基于差异混合掩码与混沌Gyrator变换的光学图像加密算法

陈艳浩*① 刘中艳② 周丽宴③
①(河南师范大学网络中心 新乡 453000)
②(南阳理工学院计算机学院 南阳 473004)
③(郑州大学信息工程学院 郑州 450001)

摘 要：为了提高光学加密技术的抗选择明文攻击能力与未知攻击下的解密质量，该文设计了基于差异混合掩码与混沌Gyrator变换的光学图像加密算法。将输入明文转换成相应的快速响应码；考虑明文特性，根据Logistic映射，生成一个混沌相位掩码；同时，联合径向希尔伯特与波带片相位函数，将其与混沌相位掩码融合，构建了混合相位掩码；随后，利用明文图像迭代Logistic映射所输出的随机序列来计算Gyrator变换的旋转角度，结合混合相位掩码，对快速响应码进行调制，形成Gyrator频谱；引入等量分解技术，将Gyrator频谱分割为两个分量，并设置不同的阶数，形成两个差异螺旋相位掩码；利用奇异值分解(SVD)方法，将其中一个Gyrator频谱分量进行处理，并联合两个差异螺旋相位掩码，分别对其相应的正交矩阵进行编码；最后，通过组合编码后的正交矩阵与对角矩阵，基于可逆SVD技术，输出加密密文。理论分析了所提算法抵抗明文攻击和裁剪攻击的能力，以及加密结果针对密钥变化的敏感性水平。实验结果验证了所提算法拥有良好的安全性能。

关键词：光学图像加密；差异混合掩码；螺旋相位掩码；Gyrator变换；奇异值分解
中图分类号：TP391 **文献标识码**：A **文章编号**：1009-5896(2019)04-0888-08
DOI: 10.11999/JEIT180456

Optical Image Encryption Algorithm Based on Differential Mixed Mask and Chaotic Gyrator Transform

CHEN Yanhao① LIU Zhongyan② ZHOU Liyan③
①(*Network Center*, *Henan Normal University*, *Xinxiang* 453000, *China*)
②(*School of Computer*, *Nanyang Institute of Technology*, *Nanyang* 473004, *China*)
③(*School of Information Engineering*, *Zhengzhou University*, *Zhengzhou* 450001, *China*)

Abstract: In order to improve the ability of anti-chosen plaintext attack and decryption quality under unknown attack in current optical encryption technology, an optical image encryption algorithm based on chaotic Gyrator transform and differential mixed mask is proposed. The input plaintext is converted into its corresponding Quick Response (QR) code. The chaotic phase mask is generated according to the Logistic map. At the same time, the radial Hilbert and the zone plate phase function are combined to fuse with the chaotic phase mask for constructing the mixed phase mask. Then, a random sequence of Logistic chaotic maps is used to calculate the rotation angle of the Gyrator transformation, and the QR code is modulated to form Gyrator spectrum by combining the mixed phase mask. The Gyrator spectrum is divided into two components by introducing the equivalent decomposition technique, and two differential spiral phase masks are obtained by setting up different orders. Then, the Singular Value Decomposition (SVD) is introduced to process one of the Gyrator spectral components so that its corresponding orthogonal matrix is encoded by combining two differential phase masks. Finally, by combining the encoded orthogonal matrix and diagonal matrix, the

收稿日期：2018-05-14；改回日期：2018-08-25；网络出版：2018-12-05
*通信作者： 陈艳浩 Chenyhao5005htc@163.com
基金项目：国家自然科学基金(U1204606)，教育部科技发展中心专项研究资助课题(2017B06113)，河南省高等学校重点科研资助项目(16A520083)，河南省信息技术研究基金(ITE12071)
Foundation Items: The National Natural Science Foundation of China (U1204606), The Special Research Funding Project of Science and Technology Development Center of Ministry Education (2017B06113), The Key Research Funding Projects of Universities in Henan (16A520083), The Information Technology Research Foundation Project of Henan Province (ITE12071)

encrypted cipher is outputted based on thereversible SVD technology. The ability of resisting plaintext attack and clipping attack, as well as the sensitivity level of the encryption results to key change is analyzed theoretically. Experimental results show that the algorithm has good security performance.

Key words: Optical image encryption; Differential hybrid mask; Spiral phase mask; Gyrator transform; Singular Value Decomposition (SVD)

1　引言

当前图像加密方法主要有混沌加密技术[1–3]与光学加密技术[4,5]。如吕群等人[1]利用图像的灰度值和安全散列算法生成加密密钥，通过2维映射变换与动态S盒来完成图像的加密。Parvaz等人[2]通过构建1维复合混沌系统，改善其混沌窗口，并借助循环移位方法及混沌序列，对明文完成加密。Jamal[3]充分利用分形几何与Logistic混沌映射对明文进行扩散加密处理。但混沌系统需要反复迭代，无法避免其周期性，使其混沌特性降低，且并行性不理想。

近年来，诸多学者提出了相应的光学图像加密技术[4]。如张博等人[5]利用混沌相位掩码来实现对明文的调制。并利用等模分解将Fourier频谱分别分割为两个子图像。最后，借助2个不同分数阶的Fourier机制分别对2个子图像进行变换，通过相位-幅度截断编码技术，输出2个密文。但是此方案仅利用混沌相位掩码来调制图像信息，难以解决光轴对准问题，且在外来攻击下的解密质量不理想。Liu等人[6]采用压缩感知机制对图像数据进行降维处理，同时，结合DPRE技术与Arnold变换，通过相应的光电混合装置，输出密文。但其光学加密过程忽略了明文，使其对初始明文的敏感性较低。Verma等人[7]利用Fourier变换获取明文的Fourier频谱，通过相位截断机制，输出其对应的幅度与相位信息。再利用主成分分析技术产生的隐式振幅随机掩码来调制幅度，以获取密文。其利用PCA方法产生的相位掩码的重构难度较大。

为了提高加密技术的安全性，本文利用QR码，提出了新的光学图像加密算法。利用明文像素与Logistic函数来获取混沌掩码。再构建一个螺旋相位掩码，将其与混沌相位掩码融合，输出混合相位掩码。并利用明文像素来计算Gyrator变换的旋转角度，借助混合相位掩码来调制明文对应的QR码。利用等量分解技术，将Gyrator频谱分割为两个分量。并基于两个差异螺旋相位掩码与奇异值分解，对其中一个Gyrator频谱分量对应的正交矩阵进行调制编码。联合对角矩阵，基于可逆SVD技术，完成图像加密。并测试该加密技术的安全性与鲁棒性。

2　Gyrator变换

令旋转角度为α，则明文图像$o(x,y)$对应的Gyrator变换为[8,9]

$$\begin{aligned} O(u,v) &= g^{\alpha}\left[o(x,y)\right](u,v) \\ &= \frac{1}{|\sin\alpha|}\iint o(x,y) \\ &\quad\cdot\exp\left(\mathrm{i}2\pi\frac{(uv+xy)\cos\alpha-(xv+yu)}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \end{aligned} \tag{1}$$

其中，α为旋转角度；$g^{\alpha}(\cdot)$是Gyrator变换；(x,y)是输入空间位置坐标；(u,v)为Gyrator变换域的频率坐标；$o(x,y)$是复杂场函数。

而$g^{\alpha}(\cdot)$的逆变换$|o_0|$为

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

初始明文从Gyrator变换的光学系统输入端进入，相应的Gyrator变换频谱在输出端显示

$$O(u,v)=\frac{1}{|2\lambda\sin\alpha_2|}\iint o(x,y)\exp\left(\mathrm{j}2\pi\frac{(uv+xy)(2\sin2\alpha_1\sin2\alpha_2-1)-\dfrac{(xv+yu)}{2\lambda z\sin2\alpha_2}}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \tag{3}$$

$$\alpha_1=-\alpha;\ \alpha_2=\alpha-\pi/2 \tag{4}$$

其中，λ是光波波长；α_1,α_2均为旋转角度。

3　新型光学图像加密算法的设计

3.1　混合相位掩码的生成

为了解决光轴校准问题[10]，本文根据文献[10]，设计螺旋相位掩码。首先，利用Logistic映射[2]的输出序列来获取随机掩码。Logistic映射为[11]

$$x_{n+1}=\mu x_n(1-x_n) \tag{5}$$

其中，μ为混沌参数；x_n,x_0分别是输出值、初始值。

为了提高算法对明文的敏感性，引入SHA-256函数[12]来获取密钥K，并将其分解为子密钥k_i

$$K=k_1k_2\cdots k_{32} \tag{6}$$

根据式(6)可知，这些子密钥k_i与明文密切相关，为了加强整个加密过程与明文的联系，本文利

用式(6)中的k_i来计算Logistic映射的初始值

$$x_0 = \mathrm{mod}\left(\left((k_2 \oplus k_4 \oplus k_6 \oplus \cdots K_{32}) + \sum_{i=1}^{32}(k_i)\right) \Big/ 2^8, 4\right) \tag{7}$$

根据式(7)得到的初始值x_0，设置参数μ，对式(5)进行迭代$M \times N$次，得到随机序列X=$\{x_1,x_2,\cdots, x_{M\times N}\}$。并将$X$=$\{x_1,x_2,\cdots, x_{M\times N}\}$组合成2D矩阵$\boldsymbol{Y}$=$\{b_{i,j}|i$=1,2,$\cdots$,$M$; j=1,2,$\cdots$,N $\}$。则其混沌相位掩码CPM为

$$S(x,y) = \exp\left[\mathrm{j}2\pi y_{i,j}(x,y)\right] \tag{8}$$

依据文献[13]可知，径向希尔伯特函数为

$$H(r,\varphi) = \exp\left[\mathrm{j}p\varphi\right] \tag{9}$$

其中，p为阶数；(r,φ)是Cartesian空间内的极坐标

$$\left.\begin{aligned} r &= x^2 + y^2 \\ \varphi &= \tan^{-1}(y/x) \end{aligned}\right\} \tag{10}$$

由文献[14]可知，波带片相位函数为

$$B(r,\varphi) = \exp\left[-\frac{\mathrm{j}\pi}{\lambda b} r^2\right] \tag{11}$$

其中，λ为光波波长；b是波带片透镜的焦距。

再将$H(r,\varphi)$与$B(r,\varphi)$相乘，构建螺旋相位掩码

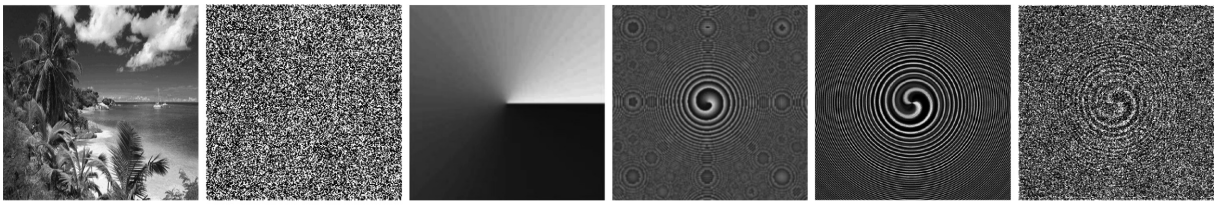
$$R(r,\varphi) = \exp\left[\mathrm{j}\left(p\varphi - \frac{\pi}{\lambda b} r^2\right)\right] \tag{12}$$

根据$R(r,\varphi)$，联合式(8)中的混沌相位掩码$S(x,y)$，形成了一个混合相位掩码

$$C(x,y) = \exp\left[\mathrm{j}\left[\left\{\arg\left(R(r,\varphi)\right)\right\} \times \left\{\arg\left(S(x,y)\right)\right\}\right]\right] \tag{13}$$

其中，arg代表相位提取；$C(x,y)$是混合相位掩码。

为了反映$C(x,y)$的优势，以图1(a)为目标，并取p_1=1, r=3,b=40 mm, λ=632.8 mm，以及μ=3，基于式(5)—式(13)，所形成的5个掩码分别见图1(b)—图1(f)。由结果可知，混合掩码更加复杂，其随机性更高。



(a)明文图像 (b)混沌相位掩码 (c)径向希尔伯特相位掩码 (d)波带片相位掩码 (e)螺旋相位掩码 (f)混合相位掩码

图 1 混合相位掩码的生成

3.2 基于混沌Gyrator变换的QR码调制

为了提高密文在未知攻击下的解密质量，本文利用草料2维码生成器，将明文转换成为QR码。再根据式(6)中的k_i重新计算Logistic映射的初始值

$$x_0 = \mathrm{mod}\left(\left((k_1 \oplus k_3 \oplus k_5 \oplus \cdots K_{31}) + \sum_{i=1}^{32}(k_i)\right) \Big/ 2^8, 4\right) \tag{14}$$

再设置参数μ，迭代式(5)$M \times N$次，输出新的序列$X' = \{x'_1, x'_2, \cdots, x'_{M\times N}\}$。为了提高Gyrator变换的调制效果，增强随机性，本文依据序列$X' = \{x'_1, x'_2, \cdots, x'_{M\times N}\}$中的元素，计算Gyrator变换的旋转角度

$$\alpha = \sum_{i=1}^{M\times N} \frac{x_i}{2\pi M \times N} \tag{15}$$

其中，α为Gyrator变换的旋转角度。

根据式(15)的α，对QR码进行调制

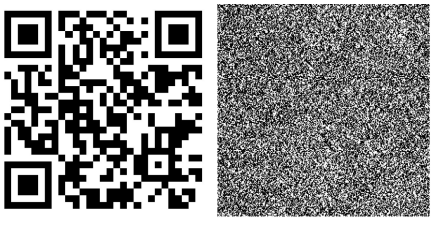
$$f(u,v) = G^{\alpha}\left\{f(x,y) \times \mathrm{MPM}\right\} \tag{16}$$

其中，G^{α}是角度为α的Gyrator变换；$f(x,y)$为明文图像对应的QR码；MPM是混合相位掩码。

图1(a)对应的QR码见图2(a)。通过上述调制过程得到的Gyrator频谱见图2(b)。由结果可知，明文被Gyrator变换调制后，所有的信息均被充分隐藏。

3.3 基于等量分解与SVD方法的图像加密

因Gyrator频谱是一个复函数。故本文将Gyrator频谱分解为子成分。首先，基于式(16)的Gyrator



(a)明文图像的QR码 (b)Gyrator频谱

图 2 混沌Gyrator变换的调制结果

频谱，用$A(u,v)=|f(u,v)|$, $P(u,v)=\arg|f(u,v)|$分别描述$f(u,v)$的幅度与相位部分。并依据文献[5]，将Gyrator频谱$f(u,v)$分解为

$$Z_1(u,v)=\frac{A(u,v)/2}{\cos[P(u,v)-\theta(u,v)]}\exp[\mathrm{j}\theta(u,v)] \tag{17}$$

$$Z_2(u,v)=\frac{A(u,v)/2}{\cos[P(u,v)-\theta(u,v)]}\cdot\exp[\mathrm{j}(2P(u,v)-\theta(u,v))] \tag{18}$$

$$\theta(u,v)=\arg[Z_1(u,v)] \tag{19}$$

再保留式(18)中的$Z_2(u,v)$分量不变，利用奇异值分解[15,16]来处理$Z_1(u,v)$分量

$$\mathrm{SVD}[Z_1(u,v)]=\boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}} \tag{20}$$

其中，$\boldsymbol{U}$, $\boldsymbol{V}$为正交矩阵；$\boldsymbol{S}$为对角矩阵。

再根据式(12)，通过设置不同的阶数p，得到两个不同的螺旋相位掩码$R_1(r,\varphi)$, $R_2(r,\varphi)$，以调制$\boldsymbol{U}$, $\boldsymbol{V}$

$$\left.\begin{aligned}\boldsymbol{U}'&=\boldsymbol{U}R_1(r,\varphi)\\ \boldsymbol{V}'&=\boldsymbol{V}R_2(r,\varphi)\end{aligned}\right\} \tag{21}$$

根据编码后的正交矩阵$\boldsymbol{U}'$, $\boldsymbol{V}'$，联合原来的对角矩阵$\boldsymbol{S}$，基于可逆SVD方法，获取最终的加密密文

$$E(u,v)=\boldsymbol{U}'\boldsymbol{S}\boldsymbol{V}'^{\mathrm{T}} \tag{22}$$

其中，(u,v)为Gyrator变换域的频率坐标。

以图2(b)为例，将其分解为两个子成分$Z_1(u,v)$与$Z_2(u,v)$，见图3(a)与图3(b)。取p=0, p=1，形成的螺旋相位掩码分别见图3(c)，图3(d)。再利用二者分别对$Z_1(u,v)$的两个正交矩阵完成调制，输出密文见图3(e)。依图可知，最终的加密密文高度隐藏了明文信息，其相应的像素分布更加均匀，见图3(f)。

3.4 密文的解密过程

(1)由奇异值分解方法，对加密密文$E(u',v')$完成分解，输出正交矩阵$\boldsymbol{U}_1$, $\boldsymbol{V}_1$和对角矩阵$\boldsymbol{S}_1$，得到

$$\mathrm{SVD}[E(u,v)]=\boldsymbol{U}_1\boldsymbol{S}_1\boldsymbol{V}_1^{\mathrm{T}} \tag{23}$$

(2)根据$R_1(r,\varphi)$, $R_2(r,\varphi)$的共轭复数$R_1^*(r,\varphi)$, $R_2^*(r,\varphi)$，对正交矩阵$\boldsymbol{U}_1$, $\boldsymbol{V}_1$进行调制

$$\left.\begin{aligned}\boldsymbol{U}_1'&=\boldsymbol{U}_1R_1^*(r,\varphi)\\ \boldsymbol{V}_1'&=\boldsymbol{V}_1R_2^*(r,\varphi)\end{aligned}\right\} \tag{24}$$

(3)再借助可逆SVD方法处理正交矩阵$\boldsymbol{U}_1'$, $\boldsymbol{V}_1'$以及对角矩阵$\boldsymbol{S}_1$，得到

$$Z_1'(u,v)=\boldsymbol{U}_1'\boldsymbol{S}_1\boldsymbol{V}_1'^{\mathrm{T}} \tag{25}$$

(4)将$Z_2(u,v)$与$Z_1'(u,v)$进行合成，得到Gyrator频谱

$$f'(u,v)=Z_2(u,v)+Z_1'(u,v) \tag{26}$$

(5)随后，利用角度为–α的Gyrator逆变换，根据混合相位掩码的共轭复数MPM*，获取QR码

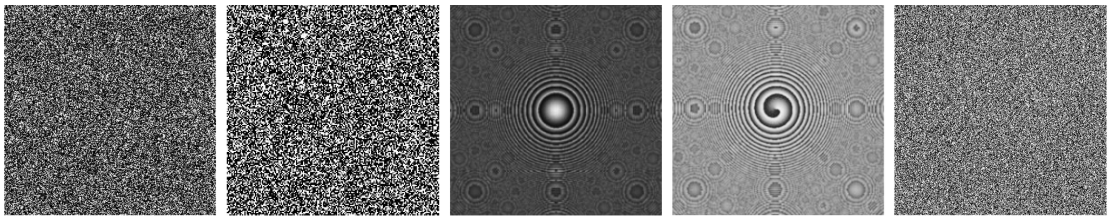
$$f(x,y)=G^{-\alpha}\{f(u,v)\times\mathrm{MPM}^*\} \tag{27}$$

(6)最后，利用成熟的QR码扫描器处理$f(x,y)$，输出解密图像。

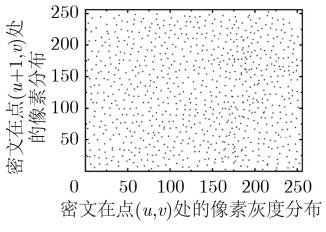
以图3(e)为例，利用上述解密过程，得到相应的QR码见图3(g)；再通过QR码扫描器，即可输出解密图像，见图3(h)。

4 实验结果与分析

利用Matlab6.5软件来测试本文方法的安全性。并将文献[7]与文献[9]视为对照组。其中，文献[9]的加密技术也采用了Gyrator变换机制。该技术通过离轴圆谐分量展开技术与不同的加密机制，有效解决了轮廓显示问题，具有良好的代表性与新颖性。



(a)子成分$Z_1(u,v)$　(b)子成分$Z_2(u,v)$　(c)p=0的螺旋相位掩码　(d)p=1的螺旋相位掩码　(e)最终加密密文



(f)密文相邻像素相关性

(g)解密的QR码

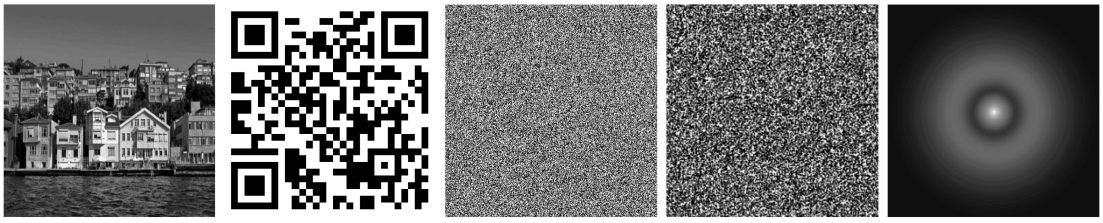
(h)解密结果

图 3 图像加密测试结果

试验参数为：p_1=1, r=3, b=40 mm, λ=632.8 mm，混沌参数μ=3，以及阶数p_2=0, p_3=3。

4.1 光学图像加密效果

将大小为256 × 256的灰度图像作为对象，见图4(a)，其对应的QR码见图4(b)。再利用本文算法、文献[7]、文献[9]技术对其加密，输出密文见图4(c)—图4(e)。由输出密文可知，明文图像经过这三者加密后，图像的视觉信息均被高度隐藏，无任何的轮廓显示问题与信息外泄，见图4(c)—图4(e)。为了客观评估这三者的加密安全性，本文利用信息熵值[17]来量化，结果见表1。由表1可知，本文光学加密技术的输出密文对应的信息熵值最大，为7.9994。而文献[7]算法的密文熵值为7.9991，与本文算法较为接近。文献[9]的密文熵值最小，为7.9985。原因是本文算法利用了与明文相关的混沌相位掩码，和螺旋相位掩码融合，形成了混合掩码，并基于Gyrator变换实现QR码的调制，有效增强其随机性与动态性。且本文技术利用了等量分解技术将Gyrator频谱分割为两个分量，基于奇异值分解方法，对其中一个Gyrator频谱分量进行处理，通过两个不同的螺旋相位掩码，分别对其相应的正交矩阵进行编码，有效破坏加密系统的线性关系，以及提高本文算法的敏感性。而文献[7]采用的相位截断机制虽然也能够破坏加密系统的线性特征，但是其采用的2个普通相位掩码的随机性不理想。另外，文献[7]技术没有考虑明文特性，使其对明文的敏感性较低，从而导致其加密安全性要低于本文技术。文献[9]算法采用的Gyrator变换的旋转角度是一个固定值，缺乏动态性。且文献[9]算法是采用纯相位掩码来调制明文，难以解决光轴校准问题，使其密文安全性有待进一步提升。



(a)初始明文 (b)明文的QR码 (c)本文算法的密文 (d)文献[7]算法的密文 (e)文献[9]算法的密文

图 4 不同算法的光学加密效果

表 1 信息熵值测试结果

名称	本文算法	文献[7]	文献[9]
密文熵值	7.9994	7.9991	7.9985

4.2 抗明文攻击能力测试

本文引入NPCR, UACI曲线来评估本文算法、文献[7]、文献[9]的抗选择明文攻击能力。其中，NPCR, UACI的函数分别为[2]

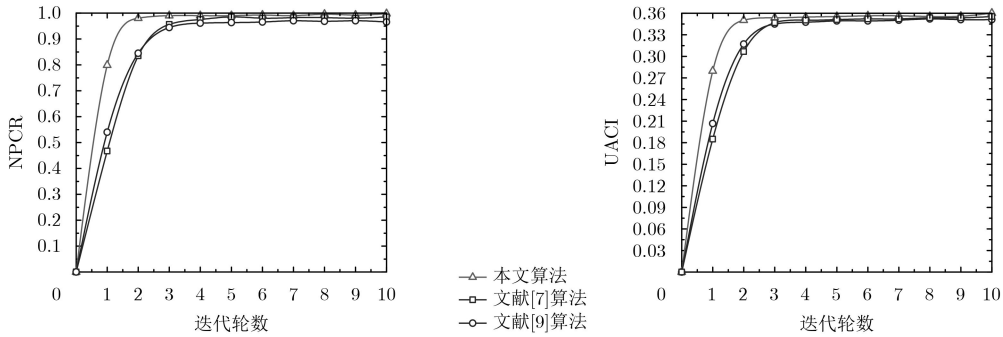
$$\left.\begin{aligned}\mathrm{NPCR}=&\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\mathrm{Difp}\left(I\left(i,j\right),I'(i,j)\right)}{W\times H}\times 100\%\\ \mathrm{Difp}\left(I\left(i,j\right),I'(i,j)\right)=&\begin{cases}0, I\left(i,j\right)=I'(i,j)\\ 1, I\left(i,j\right)\neq I'(i,j)\end{cases}\end{aligned}\right\} \tag{28}$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{\left|I(i,j)-I'\left(i,j\right)\right|}{255}\right]\times 100\% \tag{29}$$

其中，$W\times H$为图像尺寸；I, I'分别是两个明文经加密后的密文，且二者都只存在一个相异灰度值[2]。

将图4(a)视为目标，把坐标 (192, 78)的像素灰度值143修改成113，可得一个新的图像。再基于本文算法、文献[7]、文献[9]技术，对修改像素值前后的图像进行光学处理，得到2个密文。并依据式(28)，式(29)，可获取各自的NPCR, UACI曲线，如图5所示。由输出曲线可知，本文算法的抗明文攻击能力最强，均要强于文献[7]、文献[9]技术。对于本文技术，其稳定的NPCR, UACI值分别高达99.58%和33.56%。原因是本文算法利用明文图像来生成混沌相位掩码，将其与螺旋相位掩码融合，使其形成的混合掩码与明文紧密相连。另外，本文算法还利用明文特性迭代混沌映射的输出序列来计算Gyrator变换的旋转角度，提高了算法对明文的敏感度。如果攻击者借助选择明文攻击方法和大量测试不同的明文来解密密文，因其解密密钥与正确密钥存在巨大差异，使其无法准确复原明文。文献[7]、文献[9]的光学加密技术均忽略了明文信息，使其对明文的敏感性较低，导致二者的抗选择明文攻击能力不理想。

如果利用文献[18]的选择明文攻击方法来复原本文算法的密文，但其无法得到私钥$Z_2\left(u,v\right)$。同时，本文算法采用了矢量分解技术与SVD机制，高



(a) NPCR值测试　　(b) UACI值测试

图 5 3种算法的抵御选择明文攻击能力测试

度破坏了加密系统的线性特征。且该算法的加密过程均和明文有关，攻击者依赖选择明文攻击对其他明文图像进行多次测试所产生的密钥均是错误的。文献[19]的攻击方法是通过对比选择明文与密文在水平与垂直方向上的行与列矢量中的“1”元素数量来破译密文。但是，本文算法并非是置乱加密技术，而是通过光电混合装置改变明文的像素值，通过文献[19]的方法只能得到相应的位置矩阵。因此，利用此攻击方法是无法获取该密钥的。

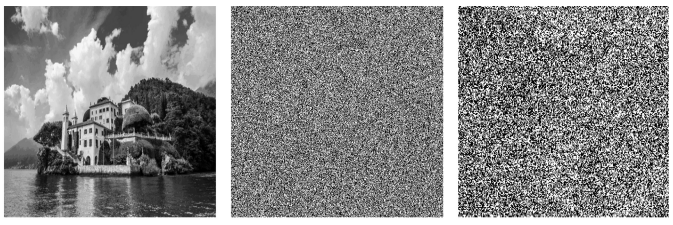
已知明文攻击也是加密算法的常用安全分析模型[20]。故利用文献[21]对本文加密技术的密文进行已知明文攻击实验。首先，以图6(a)为明文，根据本文加密方法，得到的密文见图6(b)。再依据文献[21]的攻击方法对图6(b)实施破译，得到相应的解密密钥$Z_2'(u,v)$；随后，根据$Z_2'(u,v)$，对图4(c)完成解密，结果见图6(c)。根据结果可知，本文加密技术具有较好的抗已知明文攻击能力，其不能正确解密图4(c)，破译结果没有显示明文的任何轮廓信息。

4.3 敏感性测试分析

密钥敏感性是客观量化加密方案安全性的常用指标[9]。故本文测试了$\mu=3$的敏感性。利用一个偏差值$\delta=10^{-15}$来改变μ，生成2个错误密钥：$\mu-\delta$，$\mu+\delta$。其他密钥均不变。并基于这3组密钥对图4(c)完成复原，并输出相应的MSE (Mean Square Error)曲线，结果见图7。由结果可知，当密钥出现了10^{-15}的微小偏差，非授权用户无法对密文实施复原，其解密结果是一幅噪声图像，无法清晰显示图像信息，见图7(a)与图7(b)。此时，其对应的MSE值都大于3500。只有当密钥均正确时，才能成功破译密文，见图7(c)，其对MSE值接近0，见图7(d)。

4.4 抗剪切能力测试分析

将图4(c)—图4(e)作为测试对象，并同时将相同程度的剪切攻击施加于它们，见图8(a)、图8(c)、图8(e)。通过对其解密，输出结果见图8(b)、图8(d)、图8(f)。根据复原结果可知，面对网络中



(a)明文图像　(b)加密结果　(c)攻击结果

图 6 本文算法的抗已知明文攻击能力测试

(a)错误密钥$\mu-\delta$的解密结果　(b)错误密钥$\mu+\delta$的解密结果　(c)正确密钥的解密图像　(d)MSE曲线

图 7 本文算法的密钥敏感性测试

(a)本文算法的剪切攻击密文 (b)解密图像 (c)文献[7]算法的剪切攻击密文 (d)解密图像 (e)文献[9]算法的剪切攻击密文 (f)解密图像

图 8 3种算法的抗剪切攻击能力测试

的剪切攻击，本文光学加密技术表现出更高的鲁棒性，其解密图像更加清晰完整，见图8(b)。而文献[7]和文献[9]的抗剪切攻击能力较弱，虽然也能对密文完成解密，但是输出结果不清晰，与初始明文相差较大，如图8(d)、图8(f)所示。原因是本文技术是利用光束通过相应的光电装置来加密明文QR码，充分利用了QR码的容错与纠错能力，有效提高其在外来攻击下的解密质量，从而表现出更好的抗剪切攻击能力。

5 结束语

本文利用QR码，设计了基于差异混合掩码与混沌Gyrator变换的光学加密算法。该算法利用一个与明文相关的混沌掩码与螺旋相位掩码来构建混合相位掩码，以增强算法对明文的敏感性，并解决光电装置的光轴校准问题。利用等量分解技术与SVD方法来处理Gyrator频谱分量，可充分破坏加密系统的线性特征。在加密过程中，调制掩码与Gyrator变换均依赖明文，使得密文具有较强的抗已知明文攻击和抗选择明文攻击能力。另外，该算法使用了QR码，可提高算法在外来攻击下的解密质量，尤其是剪切攻击。实验结果显示了所提光学加密技术对密钥具有强烈的敏感性，以及对明文攻击具有较高的鲁棒性，为图像信息安全保护提供了一种新的方法。

未来将考虑彩色图像RGB 3通道的关系，选择合适的颜色空间，对本文算法进行完善，使其可用于彩色图像加密，进一步提高本文算法的适应性。

参 考 文 献

[1] 吕群, 薛伟. 结合混沌系统和动态S-盒的图像加密算法[J]. 小型微型计算机系统, 2018, 39(3): 607–613. doi: 10.3969/j.issn.1000-1220.2018.03.038.
LÜ Qun and XUE Wei. Image encryption algorithm combining chaotic system and dynamic S-boxes[J]. *Journal of Chinese Computer Systems*, 2018, 39(3): 607–613. doi: 10.3969/j.issn.1000-1220.2018.03.038.

[2] PARVAZ R and ZAREBNIA M. A combination chaotic system and application in color image encryption[J]. *Optics and Laser Technology*, 2018, 101(1): 30–41. doi: 10.1016/j.optlastec.2017.10.024.

[3] JAMAL M. Image encryption based on fractal geometry and chaotic map[J]. *Diyala Journal for Pure Science*, 2018, 14(1): 166–182. doi: 10.24237/djps.1401.367A.

[4] SUI L S, XU M J, and TIAN A L. Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain[J]. *Optics and Lasers in Engineering*, 2017, 91: 106–114. doi: 10.1016/j.optlaseng.2016.11.017.

[5] 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. doi: 10.11999/JEIT170489.
ZHANG Bo, LONG Hui, and JIANG Feibo. Optical image encryption algorithm based on coherent superposition and modulus equal vector decomposition[J]. *Journal of Electronics & Information*, 2018, 40(2): 438–446. doi: 10.11999/JEIT170489.

[6] LIU Xiaoyong, CAO Yiping, LU Pei, *et al*. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. *Optik*, 2013, 124(24): 6590–6593. doi: 10.1016/j.ijleo.2013.05.092.

[7] VERMA G and SINHA A. Optical image encryption system using nonlinear approach based on biometric authentication[J]. *Journal of Modern Optics*, 2017, 64(13): 1321–1329. doi: 10.1080/09500340.2017.1287435.

[8] 李彤. 基于混沌与Gyrator变换的彩色图像加密算法研究[D]. [硕士论文], 西安邮电大学, 2017: 12–15.
LI Tong. Research on color image encryption algorithm based on chaos and Gyrator transform[D]. [Master dissertation], Xi'an University of Post and Telecommunications, 2017: 12–15.

[9] 肖宁, 李爱军. 基于圆谐分量展开与Gyrator变换域相位检索的光学图像加密算法[J]. 电子测量与仪器学报, 2017, 31(6): 876–884. doi: 10.13382/j.jemi.2017.06.009.
XIAO Ning and LI Aijun. Optical image encryption algorithm based on circular harmonic component expansion and phase retrieval in Gyrator transform domain[J]. *Journal of Electronic Measurement and Instrument*, 2017, 31(6): 876–884. doi: 10.13382/j.jemi.2017.06.009.

[10] SUI Liansheng, ZHOU Bei, NING Xiaojuan, *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. doi: 10.1364/OE.24.000499.

[11] 黄立宏. 高等数学[M]. 第4版, 上海: 复旦大学出版社, 2014: 196–223.
HUANG Lihong. Higher Mathematics[M]. Fourth Edition, Shanghai: Fudan University Press, 2014: 196–223.

[12] 王宏达. 一种基于混沌系统的新型图像加密算法[J]. 光学技术, 2017, 43(3): 260–266. doi: 10.13741/j.cnki.11-1879/o4.2017.03.015.
WANG Hongda. A new image encryption algorithm based on chaotic system[J]. *Optical Technology*, 2017, 43(3): 260–266. doi: 10.13741/j.cnki.11-1879/o4.2017.03.015.

[13] VASHISTH S, SINGH H, YADAV A K, *et al*. Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval[J]. *Optik*, 2014, 125(18): 5309–5315. doi: 10.1016/j.ijleo.2014.06.068.

[14] ABUTURAB M R. Color information security system using Arnold transform and double structured phase encoding in Gyrator transform domain[J]. *Optics & Laser Technology*, 2013, 45: 525–532. doi: 10.1016/j.optlastec.2012.05.037.

[15] SINGH P, YADAV A K, SINGH K, *et al*. Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition[J]. *American Institute of Physics Conference Series*, 2017, 1802(1): 020017. doi: 10.1063/1.4973267.

[16] SINGH P, YADAV A K, and SINGH K. Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition[J]. *Optics and Lasers in Engineering*, 2017, 91: 187–195. doi: 10.1016/j.optlaseng.2016.11.022.

[17] 孙力, 黄正谦, 梁立. 基于复合混沌映射与连续扩散的图像加密算法[J]. 计算机工程与设计, 2017, 36(12): 3374–3379. doi: 10.16208/j.issn1000-7024.2017.12.03.
SUN Li, HUANG Zhengqian, and LIANG li. Image encryption algorithm based on compound chaotic map and continuous diffusion[J]. *Computer Engineering and Design*, 2017, 36(12): 3374–3379. doi: 10.16208/j.issn1000-7024.2017.12.03.

[18] CARNICER A, MONTES-USATEGUI M, ARCOS S, *et al*. Vulnerability to chosen-cipher attacks of optical encryption schemes based on double random phase keys[J]. *Optical Letters*, 2005, 30(13): 1644–1646. doi: 10.1364/OL.30.001644.

[19] LI Chengqing, LIN Dongdong, and LÜ Jinhu. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits[J]. *IEEE MultiMedia*, 2017, 24(3): 64–71. doi: 10.1109/MMUL.2017.3051512.

[20] LI Chengqing. Cracking a hierarchical chaotic image encryption algorithm based on permutation[J]. *Signal Processing*, 2016, 118: 203–211. doi: 10.1016/j.sigpro.2015.07.008.

[21] PENG Xiang, ZHANG Pan, WEI Hengzheng, *et al*. Known-plaintext attack on optical encryption based on double random phase keys[J]. *Optical Letters*, 2006, 31(8): 1044–1046. doi: 10.1364/OL.31.001044.

陈艳浩：男，1980年生，讲师，研究方向为图像处理、信息安全、大数据分析.

刘中艳：男，1983年生，工程师，研究方向为图像处理、网络信息安全、光学应用.

周丽宴：女，1972年生，副教授，研究方向为图像处理、信息安全、人工智能.