激光与光电子学进展 先进成像

基于光场调控和频移的多图像偏振加密方法

张迪[1]，于娜娜[1]，席思星[1*]，郎利影[2]，王晓雷[3]，张寰臻[1]

[1]河北工程大学数理科学与工程学院，河北 邯郸 056038；

[2]河北工业大学先进激光技术研究中心，天津 300401；

[3]南开大学现代光学研究所，天津 300350

摘要 提出一种基于全矢量光场调控和傅里叶变换频移的多图像非对称偏振光学加密新方法。首先，多幅待加密图像经过随机相位调制、傅里叶变换和频移相位调制后相干叠加构成一幅复振幅光学图像；然后将其干涉分解成两块纯相位掩模，并编码加载到基于4F系统的全矢量光场调控系统中；最后全光调控矢量光场经过偏振片后输出振幅型加密图像和密钥，它们被CCD接收，实现多幅图像的并行加密。解密时，在正确密钥条件下，根据调控光场的全矢量分布与加密图像的关系获取多幅解密图像。偏振片旋转的任意角度和干涉分解得到的纯相位图像作为密钥，极大地提高了光学图像加密系统的安全性。此外，多幅图像加密为单幅振幅型加密图像，便于保存和传输，加密系统的加密效率得到极大提高。仿真实验验证了所提多图像加密方案的有效性和可行性，实验结果表明所提方法具有很高的安全性、抗噪性、抗剪切能力和抗选择明文攻击性，具有一定的应用前景。

关键词 光学图像加密；光场调控；频移；干涉分解；多图像加密

中图分类号 O438 **文献标志码** A **DOI**：10.3788/LOP220659

Multipleimage Polarization Encryption Method Based on Light Field Regulation and Frequency Shifting

Zhang Di[1], Yu Nana[1], Xi Sixing[1*], Lang Liying[2], Wang Xiaolei[3], Zhang Huanzhen[1]

[1]*School of Mathematics and Physics Science and Engineering, Hebei University of Engineering, Handan* 056038, *Hebei, China*;

[2]*Advanced Laser Technology Research Center, Hebei University of Technology, Tianjin* 300401, *China*;

[3]*Institute of Modern Optics, Nankai University, Tianjin* 300350, *China*

Abstract This study proposes a new multi-image asymmetric polarization optical encryption method based on the full-vector light field control and Fourier transform frequency shifting. First, multiple images to be encrypted are coherently superimposed to form a complex amplitude optical image after the random phase modulation, Fourier transforms, and frequency shifting phase modulation. Next, the distribution of the image is the interference of two pure phase masks, and is encoded and loaded into the full-vector light field control system based on the 4F system. Finally, the all-optical control vector light field outputs amplitude type encrypted images and keys after passing through the polarizer, which are received by CCD to realize parallel encryption of multiple images. Multiple decrypted images can be obtained during decryption by solving the relationship between the control light field distribution (full vector distribution) and the encrypted image under the condition of the correct key. Any rotation angle of the polarizer and the phase only image obtained by interference decomposition are used as the key, which greatly improves the security of the optical image encryption system. The encryption of multiple images into a single amplitude-type encrypted image is convenient for storage and transmission, which improves encryption efficiency. A simulation study has verified the effectiveness and feasibility of the proposed multi-image encryption scheme, and the experimental results show that the proposed method has high security, noise resistance, shear resistance, and chosen-plaintext attack resistance, which has specific application prospects.

Key words optical image encryption; light field control; frequency shifting; interference decomposition; multiple image encryption

收稿日期：2022-01-28；**修回日期**：2022-02-06；**录用日期**：2022-03-03；**网络首发日期**：2022-03-13

基金项目：国家自然科学基金(11904073,61875093)、河北省自然科学基金(F2019402351)、河北省教育厅青年拔尖人才项目(BJ2020028)、河北省科技计划(20371802D)

通信作者：*xisixing@126.com

1 引 言

随着现代互联网科技的进步，信息交流变得尤为便捷，其中信息传输的安全性问题受到广泛的关注。光学信息处理因高处理速度和高并行性等特点而被广泛应用于图像加密领域。自双随机相位加密（DRPE）方法出现后[1]，一些衍生的加密方案也随之被提出，例如基于傅里叶变换[2]、菲涅耳衍射变换[3]、哈特莱变换[4]等的加密算法，但由于存在线性特征，系统的安全性降低。为了解决该问题，研究人员提出了非对称加密来增强系统的安全性[5-6]。例如2012年Rajput等[6]提出了一种基于分数傅里叶域中的干涉原理和相位截断方法的图像加密技术。但该方法仍会受到已知明文攻击和选择明文攻击[7-9]，目前光学图像加密技术的安全性能仍需提高。此外，科技的进步、信息传输速度的不断提高、大数据产业的崛起对加密系统的容量和传输效率提出了新的要求。因此，一些多图像光学加密和彩色图像光学加密的方法被不断提出，例如基于各种复用技术[10-16]的图像加密方法、基于全息技术[17-22]的图像加密系统、基于压缩感知[23-25]、混沌系统[26-28]和光学变换[29-33]等的图像光学加密方法，还有基于鬼成像[34]、单像素成像[35]、混合图像元素与排列[36]、像素交换运算结合向量分解[37]、图像重组结合比特置乱[38]的图像加密方式。随着这些光学加密方法的不断提出，图像加密的效率和安全性得到不断提高，但仍然存在一些未解决的问题。例如，加密结果的振幅和相位必须同时保存，这不利于存储和传输；一些方法需要复杂且耗时的迭代计算；难以同时加密不同数量、类型和尺寸的多个图像。此外，光场的偏振态可以作为图像加密系统设计中的一个重要参量，具有很高的灵活性，可以大大增加密钥空间和抵抗暴力攻击的鲁棒性。2019年绪其军等[39]利用Q-plate和像素化的偏振片实现了对两幅图像的加密，验证了多图像偏振加密的可行性。

基于以上分析，本文提出一种基于全矢量光场调控和傅里叶变换频移的多图像非对称光学加密新方法。利用傅里叶频谱的频移特性，对多幅不同尺寸和类型的图像在基于4F系统的全光调控光学系统中实现并行加密，利用全光调控矢量光场经过任意旋转角度的偏振片后被CCD记录的对应强度场分布作为加密图像，将干涉分解得到的纯相位图像作为解密密钥，便于存储和传输，提高了多图像加密系统的安全性。通过理论分析和仿真实验对该多图像光学加密方法的可行性和有效性进行了分析。

2 加密过程

2.1 加密原理

所提加密方案对多个不同尺寸和类型的图像可实现并行加密，为了验证该方法的多图像加密性能，选取4幅待加密图像，如图1所示。其中图1(a)为灰度图像“小鸟”，尺寸为512×256像素，图1(b)为灰度图像“木屋”，尺寸为256×512像素，图1(c)为二值图像“光”，尺寸为256×256像素，图1(d)为灰度图像“森林”，尺寸为512×512像素。

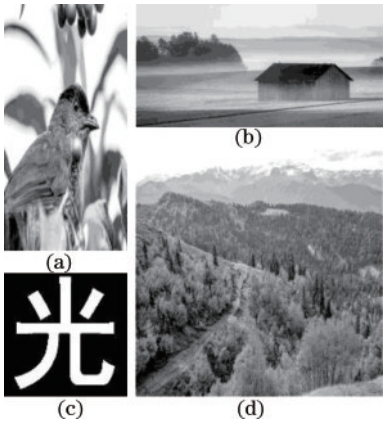

图1 待加密图像。(a)原始图像1；(b)原始图像2；(c)原始图像3；(d)原始图像4

Fig. 1 Images to be encrypted. (a) Original image 1; (b) original image 2; (c) original image 3; (d) original image 4

首先，利用傅里叶变换的频移特性将4幅待加密图像合成为1幅复振幅图像，实施过程如图2所示。待加密图像分别经过随机相位调制、傅里叶变换和频移相位调制后相干叠加构成一幅复振幅光学图像$F(u,v)$：

$$g_i(x,y)=f_i(x,y)\exp\left[\mathrm{i}2\pi\times\mathrm{rand}(m_i,n_i)\right],\quad(1)$$

$$G_i(u,v)=\mathrm{FT}\left[g_i(x,y)\right],\quad(2)$$

$$F(u,v)=\sum_{i=1}^{4}G_i(u,v)\exp\left[\mathrm{i}2\pi(a_iu+b_iv)\right],\quad(3)$$

式中：FT[·]表示傅里叶变换；$f_i(x,y)$表示待加密图像；$\exp\left[\mathrm{i}2\pi\times\mathrm{rand}(m_i,n_i)\right]$为随机相位因子；$\exp\left[\mathrm{i}2\pi(a_iu+b_iv)\right]$是频移相位因子；$(a_i,b_i)$表征各个图像的位置，本文中，$(a_1,b_1)=(0.167,0.333)$，$(a_2,b_2)=(-0.167,0.333)$，$(a_3,b_3)=(0.333,-0.333)$，$(a_4,b_4)=(-0.167,-0.167)$。

然后利用干涉分解原理将合成图像$F(u,v)$分解为两个纯相位掩模φ_1和φ_2，用两个纯相位掩模φ_1和φ_2的干涉来表示复振幅光场$F(u,v)$的分布[40]：

$$F(u,v)=\exp(\mathrm{i}\varphi_1)+\exp(\mathrm{i}\varphi_2)。\quad(4)$$

由于φ_1和φ_2都是纯相位函数，因此有

$$\left|\exp(\mathrm{i}\varphi_1)\right|^2=\left|F(u,v)-\exp(\mathrm{i}\varphi_2)\right|^2=$$

$$\left|F(u,v)-\exp(\mathrm{i}\varphi_2)\right|\left|F(u,v)-\exp(\mathrm{i}\varphi_2)\right|^*=1,\quad(5)$$

化简整理，得

$$\varphi_2=\mathrm{angle}\left[F(u,v)\right]-\arccos\left\{\mathrm{abs}\left[F(u,v)\right]/2\right\}+K_1\cdot2\pi,\quad(6)$$

$$\varphi_1=\mathrm{angle}\left[F(u,v)-\exp(\mathrm{i}\varphi_2)\right]+K_2\cdot2\pi,\quad(7)$$

式中：angle[·]表示提取相位；abs[·]表示提取振幅。

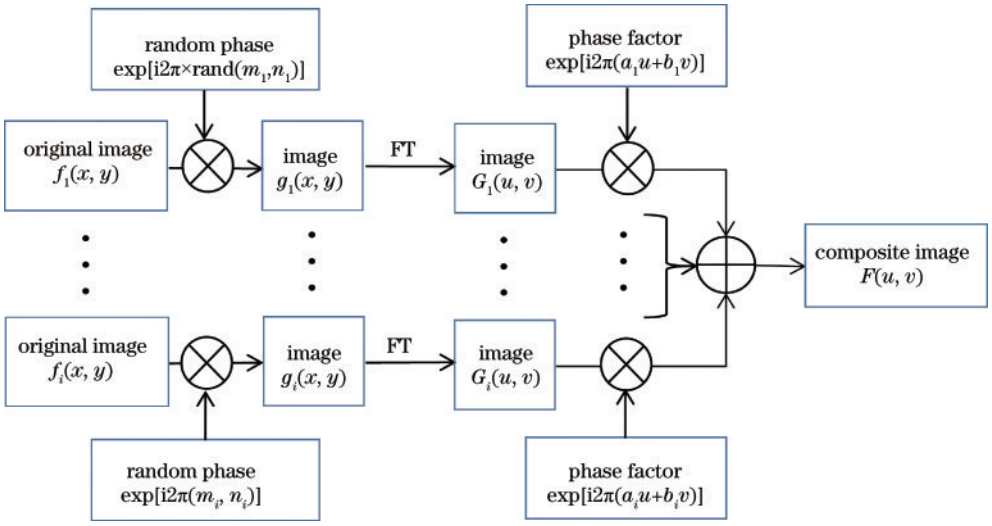

图 2　多图像傅里叶变换频移合成示意图

Fig. 2　Schematic of multi-image Fourier transform frequency shifting synthesis

这里选取 $K_1=K_2=1$，就可以获取到纯相位掩模 φ_1 和 φ_2 的场分布。

最后将两个纯相位掩模编码加载到基于 4F 系统的全矢量光场调控系统中实现加密。基于全矢量光场调控的多图像加密光路如图 3 所示。首先，氦氖激光器发射的波长为 $\lambda=633$ nm 的激光经过准直扩束和偏振调控后照射振幅型空间光调制器（SLM_1），振幅调制后的光束经一个透镜成像系统（成像系统物像距与两个 SLM 的像素尺寸成正比）到达相位型空间光调制器（SLM_2）；然后，在 4F 系统中，经过 SLM_2 加载的全息光栅被调制，分别使 x 和 y 方向的 +1 级衍射光通过 $\lambda/4$ 波片后转换成正交的左、右旋圆偏振光；最后，在 Ronchi 光栅处完成合束，输出全光调控矢量光场，经过偏振片后的光场被 CCD 接收，通过旋转偏振片 CCD 可获得振幅型加密结果，完成多幅图像的并行加密。

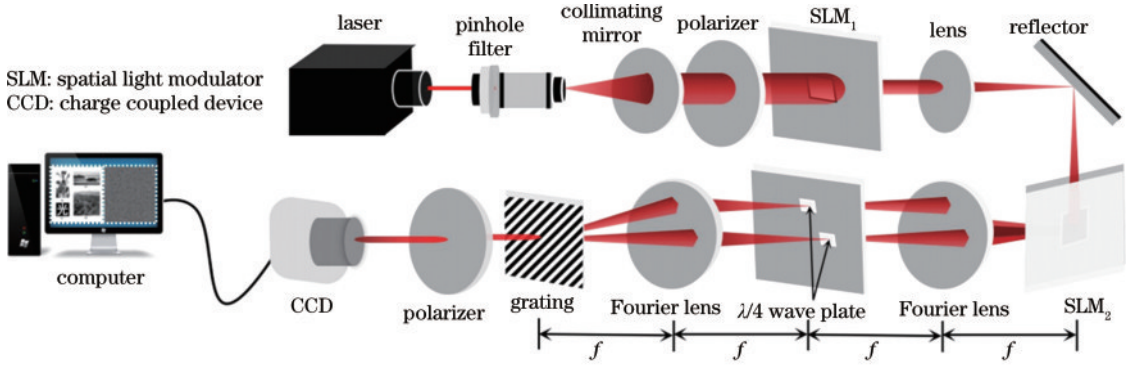

图 3　基于 4F 系统全矢量光场调控的多图像非对称加密系统

Fig. 3　Multi-image asymmetric encryption system based on full vector light field regulation of 4F system

相位型 SLM_2 上加载全息光栅透过率函数为

$$t(x,y)=\frac{1}{2}+\frac{1}{4}\times\cos\left[2\pi f_0 x+\delta_1(x,y)\right]+\frac{1}{4}\times\cos\left[2\pi f_0 y+\delta_2(x,y)\right],\tag{8}$$

式中：$\delta_1(x,y)$ 和 $\delta_2(x,y)$ 分别是全息光栅沿 x 方向和 y 方向的附加相位；f_0 是空间载频。调制后的正交圆偏振光场分布用琼斯矢量可表示为

$$\boldsymbol{E}(x,y)=\frac{A_0(x,y)}{2}\exp(\mathrm{i}\delta_1)\begin{pmatrix}1\\-\mathrm{i}\end{pmatrix}+\frac{A_0(x,y)}{2}\exp(\mathrm{i}\delta_2)\begin{pmatrix}1\\\mathrm{i}\end{pmatrix}=A_0(x,y)\exp(\mathrm{i}\beta)\begin{pmatrix}\cos\alpha\\\sin\alpha\end{pmatrix},\tag{9}$$

式中：$\alpha=(\delta_1-\delta_2)/2$，$\beta=(\delta_1+\delta_2)/2$。在加密过程中 $\delta_1=(\varphi_1+\varphi_2)/2$，$\delta_2=-(\varphi_1+\varphi_2)/2$。通过编码振幅型 SLM_1 对振幅进行调制，得

$$A_0(x,y)=\xi\varphi_1(x,y),\tag{10}$$

式中：振幅调制系数 $\xi=10^{-1}$。故经过偏振片后的光场分布为

$$\boldsymbol{E}_{\mathrm{out}}=A_0\begin{pmatrix}\cos(\varphi_1+\varphi_2)\cos\theta\\\sin(\varphi_1+\varphi_2)\sin\theta\end{pmatrix},\tag{11}$$

式中：θ 是偏振片的透射轴与水平方向的夹角。CCD 接收到的光强分布为

$$I=A_0^2\cos^2(\varphi_1+\varphi_2)\cos^2\theta+A_0^2\sin^2(\varphi_1+\varphi_2)\sin^2\theta, \tag{12}$$

式中：I为最终加密图像；θ和φ_1可作为密钥。最终CCD接收到的加密图像I如图4所示。

图4　多图像加密结果

Fig. 4　Multi-image encryption result

对比图4和图1可见，所提方案可以将4幅尺寸、形状和类型不同的待加密图像加密为单幅振幅型图像，并且密文图像中未显示任何原始图像信息。解密密钥φ_1为干涉分解得到的纯相位图像，随待加密图像的像素值、尺寸、类型、数量以及随机相位和相位因子的变化而变化，极大地提高了加密系统的安全性。

2.2　密文相关性分析

为了验证加密结果的有效性和鲁棒性，对加密结果的相关性进行分析。

图像的相关性可以表征图像相邻位置像素值的相关程度，加密图像相关性越低，加密算法的安全性越高。分别对原始图像和密文图像在水平、垂直和对角三个方向上的相关性系数进行计算，计算公式为

$$\mathrm{cov}(x,y)=\frac{1}{N}\times\sum_{i=1}^{N}\left\{\left[x_i-E(x)\right]\left[y_i-E(y)\right]\right\}, \tag{13}$$

$$C_C=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}。 \tag{14}$$

通过表1的计算结果可见，加密图像在各个方向上的相关性极低，所提加密方法有效地降低了高度相关的原始图像的统计特性，能够有效抵抗基于像素相关性的统计攻击，具有较高的安全性。

表1　原始图像和密文图像的相关性系数

Table 1　Correlation coefficient of original image and ciphertext image

Correlation	Fig. 1(a)	Fig. 1(b)	Fig. 1(c)	Fig. 1(d)	Encrypted image
Horizontal correlation	0.9735	0.9929	0.9595	0.9488	0.0013
Vertical correlation	0.9902	0.9806	0.9642	0.9652	0.0010
Diagonal correlation	0.9679	0.9771	0.9341	0.9365	−0.0003

2.3　明文敏感性分析

明文敏感性用来描述当明文图像发生微小变化时，密文改变的程度。其中常用的两个指标是像素值改变率(NPCR)和归一化平均变化强度(UACI)。当明文中任意一像素值增大0.1和某两个像素值交换时的密文相较于未改变时的密文改变的程度结果如表2所示。

$$N_{\mathrm{PCR}}=\frac{\sum_i\sum_j z(i,j)}{M\times N}, \tag{15}$$

$$U_{\mathrm{ACI}}=\frac{1}{M\times N}\left[\sum_i\sum_j\left|I(i,j)-I'(i,j)\right|\right], \tag{16}$$

式中：当$I(i,j)=I'(i,j)$时，$z(i,j)=0$；当$I(i,j)\neq I'(i,j)$时，$z(i,j)=1$。

由表2可以看出，当明文产生任意一像素值增大0.1和某两个像素值交换出现微小变化时密文几乎全部改变，而且改变强度均在17%以上，这说明所提系统具有较好的明文敏感性。

表2　明文敏感性分析

Table 2　Plaintext sensitivity analysis

Any position pixel plus 0.1		Swap positions of two pixel values	
NPCR	UACI	NPCR	UACI
0.9946	0.1733	0.9945	0.1709

3　解密过程

多图像的解密可通过求解加密图像与全光调控矢量光场分布的关系实现。首先将密文I和偏振片的角度θ代入式(12)，求解得到全矢量光场的偏振分布。

$$\varphi_1+\varphi_2=\arccos\sqrt{\frac{\dfrac{I}{A_0^2}-\sin\theta}{\cos(2\theta)}}。 \tag{17}$$

将式(10)和式(17)联立，可得

$$\varphi_2=\arccos\left(\sqrt{\frac{\dfrac{I}{\xi^2\varphi_1^2}-\sin\theta}{\cos(2\theta)}}-\varphi_1\right)。 \tag{18}$$

然后利用式(4)将两个相位掩模φ_1和φ_2合成，得到$F(u,v)$的复振幅分布。最后对复振幅图像$F(u,v)$进行一次傅里叶逆变换，利用傅里叶变换的频移性质，可在傅里叶变换平面上获得解密图像f_1～f_i。

$$\mathrm{FT}^{-1}[F(u,v)]=\mathrm{FT}^{-1}\left\{\sum_{i=1}^{4}G(u,v)\exp\left[\mathrm{i}2\pi(a_iu+b_iv)\right]\right\}=\sum_{i=1}^{4}g_i(x+Ma_i,y+Nb_i),\tag{19}$$

$$g_i(x+Ma_i,y+Nb_i)=f_i(x+Ma_i,y+Nb_i)\exp\left[\mathrm{i}2\pi\times\mathrm{rand}(m_i,n_i)\right],\tag{20}$$

$$\mathrm{abs}\left[g_i(x+Ma_i,y+Nb_i)\right]=f_i(x+Ma_i,y+Nb_i),\tag{21}$$

式中：FT^{-1}表示傅里叶逆变换；M和N为图像大小。解密结果如图5所示。

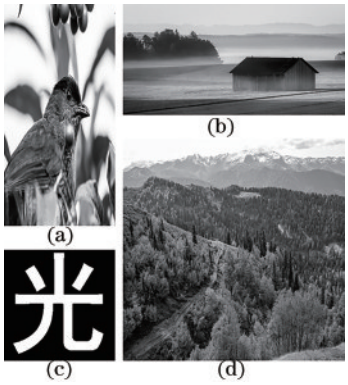

图5　解密结果。(a)解密图像1；(b)解密图像2；(c)解密图像3；(d)解密图像4

Fig. 5　Decryption result. (a) Decryption image 1; (b) decryption image 2; (c) decryption image 3; (d) decryption image 4

在仿真实验中，当解密密钥正确时，可以获得不同类型、尺寸且图像质量无损的解密结果，说明了该多图像加密方法的可行性。

4　加密系统实验及分析

4.1　密钥有效性分析

实验中密钥参数设定为$\theta=0.1\pi$，选用4张尺寸、形状和类型不同的图像进行加密解密实验。

为了研究密钥的有效性，解密密钥的微扰被引入，受干扰后的解密密钥φ_1可以表示为

$$\varphi_1'=\varphi_1+r\cdot2\pi,\tag{22}$$

式中：φ_1'是受到干扰后的解密密钥；r是微扰系数。微扰系数为$r=1.75\times10^{-7}$和$r=-4.0\times10^{-6}$时的解密结果如图6所示。另外当解密密钥φ_1受到高斯噪声(均值为0，方差为0.0001)、椒盐噪声(密度为0.001)、剪切(剪切面积为0.1%)、旋转(1°)、运动模糊(水平10个像素)和高斯低通滤波(阈值为80)等不同类型微小干扰时，解密图和原图的图像质量对比(以相关系数描述)如表3所示。

由图6可知，当解密密钥φ_1受到微扰系数r为$1.75\times10^{-7}+k<r<1+k$或$-1+k<r<-4.0\times10^{-6}+k$，$k\in\mathbf{Z}$的微扰时，均不能从灰度图像和二值图像中解密出原始图像信息。由表3可知，当解密密钥φ_1受到不同类型的微小干扰时，都无法从解密图像中获取原始图像的有效信息，说明该加密方法对解密密钥φ_1具有很高的敏感性，从而验证该加密系统具有很高的安全性。

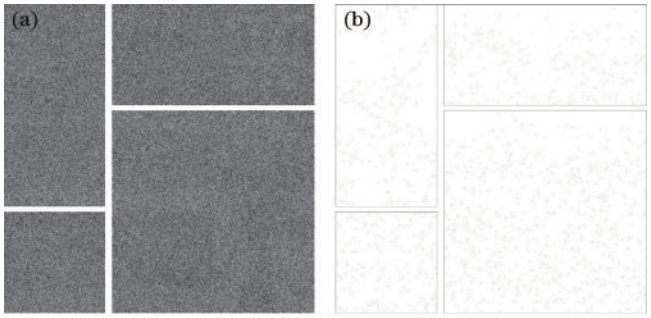

图6　解密密钥φ_1受到微扰时的解密结果。(a)$r=1.75\times10^{-7}$时的解密结果；(b)$r=-4.0\times10^{-6}$时的解密结果

Fig. 6　Decryption result when the decryption key φ_1 is perturbed. (a) Decryption result when $r=1.75\times10^{-7}$; (b) decryption result when $r=-4.0\times10^{-6}$

同理，被干扰后的密钥θ可表示为

$$\theta'=\theta+p\pi,\tag{23}$$

式中：p是微扰系数。图7分别给出了微扰系数为$p=2.0\times10^{-5}$和$p=-2.0\times10^{-5}$时的解密结果。4幅原始图像与解密图像的结构相似性系数的平均值(SSIM)被用来评判微扰系数r和p变化时对解密结果产生的影响。平均相似度随微扰系数变化的关系曲线如图8所示。

表3　当解密密钥φ_1受到微小干扰时原始图像和解密图像的相关性系数

Table 3　Correlation coefficient between the original image and the decrypted image when the decryption key φ_1 is slightly disturbed

Attack type	Fig. 1(a)	Fig. 1(b)	Fig. 1(c)	Fig. 1(d)
Gaussian noise	0.0033	0.0015	0.0008	−0.0008
Salt and pepper noise	0.0033	0.0042	−0.0021	−0.0054
Shear	0.0670	0.0892	−0.0049	−0.0566
Rotation	0.0077	0.0097	0.0079	0.0165
Motion blur	0.0308	0.0271	0.0077	−0.0207
Gaussian low pass filtering	0.0298	0.0905	−0.0035	0.0226

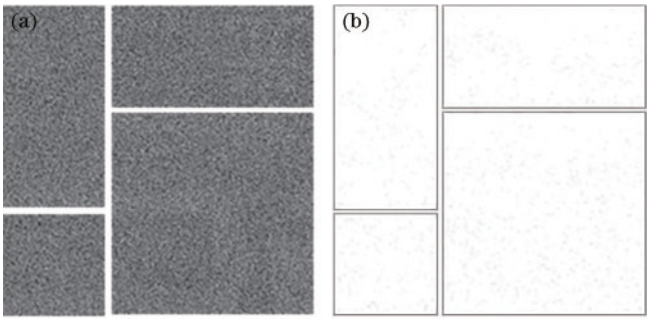

图 7　密钥 θ 受到微扰时的解密结果。(a)$p=2.0\times10^{-5}$ 时解密结果;(b)$p=-2.0\times10^{-5}$ 时解密结果

Fig. 7　Decryption result when the decryption key θ is perturbed. (a) Decryption result when $p=2.0\times10^{-5}$; (b) decryption result when $p=-2.0\times10^{-5}$

由图 7 和图 8 可见,多图像加密系统对解密密钥 θ 也具有很好的敏感性,当解密密钥 θ 受到的微扰系数 p 为 $2.0\times10^{-5}+k<p<1+k$ 或 $-1+k<p<-2.0\times10^{-5}+k$,$k\in\mathbf{Z}$ 的微扰时,均不能从灰度图像和二值图像中解密出原始图像信息。

综上所述,解密密钥 φ_1 和 θ 都具有很好的敏感性,微小扰动都会导致解密失败,使得加密系统拥有较高的安全性。

4.2　抗剪切性与抗噪性能分析

对所提多图像加密方法的抗剪切能力与抗噪性能力进行分析,以 4 幅原始图像与解密图像相关性系数的平均值(CC)来评判密文图像像素丢失时和受到噪声污染时对解密结果产生的影响。图 9(a)为平均相关性系数 CC 随密文图像丢失像素面积比(S)变化而变化的关系曲线,并分别给出了密文丢失像素面积比为 20%、50% 和 80% 时的解密结果。图 9(b)为解密图像与原始图像的平均相关性系数 CC 随密文图像中椒盐噪声密度(d)变化而变化的关系曲线,并分别给出了椒盐噪声密度为 0.2、0.5 和 0.8 时的解密结果。

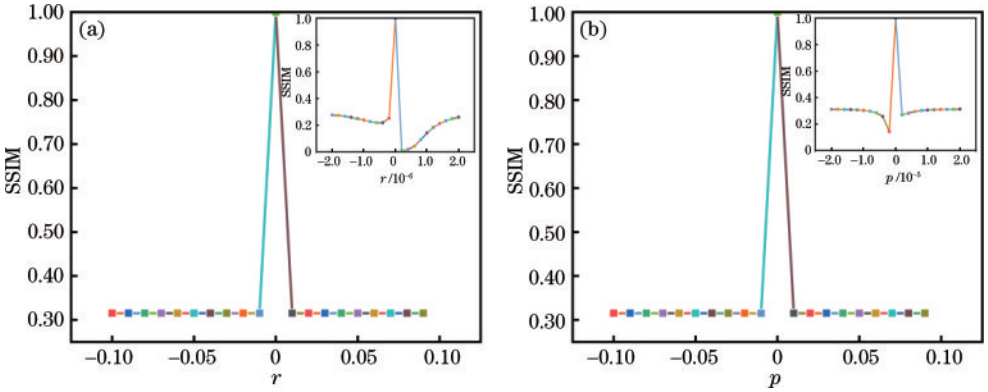

图 8　平均相似度随微扰系数变化的关系曲线。(a)微扰系数 r;(b)微扰系数 p

Fig. 8　Relationship between the average similarity and the change of the perturbation coefficient. (a) Perturbation coefficient r; (b) perturbation coefficient p

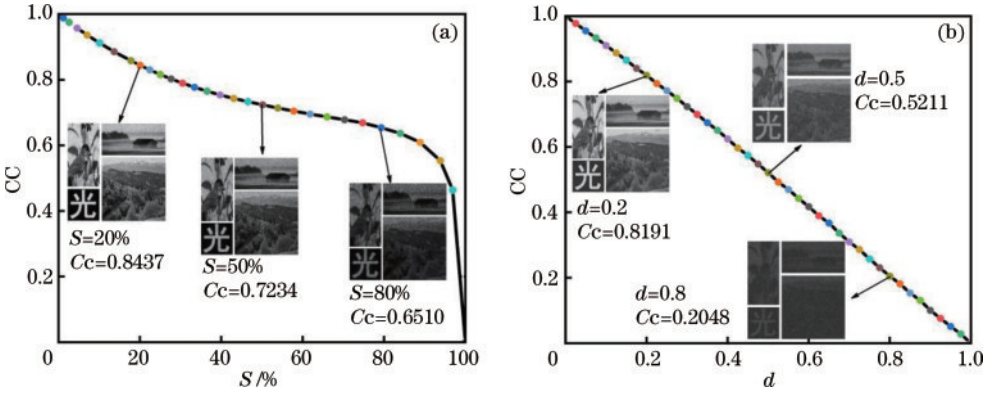

图 9　抗剪切性与抗噪性能模拟结果。(a)抗剪切性;(b)抗噪性

Fig. 9　Simulation result of shear resistance and noise immunity. (a) Shear resistance; (b) noise immunity

由图 9(a)可见,当密文丢失面积小于 50% 时,原始图像的信息仍可以被正确密钥较好解密,说明该加密系统有较好的抗剪切攻击能力,其中由于二值图的像素值较为简单,其抗剪切能力较灰度图像更强。从图 9(b)可以看出,随着密文图像中加入更大密度的噪声,被正确密钥解密出的原始图像信息随之减少,当椒盐噪声密度小于 0.5 时,就可以获取较好的解密图像,因此该加密系统有一定的抗噪性能。

4.3　抗选择明文攻击性分析

为了验证所提系统的抗选择明文攻击性，选择其他4幅图片作为伪明文图像，如图10(a)所示，假如攻击者利用该伪明文图像得到解密密钥，利用密钥对图4密文进行解密，得到的解密图如图10(b)所示。其中解密图与原图的相关系数分别为0.0127、0.0066、0.0158和0.0018，由解密结果可知，无法获取原始图像信息。这是由于所提算法的解密密钥φ_1随明文图像的像素值、尺寸、类型和数量以及随机相位和相位因子的变化而不同，由此证明该系统拥有很好的抗选择明文攻击性能。

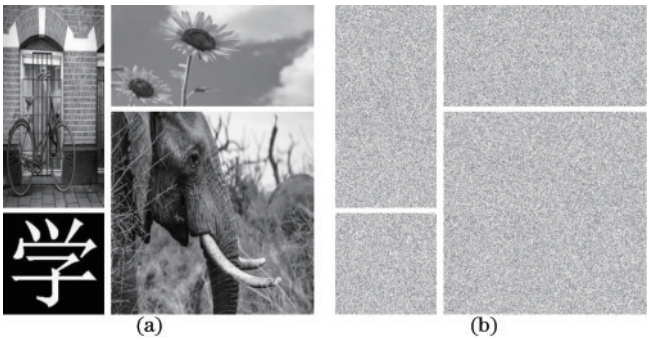

图10　抗选择明文攻击性模拟结果。(a)伪明文；(b)图4的解密结果

Fig. 10　Anti-chosen-plaintext attack simulation result. (a) Fake plaintext; (b) decrypted result of Fig. 4

4.4　算法对比分析

利用所提算法和其他的多图像加密算法对4幅256×256图像进行加密，通过对密文随机性、明文敏感性和加密所需时间进行对比来说明所提算法的先进性，结果如表4所示。

由表4可知，本文密文的相关系数最低，故所提算法的密文随机性优于文献[36]和文献[37]中的多图像加密算法，说明所提算法具有较好的抗差分能力和抗攻击能力。文献[36]中的加密算法的扩散效果较弱且明文与密钥无关，导致NPCR和UACI均为0。文献[37]和本文中明文和密钥关联性较好，明文微小的改变就可使得密钥产生较大的改变，以致密文也产生较大变动，但所提算法的UACI弱于文献[37]。此外，文献[36]中的算法一次仅能加密4幅同等尺寸的灰度图像，文献[37]中的算法只能加密任意数量同等尺寸的灰度图像，而所提算法可以同时加密任意数量、任意尺寸和任意类型的图像，实用性更高。且相较文献[36]和文献[37]中算法的加密时间，所提算法的加密时间最短，加密效率更高。

表4　算法对比分析

Table 4　Algorithm comparative analysis

Method	Correlation coefficient			NPCR	UACI	Time /s
	Horizontal	Vertical	Diagonal			
Method in Ref. [36]	−0.0781	0.0665	0.0607	0.0000	0.0000	9.656
Method in Ref. [37]	−0.0022	−0.0031	0.0016	0.9962	0.3343	0.7103
Proposed method	0.0013	0.0010	−0.0003	0.9946	0.1733	0.3417

5　结　　论

提出一种基于全光调控系统和傅里叶变换频移特性的多图像光学加密方法，实现了对多幅不同尺寸和类型的图像的并行加密和解密。多幅图像加密为单幅振幅型图像后便于保存和传输，加密系统的加密效率得到极大提高。设计了随待加密图像的像素值、尺寸、类型和数量以及随机相位和相位因子变化而变化的纯相位图像φ_1为解密密钥，极大地提高了加密系统的安全性。数值模拟实验验证了该多图像加密方案的有效性和可行性。实验结果表明所提方法具有很高的安全性，能够有效地抵抗基于像素统计的攻击手段，并且具有较好的抗噪性能、抗剪切性能、抗选择明文攻击性。

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] Deng X P, Zhao D M. Single-channel color image encryption based on asymmetric cryptosystem[J]. Optics & Laser Technology, 2012, 44(1): 136-140.

[3] Liu Z J, Guo C, Tan J B, et al. Securing color image by using phase-only encoding in Fresnel domains[J]. Optics and Lasers in Engineering, 2015, 68: 87-92.

[4] Abuturab M R. An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform[J]. Optics and Lasers in Engineering, 2015, 69: 49-57.

[5] Qin W, Peng X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Letters, 2010, 35(2): 118-120.

[6] Rajput S K, Nishchal N K. Image encryption based on interference that uses fractional Fourier domain asymmetric keys[J]. Applied Optics, 2012, 51(10): 1446-1452.

[7] Wang X G, Zhao D M. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Communications, 2012, 285(6): 1078-1081.

[8] Rajput S K, Nishchal N K. Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform [J]. Applied Optics, 2013, 52(4): 871-878.

[9] Wang X G, Chen Y X, Dai C Q, et al. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform[J]. Applied Optics, 2014, 53(2): 208-213.

[10] He M Z, Cai L Z, Liu Q, et al. Multiple image encryption and watermarking by random phase matching [J]. Optics Communications, 2005, 247(1/2/3): 29-37.

[11] Situ G H, Zhang J J. Position multiplexing for multiple-image encryption[J]. Journal of Optics A Pure and Applied Optics, 2006, 8(5): 391-397.

[12] 史祎诗, 张静娟. 相位恢复算法用于分区复用多图像加密的研究[J]. 光学学报, 2009, 29(10): 2705-2708.
Shi Y S, Zhang J J. Research on the phase retrieval algorithm used for multiple-image encryption with region multiplexing[J]. Acta Optica Sinica, 2009, 29(10): 2705-2708.

[13] Hwang H E, Chang H T, Lie W N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain[J]. Optics Letters, 2009, 34(24): 3917-3919.

[14] 秦怡, 李婧, 马毛粉, 等. 一种基于随机相位板复用的光学多二值图像加密系统[J]. 光学学报, 2014, 34(3): 0307001.
Qin Y, Li J, Ma M F, et al. System for optical multiple binary image encryption by random phase mask multiplexing[J]. Acta Optica Sinica, 2014, 34(3): 0307001.

[15] 郭飞鹏, 李婧, 巩琼, 等. 基于附加密钥复用的彩色图像加密技术[J]. 应用光学, 2014, 35(4): 626-631.
Guo F P, Li J, Gong Q, et al. Color image encryption by additional key multiplexing[J]. Journal of Applied Optics, 2014, 35(4): 626-631.

[16] Wang H J, Qin Y, Huang Y D, et al. Multiple-image encryption and authentication in interference-based scheme by aid of space multiplexing[J]. Optics & Laser Technology, 2017, 95: 63-71.

[17] Goodman J W, Lawrence R W. Digital image formation from electronically detected holograms[J]. Applied Physics Letters, 1967, 11(3): 77-79.

[18] Shen X J, Lin C, Kong D Z. Fresnel-transform holographic encryption based on angular multiplexing and random-amplitude mask[J]. Optical Engineering, 2012, 51(6): 068201.

[19] Xu D S, Lu M, Jia C Z, et al. Angular-multiplexing optical multiple-image encryption based on digital holography and random amplitude mask[J]. Journal of Russian Laser Research, 2017, 38(3): 285-293.

[20] Di H, Zheng K F, Zhang X, et al. Multiple-image encryption by compressive holography[J]. Applied Optics, 2012, 51(7): 1000-1009.

[21] Wan Y H, Wu F, Yang J H, et al. Multiple-image encryption based on compressive holography using a multiple-beam interferometer[J]. Optics Communications, 2015, 342: 95-101.

[22] 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.

[23] Liu X Y, Cao Y P, Lu P, et al. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. Optik, 2013, 124(24): 6590-6593.

[24] Deepan B, Quan C, Wang Y, et al. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique [J]. Applied Optics, 2014, 53(20): 4539-4547.

[25] 王梦婷, 周昕, 呼有军, 等. 基于压缩感知的多图像加密新方法[J]. 激光杂志, 2016, 37(3): 38-41.
Wang M T, Zhou X, Hu Y J, et al. A new multiple-image encryption method based on compressive sensing [J]. Laser Journal, 2016, 37(3): 38-41.

[26] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8(6): 1259-1284.

[27] Tang Z J, Song J, Zhang X Q, et al. Multiple-image encryption with bit-plane decomposition and chaotic maps [J]. Optics and Lasers in Engineering, 2016, 80: 1-11.

[28] 周玉鑫, 毕美华, 滕旭阳, 等. 基于混沌映射的OFDM-PON物理层加密及系统性能增强算法[J]. 光学学报, 2021, 41(16): 1606002.
Zhou Y X, Bi M H, Teng X Y, et al. Physical layer encryption and system performance enhancement algorithm based on chaos mapping in OFDM-PON[J]. Acta Optica Sinica, 2021, 41(16): 1606002.

[29] Wang X G, Zhao D M. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain[J]. Optics Communications, 2011, 284 (1): 148-152.

[30] 张文全, 周南润. 基于非对称密码系统的多图像加密算法[J]. 光电子·激光, 2012, 23(7): 1382-1388.
Zhang W Q, Zhou N R. Multiple-image encryption algorithm based on asymmetric cryptosystem[J]. Journal of Optoelectronics·Laser, 2012, 23(7): 1382-1388.

[31] Deng X P, Wen W. Optical multiple-image encryption based on fully phase encoding and interference[J]. Optik, 2015, 126(21): 3210-3214.

[32] Li X Y, Meng X F, Yang X L, et al. Multiple-image encryption based on compressive ghost imaging and coordinate sampling[J]. IEEE Photonics Journal, 2016, 8 (4): 3900511.

[33] Sui L S, Zhou B, Ning X J, et al. Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain[J]. Optics Express, 2016, 24(1): 499-515.

[34] Yuan X, Zhang L H, Chen J, et al. Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing[J]. Applied Physics B, 2019, 125(9): 174.

[35] Jiao S M, Feng J, Gao Y, et al. Visual cryptography in single-pixel imaging[J]. Optics Express, 2020, 28(5): 7301-7313.

[36] Tang Z J, Song J, Zhang X Q, et al. Multiple-image encryption with bit-plane decomposition and chaotic maps [J]. Optics and Lasers in Engineering, 2016, 80: 1-11.

[37] Zhang X Q, Wang X S. Multiple-image encryption algorithm based on mixed image element and permutation [J]. Optics and Lasers in Engineering, 2017, 92: 6-16.

[38] 郭媛, 周艳艳, 敬世伟. 基于图像重组和比特置乱的多图像加密[J]. 光子学报, 2020, 49(4): 0410002.
Guo Y, Zhou Y Y, Jing S W. Multiple-image encryption based on image recombination and bit scrambling[J]. Acta Photonica Sinica, 2020, 49(4): 0410002.

[39] 绪其军, 李德林, 常琛亮, 等. 基于Q-plate的双图像非对称偏振加密[J]. 物理学报, 2019, 68(8): 084202.
Xu Q J, Li D L, Chang C L, et al. Q-plate based dual image asymmetric polarization encryption[J]. Acta Physica Sinica, 2019, 68(8): 084202.

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