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

基于复振幅场信息复用和RSA算法的非对称多幅图像认证方法

潘雪梅 孟祥锋 杨修伦 王玉荣 彭翔 何文奇 董国艳 陈红艺

Asymmetric multiple-image authentication based on complex amplitude information multiplexing and RSA algorithm

Pan Xue-Mei Meng Xiang-Feng Yang Xiu-Lun Wang Yu-Rong Peng Xiang He Wen-Qi Dong Guo-Yan Chen Hong-Yi

引用信息 Citation: Acta Physica Sinica, 64, 110701 (2015) DOI: 10.7498/aps.64.110701
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.110701
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I11

基于复振幅场信息复用和RSA算法的非对称多幅图像认证方法*

潘雪梅[1)] 孟祥锋[1)†] 杨修伦[1)] 王玉荣[1)] 彭翔[2)] 何文奇[2)]
董国艳[3)] 陈红艺[4)]

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

2) (深圳大学光电工程学院, 深圳 518060)

3) (中国科学院大学材料科学与光电技术学院, 北京 100049)

4) (深圳大学电子科学与技术学院, 深圳 518060)

(2014 年 8 月 21 日收到; 2014 年 12 月 29 日收到修改稿)

结合相位恢复和像素行、列循环移动置乱技术, 本文提出了一种基于复振幅场信息复用和RSA 算法的非对称多幅图像认证方法, 通过菲涅耳域的相位恢复算法, 依次恢复并生成多幅图像各自所对应的输入平面的复振幅信息, 通过各自的行、列向量随机数对原始二值振幅模板进行行、列循环移动置乱操作来获得每幅图像的采样模板, 认证系统将多个复振幅场信息采样、叠加并空间复用, 同时, 行向量随机数和列向量随机数被RSA 算法公钥编码成密文. 系统认证时, 认证方利用自己持有的私钥将密文解码成行向量随机数和列向量随机数, 通过行、列循环移动置乱变换后获得各自的采样模板, 合成的复振幅信息和采样模板等认证信息均放置在各自正确位置, 当认证系统被正确波长的平面波照射时, 在输出平面能获得输出图像, 通过计算、显示输出图像和对应认证图像的非线性相关系数峰值来判断认证是否成功.

关键词: 安全认证, 相位恢复, 数字图像处理

PACS: 07.05.Pj, 42.30.Rx **DOI:** 10.7498/aps.64.110701

1 引 言

自 1995 年 Javidi 等提出基于光学 4f 傅里叶变换系统的双随机相位编码图像加密技术以来[1], 光学信息加密、隐藏和认证技术已成为信息安全领域的研究热点, 吸引着越来越多的科研工作人员投身到这一全新领域的研究中. 随后, 为了提出更为新颖的光学信息安全方案, 双随机编码技术成功与其他典型的光学信息处理技术或变换结合, 如分数傅里叶变换[2,3]、菲涅耳变换[4,5]、数字全息[6]、相移干涉术[7,8], gyrator 变换[9]、分数梅林变换[10]、双光束干涉[11−13], 等等.

除了双随机相位编码及其相关技术, 另一类光学信息加密、隐藏和认证方案, 是基于迭代相位恢复算法的, 特别是目前已报道的光学认证方法大多数都基于相位恢复算法. 1996 年, Wang 等提出一种基于相位恢复算法的光学信息安全技术, 该技术通过修正的 POCS(projection-onto-constraint-sets) 算法, 将一幅有意义的图像编码成两个随机相位掩膜[14]; Li 等改进了 Wang 的方案, 在输入面和输出面上使用迭代优化算法来设计相位板[15]; Situ 等进一步完善了上述方案, 该方案同时在输入面、频谱面和输出面使用相位恢复算

* 国家自然科学基金 (批准号: 61275014, 61307003, 61171073, 51102148, 1110488)、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) 和山东省优秀中青年科学家科研奖励基金 (批准号: BS2011DX023) 资助的课题.

† 通信作者. E-mail: xfmeng@sdu.edu.cn

法, 大大提高了收敛速度和恢复图像的质量[16,17]; 2006年, 我们提出了一种基于菲涅耳域的迭代多相位恢复算法, 在每次迭代中同时调整各个相位板的相位分布[18], 随后, 我们又发展了一种分级身份认证系统[19].

为了提高编码空间的利用率, 很多研究人员的目光开始聚焦在多幅图像的编码或认证方案上, 如Huang 等在菲涅耳域提出了一种基于改进的级联Gerchberg-Saxton算法的多幅图像加密方法[20]; 徐宁等提出了一种基于改进的多维数据叠加编码的多幅图像加密算法[21]; Chen等提出了一种基于随机采样技术的多幅图像认证方案[22]; Gong等提出了一种基于空间位置信息复用的多幅图像编码和认证方法[23]; 结合级联相位编码和改进的Gerchberg-Saxton算法, Wang等在gyrator域提出了一种多幅图像加密和认证方案[24]; 最近, Wang等在菲涅耳域提出了一种基于混合相位恢复算法的非线性多幅图像加密和认证系统[25]. 多重信息的叠加和复用是上述这些多幅图像编码、加密或认证方案的关键技术, 一般通过利用多个不同的随机采样模板对原始信息进行采样、叠加来实现, 而且一般一个随机采样模板与一幅待加密或认证的图像信息相对应(即K幅图像需要K个采样模板), 那么, 待加密或认证图像越多, 需要的采样模板数量也越多, 数据量相应也越大. 因此, 为了减少采样模板的数据存储量、提高多幅图像加密或认证系统的传输效率及安全性, 本文提出一种基于复振幅场信息复用、相位恢复、行(列)循环移动置乱和RSA算法的非对称多幅图像认证系统, 该系统只需要一幅初始的二值型掩模板, 然后利用每一幅待认证图像所对应的行向量随机数和列向量随机数实现对原始掩模板的行、列循环移动置乱, 从而获得复振幅场信息复用所需的采样模板; 而且, 行向量随机数和列向量随机数可以通过RSA算法进行非对称编码和解码, 从而能够解决传统对称密码体制的密钥的分发和管理问题, 大大提高该认证系统的安全性. 以下我们先介绍RSA算法和图像像素行、列循环移动置乱变换方法, 然后详细阐述所提认证系统的设计和认证过程、可行性分析、仿真测试等, 最后给出结论.

2 理论分析

2.1 RSA公钥加/解密算法

公钥密码体制是由Diffie和Hellman于1976年提出的[26], 也被称为非对称密码体制, 即运用单向函数的数学原理, 以实现加、解密密钥的分离, 加密密钥是公开的, 解密密钥是保密的. 公钥密码体制与传统私钥密码体制截然不同, 公开密钥密码算法基于数学函数而不是代替和替换操作; 而且公钥密码体制是非对称的, 它由两个密钥形成一个密钥对, 一个密钥交由拥有者保管, 不涉及密钥分发问题, 另一个可以公开而不用担心威胁到算法的安全, 这样基于公开的渠道就可以实现分发, 大大提高了分发的方便性, 这就解决了对称密码体制中的密钥管理、分发和数字签名难题[26,27].

1978年Rivest, Shamir和Adleman发明了著名的RSA公钥密码算法[28], RSA算法是基于数论的非对称密码体制, 公钥和私钥是一对大素数的函数, 从公钥和密文中恢复出明文的难度等价于分解两个大素数之积, 根据数论, 在实际中寻求两个大素数比较容易, 而将它们的乘积分解开则相当困难. RSA公钥密码算法正是基于这个优势在加密和数字签名系统中获得了广泛的应用[28,29].

RSA公钥密码算法的实现过程如下[28,29]:

1) 设计密钥

① 仔细选取两个互异的大素数p和q; ② 令$n = p \times q$, $z = (p-1) \times (q-1)$; ③ 接着选取一个随机数$e(0 < e < z)$, 满足$\gcd(e, z) = 1$, gcd 表示互为素数的操作; ④使用Euclidean算法$e \times d \equiv 1(\mathrm{mod}\ z)$计算$d$, 这里mod表示取模操作; ⑤目录中公开加密密钥(公钥) e和n, 保密私钥d和n, 销毁p和q.

2) 设计密文

把要求发送的明文信息m数字化、分块, 利用公钥(e, n)进行加密, 其加密过程是

$$C = m^e (\mathrm{mod}\ n) \quad (m < n). \tag{1}$$

3) 恢复明文

利用私钥(d, n)对加密密文C进行解密

$$m = C^d (\mathrm{mod}\ n). \tag{2}$$

2.2 图像像素行、列循环移动置乱变换

置乱变换, 就是通过将图像的像素信息次序打乱, 将a像素移动到b像素的位置上, b像素移动到c像素的位置上, 等等, 使原始图像变换成杂乱无章难以辨认的图像. 这里我们介绍一种通过行向量随机数和列向量随机数, 依次进行像素行、列循环移动置乱变换的方法, 该方法能够很好地实现图像像

素的随机置乱分布, 原始图像可以通过行向量随机数和列向量随机数进行逆变换来复原[18,30].

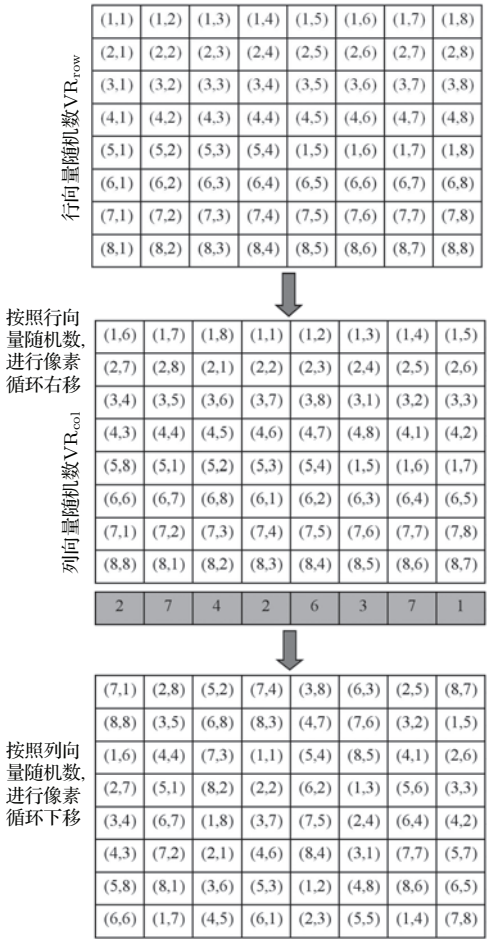

图1 像素行、列循环移动置乱变换示意图

Fig. 1. The diagram of pixels shift rotation permutation operations of row vector random numbers and column vectors random numbers.

为了简便, 以一个8 × 8的数值矩阵为例来阐述该置乱变换方法的主要原理, 如图1所示. 首先生成一个8位的行向量随机数$\mathrm{VR_{row}}$(位数与待变换矩阵的行数相同), 每位随机数是1至9之间的整数, 然后, 对初始矩阵的每一行的像素值进行循环右移操作, 每一行的循环移动次数通过对应每一位的行向量随机数来控制, 如第3位随机数为5, 则该矩阵的第三行的像素值依次向右循环移动5次, 以此类推; 与行向量随机数类似, 生成一个8位的列向量随机数$\mathrm{VR_{col}}$, 它的每一位1至9的随机整数, 用于对此前行置乱变换后的图像的每一列进行循环下移操作. 最后, 得到与原始矩阵差异很大的置乱矩阵, 置乱变换的行向量随机数$\mathrm{VR_{row}}$和列向量随机数$\mathrm{VR_{col}}$可以通过公钥密码算法, 如RSA算法, 进行非对称编码/解码, 以提高系统的安全性.

2.3 认证系统设计

1) 相位循环迭代更新

所提的认证系统是基于菲涅耳域进行实施的, 如图2所示, $f(x_0, y_0)$作为输入实振幅图像放置在输入平面(x_0, y_0)上, 假设共有N幅认证图像, 其中第i幅认证图像$g_i(x, y)$, 放置在输出平面(x, y)上, 所对应的初始值在[0, 1]之间的随机分布的相位板$A_i(x_0, y_0)$, 置于输入平面(x_0, y_0)、并紧贴于输入实振幅图像$f(x_0, y_0)$后侧, 初始值在[0, 1]之间的随机分布的相位板$B(x_t, y_t)$, 放置在变换平面(x_t, y_t)上, 两个相位板的透过率可以分别表示为$\exp[\mathrm{j}2\pi A_i(x_0, y_0)]$和$\exp[\mathrm{j}2\pi B(x_t, y_t)]$, 输入平面$(x_0, y_0)$和变换平面$(x_t, y_t)$、变换平面$(x_t, y_t)$和输出平面$(x, y)$之间的距离分别为$z_1$和$z_2$, 假设有一单位振幅、波长为$\lambda$的平面光波照射输入平面. 核心思想就是在给定输入约束$f(x_0, y_0)$和输出约束$g_i(x, y)$, 以及固定变换平面中相位板$B(x_t, y_t)$的相位分布的条件下, 通过循环迭代算法更新、恢复出输入平面上的相位板$A_i(x_0, y_0)$的分布[18,19].

相位恢复算法包含一系列的循环迭代, 其中每次迭代分为前向迭代(模拟光波从左到右传播)和后向迭代(模拟光波从右到左传播). 开始迭代时, 输入图像$f(x_0, y_0)$经随机相位板$A_i(x_0, y_0)$调制, 在菲涅耳近似的条件下, 变换平面的复振幅场$U_t(x_t, y_t)$可以表示为[7,8]

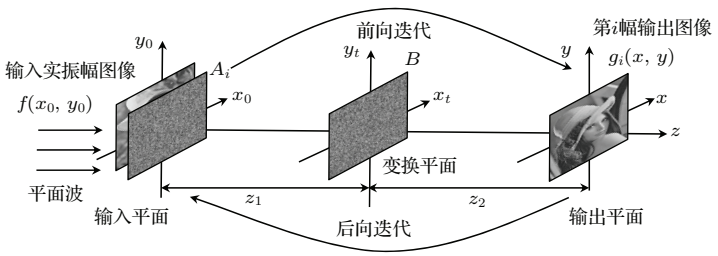

图2 菲涅耳域相位恢复迭代更新示意图

Fig. 2. The iteration process diagram of phase retrieval in Fresnel domain.

$$U_t(x_t,y_t)=\frac{\exp(\mathrm{j}kz_1)}{\mathrm{j}\lambda z_1}\iint f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_i(x_0,y_0)]\times\exp\left\{\frac{\mathrm{j}\pi}{\lambda z_1}\times[(x_t-x_0)^2+(y_t-y_0)^2]\right\}\mathrm{d}x_1\mathrm{d}y_1, \quad (3)$$

其中, $k=2\pi/\lambda$. 为了表示简便, 可以把上式写成

$$U_t(x_t,y_t)=\mathrm{FrT}_{z1}\{f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_i(x_0,y_0)]\}, \quad (4)$$

这里 FrT_{z1} 表示对距离 z_1 的菲涅耳变换. 因此, 输出平面上的复振幅场可以表示为

$$U(x,y)=\mathrm{FrT}_{z2}\{U_t(x_t,y_t)\times\exp[\mathrm{j}2\pi B(x_t,y_t)]\}, \quad (5)$$

将得到的输出图像 (即输出平面复振幅场 $U(x, y)$ 的实振幅) 与第 i 幅认证图像 $g_i(x, y)$ 进行相关系数 CC 比较, 相关系数 CC 的定义式如下 [18]:

$$\mathrm{CC}=\frac{E\{[h-E(h)]-[h'-E(h')]\}}{\sigma_h\sigma_{h'}}, \quad (6)$$

其中, h 和 h' 表示两幅实振幅图像, $E[\cdot]$ 表示数学期望, σ 表示标准差.

经过比较, 如果二者的相关系数未达到事先设定的阈值, 则用第 i 幅认证图像 $g_i(x, y)$ 对输出图像进行振幅约束 (用 $g_i(x, y)$ 替换复振幅场 $U(x, y)$ 的实振幅部分), 得到新的复振幅场分布

$$U'(x,y)=g_i(x,y)\exp\{\mathrm{jangle}[U(x,y)]\}, \quad (7)$$

angle 表示取相位操作. 该复振幅场 $U'(x, y)$ 经距离为 z_2 的逆菲涅耳变换 (IFrT, 与菲涅耳变换类似, 只是把 $-z_2$ 替换菲涅耳变换中的 z_2) 再次到达变换平面, 此时的复振幅场 $U'_t(x_t, y_t)$ 受到随机相位板 B 的调制后再经一次距离为 z_1 的逆菲涅耳变换, 到达输入平面, 此时对输入平面上的随机相位板 $A_i(x_0, y_0)$ 进行相位更新.

假设第 k 次迭代后的相位板 A_i 的相位分布为 $A_i^k(x_0, y_0)$, 那么在第 $k+1$ 次时其相位更新为

$$\begin{aligned}A_i^{k+1}&=\mathrm{angle}\left\{\mathrm{IFrT}_{z1}\left[U_t'^k\exp(-\mathrm{j}2\pi B)\right]\right\}\\&=\mathrm{angle}\{\mathrm{IFrT}_{z1}[\mathrm{IFrT}_{z2}\{g_i\times\exp\left[\mathrm{jangle}\left(U^k\right)\right]\}\exp(-\mathrm{j}2\pi B)]\}.\end{aligned} \quad (8)$$

整个相位恢复算法的迭代流程图如图 3 所示. 直至最后得到的输出图像 (即输出平面复振幅场 $U(x, y)$ 的实振幅) 与第 i 幅认证图像 $g_i(x, y)$ 的相关系数 CC, 达到事先设定的阈值, 则循环迭代过程结束. 迭代结束后输入平面的最终相位信息, 这里表示为 $A_i^{\mathrm{end}}(x_0, y_0)$, 那么, 对应于第一幅、第二幅……第 N 幅认证图像的输入平面的最终相位信息可以表示为 $A_1^{\mathrm{end}}(x_0, y_0)$, $A_2^{\mathrm{end}}(x_0, y_0)$,…, $A_N^{\mathrm{end}}(x_0, y_0)$, 它们连同输入振幅图像 $f(x_0, y_0)$ 一起保存在认证中心.

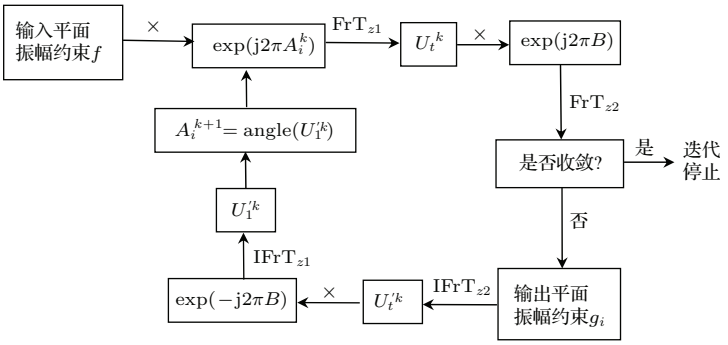

图 3 相位恢复算法的迭代过程流程图

Fig. 3. The flowchart of iterative phase retrieval algorithm.

2) 像素行、列循环移动置乱构建采样模板; 对行、列向量随机数进行公钥编码

如图 4, 认证中心生成一个由 0 和 1 随机分布的二值振幅型掩模板 M, 其大小与输入图像及认证图像相同, 像素为 1 的位置用于后续的复振幅场信息采样及复用, 像素为 0 的位置对于采样、复用及最后的认证并不起实质作用, 但是对多幅图像信息的叠加及复用提供了冗余空间. 像素为 1 或 0 的比例可以根据认证图像的总数进行相应地控制 [22,23].

认证中心为每个认证方 (每个认证方对应每一幅认证图像) 分别生成一组行向量随机数和列向量随机数: $(\mathrm{VR}_{\mathrm{row1}}, \mathrm{VR}_{\mathrm{col1}})$, $(\mathrm{VR}_{\mathrm{row2}}, \mathrm{VR}_{\mathrm{col2}})$, …, $(\mathrm{VR}_{\mathrm{row}i}, \mathrm{VR}_{\mathrm{col}i})\cdots$, $(\mathrm{VR}_{\mathrm{rowN}}, \mathrm{VR}_{\mathrm{colN}})$, 用于对振幅型掩模板 M 分别进行像素行、列循环移动置乱

变换. 置乱变换后, 得到N个新的振幅型随机采样模板: M_1, $M_2\cdots$, $M_i\cdots$, M_N, 具体仿真实施的时候, 针对每幅认证图像, 通过选取不同的行向量随机数、列向量随机数, 保证所对应的采样模板中像素1的位置的重叠比例不超过3%(如果重叠比例过高的话, 会影响最后的认证结果, 甚至无法通过认证).

针对N组行向量随机数和列向量随机数, 认证中心用事先设计好的公钥对(e_1, N_1), $(e_2, N_2)\cdots$, (e_i, N_i),$\cdots$, (e_N, N_N), 分别对每一组行向量随机数和列向量随机数: $(\mathrm{VR}_{\mathrm{row}1}, \mathrm{VR}_{\mathrm{col}1})$, $(\mathrm{VR}_{\mathrm{row}2}, \mathrm{VR}_{\mathrm{col}2})$, $\cdots$, $(\mathrm{VR}_{\mathrm{row}i}, \mathrm{VR}_{\mathrm{col}i})$, $\cdots$, $(\mathrm{VR}_{\mathrm{row}N}, \mathrm{VR}_{\mathrm{col}N})$, 进行公钥(非对称)编码(所对应的私钥对通过安全途径发送给各自的认证方), 编码后得到N对随机数密文: (C_{r1}, C_{c1}), (C_{r2}, C_{c2}), $\cdots$, (C_{ri}, C_{ci}), $\cdots$, (C_{rN}, C_{cN}), 它们存放在认证中心.

3) 输入平面的复振幅场信息采样、叠加、复用

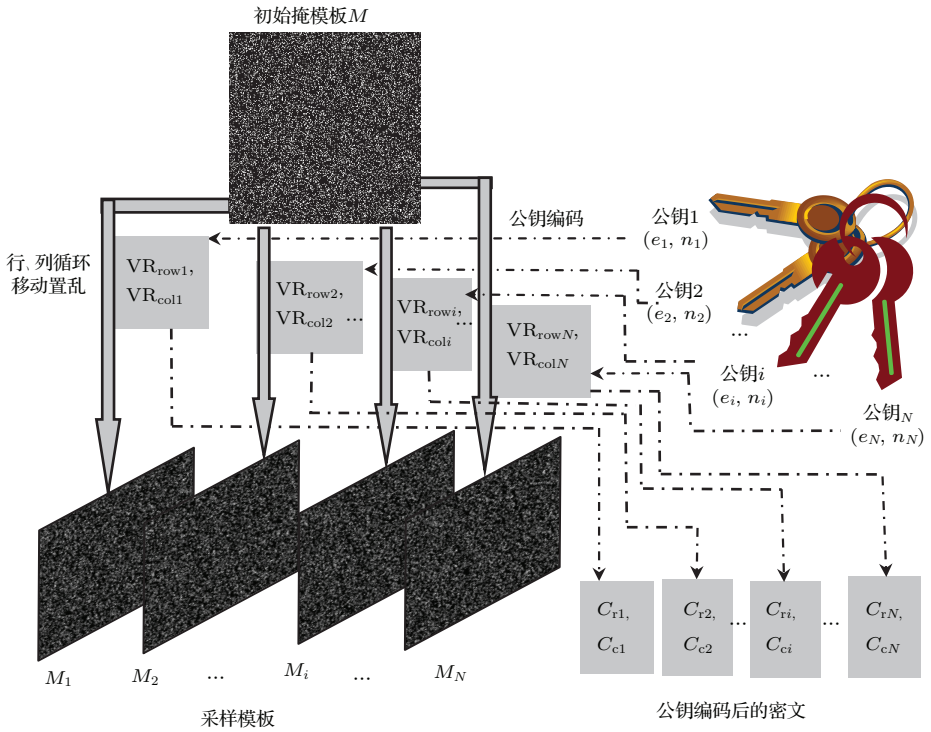

图4 采样模板生成及行、列向量随机数的公钥编码

Fig. 4. The generation of sampling masks and the public keys encoding process of row vector random numbers and column vectors random numbers.

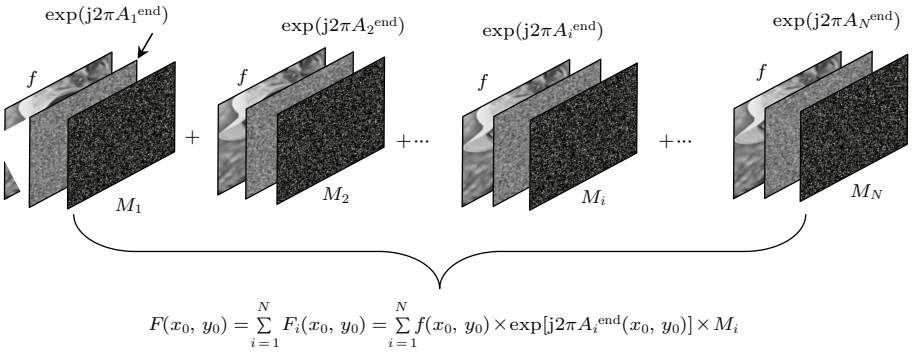

图5 复振幅场信息的采样、叠加和复用示意图

Fig. 5. The sampling, superimposition and multiplexing diagram of complex amplitude field information.

如图5, 输入图像分别经输入平面的 N 个最终相位信息调制后, 可以得到 N 个复振幅场信息:

$$F_1(x_0,y_0)=f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_1^{\mathrm{end}}(x_0,y_0)],$$
$$F_2(x_0,y_0)=f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_2^{\mathrm{end}}(x_0,y_0)],$$
$$\cdots,$$
$$F_i(x_0,y_0)=f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_i^{\mathrm{end}}(x_0,y_0)],$$
$$\cdots,$$
$$F_N(x_0,y_0)=f(x_0,y_0)\times\exp[\mathrm{j}2\pi A_N^{\mathrm{end}}(x_0,y_0)],$$

用新的振幅型采样模板: M_1, M_2, $\cdots$, M_i, $\cdots$, M_N 分别对该复振幅场信息进行采样, 然后将这 N 个采样后的复振幅场信息进行空域叠加, 得到输入平面上叠加后的总的合成复振幅分布

$$\begin{aligned}F(x_0,y_0)&=\sum_{i=1}^{N}F_i(x_0,y_0)\\&=\sum_{i=1}^{N}f(x_0,y_0)\\&\quad\times\exp\left[\mathrm{j}2\pi A_i^{\mathrm{end}}(x_0,y_0)\right]\times M_i,\end{aligned}\tag{9}$$

其中, $\sum$ 代表求和操作. 最后, 将得到的合成复振幅场 $F(x_0,\ y_0)$、变换平面的随机相位信息 $B(x_t,\ y_t)$, N 幅认证图像 $g_1(x,\ y)$—$g_N(x,\ y)$、初始二值振幅型掩模板 M 存储到认证中心.

2.4 认证过程

这里仅以第 i 幅认证图像为例, 说明该系统的具体认证过程, 其流程图如图6.

1) 认证方使用所持有的私钥对 $(d_i,\ n_i)$, 将公钥编码后的密文 $(C_{ri},\ C_{ci})$, 进行私钥解码, 得到对应的行向量随机数 $\mathrm{VR}_{\mathrm{row}i}$ 和列向量随机数 $\mathrm{VR}_{\mathrm{col}i}$.

2) 利用行向量随机数 $\mathrm{VR}_{\mathrm{row}i}$ 和列向量随机数 $\mathrm{VR}_{\mathrm{col}i}$, 对认证中心保存的初始掩模板 M 依次进行行、列循环移动置乱变换, 恢复出相应的采样模板 M_i.

3) 认证系统将合成复振幅场 $F(x_0,\ y_0)$ 放置在输入平面 $(x_0,\ y_0)$ 上, 并将2) 恢复的采样模板 M_i 紧贴其后放置; 将相位信息 $B(x_t,\ y_t)$ 放置在变换平面 $(x_t,\ y_t)$ 上.

4) 当认证系统被波长为 λ 的平面波垂直照射时, 在输出平面上可以得到输出的实振幅图像

$$\begin{aligned}g_i'(x,y)=&\mathrm{abs}(\mathrm{FrT}_{z2}\{\mathrm{FrT}_{z1}[F(x_0,y_0)\times M_i]\\&\times\exp[\mathrm{j}2\pi B(x_t,y_t)]\}),\end{aligned}\tag{10}$$

其中, abs 表示取实振幅操作.

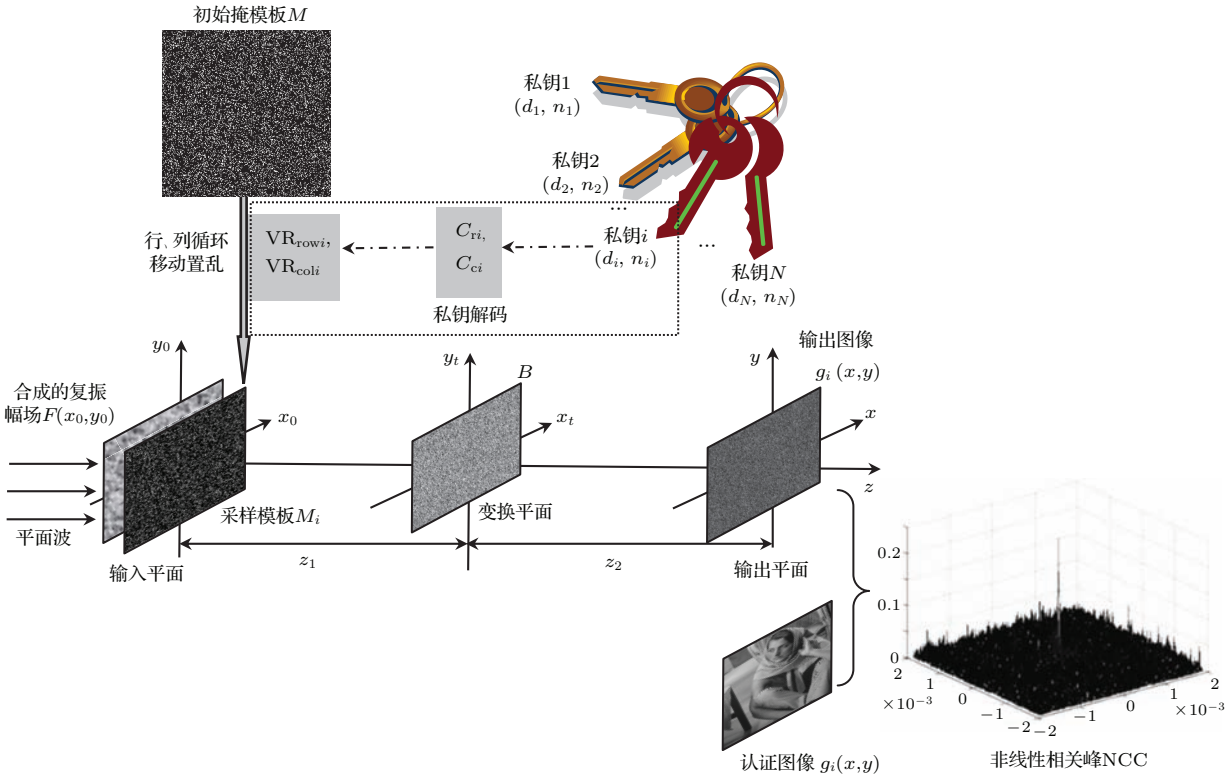

图6 认证过程示意图

Fig. 6. The authentication process diagram.

5) 由于叠加合成后的复振幅场信息 $F(x_0, y_0)$ 仅包含一部分认证图像 $g_i(x, y)$ 的采样信息, 因此, 一般最后的实振幅图像 $g_i'(x, y)$ 只是噪声图像, 很难从视觉上直接分辨, 因为它与认证图像 $g_i(x, y)$ 的相关系数很小. 但是可以通过非线性相关系数 NCC 来评价二者的相关程度, 从而实现图像信息的认证 [31]:

$$\begin{aligned}&\mathrm{NCC}(x,y)\\ =&\mathrm{IFT}\Big(|F_{g'}(u,v)\,F_g(u,v)|^{\omega}\\ &\times\exp\left\{\mathrm{j}\left[\phi_{F_{g'}}(u,v)-\phi_{F_g}(u,v)\right]\right\}\Big),\end{aligned}\tag{11}$$

其中, IFT 表示逆傅里叶变换, $F_{g'}(u, v)$ 和 $F_g(u, v)$ 分别表示输出实振幅图像 $g'(x, y)$ 与认证图像 $g(x, y)$ 的傅里叶变换频谱分布, $\phi_{F_{g'}}(u, v)$ 和 $\phi_{F_g}(u, v)$ 分别表示二者频谱的相位信息.

6) 通过计算输出实振幅图像 $g_i'(x, y)$ 和认证图像 $g_i(x, y)$ 的非线性相关系数 NCC, 如果在其三维分布图中存在一个明显的非线性相关系数峰值, 则认为认证成功, 认证方能够通过该认证系统并获得相应的使用权限.

7) 如果在三维非线性相关系数分布图中, 没有出现明显的峰值或者噪声信号过大的话, 则认为认证失败.

3 数值仿真

通过计算机仿真对所提认证系统的可行性进行了验证和测试, 选取标准灰度图像 elaine 作为输入实振幅图像, 如图 7 所示. 涉及的所有图像的大小均为 256 × 256 像素, 初始的掩模板及采样矩阵为二值图像, 其余图像均为灰度级为 256、像素大小为 15 μm 的灰度图像, 这里以 6 ($N = 6$) 幅认证图像为例进行仿真, 其他系统参数如下: 波长 $\lambda = 532$ nm, 距离参数 $z_1 = z_2 = 108.3$ mm.

选取的 6 幅认证灰度图像如图 8 (a)—(f) 所示, 变换平面中相位板 B 的相位信息如图 9, 依次经过 2000 次循环迭代后, 输入平面上的最终的相位信息 A_1^{end}, A_2^{end}, $\cdots$, A_6^{end} 如图 10 (a)—(f).

图 8 6 幅认证图像

Fig. 8. 6 standard certification images.

图 7 输入图像

Fig. 7. The input image.

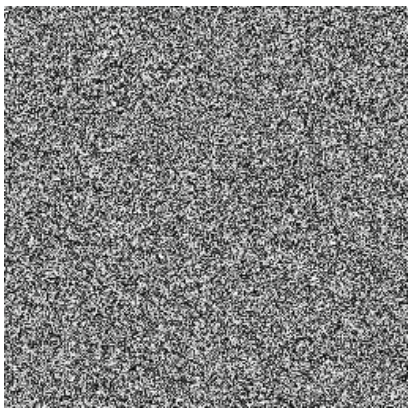

图 9 变换平面的相位信息 B

Fig. 9. The phase mask B located in the transform plane.

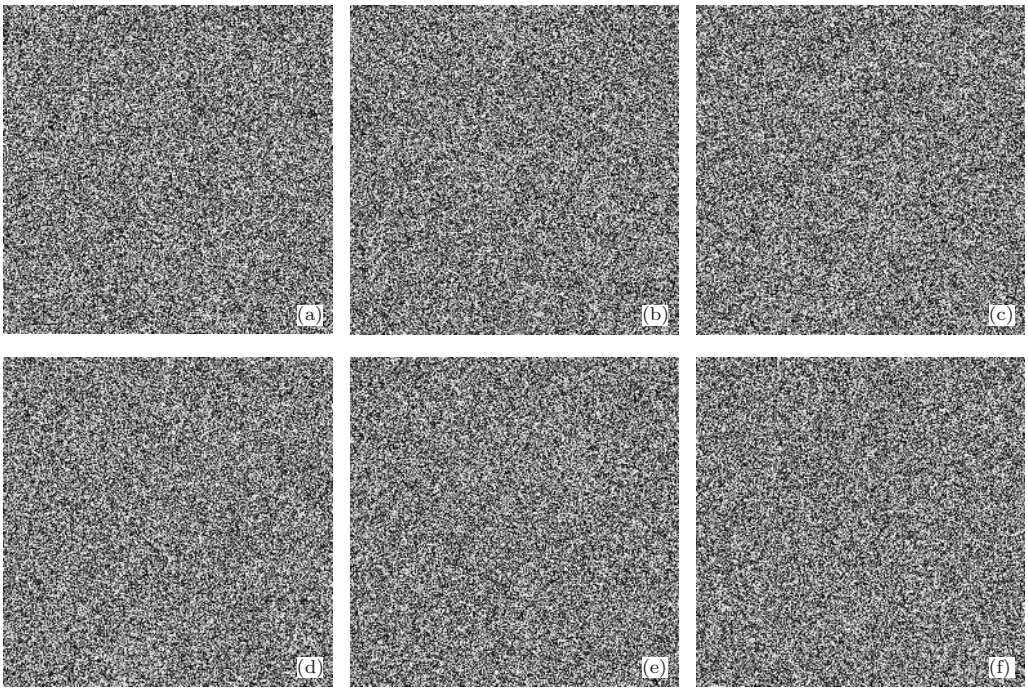

图 10 输入平面上的最终迭代后的相位信息 $A_1^{\rm end}$ 至 $A_6^{\rm end}$

Fig. 10. the final iterated phase masks $A_1^{\rm end}$—$A_6^{\rm end}$ located in the input plane.

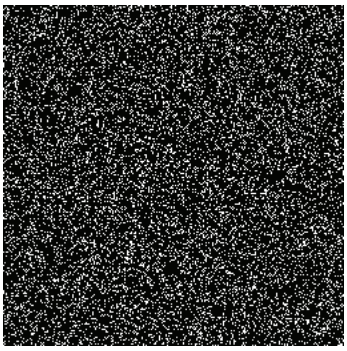

图 11 原始的二值振幅型掩模板 M

Fig. 11. Original binary amplitude mask M.

表 1 6 组行向量随机数和列向量随机数

Table 1. 6 groups of row vector random numbers and column vectors random numbers.

	行向量随机数 $\rm VR_{row}$	列向量随机数 $\rm VR_{col}$
第 1 组	$\rm VR_{row1}$: 32561389	$\rm VR_{col1}$: 27426371
第 2 组	$\rm VR_{row2}$: 76915429	$\rm VR_{col2}$: 91716672
第 3 组	$\rm VR_{row3}$: 49596252	$\rm VR_{col3}$: 37383396
第 4 组	$\rm VR_{row4}$: 32913286	$\rm VR_{col4}$: 42317554
第 5 组	$\rm VR_{row5}$: 13672456	$\rm VR_{col5}$: 62488232
第 6 组	$\rm VR_{row6}$: 53993854	$\rm VR_{col6}$: 47291159

图 11 表示初始的二值振幅型掩模板 M, 其中像素值 1 的比例为 17.2%, 为了系统设计简便, 把它进行 8 × 8 分区, 按照每一个 8 × 8 的区间进行行、列向量循环移动置乱操作, 行向量随机数 $\rm VR_{row}$ 和列向量随机数 $\rm VR_{col}$ 均为 8 位的整数, 每一位的整数值限定在 1—9 之间, 表 1 给出了 6 组不同的行向量随机数 $\rm VR_{row}$ 和列向量随机数 $\rm VR_{col}$ 的取值. 掩模板 M 分别经上述 6 组数据进行行、列向量循环移动置乱操作后, 得到的 6 个采样模板 M_1—M_6 如图 12 (a)—(f), 可以看出, 它们均为分布比较均匀的二值噪声图像.

认证系统为 6 个不同的认证方生成 6 组 RSA 公钥-私钥对的具体参数见表 2, 其中最后一栏为使用公钥对行向量随机数和列向量随机数编码后的字符串密文; 认证方只要利用自己所持有的私钥对各自的字符串密文进行非对称解码, 就能获得正确的行向量随机数 $\rm VR_{row}$ 及列向量随机数 $\rm VR_{col}$, 进而通过循环移动置乱操作, 即可获得各自的采样模板 M_i. 系统将合成的复振幅场和相位板 B 分别放置在输入平面 (x_0, y_0) 和变换平面 (x, y) 上, 认证方将得到的采样模板 M_i 紧贴合成的复振幅场放置在输入平面 (x_0, y_0) 上, 当系统被正确波长的平面波照射、距离参数也都正确时, 在输出平面上即可恢复出输出的实振幅图像, 计算它与对应认证图像的非线性相关系数 NCC, 并进行三维分布显示, 图 13 给出了在所有密钥都正确时, 6 种情况下的非线性相关系数 NCC 的三维分布图, 从图中可以清楚的分辨出明显的非线性相关系数峰值, 且周围的

干扰噪声并不明显, 说明此时认证通过. 图14表示使用错误的行向量随机数和列向量随机数时, 最后计算出的非线性相关系数NCC分布图, 此时并无明显的峰值, 说明此时认证失败.

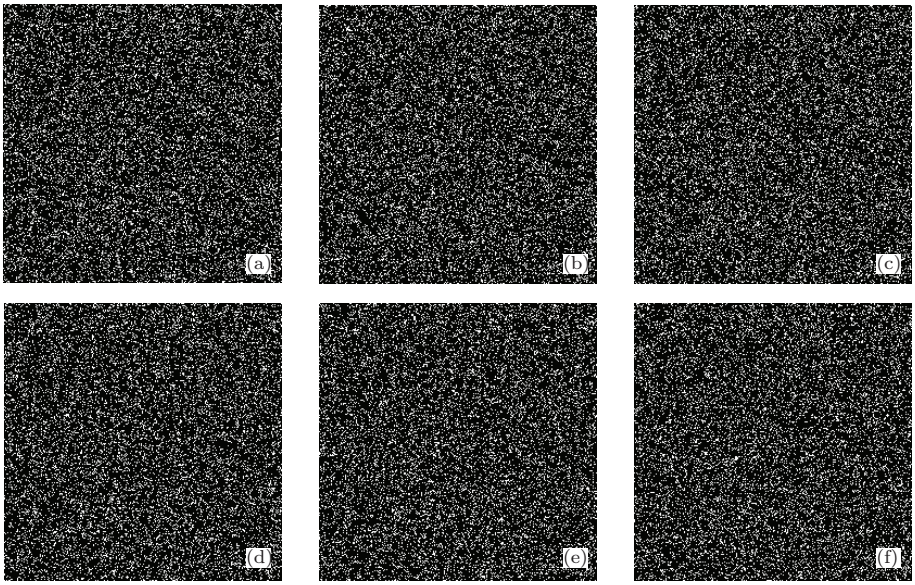

图12 6个采样模板 M_1 至 M_6

Fig. 12. 6 sampling masks M_1—M_6.

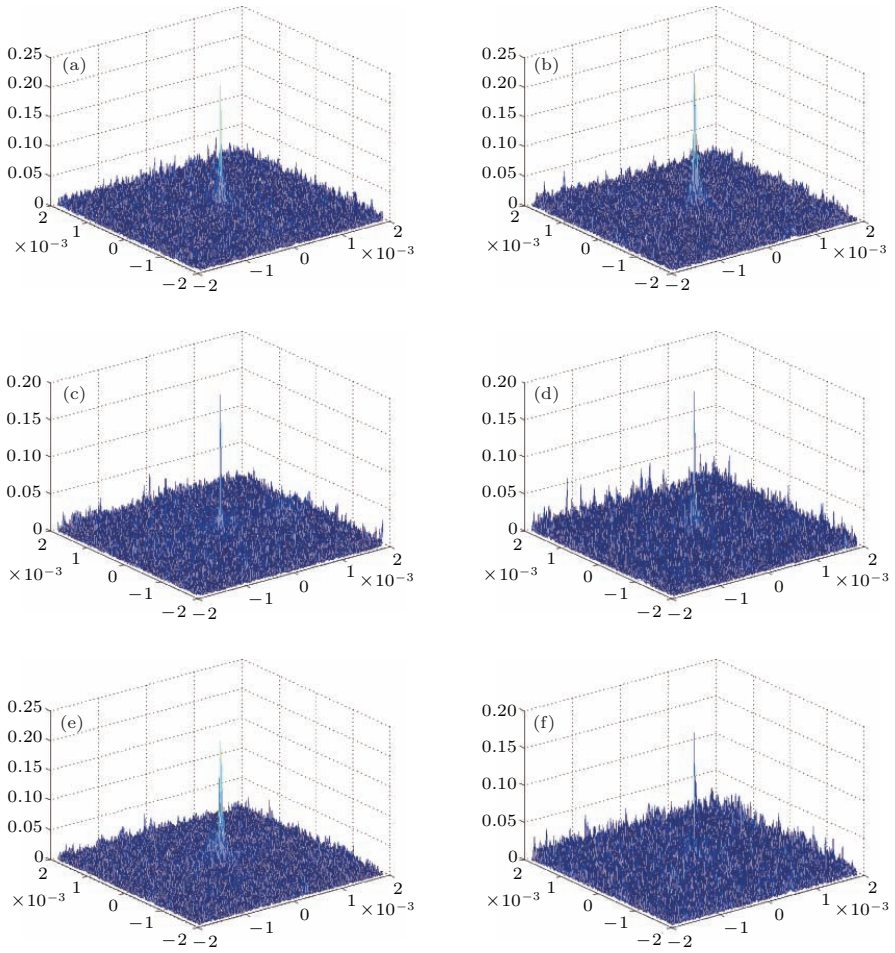

图13 所有密钥均正确时, 6种情况下的非线性相关系数NCC的三维分布图

Fig. 13. The 3D NCC distributions in 6 circumstances with all the correct keys.

表 2 6 组 RSA 公钥-私钥对的具体参数

Table 2. The parameters of 6 public-private keys.

序号	p	q	e	d	n	VR_{row}	VR_{row} 的密文	VR_{col}	VR_{col} 的密文
1	6710	6710	33370689	69912403	4503603	32561	142955927	27426	846007734
	8879	8913	98195453	2222773	922338527	389	2442878	371	102556
2	5675	5675	11552826	12289193	3221652	76915	287418587	91716	226309588
	9587	9611	50504887	05141663	078640657	429	0156442	672	9140672
3	4689	4689	19758309	12235099	2199069	49596	161625473	37383	851716561
	42389	42407	011123463	8880170503	72641990323	252	352363305	396	35450684
4	5247	5247	21814195	14599008	2754038	32913	196809946	42317	967489870
	89347	89383	9843672229	8998714481	77617102901	286	090057647	554	78805197
5	1014	1014	95192040	83966229	1028982	13672	520285492	62488	758001173
	38783	38801	14407207	88733943	8522419183	456	1205593	232	0541815
6	9143	9143	13168304	33333816	8360140	53993	546435708	47291	662979798
	3789	3819	33237007	2498703	513910191	854	1852611	159	4672211

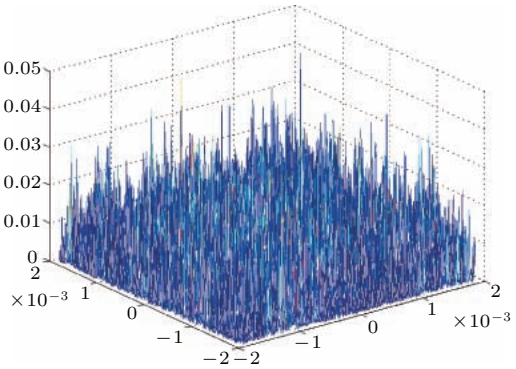

图 14 使用错误的行向量随机数和列向量随机数时, 最后的非线性相关系数 NCC 的三维分布图

Fig. 14. The 3D NCC distributions with the wrong row vector random numbers and column vectors random numbers.

4 结 论

结合相位恢复和像素行、列循环移动置乱技术, 本文提出了一种基于复振幅场信息复用和 RSA 算法的非对称多幅图像认证方法, 认证系统将多幅图像经相位恢复算法迭代后合成的复振幅信息采样、叠加并复用, 采样模板通过各自的行、列向量随机数对原始模板进行行、列循环移动置乱而获得, 行向量随机数和列向量随机数可以通过 RSA 算法进行非对称编码和解码, 该多幅图像认证方法减少了采样模板的数据存储量、提高了认证系统的传输效率及安全性. 我们阐述了所提认证系统的设计和认证过程, 并通过数值仿真对其可行性进行了验证与分析.

参考文献

[1] Refrégier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Liu S T, Mi Q L, Zhu B H 2001 *Opt. Lett.* **26** 1242
[3] Tao R, Xin Y, Wang Y 2003 *Opt. Express* **15** 16067
[4] Situ G, Zhang J 2003 *Opt. Lett.* **29** 1584
[5] Chen L F, Zhao D M 2006 *Opt. Express* **14** 8552
[6] Wang X G, Zhao D M, Jing F, Wei X F 2006 *Opt. Express* **14** 1476
[7] Meng X F, Cai L Z, Xu X F, Yang X L, Shen X X, Dong G Y, Wang Y W 2006 *Opt. Lett.* **31** 1414
[8] Fan D S, Meng X F, Yang X L, Wang Y R, Peng X, He W Q 2012 *Acta. Phys. Sin.* **61** 244204 (in Chinese) [范德胜, 孟祥锋, 杨修伦, 王玉荣, 彭翔, 何文奇 2012 物理学报 **61** 244204]
[9] Liu Z J, Guo Q, Xu L, Ahmad M A, Liu S T 2010 *Opt. Express* **18** 12033
[10] Zhou N R, Wang Y X, Gong L H 2011 *Opt. Commun.* **284** 3234
[11] Zhang Y, Wang B 2008 *Opt. Lett.* **33** 2443
[12] Chen W, Chen X 2013 *Opt. Commun.* **286** 123
[13] 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]
[14] Wang R K, Watson I A, Chatwin C 1996 *Opt. Eng.* **35** 2464
[15] Li Y Z, Kreske K, Rosen J 2000 *Appl. Opt.* **39** 5295
[16] Situ G, Zhang J 2005 *Opt. Commun.* **245** 55
[17] Situ G, Zhang J 2003 *Optik* **114** 473
[18] Meng X F, Cai L Z, Yang X L, Shen X X, Dong G Y 2006 *Appl. Opt.* **45** 3289
[19] Meng X F, Cai L Z, Wang Y R, Yang X L, Xu X F, Dong G Y, Shen X X, Zhang H, Cheng X C 2007 *J. Opt. A: Pure Appl. Opt.* **9** 1070
[20] Huang J J, Hwang H E, Chen C Y, Chen C M 2012 *Appl. Opt.* **51** 2388
[21] Xu N, Chen X L, Yang G 2013 *Acta. Phys. Sin.* **62** 084202 (in Chinese) [徐宁, 陈雪莲, 杨庚 2013 物理学报 **62** 084202]

[22] Chen W, Chen X D 2014 *Opt. Commun.* **318** 128
[23] Gong Q, Liu X Y, Li G Q, Qin Y 2013 *Appl. Opt.* **52** 7486
[24] Wang Q, Guo Q, Lei L 2014 *Opt. Commun.* **320** 12
[25] Wang Y, Quan C, Tay C J 2014 *Opt. Commun.* **330** 91
[26] Diffie W, Hellman M E 1976 *IEEE T. Inform. Theory* **IT-22** 644
[27] Bruce S 1996 *Applied Cryptography Second Edition: Protocols, Algorithms, and Scource Code in C* (New York: John Wiley & Sons) pp 461–482
[28] Rivest R, Shamir A, Adleman L 1978 *Comm. ACM* **21** 120
[29] Meng X F, Peng X, Cai L Z, Li A M, Gao Z, Wang Y R 2009 *J. Opt. A: Pure Appl. Opt.* **11** 085402
[30] Spagnolo G S, Simonetti C, Cozzella L 2005 *J. Opt. A: Pure Appl. Opt.* **7** 333
[31] Chen W, Chen X D, Stern A, Javidi B 2013 *IEEE Photon. J.* **5** 6900113

Asymmetric multiple-image authentication based on complex amplitude information multiplexing and RSA algorithm*

Pan Xue-Mei[1)] Meng Xiang-Feng[1)†] Yang Xiu-Lun[1)] Wang Yu-Rong[1)] Peng Xiang[2)]
He Wen-Qi[2)] Dong Guo-Yan[3)] Chen Hong-Yi[4)]

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

2) (*College of Optoelectronics Engineering, Shenzhen University, Shenzhen 518060, China*)

3) (*College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China*)

4) (*College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China*)

(Received 21 August 2014; revised manuscript received 29 December 2014)

Abstract

By combining the iterative phase retrieval algorithm in the Fresnel domain with the shift rotation permutation operations of row vectors and column vectors, a new kind of asymmetric multiple-image authentication based on complex amplitude information multiplexing and RSA algorithm is proposed, where multiple complex amplitude information in the input plane is retrieved and generated by the phase retrieval algorithm in the Fresnel domain. In original binary amplitude mask, the row vector and column vectors random numbers are randomly generated in advance, such that each sampling mask for each authenticator is obtained by the shift rotation permutation operations of corresponding row vector and column vectors random numbers for original binary amplitude mask. Thus, one synthesized complex amplitude is generated by the operations of sampling, overlap and multiplexing, and then sent to the certification center for authentication use. At the same time, the row vector and column vectors random numbers are encoded to ciphers by the public keys of RSA algorithm, and then delivered to the corresponding authenticators. During the authentication process, the row vector and column vectors random numbers are first decoded by the private keys possessed by the authenticator; second, the authenticator's sampling mask is reconstructed by the shift rotation permutation operations of the above decoded random numbers for original binary amplitude mask. Finally, the authenticator with other additional authentication keys is prompted to place the synthesized complex amplitude information and its sampling mask at the corresponding positions, when the system is illuminated by a plane wave with the correct wavelength. A recovered image is then recorded in the output plane, by calculating and displaying the nonlinear correlation coefficient between the recovered image and the certification image, if there exists a remarkable peak in its nonlinear correlation coefficient distributions, indicating that the authentication is successful. On the contrary, if there is no remarkable peak but uniformly distributed white noise in the map, the authentication process is a failure attempt. Any intruder with randomly generated forged authentication keys will end up with a failure which enhances the security of the system to some extent.

Keywords: security authentication, phase retrieval, digital image processing

PACS: 07.05.Pj, 42.30.Rx **DOI:** 10.7498/aps.64.110701

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61275014, 61307003, 61171073, 51102148, 1110488), the Natural Science Foundation of Shandong province, China (Grant No. ZR2011FQ011), the Natural Science and Technology programs of Shandong province, China (Grant No. 2011GGH20119), and the Research Award Fund for Outstanding Young Scientists of Shandong Province, China (Grant No. BS2011DX023).

† Corresponding author. E-mail: xfmeng@sdu.edu.cn