文章编号:1007－6735(2022)06－0519－13　DOI: 10.13255/j.cnki.jusst.20221007002

关联成像技术在光学信息加密方面的研究现状及展望

康　祎，　任治舟，　张雷洪，　张大伟，　庄松林
（上海理工大学 光学仪器与系统教育部工程研究中心，上海 200093）

摘要：光学信息安全技术因其高速、多维、并行等特点，成为现代加密技术的主要研究内容。而关联成像技术作为一种基于光场高阶关联获取物体信息的主动成像机制，具有结构简单、灵敏性好、抗干扰能力强等特点，同时其数据压缩降维的特性为光学信息安全技术提供了新的思路。基于此，根据应用场景的不同，详细介绍了关联成像技术在图像加密、保密传输、信息隐藏和认证及密钥分发等方面的国内外发展历程和应用现状，分析了关联成像加密方案存在的安全漏洞，讨论实际应用中尚存在的问题，并对关联成像加密方案的未来发展趋势进行了展望。

关键词：图像处理；信息安全；关联成像；光学加密技术
中图分类号：O 436　　**文献标志码：**A

Research progress and prospect for optical information encryption based on ghost imaging technology

KANG Yi,　REN Zhizhou,　ZHANG Leihong,　ZHANG Dawei,　ZHUANG Songlin
(*Engineering Research Center of Optical Instruments and Systems, Ministry of Educaiton, University of Shanghai for Science and Technology, Shanghai 200093, China*)

Abstract: Optical information security technology has become the main research content of modern encryption technology because of its high speed and parallel characteristics. Ghost imaging is an active imaging technique in which information of the object is obtained based on high-order correlation of light fields. It has the characteristics of simple structure, high sensitivity and anti-interference. At the same time, the characteristic of data compression provides new ideas for optical information security technology. In this paper, according to different application scenarios, the development history and application status of ghost imaging technology in image encryption, secrecy transmission, information hiding and authentication, key distribution were introduced. The security vulnerabilities were also analyzed, and the problems that still exist in practical applications were discussed. The future development trend of ghost imaging encryption scheme was prospected.

收稿日期: 2022−10−07
基金项目: 国家自然科学基金资助项目 (62205207)
第一作者: 康　祎（1993−），男，讲师．研究方向：计算成像、光学信息处理．E-mail：ky930827@sina.com
通信作者: 张大伟（1977−），男，教授．研究方向：计算成像、微纳光学．E-mail：dwzhang@usst.edu.cn

Keywords: *image processing*; *information security*; *ghost imaging*; *optical encryption technique*

随着科技的进步，信息交流愈加频繁且快速，但随着“棱镜门”的出现，人们也越来越注重信息的安全。然而，技术的不断更迭导致传统密码学面临越来越严峻的挑战，研究者不断探寻新的领域，以期获得更快更安全的保密方式。此时，光学处理技术因其高速性、并行性、多维度等优势得到广泛关注。20世纪70年代，美国利用光学处理技术实现了身份验证、防伪等[1]。20世纪80年代末期，American Banknote Holographic公司利用全息防伪技术制作Visa和MasterCard信用卡，满足了金融领域对安全性的需求[2]。20世纪90年代，计算机及相关算法的发展，促进了信息交流，同时对信息处理技术提出了更高要求。传统的信息加密技术主要依靠计算机和数字信号处理器来实现，受限于处理速度和成本，光学高速、并行的特点自然而然地成为了研究者们青睐的对象。光学信息安全技术以光作为载体，光的波长短，信息容量大，并且能够在多维度(如幅度、相位、偏振、波长、轨道角动量等)实现信息的隐藏。这些优点充分说明了光学信息安全技术在信息传输和保护方面具有得天独厚的优势[3-4]。

1 关联成像技术

光学安全系统一般由激光器、透镜、分束器、空间调制器及探测器组成。许多研究者使用这些光学设备建立了不同的实验装置，例如基于双随机相位编码的光学图像加密技术，量子密钥分发等[5-6]。而最近，关联成像技术因其成本低、易操作及高阶关联特性受到广泛关注，其独特的成像框架以及将目标图像转化为一维强度信息的机制，也为其在光学信息安全领域的应用提供了依据。

关联成像不同于传统成像技术，主要是利用光场的高阶关联来获得物体的空间和相位分布信息，具体成像过程如图1所示。光源发出的光经过设置的一系列随机空间模式R_i生成赝热光源，分束器将赝热光源分成两路，其中经过物体的一路称之为测试臂，无物体的一路称之为参考臂。在测试臂，赝热光源照射到物体$T(x,y)$上，透射或反射的光被不具有分辨率的桶探测器接收，获得一个桶探测器值A_i。而在参考臂，赝热光源直接照射到具有空间分辨率的探测器上，并记录光场强度分布$I_i(x,y)$。桶探测器值可由式(1)得到。

$$A_i = \int I_i(x,y)T(x,y)\mathrm{d}x\mathrm{d}y \tag{1}$$

由于在测试臂的桶探测器不具有空间分辨率，而参考臂的探测器不包含物体信息，因此，只用单路探测器显然无法获得物像，只有对两路信号进行符合测量才能重构出物体的像$T'(x,y)$，即

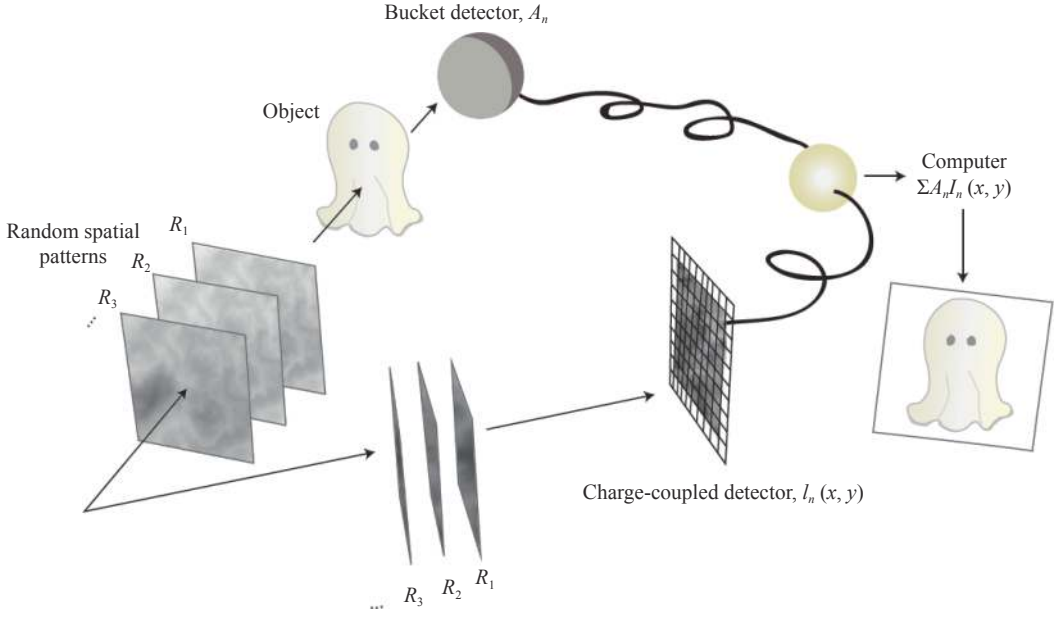


图1 关联成像原理图[7]

Fig.1 Schematic of correlated imaging [7]

$$T'(x,y)=\langle A_i I_i(x,y)\rangle-\langle A_i\rangle\langle I_i(x,y)\rangle \quad (2)$$

式中，〈 〉表示求和平均。

这种成像方式实现了物像分离，是一种非定域的成像方式，故也被称之为鬼成像[7-9]。关联成像概念一经提出就受到广泛关注，研究者们也逐渐利用纠缠光子和赝热光源实现了关联成像。为了简化设备，研究者们利用空间光调制器 (spatial light modulator, SLM) 或者数字微镜器件 (digtial micromirror device, DMD) 自发设计生成不同光场模式，免去了记录光场强度分布的参考臂，实现了仅用单光路成像的计算关联成像[10-12]。

同时，研究者们也逐渐将研究重点从空间域转向时间域，提出了时间关联成像，检测的数据也由图像转化为时变信号[13-14]。考虑到由无分辨率探测器捕获的包含物体的信息仅仅是强度序列，无法直接体现物体信息，2010 年，Clemente 等[15]将关联成像应用到光学图像加密领域，如图 2 所示。在该方案中 Alice 想要把信息加密传输给 Bob，首先在 SLM 中引入一系列随机相位模板$\varphi_i(x,y)$调制光源，然后将生成的光场$I_i(x,y)$照射到目标物体上，反射的光被桶探测器接收，生成一个桶探测值B_i。经过多次照射，将目标明文信息加密为一系列光强度序列，并将其作为密文传输给 Bob。这里密钥S_i由一系列随机相位模板构成。Bob 得到密文后，可以利用从安全信道得到的密钥进行解密，进而得到明文信息。

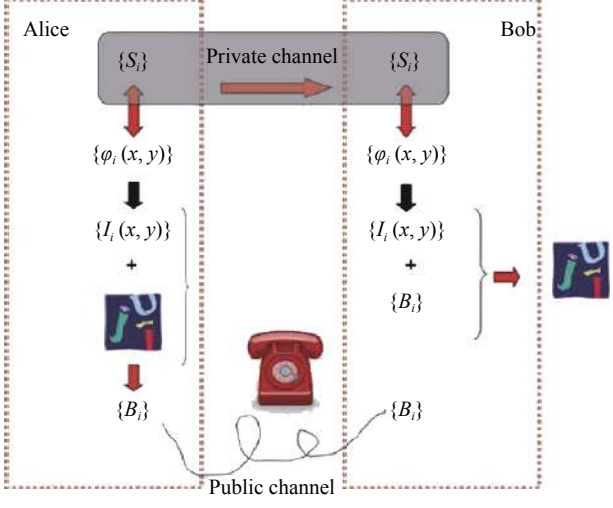


图 2　基于关联成像的图像加密方案[15]

Fig.2　Scheme of the encryption method based on computational correlated imaging [15]

基于关联成像的加密方案无需具有空间分辨率的探测器，简化了系统，同时，密文作为强度序列，更利于传输和存储。另外，随着关联成像技术的发展，基于关联成像的加密方案也向更快、更安全、更便捷、更准确的方向发展。本文将重点介绍基于关联成像的加密方案，包括图像加密、保密传输、信息隐藏等方面的发展现状，在对相关方案进行一定总结的同时，对未来发展趋势作出评估和展望。

2　基于关联成像的光学图像加密技术

图像作为一种信息载体，具有传递信息量大、具体、生动形象等优点，因而对于图像的加密是光学信息安全技术中的重要组成部分。1995 年，Refregier 等[5]利用双相位随机编码 (double random phase encoding，DRPE) 实现了图像的加密。DRPE 因为操作简单、易于实现，且能够与其他手段相结合，推动了光学图像加密技术的快速发展。分数傅里叶变换、菲涅尔变换也和 DRPE 相结合，通过扩大密钥空间，提高了信息的安全性[16-19]。而基于相位截断傅里叶变换的非对称加密系统，也实现了加密系统由对称系统向非对称系统的转变，进一步提高系统的安全性[20]。随后，研究者们利用波长复用、空间复用、位置复用等方法，实现了光学多图像加密[21-25]。但现有的光学图像加密技术，对于仪器的精度要求高，且密文是复振幅，不利于传输和存储，急需一种简单快捷的光学加密方式，而基于关联成像的图像加密技术为解决这个问题提供了新的思路。

基于关联成像的图像加密技术主要分为 3 种：一种是基于关联成像自身特性实现的加密方案，包括改变距离、调制模式等；第二种为关联成像加密方案和其他技术的有机结合，即将明文信息转化到其他数据空间域进而实现加密，包括双相位随机编码、快速响应码等；第三种就是为了提高加密的信息量实现的基于关联成像的多图像加密。

2.1　基于关联成像的图像加密方案

2012 年，在传统关联成像加密方案的基础上，文献 [26-28] 利用关联成像加密方案实现了对于灰度图像和彩色图像的加密，同时也提出可以将虚拟物体加载到 SLM 中实现加密，简化了加密过程，更容易加密不同类型的图像。2013 年，南开大学的孔令军等[29]在基于关联成像加密方案的基础上通过控制光源的初试坐标实现图像的加

密。该方案能够有效防止窃听，大大提高了信息的安全性，实验结果表明，在窃听率低于 50% 时能有效确保信息的安全性。

考虑到调制模式作为加密的密钥，其数据量大影响密钥分发，南京邮电大学的赵生妹课题组[30-31]提出了一种基于计算关联成像的双密钥加密方案，采用 Toeplitz 矩阵作为密钥，其循环移位后的矩阵仍然满足关联成像对于矩阵的需求。因此，采用 Toeplitz 矩阵只需发送一个相位掩模，大大减少了密钥数量，同时将掩模和物体到 SLM 的轴向距离作为密钥，进一步提高了信息的安全性。澳门大学的刘宏超课题组[32]则提出了一种将超表面成像作为关联成像中的掩模图像进行信息加密的结合方式，工作示意图如图 3 所示。该方案利用一个超表面代替了一系列作为密钥的掩模，降低了密钥分发和传输的成本。

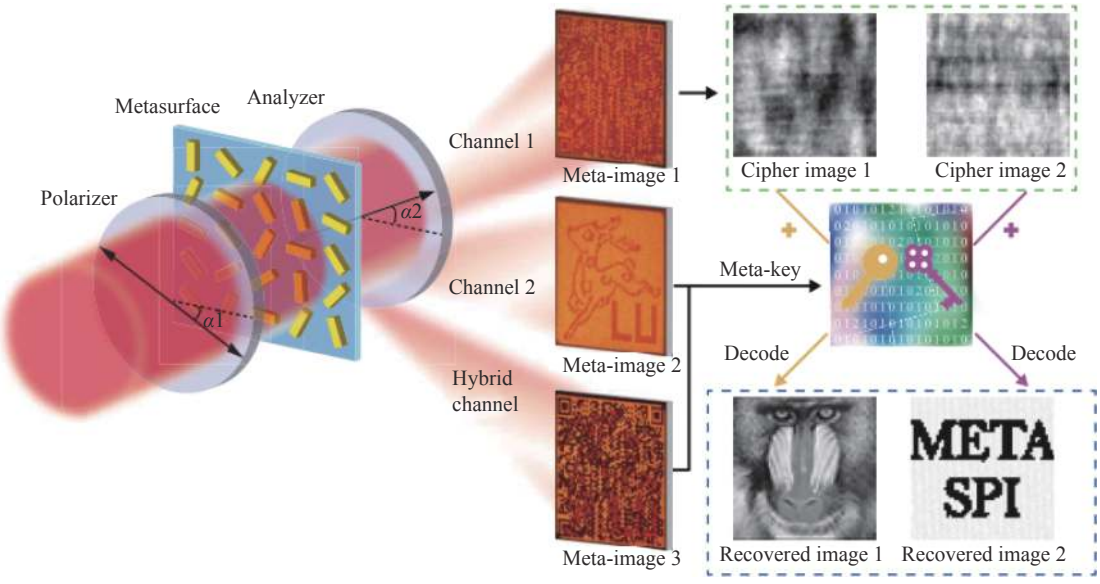


图 3 超表面作为掩模图像重构目标图像的工作示意图[32]

Fig.3 Schematic diagram of metasurface imaging as patterns to reconstruct target images[32]

由于关联成像解密过程相当于统计关联求平均，这就导致了它对密文的误差具有很高的容忍度。虽然提高了系统的鲁棒性，但也给伪造攻击留下了机会，攻击者可以根据截获的密文伪造一组信息并通过某种手段传输给接受者，接受者就可能被解密得到的伪装图像所欺骗和迷惑。基于此，华北水利水电大学的袁胜等[33]及山东大学的孟祥峰等[34]将称为“人体身份证”的指纹和调制模式的构建联合起来，增强了加密系统的安全性。

2.2 关联成像与其他技术联合加密方案

关联成像方案因为实验设备简单，易于与其他技术相结合，因而研究者们在研究基于关联成像自身的加密方案时，也不断引入其他技术，实现更为高效的加密方案，其本质属于将明文或者加密后的信息转移到其他数据空间，从而实现信息的双重防护。

2015 年，南京邮电大学的赵生妹课题组[35]将快速响应码 (quick response code, QR) 技术和计算关联成像加密方案结合起来，利用 QR 码数据密度大、占用空间小、容错率高等特性，提高传输信息的准确性并增强了系统的鲁棒性。实验结果表明，即使密钥被窃取 60%，信息的安全性仍得到保障。

基于关联成像的信息加密技术也是本课题组研究的重点之一。2015 年，我们结合双随机相位编码技术，提出了基于双随机相位编码调制的关联成像加密方案，实现了双重加密[36]，如图 4 所示。次年，我们提出了一种基于分块自适应的关联成像加密方案[37]，以解决高分辨率图像加密效率低的问题。由于关联成像加密方案有一个对称加密方案存在安全隐患，同时作为密钥的相位掩模数量巨大，不利于密钥的管理和分配，为此，我们将公钥密码学原理引入到关联成像加密方案中[38]，使对称加密机制转变为混合加密机制，在解决关联成像加密方案固有缺点的同时提高了信息安全性。

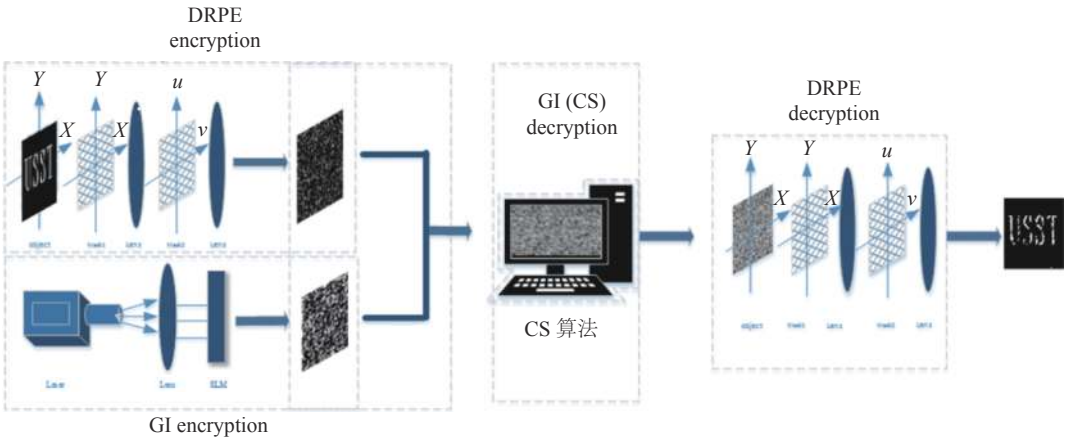


图 4　基于双随机相位编码的关联成像加密方案[36]

Fig.4　Optical encryption scheme based on double random phase encoding and correlated imaging [36]

南阳师范学院的秦怡等[39]及西安工业大学的隋连升等[40]将数据容器和异或操作引入到关联成像加密方案中来。在加密过程中，首先将明文信息转变为二进制信号，并与密钥比特流进行异或操作，然后将其编码到定制的数据容器中，最后使用关联成像加密实现信息的加密。这种方案相比较 QR 码可以实现在更低的采样率下精准重构出明文信息。2018 年，华北水利水电大学的袁胜等[41]将双随机相位编码技术和关联成像加密方案结合起来。这种方法有效解决了关联成像加密方案解密出的图像存在模糊的缺陷，同时两者结合也提高了安全性。2020 年，深圳大学的焦淑铭等[42]在关联成像框架下实现了视觉密码，利用探测器值的叠加代替了空间域的叠加，原理如式 (3) 所示。两个分享图像的信息$O_1(x,y)$和$O_2(x,y)$，分别在同系列照明模式$I_n(x,y)$照射下得到的桶探测器值的和为A_n，类似于将两个分享图像叠加后用$I_n(x,y)$照射得到的桶探测器值。

$$A_n=\int O_1(x,y)I_n(x,y)\mathrm{d}x\mathrm{d}y+\int O_2(x,y)I_n(x,y)\mathrm{d}x\mathrm{d}y=\int[O_1(x,y)+O_2(x,y)]I_n(x,y)\mathrm{d}x\mathrm{d}y \tag{3}$$

2.3　关联成像多图像加密方案

为进一步提高加密数据量，2016 年，哈尔滨工业大学的吴晶晶等[43]首先利用位置复用的办法，将每个图像放置在不同的位置，然后利用关联算法进行加密，最后将获得的每个图像强度序列叠加起来构成密文，随机相位序列和距离参数作为密钥，实现了基于关联成像的多图像加密。

同年，山东大学的孟祥峰课题组[44-47]也开展了对于多图像加密的研究，结合多种方法在提高安全性的同时优化密钥数据量大的问题。在基于关联成像和坐标采样的多图像加密方案中，采用 Logistic 映射算法生成随机相位掩模，解决了密钥数据量大的问题。2017 年，他们将行扫描、(*t*, *n*) 门限密钥分享和菲涅尔域相位回复算法引入到关联成像多图像加密方案中来。多个算法的有效结合在减少密钥冗余度的同时，解决了密钥分配和管理的问题。2018 年，他们首先利用提升小波变换和异或操作实现了多图像的加密，具体过程如图 5 所示。

2017 年，安徽光机所的时东锋等[48]利用多路复用的方式，通过设计不同且互补的编码矩阵，然后以与 Hadamard 模式的积作为照明模式照射多个物体，从而实现了多图像的加密。2018 年，本课题组[49-51]结合傅里叶变换，提出了基于傅里叶变换的关联成像多图像加密方案。2019 年，我们结合公钥密码学原理，采用多路复用的 Hadamard 模式照明加密多图像，并将桶探测值运用公钥密码学再进行加密，实现了双重加密，同时 Hadamard 照明模式的采用在一定程度上解决了图像串扰问题。

3　基于关联成像的时变信号加密技术

时变信号相比较图像，在时间上具有变化性，并在各个领域广泛存在，尤其在通信行业极为普遍。传统时变信号加密方案，通常和数字加密技术相结合，尤其是对称密码和非对称密码的应用，大大提高了信息的安全性[52-55]。但现有密码技术大多基于特定数学问题的计算复杂性，它的保密特征更多地是体现在攻击者的计算力无法实现破解，或者是破解的花费远大于信息的价值，

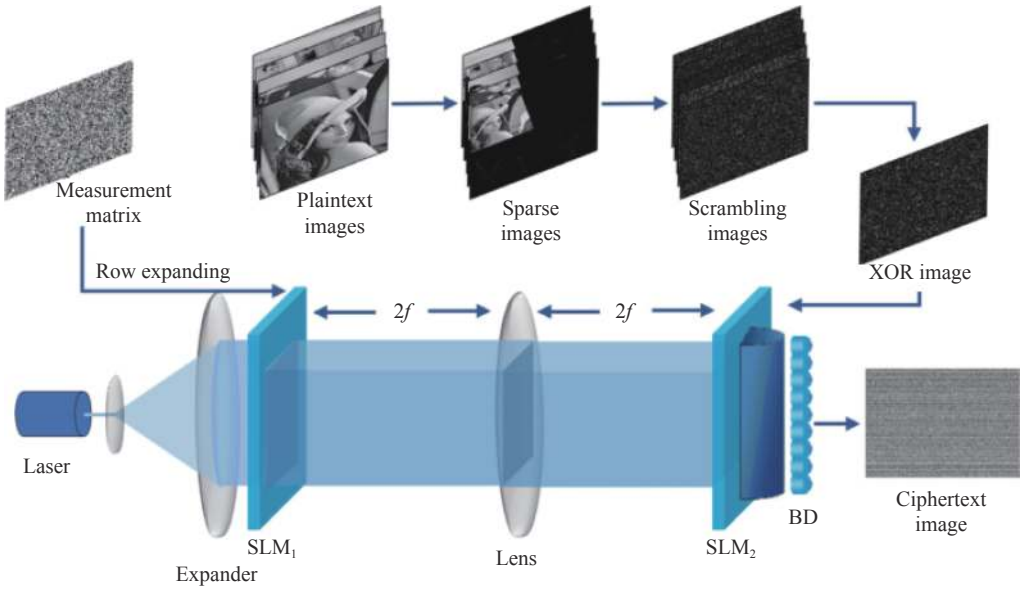


图 5 基于提升小波变换和异或操作的关联成像多图像加密方案[46]

Fig.5 A schematic diagram of the via lifting wavelet transform and XOR operation based on compressive correlated imaging scheme [46]

但从理论上并不能保证信息是绝对安全的。而在算力逐渐提高的今天，尤其是量子计算机的出现，基于计算的保密信号也不再安全。而通过内在物理特性从而实现加密的方式也就越来越受到研究者的重视。光学在维度和速度方面和时变信号相匹配，并且光学多种变换模式为实现时变信号加密提供了可能。混沌光通信和量子密钥分发等技术都是利用光学手段实现了时变信号的加密乃至传输[56-58]。

现有的光学信号加密传输技术在信道中易受吸收、散射、湍流以及噪声影响，因此，急需一种具有较强鲁棒性和安全性的加密方法，而时间关联成像的出现为解决这些问题提供了新的思路。时间关联成像是关联成像在时间域上的扩展，现有研究已经实现了皮秒量级的时间信号检测[59]。同时，时间关联成像的特性大大降低了对检测器带宽的要求，已经实现 1 kHz 带宽的探测器对时间尺度为 50 ns 的时间信号进行检测[60]。空间关联成像在光学图像加密领域的应用及其非定域性也为加密时变信号提供了新的思路。

2017 年，本课题组根据混沌光的二阶时间关联性，将混沌光引入时间关联成像中，结合混沌光的保密特性和时间关联成像的优势，提出了一种基于混沌光的时间关联成像时变信号加密方案[61-62]，方案如图 6 所示。而湖南大学的白艳峰课题组[63]也利用基于混沌光的时间关联成像方案实现了对于图像的安全传输。

可见光通信以其大带宽、抗电磁干扰能力强、集照明与通信与一体的优势受到广泛关注，但作为一种无线传输模式，天然的开放性和广播性极易受到外界威胁。山东大学的孙宝清课题组[64]将时间关联成像应用到可见光通信中，以远高于 micro-LED 运行速度的 4 GB 来传输信号，从而使发射信号变得随机且完全无法识别，从物理

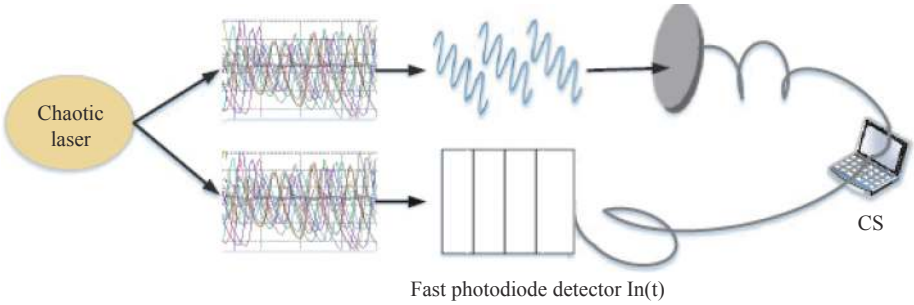


图 6 基于混沌光的时间关联成像加密方案[62]

Fig.6 Scheme of the method based on compressive temporal correlated imaging with chaotic laser [62]

层面以不可逆的方式实现了信息的保密传输，兼顾了速率和安全的并行。

考虑到时间关联成像加密方案需要进行大量采样且误码率较高的问题，同时时间关联成像对于时变信号的加密和保密通信有极大相关性，本课题组将通信编码技术应用到时间关联成像加密方案中来，利用低密度奇偶检验码和码分多址实现了大容量的、抗干扰能力强的保密传输[65-66]。

传统的时间关联成像利用两路光的位置–位置或动量–动量关联特性实现，但当光沿着单模光纤传输时，这些特性无法保持，导致很难实现长距离的加密传输。黄翊东课题组[67-68]注意到光束的频谱特性在光纤长距离传输中易于保持，因此提出并验证了基于频率关联的光纤长距离传输量子时域关联成像，并把这种方法与量子密钥分发的安全检测机制相结合，提出了一种可通过光纤长距离传输的量子安全关联成像方案。方案如图 7 所示。

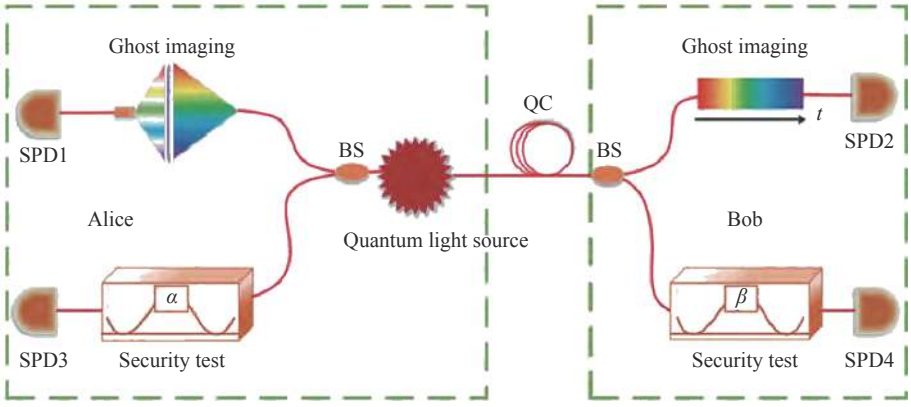


图 7　量子安全鬼成像示意图[67]

Fig.7　Illustration of quantum secure ghost imaging[67]

4　基于关联成像的信息安全技术

4.1　关联成像加密方案的破解方法

对于任何加密系统，安全性的强弱都是一个至关重要的问题，攻击方法也是验证系统安全性的工具。同时，针对攻击方法所暴露出的缺陷，也可以有针对性地改善系统，类似于矛与盾的关系，加密方法和攻击方案相互促进，最终生成更安全的系统。而关联成像加密方案作为一个对称加密系统，密钥的丢失将会直接威胁信息的安全性。而作为密钥的照明模式，数据量是巨大的，不利于密钥的保存和分发。

2015 年，袁胜等[69]通过分析发现，基于关联成像的信息安全技术，本质上一种线性加密方案，容易受到选择明文攻击，只要选择足够多的明文，就可以通过求解线性方程来破解得到密钥，进而获得被加密的信息。2019 年，焦述铭等[70]也提出了一种选择明文攻击方案。在对关联成像加密方案分析后，探测器得到的桶探测器值为照明模式和目标图像在数学上的内积。假设明文图像$\boldsymbol{T}$的像素点为N，经过不同照明模式$I_1(x,y)$采样M次得到密文$\boldsymbol{A}$，那么关联成像加密方案的过程就可以用模型 (4) 表示，这里将明文图像拉伸成了一列。

$$\begin{bmatrix} A(1) \\ A(2) \\ \vdots \\ A(M) \end{bmatrix} = \begin{bmatrix} I_1(1,1) & \cdots & I_1(1,N) \\ \vdots & & \vdots \\ I_M(M,1) & \cdots & I_M(M,N) \end{bmatrix} \begin{bmatrix} T(1) \\ T(2) \\ \vdots \\ T(N) \end{bmatrix} \tag{4}$$

而恢复图像的过程就是求解一个线性方程组并找到最优解的过程。基于此，他们提出了一种选择明文攻击方案。假设攻击者得到Q对不同明文$\boldsymbol{T}$和在固定照明模式$I_m(x,y)$下获得的密文$\boldsymbol{A}$，那么它们将满足以下关系：

$$\begin{bmatrix} T_1(1) & T_1(2) & \cdots & T_1(N) \\ T_2(1) & T_2(2) & \cdots & T_1(N) \\ \vdots & \vdots & & \vdots \\ T_Q(1) & T_Q(2) & \cdots & T_Q(N) \end{bmatrix} \begin{bmatrix} I_m(1) \\ I_m(2) \\ \vdots \\ I_m(N) \end{bmatrix} = \begin{bmatrix} A_1(1) \\ A_2(2) \\ \vdots \\ A_Q(N) \end{bmatrix} \tag{5}$$

式中：$\boldsymbol{T}$的每一行可以视作不同的照明模式；$I_m(x,y)$可以视为物体图像；$\boldsymbol{A}$为不同照明模式下获得的密文。如此，可以通过求解线性方程组得到真实的照明模式，也就破解得到了密钥。

此外，基于关联成像的重构过程本质是统计关联求平均的过程，研究者发现使用二值化的密文依然可以恢复原始明文信息。基于此缺陷，研

究者提出了一种伪造攻击方法[71]。如图 8 所示，Alice 利用一系列照明模式$R_{\text{key}}^{(t)}(x,y)$加密明文信息，并将得到的密文$C(i)$传输给 Bob。攻击者 Mallory 截获传输中的密文$C(i)$，并利用大量的随机照明模式加密伪造图像，以期得到的探测器值和密文$C(i)$接近一致。当一系列照明模式和伪造图像的桶探测器值的二值化结果与捕获密文的二值化结果相同时，可以将此时的照明模式$F_{\text{key}}^{(t)}(x,y)$作为伪造密钥传输给 Bob，Bob 就可能因为使用虚假密钥解密出伪造的明文信息而被欺骗。

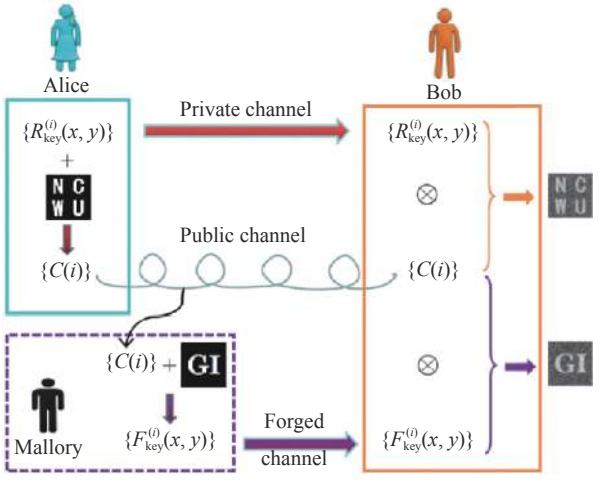


图 8 基于关联成像加密系统的信息安全通信和伪造攻击过程[71]

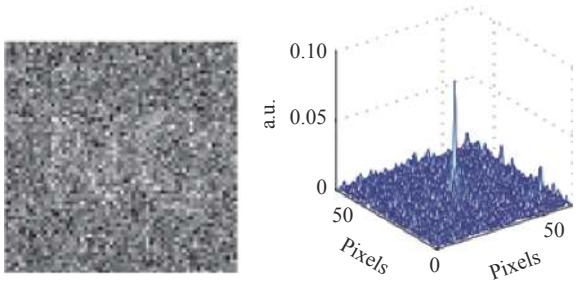
Fig.8 Process of information security communication and forgery attacks based on the ghost imaging encryption system[71]

目前基于关联成像加密方案的破解方案更多的是针对最基本的关联成像加密系统，其攻击的本质类似于穷举攻击，通过构造大量的照明模式或者同一类别的目标图像，最终实现密钥的获取或伪造。但这些攻击方案也从另一个方面对探索更快更安全的关联成像加密方案提供了新的思路。

4.2 基于关联成像的信息认证技术

关联成像加密方案受制于其特性影响，如果想要解密出高保真目标就需要进行大量采样，这就导致密钥的数据量巨大且解密效率也会受到影响。那么，是否能够用少量的采样次数来实现信息的隐藏或者认证呢？

2013 年，新加坡国立大学的陈文等[72]将随机纯相位掩模进行稀疏化，并将其进一步转化为三维空间中的类粒子分布，然后使用关联成像算法对图像进行加密。通过该方案解密出的信息并不能直接看出相关信息，但它与原图的非线性相关分布却有明显的峰值，如图 9 所示，解密信息并



(a) 使用正确密钥解密出的信息　(b) 解密信息与原始信息的非线性相关分布

图 9 低采样率下重构信息与原始信息的非线性相关分布[72]

Fig. 9 Nonlinear correlation distribution of original information and reconstructed information at low sampling rate[72]

不能获得有用信息，但与原始图像的相关性却有明显峰值。该方案实现了基于关联成像的信息认证，同时三维空间的应用进一步扩大了密钥空间。他们仅使用少量的采样次数 (小于奈奎斯特采样率的 5%) 实现物体的认证[73-74]。他们的研究成果表明了仅仅使用较少的采样次数可以实现信息的认证，扩展了关联成像在加密领域的应用。孟祥峰等[75]在此基础上，结合 (t,n) 门限方案，将密钥进行分组并分给不同的参与者，利用不同参与者拥有的不同密钥数量实现多级认证。新加坡国立大学的 Quan 等[76]则为了减少密钥传输问题，引入块处理技术，实现一维向量作为私钥传输，大大减少了私钥的传输和存储负担。

4.3 基于关联成像的图像隐藏方案

图像隐藏技术在当今时代有着重要的作用，一方面可以实现信息的安全存储和传输，避免被窃听篡改的危险，另一方面也可以实现版权保护。

数字水印是比较广泛的图像隐藏技术，但在应对复杂水印时，难免影响宿主图像并且鲁棒性较差。基于此，华北水利水电大学的袁胜等[77]、南京邮电大学的赵生妹等[78]，以及西安工业大学的隋连升等[79]则将关联成像应用到水印中，利用关联成像的特性将复杂的图像转变为少量的桶探测器值B_i，然后将桶探测器值利用最低有效位等方案嵌入到宿主图像的空间域或者小波域，如图 10 所示。相比较传统的数字水印方案，新方案具有更强的抗裁切性能，即使解密后的图像不可见，也可以通过非线性相关系数实现认证。

利用水印的方式实现信息隐藏需要将信息进行一次关联加密，那么是否能够直接将信息在结构光照射的时候隐藏在宿主图像里呢？深圳大学的张承功等[80]将秘密图像进行稀疏采样然后编码

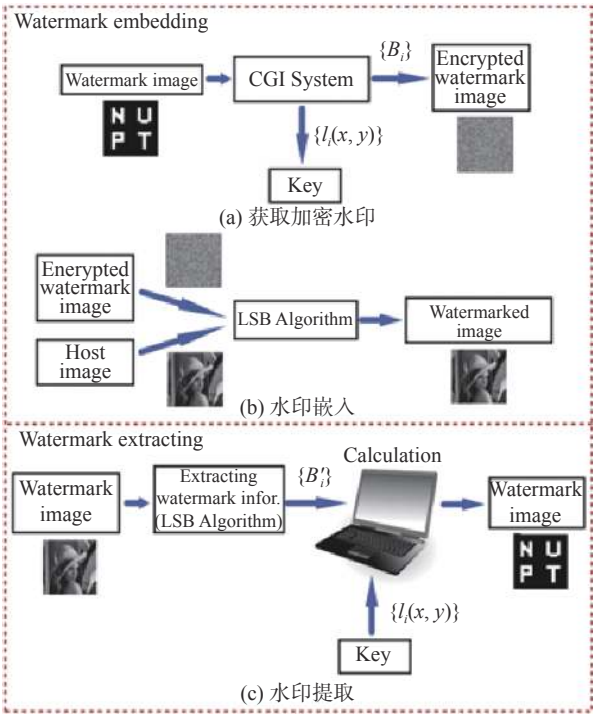


图 10　基于关联成像的图像隐藏方法[78]

Fig. 10　Schematic configuration of the proposed image hiding scheme[78]

成光照模式，以此去照射宿主图像，由桶探测器捕获的信息作为密文，将秘密信息直接通过照明隐藏在宿主密文中。如图 11 所示，该密文可以被授权的接受者和潜在的窃听者接收。通过傅里叶逆变换可以得到与宿主图像几乎一致的图像，只有授权的接受者才能从宿主图像中提取出秘密图像。北京师范大学的汪凯戈课题组[81]将秘密图像的空间信息转变为时变系数，并将其加载到照明模式中，以此照射宿主图像，实现信息的隐藏和融合。该方案可以通过改变加权系数来改变秘密图像的可见性。

在实现数字信息隐藏的同时，新加坡国立大学的 Quan 等[82]利用 2D 不可分离线性正则变换和关联成像加密方案有效保护了语音信息，这也是首次利用关联成像方案实现了对于语音信息的有效保护。

4.4　基于关联成像的密钥分享方案

传统的基于关联成像的加密方案虽然能够实现信息的安全防护，但作为密钥的调制模式反而比密文的数据量大，不利于密钥分发。研究者们在研究如何减少调制模式数量的时候也催生了另一个方向，即基于关联成像的密钥分发技术。这里关联成像方案不是用于传输图像，而是利用它来创建一个公共密钥，以实现用户之间的安全通信[83]。

基于关联成像的密钥分发方案，主要通过巧妙提取重构图像中每个像素中的最低有效位作为密钥，由于没有通信实体，该方案可以在多方之间同时生成、放大和分发公共密钥。但这种方案缺乏有效的认证机制，存在篡改泄露的风险。2022 年，北京大学的俞文凯等[84]提出了一种联合身份认证的密钥分发协议。在这种方案中，对每个授权用户分发不同的片段FP_i，片段本身并不含有任何信息，且被关联成像加密为一系列强度序列S_{Bi}。然后多个用户同时将重构的片段发送给认证中心，只有认证中心实现片段合成，并且认定合成图像FSP有效时，用户才能利用合成的片段提取出特定密钥CK_i，流程如图 12 所示。其中，

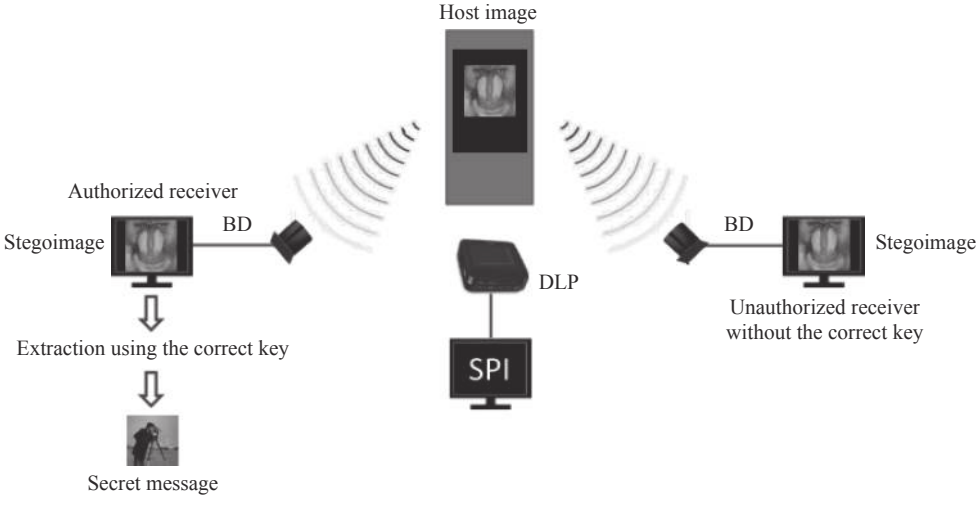


图 11　基于关联成像的光学隐写方案示意图[80]

Fig.11　The diagram of the steganography method based on the SPI system [80]

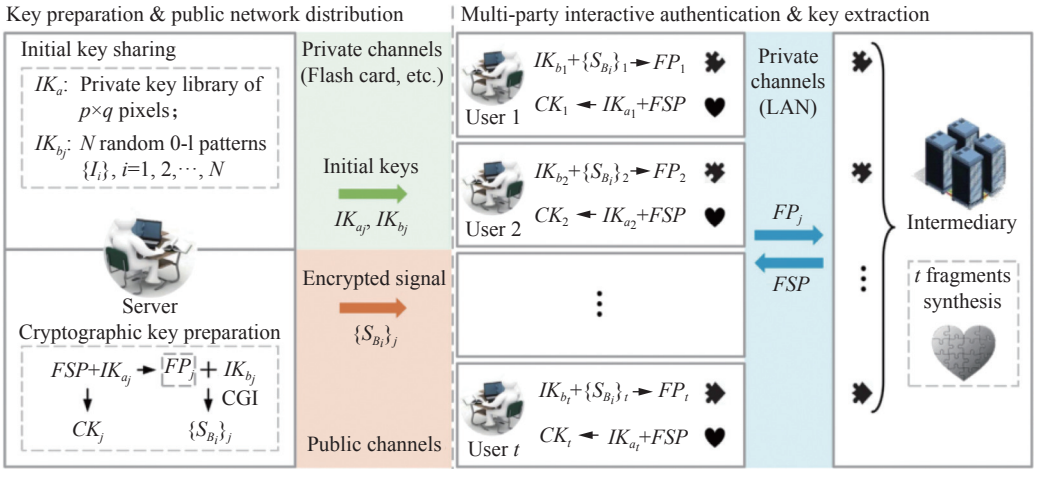


图 12 基于关联成像的多方交互式密钥分发示意图[84]

Fig.12 Schematic of multi-party interactive cryptographic key distribution protocol based on ghost imaging[84]

IK_a为每个用户不同的私钥库，用于提取密钥；IK_{b_j}为每个用户独有的调制模式，应用于解密S_{Bi}。这种方案利用基于片段合成实现了联合认证，降低了个人认证带来的风险。

5 关联成像加密技术的展望

近年来，基于关联成像的光学信息安全技术得到了迅速发展，但仍然存在以下问题值得进一步研究。

a. 解密质量问题。关联成像加密方案受制于其本身特性，需要进行大量采样，如果采样过少就会导致解密质量差。虽然压缩感知、深度学习等算法的应用在一定程度上提高了重构质量，但仍然需要优化解密方案或者探索新的解密方法，进一步提高解密的质量。

b. 密钥分发问题。关联成像加密方案作为一种线性加密方案，其密钥的分发仍是重中之重，虽然不少研究者也从密钥(即照明模式)构造或联合其他方案实现密钥的分发并减少密钥传输数量，但并没有改变线性加密的本质。因此，探究类似于截断傅里叶变换的非对称加密系统，实现基于关联成像的非对称加密，有利于提高加密系统安全性，解决密钥分发问题。

c. 对于保密光通信的探索。时间关联成像加密方案实现了时变信号的加密，而且探测器只需接收信号的总强度，一方面降低了对于带宽的要求，另一方面对于传输过程中产生的损失有较强的容忍力。这些都为应用于远距离、无线的保密光通信提供了可能。但现在并没有明确的或者系统的基于关联成像的保密传输体系，其最高传输速率、最远传输距离、最大传输容量等都值得进一步深入研究。

6 结束语

基于关联成像的光学信息安全技术为保护信息的安全性提供了新的方式。本文回顾了关联成像加密方案的发展历程，展示了关联成像加密方案对于不同场景的表现，加密方案也从开始的固定单一图像加密，逐步扩展出多图像加密、时变信号加密及信息认证。目前关联成像加密方案仍是研究者们关注的重点，如何进一步提高解密信息质量、提高系统安全性，乃至实现基于关联成像的保密光通信，仍是值得探索的方向。在信息交流愈加频繁的今天，信息的安全性更加重要，关联成像加密技术也必将顺应潮流，蓬勃发展。

参考文献：

[1] DONALD M. Unique identification card camera system with fight sealed data card insertion arrangement[P]. USA, 363177. 1972-01-04.

[2] HAINES K A. Computer aided holography and holographic computer graphics[P]. USA, 4778262, 1988-10-18.

[3] MOGENSEN P C, GLÜCKSTAD J. Phase-only optical encryption[J]. Optics Letters, 2000, 25(8): 566–568.

[4] LIU S, GUO C L, SHERIDAN J T. A review of optical image encryption techniques[J]. Optics & Laser Technology, 2014, 57: 327–342.

[5] REFREGIER P, JAVIDI B. Optical image encryption

based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767–769.
[6] CHEN Y A, ZHANG Q, CHEN T Y, et al. An integrated space-to-ground quantum communication network over 4, 600 kilometres[J]. Nature, 2021, 589(7841): 214–219.
[7] FACCIO D. Optical communications: temporal ghost imaging[J]. Nature Photonics, 2016, 10(3): 150–152.
[8] 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–R3432.
[9] 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.
[10] GATTI A, BRAMBILLA E, BACHE M, et al. Ghost imaging with thermal light: comparing entanglement and classicalcorrelation[J]. Physical Review Letters, 2004, 93(9): 093602.
[11] CHEN X H, AGAFONOV I N, LUO K H, et al. High-visibility, high-order lensless ghost imaging with thermal light[J]. Optics Letters, 2010, 35(8): 1166–1168.
[12] SHAPIRO J H. Computational ghost imaging[J]. Physical Review A, 2008, 78(6): 061802(R).
[13] RYCZKOWSKI P, BARBIER M, FRIBERG A T, et al. Magnified time-domain ghost imaging[J]. APL Photonics, 2017, 2(4): 046102.
[14] DEVAUX F, HUY K P, DENIS S, et al. Temporal ghost imaging with pseudo-thermal speckle light[J]. Journal of Optics, 2017, 19(2): 024001.
[15] CLEMENTE P, DURÁN V, TORRES-COMPANY V, et al. Optical encryption based on computational ghost imaging[J]. Optics Letters, 2010, 35(14): 2391–2393.
[16] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics Letters, 2000, 25(12): 887–889.
[17] SITU G H, ZHANG J J. Double random-phase encoding in the Fresnel domain[J]. Optics Letters, 2004, 29(14): 1584–1586.
[18] LIU S T, MI Q L, ZHU B H. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering[J]. Optics Letters, 2001, 26(16): 1242–1244.
[19] TAO R, LANG J, WANG Y. Optical image encryption based on the multiple-parameter fractional Fourier transform[J]. Optics Letters, 2008, 33(6): 581–583.
[20] PENG X, WEI H Z, ZHANG P. Asymmetric cryptography based on wavefront sensing[J]. Optics Letters, 2006, 31(24): 3579–3581.
[21] SITU G H, ZHANG J J. Multiple-image encryption by wavelength multiplexing[J]. Optics Letters, 2005, 30(11): 1306–1308.
[22] SITU G H, ZHANG J J. Position multiplexing for multiple-image encryption[J]. Journal of Optics A:Pure and Applied Optics, 2006, 8(5): 391–397.
[23] MENG X F, CAI L Z, WANG Y R, et al. Digital image synthesis and multiple-image encryption based on parameter multiplexing and phase-shifting interferometry[J]. Optics and Lasers in Engineering, 2009, 47(1): 96–102.
[24] XIAO Y L, SU X Y, LI S K, et al. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain[J]. Optics & Laser Technology, 2011, 43(4): 889–894.
[25] SUI L S, XIN M T, TIAN A L. Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain[J]. Optics Letters, 2013, 38(11): 1996–1998.
[26] 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.
[27] TANHA M, AHMADI-KANDJANI S, KHERADMAND R. Fast ghost imaging and ghost encryption based on the discrete cosine transform[J]. Physica Scripta, 2013, 2013(T157): 014059.
[28] ZAFARI M, KHERADMAND R, AHMADI-KANDJANI S. Optical encryption with selective computational ghost imaging[J]. Journal of Optics, 2014, 16(10): 105405.
[29] KONG L J, LI Y N, QIAN S X, et al. Encryption of ghost imaging[J]. Physical Review A, 2013, 88(1): 013852.
[30] 曹非, 赵生妹. 基于计算鬼成像的双密钥光学加密方案 [J]. 光学学报, 2017, 37(1): 0111001.
[31] ZHANG Y D, ZHAO S M. Optical encryption scheme based on ghost imaging with disordered speckles[J]. Chinese Physics B, 2017, 26(5): 054205.
[32] ZHENG P X, DAI Q, LI Z L, et al. Metasurface-based key for computational imaging encryption[J]. Science Advances, 2021, 7(21): eabg0363.
[33] YUAN S, CHEN D S, LIU X M, et al. Optical encryption based on biometrics and single-pixel imaging with random orthogonal modulation[J]. Optics Communications, 2022, 522: 128643.
[34] ZHU J A, YANG X L, MENG X F, et al. Computational ghost imaging encryption based on fingerprint phase mask[J]. Optics Communications, 2018, 420: 34–39.
[35] ZHAO S M, WANG L, LIANG W Q, 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.

[36] ZHANG L H, PAN Z L, LIANG D, et al. Study on the key technology of optical encryption based on compressive ghost imaging with double random-phase encoding[J]. Optical Engineering, 2015, 54(12): 125104.

[37] ZHANG L H, PAN Z L, ZHOU G L. Study on the key technology of optical encryption based on adaptive compressive ghost imaging for a large-sized object[J]. Journal of Optical Technology, 2017, 84(7): 471–476.

[38] KANG Y, ZHANG L H, ZHANG D W. Optical encryption based on ghost imaging and public key cryptography[J]. Optics and Lasers in Engineering, 2018, 111: 58–64.

[39] QIN Y, ZHANG Y Y. Information encryption in ghost imaging with customized data container and XOR operation[J]. IEEE Photonics Journal, 2017, 9(2): 7802208.

[40] SUI L S, DU C, XU M J, et al. Information encryption based on the customized data container under the framework of computational ghost imaging[J]. Optics Express, 2019, 27(12): 16493–16506.

[41] YUAN S, YANG Y R, LIU X M, et al. Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging[J]. Optics and Lasers in Engineering, 2018, 100: 105–110.

[42] JIAO S M, FENG J, GAO Y, et al. Visual cryptography in single-pixel imaging[J]. Optics Express, 2020, 28(5): 7301–7313.

[43] 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.

[44] LI X Y, MENG X F, YANG X L, et al. Multiple-image encryption based on compressive ghost imaging and coordinate sampling[J]. IEEE Photonics Journal, 2016, 8(4): 3900511.

[45] LI X Y, MENG X F, WANG Y R, et al. Secret shared multiple-image encryption based on row scanning compressive ghost imaging and phase retrieval in the Fresnel domain[J]. Optics and Lasers in Engineering, 2017, 96: 7–16.

[46] LI X Y, MENG X F, YANG X L, et al. Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme[J]. Optics and Lasers in Engineering, 2018, 102: 106–111.

[47] TAO Y C, YANG X L, MENG X F, et al. Plaintext-related multiple-image encryption based on computational ghost imaging[J]. Journal of Modern Optics, 2020, 67(5): 394–404.

[48] SHI D F, HUANG J, WANG Y J, et al. Simultaneous fusion, imaging and encryption of multiple objects using a single-pixel detector[J]. Scientific Reports, 2017, 7(1): 13172.

[49] ZHANG L H, YUAN X, ZHANG D W, et al. Research on multiple-image encryption scheme based on Fourier transform and ghost imaging algorithm[J]. Current Optics and Photonics, 2018, 2(4): 315–323.

[50] YUAN X, ZHANG L H, CHEN J, et al. Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing[J]. Applied Physics B, 2019, 125(9): 174.

[51] ZHANG L H, YUAN X, WANG K M, et al. Multiple-image encryption mechanism based on ghost imaging and public key cryptography[J]. IEEE Photonics Journal, 2019, 11(4): 7904014.

[52] WANG X G, ZHAO D M. Optical image hiding with silhouette removal based on the optical interference principle[J]. Applied Optics, 2012, 51(6): 686–691.

[53] RAWAT N, HWANG I C, SHI Y S, et al. Optical image encryption via photon-counting imaging and compressive sensing based ptychography[J]. Journal of Optics, 2015, 17(6): 065704.

[54] DAI B, GAO Z S, WADA N, et al. Orthogonal DPSK/CSK modulation and public-key cryptography-based secure optical communication[J]. IEEE Photonics Technology Letters, 2013, 25(19): 1897–1900.

[55] ABDALLAH W, HAMDI M, BOUDRIGA N. A public key algorithm for optical communication based on lattice cryptography[C]//2009 IEEE Symposium on Computers and Communications. Sousse, Tunisia: IEEE, 2009: 200–205.

[56] 姚俊良, 孙郁哲, 任海鹏. 混沌光纤通信研究进展与展望 [J]. 西安理工大学学报, 2018, 34(2): 127–133.

[57] 李文华, 袁夕征, 熊晓然. 量子保密通信关键技术及组网应用探讨 [J]. 邮电设计技术, 2019(2): 69–75.

[58] KORZH B, LIM C C W, HOULMANN R, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre[J]. Nature Photonics, 2015, 9(3): 163–168.

[59] RYCZKOWSKI P, BARBIER M, FRIBERG A T, et al. Ghost imaging in the time domain[J]. Nature Photonics, 2016, 10(3): 167–170.

[60] XU Y K, SUN S H, LIU W T, et al. Detecting fast signals beyond bandwidth of detectors based on computational temporal ghost imaging[J]. Optics Express, 2018, 26(1): 99–107.

[61] PAN Z L, ZHANG L H. Optical cryptography-based temporal ghost imaging with chaotic laser[J]. IEEE Photonics Technology Letters, 2017, 29(16): 1289–1292.

[62] KANG Y, ZHANG L H, ZHANG D W. Study of an encryption system based on compressive temporal ghost

imaging with a chaotic laser[J]. Optics Communications, 2018, 426: 535–540.

[63] HUANG X W, BAI Y F, FU X Q. Stable and secure image transmission based on temporal ghost imaging[J]. Journal of Optics, 2019, 21(5): 055701.

[64] WANG Y P, CHEN H L, JIANG W J, et al. Optical encryption for visible light communication based on temporal ghost imaging with a micro-LED[J]. Optics and Lasers in Engineering, 2020, 134: 106290.

[65] ZHANG L H, YE H L Y, ZHANG D W. Study on the key technology of image transmission mechanism based on channel coding ghost imaging[J]. IEEE Photonics Journal, 2018, 10(4): 6500913.

[66] KANG Y, ZHANG L H, YE H L, et al. One-to-many optical information encryption transmission method based on temporal ghost imaging and code division multiple access[J]. Photonics Research, 2019, 7(12): 1370–1380.

[67] YAO X, LIU X, YOU L X, et al. Quantum secure ghost imaging[J]. Physical Review A, 2018, 98(6): 063816.

[68] DONG S, ZHANG W, HUANG Y D, et al. Long-distance temporal quantum ghost imaging over optical fibers[J]. Scientific Reports, 2016, 6: 26022.

[69] 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.

[70] JIAO S M, LEI T, GAO Y, et al. Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging[J]. IEEE Access, 2019, 7: 119557–119565.

[71] YUAN S, WANG L J, LIU X M, et al. Forgery attack on optical encryption based on computational ghost imaging[J]. Optics Letters, 2020, 45(14): 3917–3920.

[72] CHEN W, CHEN X D. Ghost imaging for three-dimensional optical security[J]. Applied Physics Letters, 2013, 103(22): 221106.

[73] CHEN W, CHEN X D. Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit[J]. Optics Letters, 2013, 38(4): 546–548.

[74] CHEN W, CHEN X D. Grayscale object authentication based on ghost imaging using binary signals[J]. Europhysics Letters, 2015, 110(4): 44002.

[75] LIU X R, MENG X F, WANG Y R, et al. Optical multilevel authentication based on singular value decomposition ghost imaging and secret sharing cryptography[J]. Optics and Lasers in Engineering, 2021, 137: 106370.

[76] DU J, XIONG Y, QUAN C. High-efficiency optical image authentication scheme based on ghost imaging and block processing[J]. Optics Communications, 2020, 460: 125113.

[77] YUAN S, MAGAYANE D A, LIU X M, et al. A blind watermarking scheme based on computational ghost imaging in wavelet domain[J]. Optics Communications, 2021, 482: 126568.

[78] WANG L, ZHAO S M, CHENG W W, et al. Optical image hiding based on computational ghost imaging[J]. Optics Communications, 2016, 366: 314–320.

[79] SUI S S, CHENG Y, TIAN A L, et al. An optical watermarking scheme with two-layer framework based on computational ghost imaging[J]. Optics and Lasers in Engineering, 2018, 107: 38–45.

[80] ZHANG C G, HE W Q, HAN B N, et al. Compressive optical steganography via single-pixel imaging[J]. Optics Express, 2019, 27(9): 13469–13478.

[81] YE Z Y, WANG H B, XIONG J, et al. Simultaneous full-color single-pixel imaging and visible watermarking using Hadamard-Bayer illumination patterns[J]. Optics and Lasers in Engineering, 2020, 127: 105955.

[82] KUMAR R, ZHONG F Q, QUAN C G. Optical voice information hiding using enhanced iterative algorithm and computational ghost imaging[J]. Journal of Optics, 2019, 21(6): 065704.

[83] LI S, YAO X R, YU W K, et al. High-speed secure key distribution over an optical network based on computational correlation imaging[J]. Optics Letters, 2013, 38(12): 2144–2146.

[84] YU W K, WEI N, LI Y X, et al. Multi-party interactive cryptographic key distribution protocol over a public network based on computational ghost imaging[J]. Optics and Lasers in Engineering, 2022, 155: 107067.

（编辑：丁红艺）