doi:10.3788/gzxb20154404.0407001

可变光阑光学衍射加密系统

王红娟,刘红钊,黄义定,张颖颖,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:为了克服双随机相位编码系统的局限性,提出基于光学衍射成像原理的图像加密方法.该方法在光学衍射加密系统中加入可变光阑,形成透光面积不同的振幅板,对明文进行加密,得出多个密文.解密时,通过相位恢复算法,从多幅衍射强度图像中恢复原始明文.仿真表明,由于只需要记录光波的衍射强度,在密文记录过程无需使用干涉装置,通过可变光阑可以方便地调节振幅板的透光面积,无需改变光学结构或者移动光学器件,因此,大大降低了加密过程实施的难度.

关键词:信息光学;图像加密;光衍射;可变光阑;相位恢复算法;振幅调制;衍射强度
中图分类号:TP751 **文献标识码**:A **文章编号**:1004-4213(2015)04-0407001-6

Optical Diffraction Encryption System Based on Iris-diaphragm

WANG Hong-juan, LIU Hong-zhao, HUANG Yi-ding, ZHANG Ying-ying,
LIU Xu-yan, QIN Yi
(*College of physics and electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract: In order to overcome the disadvantages of the double random phase encoding, a novel method for image encryption by employing the diffraction imaging technique was proposed. In this method, irisdiaphragm was used in optical diffraction encryption system, and to form amplitude plate of the different transmittance. Using this encryption system to encrypt the plaintext, multiple ciphertexts were obtained. During image decryption, by iterative phase retrieval algorithm the original plaintext is completely extracted from multiple diffraction intensity patterns. Computer simulations indicate that, since only needing to record the diffraction intensity of optical wave, the ciphertexts can be recorded without using interference methods. In addition, by means of iris-diaphragm, the transmittance of amplitude plate is easily adjusted, without changing optical structure or moving optical device, so that is greatly reducing the difficulty of implementation in the encryption process. Simulation results are presented to verify the validity of the proposed approach.

Key words: Information optics; Image encryption; Optical diffraction; Iris-diaphragm; Phase retrieval algorithm; Amplitude modulation; Diffraction patterns
OCIS Codes: 070.2025; 070.4560; 070.7345

0 引言

光学信息处理具有高处理速度、高并行度、多维度密钥、大容量等特点,广泛地应用于信息存储、信息安全、图像处理等应用领域.其中,光学信息加密技术在国际学术界受到了广泛的关注[1-9].已经提出的光学信息加密的方法很多,最引人注目的是 1995 年由 Refregier 和 Javidi 提出的双随机相位编码系统(Double Random Phase Encoding ,DRPE)[10].该系统在光学 4f 系统的输入平面及傅里叶平面各放置一个随机相位板(Random Phase Mask, RPM),从而可将一幅图像加密成复平稳白噪音.然而,在 4f 系统中,两块

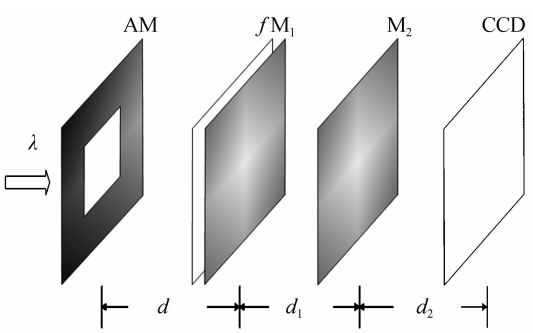
基金项目:国家自然科学基金项目(No. 61306007)、河南省科技厅重点科技攻关项目(No. 142102210476)和南阳师范学院高层次人才科研启动基金项目(No. nytc2006k100)资助
第一作者:王红娟(1979—),女,讲师,硕士,主要研究方向为光电信息处理. Email:35148784@qq.com
通讯作者:秦怡(1981—),男,讲师,硕士,主要研究方向为信息光学及图像处理. Email:641858757@qq.com
收稿日期:2014-08-14;**录用日期**:2014-12-22

相位板分别位于两个特殊的平面内，相位板的轴向位置不能作为密钥；并且该系统结构上需要两个傅里叶变换透镜，较为复杂且成本较高. 因此，在保证系统安全性能的基础上，必须尽量简化系统的装置. 针对这个问题，Situ 等人提出在菲涅耳域进行图像加密[11]. 该加密系统不需要透镜，简化了光学加密系统的复杂性. 此外，距离和波长均可以作为光学加密参量，扩大了密钥空间[12-13].

然而，以上基于双随机相位编码(Double Random Phase Encoding，DRPE)的光学加密系统中，其密文均为复数，一般应采用干涉的方法记录，而干涉系统对装置的稳定性要求非常高，这给记录带来了严重的不便. 为了解决这些问题，Chen 等人提出了基于光学衍射成像技术的图像加密系统[14-17]. 此类系统以图像在光学衍射结构中的衍射强度为密文，避免了干涉装置. 此外，由于将衍射场的强度作为密文，系统的安全性也较双随机相位编码系统(Double Random Phase Encoding，DRPE)得到了进一步提高. 然而此类系统为了实现高质量解密，必须在加密过程中改变光学结构或者移动光学器件来记录多幅衍射强度作为密文. 然而，光学元件的移动实施起来难度较大且非常耗时，这势必使得加密过程变得相当复杂和不易控制. 为了解决这一问题，本文提出一种基于可变光阑的光学衍射加密系统，在光学衍射加密系统中加入了可变光阑，形成了透光面积不同的振幅板. 而通过可变光阑可以方便地调节振幅板的透光面积，因此加密过程无需该变光学结构或者移动光学元件，即可记录多幅衍射强度，这在很大程度上降低了加密过程实施的难度. 文中给出了理论分析和计算机仿真结果.

1 理论分析

基于可变光阑的光学衍射加密系统的结构如图 1. 其中 $f(x,y)$ 为待加密的图像，M_1 和 M_2 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，



AM: amplitude plate; *f*: plaintext; M_1, M_2: phase-only mask; CCD: charge-coupled device

图 1 本文所提出的光学衍射加密系统

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

AM 为振幅板，振幅板的中心方孔区域的光强透过率为 1，其他区域为 0. 波长为 λ 的单色平面光波照射振幅板，经过距离为 d 的衍射之后到达待加密图像所在平面，照射原始图像 f. 原始图像被紧贴其的随机相位板 M_1 调制，之后经过距离为 d_1 的衍射之后到 M_2 所在平面，再被 M_2 调制，之后又经距离为 d_2 的衍射至输出平面，其强度被 CCD 记录. 在本文所提方法中，需要使用三个透射面积不同的振幅板对照明光波进行波前调制，这三个振幅板记为 $AM^{(k)}(p,q)(k=1,2,3)$，相应的，与之对应的加密密文也有三幅，记为 $I^{(k)}(\mu,\nu)(k=1,2,3)$.

在图 1 所示结构中，波长为 λ 的单色平面光波照射振幅板，经过距离为 d 的衍射之后到达待加密图像所在平面，入射到待加密图像 f 的光波的复振幅可表示为

$$U^{(k)}(x,y)=\mathrm{Fr}T_\lambda[\mathrm{AM}^{(k)}(p,q);d] \tag{1}$$

这里 (p,q)，(x,y)，(η,ξ)，(μ,ν) 分别表示 AM，M_1，M_2 及 CCD 所在平面的坐标. $\mathrm{Fr}T_\lambda$ 表示关于 λ 的菲涅尔变换. 利用式(1)的记号，入射到随机相位板 M_2 的光波的复振幅可表示为

$$U^{(k)}(\eta,\xi)=\mathrm{Fr}T_\lambda[U^{(k)}(x,y)f(x,y)M_1(x,y);d_1] \tag{2}$$

相应地，CCD 平面所记录的强度可以表示为

$$I^{(k)}(\mu,\nu)=|\mathrm{Fr}T_\lambda\{\mathrm{Fr}T_\lambda[U^{(k)}(x,y)f(x,y)\cdot M_1(x,y);d_1]M_2(\eta,\xi);d_2\}|^2 \tag{3}$$

$I^{(k)}(\mu,\nu)$ 作为密文保存. 而在加密过程中，无需进行光学结构的更改，使用可变光阑可以很方便改变振幅板的透光面积，从而得到三幅密文 $I^{(k)}(\mu,\nu)(k=1,2,3)$. 并且能从 $I^{(k)}(\mu,\nu)(k=1,2,3)$ 中恢复原始图像，解密过程可简述如下：

用 $f_n^{(1)}(x,y)(n=1,2,3\cdots)$ 表示使用第 1 个密文 $I^{(1)}(\mu,\nu)$ 经第 n 轮迭代之后得出的原始图像的估计. 明文 $f_n^{(1)}(x,y)(n=1)$ 初始化为随机实值矩阵，将其作为图 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，每轮迭代中三个振幅板和三幅衍射强度图像依次使用. 具体过程如下：

首先，在图 1 所示的加密系统中使用第一个振幅板 $AM^{(1)}(p,q)$，对所赋的初始值进行运算，在 CCD 平面得到一复函数

$$U_n^{(1)}(\mu,\nu)=\mathrm{Fr}T_\lambda\{\mathrm{Fr}T_\lambda[U^{(1)}(x,y)f_n^{(1)}(x,y)\cdot M_1(x,y);d_1]M_2(\eta,\xi);d_2\} \tag{4}$$

之后，保留此复函数的相位信息，以 CCD 记录的密文 $I^{(1)}(\mu,\nu)$ 作为振幅支撑，构造一个新函数，即

$$\overline{U_n^{(1)}(\mu,\nu)}=\frac{[I^{(1)}(\mu,\nu)]^{1/2}U_n^{(1)}(\mu,\nu)}{|U_n^{(1)}(\mu,\nu)|} \tag{5}$$

将 $\overline{U_n^{(1)}(\mu,\nu)}$ 逆衍射至输入平面，消除去振幅板 $AM^{(1)}(p,q)$ 的衍射效应之后，得到的振幅可表示为

$$\overline{f_n^{(1)}(x,y)}=|\mathrm{Fr}T_\lambda\{\mathrm{Fr}T_\lambda[\overline{U_n^{(1)}(\mu,\nu)};-d_2]\cdot$$

$$M_2^*(\eta,\xi);-d_1\}/U^{(1)}(x,y)| \tag{6}$$

此处 * 表示复共轭.

把$\overline{f_n^{(1)}(x,y)}$作为原始图像新的估计，送入图 1 所示的加密系统，此时在加密系统中使用第二个振幅板 $AM^{(2)}(p,q)$. 此时 CCD 平面得到的复函数为

$$U_n^{(2)}(\mu,\nu)=\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[U^{(2)}(x,y)\overline{f_n^{(1)}(x,y)}\cdot M_1(x,y);d_1]M_2(\eta,\xi);d_2\} \tag{7}$$

保留此复函数的相位信息，以 CCD 记录的密文 $I^{(2)}(\mu,\nu)$作为振幅支撑，构造一个新函数，即

$$\overline{U_n^{(2)}(\mu,\nu)}=\frac{[I^{(2)}(\mu,\nu)]^{1/2}U_n^{(2)}(\mu,\nu)}{|U_n^{(2)}(\mu,\nu)|} \tag{8}$$

再将$\overline{U_n^{(2)}(\mu,\nu)}$逆衍射至输入平面，并消除去振幅板 $U^{(2)}(p,q)$的衍射效应之后，得到的振幅可表示为

$$\overline{f_n^{(2)}(x,y)}=|\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[\overline{U_n^{(2)}(\mu,\nu)};-d_2]\cdot M_2^*(\eta,\xi);-d_1\}/U^{(2)}(x,y)| \tag{9}$$

之后，把$\overline{f_n^{(2)}(x,y)}$作为原始图像新的估计，再次送入图 1 所示的加密系统，此时在加密系统中使用第三个振幅板 $AM^{(3)}(p,q)$. 此时在 CCD 平面得到的复函数为

$$U_n^{(3)}(\mu,\nu)=\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[U^{(3)}(x,y)\overline{f_n^{(2)}(x,y)}\cdot M_1(x,y);d_1]M_2(\eta,\xi);d_2\} \tag{10}$$

保留此复函数的相位信息，以 CCD 记录的密文 $I^{(3)}(\mu,\nu)$作为振幅支撑，构造一个新函数，即

$$\overline{U_n^{(3)}(\mu,\nu)}=[I^{(3)}(\mu,\nu)]^{1/2}U_n^{(3)}(\mu,\nu)/|U_n^{(3)}(\mu,\nu)| \tag{11}$$

再将$\overline{U_n^{(3)}(\mu,\nu)}$逆衍射至输入平面，并消除去振幅板 $U^{(3)}(p,q)$的衍射效应之后，得到的振幅可表示为

$$\overline{f_n^{(3)}(x,y)}=|\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[\overline{U_n^{(3)}(\mu,\nu)};-d_2]\cdot M_2^*(\eta,\xi);-d_1\}/U^{(3)}(x,y)| \tag{12}$$

当式(4)～(12)所描述的过程完成时，一轮迭代过程结束. 之后，通过评估$\overline{f_{n-1}^{(3)}(x,y)}$与$\overline{f_n^{(3)}(x,y)}$所包含的图像之间的迭代误差来决定迭代是否继续，该误差定义为

$$\mathrm{Error}=\sum_{x,y}[\overline{f_n^{(3)}(x,y)}-\overline{f_{n-1}^{(3)}(x-y)}]^2 \tag{13}$$

如果计算得到的迭代误差比预先设定的阈值(δ)小，则将$\overline{f_n^{(3)}(x,y)}$作为解密图像 $f'(x,y)$；否则，将$\overline{f_n^{(3)}(x,y)}$作为原始图像新的估计，代入式(4)中，将$\overline{f_n^{(3)}(x,y)}$代替 $f_n^{(1)}(x,y)$($f_{n+1}^{(1)}(x,y)=\overline{f_n^{(3)}(x,y)}$)，开始下一轮迭代.

另外，为了评估解密图像的质量，引入相关系数来评价明文 $f(x,y)$与解密图像 $f'(x,y)$之间的相似性，相关系数(Correlation Coefficient，CC)被定义为

$$\mathrm{CC}=\frac{E\{[f-E(f)][|f'|-E(|f'|)]\}}{\sqrt{E\{[f-E(f)]^2\}E\{[|f'|-E(|f'|)]^2\}}} \tag{14}$$

这里E表示求数学期望，此处为了简单起见省略了函数坐标. 当相关系数为 1 时，表示两个图像完全相关，此时两幅图像完全一样；当相关系数为 0 时，表示两个图像完全不相关；CC 的值越大，两个图像的相关性越大，这两个图像就越接近.

2 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 MATLAB7.0 进行了实验. 被测试的图片为 Lena，大小为 256×256 像素，在图 2(a)中给出. 模拟中，照明所用光波波长 $\lambda=632.8$ μm，轴向距离取值为为 $d=200$ mm，$d_1=210$ mm，$d_2=220$ mm，迭代过程的迭代误差的阈值取值为 $\delta=0.000\ 1$. 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 M_1，M_2. 图 2(d)、(e)、(f)表示所选用的三个透光面积不同的振幅板，中心方孔透光区域大小分别为 64×64 像素、128×128 像素和 192×192 像素. 图 2(g)、(h)、(i)表示在图 1 所示系统中分别使用图 2(d)、(e)、(f)所示的三个振幅板对图像的加密结果(Ciphertext，CT)，即 CCD 所记录的衍射强度.

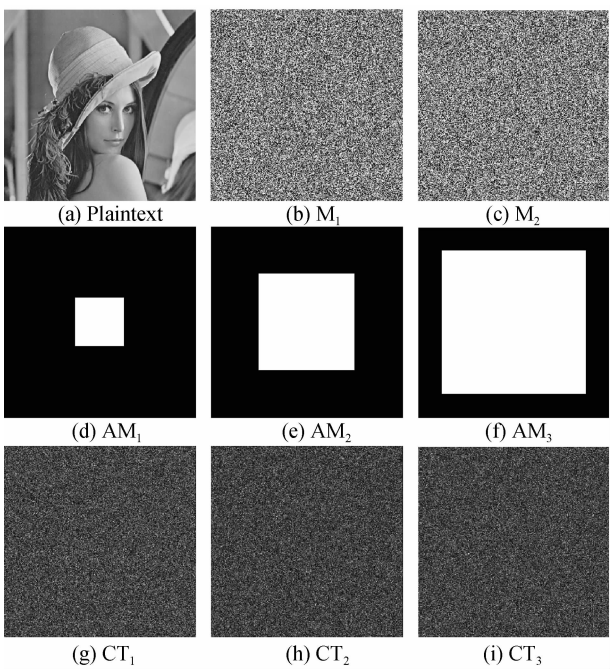


图 2 图像信息加密实验结果

Fig. 2 The experimental results of image information encryption

利用第二部分给出的相位恢复算法，使用正确的密钥对明文进行恢复，相关系数与迭代次数的关系在图 3(a)中给出. 可以看出，相关系数在迭代中迅速上升，经过 35 次迭代后达到 1. 对应于 CC=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.

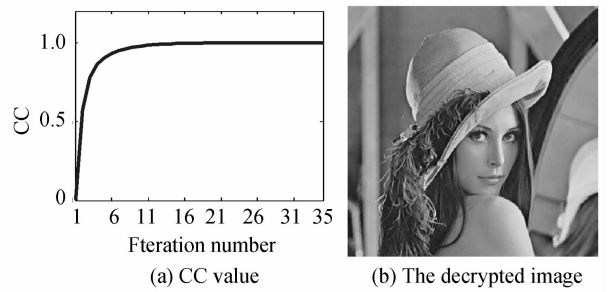


图 3 图像信息解密实验结果

Fig. 3 The experimental results of image information decryption

为了测试本方法对密钥的敏感性，我们首先模拟了在 M_1 错误而其他参量正确的情况下的解密结果，这在图 4(a)、(b)中给出. 图 4(a)给出了相关系数与迭代次数的关系，可见相关系数呈现无规律的变化，且维持在一个较低的数值水平. 迭代 35 次后的解密结果在图 4(b)中给出，其对应的相关系数 CC=－0.0173. 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. 在 M_2 错误而其他参量正确时的解密情况在图 4(c)、(d)中给出，对应于图 4(d)的相关系数为 CC=－0.018 3. 可见，当两个密钥 M_1，M_2 其中任何

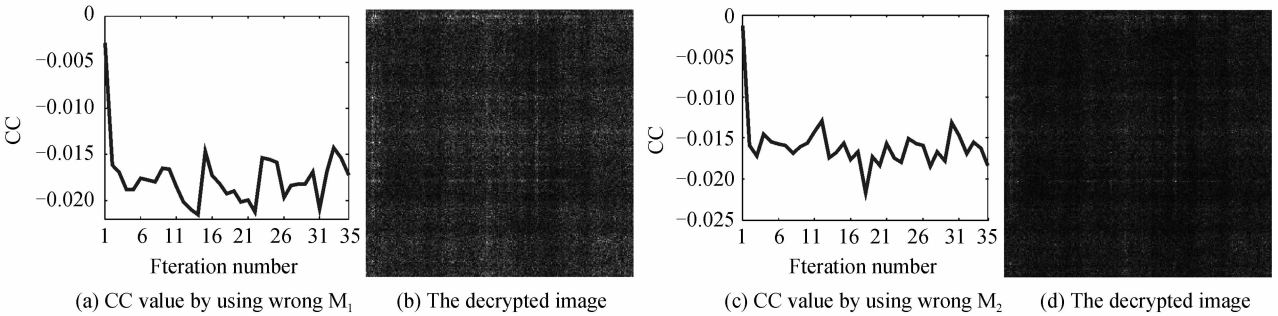
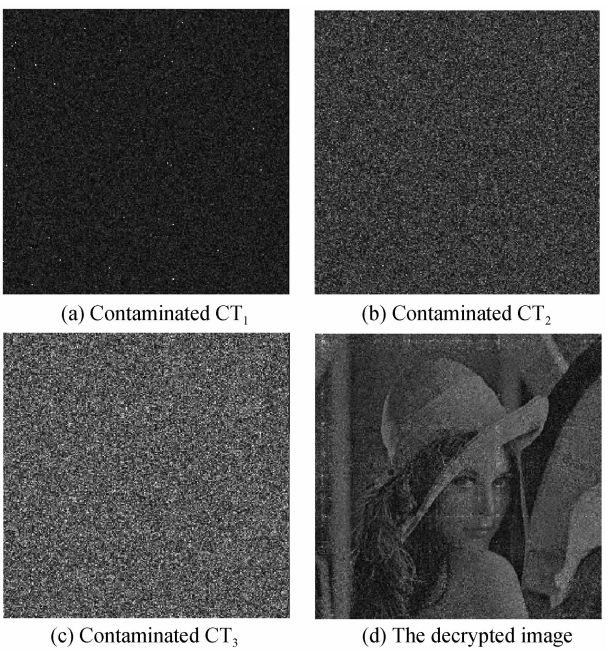


图 4 密钥错误时解密结果

Fig. 4 The decryption results with wrong keys

一个错误时，在其他参量正确的情况下均无法解密出正确结果.

在信息的存储与传输过程中，密文有可能被噪音污染或者部分丢失，因此有必要分析本方法对于这些攻击的稳健性. 为了测试本方法对于噪音攻击的稳健性，假设三个密文(Ciphertext, CT)均受噪音密度为 0.001 的椒盐噪音攻击，加噪后的密文在图 5(a)、(b)、(c)中给出. 利用含噪密文进行解密，其结果在图 5(d)、



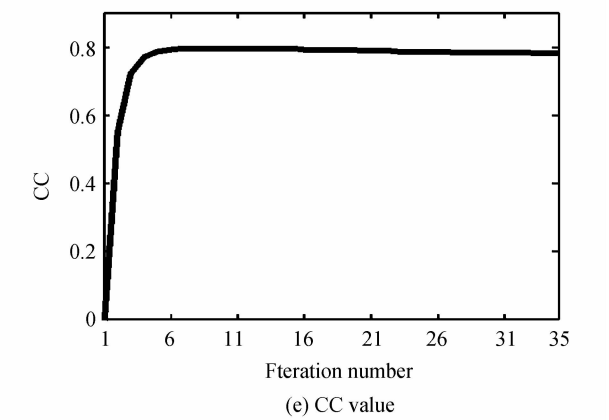


图 5 加密图像抗噪音鲁棒性分析

Fig. 5 The analysis of robustness to encrypted image with noise

(e)中给出. 图 5(d)为在这种情况下迭代 35 次后解密结果，图 5(e)则是在这种情况下相关系数与迭代次数的关系. 其对应的相关系数为 CC=0.786 6. 可见，本方法对于噪音攻击具有一定的稳健性.

图 6(a)、(b)、(c)给出了均丢失 6.25%数据后的三个密文(Ciphertext, CT)，图 6(d)为在这种情况下迭代 35 次后解密结果，图 6(e)则是在这种情况下解密时相关系数与迭代次数的关系. 其对应的相关系数为 CC=0.501 1. 可见，本方法对于剪切攻击的稳健性不高. 因此，在密文传输的过程中，应尽可能保持密文的完整性.

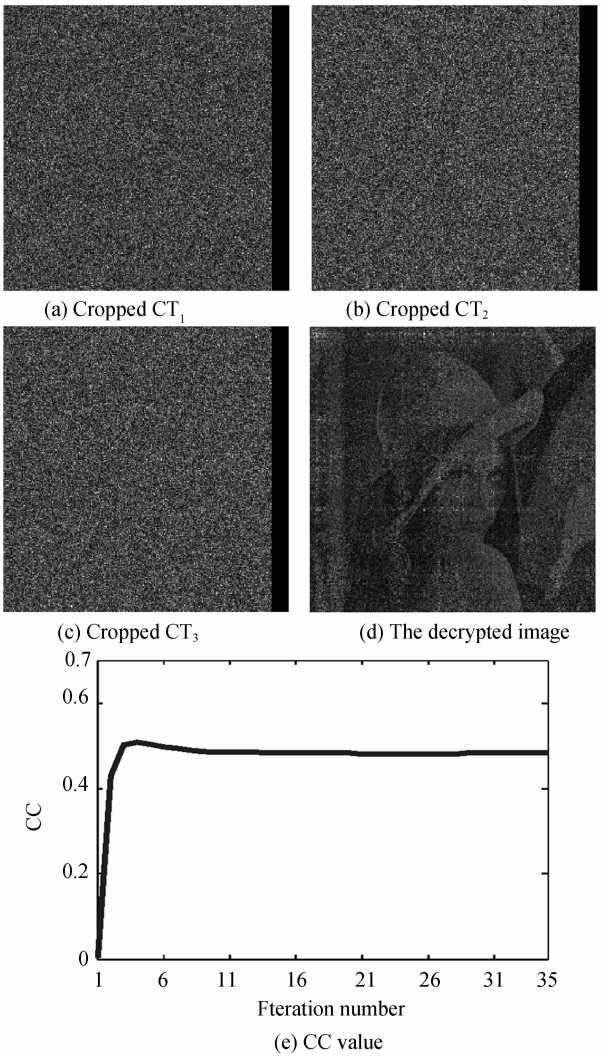


图 6　加密图像抗剪切鲁棒性分析

Fig. 6　The analysis of robustness to the pixels cropped for the encrypted image

以上的模拟结果反映了该方法的有效性，使用该加密系统，通过迭代运算可以高质量地恢复原始图像. 而图 1 中设计的 AM 振幅板的透光面积在一定程度上影响解密过程. 接下来对振幅板中心透光区域的大小变化对解密的影响进行模拟. 为简便起见，仅改变第一个振幅板（即图 2(d)所示）的透光区域面积，将其减小为 25×25 像素，见图 7(a). 另外两个振幅板不变，见图 2(e)、(f). 在图 1 所示的光学衍射加密系统中利用这三个振幅板对原始图像进行加密，对得到的三幅密文使用迭代算法解密，迭代 35 次后解密结果见图 7(b)，其对应的相关系数仅为 CC＝0.257 1，从解密结果无法获取与原始图像有关的信息. 图 7(c)则是在这种情况下解密时相关系数与迭代次数的关系，可见相关系数收敛于比较低的水平. 由此可见，振幅板的透光区域不能过小.

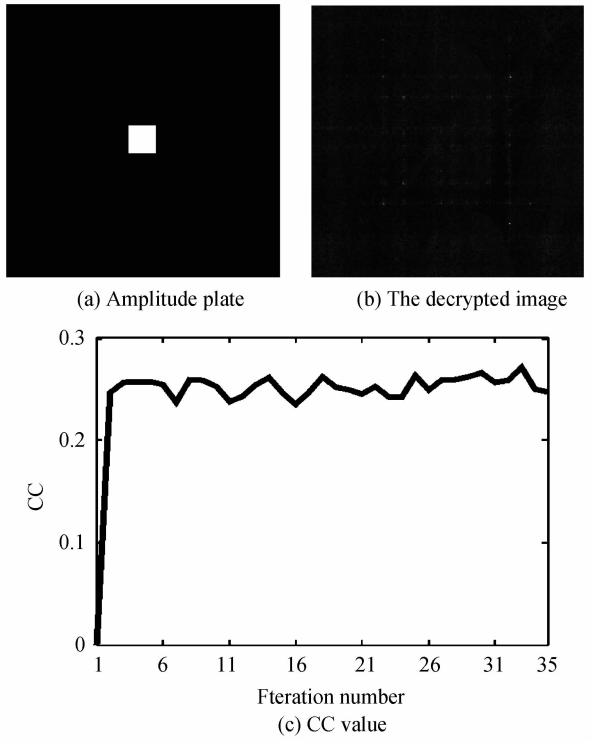


图 7　振幅板透光面积减小情况下的解密结果

Fig. 7　The decryption results when the transmitting area of the amplitude plate decreases

此外，从本文的仿真结果来看，本方法的解密原理在于，利用平面光通过三个不同光阑产生三个不同的振幅调制信息，从而在衍射系统中形成三个相应的密文. 这三个密文在恢复明文过程中产生不同的贡献，从而能够使算法收敛. 如果三个透光位置完全重合，就相当于重复使用一个振幅板，迭代过程中相关系数将停滞于比较低的水平. 因此本方法要求三块振幅板的透光位置区域不能完全重合，但可以互不重合.

3　结论

本文提出了一种新的基于光学衍射成像原理的图像加密方法. 本方法在加密系统中加入了振幅板，振幅板透光率可方便控制. 通过改变振幅板的分布，使用加密系统对明文进行加密，得出多个密文. 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[14-17]，本文所提出的方法利用光阑可以方便地实现振幅板的透光面积的大小变化，无需改变光学结构或者移动光学器件，故大大降低了加密过程的难度. 并且通过分析，为了实现解密，振幅板的透光面积不宜过小. 另外通过鲁棒性分析，该加密系统具有一定的抗噪音攻击的能力，但对于剪切攻击的稳健性不高.

参考文献

[1] WANG Bo, ZHANG Yan. Double images hiding based on optical interference[J]. *Optics Communications*, 2009, **282**(7): 3439-3443.

[2] QIN Wan, PENG Xiang. Asymmetric cryptosystem based on phase-truncated Fourier transforms[J]. *Optics Letters*, 2010, **35**(2): 118-120.

[3] ZHOU Nan-run, WANG Yi-xian, GONG Li-hua, *et al*. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform[J]. *Optics Communications*, 2011, **284**(12): 2789-2796.

[4] WANG Xiao-gang, ZHAO Dao-mu. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain[J]. *Optics Communications*, 2011, **284**(1): 148-152.

[5] ALFALOU A, BROSSEAU C. Optical image compression and encryption methods[J]. *Advance in Optics and Photonics*, 2009, **1**(3): 589-636.

[6] NIU Chun-hui, WANG Xiao-ling, MAO Xian-hui. Multiple-image hiding based on interference principle[J]. *Optical and Quantum Electronics*, 2012, **43**(6-10): 91-99.

[7] MELA C L, IEMMI C. Optical encryption using phase-shifting interferometry in joint transform correlatorr[J]. *Optics Letters*, 2006, **31**(17): 2562-2564.

[8] QIN Yi, ZHENG Chang-bo. Color image encryption based on doublerandom phase encoding[J]. *Acta Photonica Sinica*, 2012, **41**(3): 326-239.
秦怡, 郑长波. 基于双随机相位编码的彩色图像加密技术[J]. 光子学报, 2012, **41**(3): 326-239.

[9] ZHANG Da-kui, MA Li-hong, LIU Jian, *et al*. Amplitude image optical encryption based on two-step-only quadrature phase-shifting interferometry[J]. *Acta Photonica Sinica*, 2012, **41**(1): 72-76.
曾大奎, 马利红, 刘健, 等. 基于两步正交相移干涉的振幅图像光学加密技术[J]. 光子学报, 2012, **41**(1): 72-76.

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

[11] SI-TU Guo-hai, ZHANG Jing-juan. Double random-phase encoding in the Fresnel domain[J]. *Optics Letters*, 2004, **29**(14): 1584-1586.

[12] SI-TU Guo-hai, ZHANG Jing-juan. Position multiplexing for multiple-image encryption[J]. *Journal of Optics A: Pure and Applied Optics*, 2006, **8**(5): 391-397.

[13] SI-TU Guo-hai, ZHANG Jing-juan. Multiple-image encryption by wavelength multiplexing[J]. *Optics Letters*, 2005, **30**(11): 1306-1308.

[14] CHEN Wen, CHEN Xu-dong, SHEPPARD C J R. Optical image encryption based on diffractive imaging[J]. *Optics Letters*, 2010, **35**(22): 3817-3819.

[15] CHEN Wen, CHEN Xu-dong, SHEPPARD C J R. Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating[J]. *Applied Optics*, 2011, **50**(29): 5750-5757.

[16] CHEN Wen, CHEN Xu-dong, SHEPPARD C J R. Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain[J]. *Optics Express*, 2012, **20**(4): 3853-3865.

[17] CHEN Wen, CHEN Xu-dong, ANAND A, *et al*. Optical encryption using multiple intensity samplings in the axial domain[J]. *Journal of the Optical Society of America A*, 2013, **30**(5): 806-812.