基于空间角度复用和双随机相位的多图像光学加密方法*

王雪光[1)2)] 李明[1)] 于娜娜[2)] 席思星[2)†] 王晓雷[3)] 郎利影[4)]

1) (中国矿业大学信息与控制工程学院, 徐州 221116)

2) (河北工程大学数理科学与工程学院, 邯郸 056038)

3) (南开大学现代光学研究所, 天津 300350)

4) (河北工业大学, 天津 300401)

(2019 年 9 月 8 日收到; 2019 年 10 月 8 日收到修改稿)

提出了基于空间角度复用和双随机相位的多图像光学加密新方法. 加密过程中, 首先将原始图像进行随机相位调制和不同距离的菲涅耳衍射; 其次, 将携带调制后图像的参考光与携带随机相位且具有不同立体角的参考光相干叠加, 产生干涉条纹; 最后, 将不同方向的干涉条纹叠加形成复合加密图像. 解密为加密的逆过程, 将复合加密图像置于空间滤波和菲涅耳衍射系统中, 经过不同相位密钥解调和正确距离的菲涅耳衍射完成解密, 得到多幅解密图像. 该方法可以同时对多幅图像进行高效的加密, 计算简单、安全可靠、抗噪声能力强. 利用相关系数评估了该方法的加密效果, 并通过仿真实验验证了该方法的有效性和安全性.

关键词: 多图像加密, 空间角度复用, 数字全息, 干涉加密

PACS: 05.45.Gg, 42.30.Va, 42.30.Wb **DOI:** 10.7498/aps.68.20191362

1 引 言

光学图像加密技术已在信息安全领域显示出巨大的应用潜力, 成为学者们研究的热点. 1995 年, Refregier 和 Javidi[1] 首次提出了安全性高、鲁棒性强的双随机相位光学加密技术, 此后一系列派生的光学图像加密方法被不断提出, 如分数傅里叶变换加密系统[2]、菲涅耳变换加密系统[3]、分数 Hartley 变换加密系统[4]、混沌[5] 和置乱加密系统[6]、相移干涉加密系统[7]、联合变换相关器加密系统[8]、叠层衍射成像加密系统[9]、偏振加密系统[10]、数字全息加密系统[11] 和计算全息加密系统[12] 等. 但是, 上述加密方法仅针对单个图像, 随着大数据技术的快速发展和信息传输能力的不断增强, 传统的单图像加密传输已经不能满足日益增长的信息需求. 因此, 越来越多的学者开始研究多图像加密技术[13–15].

多图像加密技术的要点在于图像在加密过程中如何合成, 合成方法直接影响整个算法的计算效率和最终解密图像的质量. 目前的多图像光学加密技术主要基于复用、数字全息、压缩感知、混沌和特殊光学变换等. 例如, Situ 和 Zhang[16] 引入了波长复用来实现多图像加密. Xu 等[17] 提出了一种基于随机振幅板和菲涅耳全息图的多图像加密方法. Deepan 等[18] 将压缩感知技术应用于基于双随机相位密钥的空间复用加密系统, 实现多图像加密. Tang 等[19] 结合位平面分解和混沌映射算法对多幅图像进行了加密, Kong 等[20] 使用级联分数傅里叶变换将多个图像叠加成单个图像进行加密. 目前, 由于基于单一技术的加密方法具有局限性, 这

* 国家自然科学基金 (批准号: 11904073, 61875093)、河北省自然科学基金 (批准号: F2019402351, F2018402285) 和天津市自然科学基金 (批准号: 19JCYBJC16500) 资助的课题.

† 通信作者. E-mail: xisixing@126.com

些多图像加密方法大多是基于多种技术手段的组合, 尽管提高了加密图像的数量, 但也增加了系统的复杂性. 同时, 数据处理的时间和复杂度也随着加密能力的增加而增加. 此外, 受限于解密实验中随机相位密钥逐像素对齐的要求[21], 这些方法主要集中在数字系统或光电混合系统, 难以光学实现.

针对上述问题, 本文提出一种基于空间角度复用和双随机相位的光学多图像加密方法. 该方法利用数字全息的空间角度复用技术实现多个待加密图像的同时加密; 利用基于干涉原理的双随机相位光学图像加密技术, 将两个随机相位密钥分别置于物光束和参考光束中, 并以干涉条纹的振幅形式保存和传输, 简化了加密系统; 解密过程是正确密钥调制的空间滤波和菲涅耳衍射过程, 解决了传统方法解密实验中随机相位密钥难以逐像素对齐的问题. 此外, 本文给出了可行的实验加密和解密系统, 并通过仿真实验验证了光学加密方法的可行性. 该方法具有存储效率高、计算简单等特点, 在提高信息传输效率和多用户认证方面具有重要的应用前景.

2 加密过程

本文提出的多图像加密系统如图 1 所示, 是包含两个 $4f$ 成像系统和两个相位型空间光调制器 (SLM) 的马赫-曾德尔干涉系统. 首先待加密图像由 $4f$ 系统成像到第一个 SLM_1 上, 被加载到 SLM_1 上的随机相位密钥调制. 调制后的图像经过衍射距离为 z_i 的菲涅耳衍射过程后与携带加载在 SLM_2 上的第二个随机相位密钥的参考光相干叠加, 形成加密干涉条纹, 并由电荷耦合器 (CCD) 记录. 然后, 将待加密图像和第一个随机相位去除, 由同一 CCD 记录第二个随机相位与平行光的干涉条纹. 该干涉条纹可再现恢复第二个随机相位密钥及其共轭. 变换待加密图像时, 改变双随机相位和菲涅耳衍射距离, 并通过旋转 CCD 和调整光路改变参考光的立体角, 形成间距和方向不同的加密干涉条纹. 最后, 将多个全息图叠加构成复合加密图像.

本文选取 8 幅原始图像, 分别是“A”和“B”2 个字母, “Lena”和“baboon”两个 256 灰度图像, 以及“光”、“学”、“全”和“息”4 个汉字, 其表达式分别为 $a(x,y)$, $b(x,y)$, $c(x,y)$, $d(x,y)$, $e(x,y)$, $f(x,y)$, $g(x,y)$ 和 $h(x,y)$, 如图 2 所示.

在如图 1 所示的光学系统中, 每个原始图像被平行光垂直照射, 并被第一随机相位 p_{1i} (i 为图像序号) 调制, 第一随机相位可以表示为

$$\begin{aligned} &p_{11}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\ p_{12}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\\ &p_{13}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\ p_{14}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\\ &p_{15}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\ p_{16}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\\ &p_{17}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)],\ p_{18}=\exp[\mathrm{j}\pi\,\mathrm{rand}(x,y)], \end{aligned} \tag{1}$$

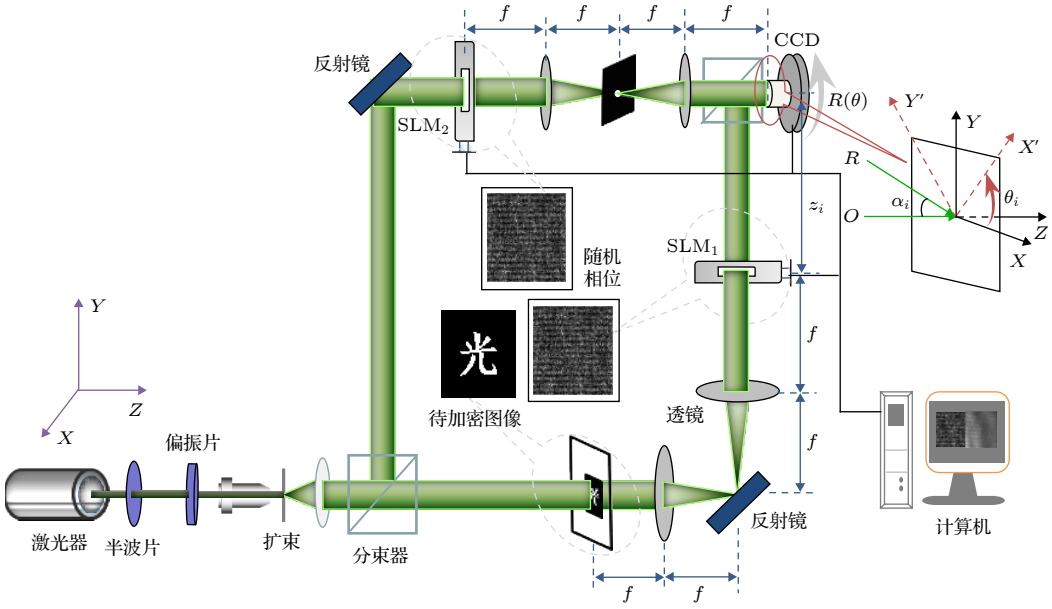

图 1 多图像光学加密系统 (SLM 是空间光调制器, f 是透镜焦距, z_i 是菲涅耳衍射距离, $R(\theta)$ 表示 CCD 旋转后与 x 轴的夹角, α_i 是物光 O 与参考光 R 的夹角)

Fig. 1. Optical setup of multiple-image encryption process. SLM is spatial light modulator, f is focal length, z_i is the distance of Fresnel diffraction, $R(\theta)$ is the rotation angle of CCD, α_i is angle between object light O and reference light R.

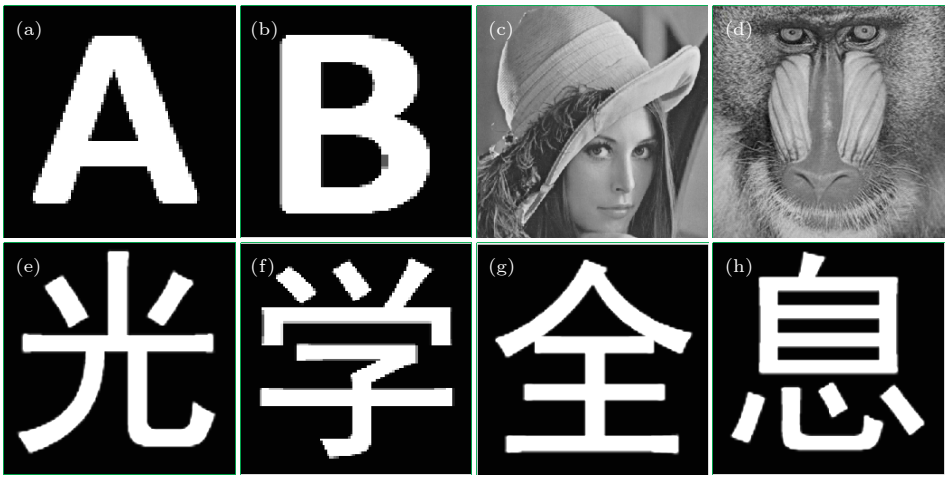

图 2 (a)—(h) 8 幅待加密图像

Fig. 2. (a)–(h) Multiple-image to be encrypted.

其中, rand(x,y)表示 0 到 1 的随机矩阵. 为了尽可能地恢复原始图像信息提高解密图像质量, 第一个随机相位的动态范围选取为0—π. 由于不同的衍射距离可以提高多图像加密的安全性, 加密过程中的菲涅耳衍射距离分别设置为 $z_1=0.5$ m, $z_2=0.55$ m, $z_3=0.6$ m, $z_4=0.65$ m, $z_5=0.7$ m, $z_6=0.75$ m, $z_7=0.8$ m 和 $z_8=0.85$ m. 经过随机相位调制和菲涅耳衍射后的光场分布可表示为

$$\begin{aligned}
a_1(x,y)&=\mathrm{FrT}z_1[a(x,y)p_{11}(x,y),\ \lambda_1],\\
b_1(x,y)&=\mathrm{FrT}z_2[b(x,y)p_{12}(x,y),\ \lambda_2],\\
c_1(x,y)&=\mathrm{FrT}z_3[c(x,y)p_{13}(x,y),\ \lambda_3],\\
d_1(x,y)&=\mathrm{FrT}z_4[d(x,y)p_{14}(x,y),\ \lambda_4],\\
e_1(x,y)&=\mathrm{FrT}z_5[e(x,y)p_{15}(x,y),\ \lambda_5],\\
f_1(x,y)&=\mathrm{FrT}z_6[f(x,y)p_{16}(x,y),\ \lambda_6],\\
g_1(x,y)&=\mathrm{FrT}z_7[g(x,y)p_{17}(x,y),\ \lambda_7],\\
h_1(x,y)&=\mathrm{FrT}z_8[h(x,y)p_{18}(x,y),\ \lambda_8],
\end{aligned}\tag{2}$$

其中, $\mathrm{FrT}z_i[\cdot,\lambda]$表示衍射距离为 z_i、波长为 λ_i 的菲涅耳衍射.

然后, (2) 式表示的光场与具有不同空间角度且携带第二个随机相位的参考光束相干叠加. 如图 1 的内插图所示, 参考光的空间角用 $(\alpha_i,\ \theta_i)$表示, 其中, α_i是参考光束与 z 轴之间的夹角, θ_i 是 CCD 逆时针旋转的角度. 当加密更多图像时, 参考光空间角度可相应调整. 本文选取参考光的立体角度 $(\alpha_i,\ \theta_i)$分别为 $(3°,0°)$, $(3°,45°)$, $(3°,90°)$, $(3°,135°)$, $(6°,0°)$, $(6°,45°)$, $(6°,90°)$和$(6°,135°)$, 相应的参考光表达式为

$$\begin{aligned}
R_1&=\exp\left[\mathrm{j}2\pi\left(x\frac{\sin3°}{\lambda_1}+p_{21}(x,y)\right)\right],\\
R_2&=\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin3°}{\lambda_2}+p_{22}(x,y)\right)\right],\\
R_3&=\exp\left[\mathrm{j}2\pi\left(y\frac{\sin3°}{\lambda_3}+p_{23}(x,y)\right)\right],\\
R_4&=\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin3°}{\lambda_4}+p_{24}(x,y)\right)\right],\\
R_5&=\exp\left[\mathrm{j}2\pi\left(x\frac{\sin6°}{\lambda_5}+p_{25}(x,y)\right)\right],\\
R_6&=\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin6°}{\lambda_6}+p_{26}(x,y)\right)\right],\\
R_7&=\exp\left[\mathrm{j}2\pi\left(y\frac{\sin6°}{\lambda_7}+p_{27}(x,y)\right)\right],\\
R_8&=\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin6°}{\lambda_8}+p_{28}(x,y)\right)\right],
\end{aligned}\tag{3}$$

其中 $p_{2i}(x,y)$为第二随机相位密钥. 为了简化解密过程, 令 8 幅待加密图像对应的第二随机相位密钥和激光波长相同, 即

$$\begin{aligned}
p_{2i}(x,y)&=p_2(x,y)=\exp[2\mathrm{j}\pi\,\mathrm{rand}(x,y)]\\
&=\exp[2\mathrm{j}\pi M(x,y)],
\end{aligned}\tag{4}$$

$$\lambda_i=\lambda=532\ \mathrm{nm}.\tag{5}$$

将 8 个待加密图像分别与 (3) 式表示的参考光束干涉. 为了降低带宽和采样点, 提高重建图像的质量, 用均匀场代替原来的偏置分量. 因此, 形成的干涉场分布分别为

$$
\begin{aligned}
I_1(x,y) &= 1 + a_1(x,y)R_1^* + a_1^*(x,y)R_1 \\
&= 1 + a_1(x,y)\exp\left[-\mathrm{j}2\pi\left(x\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right] + a_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(x\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right], \\
I_2(x,y) &= 1 + b_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x+y)\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right] + b_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right], \\
I_3(x,y) &= 1 + c_1(x,y)\exp\left[-\mathrm{j}2\pi\left(y\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right] + c_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(y\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right], \\
I_4(x,y) &= 1 + d_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x-y)\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right] + d_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin 3^\circ}{\lambda} + M(x,y)\right)\right], \\
I_5(x,y) &= 1 + e_1(x,y)\exp\left[-\mathrm{j}2\pi\left(x\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right] + e_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(x\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right], \\
I_6(x,y) &= 1 + f_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x+y)\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right] + f_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right], \\
I_7(x,y) &= 1 + g_1(x,y)\exp\left[-\mathrm{j}2\pi\left(y\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right] + g_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(y\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right], \\
I_8(x,y) &= 1 + h_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x-y)\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right] + h_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin 6^\circ}{\lambda} + M(x,y)\right)\right],
\end{aligned} \tag{6}
$$

其中*表示图像共轭. 8 幅原始图像产生的加密干涉条纹如图 3 所示, 其中干涉条纹方向与参考光的空间角θ_i参数相关, 而干涉条纹周期与参考光的空间角α_i参数相关.

最后将 8 个加密干涉条纹叠加构成最终的加密图像如图 4 所示, 其表达式为

$$
\begin{aligned}
I(x,y) = {} & I_1(x,y) + I_2(x,y) + I_3(x,y) + I_4(x,y) \\
& + I_5(x,y) + I_6(x,y) + I_7(x,y) + I_8(x,y).
\end{aligned} \tag{7}
$$

加密结果图是一幅接近随机分布的灰度图像, 相对于传统图像加密方法的加密复值图像结果, 更便于存储和传输. 该图完全隐藏了所有原始图像的信息和加密图像个数, 在存储和传输过程中更具有一般性.

3 解 密

多图像解密为加密的逆过程, 在图 5 所示的系统中完成. 该系统包含两个 $4f$ 成像系统和一次菲涅耳衍射过程. 在第一个 $4f$ 系统的入射面放置加密结果图 (图 4), 出射面放置一个相位型 SLM, 加载随机相位密钥$p_3(x,y)$.

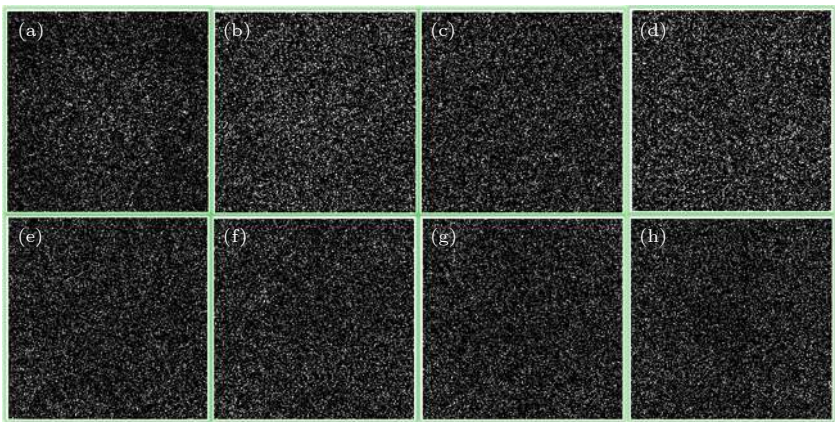

图 3 (a)—(h)8 幅原始图像对应的加密干涉条纹

Fig. 3. (a) – (h) Encrypted interference fringes corresponding to 8 original images.

其中, CCD 记录的第二个随机相位与平面波的干涉条纹再现恢复得到p_2或其共轭$p_2{}^*$, 可作为解密相位密钥, 首先应用$p_3 = p_2{}^*$, 相当于将p_3紧贴加密图像放置. 经过随机相位密钥p_3调制后的光场分布为

$$
\begin{aligned}
&I(x,y)\times p_3(x,y)\\
&=[I_1(x,y)+I_2(x,y)+I_3(x,y)+I_4(x,y)+I_5(x,y)+I_6(x,y)+I_7(x,y)+I_8(x,y)]\times p_2^*(x,y)\\
&=p_2^*(x,y)+a_1(x,y)\exp\left[-\mathrm{j}2\pi\left(x\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]+a_1^*(x,y)\exp\left[\mathrm{j}2\pi x\frac{\sin 3^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+b_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x+y)\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]+b_1^*(x,y)\exp\left[\mathrm{j}2\pi(x+y)\frac{\sin 3^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+c_1(x,y)\exp\left[-\mathrm{j}2\pi\left(y\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]+c_1^*(x,y)\exp\left[\mathrm{j}2\pi y\frac{\sin 3^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+d_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x-y)\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]+d_1^*(x,y)\exp\left[\mathrm{j}2\pi(x-y)\frac{\sin 3^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+\mathrm{e}_1(x,y)\exp\left[-\mathrm{j}2\pi\left(x\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]+e_1^*(x,y)\exp\left[\mathrm{j}2\pi x\frac{\sin 6^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+f_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x+y)\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]+f_1^*(x,y)\exp\left[\mathrm{j}2\pi(x+y)\frac{\sin 6^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+g_1(x,y)\exp\left[-\mathrm{j}2\pi\left(y\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]+g_1^*(x,y)\exp\left[\mathrm{j}2\pi y\frac{\sin 6^\circ}{\lambda}\right]\\
&\quad+p_2^*(x,y)+h_1(x,y)\exp\left[-\mathrm{j}2\pi\left((x-y)\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]+h_1^*(x,y)\exp\left[\mathrm{j}2\pi(x-y)\frac{\sin 6^\circ}{\lambda}\right]. \qquad (8)
\end{aligned}
$$

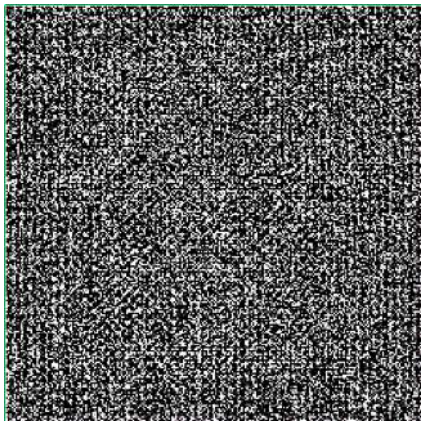

图 4 加密结果图

Fig. 4. Encrypted image.

从 (8) 式可见, 经过解密相位密钥调制后, 每个图像的 0 级和–1 级信息携带随机相位, 经过傅里叶变换后成为弥散整个频谱面的噪声, 而+1 级信息经过傅里叶变换后成为原始图像共轭的正确频谱, 频谱图如图 6(a) 所示.

由图 6(a) 所示频谱图可见, 每个原始图像的+1 级频谱被恢复, 频谱位置受参考光的立体角度$(\alpha_i,\ \theta_i)$控制, 0 级和–1 级频谱被调制为噪声弥散到整个频谱空间. 为了进行对比, 本文将p_2作为解密密钥时的频谱放置于图 6(b), 可见此时每个原始图像的–1 级频谱被恢复, 其位置受参考光的立体角度$(\alpha_i,\ \theta_i)$控制, 0 级和+1 级频谱被调制为噪声弥散到整个频谱空间. 此时 (8) 式变为

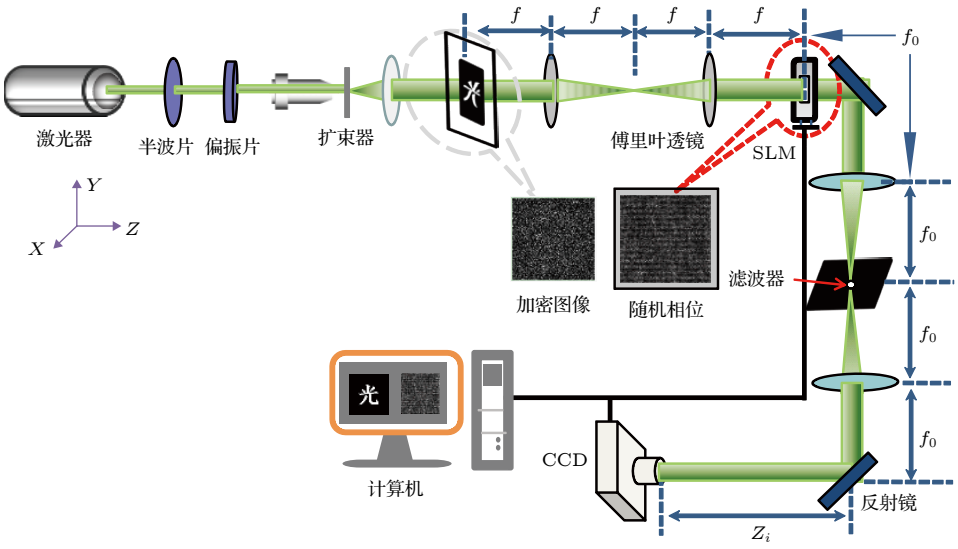

图 5 多图像解密系统

Fig. 5. Decryption system of multiple-image.

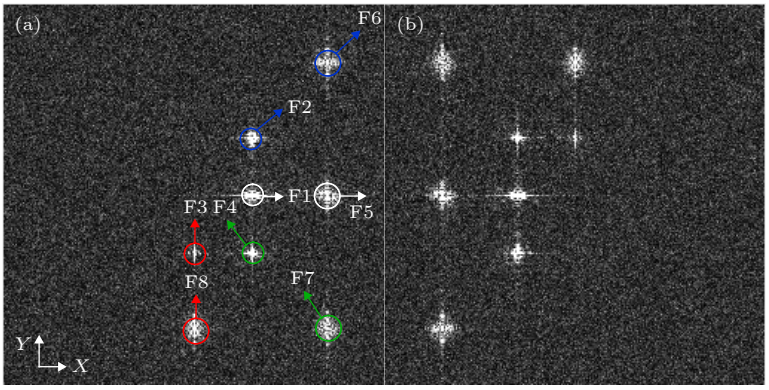

图 6 (a) p_2^*为解密密钥时频谱图, 其中 F1—F8 为相应的滤波器; (b) p_2为解密密钥时频谱图

Fig. 6. (a) Decrypted spectrum with right key p_2^*, where F1 – F8 are filters; (b) decrypted spectrum with key p_2.

$$
\begin{aligned}
&I(x,y)*p_3(x,y)\\
&=[I_1(x,y)+I_2(x,y)+I_3(x,y)+I_4(x,y)+I_5(x,y)+I_6(x,y)+I_7(x,y)+I_8(x,y)]\times p_2(x,y)\\
&=p_2(x,y)+a_1(x,y)\exp\left[-\mathrm{j}2\pi x\frac{\sin 3^\circ}{\lambda}\right]+a_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(x\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+b_1(x,y)\exp\left[-\mathrm{j}2\pi(x+y)\frac{\sin 3^\circ}{\lambda}\right]+b_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+c_1(x,y)\exp\left[-\mathrm{j}2\pi y\frac{\sin 3^\circ}{\lambda}\right]+c_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(y\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+d_1(x,y)\exp\left[-\mathrm{j}2\pi(x-y)\frac{\sin 3^\circ}{\lambda}\right]+d_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin 3^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+e_1(x,y)\exp\left[-\mathrm{j}2\pi x\frac{\sin 6^\circ}{\lambda}\right]+e_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(x\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+f_1(x,y)\exp\left[-\mathrm{j}2\pi(x+y)\frac{\sin 6^\circ}{\lambda}\right]+f_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x+y)\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+g_1(x,y)\exp\left[-\mathrm{j}2\pi y\frac{\sin 6^\circ}{\lambda}\right]+g_1^*(x,y)\exp\left[\mathrm{j}2\pi\left(y\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right]\\
&\quad+p_2(x,y)+h_1(x,y)\exp\left[-\mathrm{j}2\pi(x-y)\frac{\sin 6^\circ}{\lambda}\right]+h_1^*(x,y)\exp\left[\mathrm{j}2\pi\left((x-y)\frac{\sin 6^\circ}{\lambda}+2M(x,y)\right)\right].
\end{aligned}
\tag{9}
$$

经过图 6(a) 所示的相应滤波器滤波, 并经过正确衍射距离 z_i 的菲涅耳衍射后光场分布为

$$\begin{aligned}
&a^*(x,y)p_{11}^*(x,y) = \mathrm{FrT}z_1[\mathrm{F}_1(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_1[a_1^*(x,y),\lambda],\\
&b^*(x,y)p_{12}^*(x,y) = \mathrm{FrT}z_2[\mathrm{F}_2(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_2[b_1^*(x,y),\lambda],\\
&c^*(x,y)p_{13}^*(x,y) = \mathrm{FrT}z_3[\mathrm{F}_3(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_3[c_1^*(x,y),\lambda],\\
&d^*(x,y)p_{14}^*(x,y) = \mathrm{FrT}z_4[\mathrm{F}_4(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_4[d_1^*(x,y),\lambda],\\
&e^*(x,y){p_{15}}^*(x,y) = \mathrm{FrT}z_5[\mathrm{F}_5(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_5[e_1^*(x,y),\lambda],\\
&f^*(x,y)p_{16}^*(x,y) = \mathrm{FrT}z_6[\mathrm{F}_6(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_6[f_1^*(x,y),\lambda],\\
&g^*(x,y)p_{17}^*(x,y) = \mathrm{FrT}z_7[\mathrm{F}_7(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_7[g_1^*(x,y),\lambda],\\
&h^*(x,y)p_{18}^*(x,y) = \mathrm{FrT}z_8[\mathrm{F}_8(I(x,y)p_2^*(x,y)),\lambda] = \mathrm{FrT}z_8[h_1^*(x,y),\lambda]. \qquad (10)
\end{aligned}$$

从 (10) 式可见, 经过滤波和菲涅耳衍射后, 用 CCD 接收到原始图像的共轭, 完成解密, 获得解密图像如图 7 所示.

由图 7 可见, 用正确的密钥和滤波器可解密获得原始图像的共轭图像, 由于每个图像的 0 级和 –1 级频谱被调制为噪声弥散到整个频谱空间, 通过滤波器后形成了噪声, 对解密结果有一定的干扰. 但弥散在整个频谱的噪声通过滤波器的占比仍然较小, 对解密结果影响不大, 因此仍获得了令人满意的解密结果.

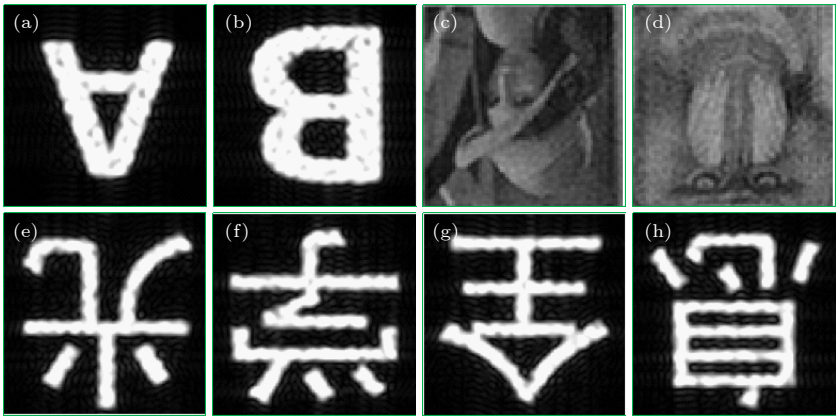

图 7 (a)—(h) 8 个图像的正确密钥解密结果

Fig. 7. (a) – (h) 8 Decrypted images with all right keys.

4 加密系统安全性及容量分析

4.1 安全性分析和测试

加密之后的图像通过公共通信信道传输后, 存在信息失真的多种可能性. 因此, 为进一步说明和验证本文所提出的多图像加密方法的可行性和有效性, 引入相关系数 CC 来评价解密结果的质量, 定义如下:

$$CC = \frac{\sum_m \sum_n (o(m,n)-\overline{o})(o'(m,n)-\overline{o'})}{\sqrt{\left(\sum_m \sum_n (o(m,n)-\overline{o})^2\right)\left(\sum_m \sum_n (o'(m,n)-\overline{o'})^2\right)}}, \qquad (11)$$

其中, $o(x,y)$和$o'(x,y)$分别表示原始图像和解密图像, $\overline{o}$和$\overline{o'}$分别表示$o(x,y)$和$o'(x,y)$的平均值.

本文提出的多图像光学加密方法中, 除随机相位密钥以外, 菲涅耳衍射距离和激光波长都可作为附加密钥. 首先, 当所有密钥都正确时解密结果 (图 7) 与原始图像 (图 2) 的 CC 值分别为 $CC_1 = 0.9239$, $CC_2 = 0.9077$, $CC_3 = 0.8432$, $CC_4 = 0.8072$, $CC_5 = 0.9029$, $CC_6 = 0.8883$, $CC_7 = 0.8929$, $CC_8 = 0.9040$. 可见, 当所有密钥都正确时通过解密可以很好地获得原始图像的信息. 将解密结果中图 7(c) 和图 7(d) 与其他二值图像解密结果对比发现, 灰度图像解密结果质量要差一些, 其 CC 值也相对较低, 可见本文提出的多图像加密方

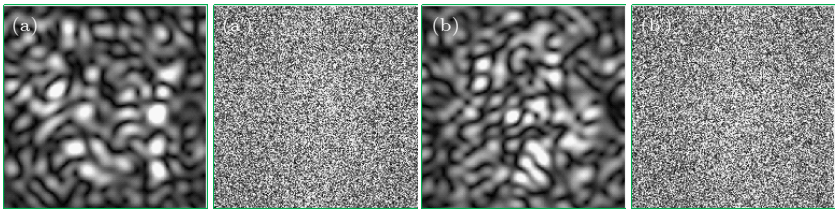

图 8 (a) 随机相位密钥 p_2^* 错误时原始图“A”解密结果; (a′) 随机相位密钥 p_2^* 错误且无滤波器时原始图“A”解密结果; (b) 随机相位密钥 p_2^* 错误时原始图“光”解密结果; (b′) 随机相位密钥 p_2^* 错误且无滤波器时原始图“光”解密结果

Fig. 8. Decrypted results with wrong key p_2^*: (a) For original image “A”; (a′) for original image “A” without filter; (b) for original image “光”; (b′) for original image “光” without filter.

法更适用于二值图像, 因为输入平面的振幅和相位随机性对解密结果影响很大. 图 8 为随机相位密钥 p_3 错误、其他密钥都正确时的解密结果图, 以原始图“A”(图 8(a)) 和原始图“光”(图 8(b)) 为例.

由图 8 可见, 当随机相位密钥错误时, 有滤波器解密得到图 8(a) 和图 8(b), 解密结果图与原始图像的相关系数仅有 $CC = 0.0873$ 和 $CC = 0.0914$, 无滤波器时解密得到图 8(a′) 和图 8(b′), 均类似均匀噪声, 没有原始图像的任何信息.

图 9 为菲涅耳衍射距离波长 λ 错误其他密钥正确时的解密结果, 以原始图“B”(图 9(a)) 和原始图“学”(图 9(b)) 为例.

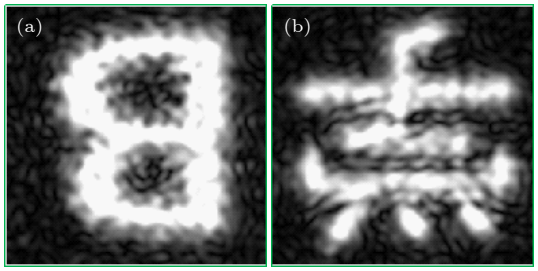

图 9 (a) 波长 $\lambda = 633$ nm 其他密钥正确时原始图“B”的解密图像; (b) 原始图“学”的解密图像

Fig. 9. Decrypted results with wrong key $\lambda = 633$ nm: (a) For original image “B”; (b) for original image “学”.

由图 9 可见, 当光源波长错误 $\lambda = 633$ nm 时, 解密得到图 9(a) 和图 9(b), 解密结果图与原始图像的相关系数仅有 $CC = 0.3038$ 和 $CC = 0.3391$, 解密结果图像质量极大地下降, 并且对每个图像应用不同波长进行加密时更具有迷惑性, 因此, 光源波长可作为该多图像加密方法的附加密钥.

解密结果与另一个重要参数菲涅耳衍射距离 z_i 依赖关系如图 10 所示 (以原始图像“息”为例). 当所有密钥正确时, CC 值在 0.9 左右, 可以获得良好的解密结果. 虽然本文将随机相位的动态范围从 0—2π 压缩到 0—π 以提高解密图像的质量, 大大降低了衍射距离的灵敏度, 但 CC 值仍随 z_i 偏差的增大而迅速减小, 当误差大于 1.5 cm 时, CC 小于 0.2, 无法区分插图中所示的解密图像. 因此, 该多图像光学加密方法对菲涅耳衍射距离 z_i 是高度敏感的, z_i 可作为附加密钥来提高安全性.

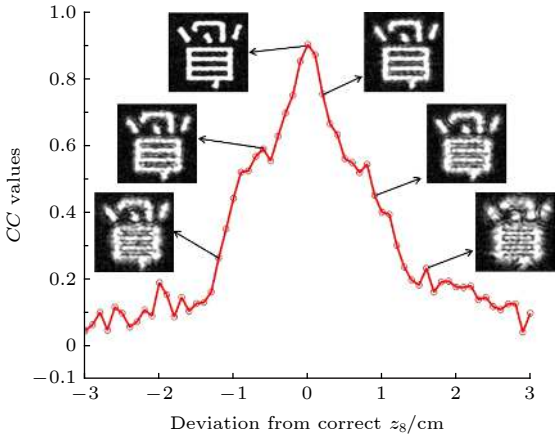

图 10 当 p_1 的动态范围为 0—π 时原始图“息”的 CC 随菲涅耳衍射距离 z_8 的变化

Fig. 10. The CC dependence on z_8 when the dynamic range of p_1 is 0 – π.

从图 9 和图 10 可见, 附加密钥波长 λ 和菲涅耳衍射距离 z_i 错误且与正确密钥差别较小时, 虽然 CC 值迅速减小, 但仍然有原始图像轮廓出现. 这是因为将随机相位 p_1 的动态范围从 0—2π 压缩到 0—π 后提高了解密图像的质量, 降低了图像加密系统对附加密钥的灵敏度. 因此, 本文将随机相位 p_1 的动态范围提高到 0—1.5π, 验证解密结果与菲涅耳衍射距离 z_i 依赖关系, 结果如图 11 所示.

通过对比图 10 和图 11, 当随机相位 p_1 的动态范围提高时, 正确解密密钥 z_i 应用时, 解密结果质量降低, 对应的 CC 值由高于 0.9 下降到 0.8 以上, 但是 CC 值随密钥 z_i 误差变化的曲线斜率明显变

大, 即图像加密系统对附加密钥 z_i 的灵敏度大幅提高. 因此, 随机相位 p_1 的动态范围应合理选取, 既要保证图像加密系统的安全性, 又要兼顾解密图像的质量.

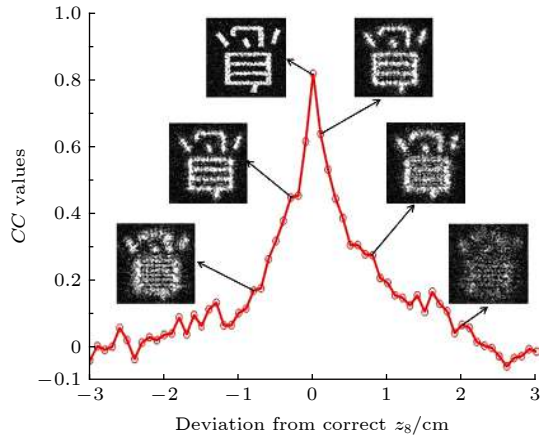

图 11 当 p_1 的动态范围为 0—1.5π时原始图“息”的 CC 随菲涅耳衍射距离 z_8 的变化

Fig. 11. The CC dependence on z_8 when the dynamic range of p_1 is 0 – 1.5π.

4.2 加密系统的复用容量分析

对于多图像加密而言, 多图像加密系统的加密容量是一个关键参数. 文献 [16] 给出了复用容量的概念, 即达到设定的图像解密质量评判阈值时, 该项复用技术可以加密的最大原始图像数量. 为了分析本文提出的多图像加密系统的复用容量, 以同时加密多个二值图像“A”字母为例, 设定所有解密图像的 CC 平均值为 0.9, 即 $\overline{CC}=0.9000$ 为图像解密质量阈值, 其中 $\overline{\bullet}$ 表示平均值. 同时加密二值图像“A”字母的个数可通过改变参考光立体角度 $(\alpha_i,\ \theta_i)$ 的 α_i 和 θ_i 参数设定, 经过模拟实验和计算获得该值为 32, 当阈值设定为 $\overline{CC}=0.8000$ 时, 得到够同时加密二值图像“A”字母的个数为 64. 可见本文提出的多图像光学加密系统具有较高的复用容量.

5 结 论

本文提出了基于空间角度复用和双随机相位的多图像光学加密方法. 该方法利用数字全息的空间角度复用技术将多个图像加密为单个灰度图像, 易于保存和传输; 利用基于干涉原理的双随机相位光学图像加密技术, 将双随机相位分别置于物光和参考光, 降低了加密系统的复杂度; 同时将第二个随机相位板放置于参考光束可克服传统方法解密实验中随机相位密钥难以逐像素对齐的问题, 而且参考光可进行随机相位复用, 进一步提高了加密系统的容量, 同时通过多图像加密系统的复用容量分析, 获得了该系统的加密容量. 因此, 该方法可以同时对多幅图像进行高效的加密, 计算简单、安全可靠、抗噪声能力强, 在信息安全领域具有重要的应用价值.

参考文献

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Liu Z, Chen H, Blondel W, Shen Z, Liu S 2018 *Opt. Lasers Eng.* **105** 1
[3] Chen L, Zhao D 2006 *Opt. Express* **14** 8552
[4] Zhao D, Li X, Chen L 2008 *Opt. Commun.* **281** 5326
[5] Xu S J, Wang J Z, Yang S X 2008 *Chin. Phys. B* **17** 4027
[6] Borujeni S E, Eshghi M 2013 *J. Telecommun. Syst.* **52** 525
[7] Toto-Arellano N, Rodriguez-Zurita G, Meneses-Fabian C, Vazquez-Castillo J 2008 *Opt. Express* **16** 19330
[8] Nomura T, Javidi B 2000 *Opt. Eng.* **39** 2031
[9] Shi Y S, Li T, Wang Y L, Gao Q K, Zhang S G, Li H F 2013 *Opt. Lett.* **38** 1425
[10] Gopinathan U, Naughton T, Sheridan J 2006 *Appl. Opt.* **45** 5693
[11] Javidi B, Nomura T 2000 *Opt. Lett.* **25** 28
[12] Xi S X, Yu N N, Wang X L, Zhu Q F, Dong Z, Wang W, Liu X H, Wang H Y 2019 *Acta. Phys. Sin.* **68** 110502 (in Chinese) [席思星, 于娜娜, 王晓雷, 朱巧芬, 董昭, 王微, 刘秀红, 王华英 2019 物理学报 **68** 110502]
[13] Li X, Meng X, Yang X, Wang Y, Yin Y, Peng X, He W, Dong G, Chen H 2018 *Opt. Lasers Eng.* **102** 106
[14] Xiao D, Li X, Liu S, Wang Q 2018 *Opt. Commun.* **410** 488
[15] Shao Z, Shu H, Wu J, Dong Z, Coatrieux G 2014 *Opt. Express* **22** 4932
[16] Situ G, Zhang J 2005 *Opt. Lett.* **30** 1306
[17] Xu D, Lu M, Jia C, Hu Z 2017 *J. Russ. Laser Res.* **38** 285
[18] Deepan B, Quan C, Wang Y, Tay C 2014 *Appl. Opt.* **53** 4539
[19] Tang Z, Song J, Zhang X 2016 *Opt. Lasers Eng.* **80** 1
[20] Kong D, Shen X, Xu Q, Wang X, Guo H 2013 *Appl. Opt.* **52** 2619
[21] Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M S, Nishchal N K, Torroba R, Barrera J F, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan J T, Situ G, Naruse M, Matsumoto T, Juvells L, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse P W, Mosk A P, Markman A 2016 *J. Opt.* **18** 083001

Multiple-image encryption method based on spatial angle multiplexing and double random phase encoding*

Wang Xue-Guang [1)2)] Li Ming [1)] Yu Na-Na [2)] Xi Si-Xing [2)†]
Wang Xiao-Lei [3)] Lang Li-Ying [4)]

1) (*School of Information and Control Engineering, China University of Mining and Technology, Xuzhou* 221116, *China*)

2) (*School of Mathematics and Physics, Hebei University of Engineering, Handan* 056038, *China*)

3) (*Institute of Modern Optics, Nankai University, Tianjin* 300350, *China*)

4) (*Hebei University of Technology, Tianjin* 300401, *China*)

(Received 8 September 2019; revised manuscript received 8 October 2019)

Abstract

An optical encryption method of multiple-image based on spatial angle multiplexing and double random phase encoding is proposed in this paper. In the encryption process, firstly the original images are modulated by random phase in Fresnel transform with different diffraction distances. Secondly, the modulated images are coherently superposed with reference beams which have different spatial angles and random phases, to generate interference fringes. Finally, the interference fringes from different directions are superposed to form a compound encrypted image. In the decryption process, the compound image is placed in a spatial filtering and Fresnel diffraction system, and the decrypted images are obtained after implementing the different phase keys' demodulation and Fresnel diffraction with correct distance. This method encrypts multiple images into a single gray-scale image, which is easy to save and transmit. The double random phases are placed in object light and reference light respectively, which reduces the complexity of the encryption system and overcomes the difficulty of pixel-by-pixel alignment of random phase keys in traditional decryption experiment. At the same time, the multiplexing capacity of the proposed encryption system is analyzed, and the result shows that the system has sufficient encryption capacity. So the proposed method possesses the characteristics of high storage efficiency, simple calculation and strong anti-noise ability, and thus can encrypt multiple images simultaneously. In this paper, the encryption effect is evaluated by correlation coefficient, while the effectiveness and security are verified by simulation experiment.

Keywords: multiple-image encryption, spatial angle multiplexing, digital holography, interference encryption

PACS: 05.45.Gg, 42.30.Va, 42.30.Wb **DOI:** 10.7498/aps.68.20191362

* Project supported by the National Natural Science Foundation of China (Grant Nos. 11904073, 61875093), the Natural Science Foundation of Hebei Province, China (Grant Nos. F2019402351, F2018402285), and the Natural Science Foundation of Tianjin, China (Grant No. 19JCYBJC16500) .

† Corresponding author. E-mail: xisixing@126.com