Opto-Electronic Engineering
光 电 工 程

Article

2018 年，第 45 卷，第 6 期

DOI: 10.12086/oee.2018.170732

分数傅里叶变换域的彩色图像非对称光学压缩加密

郎　俊*，付香雪，郭　盼

东北大学计算机科学与工程学院通信与电子工程系，辽宁 沈阳 110004

摘要：为了提高传统双随机相位编码图像光学加密系统的安全性，并减少其所需要处理的数据量，提出了一种基于压缩感知及量子 Logistic 混沌映射的彩色图像非对称光学加密方法。针对彩色图像加密过程中所需要处理数据量过大问题，首先利用压缩感知理论减少加密系统所需要处理的数据量，其次，将彩色图像三通道转换为单通道加密来减少数据量。针对传统光学加密系统为线性系统问题，采用基于相位截断的非对称光学加密方法进行加密。针对光学加密系统加密密钥为随机相位板不方便传输问题，利用量子混沌产生系统所需要的随机相位板。结果表明，此算法可以获得较为理想的图像加密和解密效果。

关键词：压缩感知；光学加密；量子混沌；单通道

中图分类号：O438　　**文献标志码：**A

引用格式：郎俊，付香雪，郭盼. 分数傅里叶变换域的彩色图像非对称光学压缩加密[J]. 光电工程，2018，**45**(6): 170732

Optical color image asymmetric compressed encryption in fractional Fourier transform domain

Lang Jun*, Fu Xiangxue, Guo Pan

Computer Science and Engineering, Northeastern University, Shenyang, Liaoning 110004, China

Abstract: In order to improve the security of traditional optical image encryption and reduce the amount of data what needs to process, we propose a color image asymmetric optical encryption method based on compressed sensing and quantum logistic map, and use the compressive sensing theory and single-channel encrypted method to deal with the problem of large amount of data in the process of color image encryption. Aiming at the linear problem of the traditional optical cryptosystem, we use asymmetric optical encryption based on phase truncation fractional Fourier transform. We also use quantum logistic map to generate the random phase masks for the convenience of transmitting random phase masks. The results show that the proposed algorithm can obtain better image encryption and decryption results.

Keywords: compressive sensing; optical encryption; quantum logistic map; single-channel

Citation: Lang J, Fu X X, Guo P. Optical color image asymmetric compressed encryption in fractional Fourier transform domain[J]. *Opto-Electronic Engineering*, 2018, **45**(6): 170732

收稿日期：2017-12-27； 收到修改稿日期：2018-02-21

基金项目：教育部中央高校基本科研业务经费基金资助项目(N150404004)

作者简介：郎俊(1982-)，男，博士，副教授，主要从事图像加密，压缩感知的研究。E-mail: langjun@mail.neu.edu.cn

1 引 言

近年来，随着信息技术的不断发展，各种各样的信息如图片、视频等可以通过网络进行方便快捷地传输，人们的日常生活和工作学习也越来越离不开网络和信息系统。因此，信息安全越来越引起人们的重视，由于图像信息可以更加清晰传达人们的思想，所以图像信息安全尤为重要。

目前已经提出了许多数字图像加密方法如基于像素置乱的图像加密技术[1]、基于 SCAN 语言的图像加密技术[2]、基于 DNA 计算的图像加密技术[3]等。随着科学技术的发展，对加密系统的要求也越来越高，传统的图像加密方法渐渐无法满足安全性和处理速度的需求。然而，光的波长短、信息量大、含有干涉衍射等多种变换、高速并行处理数据等特点，因此光学加密在图像加密领域是一个很重要的课题。1995 年 Refregier 和 Javidi 提出了最基础的光学加密系统，双随机相位编码(double random phase encoding, DPRE)，其主要原理是在输入平面与傅里叶频谱面上放置两个互不相关的随机相位板，从而对输入图像进行加密[4]。由于分数傅里叶变换在信息安全领域具有重要的地位，许多学者对于基于分数傅里叶变换的光学加密进行了研究[5-7]。2012 年 Lang 提出将分数傅里叶变换改进为多参数分数傅里叶变换，提高加密系统安全性[8]。2014 年 Zhong 提出将离散多参数傅里叶变换引入到双随机相位编码中[9]。为了解决双随机相位编码加密系统为线性系统问题，Qin 提出了基于相位截断的双随机相位编码[10]。2016 年巩琼等人提出了利用相位板抽取原理的光学加密方法，此方法利用衍射成像原理，衍射光强分布作为密文，加密过程不需要移动加密器件，简化了加密过程[11]，但是此方法的密钥为三个相位板，传输与储存不方便，而且解密过程涉及迭代算法处理计算量大。对于彩色图像，1999 年有学者提出利用双随机相位编码加密彩色图像的方案。2001 年 Zhou 提出了基于分数傅里叶变换和混沌系统的单通道彩色图像光学加密算法[12]。2007 年 Joshi 利用分数傅里叶变换对彩色图像光学加密进行了改进[13]。近期也有许多学者针对光学加密与混沌相结合进行研究，如利用超混沌进行双域加密[14]，将双随机相位编码与置换相结合的光学密码分析[15]。

在光学加密过程中会涉及大量的相位运算，加密过程十分复杂，因此有学者提出将压缩感知理论引入到光学加密系统中。压缩感知理论利用远低于奈奎斯特采样定理所需的采样数去恢复原始信号[16-18]。2011 年有学者提出了一种基于压缩感知的数字图像加密方法，只是简单的将压缩感知与传统加密方法结合[19]。2012 年周南润等人提出基于测量矩阵受控的图像压缩感知与图像加密方法[20]。2013 年有学者提出了基于压缩感知的双随机相位编码图像加密，此方法减少了光学加密系统所需要处理的数据量[21]。之后又有人提出了基于压缩感知与 Arnold 变换的光学图像加密[22]。Ahmed 等[23]利用量子混沌提出了一种基于多轮扩散图像加密算法。

本文提出了针对彩色图像的基于压缩感知及相位截断的光学加密方案，该系统实现了彩色图像单通道加密，利用量子 Logistic 混沌映射产生光学加密所需要的随机相位板，极大地减少了所需要传输的密钥的数据量。此方案减少了加密系统所需要处理的数据量同时克服了光学加密系统的线性，提高了安全性，仿真实验表明，该系统可以获得理想的图像加密和解密效果。

2 理论推导

2.1 基础理论

2.1.1 压缩感知理论

压缩感知是一种新的采样理论，完全颠覆了传统的奈奎斯特采样理论，该理论可以利用极少的采样信号恢复出原始信号。在这个过程中要求用于稀疏化的稀疏基和用于测量的测量矩阵是互不相干的。

压缩感知理论主要包含三个主要部分，即信号的稀疏化，信号的测量，信号的重构。压缩感知理论框架如图 1 所示。

假设对于一个一维长度为 N 的实值离散信号 $X(n)=\{x_1,x_2,...,x_n\}\in R^n$， $n\in\{1,2,...,N\}$ 它可以利用 $N\times N$ 的正交基矩阵 $\boldsymbol{\Psi}=\{\psi_1,\psi_2,\cdots,\psi_N\}$ 作为正交基进行稀疏化，此过程可表示为

$$X=\boldsymbol{\Psi}\cdot S \text{ 。} \tag{1}$$

如果一个信号或者它的稀疏表达只包含 $K(K<<N)$ 个非零值，则称此信号是稀疏的，信号的稀疏性是实现压缩感知的前提。之后利用一个与稀疏基 $\boldsymbol{\Psi}$ 互不相关的 $M\times N(M<N)$ 的测量矩阵 $\boldsymbol{\Phi}=\{\phi_1,\phi_2,\cdots,\phi_M\}$ 对稀疏信号进行测量，得到最终的测量值矩阵 $\boldsymbol{Y}=\{y_1,y_2,\cdots,y_M\}$，此过程可表示为

$$\boldsymbol{Y}=\boldsymbol{\Phi}X=\boldsymbol{\Phi}\boldsymbol{\Psi}\cdot S \text{ 。} \tag{2}$$

根据压缩感知理论的条件，测量矩阵 $\boldsymbol{\Phi}$ 与稀疏基

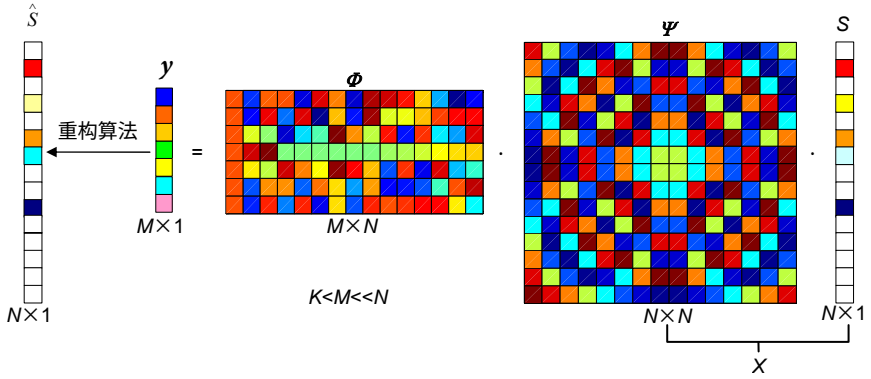


图 1　压缩感知框架示意图

Fig. 1　The schematic of compressive sensing scheme

$\boldsymbol{\Psi}$要满足有限等距性质，即$\boldsymbol{\Phi}$与$\boldsymbol{\Psi}$不相关。则求解 K 个稀疏系数问题可以转化为求解 l_1 最小范数最优化问题，即：

$$\hat{S} = \arg\min \left\| S' \right\|_1 \quad \text{s.t.} \quad \boldsymbol{Y} = \boldsymbol{\Phi\Psi} \cdot S \text{。} \tag{3}$$

在压缩感知进行压缩重构的整体过程中，测量矩阵的设计是关键部分，目前常用的测量矩阵有服从高斯分布的随机矩阵、部分傅里叶矩阵、部分哈达玛矩阵等。本文选取部分哈达玛矩阵作为压缩感知测量矩阵，由于哈达玛矩阵是正交矩阵，从中选取的部分哈达玛矩阵具有较强的非相关性和部分正交性，所以该测量矩阵精确重建所需要的测量数目较少，在同样的测量数目下部分哈达玛矩阵的重建效果较好。

在压缩感知理论中，重构部分是整个理论的核心，现有的重构算法有匹配追踪法(matching pursuit，MP)，正交匹配追踪法(orthogonal matching pursuit，OMP)[24]，基追踪法(basis pursuit，BP)[25]等，由于基追踪法相对成熟且重构效果好，因此本文选用基追踪法作为本文的重构算法。

为了实验压缩率对于信号重构的影响，选取了两幅图像通过不同的压缩率进行对比，由表 1 可以看出压缩率在大于 0.6 的情况下根据实际情况任意选取。

2.1.2　双随机相位编码

双随机相位编码光学加密系统是最基本的光学加密系统，如图 2 所示。系统由两块随机相位板与两个傅里叶变换透镜构成。两块随机相位板分别放置在输入平面与频谱平面，将待加密的原始图像与第一块随机相位板结合进行置乱，再经过透镜的傅里叶变换将

表 1　Lena 图像与 planet 图像恢复图像平均峰值信噪比对比

Table 1　Average PSNR comparison on the reconstructed image in Lena and planet　dB

压缩率	0.9 bpp	0.8 bpp	0.7 bpp	0.6 bpp	0.5 bpp	0.3 bpp
Lena-CS	37.1021	34.1527	32.2742	31.3325	25.1043	20.1543
Planet-CS	40.3420	36.8588	34.4556	32.9497	30.1059	24.5717

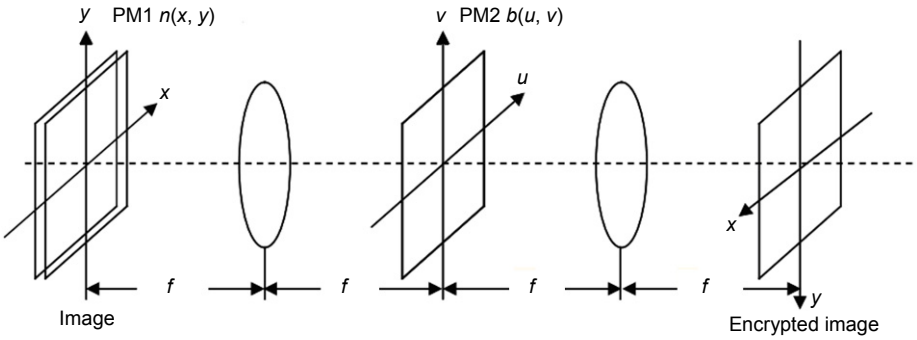


图 2　双随机相位编码加密系统

Fig. 2　The double random phase encoding cryptosystem

其投影到频谱域，再用第二块随机相位板进行置乱，最后经过第二块透镜的傅里叶逆变换输出密文。解密过程为加密的逆过程，解密密钥为两块随机相位板的复共轭。

加密过程可以表示为

$$\boldsymbol{\Psi}(x,y)=FT^{-1}\left\{FT\left\{f(x,y)\exp[\mathrm{i}2\pi n(x,y)]\right\}\cdot\exp[\mathrm{i}2\pi b(u,v)]\right\}。\tag{4}$$

解密过程可以表示为

$$f(x,y)=FT^{-1}\left\{FT\left[\boldsymbol{\Psi}(x,y)\right]\exp\left[-\mathrm{i}\pi b(u,v)\right]\right\}\times\exp\left[-\mathrm{i}2\pi n(x,y)\right]。\tag{5}$$

为了提高系统安全性，有学者提出将傅里叶变换改进为分数傅里叶变换，它是傅里叶变换的一种广义形式。将其引入到光学加密系统中，分数傅里叶变换所需要的角度参数可以作为密钥，增强加密系统的安全性以及密钥敏感度，经过实验对比不同角度的选取对于整个加密系统来说影响不大，可以进行任意的选取。二维分数傅里叶变换表达式如下：

变换核函数为

$$K_{p_1,p_2}(x,y;u,v)=\frac{\sqrt{1-\mathrm{i}\cot\alpha}\sqrt{1-\mathrm{i}\cot\beta}}{2\pi}\cdot\exp\left[\frac{x^2+u^2}{2\tan\alpha}-\mathrm{i}\frac{xu}{\sin\alpha}\right]\cdot\exp\left[\frac{y^2+v^2}{2\tan\beta}+\mathrm{i}\frac{yv}{\sin\beta}\right]，\tag{6}$$

二维分数傅里叶变换为

$$g(u,v)=F^{p_1,p_2}\left\{f(x,y)\right\}=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{p_1,p_2}(x,y;u,v)\cdot f(x,y)\mathrm{d}x\mathrm{d}y\quad，\tag{7}$$

二维分数傅里叶逆变换为

$$f(x,y)=F^{-p_1,-p_2}\left\{g(u,v)\right\}=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}K_{-p_1,-p_2}(x,y;u,v)\cdot g(u,v)\mathrm{d}u\mathrm{d}v\quad。\tag{8}$$

2.1.3 基于相位截断的非对称光学加密

由于双随机相位编码属于线性加密体制，加密密钥与解密密钥相同，无法抵抗已知明文攻击，因此学者提出基于相位截断的非对称光学加密系统如图 3 所示。

此系统加密过程可以表示为

$$g_1(u)=PT\left\{FRFT\left[f(x)R_1(x)\right]\right\}\quad，\tag{9}$$

$$g(x)=PT\left\{IFRFT\left[g(u)R_2(u)\right]\right\}\quad。\tag{10}$$

加密过程中产生的解密密钥为

$$p_2(u)=PR\left\{FRFT\left[f(x)R_1(X)\right]\right\}\quad，\tag{11}$$

$$p_2(x)=PR\left\{IFRFT\left[g(u)R_2(u)\right]\right\}\quad。\tag{12}$$

基于相位截断的光学加密系统加密密钥为两块随机相位板，而解密密钥增加了截断的相位，加密与解密密钥不同，整体系统为非对称加密系统，可以更好地抵抗已知明文攻击。

2.1.4 量子 Logistic 混沌

量子混沌具有经典混沌所具备的各种属性[26]，因此可以应用于加密系统中，对于同一个经典混沌系统，不同的量化标准可以得到不一样的量子混沌映射。Goggin 等通过反冲转子模型量化经典 Logistic 系统，生成一个与之对应的量子 Logistic 映射[27]，其定义为

$$\begin{cases}x_{n+1}=r(x_n-|x_n|^2)-ry_n\\ y_{n+1}=-y_n\mathrm{e}^{-2\beta}+\mathrm{e}^{-\beta}r\cdot\left[(2-x_n-x_n^*)y_n-x_nz_n^*-x_n^*z_n\right]\\ z_{n+1}=-z_n\mathrm{e}^{-2\beta}+\mathrm{e}^{-\beta}r\cdot\left[2(1-x_n^*)z_n-2x_ny_n-x_n\right]\end{cases}，\tag{13}$$

式中：r 为可调参数，β 为耗散参数，x_n、y_n、z_n是系统的状态值，x_n^*、y_n^*分别为 x_n、y_n的复共轭。量子混沌在表现形式上与传统的混沌类似，但由于量子混沌存在扰动量，所以对初值极其敏感，而且扰动量在迭代的过程中不会消失，因此量子混沌可以克服由于计算机精度问题引起的周期性问题。

2.2 加密系统设计

加密系统流程图如图 4，算法的具体步骤如下：

1）对 RGB 三个通道分别进行压缩感知压缩测量，

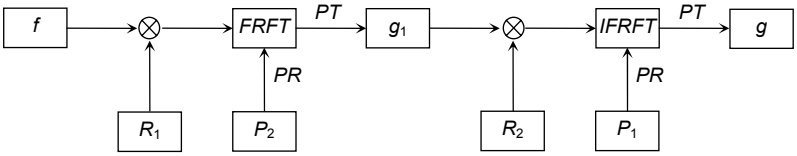


图 3 基于相位截断的非对称光学加密系统

Fig. 3 Asymmetric optical cryptosystem based on phase truncation

得到相应的测量值；

2) 将 G 通道和 B 通道的测量值矩阵进行相应的数学处理变换为两个相位板；

3) 将 R 通道的测量值矩阵作为光学加密系统的输入图像，进行非对称光学加密；

4) 对得到的图像分别进行行和列置乱得到最终的加密图像。

此算法利用压缩感知减少了输入光学加密系统的数据量，针对彩色图像，利用单通道光学加密，不仅减少了加密过程中所需要处理的数据量，而且简化了彩色图像光学加密的过程。在加密系统中，利用量子混沌产生随机相位板，简化了所需要传输的密钥。

3　实验结果

采用 Matlab2014 工具箱进行仿真实验，选取大小为 512×512 的“ Lena ”彩色图像作为原始图像，置乱过程采用随机生成的置乱矩阵，压缩感知处理过程采用部分哈达玛矩阵作为测量矩阵，压缩率选取为 0.7。量子混沌的参数分别选取为 r=3.99，β=4.489，x_0=0.463442265，y_0=0.004532285，z_0=0.002136285，两次分数傅里叶变换选取的参数分别为 0.9、0.1 和 0.5、0.2，实验结果如图 5。其中图 5(a)至图 5(c)分别为原始图像、加密图像和解密图像。

4　数据分析

4.1　直方图分析

统计特性通常利用加密图像与原始图像直方图进行分析，本文选取了三幅图像进行分析。图 6(a)、6(b)、6(c)分别为三幅不同的彩色图像的 RGB 三通道直方图，图 7 为分别对应图 6 的三幅加密图像的直方图，由图 7 中可以看出，三幅彩色图像加密图像的直方图基本一致，说明本算法可以抵抗一定的统计分析。

4.2　抵抗噪声攻击能力

加密图像在传输的过程中通常会受到噪声影响，因此本文进行了相应的抗噪声能力试验，实验结果如图 8 所示，其中图 8(a)为噪声攻击强度为 0.001 时的解密图像，图 8(b)为噪声攻击强度为 0.01 时的解密图像，图 8(c)为噪声攻击强度为 0.1 时的解密图像。从图中可以看出，随着噪声攻击强度的增加，解密图像效果也逐渐模糊，在强度为 0.1 时很难分辨出原始图像。

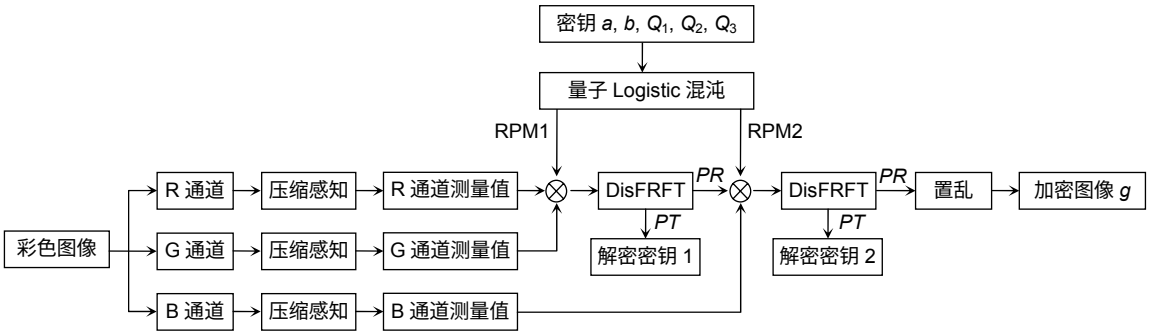


图 4　图像加密系统设计流程

Fig. 4　The flow diagram of the system for image encryption and decryption

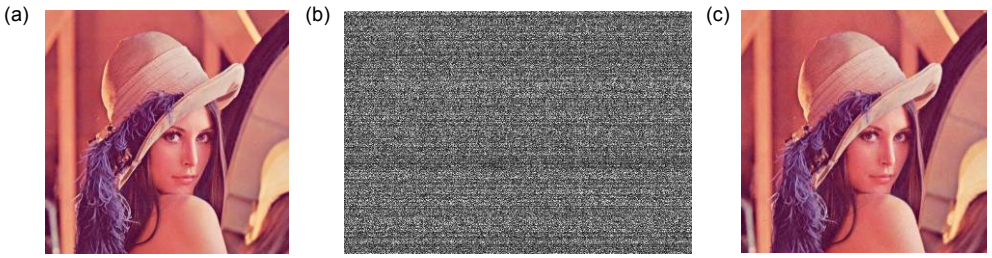


图 5　图像加密解密结果。(a) 原始图像；(b) 加密图像；(c) 解密图像

Fig. 5　The experimental results of image information encryption and decryption. (a) Original image; (b) Encrypted image; (c) Decrypted image

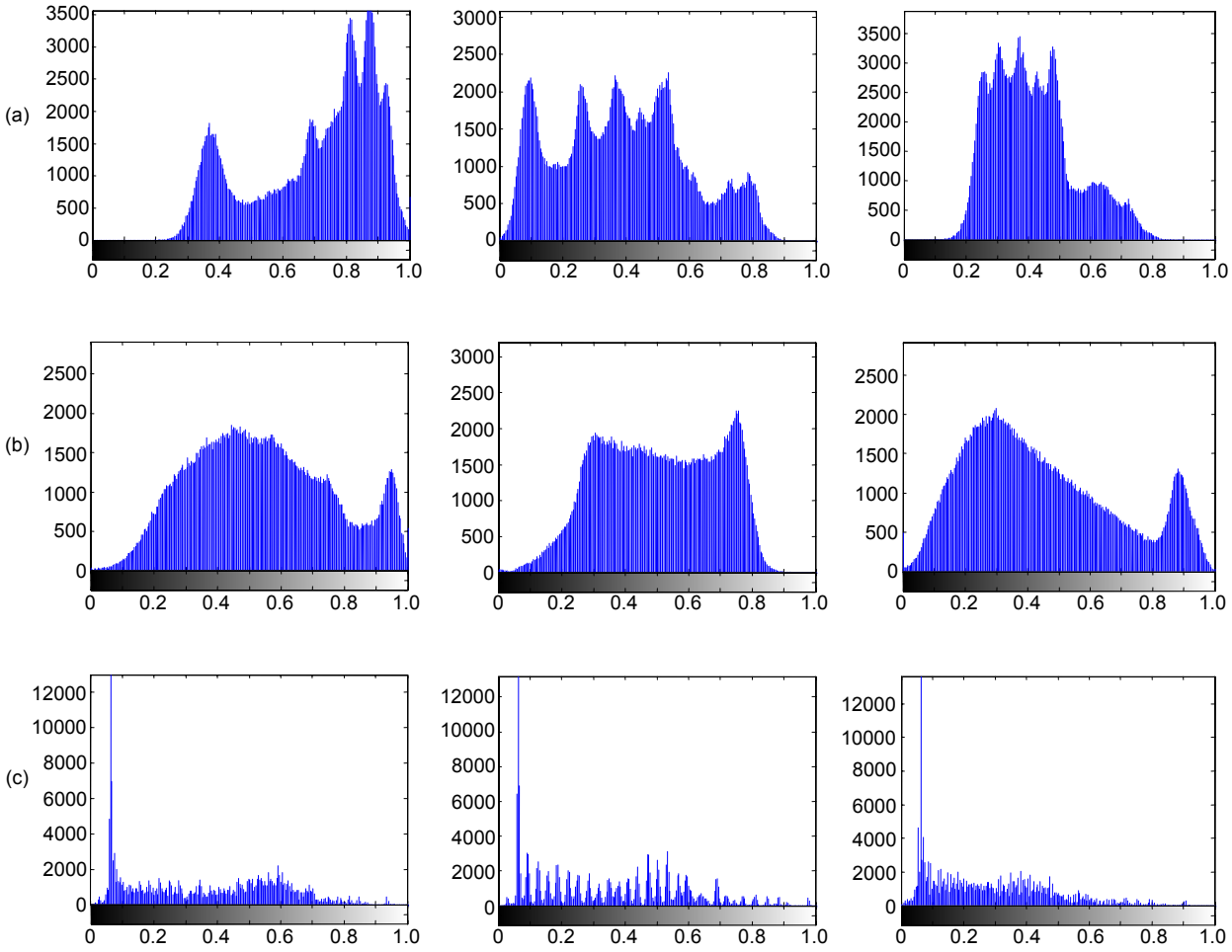


图 6 彩色图像 RGB 分量直方图。(a) Lena; (b) Baboon; (c) Babcat

Fig. 6 The histogram of RGB component of (a) Lena, (b) Baboon, (c) Babcat

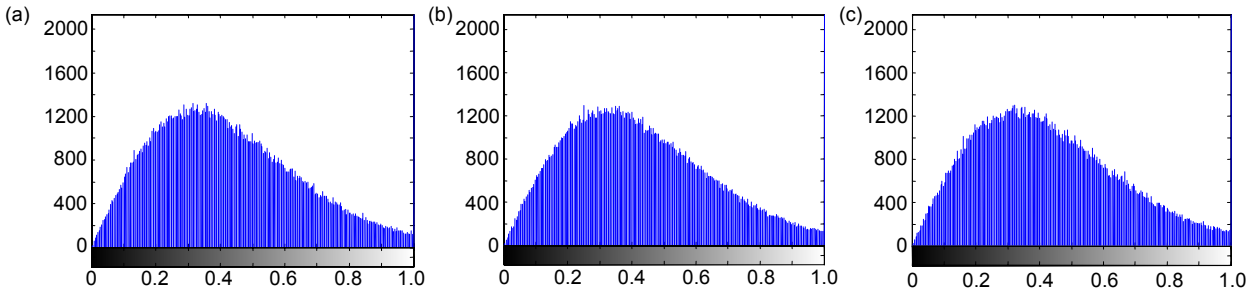


图 7 彩色图像(a) Lena，(b) Baboon 和(c) Babcat 加密后的直方图。

Fig. 7 The histogram after encryption of color images (a) Lena, (b) Baboon, (c) Babcat

4.3 抵抗数据丢失能力

抵抗数据丢失的能力通常利用裁剪来进行验证。图 9(a)、9(b)、9(c)分别为左上角丢失 1%的数据，右下角丢失 5.5%的数据以及中间部分丢失 10.9%的数据的加密图像，图 10 分别对应图 9 的解密图像。由图中可以看出当丢失数据高于 10.9%时，将很难恢复出原始数据。

4.4 密钥敏感度分析

为了分析解密系统对密钥的敏感性，采用错误密钥进行实验，如图 11(a)为分数傅里叶变换参数分别减

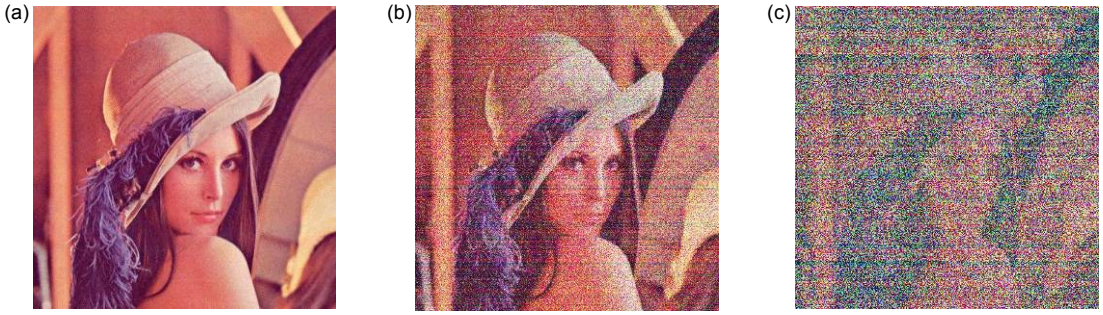


图 8 加密图像受到噪声攻击时的解密图像。(a) 噪声攻击强度为 0.001 时的解密图像; (b) 噪声攻击强度为 0.01 时的解密图像; (c) 噪声攻击强度为 0.1 时的解密图像

Fig. 8 The decryption image when the encrypted image attacked by noise. (a) The decrypted image with the noise attacked intensity of 0.001; (b) The decrypted image with the noise attacked intensity of 0.01; (c) The decrypted image with the noise attacked intensity of 0.1

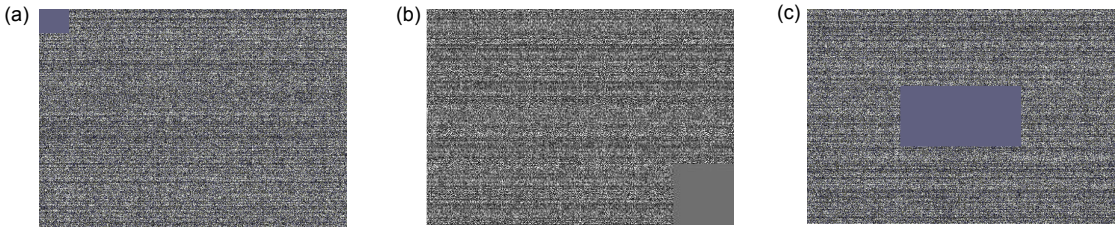


图 9 加密图像。(a) 左上角丢失 1%; (b) 右下角丢失 5.5%; (c) 中间部分丢失 10.9%

Fig. 9 The encrypted image. (a) Losing 1% in top left corner; (b) Losing 5.5% in lower right corner; (c) Losing 10.9% in the middle

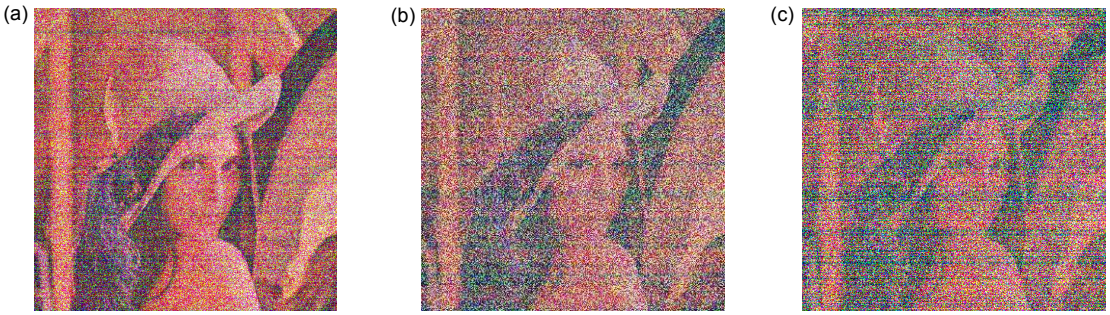


图 10 裁剪攻击图 9(a)、9(b)和 9(c)的解密图像

Fig. 10 The corresponding decrypted image of Fig. 9(a), Fig. 9(b) and Fig. 9(c)

少 0.1 时的解密图像，图 11(b)为采用随机矩阵代替截断相位时的解密图像，图 11(c)为压缩感知测量为随机矩阵时的解密图像。

利用原始信号与解密信号的均方差(mean square error，MSE)去测量系统的安全性，在密钥错误的情况下，均方差越大，表明系统对密钥越敏感，加密系统更加安全。均方差的数学表达式如下：

$$MSE = \|C - E\| = \frac{1}{N \times M} \sum_{n=1}^{N} \sum_{m=1}^{M} \left| C_{n,m} - E_{n,m} \right|^2 \quad 。(14)$$

将本文提出的方法与未经过压缩感知处理的三通道分别进行非对称光学加密的方案，针对量子混沌的参数 x_0 进行错误密钥对比试验，如图 12，实验证明，本文方案的密钥敏感度更高。

4.5 实验对比分析

本文选取了基于 Arnold 置乱的图像加密算法为方法一，基于量子 Logistic 混沌映射的图像加密算法[23]中的多轮替换扩散算法为方法二，基于相位截断的双随机相位编码加密算法[10]为方法三，与本文的算法相

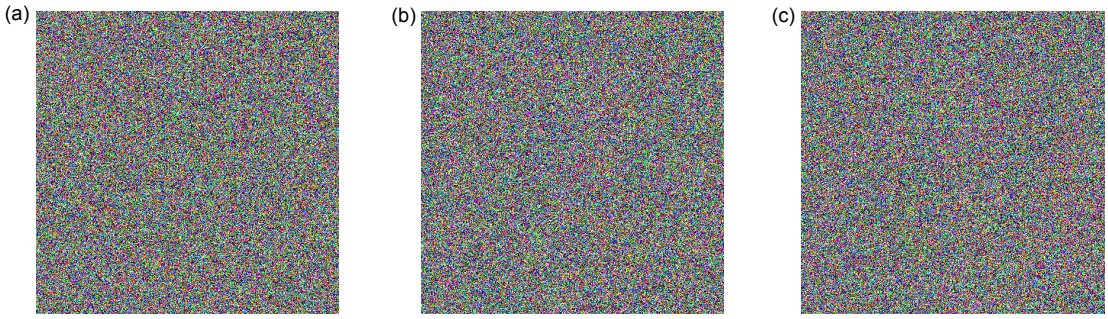


图 11　错误密钥时的解密图像。(a) 分数傅里叶变换参数分别减少 0.1 时的解密图像；(b) 采用随机矩阵代替截断相位时的解密图像；(c) 压缩感知测量为随机矩阵时的解密图像

Fig. 11　The decryption images using wrong keys. (a) The decrypted image with the parameters of FRFT reduced by 0.1; (b) The decrypted image replaced the truncated mask with the random matrix; (c) The decrypted image replaced measurement matrix with the random matrix

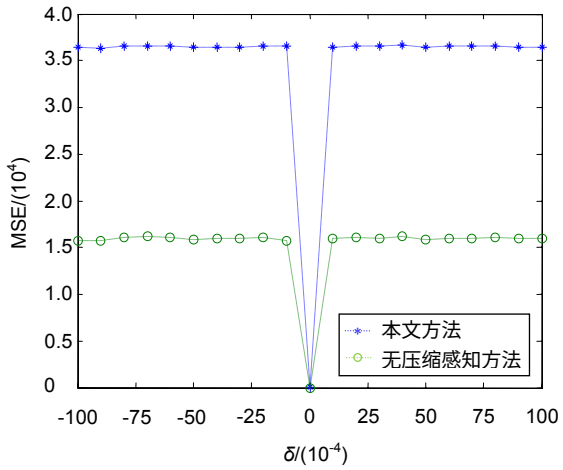


图 12　密钥敏感度对比

Fig. 12　The comparison of key sensitivity

表 2　实验对比表

Table 2　The table of the experiments comparison

方法	PSNR	是否减少数据量	安全性	密钥数据量
方法一	Inf	否	低	小
方法二	56.92	否	中	小
方法三	342.42	否	中	大
本文算法	34.78	11.3%	高	中

对比。表 2 中针对 PSNR，安全性以及密钥数据量等进行对比，由于前三种方法未对图像进行压缩处理，因此解密图像 PSNR 相对高一些，但是在加密过程中处理了许多冗余信息。本文算法经过了压缩感知光学加密等多重加密，安全性相对高一些。

5　结　论

本文提出了一种基于压缩感知与量子 Logistic 混沌映射的图像非对称光学加密，在加密过程中利用压缩感知及单通道加密方法减少系统所需要处理的数据

量，利用量子混沌生成随机相位板，使密钥更加方便传输，最后对光学系统输出的加密图像再进行一次置乱，此系统对原始图像信息进行了多重加密。经过实验分析表明，该方案有较好的加密解密效果，通过安全性分析发现本系统可以抵抗一定的噪声攻击，但抵抗数据丢失的能力较弱，在没有正确密钥的情况下很难恢复出原始信息。

参考文献

[1] Piao Y R, Shin D, Kim E S. Robust image encryption by combined use of integral imaging and pixel scrambling techniques[J]. *Optics and Lasers in Engineering*, 2009, **47**(11): 1273–1281.

[2] Panduranga H T, Naveen Kumar S K. Hybrid approach for image encryption using SCAN patterns and carrier images[J]. *International Journal on Computer Science and Engineering*, 2010, **2**(2): 297–300.

[3] Zhang Q, Guo L, Wei X P. Image encryption using DNA addition combining with chaotic maps[J]. *Mathematical and Computer Modelling*, 2010, **52**(11–12): 2028–2035.

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

[5] Liu S T, Yu L, Zhu B H. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering[J]. *Optics Communication,* 2001, **187**(1–3): 57–63.

[6] Hennelly B, Sheridan J T. Optical image encryption by random shifting in fractional Fourier domains[J]. *Optics Letter*s, 2003, **28**(4): 269–271.

[7] Singh N, Sinha A. Optical image encryption using fractional Fourier transform and chaos[J]. *Optics and Lasers in Engineering*, 2008, **46**(2): 117–123.

[8] Lang J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform[J]. *Optics Communications*, 2012, **285**(10–11): 2584–2590.

[9] Zhong Z, Zhang Y J, Shan M G, *et al*. Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform[J]. *Journal of Optics*, 2014, **16**(12): 125404.

[10] Qin W, Peng X. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Letters*, 2010, **35**(2): 118–120.

[11] Gong Q, Wang Z P, Yang X Q, *et al*. An encryption method based on diffraction imaging principle and phase mask removal method[J]. *Opto-Electronic Engineering*, 2016, **43**(1): 88–94.
巩琼, 王志鹏, 杨兴强, 等. 基于衍射成像原理结合相位板抽取的加密方法[J]. 光电工程, 2016, **43**(1): 88–94.

[12] Zhou N R, Wang Y X, Gong L H, *et al*. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform[J]. *Optics Communications*, 2011, **284**(12): 2789–2796.

[13] Joshi M, Chandrashakher, Singh K. Color image encryption and decryption using fractional Fourier transform[J]. *Optics Communications*, 2007, **279**(1): 35–42.

[14] Yuan W T, Yang X L, Guo W, *et al*. A double-domain image encryption using hyper chaos[C]// *Proceedings of the 19th International Conference on Transparent Optical Networks*, 2017: 1–4.

[15] Chen J X, Bao N, Li J C, *et al*. Cryptanalysis of optical ciphers integrating double random phase encoding with permutation[J]. *IEEE Access*, 2017, 5: 16124–16129.

[16] Candès E J, Romberg J, Tao T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information[J]. *IEEE Transactions on Information Theory*, 2006, **52**(2): 489–509.

[17] Donoho D L. Compressed sensing[J]. *IEEE Transactions on Information Theory*, 2006, **32**(4): 1289–1306.

[18] Jiao L C, Yang S Y, Liu F, *et al*. Development and prospect of compressive sensing[J]. *Acta Electronica Sinica*, 2011, **39**(7): 1651–1662.
焦李成, 杨淑媛, 刘芳, 等. 压缩感知回顾与展望[J]. 电子学报, 2011, **39**(7): 1651–1662.

[19] Huang R, Sakurai K. A robust and compression-combined digital image encryption method based on compressive sensing[C]//*Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, **53**: 105–108.

[20] Zhou N R, Zhang A H, Wu J H, *et al*. Measurement-matrix-controlled image compressive sensing and image encryption method: 102833514A[P]. 2012-12-19.
周南润, 张艾华, 吴建华, 等. 测量矩阵受控的图像压缩感知与图像加密方法: 102833514A[P]. 2012-12-19.

[21] 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-International Journal for Light and Electron Optics*, 2013, **124**(16): 2514–1518.

[22] Liu X Y, Cao Y P, Lu P, *et al*. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. *Optik-International Journal for Light and Electron Optics*, 2013, **124**(24): 6590–6593.

[23] El-Latif A A A, Li L, Wang N, *et al*. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces[J]. *Signal Processing*, 2013, **93**(11): 2986–3000.

[24] Tropp J A, Gilbert A C. Signal recovery from random measurements via orthogonal matching pursuit[J]. *IEEE Transactions on Information Theory*, 2008, **53**(12): 4655–4666.

[25] Chen S S, Donoho D L, Saunders M A. Atomic decomposition by basis pursuit[J]. *SIAM Review*, 2001, **43**(1): 129–159.

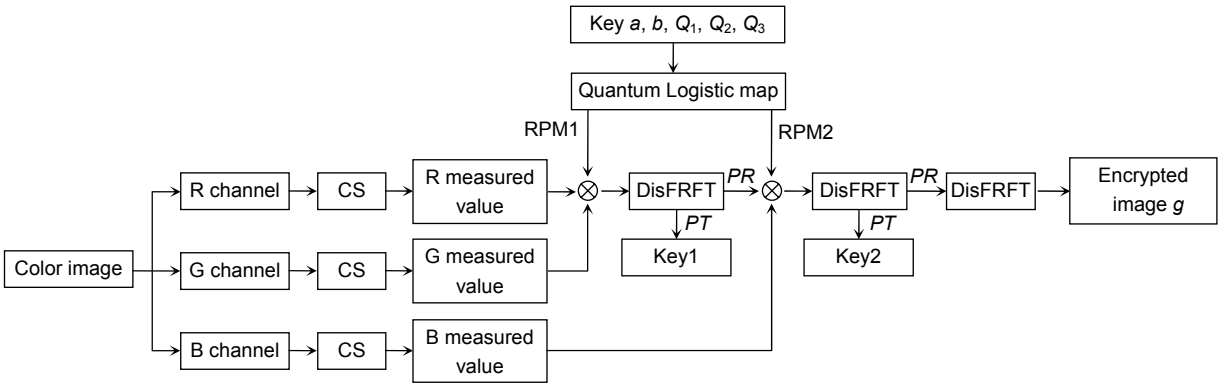
[26] Berry M V, Balazs N L, Tabor M, *et al*. Quantum maps[J]. *Annals of Physics*, 1979, **122**(1): 26–63.

[27] Goggin M E, Sundaram B, Milonni P W. Quantum Logistic map[J]. *Physical Review A*, 1990, **41**(10): 5705–5708.

Optical color image asymmetric compressed encryption in fractional Fourier transform domain

Lang Jun*, Fu Xiangxue, Guo Pan

Computer Science and Engineering, Northeastern University, Shenyang, Liaoning 110004, China



The flow diagram of the system for image encryption and decryption

Overview: In recent years, with the development of multimedia technology, various kinds of information such as pictures, videos can be transmitted conveniently and quickly through the internet. People's work and study also increasingly depend on the network and information system. Therefore, the security of information has drawn more and more attention. Image security is especially important because image information can convey people's thoughts more clearly.

In this paper, we present a novel color image encrypted system based on compressed sensing and quantum logistic map. On the one hand, the system significantly decreases the number of transferred data in the cryptosystem; on the other hand, it increases the security of an encryption system. First, two steps are used to reduce the number of data. Step one, color image traditional encrypted process needs to deal with the data of three channels. In order to convert three-channel of color image to single-channel encrypted, we use some mathematical transformations to convert the green channel and the blue channel into two phase masks and add them into the optical cryptosystem. Single-channel can not only reduce the amount of data what it needs to process, it also simplifies the optical encryption system. Step two, this system significantly decreases the number of data processed in the cryptosystem by utilizing compressed sensing (CS). The most attractive characteristic of CS is that with far fewer samples or measurements than traditional Nyquist sampling methods, one can perfectly reconstruct certain signals. The CS also provides a mechanism for data security because the signal can only be reconstructed if the sensing matrix is known. Second, to enhance security, the proposed algorithm increases the robustness of the system used asymmetric optical encryption system based on the phase truncation fractional Fourier transform. This method can make the system resistant to plaintext attacks, and also make the encryption result a real value, which can save storage space and provide convenience in transmission. At the same time, the parameters of fractional Fourier transform are the keys of the cryptosystem, it adds the number of the keys to enhance security. Finally, to simplify the key exchange, we use quantum logistic chaotic to generate the random phase masks. Instead of transmitting the random phase masks which is hard and inconvenient to transmit and save, only five parameters of quantum logistic map are required. The encryption keys of the cryptosystem are the truncated phase, the fractional orders in the fractional Fourier transform and the parameters of quantum logistic map. The results show that this algorithm can obtain better image encryption and decryption results.

Citation: Lang J, Fu X X, Guo P. Optical color image asymmetric compressed encryption in fractional fourier transform domain[J]. *Opto-Electronic Engineering*, 2018, **45**(6): 170732

Supported by Fundamental Research Funds for the Central Universities (N150404004)

* E-mail: langjun@mail.neu.edu.cn