第 43 卷 第 9 期/2023 年 5 月/光学学报 研究论文

光学学报

级联双相位密码系统中基于位置复用的双图像加密

秦怡[1,2]，万玉红[1*]，巩琼[2]

[1]北京工业大学理学部，北京 100124；

[2]南阳师范学院机电工程学院，河南 南阳 473061

摘要 级联双相位密码(CDPE)系统是一种包含两个纯相位板(密文板和密钥板)的重要光学密码系统，为了提升该系统的加密效率，提出一种双图像加密方法。加密时，将密钥板的轴向距离作为控制参数，提出一种新的迭代加密算法，该算法可将两幅明文图像加密至同一个密文板中，将传统的CDPE系统的加密效率提升了1倍。解密时，当密钥板分别处于两个设定的轴向位置时，可以在输出平面得到两幅不同的明文图像。采用数值仿真和实验验证了所提方法的有效性，并研究了密钥板两个位置之间的距离对解密结果的影响。对所提方法安全性的分析表明，所提方法对于暴力破解和选择明文攻击均具有稳健性。此外，所提方法可方便地推广至多图像加密，因此CDPE系统的加密效率可以得到进一步提升。

关键词 图像处理；光学信息安全；双图像加密；位置复用；迭代加密算法

中图分类号 O438 **文献标志码** A **DOI**：10.3788/AOS221800

1 引 言

自1995年Refregier与Javidi[1]提出双随机相位编码(DRPE)系统以来，光学信息安全技术一直是信息光学领域的研究热点[2-9]。与传统的数字或电子密码系统相比，光学密码系统有一些独特的优势[10]：1)光波天然地具备并行处理二维(图像)信息的能力，而且在理想情况下，这种并行处理以光速进行；2)光波具有多种自由度，包括波长、振幅、相位、偏振等，这些参量在光学密码系统中几乎都可以用作密钥使用，因此光学密码系统容易形成较大的密钥空间，从而具有较强的抗暴力破解能力。在DRPE系统被提出之后，人们陆续提出了多种光学密码系统。Nomura等[11]提出了基于联合变换相关器(JTC)的光学密码系统，相比于DRPE系统，该系统降低了各个组件的光学对准要求，更加容易实现。Chen等[12]提出了光学衍射成像加密(DIBE)系统，与DRPE系统相比，DIBE系统的密文不是复数而是强度分布，可以直接利用CCD等强度敏感器件对其进行记录，因而省去了复杂的干涉记录装置。

根据加密和解密方式，光学密码系统可以粗略地分为三种类型：1)光学加密，光学解密；2)光学加密，计算解密；3)计算加密，光学解密。其中DRPE和JTC系统属于第一种类型，而DIBE系统属于第二种类型。前两种类型的系统加密结果(密文)往往为复振幅或强度分布，这些密文中的振幅信息特别容易被强度敏感器件(如人眼或者CCD)所感知甚至拷贝，具有潜在的安全隐患[13-14]。相比之下，纯相位信息则不容易被感知或者测量，例如由衍射光学元件(DOE)制造的纯相位板，其外观与普通玻璃无异[13]，特别适合于信息的加密或隐藏。因此，在第三种类型的光学密码系统中，人们尤其关注如何将明文隐藏于单个或多个纯相位板中[13-17]。级联双相位密码(CDPE)系统就是该类型的代表。CDPE系统最早由Wang等[18]提出，他们在光学4*F*系统的输入面和输出面分别放置一个纯相位板，其中充当密钥的相位板位于输入面，该相位板的相位值完全随机，而充当密文角色的相位板位于频谱面，其相位值由相位恢复算法计算得到。利用单色平行光照射该系统，就可以在输出面得到解密图像。Li等[19]将两个相位板的位置进行调换，详细论证了CDPE系统更多潜在的用途。之后，人们进一步对该系统进行了改进，Situ等[20]利用相位恢复算法生成两个相位板，将CDPE系统改造为图像隐藏系统，他们去掉了该系统中用于傅里叶变换的透镜，极大地降低了系统的硬件要求[21]。近年来，人们开始在CDPE系统中探索图像压缩加密(多图像加密)的方法。Lü等[22]将两个相位板的旋转角度作为自由度，利用角度复用实现了多图像加密。同样是利用旋转角度复用，

收稿日期：2022-10-09；**修回日期**：2022-11-02；**录用日期**：2022-11-25；**网络首发日期**：2023-01-04

基金项目：国家自然科学基金(61575009，61505091)、北京市自然科学基金(4182016)

通信作者：*yhongw@bjut.edu.cn

Lu等[23]在CDPE系统中提出了一种基于相位板部分更新的相位恢复算法，一定程度上提升了系统的加密容量。上述有关CDPE系统的研究都使用了数值仿真方法，未能给出直接或间接的实验结果，这也是目前CDPE系统研究中亟待解决的问题。

本文将CDPE系统中密钥板的位置作为控制参数，提出一种基于位置复用的双图像加密方法。通过所设计的迭代加密算法，可以将两幅明文图像加密至一个纯相位板（密文板）中。解密时，在其他参数不变的情况下，将密钥板置于两个设定的轴向位置时，在输出面会分别得到两幅不同的明文图像。与传统的CDPE只能加密单幅图像相比，所提方法将加密效率提升了1倍。采用数值仿真和实验证实了所提方法的有效性，分析了所提方法的密钥空间、距离复用条件以及推广到多图像加密的可行性，并证实了所提方法对选择明文攻击具有稳健性。

2　基本原理

2.1　解密原理

所提出的基于距离复用的双图像加密方法的解密方案如图1所示。图1(a)所示为第1幅明文图像的解密系统（一种典型的CDPE系统），该系统主要由两个级联的纯相位板构成，即密文板（CM）与密钥板（KM）。密钥板的相位值完全随机且均匀地分布于$[0, 2\pi]$区间，在加密不同明文的过程中其值不变；密文板则由明文、密钥以及一些附加参数（包括波长、轴向距离等）经加密算法生成。整个系统涉及3个重要平面：输入面、密钥面、输出面。密文位于输入面，密钥位于密钥面，二者之间的距离为d_1；输出面到密钥面的距离为d_2。当采用加密时所设定的具有特定波长的单色平行光照射输入面时，明文图像“BJUT”就在输出面显示出来，可以利用CCD等强度敏感器件对其进行直接记录。将密钥板沿着光轴向输出面移动Δd的距离，则输出平面上将解密得到第2幅明文图像“NYNU”，如图1(b)所示，此时密钥板距离密文板以及输出面的距离分别为d_3和d_4。在密钥板移动的过程中，要求密文板与输出面的位置保持不变，即$d_1+d_2=d_3+d_4$。在所提方法中，用来区分两幅图像的唯一参数是密钥板的轴向位置，因此称之为位置复用。

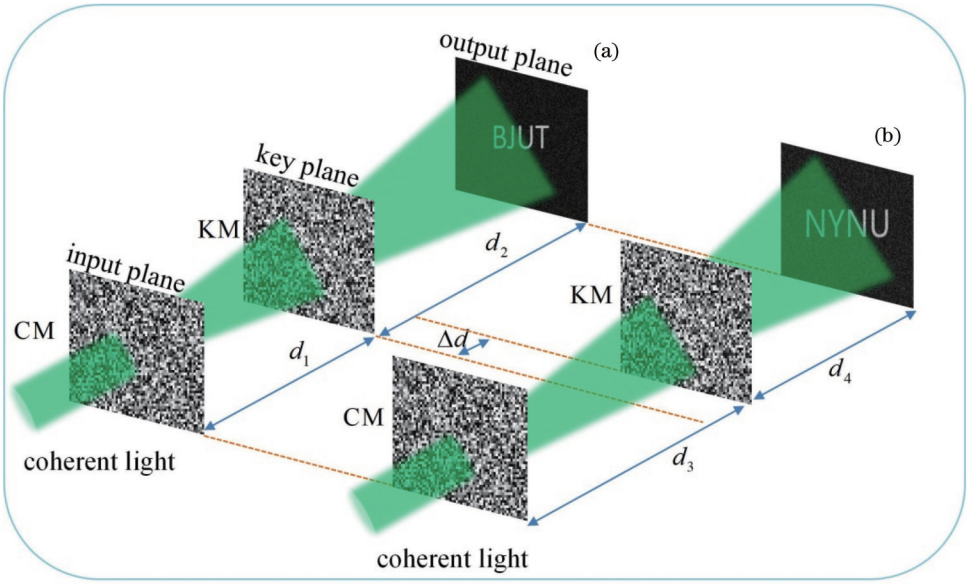

图1　CDPE系统中基于位置复用的双图像加密方法的解密方案。(a)第1幅明文图像的解密原理；(b)第2幅明文图像的解密原理

Fig. 1　Decryption principle of position-multiplexing-based double-image encryption in CDPE. (a) Decryption of plaintext image 1; (b) decryption of plaintext image 2

2.2　加密算法

根据图1所示的解密过程，所提加密算法的流程如下：假设两幅待加密的明文图像分别为$P_1(x,y)$与$P_2(x,y)$，且输入面、密钥面以及输出面的坐标分别为(ξ,η)、(μ,ν)、(x,y)。首先，给密文板赋予一个随机的初始值$C_{\mathrm{M}}^{(n)}(\xi,\eta)$，$n=1$，其中，$n$为循环轮数。每轮循环均需在图1(a)与图1(b)所示的光路中分别完成一次往复迭代，且两光路中密文板的迭代初始值均为$C_{\mathrm{M}}^{(1)}(\xi,\eta)$。

在图1(a)中，$C_{\mathrm{M}}^{(n)}(\xi,\eta)$经过距离为$d_1$的自由空间衍射至密钥面，被密钥板调制后又经距离为$d_2$的自由空间衍射到达输出面，输出面的复振幅可表示为

$$O_1^{(n)}(x,y)=\mathrm{FrT}_{\lambda}\left\{\mathrm{FrT}_{\lambda}\left[C_{\mathrm{M}}^{(n)}(\xi,\eta);\ d_1\right]K_{\mathrm{M}}(\mu,\nu);\ d_2\right\},\tag{1}$$

式中：$\mathrm{FrT}_{\lambda}[P;\ d]$表示复振幅$P$经过距离为$d$的自由空间衍射的结果；$K_{\mathrm{M}}(\mu,\nu)$为密钥板。令$P_1^{(n)}(x,y)=\left|O_1^{(n)}(x,y)\right|$，则$P_1^{(n)}(x,y)$为第1幅明文图像的估计值。

此时，保留 $O_1^{(n)}(x,y)$ 的相位，并用待加密明文图像 $P_1(x,y)$ 来取代其振幅，得到图 1(a)输出面更新后的复振幅为

$$\bar{O}_1^{(n)}(x,y)=P_1(x,y)O_1^{(n)}(x,y)\Big/\left|O_1^{(n)}(x,y)\right|。\quad(2)$$

之后，将此复振幅逆衍射至输入面，得到图 1(a)中输入面的新的复振幅为

$$I_1^{(n)}(\xi,\eta)=\mathrm{FrT}_\lambda\left\{\mathrm{FrT}_\lambda\left[\bar{O}_1^{(n)}(x,y);-d_2\right]K_\mathrm{M}^*(\mu,\nu);-d_1\right\},\quad(3)$$

式中：$K_\mathrm{M}^*(\mu,\nu)$ 为密钥板的共轭。对于图 1(b)所示的光路而言，$C_\mathrm{M}^{(n)}(\xi,\eta)$ 在输出面上形成的复振幅为

$$O_2^{(n)}(x,y)=\mathrm{FrT}_\lambda\left\{\mathrm{FrT}_\lambda\left[C_\mathrm{M}^{(n)}(\xi,\eta);d_3\right]K_\mathrm{M}(\mu,\nu);d_4\right\}。\quad(4)$$

令 $P_2^{(n)}(x,y)=\left|O_2^{(n)}(x,y)\right|$，则 $P_2^{(n)}(x,y)$ 为第 2 幅明文图像的估计值。此时，保留 $O_2^{(n)}(x,y)$ 的相位，并用明文图像 $P_2(x,y)$ 来取代其振幅，得到图 1(b)输出面更新后的复振幅为

$$\bar{O}_2^{(n)}(x,y)=P_2(x,y)O_2^{(n)}(x,y)\Big/\left|O_2^{(n)}(x,y)\right|,\quad(5)$$

将此复振幅逆衍射至输入面，得到图 1(b)输入面的新的复振幅为

$$I_2^{(n)}(\xi,\eta)=\mathrm{FrT}_\lambda\left\{\mathrm{FrT}_\lambda\left[\bar{O}_2^{(n)}(x,y);-d_4\right]K_\mathrm{M}^*(\mu,\nu);-d_3\right\}。\quad(6)$$

之后，将图 1(a)输入面上的复振幅 $I_1^{(n)}(\xi,\eta)$ 与图 1(b)输入面上的复振幅 $I_2^{(n)}(\xi,\eta)$ 进行融合，得到融合后的输入面复振幅 $I^{(n)}(\xi,\eta)$ 为

$$I^{(n)}(\xi,\eta)=I_1^{(n)}(\xi,\eta)+I_2^{(n)}(\xi,\eta)。\quad(7)$$

此时，将 $I^{(n)}(\xi,\eta)$ 的相位作为密文板的新的估计值，进入下一轮迭代，即

$$C_\mathrm{M}^{(n+1)}(\xi,\eta)=\frac{I^n(\xi,\eta)}{\left|I^n(\xi,\eta)\right|}。\quad(8)$$

式(8)所示的仅保留复振幅相位的操作被称为相位留存(PR)。至此，一轮循环完成。重复由式(1)～(8)所描述的迭代过程，直至满足循环结束条件。由于所提方法同时加密两幅图像，所以在设置循环结束条件时应要求两幅解密图像质量均出现停滞，所采用的误差函数为

$$E_\mathrm{r}(n)=\frac{1}{A}\iint\left[\left|P_1^{(n+1)}(x,y)-P_1^{(n)}(x,y)\right|\right]\mathrm{d}x\mathrm{d}y+\frac{1}{A}\iint\left[\left|P_2^{(n+1)}(x,y)-P_2^{(n)}(x,y)\right|\right]\mathrm{d}x\mathrm{d}y,\quad(9)$$

式中：A 为输出平面的面积。该误差函数实际上是两幅图像相邻两次估计结果的平均绝对误差(MAE)之和[19]。当该误差小于某个事先设定的阈值 δ 时，则迭代停止，否则迭代继续。假设迭代停止时已经完成了 K 次迭代，则将 $C_\mathrm{M}^{(K)}(\xi,\eta)$ 作为最终的密文。上述加密过程可以用图 2 描述。

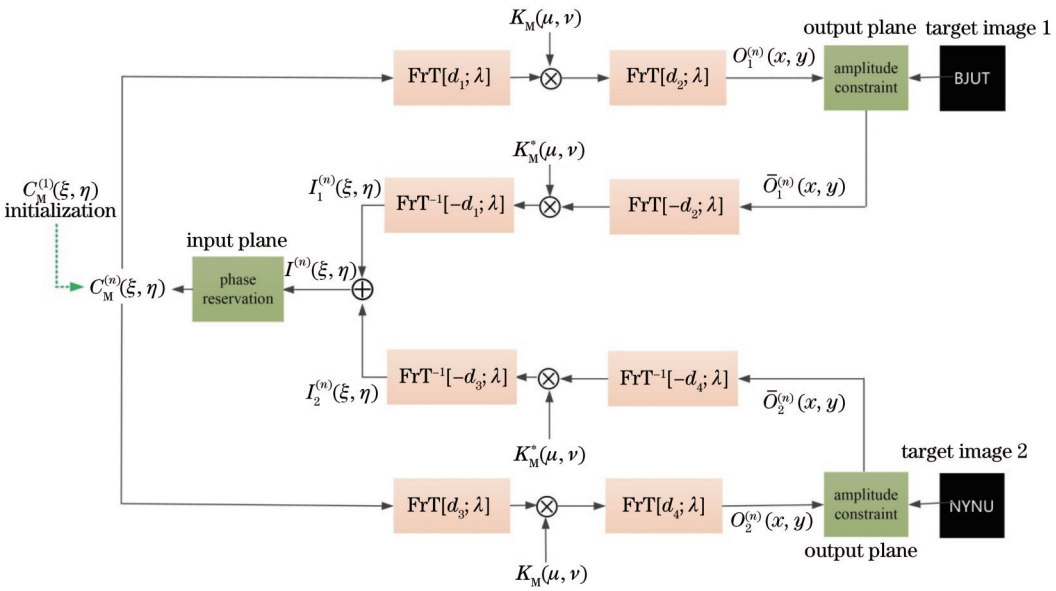

图 2　CDPE 中基于位置复用的双图像加密算法

Fig. 2　Encryption algorithm for position-multiplexing-based double-image encryption in CDPE

3　计算机仿真结果

3.1　有效性验证

首先在计算机上对所提方法的有效性进行了数值仿真研究，所采用的软件平台为 MATLAB R2016a。两幅明文图像如图 3(a)、(b)所示，其尺寸均为 256 pixel×256 pixel，像素尺寸为 6.4 μm。仿真所用的光波波长 $\lambda=532$ nm，所采用的距离参数 d_1 与 d_2 均为 200 mm，d_3 与 d_4 分别为 250 mm 和 150 mm。用于控制加密过程迭代次数的误差阈值 $\delta=0.01$。图 3

(c)给出了所采用的KM，它由MATLAB自带的rand函数生成，由加密算法生成的CM如图3(d)所示。整个加密过程一共进行了248次迭代，误差函数与迭代次数的关系如图3(g)所示。采用图1所示的解密方案进行解密，结果如图3(e)、(f)所示。为了评价解密图像的质量，引入相关系数(C_C)作为评价标准，其定义为

$$C_C=\frac{E\left\{\left[f-E(f)\right]\left[f_r-E(f_r)\right]\right\}}{\sqrt{E\left\{\left[f-E(f)\right]^2\right\}E\left\{\left[f-E(f_r)\right]^2\right\}}},\tag{10}$$

式中：$E(\cdot)$表示求数学期望；f和f_r分别为原始明文图像与解密图像。图3(e)、(f)对应的相关系数分别为0.9012和0.8907，可见明文图像得到了较好的恢复，证明了所提方法的有效性。

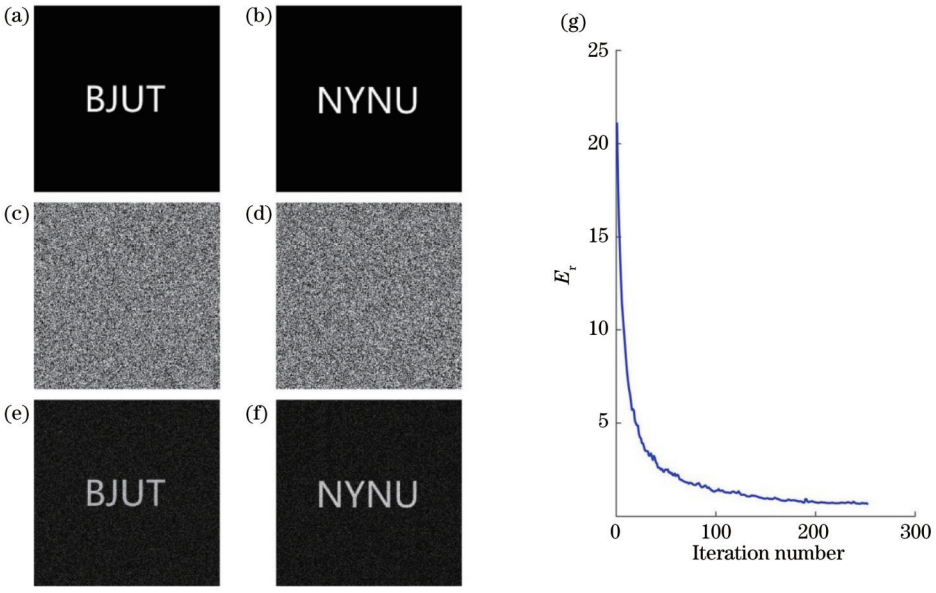

图3　所提方法有效性的数值仿真验证。(a)(b)两幅明文图像；(c)密钥板；(d)密文板；(e)(f)解密得到的两幅明文图像；(g)误差函数与迭代次数的关系

Fig. 3　Numerical demonstration of effectiveness of proposed method. (a)(b) Two plaintext images; (c) KM; (d) CM; (e)(f) two decrypted images; (g) dependence of error function on iteration number

3.2　密钥分析

在本系统中，密钥板、照明波长λ以及轴向距离$d_k(k=1,2,3,4)$均可以作为密钥使用，因此研究解密结果对这些密钥的敏感性非常必要。首先研究了解密结果对于密钥板的敏感性。所提方法中密钥板的尺寸为256 pixel×256 pixel，且像素位深度均为2^3。假设潜在的攻击者采用穷举法来搜索密钥板，图4给出了解密结果的质量(以C_C表示)与密钥板中正确元素比例之间的关系。可以看出，当攻击者猜对密钥板中全部像素的30%时，解密结果可以大致给出明文图像的基本信息。然而，当攻击者仅猜对了其中20%的像素点时，解密图像中的信息就变得难以识别。因此，为了成功实施破解，攻击者必须掌握的正确像素点的数量为$\mathrm{INT}(256\times256\times20\%)=13107$，其中，$\mathrm{INT}(\cdot)$表示取整操作。考虑到像素位深度均为$2^3$，因此由密钥板所创造的密钥空间约为$K_{S,KM}=2^{2^3\times13107}$，这是一个相当大的数值。

其次研究了解密结果对于解密波长误差的敏感性。假设解密时所采用的波长为λ'，定义波长误差为$\Delta\lambda=\lambda'-\lambda$。图5给出了解密结果质量与波长误差之

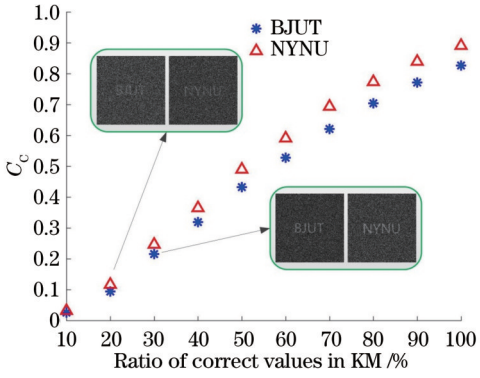

图4　解密明文质量与密钥板中正确像素点数所占比例的关系

Fig. 4　Dependence of decrypted plaintext quality on ratio of correct pixel number in KM

间的关系，图5(a)与图5(b)分别对应于图像“BJUT”与“NYNU”。可见，两幅图像的解密结果对波长误差的敏感程度非常接近：当$\Delta\lambda$达到3 nm时，两幅解密图像均可以被大致辨别；当$\Delta\lambda$达到4 nm时，两幅图像已经无法被识别。由于可见光的波长区间为390～780 nm，其变动范围为390 nm，因此由波长创建的密钥空间约为$K_{S,\lambda}=390\ \mathrm{nm}/3\ \mathrm{nm}=130$。

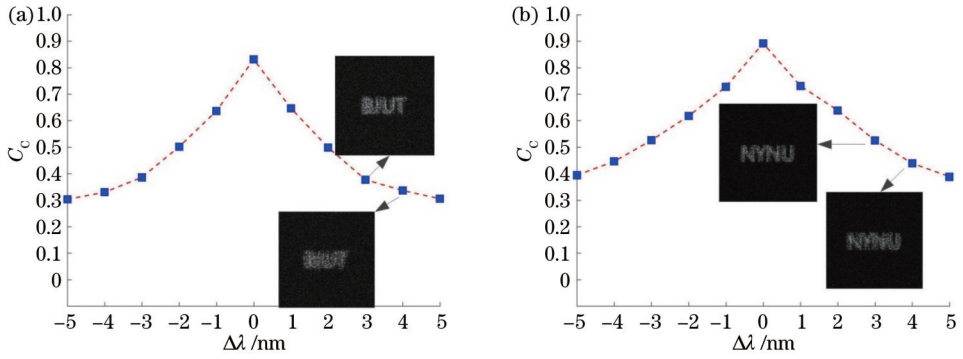

图 5　解密图像质量与波长误差的关系。(a) BJUT;(b) NYNU

Fig. 5　Dependence of decrypted image quality on wavelength error. (a) BJUT; (b) NYNU

除了密钥板和照明波长之外，正确地解密密文需要明确 4 个轴向距离 d_k，$k=1,2,3,4$。假设解密时所采用的距离为 d_k'，那么轴向距离误差可定义为 $\Delta d_k = d_k' - d_k$。图 6 给出了解密结果与轴向距离误差之间的关系。如图 6(a)、(c)所示，两幅重建明文图像对第一段衍射距离误差的敏感性相似，当距离误差 Δd_1 或 Δd_3 达到 1 mm 时，两幅重建明文图像中的有效信息已经无法被识别。假设攻击者需要在 200 mm 的范围内搜索 d_1 和 d_3，那么由它们创造的密钥空间为 $K_{S,d_1} = K_{S,d_3} = 200\ \text{mm}/1\ \text{mm} = 200$。此外，两幅图像对第二段衍射距离误差的敏感程度也非常接近，如图 6(b)、(d)所示。当距离误差 Δd_2 或 Δd_4 达到 ±45 mm 时，在解密图像中仍然可以清楚地辨别明文图像的信息，这说明该系统的解密结果对于第二段衍射距离误差 Δd_2 或 Δd_4 较不敏感。因此，如果攻击者准确掌握了第一段衍射距离(d_1 和 d_3)，即使在不精确掌握 d_2 和 d_4 的情况下仍然可以破解明文图像。也就是说，第二段衍射距离(d_2 和 d_2)无法创造出有效的密钥空间，它们在作为密钥使用时对系统的密钥空间的贡献可以忽略不计。

由于密钥板、照明波长以及轴向距离这几种密钥相互独立，因此系统的总的密钥空间为这些独立密钥所创造密钥空间的乘积，即 $K_{S,\text{total}} = K_{S,KM} K_{S,\lambda} K_{S,d_1} K_{S,d_3} \approx 2^{104878}$。这个密钥空间巨大，远

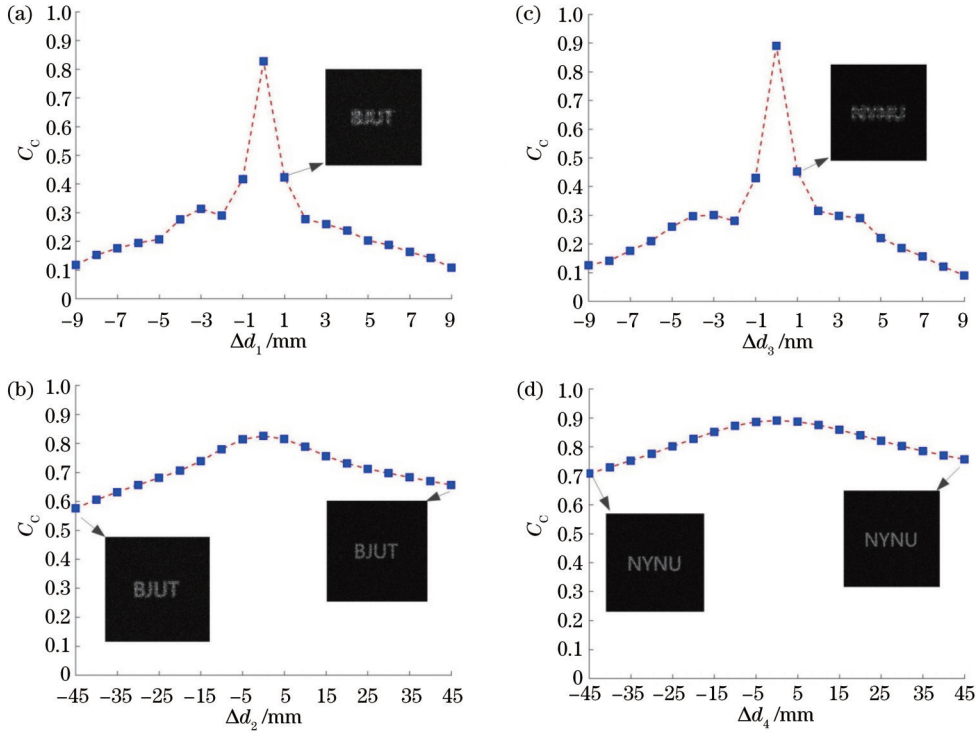

图 6　解密结果质量与轴向距离误差之间的关系。(a) Δd_1 与(b) Δd_2 对“BJUT”解密结果的影响;(c) Δd_3 与(d) Δd_4 对“NYNU”解密结果的影响

Fig. 6　Dependence of decrypted image quality on distance errors. Dependence of decrypted "BJUT" on (a) Δd_1 and (b) Δd_2; dependence of decrypted "NYNU" on (c) Δd_3 and (d) Δd_4

大于 Alvarez 等[24]提出的抵抗暴力破解的最低要求(即 2^{100})。

3.3 位置复用条件分析

本研究的出发点是位置复用,即利用图 1 中的 Δd($\Delta d = d_3 - d_1$)来区分两幅明文图像。显然,如果 $\Delta d = 0$,则用于区分两幅图像的参数消失,其对应解密结果必然出现严重的串扰。图 7 给出了在 $d_1 = d_2 = 200$ mm 的条件下,Δd 取不同值时得到的解密图像。如图 7(a)、(b)所示,当 $\Delta d = 0.1$ mm 时,两幅解密图像仍然存在严重的串扰。随着 Δd 的增加,串扰噪声逐渐减小,而当 Δd 达到 2.0 mm 时,两幅解密图像之间的串扰基本消失,如图 7(g)、(h)所示。因此,在 $d_1 = d_2 = 200$ mm 的条件下,为了得到无串扰的解密结果,Δd 的取值应大于 2.0 mm。

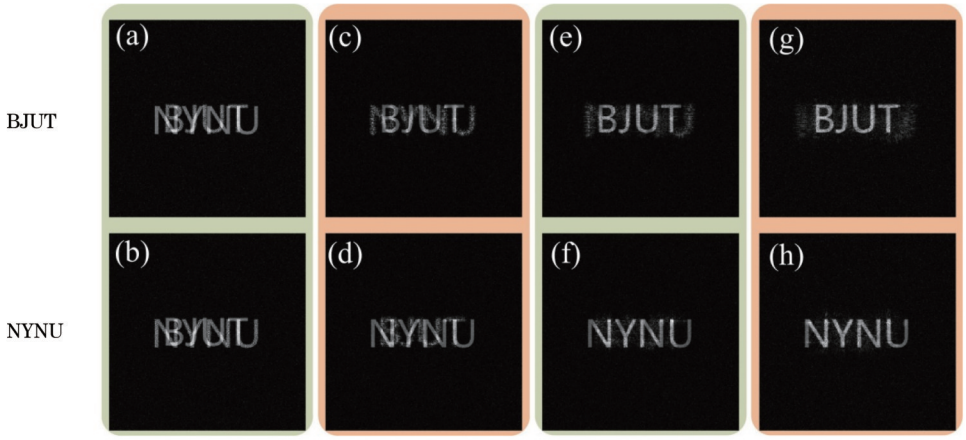

图 7　在 $d_1 = d_2 = 200$ mm 的条件下 Δd 取不同值时得到的解密结果。(a)(b) $\Delta d = 0.1$ mm;(c)(d) $\Delta d = 0.4$ mm;(e)(f) $\Delta d = 1.0$ mm;(g)(h) $\Delta d = 2.0$ mm

Fig. 7　Decrypted results when Δd takes different values in case of $d_1 = d_2 = 200$ mm. (a)(b) $\Delta d = 0.1$ mm; (c)(d) $\Delta d = 0.4$ mm; (e)(f) $\Delta d = 1.0$ mm; (g)(h) $\Delta d = 2.0$ mm

3.4 灰度图像加密与多图像加密

所提方法对二值图像的有效性已经在第 3.1 节中得到证实,本节进一步研究其对灰度图像的加密效果。用于测试的两幅灰度图像如图 8(a)、(b)所示,其尺寸同样为 256 pixel×256 pixel,像素尺寸为 6.4 μm。仿真所用参数(包括波长、距离以及误差阈值)与 3.1 节所述完全相同。采用的密钥板如图 8(c)所示,与图 3(c)所示密钥板也完全相同。用于生成密文板的迭代结果如图 8(g)所示,所生成的密文板如图 8(d)所示。从图 8(g)可以看出,本文方法在加密灰度图像时所需

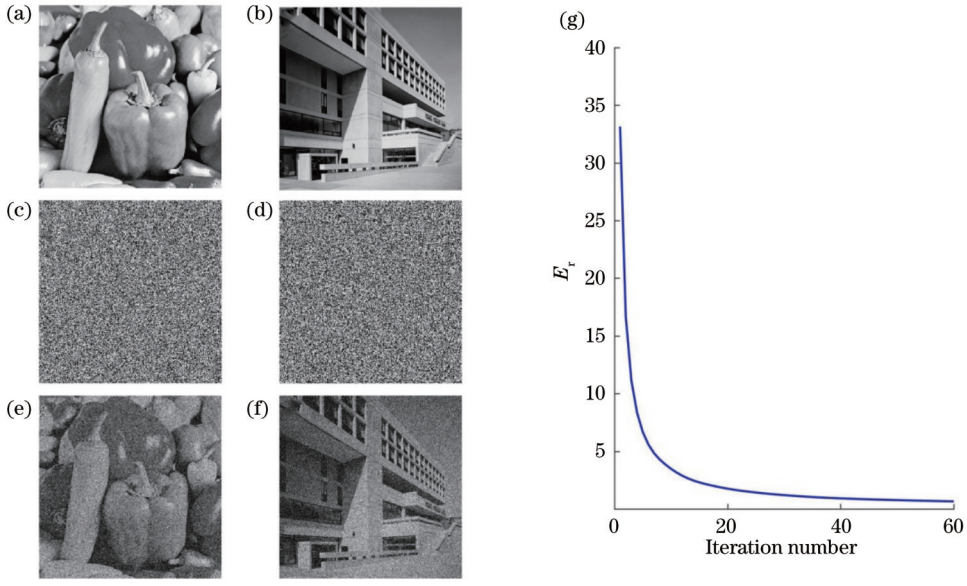

图 8　所提方法用于灰度图像加密的数值仿真验证。(a)(b)两幅明文图像;(c)密钥板;(d)密文板;(e)(f)解密图像;(g)误差函数与迭代次数的关系

Fig. 8　Numerical demonstration of proposed method for grayscale image encryption. (a)(b) Two plaintext images; (c) KM; (d) CM; (e)(f) two decrypted images; (g) dependence of error function on iteration number

的迭代次数仅为59次，相比于加密二值图像所需的238次，加密时间实现了大幅压缩。恢复的两幅明文图像分别如图8(e)、(f)所示，其对应的相关系数分别为0.8016和0.8451。可以看出，所提方法对于灰度图像仍然可以实现较好的重建。

尽管所提方法是针对双图像加密提出的，但是可以方便地将其推广到多图像加密，这里以三图像加密为例进行说明。当推广至三图像加密时，所采用的解密方案如图9(a)～(c)所示。可以看出，解密三幅图像需要密钥板处于三个不同位置，为简便起见，设两个相邻位置之间的距离均为Δd，其加密方案与图2所示的算法流程类似，区别在于迭代过程融合了三幅明文图像的信息。为了测试本文方法的效果，除了图3(a)、(b)之外，增加了第三幅明文(GXXB)，该明文的参数包括像素数与像素尺寸，与它们完全相同。模拟中，$\Delta d=50$ mm且要求$d_1+d_2=d_3+d_4=d_5+d_6$，照明波长以及误差阈值均与第3.1节所述完全相同。相应的解密结果在图9(d)～(f)中给出，其相关系数分别为0.6704、0.7501、0.8061。观察图9(d)、(e)与图3(e)、(f)并对比其相关系数可知，加密三幅图像时的解密结果质量较加密两幅图像时有一定程度的降低。这个现象可以利用加密算法原理进行解释：如式(7)所示，所提加密算法的核心是在输入面直接融合各个明文图像的相关信息，而算法的迭代过程会使所有明文图像的信息在密文板中达到均衡。显然，参与位置复用的明文图像数量越多，则最终密文板中各个明文信息之间的串扰就越严重，解密结果质量就越低。

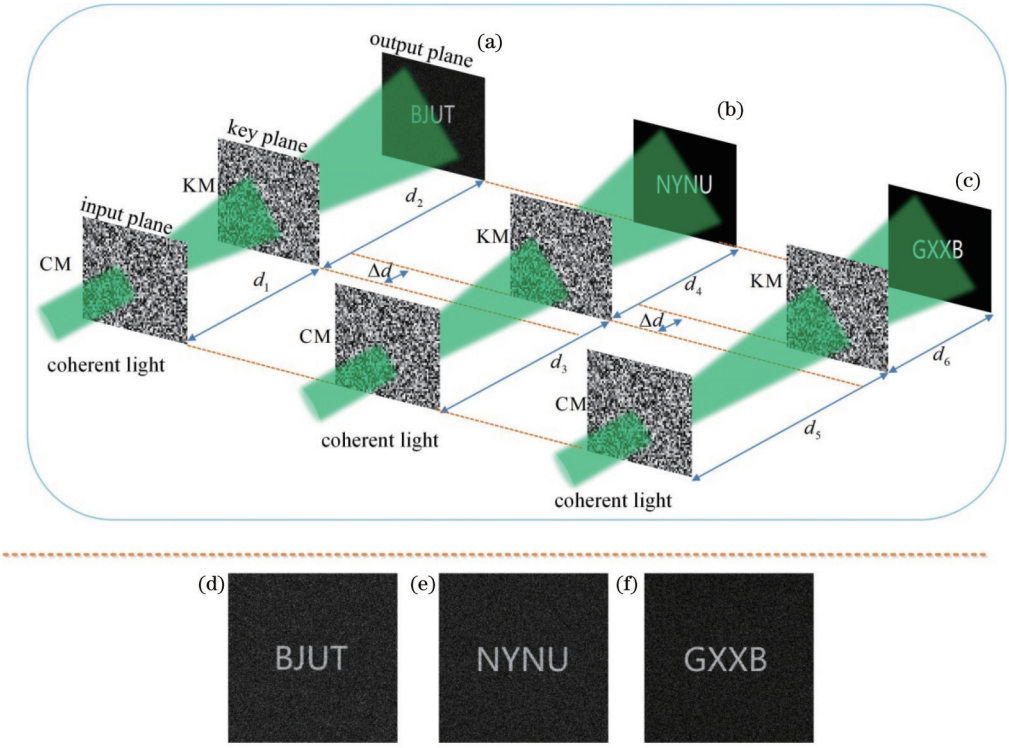

图9　所提方法推广到三图像加密时的解密方案及结果。(a)～(c)三幅明文图像的解密方案；(d)～(f)三幅明文图像的解密结果

Fig. 9　Decryption scheme and results after extension of proposed method to triple-image encryption. (a)-(c) Decryption scheme of three plaintext images; (d)-(f) decrypted results of three plaintext images

3.5　噪声稳健性分析

密文在传输的过程中经常会受到噪声干扰，因此有必要分析所提方法对于噪声的稳健性。为此，生成受噪声污染的密文$P_{\mathrm{CM}}(x,y)$：

$$P_{\mathrm{CM}}(x,y)=C_{\mathrm{M}}(x,y)+2\pi n(x,y),\tag{11}$$

式中：$n(x,y)$为振幅均匀分布于$[0,\beta]$区间的白噪声。图10给出了β分别取值为0.1、0.3、0.5和0.7时两幅明文图像的解密结果。可以看出，随着密文受污染程度的增加，解密图像质量逐渐降低。然而，当β取值为0.7时，解密图像的内容仍然可以被准确识别，这说明所提方法具有较好的噪声稳健性。

3.6　密码学分析

密码系统不仅需要具备较大的密钥空间，还需要对常见的密码学攻击具有稳健性。本节讨论所提方法对选择明文攻击(CPA)的稳健性。为此，假设攻击者已经掌握了一对如图3(a)、(b)和图3(d)所示的明文与密文，并且掌握除密钥板之外的系统其他所有参数。在图1(a)、(b)所示的解密方案中，密钥板前表面的复振幅可以由密文经衍射计算得到，而输出面的振幅为已知的明文，这种情况下可以根据广义的G-S算法[25]来推测密钥板的分布。为此，在图1(a)、(b)中分别利

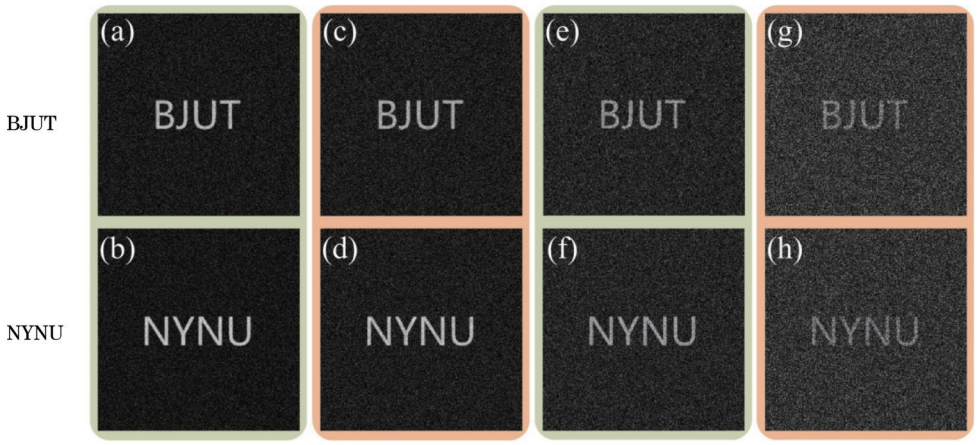

图 10 采用所提方法得到的密文在不同程度噪声污染情况下的解密结果。(a)(b) $\beta=0.1$;(c)(d) $\beta=0.3$;(e)(f) $\beta=0.5$;(g)(h) $\beta=0.7$

Fig. 10 Decrypted images for polluted ciphertexts obtained by proposed method. (a)(b) $\beta=0.1$; (c)(d) $\beta=0.3$; (e)(f) $\beta=0.5$; (g)(h) $\beta=0.7$

用G-S算法求出密钥板复振幅的估计值 K'_{M1} 和 K'_{M2},并按照式(12)将它们合成为最终的破解密钥 K'_M:

$$K'_M=\frac{K'_{M1}+K'_{M2}}{\left|K'_{M1}+K'_{M2}\right|}。\tag{12}$$

K'_M 的相位值分布如图 11(a)所示,利用它解密图 3(d)所示的密文,得到的解密结果如图 11(b)、(c)所示,可以看出 K'_M 确实满足所选择的明文-密文对的约束条件。然而,K'_M 与 K_M 之间的相关系数仅为 0.0048,这表明破解的密钥与正确密钥几乎没有相关性。用 K'_M 解密图 8(d)所示的密文[该密文与图 3(d)的加密密钥同为 K_M]得到的解密图像如图 11(d)、(e)所示,它们是与原始的明文图像[图 8(a)、(b)]完全不相关的噪声图像,对应的相关系数分别为 0.0167 和 0.0132。这说明 K'_M 仅能正确解密用于生成它时所采用的密文,无法用于解密其他的由 K_M 加密所得到的密文,这证实了所提方法对上述选择明文攻击的稳健性。

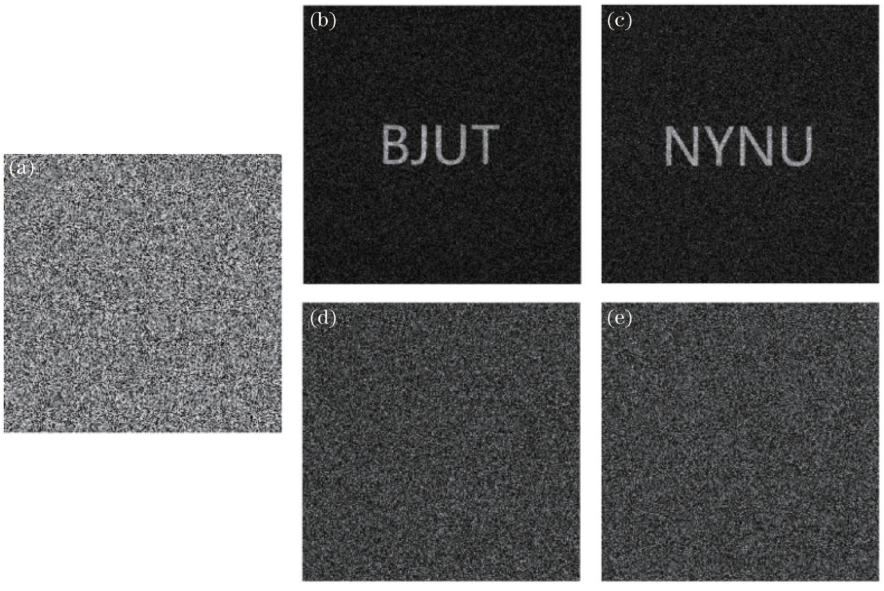

图 11 针对所提方法的选择明文攻击结果。(a)破解的密钥;(b)(c)由破解的密钥解密图 3(d)所示密文的结果;(d)(e)由破解的密钥解密图 8(d)所示密文的结果

Fig. 11 Results of CPA for proposed method. (a) Recovered key mask; (b) (c) decrypted results of Fig. 3(d) with recovered key mask; (d) (e) decrypted results of Fig. 8(d) with recovered key mask

4 实验结果

为了进一步证实所提方法的有效性,对其进行了实验验证。从原理来看,实现图 1(a)或图 1(b)所示的解密方案需要两个独立的相位调制器件(例如空间光调制器)相互协作。然而,实验中想要理想地对准第一个相位调制器件(加载的是密文板)的衍射光场与第二个相位调制器件(加载的是密钥板)非常困难,所以对

于输入面到密钥面的衍射过程，采用数字计算的方法“虚拟”地实现，即采用数值方法计算出密钥板后表面的复振幅，仅利用光学方法实现从密钥面到输出面这一段的衍射过程。此外，考虑到现有的空间光调制器无法同时独立地调制振幅和相位，通过2.2节所述的相位留存方法，将密钥面出射的复振幅近似等效为一个纯相位图像（POI）。这种做法的依据是：在对复振幅进行积分变换（如傅里叶变换）处理时，相位信息远比振幅信息更重要[26]。所采用的光学解密装置如图12所示。激光器（λ=532 nm）发出的相干光经物镜O会聚后，再经针孔空间滤波器（SF）滤波，之后被准直透镜L1（焦距为150 mm）准直。此准直光经过偏振器（P）以及分束器（BS）后照射至空间光调制器（SLM）上。解密的图像经透镜L2成像至CCD上。用来显示POI的空间光调制器（JD955B，Jasper Display Corp）的尺寸为1920 pixel×1080 pixel，像素尺寸为6.4 μm。由于POI的尺寸为256 pixel×256 pixel，通过补零的方式将其拓展为1920 pixel×1080 pixel，以适应空间光调制器尺寸。所用的CCD（GigE Vision TL，Daheng imaging）的尺寸为1920 pixel×1080 pixel，像素大小为6.4 μm。

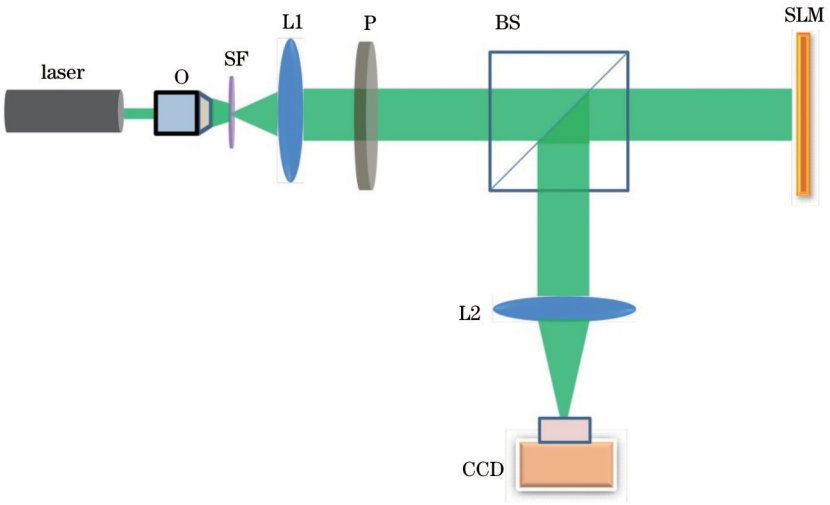

图12　用于实现解密的实验光路

Fig. 12　Experimental setup for decryption

所采用的明文图像以及相关参数与3.1节数值仿真部分完全相同。加密所采用的密钥以及所得到的密文如图3（c）、（d）所示。为了解密得到“BJUT”图像，按照图1（a）所示的解密方案，首先将密文板“虚拟”地衍射d_1的距离至密钥面，并计算由密钥板出射的复振幅，然后通过相位留存，计算出对应于“BJUT”图像的POI，如图13（a）所示。类似地，可以计算出“NYNU”图像所对应的POI图像（不同之处在于需要将密文板“虚拟”地衍射d_3的距离），结果如图13（b）所示。将这两个POI依次加载到空间光调制器上，所得到的解密图像如图13（c）、（d）所示，可见原始的明文图像被正确地解密出来，所提方法的有效性得到了进一步的证实。

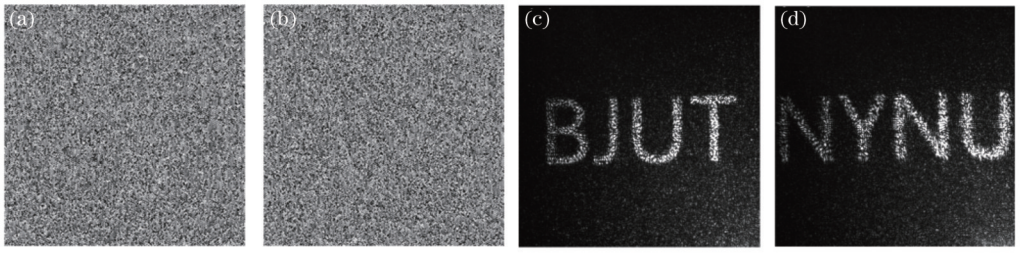

图13　所提方法有效性的实验验证。（a）（b）空间光调制器上依次加载的两幅POI图像；（c）（d）解密结果

Fig. 13　Experimental demonstration of effectiveness of proposed method. (a)(b) Two POI images displayed on SLM; (c)(d) decrypted images

此外，利用实验分析密钥板两个设定位置之间的距离Δd对解密结果的影响，如图14所示。对比图14和图7可以发现，实验结果与仿真结果吻合得非常好。当Δd=0.1 mm时，两幅解密图像几乎完全混叠在一起，导致其中任何一幅解密图像都无法被分辨，如图14（a）、（b）所示。随着Δd的增大，两幅解密图像之间的串扰逐渐减弱。当Δd=1.0 mm时，两幅图像的大致轮廓基本显现，但是图像质量较低；当Δd=2.0 mm

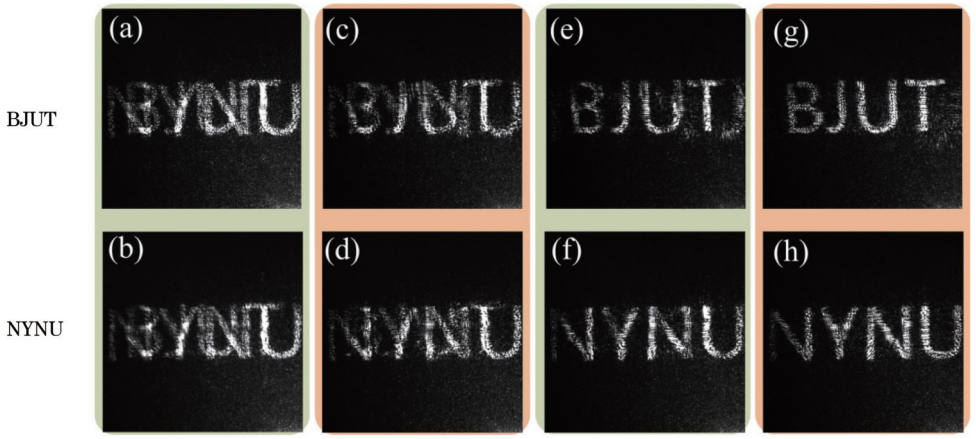

图 14 Δd 取不同值时得到的实验解密图像。(a)(b) $\Delta d=0.1$ mm;(c)(d) $\Delta d=0.4$ mm;(e)(f) $\Delta d=1.0$ mm;(g)(h) $\Delta d=2.0$ mm

Fig. 14 Experimentally decrypted results when Δd takes different values. (a)(b) $\Delta d=0.1$ mm; (c)(d) $\Delta d=0.4$ mm; (e)(f) $\Delta d=1.0$ mm; (g)(h) $\Delta d=2.0$ mm

时,两幅解密图像之间的串扰噪声基本消失,原始明文图像得到了较好的重建。

5 结 论

提出了一种在CDPE系统中基于位置复用的双图像加密方法,并利用所提出的迭代加密算法将两幅图像加密至单个纯相位板(密文板)中。与传统的CDPE系统相比,本文方法将加密效率提升了1倍。解密时,本文方法只需移动密钥板至两个事先设定的轴向位置,即可在输出面上得到两幅不同的明文图像。此外,为了成功地实施位置复用以避免串扰,密钥板所处的两个轴向位置之间距离必须大于某个特定值。密钥空间分析结果表明,本文方法具有巨大的密钥空间,足以抵抗暴力破解。利用G-S算法针对本文方法提出了一种选择明文攻击方案,结果表明它对选择明文攻击具有稳健性,同时也证实了本文方法推广至多图像加密的可行性,这表明CDPE系统的加密效率可得到进一步提升。

参 考 文 献

[1] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.

[2] Hazer A, Yildirim R. A review of single and multiple optical image encryption techniques[J]. Journal of Optics, 2021, 23(11): 113501.

[3] Qin Y, Wan Y H, Wan S J, et al. Optical compressive encryption via deep learning[J]. IEEE Photonics Journal, 2021, 13(4): 7800208.

[4] 陶冶, 祝玉鹏, 杨栋宇, 等. 基于视觉密码的远距离光学信息认证系统[J]. 光学学报, 2021, 41(16): 1607001.
Tao Y, Zhu Y P, Yang D Y, et al. Remote optical information authentication system based on visual cryptography[J]. Acta Optica Sinica, 2021, 41(16): 1607001.

[5] 王岩, 牛宏伟. 基于光学空频域变换的自适应图像分块隐藏技术[J]. 激光与光电子学进展, 2021, 58(16): 1609001.
Wang Y, Niu H W. Adaptive image block hiding technology based on optical spatial-frequency domain transform[J]. Laser & Optoelectronics Progress, 2021, 58(16): 1609001.

[6] 鲍震杰, 薛茹. 基于自动编码器的光学图像加密方法[J]. 激光与光电子学进展, 2021, 58(22): 2210011.
Bao Z J, Xue R. Optical image encryption method based on autoencoder[J]. Laser & Optoelectronics Progress, 2021, 58(22): 2210011.

[7] 吴军, 王刚, 徐刚. 结合计算全息与混沌的彩色图像加密方法[J]. 光学学报, 2021, 41(19): 1909001.
Wu J, Wang G, Xu G. Color image encryption method based on computer generated hologram and chaos[J]. Acta Optica Sinica, 2021, 41(19): 1909001.

[8] 孙宝清, 王玉鹏. 时域鬼成像及其应用[J]. 中国激光, 2021, 48(12): 1212001.
Sun B Q, Wang Y P. Temporal ghost imaging and its application [J]. Chinese Journal of Lasers, 2021, 48(12): 1212001.

[9] Javidi B, Carnicer A, Yamaguchi M, et al. Roadmap on optical security[J]. Journal of Optics, 2016, 18(8): 083001.

[10] 彭翔, 位恒政, 张鹏. 光学信息安全导论[M]. 北京: 科学出版社, 2008.
Peng X, Wei H Z, Zhang P. Introduction to optical security[M]. Beijing: Science Press, 2008.

[11] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture[J]. Optical Engineering, 2000, 39(8): 2031-2035.

[12] Chen W, Chen X D, Sheppard C J R. Optical image encryption based on diffractive imaging[J]. Optics Letters, 2010, 35(22): 3817-3819.

[13] Shi Y S, Yang X B. Optical hiding with visual cryptography[J]. Journal of Optics, 2017, 19(11): 115703.

[14] Yang N, Gao Q K, Shi Y S. Visual-cryptographic image hiding with holographic optical elements[J]. Optics Express, 2018, 26(24): 31995-32006.

[15] Wu J J, Wang J C, Nie Y G, et al. Multiple-image optical encryption based on phase retrieval algorithm and fractional Talbot effect[J]. Optics Express, 2019, 27(24): 35096-35107.

[16] Zhang Y, Wang B. Optical image encryption based on interference[J]. Optics Letters, 2008, 33(21): 2443-2445.

[17] Chang H T, Lu W C, Kuo C J. Multiple-phase retrieval for optical security systems by use of random-phase encoding[J]. Applied Optics, 2002, 41(23): 4825-4834.

[18] Wang R K, Watson I A, Chatwin C R. Random phase encoding for optical security[J]. Optical Engineering, 1996, 35(9): 2464-2469.

[19] Li Y, Kreske K, Rosen J. Security and encryption optical

systems based on a correlator with significant output images[J]. Applied Optics, 2000, 39(29): 5295-5301.
[20] Situ G H, Zhang J J. A cascaded iterative Fourier transform algorithm for optical security applications[J]. Optik, 2003, 114(10): 473-477.
[21] Situ G H, Zhang J J. A lensless optical security system based on computer-generated phase only masks[J]. Optics Communications, 2004, 232(1/2/3/4/5/6): 115-122.
[22] Lü W J, Sun X, Yang D, et al. Optical multiple information hiding via azimuth multiplexing[J]. Optics and Lasers in Engineering, 2021, 141: 106574.
[23] Lu Z, Lü W, Zhu Y, et al. Optical information encryption based on partially-update iterative system with azimuth multiplexing[J]. Optics Communications, 2022, 510: 127899.
[24] Alvarez G, Li S J. Some basic cryptographic requirements for chaos-based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(8): 2129-2151.
[25] 杨国桢, 顾本源. 光学系统中振幅和相位的恢复问题[J]. 物理学报, 1981, 30(3): 410-413.
Yang G Z, Gu B Y. On the amplitude-phase retrieval problem in optical systems[J]. Acta Physica Sinica, 1981, 30(3): 410-413.
[26] Ghiglia D C, Pritt M D. Two-dimensional phase unwrapping: theory, algorithms, and software[M]. New York: Wiley, 1998.

Position-Multiplexing-Based Double-Image Encryption in Cascaded Double-Phase Encoding Cryptosystem

Qin Yi[1,2], Wan Yuhong[1*], Gong Qiong[2]

[1]*Faculty of Science, Beijing University of Technology, Beijing* 100124, *China*;

[2]*College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang* 473061, *Henan, China*

Abstract

Objective Cascaded double-phase encoding (CDPE) is an optical cryptosystem, and it comprises two phase-only masks (ciphertext mask and key mask). Among optical cryptosystems, CDPE is of great importance due to its superiority in security. Its ciphertext is a phase-only mask whose content cannot be directly read out by the intensity-sensitive device such as the charge-coupled device (CCD) or human eyes. Although there is already published research on CDPE, few of them focus on simultaneous compression and encryption. In this paper, we propose a novel iterative encryption algorithm (IEA) to achieve double-image encryption in CDPE, which employs the position of the key mask as a controllable parameter. Compared with that of the traditional CDPE, the encryption capacity of the proposed algorithm has been substantially improved. The proposed algorithm opens up a new way for simultaneous compression and encryption in CDPE, and it may offer new inspiration for the design of other cryptosystems.

Methods The optical architecture for decryption in this paper comprises two phase-only masks (ciphertext mask and key mask). Parallel monochromatic light is employed for illumination. The positions of the ciphertext mask and the output plane are fixed during decryption. Two positions along the axis are specified for the key mask. When the key mask locates respectively at these positions, two distinct plaintexts can be individually generated at the output plane. Essentially, the decryption employs two different optical architectures which differ only in the position of the key mask. According to the decryption principle, an IEA is proposed to encrypt the two plaintexts into the ciphertext mask. The IEA requires parallel iteration in the two optical architectures. For each architecture, the light wave virtually illuminates the scheme and finally reaches the output plane after being modulated by the two phase-only masks. At the output plane, the amplitude of the wavefront is replaced with the plaintext. The renewed wavefront at the output plane then propagates back to the input plane and forms a complex amplitude. The two complex amplitudes from the two architectures are superposed and then phase-reserved to obtain a new estimation of the ciphertext mask. The first iteration completes after the update of the ciphertext mask, and then the second iteration begins. The iteration will continue until the decrypted plaintexts at the output plane sufficiently approximate the original ones.

Results and Discussions First, we validate the effectiveness of the proposed algorithm with binary images in the simulation context of MATLAB R2016a. The proposed IEA shows excellent convergence, and it terminates after 238 iterations. Both the subjective and objective metrics indicate the high quality of decrypted plaintexts (Fig. 3), which verifies the effectiveness of the proposed algorithm. Second, we analyze the key space created by each of the secret keys, including the wavelength, axial distances, and key mask. The key space of the proposed algorithm is as large as 2^{104856}, which is robust enough to resist brute-force attacks. Third, we investigate the condition for successful multiplexing. The results show that a minimum position interval of 2 mm of the key mask is required (Fig. 7), and an interval exceeding this value will cause obvious cross-talk noise in the decrypted images. Fourth, we verify the proposed algorithm with grayscale

images and successfully extend it to multiple-image encryption (Fig. 8 and Fig. 9). The corresponding results show that the quality of the decrypted images decays with the image number for multiplexing. Therefore, there must be a compromise between the encryption capacity and the quality of decryption. Fifth, we test the robustness of the proposed algorithm against noise attacks, and the results show that the ciphertext can still ensure high-quality decryption in spite of severe contamination (Fig. 10). Sixth, we analyze the robustness of the proposed algorithm to cryptoanalysis. It is found that a chosen-plaintext attack (CPA) based on the G-S algorithm fails to crack the proposed algorithm (Fig. 11). Seventh, we further demonstrate the effectiveness of the proposed algorithm with experimental results (Fig. 13 and Fig. 14), which highly agree with the simulated ones.

Conclusions In this paper, a double-image encryption method based on position-multiplexing in the CDPE system is proposed. A new IEA is presented to encrypt two plaintext images into a single phase-only mask (ciphertext mask). Compared with that of the traditional CDPE, the encryption capacity of this method is doubled. For decryption, the key mask is placed respectively at two preset axial positions, and two different plaintext images can be individually obtained at the same output plane. In addition, for successful position multiplexing to avoid crosstalk, the distance between the two axial positions of the key mask must be greater than a certain value. The security analysis shows that the proposed algorithm has a huge key space that is enough to resist brute-force attacks. Furthermore, the G-S algorithm is adopted to provide a CPA to the proposed algorithm, and the results show that the proposed algorithm is robust to the CPA. In addition, the feasibility of extending the proposed algorithm to multiple-image encryption is proven, which indicates that the encryption efficiency of CDPE systems can be further enhanced.

Key words image processing; optical information security; double-image encryption; position multiplexing; iterative encryption algorithm