激光与光电子学进展 先进成像

基于混沌卷积的光学图像分块加密方法

王佳[1*]，刘丽[2]

[1]山西金融职业学院信息技术系，山西 太原 030008；

[2]太原理工大学物理与光电工程学院，山西 太原 030024

摘要 基于分块压缩感知理论和随机卷积理论，提出了一种基于混沌卷积的光学图像分块加密方法。首先将图像分为大小相同的分块子图像，针对每个子图像，利用级联混沌系统生成混沌相位模板和混沌振幅模板，将子图像与混沌相位模板进行混沌卷积；然后利用混沌振幅模板进行混沌下采样，获得加密压缩后的分块图像；最后将各分块加密图像复原为最终的加密图像。该方法每个分块子图像具有不同的加密密钥，以提高算法的安全性，混沌卷积过程中采用分数傅里叶变换替代傅里叶变换，以增大密钥空间。对加密方法的抗噪声攻击性、抗裁剪攻击性、统计特性、密钥敏感性等进行仿真实验，结果表明了该方法的可行性和安全性。

关键词 图像处理；图像加密；随机卷积；混沌

中图分类号 TP309.7 **文献标志码** A **DOI**：10.3788/LOP212725

Optical Image Block Encryption Method Based on Chaotic Convolution

Wang Jia[1*], Liu Li[2]

[1]*Department of Information Technology, Shanxi Professional College of Finance, Taiyuan* 030008, *Shanxi, China*;

[2]*College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan* 030024, *Shanxi, China*

Abstract Based on block compressed sensing theory and random convolution theory, a new optical image block encryption method based on chaotic convolution is proposed. First, blocks of the same size are created from the plain image. A chaotic phase mask and a chaotic amplitude mask are generated for each block by a cascaded chaotic system, which is then used to convolute the block with the chaotic phase mask, and chaotic subsampling is followed using a chaotic amplitude mask to obtain the encrypted and compressed block image. Finally, all encrypted blocks are restored to the final encrypted image. Note that each block has a different key to increase the security, and fractional Fourier transform is used instead of Fourier transform in the process of chaotic convolution to increase the key space. Simulation is conducted on statistical analysis, noise attack resistance test, cropping attack resistance test, and key sensitivity test. The viability and security of the suggested encryption system are shown by numerical results.

Key words image processing; image encryption; random convolution; chaos

1 引 言

随着通信和计算机技术的飞速发展，人们对信息安全提出越来越高的要求。而光学图像加密技术因其具有大容量、高速并行、多维度、高鲁棒性等诸多优势，已成为信息安全领域的研究热点[1-2]。

现有光学图像加密方法中，最为经典的是1995年由Refregier等[3]提出的基于4*f*系统的双随机相位编码(DRPE)光学加密方法，但是由于其线性和对称性质，DRPE易受已知/选择明文攻击[4]。因此，研究人员在DRPE的基础上提出很多改进和衍生方法，如利用分数傅里叶变换[5-7]、菲涅尔域[8]、Hartley变换[9]、Gyrator变换[10-11]、分数梅林变换[12]、分数角变换[13-14]等替换傅里叶变换的方法，引入像素置乱[15]、Arnold变换[13]、Jigsaw变换[16]等的置乱方法，提高加密方法的安全性。此外：为了抵抗已知明文攻击，在输入面或频谱面引入幅度调制[17]；为了提高密钥敏感性和扩展密钥空间，引入混沌理论生成相位掩模[6-7,11]；为了增加加密方法的鲁棒性，将quick-response(QR)码[18-19]引入DRPE中；针对彩色图像加密问题，引入矢量分解，使加密系统变

收稿日期：2021-10-13；**修回日期**：2021-11-19；**录用日期**：2021-12-21；**网络首发日期**：2022-01-01

基金项目：山西省重点研发计划项目(201803D31037)

通信作者：*wangjia0313@126.com

成非对称加密系统[20]。但是这些方法都不能实现图像压缩，而图像压缩是图像在信道上传输之前的必要步骤。传统的传输图像方法都是先压缩后加密，或是先加密后压缩，将压缩和加密作为两个独立的步骤进行的。

随着压缩感知(CS)理论的不断成熟，基于压缩感知的图像加密方法因其可同时实现压缩和加密而受到广泛关注[21-27]。尽管人们认为基于CS的加密方案无法实现完美的安全性，但由于它在抵御攻击方面所需计算复杂性非常高而具有重要应用意义[21]。Lu等[22]率先将CS和DRPE结合用于多图像加密，该方法解决了DRPE的线性问题，提高了保密性，且降低了数据传输量，减小了随机相位模板的尺寸。在此基础上，研究人员引入Arnold变换[23]、混沌映射[24]、分数傅里叶变换[24]、分块压缩感知(BCS)[25]等思想，以进一步提高加密系统的安全性。但是，现有基于CS和DRPE结合的光学图像加密方法，通常都是先利用CS对图像进行采样，然后用DRPE进行加密的。CS和DRPE仅具有优先关系，这意味着图像压缩和加密操作几乎彼此独立实现。2015年，Zhang等[28]针对单幅图像同时实现压缩和加密的问题，提出基于随机卷积(RC)的方法，该方法与DRPE类似，也采用两块随机模板，但随机模板的类型和放置的位置不同，DRPE将两块随机相位模板分别放置在4f系统的输入平面和傅里叶频谱面，而RC方法将一块随机相位模版置于图像的频谱面，一块随机振幅模板置于图像的输出平面。随后，该团队又提出一种基于分块压缩感知和Sobel边缘检测器的可分级加密方案，该方案利用分块压缩感知将原图像分块，然后利用Sobel边缘检测器判断各分块的重要性，针对重要分块，利用基于混沌的结构化随机矩阵方法进行加密，对于剩余的不重要分块采用基于混沌的随机卷积方法进行加密[29]。这些工作表明，作为DRPE的一种变体，随机卷积是一个很好的图像加密选择。但是，目前针对随机卷积加密方法的研究尚未深入，文献[28]仅给出简单的结果，证明该方法的有效性，并未对加密方法的鲁棒性、统计特性等进行详细分析，文献[29]指出基于混沌的随机卷积的鲁棒性相对较弱，因此仅用于不重要分块的加密。

为了提高现有随机卷积加密方法的鲁棒性和安全性，并深入分析其加密特性，本文在随机卷积图像加密的基础上，引入级联混沌系统(称为混沌卷积)，并引入分块压缩感知和分数傅里叶变换实现单幅光学图像的压缩加密。首先对原始图像进行分块，每个分块先后进行随机卷积和随机解调处理，随机卷积和随机解调中所需的随机模版由级联混沌系统构成，并采用分数傅里叶变换代替傅里叶变换。该算法具有数据量小、安全性高、传输效率高等优点，并通过数值仿真深入分析该方法的鲁棒性、统计特性、密钥敏感度等。

2 理论基础

2.1 分块压缩感知

根据压缩感知理论，只要一个信号在某个变换域中是可压缩的或稀疏的，就可以利用测量矩阵将高维信号转换到低维空间，即信号在采集过程中实现了压缩，进而信号重构问题也就转换为一个优化求解问题。但是在实际应用中，对于数据量较大的图像，CS重构的运算量非常大。因此，Gan[30]提出BCS方法。BCS的观测和重构都对每个分块子图像单独进行操作，减少运算所需时间和存储空间，降低其计算复杂度，能快速恢复出图像[31]。

设大小为$m\times n$的灰度图像，分为B个小块，每个块大小为$m_b\times n_b$，则分块子图像$\boldsymbol{x}_j\in\boldsymbol{R}^{N_b}(N_b=m_b\times n_b)$可以稀疏表示为$\boldsymbol{x}_j=\boldsymbol{\Psi s}$，其中$\boldsymbol{\Psi}\in\boldsymbol{R}^{N_b\times N_b}$为正交变换基(如傅里叶变换基、小波基、离散余弦变换基等)，$\boldsymbol{s}$为变换系数。若$\boldsymbol{s}$中只有$K(K\ll N_b)$个非零系数，则称$\boldsymbol{s}$为K-稀疏。观测向量$\boldsymbol{y}_j\in\mathbf{R}^{M_b}$就可以用随机线性投影$\boldsymbol{y}_j=\boldsymbol{\Phi x}_j=\boldsymbol{\Phi\Psi s}$获得，其中$\boldsymbol{\Phi}\in\boldsymbol{R}^{M_b\times M_b}(M_b\ll N_b)$为观测矩阵或感知矩阵。$M_b$和$N_b$的比值称为压缩率(CR)。当接收端收到分块子图像的观测向量后，采用相同的重构算法对每个子图像进行重构，即可获得整幅图像。本研究采用的重构算法为梯度投影稀疏重构算法(GPRS)[32]。

2.2 随机卷积

2009年，Romberg[33]提出基于随机卷积的压缩感知方法，并证明结合随机卷积和随机下采样是一种普遍有效的压缩感知方法。该方法认为，一个大小为n的信号只要在某个域是稀疏的(稀疏度为K)，则可以通过与一个随机脉冲相卷积的方法从大小为$m(m\geqslant K\log n)$的测量值中复原，其中随机脉冲具有单位振幅和随机相位。该方法包括随机卷积和随机下采样两步。

随机卷积，即将信号$\boldsymbol{x}\in\mathbf{R}^n$与随机脉冲$\boldsymbol{h}\in\mathbf{R}^n$进行卷积。根据傅里叶变换的卷积定理，空间域两个函数卷积的傅里叶变换等于这两个函数的傅里叶变换的乘积。因此，随机卷积采用频域处理方法，其过程可以描述为

$$\boldsymbol{x}_c=\boldsymbol{Hx}=\sqrt{n}\,\boldsymbol{F}^*\boldsymbol{\Sigma Fx},\tag{1}$$

式中：$\boldsymbol{F}$为离散傅里叶变换矩阵；$\boldsymbol{F}^*$为$\boldsymbol{F}$的共轭；对角矩阵$\boldsymbol{\Sigma}=\mathrm{diag}\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，其对角线上的非零元素$\sigma_l$是$\boldsymbol{h}$的傅里叶变换系数，具有单位振幅和随机相位。

$$\sigma_l=\begin{cases}\pm1, & l=1,l=n/2+1\\ \exp\left(\mathrm{j}\theta_l\right), & 2\leqslant l\leqslant n/2+1\\ \sigma^*_{n-l+2}, & n/2+2\leqslant l\leqslant n\end{cases},\tag{2}$$

式中：±1等概率出现；θ_l是均匀分布于$[0,2\pi]$的独立白噪声序列；σ^*_{n-l+2}为σ_{n-l+2}的共轭。

信号经过随机卷积之后，再通过随机下采样来压缩信号。随机下采样可以通过随机位置采样和随机调制两种方法实现，前者随机地选择随机卷积结果中的

m个元素，后者将随机卷积结果分为m块，每块随机求和。由于随机解调硬件实现方便，本研究选用随机解调方式。

假设将随机卷积的结果分成m块，每块大小为n/m（假设n能整除m），则随机下采样的最终结果$\boldsymbol{y}\in\mathbf{R}^m$可由下式得到：

$$\boldsymbol{y}=\sqrt{m/n}\,\boldsymbol{P\Theta x}_c, \tag{3}$$

$$\boldsymbol{P}=\begin{bmatrix}1\,1\cdots & & & \\ & 1\,1\cdots & & \\ & & 1\,1\cdots & \\ & & & 1\,1\cdots\end{bmatrix}, \tag{4}$$

式中：$\sqrt{m/n}$为归一化参数；$\boldsymbol{\Theta}$为对角矩阵，其对角元素组成±1等概率出现的序列；$\boldsymbol{P}$是大小为$m\times n$的求和矩阵。因此，整个随机卷积过程可以写成

$$\boldsymbol{y}=\sqrt{m/n}\,\boldsymbol{P\Theta}\sqrt{n}\,\boldsymbol{F}^*\boldsymbol{\Sigma F x}=\boldsymbol{\Phi x}。 \tag{5}$$

从压缩感知的角度看，$\boldsymbol{\Phi}$为观测矩阵，从加密角度看，$\boldsymbol{\Phi}$为线性加密矩阵，该加密矩阵的实现需要两个随机模板：$\boldsymbol{\Theta}$和$\boldsymbol{\Sigma}$，分别为±1等概率随机出现的振幅模板和单位振幅随机相位模板，可以用空间光调制器（SLM）实现，傅里叶变换由透镜组成4f系统实现，矩阵$\boldsymbol{P}$由比随机模板分辨率低的光电探测器实现[28, 33]。

随机卷积方法可以看作是双随机相位编码的一种变体。在DRPE方法中，两块随机相位模板分别位于4f系统的输入平面和傅里叶频谱面，原始图像首先在空间域受到一块随机相位模板的调制，经过傅里叶变换在频率域再受到另一块随机相位模板的调制，然后再经过傅里叶逆变换在输出平面得到加密结果。与DRPE不同，随机卷积中原始图像首先经过傅里叶变换在频率域受到随机相位模板的调制，然后经过傅里叶逆变换在输出平面受到随机振幅模板的调制，最后经过低于随机模板分辨率的探测器进行压缩得到加密结果。因此，受DRPE方法的各种衍生方法的启发，本研究将混沌和分数傅里叶变换用于随机卷积方法中，以期提高随机卷积加密方法的安全性和鲁棒性。

2.3　级联混沌系统

级联混沌系统为两个或多个混沌系统级联之后形成的混沌系统，已证明其具有更高的随机性和安全性[34]。本研究选择Tent-Logistic级联混沌映射生成随机掩模版，其数学表达式如下：

$$h_{n+1}=\begin{cases}\alpha\beta h_n\left(1-\beta h_n\right), & h_n<0.5\\ \alpha\beta\left(1-h_n\right)\left[1-\beta\left(1-h_n\right)\right], & h_n\geqslant 0.5\end{cases}, \tag{6}$$

式中：控制参数$\alpha\in[3.57,4]$、$\beta\in(1,2]$。

3　基于混沌卷积的光学图像分块加密方法

在随机卷积光学图像加密方法[28]的基础上，引入级联混沌系统、分数傅里叶变换和分块压缩感知进一步提高加密方法的安全性和鲁棒性。具体算法流程如图1所示，步骤如下：

输入：待加密图像$\boldsymbol{X}\in\mathbf{R}^{m\times n}$，多维密钥（KEY1，KEY2，KEY3）=$\left(\alpha_1,\beta_1,h_1,\gamma_1,\gamma_2,\alpha_2,\beta_2,h_2\right)$。

输出：加密后图像$\boldsymbol{Y}$。

1）将待加密图像$\boldsymbol{X}\in\mathbf{R}^{m\times n}$分成$B$块子图像，每块子图像$\boldsymbol{X}_j$大小为$m_b\times n_b$。

2）生成随机相位模板。

①根据密钥KEY1中的参数α_1、β_1和初值h_1，按照式（6）产生长度为$2\times m_b\times n_b$的随机序列$\boldsymbol{L}$，将前$m_b\times n_b$元素舍弃，剩余的元素组成$m_b\times n_b$的矩阵$\boldsymbol{R}_1$；

②生成随机相位矩阵$\boldsymbol{R}_p=\exp\left(\mathrm{j}2\pi\boldsymbol{R}_1\right)$；

③从$\boldsymbol{L}$中选择最后一个元素作为下一个子图像的初值h_1'，得到新的KEY1(α_1,β_1,h_1')。

3）混沌卷积。

在随机卷积的基础上，用分数傅里叶变换替代傅里叶变换，用级联混沌系统产生随机相位模板。在进

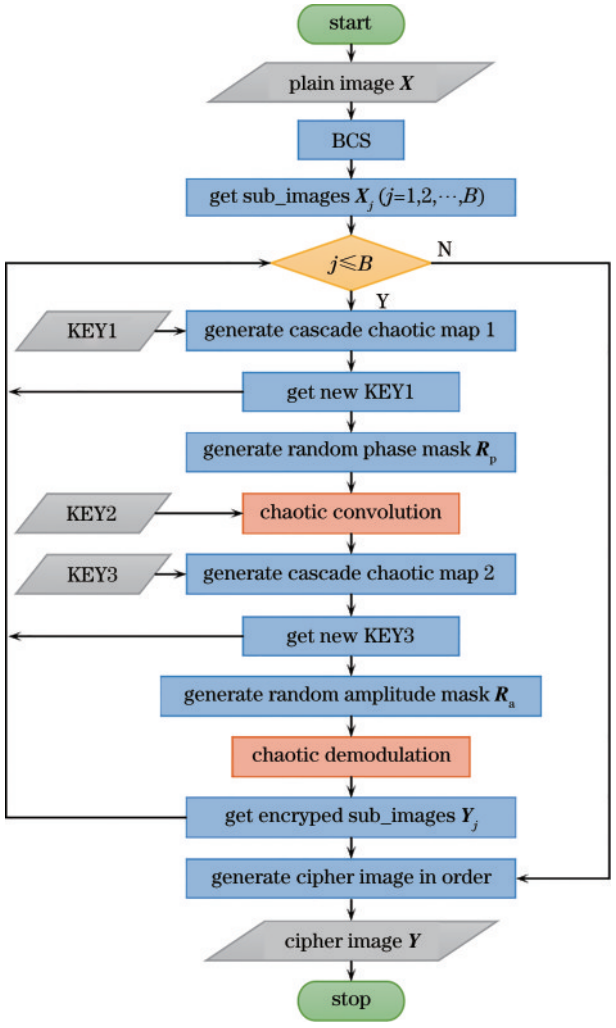

图1　基于混沌卷积的图像加密算法流程图

Fig. 1　Flow chart of proposed image encryption method based on chaotic convolution

行卷积运算时，根据式(1)，需要先将二维矩阵转为一维长向量，然后再进行矩阵相乘，得到卷积后的长向量后再转为二维图像矩阵，这种计算方式较费时，因此采用二维矩阵点乘方法：

$$\boldsymbol{X}_{cj}=\mathrm{Fr}_{\gamma_2}\left\{\boldsymbol{R}_{\mathrm{p}}\odot\mathrm{Fr}_{\gamma_1}\left\{\boldsymbol{X}_j\right\}\right\},\tag{7}$$

式中：$\mathrm{Fr}_{\gamma_1}\{\cdot\}$表示$\gamma$阶分数傅里叶变换；分数阶数$\gamma_1$和$\gamma_2$为密钥KEY2；$\odot$表示矩阵点乘，即矩阵相应位置的元素相乘；$\boldsymbol{R}_{\mathrm{p}}$的元素对应式(1)中$\boldsymbol{\Sigma}$矩阵的对角元素。与式(1)相比，式(7)的计算量更少，更适合于二维图像运算。

4) 生成随机振幅模板。

①根据密钥KEY3中的参数α_2、β_2和初值h_2，按照步骤2)中①和③的方式生成$m_b\times n_b$的矩阵$\boldsymbol{R}_2$和新的初值h_2'，得到新的KEY3(α_2,β_2,h_2')，并对矩阵$\boldsymbol{R}_2$进行去均值处理，即$\boldsymbol{R}_2=\boldsymbol{R}_2-\bar{\boldsymbol{R}}_2$。

②生成随机振幅矩阵$\boldsymbol{R}_{\mathrm{a}}=[\boldsymbol{R}_2]+1$，$[\cdot]$表示取整运算，$\boldsymbol{R}_{\mathrm{a}}$的取值为1或0。$\boldsymbol{R}_{\mathrm{a}}$的元素对应式(3)中$\boldsymbol{\Theta}$矩阵的对角元素。

5)混沌解调。

混沌解调先采用随机振幅矩阵置乱卷积后的结果，然后进行下采样。考虑到运算量和时间，仍采用矩阵点乘的方式进行置乱，下采样采用文献[33]所用的方法，即先经过离散小波变换再进行截断：

$$\boldsymbol{Y}_j=[1:m_d,1:n_d]\odot W\left\{\boldsymbol{X}_{cj}\odot\boldsymbol{R}_{\mathrm{a}}\right\},\tag{8}$$

式中：$W\{\cdot\}$表示二维离散小波变换；$[1:m_d,1:n_d]\odot$表示截取矩阵的$1:m_d$行和$1:n_d$列；$\boldsymbol{Y}_j$为加密后的子图像。小波基采用小波9/7基，经解调后子图像的大小被压缩为$m_d\times n_d$，压缩率$C_{\mathrm{r}}=(m_d\times n_d)/(m_b\times n_b)$。

6)对于某一块子图像，执行步骤2)～5)，将所获得的加密子图像按顺序拼成最终的密文图像$\boldsymbol{Y}\in\mathbf{R}^{\sqrt{C_{\mathrm{r}}}m\times\sqrt{C_{\mathrm{r}}}n}$。值得注意的是，由于混沌序列的初值不同，每块子图像所用的随机模板都不同，从而增加了加密系统的安全性。

上述加密过程在具体实现时：原始图像的分块和混沌序列生成等预处理操作可以在计算机上完成；预处理后的子图像、随机相位模板和随机振幅模板分别用相同分辨率的空间光调制器实现；分数傅里叶变换可以采用两个透镜组成Lohmann Ⅰ型单透镜系统来实现；混沌解调中的下采样可以用分辨率低于空间光调制器的光电探测器实现。因此该加密方法相比DRPE方法，降低了对光电探测器分辨率的要求。

该算法是对称加密算法，解密过程是加密的逆过程，其解密算法可简单描述如下：

输入：密文图像$\boldsymbol{Y}$，多维密钥(KEY1，KEY2，KEY3)$=(\alpha_1,\beta_1,h_1,\gamma_1,\gamma_2,\alpha_2,\beta_2,h_2)$。

输出：解密后图像$\boldsymbol{X}'$。

1) 将密文图像$\boldsymbol{Y}$分成B块子图像；

2) 利用KEY3密钥生成随机振幅矩阵$\boldsymbol{R}_{\mathrm{a}}$，并更新KEY3；

3) 针对子图像进行混沌解调的逆运算

$$\boldsymbol{X}_{cj}=\boldsymbol{R}_{\mathrm{a}}\odot W'\left\{\boldsymbol{Y}_j\right\},\tag{9}$$

式中：$W'\{\cdot\}$为二维离散小波逆变换，变换时小波基扩展到$m_b\times n_b$大小。

4) 利用KEY1密钥生成随机相位矩阵$\boldsymbol{R}_{\mathrm{p}}$，并更新KEY1；

5) 利用KEY2密钥进行混沌卷积逆运算：

$$\boldsymbol{X}_j=\mathrm{Fr}_{-\gamma_1}\left\{\boldsymbol{R}_{\mathrm{p}}^{*}\odot\mathrm{Fr}_{-\gamma_2}\left\{\boldsymbol{X}_{cj}\right\}\right\},\tag{10}$$

式中：$\boldsymbol{R}_{\mathrm{p}}^{*}$表示$\boldsymbol{R}_{\mathrm{p}}$的共轭。

6) 对于每一块子图像，执行步骤2)～5)，将所获得的解密子图像按顺序拼成最终的明文图像$\boldsymbol{X}'\in\mathrm{R}^{m\times n}$。

4 仿真及性能分析

使用Matlab2015a进行系统仿真，测试图像为256×256的Lena、Peppers、Boat等3幅标准灰度图。加密系统的多维密钥参数$(\alpha_1,\beta_1,h_1,\gamma_1,\gamma_2,\alpha_2,\beta_2,h_2)=(3.99,1.99,0.35,0.40,0.50,3.97,1.94,0.45)$。为定量分析图像加密解密效果，采用峰值信噪比($P_{\mathrm{SNR}}$)作为评价标准：

$$P_{\mathrm{SNR}}=10\lg\frac{255^2\times M\times N}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij}-X_{ij}'\right)^2},\tag{11}$$

式中：$\boldsymbol{X}$、$\boldsymbol{X}'$分别表示大小为$M\times N$的原图像和解密图像矩阵，X_{ij}，X_{ij}'为对应(i,j)位置处的像素值。

4.1 加密算法有效性分析

以Lena和Peppers测试图像为例，将图像分成大小为128×128的非重叠块，每个块中随机子采样的块大小为2×2，即加密图像的大小为128×128，压缩率为0.25。图2给出测试图像的加密和解密结果。从图2可以看出，加密图像在视觉上与噪声类似，完全看不出原图信息，解密图像可以正确恢复原始图像。

进一步分析分块大小和压缩比对解密图像质量的影响。表1为压缩率为0.25(即加密图像为128×128)、分块子图像不断减小时，解密图像的P_{SNR}值。从表1可以看出，随着分块子图像的减小，解密图像的质量会小幅度下降，因此一般采用128×128大小的图像块进行加密处理。表2为当压缩率不断减小时，解密图像的P_{SNR}值。显然，随着压缩率的降低，解密图像的图像质量变差。但是，即使压缩率降到0.02左右，P_{SNR}也在20 dB以上，这意味着解密后的图像也可以被识别。因此，该方法不仅具有良好的加密能力，而且具有较高的压缩能力。

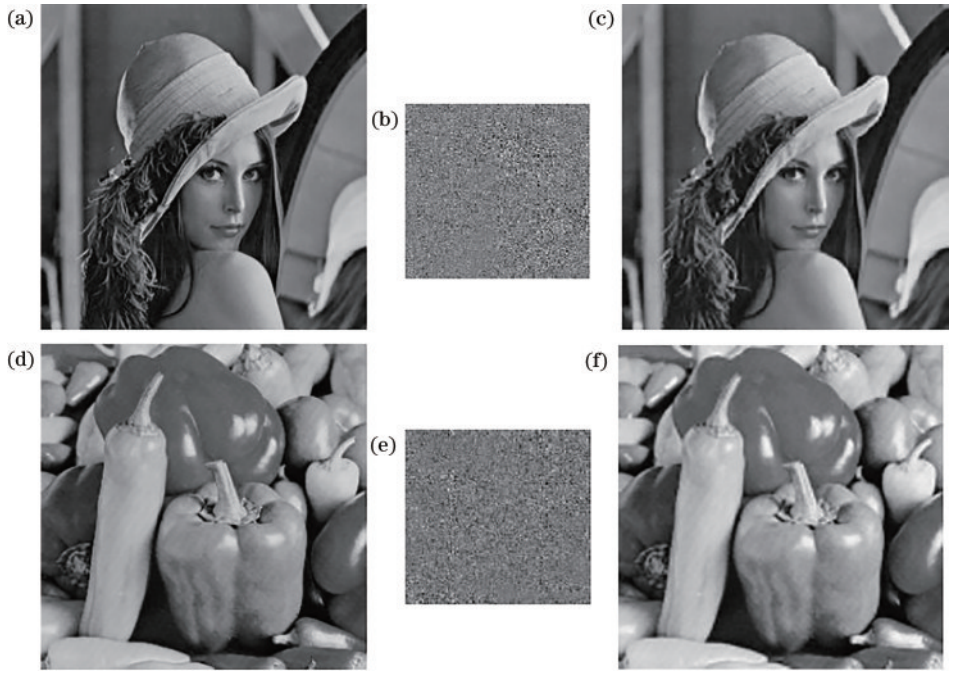

图 2　所提算法加密解密结果图。(a) (d) Lena 和 Baboon 原图；(b) (e) 相应的加密图像；(c) (f) 相应的解密图像

Fig. 2　Encryption and decryption results of proposed algorithm. (a) (d) Original Lena and original Baboon; (b) (e) corresponding encrypted images; (c) (f) corresponding decrypted images

表 1　不同分块大小下解密图像的 P_{SNR} 值

Table 1　P_{SNR} values of decrypted images with different block size

P_{SNR} /dB	256×256	128×128	64×64	32×32
Lena	31.4661	31.4574	31.4500	31.1969
Peppers	30.7387	30.7340	30.7016	30.6177
Boat	31.9350	31.3812	31.3271	31.0849

此外，为了进一步说明混沌卷积方法的优越性，将所提方法与现有基于随机卷积的加密方法[28]及基于 CS 和 FrFT 的 DRPE 方法（类似于[25]中的方案，但没有混沌置乱）进行对比。后者采用与所提方法相同的参数，由级联混沌系统生成两个随机相位掩模，观测矩阵采用高斯随机矩阵。表 2 列出了不同压缩率下 50 次平均后的 P_{SNR} 值。显然，与随机卷积方法相比，所提方法在相同压缩率的情况下，解密图像的质量更好。此外，与 DRPE 方法相比，所提方法在具有相当的重建质量的同时，所需的测量量更少，即具有更强的压缩能力。

表 2　不同压缩率下解密图像的 P_{SNR} 值

Table 2　P_{SNR} values of decrypted images with different compression ratio

Image	Proposed method		Random convolution in reference[28]		DRPE based on CS and FrFT	
	C_r	P_{SNR} /dB	C_r	P_{SNR} /dB	C_r	P_{SNR} /dB
Lena	0.2500 (128×128)	31.4574	0.2500 (128×128)	28.8792	0.5000(128×256)	31.9065
	0.0625 (64×64)	25.9983	0.0625 (64×64)	23.5417	0.3320(85×256)	26.1014
	0.1250^2(32×32)	22.1047	0.1250^2(32×32)	20.4360	0.2500(64×256)	14.0980
Peppers	0.2500 (128×128)	30.7340	0.2500 (128×128)	28.6278	0.5000(128×256)	32.0356
	0.0625 (64×64)	25.9754	0.0625 (64×64)	23.4546	0.3320 (85×256)	25.6076
	0.1250^2 (32×32)	21.7120	0.1250^2 (32×32)	20.2588	0.2500(64×256)	11.6111
Boat	0.2500 (128×128)	31.3812	0.2500 (128×128)	29.2567	0.5000(128×256)	31.8176
	0.0625 (64×64)	26.4538	0.0625 (64×64)	23.8030	0.3320 (85×256)	26.3899
	0.1250^2 (32×32)	22.0111	0.1250^2 (32×32)	21.1395	0.2500(64×256)	11.2389

4.2　鲁棒性分析

图像在传输过程中易受到噪声的污染或被损坏，造成图像信息的失真，因此图像加密算法对噪声和数据损失的稳健性是衡量其性能的一个重要指标。选择 Lena 图像进行测试。

假设加密图像 $\boldsymbol{E}$ 被噪声污染成为 $\boldsymbol{E}'=\boldsymbol{E}(1+k\boldsymbol{G})$，$k$ 是与噪声强度有关的系数，$\boldsymbol{G}$ 表示零均值、标准方差为 1 的高斯噪声。图 3 为不同噪声强度攻击下的解密图像。显然，随着噪声强度的增加，解密后的图像逐渐模糊，但即使在噪声强度较大时图像仍可以分辨。

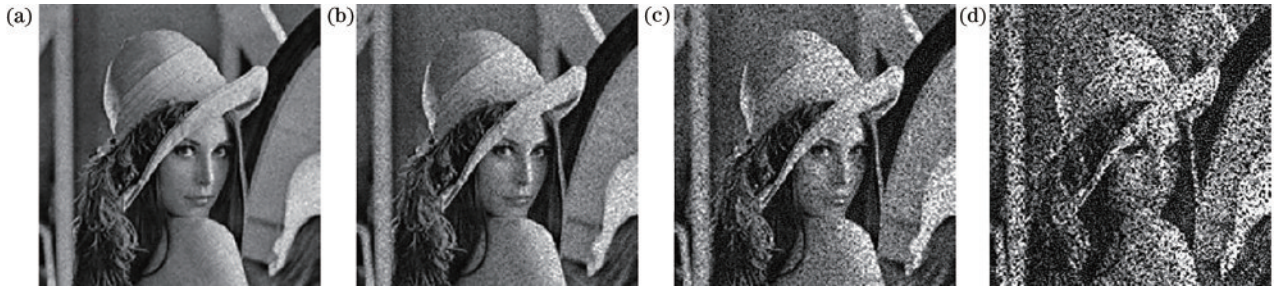

图 3　不同强度噪声攻击下的解密图像。(a) k=0.05、P_{SNR}=28.6261 dB；(b) k=0.1、P_{SNR}=24.0310 dB；(c) k=0.2、P_{SNR}=18.6476 dB；(d) k=0.5、P_{SNR}=11.7872 dB

Fig. 3　Decrypted images of noise attack with different intensities. (a) k=0.05, P_{SNR}=28.6261 dB; (b) k=0.1, P_{SNR}=24.0310 dB; (c) k=0.2, P_{SNR}=18.6476 dB; (d) k=0.5, P_{SNR}=11.7872 dB

图 4 为加密图像在 1/8、3/8 和 1/2 像素被裁剪后的解密结果。从图 4 可以看出，随着缺失像素的增加，解密图像的质量下降，但即使裁剪一半像素，也能识别出图像的重要特征。此外，由于使用分块压缩感知，如果一个块中缺少像素，则只有解密图像的对应块模糊，其他块仍可以很好地重构，如图 4(a)所示。

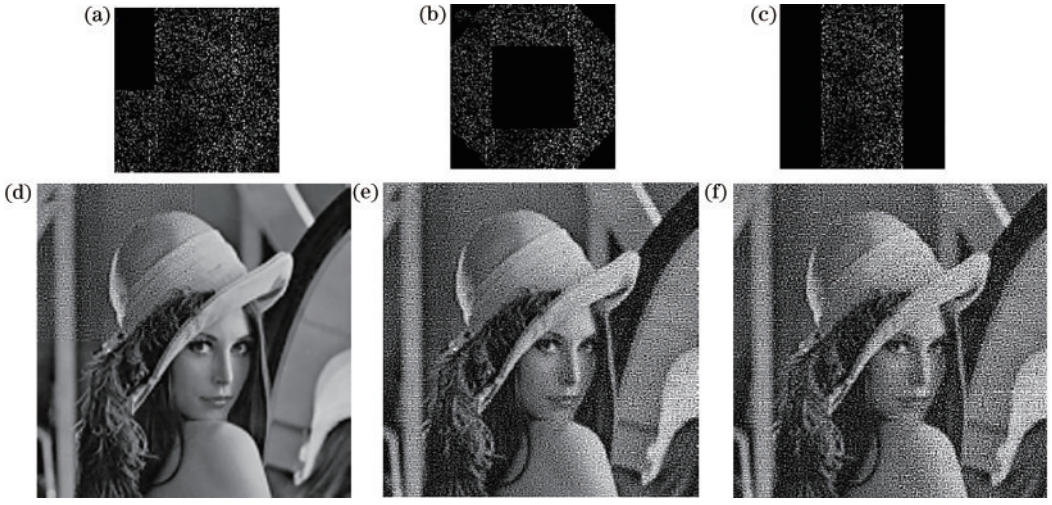

图 4　裁剪攻击。(a)裁剪 1/8 的加密图像；(b)裁剪 3/8 的加密图像；(c)裁剪 1/2 的加密图像；(d)图 4(a)的解密图像，P_{SNR}=24.3597 dB；(e)图 4(b)的解密图像，P_{SNR}=19.4396 dB；(f)图 4(c)的解密图像，P_{SNR}=17.6242 dB

Fig. 4　Cropping attack. (a) Encrypted image with 1/8 cropping; (b) encrypted image with 3/8 cropping; (c) encrypted images with 1/2 cropping; (d) decrypted image of Fig. 4 (a), P_{SNR}=24.3597 dB; (e) decrypted image of Fig. 4 (b), P_{SNR}=19.4396 dB; (f) decrypted image of Fig. 4 (c), P_{SNR}=17.6242 dB

4.3　统计特性分析

灰度直方图是图像统计特性的一个重要特征。理想的加密算法应使不同的原始图像具有均匀的统计分别或者类似的与原始图像无关的直方图。

图 5(a)为用于测试的原始图像，图 5(b)为原始图像的直方图，图 5(c)为相应加密图像的直方图。其中，横坐标表示灰度级，纵坐标表示各灰度级在图像中出现的频率，横纵坐标均无量纲。从图 5 可以看出，虽然原始图像的直方图完全不同，但是加密后的图像直方图都具有相似的分布特征，表明攻击者无法从加密图像的直方图分析中获得有用的原始信息。

相邻像素间的相关系数是另一个常用的统计特性。理想的加密系统，加密图像相邻像素间的相关系数应该很低，趋向于 0，其计算方法如下：

$$r_{xy}=\frac{\left|C_{ov}(x,y)\right|}{\sqrt{D(x)}\sqrt{D(y)}},\tag{12}$$

$$\begin{cases}D(x)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left[x_i-\bar{x}\right]^2\\ D(y)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left[y_i-\bar{y}\right]^2\\ C_{ov}(x,y)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left[x_i-\bar{x}\right]\left[y_i-\bar{y}\right]\end{cases},\tag{13}$$

式中：N 是像素对 (x_i,y_i) 的总数；$\bar{x}$ 和 $\bar{y}$ 分别是 x_i 和 y_i 的平均值。

表 3 为原始图像和相应的加密图像在垂直、水平和对角等 3 个方向的相邻像素间的相关系数。从表 3

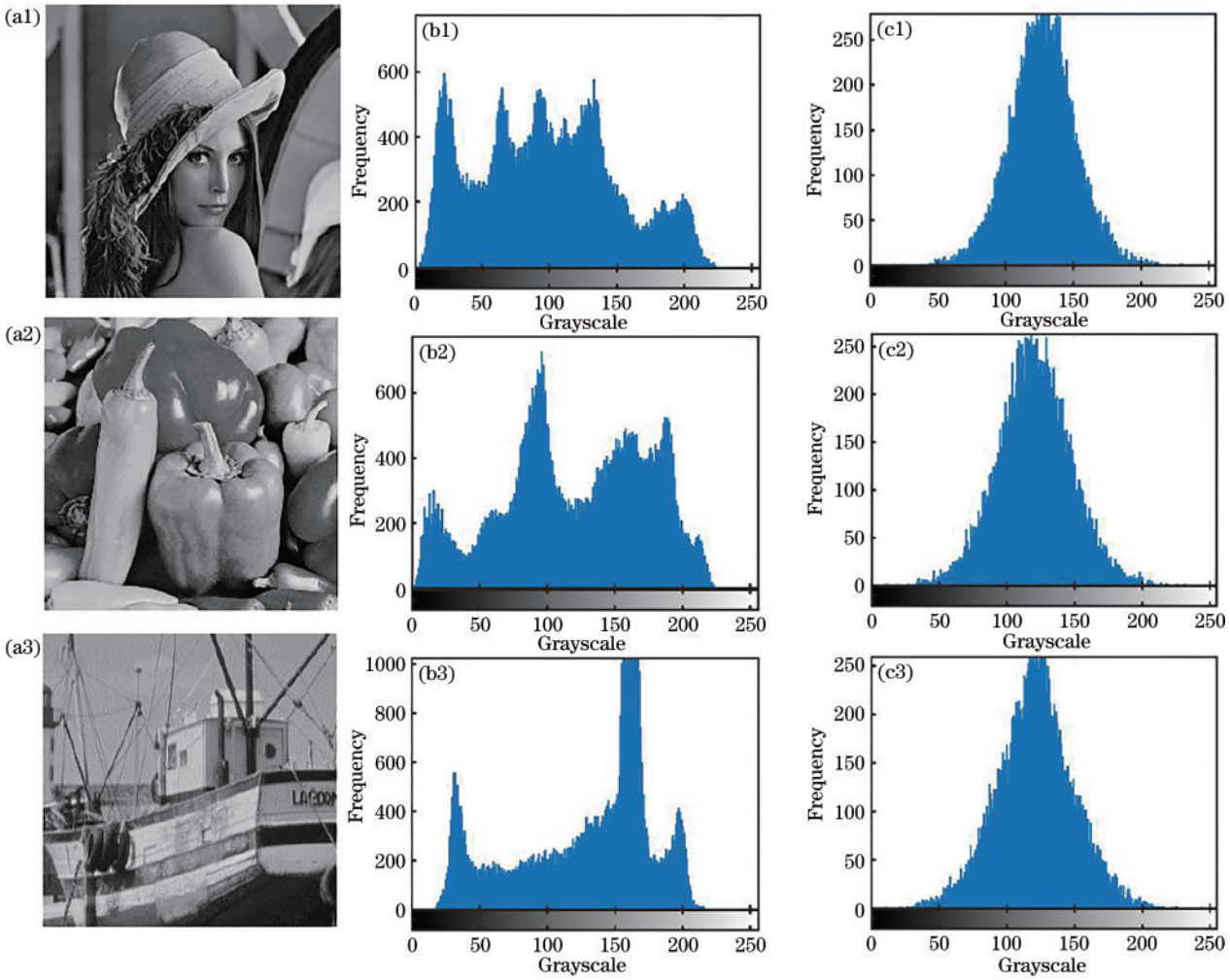

图5　直方图分析。(a)原始图像;(b)原始图像直方图;(c)加密图像直方图

Fig. 5　Histograms analysis. (a) Original images; (b) histograms corresponding to original image; (c) histograms corresponding to encrypted image

表3　原始图像与加密图像的相邻像素相关系数

Table 3　Correlation coefficients of adjacent pixels in plain image and cipher image

Image	Vertical		Horizontal		Diagonal	
	Plain image	Ciper image	Plain image	Ciper image	Plain image	Ciper image
Lena	0.9679	0.0044	0.9342	0.0005	0.9680	0.0024
Peppers	0.9575	0.0014	0.9508	0.0032	0.9575	0.0028
Boat	0.9664	0.0028	0.9419	0.0001	0.9667	0.0024

可以看出,原图像的相邻像素之间的相关系数都很高,而加密后的图像的相关系数非常小,接近于0,表明加密算法破坏了原始图像的相邻像素间的相关性,对统计攻击具有很强的鲁棒性。

4.4　密钥敏感度分析

通常,只要解密密钥发生变化,解密图像就会产生显著变化,称之为密钥敏感性。在所提图像加密方案中,KEY1、KEY3用于产生混沌序列,KEY2对应分数傅里叶变换的分数阶。图6为级联混沌系统的密钥有

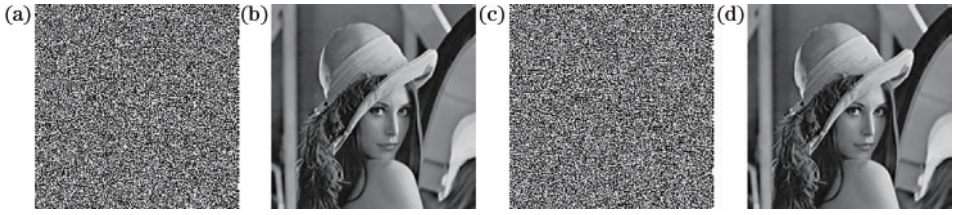

图6　级联混沌系统参数偏差时的解密图像。(a)$\Delta\alpha_2=10^{-15}$、$P_{SNR}=0.9433$ dB;(b)$\Delta\alpha_2=10^{-16}$、$P_{SNR}=31.4574$ dB;(c)$\Delta h_2=10^{-16}$、$P_{SNR}=0.9384$ dB;(d)$\Delta h_2=10^{-17}$、$P_{SNR}=31.4574$ dB

Fig. 6　Decrypted images with deviation in cascade chaotic system parameters. (a) $\Delta\alpha_2=10^{-15}$, $P_{SNR}=0.9433$ dB; (b) $\Delta\alpha_2=10^{-16}$, $P_{SNR}=31.4574$ dB; (c) $\Delta h_2=10^{-16}$, $P_{SNR}=0.9384$ dB; (d) $\Delta h_2=10^{-17}$, $P_{SNR}=31.4574$ dB

极小偏差时的解密图像。从图 6 可以看出：当参数 α_2 在偏差为 $\Delta\alpha_2=10^{-15}$ 时，由于参数错误，解密后的图像不能显示原始图像的任何信息；当偏差为 10^{-16} 时可以正确解密。对于初值 h_2，在偏差为 $\Delta h_2=10^{-16}$ 时不能正确解密，而偏差 10^{-17} 时能恢复原图像，即这两个密钥的灵敏度分别为 10^{-15} 和 10^{-16}。表 4 列出所有密钥参数在极限偏差下相应的解密图像的 P_{SNR} 值。从表 4 可以看出，所提方法对密钥非常敏感，α_1、α_2、β_1、β_2、h_1 的密钥空间均高达 10^{15}，h_2 的灵敏度比 h_1 高一个数量级。

表 4　各密钥偏差时解密图像的 P_{SNR} 值

Table 4　P_{SNR} values of decrypted images with deviation

Parameter deviation	$\Delta\alpha_1=10^{-15}$	$\Delta\beta_1=10^{-15}$	$\Delta h_1=10^{-15}$	$\Delta\alpha_2=10^{-15}$	$\Delta\beta_2=10^{-15}$	$\Delta h_2=10^{-16}$	$\Delta\gamma_1=10^{-2}$	$\Delta\gamma_2=10^{-2}$
P_{SNR} /dB	0.9359	0.9314	0.9423	0.9433	0.9443	0.9384	0.9474	0.9415

根据上述分析，由级联混沌系统的参数构成的密钥空间 $S_1\geqslant 10^{15+15+15+15+15+16}$，分数阶构成的密钥空间 $S_2\geqslant 10^{2+2}$。由于密钥之间的独立关系，整个密钥空间是 S_1 和 S_2 的乘积，即 10^{95}。因此所提算法足以抵抗穷举攻击。

5　结　　论

提出一种基于混沌卷积和混沌下采样技术的光学图像分块加密方法，可同时实现单幅光学图像的压缩和加密。该方法在随机卷积加密方法的基础上，结合级联混沌系统、分数傅里叶变换及分块压缩感知，以提高加密方法的安全性和鲁棒性：利用级联混沌系统产生随机模板，以减少数据的处理和传输，同时满足加密系统的灵敏度要求；利用分数傅里叶变换代替傅里叶变换以进一步增加密钥空间；分块处理可以降低硬件实现时空间光调制器的成本，且混沌下采样技术进一步降低了对光电探测器分辨率的要求，分块并行加密也可以节约时间成本。仿真结果表明：该方法能够抵抗统计攻击、噪声攻击和裁剪攻击。与现有的基于 CS 的 DRPE 方案相比，该方法具有以下 3 个优点：将图像分块，不同的块具有不同的密钥可以提高系统的安全性，同时降低硬件成本和时间成本；不需要单独生成 CS 所需的测量矩阵，加密矩阵即为测量矩阵，可以实现同时加密和压缩；在获得良好加密能力的同时，具有较高的压缩能力。受硬件条件所限，本研究未给出实验结果，今后将进一步研究算法的变形和硬件实现。

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] 王雪, 邵珠宏, 王云飞, 等. 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[J]. 激光与光电子学进展, 2021, 58(4): 0410021.
Wang X, Shao Z H, Wang Y F, et al. Color image encryption based on symmetry of Fourier transform and R-MRSVD[J]. Laser & Optoelectronics Progress, 2021, 58(4): 0410021.

[3] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.

[4] Li G W, Yang W Q, Li D Y, et al. Cyphertext-only attack on the double random-phase encryption: experimental demonstration[J]. Optics Express, 2017, 25(8): 8690-8697.

[5] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics Letters, 2000, 25(12): 887-889.

[6] Lang J, Tao R, Wang Y. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function[J]. Optics Communications, 2010, 283(10): 2092-2096.

[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] Situ G H, Zhang J J. Double random-phase encoding in the Fresnel domain[J]. Optics Letters, 2004, 29(14): 1584-1586.

[9] Chen L F, Zhao D M. Optical image encryption with Hartley transforms[J]. Optics Letters, 2006, 31(23): 3438-3440.

[10] Li H J, Wang Y R. Double-image encryption based on iterative gyrator transform[J]. Optics Communications, 2008, 281(23): 5745-5749.

[11] 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.
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.

[12] 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.

[13] Sui L S, Duan K K, Liang J L. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps[J]. Optics Communications, 2015, 343: 140-149.

[14] 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.

[15] 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.

[16] Joshi M, Shakher C, Singh K. Fractional Fourier plane image encryption technique using radial Hilbert- , and Jigsaw transform[J]. Optics and Lasers in Engineering, 2010, 48(7/8): 754-759.

[17] Cheng X C, Cai L Z, Wang Y R, et al. Security enhancement of double-random phase encryption by amplitude modulation[J]. Optics Letters, 2008, 33(14): 1575-1577.

[18] Jiao S M, Zou W B, Li X. QR code based noise-free optical encryption and decryption of a gray scale image[J]. Optics Communications, 2017, 387: 235-240.

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

[20] 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.
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.

[21] Rachlin Y, Baron D. The secrecy of compressed sensing measurements[C]//2008 46th Annual Allerton Conference on Communication, Control, and Computing, September 23-26, 2008, Monticello, IL, USA. New York: IEEE Press, 2008: 813-817.

[22] Lu P, Xu Z Y, Lu X, et al. Digital image information encryption based on compressive sensing and double random-phase encoding technique[J]. Optik, 2013, 124(16): 2514-2518.

[23] Liu X Y, Cao Y P, Lu P, et al. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. Optik, 2013, 124(24): 6590-6593.

[24] Liu X B, Mei W B, Du H Q. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain[J]. Journal of Modern Optics, 2014, 61(19): 1570-1577.

[25] Liu H, Xiao D, Liu Y B, et al. Securely compressive sensing using double random phase encoding[J]. Optik, 2015, 126(20): 2663-2670.

[26] Wang K S, Wu X J, Gao T G. Double color images compression-encryption via compressive sensing[J]. Neural Computing and Applications, 2021, 33(19): 12755-12776.

[27] Zhou N R, Zhang A D, Zheng F, et al. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing[J]. Optics & Laser Technology, 2014, 62: 152-160.

[28] Zhang Y S, Zhang L Y. Exploiting random convolution and random subsampling for image encryption and compression[J]. Electronics Letters, 2015, 51(20): 1572-1574.

[29] Zhang Y S, Zhou J T, Chen F, et al. A block compressive sensing based scalable encryption framework for protecting significant image regions[J]. International Journal of Bifurcation and Chaos, 2016, 26(11): 1650191.

[30] Gan L. Block compressed sensing of natural images[C]// 2007 15th International Conference on Digital Signal Processing, July 1-4, 2007, Cardiff, UK. New York: IEEE Press, 2007: 403-406.

[31] 李金凤, 赵雨童, 黄纬然, 等. 基于灰度共生矩阵的多尺度分块压缩感知算法[J]. 激光与光电子学进展, 2021, 58(4): 0410002.
Li J F, Zhao Y T, Huang W R, et al. Multi-scale block compressed sensing algorithm based on gray-level co-occurrence matrix[J]. Laser & Optoelectronics Progress, 2021, 58(4): 0410002.

[32] Figueiredo M A T, Nowak R D, Wright S J. Gradient projection for sparse reconstruction: application to compressed sensing and other inverse problems[J]. IEEE Journal of Selected Topics in Signal Processing, 2007, 1(4): 586-597.

[33] Romberg J. Compressive sensing by random convolution [J]. SIAM Journal on Imaging Sciences, 2009, 2(4): 1098-1128.

[34] Zhou Y C, Hua Z Y, Pun C M, et al. Cascade chaotic system with applications[J]. IEEE Transactions on Cybernetics, 2015, 45(9): 2001-2012.