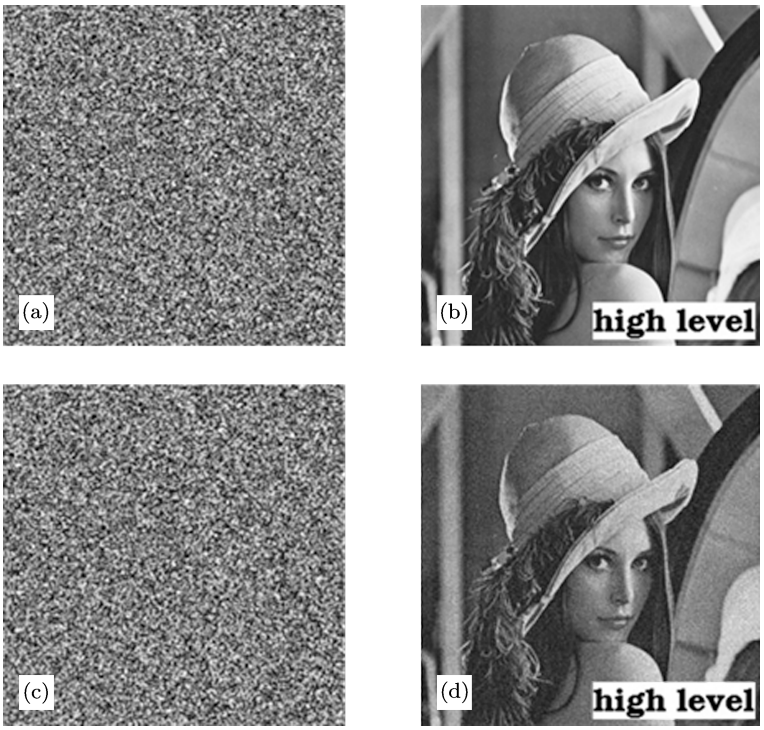

图 6 系统授权一个高级别用户的相关仿真结果 (a) 随机生成的相位锁; (b) 对应高级别的标准认证图像; (c) 利用修正相位恢复算法确定的相位钥; (d) 实际认证过程中得到的输出图像

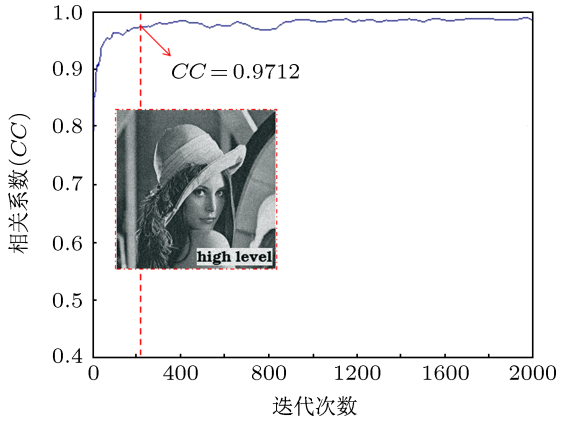

图 7 利用修正相位恢复算法确定相位钥: 迭代至 217 次时, 相关系数首次高于阈值 0.97

根据上述数据, 值得注意的是: 同一个相位钥, 与不同的相位锁都可以得到类似的输出图像 (因为相位钥中包含了认证图像中的绝多数信息), 但只有与原配的相位锁才能得到足够接近相应标准认证图像的输出图像 (具体数据见表 1). 因此, 在实际认证过程中, 这并不影响多级身份认证功能的实现, 因为只有当用户同时具备正确的相位锁和相位钥, 才能认证通过. 同时需要指出的是, 尽管本方法所得的认证结果中存在一定的噪声 (输出图像与标准认证图像之间存在细微的误差), 但是如前所述, 我们可以通过设定一个合理的阈值来消除这种影响, 而不会影响认证结果. 当采用实际光学元器件来实

现此方案时, 元器件的精度 (SLM, 透镜等) 以及人为操作都会引入不同的误差, 但我们认为, 优先采用二值的简单图像作为标准认证图像会大幅度地降低误差带来的影响, 同时采取设定合理阈值等技巧也可以有效地规避误差带来的不利影响. 最后值得说明的是: 本方法并不局限于上述仿真实验中的三个级别六个用户的情形, 完全可以根据实际情况拓展至更多级别更多用户的情形.

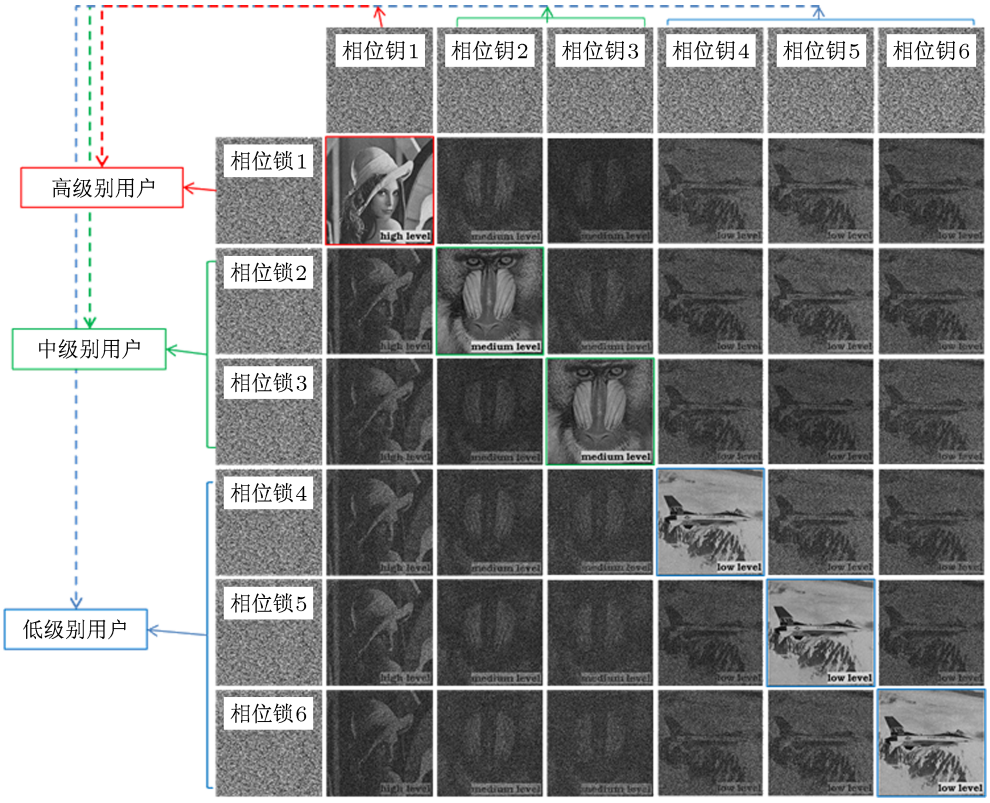

图 8 不同级别的用户在实际认证过程中得到的输出图像

表 1 不同相位钥和相位锁得到的输出图像与相应标准认证图像之间的相关系数

	相位钥 1	相位钥 2	相位钥 3	相位钥 4	相位钥 5	相位钥 6
相位锁 1	0.9712	0.2865	0.1211	0.2185	0.2124	0.3025
相位锁 2	0.3121	0.9790	0.2260	0.3160	0.2412	0.2145
相位锁 3	0.2856	0.3221	0.9708	0.2581	0.1854	0.2856
相位锁 4	0.2865	0.2150	0.1865	0.9765	0.2652	0.3125
相位锁 5	0.1353	0.3231	0.2121	0.1985	0.9731	0.2652
相位锁 6	0.3324	0.2112	0.3250	0.2895	0.2568	0.9715

4 结 论

提出一种基于双光束干涉的多级身份认证方案. 本方案以双光束干涉的光学结构为核心单元, 结合使用修正的相位恢复技术, 从理论上论证了对用户进行分级身份认证的可行性并给出了仿真实验的结果. 相比于一般的认证方法, 此方法的主要优点在于: 不仅可以鉴别某个用户是否合法, 还可以判断出其身份级别, 从而实现对不同用户进行分级访问的控制, 而且此认证过程是一个双重安全强度的认证, 只有当用户同时拥有相位锁 (由用户口令控制) 和相位钥时, 才能通过认证.

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Situ G H, Zhang J J 2005 *Opt. Lett.* **30** 1306
[3] Situ G H, Zhang J J 2004 *Opt. Lett.* **29** 1584
[4] Peng X, Wei H Z, Zhang P 2006 *Opt. Lett.* **31** 3579
[5] Lin Q Q, Wang F Q, Mi J L, Liang R S, Liu S H 2007 *Acta Phys. Sin.* **56** 5796 (in Chinese) [林青群, 王发强, 米景隆, 梁瑞生, 刘颂豪 2007 物理学报 **56** 5796]
[6] Peng X, Tang H Q, Tian J D 2007 *Acta Phys. Sin.* **56** 2629 (in Chinese) [彭翔, 汤红乔, 田劲东 2007 物理学报 **56** 2629]
[7] He W Q, Peng X, Qin W, Meng X F 2010 *Opt. Commun.* **283** 2328
[8] He W Q, Peng X, Meng X F 2012 *Opt. Laser Technol.* **44** 1203
[9] He W Q, Peng X, Qi Y K, Meng X F, Qin W, Gao Z 2010 *Acta Phys. Sin.* **59** 1762 (in Chinese) [何文奇, 彭翔, 祁勇坤, 孟祥锋, 秦琬, 高志 2010 物理学报 **59** 1762]
[10] Meng X F, Peng X, Cai L Z, He W Q, Qin W, Guo J P, Li A M 2010 *Acta Phys. Sin.* **59** 6118 (in Chinese) [孟祥锋, 彭翔, 蔡履中, 何文奇, 秦琬, 郭继平, 李阿蒙 2010 物理学报 **59** 6118]
[11] Shi W S, Wang Y L, Xiao J, Yang Y H, Zhang J J 2011 *Acta Phys. Sin.* **60** 034202 (in Chinese) [史祎诗, 王雅丽, 肖俊, 杨玉花, 张静娟 2011 物理学报 **60** 034202]
[12] Liu Z J, Guo Q, Xu L, Ahmad M A, Liu S T 2010 *Opt. Express* **18** 12033
[13] Liu Z J, Xu L, Ahmad M A, Liu S T 2011 *Opt. Commun.* **284** 123
[14] Wang X G, Zhao D M 2011 *Opt. Commun.* **284** 148
[15] Zhou N R, Wang Y X, Gong L H 2011 *Opt. Commun.* **284** 3234
[16] Zhou N R, Wang Y X, Gong L H, He H, Wu J H 2011 *Opt. Commun.* **284** 2789
[17] Zhang Y, Wang B 2008 *Opt. Lett.* **33** 2443
[18] Wang B, Zhang Y 2009 *Opt. Commun.* **282** 3439
[19] Zhu N, Wang Y T, Liu J, Xie J H, Zhang H 2009 *Opt. Express* **17** 13418
[20] Kumar P, Joseph J, Singh K 2010 *J. Opt.* **12** 095402
[21] Tay C J, Quan C, Chen W, Fu Y 2010 *Opt. Laser Technol.* **42** 409
[22] Kumar P, Joseph J, Singh K 2011 *Appl. Opt.* **50** 1805
[23] Weng D D, Zhu N, Wang Y T, Xie J H, Liu J 2011 *Opt. Commun.* **284** 2485
[24] Yang B, Liu Z J, Wang B, Zhang Y, Liu S T 2011 *Opt. Express* **19** 2634
[25] Wang X G, Zhao D M 2012 *Appl. Opt.* **51** 686

Multi-level authentication based on two-beam interference*

He Wen-Qi[1)†] Peng Xiang[1)‡] Meng Xiang-Feng[2)] Liu Xiao-Li[1)]

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

2) (*Department of Optics, School of Information Science and Engineering and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan* 250100*, China*)

(Received 24 August 2012; revised manuscript received 20 September 2012)

Abstract

A method of multi-level authentication based on two-beam interference is proposed. By verifying the "password" and "phase key" of one user simultaneously, the system can thus achieve the two-factor authentication on the user's identity. This scheme can not only check the legality of one user, but also verify his identity level as an authorized user and then grant the user the corresponding permissions to access the system resources. While operating the authentication process, which largely depends on an optical setup based on interference, a "phase key" and a password-controlled "phase lock" are firstly loaded on two spatial light modulators (SLMs), separately. Then two coherent beams are respectively, modulated by the two SLMs and then interfere with each other, leading to an interference pattern in the output plane. It is recorded and transmitted to the computer to finish the last step of the authentication process: comparing the interference pattern with the standard verification images in the database of the system to verify whether it is an authorized user. When it turns to the system designing process for a user, which involves an iterative algorithm to acquire an estimated solution of an inverse problem, we need to determine the "phase key" according to a modified phase retrieval iterative algorithm under the condition of an arbitrarily given "phase lock" and a previously determined identity level (corresponding to a certain standard verification image). The theoretical analysis and simulation experiments both validate the feasibility and effectiveness of the proposed scheme.

Keywords: interference, fourier optics, phase retrieval, authentication

PACS: 42.25.Hz, 42.30.Kq, 42.30.Rx, 42.82.Fv **DOI:** 10.7498/aps.62.064205

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61171073, 61275014, 61201355, 60907005), the Sino-German Center for Research Promotion (SGCRP) (Grant No. GZ760), the National Natural Science Foundation of Shandong Province, China (Grant No. ZR2011FQ011), the National Science and Technology Program of Shandong Province, China (Grant No. 2011GGH20119), the Research Award Fund for Outstanding Young Scientists of Shandong Province, China (Grant No. BS2011DX023), the Science and Technology Bureau of Shenzhen, China (Grant No. 0014632063100426032), and the Independent Innovation Foundation of Shandong University, China (Grant No. 2010TB019).

† Corresponding author. E-mail: hewenqi@outlook.com

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