©2014《中国激光》杂志社

以单幅衍射强度图像为密文的光学衍射成像加密系统

白音布和[1] 李根全[2] 吕林霞[2] 秦 怡[2*]

[1]通辽职业学院机电工程学院, 内蒙古 通辽 028000

[2]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成像原理的图像加密方法,并以具有两个随机相位板的自由空间衍射结构为例,说明该方法的原理。该系统加密过程简单,加密过程只需要记录一幅衍射强度图像,即作为密文保存。为了从密文中完全恢复明文,需要除了3个相位板之外的第四个密钥,即原始图像的稀疏数据。这需要在对原始图像加密之前,利用数字方法提取其稀疏数据。在利用相位恢复算法恢复明文的过程中,这些稀疏数据作为输入平面的部分振幅支撑,可以避免迭代过程的停滞问题并提高收敛速率,从而完全恢复明文。由于完成加密过程只需要记录单幅强度图像,避免了干涉装置,提高了记录效率,较大地方便了密文的传输。计算机模拟结果证实了本方法的有效性。

关键词 图像处理; 光学图像加密; 衍射成像; 稀疏数据

中图分类号 TP751 **文献标识码** A **doi:** 10.3788/LOP51.100701

Optical Image Encryption with Ciphertext of a Single Diffraction Intensity Pattern

Bai Yinbuhe[1] Li Genquan[2] Lü Linxia[2] Qin Yi[2]

[1]*School of Mechanical and Electric Engineering Technology, TongliaoTechnical College, Tongliao, Inner Mongolia* 028000, *China*

[2]*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*

Abstract A novel method for image encryption by employing the diffraction imaging technique is proposed. This method is in principle suitable for most of the diffractive-imaging-based optical encryption schemes, and the classical double random phase encoding in the Fresnel domain is taken for an example for illustrating it. The encryption process is rather simple because only a single diffraction intensity pattern is needed to be recorded. The security keys include, in addition to the two phase only masks in the input and the Fresnel plane, the sparse data of the plaintext that can be obtained with a simple digital means. The sparse data serve as partial input plane support constraint in a phase retrieval algorithm, which is employed for completely retrieving the plaintext. Simulation results are presented to verify the validity of the proposed approach.

Key words image processing; opticl image encryption; diffraction imaging; sparse data

OCIS codes 070.2025; 070.4560; 070.7345

1 引 言

近年来,光学信息处理在信息安全领域内的应用引起了极大的兴趣与关注,成为目前信息光学的研究热点之一[1-5]。利用光学信息处理技术,可以实现对二维数据的高速并行加密及解密。该领域内的开拓性成果是1995年由Refregier与Javidi提出的双随机相位编码(DRPE)系统。该系统在经典的光学4*f*系统的输入平面与傅里叶平面各放置一块随机相位板,可以将原始图像加密成为复平稳白噪声[6]。DRPE系统具有显著的优点:首先,由于在加密过程中使用随机相位板,使得入侵者即使在窃取密文的情况下无法使用相位恢复算法来获取明文,对盲反卷积攻击具有稳健性[6];其次,其密文为复平稳白噪声,由密文的统计特性无法获知

收稿日期: 2014-04-18; **收到修改稿日期**: 2014-05-08; **网络出版日期**: 2014-09-09

基金项目: 国家自然科学基金(10947020)、南阳师范学院青年基金(QN2014016)

作者简介: 白音布和(1963—),男,学士,副教授,主要从事光电信息处理方面的研究。E-mail: BYBH@163.com

* **通信联系人**。E-mail: 641858757@qq.com

任何信息。由于这些突出的优点,DRPE系统随即被推广到了菲涅耳域[7]和分数傅里叶域[8]。然而,DRPE系统也存在一些安全漏洞,已经证实该系统可以被选择明文攻击[9]、已知明文攻击[10]以及唯密文攻击[11]所攻破。此外,由于DRPE系统的密文为复数,必须采用干涉的方法记录,而干涉系统对装置的稳定性要求极高,这给记录带来了极大的不便。

最近,为了克服DRPE系统的这些缺点,Chen等[12-14]提出了基于光学衍射成像技术的图像加密系统。此系统以图像在光学衍射结构中的衍射强度为密文,避免了干涉过程。此外,由于只保留了衍射场的强度信息,系统的安全性也较DRPE系统得到了进一步提高。然而,此系统的解密过程均采用相位恢复算法,为了能够高质量地恢复出原始图像,必须记录3幅以上的衍射强度图像作为密文。这是因为单幅或者两幅衍射图像所包含的原始明文信息太少,在迭代过程中会使算法停滞,从而使解密结果含有严重的噪声。这些方法要求的密文数据太多,传输起来较为不便。更重要的是,为了记录3幅以上的衍射强度,加密过程需要移动光学元件[12-13]或者改变照明方式[14],增大了加密过程实施的难度。为了解决这些问题,本文提出一种新的光学衍射成像加密方法,该方法仅利用单幅衍射图像即可完全恢复出原始明文。与文献[12-14]所用明文恢复算法不同,本方法在对原始图像加密前提取其稀疏数据,这些稀疏数据不透露原始数据的有效信息,因而作为密钥保存非常安全。解密时,这些稀疏数据作为迭代过程中输入平面的部分振幅支撑,使得明文恢复算法可以快速收敛,同时消除了停滞问题。文中给出了理论分析和计算机仿真结果。

2 理论分析

从原理上说,所提的方法适合于所有的基于光学衍射成像原理的加密系统。以一种简单的衍射成像系统为例来说明该方法,结构如图1所示。其中U为待加密的图像,M1,M2为两个统计独立的随机相位板,其相位均匀地分布在$[0, 2\pi]$区间。原始图像被波长为λ的单色平面光波所照射,首先被紧贴其的随机相位板M1调制,之后经过距离为d_1的衍射之后到M2所在平面,再被M2调制,之后衍射至输出平面,其强度被CCD记录,该衍射强度即作为密文保存。

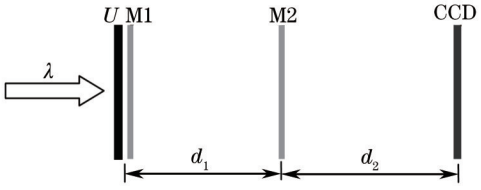

图1 用来测试所提方法的光学衍射加密结构

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

在图1所示结构中,入射到随机相位板M2的光波的复振幅可表示为[9]

$$U(\eta,\xi)=\frac{\exp\left(\mathrm{j}2\pi d_1/\lambda\right)}{\mathrm{j}\lambda d_1}\iint U(x,y)M_1(x,y)\exp\left[\mathrm{j}\pi\left[(x-\eta)^2+(y-\xi)^2\right]\Big/(\lambda d_1)\right]\mathrm{d}x\mathrm{d}y\,, \tag{1}$$

式中(x,y),(η,ξ),(μ,ν)分别表示M1,M2及CCD所在平面的坐标,M_1表示相位板M1的相位值。简明起见,将(1)式改写为

$$U(\eta,\xi)=T_{\mathrm{Fr}}\left[U(x,y)M_1(x,y);d_1\right], \tag{2}$$

式中T_{Fr}表示菲涅耳变换,利用(2)式的记号,CCD平面所记录的强度可以表示为

$$I(\mu,\nu)=T_{\mathrm{Fr}}\left\{T_{\mathrm{Fr}}\left[U(x,y)M_1(x,y);d_1\right]M_2(\eta,\xi);d_2\right\}, \tag{3}$$

式中M_2表示相位板M2的相位值,$I(\mu,\nu)$作为密文保存。所提的方法即由单幅强度图像$I(\eta,\xi)$完全恢复原始明文。

在介绍明文恢复算法之前,需要对先前提出的光学衍射加密系统[14-16]进行一下回顾。在这些系统中,恢复原始图像(明文)一般都采用传统的广义相位恢复算法,即以CCD所记录的衍射图像为输出平面的振幅支撑限制,通过在输入平面和输出平面进行往返迭代完成原始图像的解密过程。然而,为了完全恢复出原始图像,这些系统在加密过程中必须改变参数(改变随机相位板位置或者照明方式),使CCD记录至少3幅不

同的衍射图像。如果只有两幅或者更少的衍射图像用于解密，所使用的相位恢复算法就会出现停滞，无法准确地恢复出原始图像，这是因为两幅衍射图像所包含的原始图像信息太少。需要指出的是，这些恢复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[15]，迭代过程对输入平面(原始明文平面)无振幅支撑。事实上，光学加密系统的明文恢复过程并非一个严格的盲相位恢复过程，因为原始明文加密前已经被加密者知晓。因此，在加密前提取原始图像的稀疏数据，这些稀疏数据作为附加密钥保存，解密时作为输入平面的部分振幅支撑。迭代过程获取这个支持之后，可以预期其收敛速度将会加快，并且停滞问题也会不复存在。文献[16-17]中给出了提取原始图像 $U(x,y)$ 的稀疏数据的一种方法

$$U^{\mathrm{SP}}(x,y)=U(x,y)\times \boldsymbol{R}\left[(x,y);\rho\right], \tag{4}$$

式中 $U^{\mathrm{SP}}(x,y)$ 为提取出的稀疏数据。 $\boldsymbol{R}\left[(x,y);\rho\right]$ 表示一个二值矩阵，该矩阵只包含0和1，其中取值为1的像素数占全部像素数的百分比为 ρ。一般来说应满足 $\rho\ll 100$，因为只想保留原始图像较少的稀疏数据。

基于以上分析，首先，给欲恢复的图像赋予一个初始值，即随机实值矩阵 $\boldsymbol{T}_n(x,y)$，$n=1$，此处 n 表示迭代次数。将 $\boldsymbol{T}_n(x,y)$，$n=1$ 作为图1所示加密系统的输入图像，此时在CCD平面得到一复函数

$$U_n(\mu,\nu)=T_{\mathrm{Fr}}\left\{T_{\mathrm{Fr}}\left[\boldsymbol{T}_n(x,y)M_1(x,y);\lambda;d_1\right]M_2(\eta,\xi);\lambda;d_2\right\}, \tag{5}$$

之后，保留此复函数的相位信息，以CCD先前记录的密文[即 $I(\eta,\xi)$]作为振幅支撑，构造一个新函数

$$\overline{U_n(\mu,\nu)}=I(\mu,\nu)^{1/2}U_n(\mu,\nu)\Big/\left|U_n(\mu,\nu)\right|, \tag{6}$$

之后，将 $\overline{U_n(\mu,\nu)}$ 逆衍射至输入平面，此时得到输入平面的振幅可表示为

$$\overline{T_n(x,y)}=\left|T_{\mathrm{Fr}}\left\{T_{\mathrm{Fr}}\left[\overline{U_n(\mu,\nu)};\lambda;-d_2\right]M_2^{*}(\eta,\xi);\lambda;-d_1\right\}\right|^2, \tag{7}$$

*表示复共轭。之后，利用加密时保存的稀疏数据模板作为振幅支撑，与 $\overline{T_n(x,y)}$ 结合来形成一个对输入图像的新的估计 $\boldsymbol{T}_{n+1}(x,y)$，此过程可表示为

$$\boldsymbol{T}_{n+1}(x,y)=U^{\mathrm{SP}}(x,y)+\overline{T_n(x,y)}\left[1-\boldsymbol{R}\left[(x,y);\rho\right]\right], \tag{8}$$

当(8)式所描述的过程完成时，一次迭代过程结束。之后，通过评估 $\boldsymbol{T}_{n+1}(x,y)$ 所包含的图像 $\boldsymbol{T}_{n+1}(x,y)$ 与原始图像之间的相似性来决定迭代是否继续。为此，引入相关系数来评价这种相似性，相关系数(CC，C_{C})被定义为

$$C_{\mathrm{C}}=\frac{E\left\{\left[U-E(U)\right]\left[\left|\boldsymbol{T}_{n+1}\right|-E\left(\left|\boldsymbol{T}_{n+1}\right|\right)\right]\right\}}{\sqrt{E\left\{\left[U-E(U)\right]^2\right\}E\left\{\left[\left|\boldsymbol{T}_{n+1}\right|-E\left(\left|\boldsymbol{T}_{n+1}\right|\right)\right]^2\right\}}}, \tag{9}$$

这里 $E[]$ 表示数学期望，此处为了简单起见省略了坐标。如果相关系数没有达到预先设定的阈值，则将 $\boldsymbol{T}_{n+1}(x,y)$ 代入(5)式中进行下一次迭代。否则，就将 $\boldsymbol{T}_{n+1}(x,y)$ 作为解密图像。

3 计算机仿真及讨论

为了验证所提方法的有效性，在PC机上使用MATLAB2011a进行了实验。被测试的图片为Baboon，大小为256 pixel×256 pixel，在图2(a)中给出。模拟中，照明所用光波波长 $\lambda=632.8$ mm，轴向距离取值为为 $d_1=d_2=50$ mm，迭代过程的相关系数的阈值取值为 C_{C}=1。图2(b)，(c)则表示在对原始图像进行加密时所采用的两个随机相位板，即M1, M2。图2(d)表示利用图1所示系统对图像的加密结果，即CCD所记录的衍射强度。按照第2部分所述方法提取原始图像的稀疏数据，取参数 ρ=6，提取到的原始数据如图2(e)所示。图(f)表示图(e)中白色方框的放大图像。

利用所提方法对明文进行恢复，相关系数与迭代次数的关系在图3(a)中给出。可以看出，相关系数在最初的50次迭代中即迅速上升，经过3510次迭代后达到1。对应于 C_{C}=1的重建图像在图3(b)中给出，这说明原始图像被完全恢复，因而本方法的有效性得到了证实。作为比较，在图3(c)中给出了不使用稀疏数据作为振幅部分支撑[对应于 ρ=0，即迭代过程中将公式(8)中等式右端的第二项去掉]的情况下相关系数与迭代次数之间的关系。可以看出，尽管收敛速度也较快，但是在迭代超过50次以后，相关系数始终停滞在0.73

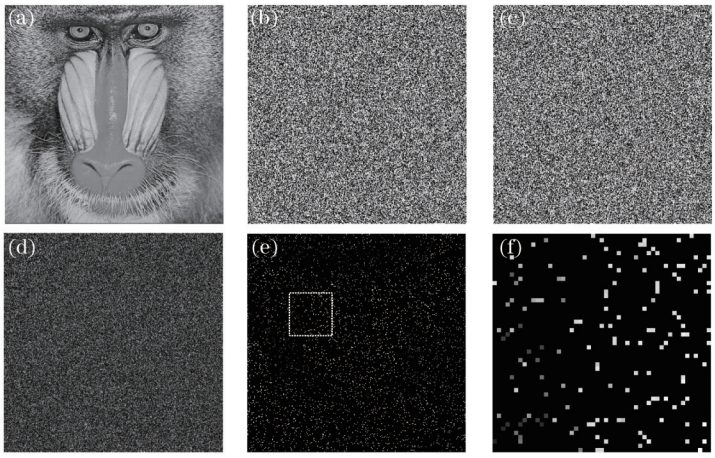

图2 被测试的Baboon图片、相位板及模拟结果。(a) 原始明文; (b) 随机相位板M1; (c) 随机相位板M2; (d) CCD记录的密文; (e) 原始图像的稀疏数据;(f) 图(e)中白色方框的放大图像

Fig.2 Measured baboon′s picture, phase plate and simulation results. (a) Plaintext (512 pixel×512 pixel and 8 bits); (b) phase-only masks M1 and (c) M2; (d) diffraction intensity pattern; (e) sparse data of the primary image; (f) magnified area marked with a white rectangle in Fig.(e)

左右的平台上,即迭代过程出现了停滞。对应于C_c=0.73的重建图像在图4(d)中给出,可见恢复结果含有严重的噪声,这进一步证实了本方法的有效性。

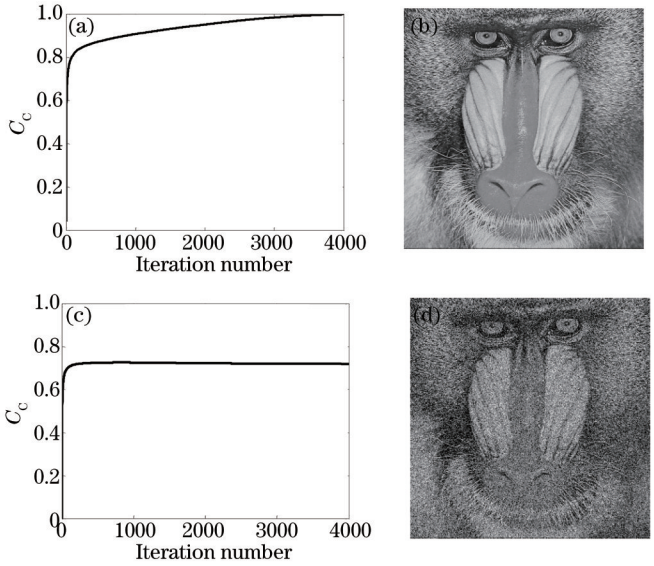

图3 相关系数与迭代次数的关系[(a) ρ =6; (c) ρ =0],以及与这两种情况对应的4000次迭代后的解密结果[(b) ρ =6; (d) ρ =0]

Fig.3 Dependence of CC on iteration number [(a) ρ =6; (c) ρ =0] and the corresponding decrypted images after 4000 iterations [(b) ρ =6; (d) ρ =0]

图4(a)给出了解密时当M1错误而其他参数正确的情况下,使用解密算法迭代4000次后的解密结果。可以看出,从解密结果无法获取任何与原始图像有关的信息。其对应的相关系数为C_c=0.00274,这进一步证实了在密钥M1错误的情况下,解密结果与原始图像毫不相关。与此对应的相关系数与迭代次数的关系在图4(b)中给出,可见相关系数呈无规律变化形态,且始终在一个非常小的数值范围变化。此外,当M2错误时的仿真结果在图4(c),(d)中给出。可见,当两个密钥M1,M2其中任何一个错误时,在其他参数正确的情况下均无法解密出正确结果。由于M1,M2统计独立,因此方法具有巨大的密钥空间,对于暴力攻击具有较高安全性。

在实际应用中,波长λ以及轴向距离d_1,d_2可以作为附加密钥使用,因此也研究了解密结果对这些参数的敏感性。图5(a),(b)给出了其他参数正确情况下,所使用波长偏离正确波长(加密时所用波长)10 μm情况下的解密结果。其中,图5(a)为迭代4000次之后的结果,对应的相关系数为C_c=0.0077,图5(b)为相关系

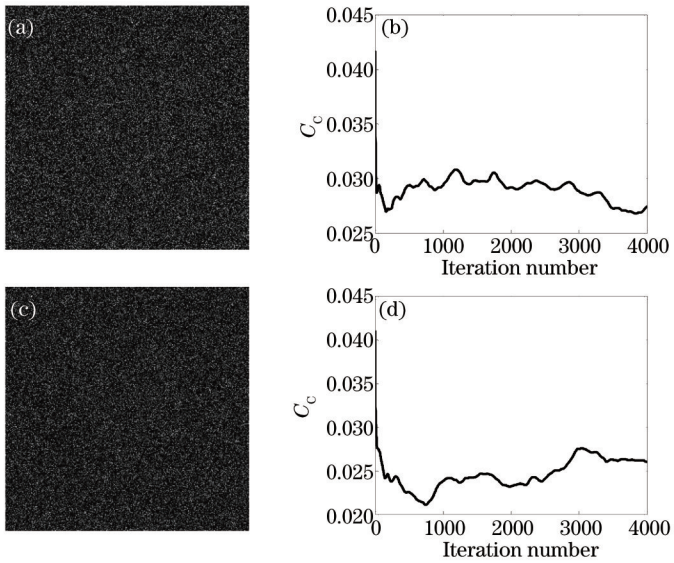

图 4 解密时候(a)M_1和(c)M_2错误时迭代 4000 次之后的解密结果; (b), (d)是与(a), (c)对应的相关系数与迭代次数的关系

Fig.4 Dependence of CC on iteration number by using (a) wrong $M1$ and (c) wrong $M2$, and the decrypted images [(b) and (d)] after 4000 iterations corresponding to Figs.(a) and (c)

数与迭代次数之间的关系。图 5(c),(d)则给出了解密时轴向距离 d_1与正确值相差 1 mm 的解密结果,其中图 5(c)为迭代 4000 次之后的结果,图 5(d)为相关系数与迭代次数之间的关系,对应的 C_c=0.00305。由于对 d_2,存在偏差的情况下的仿真结果与 d_1类似,因此这里不再给出。由以上结果可以看出,在附加参数不正确的情况下,利用解密算法无法得到正确解密结果,并且,解密结果对附加参数特别敏感,这进一步证实了本方法的安全性。

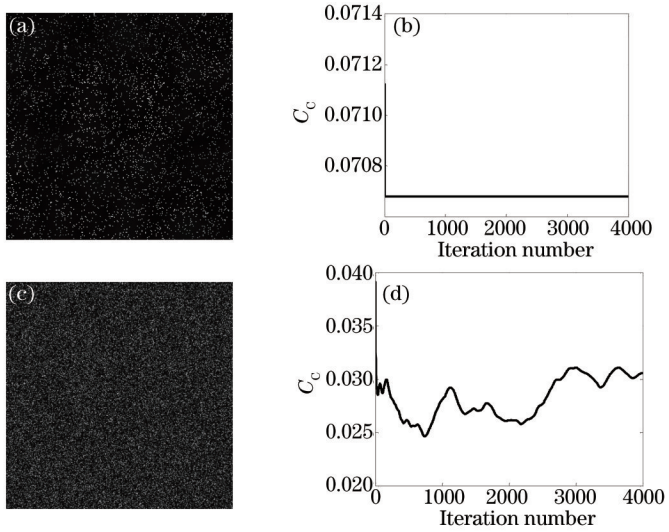

图 5 (a),(c)迭代 4000 次后的解密结果及(b),(d)相关系数与迭代次数的关系,(a)和(b)对应于波长误差为 10 mm; (c)和(d)对应于轴向误差为 1 mm

Fig.5 Decrypted images (a), (c) after 4000 iterations and (b), (d) dependence of CC on the iteration number, Figs.(a) and (b) are for wavelength deviation equal to 10 mm; Figs.(c) and (d) are for d_1 deviation equal to 1 mm

在数据存储和传输的过程中,密文有可能被噪声污染或者部分丢失,因此研究了本方法对于噪声攻击和剪切攻击的稳健性。图 6(a)给出了丢失 6.25%数据后的密文,图 6(b)为在这种情况下迭代 4000 次后解密结果,其对应的相关系数为 C_c=0.3804。图 6(c)则是在这种情况下相关系数与迭代次数的关系。可见,方法对于剪切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的丢失。为了测试本方法对于噪声攻击的稳健性,给密文加入了分布于[0; 0.01]的白噪声,加噪后的密文在图 6(d)中给出。图 6(e)为在这种情况下迭代 4000 次后解密结果,其对应的相关系数为 C_c=0.9615。图 6(f)则是在这种情况下相关系数与迭代

次数的关系。可见,本方法对于噪声攻击具有较强的稳健性。

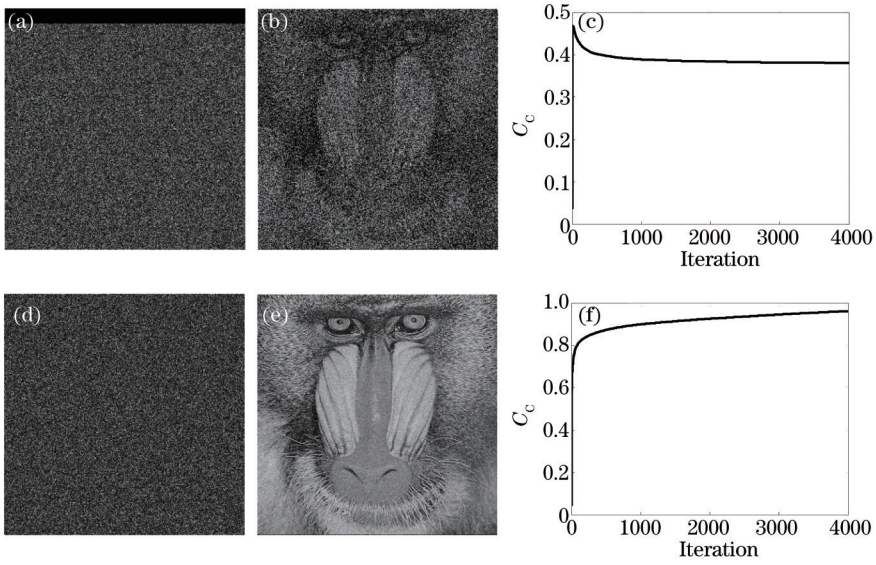

图6 (a)丢失6.25%数据和(d)被噪声污染的密文,(b),(e)迭代4000次之后的解密结果,以及(c),(f)相关系数与迭代次数的关系. (a),(b),(c)对应于丢失6.25%数据的, (d),(e),(f)对应于被噪声污染的

Fig.6 6.25% occluded or contaminated cypertext (a), (d) decrypted images (b), (e) after 4000 iterations and dependence of CC on the iteration number (c), (f). The upper columns (a), (b), (c) is for the 6.25% occluded, while the bottom column (d), (e), (f) is for contaminated

事实上,参量 ρ 在加密过程中具有重要的作用。 ρ 越大,表明加密前提取原始图像的稀疏数据越多,这使得相位恢复的迭代过程中输入平面的支撑越强(掌握的原始图像的信息就越多),因而可以预期,迭代过程的收敛速度就越快。图7(a)给出了 ρ 取不同数值时相关系数与迭代次数之间的函数关系,图7(b), (c), (d)给出了对应于当 ρ =10,20,30时所提取出来的稀疏数据。由图7(a)可知,当 ρ =10,20,30时相关系数达到 C_C=1之前需要的迭代次数分别为465次,154次以及87次,这证实了上述预言。因此,为了提高解密速度,应该使 ρ 尽可能大。然而, ρ 越大,意味着稀疏数据所透露出的原始图像就越多[图7(b),(c),(d)],相应地会降低本加密方法的安全性。因此,实际应用中应该根据具体的情况来确定 ρ 的值。

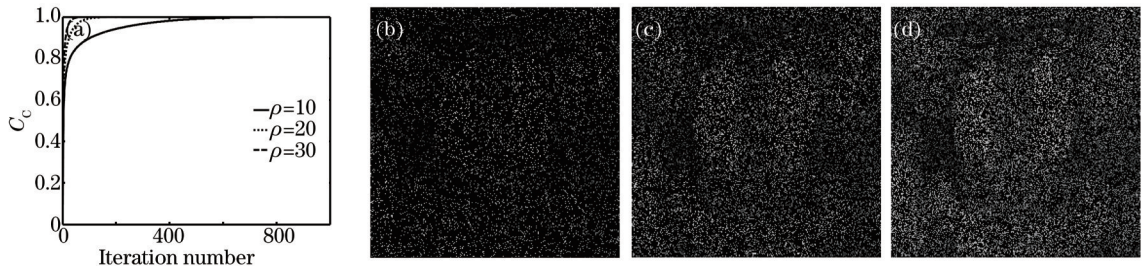

图7 (a) ρ 取不同值时相关系数与迭代次数的关系和分别对应于(b) ρ =10, (c) ρ =20, (d) ρ =30的稀疏数据

Fig.7 Relationship between C_C and iteration number when (a) ρ takes different values and the sparse data of the primary image corresponding to (b) ρ =10, (c) ρ =20, and (d) ρ =30

4 结 论

提出了一种新的基于光学衍射成像原理的图像加密方法。该方法在加密前提取原始图像的稀疏数据,在相位恢复算法的迭代过程中,这些稀疏数据作为输入平面的部分支撑。通过这种新的相位恢复算法,该方法可以从单幅衍射图像强度中完全恢复原始明文。由于只需要记录光波的衍射强度,因此密文记录过程无需使用干涉方法,对加密系统的环境条件较为宽松。此外,与先前提出的一些方法相比[12-14],本文所提出的方法只需要记录单幅强度图像,这使得加密过程变得非常简单,从而较大地提高了加密的效率。计算机仿真结果证实了本方法的可行性和有效性。

参 考 文 献

1 Wan Qin, Xiang Peng. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. Opt Lett, 2010, 35 (2): 118-120.

2 Zhou N, Zhang A, 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.

3 Xi Sixing, Sun Xin, Liu Bing, *et al.*. New image encryption technology of image based on computer generated hologram [J]. Laser and Optoelectronics Progress, 2012, 49(4): 040902.
席思星, 孙 欣, 刘 兵, 等. 基于计算全息的双随机相位图像加密技术[J]. 激光与光电子学进展, 2012, 49(4): 040902.

4 Qin Yi, Zhang Shuai, Gong Qiong, *et al.*. Virtual optical image encryption based on interference[J]. Acta Optica Sinica, 2012, 32(10): 1007001.
秦 怡, 张 帅, 巩 琼, 等. 基于干涉原理的虚拟光学加密系统[J]. 光学学报, 2012, 32 (10): 1007001.

5 Chen Daqing, Zhou Hao, Tao Zhi, *et al.*. Fourier computer-generated hologram digital watermarking with nonlinear amplitude limiting[J]. Acta Optica Sinica, 2011, 31(2): 0207002.
陈大庆, 周 皓, 陶 智, 等. 非线性限幅傅里叶计算全息的数字水印方法[J]. 光学学报, 2011, 31(2): 0207002.

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

7 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.

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

9 Peng X, Zhang P, Wei H, *et al.*. Known-plaintext attack on optical encryption based on double random phase keys[J]. Opt Lett, 2006, 31(8): 1044-1046.

10 Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain[J]. Opt Lett, 2006, 31(22): 3261-3263.

11 Carnicer A, Montes-Usategui M, Arcos S, *et al.*. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. Opt Lett, 2005, 30(13): 1644-1646.

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

13 Wen Chen, Xudong Chen, Colin 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, 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.

15 Rotha P Y, Paganin D M. Blind phase retrieval for aberrated linear shift-invariant imaging systems[J]. New Journal of Physics, 2010, 12(7): 073040.

16 W Chen, X Chen, A Stern, *et al.*. Phase-modulated optical system with sparse representation for information encoding and authentication[J]. IEEE Photonics Journal, 2013, 5(2): 6900113.

17 Gong Q, Liu X, Li G, *et al.*. Multiple-image encryption and authentication with sparse representation by space multiplexing[J]. Appl Opt, 2013, 52(31): 7486-7493.