基于混合幅度-相位检索技术与二维耦合混沌映射的光学图像加密算法

赵瑜
（江苏食品药品职业技术学院 基础教学部，淮安 223003）

摘要：目的 为了解决当前光学图像加密算法主要将单色光束直接作用于明文，使其在解密过程中易出现丢失颜色信息等问题。**方法** 文中设计基于混合幅度-相位检索技术与二维耦合混沌映射的光学图像加密算法。首先，提取彩色图像的 *R*, *G*, *B* 分量；随后，引入 Logistic 映射与 Sine 映射，通过对二者进行非线性耦合，形成二维复合混沌映射；利用彩色图像的像素信息来迭代复合映射，获取 3 个混沌序列，通过构建位置引擎混淆机制，对 *R*, *G*, *B* 分量进行置乱；基于 Logistic 映射，利用明文像素生成的初值条件对其进行迭代，输出一个混沌随机掩码；最后，基于幅度-相位截断方法和 Gyrator 变换，设计混合幅度-相位检索技术，利用单向二进制相位函数和随机掩码，对置乱后的 *R*, *G*, *B* 分量进行加密，获取相应的检测振幅，再将其进行组合，形成实值函数的加密密文。**结果** 实验结果显示，与当前光学图像加密机制相比，所提算法具有更高的安全性与解密质量，具备较强的抗明文攻击能力。**结论** 所提加密技术具有较高的抗攻击能力，能够安全保护图像在网络中传输，在信息防伪等领域具有较好的应用价值。

关键词： 光学图像加密；混合幅度-相位检索；耦合混沌映射；位置引擎混淆机制；随机掩码；单向二进制相位；实值函数
中图分类号： TP309 **文献标识码：** A **文章编号：** 1001-3563(2018)19-0233-11
DOI： 10.19554/j.cnki.1001-3563.2018.19.039

Optical Image Encryption Algorithm Based on Hybrid Amplitude-Phase Retrieval Technique and Two-dimensional Coupled Chaotic Map

ZHAO Yu
(Department of Basic Education, Jiangsu Food & Pharmaceutical Science College, Huai'an 223003, China)

ABSTRACT: The work aims to solve such defects as easy occurrence of color information loss in the decryption process induced by the current optical image encryption algorithm that mainly directly applies the monochromatic beam to the plaintext. An optical image encryption algorithm based on hybrid amplitude-phase retrieval technique and two-dimensional coupled chaotic map was designed herein. Firstly, the *R, G* and *B* components of the color image were extracted. Then, the two-dimensional composite map was formed by nonlinearly coupling the Logistic map and Sine map. The three chaotic sequences were obtained by the pixel information of color image that iterated the composite map, so that the *R, G* and *B* components were scrambled by constructing the position engine obfuscation mechanism. Based on Logistic map, the initial value conditions generated by the plaintext pixels were used for the iteration of the Logistic map to output one chaotic random mask. Finally, the hybrid amplitude-phase retrieval technique was designed based on the amplitude-phase truncation method and Gyrator transform. The scrambled *R, G* and *B* components were encrypted by the unidirectional binary phase function and random mask to obtain the corresponding detection amplitude. Then, these components were combined to form the encrypted ciphertext of real-valued function. The experimental results showed that, with higher security and decryption quality, the proposed algorithm had stronger ability to resist plaintext attack compared with the current optical image encryption mechanism. The proposed encryption algorithm has higher anti-attack ability and can

收稿日期： 2017-11-28
基金项目： 江苏省教育信息化研究项目（20172203）
作者简介： 赵瑜（1982—），女，江苏食品药品职业技术学院讲师，主要研究方向为应用数学、图像处理。

protect the safe transmission of images in the network. It has better application value in the field of information security and anti-counterfeiting.

KEY WORDS: optical image encryption; hybrid amplitude-phase retrieval; coupled chaotic map; position engine obfuscation mechanism; random mask; unidirectional binary phase; real-valued function

随着计算机与因特网的普及，网络已经成为当代人们生活中必不可少的载体，在带给用户便利的同时，信息安全问题也日益突出，用户的信息被肆意攻击与窃取，给用户造成巨大的隐患[1]。图像作为多媒体技术中常用的介质之一，其包含了用户的诸多信息，且具有相当好的直观描述特性，使其在各大领域得到了广泛应用，如包装印刷、版权保护和信息防伪等领域[2]。在当前的数字图像中，彩色图像因其具备良好的视觉感知信息，能够提供更加丰富的表达内容，在图像领域中应用较广[3]，因此，如何确保彩色图像在网络中安全传输，使得用户接收到的图像内容不被篡改，已成为当前国内外学者的研究焦点[3]。在当前的彩色图像加密技术中，主要分类两大类：混沌加密与光学加密[4—5]。混沌加密技术[4]主要是利用高维混沌系统的复杂相空间等特性来实现图像的置乱与扩散，具有良好的加密效果，但是，混沌系统存在周期性，且加密安全性与效率不理想。近年来，光学加密技术，因其具有高效、并行处理能力、存储量大以及多维度密钥等特性，被广泛用于图像加密领域。如张国平等[5]为了解决串扰问题，设计了一种基于菲涅耳变换（FrT）域 MGSA 融合波分复用的光学图像加密算法，利用 MGSA 来计算 3 个纯相位函数，联合菲涅耳变换变换，对彩色图像的 *R*, *G*, *B* 分量进行加密，并利用相应的解密方法与光电装置来解密图像，实验结果验证了其算法具有良好的安全性。但是此技术是将单色光束直接作用于彩色图像，使其丢失了部分颜色信息，且菲涅耳变换存在缩放因子问题，使其解密质量不理想。Abuturab MR 等[6]为了提高密文的安全性，设计了基于 Gyrator 变换域的 Schur 分解机制的光学彩色图像加密算法，利用 3 个随机掩码对 *R*, *G*, *B* 分量进行调制，并基于卷积操作与 Gyrator 变换，将 3 个调制成分融合为灰度信息，利用相位幅度截断机制，完成图像加密，实验结果验证了其算法的有效性与优异性。但是，此技术是将相位密钥视为私钥，且密文图像是个复数函数，不方便密文信息的存储、传输与管理。Muhammad 等[7]为了改善密文的安全性，设计了基于 Hartley 变换和 Gyrator 变换的单通道光学彩色加密技术，利用 Hartley 变换分别处理彩色图像的 *R*, *G*, *B* 分量，利用相位-幅度截断机制，输出第一个密文，同时，利用相位随机掩码与密文进行卷积与 gyrator 变换处理，再次利用相位-幅度截断机制处理调制后的图像信息，输出实值函数形式的密文。此技术利用了相位-幅度截断技术，有效破坏了系统的内在线性关系，显著提高了密文的安全性，且将最终密文加密成实值函数，便于密文信息的存储与管理，但是此技术是利用相同的 Hartley 变换来处理 3 个分量，降低了算法的随机性，且将单色光束直接作用于彩色图像，使其丢失了部分颜色信息，导致其解密图像质量不理想。

针对上述问题，文中基于文献[7]思想，为了使得输出的密文是一个实值函数，并提高算法的随机性与解密质量，文中利用混合幅度-相位检索技术与混沌映射，提出一种新的光学图像加密算法。并验证了所提光学加密机制的安全性与解密质量。

1 Gyrator 变换

Gyrator 变换是处理二维信号的新技术，属于线性正则积分变换范畴，该技术的内核是双曲面与平面波的内积[8]。在 Gyrator 变换的光学系统中，透镜与输入、输出平面的距离是固定的，这意味着对于任何的旋转角度，通过校正旋转柱面透镜来进行 Gyrator 变换[8]。若其旋转角度是 α，对于二维图像 $f_i(x_i, y_i)$，其 Gyrator 变换为[8]：

$$O(x_0,y_0)=G^{\alpha}\left[f_i(x_i,y_i)\right](x_0,y_0)=\frac{1}{|\sin\alpha|}\iint f_i(x_i,y_i)\times \exp\left(i2\pi\frac{(x_0y_0+x_iy_i)\cos\alpha-(x_iy_0+x_0y_i)}{\sin\alpha}\right)\mathrm{d}x_i\mathrm{d}y_i \tag{1}$$

式中：$G^{\alpha}[\ ]$代表 Gyrator 变换；(x_i, y_i)，(x_0, y_0)分别为输入、输出位置；$O(x_0, y_0)$代表复杂场函数。

$G^{\alpha}[\ ]$的可逆变换$|O_0|$为：

$$G^{-\alpha}\left(O(x_i,y_i)\right)=G^{2\pi-\alpha}\left(O(x_i,y_i)\right) \tag{2}$$

当旋转角度 α=0，$G^{\alpha}[\ ]$为恒等变换；当 α=π 时，$G^{\alpha}[\ ]$为可逆变换。同时，若 α=π/2 或 α=3π/2 时，$G^{\alpha}[\ ]$成为一个 Fourier 变换与其对应的可逆变换。在文中加密算法中，是通过利用 Gyrator 变换中的透镜的级联结构来完成像素加密。Gyrator 变换的光学系统见图 1。图 1a 是 Gyrator 变换的光学结构，主要是由 3 个透镜组成，相邻 2 个透镜间的距离是相等的，大小为 z。另外，透镜 L_1, L_3 的焦距[8]均等于 z，而 L_2 的焦距为 z/2。P_1，P_2 分别代表输入和输出平面。图 1b 是 Gyrator 变换中的透镜的结构，α_1，α_2 均是旋转

角度：

$$\alpha_1=-\alpha;\ \alpha_2=\alpha-\pi/2 \tag{3}$$

初始图像由 P_1 平面进入，通过 Gyrator 变换的光学结构对其进行调制，则明文的 Gyrator 变换频谱将记录 P_2 上：

$$O(x_0,y_0)=\frac{1}{|2\lambda\sin\alpha|}\times\iint f_i(x_i,y_i)\times \exp\left\{i2\pi\frac{(x_0y_0+x_iy_i)(2\sin2\alpha_1\sin2\alpha_2-1)-\dfrac{(x_iy_0+x_0y_i)}{2\lambda\sin2\alpha_2}}{\sin\alpha}\right\}\mathrm{d}x_i\mathrm{d}y_i \tag{4}$$

式中：λ 为输入光波波长。

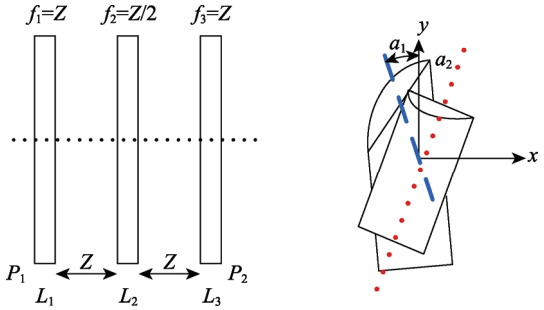


图 1　Gyrator 变换的光学系统

Fig.1 Optical system of Gyrator transform

2　混合幅度–相位检索技术

相位检索技术[9]因其解密密钥与加密密钥并非完全一致，使其具有较高的加密安全性，被广泛用于光学加密领域，但是，普通的相位检索技术只考虑了相位信息，忽略了幅度信息，不能形成非对称加密机制，使其安全性有待进一步提高。为此，文中通过引入幅度-相位截断机制[10]，设计了混合幅度-相位检索方法，使其检索解密所需的相位密钥与幅度密钥，其过程见图 2。令初始明文为 $r(x,y)$，$e(u,v)$ 为实值密文，则依据 Yang-Gu 算法[11]，可得：

$$e(u,v)P(u,v)=FT\left\{r(x,y)\exp\left[i\varphi(x,y)\right]\right\} \tag{5}$$

式中：$FT\{\}$ 为 Fourier 变换；$p(u,v)$ 为公共随机相位密钥；$\varphi(x,y)$ 为待检索的未知相位密钥。

由于 Fourier 机制的变换核是一个球面与平面波的内积，且存在 4 个交叉二次相位因子，使其较为复杂，而 Gyrator 变换的核是一个双曲面与平面波的内积，使其容易实现，因此，文中利用 Gyrator 变换替换式（5）中的 Fourier 变换，可得：

$$e(u,v)P(u,v)=G^{\alpha}\left\{r(x,y)\exp\left[i\varphi(x,y)\right]\right\} \tag{6}$$

式中：$G^{\alpha}\{\}$ 为 Gyrato 变换。

由于所提混合幅度-相位检索方法需多次迭代，因此，文中利用 Logistic 映射[12]的输出值作为初始的 $e_0(u,v)$。依据相位检索技术，假设第 k 次迭代的 $e_k(u,v)$ 是已知的，则基于 Gyrato 逆变换与密钥 $P(u,v)$，可形成一个复函数 $F_k(x,y)$：

$$F_k(x,y)=G^{-\alpha}\left\{e_k(u,v)P(u,v)\right\} \tag{7}$$

再基于幅度-相位截断机制[10]，计算 $f_k(x,y)$ 的相位与幅度部分：

$$\begin{cases}f_k(x,y)=AT\left[F_k(x,y)\right]=\left|F_k(x,y)\right|\\ P(x,y)=PT\left[F_k(x,y)\right]=\arg\left\{F_k(x,y)\right\}\end{cases} \tag{8}$$

则在下一轮迭代检索中，根据式（9）函数来更新幅度信息 $e_{k+1}(u,v)$：

$$\begin{cases}E_{k+1}(u,v)=G^{\alpha}\left\{r(x,y)\exp\left[\varphi_k(x,y)\right]\right\}\\ e_{k+1}(u,v)=\left|E_{k+1}(u,v)P^*(u,v)\right|\end{cases} \tag{9}$$

式中：*为卷积操作。

为了检测这种迭代检索如何停止，文中将明文 $r(x,y)$ 与第 k 次迭代的 $f_k(x,y)$ 之间的归一化均方误差若 N_{MSE} 作为收敛标准：

$$N_{\mathrm{MSE}}=\frac{\sum_{x,y}\left[r(x,y)-f_k(x,y)\right]^2}{\sum_{x,y}r^2(x,y)} \tag{10}$$

在上述迭代期间，若 N_{MSE} 值小于预设值（是一个非常小的值，接近 0），则迭代检索过程停止。由于幅度信息 $e_{k+1}(u,v)$ 中包含了正负元素，为了便于在 CCD 相机中检测其振幅，文中利用了单向二进制相位函数 $\exp\left[i\pi b(u,v)\right]$ 来调制处理。其中，$b(u,v)$ 计算函数为：

$$b(u,v)=\begin{cases}1 & e_{k+1}(u,v)<0\\ 0 & e_{k+1}(u,v)>0\end{cases} \tag{11}$$

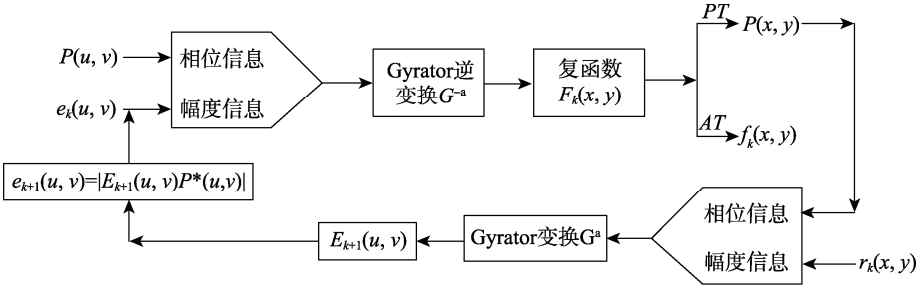


图 2　混合幅度-相位迭代检索技术过程

Fig.2 Hybrid amplitude-phase iterative retrieval process

依据式（11）得到的单向二进制相位函数 $\exp\left[i\pi b(u,v)\right]$，将其检测得到的振幅视为最终密文：

$$e'_{k+1}(u,v)=e_{k+1}(u,v)\exp\left[i\pi b(u,v)\right] \tag{12}$$

在上述混合幅度-相位迭代检索技术中，相位函数 $P(u, v)$ 被作为加密密钥。如果直接将普通的随机相位掩码作为私钥，则整个 $P(u, v)$ 则需要在发送者与接受者之间传输，从而降低了算法的安全性，且需要更大的传输容量。为了解决此问题，文中利用 Logistic 映射生成的随机相位掩码视为 $P(u, v)$，且只将 Logistic 映射的初值视为私钥。通过这种方式，私钥的传输容量大幅降低；且因着 Logistic 映射的敏感性，提高了密文的安全性。

3　文中光学图像加密算法

所提基于混合幅度-相位检索技术与二维耦合混沌映射的光学图像加密算法的过程见图 3，其主要分为 2 个过程：基于二维复合映射的彩图 R, G, B 分量的置乱；利用 Logistic 映射来生成混沌随机掩码；基于混合幅度-相位检索技术的图像加密。

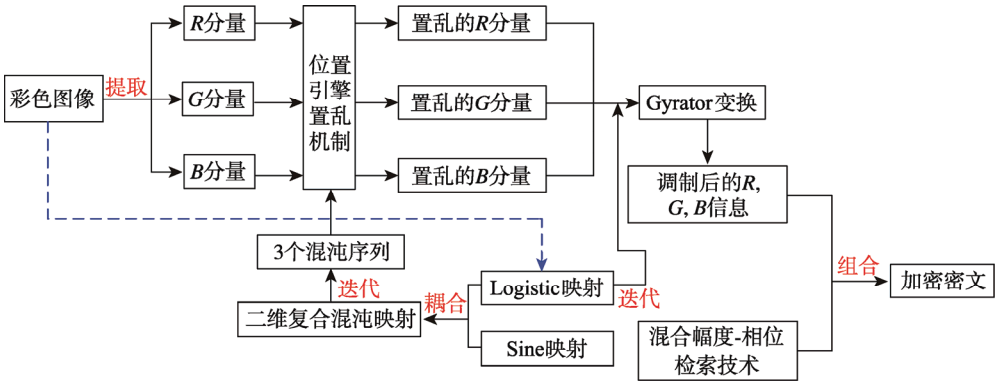


图 3　所提光学图像加密技术的过程

Fig.3 Process of the proposed optical image encryption technology

令彩色图像为 $f(x, y)$，其大小为 $M\times N$，通过如下程序来提取其相应的 R, G, B 分量，分别记为 $f_{\mathrm{R}}(x, y)$，$f_{\mathrm{G}}(x, y)$，$f_{\mathrm{B}}(x, y)$。

```
I=imread('caise.tif');
IR=I;IG=I;IB=I;
IR(:,:,2)=0;
IR(:,:,3)=0;
IG(:,:,1)=0;
IG(:,:,3)=0;
IB(:,:,1)=0;
IB(:,:,2)=0;
Figure;
Subplot(2,2,1);imshow(1,[]);title('I');
Subplot(2,2,2);imshow(IR,[]);title('IR');
Subplot(2,2,3);imshow(IG,[]);title('IG');
Subplot(2,2,4);imshow(IB,[]);title('IB');
```

为了避免直接将单色光束作用于 $f_{\mathrm{R}}(x, y)$, $f_{\mathrm{G}}(x, y)$, $f_{\mathrm{B}}(x, y)$，文中通过组合一维 Logistic 映射[12]与 Sine 映射[13]，设计了二维复合混沌映射，通过利用其输出的混沌序列来置乱 $f_{\mathrm{R}}(x, y)$，$f_{\mathrm{G}}(x, y)$，$f_{\mathrm{B}}(x, y)$，使其呈现一幅噪声图像。其中，Logistic 映射[12]模型为：

$$x_{n+1}=\mu x_n(1-x_n) \tag{13}$$

式中：$\mu\in[0,4]$为混沌参数；$x_n\in[0,1]$, x_0 分别为输出值与初始值。

Sine 映射[13]函数为：

$$x_{i+1}=\frac{a\sin(\pi x_i)}{4} \tag{14}$$

通过联合式（13）与式（14），形成二维复合混沌映射：

$$\begin{cases}x_{i+1}=a\left(\dfrac{\sin\pi y_i}{4}+\mu\right)x_i(1-x_i)\\ y_{i+1}=a\left(\dfrac{\sin\pi x_{i+1}}{4}\right)y_i(1-y_i)\end{cases} \tag{15}$$

式中：$\alpha\in[0,1]$, $\mu\in[0,3]$均为混沌控制参数；

所提的二维复合混沌系统综合了 2 个一维混沌映射的优势，不仅兼顾了一维混沌映射的简单结构，且其输出的混沌序列的自相关性更好。为了测试式(15)输出序列的随机性，取 α=0.52, μ=3、序列长度 N=4000，在测试库 TestU01[14]上来获取式（13）、式（14）、式（15）各自输出的混沌序列的自相关性，数据见图 4。依图可知，所提复合混沌系统所输出序列的随机性最高，对应的自相关性系数最低，都趋于 0。式（13）、式（14）2 个映射的输出序列的自相关性均高于所提映射。这表明所提复合映射具有更高的混沌性能。

为了提高密文的抗明文攻击能力，文中利用输出明文 $f(x, y)$ 的像素来计算式（15）的初值 x_0 与 y_0：

$$\begin{cases}x_0=\dfrac{T}{5\times10^7}\\ y_0=1-x_0\end{cases} \tag{16}$$

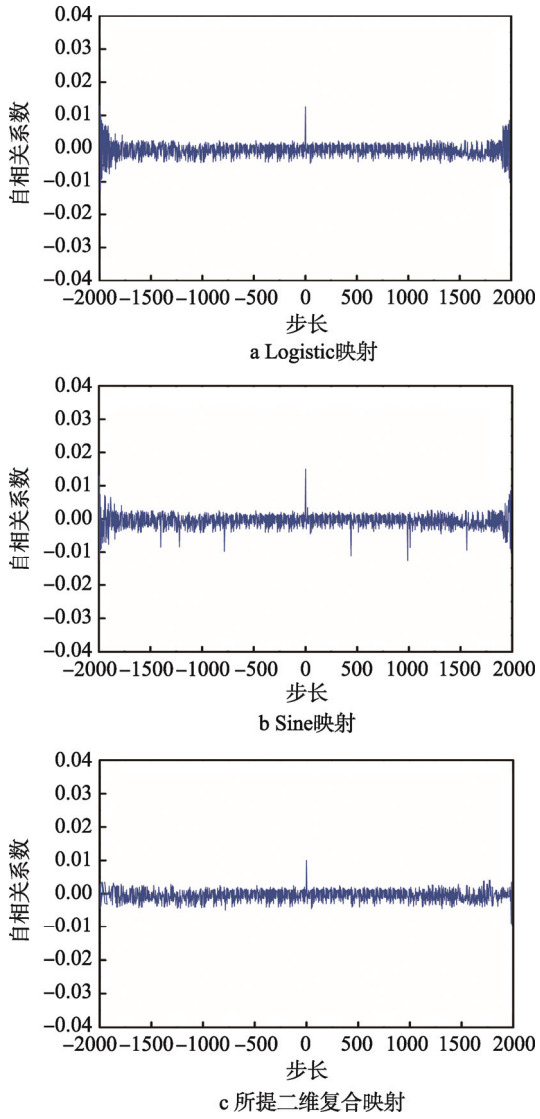


图 4　不同混沌映射的混沌性能测试

Fig.4 Chaotic performance test of different chaotic maps

随后，设置好混沌参数 α,β，联合 x_0,y_0，对式(15)进行迭代 $M\times N+K$ 次，输出 2 个随机数组 $\boldsymbol{X}=\{x_1,x_2....x_{M\times N+K}\}$，$\boldsymbol{Y}=\{y_1,y_2....y_{M\times N+K}\}$。为了消除瞬态效应，将序列 $\boldsymbol{X}$, $\boldsymbol{Y}$ 中的前 K 个元素值删除，形成新的序列 $\boldsymbol{X'}=\{x'_1,x'_2....x'_{M\times N}\}$，$\boldsymbol{Y'}=\{y'_1,y'_2....y'_{M\times N}\}$。再根据序列 $\boldsymbol{X'}$与 $\boldsymbol{Y'}$来计算第 3 个序列 $\boldsymbol{Z'}=\{z'_i\}$：

$$z'_i=\frac{x'_i+y'_i}{2} \tag{17}$$

为了对 $f_{\mathrm{R}}(x,y)$，$f_{\mathrm{G}}(x,y)$，$f_{\mathrm{B}}(x,y)$ 完成置乱，文中利用序列 $\boldsymbol{X'}$, $\boldsymbol{Y'}$与 $\boldsymbol{Z'}$来构建像素位置引擎混淆机制，过程如下：首先，按照升序对序列 $\boldsymbol{X'}=\{x'_1,x'_2....x'_{M\times N}\}$ 中的元素进行排列，得到一组新的数组 $\boldsymbol{X''}=\{x''_1,x''_2....x''_{M\times N}\}$。随后，从 $\boldsymbol{X'}=\{x'_1,x'_2....x'_{M\times N}\}$ 中确定出 $\boldsymbol{X''}=\{x''_1,x''_2....x''_{M\times N}\}$ 对应元素的位置，获取一组地址编码 $\boldsymbol{W}=\{w_1,w_2....w_{M\times N}\}$：

$$x''_i=x'_{w_i} \tag{18}$$

将 R 分量 $f_{\mathrm{R}}(x,y)$ 演变为一维数组，利用地址编码 $\boldsymbol{W}=\{w_1,w_2....w_{M\times N}\}$ 对 $f_{\mathrm{R}}(x,y)$ 进行置乱，高度改变其像素位置，形成置乱图像 $f'_{\mathrm{R}}(x,y)$。对于其他 2 个分量 $f_{\mathrm{G}}(x,y)$，$f_{\mathrm{B}}(x,y)$，分别通过序列 $\boldsymbol{Y'}$与 $\boldsymbol{Z'}$，按照像素位置引擎混淆机制，对其进行置乱，得到 $f'_{\mathrm{G}}(x,y)$，$f'_{\mathrm{B}}(x,y)$。以图 5a 为例，提取其 3 个分量 $f_{\mathrm{R}}(x,y)$，$f_{\mathrm{G}}(x,y)$，$f_{\mathrm{B}}(x,y)$，分别见图 5b—d。$f_{\mathrm{R}}(x,y)$，$f_{\mathrm{G}}(x,y)$，$f_{\mathrm{B}}(x,y)$ 经过文中像素位置引擎混淆机制处理后，分别见图 5e—g，可见，R, G, B 分量信息被高度隐藏，呈现一幅噪声分布图像。

彩色图像的 R, G, B 分量经过置乱处理后，得到了 $f'_{\mathrm{R}}(x,y)$，$f'_{\mathrm{G}}(x,y)$，$f'_{\mathrm{B}}(x,y)$。再利用式(13)

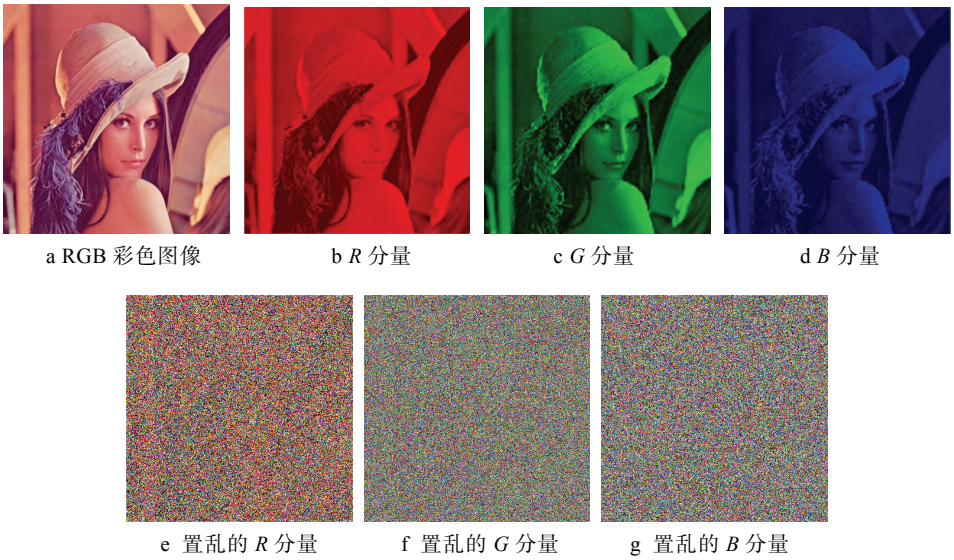


图 5　像素位置引擎混淆机制的置乱效果

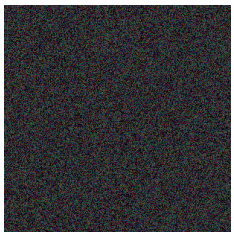
Fig.5 Scrambling effect of pixel position engine obfuscation mechanism

的输出随机序列来获取式（6）中的相位密钥 $P(u, v)$。为了增强密文的安全性，文中联合明文像素 $x_0=T/10^7$ 与 3 个不同的混沌控制参数 μ_R, μ_G, μ_B 对式（13）进行迭代，形成 3 个不同的混沌序列：$\boldsymbol{X}_R=\left\{x_1^R, x_2^R \ldots . x_{M\times N}^R\right\}$，$\boldsymbol{Y}_G=\left\{y_1^G, y_2^G \ldots . y_{M\times N}^G\right\}$，$\boldsymbol{Z}_G=\left\{z_1^B, z_2^B \ldots . z_{M\times N}^B\right\}$。并将这三者将其重组为对应的二维矩阵，利用式（19）处理 $\boldsymbol{X}_R$, $\boldsymbol{Y}_G$ 与 $\boldsymbol{Z}_G$ 中的每个元素，即可得到 R, G, B 分量对应的相位密钥 $P_R(u, v)$, $P_G(u, v)$, $P_B(u, v)$：

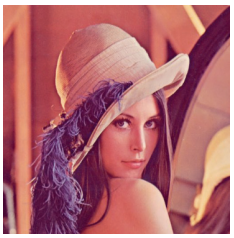
$$\begin{cases} P_R(u,v)=\exp\left(i\pi\times x_{i,j}^{\mathrm{R}}\right) \\ P_G(u,v)=\exp\left(i\pi\times y_{i,j}^{\mathrm{G}}\right) \\ P_B(u,v)=\exp\left(i\pi\times z_{i,j}^{\mathrm{B}}\right) \end{cases} \tag{19}$$

在相位密钥生成过程中，用初值 x_0 作为私钥，以替代相位 $P(u, v)$。为了降低复杂度，文中取 $\mu_R=\mu_G=\mu_B=3.95$，结合 $x_0=0.262$ 对式（13）进行迭代，经过上述过程处理后，得到 3 个相同的混沌相位掩码，见图 6a。

a 混沌相位掩码



b 加密密文



c 解密图像

图 6 混沌掩码及其加密方法的输出结果

Fig.6 Chaotic mask and its output results of encryption method

随后，根据混合幅度-相位迭代检索技术，联合式（19），将置乱后的 R, G, B 分量加密为实值密文：

$$\begin{cases} e_R(u,v)P_R(u,v)=G^{\alpha_R}\left\{f_R'(x,y)\exp\left[i\varphi_R(x,y)\right]\right\} \\ e_G(u,v)P_G(u,v)=G^{\alpha_G}\left\{f_G'(x,y)\exp\left[i\varphi_G(x,y)\right]\right\} \\ e_B(u,v)P_B(u,v)=G^{\alpha_B}\left\{f_B'(x,y)\exp\left[i\varphi_B(x,y)\right]\right\} \end{cases} \tag{20}$$

在加密过程中，为了破坏加密系统的线性关系，文中利用了 3 个不同的 Gyrator 变换角度 α_R, α_G, α_B。同样将这些参数 α_R, α_G, α_B 视为私钥。随后，再利用式（11）生成 3 个单向二进制相位函数 $\exp\left[i\pi b_R(u,v)\right]$，$\exp\left[i\pi b_G(u,v)\right]$，$\exp\left[i\pi b_B(u,v)\right]$，对式（20）中的 $e_R(u, v)$，$e_G(u, v)$，$e_B(u, v)$ 进行处理，获取 3 个正实值密文：

$$\begin{cases} e_R'(u,v)=e_R(u,v)\exp\left[i\pi b_R(u,v)\right] \\ e_G'(u,v)=e_G(u,v)\exp\left[i\pi b_G(u,v)\right] \\ e_B'(u,v)=e_B(u,v)\exp\left[i\pi b_B(u,v)\right] \end{cases} \tag{21}$$

根据式（21）输出的结果，通过对其组合，形成了最终的实值加密密文 $e(u, v)$，见图 6b。由图 6b 可知，经过混合幅度-相位迭代检索技术处理后，形成一幅与置乱结果截然不同的噪声图像，明文的信息被充分隐秘。

解密是加密方法的逆过程，较为简单，见图 7a；解密过程对应的光电结构见图 7b。其中，密文 $e(u, v)$ 经过相应的空间光调制器 SLM_1, SLM_2，以及焦距为 z 的 3 个透镜 L_1, L_2, L_3 之后，所输出的图像信息被记录在 CCD 中。解密过程如下所述。

1）利用前文的 R, G, B 分量提取程序，获取密文 $e(u, v)$ 的 3 个密文分量 $e'_R(u, v)$，$e'_G(u, v)$，$e'_B(u, v)$。

2）利用式（7）分别处理 $e'_R(u, v)$, $e'_G(u, v)$, $e'_B(u, v)$；然后，再根据式（8）获取 $e'_R(u, v)$, $e'_G(u, v)$, $e'_B(u, v)$ 的幅度信息。在进行角度 α_R, α_G, α_B 的 Gyrator 逆变换之前，需要利用解密密钥 $D_R(u, v)$, $D_G(u, v)$, $D_B(u, v)$ 分别乘以相应的密文分量 $e'_R(u, v)$, $e'_G(u, v)$, $e'_B(u, v)$。解密密钥的计算如下：

$$\begin{cases} D_{\mathrm{R}}(u,v)=P_{\mathrm{R}}(u,v)\exp\left[i\pi b_R(u,v)\right] \\ D_{\mathrm{G}}(u,v)=P_{\mathrm{G}}(u,v)\exp\left[i\pi b_G(u,v)\right] \\ D_{\mathrm{B}}(u,v)=P_{\mathrm{B}}(u,v)\exp\left[i\pi b_B(u,v)\right] \end{cases} \tag{22}$$

3）基于像素位置引擎混淆机制，利用相应的解密密钥 x_0, y_0, α, μ 得到的 3 个序列 $\boldsymbol{X}_R$, $\boldsymbol{Y}_G$ 与 $\boldsymbol{Z}_G$ 对 $f'_R(x, y)$, $f'_G(x, y)$, $f'_B(x, y)$ 进行置乱，从而得到了 R, G, B 分量 $f_R(x, y)$, $f_G(x, y)$, $f_B(x, y)$，再将这三者进行组合，获取解密图像，见图 6c。依图 6c 可知，复原图像质量较高，很好地保存了初始明文的细节与颜色信息。

根据上述加密与解密的过程可知，加密密文是一个实值函数，非常方便密文信息的存储与传输。将混沌系统的参数 α, μ, x_0, y_0 以及 gyrator 变换的 3 个角度 α_R, α_G, α_B 被视为私钥，以替代随机相位掩码，便于私钥的管理，并有效降低传输容量。另外，在进行光学加密之前，设计了一个像素位置引擎混淆机制，高度置乱图像，再将单色光色作用于置乱密文上，有效避免了彩色信息的丢失；同时利用了混沌系统的敏感性，以及 3 个不同变换角度的 gyrator 变换，充分破坏了算法的线性关系，提高了密文的安全性。

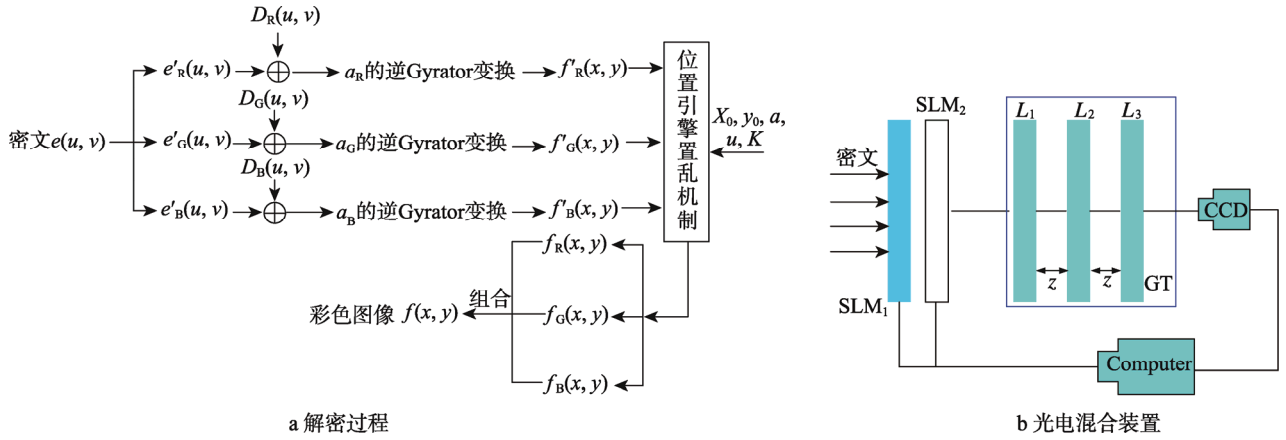


图 7　解密过程
Fig.7 Decryption process

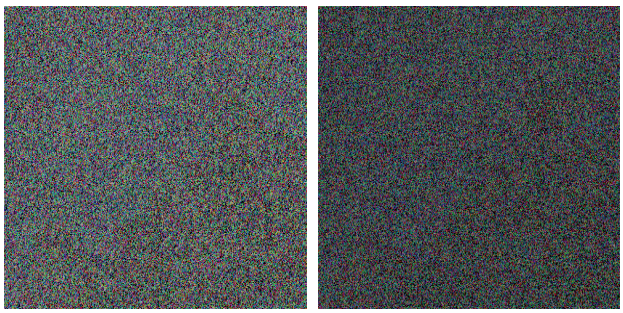
4　实验结果与分析

为了验证文中光学加密机制的合理性与安全性，在 Matlab 7.0 软件中完成加密测试验证。另外，为了反映文中技术的优异性，将当前较为先进的光学加密方法作为对照组：文献[5]与文献[15]。其中，文献[15]是利用高维混沌系统与快速响应码来实现图像的光学加密，利用明文来生成一个快速响应码，将其置于双随机相位编码结构的输入平面中，再利用高维混沌系统与 Gyrator 变换将其变为一个似噪声分布的密文，并利用相位检索技术来重构快速响应码的信息，显著增强了密文的安全性与解密质量，具有很好的代表性。执行该次实验的实验参数为：Gyrator 变换角 α_R=0.5°，α_G=0.7°，α_B=0.8°，混沌参数 μ=3.9，α=0.35，K=2000、焦距 z=0.06 m、波长为 632.8 mm、预设值为 10^{-5}。

4.1　图像加密效果测试

以图 8a 为测试对象，基于文中光学加密机制、文献[5]、文献[15]算法对其完成处理，结果见图 8b—d。依据输出结果可知，3 种光学加密算法都能够充分隐藏图像信息，均具有良好的保密效果，初始图像均被加密为噪声分布图像，攻击者很难从其密文中得到相关线索。但是，文献[5]、文献[15]算法的加密密文存在一定的轮廓显示问题，见图 8c—d。为了量化所提技术、文献[5]、文献[15]方法的安全性差异，利用信息熵值[16]来评估，输出数据见表 1。根据表中数据可知，所提算法的密文熵值最大，约为 7.9984，文献[15]密文熵值要略小于所提技术，约为 7.9946，而文献[5]算法的密文熵值最小，为 7.8932。原因是所提算法利用了明文像素来设计像素位置引擎混淆机制，在进行光学处理前，将其变为一个置乱密文，且利用幅度-相位截断方法，兼顾了图像的幅度与相位信息来完成光学加密，充分利用混沌系统的敏感性，以及 3 个不同变换角度的 gyrator 变换，充分破坏了算法的线性关系，提高了密文的安全性。文献[15]则是联合高维混沌系统与快速响应码来完成加密，虽然高维混沌系统的复杂相空间与轨迹给其算法提供了较高的安全性，但是该技术则是将明文所有的信息集中在一个纯相位掩码中，导致其密文存在轻微的轮廓显示问题。文献[5]算法则是利用基于菲涅耳变换

a 初始彩色明文　　b 文中算法的密文



c 文献[5]算法的密文　　d 文献[15]算法的密文

图 8　不同算法的加密效果测试
Fig.8 Encryption effect test of different algorithms

表 1　信息熵值的测试测试果
Tab.1 Test results of information entropy

名称	密文熵值
文中算法	7.9984
文献[5]	7.8932
文献[15]	7.9946

（FrT）域 MGSA 融合波分复用技术来完成彩图加密，但是此技术是利用相同阶数的 FrT 变换，使其随机性不高，且此技术的加密过程忽略了明文特性，使其抗明文攻击能力较弱。

4.2 密文相关性测试

图像中任意 2 个相邻像素间具有非常高的关联性，能够为攻击者提供一定的线索，对图像的安全传输产生了较大的威胁[2]，因此，数字图像加密技术应可有效破坏相邻像素间的强烈关联性[2]。为了验证 3 种算法的安全性，从图 8a—d 中任意选择 2500 对相邻像素点来评估其关联性，一般用相关性系数 c_{xy} 来描述，其模型为[2]：

$$C_{xy}=\frac{\frac{1}{n}\sum_{i=1}^{n}\left(x_i-E(x_i)\right)\left(y_i-E(y_i)\right)}{\sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}\left(x_i-E(x_i)\right)^2\right)\left(\frac{1}{n}\sum_{i=1}^{n}\left(y_i-E(y_i)\right)^2\right)}} \tag{23}$$

图 9a—d 分别是初始图像、文中算法与其他 2 种算法的密文像素在水平方向上的相关性测试结果。由图 9a 可知，初始图像间的任意 2 个相邻像素的关联性较高，所有像素的分布状态不理想，堆积为一条“对角线”，对应的 c_{xy} 值达到了 0.9601。但是，初始图像经过所提算法、文献[5]、文献[15]处理后，原来的高度关联性得到了大幅削弱，相应的加密密文像素分布较为均匀，其 c_{xy} 值分别为 0.0012, 0.0059, 0.0037。再比较图 8b—d 可知，文中光学加密机制的密文关联性最低，对应的像素分布最为均匀，没有像素点聚集或者消失现象。

另外 2 个方向的 c_{xy} 数据见表 2。根据表 2 中数据，不管是图像中的哪个测试方向，初始图像的 c_{xy} 值均为最高。但是，经过所提算法、文献[5]、文献[15]加密后，其对应的 c_{xy} 值明显变小，且文中算法的密文 c_{xy} 值总体上要小于文献[5]、文献[15]的技术，只有对角线的相关性系数 c_{xy} 要略大于文献[15]。

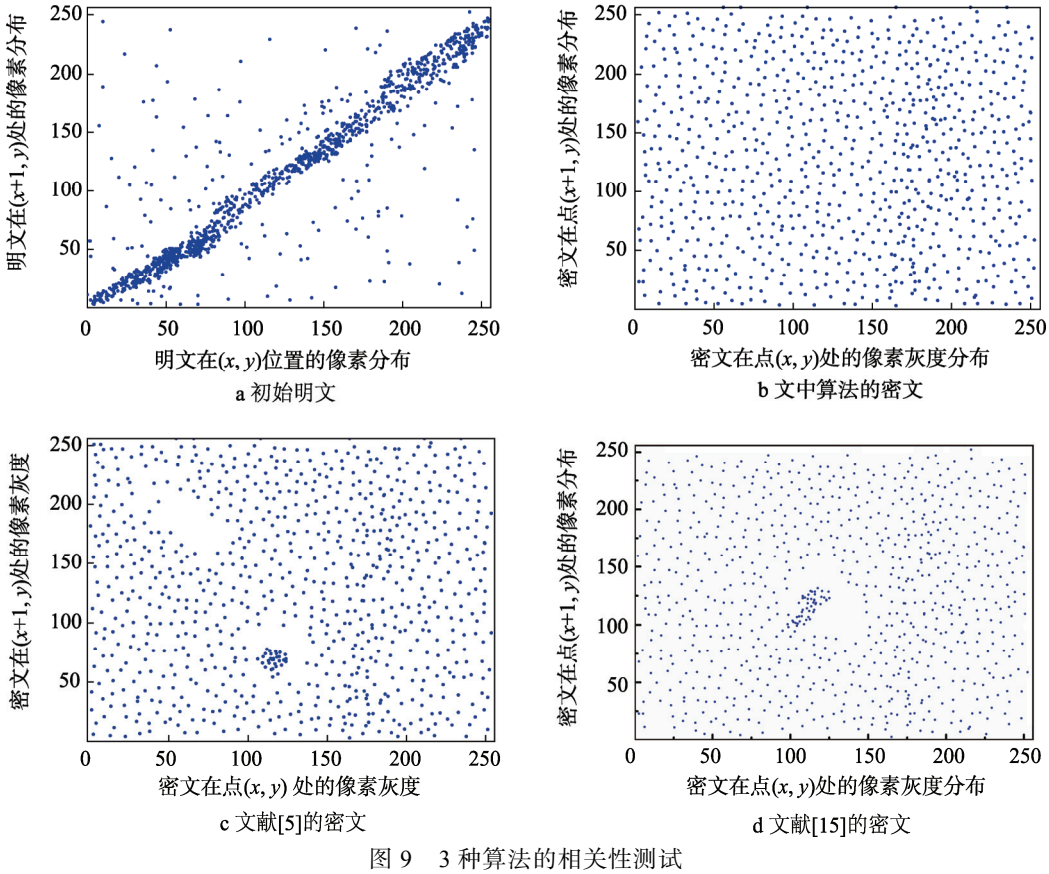


图 9 3 种算法的相关性测试

Fig.9 Correlation test of three algorithms

表 2 不同方向的相关系数测试结果

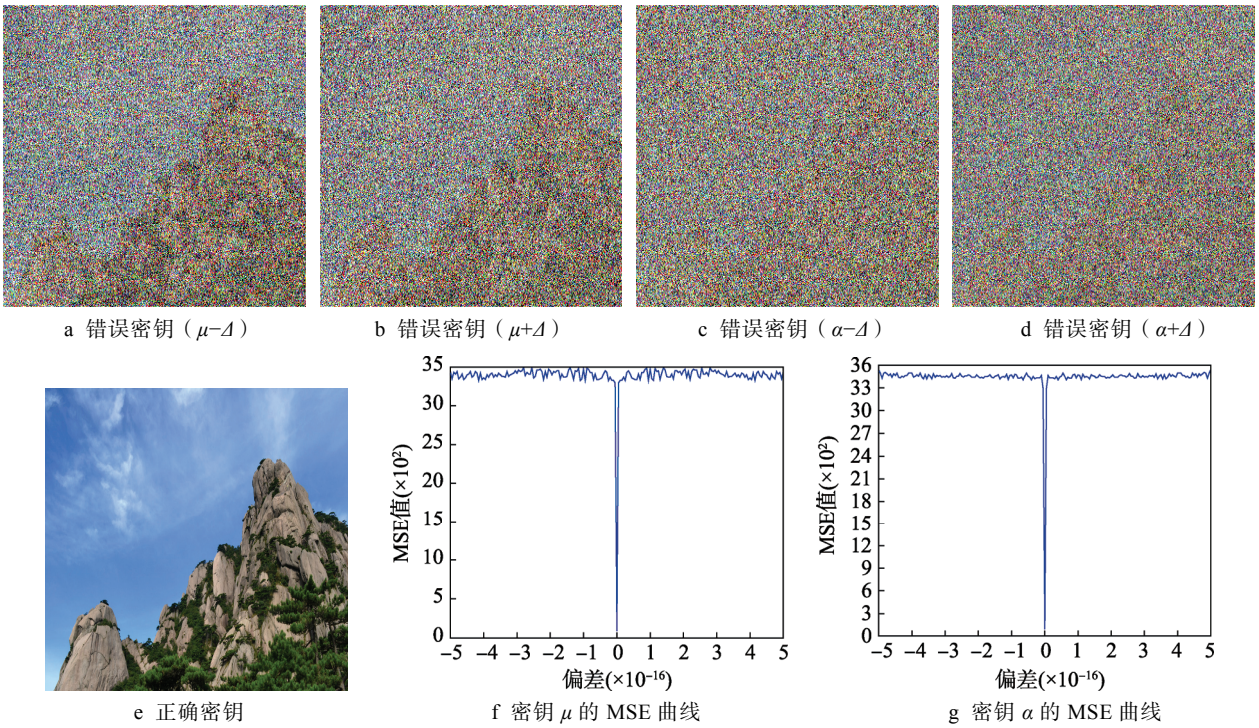
Tab.2 Correlation coefficient test results in different directions

选取方向	图 8a	图 8b	图 8c	图 8d
水平	0.9601	0.0012	0.0059	0.0037
垂直	0.9832	0.0039	0.0093	0.0051
对角线	0.9274	0.0026	0.0071	–0.0034

4.3 密钥敏感性测试分析

密钥敏感性是衡量加密算法安全性的重要指标，需满足严格的“雪崩效应”，当密钥发生微小波动时，所产生的解密图像差异是巨大的[17]。对此，文中测试了混沌参数 μ=3.9 以及 α=0.35 的敏感性。首先，通过偏差值 $\Delta=10^{-16}$ 来变动 μ 与 α，形成错误密钥（$\mu-\Delta$），

（$\mu+\Delta$），（$\alpha-\Delta$）和（$\alpha+\Delta$）。而其余密钥均不变。再利用正确的密钥，以及这些错误密钥对图 8b 进行复原，并得到了 μ 与 α 的 MSE 曲线，输出结果见图 10。由图 10a—d 可知，即使私钥 μ 与 α 发生了 10^{-16} 的微小变化，非授权用户仍然是不能得到清晰完整的初始图像，相应的 MSE 值均接近了 3500。只有借助正确密才能准确解密图像，见图 10e，此时对应的 MSE 曲线发生剧烈变动，其 MSE 值接近 0，见图 10f。这表明所提算法与文献[5]、文献[15]算法一样，具有强烈的敏感性，可满足严格的“雪崩效应”。



a 错误密钥（$\mu-\Delta$）　b 错误密钥（$\mu+\Delta$）　c 错误密钥（$\alpha-\Delta$）　d 错误密钥（$\alpha+\Delta$）

e 正确密钥　f 密钥 μ 的 MSE 曲线　g 密钥 α 的 MSE 曲线

图 10　文中算法的敏感度测试结果

Fig.10 Sensitivity test results of the proposed algorithm

4.4　抗选择明文攻击能力测试

选择明文攻击对图像安全传输的威胁较大，优异的加密算法应能有效抗击此类攻击[18]。依据国内外研究可知[18]，NPCR 与 UACI 曲线是衡量加密方法抗选择明文攻击性能的常用指标。其中，NPCR 与 UACI 模型为[18]：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\mathrm{Difp}\left(I(i,j),I'(i,j)\right)}{W\times H}\times 100\% \tag{24}$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{\left|I(i,j)-I'(i,j)\right|}{255}\right]\times 100\% \tag{25}$$

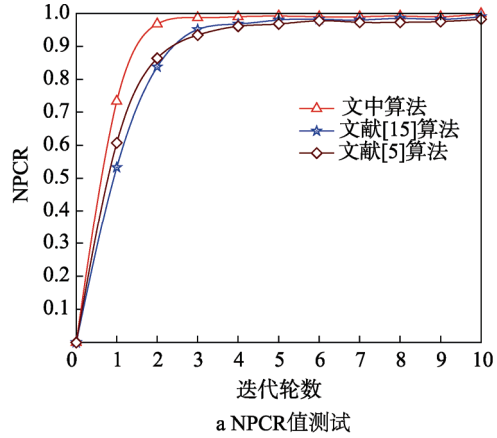
$$\mathrm{Difp}\left(I(i,j),I'(i,j)\right)=\begin{cases}0, & I(i,j)=I'(i,j)\\ 1, & I(i,j)\neq I'(i,j)\end{cases} \tag{26}$$

式中：W, H 分别是明文的高度与宽度；I, I'分别为 2 个明文经加密处理后的 2 个密文，且这 2 个明文都只存在一个相异灰度值。

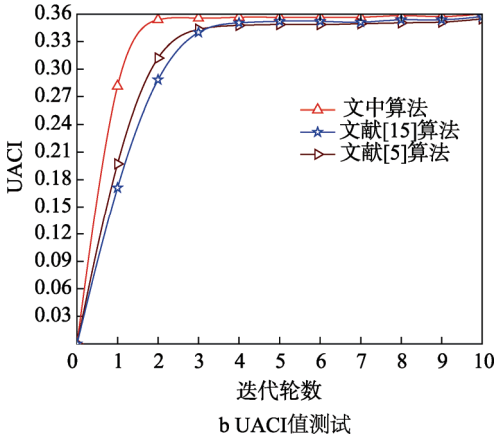
把图 8a 作为实验对象，将坐标（39, 145）处的像素值 117 篡改为 68，从而得到了一个新的图像；随后，借助文中机制、文献[5]、文献[15]对初始图像和修改后的明文实施加密，根据式（24—26）得到了三者对应的 NPCR, UACI 曲线，见图 11。基于测试数据可知，文中光学加密方法的抗明文攻击性能最优，其 NPCR, UACI 值均高于文献[5]、文献[15]技术，分别为 99.82%, 35.49%，而文献[5], 文献[15]机制的 NPCR, UACI 值较低，均小于所提方法。主要原因是所提算法的置乱过程与明文密切相关，通过明文像素数量来生成置乱所需的混沌序列，且在光学加密期间，借助明文像素来生成 3 个相位密钥，使得整个加密过程均依赖于明文，使得算法对明文的敏感性非常强烈，攻击者试图利用其他明文来破译所提技术的密文，因着明文的不同，使得其加密与解密的密钥是截然不同的，最终不能正确解密图像。文献[5]、文献[15]的加密机制均没有考虑明文信息，使其对明文的敏感性不佳，因此，攻击者可通过大量选择明文攻击实验来解密密文。

4.5　解密质量测试

加密算法除了其安全性之外，解密质量也是其重要评估指标[2]。为了量化所提技术、文献[5]、文献[15]的复原质量，利用三者各自的解密过程及其相应的密钥，对图 8b—d 实施解密，结果见图 12。由图 12 可



a NPCR值测试



b UACI值测试

图 11 不同算法的抗选择明文攻击性能测试

Fig.11 Anti-chosen plaintext attack performance test of different algorithms

a 文中算法

b 文献[5]

c 文献[15]算法

图 12 3 种算法的解密效果测试

Fig.12 Decryption effect test of three algorithms

知，文中光学加密技术的复原质量最好，解密图像清晰，完整地保留了初始图像颜色信息，见图 12a。虽然文献[5]、文献[15]技术的解密图像视觉质量也较为理想，细节内容没有失真，但是二者的复原结果与初始明文存在一定的颜色差异，见图 12b—c。主要原因是所提技术在进行光学加密之前，利用像素位置置乱方法将初始图像演变为一个噪声分布图像，在后续的单色光处理过程中，能够较好地保留初始图像的颜色与细节信息。文献[5]、文献[15]算法则是直接将单色光照亮在初始图像上，在其加密过程中，丢失了部分颜色信息，使其复原质量不佳。

5 结语

为了兼顾加密算法的安全性与解密质量，文中设计了基于混合幅度-相位检索技术与二维耦合混沌映射的光学彩色图像加密技术，在空域与 Gyrator 域上实现像素的混淆，增强了密文的非线性关系。攻击者只有得到正确的密钥，如 logistic 映射、二维复合混沌映射的初值条件，以及 Gyrator 变换的旋转角度等，才能对密文正确复原。明文图像经过所提技术加密后，可以输出一个实值密文，便于其存储与管理。实验结果验证了所提光学加密技术的有效性与优异性。

未来将引入 Fresnel 波带与 Hilbert 相位函数，与 Logistic 映射生成的混沌相位掩码进行融合，形成一个混合掩码，进一步提高密文的随机性与安全性。

参考文献：

[1] STOYANOV B, KORDOV K. Image Encryption Using Chebyshev Map and Rotation Equation[J]. Entropy, 2015, 17(4): 2117—2139.

[2] 马建明，高正平，任兴东. 基于混沌切换系统与余弦数量变换的图像加密[J]. 计算机工程与设计，2016, 37(9): 2490—2496.
MA Jian-ming, GAO Zheng-ping, REN Xing-dong. Image Encryption Based on Chaotic Switching System and Cosine Number Transformation[J]. Computer Engineering and Design, 2016, 37(9): 2490—2496.

[3] ENAYATIFARA R, ABDULLAH A H. Image Encryption Using a Synchronous Permutation-diffusion Technique[J]. Optics and Lasers in Engineering, 2017, 90: 146—154.

[4] WU X J, WANG K S, WANG X Y. Lossless Chaotic Color Image Cryptosystem Based on DNA Encryption and Entropy[J]. Nonlinear Dynamics, 2017, 90(2): 855—875.

[5] 张国平，黄淼，马丽. 基于 MGSA 融合波分复用的光学彩色图像加密[J]. 激光杂志，2015, 36(7): 63—67.
ZHANG Guo-ping, HUANG Miao, MA Li. Optical Color Image Encryption Based on MGSA Integrated Wavelength Division Multiplexing[J]. Laser Journal, 2015, 36(7): 63—67.

[6] ABUTURAB M R. An Asymmetric Color Image Cryptosystem Based on Schur Decomposition in Gyrator Transform Domain[J]. Optics & Lasers in Engineering, 2014, 58(4): 39—47.

[7] ABUTURAB M R. An asymmetric Single-Channel Color Image Encryption Based on Hartley Transform and Gyrator Transform[J]. Optics & Lasers in Engineering, 2016, 69: 49—57.

[8] 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.
XIAO Ning, LI Ai-jun. Optical Image Encryption Algorithm Based on Circular Harmonic Components Expansion and Phase Retrieval in Gyrator Transform Domain[J]. Journal of Electronic Measurement and Instrument, 2017, 31(6): 876—884.

[9] CHEN L F, CHAN G J, HE B Y. Optical Image Conversion and Encryption by Diffraction, Phase Retrieval Algorithm and Incoherent Superposition[J]. Optics and Lasers in Engineering, 2017, 88(3): 221—232.

[10] MEHRA I, RAJPUT S K. 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(1): 167—173.

[11] LIU W, LIU Z, LIU S. Asymmetric Cryptosystem Using Random Binary Phase Modulation Based on Mixture Retrieval Type of Yang-Gu Algorithm[J]. Optics Letters, 2013, 38(10): 1651—1653.

[12] 谢国波, 丁煜明. 基于 Logistic 映射的可变置乱参数的图像加密算法[J]. 微电子学与计算机, 2015, 23(4): 111—115.
XIE Guo-bo, DING Yu-ming. Image Encryption Algorithm Based on Logistic Map with Variable Scrambling Parameters[J]. Microelectronics & Computer, 2015, 23(4): 111—115.

[13] 彭英杰, 陈豪颉. 多特征检测耦合混沌映射的红外图像加密算法[J]. 计算机工程与设计, 2017, 38(11): 3099—3105.
PENG Ying-jie, CHEN Hao-jie. Infrared Image Encryption Algorithm with Multi-feature Detection Coupled Chaotic Map[J]. Computer Engineering and Design, 2017, 38(11): 3099—3105.

[14] L'ECUYER P, SIMARD R. TestU01: A C Library for Empirical Testing of Random Number Generators[J]. Acm Transactions on Mathematical Software, 2007, 33(4): 22—28.

[15] SUI L S, XU M J, 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(10): 106—114.

[16] SU X, LI W H, HU H G. Cryptanalysis of A Chaos-based Image Encryption Scheme Combining DNA Coding and Entropy[J]. Multimedia Tools and Applications, 2017, 76(12): 14021—14033.

[17] 郭静博, 孙琼琼. 改进的引力模型耦合明文像素相关交叉机制的图像加密算法[J]. 包装工程, 2016, 37(13): 165—172.
GUO Jing-bo, SUN Qiong-qiong. An Image Encryption Algorithm Based on the Improved Gravitational Model Coupling Plaintext Pixel Correlation Cross Mechanism[J]. Packaging Engineering, 2016, 37(13): 165—172.

[18] LIU Y S, ZHANG L Y, WANG J. Chosen-plaintext Attack of An Image Encryption Scheme Based on Modified Permutation-diffusion Structure[J]. Nonlinear Dynamics, 2016, 84(4): 2241—2250.