文章编号：2095-4980(2020)03-0462-08

# 基于 QR 码与级联 Fourier 变换的图像光学加密算法

史　进[1a]，蔡　竞[1b]，徐　锋[2]

(1.浙江警察学院 a.现代教育技术实验中心；b.刑事科学技术系，浙江 杭州 310053；
2.浙江大学 信息技术中心，浙江 杭州 310058)

**摘　要：**为实现对多幅图像完成同步加密，并提高密文的安全性与抗几何变换攻击能力，提出基于快速响应码(QR)与级联分数阶 Fourier 变换的多图像光学加密算法。借助 Logistic 映射，获取随机掩码，联合 Fresnel 波带、Hilbert 模型，构建调制掩码；引入复数理论，借助模板图像对第一幅明文实施处理，形成复数图像；采用分数阶 Fourier 变换，借助调制掩码，对复数图像实施处理，并基于相位-幅度截断机制，得到相位分布与密钥；再结合相位截断方法与分数阶 Fourier 变换，设计级联快速傅里叶变换(FFT)加密机制，通过调制掩码与相位分布，对剩余的多幅明文实施频域变换处理，输出融合幅度图像，并将其转换为对应的 QR 码；引入 Gyrator 变换，通过相应的光电装置，利用激光束对 QR 码完成干涉处理，得到密文。测试数据表明：相对已有的多图像光学加密技术，本算法具备更高的保密安全性与抗攻击能力，在裁剪变换下，其复原图像的失真度更小。

**关键词：**多图像光学加密；QR 码；分数阶 Fourier 变换；相位-幅度截断；Fresnel 波带

**中图分类号：**TN911；TP391　　**文献标识码：**A　　**doi：**10.11805/TKYDA2019217

# Multi-image optical encryption algorithm based on QR code and concatenated fractional Fourier transform

SHI Jin[1a]，CAI Jing[1b]，XU Feng[2]

(1a.Center of Modern Educational Technology Experiment；1b.Department of Criminal Science and Technology，Zhejiang Police College，Hangzhou Zhejiang 310053，China；2.Center of Information Technology，Zhejiang University，Hangzhou Zhejiang 310058，China)

**Abstract：**In order to achieve synchronous encryption of multiple images and improve the security of ciphertext and the ability to resist geometric transformation attacks, the multi-image optical encryption algorithm based on quick response and cascaded fractional transform is proposed in this paper. By introducing complex number theory, the first plaintext is processed with template image to form complex image. The complex image is decomposed based on the phase-amplitude truncation mechanism to obtain the phase distribution. With the help of Logistic map, the random masks are obtained, and the modulation masks are constructed by combining Fresnel band and Hilbert models. Combining the phase truncation method with fractional order Fourier transform, a cascaded Fast Fourier Transform(FFT) encryption mechanism is designed, and the remaining plaintext is processed by frequency domain transformation based on modulating mask and phase distribution to output the amplitude image, then it is converted into corresponding Quick Response(QR) code. The Gyrator transform is introduced, and the QR code is interfered by laser beam through the corresponding photoelectric device to get the cipher. The test data show that compared with the existing multi-image optical encryption technology, the proposed algorithm has higher security and anti-attack ability, and the distortion of the restored image is smaller under the clipping transformation.

**Keywords：**multi-image optical encryption；QR code；fractional Fourier transform；phase-amplitude truncation；Fresnel band

**收稿日期：**2019-06-18；**修回日期：**2019-04-16

**基金项目：**公安部科技强警基础科学技术研究专项资助项目(2018GABJC34)；教育部—中国移动科研基金资助项目(MCM20130671)

**作者简介：**史　进(1978–)，男，硕士，主要研究方向为图像处理、信息安全、数据挖掘与机器学习。email:shijg1978zjplo@sina.com

图像在不同地点使用时，通常要依赖网络来实现，在这种条件下，其易遭受未知攻击，使得相关信息被肆意攻击与非法传播，给其内容的真伪辨别增加了困难[1−3]。为了解决图像在存储与传输过程中的安全问题，国内外学者们提出了相应的数字图像加密方法，尤其是光学加密技术，因其具有多维性操作，且效率高的优势，在诸多领域得到了广泛应用。如李建军等[4]为了增强密文的可靠性，提出了新的光学加密方案，得到对应的密文。SUN 等[5]为了提高密文抵御外来攻击的能力，提出了伽马分布与 Gyrator 变换的光学加密算法，得到密文。LIU 等[6]为了优化光学密文的安全性，提出了分数小波域中基于混沌压缩传感和相移干涉的光学图像加密，获取密文。

数字图像光学加密主要分为 2 大类：单幅图像加密[4−6]和多图像同步加密[7−8]。单图像的光学加密技术虽然可以解决图像在存储与传输过程中的安全问题，但难以对多幅图像实施同步加密，无法迎合实际工程需求[3]。针对此问题，研究人员开发了多图像光学加密方案，如郭静博等[3]利用离散余弦变换(Discrete Cosine Transform，DCT)来分解压缩明文，得到每个明文对应的 DCT 系数，通过迭代复数模型，将多图像融合为单幅图像，再利用圆柱衍射域的相位截断机制，联合混合掩码，对复合图像实施调制，输出加密密文。此技术直接利用激光束作用于明文，得到的密文对噪声、裁剪等攻击的鲁棒性不理想。PAN 等[7]联合 DCT 方法与 FMT(Fractional Mellin Transform)机制，设计了新的光学加密技术。该技术主要是通过对图像实施裁剪和拼接来构建融合图像，忽略了明文的其他信息，导致其复原图像的质量不理想，尤其是在几何变换条件下，其失真度较大。CHEN 等[8]引入小波变换获取每幅明文的频谱信息，并分别组合高频、低频信息，以此构建相应的高频、低频映射，再使用 CS 方法获取高频映射的测量矩阵，通过 Fresnel 变换，对低频映射以及测量矩阵实施光学调制，形成密文。该方案在对明文信息进行调制时，主要借助随机掩码来实现，难以解决光学系统中的光轴校准缺陷，削弱了密文的抗攻击能力。

为了提高密文的安全性与抗外部攻击能力，本文提出了基于 QR 码与级联分数阶 Fourier 变换的多图像光学加密算法。

## 1　多图像光学加密算法

基于 QR 码与级联分数阶 Fourier 变换的多图像光学加密算法过程如图 1 所示。该算法主要有 3 个过程：a) 调制掩码的构建；b) 基于级联 FFT 变换的多图像同步调制；c) 基于 QR 码与 Gyrator 变换的图像加密。

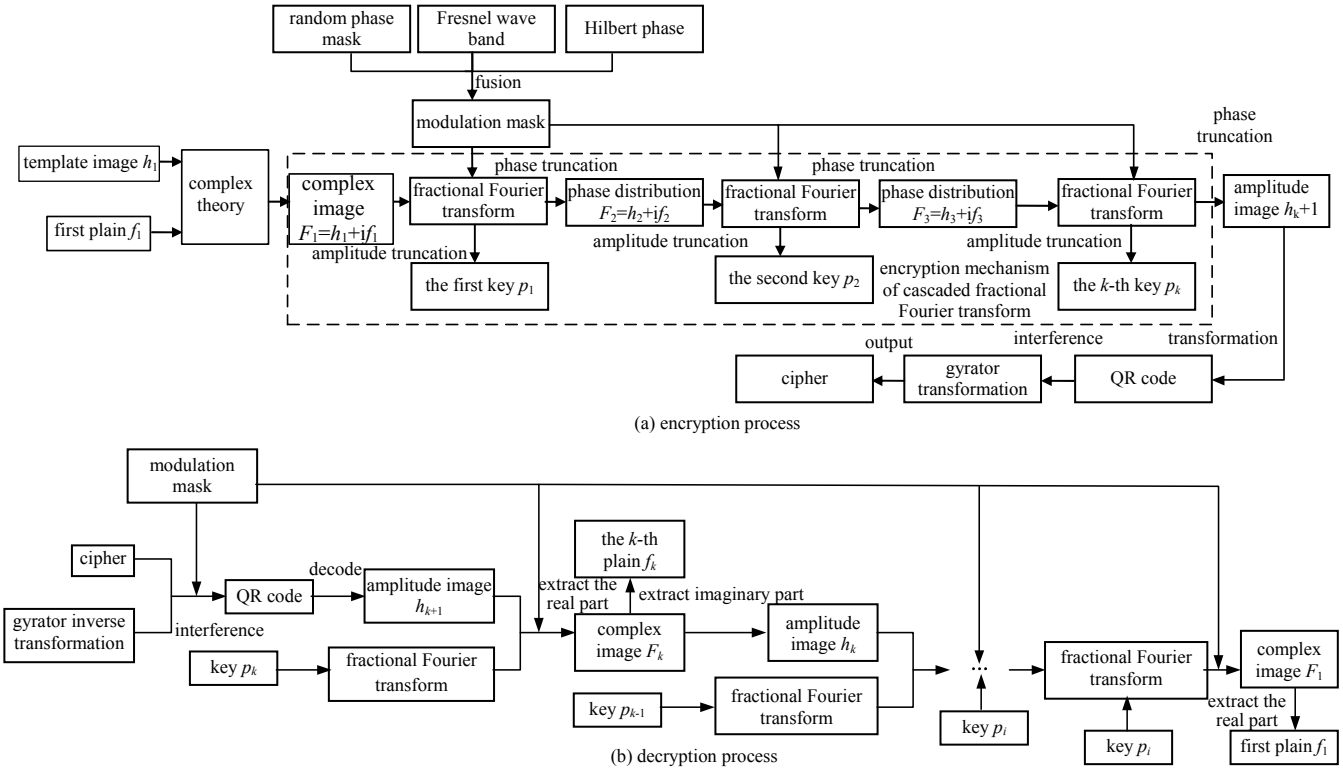



Fig.1 Multi-image optical encryption process of the proposed algorithm

图 1 所提算法的多图像光学加密过程

### 1.1 调制掩码的构建

在光学加密系统中，调制掩码至关重要，对密文的抗破译能力影响较大。当前的大部分光学加密技术中，主要采用随机相位掩码实施明文的调制，虽然改善了密文的随机性，但容易产生较大的光轴对准误差，限制了系统的安全性[9]。为此，本文利用 Logistic 映射生成随机掩码，将其与 Fresnel 波带[10]、Hilbert 模型[11]融合，得到新的调制掩码，不仅可以兼顾系统的随机性，而且可以充分利用 Fresnel 波带、Hilbert 模型自身的光学元件来校准光轴。Logistic 映射具有结构简单等特点，其函数为[12]：

$$x_{n+1}=\mu x_n\left(1-x_n\right) \tag{1}$$

式中：$\mu\in[0,4]$为混沌轨迹控制参数；$x_n\in[0,1]$，$x_0$分别为输出和初始值。

为强化加密系统对明文内容变化的敏感度，采用 SHA–256 方法[13]得到密钥 $K$，再把它分割成子密钥 $k_i$：

$$K=k_1,k_2,\cdots,k_{32} \tag{2}$$

随后，借助式(2)中的 $k_i$ 计算 $x_0$：

$$x_0=\mathrm{mod}\left(\left(\left(k_1\oplus k_3\oplus k_5\oplus\cdots\oplus K_{31}\right)+\sum_{i=1}^{32}\left(k_i\right)\right)/2^8,4\right) \tag{3}$$

利用 $\mu$ 和 $x_0$，对式(1)执行 $M\times N$ 次映射，形成混沌序列 $X=\left\{x_1,x_2,\cdots,x_{(M\times N)}\right\}$，并把 $X=\left\{x_1,x_2,\cdots,x_{(M\times N)}\right\}$重排为二维矩阵 $Y=\left\{b_{i,z}\middle|i=1,2,\cdots,M;z=1,2,\cdots,N\right\}$。根据式(4)，得到随机相位掩码 $S(x,y)$为：

$$S(x,y)=\exp\left[\mathrm{j}2\pi y_{i,z}(x,y)\right] \tag{4}$$

虽然 $S(x,y)$方便密钥的管理，但在光电混合装置中利用激光束对图像实施干涉时，会增大光轴对准误差[14]。本文联合 Fresnel 波带[10]与 Hilbert 模型[11]来确保整个系统光轴的对准度。由文献[10]发现，Fresnel 波带自身带有 1 个聚焦环，在光电装置中，可视为 1 个衍射部件，能够与光轴对准，相位模型如下[10]：

$$R(r,\varphi)=\exp\left[-\frac{\mathrm{j}\pi}{\lambda b}r^2\right] \tag{5}$$

式中：$\lambda$ 为波长；$b$ 为焦距；$r$ 为半径；j 为虚数单位。

在 Hilbert 相位掩码中，其任意径向线能够容忍一个 $P\pi$ 弧度的相对位误差，可提高光轴的对准度[11]。依据文献[11]，Hilbert 模型为：

$$H(r,\varphi)=\exp\left[\mathrm{j}p\varphi\right] \tag{6}$$

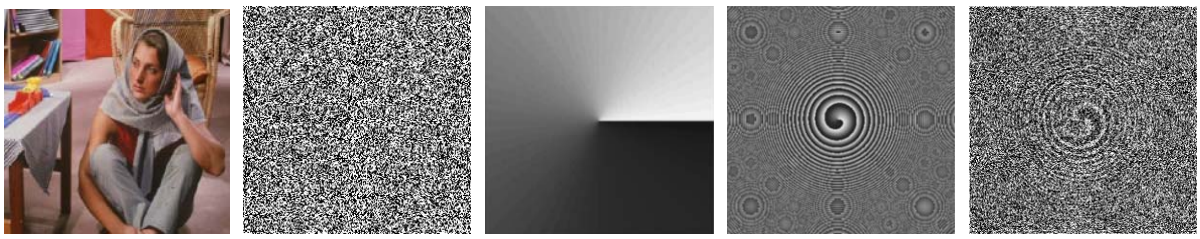
式中：$p$ 为 Hilbert 模型的阶数；$(r,\varphi)$为极坐标：$\begin{cases}r=x^2+y^2\\ \varphi=\arctan(y/x)\end{cases}$。

为了兼顾密文的随机性与系统光轴的校准，联合式(4)~式(6)，形成新的调制掩码 $C$：

$$C=\exp\left[\mathrm{j}\left[\left\{\arg\left(T(r,\varphi)\right)\right\}\times\left\{\arg\left(S(x,y)\right)\right\}\right]\right] \tag{7}$$

式中：$\arg(\bullet)$为相位提取操作；$T(r,\varphi)=\exp\left[\mathrm{j}\left(p\varphi-\frac{\pi}{\lambda b}r^2\right)\right]$。

新的调制掩码 $C$ 所含有的参数比 $S(x,y)$, $R(r,\varphi)$ 和 $H(r,\varphi)$ 中的任意一个都多，将其视为密钥，可显著扩大密钥空间与敏感性，具备更高的抗破译能力。将图 2(a)当作模板图像，设置 $p=1$, $r=3$, $b=40$ mm, $\lambda=632.8$ mm 和 $\mu=3$，通过式(1)~式(7)，得到的 $S(x,y)$, $R(r,\varphi)$, $H(r,\varphi)$ 和 $C(x,y)$ 分别见图 3(b)~3(e)。结果发现，$C(x,y)$综合了 $S(x,y)$, $R(r,\varphi)$ 和 $H(r,\varphi)$ 的优势，还可提高光轴对准度。



(a) template image (b) $S(x,y)$ (c) $H(r,\varphi)$ (d) $R(r,\varphi)$ (e) $C(x,y)$

Fig.2 Formation of modulation mask

图 2 调制掩码的形成

### 1.2 基于级联 FFT 变换的多图像同步调制

分数阶 Fourier 变换(FFT)是经典 Fourier 的推广，不仅保留了 Fourier 的特点，而且增加了模系数的能量聚集变化等优点[15]。对于二维图像 $f(x,y)$，其相应的 FFT 函数如下[15]：

$$g(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{\alpha,\beta}(x,y,u,v)f(x,y)\mathrm{d}x\mathrm{d}y \tag{8}$$

式中：$(u,v)$为输出的频域坐标；$K_{\alpha,\beta}(x,y,u,v)$为变换核函数。

$$K_{\alpha,\beta}(x,y,u,v)=\frac{\sqrt{1-\mathrm{j}\cot\alpha}\sqrt{1-\mathrm{j}\cot\beta}}{2\pi}\exp\left[\frac{x^2+u^2}{2\tan\alpha}-\mathrm{j}\frac{xu}{\sin\alpha}\right]\exp\left[\frac{y^2+v^2}{2\tan\beta}-\mathrm{j}\frac{yv}{\sin\beta}\right] \tag{9}$$

式中 $\alpha,\beta$ 为 FFT 的阶数。

通过式(8)，可获取任意图像的频域；再根据其可逆变换，实施复原[15]：

$$f(x,y)=F^{-\alpha,-\beta}\{g(u,v)\}=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{-\alpha,-\beta}(x,y,u,v)g(u,v)\mathrm{d}u\mathrm{d}v \tag{10}$$

为提高各明文直接的联系，提高密文的抗破译能力，本文多次利用 FFT 方法，形成基于级联 FFT 的多图像同步调制方法，过程如下：

1) 令明文为 $f_z(x,y),z=1,2,\cdots,K$，其大小为 $M\times N$。任意选择一幅图像 $h_1$ 作为模板，根据复数理论[16]，构建复数图像：

$$F_1=h_1+\mathrm{j}f_1 \tag{11}$$

2) 根据调制掩码 $C(x,y)$，基于 FFT 方法，对复数图像 $F_1$ 实施处理，得到频谱：

$$F'_1=\mathrm{FFT}^{\alpha,\beta}\{F_1\exp(\mathrm{j}C(x,y))\} \tag{12}$$

3) 引入幅度—相位截断机制[17]，对 Fourier 频谱实施分解，得到相位分布 $h_2$ 和第 1 个密钥 $P_1$：

$$\begin{cases}h_2=\mathrm{PT}\{F'_1\}\\P_1=\mathrm{AT}\{F'_1\}\end{cases} \tag{13}$$

式中：PT{ }为相位截断操作；AT{ }为幅度截断操作。

4) 根据 $h_2$ 及复数理论，对第 2 幅明文 $f_2$ 实施处理，得到新的复数图像 $F_2=h_2+if_2$；再对 $F_2$ 执行步骤 2)~3)，得到相位分布 $h_3$ 和第 2 个密钥 $P_2$：

$$\begin{cases}h_3=\mathrm{PT}\{F'_2\}\\P_2=\mathrm{AT}\{F'_2\}\end{cases} \tag{14}$$

5) 对于其他剩余的明文 $f_z(x,y),z=3,4,\cdots,K$，根据步骤 4)，通过多次使用 FFT，形成级联分数阶 Fourier 变换的加密方法，最终得到所有明文图像的融合幅度图像 $h_{K+1}$ 与密钥 $P_K$：

$$\begin{cases}h_{K+1}=\mathrm{PT}\{F'_K\}\\P_K=\mathrm{AT}\{F'_K\}\end{cases} \tag{15}$$

### 1.3 基于 QR 码与 Gyrator 变换的图像加密

明文经过级联 Fourier 变换后，虽具备较好的视觉隐秘性，但其抵御攻击能力较弱，尤其是在裁剪和噪声攻击下，其复原图像存在较大的失真。本文利用 QR 码的容错和纠错特性来解决此问题。借助 QR 码生成器得到相位分布 $h_5$ 的 QR 码；然后，让激光束直接照射在 QR 码上，经过 Gyrator 变换[18]获取最终密文，对应的光电结构见图 3。图 3 中，MPM 代表调制掩码 $C$；$\mathrm{SLM}_1$,$\mathrm{SLM}_2$ 为调制解调器；$L_1$,$L_2$,$L_3$ 为广义透镜。

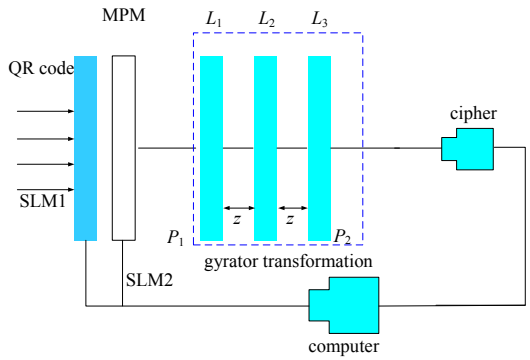


Fig.3 Photoelectric hybrid structure
图 3 光电混合结构

Gyrator 变换含有变换参数，可被视为加密钥，有效扩大密钥空间，在光学加密领域中具有重要作用[18]。令 QR 码为 $o(x,y)$，借助 Gyrator 变换对其完成处理：

$$O(u,v)=g^{\alpha}\{o(x,y)\}(u,v)=\frac{1}{|\sin\alpha|}\iint o(x,y)\exp\left(\mathrm{j}2\pi\frac{(uv+xy)\cos\alpha-(xv+yu)}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \tag{16}$$

式中：$\alpha$ 为旋转角度；$g^{\alpha}(\ )$ 为 Gyrator 变换函数；$(x,y),(u,v)$ 分别为初始、输出坐标。

随后，根据式(17)，对 Gyrator 频谱完成复原：

$$g^{-\alpha}\left(o(x,y)\right)=g^{2\pi-\alpha}\left(o(x,y)\right) \tag{17}$$

Gyrator 变换的加密过程中，数据从 $P_1$ 端输入，经过图 3 所示的光电混合装置，得到的频谱将记录 $P_2$ 端：

$$O(u,v)=\frac{1}{\left|2\lambda\sin\alpha_2\right|}\times\iint o(x,y)\exp\left(\mathrm{j}2\pi\frac{(uv+xy)(2\sin2\alpha_1\sin2\alpha_2-1)-\dfrac{(xv+yu)}{2\lambda z\sin2\alpha_2}}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \tag{18}$$

式中：$o(u,v)$为 Gyrator 变换结果；$(u,v)$为频域坐标；$(x,y)$为空间坐标；$a_1,a_2$ 均为 Gyrator 变换的旋转角度；$\lambda$ 为波长。

根据式(16)，采用调制掩码 $C$，对 QR 码实施干涉加密：

$$o(u,v)=g^{\alpha}\left\{o(x,y)\times MPM\right\} \tag{19}$$

解密是加密的逆过程，依据图 1(b)，借助相应的密钥，对式(19)输出的密文实施复原，其过程如下：

1) 令密文为 $o'(u,v)$，通过 Gyrator 逆变换，得到 QR 码 $o(x,y)$：

$$o(x,y)=g^{-\alpha}\left\{o(u,v)\times\mathrm{MPM}\right\} \tag{20}$$

2) 对 $o(x,y)$进行解码，获取相位分布 $h_5$；再借助密钥 $P_4$，利用幅度截断操作提取 FFT 频谱 $F'_4$：

$$F'_4=P_4\otimes\mathrm{AT}\left\{h_5\right\} \tag{21}$$

3) 基于 FFT 逆变换，对 $F'_4$ 完成复原，得到融合图像 $F_4$：

$$F_4=\mathrm{FFT}^{-\alpha,-\beta}\left\{F'_4\exp\left(\mathrm{j}C(x,y)\right)\right\} \tag{22}$$

4) 从融合图像 $F_4$ 中提取虚部、实部，复原明文 $f_4$ 与 $h_4$：

$$\begin{cases}h_4=\mathrm{Re}\left\{F_4\right\}\\ f_4=\mathrm{Im}\left\{F_4\right\}\end{cases} \tag{23}$$

5) 根据相应的密钥 $P_i$，反复执行步骤 2)~步骤 4)，得到对应的明文 $f_1$ 与相位分布 $h_1$：

$$F'_i=P_i\otimes\mathrm{AT}\left\{h_{i+1}\right\} \tag{24}$$

$$F_i=\mathrm{FFT}^{-\alpha,-\beta}\left\{F'_i\exp\left(\mathrm{j}C(x,y)\right)\right\} \tag{25}$$

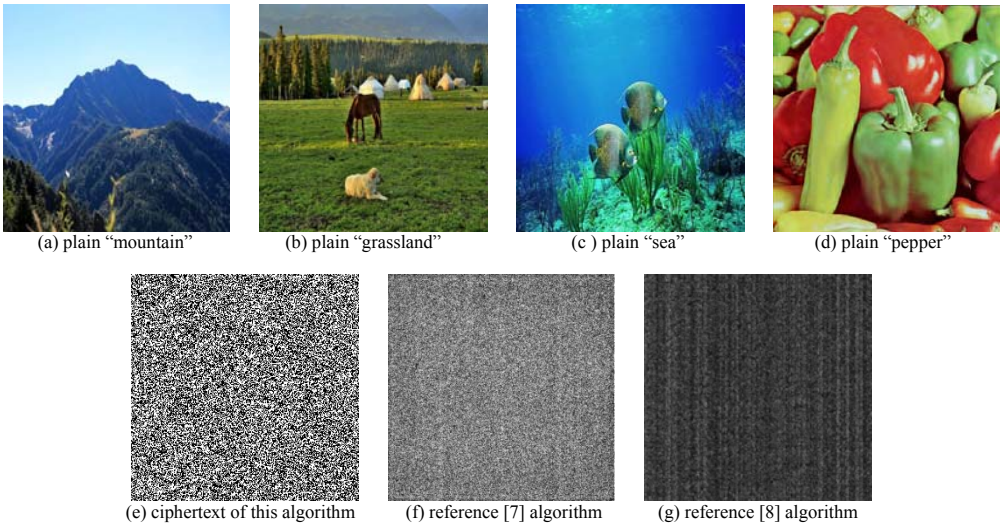
$$\begin{cases}h_i=\mathrm{Re}\left\{F_i\right\}\\ f_i=\mathrm{Im}\left\{F_i\right\}\end{cases} \tag{26}$$

## 2 实验结果与分析

为验证本文多图像光学同步加密技术的安全性与抗攻击能力，采用 Matlab 软件实施信息加密与复原测试。同时，以文献[7–8]中 2 个安全性较高的多图像加密方法为对照组。根据反复测试效果，参数设置如下：$\beta$=0.9, $\alpha$=0.6, $p$=1, $r$=3, $b$=40 mm, $\lambda$=632.8 mm, $\mu$=3。

### 2.1 多图像同步加密测试

以图 4(a)~4(d)为测试样本，采用本文方案与文献[7–8]的多目标同步加密技术，对其实施光学干涉，形成的密文如图 4(e)~4(g)所示。由加密效果发现，三者均可完成多目标的同步干涉处理，4 幅明文的信息隐藏程度较为理想，人眼不能从中得到有用的破译线索，呈现出较大的安全度。同时，借助图像熵值[3]评估 3 种加密结果的抗破译能力，得到的数据见表 1。基于测试熵值可知，本文技术得到的密文具备更强的抗破译能力，其熵值达到了 7.997，与理想值“8”相差甚小；文献[7]与文献[8]算法的安全度要弱于本文技术，二者的熵值分别为 7.981, 7.992。相对于文献[7]与文献[8]，本文光学加密技术具备更好的可靠性。原因是所提技术通过复数理论与分数阶 Fourier 变换构建了级联 Fourier 变换机制，并利用 Fresnel 波带、Hilbert 模型与随机相位掩码组成的调制掩码对明文实施干涉处理，增强了每幅明文之间的联系，显著提高了光轴的对准度，且采用了幅度—相位截断机制破坏系统的线性特征，使密文兼顾了理想的随机性与隐秘性，并借助 QR 码、Gyrator 变换，将光束作用于 QR 码，其强大的容错与纠错能力可以增强密文的抗外来攻击能力。



(a) plain “mountain”　(b) plain “grassland”　(c ) plain “sea”　(d) plain “pepper”

(e) ciphertext of this algorithm　(f) reference [7] algorithm　(g) reference [8] algorithm

Fig.4 Test results of multi-image synchronous encryption with different algorithms
图 4 不同算法的多图像同步加密测试结果

## 2.2 密钥敏感性测试

密钥敏感性是体现加密方案的抗破译能力的重要指标。当未授权用户利用错误密钥解密密文时，即使其与正确密钥之间存在很小的差异，攻击者也无法准确复原图像[3]。本文以混沌参数 $\mu$=3 为基准，测试算法的敏感性。采用差异因子 $\Delta=10^{-15}$ 来改变 $\mu$ 值，得到 $\mu+\Delta$,$\mu-\Delta$。采用这 2 组篡改密钥与正确密钥解密图 4(e)，结果如图 5 所示。观察解密效果发现，当密钥发生 $10^{-15}$ 的微小修改，攻击者无法得到清晰完整的初始图像，如图 5(a)~(h)所示，这些图像呈现出噪声干扰，视觉质量不理想，此时的均方误差(Mean Squared Error，MSE)值大于 3 500。只有密钥无任何变动时，才能准确解密密文，如图 5(i)~(l)所示，图像呈现出较高的视觉质量，失真度较小，其 MSE 值趋于 0，见图 6，表明本文光学加密方案具有高度的敏感性。

(a) first decrypted image of $\mu$+Δ　(b) second decrypted image of $\mu$+Δ　(c) third decrypted image of $\mu$+Δ　(d) fourth decrypted image of $\mu$+Δ

(e) first decrypted image of $\mu$-Δ　(f) second decrypted image of $\mu$-Δ　(g) third decrypted image of $\mu$-Δ　(h) fourth decrypted image of $\mu$-Δ

(i) first decrypted image of $\mu$　(j) second decrypted image of $\mu$　(k) third decrypted image of $\mu$　(l) fourth decrypted image of $\mu$

Fig.5 Test results of key sensitivity
图 5 密钥敏感性测试结果

### 2.3 抗裁剪能力测试

在已有的外来攻击中，裁剪攻击对密文的安全性威胁较大，会严重影响图像的解密质量[3]。将图 4(e)~(g)当作测试目标，对其进行相同程度的裁剪操作，如图 7(a)、图 7(g)、图 7(l)所示。采用本文技术与文献[7–8]的解密过程，对这些裁剪密文完成复原，输出的数据见图 7。由解密数据可知，面对这种裁剪干扰，本文同步光学加密机制具备更优异的稳健性，其输出结果只存在轻度破坏，整体的细节与清晰度都保持较好，见图 7(c)~(f)。文献[7]的解密结果不理想，虽然得到明文的大概轮廓，但丧失较多的信息，见图 7(h)~(k)；整体视觉上文献[8]也具备较好的解密效果，但其输出结果也存在细节丢失与较多的噪声干扰等现象，见图 7(m)~(p)。本文算法综合 Fresnel 波带、Hilbert 模型与混沌掩码的优势，利用新的调制掩码改善光电装置中的光轴对准度，增强密文的安全性，利用激光束照射在 QR 码上，通过 QR 码的容错与纠错特性，面对裁剪攻击时，可以较好地恢复图像信息，失真度较小。文献[7–8]采用简单的随机相位掩码来完成明文的光学调制，不能调整加密系统的光轴对齐度，并且直接将光束作用于图像，遇到裁剪攻击时，缺乏纠错能力，不能较好地复原图像信息。

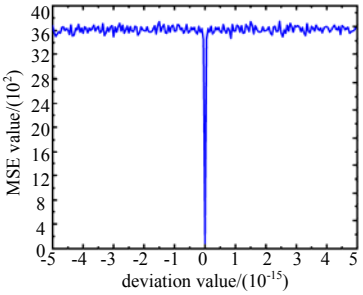



Fig.6 MSE curve of this algorithm
图 6 所提算法的 MSE 曲线测试结果

Fig.7 Test of anti-cutting attack ability of three synchronous encryption technologies
图 7 三种同步加密技术的抗裁剪攻击能力测试

## 3 结论

为能够对多幅图像实施同步加密，并增强密文的安全性与抗裁剪攻击能力，本文提出了基于 QR 码与级联分数阶 Fourier 变换的多图像光学加密算法。该算法构建了一种新的调制掩码，利用 Fresnel 波带、Hilbert 模型的

自身优势来提高整光电装置中的光轴对准度，并兼顾了随机性，有效提高了加密结果的安全性。同时，引入幅度－相位截断方法，通过多次使用分数阶 Fourier 变换，设计了级联 FFT 加密方案，增强所有明文之间的关联度，使密文呈现出较高的非线性特征。基于 Gyrator 变换，利用光束对 QR 码完成干涉，得到加密结果。实验数据表明，本文加密方法具备较高的安全度，对明文内容变化非常敏感，在裁剪操作下，其输出结果的失真度较小，很好地保持了初始图像的细节与纹理，呈现出理想的鲁棒性。

**参考文献：**


[1] 唐洪涛,唐远新. 基于多参数分阶角变换与四元超复数的多图像同步无损加密算法[J]. 西南师范大学学报(自然科学版), 2018,43(7):75–83. (TANG Hongtao,TANG Yuanxin. Multi image synchronous lossless encryption algorithm based on multi parameter step angle transformation and quaternion hypercomplex[J]. Journal of Southwest Normal University(Natural Science Edtion), 2018,43(7):75–83.)

[2] SUN Wenqing,WANG Lei,WANG Jun. Optical hyperspectral data encryption by using gamma distributed phase masks in gyrator domain[J]. Optical Review, 2019,26(3):332–341.

[3] 郭静博. 基于圆柱衍射与离散余弦变换的图像光学加密算法[J]. 包装工程, 2019,40(9):205–215. (GUO Jingbo. Image optical encryption algorithm based on cylinder diffraction and DCT[J]. Packaging Engineering, 2019,40(9):205–215.)

[4] 李建军,梁利利,张福泉. 基于混合相位掩码与 Gyrator 小波变换的光学图像加密算法[J]. 光学技术, 2018,44(6):717–726. (LI Jianjun,LIANG Lili,ZHANG Fuquan. Optical image encryption algorithm based on hybrid phase mask and gyrator wavelet transform[J]. Optical Technology, 2018,44(6):717–726.)

[5] SUN Wenqing,WANG Lei,WANG Jun. Optical image encryption using gamma distribution phase masks in the gyrator domain[J]. Journal of the European Society of Optics-Quick Publications, 2018,14(5):102–113.

[6] LIU Qi,WANG Ying,WANG Jun. Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain[J]. Optical Review, 2018,25(1):46–55.

[7] PAN Shumin,WEN Ruhong,ZHOU Zhihong. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional mellin transform[J]. Multimedia Tools and Applications, 2017,76(2):2933–2953.

[8] CHEN Xudong,LIU Qi,WANG Jun. 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.

[9] 赵亮,王文顺,张维. 基于混合相位掩码与非线性像素互换的光学图像加密算法[J]. 电子测量与仪器学报, 2018,32(11):154–165. (ZHAO Liang,WANG Wenshun,ZHANG Wei. Optical image encryption algorithm based on the exchange of mixed phase mask and nonlinear pixel[J]. Journal of Electronic Measurement and Instrument, 2018,32(11):154–165.)

[10] ABUTURAB Muhammadrafiq. Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain[J]. Optics and Laser Technology, 2013,45(9):525–532.

[11] VASHISTH Sunanda,SINGH Hukum. Image encryption using fractional mellin transform,structured phase filters, and phase retrieval[J]. Optik, 2014,125(18):5309–5315.

[12] LIANG Haoran,TAO Xiangyang,ZHOU Nanrun. Quantum image encryption based on generalized affine transform and logistic map[J]. Quantum Information Processing, 2016,15(7):2701–2724.

[13] REHMAN Aqeelur,LIAO X,KULSOOM A. A modified(dual) fusion technique for image encryption using SHA–256 hash and multiple chaotic maps[J]. Multimedia Tools and Applications, 2016,75(18):1–26.

[14] 潘良,邱建林. 基于分阶 Fourier 频谱分解与混合随机掩码的光学加密算法[J]. 科学技术与工程, 2019,19(14):249–256. (PAN Liang,QIU Jianlin. Optical encryption algorithm based on hierarchical Fourier spectrum decomposition and hybrid random mask[J]. Science Technology and Engineering, 2019,19(14):249–256.)

[15] ZHANG D,LIAO X,YANG B. A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform[J]. Multimedia Tools and Applications, 2018,77(2):2191–2208.

[16] 张智高,张红梅,裴志利. 混沌掩码耦合复数模型的彩图 RGB 同步加密算法[J]. 计算机工程与设计, 2015,36(8):2058–2063. (ZHANG Zhigao,ZHANG Hongmei,PEI Zhili. RGB synchronization encryption algorithm of color image based on chaos mask coupled complex model[J]. Computer Engineering and Design, 2015,36(8):2058–2063.)

[17] ISHA M,SUDHEESH K R,NAVEEN K N. Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude and phase truncation approach[J]. Optics and Lasers in Engineering, 2014,52(9):167–173.

[18] 程宁,王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报, 2019,33(1):191–202. (CHENG Ning,WANG Xijuan. Optical image encryption algorithm based on chaotic gyrator transformation and matrix decomposition[J]. Journal of Electronic Measurement and Instruments, 2019,33(1):191–202.)