图文信息技术

# 基于圆柱衍射与离散余弦变换的图像光学加密算法

郭静博
（平顶山教育学院 计算机系，平顶山 467000）

**摘要：目的** 为了实现多幅图像的同步加密，并增强加密系统的抗破译能力，提出一种基于圆柱衍射域的相位截断与离散余弦变换的多图像光学加密算法。**方法** 首先引入压缩感知（CS，Compress Transform）方法，对输入明文实施压缩；基于离散余弦变换 DCT（Discrete Cosine Transform）对压缩明文完成分解，获取相应的 DCT 系数，形成系数矩阵；构建迭代复数，将每个压缩明文对应的系数矩阵融合为一个复矩阵，通过 DCT 逆变换，形成一幅组合图像。联合 Hilbert 变换与波带片相位模型，构建调制掩码；引入圆柱衍射域的相位截断机制，联合调制掩码，对组合图像实施光学加密，获取密文与私钥。**结果** 实验数据表明，相对于已有的多图像同步加密方法而言，所提算法具备更高的加密安全性，密文熵值以及相邻像素间的相关系数分别达到了 7.998，0.0012，且具有强烈的密钥敏感性。**结论** 所提加密算法可以抵御网络中外来攻击，在图像信息防伪领域具有一定的参考价值。

**关键词：**多图像同步加密；圆柱衍射；相位截断；离散余弦变换；Hilbert 变换；调制掩码
**中图分类号：**TP391 **文献标识码：**A **文章编号：**1001-3563(2019)09-0205-11
**DOI：**10.19554/j.cnki.1001-3563.2019.09.033

## Image Optical Encryption Algorithm Based on Cylindrical Diffraction and Discrete Cosine Transform

*GUO Jing-bo*
(Department of Computer, Pingdingshan College of Education, Pingdingshan 467000, China)

**ABSTRACT:** The paper aims to propose a multi-image synchronous encryption algorithm based on phase truncation in cylindrical diffraction domain and discrete cosine transform to realize the fast-synchronous encryption of multi-images and enhance the anti-cracking ability of the encryption system. Firstly, the compress transform (CS) was introduced to compress input plaintext. The compressed plaintext was decomposed based on discrete cosine transform (discrete cosine transform) to obtain the corresponding DCT coefficients. And these coefficients were combined into matrices. Iterative complex function was constructed to fuse the coefficient matrix corresponding to each compressed plaintext into a complex matrix. And a combined image was formed by reversible DCT method. The modulation mask was constructed by combining Hilbert transform with waveband plate phase model. Finally, the ciphertext and private key of combined images were obtained by introducing the phase truncation mechanism in cylindrical diffraction domain and modulation mask. The experimental data showed that compared with existing multi-image synchronous encryption, the proposed algorithm had higher encryption security. Its entropy of ciphertext and correlation coefficients between adjacent pixels were 7.998 and 0.0012, respectively. It also has stronger key sensitivity. This encryption algorithm can resist external attacks in the network, which has certain reference value in the field of anti-counterfeiting of image information.

**收稿日期：**2018-12-23
**基金项目：**河南省科技计划重点项目（172400410498）；河南省科技厅计划（152400410323）
**作者简介：**郭静博（1982—），女，硕士，平顶山教育学院讲师，主要研究方向为图像处理、信息安全。

**KEY WORDS:** multi-image synchronous encryption; cylindrical diffraction; phase truncation; discrete cosine transform; Hilbert transform; modulation mask

随着因特网与多媒体技术的快速发展，各国、各领域之间的信息交流变得日益频繁，与此同时，信息被窃取问题也较为严重，而图像含有丰富的内容信息，具有较为直观的表达方式，成为当前的信息交流的重要介质之一，带给各领域、各国人们巨大的生活便利[1—2]。图像在跨区域使用时，常需借助网络来实现，此时，其易遭受未知攻击，使得相关信息被肆意攻击，给其内容的真伪辨别增加了困难[3]。为了防止图像内容在传输阶段中被修改，学者们提出了相应的图像加密算法主要有单图像加密[4—6]与多图像同步加密算法[7—9]。如 Chai 等[4]为了改善密文的抗破译能力，提出了混沌系统耦合压缩感知的快速图像加密方法，首先，对原始图像进行离散小波变换，得到稀疏系数矩阵，并利用采用锯齿扫描与元胞自动机对该矩阵实施置乱，然后，利用记忆混沌系统产生的测量矩阵对置乱后的图像进行压缩感知，得到最终的密码图像，仿真数据验证了其加密效率与安全性。Wang 等[5]为了改善加密系统的效率，提出了多混合哈希函数与循环移位的图像加密算法，联合 SHA1 和 MD5 哈希算法，来生成明文对应的哈希值，并以此来混沌系统的初值，并借助利用非线性方程和 logistic 映射来获取置乱序列，改变明文像素位置，随后，通过循环移位函数与分段线性混沌映射，对置乱密文实施扩散，完成信息加密。Ghebleh 等[6]提出了分段线性混沌映射耦合最小二乘逼近的数字图像加密算法，该算法由像素置乱与掩蔽这 2 个阶段组成，利用 1D 混沌映射的输出序列来高度混淆像素位置，并通过最小二乘逼近来增强系统的安全性，测试结果显示了该算法的有效性与优势，可以有效抵御统计攻击。

以上图像加密算法虽然能够改善信息在网络传输中的抗破译能力，然而，此类算法无法对多图像同步加密，难以满足实际工程的需求[7]。为此，国内外学者提出了多图像同步加密算法，如张红梅等[7]为了能够同步对多幅图像实施加密，提出了基于迭代复数模型的多图像无损同步加密算法，利用迭代图像复数模型与可逆 DCT 变换，将多幅图像融合为成单图像，并借助 Logistic 映射来混淆融合图像，再结合混沌掩码，构造双重加密函数，对复合置乱图像进行扩散，输出密文；但是，此算法是单纯的混沌加密方法，存在迭代周期性，使密文安全性不佳。Pan 等[8]为了改善密文抗攻击能力，提出了基于离散余弦变换 DCT 与非线性分数梅林变换的多图像光学加密方法，可以避免线性加密系统的弱点，利用 DCT 机制，获取每个明文对应的光谱，然后将光谱进行切割与拼接，形成复合光谱，通过采用非线性分数梅林变换对其实施加密，测试数据表明该算法能够较好地对多幅图像实施同步加密，且输出的密文具备较好的安全性。这种通过切割与拼接来形成复合图像，容易丢失明文信息，降低了解密图像质量。Chen 等[9]为了降低存储空间与改善密文安全性，提出了压缩感知与特征融合的多图像光学加密算法，借助光学小波变换来获取每个明文对应的光谱，根据小波谱系数的不同特征，将 4 幅图像的高频分量和低频分量分别合并为高频融合图像和低频融合图像，并借助压缩感知，将高频融合图像分解为 2 个测量矩阵，并利用菲涅耳域中的相位截断（PT）和相位保留操作，将低频融合图像与测量矩阵加密成密文。此算法在利用光学小波变换时，只是采用了随机相位掩码来调制，容易引起光电装置中的光轴对准问题，限制其密文的安全性。

为了解决上述问题，有效增强光学加密系统的安全性，文中拟设计一种圆柱衍射域的相位截断耦合离散余弦变换的多图像光学加密算法。通过压缩感知（CS，Compress Transform）对明文实施压缩，消除冗余数据，降低存储空间；借助 DCT（Discrete Cosine Transform）来分解压缩明文，得到 DCT 系数，并把系数变为矩阵；采用迭代复数函数来组合这些矩阵，通过 DCT 逆变换，实现多图像的无损融合，形成一幅组合图像，避免丢失明文数据。将 Hilbert 变换与波带片相位模型组合，形成调制掩码，有效解决光电装置中的光轴校准问题；并基于圆柱衍射域的相位截断机制，对复合图像实施光学加密，输出密文。最后，对所提光学加密算法的安全性与敏感性进行测试。

## 1 压缩感知理论

压缩感知主要分为编码与解码 2 个阶段[10]，见图 1。如果输入信号是稀疏的，那么可以采用远低于采样定理的采样点来对其实施重构[10]。在 CS 中，不需要任何关于原始信号的像素域对应的信息，只有观察域信息。令 $\boldsymbol{\phi}$ 是一组变换基或者正交基，且是稀疏的，则稀疏信号 $\alpha$ 可表示为：

$$\alpha = \boldsymbol{\phi}^{\mathrm{T}} x \tag{1}$$

式中：$\boldsymbol{\phi} = [\phi_1, \phi_2 \cdots \phi_N]$ 为一组长度为 $N$ 的正交基；$\alpha$ 是初始信号 $x$ 在 $\boldsymbol{\phi}$ 的描述。

如果 $x$ 中只有 $k$ 个非零项，那么在 $\boldsymbol{\phi}$ 中的信号稀疏就是 $k$。为了增强变换信号的稀疏性，通常将 $\boldsymbol{\phi}$ 看作为一个过完备的词典。对于大小为 $M \times N$ 的测量矩阵 $\boldsymbol{\varphi}$，则接收信号 $y$ 为：

$$y = \boldsymbol{\varphi} x = \boldsymbol{\varphi}\boldsymbol{\phi}\alpha \tag{2}$$

在其信号的重构过程中，$\boldsymbol{\varphi}$ 必须满足受限等距性

质[11]。在 $\boldsymbol{\varphi}$ 中的受限等距常量 $\delta_k$ 需满足式（3）的最小值：

$$(1-\delta_k)\|x\|_2^2 \leqslant \|\varphi x\|_2^2 \leqslant (1+\delta_k)\|x\|_2^2 \tag{3}$$

其中，$\delta_k \in [0,1]$，若 $\delta_k < 1$，则测量矩阵 $\boldsymbol{\varphi}$ 满足第 $k$ 阶受限等距。

通过式（2）和（3），即可精确重构信号 $x$。

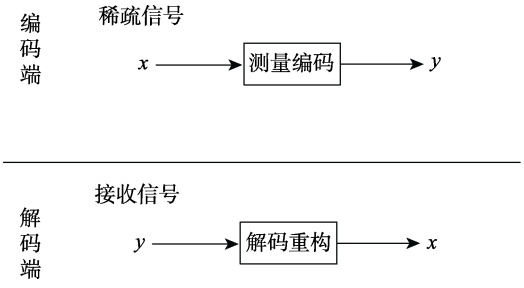



图 1　压缩感知过程

Fig.1 Compressive sensing process

## 2　圆柱衍射域中的相位阶段

圆柱衍射（CyD，Cylindrical Diffraction）是一种非线性衍射传播模式，其目标和观察表面分别是 2 个同心圆柱的内表面和外表面[12]，见图 2。其中的 $R$，$r$ 分别是内外表面的半径，因此，有 2 种传播模型，即从内部到外部以及从外部到内部的传播，分别见图 2a 和图 2b。对于由内到向外传播模式（IOP，Inside-Out Propagation）而言，$P_r(\theta_r,z_r)$，$Q_r(\theta_r,z_r)$分别表示圆柱坐标中的目标物体和观测点。对于由外到向内传播模式（OIP，Out-Inside Propagation）而言，$P_R(\theta_R,z_R)$，$Q_R(\theta_R,z_R)$分别表示圆柱坐标中的目标物体和观测点。另外，$z_R$，$z_r$ 的取值范围在$[-H/2, H/2]$，$H$ 是圆柱面的高度。那么这 2 种模型的衍射积分函数为[12]：

$$u_R(\theta_R,z_R) = C\iint_S u_r(\theta_r,z_r)\frac{\exp\left(\mathrm{i}kd_{P_rQ_R}\right)}{d_{P_rQR}}\mathrm{d}\theta_r\mathrm{d}z_r = CyD_r\left(u_r(\theta_r,z_r)\right) \tag{4}$$

$$u_r(\theta_r,z_r) = C\iint_S u_R(\theta_R,z_R)\frac{\exp\left(\mathrm{i}kd_{P_RQ_R}\right)\left[r-R\cos(\theta_r-\theta_R)\right]}{d^2{}_{P_rQ_R}}\mathrm{d}\theta_R\mathrm{d}z_R = CyD_R\left(u_R(\theta_R,z_R)\right) \tag{5}$$

$$d=dP_rQ_R = dP_RQ_r = \left[R_2+r_2-2Rr\cos(\theta_R-\theta_r)+(z_R-z_r)^2\right]^{1/2} \tag{6}$$

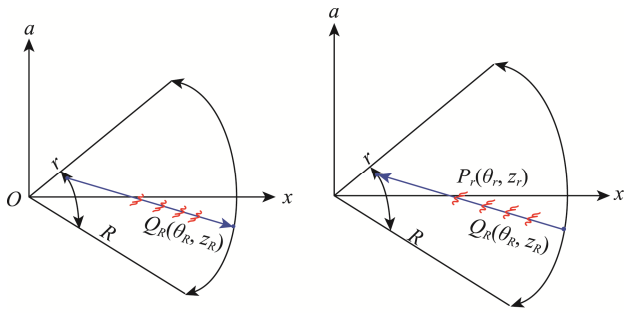
式中：$k$ 为入射光的波数；$C$ 为一个常量；$S$ 为目标表面；$d$ 为目标物体和观测点之间的距离。

以 OIP 模式为例，基于圆柱衍射的相位截断模型为：

$$A(\theta_r,z_r) = PT\left\{CyD_R\left[f(\theta_R,z_R)\cdot R_1(\theta_R,z_R)\right]\right\} \tag{7}$$

$$P(\theta_r,z_r) = PR\left\{CyD_R\left[f(\theta_R,z_R)\cdot R_1(\theta_R,z_R)\right]\right\} \tag{8}$$

式中：$PT$ 为相位截断操作；$PR$ 为相位保留操作；$P(\theta_r, z_r)$为解密过程中的私钥；$A(\theta_r, z_r)$为密文。




a IOP模式　　b OIP模式

图 2　圆柱衍射的几何关系

Fig.2 Geometric relation of cylindrical diffraction

## 3　多图像光学同步加密算法

圆柱衍射域的相位截断耦合离散余弦变换的多图像光学加密算法过程见图 3。由图 3 发现，所提算法有 3 个步骤：基于 DCT 与迭代复数模型的压缩图像无损融合；调制掩码的生成；基于圆柱衍射域的相位截断机制的图像同步加密。

### 3.1　基于 DCT 与迭代复数模型的压缩图像无损融合

1）令 $n$ 个输入明文为 $f_1, f_2 \ldots f_n$，其大小都是 $m \times z$。利用前文的 CS 方法，对 $f_1$，$f_2 \ldots f_n$ 实施压缩，获取相应的压缩图像 $I_1$，$I_2 \ldots I_n$。

2）采用 DCT（Discrete Cosine Transform）变换[13]，对 $I_1$，$I_2 \ldots I_n$ 实施分解，获取对应的系数矩阵 $\boldsymbol{M}_1$，$\boldsymbol{M}_2 \ldots \boldsymbol{M}_n$。首先，将每个压缩图像 $I_1$，$I_2 \ldots I_n$ 分割为 $n \times n$ 的子块，再借助 DCT 变换处理这些子块，获取 $I_1$，$I_2 \ldots I_n$ 对应的系数；并将 DCT 系数组合为矩阵 $\boldsymbol{M}_1$，$\boldsymbol{M}_2$，$\boldsymbol{M}_3 \ldots \boldsymbol{M}_n$。其中，DCT 模型如下[13]：

$$C(u,v) = S(u)S(v)\sqrt{\frac{2}{mz}}\cdot \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi}{m}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{z}v\left(y+\frac{1}{2}\right)\right] \tag{9}$$

式中：$C(u,v)$为 DCT 函数；$x$，$y$ 为压缩图像 $I_n$ 的像素点位置；$m \times z$ 为压缩图像的大小；$u$，$v$ 为 $C(u,v)$ 的坐标值；$\cos(A)$为余弦变换；$S(u)$，$S(v)$都为 $C(u,v)$ 的核变换，计算函数分别为[13]：

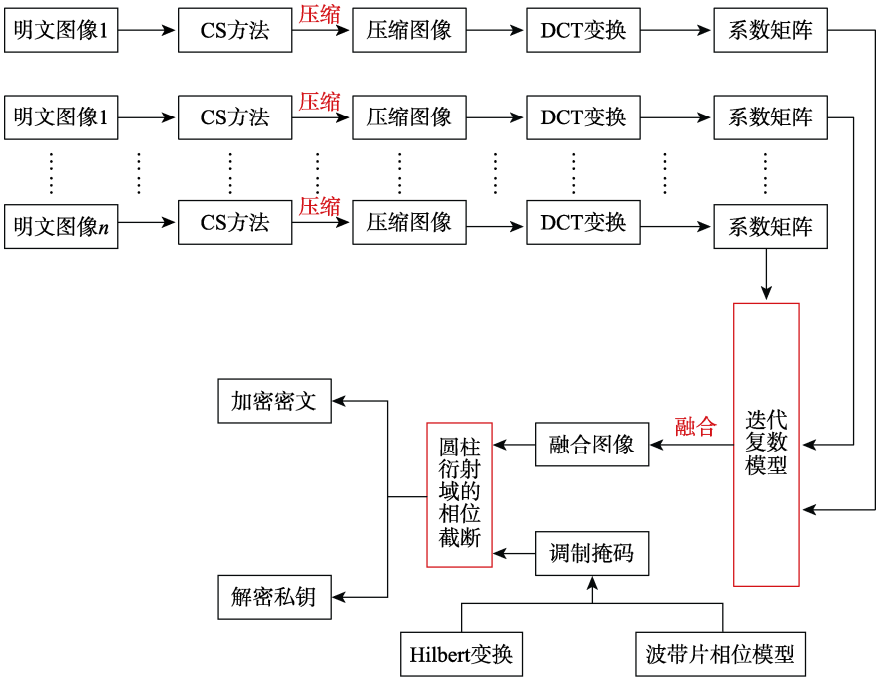



图 3　所提的多图像同步光学加密过程

Fig.3 Proposed multi-image synchronous optical encryption process

$$S(u)=\begin{cases}\sqrt{\dfrac{1}{2}} & u=0\\ 1 & 1\leqslant u\leqslant L-1\end{cases};\quad S(v)=\begin{cases}\sqrt{\dfrac{1}{2}} & v=0\\ 1 & 1\leqslant v\leqslant H-1\end{cases} \tag{10}$$

以图 4a、4c 为样本，其大小均为 256×256，将其分割为 4×4，形成一系列的子块 $B_i$；再借助式（9）对其分解，形成相应的 DCT 系数。取左上角的 4×4 子块为例，其对应的 4×4DCT 系数分别见图 4b 和图 4d。

| | | | |
|---|---|---|---|
| 362.09 | -187.15 | 59.82 | 66.37 |
| 101.17 | 88.39 | 6.54 | 26.91 |
| 25.50 | -81.04 | -21.57 | 2.85 |
| 9.88 | 59.31 | 109.03 | 1.33 |

a Scenery　　b 图 4a 左上角的 4×4 子块对应的 DCT 系数

| | | | |
|---|---|---|---|
| 522.87 | -36.4 | -101.53 | 78.26 |
| 327.81 | 109.60 | 52.23 | 12.81 |
| 112.37 | 91.17 | -28.06 | 7.79 |
| 23.55 | 69.13 | 8.21 | 1.72 |

c Scenery　　d 图 4c 左上角的 4×4 子块对应的 DCT 系数

图 4　输入明文

Fig.4 Input plaintext

3）利用 $I_1$，$I_2$…对应的 DCT 系数矩阵 $\boldsymbol{M}_1$，$\boldsymbol{M}_2$，$\boldsymbol{M}_3$…$\boldsymbol{M}_n$，构建迭代复数机制：

$$\boldsymbol{A}_1=\boldsymbol{M}_1+\boldsymbol{M}_2\mathrm{j} \tag{11}$$

$$\boldsymbol{A}_2=\boldsymbol{A}_1+\boldsymbol{M}_3\mathrm{j} \tag{12}$$

$$\boldsymbol{A}_{n-1}=\boldsymbol{A}_{n-2}+\boldsymbol{M}_n\mathrm{j} \tag{13}$$

式中：$\boldsymbol{A}_i$ 为一个复数矩阵；$\boldsymbol{M}_i$ 为第 $i$ 个 DCT 系数矩阵；$\mathrm{j}=\sqrt{-1}$，为复数参量。

4）依据如下的 DCT 逆变换，把矩阵 $\boldsymbol{A}_{n-1}$ 复原为融合图像 $I_{\mathrm{F}}$，见图 5。DCT 逆变换函数为[14]：

$$f(x,y)=S(u)S(v)\sqrt{\frac{2}{mz}}\cdot\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}C(u,v)\cos\left[\frac{\pi}{m}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{z}v\left(y+\frac{1}{2}\right)\right] \tag{14}$$

图 5　融合图像

Fig.5 Fusion image

## 3.2　调制掩码的生成

对于光学加密而言，调制掩码至关重要，在当前的光学加密方法中，大都是采用随机相位掩码作为调制掩码来实现图像的加密，这种随机相位掩码容易引起严重的光轴对准问题[15]，从而削弱了密文的抗破译能力。在光学加密中，其光电混合装置中含有较多的

光学元器件，如透镜，空间光调制解调器、分束器等，由于这些元器件的制造与安装误差，在实际应用中，这些元件的光轴不能对齐，从而影响了光学调制参数与光束强度，限制了系统的加密性能，因此，在文中的光学加密算法中，融合 Hilbert 变换[17]与波带片相位模型，构建一个新的调制掩码，充分发挥二者的光学特点来解决光电装置中的光轴校准问题。Hilbert 变换的任意径向线的相对半部存在一个 $P\pi$ 弧度的相对位误差[15]，这种弧度具有较好的容错能力，可以通过调整 Hilbert 变换的阶数 $P$ 的大小来改变 $P\pi$ 弧度，使其与其他光学元器件的光轴对准，从而有助于对准光学装置的轴线，其模型为[15]：

$$H(r,\varphi)=\exp[\mathrm{i}P\varphi] \tag{15}$$

其中，$P$ 为阶数；$(r,\varphi)$为 Cartesian 坐标：

$$\begin{cases} r=x^2+y^2 \\ \theta=\arctan(y/x) \end{cases} \tag{16}$$

另外，波带片相位中存在一个聚焦环，在光电混合结构中，通过调整每个光学器件的光轴，使之与聚焦环对齐，可以提高光学加密装置的光轴对准度，因此，把它当作衍射光学元件，可改善系统的光轴校准度[16]：

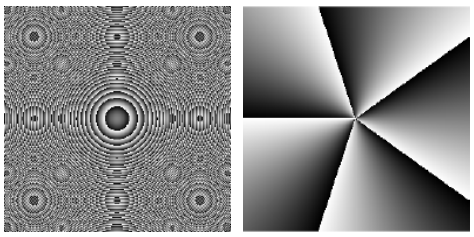
$$R(r,\varphi)=\exp\left[-\frac{\mathrm{i}\pi}{\lambda g}r^2\right] \tag{17}$$

式中：$\lambda$ 为光波波长；$g$ 为透镜焦距。

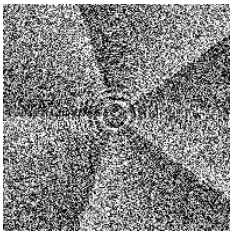
通过 $H(r,\varphi)$，$R(r,\varphi)$，构建新的光学调制掩码：

$$S(r,\varphi)=\exp\left[\mathrm{i}\left(P\varphi-\frac{\pi}{\lambda g}r^2\right)\right] \tag{18}$$

采用文献[15—16]中的光学参数，取 $P$=1，$r$=3，$g$=40 mm，$\lambda$=632.8 mm，并依据式（15—18），所得到的 $H(r,\varphi)$，$R(r,\varphi)$，$S(r,\varphi)$分别见图 6a—c。



a $R(r,\varphi)$　　b $H(r,\varphi)$



c $S(r,\varphi)$

图 6　光学调制掩码的生成

Fig.6 Generation of optical modulation mask

## 3.3　基于圆柱衍射域的相位截断机制的图像同步加密

通过上述得到的光学调制掩码，记为 FPM；借助前文描述的圆柱衍射域的相位截断机制，对融合图像实施加密：

$$E(\theta_r,z_r)=PT\{CyD_R[I_{\mathrm{F}}\cdot \mathrm{F}_{\mathrm{PM}}]\} \tag{19}$$

$$Q(\theta_r,z_r)=PR\{CyD_R[I_{\mathrm{F}}\cdot \mathrm{F}_{\mathrm{PM}}]\} \tag{20}$$

式中：$PT$ 为相位截断操作；$PR$ 为相位保留操作；$E(\theta_r,z_r)$为输出密文；$Q(\theta_r,z_r)$为私钥；$\mathrm{F}_{\mathrm{PM}}$ 代表光学调制掩码 FPM。

以图 5 所示的融合图像为样本，基于图 6c，通过式（19—20）以及图 7 所示的光学结构，形成的密文与私钥分别见图 8a 和图 8b。依图 8a 发现，融合图像经过圆柱衍射域的相位截断处理后，输出的密文充分隐蔽了其信息，人眼无法从中获取任何明文的信息，具备较高的保密性。

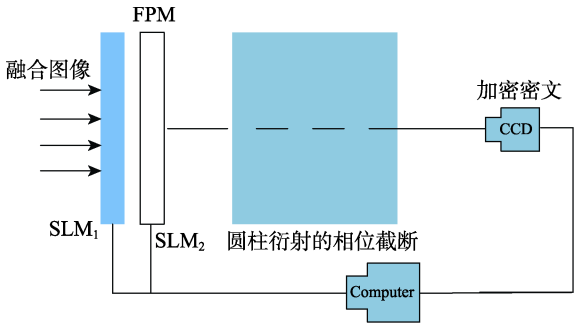
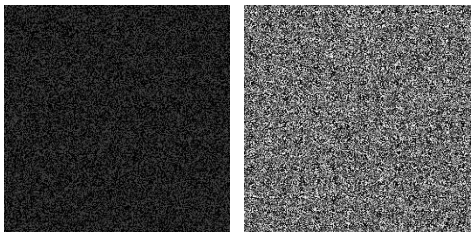



图 7　光电混合装置

Fig.7 Photoelectric hybrid device



a 密文　　b 私钥

图 8　光学加密结果

Fig.8 Optical encryption results

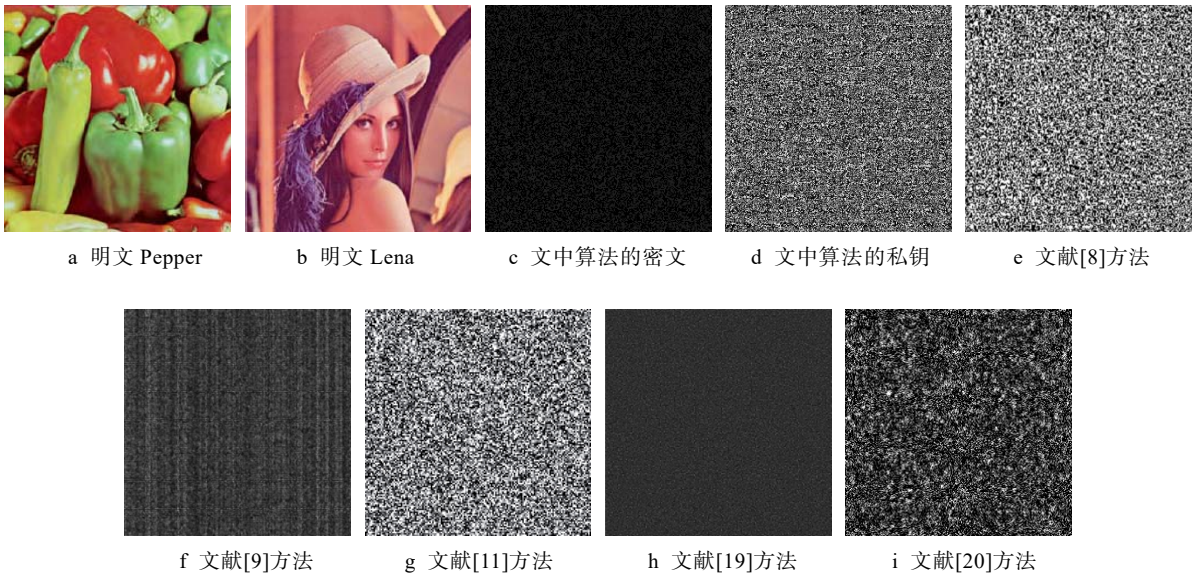
## 4　实验结果与分析

为了测试所提多目标光学同步加密算法的优势，根据 Matlab 软件来完成加密测试，并将安全度较高、新颖的加密方法视为对比组，即文献[8]、文献[9]、文献[11]、文献[19]和文献[20]，其均为多图像光学同步加密算法，仿真平台也是 Matlab，具备较好的可比性。其中，文献[11]通过利用压缩感知处理每个明文，并引入正交编码来融合每个压缩图像，形成单幅图

像，并借助双随机相位编码来实现多图像的同步加密，其采用压缩感知与双随机相位编码是当前较为经典且常用的方法，可获得较好的加密安全性，是一种经典的光学加密方法。文献[19]算法将每个明文分解为 2 个纯相位图像，分别视为密钥图像与解密密钥，并把密钥图像均等分割为 4 个部分，通过 4 阶 Hadamard 矩阵与多个光束干涉来处理密钥图像的 4 个部分，形成编码密文，通过组合所有明文对应的编码密文，获取加密结果。这种算法通过信息分割，较好地破坏了密文的线性关系，且采用的 Hadamard 矩阵可以增强密文的随机性，可以获取安全性较高的密文，具备较好的代表性与新颖性。文献[20]算法是利用正交基矩阵来调制压缩感知，以此对每个明文进行数据压缩，通过组合这些压缩信号，形成一个复合随机信号，再利用双随机相位编码方法随机信号实施加密，其采用的双随机相位编码方法是较为经典的光学加密方法，且对传统的压缩感知进行了改进，具有较好的代表性。通过多次试验，取一组较优的参数为：受限等距常量 $\delta_k$=0.65、入射光的波数 $k$=0.314、子块尺寸 $n\times n$=4×4，$P$=1，$r$=3，$g$=40 mm，$\lambda$=632.8 mm。

## 4.1 光学加密测试

将图 8a、8b 当作此次多图像同步加密的源数据，通过所提算法和文献[8]、文献[9]、文献[11]、文献[19]和文献[20]的加密算法，对二者完成光学调制，得到各自的密文数据见图 8c—i。通过观察输出数据发现，虽然这 6 种算法的输出形式存在较大差异，但其都可成功地实现多图像同步加密，较好地隐秘了所有明文数据，肉眼难以从中获取任何有关线索，具备较高的保密性。另外，采用信息熵值[1]与相邻像素间的相关系数[18]来客观量化 3 个密文的安全度高低，测试数据见表 1 和图 10。通过对比表 1 中的熵值发现，所提算法的输出密文安全度更高，对应的熵值最大，约为 7.998，文献[19]也具有较高的安全性，与所提算法接近，其对应的熵值为 7.995，二者非常接近理论值 8，文献[8]、文献[9]、文献[11]、文献[20]这 4 种算法的熵值都要低于所提算法，分别是 7.984，7.993，7.989，7.992。另外，从图 10 与表 3 中可知，明文图像的相邻像素间的相关性非常高，所有像素堆积为一条对角线，二者的相关系数与 1 非常接近，所提算法输出密文的像素分布更为均匀，没有像素堆积与空洞效应，见图 10c，其相邻像素间的相关系数最低，约为 0.0012。文献[19]算法的输出密文的像素分布也较为均匀，其相关系数为 0.027，见图 10d。文献[9]、文献[20]算法的密文像素分布均匀性要低于所提算法与文献[19]，其存在轻微的空洞现象，见图 10f、图 10g，二者的相邻像素间的相关系数分别为 0.0034，0.0051。文献[8]、文献[11]的输出密文像素分布均匀性较差，存在像素堆积与空洞效应，见图 10c、图 10e，二者的相邻像素间的相关系数分布为 0.0095，0.0067。可见，与文献[8]、文献[9]、文献[11]、文献[19]和文献[20]相比较而言，所提多目标同步加密算法的安全度更理想。原因是所提同步加密算法利用了联合 Hilbert 变换与波带片相位模型来构建了一个新的调制掩码，将其至于光电装置中，能够解决光轴校准问题，而且引入圆柱衍射域的相位截断机制，对融合图像实施加密，增强了密文的非线性特性，充分破坏了加密系统的线性特征。文献[19]通过将明文分解为 2 个纯相位图像，并将其进行均等分割，通过 4 阶 Hadamard 矩阵对分割子图像实施差异调制，可以



a 明文 Pepper　b 明文 Lena　c 文中算法的密文　d 文中算法的私钥　e 文献[8]方法

f 文献[9]方法　g 文献[11]方法　h 文献[19]方法　i 文献[20]方法

图 9 不同加密算法的输出密文

Fig.9 Output ciphertext of different encryption algorithms

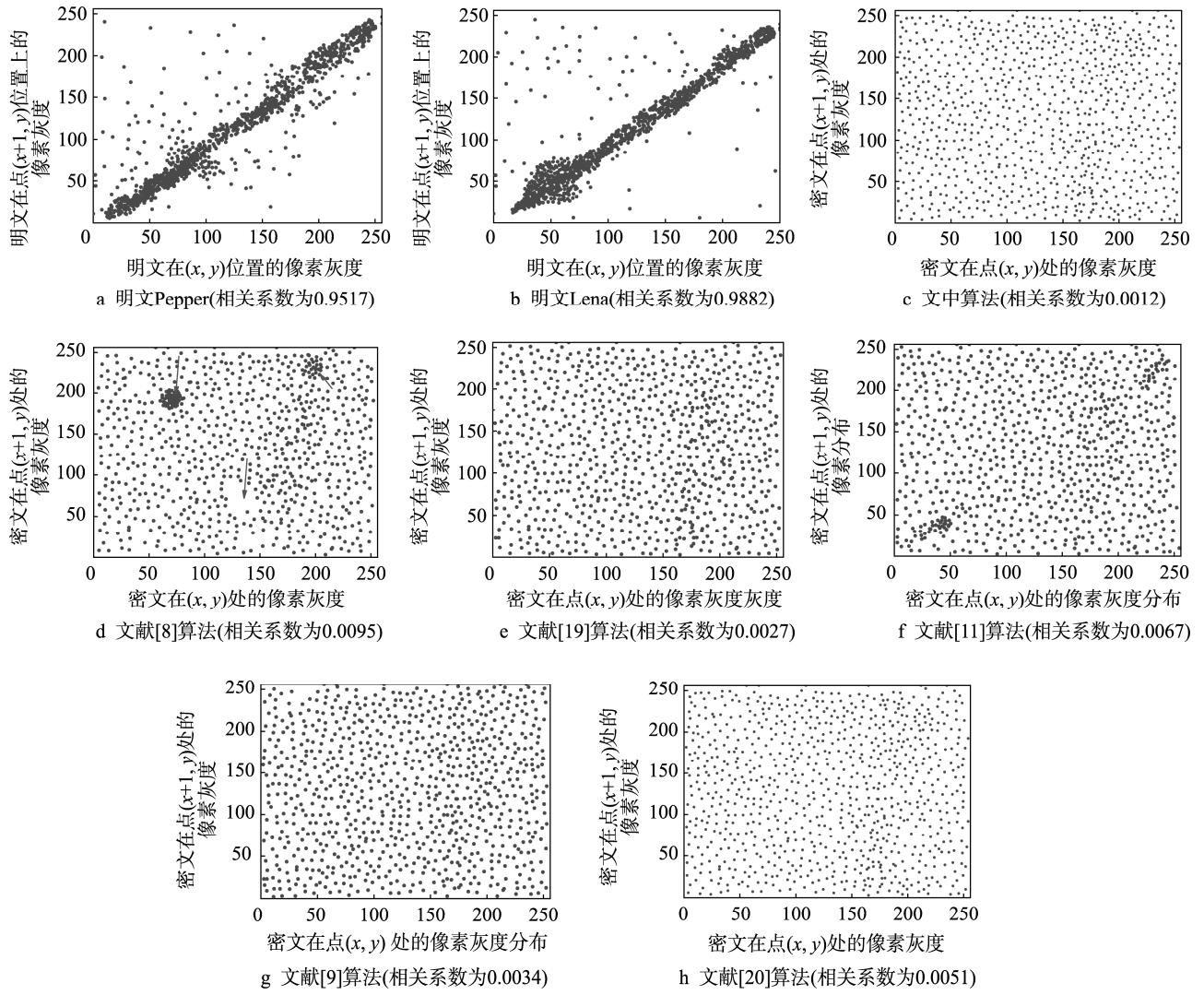



图 10　不同算法输出密文的相邻像素间的相关系测试

Fig.10 Correlation between adjacent pixels of ciphertext output by different algorithms

**表 1　密文熵值测试**

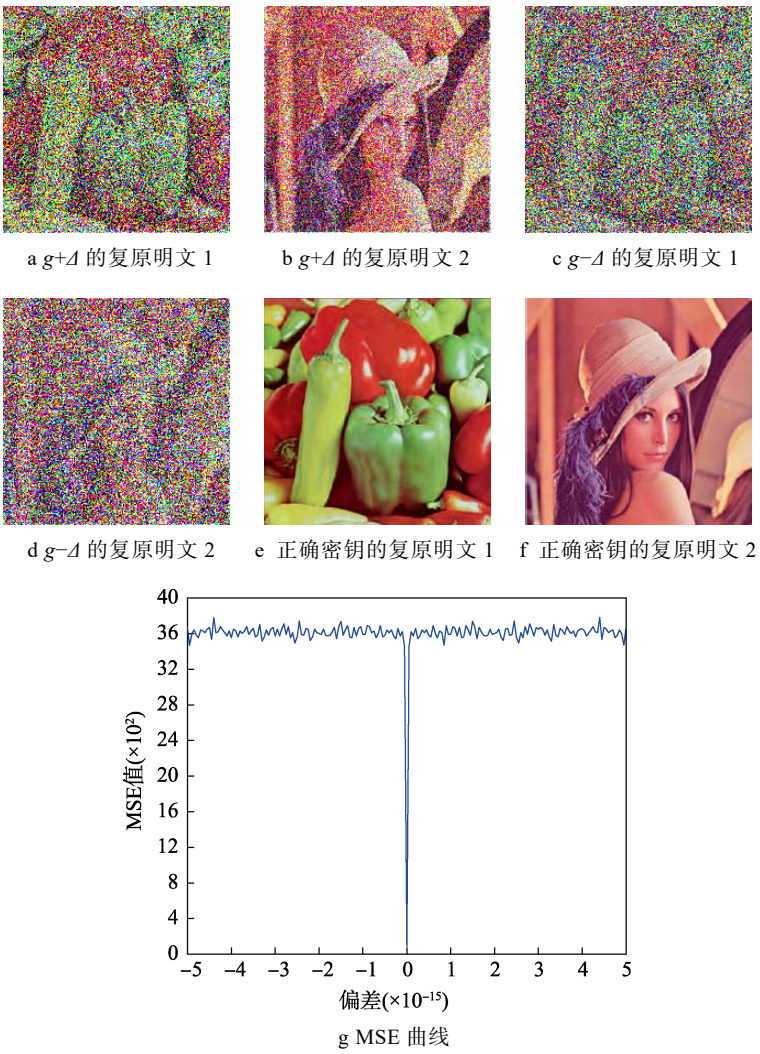
**Tab.1 Entropy test of ciphertext**

| 算法名称 | 密文熵值 | 相关系数 |
|---|---|---|
| 文中算法 | 7.998 | 0.0012 |
| 文献[8] | 7.984 | 0.0095 |
| 文献[9] | 7.993 | 0.0034 |
| 文献[11] | 7.989 | 0.0067 |
| 文献[19] | 7.995 | 0.0027 |
| 文献[20] | 7.992 | 0.0051 |

较好地增强加密系统的随机性，改善密文的非线性特性，然而，此算法主要是依赖多个光束的干涉来实现图像加密，使得所有信息被完全保留在 POMS 中，易导致隐式轮廓显现问题，在一定程度上削弱了密文安全性。文献[8]虽然采用了切割与拼接技术来破坏密文的线性特征，但是在光学调制时，是采用了普通的混沌相位掩码，容易引起严重的光轴校准问题，使其安全性不理想。文献[9]则是根据小波谱系数的不同特征，将 4 幅图像的高频分量和低频分量分别合并为高频融合图像和低频融合图像，通过菲涅耳域中的相位截断和相位保留操作来获取密文，相对于文献[8]而言，其密文的非线性特性更高，但是，该算法也是将随机掩码置于光制解调器后，无法校准光轴，限制其安全性。文献[11]和文献[20]这 2 种算法均是采用压缩感知与双随机相位掩码来完成多图像的光学加密，但是，这种双随机相位掩码都是普通的随机掩码，虽然可以改善密文的随机性，但是当光束作用于相位掩码上，由于这种随机掩码缺乏校正能力，使得光电装置中的光学元件不能对齐，影响了光学调制的参数，从而降低了系统的加密性能，使其密文安全性不佳。文献[11]和文献[20]是采用 2 个不同的随机掩码，而且均采用了正交矩阵对初始明文信号进行了处理，相对于文献[8]而言，其加密系统具有更好的随机性，因此，二者的密文安全性也要高于文献[8]。

## 4.2　密钥敏感性测试

密钥敏感性是评估当前加密算法安全性的常用手段，也就是满足严格的“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[2]。故在此次试验中，验证了焦距 $g$=40 mm 的敏感性。借助一个固定偏差值 $\Delta=10^{-15}$ 来修改 $g$ 值，获取 $g+\Delta$，$g-\Delta$；并联合私钥等其他密钥，对图 10c 实施复原，输出数据见图 11。由测试数据发现，当加密系统中的一个密钥出现了 $10^{-15}$ 这种级别的变化时，仍然不能得到正确的明文内容，这 2 组错误密钥的复原质量较差，均呈现重度噪声破坏图像，分别见图 11a—d，且其相应的 MSE 值均超过了 3500。当所有的密钥均无误时，才可得到完整清晰的明文，对应的 MSE 值与零非常接近，见图 10e—f。该组实验数据显示了所提光学加密算法具备严格的“雪崩效应”。




a $g+\Delta$ 的复原明文 1　b $g+\Delta$ 的复原明文 2　c $g-\Delta$ 的复原明文 1

d $g-\Delta$ 的复原明文 2　e 正确密钥的复原明文 1　f 正确密钥的复原明文 2

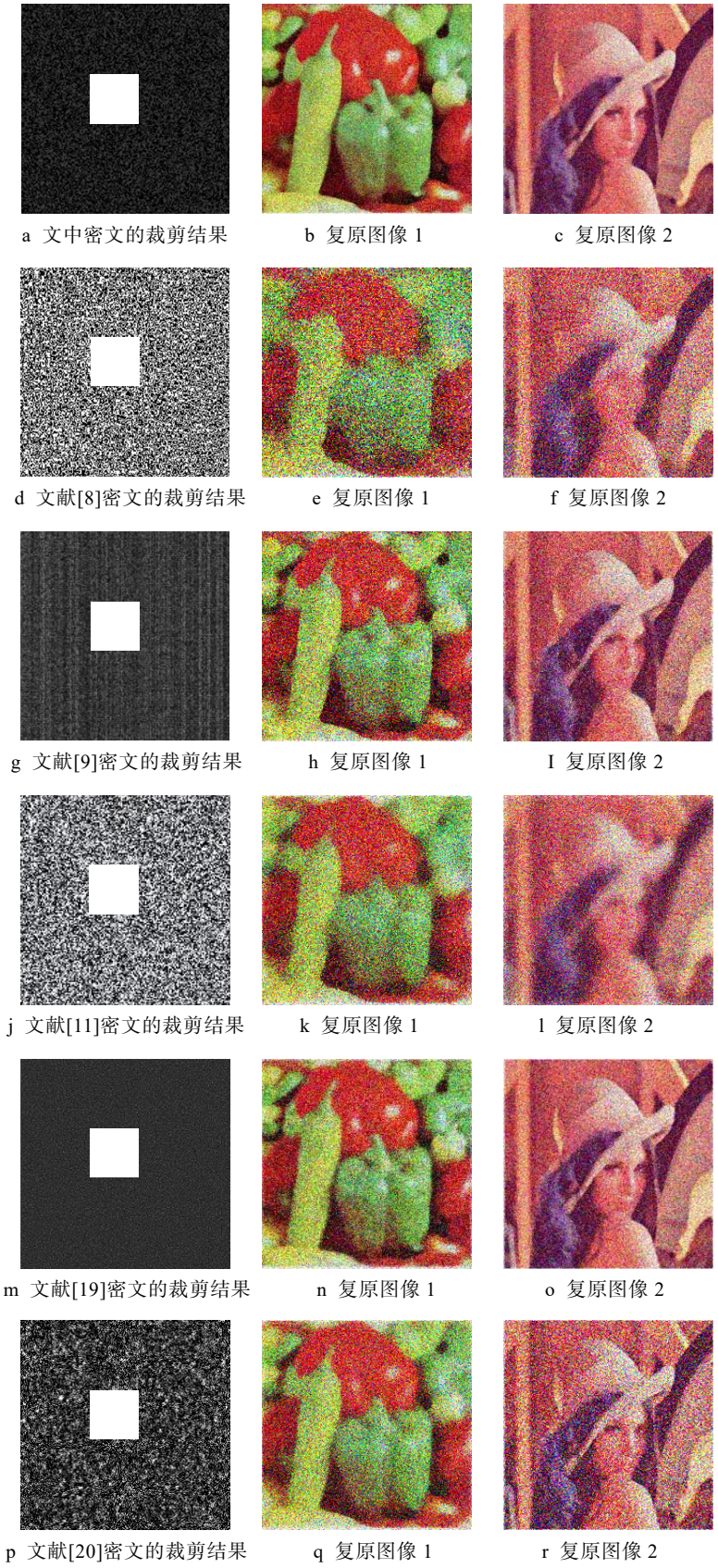
g MSE 曲线

图 11　所提光学加密算法的敏感性测试

Fig.11 Sensitivity testing of the optical encryption algorithm

## 4.3　抗裁剪攻击能力测试

裁剪攻击是评估加密系统的安全性的重要指标[17]。在此次测试中，以图 10c、图 10e—i 为样本，对三者实施裁剪，分别见图 12a，d，g，j，m，p；再借助所提加密算法、文献[8]与文献[9]对其复原，输出数据见图 12。根据复原数据发现，对于裁剪攻击，所提光学加密算法呈现出更强的鲁棒性，输出的复原图像虽然丢失了部分信息，但其质量尚可接受，轮廓等信息较为清晰完整，见图 12b—c。文献[19]算法的复原图像也具有较好的质量，见图 12n—o。文献[11]、文献[20]、文献[9]的复原图像质量都要优于文献[8]，但其图像模糊，轮廓等信息完整度要低于所提算法与文献[19]，见图 12k—l，图 12q—r、图 12h—i。文献[8]的复原质量最低，无法看到明文的轮廓内容，见图 12e—f。为了客观评估这些算法的抵御裁剪攻击能力，文中引用结构相似度（structural similarity index, SSIM）[21]，计算了复原图像与初始图像之间的



a 文中密文的裁剪结果　b 复原图像 1　c 复原图像 2
d 文献[8]密文的裁剪结果　e 复原图像 1　f 复原图像 2
g 文献[9]密文的裁剪结果　h 复原图像 1　I 复原图像 2
j 文献[11]密文的裁剪结果　k 复原图像 1　l 复原图像 2
m 文献[19]密文的裁剪结果　n 复原图像 1　o 复原图像 2
p 文献[20]密文的裁剪结果　q 复原图像 1　r 复原图像 2

图 12 不同算法的抗裁剪攻击能力测试
Fig.12 Test of resistance to clipping attack of different algorithms

相似程度，若 SSIM 越大，与接近理论值“1”，则表明复原质量越好。6 种算法的复原图像与初始图像之间的 SSIM 值见表 2。由表 2 发现，所提算法和文献[19]的复原质量较好，二者的 SSSIM 值均维持在 0.9

左右，但是，所提算法的 SSIM 仍然要高于文献[19]，分别为 0.9312，0.9159。文献[8]的复原图像与初始图像之间的 SSIM 值最小，分别为 0.5982，0.5817。主要原因是所提算法采用了 Hilbert 变换与波带片相位模型所构成的融合掩码来调制图像，有效解决了光轴对准问题，而且借助相位截断机制来破坏其输出密文的线性特征，从而增强了其抗攻击能力，另外，在实施多图像融合时，所提算法是一种无损融合，通过迭代复数模型，将所有的明文内容实施组合，有助于图像复原。文献[19]、文献[20]、文献[11]以及文献[9]在进行多图像融合时，均是采用了无损融合方法，但其采用了随机相位掩码，导致加密系统无法解决光轴校准问题，使得光电混合装置中的各个光学元件的光轴不能对其，影响了光学调制参数，从而使其安全性不理想，削弱了密文抵御裁剪攻击的能力，导致其复原质量有待提高。文献[8]采用信息切割与拼接来实施多图像的融合，为一种信息有损组合方法，而且加密系统也存在光轴校准问题，从而导致复原质量较差。

表 2 不同算法的复原图像的结构相似度测试

**Tab.2 Structural similarity testing of restored images based on different algorithms**

| 算法名称 | 图像 | SSIM |
|---|---|---|
| 文中算法 | 复原 Pepper 图像 | 0.9312 |
| | 复原 Lena 图像 | 0.9159 |
| 文献[8]算法 | 复原 Pepper 图像 | 0.5982 |
| | 复原 Lena 图像 | 0.5817 |
| 文献[9]算法 | 复原 Pepper 图像 | 0.8723 |
| | 复原 Lena 图像 | 0.8554 |
| 文献[11]算法 | 复原 Pepper 图像 | 0.6212 |
| | 复原 Lena 图像 | 0.5903 |
| 文献[19]算法 | 复原 Pepper 图像 | 0.9086 |
| | 复原 Lena 图像 | 0.9025 |
| 文献[20]算法 | 复原 Pepper 图像 | 0.8491 |
| | 复原 Lena 图像 | 0.8257 |

## 5 结语

为了实现多图像的同步加密，降低系统的存储空间，文中基于圆柱衍射域的相位截断与离散余弦变换的多图像光学加密算法。联合压缩感知与 DCT 变换，对各个明文实施压缩与分解，形成相应的 DCT 系数矩阵；为了最大程度地保留明文信息，实现无损融合，文中定义了迭代复数方法，将所有系数矩阵组合为一个复矩阵，再基于 DCT 逆变换，得到复合图像。为了消除光电装置中的光轴对准问题，该算法采用 Hilbert 变换与波带片相位函数来建立一个新的调制掩码；最后，通过圆柱衍射域的相位截断机制，对复合图像完成加密，将幅度部分视为密文，便于管理与传输。测试数据显示所提算法具备较为理想的保密安全性与敏感性，能够有效抵御裁剪攻击。

在所提光学同步加密算法中，忽略了明文内容特性，导致其抗明文破译能力不理想。在后续研究计划中，将引入 Hash-256 方法与混沌映射来改进光学调制掩码，在解决光轴校准问题的同时也增加其随机性，进一步优化密文的安全性；并融入考虑快速响应码，进一步优化密文的抗裁剪攻击能力。

**参考文献：**


[1] 郭静博, 王彦超, 周丽宴. 基于离散分数阶角变换与关联混沌映射的双图像加密算法[J]. 量子电子学报, 2017, 34(4): 420—431.
GUO Jing-bo, WANG Yan-chao, ZHOU Li-yan. Double Image Encryption Algorithm Based on Discrete Fractional Order Angle Transformation and Associated Chaotic Map[J]. Quantum Electronic Journal, 2017, 34(4): 420—431.

[2] 郭静博. 基于物理随机位生成器与混沌像素交叉互换的图像加密算法[J]. 包装工程, 2018, 39(13): 222—232.
GUO Jing-bo. Image Encryption Algorithm Based on Physical Random Bit Generator and Chaotic Pixel Cross Interchange[J]. Packaging Engineering, 2018, 39(13): 222—232.

[3] 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 Fei-bo. Optical Image Encryption Algorithm Based on Coherent Superposition and Modulus Equal Vector Decomposition[J]. Journal of Electronics and Information, 2018, 40(2): 438—446.

[4] CHAI Xiu-li, ZHENG Xiao-yu, GAN Zhi-hua. An Image Encryption Algorithm Based on Chaotic System and Compressive Sensing[J]. Signal Processing, 2018, 148(19): 124—144.

[5] WANG Xing-yuan, ZHU Xiao-qiang, WU Xiang-jun. Image Encryption Algorithm Based on Multiple Mxed Hash Functions and Cyclic Shift[J]. Optics and Lasers in Engineering, 2018, 107(8): 370—379.

[6] GHEBLEH M, KANSO A, STEVANOVIC D. A Novel Image Encryption Algorithm Based on Piecewise Linear Chaotic Maps and Least Squares Approximation [J]. Multimedia Tools and Applications, 2018, 77(6): 7305—7326.

[7] 张红梅, 张智高, 裴志利. 基于迭代复数模型的多图像无损同步加密算法研究[J]. 科学技术与工程, 2014, 14(26): 123—130.
ZHANG Hong-mei, ZHANG Zhi-gao, PEI Zhi-li. Study on Synchronous Lossless Encryption Algorithm

for Multi-Image Based on Iteration Plural Model[J]. Science Technology and Engineering, 2014, 14(26): 123—130.

[8] PAN Shu-min, WEN Ru-hong, ZHOU Zhi-hong. 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.

[9] CHEN Xu-dong, 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.

[10] CHAI Xiu-li, GAN Zhi-hua, CHEN Yi-ran. A Visually Secure Image Encryption Scheme Based on Compressive Sensing[J]. Signal Processing, 2017, 134(9): 35—51.

[11] HUO Dong-ming, ZHOU Xin, ZHANG Luo-zhi. Multiple-Image Encryption Scheme Via Compressive Sensing and Orthogonal Encoding Based on Double Random Phase Encoding[J]. Journal of Modern Optics, 2018, 65(18): 2093—2102.

[12] WANG Jun, LI Xiao-wei, HU Yu-hen. Phase-retrieval Attack Free Cryptosystem Based on Cylindrical Asymmetric Diffraction and Double-Random Phase Encoding[J]. Optics Communications, 2018, 410(29): 468—474.

[13] JI Xiao-yong, BAI Sen, ZHU Gui-bin. Image Encryption and Compression Based on the Generalized Knight's Tour, Discrete Cosine Transform and Chaotic Maps[J]. Multimedia Tools and Applications, 2017, 76(10): 12965—12979.

[14] MOHAMMED H A, GHAZALI S, TANZILA S. Detection of Copy-move Image Forgery Based on Discrete Cosine Transform[J]. Neural Computing and Applications, 2018, 30(1): 183—192.

[15] 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 Jian-jun, LIANG Li-li, ZHANG Fu-quan. Optical Image Encryption Based on Hybrid Phase Mask and Gyrator Wavelet Transform[J]. Optical Technology, 2018, 44(6): 717—726.

[16] ZHAO Meng-dan, GAO Xu-zhen, PAN Yue. Image Encryption Based on Fractal-structured Phase Mask in Fractional Fourier Transform Domain[J]. Journal of Optics, 2018, 20(4): 45703—45711.

[17] 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 Component Expansion and Gyrator Transform Domain Phase Retrieval[J]. Journal of Electronic Measurement and Instrument, 2017, 31(6): 876—884.

[18] 徐嵩松, 蒲斌. 基于8方向折叠与自更新置乱的图像加密算法[J]. 西南大学学报(自然科学版), 2018, 40(4): 139—150.
XU Song-song, PU Bin. Image Encryption Based on Eight Directions Folding and Self-Updating Scrambling[J]. Journal of Southwest University (Natural Science Edition), 2018, 40(4): 139—150.

[19] YOUHYUN K, JAEHUM S, INKYU M. Interference-Based Multiple-Image Encryption Using Binary Phase Masks[J]. Optics & Lasers in Engineering, 2018, 107(8): 281—287.

[20] ZHANG Luo-zhi, ZHOU Yuan-yuan, HUO Dong-ming. Multiple-Image Encryption Based on Double Random Phase Encoding and Compressive Sensing by Using a Measurement Array Preprocessed with Orthogonal-basis Matrices[J]. Optics Communications, 2016, 361(15): 6—12.

[21] 耿卫江. 结构相似度索引耦合最优稀疏表示的大规模损坏图像动态修复[J]. 科学技术与工程, 2013, 14(25): 107—114.
GENG Wei-jiang. Study on the Large-scale Damage Image Inpainting Mechanism Based on Structural Similarity Index Coupled Optimal Sparse Representations[J]. Science and Technology and Engineering, 2013, 14(25): 107—114.