第 58 卷 第 4 期/2021 年 2 月/激光与光电子学进展 研究论文

激光与光电子学进展 先进成像

# 结合 Fourier 变换对称性和随机多分辨率奇异值分解的彩色图像加密

王雪[1]，邵珠宏[1*]，王云飞[2]，尚媛园[1,2,3]

[1] 首都师范大学信息工程学院，北京 100048；

[2] 首都师范大学物理系，北京 100048；

[3] 北京成像理论与技术高精尖创新中心，北京 100048

**摘要** 提出一种基于 Fourier 变换对称性和随机多分辨率奇异值分解(R-MRSVD)的彩色图像加密算法。首先计算归一化明文图像的平均值作为 logistic-exponent-sine 映射的初值，并生成随机矩阵和位置索引；然后对每个颜色通道分别进行二维离散 Fourier 变换，根据共轭对称性仅保留一半的频谱系数，并提取实部分量和虚部分量构建实数矩阵；最后对实数矩阵进行 R-MRSVD 和 Josephus 置乱操作，得到密文图像。将明文图像的像素特征作为混沌序列的初值，保证算法具有高敏感性和高安全性，同时实值的密文便于存储和传输。对算法的解密图像质量、统计特性、密钥敏感性、抗选择明文攻击、鲁棒性等性能进行测试，仿真结果表明，所提加密算法具有可行性和安全性。

**关键词** 图像处理；彩色图像加密；Fourier 变换；随机多分辨率奇异值分解；LES 映射；Josephus 置乱

**中图分类号** TP309.7 **文献标志码** A **doi**：10.3788/LOP202158.0410021

# Color Image Encryption Based on Symmetry of Fourier Transform and R-MRSVD

Wang Xue[1], Shao Zhuhong[1*], Wang Yunfei[2], Shang Yuanyuan[1,2,3]

[1] *Information Engineering College, Capital Normal University, Beijing* 100048, *China*;

[2] *Department of Physics, Capital Normal University, Beijing* 100048, *China*;

[3] *Beijing Advanced Innovation Center for Imaging Theory and Technology, Beijing* 100048, *China*

**Abstract** In this study, a color image encryption algorithm is proposed based on the symmetry of Fourier transform and random multiresolution singular value decomposition (R-MRSVD). First, the average value of normalized plaintext images is considered to be the initial value of logistic-exponent-sine mapping. Thus, a random matrix and position index are generated. Then, a two-dimensional discrete Fourier transform is applied to each color channel. Because of the conjugate symmetry property of Fourier transforms, only half of the Fourier transform spectrum coefficients are preserved. Further, a real matrix is constructed by extracting the real and imaginary parts. Finally, R-MRSVD is performed, and the ciphertext image is obtained using Josephus scrambling operation. The pixel characteristic of the plaintext image is considered to be the initial value of the chaotic sequence; thus, the high sensitivity and security of the algorithm can be ensured. The real-valued ciphertext image is convenient for storage and transmission. The quality of the decrypted image, statistical characteristic, key sensitivity, chosen-plaintext attack, and robustness of the algorithms are verified. The simulation results demonstrate the feasibility and security of the proposed color image encryption algorithm.

**Key words** image processing; color image encryption; Fourier transform; R-MRSVD; logistic-exponent-sine

**收稿日期**：2020-07-10；**修回日期**：2020-07-22；**录用日期**：2020-08-13

**基金项目**：国家自然科学基金(61876112,61601311)

* **E-mail**：zhshao@cnu.edu.cn

mapping; Josephus scrambling
**OCIS codes** 100.4998; 070.0070; 070.2615

## 1 引 言

如今，随着网络通信和多媒体技术的快速发展，数字图像成为互联网内容和应用中的主要交互对象之一。由于网络的共享性，图像传播方便的同时也面临着恶意篡改、非法传播等安全问题[1-2]。

自双随机相位编码技术提出以来，图像加密技术得到不断发展。双随机相位编码技术在空域和 Fourier 变换域使用随机相位掩模，从而将视觉上可理解的图像调制为一幅类似白噪声的图像。为了增加系统的安全性，随后包含变化参数的变换不断被引入到图像加密算法中。文献[3]使用 Shearlet 变换对明文图像进行分解，再结合螺旋相位变换得到密文。Kaur 等[4]提出一种基于分数变换和置乱的加密算法，该算法利用多模态生物特征密钥对图像进行加密，增强了密钥安全性。文献[5]提出 Gyrator 变换域下的光学多图像认证，利用分数阶超混沌系统提高算法的安全性。Tao 等[6]提出一种基于 Fresnel 变换域奇异值分解的光学图像密码系统，该系统利用掌纹相位掩模生成生物特征密钥，提高数据安全性。Yu 等[7]提出一种结合短时分数阶 Fourier 变换的图像加密算法，超混沌系统有效地增大了密钥空间。Wang 等[8]使用分数阶 Mellin 变换实现图像加密。然而，这些算法主要解决灰度图像的内容保护和安全传输问题。

彩色图像提供了比灰度图像更为丰富的信息，因此彩色图像的加密受到人们越来越多的关注。Kang 等[9]提出一种基于空间域和保实多参数离散分数角度变换域的彩色图像加密算法。Faragallah 等[10]提出一种使用分数阶 Fourier 变换和二维 logistic 映射进行彩色图像加密的方案，但是在该方案下，复数值形式的密文不便于存储和传输。Wang 等[11]使用 Fresnel 域的相位截断和随机幅值掩模进行彩色图像加密。Xiong 等[12]提出一种联合相移干涉和随机分解的彩色图像加密方法，但是此方法在彩色明文图像转换成索引格式的过程中存在颜色信息丢失的问题。Chen 等[13]将彩色明文图像拼接成单通道图像，并使用 Ushiki 映射和等模分解进行彩色图像加密。Yao 等[14]设计了一种基于推导 gyrator 变换的彩色图像加密方法。Kumar 等[15]使用多分辨率奇异值分解和离散余弦 Stockwell 变换构建彩色图像加密方案。刘禹佳等[16]利用矢量运算和副像相位掩模对彩色遥感图像进行加密，降低系统运算复杂度。陶珊等[17]提出一种基于矢量分解和混沌随机相位掩模编码的光学非对称彩色图像加密系统。

本文提出一种结合 Fourier 变换对称性和随机多分辨率奇异值分解(R-MRSVD)的彩色图像加密算法。该算法首先对彩色图像的每个颜色通道分别进行离散 Fourier 变换(DFT)，然后保留一半的频谱系数并构造实数矩阵，最后进行随机多分辨率奇异值分解和 Josephus 置乱，从而得到密文。

## 2 基本原理

### 2.1 Logistic-exponent-sine(LES)映射

Hua 等[18]提出一种基于指数混沌模型框架的 LES 映射，该映射具有更好的鲁棒性，定义为

$$x_{i+1}=\left[4ax_i(1-x_i)\right]^{\ln\left[b\sin(\pi x_i)+c\right]}, \tag{1}$$

式中：控制参数 $a\in[0,1]$、$b\in[0,1]$；平衡参数 $c\in[2,2.8]$；$x_i$ 为混沌序列的第 $i$ 个值。所提算法使用 LES 映射生成随机矩阵和位置索引序列。

### 2.2 随机多分辨率奇异值分解

假设图像 $\boldsymbol{I}$ 的尺寸为 $m\times n$，随机多分辨率奇异值分解的具体过程[19]描述为

1) 沿左上角到右下角的方向，将图像 $\boldsymbol{I}$ 划分成非重叠的图像块，每个子块的尺寸为 $p\times q$，把子块排列成 $pq\times1$ 的列向量并组合成一个 $pq\times mn/pq$ 大小的矩阵 $\boldsymbol{I}_1$；

2) 对矩阵 $\boldsymbol{I}_1$ 进行中心化并计算散布矩阵 $\boldsymbol{T}_1=\bar{\boldsymbol{I}}_1\bar{\boldsymbol{I}}_1^{\mathrm{T}}$，$\bar{\boldsymbol{I}}_1$ 为中心矩阵；

3) 对散布矩阵 $\boldsymbol{T}_1$ 进行对角化，即 $\boldsymbol{U}_1^{\mathrm{T}}\boldsymbol{T}_1\boldsymbol{U}_1=\boldsymbol{S}_1^2$，$\boldsymbol{U}_1$ 为特征向量矩阵；

4) 随机化中心矩阵 $\bar{\boldsymbol{I}}_1$，$\boldsymbol{R}$ 是可逆随机矩阵，$\bar{\boldsymbol{I}}_1^{\mathrm{r}}=\boldsymbol{R}\bar{\boldsymbol{I}}_1$，$\bar{\boldsymbol{I}}_1^{\mathrm{r}}$ 为随机化后矩阵；

5) 重构矩阵 $\hat{\boldsymbol{I}}$，$\hat{\boldsymbol{I}}=\boldsymbol{U}_1^{\mathrm{T}}\bar{\boldsymbol{I}}_1^{\mathrm{r}}$。

矩阵 $\hat{\boldsymbol{I}}$ 的第一行对应最大的奇异值，并将其作为原图像的近似部分，即低频分量。剩余细节部分为图像的高频分量。

## 3 加密及解密算法

所提算法流程如图 1 所示，假设待加密的明文

图像 $\boldsymbol{f}(x,y)$，大小为 $M\times N\times 3$，则加密过程如图 1(a)所示。

图 1(b)为解密过程，其中 IDFT、IR-MRSVD 分别表示离散傅里叶逆变换，逆随机多分辨率奇异值分解。加密过程具体如下。

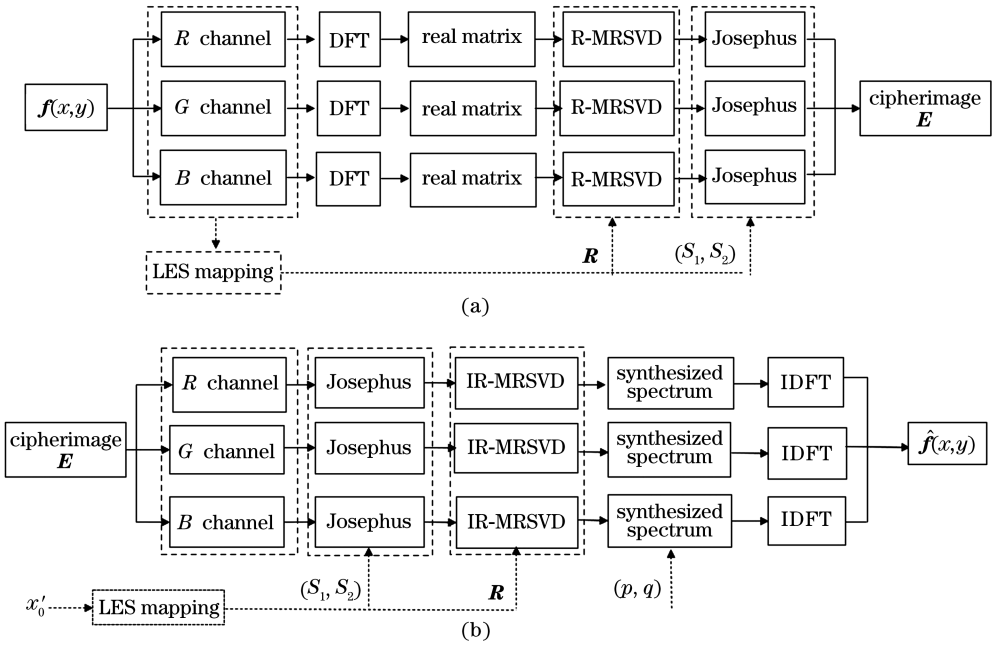


图 1　所提算法的流程。(a)加密过程；(b)解密过程

Fig. 1　Flowchart of the proposed algorithm. (a) Encryption process; (b) decryption process

1) 将明文图像 $\boldsymbol{f}(x,y)$ 分解为 $R$、$G$、$B$ 三个颜色分量 $\boldsymbol{f}_c(x,y)$，$c=[R,G,B]$，然后计算归一化三个通道平均亮度 $x_0$ 并进行取余运算，表达式为

$$x_0'=\mathrm{mod}(x_0,1)。\tag{2}$$

将 $x_0'$ 作为 LES 映射的初值，由(1)式得到长度为 $M+N+4+p^2q^2$ 的序列 $X_i$，$i=p^2q^2+1,\cdots,(M+N+4+p^2q^2)$。

2) 在每个通道分量的第一行和第一列之前各添加一行、一列零向量，然后进行 DFT 并平移得到关于原点共轭对称的复频谱 $\boldsymbol{F}_c$，即 $\boldsymbol{F}_c(u,v)=\boldsymbol{F}_c^*(M+2-u,N+2-v)$。根据共轭对称性，保留复频谱 $\boldsymbol{F}_c$ 左上半部分系数，将 $\boldsymbol{F}_c$ 右下半部分系数置为 0，即

$$\boldsymbol{F}_c^{\mathrm{L}}=\begin{bmatrix} a_{1,1}+\mathrm{j}b_{1,1} & \cdots & a_{1,\frac{N}{2}+1}+\mathrm{j}b_{1,\frac{N}{2}+1} & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ a_{\frac{M}{2},1}+\mathrm{j}b_{\frac{M}{2},1} & \cdots & a_{\frac{M}{2},\frac{N}{2}+1}+\mathrm{j}b_{\frac{M}{2},\frac{N}{2}+1} & \cdots & 0\\ a_{\frac{M}{2}+1,1}+\mathrm{j}b_{\frac{M}{2}+1,1} & \cdots & a_{\frac{M}{2}+1,\frac{N}{2}+1} & \cdots & 0\\ a_{\frac{M}{2}+2,1}+\mathrm{j}b_{\frac{M}{2}+2,1} & \cdots & 0 & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ a_{M+1,1}+\mathrm{j}b_{M+1,1} & \cdots & 0 & \cdots & 0 \end{bmatrix}。\tag{3}$$

3) 分别提取矩阵 $\boldsymbol{F}_c^{\mathrm{L}}$ 的实部分量 $\boldsymbol{D}_{\mathrm{Re}}$ 和虚部分量 $\boldsymbol{D}_{\mathrm{Im}}$，对 $\boldsymbol{D}_{\mathrm{Im}}$ 进行水平和垂直翻转，并与 $\boldsymbol{D}_{\mathrm{Re}}$ 进行叠加得到 $\boldsymbol{G}_c$，即

$$\boldsymbol{G}_c=\boldsymbol{D}_{\mathrm{Re}}+T_1\{T_2\{\boldsymbol{D}_{\mathrm{Im}}\}\},\tag{4}$$

式中：$T_1$、$T_2$ 分别为水平和垂直翻转。

$$\boldsymbol{G}_c=\begin{bmatrix} a_{1,1} & \cdots & a_{1,\frac{N}{2}+1} & \cdots & b_{M+1,1}\\ \vdots & & \vdots & & \vdots\\ a_{\frac{M}{2},1} & \cdots & a_{\frac{M}{2},\frac{N}{2}+1} & \cdots & b_{\frac{M}{2}+2,1}\\ a_{\frac{M}{2}+1,1} & \cdots & a_{\frac{M}{2}+1,\frac{N}{2}+1} & \cdots & b_{\frac{M}{2}+1,1}\\ a_{\frac{M}{2}+2,1} & \cdots & b_{\frac{M}{2},\frac{N}{2}+1} & \cdots & b_{\frac{M}{2},1}\\ \vdots & & \vdots & & \vdots\\ a_{M+1,1} & \cdots & b_{1,\frac{N}{2}+1} & \cdots & b_{1,1} \end{bmatrix}。\tag{5}$$

4) 在实数矩阵 $\boldsymbol{G}_c$ 的第一行、第一列之前各添加一行、一列零向量；将序列 $X_i$ 中的前 $p^2q^2$ 个元素调整为一个 $pq\times pq$ 的随机矩阵 $\boldsymbol{R}$；然后进行参数为 $(p,q)$ 的 R-MRSVD，最终得到 $\boldsymbol{G}_c'$，尺寸为 $(M+2)\times(N+2)$。

5) 将序列 $X_i$ 分成长度为 $(M+2)$、$(N+2)$ 的两个子序列 $S_1(i=p^2q^2+1,\cdots,p^2q^2+M+2)$、$S_2(i=p^3q^3+M+3,\cdots,p^2q^2+M+N+4)$，对子序

列 $S_1$、$S_2$ 分别进行升序和降序排列得到相应的位置索引序列 $L_1$、$L_2$。然后对 $L_1$、$L_2$ 进行报数间隔为 $k_1$、$k_2$ 的 Josephus 遍历得到新的位置索引 $\xi$、$\zeta$，其中 $\xi=1,2,\cdots,M+2$、$\zeta=1,2,\cdots,N+2$。对矩阵 $\boldsymbol{G}_c'$ 进行置乱得到每个通道的相应密文 $\boldsymbol{E}_c$，表达式为

$$\boldsymbol{E}_c[L_1(\xi),L_2(\zeta)]=\boldsymbol{G}_c'(\xi,\zeta)。\tag{6}$$

将每个通道的置乱结果叠加在一起作为最终的彩色密文图像 $\boldsymbol{E}$，其尺寸为 $(M+2)\times(N+2)\times3$。

在加密过程中，将 LES 映射的控制参数 $\{a,b\}$、平衡参数 $c$、初值 $x'_0$、R-MRSVD 的参数 $(p,q)$ 和 Josephus 遍历的起始位置、报数间隔作为恢复明文图像时的密钥。

使用授权的正确密钥，通过上述加密算法的逆过程可以解密出明文图像。解密的具体过程描述如下，流程如图 1(b)所示。

1) 将密文图像 $\boldsymbol{E}(x',y')$ 分解为 $R$、$G$、$B$ 三个颜色分量 $\hat{\boldsymbol{E}}_c(x',y')$。根据密钥生成随机序列构造的位置索引 $\xi$、$\zeta$ 对每个通道进行 Josephus 置乱逆序重排，得到 $\hat{\boldsymbol{G}}_c'$：

$$\hat{\boldsymbol{G}}_c'(\xi,\zeta)=\hat{\boldsymbol{E}}_c[L_1(\xi),L_2(\zeta)]。\tag{7}$$

2) 由密钥生成随机序列构造的随机矩阵 $\boldsymbol{R}$，对矩阵 $\hat{\boldsymbol{G}}_c'$ 进行参数为 $(p,q)$ 随机多分辨率奇异值分解的逆过程，并截去第一行和第一列的零向量，得到矩阵 $\hat{\boldsymbol{G}}_c$。

3)把矩阵 $\hat{\boldsymbol{G}}_c$ 划分成左上半部分 $\hat{\boldsymbol{G}}_c^{\mathrm{L}}$ 和右下半部分 $\hat{\boldsymbol{G}}_c^{\mathrm{R}}$，将矩阵 $\hat{\boldsymbol{G}}_c^{\mathrm{L}}$ 作为实部分量，将水平和垂直翻转后的矩阵 $\hat{\boldsymbol{G}}_c^{\mathrm{R}}$ 作为虚部分量，构建复数矩阵 $\hat{\boldsymbol{F}}_c^{\mathrm{L}}$，表达式分别为

$$\hat{\boldsymbol{G}}_c^{\mathrm{L}}=\begin{bmatrix} d_{1,1} & \cdots & d_{1,\frac{N}{2}+1} & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ d_{\frac{M}{2},1} & \cdots & d_{\frac{M}{2},\frac{N}{2}+1} & \cdots & 0\\ d_{\frac{M}{2}+1,1} & \cdots & d_{\frac{M}{2}+1,\frac{N}{2}+1} & \cdots & 0\\ d_{\frac{M}{2}+2,1} & \cdots & 0 & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ d_{M+1,1} & \cdots & 0 & \cdots & 0 \end{bmatrix},\tag{8}$$

$$\hat{\boldsymbol{G}}_c^{\mathrm{R}}=\begin{bmatrix} 0 & \cdots & 0 & \cdots & d_{1,N+1}\\ \vdots & & \vdots & & \vdots\\ 0 & \cdots & 0 & \cdots & d_{\frac{M}{2},N+1}\\ 0 & \cdots & 0 & \cdots & d_{\frac{M}{2},N+1}\\ 0 & \cdots & d_{\frac{M}{2}+2,\frac{N}{2}+1} & \cdots & d_{\frac{M}{2}+2,N+1}\\ \vdots & & \vdots & & \vdots\\ 0 & \cdots & d_{M+1,\frac{N}{2}+1} & \cdots & d_{M+1,N+1} \end{bmatrix},\tag{9}$$

$$\hat{\boldsymbol{F}}_c^{\mathrm{L}}=\begin{bmatrix} d_{1,1}+\mathrm{j}d_{M+1,N+1} & \cdots & d_{1,\frac{N}{2}+1}+\mathrm{j}d_{M+1,\frac{N}{2}+1} & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ d_{\frac{M}{2},1}+\mathrm{j}d_{\frac{M}{2}+2,N+1} & \cdots & d_{\frac{M}{2},\frac{N}{2}+1}+\mathrm{j}d_{\frac{M}{2}+2,\frac{N}{2}+1} & \cdots & 0\\ d_{\frac{M}{2}+1,1}+\mathrm{j}d_{\frac{M}{2}+1,N+1} & \cdots & d_{\frac{M}{2}+1,\frac{N}{2}+1} & \cdots & 0\\ d_{\frac{M}{2}+2,1}+\mathrm{j}d_{\frac{M}{2},N+1} & \cdots & 0 & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ d_{M+1,1}+\mathrm{j}d_{1,N+1} & \cdots & 0 & \cdots & 0 \end{bmatrix}。\tag{10}$$

4) 对复数矩阵 $\hat{\boldsymbol{F}}_c^{\mathrm{L}}$ 进行水平、垂直翻转和取共轭，将结果与复数矩阵 $\hat{\boldsymbol{F}}_c^{\mathrm{L}}$ 叠加，得到每个通道的频谱矩阵 $\boldsymbol{F}_c'$：

$$\boldsymbol{F}_c'=\hat{\boldsymbol{F}}_c^{\mathrm{L}}+[T_2[T_1[\hat{\boldsymbol{F}}_c^{\mathrm{L}}]]]^*,\tag{11}$$

式中：$[\cdot]^*$ 为共轭运算符号。

5) 对每个通道的频谱矩阵 $\boldsymbol{F}_c'$ 进行 Fourier 逆变换，并截去第一行、第一列的零向量得到解密的颜色分量 $\hat{\boldsymbol{f}}_c(x,y)$，对三个通道进行组合，恢复得到彩色明文图像 $\hat{\boldsymbol{f}}(x,y)$。

## 4　实验结果分析

为了测试所提算法的有效性和鲁棒性，使用 Matlab 2016a 软件进行仿真。随机选取如图 2(a)～(e)所示的 5 幅彩色图像[20]作为明文图像，尺寸为 256×256×3。LES 映射的控制参数设置为 $a=1$、$b=0.5805$、$c=2.8$。Josephus 遍历的报数间隔 $k_1=4$、$k_2=4$。

### 4.1　加密和解密的效果

首先分析 R-MRSVD 参数的选取对解密图像


图 2　测试图像。(a) Lena;(b) Elephant;(c) Grnpeace;(d) Peppers;(e) Butterfly

Fig. 2　Tested images. (a) Lena; (b) Elephant; (c) Grnpeace; (d) Peppers; (e) Butterfly

质量的影响，实验中分别按照 $p\times q=\{2\times2,2\times3,3\times2\}$ 对图 2 中 5 幅明文图像进行加密和解密。为了客观评价解密图像的质量，使用峰值信噪比(PSNR)、相关系数(CC)作为评价指标。明文图像 $\boldsymbol{f}(x,y)$ 和解密图像 $\hat{\boldsymbol{f}}(x,y)$ 的 PSNR、CC 的计算公式分别为

$$R_{\mathrm{PSNR}}=10\log_{10}\times\left(\frac{255^2}{\frac{1}{MN}\sum_{y=0}^{N-1}\sum_{x=0}^{M-1}[\boldsymbol{f}(x,y)-\hat{\boldsymbol{f}}(x,y)]^2}\right),\tag{12}$$

$$R_{\mathrm{CC}}=\frac{E\{[\boldsymbol{f}-E(\boldsymbol{f})]\,[\hat{\boldsymbol{f}}-E(\hat{\boldsymbol{f}})]\}}{\sqrt{E\{[\boldsymbol{f}-E(\boldsymbol{f})]^2\}}}\times\frac{1}{\sqrt{E\{[\hat{\boldsymbol{f}}-E(\hat{\boldsymbol{f}})]^2\}}},\tag{13}$$

式中：$E(\cdot)$ 为期望运算。根据定义，PSNR 越高、CC 越接近 1，表示解密图像的质量越好。

考虑到矩阵存在一维和二维离散 Fourier 变换，实验时分别使用一维离散 Fourier 变换、二维离散 Fourier 变换评估不同分解参数对解密图像质量的影响。表 1 列出了所提算法与文献[16]、[17]中算法的 PSNR。可以看出，所提算法在两种不同方案下，分解参数为 $p\times q=2\times2$ 时，解密图像的质量更好，PSNR 的平均值分别为 301.9349 dB，300.3393 dB。对颜色分量进行一维离散 Fourier 变换时，需要先将矩阵转成向量，再将变换结果转成矩阵。为了避免繁琐的操作，以下实验使用二维离散 Fourier 变换并将 R-MRSVD 的参数设置为 $p\times q=2\times2$。此时所提算法与文献[16]、[17]中算法的 PSNR 均值分别为 300.3393 dB、258.2906 dB、304.5765 dB，解密图像质量较好。

表 1　正确解密时的 PSNR

Table 1　PSNR of correctly decryption

| Image | Proposed algorithm | | | | | | Algorithm in Ref. [16] | Algorithm in Ref. [17] |
|---|---|---|---|---|---|---|---|---|
| | 1D-DFT | | | 2D-DFT | | | | |
| | 2×2 | 2×3 | 3×2 | 2×2 | 2×3 | 3×2 | | |
| Lena | 300.4656 | 291.7590 | 287.9488 | 298.4824 | 289.0684 | 295.0256 | 262.7863 | 302.4648 |
| Elephant | 291.8283 | 294.5651 | 303.3073 | 293.4864 | 300.8966 | 299.7538 | 272.0697 | 304.3388 |
| Grnpeace | 315.7956 | 293.4830 | 286.2010 | 311.1888 | 291.8217 | 296.4422 | 253.9804 | 308.4498 |
| Peppers | 296.8666 | 290.3514 | 283.4614 | 296.7653 | 292.6517 | 282.7151 | 259.1771 | 303.3361 |
| Butterfly | 304.7186 | 296.1617 | 294.6717 | 301.7734 | 298.5181 | 298.4478 | 243.4396 | 304.2931 |
| Mean/standard deviation | 301.9349/9.0810 | 293.2640/2.2850 | 291.1180/7.9695 | 300.3393/6.7630 | 294.5913/4.9273 | 294.4769/6.8212 | 258.2906/10.6065 | 304.5765/2.2988 |

图 3(a)为 $p\times q=2\times2$ 时图 2 的加密结果，可以看出，密文图像类似噪声且在视觉上无法得到任何有意义的明文图像信息。图 3(b)为使用正确密钥的解密结果，PSNR 均值为 300.3393 dB，CC 值均为 1，无法从视觉上分辨与明文图像间的差异。

### 4.2　抗统计攻击性能分析

抗统计攻击性能分析包括明文、密文的直方图和相邻像素间的相关性。图像直方图描述像素的强度分布，包含有图像中视觉内容相关的一些重要信息，加密后的图像直方图应该与明文图像完全不同。图 4(a)、(b)分别为图 2、图 3(a)的灰度直方图。可

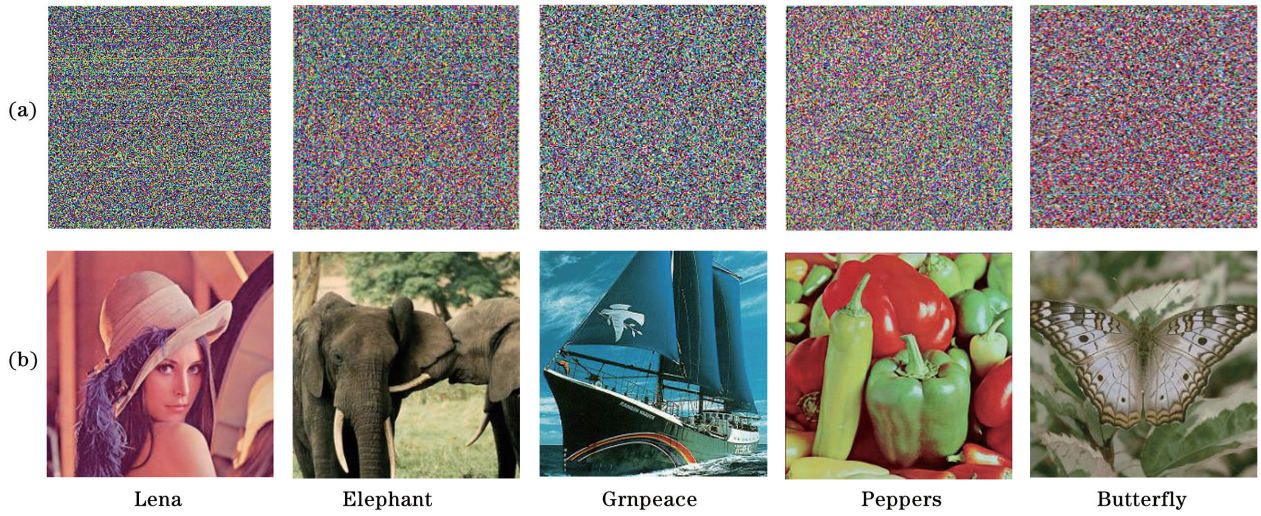


图 3　加密和解密结果。(a)密文图像;(b)恢复的图像

Fig. 3　Results of encryption and decryption. (a) Cipherimages; (b) restituted images

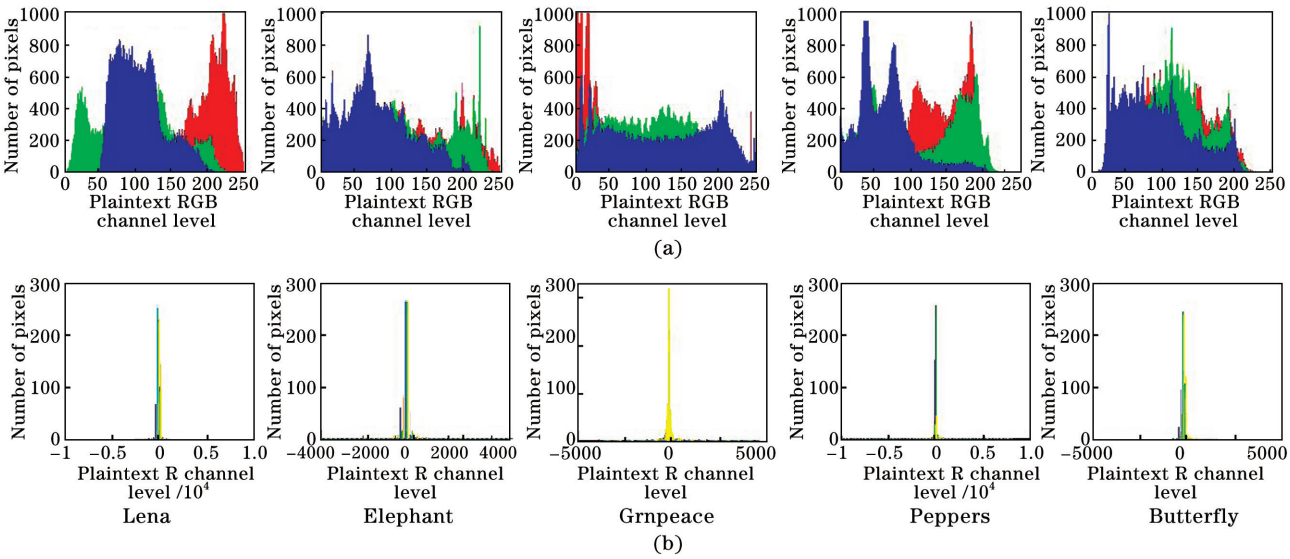


图 4　直方图结果。(a)明文图;(b)密文图

Fig. 4　Histogram results. (a) Plaintext images; (b) ciphertext images

以看出:明文图像与密文图像的像素分布差距较大,不同明文的灰度分布不均匀;而密文的直方图更加集中且均呈接近高斯白噪声的分布,能够掩盖明文图像的信息,打乱了原明文图像的灰度特征。

另外,明文图像的相邻像素之间具有很强的相关性,其相关系数接近 1.0000。而加密后将破坏原图相邻像素间的强相关性,使其接近于 0。从明文图像和其对应的加密图像上分别随机选取 5000 对相邻像素点,计算其在水平、垂直和对角线方向上相邻像素之间的相关系数。

表 2 为图 2 和图 3(a)在水平、垂直和对角线方向上相邻像素之间的相关系数。图 5 为明文图像 Lean及其密文在水平、垂直、对角三个方向的相邻

表 2　明文及密文图像的相关系数

Table 2　Correlation coefficients of plaintext and ciphertext images

| Image | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Lena in Fig. 2 | 0.9469 | 0.9088 | 0.8829 |
| Elephant in Fig. 2 | 0.9645 | 0.9519 | 0.9319 |
| Grnpeace in Fig. 2 | 0.7127 | 0.7933 | 0.7001 |
| Peppers in Fig. 2 | 0.9469 | 0.9407 | 0.9289 |
| Butterfly in Fig. 2 | 0.8776 | 0.8930 | 0.8386 |
| Lena in Fig. 3(a) | 0.0156 | 0.1012 | −0.0047 |
| Elephant in Fig. 3(a) | 0.0440 | 0.0564 | −0.0013 |
| Grnpeace in Fig. 3(a) | 0.0377 | −0.0119 | 0.0042 |
| Peppers in Fig. 3(a) | 0.0449 | 0.0018 | −0.0010 |
| Butterfly in Fig. 3(a) | −0.0419 | 0.0165 | 0.0238 |

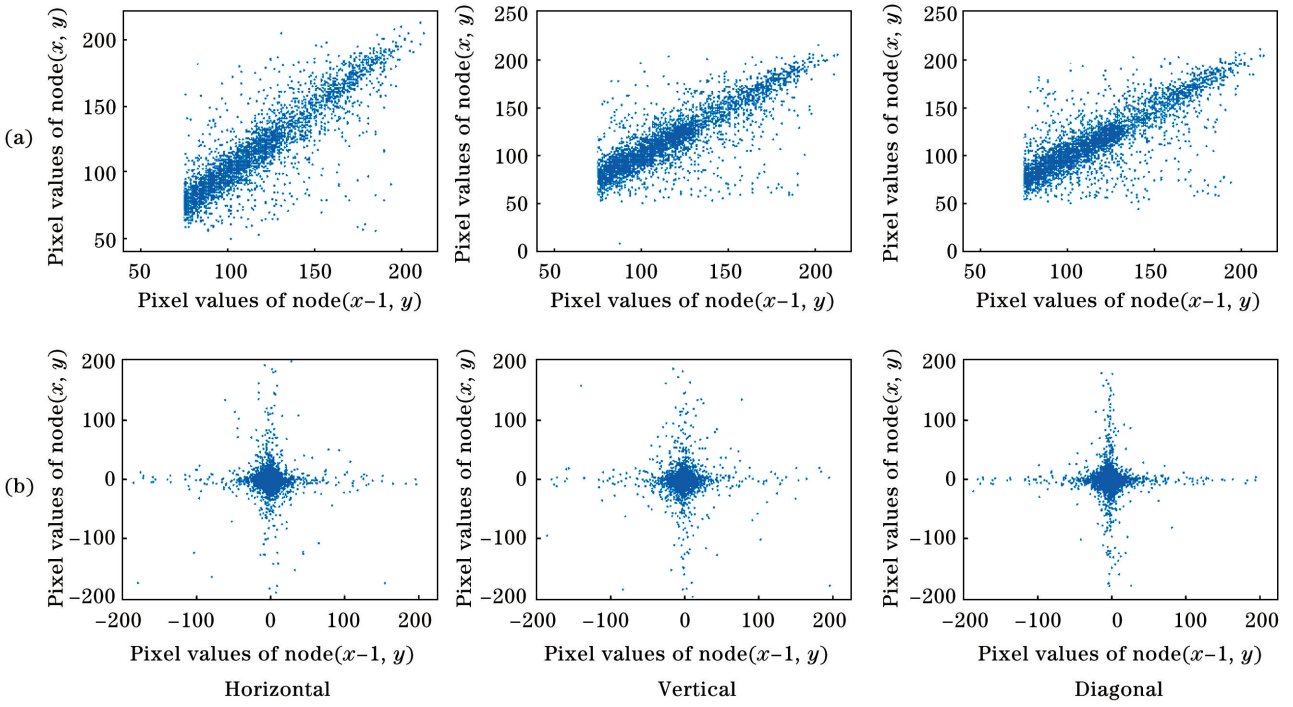


图 5　相邻像素的相关分布。(a)Lena 的明文图像;(b)Lena 的密文图像

Fig. 5　Correlation distribution of adjacent pixels. (a) Lena′s plaintext image; (b) Lena′s ciphertext image

像素的相关分布。可以看出:图 2 在水平、垂直、对角线方向的相关系数大于 0.7,表明明文图像的相邻像素间相关性很强;而图 3(a)在水平、垂直、对角线方向的相关系数接近于 0,几乎没有相关性,说明所提算法能够抵抗统计攻击。

### 4.3　抗选择明文攻击分析

为了测试所提算法抵抗选择明文攻击的能力,从 BSDS500 数据库[21]随机选取 5 幅图像作为伪明文,如图 6(a)所示。假设攻击者利用伪明文产生对应的解密密钥,并对图 3(a)进行解密。由图 6(b)可知,攻击者无法得到原始明文图像的任何信息。这是由于所提算法与明文的像素有很大联系,每次加密时利用明文像素来迭代 LES 映射,使得加密算法随着明文的不同而形成不同的密钥。结果表明,所提算法具有较强的抗选择明文攻击能力。

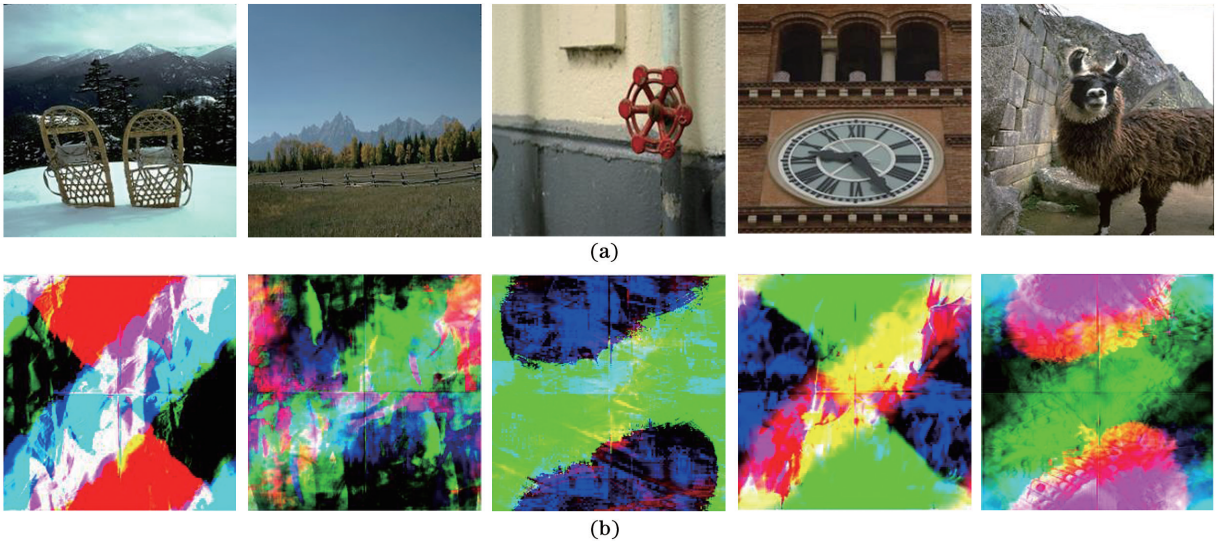


图 6　选择明文攻击结果。(a)伪明文图像;(b)图 3(a)的解密结果

Fig. 6　Results of chosen-plaintext attack. (a) Fake plaintext images; (b) decrypted results of Fig. 3(a)

### 4.4　算法敏感性分析

当解密密钥存在微小差异时，所产生的解密图像应该没有任何原明文图像的信息。所提算法将 LES 映射控制参数 $a$、$b$、$c$ 和初值 $x_0'$ 作为解密过程的主密钥，当一个密钥发生微小变化时，其余密钥均保持正确。图 7 分别为 $a$、$b$、$c$ 及初值 $x_0'$ 存在偏差 $\delta=10^{-15}$ 时的解密结果。可以看出，当任何一个解密密钥发生微小变化，即使其他密钥均保持正确时，攻击者都不能进行正确解密。

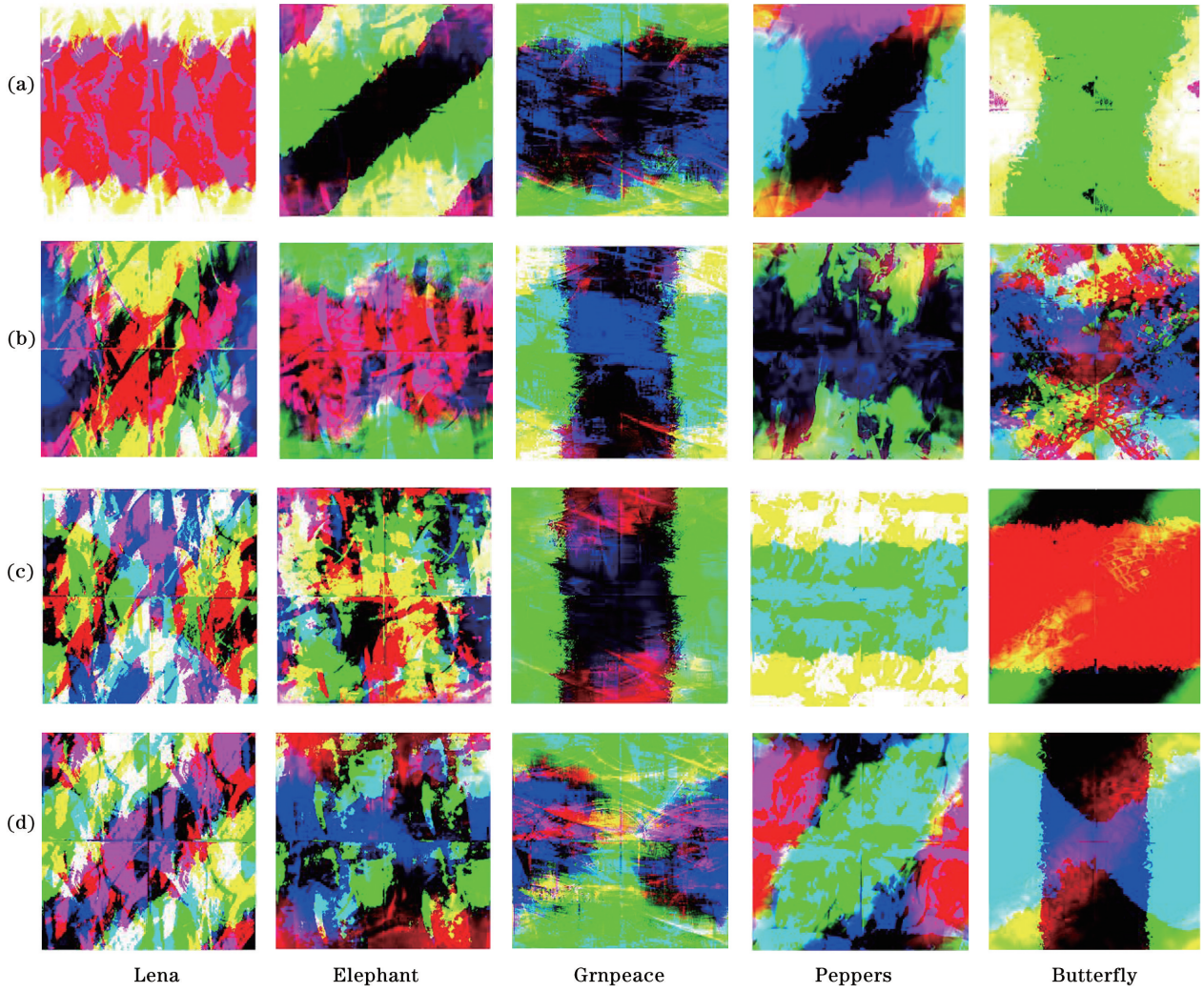


图 7　密钥存在偏差时的解密结果。(a)$a$；(b)$b$；(c)$c$；(d)$x_0'$

Fig. 7　Decrypted results using a slightly deviated key. (a) $a$; (b) $b$; (c) $c$; (d) $x_0'$

当明文图像发生微小变化时，新的密文应该与原密文之间存在显著差异。用像素数改变率(NPCR)和归一化改变强度(UACI)来评价加密算法的明文敏感性。设加密图像在点$(i,j)$处的像素值分别为 $C_1(i,j)$ 和 $C_2(i,j)$，则 NPCR 和 UACI 的计算公式分别为

$$R_{\mathrm{NPCR}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}T(i,j)\times 100,\quad(14)$$

$$R_{\mathrm{UACI}}=\frac{1}{M\times N}\times\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100,\quad(15)$$

式中：$T(i,j)=\begin{cases}0, & C_1(i,j)=C_2(i,j)\\ 1, & C_1(i,j)\neq C_2(i,j)\end{cases}$。

任选明文图像一个像素点，将其像素值增加 20，经计算，NPCR 和 UACI 值分别为 99.9960%和 33.3346%。结果表明，所提算法对像素值具有较强的敏感性。这是由于明文图像的像素特性作为 LES 映射的初值，当像素值发生改变时，将会使混沌序列发生变化，进而使得密文图像发生改变。

### 4.5　密钥空间分析

当密钥空间足够大时，加密系统才具有更高的安全性。所提加密系统的密钥包括 LES 映射的控

制参数 $a\in(0,1)$、$b\in(0,1)$、平衡参数 $c\in(2,2.8)$、初值 $x_0'\in(0,1)$。假设计算精度为 $10^{-15}$，则加密算法的密钥空间为 $0.8\times10^{15}\times10^{15}\times10^{15}\times10^{15}=8\times10^{59}$，表明所提算法足以抵抗对密钥空间的暴力攻击。

### 4.6　抗噪声攻击分析

为了测试所提算法对噪声攻击的鲁棒性，对密文添加均值为 0、方差为 $\sigma$ 的高斯白噪声并进行正确解密，使用 PSNR 和 CC 作为评价指标。对所提算法的解密结果与文献[16]、[17]中算法的解密结果进行比较。

图 8 为高斯噪声强度为 1 时不同算法的解密图像，可以看出：密文在受到较小强度的噪声污染后，所提算法得到的解密图像依然清晰；而噪声污染对文献[16]中算法的解密结果影响最大；文献[17]中算法的解密结果存在一定的轮廓。图 9 为不同高斯噪声时的 PSNR 和 CC 均值，随着噪声强度的增加，解密图像的质量不断退化，但是所提算法得到的 PSNR、CC 值均较高。实验结果表明，所提算法对高斯噪声攻击具有较好的鲁棒性。

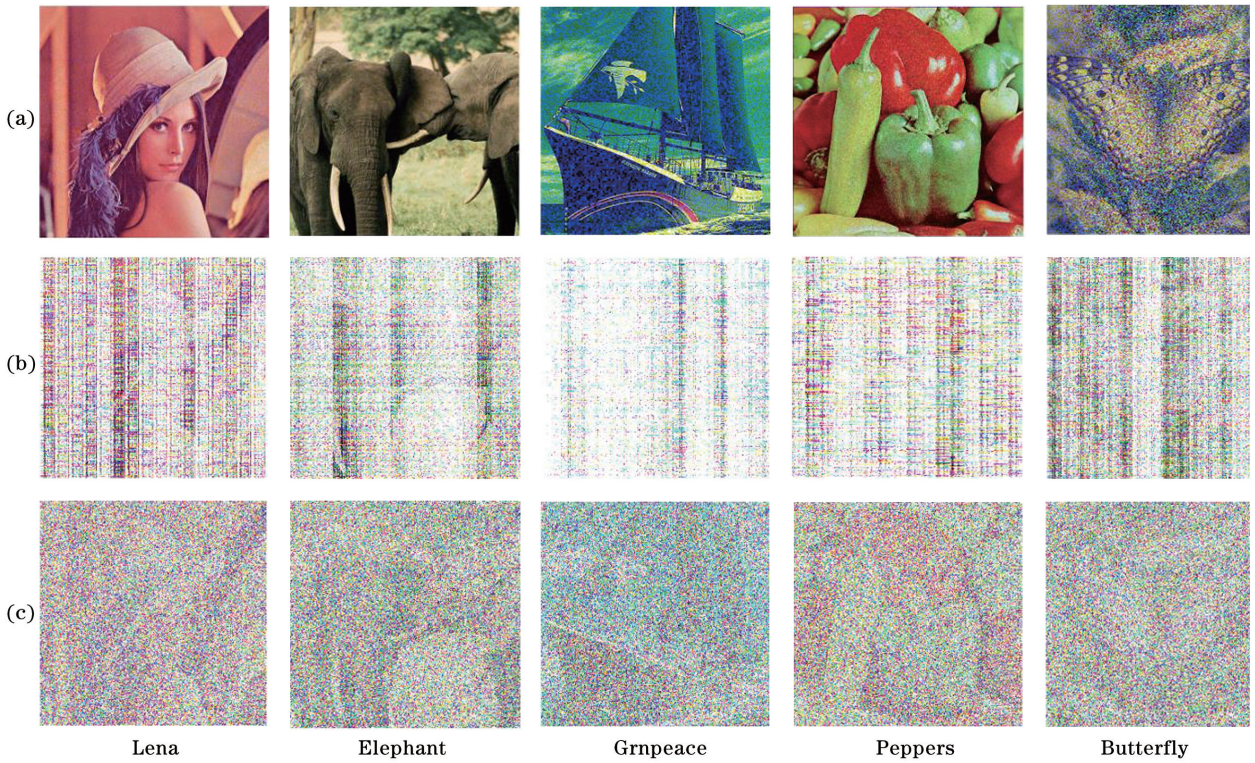


图 8　高斯噪声强度为 1 的解密结果。(a)所提算法；(b)文献[16]中的算法；(c)文献[17]中的算法

Fig. 8　Decrypted results when the intensity of Gaussian noise is 1. (a) Proposed algorithm; (b) algorithm in Ref. [16]; (c) algorithm in Ref. [17]

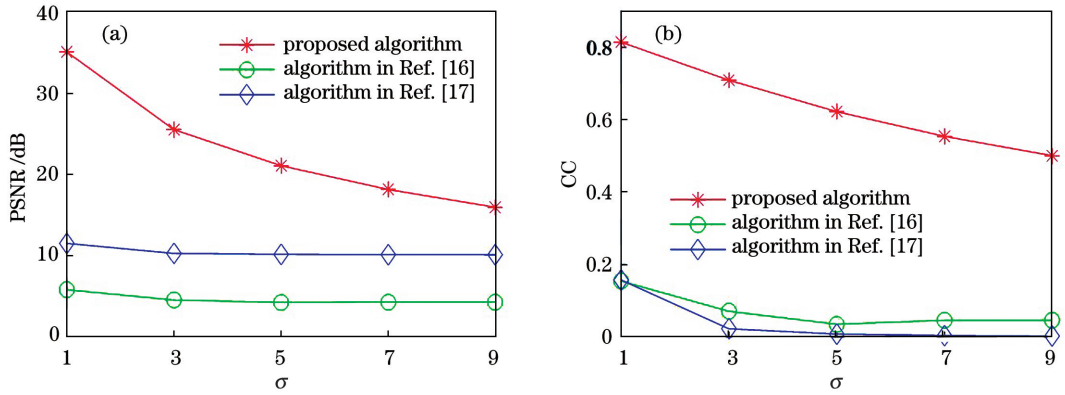


图 9　高斯噪声攻击下的 PSNR 和 CC 均值。(a)PSNR；(b)CC

Fig. 9　Average PSNR and CC under Gaussian noise attack. (a) PSNR; (b) CC

### 4.7　抗裁剪攻击分析

为了测试所提算法的抗裁剪能力，分别按 $\eta$ 为5%，10%，15%，20%，25%的比例对密文进行中心位置裁剪并进行正确解密，对所提算法、文献[16]中算法、[17]中算法的结果进行比较。图 10 为密文中心裁剪 20%的解密图像，图 11 为 PSNR 和 CC 均值随裁剪百分比 $\eta$ 增大而变化的曲线。从图 10 可以看出，所提算法与文献[16]、[17]中的算法均能恢复明文图像。由图 11 可以看出，所提算法的抗裁剪攻击能力要优于文献[16]、[17]中的算法。结果表明，所提算法具有一定的抗裁剪能力，不易受密文损失大小影响。

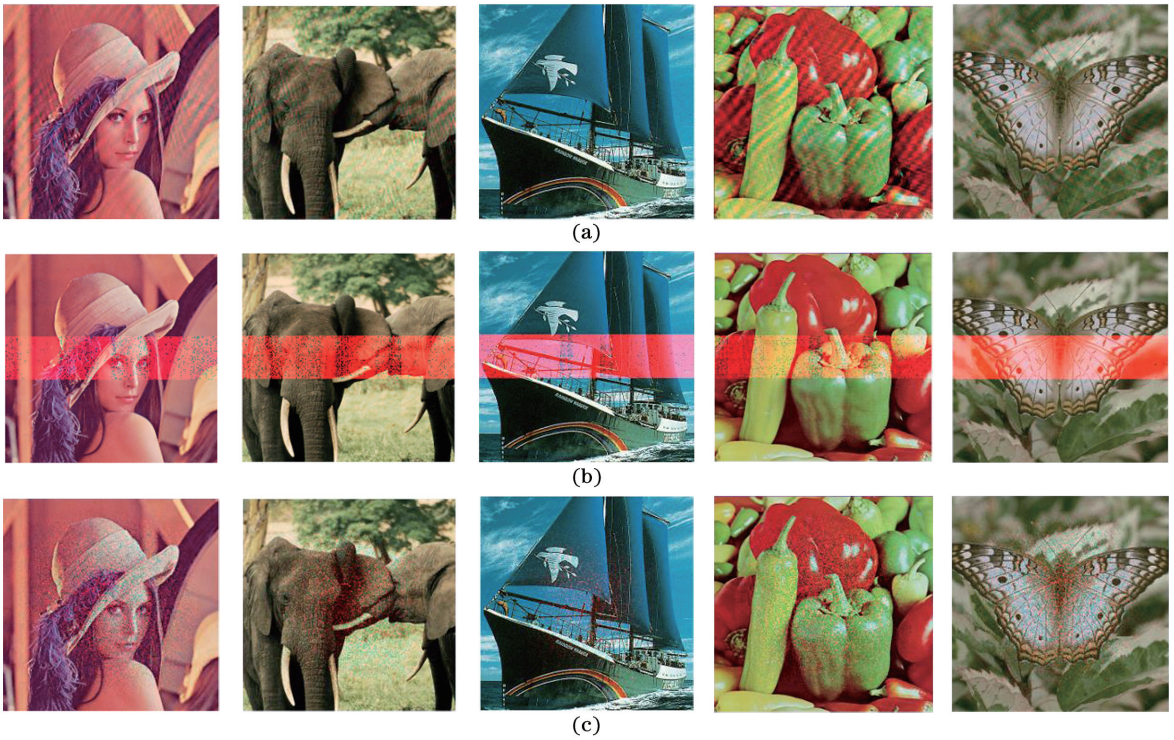


图 10　裁剪攻击($\eta$=20%)的解密图像。(a)所提算法；(b)文献[16]中的算法；(c)文献[17]中的算法

Fig. 10　Decrypted images under cropping attack($\eta$=20%). (a) Proposed algorithm; (b) algorithm in Ref. [16]; (c) algorithm in Ref. [17]

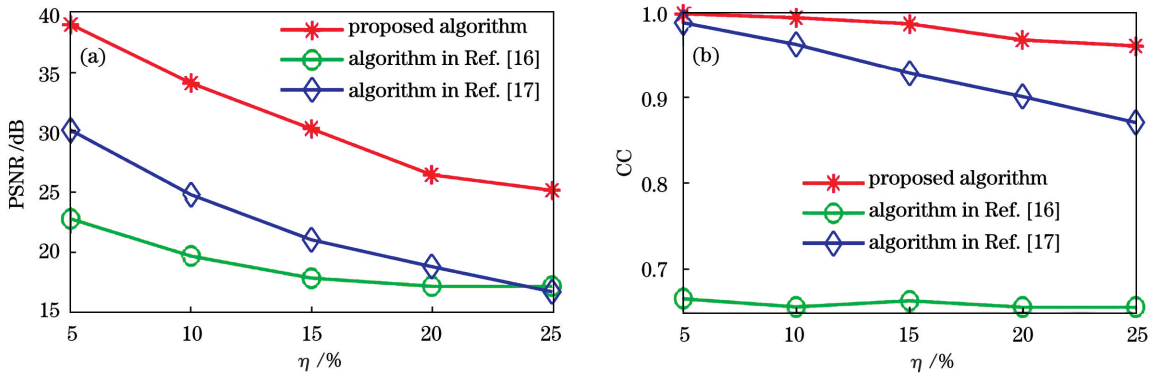


图 11　裁剪攻击下的 PSNR 和 CC 均值。(a)PSNR；(b)CC

Fig. 11　Average PSNR and CC under cropping attack. (a) PSNR; (b) CC

## 5　结　　论

结合 Fourier 变换对称性和随机多分辨率奇异值分解，提出一种保实的图像加密算法。对每个颜色通道使用 Fourier 变换并根据频谱的共轭对称性构建实数矩阵，有效地节省密文的存储空间；再结合随机多分辨率奇异值分解的多尺度适应性和 Josephus 置乱，使得加密算法具有更高的安全性。另外，将明文图像的像素特性作为混沌映射的初值，使得算法敏感性高、密钥空间大，能够抵御选择明文

攻击。与已有的加密算法相比，所提算法在能够高质量地恢复出明文图像同时，具有更好的抗噪声攻击和抗裁剪能力。

## 参 考 文 献


[1] Jiao S M, Zhou C Y, Shi Y S, et al. Review on optical image hiding and watermarking techniques [J]. Optics & Laser Technology, 2019, 109: 370-380.

[2] Ghadirli H M, Nodehi A, Enayatifar R. An overview of encryption algorithms in color images [J]. Signal Processing, 2019, 164: 163-185.

[3] Kumar R, Bhaduri B, Hennelly B. QR code-basednon-linear image encryption using Shearlet transform and spiral phase transform [J]. Journal of Modern Optics, 2018, 65(3): 321-330.

[4] Kaur J, Jindal N. A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys [J]. Multimedia Tools and Applications, 2019, 78(9): 11585-11606.

[5] Liu Y J, Zhang N, Zhang F Q, et al. Optical multiple-image authentication method based on hyper-chaos and phase information multiplexing in Gyrator transform domain [J]. Acta Optica Sinica, 2020, 40(5): 0510003.
刘禹佳, 张宁, 张福琦, 等. 基于超混沌和 Gyrator 域相位信息复用的光学多图像认证方法[J]. 光学学报, 2020, 40(5): 0510003.

[6] Tao S, Tang C, Tang C, et al. Optical image encryption based on biometric keys and singular value decomposition [J]. Applied Optics, 2020, 59(8): 2422-2430.

[7] Yu S S, Zhou N R, Gong L H, et al. Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system [J]. Optics and Lasers in Engineering, 2020, 124: 105816.

[8] Wang M M, Pousset Y, Carré P, et al. Optical image encryption scheme based on apertured fractional Mellin transform [J]. Optics & Laser Technology, 2020, 124: 106001.

[9] Kang X J, Ming A L, Tao R. Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(6): 1595-1607.

[10] Faragallah O S, AlZain M A, El-Sayed H S, et al. Secure color image cryptosystem based on chaotic logistic in the FrFT domain [J]. Multimedia Tools and Applications, 2020, 79(3/4): 2495-2519.

[11] Wang Y, Quan C, Tay C J. Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask [J]. Optics Communications, 2015, 344: 147-155.

[12] Xiong Y, Du J, Quan C. Single-channel optical color image cryptosystem using two-step phase-shifting interferometry and random modulus decomposition [J]. Optics & Laser Technology, 2019, 119: 105580.

[13] Chen H, Zhu Z, Tanougast C, et al. Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional Fourier transform domains [J]. Optics and Lasers in Engineering, 2019, 112: 7-15.

[14] Yao L L, Yuan C J, Qiang J J, et al. An asymmetric color image encryption method by using deduced gyrator transform [J]. Optics and Lasers in Engineering, 2017, 89: 72-79.

[15] Kumar M, Vaish A. Encryption of color images using MSVD in DCST domain [J]. Optics and Lasers in Engineering, 2017, 88: 51-59.

[16] Liu Y J, Xu X P, Xu J H, et al. Remote sensing image encryption using vector operations and secondary image phase masks [J]. Acta Photonica Sinica, 2019, 48(2): 0210002.
刘禹佳, 徐熙平, 徐嘉鸿, 等. 基于矢量运算和副像相位掩模的遥感图像加密技术[J]. 光子学报, 2019, 48(2): 0210002.

[17] Tao S, Tang C, Lei Z K. Image encryption based on vector decomposition and chaotic random phase mask [J]. Laser & Optoelectronics Progress, 2020, 57(4): 041002.
陶珊, 唐晨, 雷振坤. 基于矢量分解和混沌随机相位掩模的图像加密[J]. 激光与光电子学进展, 2020, 57(4): 041002.

[18] Hua Z Y, Zhou Y C. Exponential chaotic model for generating robust chaos [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019: 1-12.

[19] Bhatnagar G, Saha A, Wu Q M J, et al. Analysis and extension of multiresolution singular value decomposition [J]. Information Sciences, 2014, 277: 247-262.

[20] University of Granada. Test images [EB/OL]. (2014-03-13)[2020-07-09]. http://decsai.ugr.es/cvg/dbimagenes/.

[21] Arbelaez P, Maire M, Fowlkes C, et al. Contour detection and image segmentation resource [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 33(5): 898-916.