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

基于计算全息和θ调制的彩色图像加密方法

席思星 于娜娜 王晓雷 朱巧芬 董昭 王微 刘秀红 王华英

Color image encryption method based on computer generated hologram and θ modulation

Xi Si-Xing Yu Na-Na Wang Xiao-Lei Zhu Qiao-Fen Dong Zhao Wang Wei Liu Xiu-Hong Wang Hua-Ying

引用信息 Citation: Acta Physica Sinica, 68, 110502 (2019) DOI: 10.7498/aps.68.20182264
在线阅读 View online: https://doi.org/10.7498/aps.68.20182264
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于计算全息和 θ 调制的彩色图像加密方法*

席思星[1)] 于娜娜[1)] 王晓雷[2)†] 朱巧芬[1)] 董昭[1)]
王微[1)] 刘秀红[1)] 王华英[1)]

1) (河北工程大学数理科学与工程学院, 邯郸 056038)

2) (南开大学现代光学研究所, 天津 300350)

(2018 年 12 月 25 日收到; 2019 年 3 月 19 日收到修改稿)

提出了一种基于计算全息和 θ 调制的彩色图像光学加密新方法. 该方法利用彩色三基色原理和计算全息编码技术, 首先将彩色图像的红、绿、蓝三基色分量进行随机相位调制和菲涅耳衍射变换, 然后经过 θ 调制后进行图像叠加并编码为计算全息图, 即加密过程是将一幅彩色图像加密为一幅实值的二元计算全息图, 得到单幅密文. 解密为加密的逆过程, 首先将加密的计算全息图置于空间滤波和菲涅耳衍射系统中, 经过相位密钥解调和基于滤光片的滤波器滤波, 最后通过正确距离的菲涅耳衍射完成解密, 得到彩色明文图像. 计算机模拟结果证明了该方法的有效性和可行性.

关键词: 彩色图像加密, 计算全息, θ 调制, 非对称加密

PACS: 05.45.Gg, 42.30.Va, 42.30.Wb **DOI:** 10.7498/aps.68.20182264

1 引 言

在双随机相位图像加密技术[1]提出后, 不断出现了许多改进的加密系统, 如分数傅里叶变换加密系统[2]、菲涅耳变换加密系统[3]、混沌和置乱加密系统[4], 这些系统在加密时除了两个随机相位密钥以外, 还有附加密钥, 增强了系统的安全性和抵御攻击的能力. 但这些加密系统都采用单色光照射, 解密的图像都是二值图像或者灰度图像. 近年来, Shi 等[5]首次提出将叠层衍射成像技术应用于光学图像加密, 他们在 $4f$ 系统中用光学探针扫描原始灰度图像并经过随机相位密钥调制, 最后记录加密图像的振幅完成加密; 解密通过叠层衍射成像的迭代运算完成. 随后他们[6]又提出了一种基于可视密码和体全息光栅技术的光学图像加密方法, 该方法将二值图像加密到可视密码中并将其伪装成二维码, 最后通过体全息光栅曝光记录完成加密; 解密通过体全息光栅的光学再现完成. 然而, 彩色图像在图像细节、逼真度和色彩表现等方面是灰度图像所不能比拟的, 因此彩色图像加密有巨大的研究价值和应用空间, 彩色图像加密也逐渐成为国内外学者和研究人员的研究热点[7–10]. 当前的彩色图像加密方案主要基于空域彩色图像加密和变换域彩色图像加密, 前者主要利用混沌系统直接置乱图像的像素 (值) 和位置, 后者是对变换域系数进行加密处理. 例如肖迪和谢沂均[11]采用彩色图像 JPEG 压缩编码提出了一种彩色图像加密方法. 秦怡和郑长波[12]提出了基于傅里叶变换和双随机相位编码的彩色图像加密方案. Yuan 等[13]利用棋盘光栅和衍射成像实现了彩色图像的单通道光学加密.

目前彩色图像的加密方法主要基于彩色三基色原理和彩色图像的编码方法[14], 其在加密过程中把彩色图像分解为红、绿、蓝三个通道的子图像,

* 国家自然科学基金 (批准号: 61875093, 61465005) 和河北省自然科学基金 (批准号: F2018402285) 资助的课题.

† 通信作者. E-mail: wangxiaolei@nankai.edu.cn

每个子图像采用灰度图像的加密方法. 每个通道的参数和随机相位掩模都可作为密钥, 只要有一条通道上的解密密钥是未知的, 就无法获得正确的明文信息[15]. 这类方法提高了加密的安全性, 但是其加密系统相对比较复杂, 实现成本比较高, 不利于实际应用. 因此, 杨晓苹等[16,17]利用彩色图像空间转化提出了基于双相位编码的单通道彩色图像加密方法; Zhou 等[18]提出单通道彩色图像加密方法, 将彩色图像 R, G, B 三个分量编码成一个灰度图像, 再对灰度图像进行加密, 降低了加密装置的要求和成本. 本文在双随机相位图像加密和计算全息的基础上, 提出基于 θ 调制原理的彩色图像加密技术, 即对彩色图像的 R, G, B 三个分量分别进行加密并在空域叠加, 其中 θ 调制的作用是使 R, G, B 三个分量在空域重叠而在频域分离, 从而可以在解密过程中恢复出每个色彩分量. 由于该方法只需要一个菲涅耳衍射和 θ 调制的加密和解密装置, 因此降低了对实验装置和操作性的要求. 最终的加密结果为一幅二元实值的计算全息图 (computer generated hologram, CGH), 不仅完全隐藏了彩色图像的信息, 而且易于存储和传输. 除了传统的双随机相位密钥外, 该方法中的菲涅耳衍射距离和 θ 调制的滤波器等都是关键的密钥, 并且计算全息加密图像具有高的抗剪切和抗噪能力. 同时, 本文采取了相位截断非对称加密系统, 并进行低频滤波处理的方法, 使得安全性被进一步提高[19,20]. 因此, 本文提出的彩色图像加密技术在信息安全领域具有重要的应用价值.

2 加密过程

本文提出的彩色图像的加密过程分为三基色分量 θ 调制加密和计算全息编码两个步骤, 第一个步骤在图 1 所示的菲涅耳衍射和 θ 调制的 $4f$ 系统中完成.

在图 1 所示的加密系统中, 待加密彩色图像放置于物平面 Σ_1, 紧贴待加密图像的是随机相位板 $p_1(x,y)$(random phase mask, RPM_1). 红色、绿色和蓝色激光器同时照射物平面 Σ_1 加载待加密彩色图像信息, 然后经过 RPM_1 的调制和距离为 z_0 的菲涅耳衍射, 到达菲涅耳衍射物平面 Σ_2, 衍射过程中依次使用红、绿、蓝三个单色滤波光片分别选出三基色分量. 每个分量经过平面 Σ_2 上的透射式振幅型正弦光栅和傅里叶频谱面 Σ_3 的滤波器调制. 每加密一个分量, 正弦光栅和滤波器同步逆时针旋转 60°, –1 级频谱经过傅里叶变换到达像面 Σ_4 被二维图像探测器记录.

本文所选取的待加密彩色图像如图 2 所示, 其图像分布可表达为 $o(x,y)$, 像素数为 128 × 128 的三维矩阵, 其三基色分量分别为 $o_{\mathrm{R}}(x,y)$, $o_{\mathrm{G}}(x,y)$, $o_{\mathrm{B}}(x,y)$, 因此可以得到

$$o(x,y)=o_{\mathrm{R}}(x,y)+o_{\mathrm{G}}(x,y)+o_{\mathrm{B}}(x,y). \tag{1}$$

菲涅耳衍射距离选取 $z_0=0.3$ m, 加密过程可表示为:

$$\begin{aligned}
o'_{\mathrm{R}}(x,y)r_{\mathrm{R}}(x,y)&=F_1\{FrT_{z_0}[o_{\mathrm{R}}(x,y)p_1(x,y),633\ \mathrm{nm}]H_0(x,y)\},\\
o'_{\mathrm{G}}(x,y)r_{\mathrm{G}}(x,y)&=F_2\{FrT_{z_0}[o_{\mathrm{G}}(x,y)p_1(x,y),532\ \mathrm{nm}]H_{60}(x,y)\},\\
o'_{\mathrm{B}}(x,y)r_{\mathrm{B}}(x,y)&=F_3\{FrT_{z_0}[o_{\mathrm{B}}(x,y)p_1(x,y),400\ \mathrm{nm}]H_{120}(x,y)\},
\end{aligned} \tag{2}$$

其中 $p_1(x,y)$为随机相位, $FrT_{z_0}[\bullet,633\ \mathrm{nm}]$表示衍射距离为 z_0、波长为 633 nm 的菲涅耳衍射, $Hi(x,y)$ 为光栅条纹与 x 轴夹角为 i°的光栅函数, 其中 i 分别为 0°, 60°和 120°, $F_1\{\bullet\}$表示与 $H_0(x,y)$对应的

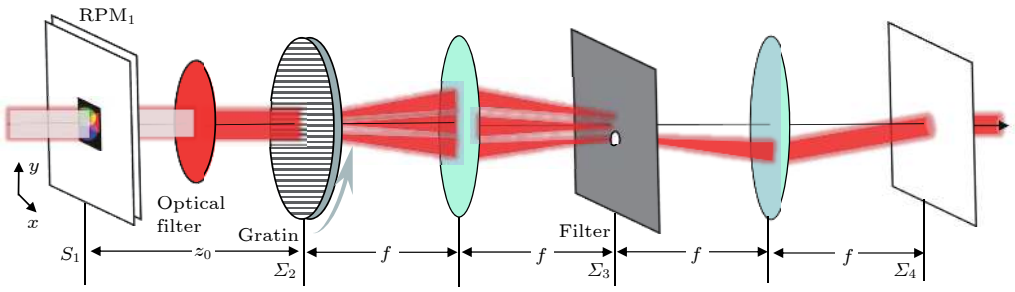


图 1 彩色图像的菲涅尔衍射和 θ 调制系统

Fig. 1. Fresnel diffraction and θ modulation system for color image.

图 2 待加密彩色图像

Fig. 2. Color image to be encrypted.

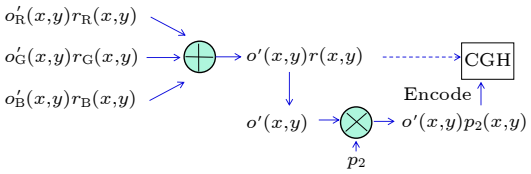


图 3 彩色图像加密的计算全息编码流程图

Fig. 3. Flow chart of color image encryption by computer generated hologram.

滤波过程, 其余同理.

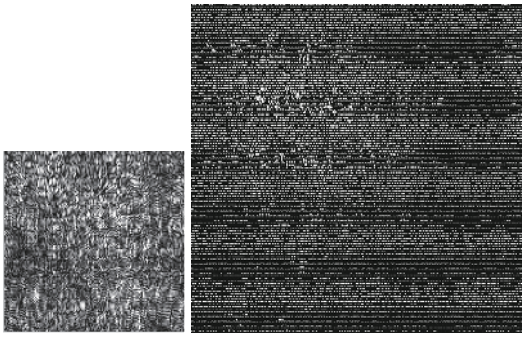
第二个步骤为计算全息编码过程, 编码流程如图 3 所示.

图 3 中, 经过第一步调制后的三基色分量复振幅分别为$o'_R(x,y)r_R(x,y)$, $o'_B(x,y)r_B(x,y)$和$o'_G(x,y)r_G(x,y)$. 将三个复振幅进行叠加, 叠加过程可用下式表示:

$$\begin{aligned} &o'(x,y)r(x,y)\\ &=o'_R(x,y)r_R(x,y)+o'_G(x,y)r_G(x,y)\\ &\quad+o'_B(x,y)r_B(x,y). \end{aligned} \tag{3}$$

为了提高加密系统的安全性, 将振幅$o'(x,y)$保留而将相位信息$r(x,y)$去除, 以破坏加密系统的线性关系. 振幅$o'(x,y)$经过第二个随机相位$p_2(x,y)$的调制, 获得加密复振幅$o'(x,y)p_2(x,y)$, 其强度分布如图 4(a) 所示. 最后对所获得的加密复振幅$o'(x,y)p_2(x,y)$进行计算全息编码得到二元实值计算全息加密图, 在此过程中, 采用的计算全息编码单元为 9 pixel× 9 pixel, 所以最终得到加密全息图总像素数为 128 × 128 × 9 × 9, 如图 4(b) 所示, 完成加密.

传统彩色图像加密方法的加密结果为 R, G, B 三幅图或单幅彩色图[7–12], 而图 4(b) 显示的加密结果为一幅灰度二元实值计算全息图[21], 该图完全隐藏了原始彩色图像的灰度和色彩信息, 在传输和存储过程中更具有一般性和迷惑性.



(a) (b)

图 4 (a) 加密结果图; (b) 加密计算全息图

Fig. 4. (a) The encrypted image; (b) the encrypted computer generated hologram.

3 解 密

彩色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 系统和一次菲涅耳衍射过程, 光源为与加密过程相同的红色、绿色和蓝色激光. 在第一个 4f 系统的入射面放置一个纯相位型空间光调制器 (SLM), 用以加载加密计算全息图 (图 4); 在该 4f 系统的出射面放置第二个 SLM, 用以加载计算全息相位密钥. 其中相位密钥表达式为

$$p_2'(x,y)=\frac{r(x,y)}{p_2(x,y)}. \tag{4}$$

(4) 式表明相位密钥p_2'为 128 × 128 像素, 为了达到解密的效果, 相位密钥p_2'应与加密全息图 (图 4 所示) 具有相同的像素数, 因此利用计算全息方法将解密密钥p_2'进行编码扩充, 编码单元也是 9 pixel × 9 pixel, 即计算全息相位密钥最终具有 128 pixel × 9 pixel × 128 pixel× 9 pixel.

图 5 中由第一个 4f 系统连接的两个 SLM, 其作用相当于将计算全息相位密钥紧贴计算全息加密图放置, 在该 4f 系统的出射面上的光场可表示为

$$\begin{aligned} &o'(x,y)p_2(x,y)p_2'(x,y)=o'_R(x,y)r_R(x,y)\\ &\quad+o'_G(x,y)r_G(x,y)+o'_B(x,y)r_B(x,y). \end{aligned} \tag{5}$$

在图 5 中的第二个 4f 系统中, 频谱面上放置带有三色滤光片的滤波器. 由于在加密过程中对三基色分别进行了不同角度的 θ 调制, 因此携带颜色信息的–1 级衍射光将分别经过滤波器的不同位置, 并通过相应的滤光片从而恢复出色彩值. 在此之后, 经过距离z_0的菲涅耳衍射, 此时所恢复的三基色光

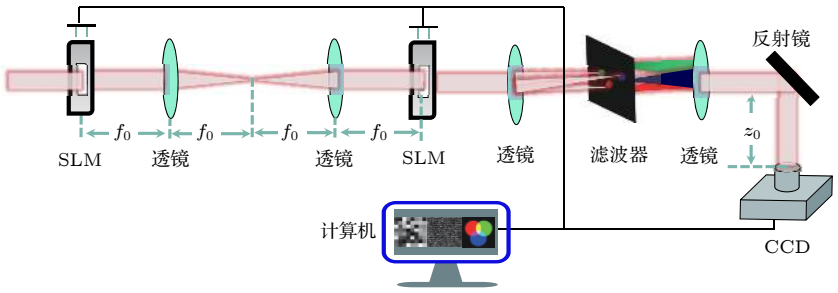


图 5 彩色图像解密系统

Fig. 5. Decryption system of color image.

$$\begin{aligned} o^*{}_{\mathrm{R}}(x,y)p^*{}_1(x,y) &= FrT_{z_0}[F_1\{o'_{\mathrm{R}}(x,y)r_{\mathrm{R}}(x,y)\}, 633\ \mathrm{nm}], \\ o^*{}_{\mathrm{G}}(x,y)p^*{}_1(x,y) &= FrT_{z_0}[F_2\{o'_{\mathrm{G}}(x,y)r_{\mathrm{G}}(x,y)\}, 532\ \mathrm{nm}], \\ o^*{}_{\mathrm{B}}(x,y)p^*{}_1(x,y) &= FrT_{z_0}[F_3\{o'_{\mathrm{B}}(x,y)r_{\mathrm{B}}(x,y)\}, 400\ \mathrm{nm}]. \end{aligned} \tag{6}$$

上述三基色分量叠加得到解密彩色图像, 由电荷耦合器接收. 在正确的解密密钥p_2'、正确的滤波器和正确的菲涅耳衍射距离下, 解密结果如图 6(a)所示, 解密图像为原始彩色图像的共轭图像, 经过反转可获得原始彩色图像, 如图 6(b) 所示, 可见较好地恢复了彩色图像的灰度和色彩信息, 完成解密.

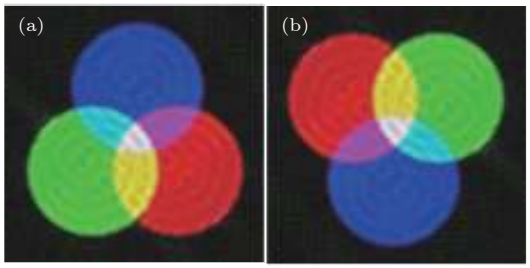


图 6 解密彩色图像

Fig. 6. Decrypted color image.

4 安全性分析和测试

4.1 密钥安全性分析

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方法的可行性和有效性, 引入相关系数 (correlation coefficien, CC) 和图像逼真度 (image fidelity, IF) 来评价解密结果的质量, 分别定义如下:

$$\mathrm{CC} = \frac{\sum_m \sum_n (o(m,n)-\overline{o})(o'(m,n)-\overline{o'})}{\sqrt{\left(\sum_m \sum_n (o(m,n)-\overline{o})^2\right)\left(\sum_m \sum_n (o'(m,n)-\overline{o'})^2\right)}}, \tag{7}$$

其中$\overline{o}$和$\overline{o'}$分别表示$o(x,y)$和$o'(x,y)$的平均值.

$$\mathrm{IF} = 1 - \sum_{i=1}^{L}(o_i - o_i')^2 \Big/ \sum_{i=1}^{L} o_i{}^2, \tag{8}$$

式中o_i和o_i'分别表示图像中的某个像素点灰度值和对应的破解结果值, L表示图像中具有的像素总数. 由 (8) 式和 (9) 式可知, 相关系数和图像逼真度的值越大, 破解图像与原始图像的差异就越小, 图像逼真度值就越高.

本文提出的光学图像加密方法中, 除双随机相位密钥以外, 菲涅耳衍射距离和滤波器都可作为附加密钥. 图 7(a) 为随机相位密钥p_2'错误、其他密钥都正确时的解密结果图, 可见解密结果图完全丢失了原始彩色图像的信息, 解密结果图与原始图像的相关系数为$\mathrm{CC} = 0.007$, 图像逼真度$\mathrm{IF} = 0.011$. 图 7(b) 为菲涅耳衍射距离$z_0 = 0.35$ m、其他密钥都正确时的解密结果图, 解密结果图与原始图像的相关系数为$\mathrm{CC} = 0.021$, 图像逼真度$\mathrm{IF} = 0.043$, 可

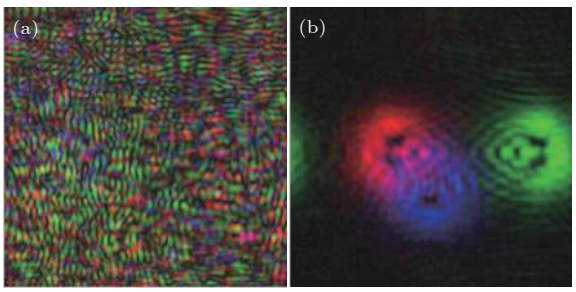


图 7 密钥错误时的解密结果 (a) 相位密钥p_2'错误; (b) 菲涅耳衍射距离错误 ($z_0 = 0.35$ m)

Fig. 7. Decrypted results with wrong keys: (a) Wrong key p_2'; (b) wrong key Fresnel diffraction distance with $z_0 = 0.35$ m.

见菲涅耳衍射距离作为图像加密密钥也获得了很好的加密效果.

解密时, 设置滤波器分别只恢复彩色图像的R, G 和 B 三个分量, 如图 8(a)—(c) 所示, 图 8(a)—(c) 是相应的原始三基色分量, 它们对应的相关系数分别为CC = 0.876, CC = 0.891, CC = 0.903, 图像逼真度分别为IF = 0.881, IF = 0.900, IF = 0.911. 从图 8 可以看出, 恢复出来的图像丢失了部分细节信息. 造成该现象的原因有两个: 一是由于第一个随机相位密钥的散射作用使得部分高频分量在截取傅里叶频谱时被舍去; 二是加密结果的计算全息量化编码引入了一定误差. 经验证, 当降低第一个随机相位密钥的动态取值范围并增加计算全息量化编码的像素点数时, 解密图像的质量会出现很大提升. 因此, 原始图像的灰度和色彩信息可以被恢复出来, 其恢复质量在一定程度上取得了令人满意的效果.

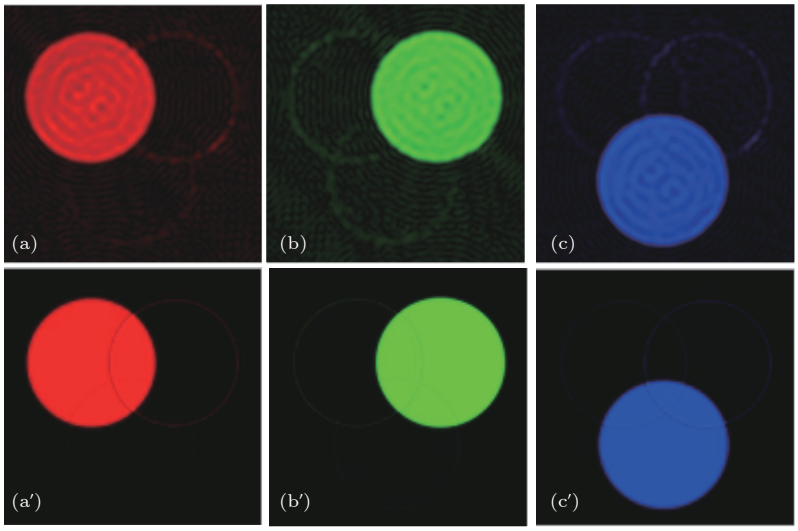


图 8 解密彩色图像三基色分量 (a) 红色分量; (b) 绿色分量; (c) 蓝色分量; (a'), (b'), (c') 原始图像三基色分量

Fig. 8. Tricolor components of color image: (a) Red component; (b) green component; (c) blue component; (a'), (b'), (c') red, green and blue components of original color image.

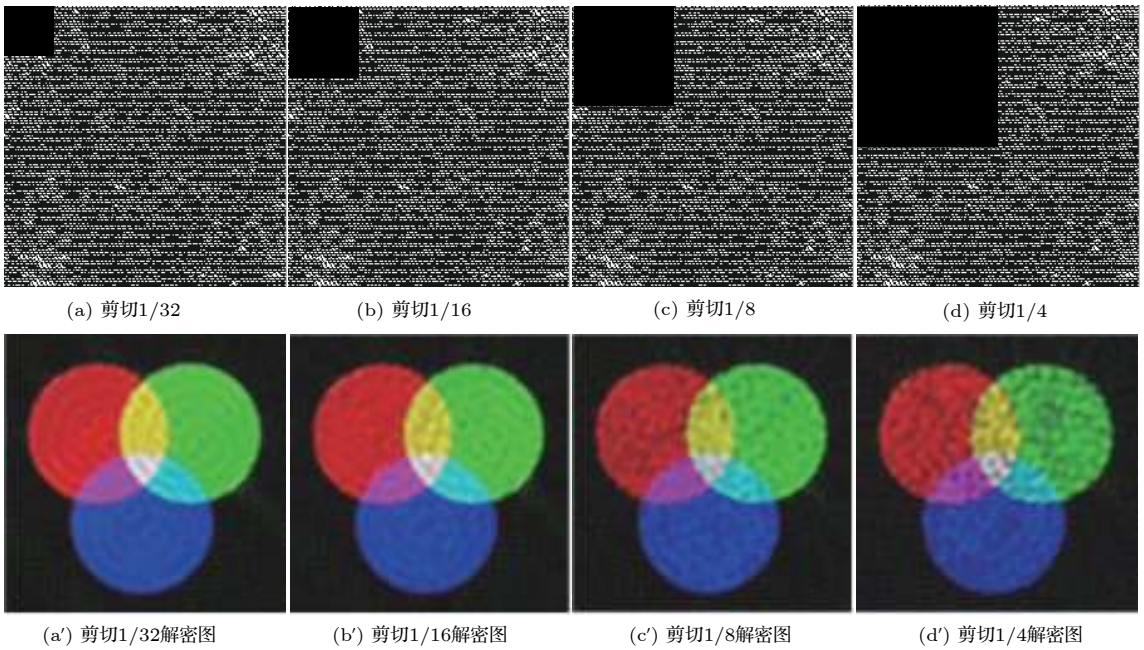


图 9 不同程度的剪切攻击和剪切攻击后的恢复图像

Fig. 9. Shear attack of different levels and image restoration after shear attack.

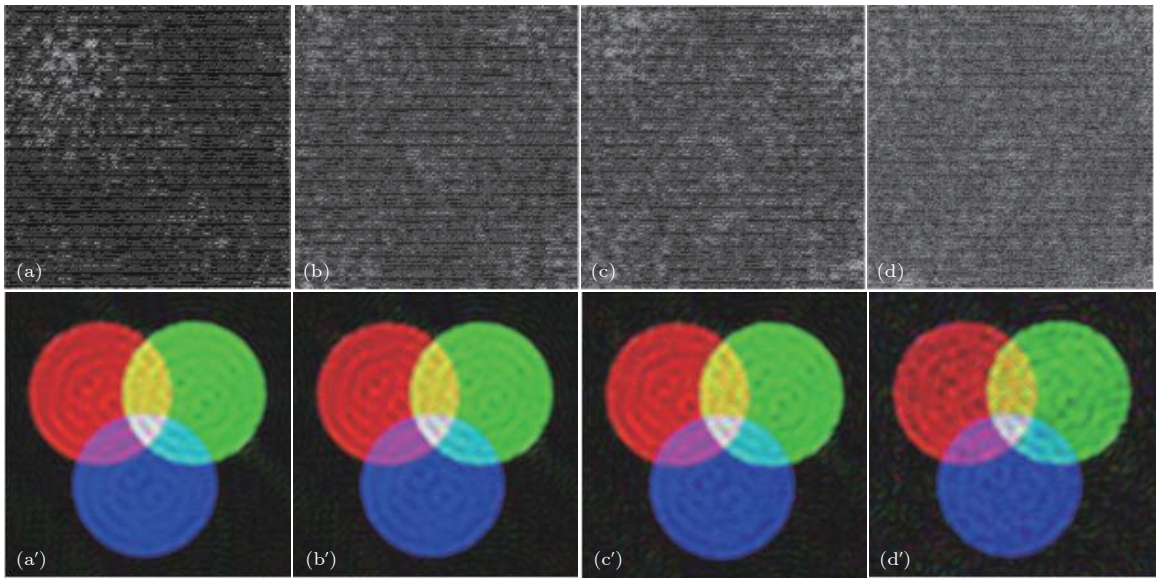


图 10 (a)—(d) 分别加入密度 0.1, 0.3, 0.5 和 1.0 的椒盐噪声后的加密图像; (a')—(d') 相应的解密结果图

Fig. 10. (a) – (d) Encrypted images with salt and pepper noises with density of 0.1, 0.3, 0.5 1.0; (a') – (d') corresponding decryption results.

4.2 抗剪切攻击测试

本文还针对加密图像做了抗剪切和抗噪声模拟实验, 图 9 给出了对加密图像做不同程度剪切后的实验结果和经剪切攻击后恢复得到的解密图像.

表 1 为针对加密图像做剪切攻击实验的数据, 重构的解密图像仍然具有较好的视觉效果.

表 1 剪切攻击处理

Table 1. Treatment of shear attack.

剪切攻击		1/32	1/16	1/8	1/4
评价标准	CC	0.858	0.803	0.765	0.668
	IF	0.873	0.811	0.750	0.671

4.3 抗噪声攻击测试

为了测试该图像加密系统的抗噪声性能, 将不同密度的椒盐噪声加入到加密图像中. 图 10 是密度分别为 0.1, 0.3, 0.5 和 1.0 的噪声攻击下的加密图像及其解密结果图.

图 10 表明, 当攻击噪声的密度增大时, 加密图像变化明显, 但对解密结果影响不大, 明文图像的全部信息能够被解密出来, 获得了高质量的解密结果图. 这说明本方法具有很高的抗噪性能,该加密系统能够抵御噪声的攻击.

将本方法与文献 [13, 16, 18] 进行了抗噪性能对比, 结果如表 2 所列. 从表 2 中可以看出, 本算法对噪声攻击具有较好的鲁棒性, 在噪声密度较小时与文献 [13,16,18] 相当; 当噪声度较大时, 本文方法具有明显优势. 因此, 该加密系统是安全可行的.

表 2 噪声攻击处理

Table 2. Treatment of noise attack.

噪声攻击		CC			
		本文方法	文献[13]方案	文献[16]方案	文献[18]方案
椒盐噪声	0.1	0.861	0.853	0.835	0.868
	0.3	0.823	0.700	0.687	0.719
	0.5	0.802	0.620	0.577	0.606
	1.0	0.712	0.284	0.314	0.211

5 结 论

利用 θ 调制的空间频谱复用和计算全息技术提出了一种新型的彩色图像光学加密方法. 加密过程中, 首先利用红、绿、蓝三色激光器和三色滤光片将彩色图像分为三个信道, 每个信道引入不同方向的透射式振幅型正弦光栅, 使得三基色分量在空间频谱面上分离; 然后对三基色分量进行叠加和相位截断非对称处理; 最后进行罗曼型计算全息编码, 从而将彩色图像加密成二元实值的灰度 CGH. 该 CGH 加密图完全隐藏了原始彩色图像的灰度和色彩信息, 在传输和存储过程中更具有一般性和迷惑性. 解密过程中, CGH 加密图和 CGH 密钥在 $4f$ 和菲涅耳衍射系统中完成, 计算机模拟结果

证明了该方法的有效性和安全性. 此外, 对该彩色图像加密方法的抗噪声攻击和抗剪切攻击性能进行了研究, 并与文献中的方法进行了对比, 发现该方法对噪声攻击和剪切攻击具有较好的鲁棒性; 而且当攻击噪声密度较大时, 本文方法的优势更为明显. 因此, 该方法具有高的安全性、抗剪切和抗噪能力, 这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] Borujeni S E 2013 *J. Telecommun. Syst.* **52** 525

[5] Shi Y S, Li T, Wang Y L, Gao Q K, Zhang S G, Li H F 2013 *Opt. Lett.* **38** 1425

[6] Yang N, Gao Q K, Shi Y S 2018 *Opt. Express* **26** 31995

[7] Su Y, Tang C, Li B, Chen X, Xu W, Cai Y 2017 *Appl. Opt.* **56** 498

[8] Liu Z, Dai J, Sun X, Liu S 2010 *Opt. Lasers Eng.* **48** 800

[9] Abuturab M R 2012 *Appl. Opt.* **51** 3006

[10] Sui L S, Xin M T, Tian A L, Jin H 2013 *Opt. Lasers Eng.* **51** 1297

[11] Xiao D, Xie Y J 2013 *Acta Phys. Sin.* **62** 240508 (in Chinese) [肖迪, 谢沂均 2013 物理学报 **62** 240508]

[12] Qin Y, Zheng C B 2012 *Acta Phot. Sin.* **41** 326 (in Chinese) [秦怡, 郑长波 2012 光子学报 **41** 326]

[13] Yuan Q P, Yang X P, Gao L J, Zhai H C 2009 *Optoelectron. Lett.* **5** 147

[14] Faraoun K M 2014 *Opt. Laser Technol.* **64** 145

[15] Liu Z, Guo C, Tan J, Liu W, Wu J, Wu Q, Pan L, Liu S 2015 *Opt. Lasers Eng.* **68** 87

[16] Gao L J, Yang X P, Li Z L, Wang X L, Zhai H C, Wang M W 2009 *Acta Phys. Sin.* **58** 1053 (in Chinese) [高丽娟, 杨晓苹, 李智磊, 王晓雷, 翟宏琛, 王明伟 2009 物理学报 **58** 1053]

[17] Yang X P, Gao L J, Wang X L, Zhai H C, Wang M W 2009 *Acta Phys. Sin.* **58** 1662 (in Chinese) [高丽娟, 杨晓苹, 李智磊, 王晓雷, 翟宏琛, 王明伟 2009 物理学报 **58** 1662]

[18] Zhou N R, Wang Y X, Gong L H, He H, Wu J H 2011 *Opt. Commun.* **284** 2789

[19] Wang X, Zhao D 2012 *Opt. Express* **20** 11994

[20] Ding X L, Yuan Q, Zhang L B 2014 *Laser Technol.* **38** 561 (in Chinese) [丁湘陵, 袁倩, 张乐冰 2014 激光技术 **38** 561]

[21] Xi S X, Wang X L, Song L P, Zhu Z Q, Yu N N, Wang H Y 2017 *Opt. Express* **25** 8212

Color image encryption method based on computer generated hologram and θ modulation*

Xi Si-Xing [1)] Yu Na-Na [1)] Wang Xiao-Lei [2)†] Zhu Qiao-Fen [1)] Dong Zhao [1)]
Wang Wei [1)] Liu Xiu-Hong [1)] Wang Hua-Ying [1)]

1) (*School of Science*, *Hebei University of Engineering*, *Handan* 056038, *China*)

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

(Received 25 December 2018; revised manuscript received 19 March 2019)

Abstract

In this paper, a new method of encrypting a color image based on θ modulation is proposed by using the tricolor principle and computer-generated hologram (CGH) technology. The encryption process includes the θ-modulated three primary color components and the coding of computer-generated hologram, which is implemented in a Fresnel diffraction and spatial filtering system. Firstly, the color image modulated by the first random phase key is divided into three encryption channels by red laser, green laser, blue laser, and tricolor filters. Each channel is introduced by a transmissive amplitude-type sinusoidal grating with different directions, which is used to separate the three primary color components in the spatial spectrum plane. Secondly, the modulation results of tricolor components are superimposed together to form a compound image, and the phase truncation of the superposition result is performed to achieve the asymmetric encryption. Finally, the amplitude of the compound image is modulated by the second random phase key and is encoded into a binary real-value gray-color CGH by Roman-type coding method. Therefore, the gray-color information of the original image is completely hidden in the encrypted CGH, which is more general and deceptive in the storage and transmission process. Decryption is an inverse process of the encryption. Firstly, the encrypted CGH is placed on the input plane of the spatial filtering and Fresnel diffraction system. Secondly, the demodulation of CGH phase key and the spatial filtering based on optical filter are performed. Finally, the color plaintext image is obtained by using the correct Fresnel diffraction. The simulation results show the validity and feasibility of the proposed method. In addition, the anti-noise attack and anti-shearing attack performance of this color image encryption method are investigated. Compared with results from the three presented methods reported in the literature, our investigated results demonstrate that this method has good robustness to noise attack and shearing attack, and has obvious advantages when the attack noise density is larger. Due to the characteristics of high security and anti-noise, we believe that this color image encryption method promises to have important applications in the information transmission and multi-user authentication.

Keywords: color image encryption, computer generated holography, θ modulation, asymmetric encryption

PACS: 05.45.Gg, 42.30.Va, 42.30.Wb **DOI:** 10.7498/aps.68.20182264

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61875093, 61465005) and the Natural Science Foundation of Hebei Province, China (Grant No. F2018402285).

† Corresponding author. E-mail: wangxiaolei@nankai.edu.cn