基于单像素成像的函数加密方法研究综述

杨寒冰
华北水利水电大学　电子工程学院　河南郑州　450046

摘　要：本文全面探讨了基于单像素成像的函数加密这一前沿且极具挑战性的领域。详细阐述了其研究背景，系统梳理了国内外在函数加密、单像素成像及二者结合方向的研究现状，客观评述了相关文献成果，并展望了未来发展方向。旨在为该领域的学术研究与实际应用提供坚实的理论支撑与实践指引。

关键词：单像素成像；函数加密；公钥加密

引言

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。本课题主要研究的是网络信息安全，保证其中的数据信息不被篡改、非法增删、复制、解密、显示、使用等。这也是保障网络安全最根本的目的。访问控制作为解决授权用户合法访问数据的关键技术，近年来已被引入大数据领域保障数据安全共享[1]，为适用于复杂开放的云计算环境，诸多学者关注云环境下的访问控制密码技术。函数加密克服了公钥加密所固有的“全有或全无”的访问，即原来解密的结果或者是明文或者是不泄露任何明文信息。简单地说，函数加密中拥有解密密钥的用户，可以获得的秘密数据的函数值，即不会获得其他有关明文的任何信息。可以实现对数据细粒度的访问控制，但其加解密速率较慢，实现需要高级的数学算法和计算机，实用性较差。研究函数加密领域，关键在于能否在保证安全的前提下，减少密文膨胀，提高函数加密系统的实用性，单像素成像因其天然的并行性和高速率受到当前许多研究者的关注，二者的相关机理进行结合可以优化函数加密系统的性能。

一、国内外研究现状

（一）研究现状及发展动态

近年来，函数加密成为公钥密码学中研究的热点话题。2005年欧密会上首次提出的《模糊身份加密方案》中基于属性加密（Attribute-Based Encryption，ABE）这一概念[2]。在一个基于属性加密的方案（密钥策略或密文策略）中，加密明文消息时，通过为密文选择属性集合使得密文和这一属性关联起来，当且仅当与密文相关联的属性集合和用户的属性集合相交的元素达到某一设定的门限值时，用户才能解密。早期的函数加密一般指的就是这种类型的属性加密、身份加密和谓词加密等。而“函数加密”一词最早来自于2008年Sahai和Waters的一次讨论中，直到2011年Waters等人才给出具体的形式化定义，并提出了函数加密语义安全下基于模拟和不可区分游戏模型的定义。

函数加密成为公钥密码学研究的热点问题，大多数集中在自适应性安全性证明、密钥撤销多个可信中心提高函数的隐私性以及函数加密定义的研究等上面，并取得了一些好的研究成果。2013年Goldwasser等人结合Yao的混淆电路提出了以全同态加密（fully homomorphic encryption）为基础的满足对任意函数可行的函数加密方案，Tatsuaki Okamoto等人[3]提出的内积加密方案中，当且仅当与密文相关的向量Z和与解密密钥相关的向量R的内积为0，即R，Z=0时，才能解密得到明文m，否则解密失败；基于传统的公钥加密，Abdall等人首次提出了满足线性密钥同态和线性密文同态的函数加密方案，在他们的方案中定义的明文空间较小，解密可得到相关的具体函数，即拥有与向量$\vec{y}$相关的密钥SK$\vec{y}$的用户通过解密由向量$\vec{x}$加密后的密文CT，得到内积函数$\langle \vec{x}, \vec{y} \rangle$，而不是原具体的明文$\vec{x}$。内积加密是函数加密的一种特殊情况，它支持向量内积的运算。内积函数加密对涉及隐私保护内积计算的应用具有重要的意义。具体来说，内积函数加密可以用于隐私保护的统计分析、外包

作者简介：杨寒冰（2000—），女，汉族，河南开封人，硕士，研究生，研究方向为单像素成像及其加密。

计算、加密生物特征认证和机器学习等场景中。目前，已有许多工作研究了内积函数加密方案的构造方法，但现有的内积函数加密方案在效率、安全性、灵活性和实用性方面还存在不足。大部分方案在解密时需要求解离散对数问题，当加密数据较大时，往往解密效率较低；目前能实现不可区分性安全或模拟安全的方案还较少；大多数方案都是静态的，即方案所支持的用户数量是固定的，不支持用户的动态加入与退出，这使得内积函数加密的灵活性较差；传统的内积函数加密存在固有的缺陷，即通过线性无关的向量所对应的解密密钥可以将明文完全恢复出来。这使得内积函数加密的实用性较差。如何设计更高效、更安全、更灵活、更实用的内积函数加密方案仍是一个难题。

光学信息处理技术由于其并行性和高速度的特性受到了国内外研究者的关注。1995年Refergier和Javidi提出了双随机相位编码（DRPE）的光学图像加密系统，他们在4f光学系统中通过两个分别位于空域和频域的相互独立的随机相位掩膜（RPM）将明文图像加密为平稳白噪声图像，两个RPM被当作密钥，该方法可以称为光学图像加密领域的经典——双随机相位编码（DRPE）[4]。然而当使用DRPE加密图像、相位掩膜作为密钥时，仅使用频域相位解密就可以得到含有铭文轮廓的图像。因此对于传统基于傅里叶变换的DRPE，密钥空间小和固有的线性使其极易遭受非法攻击。

单像素成像，是利用没有空间分辨能力的单像素桶探测器进行成像的技术，1995年马里兰大学的史延华团队完成了用量子纠缠光源进行的单像素成像实验，随后，2002年，罗切斯特大学的R.Boyd团队通过实验证明了使用经典光源也可实现鬼成像，从而得出鬼成像不需要量子纠缠，这种方法被称为热光鬼成像[5]。2008年，麻省理工学院的J.H.Shapiro教授提出计算鬼成像，他们首先根据标量衍射理论预先计算电荷耦合器件CCD在鬼成像实验中记录的光强分布，然后仅使用一个单像素检测器完成实验。

单像素成像根据光源类型可以分为随机光单像素成像和结构光单像素成像[6]。在随机光单像素成像中，其使用随机相位掩摸（RPM）调制的照明光照射成像物体，通过关联算法重构图像，为了重建高质量的图像，这种方法要求不同照明光对目标物体进行多次单像素测量，耗费了大量时间，成像效率低，后来研究人员提出了基于压缩感知鬼成像方法，该方法基于压缩感知原理，通过一个传感矩阵将稀疏域中的目标图像编码改为强度值序列，使用凸优化算法重构图像。然而常见的压缩感知重构算法需要多次迭代求解最优值，需要大量时间。相比于随机光单像素成像，结构光单像素成像则用结构相位掩模调制的照明光照射物体，结构光（如Hadamard基图案、傅里叶基图案和离散余弦基图案等）由于其完备的正交性使得相同的测量次数，其成像质量要明显优于随机光单像素成像，并且可以在欠采样的情况下高质量地恢复图像。如2014年Zhang等人提出了一种基于傅里叶频谱的单像素成像技术，该方案通过一系列傅里叶基图案照射成像物体，根据单像素探测器采集到的总光强重构频谱后执行二维傅里叶逆变换恢复图像，图像重构时间可忽略不记，并且其可以在低频采样下高质量成像，虽然该方案使用四步相移和差分测量方法有效去除了环境光和直流分量的影响，但成像时间仍然不容乐观，严重影响了其实际应用。2016年，Wang等人提出了一种基于Walsh-Hadamard变换快速单像素成像技术，他们利用Walsh-Hadamard图案光照射物体产生一个检测结果对，并对其进行差分变换处理，最后通过对差分结果进行快速Walsh-Hadamard变换来恢复物体的图像。

基于光学理论和方法的信息安全技术具有快速并行数据处理能力、多维度、大容量、高鲁棒性、大密钥空间等独特优势，使其成为当前信息安全的一个新兴领域和研究热点[7]。近年来，随着理论、实验及相关技术的积累，单像素成像技术在实际应用方面获得了实质性进展。目前函数加密的应用涉及其他功能的函数加密、可搜索加密、加密数据线性回归、加密生物特征认证、外包计算、隐私保护机器学习等。

（二）研究问题在本研究领域应用上的地位与价值

综上所述，国内外学者针对图像加密技术已经做了大量的研究，但是，函数加密系统的安全性、实用性、密文膨胀等问题仍有待提升。单像素成像具备并行性和高速率的特点，跟函数加密机理进行结合，可以改善函数加密目前存在的缺点。因此本课题的应用价值在于通过基于单像素成像的函数加密方法研究，提高函数加密算法的性能，减少加密中数据拓展并实现对加密数据的细粒度访问[8]。

二、文献评述

纵观现有文献，在函数加密领域，众多学者围绕安全性、效率、灵活性等核心问题展开了深入研究，取得了丰硕成果。从理论层面的形式化定义完善到实际应用中的加密方案创新，都为函数加密技术的发展奠定了坚实基础。然而，不可忽视的是，当前函数加密系统仍然

面临着诸多棘手难题，如内积函数加密方案在效率、安全性、灵活性和实用性方面的短板，严重制约了其大规模推广与应用。大部分内积函数加密方案在解密时需要求解离散对数问题，当加密数据量庞大时，解密效率急剧下降，成为制约系统性能的瓶颈；在安全性方面，能够实现高标准不可区分性安全或模拟安全的方案凤毛麟角，难以抵御复杂多变的攻击手段；灵活性欠佳，多数方案为静态设计，无法适应动态变化的用户环境，不支持用户的动态加入与退出；实用性受限，传统内积函数加密存在严重缺陷，通过线性无关的向量所对应的解密密钥可以将明文完全恢复出来，使得加密数据的保密性大打折扣。

在单像素成像领域，从早期的开创性实验到如今多样化的技术分支发展，研究人员付出了巨大努力，为该技术的成熟与应用积累了丰富经验[9]。不同类型的单像素成像技术各有优劣，随机光单像素成像虽然原理简单，但成像效率问题始终困扰着研究者；结构光单像素成像在成像质量上有显著提升，但在应对复杂场景时，仍需进一步优化成像稳定性与适应性。此外，光学信息处理技术在信息安全应用中的探索也取得了一定进展，如双随机相位编码（DRPE）光学图像加密系统的提出为图像加密提供了新思路，但同样面临着密钥安全性提升等后续问题[10]。

值得欣慰的是，已有部分学者敏锐地捕捉到函数加密与单像素成像技术结合的潜在价值，并开展了初步探索。他们试图将单像素成像的独特优势融入函数加密体系，以弥补函数加密当前存在的不足。然而，目前这方面的研究仍处于起步阶段，尚未形成完善的理论体系与成熟的应用方案。多数研究仅聚焦于二者结合的某一局部问题，缺乏对整体架构、性能优化以及实际应用场景的全面考量，距离实现高效、安全、实用的基于单像素成像的函数加密系统仍有很长的路要走。

结论

综上所述，基于单像素成像的函数加密研究处于多学科交叉的前沿阵地，既承载着解决传统加密技术困境的厚望，又面临着函数加密与单像素成像各自技术瓶颈以及二者深度融合难题的多重挑战。通过对现有研究现状的全面梳理与文献评述，我们清晰地认识到，未来需要进一步加强跨学科协作，整合光学、密码学、信息论等多学科知识，深入挖掘单像素成像在函数加密中的潜在应用价值。一方面，持续优化函数加密算法，攻克内积函数加密现存的效率、安全性、灵活性和实用性难题；另一方面，不断改进单像素成像技术，提升其成像质量、效率与稳定性，使其更好地适配加密需求。同时，注重理论研究与实际应用的紧密结合，针对云计算、物联网、大数据等具体应用场景，量身定制基于单像素成像的函数加密解决方案，推动该领域从理论探索迈向广泛的实际应用，为信息安全防护铸就一道坚不可摧的屏障。

在未来的研究中，还应密切关注新兴技术的发展动态，如量子计算、人工智能等，积极探索这些技术与基于单像素成像的函数加密方法的融合可能性，提前布局应对潜在的安全挑战，确保信息安全技术始终走在时代前列。相信随着研究的不断深入，基于单像素成像的函数加密技术必将在信息安全领域绽放出耀眼光芒，为数字化社会的蓬勃发展保驾护航。

参考文献

[1]Qian Wen-Jun，Shen Qing-Ni, Wu Peng-Fei, et al. Research progress on privacy-preserving techniques in big data computing Chinese Journal of Computers，2022，45(4) environment.669-701(in Chinese)

[2]John B, Amit S, Brent W. Ciphertext-policy attribute-based encryption [J]. In IEEE Symposium on Security and Privacy ,2007:321-334

[3]Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhan dry. Fully secure functional28encryption without obfuscation. Technical report, Cryptology e Print Archive, Report2014/666，2014.

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

[5]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.

[6]刘瑞丰，赵书朋，李福利.单像素复振幅成像（特邀）[J].红外与激光工程，2021，50（12）：20210735.

[7]苏杰，翟爱平，赵文静，韩青，王东.自适应斜Z字形采样Hadamard单像素成像[J].光子学报，2021，50（3）：22.

[8]姚昱.基于单像素成像的边缘提取技术研究[D].长春理工大学，2024.

[9]管擎天.单像素成像信号中的源分离分析与应用[D].合肥工业大学，2023.

[10]苏恒志.单像素成像技术及其在边缘检测中的应用[D].北京邮电大学，2023.