基于计算鬼成像的双密钥光学加密方案

曹 非, 赵生妹

南京邮电大学信号处理与传输研究院, 江苏 南京 210003

摘要 提出了一种基于计算鬼成像(CGI)的 Toeplitz 矩阵和轴向距离的双密钥光学加密方案。在该方案中,只需发送一个相位掩模密钥,就可以产生多种不同的随机散斑,大大减少了密钥的传输量;在接收端采用压缩感知技术进行解密。数值仿真和实验结果表明,密钥合法用户能完全恢复物体图像,而窃听者在窃听率即使达到 60%的情况下,也不能获得图像的任何信息。双密钥的使用有效地提高了方案的安全性。

关键词 成像系统; 光学加密; 计算鬼成像; 双密钥; Toeplitz 矩阵; 轴向距离; 压缩感知

中图分类号 O438 **文献标识码** A

doi: 10.3788/AOS201737.0111001

Optical Encryption Scheme with Double Secret Keys Based on Computational Ghost Imaging

Cao Fei, Zhao Shengmei

Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, *China*

Abstract One optical encryption scheme with double secret keys based on the Toeplitz matrix and axial distance in the computational ghost imaging (CGI) is proposed. In this scheme, multiple random speckle patterns can be obtained by the transmission of a single random phase mask in legitimate users. At the receiving terminal, the image is decrypted with compressive sensing technique. The numerical simulation and experimental results indicate that the authorized users can recover the original image completely, but the eavesdroppers cannot obtain any information of the original image even if the eavesdropping rate is up to 60%. The use of double secret keys can effectively improve the security of this scheme.

Key words imaging systems; optical encryption; computational ghost imaging; double secret keys; Toeplitz matrix; axial distance; compressive sensing

OCIS codes 110.1758; 060.4785; 110.3010; 030.6140

1 引 言

光学加密信息处理技术具有并行高速处理的特性,且可以采用光的多种维度加密信息,如相位、波长、空间频率和偏振等[1-4]。同时,光是处理图像的天然介质,随着光电设备的不断进步,光学加密信息处理技术在信息安全和知识产权保护中起到越来越重要的作用。

鬼成像(GI)[5-7]又称为关联成像,是通过光场强度的关联测量来获得物体信息的方法。这种成像技术最早是通过量子的纠缠特性来实现的。然而,现有实验证明,赝热光源也能实现鬼成像[8]。传统鬼成像系统包含两束光路,一束通过待测物体,被无空间分辨率的点探测器(桶探测器)接收,称为信号光路;另一束被具有空间分辨率的探测器接收,如电荷耦合元件(CCD),称为参考光路。通过对两路光场强度的复合测量,可

收稿日期: 2016-07-15; **收到修改稿日期**: 2016-08-05

基金项目: 国家自然科学基金(61271238,61475075)、南京邮电大学宽带无线通信与传感网技术教育部重点实验室开放研究基金(NYKL2015011)

作者简介: 曹 非(1979—),男,博士研究生,主要从事关联成像方面的研究。E-mail: njustsword@163.com

导师简介: 赵生妹(1968—),女,博士,教授,主要从事量子信息技术和无线通信与信号处理技术方面的研究。E-mail: zhaosm@njupt.edu.cn(通信联系人)

在没有物体的参考光路中获取物体的像。由于热光鬼成像实现简单，对实验设备要求较低，近年来国内对热光鬼成像进行了很多研究，并提出了各种热光鬼成像方案[9-13]。

2008 年，Erkmen 等[14]提出了一种计算鬼成像(CGI)方案，可通过离线计算方式获取参考光路的光场强度。CGI 的出现使得应用 GI 进行光学加密成为可能。2009 年，Bromberg 等[15]进一步提出了单探测光路的鬼成像方案，其中旋转的毛玻璃由受计算机控制的空间光调制器(SLM)替代。2010 年，Clemente 等[16]提出了基于 CGI 的光学加密方案，简称 CGI-OE 方案。2012 年，Tanha 等[17]提出了基于 CGI 的灰色和彩色光学加密的方案来提高安全性。2014 年，Zafari 等[18]提出了基于选择性 CGI 提高光学加密的方案。2015 年，Zhao 等[19]提出了基于 CGI 的使用快速反应(QR)编码和压缩感知技术的高性能光学加密方案。2016 年，Wu 等[20]提出了基于 CGI 的使用位置复用的多图像加密方案。2016 年，Yuan 等[21]提出了通过调节可逆矩阵来降低 CGI 图像加密被攻击的风险的加密方案。

CGI-OE 通过 SLM 产生[0，2π]区间内随机分布的相位掩模，将其作为密钥经过秘密通道发送给合法用户，具有较大的密钥量和较长的密钥传输时间。Toeplitz 矩阵的任意一行可以通过第一行循环移位获得。若是将某一个随机相位掩模作为 Toeplitz 矩阵的第一行，其循环移位也是随机相位掩模。因此，在以一系列随机相位掩模为密钥的 CGI-OE 方案中，如果采用 Toeplitz 矩阵，只需发送一个相位掩模作为密钥，其他相位密钥可通过该密钥循环移位获得，大大降低了密钥传输量。为了进一步提高光学加密方案的安全性，根据计算关联成像的特点，同时引入了物体到 SLM 之间的距离作为另一密钥。

本文提出一种基于计算鬼成像的双密钥光学加密方案，简称 TD-CCGI-OE 方案。该方案将一个随机相位掩模和物体到 SLM 的轴向距离作为光学加密的双密钥，其中相位密钥是该相位掩模循环移位后得到的随机分布的 Toeplitz 矩阵，而距离密钥是随机分布的轴向距离。只有在两个密钥都已知的条件下才能完全恢复物体图像。解密过程应用了压缩感知(CS)技术。通过数值仿真和实验测量两种手段验证了方案的有效性和安全性。

2　基于 CGI 的 Toeplitz 矩阵和轴向距离的双密钥加密方案

基于 CGI 的随机相位掩模和轴向距离的光学加密方案如图 1 所示。Alice 和 Bob 分别是合法的发送者和接收者。Alice 通过计算机控制 SLM，利用空间相干单色激光束产生了不同的相位掩模，其变化量 $\varphi_i(x,y)$ 在[0，2π]区间内随机分布；传播轴向距离 z_i 后，到达物体面的散斑光场强度为 $I_i(x,y,z_i)$，再通过透射函数为 $T(x,y)$ 的物体，被桶探测器接收的光场强度值为 B_i。假设采样次数为 M，第一次通过 SLM 在光束上附加一个随机的空间相位掩模 $\varphi_1(x,y)$，按行将其拉长为一行，然后每次行元素循环右移一位作为新的相位掩模 $\varphi_i(x,y)(i=2,\cdots,M)$，这些相位掩模形成了具有随机分布的 Toeplitz 矩阵。而轴向距离每次选取随机的 z_i，得到对应的 M 个桶测量值 $B_i(i=1,\cdots,M)$。在发送端，Alice 将相位掩模 $\varphi_1(x,y)$ 和 M 个距离 z_i 作为密钥，通过秘密通道发送给合法用户 Bob，$B_i(i=1,\cdots,M)$ 则通过公共通道发送给 Bob。Bob 根据相位掩模 $\varphi_1(x,y)$ 和距离 $z_i(i=1,\cdots,M)$ 密钥计算出 $I_i(x,y,z_i)(i=1,\cdots,M)$，将测量值 $B_i(i=1,\cdots,M)$ 和计算值 $I_i(x,y,z_i)(i=1,\cdots,M)$ 作为 CS 算法的测量向量和测量矩阵，基于 CS 算法重建物体图像，完成解密。双密钥的使用，有效地增加了密钥的安全性。根据香农信息安全理论，双密钥将极大地提升加密方案的安全性。

假设波长为 λ 的激光照射到 SLM 上的光场为 $E^{(\mathrm{in})}$，经过 SLM 相位调制 $\varphi_i(x,y)(i=1,\cdots,M)$ 后，光场 $E_i(x,y,z=0)=E^{(\mathrm{in})}\exp[\mathrm{j}\varphi_i(x,y)]$，根据 Fresnel-Huygens 传播方程，距离 SLM 为 $z=z_i$ 处的物平面光场为[15]

$$E_i(x,y,z_i)=\frac{\exp(\mathrm{j}\lambda z_i)}{\mathrm{j}\lambda z_i}\iint \mathrm{d}\xi\mathrm{d}\eta E_i(x-\xi,y-\eta,0)\exp\{[\mathrm{j}\pi/(\lambda z_i)](\xi^2+\eta^2)\},\tag{1}$$

式中 ξ,η 表示垂直于 z 的平面空间坐标。散斑到达物平面的光场强度为

$$I_i(x,y,z_i)=|E_i(x,y,z_i)|^2,\tag{2}$$

通过透射函数为 $T(x,y)$ 的物体后，被桶探测器接收的光场强度为

$$B_i=\iint \mathrm{d}x\,\mathrm{d}y I_i(x,y,z_i)T(x,y),\tag{3}$$

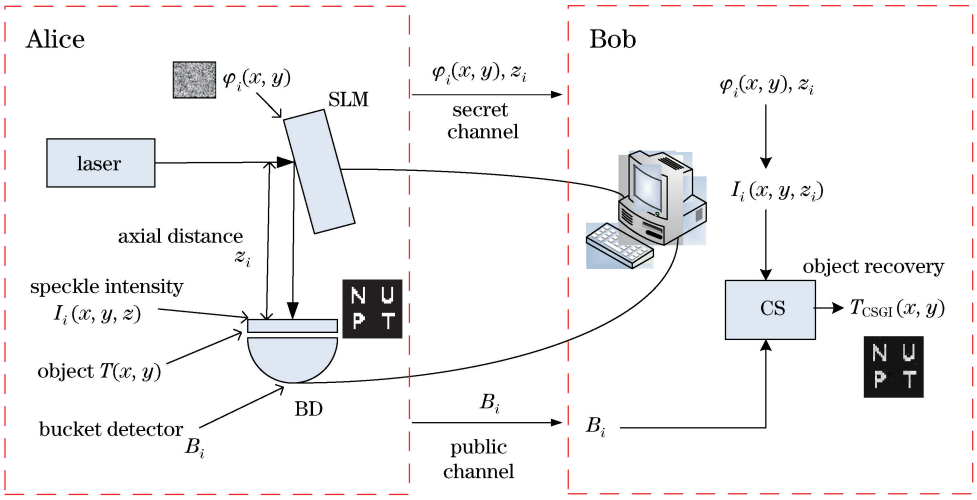

图 1　基于 CGI 的随机相位掩模和轴向距离的光学加密方案示意图

Fig. 1　Schematic diagram of optical encryption scheme based on random phase mask and axial distance in CGI

距离变化的光场强度关联函数为

$$R_{GI}(x,y,z_i)=\frac{1}{M}\sum_{i=1}^{M}(B_i-\langle B\rangle)I_i(x,y,z_i)=\langle BI(x,y,z_i)\rangle-\langle B\rangle\langle I(x,y,z_i)\rangle,\tag{4}$$

式中 $R_{GI}(x,y,z_i)$ 为两光路的光场强度关联后恢复的物体图像信息，是 M 次测量的平均值。由(1)式和(2)式可知，散斑光场强度 $I_i(x,y,z_i)$ 不但和相位掩模 $\varphi_i(x,y)$ 有关，而且和物平面到 SLM 的轴向距离 z_i 有关。根据(3)式，桶探测值 B_i 可看作 $T(x,y)$ 在散斑强度 $I_i(x,y,z_i)$ 上的投影值之和。由(4)式可知，物体图像的恢复取决于 $I_i(x,y,z_i)$ 和强度涨落 B_i-$\langle B\rangle$ 的线性重叠。因此，散斑到达物体前的光场强度 $I_i(x,y,z_i)$ 的选择和包含物体信息的 B_i 是重建物体图像的关键。

假设激光照射到 SLM 上产生的散斑大小和物体大小相同，二维物体的大小是 $N\times N$ 个像素点，经过 M 次采样，(3)式的矩阵形式为

$$\boldsymbol{B}=\begin{pmatrix}B_1\\B_2\\\vdots\\B_M\end{pmatrix}=\begin{pmatrix}I_{11}^{1}&\cdots&I_{1N}^{1}&\cdots&I_{NN}^{1}\\I_{11}^{2}&\cdots&I_{1N}^{2}&\cdots&I_{NN}^{2}\\\vdots&&\vdots&&\vdots\\I_{11}^{M}&\cdots&I_{1N}^{M}&\cdots&I_{NN}^{M}\end{pmatrix}\begin{pmatrix}T_{11}\\\vdots\\T_{1N}\\\vdots\\T_{NN}\end{pmatrix}=\boldsymbol{IT},\tag{5}$$

式中 $(T_{11}\cdots T_{1N}\cdots T_{NN})^{\mathrm{T}}$ 为二维透射函数 $T(x,y)(x,y=1,\cdots,N)$ 在不同像素点处形成的二维向量按行拉长的一列，$I_{ij}^{k}(i,j=1,\cdots,N,\ k=1,\cdots,M)$ 为第 k 次测量照射到物体上的各像素点的散斑光场强度，B_k 是第 k 次测量值。

大多数自然物体的图像经过离散余弦变换(DCT)或者离散小波变换(DWT)等特定变换后具有稀疏性，且散斑强度和稀疏变换满足约束等距特性准则(RIP)。因此(5)式中 $\boldsymbol{B}$ 和 $\boldsymbol{I}$ 可作为 CS 算法的测量向量和测量矩阵，由恢复图像(4)式可以重建物体图像：

$$T_{CS}=T(x,y):\ \mathrm{argmin}\ \|\psi[T(x,y)]\|_{l_1},\tag{6}$$

$$\text{s.t.}\quad B_i=\iint\mathrm{d}x\,\mathrm{d}y I_i(x,y,z=L_i)T(x,y),\ i=1,\cdots,M,\tag{7}$$

式中 $\|\cdot\|_{l_1}$ 表示 l-范数，ψ 为稀疏基，T_{CS} 为 CS 重建的恢复图像。

Toeplitz 矩阵的每一个行向量是由前一个行向量的各元素依次循环右移一个位置得到的，因此可以通过任意一行元素的循环移位获得该矩阵，如图 2 所示。假设图 2(a)所示的相位掩模 $\varphi_i(x,y)$ 是一个 3×3 随机相位矩阵，将其按行拉长为一行，如图 2(b)所示；通过循环移位，可以获得不同的随机相位掩模，如图 2(c)所示；循环一个周期即 8 次循环后，形成散斑的 Toeplitz 相位矩阵，如图 2(d)所示。

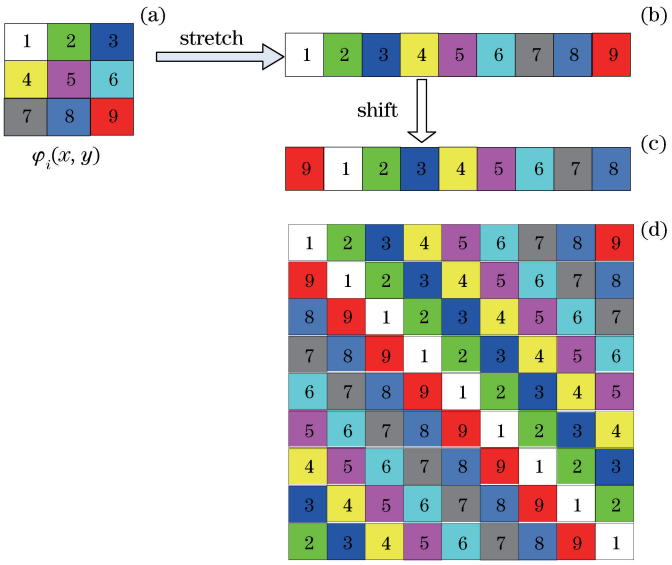

图 2　散斑相位 Toeplitz 矩阵的形成

Fig. 2　Construction of Toeplitz matrix with speckle phase

文献[22-23]证明 Toeplitz 结构的随机测量矩阵可作为 CS 的测量矩阵，满足约束等距性质；在同等条件下，基于 Toeplitz 随机测量矩阵的恢复结果优于随机高斯测量矩阵[24]。

3　数值仿真和实验结果

现通过数值仿真和实验进行分析，在密钥完全已知的条件下验证提出的 TD-CCGI-OE 方案的可行性，在密钥窃取率不同的条件下验证该方案受到攻击时的安全性。

数值仿真使用的散斑图由波长 $\lambda=633$ nm、束腰半径 $w_0=0.1$ mm 的高斯激光衍射得到，目标物体的大小为 32 pixel×32 pixel。相位掩模密钥 $\varphi_1(x,y)$ 是在[0,2π]区间内随机产生的，其他随机相位掩模通过其循环移位获得。物体到 SLM 的轴向距离密钥是随机分布的，使用 0.5 m 和 1 m 两种距离。重建图像的 CS 算法为正交匹配追踪(OMP)算法，对于非稀疏信号，先采用 DCT 作为稀疏变换，再用 OMP。

实验结构如图 3 所示，使用波长为 633 nm 的 He-Ne 激光器，发出空间相干的单色激光束，照到空间光调制器 SLM 上。SLM 由计算机控制，通过 LabVIEW 软件使散斑相位改变 $\varphi_i(x,y)$，相位掩模 $\varphi_i(x,y)(i=1,\cdots,M)$ 是 Toeplitz 矩阵，只需存储一个相位掩模。再经过随机轴向距离 z_i 传输(z_i 取 0.5 m 和 1 m 两个值)，光束照射到 NUPT、Lena 透明塑料卡片上。然后通过焦距 $f=250$ mm 的透镜聚焦，由功率探测器接收；利用一个光电二极管传感器将其转换为电信号，这个信号记作 B_i，经过 M 次测量，获得 M 个桶探测器值 $B_i(i=1,\cdots,M)$。发送者将 $\varphi_1(x,y)$ 和 z_i 作为密钥、$B_i(i=1,\cdots,M)$ 作为加密结果发送给合法用户，该接收者根据相位掩模和距离密钥，由菲涅耳衍射公式计算出散斑到达物平面的光场强度 $I_i(x,y,z_i)$；将 $B_i(i=1,\cdots,M)$ 和 $I_i(x,y,z_i)(i=1,\cdots,M)$ 作为测量向量和测量矩阵，通过 CS 算法恢复物体图像。实验中为了测量方便，在同一初始相位掩模条件下，分别测量轴向距离为 0.5 m 和 1 m 的桶探测器值 $B_i(i=1,\cdots,M)$，然后按照距离的随机分布选取相对应的 B_i。

为了更直观地说明成像质量，引入均方误差(E_{MS})和峰值信噪比(R_{PSN})两个参数来评估恢复的图像质量，其定义分别为

$$E_{\mathrm{MS}}=\frac{1}{M\times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[R(x,y)-S(x,y)]^2, \tag{8}$$

$$R_{\mathrm{PSN}}=10\lg\frac{[\max(V)]^2}{E_{\mathrm{MS}}}, \tag{9}$$

式中 $R(x,y)$ 和 $S(x,y)$ 分别表示原始图像和恢复图像在位置 (x,y) 上的强度值，图像大小为 $M\times N$，$\max(V)$ 为图像最大的像素值。E_{MS} 越小，R_{PSN} 越大，图像的失真越小，恢复质量越好。

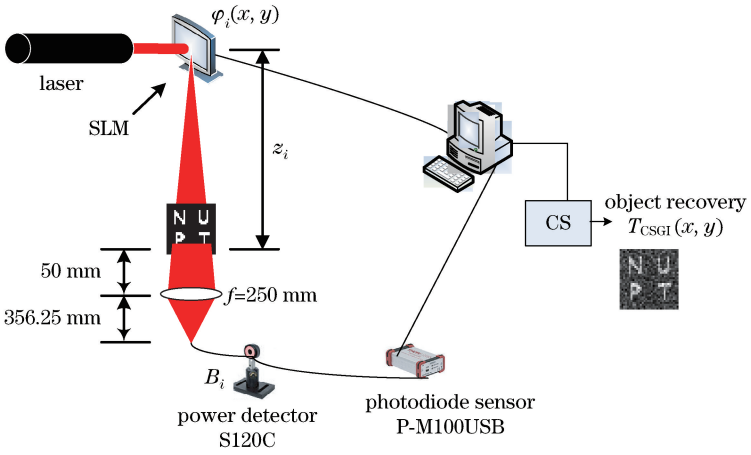

图 3　实验结构示意图

Fig. 3　Schematic diagram of experimental setup

首先验证 TD-CCGI-OE 方案的有效性。物体为二灰度的 NUPT 图和八灰度的 Lena 图。为了对比结果，同时采用 T-CCGI-OE 方案（仅包含单 SLM 的随机相位密钥）、CGI-OE 方案（解密算法为二阶关联）和 CCGI-OE 方案（解密算法为 CS 重建），结果如图 4 所示。仿真物体的大小为 32 pixel×32 pixel，实验物体的大小均为 18 mm×18 mm。NUPT 图仿真采样 450 次，采样率约为 44%，实验采样 650 次。Lena 图仿真采样 600 次，实验采样 800 次，CS 算法中使用 DCT 作稀疏变换。

仿真中一个像素点用 4 个字节表示，传输一帧 $N\times N$ 的物体需要 $4\times N\times N$ 个字节，采样 M 次，CGI-OE 的密钥量是 $4\times N\times N\times M$ 个字节，TD-CCGI-OE 需要传输 $4\times N\times N$（相位密钥）加上 $4M$（距离密钥）个字节，密钥量约为 CGI-OE 的 $1/M$。本文仿真采样 600 次，密钥量约为 CGI-OE 的 0.2%，可见 TD-CCGI-OE 方案的密钥传输量大大降低。由图 4 可知，无论是二灰度还是多灰度物体，无论是仿真还是实验，TD-CCGI-OE 方案在相位和轴向距离双密钥都已知的条件下，使用 CS 算法解密能使物体图像恢复。因为实验中存在噪声和测量误差，所以重构图像质量比仿真结果差。T-CCGI-OE 方案与本文提出的双密钥 TD-CCGI-OE 方案恢复效果基本一致；相对于 CGI-OE 方案及 CCGI-OE 方案，在采样次数相同的条件下，前两者的 R_{PSN} 值高于后两者，图像的恢复质量明显提高。

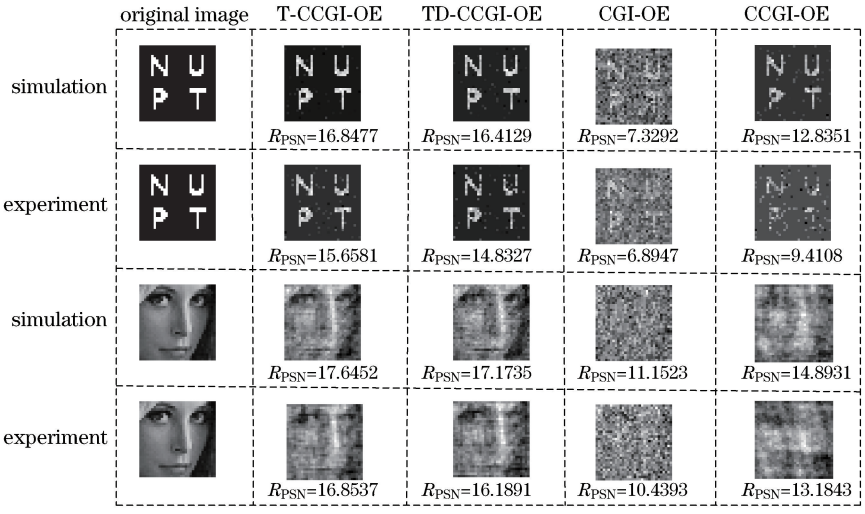

图 4　物体解密的仿真和实验结果

Fig. 4　Simulation and experimental results of object decryption

下面讨论受到攻击、密钥被窃取时 TD-CCGI-OE 方案的安全性。非法用户窃取不同比例的密钥，在恢复机制完全已知的条件下，分别采用 CGI-OE 方案、T-CCGI-OE 方案和 TD-CCGI-OE 方案，NUPT 图信息泄露的仿真和实验结果如图 5 所示。仿真采样次数为 900 次，实验采样次数为 1100 次，图上方标注的是窃

听率，下方是对应的 R_{PSN} 值。CGI-OE 方案采用随机相位作为密钥，解密算法是光场强度的二阶关联，其窃听率是指窃听的相位密钥和总密钥的比值；TD-CCGI-OE 方案采用 Toeplitz 矩阵和轴向距离的双密钥，解密算法是 CS 算法，其窃听率是指相位和距离密钥与对应总密钥的比值。三种方案在不同的窃听率下，对应的 R_{PSN} 值曲线图如图 6，7 所示。

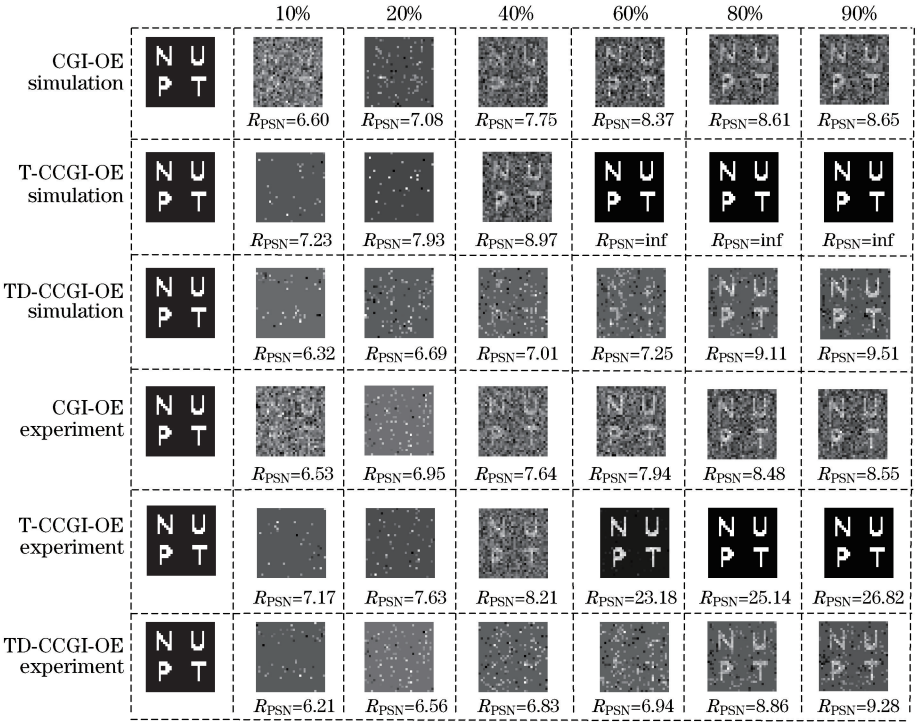

图 5　不同窃听率下的仿真和实验结果

Fig. 5　Simulation and experimental results under different eavesdropping rates

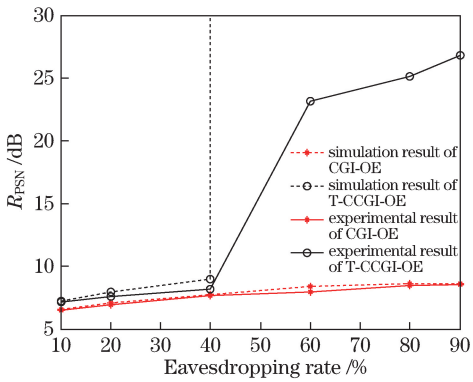

图 6　CGI-OE 方案和 T-CCGI-OE 方案中，峰值信噪比随窃听率的变化

Fig. 6　Variations of R_{PSN} with eavesdropping rate in CGI-OE and T-CCGI-OE schemes

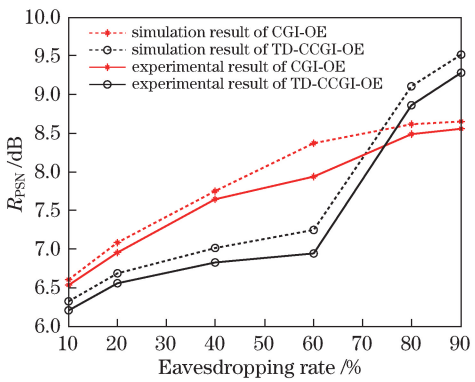

图 7　CGI-OE 方案和 TD-CCGI-OE 方案中，峰值信噪比随窃听率的变化

Fig. 7　Variations of R_{PSN} with eavesdropping rate in CGI-OE and TD-CCGI-OE schemes

由图 5 可知，在这三种方案的仿真和实验结果中，窃听率越大，R_{PSN} 值越大，图像信息泄露越多，重建效果越好。这是因为随着窃听率的提高，获得的密钥量增加，窃听者通过计算获得了更多正确的光强 $I_i(x,y,z_i)$，从而更准确地恢复物体图像。仿真中，CGI-OE 方案在窃听率为 40%时可以获得图像的模糊轮廓；T-CCGI-OE 方案在窃听率为 40%时获得了比较清楚的图像，60%时图像已经非常清晰，这说明采用 Toeplitz 矩阵代替随机阵作相位密钥，T-CCGI-OE 方案的安全性相对于 CGI-OE 方案有所下降；而使用双密钥的 TD-CCGI-OE 方案在窃听率为 60%时无法获得图像的信息，在 80%才能获得比较清晰的图像，安全性较高。

由图 6 可知，T-CCGI-OE 方案的 R_{PSN} 值比 CGI-OE 方案大，且在窃听率大于 40%后迅速增大，窃听率为 60%时图像信息基本泄露。由图 7 可知，CGI-OE 方案的 R_{PSN} 曲线随着窃听率的增加呈缓慢近似线性增长；而 TD-CCGI-OE 方案在窃听率为 60%以下时，R_{PSN} 曲线也是缓慢地近似线性增长，但窃听率超过 60%后，R_{PSN} 值迅速增加，上升的幅度远远超过了 CGI-OE 方案。对比两者的 R_{PSN} 曲线，当仿真的窃听率在 72%(实验中 75%)以下时，TD-CCGI-OE 方案的 R_{PSN} 值比 CGI-OE 方案小，即前者的图像恢复效果较差，保密性能较好；但当窃取率大于 72%(实验中 75%)时，TD-CCGI-OE 方案的 R_{PSN} 值反而超出了 CGI-OE 方案，恢复效果较好。这是因为 TD-CCGI-OE 方案在加密中使用了 Toeplitz 矩阵，在解密中使用了 CS 算法，当密钥被大量窃取时，恢复效果越来越接近恢复上限，而这个上限远超 CGI-OE 方案，也就是说窃听率超过一定比例后，TD-CCGI-OE 方案还能大幅提高恢复效果，而 CGI-OE 方案的提升效果有限。所以，在窃听率比较小的情况下(本文是 72%以下)，基于 CGI 方案的相位和距离的双密钥 TD-CCGI-OE 方案与 CGI 方案相比，泄露的图像信息少，恢复效果差，保密性能高。

4　结　论

在原有 CGI-OE 方案的基础上，提出了基于 CGI 方案的双密钥光学加密方案。方案中只需发送一个相位掩模密钥，就可以产生多种不同的随机散斑，大大减少了密钥的传输量。同时引入物体到 SLM 的轴向距离作为另一密钥来有效地提高方案的安全性。在解密过程中，采用 CS 算法有效解决了 CGI-OE 方案采样次数多、图像恢复质量差的问题。数值仿真和实验结果表明，TD-CCGI-OE 方案的密钥传输量和 CGI-OE 方案的密钥传输量的比值约为测量次数的倒数；在双密钥完全已知的条件下，TD-CCGI-OE 方案根据对应的 CS 算法可恢复图像，且恢复效果好于 CGI-OE 方案。在安全性方面，当非法用户的窃听率低于 60%时，TD-CCGI-OE 方案不能重建图像，而 CGI-OE 方案在窃听率为 40%时就能获得图像轮廓；在较低的窃取率下(低于 72%)，TD-CCGI-OE 方案的峰值信噪比低于 CGI-OE 方案的，泄露的图像信息少，保密性能好。

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] Goudail F, Bollaro F, Javidi B, *et al*. Influence of a perturbation in a double phase-encoding system[J]. Journal of the Optical Society of America A, 1998, 15(10): 2629-2638.

[3] Wang B, Sun C C, Su W C. Shift-tolerance property of an optical double-random phase-encoding encryption system[J]. Applied Optics, 2000, 39(26): 4788-4793.

[4] Javidi B, Sergent A, Zhang G, *et al*. Fault tolerance properties of a double phase encoding encryption technique[J]. Optical Engineering, 1997, 36(4): 992-998.

[5] Pittman T B, Shih Y H, Strekalov D V, *et al*. Optical imaging by means of two-photon quantum entanglement[J]. Physical Review A, 1995, 52(5): R3429.

[6] Abouraddy A F, Saleh B E A, Sergienko A V, *et al*. Role of entanglement in two-photon imaging[J]. Physical Review Letters, 2001, 87(12): 123602.

[7] Shapiro J H, Boyd R W. The physics of ghost imaging[J]. Quantum Information Processing, 2012, 11(4): 949-993.

[8] Bennink R S, Bentley S J, Boyd R W. "Two-photon" coincidence imaging with a classical source[J]. Physical Review Letters, 2002, 89(11): 113601.

[9] Chen Mingliang, Li Enrong, Han Shensheng, *et al*. Ghost imaging based on sparse array pseudo thermal light system [J]. Acta Optica Sinica, 2012, 32(5): 0503001.
陈明亮, 李恩荣, 韩申生, 等. 基于稀疏阵赝热光系统的强度关联成像研究[J]. 光学学报, 2012, 32(5): 0503001.

[10] Mei Xiaodong, Gong Wenlin, Han Shensheng, *et al*. Experimental research on prebuilt three-dimensional ghost imaging lidar[J]. Chinese J Lasers, 2016, 43(7): 0710003.
梅笑冬, 龚文林, 韩申生, 等. 可预置激光三维强度关联成像雷达实验研究[J]. 中国激光, 2016, 43(7): 0710003.

[11] Liu Xuefeng, Yao Xuri, Wu Ling'an, *et al*. The role of intensity fluctuations in thermal ghost imaging[J]. Acta Physica Sinica, 2013, 62(18): 184205.
刘雪峰, 姚旭日, 吴令安, 等. 强度涨落在热光鬼成像中的作用[J]. 物理学报, 2013, 62(18): 184205.

[12] Wang Sen, Li Hongguo, Wang Kaige, *et al*. The influence of rotational speed of ground-glass on the quality of ghost imaging with thermal light[J]. Acta Sinica Quantum Optica, 2015, 21(1): 9-13.
王　森, 李洪国, 汪凯戈, 等. 毛玻璃转速对热光鬼成像质量的影响[J]. 量子光学学报, 2015, 21(1): 9-13.

[13] Tang Wenzhe, Cao Zhengwen, Zeng Guihua, *et al*. Back-side correlation imaging with digital micro mirror[J]. Acta Optica Sinica, 2015, 35(5): 0511004.
唐文哲, 曹正文, 曾贵华, 等. 基于数字微镜器件的"后视"关联成像[J]. 光学学报, 2015, 35(5): 0511004.

[14] Erkmen B I, Shapiro J H. Unified theory of ghost imaging with Gaussian-state light[J]. Physical Review A, 2008, 77(4): 043809.

[15] Bromberg Y, Katz O, Silberberg Y. Ghost imaging with a single detector[J]. Physical Review A, 2009, 79(5): 053840.

[16] Clemente P, Durán V, Tajahuerce E, *et al*. Optical encryption based on computational ghost imaging[J]. Optics Letters, 2010, 35(14): 2391-2393.

[17] Tanha M, Kheradmand R, Ahmadi-Kandjani S. Gray-scale and color optical encryption based on computational ghost imaging[J]. Applied Physics Letters, 2012, 101(10): 101108.

[18] Zafari M, Ahmadi-Kandjani S. Optical encryption with selective computational ghost imaging[J]. Journal of Optics, 2014, 16(10): 105405.

[19] Zhao S M, Wang L, Liang W, *et al*. High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique[J]. Optics Communications, 2015, 353: 90-95.

[20] Wu J J, Xie Z W, Liu Z J, *et al*. Multiple-image encryption based on computational ghost imaging[J]. Optics Communications, 2016, 359: 38-43.

[21] Yuan S, Yao J B, Liu X M, *et al*. Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging[J]. Optics Communications, 2016, 365: 180-185.

[22] Rauhut H. Circulant and Toeplitz matrices in compressed sensing[EB/OL]. (2009-02-25)[2016-07-10]. http://arxiv.org/pdf/0902.4394v1.pdf.

[23] Haupt J, Bajwa W U, Raz G, *et al*. Toeplitz compressed sensing matrices with applications to sparse channel estimation[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5862-5875.

[24] Zhan Kejun, Song Jianxin. Performance comparison of commonly used measurement matrix in image compressed sensing[J]. TV Technology, 2014, 38(5): 1-4.
詹可军, 宋建新. 图像压缩感知中常用测量矩阵的性能比较[J]. 电视技术, 2014, 38(5): 1-4.