引用格式：GUO Yuan, WU Lanlan, JING Shiwei. A Phase-truncated Fourier Transform Asymmetric Optical Compression and Encryption System[J]. Acta Photonica Sinica, 2022, 51(6):0610001
郭媛,吴兰兰,敬世伟.一种相位截断傅里叶变换非对称光学压缩加密系统[J].光子学报,2022,51(6):0610001

一种相位截断傅里叶变换非对称光学压缩加密系统

郭媛,吴兰兰,敬世伟
(齐齐哈尔大学 计算机与控制工程学院,黑龙江 齐齐哈尔 161006)

摘 要:基本相位截断傅里叶变换系统面对两步傅里叶迭代等攻击算法时,防御能力差极易被攻破,且加密时间长,密文密钥体积大,不便于分发与传输。提出将压缩感知与相位截断傅里叶变换光学非对称加密相结合,明文经离散小波变换分为低频信息和高频信息,利用压缩感知对高频信息压缩2/3,将其转化为低频信息的相位信息,共同构造大小为原明文图像1/4的待加密复图像。在第一块相位调制模板后增加一块振幅模板,采用设定阈值振幅截断方式,将部分振幅信息作为新私钥,相位角作为密文,实现加解密密钥完全不同,且一图一密。系统安全性能实验、攻击实验和对比实验表明,该加密系统可有效抵御各种攻击,鲁棒性高、传输量小、加密耗时短、解密图像重构质量好,整体性能优良。

关键词:相位截断傅里叶变换;抗攻击性;非对称光学图像加密;压缩感知;离散小波变换
中图分类号:TP391 **文献标识码**:A **doi**:10.3788/gzxb20225106.0610001

0 引言

美国学者 REFREGIER P 和 JAVIDI B[1]于 1995 年提出双随机相位编码(Double Random Phase Encoding, DRPE)光学加密系统,使光学图像加密技术得到快速发展。最近,JMV A[2]提出一种使用非线性联合变换相关因子来实现双随机相位编码的光学安全技术。TAO Yuanchun[3]提出一种明文关联鬼成像加密系统,将参数密钥用椭圆曲线加密,降低密钥空间且提高系统抗攻击能力。ABD-EL-ATTY B[4]提出一种基于量子游走和双随机相位编码技术的新型光学加密,在两个加密阶段使用替代量子漫游(Alternate Quantum Walks, AQW)抵抗来自数字和量子计算机攻击。WW A[5]提出一种通过相位优化生成可信的纯相位全息图方法,用于隐写光学图像加密;利用菲涅尔域优化随机相位和相位约束下改进的两步迭代傅里叶变换算法,计算出全息图,为光学图像提供了一种全息加密新方法。传统DRPE系统是线性对称光学加密系统,加密密钥和解密密钥相同,安全性得不到保障。PENG W Q[6]于2010年提出一种基于PTFT的非对称密码体制,在加密过程中采用相位截断方式得到解密密钥,打破算法的线性运算,实现了加密密钥与解密密钥的分离,系统安全性有了很大提高。2011年WANG X提出基于PTFT图像加密算法的安全增强算法[7],在原来的光学加密系统频谱域中加入一个振幅掩膜。2012年WANG X等[8-9]利用密文和两个公钥这两个约束条件,仅需两步迭代傅里叶变换,便可恢复PTFT系统的私钥信息,攻破PTFT加密系统。针对这个问题,有很多学者对PTFT系统进行改进,2013年DING Xiangling等[10]在原来PTFT系统的输入图像前添加一块不公开的随机相位掩膜,达到扰乱输入图像空间的效果,破坏傅里叶迭代算法的约束条件。2014年WANG X用一种新的攻击算法振幅-相位迭代恢复算法[11]攻破了2011年的安全增强算法[7],2015年GAO Xiong[12]针对幅相迭代恢复算法提出对原来的振幅模板的分布进行调整,设计一种特殊的振幅掩膜板,在原来PTFT加密系统中将调整后的振幅模板放在傅里叶频谱面上来提高抗攻击性。此算法虽然安全

基金项目:国家自然科学基金(No.61872204),黑龙江省自然科学基金(No. LH2021F056),黑龙江省省属高等学校基本科研业务费科研项目(No.135509113),研究生创新科研项目(No.YJSCX2020050)
第一作者:郭媛(1974—),女,教授,博士,主要研究方向为光学检测及图像信息处理。Email:guoyuan171@126.com
通讯作者:吴兰兰(1997—),女,硕士研究生,主要研究方向为图像处理。Email:670913520@qq.com
收稿日期:2021-11-23;**录用日期**:2022-02-17

性提升了，但密文的直方图和相邻相关性分布图不均匀，系统统计特性不好。同时以上加密算法密文体积大，特别是非对称加密，解密密钥与明文一样大小，且无法运用混沌代替，使得传输量进一步加大。2021年XU Zhao等针对基本PTFT系统提出一种深度学习攻击算法[13]，通过以残差网络为基础训练大量的明密文对使神经网络拟合明文和密文之间的对应关系，训练大量手写数字图像后攻破PTFT加密系统，使密文图像基本恢复。

综上，PTFT算法提出至今，虽然实现了非线性光学加密，但仍然存在抗攻击性差的问题，特别是随着深度学习算法的出现，使PTFT系受到了更大的攻击威胁。另外，PTFT加密系统在信息传输时，除了传输一组密文信息外，还需传输两组截取的振幅（相位）信息，信息的传输量增大三倍，传输效率大大降低，运算时间复杂度高。

针对上述问题，本文设计的系统一方面在原来的PTFT加密系统第一块相位掩膜后又加了一块特殊阈值设定的振幅掩膜，用部分振幅截断后保留的相位角作为最终密文，破坏了迭代直接得到全部振幅的可能，使加密系统安全性得到了保证，且密文直方图和相邻相关性分布均匀。另一方面本文提出用压缩感知[14-17]对明文图像进行预处理，运用离散小波变换将图像高低频信息分离，将待加密图像压缩至明文图像的1/4，且有效保留高频信息，减小密文密钥传输体积，缩小传输量节省加密时间。

1 压缩加密原理

可加密系统由图像压缩和PTFT非对称加密两部分构成，如图1。

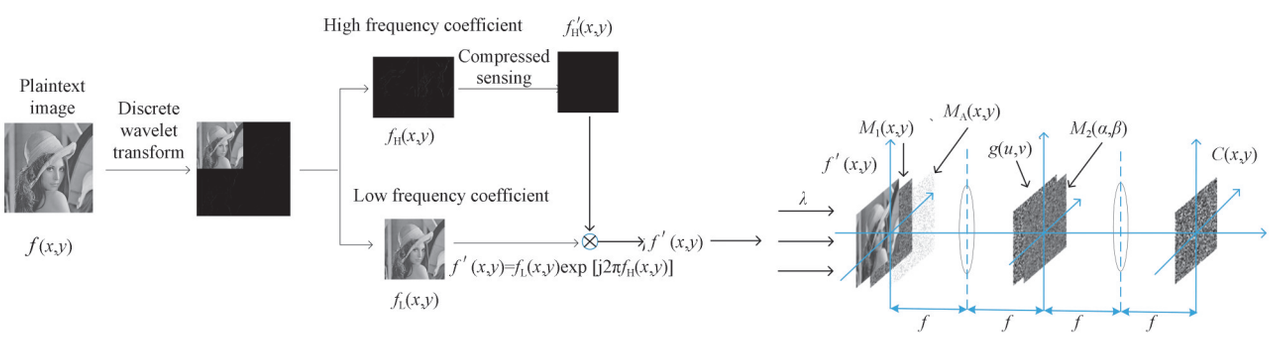


图1 PTFT光学压缩加密系统工作原理

Fig.1 Working principle of PTFT optical compression encryption system

图像压缩部分先将明文图像进行离散小波变换，分为低频系数和高频系数，再将高频部分用压缩感知压缩至原大小的1/3，并以相位形式融入低频系数，构造大小为明文图像1/4的待加密复数图像。图像高低频的分离及高频信息压缩以相位形式共同构造复图像，不但可以更好地保存明文图像有效信息，高质量重构图像，而且有效减少图像传输量，用时更少、效率更高。

本文PTFT非对称加密部分在基本PTFT系统基础上于第一块相位模板后增加一块振幅模板。复数图像经过相位-振幅模板双重调制后经过透镜进行一次傅里叶变换，取得部分振幅用作私钥一，相位角作为中间值受到第二块相位掩膜的调制后再进行一次傅里叶逆变换，取得振幅用作私钥二，相位角作为最终密文，有效抵抗两步迭代傅里叶变换等多种算法攻击，抗攻击性好，灰度直方图及相邻像素相关性分布更均匀。

2 算法描述

本文加密系统工作流程如图2。

1）首先对明文图像$f(x,y)$进行离散小波变换，将图像分为低频系数$f_L(x,y)$和高频系数$f_H(x,y)$，用压缩感知将高频系数压缩为原来的1/3并以相位形式融入低频系数，构造一个大小为明文图像1/4的待加密复图像$f'(x,y)$，即

$$f'(x,y)=f_L(x,y)\cdot\exp\left(j2\pi f'_H(x,y)\right) \tag{1}$$

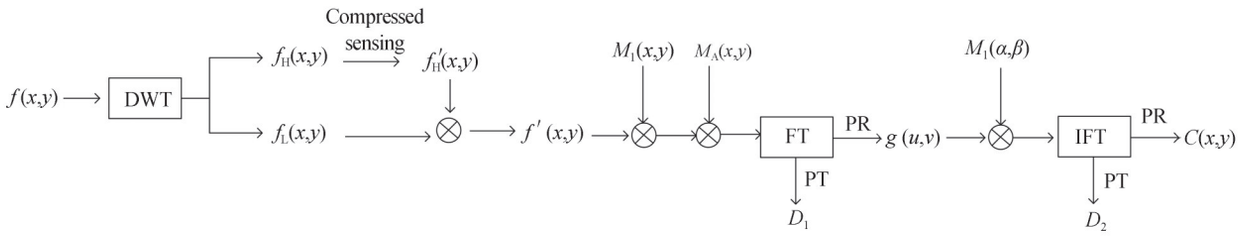


图2　基于压缩感知的PTFT系统加密流程

Fig.2　Encryption flowchart of PTFT system based on compressed sensing

2）设(x,y)为空域坐标系，(α,β)为频域坐标系，$f'(x,y)$经相位模板$M_1(x,y)$和振幅模板$M_A(x,y)$的双重调制，再进行傅里叶变换后截取部分振幅D_1用作私钥给用户保存，保留相位$g(u,v)$作为中间值进一步调制。

$$D_1(x,y)=\mathrm{PT}\left\{\mathrm{FT}\left\{f'(x,y)\cdot M_1(x,y)\cdot M_A(x,y)\right\}\right\} \tag{2}$$

$$g(u,v)=\mathrm{PR}\left\{\mathrm{FT}\left\{f'(x,y)\cdot M_1(x,y)\cdot M_A(x,y)\right\}\right\} \tag{3}$$

式中，$f'(x,y)$为压缩后的复数图像，$M_1(x,y)=\exp\left\{\mathrm{j}2\pi\varphi(x,y)\right\}$和$M_2(\alpha,\beta)=\exp\left\{\mathrm{j}2\pi\phi(\alpha,\beta)\right\}$为两个相位模板，PT{ }为截取振幅操作，PR{ }为相位保留操作，FT{ }表示傅里叶变换，$M_A(x,y)$是根据$M_1(x,y)$而产生的阈值thr再进行赋值而得到的振幅模板，r设定为0.8。

$$M_A(x,y)=\begin{cases}1 & \text{if } m_{ij}\geqslant \mathrm{thr}\\ r & \text{if } m_{ij}<\mathrm{thr}\end{cases} \tag{4}$$

3）$g(u,v)$经相位模板$M_2(\alpha,\beta)$的调制，再进行傅里叶逆变换，截取部分振幅D_2为私钥二保存，相位保留取其相位角为最终密文$C(x,y)$。

$$D_2(\alpha,\beta)=\mathrm{PT}\left\{\mathrm{IFT}\left\{g(u,v)\cdot M_2(\alpha,\beta)\right\}\right\} \tag{5}$$

$$C(x,y)=\arg\left\{\mathrm{IFT}\left\{g(u,v)\cdot M_2(\alpha,\beta)\right\}\right\} \tag{6}$$

式中，IFT{ }表示逆傅里叶变换，arg{ }为取相位角操作。

解密流程和加密流程相反，解密流程如图3。

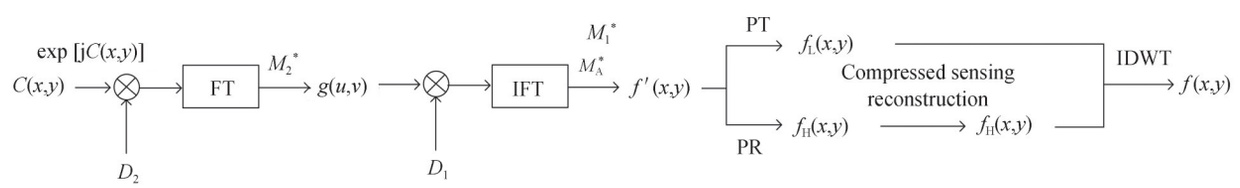


图3　基于压缩感知的PTFT系统解密流程

Fig.3　Decryption flow of PTFT system based on compressed sensing

1）密文$C(x,y)$转化为相位形式后和私钥二D_2相乘，经傅里叶变换后与$M_2(\alpha,\beta)$的复共轭$M_2{}^*(\alpha,\beta)=\exp\left\{-\mathrm{j}2\pi\phi(\alpha,\beta)\right\}$相乘保留相位$g(u,v)$。

$$g(u,v)=\mathrm{PR}\left\{\mathrm{FT}\left\{\exp\left[\mathrm{j}C(x,y)\right]\cdot D_2(\alpha,\beta)\right\}\cdot M_2(\alpha,\beta)^*\right\} \tag{7}$$

2）$g(u,v)$与私钥一D_1相乘后经傅里叶逆变换，乘以$M_A(x,y)$的逆振幅调制器$M_A^*(x,y)$和$M_1(x,y)$的复共轭$M_1{}^*(x,y)$得到正确的复图像$f'(x,y)$。

$$f'(x,y)=\mathrm{IFT}\left[g(u,v)\cdot D_1(x,y)\right]\cdot M_A(x,y)^*\cdot M_1(x,y)^* \tag{8}$$

$$M_A^*(x,y)=\begin{cases}1 & \text{if } m_{ij}\geqslant \mathrm{thr}\\ 1/r & \text{if } m_{ij}<\mathrm{thr}\end{cases} \tag{9}$$

3）复图像$f'(x,y)$提取振幅和相位，相位角除以2π后作为高频系数$f_H{}'(x,y)$，振幅作为低频系数

$f_L(x,y)$，高频系数通过正交匹配追踪算法（Orthogonal Matching Pursuit Algorithm，OMP）[18-19]进行重构恢复初始的高频系数$f_H(x,y)$。

4）再将恢复的高频系数$f_H(x,y)$和拆分的低频系数$f_L(x,y)$进行离散小波逆变换，得到明文图像$f(x,y)$。

3 系统特性实验

为验证加密系统的可行性和安全性，选用不同种类的5幅灰度图像在Python3.7和Pycharm环境下进行实验，加解密效果如图4。

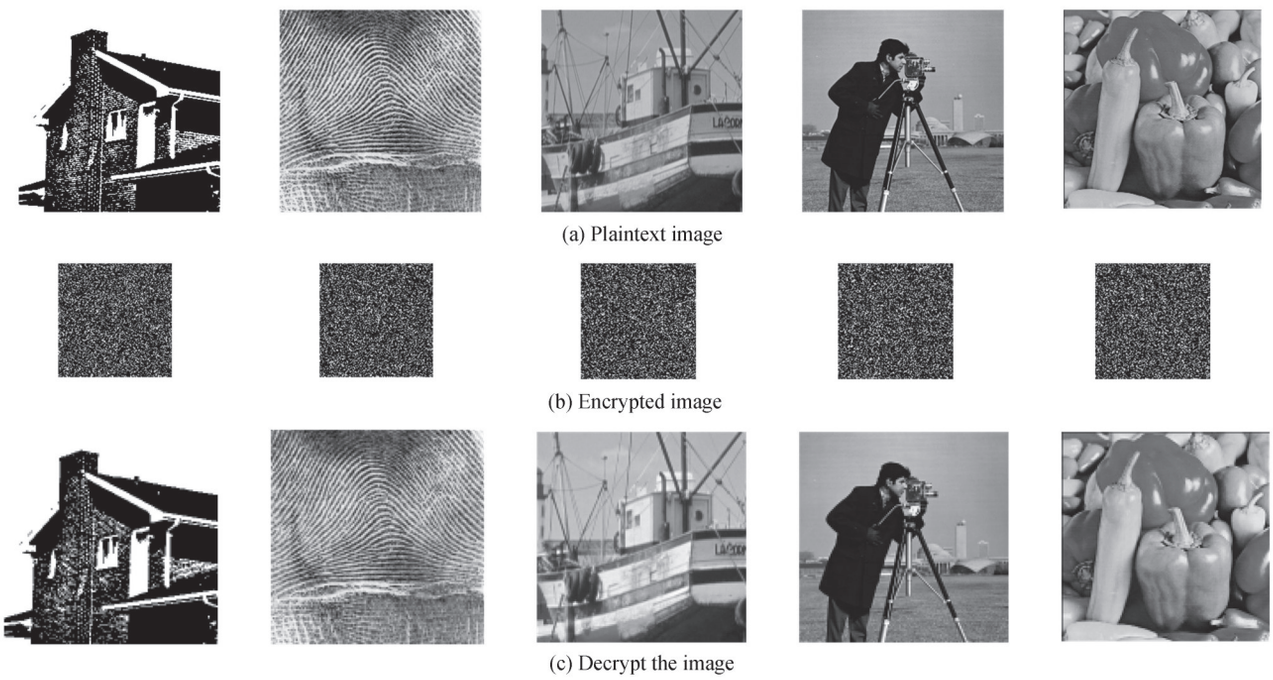


图4 加密系统的加解密图像

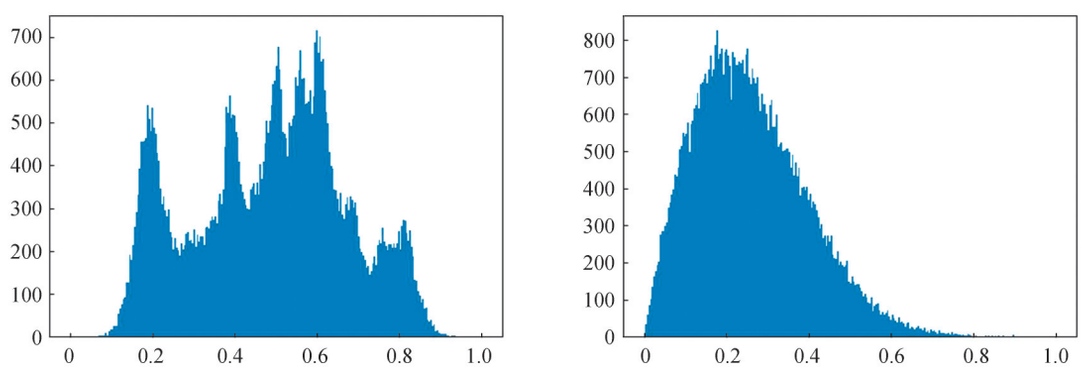
Fig.4 Encryption and decryption image of the encryption system

由图4可见，无论是二值图像、医学图像，还是对比度不同的其他灰度图像，密文图像大小均为明文图像的1/4，且加密图像完全掩盖明文图像的信息，解密图像恢复质量好。

3.1 统计特性分析

3.1.1 灰度直方图

灰度直方图反映图像像素值统计特性，加密图像直方图应尽量均匀与明文图像直方图分布差异较大。本文对明文图像，截断振幅用作密文图像，及相位角用作密文图像和解密图像对比，如图5所示。



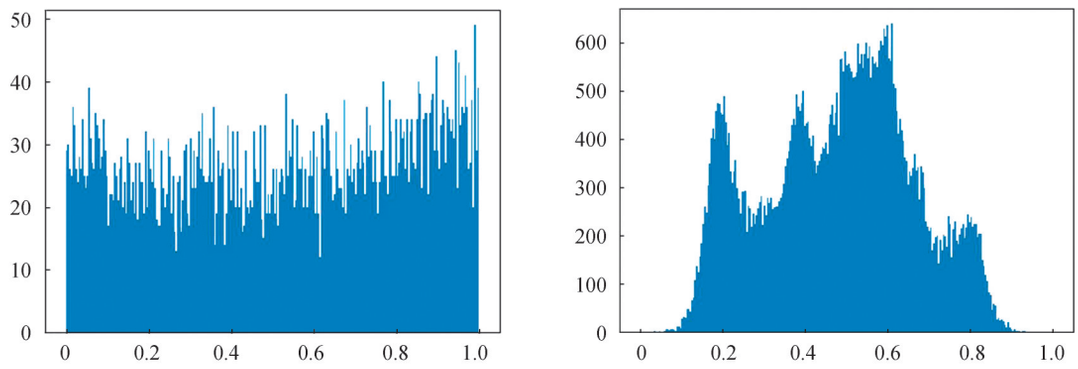


图5　灰度直方图

Fig.5　Grayscale histogram

由图5可见，明文图像和解密图像的灰度值分布不均匀，呈现出明显的分布规律，不管是振幅作为密文还是相位角作为密文直方图都和明文直方图差距明显，本文提出相位角作为密文直方图分布更均匀，更好隐藏明文图像信息。

3.1.2　相邻像素相关性

好的加密方法应对相邻像素相关性具有较强的破坏作用，相邻像素相关性越低，相邻像素相关图越散，系统越安全。

图6是水平方向相邻像素相关性分布图，可见明文图像和解密图像明显相关性较强，提出的以相位角作为密文的分布比以振幅为密文的分布图更散，相关性破坏地更彻底。

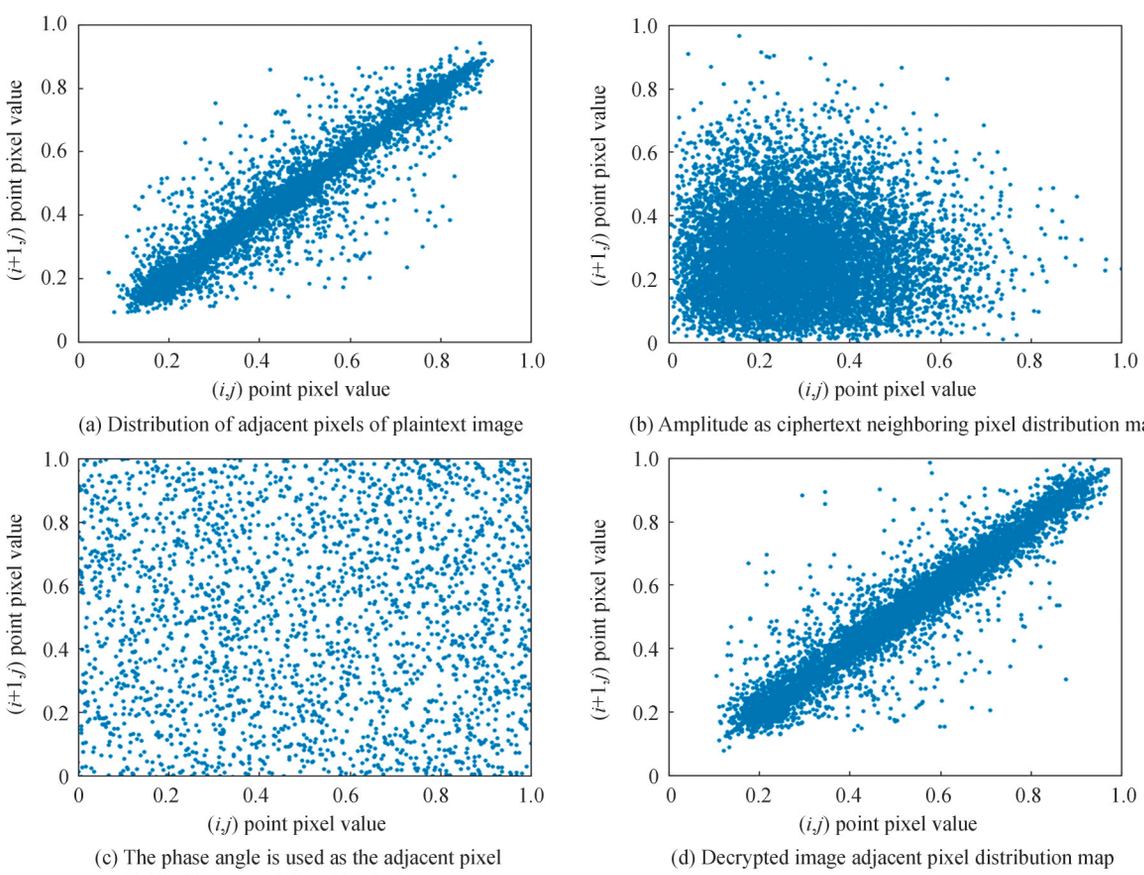


图6　相邻像素相关性分布

Fig.6　Correlation distribution of adjacent pixels

表1中明文图像的水平、垂直和对角的相邻系数都接近于1，而本文提出的相位角作为密文的相关系数更接近于0，效果比振幅作为密文好。

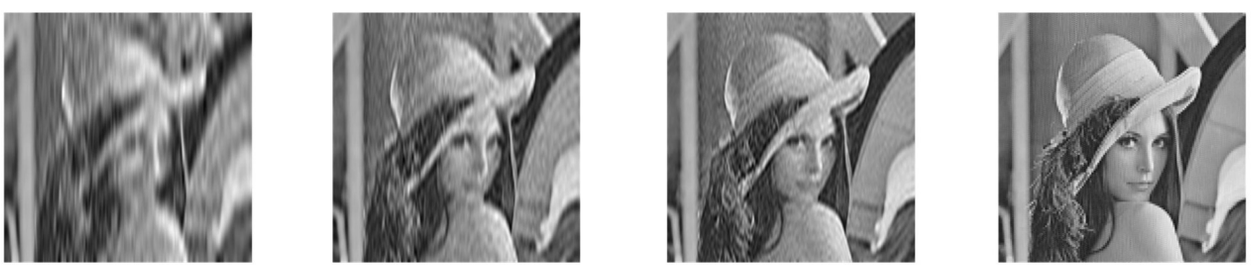
表1 相关系数分析

Table 1 Correlation coefficient analysis

Direction	Level	Vertical	Diagonal
Plaintext image	0.927 244	0.963 116	0.899 516
Amplitude as ciphertext	0.117 206	0.108 999	0.104 825
Phase angle as ciphertext	0.030 592	−0.003 942	0.006 044

3.2 压缩重构质量对比分析

为测试本文压缩后重构质量，与文献[14]压缩方式作对比，具体效果如图7。



(a) Ref. [14] method compressed to 1/4 (b) Ref. [14] method compressed to 1/2 (c) Ref. [14] method compressed to 4/5 (e) The method in this article is compressed to 1/4

图7 不同压缩方式不同比例重构图像

Fig.7 The reconstructed image with different compression methods and different scales

由图7可见，压缩相同比例，本文压缩至明文图像1/4后重构图像比文献[14]压缩至明文图像1/4后重构图像质量好很多，本文压缩至1/4甚至比文献[14]压缩至4/5重构质量更好。

表2可见，本文压缩至明文图像的1/4后重构图像与明文图像的峰值信噪比(Peak Signal-to-noise Ratio，PSNR)比文献[14]压缩至明文图像的4/5后重构图像与明文图像的PSNR更高，说明本文压缩方式图像恢复质量好。

表2 不同方式压缩不同比例的峰值信噪比

Table 2 Different methods of compressing different ratios of peak signal-to-noise ratio

Compression method	Compression ratio	PSNR/dB
Ref. [14]	Compressed to 1/4 of the plaintext image	21.467 1
Ref. [14]	Compressed to 1/2 of the plaintext image	24.464 5
Ref. [14]	Compressed to 4/5 of the plaintext image	26.746 4
This article	Compressed to 1/4 of the plaintext image	26.797 8

3.3 加密时间及传输量对比分析

为测试本文系统加密时间与传输量，选取文献[7,10,12]作对比，结果如表3。

由表3可见，本文加密系统耗时缩短了3～4倍，压缩加密使加密过程传输量大大减小，存储空间缩小，运算速度大幅提高。

表3 时间以及密钥传输量对比分析

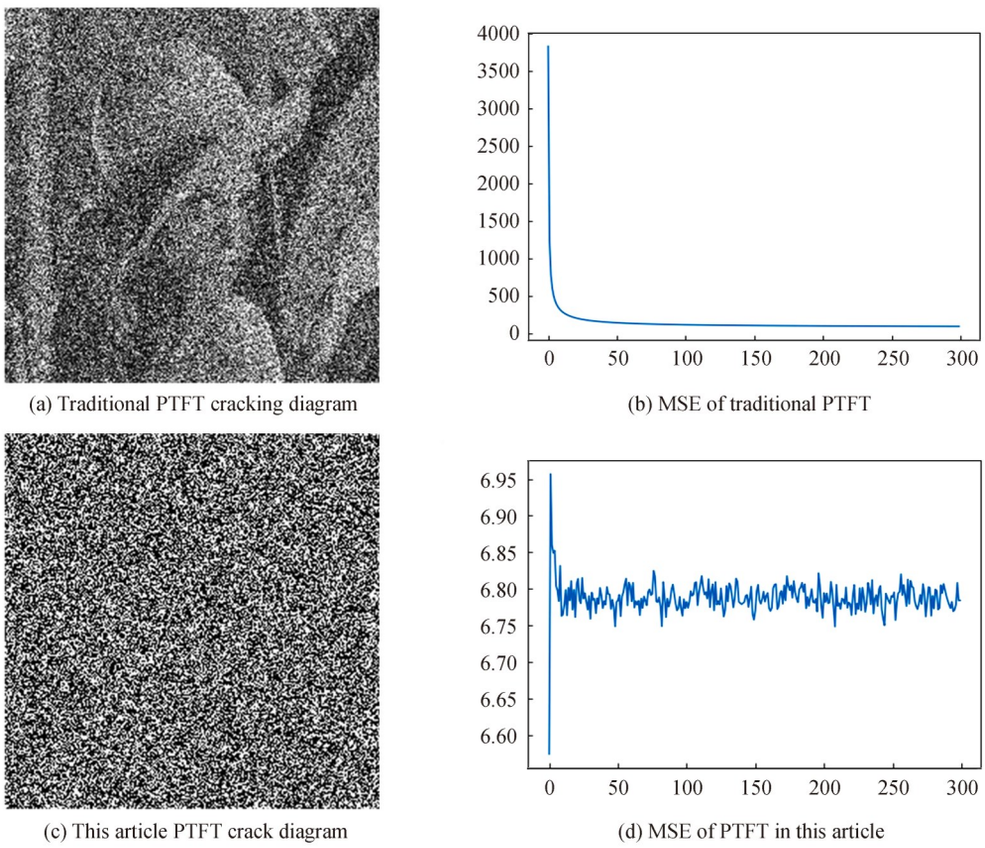
Table 3 Comparative analysis of time and key transmission volume

Reference	Encryption time/s	Key transfer volume
[7]	0.076 796	256×256×2
[10]	0.083 484	256×256×2
[12]	0.079 837	256×256×2
This article	0.022 088	128×128×2

4 抗攻击实验

4.1 抗两步迭代傅里叶变换攻击

传统PTFT非对称加密系统不能抵御两步迭代傅里叶变换的攻击，当迭代次数为300次时，加密图像可破解。本文方法和传统PTFT加密方法抗两步迭代傅里叶攻击结果如图8。



(a) Traditional PTFT cracking diagram　(b) MSE of traditional PTFT

(c) This article PTFT crack diagram　(d) MSE of PTFT in this article

图8　攻击破解对比图和均方误差(MSE)对比图

Fig.8　Comparison diagram of attack cracking and Mean Square Error (MSE) comparison chart

图8(a)为传统PTFT加密系统经300次迭代攻击的破解结果，可分辨出明文“lena”图像，图8(c)为本文增加振幅掩膜后的PTFT加密系统，同样经过300次迭代攻击，无法得到原始图像轮廓，说明本文算法可有效抵御两步迭代傅里叶变换攻击。图8(b)和图8(d)分别是为传统PTFT加密系统和本文加密系统迭代次数与MSE值的关系曲线。图8(b)MSE值随迭代次数的增加而趋向于平行，通过傅里叶变换的迭代运算，逐步逼近私钥信息的近似值，破解图可以看出明文图像“lena”的轮廓，而图8(d)在300次迭代中MSE曲线不收敛，获取不到私钥信息，破解图完全看不出明文图像的信息，本文PTFT系统可有效抵抗两步迭代傅里叶算法攻击。

4.2 抗深度学习方法攻击

文献[13]提出了一种基于深度学习的PTFT攻击方法，用基于残差网络ResNet的神经网络训练10 000张明密文对，网络自动学习密文到明文的拟合过程，训练后用手写数字图像进行测试，图像基本恢复，表明可完全攻破传统的PTFT加密系统。此方法攻击本文PTFT系统，分别用10 000张64×64的二值图像、医学图像和不同对比度灰度图像进行训练测试，结果如图9。

图9中，(a)～(d)为被攻击明文图像，(e)～(f)为密文图像，(i)～(l)为各明文攻击破解图。(i)为传统PTFT系统经深度学习攻击破解后解密图像，可见，解密图像与明文图像基本一致。(j)～(l)为本文PTFT系统经深度学习攻击后解密图像，可见，二值图像、医学图像和灰度图像经深度学习方法攻击后解密图像与明文图像相差甚大，解密图像完全看不出明文图像的信息，说明文献[13]的深度学习的攻击方法并不能攻破

本文PTFT加密系统。

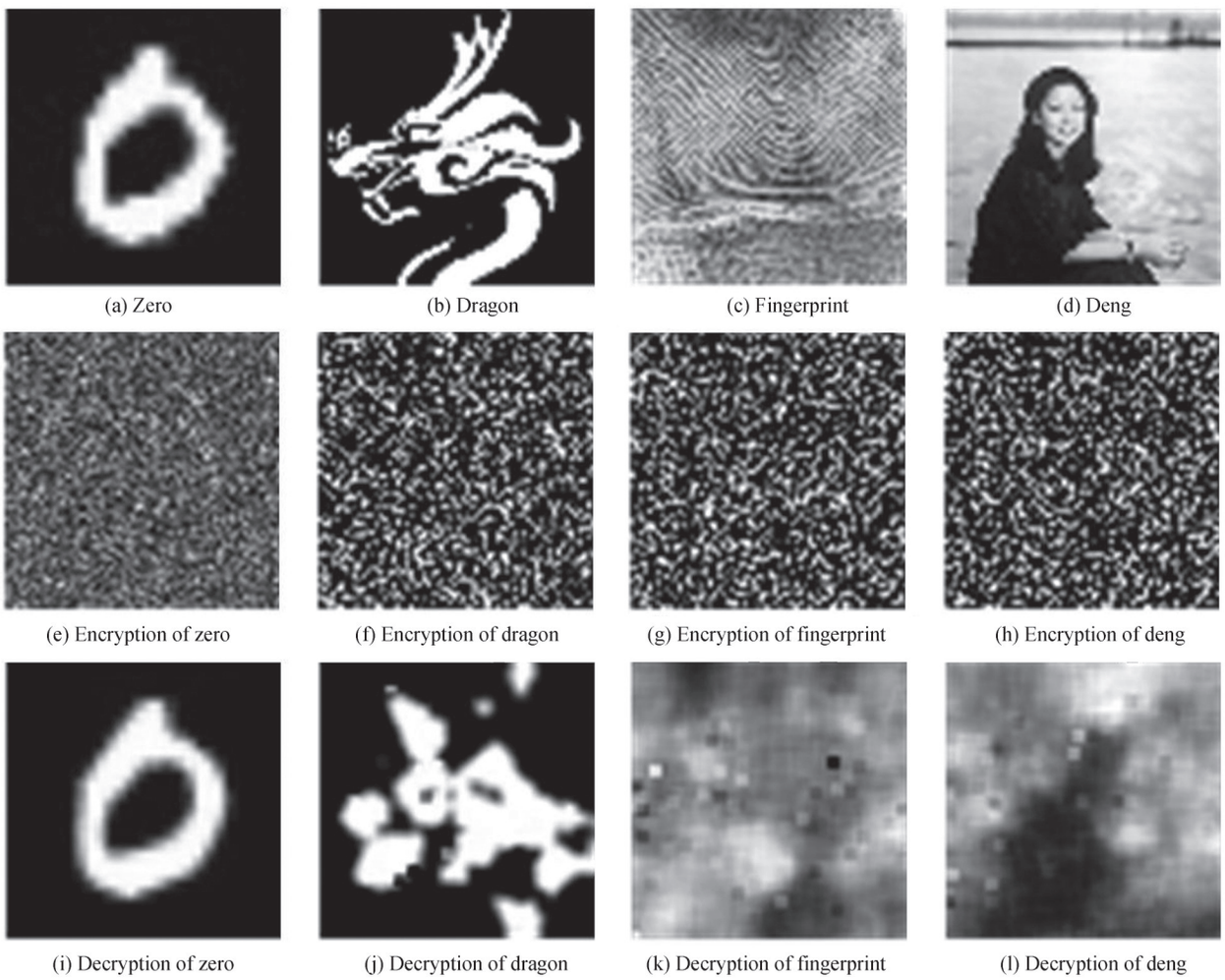


图9 攻击破解图

Fig.9 Comparison diagram of attack cracking

4.3 抗噪声攻击

为测试本文加密系统的抗噪声攻击性能力，分别为密文添加不同强度的椒盐噪声和高斯噪声，解密效果如图10～11。

图10四幅图像分别是添加不同噪声比例的椒盐噪声后的解密图像，噪声比例越大解密图像越模糊，图11四幅图像分别是添加均值为0，不同方差的高斯噪声后的解密图像，方差越大，解密图像越模糊，当椒盐噪

图10 不同噪声比例下椒盐噪声干扰的解密图像

Fig.10 Decrypted images of salt and pepper noise interference under different noise ratios

图 11　不同方差下高斯噪声干扰的解密图像

Fig.11　Decrypted images with Gaussian noise interference under different variances

声比例为0.1和高斯噪声方差为0.3时仍能分辨出明文图像，可见本文加密系统抗噪声攻击高。

4.4　抗剪切攻击

抗剪切攻击也是衡量一个加密系统的抗攻击性能高低的一个指标，本文光学图像加密系统进行抗剪切攻击能力测试，结果如图 12。

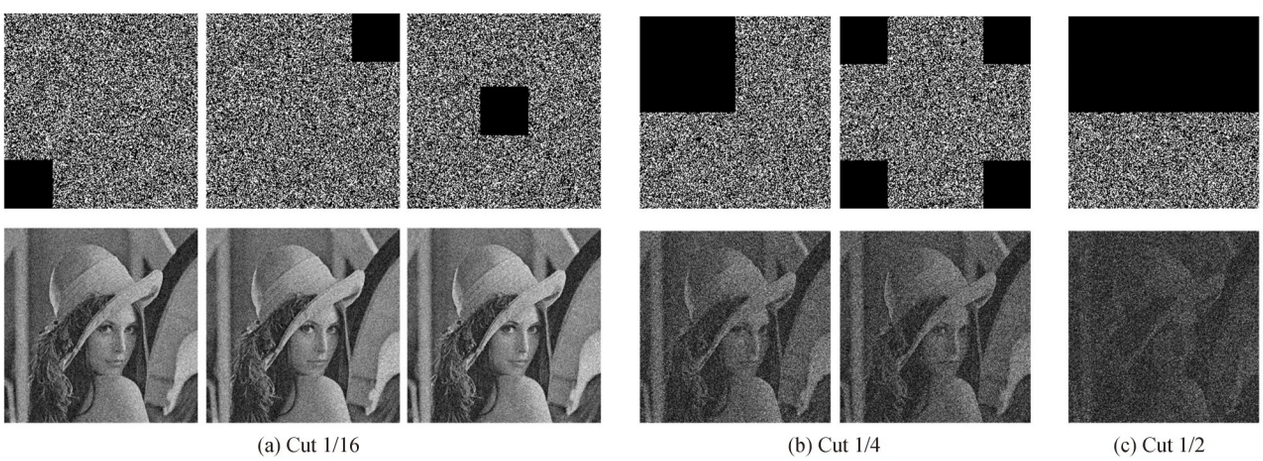


图 12　剪切不同尺寸的加密图像和解密图像

Fig.12　Cut encrypted and decrypted images of different sizes

如图 12，图(a)、(b)表明图像不同位置任意剪切大小为1/16或1/4，解密效果依旧好。图(c)尽管剪切密文图像的1/2，但还是能从解密图像看出明文图像“lena”的轮廓，输出图像较好地保留了明文信息，本文的光学加密算法抗剪切攻击能力高。

4.5　选择明文攻击

针对加密系统的攻击主要有选择明文攻击、已知明文攻击、选择密文攻击和唯密文攻击。而选择明文攻击对加密系统最具有威胁性，若本文加密系统能抵抗此攻击，那么完全可以抵抗另外三种攻击。

图 13 中 P_1 为 256×256 全 0 的明文图像，P_2 为只改变 P_1 其中一个像素值的图像，$P_3=\left|P_1-P_2\right|$，C_1 和 C_2 分别为 P_1 和 P_2 加密后的加密图像，$C_3=\left|C_1-C_2\right|$。从图中可以看出 C_3 完全获取不到明文图像的任何信息，可见本文提出的加密算法完全抵抗选择明文攻击。

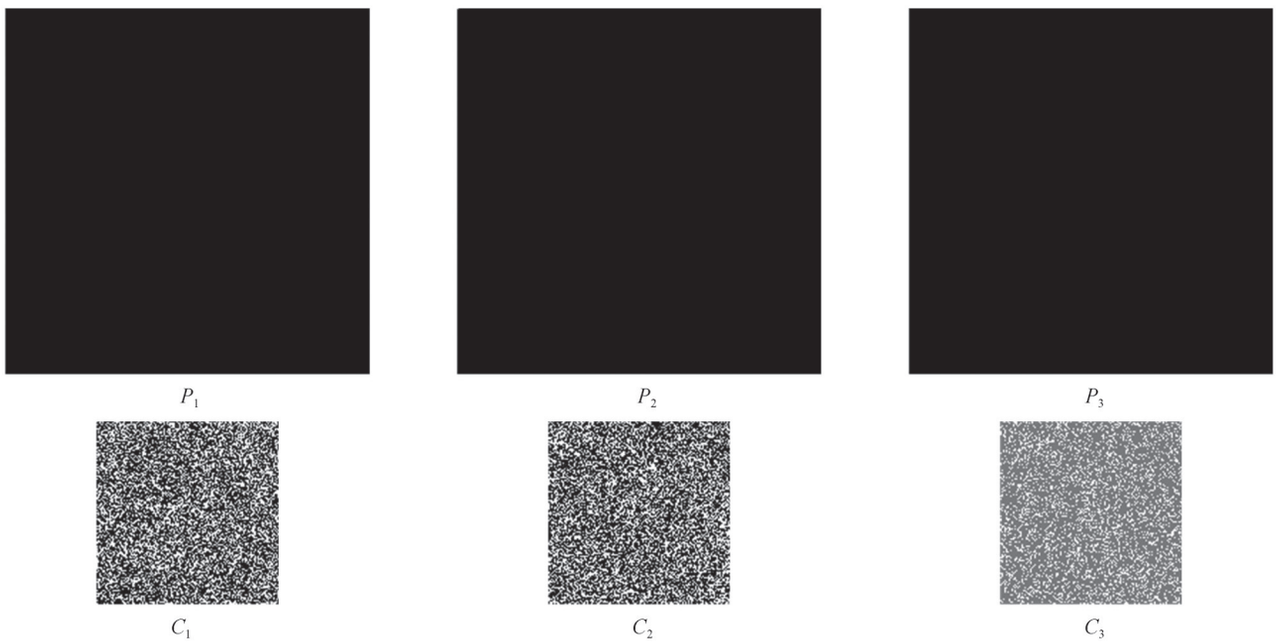


图13 选择明文攻击效果图

Fig.13 Selected plaintext attack effect diagram

5 结论

本文将压缩感知与PTFT非对称加密相结合，用压缩感知对明文图像经小波分离的高频信息压缩2/3，使其作为低频信息的相位信息，最终将明文图像压缩至1/4，不仅缩短加密时间、减小密钥传输量，且在相同重构算法下重构质量提高5.2 dB。在原系统第一块相位模板后增加一块振幅模板，并保留相位信息作为中间传输信息且将相位角作为最终密文，将两次截取的部分振幅作为两组私钥，有效提高系统对各种攻击算法的抵抗能力，保障系统安全性。将相位信息作为密文，密文分布更加均匀，抗统计特性更好。

参考文献

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

[2] JMV A, MSM B, PC B. Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator[J]. Optik, 2020, 217: 164653.

[3] TAO Yuanchun. Research on optical image encryption technology based on computational ghost imaging[D]. Jinan: Shandong University, 2021.
陶元春. 基于计算鬼成像的光学图像加密技术的研究[D]. 济南: 山东大学, 2021.

[4] ABD-EL-ATTY B, ILIYASU A M, ALANEZI A, et al. Optical image encryption based on quantum walks[J]. Optics and Lasers in Engineering, 2021, 138: 106403.

[5] WW A, XWA B, BX B, et al. Optical image encryption and authentication using phase-only computer-generated hologram [J]. Optics and Lasers in Engineering, 146: 106722.

[6] PENG W Q. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Letters, 2010, 35(2): 118-120.

[7] WANG X, ZHAOD. Security enhancement of a phase-truncation based image encryption algorithm[J]. Applied Optics, 2011, 50(36): 6645-6651.

[8] WANG X, ZHAO D. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Optics Communications, 2012, 285(6): 1078-1081.

[9] WANG X, ZHAO D. Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask[J]. Optics Letters, 2013, 38(18): 3684-3686.

[10] DING Xiangling, CUI Yongzhong. Security analysis and improvement of asymmetric encryption system based on phase truncation[J]. Laser Magazine, 2013, 34(2): 27-29.
丁湘陵, 崔永忠. 基于相位截断的非对称加密系统安全性的分析与改进[J]. 激光杂志, 2013, 34(2): 27-29.

[11] WANG X, CHEN Y, DAI C, et al. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-

truncated Fourier transform[J]. Applied Optics, 2014, 53(2):208-213.
[12] GAO Xiong, CHEN Linfei. Security analysis of truncated fourier transform encryption system[J]. Journal of Hangzhou Dianzi University, 2015,35(4):106-110.
高雄 陈林飞. 截断傅里叶变换加密系统的安全性分析[J]. 杭州电子科技大学学报, 2015,35(4):106-110.
[13] XU Zhao, ZHOU Xin, BAI Xing, et al. The attack method of phase truncated Fourier transform asymmetric encryption system based on deep learning[J]. Acta Physica Sinica,2021,70(14):226-232 .
徐昭,周昕,白星, 等. 基于深度学习的相位截断傅里叶变换非对称加密系统攻击方法[J]. 物理学报,2021,70(14):226-232.
[14] DONOHO D L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4):1289-1306.
[15] YU J, LI C, SONG X, et al. Parallel mixed image encryption and extraction algorithm based on compressed sensing[J]. Entropy, 2021, 23(3):278.
[16] WANG X, SU Y. Image encryption based on compressed sensing and DNA encoding[J]. Signal Processing Image Communication, 2021(12):116246.
[17] LI H, YU C, WANG X. A novel 1D chaotic system for image encryption, authentication and compression in cloud[J]. Multimedia Tools and Applications, 2021, 80(5):1-38.
[18] LIU Xiaoyong, CAO Yiping, LU Pei. Research on optical image encryption technology based on compressed sensing[J]. Acta Optica Sinica, 2014,34(3):0307002.
刘效勇, 曹益平, 卢佩. 基于压缩感知的光学图像加密技术研究[J]. 光学学报, 2014,34(3):0307002.
[19] LIANG Yaru, WU Jianhua. Image encryption based on compressed sensing and variable parameter chaotic mapping[J]. Optoelectronics·Laser, 2015,26(3):605-610.
梁亚茹, 吴建华. 基于压缩感知和变参数混沌映射的图像加密[J]. 光电子·激光, 2015,26(3):605-610.

A Phase-truncated Fourier Transform Asymmetric Optical Compression and Encryption System

GUO Yuan, WU Lanlan, JING Shiwei
(*School of Computer and Control Engineering*, *Qiqihar University*, *Qiqihar*, *Heilongjiang* 161006, *China*)

Abstract: Symmetric encryption is a classic encryption method. The algorithm is relatively mature. The encryption and decryption keys are the same key. The decryption method of the algorithm is basically the inverse operation of the encryption algorithm. Although the calculation speed is fast and the complexity is low, the encryption system is linear. Features also bring great hidden dangers to the security of the system. Classical optical encryption systems are mostly symmetrical encryption methods. The asymmetric encryption method distinguishes the encryption key and decryption key of the system, encrypts the information with the public key, and only the corresponding private key information can complete the correct decryption. This encryption method that divides the key into key pairs is not only suitable for actual key information distribution and management, but also destroys the linear characteristics of the encryption system, and the encryption system is more secure. The asymmetric cryptosystem based on Phase-truncated Fourier Transforms (PTFT) uses phase truncation to obtain the decryption key in the encryption process, breaking the linear operation of the algorithm. The separation of the encryption key and the decryption key is realized, and the security of the system has been greatly improved. Although the PTFT system hides the phase information in the encryption system by intercepting the phase and constructs an asymmetric encryption system; but under the condition of satisfying the "Kerckhoffs assumption", the deciphering of the asymmetric encryption system with phase interception only takes two steps to iterate the Fourier transform algorithm to recover the private key information of the system. The security of the encryption system is insufficient. From the cracking algorithm of the system, we can see that the complex value information of the system is divided into phase and amplitude, so that the encrypted values are all amplitude information; the cracking of the system takes advantage of this feature. In this paper, an undisclosed amplitude template is added after the first phase modulation template, and the threshold amplitude truncation method is adopted. Part of the amplitude information is used as the new private key, and the phase angle is used as the ciphertext. The conditions are broken and the security of the encryption

system is enhanced. Although the security of the improved system is guaranteed, in addition to a set of ciphertext information, two sets of intercepted phase information need to be transmitted during information transmission, and the amount of information transmission is tripled. This encryption method brings huge compression to the transmission and storage of information, especially for large-capacity information transmission, the efficiency of information transmission is reduced. In order to achieve the data compression of the transmitted information, this paper proposes to combine compressed sensing with PTFT optical asymmetric encryption. The plaintext is divided into low-frequency information and high-frequency information by discrete wavelet transform. The high-frequency information is compressed by 2/3 by using compressed sensing. It is transformed into phase information of low-frequency information, and jointly constructs a complex image to be encrypted whose size is 1/4 of the original plaintext image. System security performance experiments, attack experiments and comparative experiments show that the encryption system in this paper can effectively resist various attacks, has high robustness, small transmission volume, short encryption time, good quality of decrypted image reconstruction, and excellent overall performance.

Key words: Phase-truncated Fourier transforms; Resistance to attack; Asymmetric optical image encryption; Compressed sensing; Discrete wavelet transform

OCIS Codes: 100.1160; 100.2000; 100.7410; 070.4560; 070.5040

Foundation item: National Natural Science Foundation of China (No. 61872204), Natural Science Foundation of Heilongjiang Province (No. LH2021F056), Fundamental Scientific Research Business Expenses of Colleges and Universities in Heilongjiang Province (No. 135509113), Graduate Innovative Research Project (No.YJSCX20200050)