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

基于Q-plate的双图像非对称偏振加密

绪其军 李德林 常琛亮 袁操今 冯少彤 聂守平

Q-plate based dual image asymmetric polarization encryption

Xu Qi-Jun Li De-Lin Chang Chen-Liang Yuan Cao-Jin Feng Shao-Tong Nie Shou-Ping

引用信息 Citation: Acta Physica Sinica, 68, 084202 (2019) DOI: 10.7498/aps.68.20181902
在线阅读 View online: https://doi.org/10.7498/aps.68.20181902
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于 Q-plate 的双图像非对称偏振加密*

绪其军 李德林 常琛亮 袁操今 冯少彤 聂守平†

(南京师范大学, 江苏省光电技术重点实验室, 南京 210023)

(2018 年 10 月 25 日收到; 2019 年 1 月 11 日收到修改稿)

基于 Q-plate 提出了一种对两幅图像做非对称偏振加密的新方法. 在该方法中, 首先, 将待加密的两幅图像通过干涉分解成两块纯相位板; 其次, 将这两块纯相位板分别编码到偏振光的两个正交分量中; 最后, 利用 Q-plate 和像素化的偏振片改变这束光的偏振分布, 达到对图像的加密效果, 用电荷耦合器件接收输出面的强度分布图作为最终的密文. 其中一块纯相位板作为解密密钥. 算法的解密密钥不同于加密密钥, 由此实现了非对称加密. 由于 Q-plate 是电调控的, 它的每个像素点的光轴各不相同, 所以能够根据描述变面结构空间旋转率的常数 q 来改变每个像素的偏振态. 加密过程中用 Q-plate 的 q 值和像素化的偏振片的偏振角度作为加密密钥, 这两个加密密钥具有很高的敏感性, 极大地提高了算法的安全性. 数值模拟结果验证了该方法的可行性和有效性.

关键词: Q-plate, 非对称加密, 偏振

PACS: 42.30.–d, 42.25.Ja, 42.30.Va **DOI:** 10.7498/aps.68.20181902

1 引 言

随着计算机网络的迅猛发展, 信息的安全传输和存储已成为商业、工业和国防等多个不同领域的重要课题. 由于光波的固有属性, 用光学硬件实现加密和解密具有处理速度快、加密自由度多等优势, 因此光学加密技术成为一个热门的研究领域. 自从 Refregier 和 Javidi[1] 在 1995 年提出双随机相位加密以来, 越来越多的光学加密方法相继被提出 [2–7]. 然而, 进一步分析这些方法的安全性发现, 由于它们的线性特性, 大部分方法的抗攻击性较低, 容易受到不同类型的攻击. 其中, 基于变换域的加密方法 (例如傅里叶变换 [2]、gyrator 变换 [3]、菲涅耳变换 [4] 等) 都是线性对称加密系统, 属于对称密码学, 加密密钥与解密密钥相同, 在网络环境下会遇到密钥管理问题. 为了解决这一问题, 研究人员提出许多改进的非对称光学加密系统 [8–11], 解决了线性问题, 有效提高了系统的安全性. 其中, Qin 和 Peng[8] 于 2010 年提出了一种基于相位截断傅里叶变换 (phase-truncated Fourier transform, PTFT) 的光学非对称加密方法,通过在光学加密过程中引入相位截断, 去除了双随机相位加密系统的线性特性. 然而, 又有人提出可使用已知明文攻击及选择明文攻击来破译这些加密方法 [12–14]. 因此, 虽然非对称光学加密方法提高了光学图像加密的鲁棒性, 但仍然需要更高安全性的加密方法来抵抗攻击.

除了采用相位作为密钥的光学加密系统之外, 采用偏振态作为密钥的光学加密系统近些年来也被提及. 由于偏振加密在加密密钥的设计中具有额外的灵活性, 使得密钥具有更多的组合, 可以提高

* 国家自然科学基金 (批准号: 61775097, 11574152, 61605080)、国家重点研发计划 (批准号: 2017YFB0503505)、中国教育部虚拟地理环境重点实验室 (南京师范大学) 开放基金 (批准号: 2017VGE02) 和江苏省研究生科研与实践创新计划项目 (批准号: SJCX17_0336) 资助的课题.

† 通信作者. E-mail: nieshouping@njnu.edu.cn

光学加密方法抵抗暴力攻击的鲁棒性, 所以使用偏振光的光学加密引起了很多的关注[15–19]. 2010 年, Alfalou 和 Brosseau[15] 使用穆勒矩阵对图像做偏振加密, 通过波片、水平线偏振片以及像素化的偏振片来改变原始图像的偏振态, 实现对图像的偏振加密. 由于拥有大量可能的密钥组合, 该方案能够抵抗暴力攻击. 在此基础上, 2013 年, Sudheesh 和 Naveen[7] 在菲涅耳域使用相位截断的方法对图像进行偏振加密, 该方法能够很好地抵抗已知明文攻击和选择明文攻击. 另外, 偏振选择光学元件[16]、菲涅耳域干涉法[17]、基于椭圆偏振光的振幅重建[18]、非相干成像[19] 等也被运用到偏振加密中实现对图像信息的加密, 以此来提高加密系统的安全性. 2017 年, Fatima 和 Nishchal[20] 使用空间变化的偏振态对图像加密, 通过改进的迭代算法将加密图像强度信息编码到纯相位模板中, 测量矢量光束的斯托克斯参数作为最后的密文.

但是, 上述这些方法都是对单幅图像做偏振加密, 并没有涉及双图像的偏振加密. 文献 [15–17] 都是采用两束光叠加的方法对单幅图像做偏振加密, 光路繁琐, 不简便, 而且只能对一幅图像加密. 在本文中, 我们基于 Q-plate, 用一束光对两幅图像做非对称偏振加密. 不仅光路简单, 还能够对两幅图像同时加密. 另外, 利用 Q-plate 能够调控每个像素点的偏振态, 从而增强密钥的敏感性, 提高算法的安全性. 在该方法中, 首先, 将待加密的两幅图像通过干涉分解成两块纯相位板; 其次, 将这两块纯相位板编码到偏振光的两个正交分量当中; 最后, 利用 Q-plate 和像素化的偏振片改变这束光的偏振分布, 用 CCD 接收输出面的强度分布图作为最终的密文. 由于解密密钥和加密密钥不同, 因此实现了非对称加密, 提高了算法的安全性.

2 原 理

2.1 非对称偏振加密原理

Q-plate 是由石英玻璃中自组装纳米结构的飞秒激光制造的具有局部变化光轴的人造单轴晶体[21]. 它的局部光轴的取向平行并垂直于子波长槽, 其结构图如图 1 所示. 局部光轴的方向可以表示为

$$\alpha(r,\varphi)=q\varphi+\alpha_0, \tag{1}$$

其中 (r,φ) 表示极坐标, α_0 表示 $\varphi=0$ 时光轴的角度, q 为描述变面结构空间旋转率的常数.

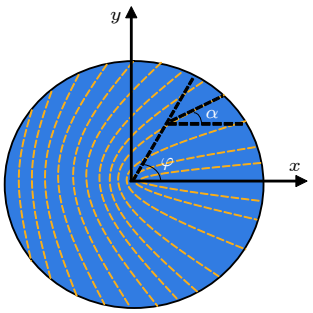

图 1 当 q 为 0.5 时的结构化示意图 ((x, y) 代表笛卡尔坐标, 黄色虚线代表子波长槽, α 表示局部光轴的方向)

Fig. 1. Structural diagram when q is 0.5 ((x, y) represents Cartesian coordinates; yellow dashed line represents sub-wavelength scale; α represents local optical axes).

假设输入光场为 $E_{\rm in}(r,\varphi)$, 通过 Q-plate 后, 输出光场可表示为 $E_{\rm out}(r,\varphi)=\boldsymbol{T}(r,\varphi)E_{\rm in}(r,\varphi)$, 其中 $\boldsymbol{T}(r,\varphi)$ 可用琼斯矩阵表示[22,23]:

$$\boldsymbol{T}(r,\varphi)=\mathrm{i}\begin{bmatrix}\cos(2\alpha) & \sin(2\alpha)\\ \sin(2\alpha) & -\cos(2\alpha)\end{bmatrix}, \tag{2}$$

这里假设 $\alpha_0=0$.

假设输入光场的偏振态为线偏振态, 用琼斯矩阵可表示为 $\boldsymbol{E}_{\rm in}(r,\varphi)=\begin{bmatrix}\cos\theta & \sin\theta\end{bmatrix}$. 根据 (2) 式中 Q-plate 的琼斯矩阵表达式, 输出光场 (琼斯矩阵表示) 可由下式计算:

$$\boldsymbol{E}^{\rm II}_{\rm out}(r,\varphi)=\begin{bmatrix}\cos(2q\varphi-\theta)\\ \sin(2q\varphi-\theta)\end{bmatrix}. \tag{3}$$

(3) 式中的偏振态可以看作矢量偏振[24], 这意味着可以利用 Q-plate 来改变输入光场的空间偏振态, 出现这种现象是因为当光束通过 Q-plate 时有自旋相关的几何相位出现[25,26]. 因此, 可以使用Q-plate 有效地改变输入光场的偏振态, 生成任意矢量光束.

下面介绍基于 Q-plate 的双图像加密过程. 输入平面的原始偏振态分布可以用两个正交的线偏振分布来表示, 这种偏振状态可以通过使用一个偏振片转换成强度分布来获得. 首先, 按照 Zhang 和 Wang[27]提出的基于干涉的光学图像加密方法将两幅图像分解成两个纯相位板, 然后 把两个纯相位板编码到椭圆偏振光的两个正交分量里, 将其中一个纯相位板作为解密密钥. 所以, 加密首先要做的就是把两幅图像分解成两个纯相位函数 φ_1 和 φ_2. 我们用 I_0 和 I_1 分别表示待加密图像 1 和待加密图像 2. 建立运算:

$$I' = \mathrm{FT}\left\{\sqrt{I_0}\cdot\exp\left[\mathrm{i}2\pi I_1\right]\right\}, \tag{4}$$

这里 FT{} 表示傅里叶变换, I_0 表示待加密图像 1, I_1 表示待加密图像 2. 因此复光场 I' 可以分解为两个纯相位分布 φ_1 和 φ_2 的干涉:

$$I' = \exp\left(\mathrm{i}\varphi_1\right) + \exp\left(\mathrm{i}\varphi_2\right). \tag{5}$$

由于 φ_1 和 φ_2 都是纯相位函数, 可以得到

$$\begin{aligned}&\left|\exp\left(\mathrm{i}\varphi_1\right)\right|^2\\ &= \left|I' - \exp\left(\mathrm{i}\varphi_2\right)\right|^2\\ &= \left|I' - \exp\left(\mathrm{i}\varphi_2\right)\right|\left|I' - \exp\left(\mathrm{i}\varphi_2\right)\right|^* = 1.\end{aligned} \tag{6}$$

经化简后, 可以得到这两个纯相位函数:

$$\varphi_1 = \arg\left(I'\right) - \arccos\left[\mathrm{abs}\left(I'\right)/2\right] + K_1\cdot 2\pi, \tag{7}$$

$$\varphi_2 = \arg\left[I' - \exp\left(\mathrm{i}\varphi_1\right)\right] + K_2\cdot 2\pi, \tag{8}$$

这里 arg() 和 abs() 分别表示取相位和振幅, K_1 和 K_2 都是整数. 由于振幅值都是大于零的, 所以 $K_1 \geqslant 1$, $K_2 \geqslant 1$. 本文中, 令 K_1=$K_2 = 2$. 这样, 就可以计算得到 φ_1 和 φ_2, 并且通过光学系统将它们编码到椭圆偏振光的两个正交分量中. φ_2 作为解密密钥.

图 2 所示为双图像非对称偏振加密的全过程. 使用波长为 671 nm 的单模固态激光器来产生高斯光束. 高斯光束经过 4f 系统扩束后, 再通过偏振片将其转化为水平线偏振光. 首先, 通过振幅型的空间光调制器 (spatial light modulator, SLM) 对该光束进行振幅调制; 随后, 通过 Q-plate 对其进行偏振态调制; 接着, 通过像素化的偏振片对其偏振态进行筛选; 最后, 通过 CCD 来记录调制后的高斯光的光强信息. 这样一来, 便得到了所需要的密文. 其中, SLM 上所加载的图像 A 的灰度分布为[18]

$$A = \sqrt{\varphi_1^2 + \varphi_2^2}. \tag{9}$$

光束经过 SLM 后, 通过 Q-plate 调制, 输出面

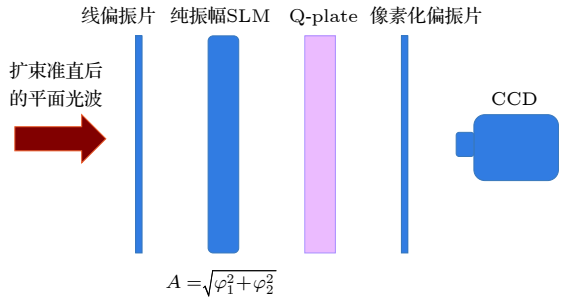

图 2 加密流程图

Fig. 2. Flowcharts of encryption.

的 Jones 矩阵可以表示为

$$\begin{aligned}\boldsymbol{E}_{\mathrm{out1}} &= \begin{bmatrix}\cos(2\alpha) & \sin(2\alpha)\\ \sin(2\alpha) & -\cos(2\alpha)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} * \boldsymbol{A}\\ &= \begin{bmatrix}\cos(2q\varphi) & \sin(2q\varphi)\\ \sin(2q\varphi) & -\cos(2q\varphi)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} * \boldsymbol{A}.\end{aligned} \tag{10}$$

然后, 再经过一个像素化的偏振片 $\theta_{\mathrm{rand}}^{(u,v)}$ 编码[15], 这个像素化偏振片 $\theta_{\mathrm{rand}}^{(u,v)}$ 的每个像素的偏振角度都随机均匀分布在 $[-\pi,\pi)$ 上. 那么输出面的 Jones 矩阵变为

$$\begin{aligned}\boldsymbol{E}_{\mathrm{out}} =& \begin{bmatrix}\cos^2\theta_{\mathrm{rand}}^{(u,v)} & \dfrac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)})\\ \dfrac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)}) & \sin^2\theta_{\mathrm{rand}}^{(u,v)}\end{bmatrix}\\ &\times\begin{bmatrix}\cos(2q\varphi) & \sin(2q\varphi)\\ \sin(2q\varphi) & -\cos(2q\varphi)\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} * \boldsymbol{A}.\end{aligned} \tag{11}$$

最后, 在 CCD 上采集到的光强 I 为

$$\begin{aligned}I =& A^2\left(\cos^2\theta_{\mathrm{rand}}^{(u,v)}\cos(2q\varphi) + \frac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)})\sin(2q\varphi)\right)^2\\ &+A^2\left(\frac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)})\cos(2q\varphi)+\sin^2\theta_{\mathrm{rand}}^{(u,v)}\sin(2q\varphi)\right)^2,\end{aligned} \tag{12}$$

其中 q 作为加密密钥 1, $\theta_{\mathrm{rand}}^{(u,v)}$ 作为加密密钥 2, φ_2 作为解密密钥. 这三个密钥任何一个出错, 解密时都不能得到原始图像, 这就是加密的全过程. 这里, 我们使用 Q-plate 是为了改变振幅 A 的偏振态. 用像素化偏振片筛选偏振态从而起到改变光强的作用.

2.2 非对称偏振解密原理

已知加密密钥 $\theta_{\mathrm{rand}}^{(u,v)}$ 和加密密钥 q, 解密过程可以通过数值计算的方式进行, 对公式 (12) 进行逆推, 可以得到

$$\begin{aligned}A'^2 =& \frac{I}{\left(\cos^2\theta_{\mathrm{rand}}^{(u,v)}\cos(2q\varphi)+\frac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)})\sin(2q\varphi)\right)^2}\\ &+\frac{I}{\left(\frac{1}{2}\sin(2\theta_{\mathrm{rand}}^{(u,v)})\cos(2q\varphi)+\sin^2\theta_{\mathrm{rand}}^{(u,v)}\sin(2q\varphi)\right)^2}.\end{aligned} \tag{13}$$

已知解密密钥 φ_2, 由 (9) 式可以获得 φ_1:

$$\varphi_1 = \sqrt{A'^2 - \varphi_2^2}. \tag{14}$$

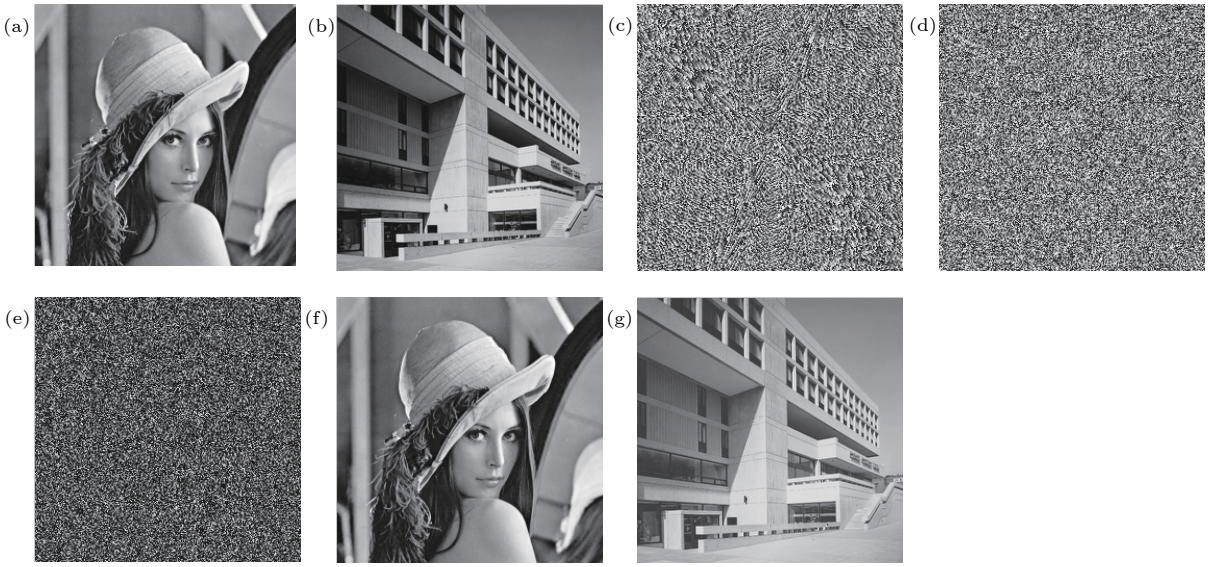

图 3 加密算法的模拟结果 (a), (b) 原图 1 和原图 2; (c) 密文图像; (d) 加密密钥 $\theta_{\text{rand}}^{(u,v)}$; (e) 解密密钥 φ_2; (f), (g) 解密得到的两幅图像

Fig. 3. Simulation result of encryption algorithm: (a), (b) Original image of Lena and library; (c) ciphertext image; (d) encryption key $\theta_{\text{rand}}^{(u,v)}$; (e) decryption key; (f), (g) decrypted image.

最后, 通过 φ_1 和 φ_2 解密获得原始图像 1 和原始图像 2:

$$I_1' = \left|\text{FT}^{-1}\left\{\exp\left(\text{i}\varphi_1\right) + \exp\left(\text{i}\varphi_2\right)\right\}\right|^2, \tag{15}$$

$$I_2' = \text{angle}\left(\text{FT}^{-1}\left\{\exp\left(\text{i}\varphi_1\right) + \exp\left(\text{i}\varphi_2\right)\right\}\right)^2, \tag{16}$$

其中 $\text{FT}^{-1}\{\}$ 表示逆傅里叶变换, $\text{angle}()$ 表示振幅截断.

3 仿真模拟结果及安全性分析

我们使用 MATLAB 2014 版本对所提出的方案进行计算机仿真模拟. 在本文中, 使用的待加密的两幅图像如图 3(a) 和图 3(b) 所示, 像素大小为 256×256, 加密密钥 $\theta_{\text{rand}}^{(u,v)}$ 取 $[-\pi, \pi)$ 上的任意值, q 取 2, 加密结果如图 3(c) 所示. 对比原始图像可以发现, 加密图像已经无法识别原始图像的任何信息, 加密效果较好. 加密密钥 $\theta_{\text{rand}}^{(u,v)}$ 如图 3(d) 所示, 解密密钥 ϕ_2 如图 3(e) 所示; 而解密是加密的逆过程, 解密结果如图 3(f) 和 (g) 所示. 与原始图像相比, 可以清楚地看到解密后图像能够近乎无损地还原原始图像的所有信息, 解密效果较好.

3.1 密钥敏感性分析

对于本文中的偏振加密算法, 它的加密密钥中有两个变量: q 和 $\theta_{\text{rand}}^{(u,v)}$. 为了研究解密时加密密钥错误对解密效果的影响, 分别对加密密钥 q 和加密密钥 $\theta_{\text{rand}}^{(u,v)}$ 的灵敏度进行分析. 当加密密钥 q 和加密密钥 $\theta_{\text{rand}}^{(u,v)}$ 受到干扰时, 其值会在一定范围内浮动, 这个浮动的范围非常小. 假设加密密钥 q 受到一定的干扰, 那么干扰后的 q 可以表示为

$$q' = q + d, \tag{17}$$

其中 q' 和 q 分别表示受干扰后的 q 值和原始的 q 值, d 非常小. 图 4 为 $d = 0.0001$ 时的解密图, 可以看到, 当密钥受到很小的干扰时, 解密图就已经无法识别到任何原始信息. 因此, 加密系统对加密密钥 q 的敏感性非常高, 完全可以抵抗暴力攻击. 当然, 当加密密钥 q 值错误时, 更加不能够解密出原始图像.

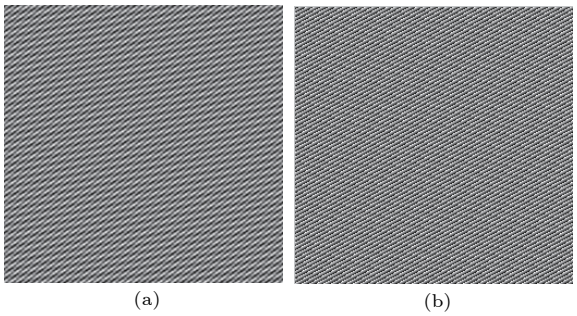

图 4 加密密钥 q 加上 0.0001 时的解密图像 (a) 解密图像 1; (b) 解密图像 2

Fig. 4. Decrypted image when the encryption key q is added with 0.0001: (a) Decrypted image 1; (b) decrypted image 2.

同理, 对加密密钥$\theta_{\text{rand}}^{(u,v)}$的灵敏度进行测试, 当它的值在一定范围内浮动时, 我们将其表示为

$$\theta' = \theta + d\theta, \tag{18}$$

其中d为系数, 其值分布在$(-1,1)$上. 图 5 给出了$d = 0.0001$时的解密图. 可以发现解密图看不到原始图像的任何信息, 这说明加密系统对加密密钥$\theta_{\text{rand}}^{(u,v)}$的敏感性也很高, 能够抵抗暴力攻击.

综合以上模拟分析可见, 本文的加密密钥的敏感性很高, 能够很好地抵抗暴力攻击. 解密时加密密钥错误不能得到原始图像的任何信息.

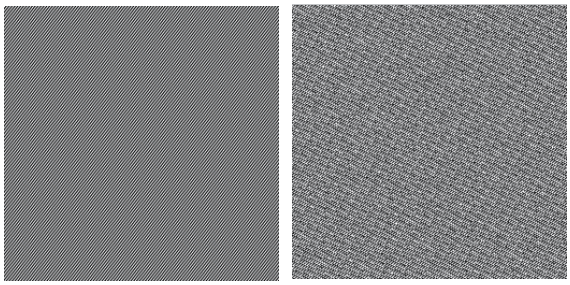

图 5 加密密钥θ增加了 0.0001 倍后的解密图像 (a) 解密图像 1; (b) 解密图像 2

Fig. 5. Decrypted image when the encryption key$\theta$is add with 0.0001 times: (a) Decrypted image 1; (b) decrypted image 2.

3.2 抗剪切攻击分析

在现实生活中, 密文在传输过程中可能会遇到各种问题, 有时会丢失密文图的部分信息, 在这种情况下, 仍然希望能够解密出原始图像. 所以, 我们将密文的某些像素值置 0, 测试加密系统的抗剪切能力. 图 6(a) 模拟的是密文信息丢失 6.25% 时, 使用解密密钥做非对称偏振解密. 从图 6(b) 和 (c) 可以看出, 解密可以得到原始图像的大部分信息, 但只是灰度值略有下降. 图 6(d) 模拟的是密文信息丢失 25% 时, 使用解密密钥做非对称偏振解密. 从图 6(e) 和 (f) 可以看出, 解密仍可以看到明文的主要特征, 说明加密系统有较高的抗剪切能力.

3.3 抗噪声攻击分析

在现实生活中, 实际条件及环境可能会对算法有干扰. 因此, 我们在密文中掺杂了噪声, 测试能否解密出原文. 在这个过程中, 我们假设加密的结果在实际环境中受到噪声的干扰, 对密文模拟添加了均值为 0, 方差为 1 的高斯随机噪声 N, 噪声干扰密文的方式为

$$e = I\left(1 + kN\right), \tag{19}$$

其中I和e分别为原始密文和受到干扰后的密文, k为噪声强度系数. 我们用相关系数 (correlation coefficient, CC) 来评估解密图像的质量,

$$\mathrm{CC} = \frac{E\left\{\left(f - E\left(f\right)\right)\left(f' - E\left(f'\right)\right)\right\}}{\sqrt{E\left\{\left(f - E\left(f\right)\right)^2\right\}}\sqrt{E\left\{\left(f' - E\left(f'\right)\right)^2\right\}}}, \tag{20}$$

其中$f\left(x,y\right)$代表原始图像, $f'\left(x,y\right)$代表解密后的图像, $E\left(\cdot\right)$代表期望值.

图 7 给出了相关系数值随噪声强度系数k变

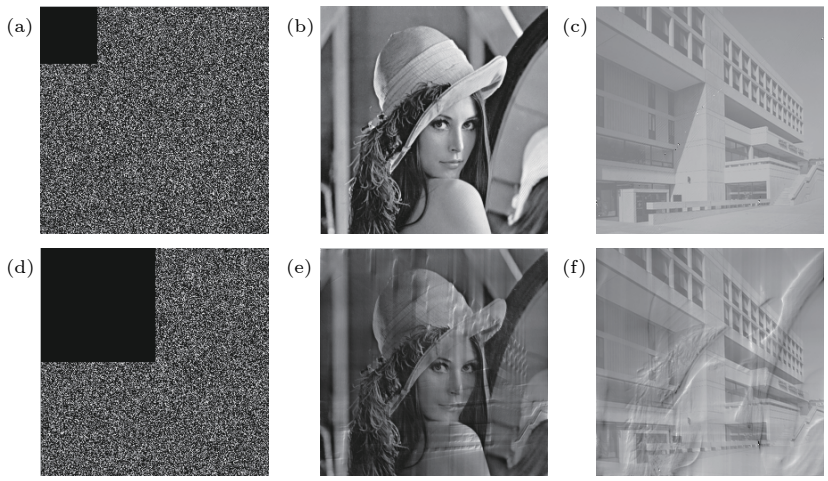

图 6 抗剪切攻击模拟结果图 (a) 信息丢失 6.25% 的密文图; (b), (c) 密文信息丢失 6.25% 后的解密图; (d) 信息丢失 25% 的密文图; (e), (f) 密文信息丢失 25% 的解密图

Fig. 6. Simulation t diagram of anti-shear attack: (a) Ciphertext with 6.25% occlusion; (b), (c) decrypted images from (a); (d) 25% occlusion; (e), (f) decrypted images from (d).

化的曲线图以及当噪声强度系数为 0.02 和 0.06 时得到的解密图, 其中图 7(a) 是解密得到的原始图像 1, 图 7(b) 是解密得到的原始图像 2. 从图 7 可以看出, 当噪声强度系数为 0.06 时, 仍可以辨别出原始图像的信息, 因此, 该算法具有一定的抗噪攻击能力. 也就是说在实际条件和环境中, 该算法具有很好的适应性, 即便受到一些干扰, 也能完成加解密.

3.4 传统偏振加密和使用 Q-plate 做偏振加密的比较

传统偏振加密是用波片通过两束光的叠加对单幅图像做偏振加密, 它的其中一个加密密钥是波片的角度, 密钥的敏感性不高. 本文基于 Q-plate, 用一束光对两幅图像做偏振加密, 其中一个加密密钥是 q 值. 本文中对传统偏振加密和使用 Q-plate 做偏振加密就加密密钥的敏感性和密文抗剪切攻击这两方面做了比较. 首先, 分别将传统偏振加密的加密密钥 (波片的角度) 和 Q-plate 的 q 值各改变万分之一, 用改变后的加密密钥做解密模拟. 模拟结果如图 8 所示. 图 8(a) 表示传统的用波片做偏振加密, 波片的角度改变万分之一后的解密图. 从图 8(a) 中可以看出, 解密图已经能够清晰地看到原图的信息, 所以加密密钥的敏感性并不是很好. 图 8(b) 和 (c) 是使用 Q-plate 做偏振加密, q 值改变万分之一后的解密图, 从中并不能看到原图的信息, 加密密钥的敏感性很高.

其次, 分别对使用 Q-plate 做偏振加密以及传统偏振加密的密文做了抗剪切攻击的测试. 模拟结果如图 9 所示. 图 9(a), (b), (c) 分别表示用 Q-plate 做偏振加密信息丢失 6.25% 的密文和解密图. 从图 9 可以看出, 解密得到的结果能够看出原始图像的信息, 这说明, 使用 Q-plate 做偏振加密具有很好的抗剪切攻击. 图 9(d) 和 (e) 分别表示传统偏振加密信息丢失 6.25% 的密文和解密图. 显然, 就抗

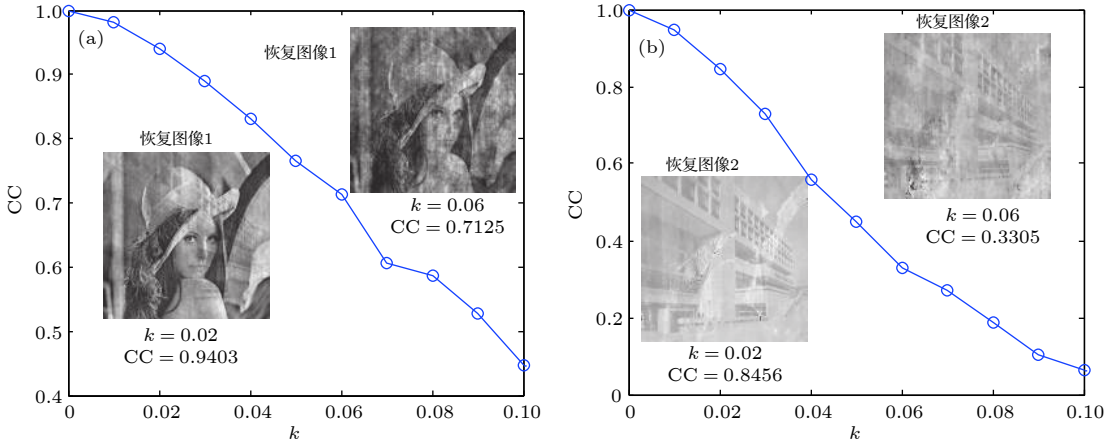

图 7 抗噪声攻击模拟图 (a) 第一幅解密图的相关系数 CC 随 k 变化的曲线图及 $k = 0.02, 0.06$ 时的解密图; (b) 第二幅解密图的相关系数 CC 随 k 变化的曲线图及 $k = 0.02, 0.06$ 时的解密图

Fig. 7. Simulation diagram of anti-noise attack: (a) CC curve of noise attack including decrypted the first image obtained with $k = 0.02, 0.06$; (b) CC curve of noise attack including decrypted the second image obtained with $k = 0.02, 0.06$.

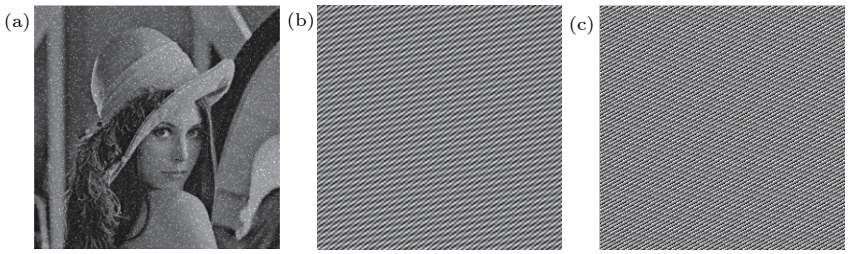

图 8 传统偏振加密和使用 Q-plate 做偏振加密比较 (a) 传统用波片做偏振加密, 加密密钥波片角度改变万分之一后的解密图; (b), (c) 用 Q-plate 做偏振加密, 密钥 q 值改变万分之一后的解密图

Fig. 8. Traditional polarization encryption compared with polarization encryption utilizing a q-plate: (a) Decryption image of traditional polarization encryption employing wave plates with the angle changed by 1/10000; (b), (c) decryption image of polarization encryption employing a Q-plate with the parameter q changed by 1/10000.

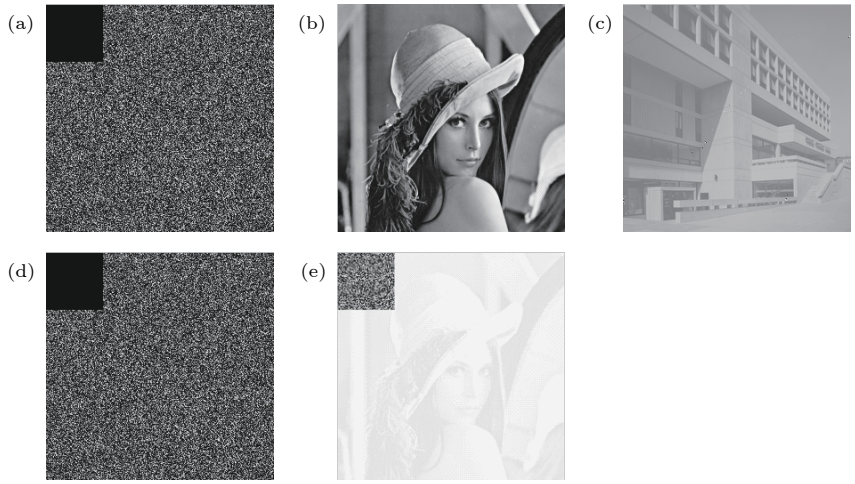

图 9 使用 Q-plate 做偏振加密和传统偏振加密比较 (a) 用 Q-plate 做偏振加密, 信息丢失 6.25% 的密文图; (b), (c) 用 Q-plate 做偏振加密, 密文信息丢失 6.25% 的解密图; (d) 传统偏振加密, 信息丢失 6.25% 的密文图; (e) 传统偏振加密, 信息丢失 6.25% 的解密图

Fig. 9. Polarization encryption utilizing a q-plate compared with traditional polarization encryption: (a) Ciphertext with 6.25% occlusion of polarization encryption employing a Q-plate; (b), (c) decrypted image from (a); (d) ciphertext with 6.25% occlusion of traditional polarization encryption; (e) decrypted image from (d).

剪切攻击方面而言, 使用 Q-plate 做偏振加密要比使用波片做偏振加密抗剪切效果好.

4 结 论

本文基于 Q-plate, 对两幅图像做非对称偏振加密. 首先, 将待加密的两幅图像通过干涉光分解成两块纯相位板; 其次, 将这两块纯相位板分别编码到偏振光的两个正交分量当中; 最后, 利用 Q-plate 和像素化的偏振片改变这束光的偏振分布, 达到对图像的加密效果, 用 CCD 接收输出面的强度分布图作为最终的密文. 其中一块纯相位板作为解密密钥, Q-plate 的 q 值作为第一个加密密钥, 像素化的偏振片的偏振角度作为第二个加密密钥. 由于解密密钥不同于加密密钥, 攻击者无法使用加密密钥进行解密. 另外, 这两个加密密钥具有很高的敏感性, 增大了加密系统的安全性. 解密时任何一个密钥错误都不能得到最后的解密图像. 仿真模拟证明了该加密方法能够很好地抵抗暴力攻击、剪切攻击以及噪声攻击.

参考文献

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Deng X P, Zhao D M 2012 *Opt. Laser Technol.* **44** 136
[3] Abuturab M R 2015 *Opt. Lasers Eng.* **69** 49
[4] Liu Z J, Guo C, Tan J B, Liu W, Wu J J, Wu Q, Pan L Q, Liu S T 2015 *Opt. Lasers Eng.* **68** 87
[5] Sui L S, Xin M T, Tian A L, Jin H Y 2013 *Opt. Lasers Eng.* **51** 1297
[6] Chen W, Chen X 2012 *Appl. Opt.* **51** 6076
[7] Rajput S K, Nishchal N K 2013 *Appl. Opt.* **52** 4343
[8] Qin W, Peng X 2010 *Opt. Lett.* **35** 118
[9] Chen W, Chen X D 2011 *Opt. Commun.* **284** 3913
[10] Rajput S K, Nishchal N K 2012 *Appl. Opt.* **51** 1446
[11] Liu W, Liu Z J, Liu S T 2013 *Opt. Lett.* **38** 1651
[12] Wang X G, Zhao D M 2012 *Opt. Commun.* **285** 1078
[13] Rajput S K, Nishchal N K 2013 *Appl. Opt.* **52** 871
[14] Wang X G, Chen Y X, Dai C Q, Zhao D M 2013 *Appl. Opt.* **53** 208
[15] Alfalou A, Brosseau C 2010 *Opt. Lett.* **35** 2185
[16] Rajput S K, Nishchal N K 2012 *Appl. Opt.* **51** 5377
[17] Wang Q, Guo Q, Zhou J Y 2013 *Appl. Opt.* **52** 8854
[18] Cai J J, Shen X J, Lei M 2017 *Opt. Commun.* **403** 211
[19] Wang Q, Xiong D, Alfalou A, Brosseau C 2018 *Opt. Commun.* **415** 56
[20] Fatima A, Nishchal N K 2018 *Opt. Commun.* **417** 30
[21] Zhou J X, Liu Y C, Ke Y G, Luo H L, Wen S C 2015 *Opt. Lett.* **40** 3193
[22] Marrucci L, Manzo C, Paparo D 2006 *Rev. Lett.* **96** 163905
[23] Yi X N, Ling X H, Zhang Z Y, Li Y, Zhou X X, Liu Y C, Chen S Z, Luo H L, Wen S C 2014 *Opt. Express* **22** 17207
[24] Zhan Q W 2009 *Adv. Opt. Photonics* **1** 1
[25] Hasman E, Kleiner V, Biener G, Niv A 2003 *Appl. Phys. Lett.* **82** 328
[26] Niv A, Biener G, Kleiner V, Hasman E 2005 *Opt. Lett.* **30** 2933
[27] Zhang Y, Wang B 2008 *Opt. Lett.* **33** 2443

Q-plate based dual image asymmetric polarization encryption*

Xu Qi-Jun Li De-Lin Chang Chen-Liang Yuan Cao-Jin
Feng Shao-Tong Nie Shou-Ping †

(*Key Laboratory for Opto-Electronic Technology of Jiangsu Province*, *Nanjing Normal University*, *Nanjing* 210023, *China*)

(Received 25 October 2018; revised manuscript received 11 January 2019)

Abstract

With the rapid development of computer network technology, information security has drawn considerable attention in recent years. Owing to the characteristics of multi-dimensional operation and parallel processing capability, optical image encryption techniques are arousing great interest in many exciting fields. Since the pioneering work on optical image encryption using double random phase encoding technique, a large number of algorithms and architectures have been proposed and realized. However, with the further analysis of the securities of these schemes, most of them have been verified to be vulnerable to different types of attack algorithms. Recently, optical encryption schemes based on the polarization properties of light wave have been extensively studied, for an additional flexibility in the encryption key design is provided, which can achieve high robustness against brute force attack by a combination of multiple private keys. Nevertheless, optical encryption schemes based on the polarization properties of light wave could still be vulnerable to known- and chosen- plaintext attacks. Therefore, in this paper, a novel asymmetric polarization encryption method is implemented for dual images, and combined with interference-based optical image encryption method and a Q-plate. First, the information about the two images to be encrypted is separated into two pure phase plates by means of interference optical image encryption, which will be further encoded into two mutually orthogonally polarized light beams. Next, the Q-plate and pixelated polarizer are used for realizing different polarization distributions of the two light beam. Ultimately, the output intensity distribution is recorded by a charge coupled device (CCD) which will be treated as the final ciphertext. For actualizing the asymmetric encryption, one of the pure phase plates acts as a decryption key, which is different from the encryption key. We can control the polarization state of each pixel according to the parameter q, causing the Q-plate to be electrically controllable and the optic-axis orientation of each pixel to differ from one another. It should be emphasized that the value of q and the polarization angle of the pixelated polarizer play the role of two encryption keys, which improves the security of the algorithm extremely, due to their high sensitiveness. Theoretical analyses and numerical simulations verify the feasibility and effectiveness of the proposed encryption scheme.

Keywords: Q-plate, asymmetric encryption, polarization

PACS: 42.30.–d, 42.25.Ja, 42.30.Va **DOI:** 10.7498/aps.68.20181902

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61775097, 11574152, 61605080), the National Key Research and Development Program of China (Grant No. 2017YFB0503505), the Open Foundation of Key Lab of Virtual Geographic Environment (Nanjing Normal University), Ministry of Education of China (Grant No. 2017VGE02), and the Postgraduate Research and Practice Innovation Program of Jiangsu Province, China (Grant No. SJCX17_0336).

† Corresponding author. E-mail: nieshouping@njnu.edu.cn