# 利用冗余数据在衍射加密系统中实现二值图像无损恢复

王红娟 王志鹏 海 涛 刘旭焱 秦 怡*
南阳师范学院物理与电子工程学院, 河南 南阳 473061

**摘要** 提出了一种基于光学衍射的二值图像加密方法。该方法仅需记录单幅衍射强度图像,加密过程避免了干涉装置,提高了记录效率,且单幅密文的传输更为方便。在加密前,先提取原始二值图像的冗余数据作为密钥保存,再使用光学衍射图像加密方法对原始二值图像加密,得到的衍射强度图像即为密文。解密时使用相位恢复算法进行迭代运算,把先前提取的冗余数据作为输入平面的部分振幅支撑,使算法能够快速收敛,从而完全恢复明文。计算机模拟结果证实了该方法的有效性,也分析了其对剪切和噪音攻击的稳健性。

**关键词** 傅里叶光学; 图像加密; 光学衍射; 相位恢复算法; 衍射强度
**中图分类号** TP751 **文献标识码** A
**doi:** 10.3788/CJL201542.0709002

# Lossless Binary Image Reconstruction in Diffractive Encryption System with Redundant Data

Wang Hongjuan Wang Zhipeng Hai Tao Liu Xuyan Qin Yi
*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*

**Abstract** A method for image encryption by employing the diffraction imaging technique is proposed. Only a single diffraction intensity image is recorded without using interference equipment that makes the method much more efficient, and the transmision of the single ciphertext more convenient. Before encrypting, the redundant data of the original binary image are extracted as the secret key, then the original binary image is encrypted by using optical diffraction image encryption method and the diffraction intensity image is the ciphertext. During image decryption, the redundant datas serve as partial input plane support constraint in phase retrieval algorithm iterative operation, which is employed for making algorithm convergences fastly. Computer simulation results verify the validity of the proposed approach. Its robustness against occlusion and noise attacks are also analyzed.

**Key words** Fourier optics; image encryption; optical diffraction; phase retrieval algorithm; diffraction patterns
**OCIS codes** 070.2025; 070.4560; 070.7345

## 1 引 言

随着信息科学和网络技术的快速发展,信息安全技术得到越来越多的关注[1-8]。其中,光学加密技术由于其具有大容量、多维度及高速并行处理数据能力等优点,逐步发展成为新一代的信息安全处理技术,已成为信息处理研究中的一个热门领域。该领域内的开拓性成果是1995年由Refregier等[9]提出的双随机相位编码系统(DPRE)。该系统是在光学系统的输入平面和傅里叶频谱面上各放置一个互不相关的随机相位掩模板,通过对输入图像空域信息和频域信息分别进行扰乱得到加密图像,具有加密维度高,稳健性好等优点,

**收稿日期**: 2015-02-09; **收到修改稿日期**: 2015-03-20
**基金项目**: 国家自然科学基金(61306007)、河南省基础与前沿技术研究计划(142300410184)、南阳师范学院高层次人才科研启动基金(nytc2006k100)、南阳师范学院青年基金(QN2015013)
**作者简介**: 王红娟(1979—),女,硕士,讲师,主要从事光电信息处理方面的研究。E-mail: 35148784@qq.com
*通信联系人。E-mail: 641858757@qq.com

随后被推广到了菲涅耳域[10]和分数傅里叶域[11]。后来一些研究人员发现此系统存在不足之处，如加密结果为复数形式，必须以全息方式存储，密文不便于传输等。

为了克服DPRE系统的缺点，Chen等[12-15]提出了基于光学衍射成像技术的图像加密系统。该加密方法只需要记录衍射场的强度分布，传输方便，简化了光学系统结构。为了使解密时所采用的相位恢复算法收敛，必须有足量的原始明文信息参与迭代过程，三幅以下的衍射图像所包含的原始明文信息太少，解密结果会含有较大的噪声。为了实现高质量解密，此类系统需要在加密时改变光学结构或者移动光学器件来记录至少三幅衍射强度图像。为了简化基于衍射成像技术图像加密系统，本文提出了一种在这种系统中利用冗余数据实现二值图像无损恢复的方法，该方法仅需记录单幅衍射强度图像即可。在加密前首先提取原始二值图像的部分冗余数据。在解密时使用相位恢复算法，这些冗余数据作为该迭代算法中输入平面的部分振幅支撑，使得算法快速收敛。并且所提取的数据仅为原始二值图像的冗余数据，与图像本身相互独立，不会透漏原始图像的任何有效信息，因此把冗余数据作为密钥相对比较安全。

## 2　理论分析

光学衍射加密系统的结构如图1所示，其中$f$为明文，$M_1$和$M_2$为两个统计独立的随机相位板，其相位均匀分布在0~2π之间，原始二值图像$f(x,y)$被波长为$\lambda$的单色平面光波照射，随机相位板$M_1$紧贴于原始二值图像并对其进行调制，经过距离为$d_1$的衍射后到达随机相位板$M_2$所在平面，并被$M_2$调制，又经距离为$d_2$的衍射到达输出平面，其衍射强度被电荷耦合器件(CCD)记录。

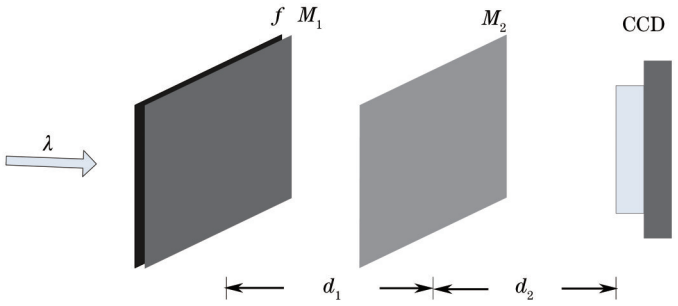


图1　光学衍射加密系统

Fig.1　Schematic of optical setup for the optical security system

图1中入射到随机相位板$M_2$的复振幅表示为

$$U(x',y')=\mathrm{FrT}_{\lambda}\left[f(x,y)M_1(x,y);d_1\right], \tag{1}$$

式中$(x,y)$，$(x',y')$分别表示$M_1$，$M_2$所在平面的坐标。$\mathrm{FrT}_{\lambda}$表示关于$\lambda$的菲涅耳变换，关于$u(x,y)$的二维菲涅耳变换定义为

$$\mathrm{FrT}_{\lambda}\left[u(x,y),d\right]=\frac{\exp\left(\mathrm{j}2\pi d/\lambda\right)}{\mathrm{j}\lambda d}\iint u(x,y)\exp\left\{\mathrm{j}\frac{\pi}{\lambda d}\left[\left(x'-x\right)^2+\left(y'-y\right)^2\right]\right\}\mathrm{d}x\mathrm{d}y, \tag{2}$$

式中$\lambda$，$d$分别是波长和传播距离。

相应地，在CCD平面所记录的强度可以表示为

$$I(x'',y'')=\left|\mathrm{FrT}_{\lambda}\left\{\mathrm{FrT}_{\lambda}\left[f(x,y)M_1(x,y);d_1\right]M_2(x',y');d_2\right\}\right|^2, \tag{3}$$

式中$(x'',y'')$表示CCD所在平面的坐标，$I(x'',y'')$即作为密文保存，从所记录的密文中，使用相位恢复算法恢复原始明文。为了使解密时所采用的相位恢复算法收敛，从而实现高质量的解密，必须有足量的原始明文信息参与迭代过程。基于光学衍射成像技术的图像加密系统中，需要在加密时改变光学结构或者移动光学器件来记录至少三幅衍射强度图像。而多幅密文的信息量大，不方便存储和传送，且记录多幅密文的实施过程比较复杂和不易控制。而本文方法仅需记录单幅衍射图像，即可使用相位恢复算法恢复原始明文。本文方法与Chen等所使用的相位恢复算法有所不同，Chen等使用的算法都以原始图像完全未知为前提，将原始图像的恢复过程视为一个盲相位恢复过程，这就使得在恢复过程中，必须有多幅密文参与迭代，才能使得

算法收敛。而本文方法仅需记录一幅衍射强度图像，仅有一幅密文参与迭代过程。为了使算法快速收敛，加密前在原始图像的一些区域取得部分信息并保存下来，且这些信息是原始图像中的冗余信息，将其作为迭代过程中输入平面的部分振幅支撑，所取得的冗余信息用 $T(x,y)$ 表示。可以预期，算法能够快速收敛。

用 $f_n(x,y)\,(n=1,2,3,\cdots)$ 表示使用相位恢复算法经第 $n$ 轮迭代之后得出的原始图像的估计。本文算法步骤如下：

1) 将明文 $f_n(x,y)\,(n=1)$ 初始化，初始化为随机实值矩阵，将其作为如图1所示加密系统的输入图像，使用相位恢复算法进行迭代运算，在CCD平面得到一复函数

$$U_n(x'',y'')=\mathrm{FrT}_\lambda\left\{\mathrm{FrT}_\lambda\left[f_n(x,y)M_1(x,y);d_1\right]M_2(x',y');d_2\right\}. \tag{4}$$

2) 保留 $U_n(x'',y'')$ 的相位信息，以CCD记录的密文 $I(x'',y'')$ 作为振幅支撑，构造一个新函数

$$\overline{U_n(x'',y'')}=I(x'',y'')^{1/2}U_n(x'',y'')\Big/\left|U_n(x'',y'')\right|. \tag{5}$$

3) 将 $\overline{U_n(x'',y'')}$ 逆衍射至输入平面，得到的振幅可表示为

$$\overline{f_n(x,y)}=\left|\mathrm{FrT}_\lambda\left\{\mathrm{FrT}_\lambda\left[\overline{U_n(x'',y'')};-d_2\right]M_2^*(x',y');-d_1\right\}\right|, \tag{6}$$

式中*表示复共轭。将加密前所取得的冗余信息 $T(x,y)$ 作为振幅支撑，与 $\overline{f_n(x,y)}$ 结合起来作为对输入图像的新的估计 $f_{n+1}(x,y)$，具体过程表示为

$$f_{n+1}(x,y)=T(x,y)+\overline{f_n(x,y)}\left[1-T(x,y)\right]. \tag{7}$$

(4)~(7)式所描述的过程完成时，一轮迭代过程结束。对 $\overline{f_{n-1}(x,y)}$ 与 $\overline{f_n(x,y)}$ 所包含的图像之间的迭代误差进行评估，来决定迭代是否继续，误差定义为

$$f_{\mathrm{error}}=\sum_{x,y}\left[\overline{f_n(x,y)}-\overline{f_{n-1}(x-y)}\right]^2, \tag{8}$$

若通过计算得到的迭代误差比预先限定值小，则把 $\overline{f_n(x,y)}$ 作为解密结果；若得到的迭代误差比预先限定值大，则把 $\overline{f_n(x,y)}$ 与 $T(x,y)$ 按照(7)式的关系形成 $f_{n+1}(x,y)$，送入迭代算法的输入平面，代入(4)式进行下一轮迭代。该循环对应的流程图如图2所示。

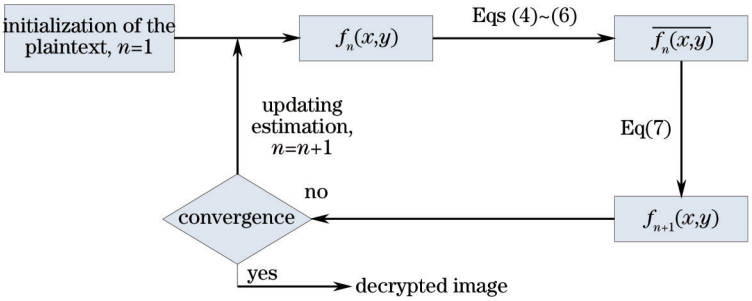


图2　解密过程流程图

Fig.2　Flow chart of decryption process

## 3　计算机仿真及讨论

为了验证本文方法的有效性，在个人计算机(PC)上使用Matlab7.0软件对二值图像进行了模拟实验。所选择的原始二值图像如图3(a)所示，大小为256 pixel×256 pixel。模拟所取参数分别为 $d_1=50$ mm，$d_2=80$ mm，照明所用光波波长 $\lambda=632.8$ μm。图3(b)~(c)是在对原始图像进行加密时所采用的两个随机相位板，即 $M_1$，$M_2$。图3(d)表示利用图1系统对原始二值图像的加密结果。对图3(a)二值图像提取出的冗余信息如图3(e)所示，作为密钥保存。

利用理论分析部分给出的方法对明文进行恢复，相关系数(CC)与迭代次数的关系如图4(a)所示。由图可知，相关系数迅速上升，经过182次迭代后达到1，对应于相关系数为1的解密图像如图4(b)所示，图像被完

全恢复，从而证实了该方法的有效性。迭代过程中对明文的初始估计无论是随机矩阵或者非随机矩阵对结果没有显著影响。

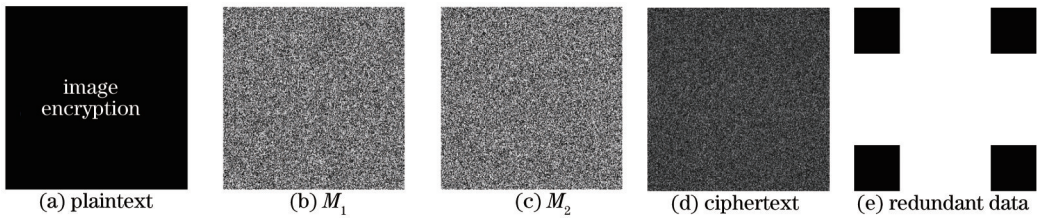


图3 图像信息加密实验结果

Fig.3 Experimental results of image information encryption

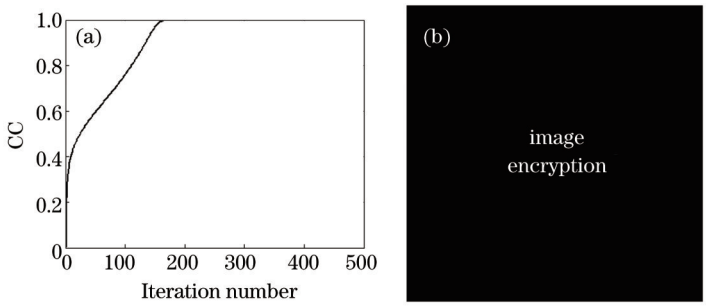


图4 图像解密实验结果。(a) 相关系数; (b) 解密图像

Fig.4 Experimental results of image decryption. (a) CC value; (b) decrypted image

作为对比，也模拟了没有使用冗余信息作为振幅支撑的情况下的仿真结果。此时相关系数与迭代次数的关系如图5(a)所示，可以看出相关系数缓慢上升，迭代次数达到1500次时，相关系数缓慢上升至0.5771，相应的解密结果如图5(b)所示。

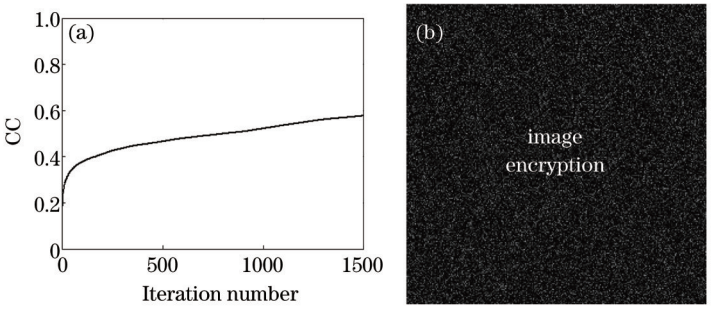


图5 无振幅支撑情况下解密实验结果。(a) 相关系数; (b) 解密图像

Fig.5 Experimental results of decryption without constraint in the input plane. (a) CC value; (b) decrypted image

密文被截获时，攻击者使用随机选取的错误的密钥进行解密的情况如图6所示。图6(a)为密钥$M_1$错误而其他参数正确时迭代1500次的解密情况，从解密结果来看，不能得到原始明文的任何有效信息。迭代过程中相关系数与迭代次数的关系如图6(b)所示。可以看出相关系数一直在比较小的范围内无规律地变化。

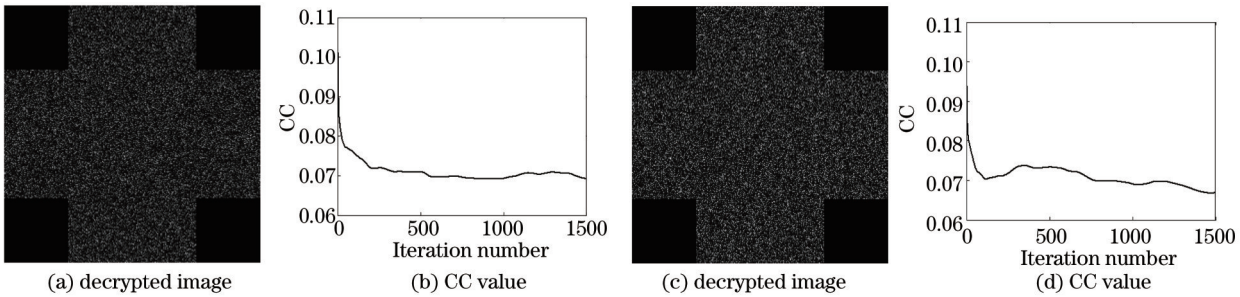


图6 密钥错误时解密结果。(a,b) $M_1$错误; (c,d) $M_2$错误

Fig.6 Decryption results with wrong keys. (a,b) Wrong $M_1$; (c,d) wrong $M_2$

同样也给出在密钥$M_2$错误时的解密情况，迭代1500次的解密结果如图6(c)所示，相应的相关系数为0.0692，同样也不能从解密图像中获取原图像的有效信息。相关系数与迭代次数的关系如图6(d)所示。可见，在密钥$M_1$或$M_2$任何一个错误而其他参数都正确时，均不能得出正确的解密结果。

在信息的存储与传输过程中，密文很可能遭受噪音攻击及剪切攻击，因此有必要分析本文方法对于这些攻击的稳健性。测试对于剪切攻击的稳健性，丢失6.25%数据后的密文如图7(a)所示，利用冗余数据作为部分振幅支撑的相位恢复算法进行解密，其相关系数与迭代次数的关系如图7(b)所示，迭代1500次的解密结果如图7(c)所示，此时的相关系数为0.9221。可见，本文方法对于剪切攻击具有一定的稳健性。为测试本文方法对噪音攻击的稳健性，对密文加入了噪声密度为0.02的椒盐噪声，加噪之后的密文如图7(d)所示。迭代解密时相关系数与迭代次数的关系如图7(e)所示，迭代1500次的解密结果如图7(f)所示，此时的相关系数为0.5715。可见，本文方法对于噪音攻击的稳健性并不高，因此在密文传输过程中应尽量避免数据受到污染。

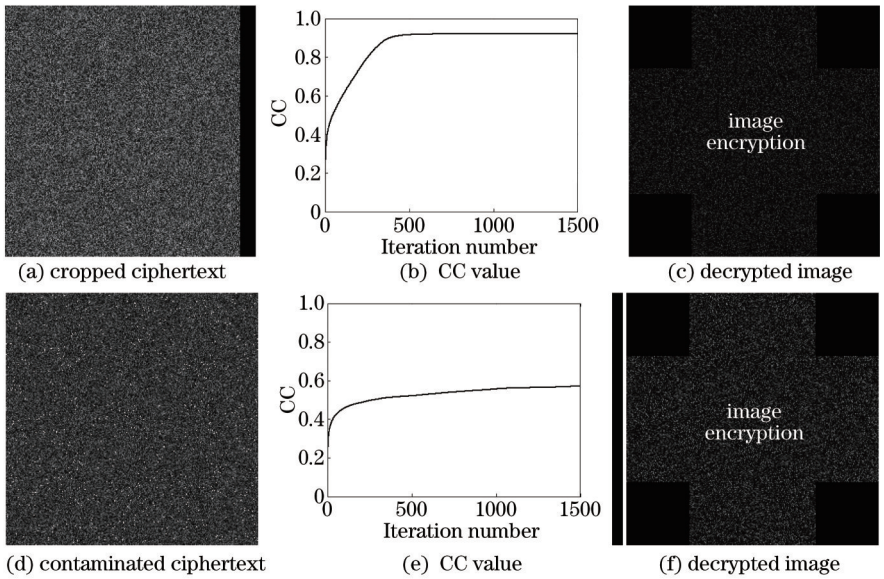


图7 加密图像稳健性分析

Fig.7 Analysis of robustness for the encrypted image

模拟结果反映了本文方法的有效性，使用如图1所示的光学衍射加密系统，通过冗余数据参与的迭代运算，可以较快且高质量恢复原始图像。而冗余数据的选取在一定程度上影响解密过程，其主要的选取原则是不透漏原始二值图像的有效信息。只要遵循这个原则，冗余数据的选取对位置、形状均无特殊要求。图3(e)为冗余数据选取在原始图像的四角位置方形区域。对冗余数据选取的区域大小变化对解密的影响进行模拟。在图3(e)基础上增大选取区域，如图8(a)所示。利用图1光学衍射加密系统对原始二值图像进行加密，对得到的密文使用迭代算法解密，并把此冗余数据作为输入平面的部分振幅支撑，经迭代运算，相关系数与迭代次数的关系如图8(b)所示。可见相关系数迅速上升，仅迭代81次后相关系数即达到1，图像被完全恢复。由此可见，选取的冗余数据量越大，迭代运算收敛速度越快。另外，对于选取冗余数据时所选的区域形状变化的情况也进行模拟，另一种选取的区域如图9(a)所示，此时圆形以外的黑色区域即为冗余数据。解密时相关系数与迭代次数的关系如图9(b)所示。可以看出相关系数也迅速上升，迭代70次后相关系数1，图像也被完全恢复。

计算机模拟结果表明，在原始图像加密前，冗余数据的选取对解密是非常重要的。在不透漏原始二值图像有效信息的前提下，适当的尽可能多的选取其冗余数据，将会加快解密时迭代算法的收敛速度。

将本文方法与课题组先前的工作进行比较。先前的方法中[16]，为了高质量的恢复原始图像，在加密之前给原始图像外围增加数据，这些数据作为解密时迭代运算输入平面的部分振幅支撑，从而加快了迭代收敛速率。但该方法会使得待加密图像的数据量变大，密文的数据量也随之变大，不便于信息的传输和存储。课题组也提出另外一种从单幅衍射图像使用迭代算法恢复原始明文的方法[17]。为了高质量地恢复明文，解

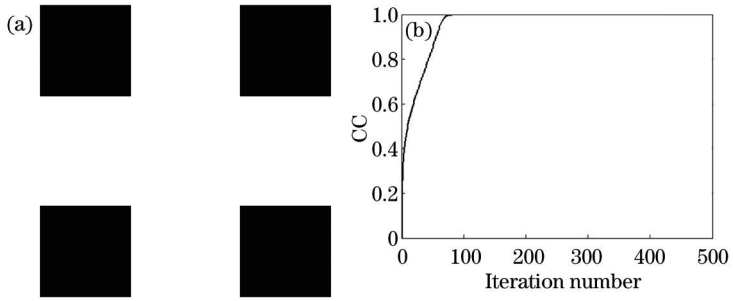


图8 冗余数据量增大情况下的解密结果。(a) 冗余数据; (b) 相关系数

Fig.8 Decryption results when the amount of redundant data increases. (a) Redundant data; (b) CC value

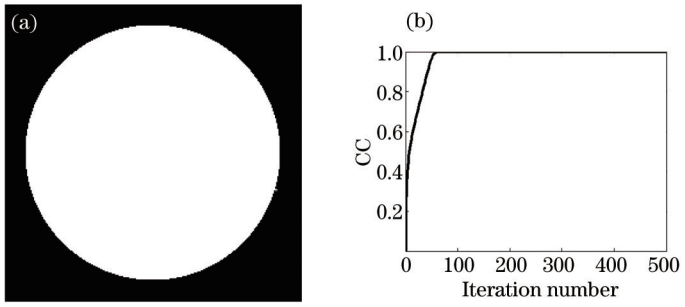


图9 冗余数据区域变化情况下的解密结果。(a) 冗余数据; (b) 相关系数

Fig.9 Decryption results when the region of redundant data changes. (a) Redundant data; (b) CC value

密过程中的每一轮迭代均需进行低通滤波运算,极大地增加了解密所需的时间。相比之下,本文方法是在原始二值图像上提取部分冗余数据,不需要向原始图像添加数据。此外,由于将冗余数据作为输入平面的振幅支撑,本文方法迭代收敛速率较快,恢复明文质量较高。但是,本文方法的局限性也很明显,即该方法只适合于加密二值图像。而对于灰度图像,如果提取原图像中的小部分数据作为密钥,这些数据会导致该原始图像的数据透漏,安全性会大大降低。

## 4 结　论

提出了一种光学衍射图像加密方法。该方法在加密前先提取原始二值图像的冗余数据,作为相位恢复算法中迭代运算时,输入平面的部分振幅支撑,算法能够快速收敛。且该方法仅需记录单幅衍射强度图像,加密过程变得简单,容易实现,单幅密文的数据量小,传输方便。另外加密前所提取的冗余数据仅为原始二值图像中有效信息之外的数据,不会透漏原始图像的任何有效信息,把所提取的冗余数据作为密钥也相对比较安全。

## 参 考 文 献

1 Chen Yixiang, Wang Xiaogang. Image encryption based on iterative amplitude-phase retrieval and nonlinear double random phase encoding[J]. Acta Optica Sinica, 2014, 34(8): 0810003.
陈翼翔, 汪小刚. 一种基于迭代振幅-相位恢复算法和非线性双随机相位编码的图像加密方法[J]. 光学学报, 2014, 34(8): 0810003.

2 Qin Yi, Li Jing, Ma Maofen, *et al*.. System for optical multiple binary image encryption by random phase mask multiplexing[J]. Acta Optica Sinica, 2014, 34(3): 0307001.
秦　怡, 李　婧, 马毛粉, 等. 一种基于随机相位板复用的光学多二值图像加密系统[J]. 光学学报, 2014, 34(3): 0307001.

3 Y Zhang, B Wang. Optical image encryption based on interference[J]. Opt Lett, 2008, 33(21): 2443-2445.

4 Y Li, K Kreske, J Rosen. Security and encryption optical systems based on a correlator with significant output images[J]. Appl Opt, 2000, 39(29): 5295-5301.

5 Yin Shen, Tao Shaohua. Technique based on image superposition for optical image storage and reconstruction[J]. Acta Optica Sinica, 2013, 33(12):1205002.
尹　珅, 陶少华. 基于图像叠加的光学图像存储与恢复[J]. 光学学报, 2013, 33(12): 1205002.

6 L Chen, D Zhao. Optical image encryption based on fractional wavelet transform[J]. Opt Commun, 2005, 254(4-6): 361-367.

7 P Tsang, K W K Cheung, T C Poon. Fast numerical generation and hybrid encryption of a computer-generated Fresnel holographic video sequence[J]. Chin Opt Lett, 2013, 11(2): 020901.

8 Zhenbo Ren, Ping Su, Jianshe Ma, *et al*.. Secure and noise-free holographic encryption with a quick-response code[J]. Chin Opt Lett, 2014, 12(1): 010601.

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

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

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

12 W Chen, X Chen, C J R Sheppard. Optical image encryption based on diffractive imaging[J]. Opt Lett, 2010, 35(22): 3817-3819.

13 W Chen, X Chen, C J R Sheppard. Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating[J]. Appl Opt, 2011, 50(29): 5750-5757.

14 W Chen, X Chen, C J R Sheppard. Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain[J]. Opt Express,2012, 20(4): 3853-3865.

15 W Chen, X Chen, A Anand, *et al*.. Optical encryption using multiple intensity samplings in the axial domain[J]. J Opt Soc Am A, 2013, 30(5): 806-812.

16 Y Qin, Z Wang, Q Gong. Diffractive-imaging-based optical image encryption with simplified decryption from single diffraction pattern[J]. Appl Opt, 2014, 53(19): 4094-4099.

17 Y Qin, Q Gong, Z Wang. Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme[J]. Opt Express, 2014, 22(18): 21790-21799.

**栏目编辑**：苏　岑