利用 QR 码在光学干涉多图像加密系统中实现信息高质量恢复

王红娟 王志鹏 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 为了解决解密图像之间的串扰噪声,在基于干涉原理的多图像加密系统中引入了快速响应矩阵(QR)码。该光学加密系统加密过程使用计算机进行数字运算实现,而解密过程可以使用数字实现,也可以使用光学方法实现。加密时多组原始信息首先被转换为相应的 QR 码,然后多组 QR 码被解析地隐藏于两个纯相位板中。解密时,使用相干光照射两个纯相位板,并通过分束镜使二者的衍射光场进行叠加,再经不同的衍射距离后所得的衍射强度即为解密图像,把得到的几组解密图像直接用智能手机进行扫描,即可完全恢复原始信息。相较于原来的基于干涉原理的多图像加密方法,该加密方法成功地解决了串扰噪声问题,实现了信息的高质量恢复。计算机模拟结果证实了该方法的有效性,也分析了对裁剪和噪音攻击的稳健性。

关键词 信号处理;光学加密;干涉原理;QR 码;多图像加密
中图分类号 TP751 **文献标识码** A **doi**: 10.3788/AOS201434.0907001

Using QR Codes in Multi-Image Optical Interference Encryption System to Reconstruct High Quality Original Information

Wang Hongjuan Wang Zhipeng Zhang Yingying Liu Xuyan Qin Yi
(*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang, Henan* 473061, *China*)

Abstract In order to solve the crosstalk problem between decrypted images, quick response (QR) code is introduced in the image encryption system based on principle of interference. The encryption process is realized on computer digitally and the decryption process can be completed optically or digitally. For encryption, multiple sets of the information to be encrypted is first transformed into the corresponding QR code, then these QR codes are analytically hidden into two phase only masks (POMs). For decryption, the diffraction field of the two POMs is superposed by utilizing the beam splitters. After that the wavefront propagates to different distances and the intensity of the complex field, which are exactly the decrypted images. Directly scanning by a smartphone, original information can be completely retrieved. The encryption method successfully solves the problem of crosstalk noise. Simulation results are presented to verify the validity of the proposed approach. The feasibility and robustness against occlusion and noise attacks are verified by a series of numerical simulations.

Key words signal processing; optical encryption; principle of interference; QR codes; multiple images encryption
OCIS codes 070.2025; 070.4560; 070.7345

1 引 言

当今,信息安全是一个很重要的议题,信息安全技术引起了人们空前的重视。光学加密技术作为信息安全技术中的一种,由于其能够并行高速处理二维信息,还能融合各种物理参数,因而在信息安全领域内得到了广泛的应用[1-6]。最为典型的成果是 1995 年由 Refregier 等[7]提出的双随机相位编码系统(DRPE),该系统能把一幅图像加密为平稳白噪

收稿日期: 2014-03-28; **收到修改稿日期**: 2014-04-30
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(QN2014016)
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

声。自该系统被提出以来，越来越多的光学加密方法被研究[8-11]。近几年来，由于多图像加密技术能提高信息传输的效率，多图像加密越来越受到了重视，人们对此做了许多研究并形成了一些基于DRPE系统的多图像加密方法。Situ等[12-13]提出的波长复用和位置复用，Liu等[14]提出的利用频谱转移实现多图像加密。

然而，基于DRPE系统的加密结果均为复数，这很不便于对信息的传输与记录，很难用目前的光学技术来实现。于是，人们考虑将图像隐藏到纯相位板中[15-17]，Zhang等[17]提出的基于干涉原理的加密方法最具代表性，该方法不需要复杂的迭代运算，原理非常简单，将原始图像信息隐藏到两个相位板，这两个相位板可以解析获得，解密图像可以直接用强度设备进行记录。Wang等[18-19]在该系统上实现了双图像和多图像加密。但是该方法必须进行迭代，这也就削弱了干涉加密方法无需迭代和省时的优点。Qin等[20]实现了完全无需迭代的、基于干涉原理的多图像加密。但是从结果可以看出，多图像之间的串扰噪声问题比较突出。为了解决图像之间的串扰噪声，受Barrera等[21]的启发，本文把快速响应矩阵(QR)码引入基于干涉原理的多图像加密系统中，原始信息的QR码被加密系统隐藏于两个纯相位板。解密时，两个纯相位板(POM)经相应距离的衍射之后干涉叠加，干涉场的强度即为恢复的QR码，此时的QR码带有较大的噪声，由于QR码具有强大的错误纠正能力，利用智能移动设备的QR码识别软件能够高质量地恢复原始信息，成功地解决了多信息加密时产生的串扰噪声问题。

2　理论分析

图1给出了Qin等[20]提出的光学加密解密系统结构。利用该系统进行加密解密时，加密过程使用计算机进行数字运算实现，而解密过程可以使用数字实现，也可以使用光学方法实现。为了实现解密，随机相位板M1被波长为λ的单色平面波照射，经过距离为l的菲涅耳衍射到达g平面位置(图中虚线)。同时随机相位板M2也被波长为λ的单色平面波照射，经过距离为l的菲涅耳衍射也到达g平面。之后，两束光的干涉就会在轴向的不同位置产生所需要的明文，使用图像传感器(如CCD等)即可记录解密后的图像。Qin等[20]提出的光学加密解密系统结构中M3的设置是为了消除轮廓像，这里，为了简便起见，省去了M3。

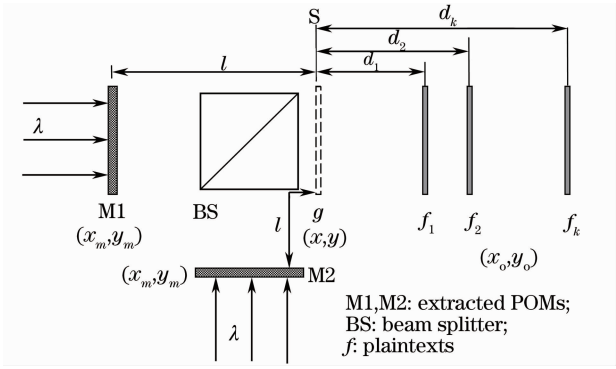

图1　所提加密系统的解密结构

Fig. 1　Schematic of the optical decryption system

其加密过程可简述如下：假设$f_k(x_o,y_o)$为第$k(k=1,\cdots,N)$幅待加密图像，对每幅明文分配一个随机相位，得到复函数

$$f'_k(x_o,y_o)=\sqrt{f_k(x_o,y_o)}\exp[\mathrm{i}2\pi\mathrm{rand}(x_o,y_o)], \tag{1}$$

式中rand函数产生位于[0,1]之间的随机白噪声。对得到的复图像$f'_k(x_o,y_o)$用波长为λ单色平面波照射，经过距离为d_k的菲涅耳逆衍射，该过程的数学表达式为

$$g_k(x,y)=\mathrm{FrT}_\lambda[f'_k(x_o,y_o);-d_k], \tag{2}$$

式中FrT_λ表示关于λ的菲涅耳变换。然后把这些$g_k(x,y)$相加，得到

$$g(x,y)=\sum_{k=1}^{N}g_k(x,y), \tag{3}$$

$g(x,y)$在图1所示的解密光路中用虚线表示，用以说明加密过程。再把得到的$g(x,y)$，用干涉原理的加密方法，隐藏于两个纯相位板M1和M2中：

$$g(x,y)=\exp(\mathrm{i}M_1)*h(x_m,y_m,l)+\exp(\mathrm{i}M_2)*h(x_m,y_m,l), \tag{4}$$

式中

$$h(x_m,y_m,l)=\frac{\exp(\mathrm{i}2\pi l/\lambda)}{\mathrm{i}\lambda l}\exp[\mathrm{i}\pi(x_m^2+y_m^2)/(\lambda l)], \tag{5}$$

表示菲涅尔衍射过程的单位冲击响应，$*$表示卷积运算，l表示相位板至$g(x,y)$所在平面的距离。至此，就把N幅图像隐藏于纯相位板M1和M2，实现了多幅图像的加密。

根据加密过程的原理，下面分析如图1所示的解密过程。首先，分别经M1和M2调制的两束光，经过距离l的传播之后干涉，在g平面位置形成干涉场函数$g(x,y)$。中间函数$g(x,y)$经距离d_k的衍射之后，在输出面上就可以获得第k幅解密图像为

$$\hat{f}_k(x_o,y_o)=\mathrm{FrT}_\lambda[g(x,y);d_k]=f'_k(x_o,y_o)+n^k(x_o,y_o),\tag{6}$$

式中

$$n^k(x_o,y_o)=\sum_{q\neq k}n_q(x_o,y_o)=\sum_{q\neq k}\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[f'_q(x_o,y_o);-d_q];d_k\},\tag{7}$$

解密结果由两部分组成。一部分为 $f'_k(x_o,y_o)$，这正是加密时被加密的第 k 幅复数图像。第二部分为 $n^k(x_o,y_o)$，这是 $g(x,y)$ 中所包含的另外 $N-1$ 幅图像的信息经不正确衍射距离得到的结果，是其他所有的 $f'_q(x_o,y_o)$ $(q\neq k)$ 经 d_k 而不是 d_q 距离衍射的结果，这也就形成了对 $f'_k(x,y)$ 的串扰噪声。用图像传感器(如 CCD 等)记录 $f'_k(x,y)$ 的强度，就恢复出来了第 k 幅原始图像 $f_k(x_o,y_o)$。

下面，在计算机上使用 Matlab 7.0 对用 Qin 方法进行模拟。把分别包含“optical encryption”、“secret picture”、“physics college”信息的三幅图像用图 1 所示的系统进行加密与解密，这三幅图在图 2(a)～(c)中给出，大小均为 512×512×8 bit。模拟中，所取参数分别为 $d_1=50$ mm，$d_2=80$ mm，$d_3=110$ mm，$l=50$ mm，照明所用光波波长 $\lambda=632.8$ nm。在解密参数正确的情况下得到的解密结果在 2(d)～(f)中给出。

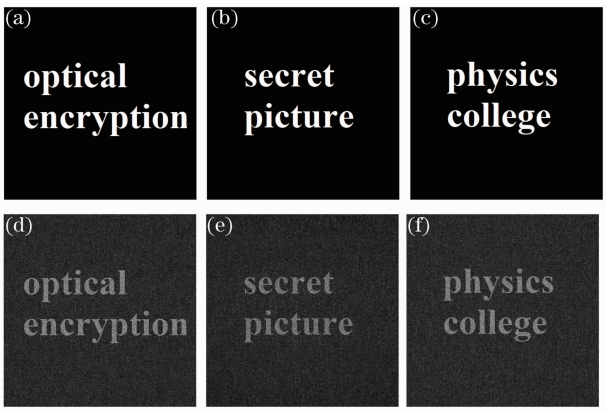

图 2 原始图像与 Qin 方法的解密结果

Fig. 2 Original image and decryption results of the Qin method

为了客观地评价原始图像与恢复图像之间的相似程度，这里引入相关系数作为评价标准。原始图像 $f_k(x_o,y_o)$ 与恢复图像 $|\hat{f}_k(x_o,y_o)|$ 之间的相关系数(C)被定义为

$$C=\frac{E\{[f_k-E(f_k)][|\hat{f}_k|-E(|\hat{f}_k|)]\}}{\sqrt{E\{[f_k-E(f_k)]^2\}E\{[|\hat{f}_k|-E(|\hat{f}_k|)]^2\}}},\tag{8}$$

式中 E 表示求数学期望，这里省去了函数坐标。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；C 的值越大，两个图像的相关性越大，这两个图像就越接近。经计算可得以上三幅图像与原始图像之间的相关系数分别为 $C=0.685$、0.594、0.635。可见，恢复图像与原始图像的相关性并不高，该方法的解密图像质量不高，其原因主要在于解密过程中产生的串扰噪声比较大，串扰噪声正如(7)式所描述。

QR 码作为二维条码的一种，是日本 Denso 公司于 1994 年研制的矩阵式二维条码。它具有强大的错误纠正能力，即使在 QR 码缺损情况下，依然可以完全恢复原始信息，还可根据实际应用设置不同的安全等级。它还具有 360°全方位，超高速识读等优点，并且随着智能手机和平板电脑的普及，QR 码的读取更加方便。QR 码的生成与识别软件也可以很方便地免费下载到。在 Qin 等提出的基于干涉原理的多图像加密系统中，解密图像质量不高，这主要是由于叠加在解密图像之上的串扰噪声所引起的。为了解决图像之间的串扰噪声，在 Qin 等提出的基于干涉原理的多图像加密系统中尝试引入 QR 码，其基本思路可以用图 3 表示。把原始信息转换成与其相对应的 QR 码，使用 Qin 方法将这些 QR 码隐藏于两个纯相位板中，再使用相干光照射两个纯相位板，并通过分束镜使二者的衍射光场进行相干叠加，经相应的衍射距离后所得的衍射强度为解密图像，即含噪的 QR 码，最后使用智能设备进行识别，从而实现信息的无损恢复。

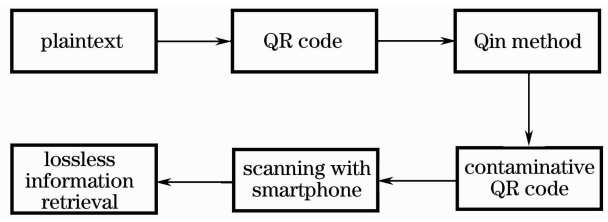

图 3 本文所提出的方法

Fig. 3 Proposed method in this paper

需要指出的是，在图 3 所示的本文所提出的方法中，使用智能手机识别含噪声的 QR 码是最为关键的步骤。QR 码的识别过程在图 4 中给出。

由图 4 可以看出，QR 码的译码过程包含两个

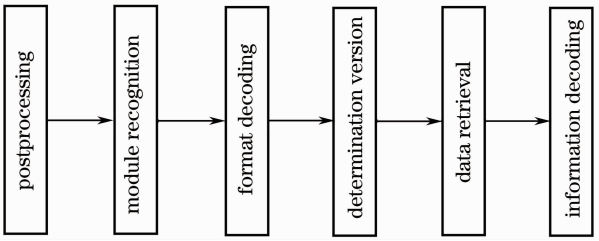

图 4　QR 码译码步骤

Fig. 4　Decoding process of the QR code

重要的信息修复技术。第一种为图像预处理技术。由于 QR 码为典型的二值图像，因此图像的预处理过程可以极大的抑制各种噪声。第二种为纠错技术，QR 码的纠错算法最高可纠正 30%数据码字。这两种信息修复技术可以保证 QR 可以抵抗强烈的噪声干扰，从而在强噪声环境下实现信息的准确恢复。

3　计算机仿真

为了证实本文提出方法的有效性和可行性，在计算机上使用Matlab7.0进行了模拟。在模拟中所使用的 QR 码生成软件是 PsQREdit_chs。把“optical encryption”、“secret picture”、“physics college”三组信息分别转换为 QR 码，在图 5(a)～(c)中给出，大小均为 512×512×8 bit。把这三幅 QR 码送入图 1 所示的系统进行加密与解密。

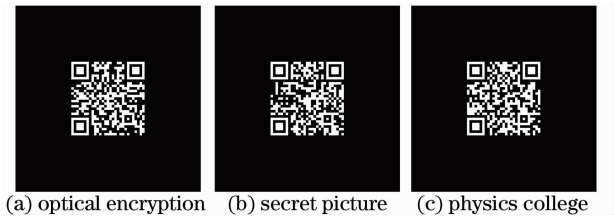

图 5　与原始信息对应的 QR 码

Fig. 5　QR codes corresponding to the original information

模拟中，参数的取值与第二部分中一样，分别为 $d_1=50$ mm，$d_2=80$ mm，$d_3=110$ mm，$l=50$ mm，照明所用光波波长 $\lambda=632.8$ nm。图 6(a)、(b)给出了使用本文所提方法的加密结果，即纯相位板 M1 及 M2。在解密参数正确的情况下得到的解密结果在图 6(c)～(e)中给出。

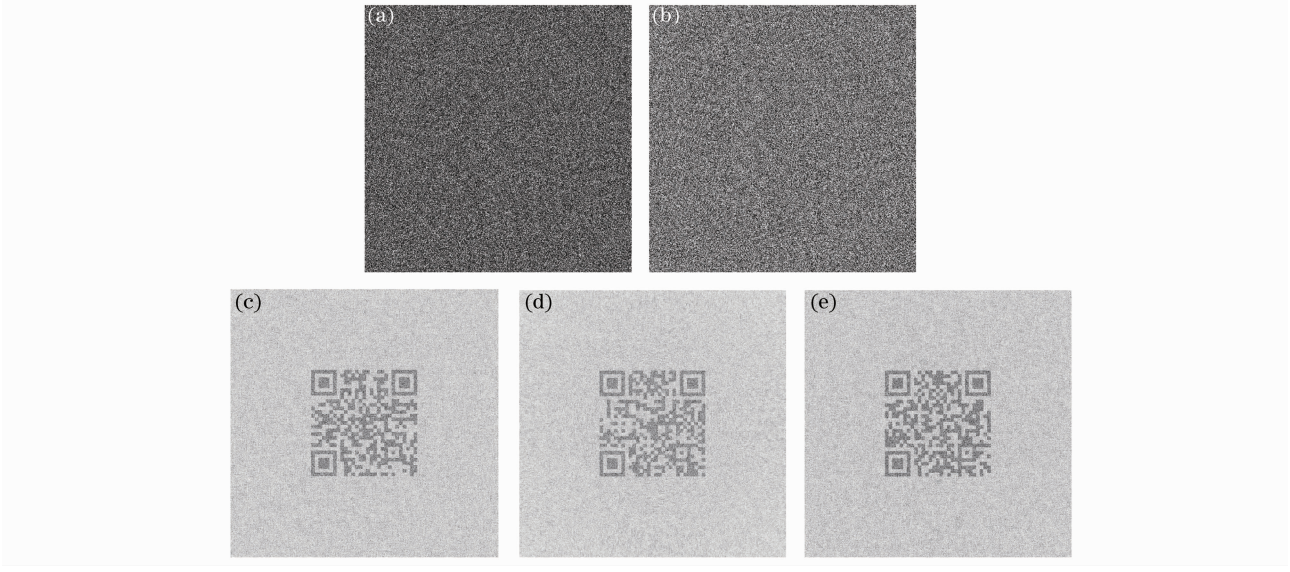

图 6　加密及解密结果。(a) M1；(b) M2；(c)～(e)解密结果

Fig. 6　Encryption and decryption results. (a) M1; (b) M2; (c)～(e) decryption result

从图 6 可见，由于解密过程中的串扰噪声，解密出来的图像的质量不高。对图 6(c)～(e)所示的解密结果用手机直接扫描，扫描结果在图 7(a)～(c)中给出。经计算，解密结果与原始图像的相关系数 $C=1$。可见，即使在解密的 QR 码存在噪声的情况下，仍然能够被智能设备成功扫描并读取信息，从而实现了信息的无损恢复，至此成功地解决了串扰噪声问题，本方法的有效性得到了证实。为了研究本文中 QR 码对噪声的容忍程度，给图 5 所示的原始 QR 码加入均匀分布于$[0,\alpha]$的加性白噪声，结果发现当 $\alpha>0.3$ 时，QR 无法继续被识别，因此本方法中 QR 码对白噪声的容忍阈值为 0.3。

图 7 使用手机对图 6(c)～(e)进行扫描的结果

Fig. 7 Scan results of Figs. 6(c)～(e) using smart phone

在信息的存储与传输过程中，两相位板 M1，M2 很可能遭受噪音攻击及剪切攻击，因此有必要分析本方法对于这些攻击的稳健性。测试对于剪切攻击的稳健性，被剪切之后的相位板在图 8(a)、(b)给出，20%的密文信息被剪切掉。对被部分剪切之后的相位板应用图 1 所示的解密系统进行解密，得到一组解密的 QR 码，在图 8(c)～(e)中给出。对解密的 QR 码再用智能设备进行扫描恢复，识别结果在图 8(f)～(h)给出。可见即使在密文丢失 20%的情况下，利用本方法依然可以完全恢复原始信息。为了进一步研究本方法对剪切攻击的稳健性，对密文被剪切掉更多数据的情况进行了测试，结果表明，本方法的剪切容忍阈值为 25%，也即密文丢失 25%数据的情况下，QR 所附加的噪声超出了扫描设备的识别能力，其内容无法读出。

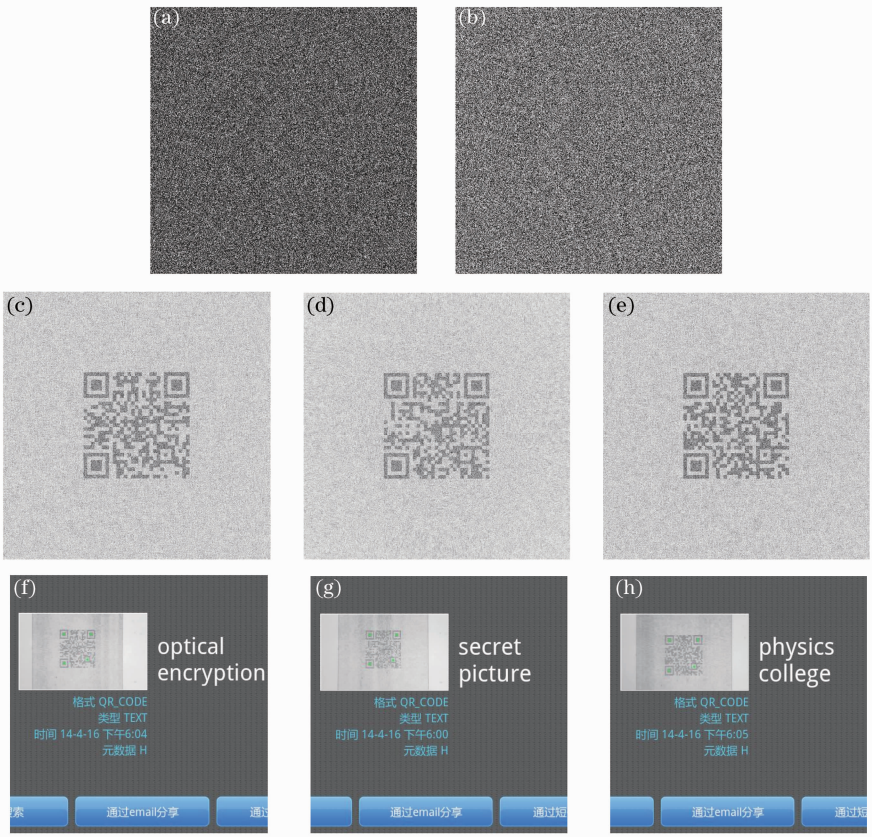

图 8 被规则剪切的相位板。(a) M1；(b) M2；(c)～(e) 解密出来的 QR 码；(f)～(h) 对(c)～(e)扫描结果

Fig. 8 POMs by regularly shearing. (a) M1; (b) M2; (c)～(e) decrypted QR codes; (f)～(h) scan results of (c)～(e)

分别对两个相位板进行加噪处理，图 9(a)、(b)表示两相位板分别受噪声密度为 0.02 的椒盐噪声攻击之后的结果，用图 1 所示的解密系统对被椒盐噪声攻击后的相位板进行解密，解密出来的 QR 码在图 9(c)～(e)中给出。对解密的 QR 码再用智能设备进行扫描恢复，识别结果在图 9(f)～(h)给出。

可见，在噪声密度为 0.02 的噪声攻击下，本方法可以完全恢复原始信息。经过进一步测试，发现本方法中密文所容忍的椒盐噪声的参数可以达到 0.05，所提方法对椒盐噪声的容忍程度较大。

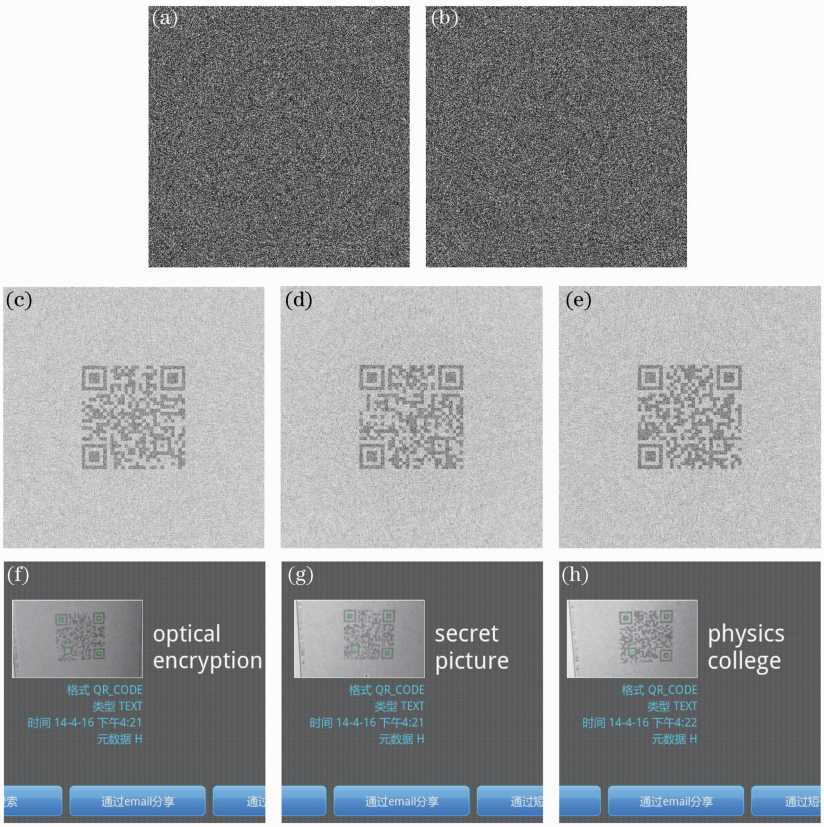

图 9　加噪后的相位板。(a) M1；(b) M2；(c)～(e)解密出来的 QR 码；(f)～(h)对(c)～(e)扫描的结果

Fig. 9　POMs polluted by noise. (a) M1; (b) M2; (c)～(e) corresponding decrypted QR codes; (f)～(h) scan results of (c)～(e)

4　结　　论

提出了一种在多图像加密系统中消除串扰噪声的方法。该方法是在 QR 码的辅助下将多组信息解析地隐藏于两个纯相位板中，过程中无需迭代，非常省时。QR 码可以方便地用软件生成，而其识别可用移动智能设备扫描。由于 QR 码强大的抗噪声能力，相较于原来的基于干涉原理的多图像加密方法，本文提出的方法成功地解决了串扰噪声问题，实现了信息的高质量恢复，并且通过稳健性分析，该加密系统具有一定的抗剪切和噪声攻击的能力。

参　考　文　献

1 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.

2 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.

3 Nanrun Zhou, Yixian Wang, Lihua Gong, *et al*.. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform [J]. Opt Commun, 2011, 284(12): 2789－2796.

4 Qin Yi, Gong Qiong, Li Genquan, *et al*.. An optical encryption method with silhouette removal [J]. Chinese J Lasers, 2012, 39(12): 1209002.
秦　怡，巩　琼，李根全，等. 一种无轮廓像干扰光学加密系统[J]. 中国激光，2012，39(12)：1209002.

5 Bahram Javidi. Securing information with optical technologies [J]. Physics Today, 1997, 50(3): 27－32.

6 Ayman Alfalou, C Brosseau. Optical image compression and encryption methods [J]. Advance in Optics and Photonics, 2009, 1(3): 589－636.

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

8 Bahram Javidi, Esmail Ahouzi. Optical security system with Fourier Plane encoding [J]. Appl Opt, 1998, 37(26): 6247－6255.

9 S Kishk, B Javidi. Information hiding technique with double random phase encoding [J]. Appl Opt, 2002, 41(26): 5462－5470.

10 B Hennelly, J T Sheridan. Optical image encryption by random

shifting in fractional Fourier domains [J]. Opt Lett, 2003, 28 (4): 269－271.
11 P C Mogensen, J Glückstad. Phase-only optical encryption [J]. Opt Lett, 2000, 25(8): 566－568.
12 Guohai Situ, Jingjuan Zhang. Multiple-image encryption by wavelength multiplexing [J]. Opt Lett, 2005, 30(11): 1306－1308.
13 Guohai Situ, Jingjuan Zhang. Position multiplexing for multiple-image encryption [J]. J Opt A, 2006, 8(5): 391－397.
14 Zhengjun Liu, Yan Zhang, Haifa Zhao, *et al*.. Optical multi-image encryption based on frequency shift [J]. Optik, 2011, 122 (5): 1010－1013.
15 Hsuan T Chang, Wei C Lu, Chung J Kuo. Multiple-phase retrieval for optical security systems by use of random-phase encoding [J]. Appl Opt, 2002, 41(23): 4825－4834.
16 Youzhi Li, Kathi Kreske, Joseph Rosen. Security and encryption optical systems based on a correlator with significant output images [J]. Appl Opt, 2000, 39(29): 5295－5301.
17 Yan Zhang, Bo Wang. Optical image encryption based on interference [J]. Opt Lett, 2008, 33(21): 2443－2445.
18 Bo Wang, Yan Zhang. Double images hiding based on optical interference [J]. Opt Commun, 2009, 282(17): 3439－3443.
19 Wen Chen, Xudong Chen. Optical multiple-image encryption based on multiplane phase retrieval and interference [J]. J Opt, 2011, 13(11): 115401.
20 Yi Qin, Qiong Gong. Interference-based multiple-image encryption with silhouette removal by position multiplexing [J]. Appl Opt, 2013, 52(17): 3987－3992.
21 John Fredy Barrera, Alejandro Mira, Roberto Torroba. Optical encryption and QR codes: secure and noise-free information retrieval [J]. Opt Express, 2013, 21(5): 5373－5378.

栏目编辑：何卓铭