中国激光

多维调制的全息加密光存储

林达奎[1,2,3,4,5]，宋海洋[1,2,3,4,5]，李枷楠[1,2,3,4,5]，王琨[1,2,3,4,5]，林枭[1,2,3,4,5]，谭小地[1,2,3,4,5*]

[1]福建师范大学光电与信息工程学院，福建 福州 350117；
[2]医学光电科学与技术教育部重点实验室，福建 福州 350117；
[3]福建省光子技术重点实验室，福建 福州 350117；
[4]福建省光电传感应用工程技术研究中心，福建 福州 350117；
[5]福建师范大学信息光子学研究中心，福建 福州 350117

摘要 大数据时代对数据存储提出了新的需求，数据的存储安全关乎社会稳定与发展。全息加密光存储具有高存储密度、快读取速度、长保存寿命等特点，为海量数据存储提供了有效的解决方案，是保障数据存储安全的有力手段。聚焦于全息光存储领域，论述了以振幅、相位和偏振等作为调制变量的全息加密光存储的基本原理，介绍了常见的全息加密光存储技术及其性能影响因素，梳理了大量密钥的管理方法，最后总结了各技术特点，并对全息加密光存储的未来发展进行了展望。

关键词 全息；全息存储；全息加密光存储；光的多维调制；存储安全

中图分类号 O438 **文献标志码** A **DOI**：10.3788/CJL230726

1 引 言

大数据时代下的海量数据存储和数据安全是关乎社会发展的重要研究领域。传统的以磁存储为代表的技术路线由于能耗高、存储密度接近理论值等因素而难以满足指数增长的数据量存储需求。20 世纪 60 年代，光全息技术被应用于数据存储领域[1-3]。该技术以光为信息载体，以光的振幅、相位、偏振、波长等多维参数作为信息编码参量，增加了信息编码的灵活性与复杂度。利用光响应材料卤化银卤胶、光折变晶体、光致聚合物等[4-6]，在三维空间内记录下二维信息光数据，数据的存储密度得到极大增加。此外，由于全息光存储技术的二维数据页是并行存取的，且聚合物长期稳定，因此其具有高速读取、存储寿命长等优势[7-11]，一经提出就广受关注。在现今的大数据时代背景下，超高存储密度技术的发展迫在眉睫，全息光存储技术迎来了新的发展机遇[12-14]。

在开展高存储密度研究的同时，另一个数据存储安全问题也受到广泛关注。传统数字加密技术通过对数字信号进行某种特定变换，将数据变换为无意义的密文并进行数据传输，接收方通过密钥进行密文解密。为了增加加密系统的安全性，非对称加密技术[15]、Hash 函数[16]等技术被相继提出。传统数据加密手段表现出了出色的加密性能，但随着技术的发展，信息流通的大数据时代对加密技术的安全性提出了更高的要求。光的多维参数可调特性为加密技术提供了灵活度更高的实现路径。自 Refregier 等[17]提出双随机相位编码（DRPE）加密技术以来，研究人员在加密系统性能[18-19]、加密手段[20-22]以及攻击手段[23-25]等方面开展了一系列研究工作。传统的光学加密技术主要是对光信息传输过程进行加密[26-27]，即对载有信号的光束进行特殊变换，将其变为平稳白噪声后再进行传输，这样可实现安全传输。而全息加密光存储聚焦于存储过程，通过对信号光或参考光进行调制，实现信号光的加密存储，可以在源头上防止数据泄漏[28]。研究者在全息加密光存储领域进行了系列研究，同时在全息存储理论[14,29-30]、全息存储系统[8-9,31]、全息存储材料[6,32-33]等方面也开展了大量的研究。在全息加密光存储方面，研究者发现：相位型数据页比振幅型数据页在安全性能上更有优势[34]；双随机相位加密除了具有很高的存储安全性之外，还有利于提升存储系统的存储密度[35]。Tan 等[36]率先基于偏振维度，利用随机偏振掩模调制线偏振数据页，实现加密存储。

全息加密光存储利用了光的多维可调特性，具有海量的密钥空间。全息加密光存储是在物理层面对信息进行加密，与全息图在材料中的分布状态（密文）相

收稿日期：2023-04-17；**修回日期**：2023-05-31；**录用日期**：2023-06-13；**网络首发日期**：2023-06-23

基金项目：国家自然科学基金（62105065，U22A2080）、国家重点研发计划（2018YFA0701800）、福建省科技重大专项（2020HZ01012）

通信作者：*xtan@fjnu.edu.cn

关，但其状态无法直接探测，即无法直接获得其密文信息。全息加密光存储的海量密钥空间与记录介质中存储状态的复杂性保障了数据的存储安全。此外，实际应用时可将传统数字加密技术与光学加密技术相结合，以满足更高的加密需求。本文基于下一代大数据存储方案——光全息存储，综述了几类全息加密光存储技术的基本原理及发展现状，对全息加密光存储未来的发展进行了展望，并分析了可能面临的挑战。

2 全息加密光存储基本原理

1963 年，van Heerden[1]提出全息光存储，并分析了其理论存储密度将达到 $1/\lambda^3$（λ 为波长）。全息光存储基本原理是：利用信息光与参考光在记录介质中进行干涉记录，再用同一束参考光对全息图进行衍射读取，获得再现信息光中的数据。1969 年，Kogelnik[3]提出了利用耦合波理论模拟计算入射光束在体光栅中的衍射特性的理论，该理论为全息光存储中的信息光衍射再现特性研究提供了坚实的理论基础。全息光存储通常采用复用的方式增加系统的数据存储容量，其系统实现主要有离轴和同轴两个技术路线[11]，其中以 Optware 公司为代表的同轴全息光存储系统通常采用位移复用[8-9]，而以 InPhase 公司为代表的离轴全息光存储系统通常采用角度复用方式[7]。为了增加存储容量，光的振幅、相位、偏振、波长等参量相继被用作复用的调制参数，在一般的数据存储系统中，这些调制参数无需保密，且相对固定。

全息加密光存储与全息光存储中的复用技术基本原理一致，因此理论上只需将复用参数作为密钥，包括振幅、相位、偏振、波长、角度等[35-41]所有的复用参数都可以用于全息加密。图 1 所示为最常见的信号光加密原理图，加密过程中用密钥（振幅、相位、偏振等）对信号光进行调制以形成密文，在感光材料中记录该密文与参考光以形成全息图；解密过程中利用参考光和全息图再现出密文信息，该密文再与解密密钥作用以再现数据，正确的解密密钥将得到原始数据，错误的解密密钥将得到统计无关的白噪声。此过程中信号光的调制参数即为密钥，参考光直接再现图为密文，信号光为明文。同样也可对参考光进行振幅、相位等调制，实现信息加密存储。为了满足不同客户的需求，保证数据存储安全，在加密这一应用领域中需要大量的无再现信号串扰的可选参考光参数以抵抗暴力破解的风险。与之相比，为了满足大存储容量，所需的参考光数量较少。因为受限于材料的响应能力，材料同一位置的复用数量有限，需配合位移复用将材料移动到下一位置进行再次记录，而此时可重复使用上一记录位置的参考光参数，记录效果不受影响。

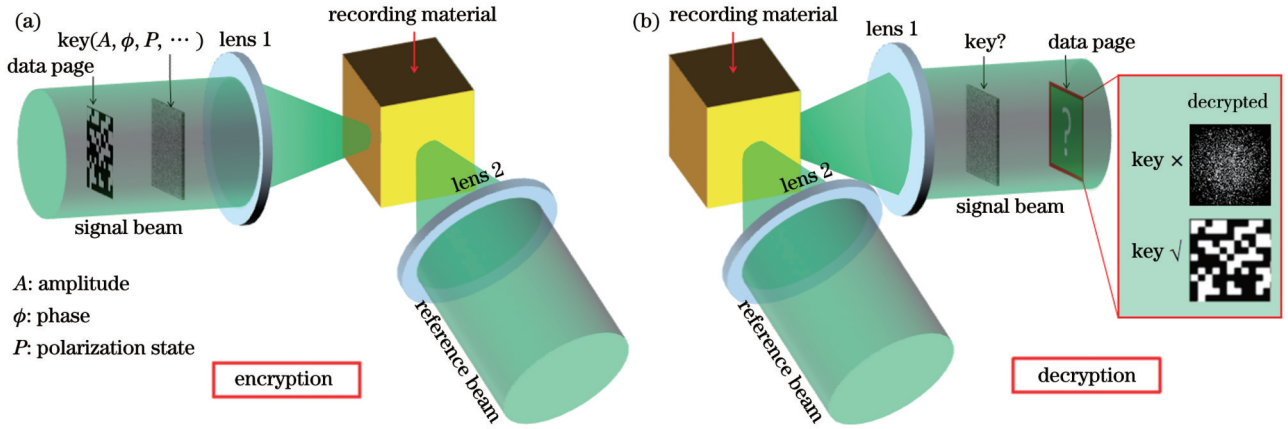

图 1 全息加密光存储原理图。(a)加密过程；(b)解密过程

Fig. 1 Schematics of holographic encrypted optical storage. (a) Encryption process; (b) decryption process

3 全息光存储加密技术

光的多维可调特性给加密存储带来了巨大的密钥空间，近年来，研究人员基于振幅、相位、偏振、波长等参数调制进行了加密存储方面的研究，并取得了丰硕的成果。

3.1 振幅调制加密光存储技术

振幅调制具有可用普通器件实现、成本低且能直接探测等特点，是最早用于光场调制的光学参数之一。在加密存储领域中，振幅分布作为密钥之一可用于数据的加密存储。Kim 等[42]利用二值振幅掩模记录纯振幅信息页，在同一记录位置，再利用二值振幅掩模的振幅互补掩模进行振幅图像的互补图像记录。在此参数设置下，两个振幅图像在材料中形成的记录光栅被错开一定距离，当再现时参考光使用的振幅掩模与原来记录时的振幅掩模分布不一致时，将再现出原来图像及其互补图像，由此得到随机白噪声的结果，只有使用了正确振幅掩模才能得到准确的二值纯振幅信息页。其实验结果表明，当振幅掩模正确率在 2% 以下时才无法破解出信息，因此该方法的安全性

有限。

上述的二值互补振幅加密方式需要通过两次存储来实现一幅信息图像的加密存储，加密效率及存储密度较低。Toishi等[43]将振幅调制加密技术进一步拓展到多幅图像的加密存储。如图2所示，利用不同图案的振幅参考光记录不同的数据页，各个参考光和信号光小块在记录介质中发生干涉形成微全息图，每个微全息图在介质中的空间位置是错开的。当利用正确的振幅参考光进行再现时，相应的微全息图发生衍射，再现出数据页；当利用错误的随机振幅参考光时，多个密钥的一部分发生叠加，再现结果是多个数据页的叠加；当振幅参考光所有像素点都亮时，再现信息则是所有数据页的叠加结果。所以，错误的振幅参考光再现出的各个数据页将成为彼此的噪声互相干扰而无法分辨，从而实现加密效果。当参考光像素个数为100时，其被破解的概率将小于10^{-14}，相比二值互补型振幅加密方式其安全性得到进一步的提高。此外，通过控制数据页曝光时间可实现二值空间光调制器的多灰阶全息存储[44]，为更高阶的振幅调制全息加密光存储提供了思路。还可通过增加参考光像素个数、增加单个记录位置的全息图记录个数和结合其他加密技术来增加系统的安全性。

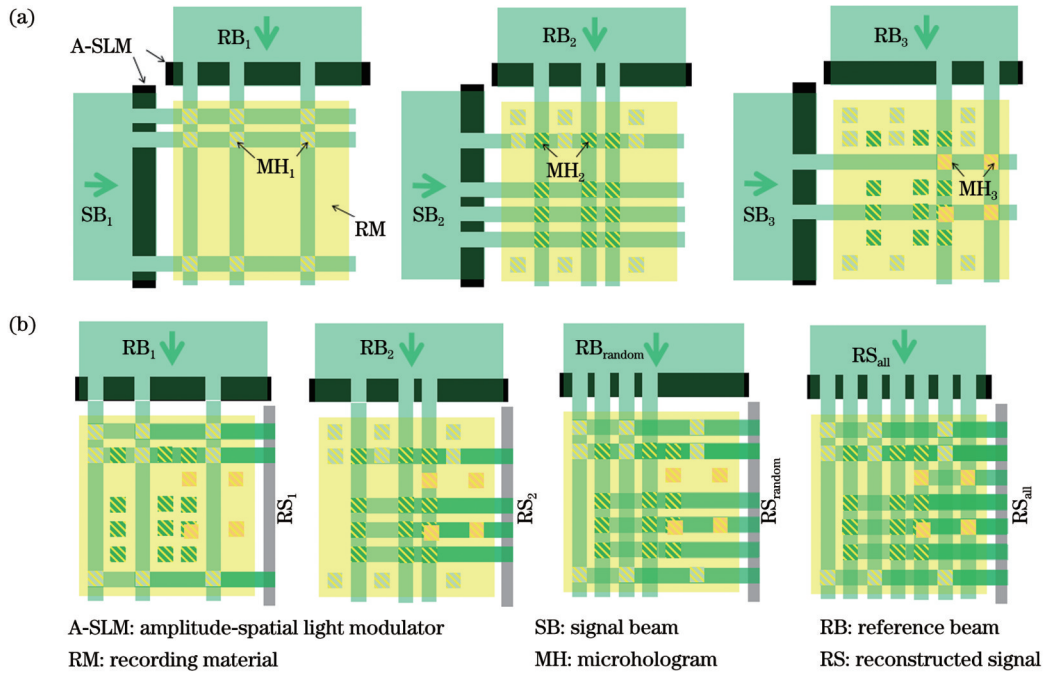

图2 振幅加密全息存储。(a)加密过程；(b)解密过程

Fig. 2 Holographic data storage by amplitude encryption. (a) Encryption process; (b) decryption process

3.2 相位调制加密光存储技术

相位调制由于其光的利用率高、实现方便等特点而在全息加密光存储中得到广泛应用。基于相位调制技术的全息加密光存储研究可追溯到1995年Refregier等[17]提出的DRPE。此后，Javidi等[45]将DRPE应用于全息加密光存储。基于DRPE的典型加密存储系统如图3所示。在离轴全息存储系统的信息光路中设置4f系统，在物面与傅里叶面分别放置两个统计无关的随机相位板，利用物面位置的空间光调制器(SLM)生成待加密图像，其与该位置的随机相位掩模M_1发生作用，经相位调制后穿过透镜L_1在傅里叶面与该位置的随机相位掩模M_2发生作用，进而进行二次相位调制，然后经过L_2在4f的像面上形成加密的随机白噪声，并与参考光发生干涉，从而加密图案被存储在记录介质

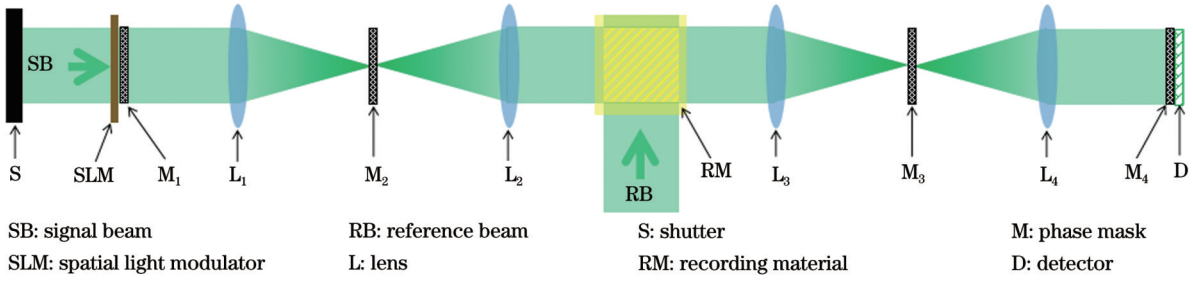

图3 双随机相位编码加密全息存储

Fig. 3 Holographic data storage by double random phase encoding encryption

中，通过改变随机相位掩模实现多幅图像的分别加密。解密时将信息光路关闭，只用平行参考光读取记录介质中的加密图像，且在读取过程中傅里叶面放置的掩模是记录时使用的掩模复共轭，若加密的图像为振幅图像则可直接利用像面位置的探测器得到解密后的图像，解密过程中需对傅里叶面的掩模进行精准对齐。在DRPE技术诞生之后的十多年，研究人员发展出了一系列的可提供巨大密钥空间的加密存储系统。Matoba等[46]将加密系统随机相位掩模放置位置拓展到更一般的菲涅耳域进行加密，增加了空间位置这一密钥，解密时需同时掌握随机相位掩模分布及其空间位置才能获取数据，并在该系统中评估了空间位置的密钥数量为3×10^{18}量级[46]。Ahouzi等[47]在对信号光进行双随机相位加密的基础上，通过对信号光进行再一次的随机相位加密，或对参考光进行随机相位加密，实现了三重随机相位加密。Tan等[34]在离轴全息存储系统中使用相位调制进行了加密存储的系列研究。在全相位加密存储研究中，利用双随机相位编码将相位型数据页加密成白噪声形式的密文，解密时将掩模（与记录时的掩模一致）放置在相位共轭的读取状态下，便可读取出原始信息。该研究发现，在一定的系统带宽下，相位型加密比振幅型加密有更好的性能、更高的安全性。在研究双随机相位加密对存储系统性能的影响时，研究者在角度复用基础上使用不同的双随机相位掩模实现了多幅数据页的加密存储；利用其中一个图像的随机相位掩模进行再现时，虽然复用角度间隔很小（小到足以产生串扰），会再现出相邻图像的串扰，但两个相邻数据页的随机相位掩模统计无关，导致串扰的形式为白噪声，因此能准确再现出其中一幅图像而不受串扰的影响；双随机相位加密方式相比传统技术能进一步减小角度复用的间隔，具有更高的存储密度[35]。该研究对于提升全息光存储容量具有重要意义。随机相位编码加密存储方式因其巨大的密钥空间而具有极高安全性，而正交相位编码具有低串扰的特性。Heanue等[28]将正交相位编码与随机相位编码结合并应用于全息加密光存储，在保持正交编码的低串扰特性的同时，还具有随机相位编码的高安全性。此外，可将傅里叶变换域[48-49]进一步拓展到分数傅里叶变换域[50]、局域分数傅里叶变换域[51-52]以及级联分数傅里叶变换域[53]。Nomura等[54]基于联合变换器的随机相位体全息加密光存储，进一步增加了加密存储系统的复杂度，提高了安全性。

基于随机相位调制的全息加密光存储在系统实现上有两种方式[55]：一是信息光在记录时不进行调制，利用相位加密后的参考光实现不同图像的分别加密存储，再现时需利用加密时的参考光才能再现出信息光数据页，这样便可防止未授权用户获取数据[56]；二是对信息光进行相位加密[34]，利用随机相位掩模配合其位置等信息进行信息光调制加密，进而在记录介质位置通过与参考光的干涉实现加密存储；此外也可对信息光和参考光同时进行随机相位加密[57]。Mita等[58-59]对参考光和信号光同时进行随机相位掩模加密，对于授权用户，获得的再现结果是平稳白噪声形式的信号光，对于未经授权的用户，获得的再现结果不再是同样亮度的平稳白噪声，而是强度为正确再现强度20%左右的图像。因此可以通过监测再现出来的图像强度，轻易判断是否有未经授权的用户在窃取信息。Kitano等[60]分析了信号光和参考光同时编码加密时的存储系统的安全性，结果表明，其解密密钥与加密密钥的相关系数达到0.2时才可能破解出信息，在密钥长度为2313的双波束加密系统中，等效被破解的概率将小于10^{-6}。

相位加密光存储技术中的信息光可以使用振幅编码，也可使用相位编码。在振幅编码信息光进行相位加密存储后，使用正确密钥，通过电荷耦合器件(CCD)，可直接读取到所存储的信息。相位编码信息光在信息读取时需通过干涉[29,61-62]或非干涉方式（包括傅里叶迭代[63-64]、深度学习[65]等）进行相位重建。Tan等[34]利用干涉法提取了相位型数据页的双随机相位加密离轴全息存储系统的相位数据，结果显示，在系统带宽一定的情况下，相位型加密系统比振幅型加密系统的安全性高。传统干涉读取往往对光路的要求较高且光路较复杂。Koppa[66]设计信息页的相位分布时，在光路中设置了平行玻璃板，使数据页相对其反射光出现一定位移，进而二者发生干涉，由此直接解出相位信息页的相位分布。该技术无需额外的干涉光路，具有光路简单、稳定的优势。

3.3 偏振调制加密光存储技术

光的偏振态可用琼斯向量描述。偏振光有取向角和椭偏度两个可调参数，这两个参数由两个正交偏振基矢的幅值和相位差决定，因此利用偏振进行加密具有更大的密钥空间[67-70]。Tan等[36]率先利用正交线偏振态实现偏振全息加密光存储，将数据页编码为正交线偏振二维数据页，加密时使用随机偏振掩模将数据页调制为随机偏振态形成密文，在偏振响应材料中记录形成全息图后，再用对应偏振掩模调制后的共轭参考光解密出二维线偏振数据页。Matoba等[71]结合DRPE框架，提出双随机偏振加密，通过在4f输入面与傅里叶面放置随机偏振调制掩模，实现了双随机偏振加密系统，进一步发展了偏振维度的全息加密光存储。如图4所示，也可利用正交的圆偏光编码二维数据页，编码后的正交偏振信息光可用随机偏振掩模进行调制。该偏振掩模中的每一个像素都可以用于调制偏振数据页中每个像素的相位延迟量以及主轴旋

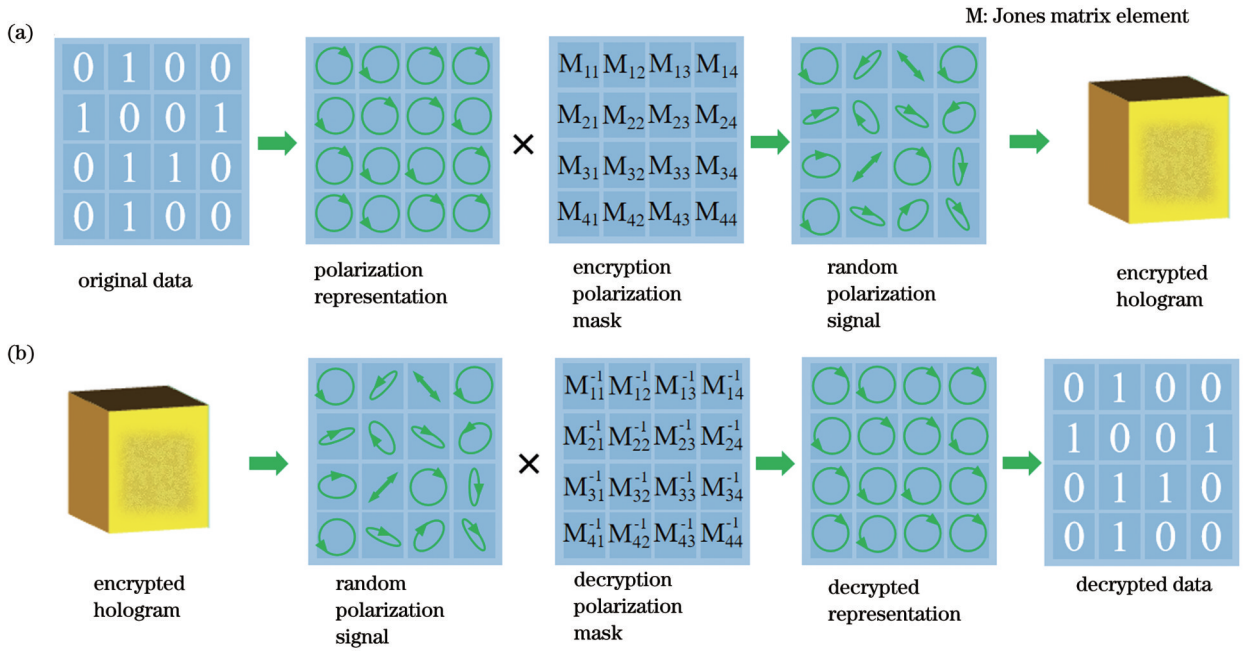

图 4 偏振加密全息存储。(a)加密过程;(b)解密过程

Fig. 4 Holographic data storage by polarization encryption. (a) Encryption process; (b) decryption process

转角度,并可用琼斯矩阵表示该变换掩模。调制后的二维数据光场为偏振态随机的信息光,该信息光再与参考光发生干涉,被记录在偏振响应的全息记录材料上。再现时,用一个共轭参考光照射全息图,便可再现出偏振密文光场,使该光场经过逆变换后的偏振掩模抵消原来加密过程中偏振掩模的相位延迟与主轴旋转的调制,从而解密出原来的正交偏振态。其中二维随机偏振掩模可由两个半波片和夹在中间的相位空间光调制器组成[72]。理论上可以将数据编码成任意偏振态的偏振光,从而实现任意比特的编码,增加加密系统的安全性。

3.4 空间姿态调制加密光存储技术

全息加密光存储中的信息再现需要参考光和信息光路中的掩模保持特定姿态才能实现,一旦有少许几何位置的偏差,都将无法再现出原始信息[73]。利用这一特征,开发出一系列以掩模姿态(位置、偏转角度等)[74]和角度[75]等为密钥的全息加密存储技术。

全息光存储系统通常利用体全息的布拉格选择性进行角度复用,同一材料记录位置可存储多幅数据页,达到增加存储容量的效果。而加密存储系统同样可利用角度复用实现数据的安全存储。Matob等[76-77]基于双随机相位加密,利用角度复用进行二维数据页的加密与解密,并评估了光学系统带宽对解密效果的影响,指出低空间带宽的数据有利于带宽受限系统中的数据恢复。Jia等[78]提出了单束光的数据编码方式,信号光与参考光都用同一个SLM进行调制,其中信号光为振幅信息,参考光的相位可以通过闪耀光栅的形状进行调制,参考光的入射角度可以通过光栅的周期进行调制。该结构相比传统离轴式的角度复用技术有着结构紧凑、易调试、对环境稳定性要求低等优势,在数据加密存储方面具有潜在的应用。

随机相位加密系统因其巨大的相位分布密钥空间而具有极高的安全性。利用随机相位掩模的几何姿态这一维度可进一步增大密钥空间。Xi等[79]将随机相位密钥放置在菲涅耳域中的不同位置以实现不同图像的加密。通过同时切换原始图像和旋转记录介质(CCD),可同时记录下多张全息图的叠加图,从而实现多张图的同时记录。且在解密过程中,通过偏离菲涅耳域掩模位置或使用错误解密波长等考察解密图像与原始图像的相关系数,进而实现系统的安全性定性评估。Sun等[80]利用毛玻璃生成随机相位对信息光进行加密,然后垂直于光轴方向移动毛玻璃以实现不同图像的加密存储,且理论分析了毛玻璃移动量对再现加密信息的敏感性。同年,参考光中的随机相位掩模板的旋转维度被一起用于加密[81],研究者指出更细密的随机掩模可增加旋转复用中的角度选择性。Su等[82]在双随机加密系统中进行了随机相位掩模的面内和光轴三个维度的移动存储,指出掩模三维移动选择性除了受掩模的相关长度影响外,还与记录介质尺寸及掩模与全息图的距离有关。Situ等[83]通过在光轴上移动随机相位掩模实现了多图像加密,并探究了最小的移动间距,通过高斯低通滤波增加了系统复用加密的图像数量。Sun等[84]研究发现,毛玻璃的旋转选择性随毛玻璃与记录介质的距离的减少或照射面积的增加而增强,且旋转中心偏离掩模照射中心越远,布拉格选择性越高。

图5所示为典型的空间姿态调制加密存储的示意

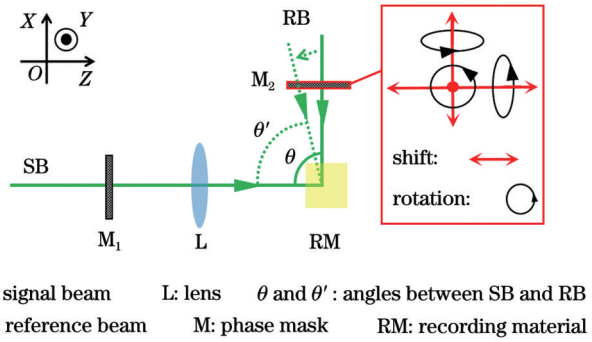

图 5 姿态调制全息加密光存储

Fig. 5 Holographic data storage by geometric modulation of reference beam

图。以参考光姿态调整为例，参考光通过随机相位掩模 M_2 进行调制，利用参考光入射角度及 M_2 在 X、Y、Z 三个轴向上的平移量和绕轴的旋转量作为附加的加密维度。同理，可在信息光中进行同样的姿态调制，进一步增加加密系统的安全性。

3.5 多维复用全息加密光存储技术

为了充分挖掘全息加密光存储的性能，研究人员对多个加密维度的同时复用进行了相关研究。研究人员提出了一个简单有效的全息加密光存储方案，即通过旋转或平移随机相位板实现随机相位与其空间位置的结合[45,85]。在双随机相位掩模及其位置基础上，通过增加波长作为密钥[43-44]，进一步验证了多维复用提升加密系统安全性的可行性。Sarkadi 等[86]提出，同时利用振幅和相位调制参考光可有效提高双随机相位加密系统的安全性。总体上，多维复用加密存储的相关研究较少，特别是偏振维度和其他加密维度的结合。

3.6 其他全息加密光存储技术

为满足应用需求，研究者提出密钥复制方式[87]。但由于随机相位的复杂性，完全复制一个随机相位很困难，若用户发生密钥损坏或丢失，则无法准确进行加密数据的重新获取。在密级要求不高的场景下，Chang 等[88]采用一种柱透镜阵列进行参考光相位变换，通过旋转实现多幅信息分别加密。以上特殊设计的透镜阵列在满足特殊应用要求的同时，还可降低调整难度。针对随机相位掩模对准困难的问题，Su 等[89]提出掩模姿态调整技术，进一步降低了掩模调整难度，将对准时间控制在 1 min 之内。

Matoba 等[90]和 Zhang 等[91]基于再现波长与记录波长不同导致布拉格失配，进而无法再现出信息这一特点，先后利用波长这一维度作为密钥，实现了不同数据页的存储。Matoba 等[90]指出波长的有效密钥数量取决于相位掩模的相关长度，但波长的连续调控在实际操作中不易实现。Tebaldi 等[92]基于联合变换相关器原理，利用信号光和分型波带片作为联合变换的两个输入，使用分型波带片的分型级数和段数两个参数作为密钥，由于只传输分型波带片的两个参数，传统随机相位掩模传输过程易损坏的问题得到消除。该方法虽无法抵抗所有攻击手段，但为加密系统的多样性提供了思路。Sheeja 等[93]提出，基于胶带式聚合物材料的全息加密光存储具有不易被修改和复制的特点。Sando 等[94]基于磷酸铁锂折射率时间渐变的特性进行了数据加密存储。此外，可通过使用和不使用随机相位掩模，实现加密和不加密状态可切换的存储系统[75]。

4 加密光存储系统性能的分析

一个加密光存储系统的性能可从密钥空间、恢复数据保真度、不同密钥间再现信息的串扰等方面进行评估。一般加密系统的安全性由其密钥空间（即加密系统密钥的所有组合可能性）决定，例如一个具有 n 个像素的二灰阶随机相位板的密钥空间为 2^n，那么被破解概率将为 $1/2^n$，其中 2 对应为该随机相位板的相位调制灰阶数。通过增加灰阶数量和像素个数，很容易实现密钥空间数量级的增长，但实际的安全性受具体的加密技术影响。如在互补型振幅加密存储中，Kim 等[42]研究发现，部分正确的密钥将再现出信息，即产生串扰，当编码单元为 2400 时，解密密钥正确率达到 2% 以上时将再现出信息。Sarkadi 等[86]在相位与振幅同时调制加密系统中，通过优化相位与振幅调制参数，大幅提升了加密系统的安全性，在该系统中密钥长度为 73 bit，且该密钥长度随着信噪比的增加而增加。Kitano 等[60]研究了双波束的加密存储系统的安全性，结果表明，若解密密钥与加密密钥的相关系数达到 0.2 时就有可能破解出信息，在密钥长度为 2313 的双波束加密系统中，被破解的概率将小于 10^{-6}。研究者将双随机相位引入到全息加密光存储中，发现相位型数据页相比振幅型数据页在加密存储数据保真方面更有优势[18-19]。研究者分析了有限带宽的光学系统对数据信息解密质量的影响[34]，由于带相位的数据的恢复更复杂，因此该系统具有更高的安全性。Mita 等[58]指出，随机相位掩模的随机性将影响加密系统的安全性。Wang 等[95]研究了随机二阶相位编码加密存储，结果显示，当随机相位块数目为 100 个时，被破解概率小于 10^{-10}。

在加密系统中，解密过程的复杂程度将影响系统的使用成本。传统计算加密对应的解密过程涉及大量的计算，计算成本巨大。而在全息加密技术中，解密时只需在光路中使用正确状态的参考光或掩模即可，因此不存在传统加密技术中的解密速度问题。但全息加密存储系统也有自身局限。例如，使用掩模时，掩模的高选择性决定了解密时需精确对准掩模。为了解决解密过程对掩模对准精度要求高的问

题，研究者通常使用较简单的加密策略[88]、掩模调整技术[89]等。

5 密钥管理

双随机相位编码由于其相位分布的随机性，为加密存储系统提供了很大的密钥空间，因此系统具有极高的安全性。利用随机相位进行加密存储时，若每加密一张图像就需要一个密钥相位掩模，则该密钥相位掩模的数据量与所存储的数据量相当。因此，在实际应用中实现大量密钥的高效管理对加密存储系统具有重要的意义。

1991年，Denz等[96-97]基于离轴全息系统，提出了正交相位编码复用全息存储技术，在理论和实验上证明了该技术能确保记录再现的多幅图像间无串扰。此后，Heanue等[28]利用该技术发展了随机相位正交编码加密存储技术，利用像素尺寸为40 μm的随机相位板生成随机相位，再用相位型空间光调制器产生正交的相位调制量。在该技术中，只要存储一个随机相位板和每个正交变换序号，通过正交变换就可以生成不同密钥，因此大大减少了密钥所需的存储量。Li等[98]将可移动二维正交随机交织掩模用于全息存储，制作了一块像素为256×512的二维随机交织相位掩模，掩模板每移动一列就生成新的正交相位，由此通过单个相位掩模板生成了256个正交掩模。研究者利用正交参考光进行全息光存储的复用[99-100]，密钥管理时只存储一个密钥参考光分布，其他密钥可通过简单的转动角度实现。因此，正交编码技术可以通过正交变换实现成千上万个密钥的统一管理，密钥数据量由正交变换的阶数决定。

Situ等[83]利用一份随机密钥和一组可变参量菲涅耳域位置，实现了多幅图像的加密，该技术实现了密钥数据量的压缩。Tebaldi等[92]基于联合变换相关器原理，用分型波带片作为联合变换的另一个输入，用分型波带片的参数作为密钥，与随机相位掩模相比，密钥存储量减少。此外，波长[90-91]、空间位置[80-82]、偏转角度[101]等维度也可以用于减少双随机相位加密存储技术的密钥管理压力。曹非等[102]利用Toeplitz矩阵进行多个随机相位掩模的生成，将随机相位掩模的相位分布作为Toeplitz矩阵的一列，对于多个用户的掩模密钥传输，只需传输一个随机相位掩模。

但总体上，针对密钥空间数量，传统的正交变换、附加可变参量的方式提高密钥管理效率的能力有限。因此还需开发新型的、可管理更多密钥数量的高效密钥管理技术。

6 总结与展望

全息光存储利用光的多维可调制特性进行数据的加密存储，具有密钥空间巨大、存储介质中的光场状态不可探测等特点。全息加密光存储技术在物理存储层面实现加密，在数据加密方面有着天然的优势。当前全息加密光存储技术在利用相位调制及几何姿态实现加密方面取得了丰硕的成果。随机相位板为加密系统提供了海量的密钥空间，实现了数据的安全存储；利用随机相位掩模，结合波长、角度、位移等复用维度，可增大密钥空间，进而提升系统的安全性；密钥选择性决定了实际有效的密钥空间，一般随机相位掩模的随机性越强，掩模的相关长度越短，其密钥选择性越高，加密存储系统越安全。但关于偏振全息加密光存储、多维度的综合加密存储技术的研究还不够深入。由于偏振维度的调制灵活性大，具有较大的应用潜力，因此偏振维度的全息加密光存储是重要研究方向之一。另外，全息加密光存储系统的安全性分析研究较少，合理评估全息加密光存储系统的各项性能具有重要意义。此外，海量密钥的管理也是加密光存储在实际应用中的难题，如何高效实现密钥管理也是一个重要研究方向。近年来，高速发展的深度学习技术在各个领域中起到越来越重要的作用，未来可探索利用深度学习工具进行全息加密光存储系统的优化设计和安全性分析等。综上，全息加密光存储技术为海量数据的安全存储提供了重要保障，但仍有一些问题亟待解决。发展具有多维调制相结合、密钥选择性高、密钥易管理等特点的全息加密光存储技术对大数据时代的数据安全具有重要意义。

参 考 文 献

[1] van Heerden P J. Theory of optical information storage in solids[J]. Applied Optics, 1963, 2(4): 393-400.

[2] Leith E N, Kozma A, Upatnieks J, et al. Holographic data storage in three-dimensional media[J]. Applied Optics, 1966, 5(8): 1303-1311.

[3] Kogelnik H. Coupled wave theory for thick hologram gratings[J]. The Bell System Technical Journal, 1969, 48(9): 2909-2947.

[4] Sharnoff M. Storage capacity of holo-interferograms[J]. Applied Optics, 2003, 42(35): 7077-7084.

[5] 万玉红，袁韡，刘国庆，等. 光折变晶体全息存储中散射噪声特性的研究[J]. 中国激光，2003，30(6)：529-532.
Wan Y H, Yuan W, Liu G Q, et al. Study on the characteristics of scattering noise in photorefractive holographic storage[J]. Chinese Journal of Lasers, 2003, 30(6): 529-532.

[6] Hu P, Li J H, Jin J C, et al. Highly sensitive photopolymer for holographic data storage containing methacryl polyhedral oligomeric silsesquioxane[J]. ACS Applied Materials & Interfaces, 2022, 14(18): 21544-21554.

[7] Anderson K, Curtis K. Polytopic multiplexing[J]. Optics Letters, 2004, 29(12): 1402-1404.

[8] Horimai H, Tan X D, Li J. Collinear holography[J]. Applied Optics, 2005, 44(13): 2575-2579.

[9] Horimai H, Tan X D. Advanced collinear holography[J]. Optical Review, 2005, 12(2): 90-92.

[10] 李建华，曹良才，谭小地，等. 基于$LiNbO_3$晶体的透射式共光轴体全息存储技术[J]. 光学学报，2012，32(4)：0409001.
Li J H, Cao L C, Tan X D, et al. Transmission type of collinear volume holographic storage technology based on $LiNbO_3$ crystal[J].

Acta Optica Sinica, 2012, 32(4): 0409001.
[11] 林枭, 郝建颖, 郑明杰, 等. 光全息数据存储: 新发展时机已至[J]. 光电工程, 2019, 46(3): 180642.
Lin X, Hao J Y, Zheng M J, et al. Optical holographic data storage—the time for new development[J]. Opto-Electronic Engineering, 2019, 46(3): 180642.
[12] 万玉红, 陶世荃. 微全息存储技术及其研究进展[J]. 激光与光电子学进展, 2012, 49(10): 100004.
Wan Y H, Tao S Q. Micro-holographic data storage technology and its research progress[J]. Laser & Optoelectronics Progress, 2012, 49(10): 100004.
[13] 李建华, 刘金鹏, 林枭, 等. 体全息存储研究现状及发展趋势[J]. 中国激光, 2017, 44(10): 1000001.
Li J H, Liu J P, Lin X, et al. Volume holographic data storage[J]. Chinese Journal of Lasers, 2017, 44(10): 1000001.
[14] 刘金鹏, 许可, 刘金岩, 等. 相位调制的同轴全息存储[J]. 光电工程, 2019, 46(3): 180596.
Liu J P, Xu K, Liu J Y, et al. Phase modulated collinear holographic storage[J]. Opto-Electronic Engineering, 2019, 46(3): 180596.
[15] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
[16] Wang X Y, Yu H B. How to break MD5 and other hash functions [M]//Cramer R. Advances in cryptology-EUROCRYPT 2005. Lecture notes in computer science. Heidelberg: Springer, 2005, 3494: 19-35.
[17] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.
[18] 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.
[19] Javidi B, Sergent A, Zhang G S, et al. Fault tolerance properties of a double phase encoding encryption technique[J]. Optical Engineering, 1997, 36(4): 992-998.
[20] 于斌, 彭翔. 基于级联相位恢复算法的光学图像加密[J]. 光学学报, 2005, 25(7): 881-884.
Yu B, Peng X. Optical image encryption based on cascaded phase retrieval algorithm[J]. Acta Optica Sinica, 2005, 25(7): 881-884.
[21] 王志鹏, 马毛粉, 秦怡. 基于JTC和扩频技术的多二值图像光学加密技术[J]. 光电工程, 2014, 41(1): 54-59.
Wang Z P, Ma M F, Qin Y. Multiple binary images optical encryption technology based on JTC and spread spectrum technology[J]. Opto-Electronic Engineering, 2014, 41(1): 54-59.
[22] 刘杰, 白廷柱, 沈学举, 等. 联合变换相关器光学多图像并行加密系统稳健性分析与优化[J]. 光学学报, 2017, 37(12): 1210001.
Liu J, Bai T Z, Shen X J, et al. Robustness analysis and optimization of parallel encryption system for multi-channel images in an optical joint transform correlator architecture[J]. Acta Optica Sinica, 2017, 37(12): 1210001.
[23] Peng X A, Wei H Z, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain[J]. Optics Letters, 2006, 31(22): 3261-3263.
[24] 位恒政, 彭翔, 张鹏, 等. 双随机相位加密系统的选择明文攻击[J]. 光学学报, 2007, 27(5): 824-829.
Wei H Z, Peng X, Zhang P, et al. Chosen-plaintext attack on double phase encoding encryption technique[J]. Acta Optica Sinica, 2007, 27(5): 824-829.
[25] Peng X A, Zhang P, Wei H Z, et al. Known-plaintext attack on optical encryption based on double random phase keys[J]. Optics Letters, 2006, 31(8): 1044-1046.
[26] Javidi B, Carnicer A, Yamaguchi M, et al. Roadmap on optical security[J]. Journal of Optics, 2016, 18(8): 083001.
[27] Liao M H, Zheng S S, Pan S X, et al. Deep-learning-based ciphertext-only attack on optical double random phase encryption [J]. Opto-Electronic Advances, 2021, 4(5): 200016.
[28] Heanue J F, Bashaw M C, Hesselink L. Encrypted holographic data storage based on orthogonal-phase-code multiplexing[J]. Applied Optics, 1995, 34(26): 6012-6015.
[29] Wang J Y, Tan X D, Qi P L, et al. Linear polarization holography [J]. Opto-Electronic Science, 2022, 1(2): 210009.
[30] Hao J Y, Lin X A, Lin Y K, et al. Lensless complex amplitude demodulation based on deep learning in holographic data storage[J]. Opto-Electronic Advances, 2023, 6(3): 220157.
[31] Lin X A, Liu J P, Hao J Y, et al. Collinear holographic data storage technologies[J]. Opto-Electronic Advances, 2020, 3(3): 190004.
[32] Chen Y X, Hu P, Huang Z Y, et al. Significant enhancement of the polarization holographic performance of photopolymeric materials by introducing graphene oxide[J]. ACS Applied Materials & Interfaces, 2021, 13(23): 27500-27512.
[33] Li J H, Hu P, Jin J C, et al. Highly sensitive photopolymer for holographic data storage[J]. Optics Express, 2022, 30(22): 40599-40610.
[34] Tan X D, Matoba O, Shimura T, et al. Secure optical storage that uses fully phase encryption[J]. Applied Optics, 2000, 39(35): 6689-6694.
[35] Tan X D, Matoba O, Shimura T, et al. Improvement in holographic storage capacity by use of double-random phase encryption[J]. Applied Optics, 2001, 40(26): 4721-4727.
[36] Tan X D, Matoba O, Okada-Shudo Y, et al. Secure optical memory system with polarization encryption[J]. Applied Optics, 2001, 40(14): 2310-2315.
[37] Rakuljic G A, Yariv A, Leyva V. Optical data storage by using orthogonal wavelength-multiplexed volume holograms[J]. Optics Letters, 1992, 17(20): 1471-1473.
[38] John R, Joseph J, Singh K. Holographic digital data storage using phase-modulated pixels[J]. Optics and Lasers in Engineering, 2005, 43(2): 183-194.
[39] Yao B L, Ren Z W, Menke N, et al. Polarization holographic high-density optical data storage in bacteriorhodopsin film[J]. Applied Optics, 2005, 44(34): 7344-7348.
[40] Darsky A M, Markov V B. Angular sensitivity of holograms with a reference speckle wave[J]. Proceedings of SPIE, 1991, 1238: 54-62.
[41] Psaltis D, Curtis K, Levene M, et al. Holographic storage using shift multiplexing[J]. Optics Letters, 1995, 20(7): 782-784.
[42] Kim H, Lee Y H. Encryption of a volume hologram by complementary input image and binary amplitude mask[J]. Optics Communications, 2006, 258(1): 9-17.
[43] Toishi M, Hara M, Tanaka K, et al. Novel encryption method using multi reference patterns in coaxial holographic data storage [J]. Japanese Journal of Applied Physics, 2007, 46(6B): 3775-3781.
[44] 顾华荣, 赵瑱, 曹良才, 等. 用二值空间光调制器实现多灰阶全息存储[J]. 光学学报, 2010, 30(7): 2080-2083.
Gu H R, Zhao T, Cao L C, et al. Multi-gray-level holographic storage using a binary spatial light modulator[J]. Acta Optica Sinica, 2010, 30(7): 2080-2083.
[45] Javidi B, Zhang G S, Li J A. Encrypted optical memory using double-random phase encoding[J]. Applied Optics, 1997, 36(5): 1054-1058.
[46] Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain[J]. Optics Letters, 1999, 24(11): 762-764.
[47] Ahouzi E, Zamrani W, Azami N, et al. Optical triple random-phase encryption[J]. Optical Engineering, 2017, 56(11): 113114.
[48] Singh M, Kumar A. Optical encryption and decryption using a sandwich random phase diffuser in the Fourier plane[J]. Optical Engineering, 2007, 46(5): 055201.
[49] Su W C, Chen Y W, Chen Y J, et al. Security optical data

storage in Fourier holograms[J]. Applied Optics, 2012, 51(9): 1297-1303.
[50] Unnikrishnan G, Joseph J, Singh K. Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system[J]. Applied Optics, 2001, 40(2): 299-306.
[51] Mendlovic D, Zalevsky Z, Lohmann A W, et al. Signal spatial-filtering using the localized fractional Fourier transform[J]. Optics Communications, 1996, 126(1/2/3): 14-18.
[52] Nishchal N K, Unnikrishnan G, Joseph J, et al. Optical encryption using a localized fractional Fourier transform[J]. Optical Engineering, 2003, 42(12): 3566-3571.
[53] Nishchal N K, Joseph J, Singh K. Fully phase-encrypted memory using cascaded extended fractional Fourier transform[J]. Proceeding of SPIE, 2003, 5202: 106-113.
[54] Nomura T, Mikan S J, Morimoto Y, et al. Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator[J]. Applied Optics, 2003, 42(8): 1508-1514.
[55] Su W C, Sun C C. Review of random phase encoding in volume holographic storage[J]. Materials, 2012, 5(9): 1635-1653.
[56] Denz C, Müller K O, Visinka F, et al. Digital data storage and encryption using a phase-coded holographic memory system[C]// Advances in Photorefractive Materials, Effects and Devices, June 27, 1999, Elsinore, Denmark. Washington, D.C.: Optica Publishing Group, 1999: ODS2.
[57] Zhu Y C, Zhang J S, Yi T, et al. Signal and reference wave dually encrypted holographic memory with shift multiplexing[J]. Optics Communications, 2008, 281(6): 1450-1454.
[58] Mita A, Okamoto A, Funakoshi H. Effect of random phase mask on input plane in photorefractive authentic memory with two-wave encryption method[J]. Proceeding of SPIE, 2004, 5362: 61-68.
[59] Okamoto A, Mita A, Funakoshi H, et al. Secure holographic memory by two-wave encryption method with a photorefractive crystal[J]. Journal of Modern Optics, 2007, 54(4): 599-609.
[60] Kitano M, Okamoto A, Sano T. Security assessment of two-wave encryption[J]. Japanese Journal of Applied Physics, 2009, 48(3): 03A036.
[61] Lin X A, Huang Y, Li Y, et al. Four-level phase pair encoding and decoding with single interferometric phase retrieval for holographic data storage[J]. Chinese Optics Letters, 2018, 16(3): 032101.
[62] Vu T V, Lee S W, Kim N, et al. Secure holographic storage using single phase encoding[J]. Proceeding of SPIE, 2008, 6912: 691216.
[63] Lin X A, Hao J Y, Wang K, et al. Frequency expanded non-interferometric phase retrieval for holographic data storage[J]. Optics Express, 2020, 28(1): 511-518.
[64] Chen R X, Hao J Y, Yu C Y, et al. Dynamic sampling iterative phase retrieval for holographic data storage[J]. Optics Express, 2021, 29(5): 6726-6736.
[65] Hao J Y, Lin X, Lin Y K, et al. Lensless phase retrieval based on deep learning used in holographic data storage[J]. Optics Letters, 2021, 46(17): 4168-4171.
[66] Koppa P. Phase-to-amplitude data page conversion for holographic storage and optical encryption[J]. Applied Optics, 2007, 46(17): 3561-3571.
[67] Javidi B, Nomura T. Polarization encoding for optical security systems[J]. Optical Engineering, 2000, 39(9): 2439-2443.
[68] 林超, 沈学举, 杜霜, 等. 随机偏振光学加密算法的加密及解密特性分析[J]. 激光技术, 2014, 38(4): 515-521.
Lin C, Shen X J, Du S, et al. Characteristic analysis of encryption and decryption in random polarization optical encryption algorithm [J]. Laser Technology, 2014, 38(4): 515-521.
[69] Ujvari T, Koppa P, Loerincz E, et al. Phase-coded recording in polarization holograms for data multiplexing and encryption[J]. Proceeding of SPIE, 2000, 4149: 342-352.
[70] Ujvári T, Koppa P, Lovász M, et al. A secure data storage system based on phase-encoded thin polarization holograms[J]. Journal of Optics A: Pure and Applied Optics, 2004, 6(4): 401-411.
[71] Matoba O, Javidi B. Secure holographic memory by double-random polarization encryption[J]. Applied Optics, 2004, 43(14): 2915-2919.
[72] Davis J A, McNamara D E, Cottrell D M, et al. Two-dimensional polarization encoding with a phase-only liquid-crystal spatial light modulator[J]. Applied Optics, 2000, 39(10): 1549-1554.
[73] John R, Joseph J, Singh K. Phase-image-based content-addressable holographic data storage with security[J]. Journal of Optics A: Pure and Applied Optics, 2005, 7(3): 123-128.
[74] Barrera J F, Henao R, Tebaldi M, et al. Multiplexing encryption-decryption via lateral shifting of a random phase mask[J]. Optics Communications, 2006, 259(2): 532-536.
[75] Su W C, Sun C C, Su W C. Encryption-selectable holographic storage in $LiNbO_3$ with angle multiplexing[J]. Microwave and Optical Technology Letters, 2004, 42(3): 227-230.
[76] Matoba O, Javidi B. Encrypted holographic memory using angular multiplexing in $LiNbO_3$: Fe[J]. Proceeding of SPIE, 1999, 3804: 172-179.
[77] Matoba O, Javidi B. Encrypted optical storage with angular multiplexing[J]. Applied Optics, 1999, 38(35): 7288-7293.
[78] Jia W, Chen Z Y, Wen F J, et al. Single-beam data encoding using a holographic angular multiplexing technique[J]. Applied Optics, 2011, 50(34): H30-H35.
[79] Xi S X, Yu N N, Wang X L, et al. Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram[J]. Optics and Lasers in Engineering, 2020, 127: 105953.
[80] Sun C C, Su W C, Wang B, et al. Lateral shifting sensitivity of a ground glass for holographic encryption and multiplexing using phase conjugate readout algorithm[J]. Optics Communications, 2001, 191(3/4/5/6): 209-224.
[81] Chang C C, Hu G W, Lin C Y, et al. Encrypted holographic memory using rotationally random phase encoding[C]// Photorefractive Effects, Materials, and Devices, July 8, 2001, Delavan, Wisconsin. Washington, D.C.: Optica Publishing Group, 2001: 188.
[82] Su W C, Lin C H. Three-dimensional shifting selectivity of decryption phase mask in a double random phase encoding holographic memory[J]. Optics Communications, 2004, 241(1/2/3): 29-41.
[83] 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.
[84] Sun C C, Hsu C Y, Ma S H, et al. Rotation selectivity of random phase encoding in volume holograms[J]. Optics Communications, 2007, 276(1): 62-66.
[85] Hu G W, Chang C C, Lin C Y, et al. Hybrid holographic multiplexing for data storage and application to optical encryption [J]. Japanese Journal of Applied Physics, 2002, 41(Part 2, No. 5A): L518-L520.
[86] Sarkadi T, Koppa P. Quantitative security evaluation of optical encryption using hybrid phase- and amplitude-modulated keys[J]. Applied Optics, 2012, 51(6): 745-750.
[87] Su W C, Sun C C, Chen Y C, et al. Duplication of phase key for random-phase-encrypted volume holograms[J]. Applied Optics, 2004, 43(8): 1728-1733.
[88] Chang C C, Chen G L, Young W K, et al. Deterministic phase encoded holographic data storage using lenticular lens array[J]. Optical Review, 2007, 14(4): 214-218.
[89] Su W H, Su W C, Kao H J, et al. Correlator-aided alignment of phase key in encrypted holographic storage systems[J]. Optics Communications, 2007, 280(1): 27-32.
[90] Matoba O, Javidi B. Encrypted optical storage with wavelength-

key and random phase codes[J]. Applied Optics, 1999, 38(32): 6785-6790.
[91] Zhang G P, Chen S J, Zhu Z R. Optical data storage with double random phase codes and wavelength encryption[J]. Proceeding of SPIE, 2002, 4930: 536-543.
[92] Tebaldi M, Furlan W D, Torroba R, et al. Optical-data storage-readout technique based on fractal encrypting masks[J]. Optics Letters, 2009, 34(3): 316-318.
[93] Sheeja M K, Ajith Kumar P T, Achuthsankar S N. Photopolymer-based holographic variable data storage system for security applications[J]. Proceeding of SPIE, 2006, 6352: 635224.
[94] Sando D, Jaatinen E. Optical data encryption using time-dependent dynamics of refractive index changes in $LiNbO_3$[J]. Optics Express, 2013, 21(17): 19510-19517.
[95] Wang B, Chang J Y, Su W C, et al. Optical security using a random binary phase code in volume holograms[J]. Optical Engineering, 2004, 43(9): 2048-2052.
[96] Denz C, Pauliat G, Roosen G, et al. Volume hologram multiplexing using a deterministic phase encoding method[J]. Optics Communications, 1991, 85(2/3): 171-176.
[97] Denz C, Pauliat G, Roosen G, et al. Potentialities and limitations of hologram multiplexing by using the phase-encoding technique[J]. Applied Optics, 1992, 31(26): 5700-5705.
[98] Li J H, He M Z, Zheng T X, et al. Two-dimensional shift-orthogonal random-interleaving phase-code multiplexing for holographic data storage[J]. Optics Communications, 2011, 284(24): 5562-5567.
[99] Li J H, Cao L C, Gu H R, et al. Orthogonal-reference-pattern-modulated shift multiplexing for collinear holographic data storage [J]. Optics Letters, 2012, 37(5): 936-938.
[100] Cao L C, Liu J Q, Li J H, et al. Orthogonal reference pattern multiplexing for collinear holographic data storage[J]. Applied Optics, 2013, 53(1): 1-8.
[101] 刘杰, 白廷柱, 沈学举, 等. 基于联合功率谱分区复用的光学多图像加密方法与实验[J]. 中国激光, 2018, 45(12): 1209003.
Liu J, Bai T Z, Shen X J, et al. Optical multi-image encryption method and experiment based on joint power spectrum partition multiplexing[J]. Chinese Journal of Lasers, 2018, 45(12): 1209003.
[102] 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.
Cao F, Zhao S M. Optical encryption scheme with double secret keys based on computational ghost imaging[J]. Acta Optica Sinica, 2017, 37(1): 0111001.

Multi-Modulated Holographic Encrypted Optical Storage

Lin Dakui[1,2,3,4,5], Song Haiyang[1,2,3,4,5], Li Jianan[1,2,3,4,5], Wang Kun[1,2,3,4,5], Lin Xiao[1,2,3,4,5], Tan Xiaodi[1,2,3,4,5*]

[1]*College of Photonic and Electronic Engineering, Fujian Normal University, Fuzhou* 350117, *Fujian, China*;
[2]*Key Laboratory of Opto-Electronic Science and Technology for Medicine of Ministry of Education, Fuzhou* 350117, *Fujian, China*;
[3]*Fujian Provincial Key Laboratory of Photonics Technology, Fuzhou* 350117, *Fujian, China*;
[4]*Fujian Provincial Engineering Technology Research Center of Photoelectric Sensing Application, Fuzhou* 350117, *Fujian, China*;
[5]*Information Photonics Research Center, Fujian Normal University, Fuzhou* 350117, *Fujian, China*

Abstract

Significance The era of big data has presented new demands for mass data storage, and data storage security is critical to social stability and development. Holographic optical storage has not only become a powerful solution for mass data storage because of its high storage density, fast reading speed, and long storage life, but also provides an effective encryption means to ensure data storage security by utilizing the multi-dimensional modulated characteristics of light. Holographic encrypted optical storage has many advantages, including multiple adjustable parameters, a large key space, and a complex storage state in material. By modulating reference or information light, it can prevent unauthorized users from obtaining data and thus can provide a sufficient guarantee for safe data storage.

Progress Since double-random phase encoding was first used in optical encryption in the early 1990s, holographic encrypted optical storage has developed rapidly. In general, encrypted optical storage can be divided into four categories. First, as shown in Fig. 2, holographic encrypted optical storage can be realized by amplitude modulation. Specific reference and information light encoded with different amplitudes are recorded in the same position of the material. Only the correct amplitude reference light can reconstruct the stored information when reading, whereas the wrong amplitude reference light will reproduce only a portion of the information of multiple data pages and interfere with each other, and thus the correct information will not be obtained. Second, as shown in Fig. 3, holographic encrypted optical storage is realized through phase modulation. Specifically, a random phase plate can be placed on the image plane and Fourier plane of the information light to realize phase encryption. Only by mastering the mask in the optical path can the information be accurately reproduced. Here, the same encryption process can be implemented for reference light. In addition, phase modulation can be extended to the Fresnel and fractional Fourier transform domains to increase the security of the encryption system. Third, as shown in Fig. 4, holographic encrypted optical storage can be achieved through polarization modulation. The polarization data page is used to represent the original data, and the polarization state modulation is performed on the polarization data page with the polarization mask to realize polarization encryption. The encrypted polarization information is then stored in the polarization response recording medium. Decryption requires using an inverse polarization mask to reconstruct the original data.

Fourth, as shown in Fig. 5, encrypted optical storage can be realized through geometric attitude modulation of the optical path, specifically by changing the location, angle, and other parameters of the mask. To increase the security of encrypted storage systems, simultaneous encryption of multi-dimensional modulation parameters has become a trend and shown great potential.

Conclusions and Prospects Holographic encryption optical storage technology implements encryption at the physical storage level and has natural advantages in terms of data encryption. Currently, research on holographic encryption optical storage technology using phase modulation and geometric attitude has achieved fruitful results. However, the research on polarization holographic encryption optical storage and multi-dimensional integrated encryption optical storage technology remains insufficient. In addition, security analyses of holographic encrypted optical storage systems are scarce. Therefore, obtaining methods for reasonably evaluating the performance of holographic encrypted optical storage systems is of great significance.

Key words holography; holographic storage; holographic encrypted optical storage; multidimensional modulation of light; storage security