文章编号：2095-4980(2022)05-0470-09

基于回转器变换与非等模分解的光学加密算法

李　培[1]，朱春华[2]

(1.郑州旅游职业学院 文化艺术学院，河南 郑州 450009；2.河南工业大学 信息科学与工程学院，河南 郑州 450001)

摘　要：为解决当前基于干涉的多图像密码系统中易出现轮廓和串扰噪声问题，设计了基于回转器(Gyrator)变换与非等模矢量分解的多彩色图像非对称光学加密算法。将所有彩色图像分解成红、绿、蓝三基色分量，再对每种颜色分类叠加，融合成三通道形式；利用Logistic映射生成随机相位掩码，对叠加后的颜色分量进行调制处理。将调制后的图像分量分别在Gyrator变换域下进行旋转变换，形成3个复杂分布函数。利用非等模矢量分解方法，将其分解成振幅和相位均不相同的2个矢量，并将其中一个视为固定的共享矢量，另一个作为解密矢量。对共享矢量实施Gyrator逆变换，输出最终的密码图像。实验数据显示，较已有的多目标加密技术而言，该算法具备更强的抗破译能力，可以更好地解决串扰噪声问题。

关键词：光学图像加密；Logistic映射；Gyrator变换；非等模分解；串扰噪声；共享矢量

中图分类号：TP391　　**文献标志码：**A　　**doi：**10.11805/TKYDA2020302

Multiple color image optical encryption based on Gyrator transform and unequal modulus decomposition

LI Pei[1]，ZHU Chunhua[2]

(1.School of Culture and Arts，Zhengzhou Tourism Vocational College，Zhengzhou Henan 450009，China；
2.School of Information Science and Engineering，Henan University of Technology，Zhengzhou Henan 450001，China)

Abstract：In order to eliminate the problems of the silhouette and crosstalk noise in the interference-based and multiple image cryptosystems，an asymmetric optical cryptography mechanism for multiple color images based on Gyrator transform and unequal modulus vector decomposition is designed. Firstly，all color images are decomposed into three primary color components of red，green and blue. Then，each color is classified and superimposed，and fused into a three-channel form. The random phase mask is generated by Logistic mapping to modulate the superimposed color components. Secondly，the modulated image components are rotated under the Gyrator transform domain to form three complex distribution functions. Thirdly，it is decomposed into two vectors with different amplitudes and phases，the first vector is a fixed shared，and the second vector is a different decrypted. Finally，the shared vector is further applied with inverse Gyrator transform to produce the final password image. The encryption process is characterized by no contour，no crossover and high sensitivity. Experimental data show that the proposed algorithm has stronger anti-cracking ability than the existing multi-target encryption technology，which can better solve the problem of crosstalk noise.

Keywords：optical image encryption；Logistic mapping；Gyrator transform；unequal modulus decomposition；crosstalk noise；shared vector

光学信息处理是利用光学的方法将需要处理的数据信息进行相关的变换，已经在很多领域被广泛采纳和应用，主要包括全息领域、信息安全领域、数据存储及计算领域等[1-2]。光学信息处理相比于其他技术，其具有很高的实现效率和并行能力等特点，已成为信息科学的重要研究内容[3-4]。

收稿日期：2020-06-30；**修回日期：**2020-09-28

基金项目：国家自然科学基金资助项目(61871176)；河南省高等学校重点科研项目应用研究计划(202102110265)；河南省科技厅重点基金资助项目(172102210230)；河南工业大学创新基金计划(2020ZKCJ02)；河南省高等学校青年骨干教师培养计划(2019GZGG083)

光学图像加密技术是一种适用于图像信息安全的处理手段，将光学方法运用到图像的密码系统，是一种非常有效的加密方法。该技术有效地提高了数据处理速度，能够实现高冗余和多维度信息的处理，因此非常适合于图像信息的加密。光学图像加密技术具有很高的安全性，加密后的图像不易受到非法攻击和破解，在图像加密领域得到了广泛关注[5−8]。LIU 等[9]对双随机相位编码光学加密进行了深入研究，表明双随机相位编码技术虽然具有加密速度快、容易实现等优点。但是该算法存在较强的线性特性，密文图像很容易遭受各种外在非法攻击。针对传统的双随机相位编码算法存在的不足，张博等[10]提出一种非对称的加密方法，通过等模分解方法结合分数阶 Fourier 对图像进行加密，并利用相位–幅度截断编码技术改变密码系统的对称性，实现了图像的加密。但该加密方法存在抗剪切攻击能力不高，并且还会出现解密质量不够理想等问题。MU 等[11]设计了一种多图像的加密算法，该方法通过像素排序实现置乱处理，并采用了傅里叶域中的向量分解加密方式来实现图像的安全加密。但多图像光学加密采用纵向叠加操作，极易引起串扰噪声问题，导致降低了解密图像的质量，并且算法的复用容量较小。陈晓东等[12]提出了一种彩色图像的光学加密方法，利用多混沌进行置乱来降低明文像素的相关性，并采用量子细胞神经网络，结合它的非线性属性，来有效地完成随机相位模板的调制处理。该方法能有效增大密钥空间，获得良好的加密效果。但使用超混沌系统进行相位调制的同时，也使得系统复杂程度过大，导致实现难度加大。CHEN 等[13]通过变换将彩色明文图像的 R(Red)、G(Green)、B(Blue)三通道分量进行处理，并利用等模分解方法对变换结果进行相同矢量分解，最后使用 Baker 映射完成置乱处理来实现图像的加密。但该方法在 Gyrator 变换过程中，使用的旋转角度是固定的，并且等模分解得到的加密和解密密钥是相同的，导致密钥的安全程度有所降低。

针对上述问题，本文提出了一种多彩色图像的非对称光学加密算法。该算法利用 Gyrator 变换的高敏感度优势，对图像分量进行旋转变换获得复杂分布函数，既增强了系统的敏感度，又增大了密钥空间。然后，结合非等模分解的非线性优势，使得加密和解密密钥各不相同，显著地提高了系统的安全性。通过联合变换和非等模分解，能够很好地消除干涉的多图像中出现的轮廓和串扰噪声问题。最后，文中通过实验测试来分析该算法的加密性能。相比于其他相关算法，本文算法的优势在于：1) 通过非等模分解技术，将明文加密为两个不同的矢量，有效消除了典型的基于干扰和多图像密码系统固有的轮廓显示和串扰问题；2)传统的多彩色图像加密方法，通常采用级联多层光电系统，导致密码系统的复杂性过高，而本文加密算法采用了多路复用紧凑光电系统，算法更为简便，且有效增大了加密容量，克服串扰噪声问题；3) 传统的基于变换的加密技术大都是采用固定的旋转角度，而本文算法采用的是一个动态变换过程，其旋转角度是根据不同的加密目标来变化的，有效增加了密文的复杂性，增强算法的抗攻击能力。

1　Gyrator 变换

Gyrator 变换 (Gyrator Transform，GT)[14]是一种线性正则变换，它产生相位空间中的位置和频率平面上的旋转，是处理二维信号的有效变换。设定输入信号为 $f(x,y)$，则旋转角度为 α 的 GT 形式可以表示为：

$$F(u,v)=\mathrm{GT}_{\alpha}\{f(x,y)\}=\frac{1}{|\sin\alpha|}\iint f(x,y)\cdot K_{\alpha}\,\mathrm{d}x\mathrm{d}y \tag{1}$$

式中：(x,y) 和 (u,v) 分别为输入平面和输出平面的坐标；α 为旋转角度；K_{α} 为 GT 的核函数，其模型为：

$$K_{\alpha}=\exp\left[\mathrm{j}2\pi\frac{(xy+uv)\cos\alpha-xv-yu}{\sin\alpha}\right] \tag{2}$$

GT 输出的主要控制参数是旋转角 α。它与傅里叶变换不同的地方在于，使用的控制参数 α 能够作为系统的额外密钥，它拥有较强的密钥敏感性，能够有效地提升系统的安全性能。GT 是通过 3 个具有固定距离的广义透镜来完成光学实现，其光学系统如图 1 所示。

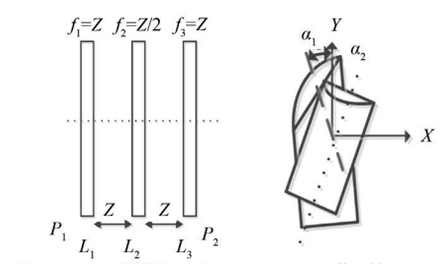


Fig.1 Optical system of Gyrator transform
图 1 Gyrator 变换的光学系统

2　非等模分解

非等模分解 (Unequal Modulus Decomposition, UMD)[15]是将二维图像分解成 2 个具有不等相位和幅值的独立掩模的过程。在数学表达中，复数形式也可以表示为二维笛卡尔坐标系中对应的向量形式，其中横轴表示实部，纵轴表示虚部。假设 $\boldsymbol{X}(u,v)$ 是一个表示原始图像的

矢量，$\boldsymbol{X}(u,v)$的振幅A和相位φ分别为$A=\left|\boldsymbol{X}(u,v)\right|$和$\phi=\arg\left[\boldsymbol{X}(u,v)\right]$。非等模分解模型如图2所示。其中，$\beta(u,v)$和$\gamma(u,v)$是分布在$[0,2\pi]$区间内的随机函数。通过几何变换，$\boldsymbol{X}(u,v)$被分解成2个矢量$\boldsymbol{Z}_1$和$\boldsymbol{Z}_2$，并且两者的振幅和相位均不相等。矢量$\boldsymbol{Z}_1$和$\boldsymbol{Z}_2$表示为：

$$\boldsymbol{Z}_1=\frac{A\sin(\beta-\phi)}{\sin(\beta-\gamma)}\mathrm{e}^{\mathrm{j}\gamma} \tag{3}$$

$$\boldsymbol{Z}_2=\frac{A\sin(\phi-\gamma)}{\sin(\beta-\gamma)}\mathrm{e}^{\mathrm{j}\beta} \tag{4}$$

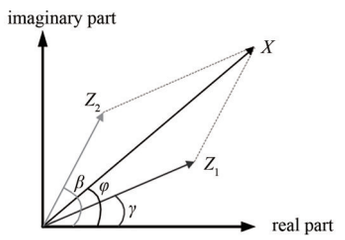


Fig.2 Schematic diagram of non equimodular vector decomposition

图2 非等模矢量分解示意图

式中：j为虚数；e为常量指数；sin( )为正弦函数。

为了便于表达，UMD过程可表示为：

$$\left[\boldsymbol{Z}_1(u,v),\boldsymbol{Z}_2(u,v)\right]=\mathrm{UMD}_{\beta,\gamma}\left[\boldsymbol{X}(u,v)\right] \tag{5}$$

3 本文光学图像加密算法

本文结合Gyrator变换和非等模矢量分解，对多幅彩色图像进行光学干涉处理。通过利用不同的旋转角度来分别对彩色图像三基色分量进行Gyrator变换，以获得相应的复杂分布函数。借助非等模矢量分解技术进行不等矢量分解，接着利用Gyrator逆变换对其中一个矢量逆变换处理，以生成密文图像。加密过程如图3所示，其对应的光学系统见图4。假设本文加密使用的彩色图像数量为N。根据基色理论，每幅彩色图像均由红、绿、蓝三基色组成。设定第i个图像的第j个分量记为$I_{i,j}$(其中，$i=1,2,3,\cdots,N$和$j=\{R,G,B\}$)，则第一幅彩色图像可表示为：

$$I_{1,j}(x,y)=\left[I_{1,R}(x,y),\ I_{1,G}(x,y),\ I_{1,B}(x,y)\right] \tag{6}$$

式中$I_{1,\mathrm{R}}$为第1个图像的R分量。

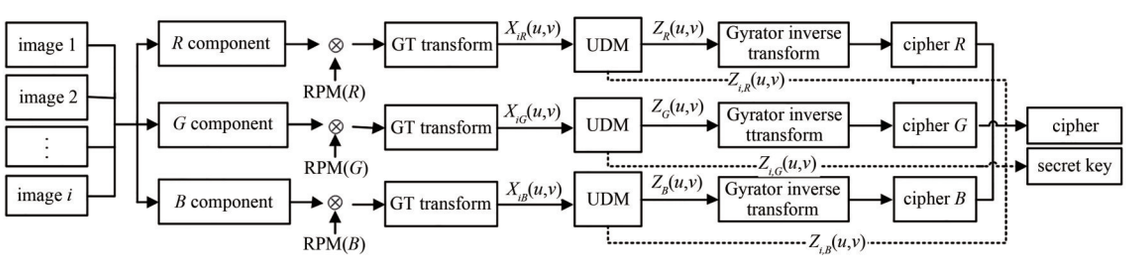


Fig.3 Process of optical encryption algorithm in this paper

图3 本文光学加密算法的过程

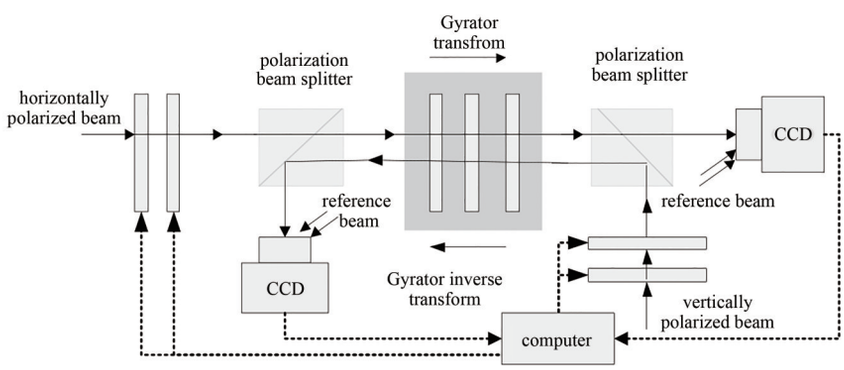


Fig.4 Optical system of the proposed algorithm

图4 所提算法的光学系统

在本文的加密系统中，将N幅彩色图像按其三色分量(R,G和B)进行分类叠加，共分成3组(分别为R,G,B分量)，然后单独对这三通道进行编码，并且3个通道的编码过程均相同。这里只介绍R分量的编码过程。具体的加密过程如下：

1) R 分量的调制。利用 Logistic 映射生成一组随机序列 $X=\{x_1,x_2,\cdots,x_{M\times N}\}$，然后将其重新排列，得到二维矩阵 $\boldsymbol{Y}=\{y_{i,j}\,|\,i=1,2,\cdots,M;\ j=1,2,\cdots,N\}$，则随机相位掩码为 $M_{i,R}=\exp(\mathrm{i}2\pi\varphi(x,y))$，其中，$\varphi(x,y)$ 为随机分布在[0, 2π]的相位。Logistic 映射函数为：

$$x_{i+1}=\mu x_i(1-x_i) \tag{7}$$

式中：$\mu\in[0.82,4]$ 为控制参数；x_i 为系统变量。

再利用 $M_{i,R}$ 对 R 分量图像 $I_{i,R}(x,y)$ 进行调制，使其相位值均匀地分布在区间 $[0,2\pi]$，得到调制处理图像 $I'_{i,R}(x,y)$：

$$I'(x,y)=\sqrt{I_{i,R}(x,y)}\exp[\mathrm{i}2\pi\varphi(x,y)] \tag{8}$$

式中 $I_{i,R}$ 为第 i 个图像的 R 分量。

2) Gyrator 变换处理。为提高系统的安全性，本文采用 Gyrator 变换来完成图像 $I'_{i,R}(x,y)$ 的初始预处理，得到复杂分布函数 $X_{i,R}(u,v)$：

$$X_{i,R}(u,v)=\mathrm{GT}_{\alpha}\{\sqrt{I_{i,R}(x,y)}\cdot M_{i,R}(x,y)\} \tag{9}$$

式中 α 是旋转角度为 α 的 Gyrator 变换。

3) 非等模矢量分解。将 R 分量的 $\boldsymbol{X}_{i,R}(u,v)$ 分解成 2 个矢量，第 1 个矢量是固定的，并在所有图像的所有 R 分量之间共享，第 2 个矢量被用作 R 分量的解密密钥，并且在每幅图像中这个矢量是各不相同的。令 $i=1$，则 $\boldsymbol{X}_{i,R}(u,v)$ 为第一幅图像 R 分量的矢量，通过非等模矢量分解，将 $\boldsymbol{X}_{1,R}(u,v)$ 分解成 2 个矢量 $\boldsymbol{Z}_1=\boldsymbol{Z}_R(u,v)$ 和 $\boldsymbol{Z}_2=\boldsymbol{Z}_{1,R}(u,v)$：

$$\lfloor\boldsymbol{Z}_R(u,v),\boldsymbol{Z}_{1,R}(u,v)\rfloor=\mathrm{UMD}_{\alpha_R,\beta_R}\lfloor\boldsymbol{X}_{1,R}(u,v)\rfloor \tag{10}$$

式中：α_R 和 β_R 为分布在 $[0,2\pi]$ 区间内的随机函数；$\boldsymbol{Z}_R(u,v)$ 为共享矢量；$\boldsymbol{Z}_{1,R}(u,v)$ 为用于第一幅图像 R 分量解密的矢量；UMD 代表非等模矢量分解。

类似的，令 $i=2,3,\cdots,N$，则其余的 $\boldsymbol{X}_{i,R}(u,v)$ 被分解为解密密钥矢量 $\boldsymbol{Z}_{i,R}(u,v)$ 和共享矢量 $\boldsymbol{Z}_R(u,v)$。

4) Gyrator 逆变换处理。利用 Gyrator 逆变换对共享矢量 $\boldsymbol{Z}_R(u,v)$ 进行处理，得到 R 分量的密文图像 $C_R(x',y')$：

$$C_R(x',y')=\mathrm{GT}_{-\gamma}\{\boldsymbol{Z}_R(u,v)\} \tag{11}$$

式中 α 是旋转角度为 α 的 Gyrator 逆变换。

5) 输出密文图像。重复步骤 1)~4)，对图像的 G 分量和 B 分量分别进行加密操作，得到 G 分量密文 $C_G(x',y')$ 和 B 分量密文 $C_B(x',y')$，然后将这 3 个分量密文再融合，输出最终的密文 $C(x,y)$：

$$C(x,y)=[C_R(x',y'),C_G(x',y'),C_B(x',y')] \tag{12}$$

图像的解密是一个相反的过程，且该过程使用了密钥 $\boldsymbol{Z}_{i,R}(u,v)$ 来完成解密。详细过程如下：

1) 利用旋转角度为 α 的 Gyrator 变换对密文图像进行处理，得到共享矢量 $\boldsymbol{Z}'_R(u,v),\boldsymbol{Z}'_G(u,v)$ 和 $\boldsymbol{Z}'_B(u,v)$：

$$\begin{cases}\boldsymbol{Z}'_R(u,v)=\mathrm{GT}_{\alpha}\{C_R(x',y')\}\\ \boldsymbol{Z}'_G(u,v)=\mathrm{GT}_{\alpha}\{C_G(x',y')\}\\ \boldsymbol{Z}'_B(u,v)=\mathrm{GT}_{\alpha}\{C_B(x',y')\}\end{cases} \tag{13}$$

2) 将共享向量和密钥向量进行矢量合成，再分别用 Gyrator 逆变换进行解密处理：

$$\begin{cases}I'_R(x,y)=\left|\mathrm{GT}_{-\alpha}\{\boldsymbol{Z}'_R(u,v)+\boldsymbol{Z}_{i,R}(u,v)\}\right|^2\\ I'_G(x,y)=\left|\mathrm{GT}_{-\alpha}\{\boldsymbol{Z}'_G(u,v)+\boldsymbol{Z}_{i,G}(u,v)\}\right|^2\\ I'_B(x,y)=\left|\mathrm{GT}_{-\alpha}\{\boldsymbol{Z}'_G(u,v)+\boldsymbol{Z}_{i,G}(u,v)\}\right|^2\end{cases} \tag{14}$$

式中$|\cdot|$为模运算。

3) 将解密得到的三分量图像进行融合，输出最终的解密图像$I'(x,y)$：

$$I'(x,y)=\left[I'_R(x,y),I'_G(x,y),I'_B(x,y)\right] \tag{15}$$

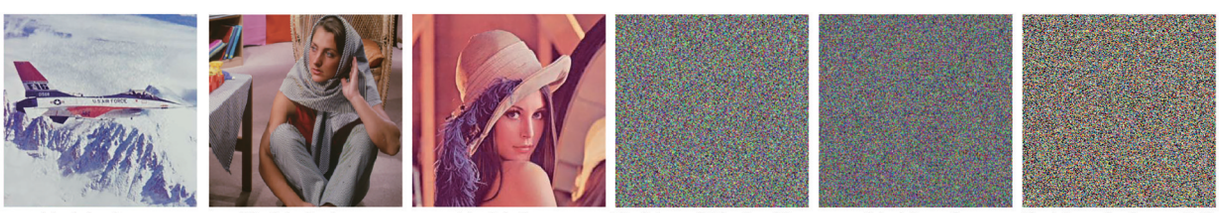
4 实验结果与分析

为了充分检验所提光学加密方法的可靠性，设置多组实验来完成相关性能的评估。使用 Windows 7操作系统，处理器 CPU 主频为 3.60 GHz，内存为 RAM 4 GB，实验全部过程在 MATLAB 2017a 条件下进行仿真测试。实验过程中，选取了 2 种多图像加密算法作为对照组：文献[16]与文献[17]。选用 3 幅彩色图像作为样本，尺寸均为 256×256。经反复测试，设置参数为：Logistic 控制参数$u=3.98$，GT 旋转角度$\alpha=2.0$ rad，波长$\lambda=632.8$ mm。

4.1 光学图像加密效果

本文使用了图像 Airplain,Lena 和 Barbara 作为测试样本进行了相关实验，且将文本加密算法以及文献[16]和文献[17]的算法分别对这 3 副图像进行了联合测试。由测试效果可知，3 种算法加密后的密文均类似于随机的噪声图像，原始信息均完全被隐藏，无法从密文中观察到与原始图像相关的信息，说明了 3 种算法均实现了原始信息的充分混乱，具有较好的信息隐藏能力。

为客观验证算法的合理性，借助信息熵值[18]对 3 种密文进行评估，测试结果见表 1。由实验数据可知，本文获得的信息熵值数据最好，其数值为 7.997，这一结果比较靠近理想数值 8；而其他两者算法相对更低，分别为 7.993 和 7.991。说明了本文得到的密文混乱效果更好，保密能力更强。原因是本文算法利用 Gyrator 变换的高敏感性分别对彩色图像的三基色分量进行处理，而后采用非等模方法进行振幅和相位信息不均等分解，并且密文图像由多副图像融合而成，使得加密后的图像随机性更强。而文献[16]只对图像的低频和高频信息进行分解加密，该算法只将图像的高频映射图像分割为 2 个矩阵，而没有对低频映射图像进行分割。然而图像大部分信息集中在低频，虽然联合了 2 次感知矩阵，但图像信息的相关性没有被充分破坏，使得密文的混乱程度不够。文献[17]使用了分数傅里叶变换进行处理，而傅里叶变换具有一定的线性特性，因此其非对称性不强，导致加密图像相关性较高，使算法安全性不高。



(a) plain airport (b) plain Barbara (c) plain Lena (d) cipher of this algorithm (e) cipher of reference[16] algorithm (f) cipher of reference[17] algorithm

Fig.5 Joint encryption effect of three kinds of images

图 5 3 种图像的联合加密效果

表 1 密文熵值测试

Table1 Entropy test of cipher

name	algorithm	reference[16]	reference[17]
entropy value	7.997	7.993	7.991

4.2 密钥敏感性测试

密钥敏感性能够较好地衡量算法有效性，当密钥信息产生微小的变化便不能解密出原始信息，具备严格的“雪崩效应”[19]。对此，本文对旋转角度α进行了敏感性测试。将其做非常细微的调整$\alpha'=\alpha\pm10^{-14}$，然后用$\alpha'$来完成相应的解密。解密后的效果见图 6。由图可知，解密出来的所有图像丢失了原始信息，且对应的均方误差(Mean Square Error, MSE)值均高于 2 500；而只有当使用正确的密钥时，才能解密出所有图像的真实信息，其 MSE 值接近于零。因此，实验测试结果说明了本算法拥有较好的密钥敏感性。其原因是所提加密算法采用了 Logistic 混沌映射生成的随机掩码来预处理彩色图像的三基色分量，充分考虑了混沌掩码对密钥的敏感性，而且对明文进行不同旋转角度α的 Gyrator 变换，并将α作为控制参数，从而显著增强了算法的密钥敏感性。

4.3 抗剪切攻击能力测试

为检验本文方法的抵抗攻击能力，对其进行了抗剪切攻击测试。采用的测试方法为：对 3 种算法的密文图像进行同等剪切，然后利用各种算法完成解密。测试效果见图 7~图 9。由图可知，本文加密方法解密得到的图像效果接近于初始明文，几乎保留了所有原始信息。而其他 2 种算法得到的解密图像质量明显更差，虽然能够分辨出整体外观特性，但是图像的部分细节信息出现了丢失，未能准确复原出所有的原始信息。通过对比测试结果可知，本文算法的抗剪切性能要优于文献[16]和文献[17]，也表明本文算法拥有更强的鲁棒性。主要原因是本算法通过非等模分解技术，分别对图像三基色的振幅信息进行了 Gyrator 逆变换处理，密文的相邻像素间的相关性被大大降低，像素灰度分布的随机性能更好，即使部分信息被剪切掉，内容信息的丢失会更少，解密出的图像质量会更好，从而其抗剪切攻击性能会更优越。文献[16]中的密文低频信息没有被充分混乱，像素间相关性更高，像素分布均匀程度不够，使得受剪切攻击后恢复出来的图像质量更差，因此其抗剪切攻击能力更差。文献[17]密码系统通过分数傅里叶变换进行处理，线性特征明显，导致密文像素间相关性较高，也就降低了其抗剪切攻击能力。

4.4 噪声攻击测试

噪声干扰是图像加密过程中经常出现的问题，会使图像的解密质量下降[12]。对此，为检验本文算法有效性，引入高斯噪声进行测试。图像经噪声干扰后的表达式如下：

$$C'=C+KG \tag{16}$$

式中：C 为明文图像；C' 为噪声干扰图像；G 为使用的高斯噪声；K 为噪声强度系数。

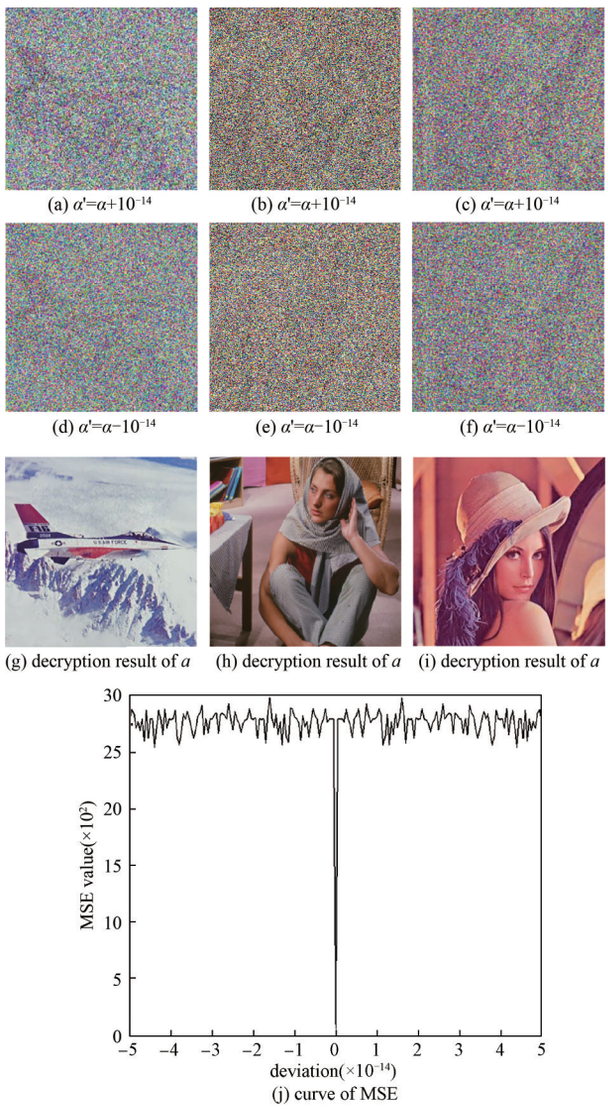


Fig.6 Key sensitivity test
图 6 密钥敏感性测试

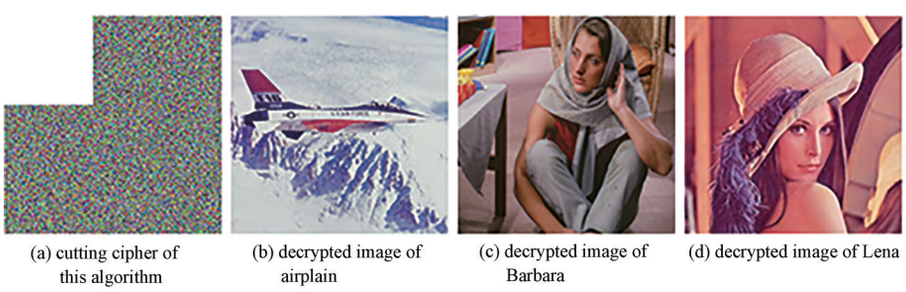


Fig.7 Anti-cutting effect of this algorithm
图 7 本文算法的抗剪切攻击效果

设定噪声强度 K=0.1，对密文进行解密，解密结果如图 10 所示。由图可知，在相同的噪声强度情况下，3 种算法均能解密出图像的大部分信息，但是与本文算法相比，其他 2 种算法解密图像质量更模糊，部分纹理细节信息出现丢失。图 11 为 3 种算法的抗噪声攻击性能对比测试。由数据可知，3 种算法解密图像的 *MSE* 值与 K 成线性关系，即 *MSE* 值随着 K 的增大而增大，而本算法的 *MSE* 值整体均低于其他 2 种算法。因此，这也说明了本文加密方法的抵抗噪声攻击性能更好。其原因是因为本文利用 Gyrator 变换和 Gyrator 逆变换操作以及非等模分解，使

得整个加密过程都是在频域内完成的，将输入明文分解为 2 个不同的矢量，呈现出更强的非线性特征与抗噪能力。而文献[16]和文献[17]算法虽然采用了相位截断技术，也具备一定的非对称性和频域特性，但其没有对保留信息进行处理，从而导致了密文的安全性不佳，削减了抗噪声攻击能力。

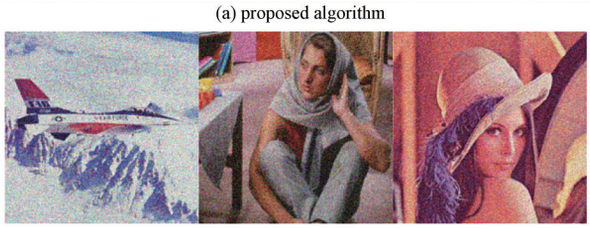
(a) cutting cipher of reference[16] algorithm (b) decrypted image of airplain (c) decrypted image of Barbara (d) decrypted image of Lena

Fig.8 Anti-cutting effect of reference[16] algorithm
图 8 文献[16]的抗剪切攻击效果

(a) cutting cipher of reference[17] algorithm (b) decrypted image of airplain (c) decrypted image of Barbara (d) decrypted image of Lena

Fig.9 Anti-cutting effect of reference[17] algorithm
图 9 文献[17]的抗剪切攻击效果

(a) proposed algorithm



(b) reference[16] algorithm

(c) reference[17] algorithm

Fig.10 Test results of three algorithms against noise attack (K=0.1)
图 10 3 种算法的抗噪声攻击测试结果(K=0.1)

4.5 串扰噪声测试

串扰噪声[11]是多图像加密系统中常见的问题，在一定程度上会限制系统的加密能力。为了验证本算法的有效性，引入相关性系数 R 进行评估，相关性系数[20] R 可表示为：

$$R=\frac{E\left\{[I-E(I)]\cdot[I'-E(I')]\right\}}{\sqrt{E[I-E(I)]^2\cdot E[I'-E(I')]^2}} \tag{17}$$

式中：I和I'分别为明文图像和密文图像；E为期望算子。

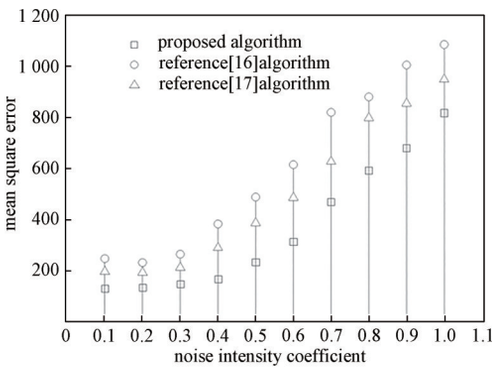


Fig.11 Comparative test of anti noise attack performance

图 11 抗噪声攻击性能对比测试

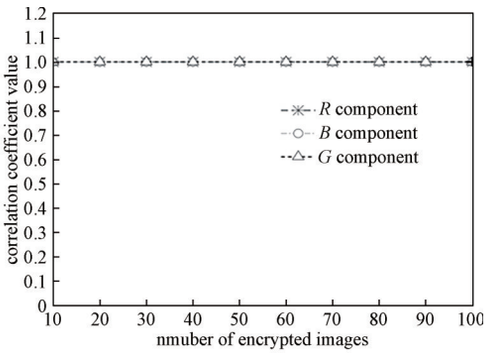


Fig.12 Test of the anti crosstalk noise capability of this algorithm

图 12 所提算法的抗串扰噪声能力测试

为评估串扰噪声对本密码系统解密图像的影响，文中使用100幅彩色图像作为加密图像。当所有密钥都匹配正确时，计算解密图像的每个颜色分量的相关性系数值(从10到100，递增10张图像)，测试数据结果见图12。由图可知，随着加密图像数量的增加，解密图像各颜色分量的相关系数值均保持理想值1，说明当所提算法采用高加密容量时，解密图像的质量仍然保持不变。可见，本文加密算法不会受到串扰噪声的影响。其主要原因为本文采用了紧凑的偏振光电实现系统，具有较好的多路复用能力，加密容量更高，图像之间的加密独立性更强，充分解决了串扰噪声问题，使得解密图像质量更好。

5　结论

为消除通常光学图像加密系统容易出现轮廓问题和串扰噪声问题，本文提出了一种基于Gyrator变换和非等模分解的多彩色图像加密方法。利用Gyrator变换的高敏感度对彩色图像的三基色分量进行旋转变换，然后借助非等模分解方法，将变换后的结果分解成两个振幅和相位均不等的矢量，进一步提高了加密系统的非线性特性。实验测试结果表明，本算法能够有效地解决轮廓和串扰噪声问题，并具备较强的密钥敏感性和鲁棒性，能够有效抵抗各种攻击等。

参考文献：

[1] 史进,蔡竞,徐锋. 基于QR码与级联Fourier变换的图像光学加密算法[J]. 太赫兹科学与电子信息学报, 2020,18(3):462-469. (SHI Jin, CAI Jing, XU Feng. Multi-image optical encryption algorithm based on QR code and concatenated fractional Fourier transform[J]. Journal of Terahertz Science and Electronic Information Technology, 2020,18(3):462-469.)

[2] GIRIJA Riakuy,SINGH Hukum. A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition[J]. Optics and Quantity Electronics, 2018,50(5):210. doi:10.1007/s11082-018-1472-6.

[3] SUI Liansheng, ZHAO Xiaoyu, HUANG Chongtian. An optical multiple-image authentication based on transport of intensity equation[J]. Optics and Lasers in Engineering, 2019,11(6):116-124. doi:10.1016/j.optlaseng.2019.01.006.

[4] SUI Liansheng,DU Cong,ZHANG Xiao. Double-image encryption based on interference and logistic map under the framework of double random phase encoding[J]. Optics and Lasers in Engineering, 2019,122(11):113-122. doi:10.1016/j.optlaseng.2019.06.005.

[5] FARAGALLAH O S, AFIFI A. Optical color image cryptosystem using chaotic baker mapping based double random phase encoding[J]. Optical and Quantum Electronics, 2017,49(3):89-96. doi:10.1007/s11082-017-0909-7.

[6] SUI Liansheng, CHEN Yin, WANG Zhanmin. Single-pixel correlated imaging with high-quality reconstruction using iterative phase retrieval algorithm[J]. Optics and Lasers in Engineering, 2018,111(12):108-113. doi:10.1016/j.optlaseng.2018.08.001.

[7] CHEN Xudong,LIU Qi,WANG Qionghua. Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction[J]. Optics and Laser Technology, 2018,107(11):302-312. doi:10.1016/j.optlastec.2018.06.016.

[8] LUAN Guangyu,LI Aichuan,ZHANG Dongmei. Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain[J]. IEEE Photonics Journal, 2018,11(1):1-7. doi:10.1109/JPHOT.2018.2886295.

[9] LIU Xiaoli,WU Jiachen,HE Wenqi. Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding[J]. Optics Express, 2015,23(15):18955-18968. doi:10.1364/oe.23.018955.

[10] 张博,龙慧,江沸菠. 基于相干叠加与模均等矢量分解的光学图像加密算法[J]. 电子与信息学报, 2018,40(2):438-446. (ZHANG Bo,LONG Hui,JIANG Feibo. Optical image encryption algorithm based on coherent superposition and equal modulus vector decomposition[J]. Electronics and Information Technology, 2018,40(2):438-446.) doi:10.11999/JEIT170489.

[11] MU Xiaofang,QI Hui,LI Xiaobin. High efficiency optical multi-image encryption algorithm based on the vector computation in Fourier domain[J]. Machine Tool Hydraulics, 2019,47(18):126-131.) doi:10.3969/j.issn.1001-3881.2019.18.022.

[12] 陈晓冬,底晓强,李锦青. 基于多混沌和分数Fourier的光学图像加密算法[J]. 南京大学学报(自然科学), 2019,55(2):251-263. (CHEN Xiaodong,DI Xiaoqiang,LI Jinqing. Optical image encryption algorithm based on multi-chaos and fractional Fourier[J]. Journal of Nanjing University(Natural Science), 2019,55(2):251-263.) doi:10.13232/j.cnki.jnju.2019.02.010.

[13] CHEN Hang,TANOUGAST Camel,LIU Zhengjun. Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains[J]. Optics and Lasers in Engineering, 2017,93(8):1-8. doi:10.1016/j.optlaseng.2017.01.005.

[14] 康万杰. 基于Gyrator频谱分解与混沌螺旋相位掩码的多图像光学加密算法[J]. 电子测量与仪器学报, 2018,32(5):116-125. (KANG Wanjie. Multi image optical encryption algorithm based on gyrator spectrum decomposition and chaotic helical phase mask[J]. Journal of Electronic Measurement and Instrumentation, 2018,32(5):116-125.) doi:10.13382/j.jemi.2018.05.015.

[15] CHEN Linfei,GAO Xiong,CHEN Xudong. A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition[J]. Optics Laser Technology, 2016,78(8):167-174. doi:10.1016/j.optlastec.2015.11.009.

[16] 薛娟,刘萍. 基于混沌Gyrator变换与离散小波变换的多图像光学同步加密算法[J]. 电子测量与仪器学报, 2019,33(11):136-146. (XUE Juan,LIU Ping. Multi-image optical encryption algorithm based on fusion of chaotic gyrator transform and discrete wavelet transform[J]. Electronic Measurement and Instrumentation, 2019,33(11):136-146.) doi:10.13382/j.jemi.B1902337.

[17] SUI Liansheng,ZHANG Xiao,HUANG Chongtian. Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms[J]. Optics Laser and Engineering, 2019,113(10):29-37. doi:10.1016/j.optlaseng.2018.10.002.

[18] LIU Lei, SHAN Mingguang, ZHONG Zhi. Color image encryption based on enhanced optical interference with different diffraction distances and linear phase color-blend[J]. Journal of Optics, 2019,21(1):1-13. doi:10.1088/2040-8986/aaf0f4.

[19] MUHAMMAD Rafiqabuturab. Asymmetric multiple information cryptosystem based on chaotic spiral phase mask and random spectrum decomposition[J]. Optics and Laser Technology, 2018,98(6):298-308. doi:10.1016/j.optlastec.2017.08.010.

[20] MUHAMMAD Rafiqabuturab. A superposition based multiple-image encryption using Fresnel-domain high dimension chaotic phase encoding[J]. Optics Laser and Engineering, 2020,129(7):38-47. doi:10.1016/j.optlaseng.2020.106038.

作者简介：

李 培(1985-)，女，河南省新郑市人，硕士，副教授，主要研究方向为图像处理、信息技术. email: Lipei1985zly@21cn.com.

朱春华(1976-)，女，郑州市人，博士，教授，主要研究领域为数字图像处理、光学应用技术、宽带无线通信.