云辅助物联网环境下可验证的安全图像检索

郭佳琦，马智，王文胜，田聪，段振华
（西安电子科技大学计算机科学与技术学院，陕西 西安 710071）

摘　要：针对现有的云辅助物联网环境中图像检索精度和效率低、服务器潜在恶意性问题，提出一种可验证的安全图像检索方案。采用矩阵形式的索引和查询，结合基于容错学习的改进安全k近邻算法加密特征矩阵，提升索引和查询安全性。利用区块链技术，并结合四叉默克哈希树和高效短签名，实现搜索结果的可验证性。安全性和性能分析表明，所提方案在保证索引和查询安全性的同时，显著降低了索引和查询的加密计算复杂度及密钥存储开销。所提方案在提高图像检索精度和安全性的同时，优化了计算与存储资源，适用于云辅助物联网环境。

关键词：图像安全检索；安全k近邻算法；容错学习问题；物联网
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025050

Verifiable secure image retrieval for cloud-assisted IoT environments

GUO Jiaqi, MA Zhi, WANG Wensheng, TIAN Cong, DUAN Zhenhua
School of Computer Science and Technology, Xidian University, Xi’an 710071, China

Abstract: To address the challenges of low accuracy and efficiency in image retrieval, as well as the potential malicious behavior of servers in cloud-assisted Internet of things (IoT) environments, a verifiable and secure image retrieval scheme was proposed. A matrix-based approach was employed for indexing and querying, and the feature matrix was encrypted using an enhanced secure k-nearest neighbor (kNN) algorithm based on the learning with errors (LWE), ensuring improved security in indexing and querying. Blockchain technology was integrated with the quad Merkle Hash tree and efficient short signature to enable the verifiability of search results. Security and performance analyses demonstrated that the security of indexing and querying was ensured by the proposed scheme while the encryption computational complexity and key storage overhead were reduced. The proposed scheme improves image retrieval accuracy and security while optimizing computational and storage resources, making it suitable for cloud-assisted IoT environments.

Keywords: secure image retrieval, secure kNN algorithm, LWE problem, IoT

0　引言

物联网（IoT, Internet of things）作为现代社会的重要组成部分，广泛应用于生活、医疗、农业、工业等领域。如图1所示，各类物联网设备持续生成海量图像数据。由于本地存储空间有限，云存储逐渐成为物联网环境的核心解决方案。然而，将数据上传至云服务器会导致数据所有者失去对数据的直接控制，引发隐私和安全问题。尽管加密可以有效保护数据安

收稿日期：2024–12–31；**修回日期：**2025–03–07
通信作者：田聪，ctian@mail.xidian.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2018AAA0103202）；国家自然科学基金资助项目（No.62402372, No.62202371, No.62192730, No.62192734）
Foundation Items: The National Key Research and Development Program of China (No.2018AAA0103202), The National Natural Science Foundation of China (No.62402372, No.62202371, No.62192730, No.62192734)

全，但加密后的数据难以支持图像检索等常见操作。具体来说，基于内容的图像检索（CBIR, content-based image retrieval）[1-2]技术在明文环境中表现优异，但加密数据的随机性，相似性难以度量，因此无法直接应用于密文环境。为此，设计实用的密文图像检索方案对于物联网的广泛应用至关重要。

图 1　物联网与云计算

可搜索加密技术[3]为密文检索提供了可能，研究人员陆续提出基于可搜索加密的安全图像检索方案。Lu 等[4]首次提出一个基于保序加密和最小哈希的安全图像检索方案，该方案采用视觉特征词来描述图像，搜索精度较低。近年来，随着深度学习的迅速发展，基于卷积神经网络（CNN, convolution neural network）的特征提取方法逐渐取代传统方法，提升了搜索精度。基于安全 k 近邻（kNN, k-nearest neighbor）算法[5]的 CBIR 方案由于其高效性，得到学术界和工业界的广泛关注。然而，根据 Yao 等[6]的安全分析，普通的安全 kNN 算法无法抵抗线性分析攻击，在实际应用中存在安全隐患。因此，在基于容错学习（LWE, learning with errors）[7]问题的 k 均值聚类方案[8]的启发下，Li 等[9]使用基于 LWE 的安全 kNN 算法对 CNN 模型提取的图像特征进行加密，但该方案的索引向量与密钥矩阵的大小都会在图像特征向量增大时给物联网设备带来存储和计算上的压力。此外，鉴于云服务器可能因利益驱动而删除或篡改存储内容，使用默克哈希树（MHT, Merkle Hash tree）验证搜索结果是一种可行的方法[9-10]。然而，用户使用现有的方法自行验证会增加物联网设备的资源消耗，而引入第三方机构[11]进行验证则可能带来新的安全风险，例如第三方与云服务器合谋获取隐私内容。此外，这些验证方案尚未考虑验证失败后的应对措施。

总体来说，在云辅助物联网环境中构建轻量级的安全图像检索方案仍面临以下几个关键挑战。首先，传统的基于手动图像特征提取的方案依赖预定义的规则和参数，缺乏灵活性且精度不足，无法满足高查询精度的需求。其次，加密索引和查询中常用的安全 kNN 算法存在安全漏洞，难以抵抗线性攻击。虽然改进后的安全 kNN 算法提升了安全性，但其索引和密钥的大小与特征向量维数成正比，在特征向量维数增大时会导致存储和计算开销过大，对资源受限设备造成过重负担。最后，传统的结果验证方案在实际操作中同样会加剧物联网设备的资源消耗，且缺乏有效的恢复机制可能会影响设备的正常运作和决策可靠性。

针对上述挑战，本文采用预训练的 CNN 模型更准确地表达图像，同时更快地构建索引，提高检索准确性。将特征向量转换为矩阵形式并计算矩阵间的哈达玛积，从而有效计算特征向量之间的相似性，降低存储和计算开销。对基于 LWE 的安全 kNN 算法进行改进后应用于矩阵加密，提高对线性攻击的抵抗能力。基于四叉 MHT（4-MHT）和高效短签名构造结果验证方案，由分布式、防篡改的区块链替代第三方审计中心存储并验证根节点签名，并提供验证失败后的处理措施，安全、高效地实施结果验证。基于以上具体算法和技术，本文提出一个云辅助物联网环境下可验证的安全图像检索方案，主要贡献如下。

1) 设计基于矩阵哈达玛积的安全 kNN 算法，利用 CNN 模型构建的索引向量和查询向量，通过矩阵哈达玛积实现高效的相似性计算。支持图像所有者和用户快速生成安全索引和查询，并显著提升云服务器的检索效率和结果精度。

2) 构建基于区块链的结果验证机制，结合 4-MHT 和高效短签名算法实现高效验证，确保验证结果的可信性的同时消除传统验证方式对用户设备资源的额外消耗。

3) 对所提方案进行安全性分析，证明其在已知密文模型和背景模型中均能保证索引和查询的安全性。对所提方案进行理论和实验分析，将其存储代价和计算代价与其他典型方案对比，验证其高效

性适用于资源受限的物联网设备。

1 相关工作

早期关于密文图像检索，如Lu等[4]提出的基于保序加密和最小哈希的隐私保护CBIR方案，尽管采用了视觉特征词描述图像，但在查询精度方面仍显不足。此外，尽管其他方案通过采用不同的图像特征提取技术如多媒体内容描述接口[12-13]、局部不变特征[14-15]等来提高效率，但这些基于传统特征提取方式的方案，普遍存在搜索精度低的问题。近年来，随着深度学习的兴起，CNN作为一种能够自动从数据中学习特征的强大工具，已被广泛应用于图像检索中。Yang等[16]采用视觉几何组16层网络（VGG16, visual geometry group 16-layer network）模型提取图像的特征，Li等[17]则采用50层残差网络（ResNet50, residual network with 50 layer）模型提取图像特征，这些经典的CNN模型能够有效地提取图像的高层次语义特征，相比传统的手工设计特征，显著提高了检索精度。

在加密方式的选取上，基于同态加密[18-19]或代理重加密[20-21]等复杂的加密方式，虽然能提供较高的安全性，但极高的计算成本限制了其在资源受限的物联网设备上的应用。为了提高安全检索的效率，相比之下，基于安全kNN的隐私保护CBIR方案在保证安全性的同时，依然维持了较高的搜索效率。Li等[22]使用CNN模型从图像中提取特征并转换为二进制编码，进一步通过安全kNN进行加密，不仅提高了搜索精度，也降低了存储和通信成本。Zhu等[23]设计了一种基于马氏距离比较的方法以抵抗已知背景攻击。Li等[17]使用k均值聚类法提高图像的检索效率。然而，Yao等[6]的安全分析指出，普通的安全kNN算法在实际应用中无法抵抗线性分析攻击。对此问题，Yuan等[8]提出了一种基于LWE的k均值聚类方案，该方案在已知密文模型和已知背景模型中都能有效抵御线性分析攻击。鉴于搜索方案和聚类方案之间的相似性，Li等[9]基于相同的LWE假设，采用CNN模型提取图像特征，在多所有者和多用户模型中提出了一种隐私CBIR方案。Song等[24]采用一个预定义的相似性阈值来防止相似性得分顺序的泄露。Khan等[10]考虑了更多的方案特性如访问控制、结果验证和动态更新，增强了图像搜索的安全性和功能性。Gu等[25]针对实用的多源数据场景，提出适用于该场景的安全检索方案。李颖莹等[26]在边缘计算环境中考虑了支持不同密钥加密的图像集的搜索情况。宋甫元等[27]通过引入矩阵变换和代理重加密，实现了多用户环境下的密文图像检索，这些方案进一步丰富了安全图像检索的使用环境。

考虑到云服务器可能存在潜在的恶意行为，如删除或篡改存储内容，Zhang等[28]基于属性加密、盲签名以及布隆过滤器提供细粒度的访问控制和结果验证。文献[9-10]中的方案则通过构造MHT完成结果验证可以确保搜索结果的正确性和完整性。然而，用户自行验证可能会增加资源受限设备的负担，使得部署变得困难。因此，Lu等[11]引入第三方机构来代替资源受限的物联网设备进行验证，但这也可能带来新的安全风险和隐私泄露问题。Li等[17]基于变色龙哈希和BLS（Boneh-Lynn-Shacham）签名对搜索结果构造了一个自适应验证框架。Liu等[29]针对数据共享和审计安全，提出了结合区块链的审计技术，保证安全的基础上节省了计算资源。陈建伟等[30]在智能电网数据共享的环境中，设计新的签名算法并利用区块链的不可篡改性，确保了数据的真实性和完整性。得益于区块链的去中心化和不可篡改的特性，基于区块链的无可信第三方的验证框架，给物联网环境中的数据完整性验证带来了新的机遇。

然而，上述现有方案要在云辅助物联网环境中使用，普遍存在搜索精度低、加密和验证效率不足的情况。本文通过CNN模型提取图像特征，改进安全kNN算法用于矩阵形式的索引和查询，结合四叉MHT和高效短签名算法，提出云辅助物联网环境下可验证的安全图像检索方案。

2 预备知识

本节给出哈达玛积、LWE问题和4-MHT的相关定义。

2.1 哈达玛积

定义1 给定2个行列数相同的矩阵$\boldsymbol{X}$和$\boldsymbol{Y}$，$\boldsymbol{Z}=\boldsymbol{X}\circ\boldsymbol{Y}$表示$\boldsymbol{X}$和$\boldsymbol{Y}$的哈达玛积。矩阵$\boldsymbol{Z}$中的元素可以表示为$\boldsymbol{Z}_{ij}=\boldsymbol{X}_{ij}\boldsymbol{Y}_{ij}$。矩阵$\boldsymbol{Z}$的所有元素之和定义为$\mathrm{sum}(\boldsymbol{Z})$。

2.2 LWE问题

定义2 给定多项式个采样$\boldsymbol{a}\in\mathbb{Z}_q^m$，$b\in\mathbb{Z}_q$，满足

$$b = \boldsymbol{x} \cdot \boldsymbol{a} + r \tag{1}$$

其中，$\mathbb{Z}_q$表示q阶整数域，q是系统选定的大素数。误差项r是从特定概率分布中随机提取的，恢复$\boldsymbol{x}$被称为LWE问题[7]，以不可忽略的概率求解LWE问题在计算上是不可行的。

2.3　4-MHT

4-MHT是传统默克哈希树[31]的一个变体。在4-MHT结构中，每个叶节点存储数据的哈希值，而每个非叶节点则存储其4个孩子的哈希值。与传统的二叉默克哈希树（2-MHT）类似，任何数据的更改都会引起根节点哈希值的变化，因此可以利用根节点的哈希值来验证数据的完整性。

图2为4-MHT生成和验证示例，共有16个数据$\{c_1,c_2,\cdots,c_{16}\}$，首先生成16个叶节点$H_1 = H(c_1), H_2 = H(c_2), \cdots, H_{16} = H(c_{16})$。随后，根据叶节点生成非叶节点$H_{1\sim4} = H(H_1\|H_2\|H_3\|H_4)$，以此类推生成$H_{5\sim8}$，$H_{9\sim12}$，$H_{13\sim16}$。最后，生成根节点$H_{1\sim16} = H(H_{1\sim4}\|H_{5\sim8}\|H_{9\sim12}\|H_{13\sim16})$，4-MHT生成完毕。如果验证其中一个数据，例如$c_1$，需要的辅助信息包括$\{H_2,H_3,H_4,H_{5\sim8},H_{9\sim12},H_{13\sim16}, H_{1\sim16}\}$。根据辅助信息，首先计算$c_1$的哈希值为$H_1' = H(c_1)$，再计算$H'_{1\sim4} = H(H_1'\|H_2\|H_3\|H_4)$，然后计算$H'_{1\sim16} = H(H'_{1\sim4}\|H_{5\sim8}\|H_{9\sim12}\|H_{13\sim16})$。最后，判断$H'_{1\sim16}$是否等于$H_{1\sim16}$。如果相等，则$c_1$完好，否则$c_1$已被破坏。

3　系统模型、威胁模型及设计目标

3.1　系统模型

如图3所示，本文场景是基于云辅助物联网的图像检索系统。系统模型包含4个实体：图像所有者（IO, image owner）、图像用户（IU, image user）、云服务器（CS, cloud server）以及区块链网络（BCN, blockchain network）。

图像所有者。采用CNN模型从原始图像中提取特征向量，转换为矩阵并加密以生成安全索引矩阵。创建MHT并对其根节点进行签名。将安全索引矩阵、加密图像和MHT一同上传至云服务器，而根节点的签名发送至区块链进行存储。

图像用户。采用CNN模型从查询图像中提取特征向量，转换为矩阵并加密以生成安全查询矩阵，传送至云服务器以请求查询。根据云服务器返回的结果向区块链发出结果验证请求，验证通过后对结果解密。

云服务器。收到安全查询后，检索存储的图像。结果验证时配合区块链生成验证所需的辅助信息。

区块链网络。只存储MHT根节点的签名值。对于IU发起的结果验证请求，从CS获取必要的辅助信息以执行验证，并将验证结果告知IU和CS。

3.2　威胁模型

CS可能存在恶意行为，尽管在存储和检索过程中会诚实地执行搜索等算法，但它可能出于好奇对存储的图像进行查看，甚至篡改或删除。而由于其去中心化和不可篡改性，BCN可被视为一个可信实体。

1) 已知密文模型。CS仅能访问有限数量的图像、索引矩阵和查询矩阵的密文，且无法获取任何明文数据或密钥信息。

2) 已知背景模型。CS除了可以访问密文外，还能获取额外的信息，例如部分明文数据，利用这些数据可以推断并获取更深入的信息。

3.3　设计目标

为了在云辅助物联网环境中实现安全检索，所

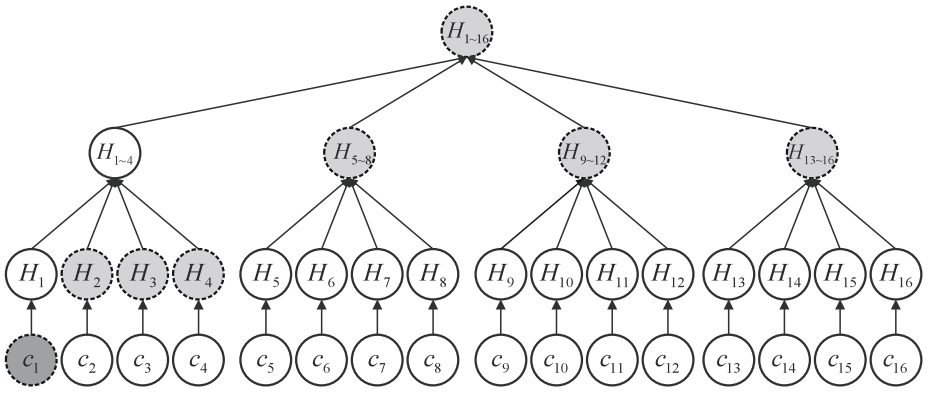


图2　4-MHT生成和验证示例

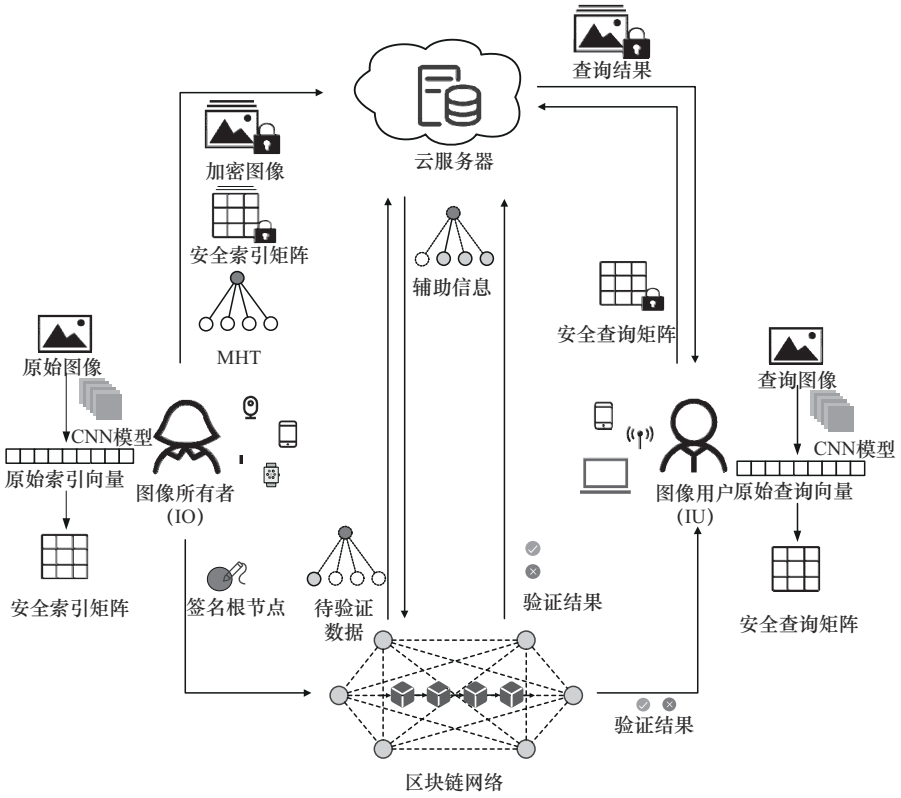


图3　系统模型

提方案设定了以下设计目标。

1) 高效性。确保CS能够高效地执行安全图像检索，同时索引和密钥占用的存储空间极小。

2) 准确性。保证检索结果与查询图像的高度相似性。

3) 安全性。保护IO和IU的隐私，防止任何恶意实体获取有关图像集合、索引和查询的敏感信息。安全性包含以下子目标。

① 索引和查询机密性。确保敌手无法访问索引向量、查询向量及其隐含的内容。

② 查询不可链接性。敌手无法判定任意2个安全索引矩阵是否由同一查询图像生成。

③ 搜索结果可验证性。在图像被删除或篡改的情况下，搜索结果将无法通过BCN的验证。

4　可验证的安全图像检索方案

传统特征提取方法存在查询精度不足的问题，安全kNN算法则面临较大的存储负担和高昂的计算开销。此外，结果验证过程进一步加剧了物联网设备的资源消耗。针对这些问题，本节提出了一种可验证的安全图像检索方案。该方案利用预训练的CNN模型提取图像特征，以提高查询精度；将特征向量转换为特征矩阵，以降低存储和计算成本；通过结合4-MHT和高效短签名并由区块链网络辅助实现结果验证，从而有效减少物联网设备的资源消耗。

该方案的具体构造包含8个主要阶段：索引生成、索引加密、4-MHT生成、查询生成、查询加密、搜索、验证和图像更新。在详细描述具体方案之前，首先在表1中列出该方案中使用的主要符号，并给出2个补充定义。

表1　本文主要符号

符号	描述
N	图像提取的特征向量维数
n	索引(查询)矩阵的行(列)数
m	系统中的图片数量
$\boldsymbol{x}(\boldsymbol{y})$	索引(查询)向量
$\boldsymbol{x}'(\boldsymbol{y}')$	扩展后的索引(查询)向量
$\boldsymbol{X}(\boldsymbol{Y})$	索引(查询)矩阵
$\boldsymbol{K}$	密钥矩阵

定义 3　给定 $r \in \mathbb{R}$，$\lceil r \rfloor$ 表示与 r 最接近的整数，$\lceil r \rfloor_q$ 则是与 r 最接近的整数模 q 的结果。

定义 4　给定矩阵 $\boldsymbol{X}$，$|\max(\boldsymbol{X})|$ 表示矩阵 $\boldsymbol{X}$ 的元素的最大绝对值。

4.1　索引生成

首先，IO 使用预训练的 CNN 模型提取每幅图像的特征值，表示为向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_i,\cdots,x_N)$，其中，$N$ 表示提取的特征索引向量的维数；$x_i \in \mathbb{Z}_{q_1}$，q_1 是系统定义的大素数，因此向量中的每个元素 x_i 都是一个大整数。接着，将提取的特征向量 $\boldsymbol{x}$ 扩展为 $\boldsymbol{x}'$，表示为 $\boldsymbol{x}'=(x_1,x_2,\cdots,x_i,\cdots,x_N,-\sum_{i=1}^{N}x_i^{\,2},1,0,r_x,-1,\cdots,-1)$，其中 r_x 是 $\mathbb{Z}_{q_1}$ 中的随机数。最后，将 $\boldsymbol{x}'$ 转换成一个 $n \times n$ 的索引矩阵 $\boldsymbol{X}$，表示为

$$\boldsymbol{X}=\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & \cdots & x_n \\ x_{n+1} & x_{n+2} & x_{n+3} & x_{n+4} & x_{n+5} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ x_{n'+1} & x_{n'+2} & x_{n'+3} & x_{n'+4} & x_{n'+5} & \cdots & x_N \\ -\sum_{i=1}^{N}x_i^{\,2} & 1 & 0 & r_x & -1 & \cdots & -1 \end{bmatrix}$$

假设 IO 从图像中提取一个 10 维的特征向量 $\boldsymbol{x}_{\mathrm{eg}}=(x_1,x_2,\cdots,x_{10})$。接着，IO 将该特征向量扩展为一个 $n^2=16$ 维的向量 $\boldsymbol{x}'_{\mathrm{eg}}$（$n=\left\lceil\sqrt{10+4}\right\rfloor=4$）。$\boldsymbol{x}'_{\mathrm{eg}}$ 表示为 $(x_1,x_2,\cdots,x_{10},-\sum_{i=1}^{10}x_i^{\,2},1,0,r_x,-1,-1)$，$r_x$ 为随机数。最后，IO 生成一个大小为 4 × 4 的索引矩阵 $\boldsymbol{X}_{\mathrm{eg}}$，具体为

$$\boldsymbol{X}_{\mathrm{eg}}=\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & -\sum_{i=1}^{10}x_i^{\,2} & 1 \\ 0 & r_x & -1 & -1 \end{bmatrix}$$

4.2　索引加密

IO 首先生成密钥 $\boldsymbol{K}$，用来加密索引矩阵。给定参数 n，随机选取一对 $n \times n$ 的可逆矩阵 $\boldsymbol{K}$ 和 $\boldsymbol{K}^{-1}$。

IO 使用对称加密，如高级加密标准（AES, advanced encryption standard）等，对隐私图像进行加密得到密文图像集合 $\{c_1,\cdots,c_j,\cdots,c_m\}$，其中 m 为图像总数。然后，用 $\boldsymbol{K}$ 加密 4.1 节中生成的索引矩阵 $\boldsymbol{X}$，加密过程为

$$E(\boldsymbol{X})=(p\boldsymbol{X}+\boldsymbol{R})\times\boldsymbol{K} \tag{2}$$

其中，p 是一个大整数，满足 $p \in \mathbb{Z}_{q_2}$，$q_2 \gg q_1$ 且 $p \gg 2|\max(\boldsymbol{R})|$，$p$ 作为系统参数会共享给每个 IU，从而在生成安全查询时使用；$\boldsymbol{R}$ 是一个是从概率分布中随机选择的 $n \times n$ 的噪声矩阵，其元素均属于 $\mathbb{Z}_{q_2}$。

最后，IO 通过安全信道将 $\boldsymbol{K}^{-1}$ 发送给授权 IU，用来生成安全查询。

4.3　4-MHT 生成

为了便于 IU 验证搜索结果的正确性，IO 生成一个 4-MHT，表示为 $\mathcal{T}$。首先，IO 计算密文图像集合 $\{c_1,\cdots,c_j,\cdots,c_m\}$ 中每个 c_i 的哈希值 $H(c_i\|id_i)$，其中，id_i 是 c_i 的编号。为方便实际中的计算，此处的哈希运算和下文签名中的哈希运算选取同一函数。根据上文关于 4-MHT 的描述生成 $\mathcal{T}$，其中的根节点表示为 root($\mathcal{T}$)。

随后，IO 对根节点 root($\mathcal{T}$) 进行签名。选择 $\theta \in \mathbb{Z}_q^*$ 作为签名私钥，计算 g^θ 作为公钥，其中 g 为以 q 阶乘法循环群 $\mathbb{G}$ 的生成元。计算 $P=e(g,g)$ 作为公共参数，其中 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是双线性映射。IO 选择一个哈希函数 $H:\{0,1\}^*\to\mathbb{Z}_q^*$ 对根节点进行签名得到 σ_{root}，如式(3)所示。

$$\sigma_{\mathrm{root}}=g^{\frac{1}{H(\mathrm{root}(\mathcal{T})\|\mathrm{Time})+\theta}} \tag{3}$$

其中，Time 表示签名的最新时间，可以表示为 IO 常用的更新时间段，例如日、周、月等。如果该阶段没有发生数据更新，IO 将图像密文、安全索引矩阵以及默克哈希树 $\mathcal{T}$ 都上传至 CS，并将 σ_{root} 和当前时间 Time 发送至 BCN 进行存储，将公钥 g^θ 以及 g、P、H 作为公共参数公开。

4.4　查询生成

当 IU 搜索时，也使用预训练的 CNN 模型提取搜索图像的特征值，表示为 $\boldsymbol{y}=\{y_1,y_2,\cdots,y_i,\cdots,y_N\}$，其中 N 和 IO 提取的索引向量维数相同，每个元素 $y_i(i\in[1,N])$ 是 $\mathbb{Z}_{q_1}$ 中的大整数。接着，将 $\boldsymbol{y}$ 扩展为一个长度为 n^2 的向量 $\boldsymbol{y}'$，表示为 $\boldsymbol{y}'=(2ry_1,2ry_2,\cdots,2ry_N,r,-r\sum_{i=1}^{N}y_i^{\,2},r_y,0,r_1,\cdots,r_{n^2-(N+4)})$。其中 r、r_y 以及 $r_1,\cdots,r_{n^2-(N+4)}$ 都由 IU 根据安全需求自行随机选择，随机数取值越大，安全性越高而准确性越低。最后，将向量 $\boldsymbol{y}'$ 转换为如下 $n \times n$ 的查询矩阵 $\boldsymbol{Y}$。

$$\boldsymbol{Y}=\begin{bmatrix} 2ry_1 & 2ry_2 & 2ry_3 & 2ry_4 & 2ry_5 & \cdots & 2ry_n \\ 2ry_{n+1} & 2ry_{n+2} & 2ry_{n+3} & 2ry_{n+4} & y_{n+5} & \cdots & 2ry_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 2ry_{n'+1} & 2ry_{n'+2} & 2ry_{n'+3} & 2ry_{n'+4} & 2ry_{n'+5} & \cdots & 2ry_N \\ r & -r\sum_{i=1}^{N}y_i^{\,2} & r_y & 0 & r_1 & \cdots & r_{n^2-(N+4)} \end{bmatrix}$$

假设IU从感兴趣的图像中提取一个10维的特征向量$\boldsymbol{y}_{\mathrm{eg}}=(y_1,y_2,\cdots,y_{10})$，并将该特征向量扩展为一个$n^2=16$维的向量$\boldsymbol{y}'_{\mathrm{eg}}$。扩展后的向量$\boldsymbol{y}'_{\mathrm{eg}}$表示为$(y_1,y_2,\cdots,y_{10},r,-r\sum_{i=1}^{10}y_i^{\,2},r_y,0,r_1,r_2)$，后2位填充随机数$r_1$、$r_2$。最后，IU生成一个4×4的查询矩阵$\boldsymbol{Y}_{\mathrm{eg}}$。

$$\boldsymbol{Y}_{eg}=\begin{bmatrix} y_1 & y_2 & y_3 & y_4 \\ y_5 & y_6 & y_7 & y_8 \\ y_9 & y_{10} & r & -\sum_{i=1}^{10}y_i^{\,2} \\ r_y & 0 & r_1 & r_2 \end{bmatrix}$$

4.5　查询加密

为了保护查询隐私，IU对生成的查询矩阵$\boldsymbol{Y}$进行如下加密计算。

$$E(\boldsymbol{Y})=\boldsymbol{K}^{-1}\times(p\boldsymbol{Y}^{\mathrm{T}}+\boldsymbol{R}) \tag{4}$$

其中，p是系统参数，$\boldsymbol{R}$是IU选择的噪声矩阵。随后IU选择一个随机整数k，要求CS返回前k个结果，最后将$E(\boldsymbol{Y})$和k一起发送至CS。

4.6　搜索

当CS收到IU的搜索请求后，计算每个安全索引矩阵$E(\boldsymbol{X})$和当前搜索请求中的安全查询矩阵$E(\boldsymbol{Y})$的距离Dist，并将Dist从小到大进行排序，来选择Dist最小的k幅图像作为搜索结果。Dist的具体计算过程如式(4)所示。具体来说，计算$E(\boldsymbol{X})$和$E(\boldsymbol{Y})$的Dist，就是将$E(\boldsymbol{X})$和$E(\boldsymbol{Y})$的转置矩阵的哈达玛积按照定义1求其元素之和，再对其除以p^2的结果按照定义3求与其最接近的整数模q_2的结果，具体的推导过程见5.1节搜索正确性证明。

$$\mathrm{Dist}(E(\boldsymbol{X}),E(\boldsymbol{Y}))=$$

$$\left\lceil\frac{-\mathrm{sum}(E(\boldsymbol{X})\circ(E(\boldsymbol{Y})))}{p^2}\right\rfloor_{q_2}=$$

$$\left\lceil\frac{-\mathrm{sum}(((p\boldsymbol{X}+\boldsymbol{R})\times\boldsymbol{K})\circ(\boldsymbol{K}^{-1}\times(p\boldsymbol{Y}^{\mathrm{T}}+\boldsymbol{R})))}{p^2}\right\rfloor_{q_2}=$$

$$-\mathrm{sum}(\boldsymbol{X}\circ\boldsymbol{Y})+\sum_{k=N+4}^{n^2-(N+4)}r_k=$$

$$-2r(\boldsymbol{x}\cdot\boldsymbol{y})+r\sum_{i=1}^{n}x_i^{\,2}+r\sum_{i=1}^{n}y_i^{\,2}+\sum_{k=N+4}^{n^2-(N+4)}r_k=$$

$$r(\mathrm{eDist}(\boldsymbol{x},\boldsymbol{y}))^2+\sum_{k=N+4}^{n^2-(N+4)}r_k \tag{5}$$

其中，eDist($\boldsymbol{x}$,$\boldsymbol{y}$)表示向量$\boldsymbol{x}$和$\boldsymbol{y}$之间的欧氏距离，$\sum_{k=N+4}^{n^2-(N+4)}r_k$为一个随机数。

最后，CS选择将密文搜索结果发送给IU。

4.7　验证

当IU收到搜索结果后，首先将结果的编号集合发送给BCN。随后，BCN向CS请求验证所需的辅助信息，并利用辅助信息对搜索结果进行验证。假设要验证的图像为c_1，BCN首先生成$H(c_1\|id_1)$，然后根据CS返回的辅助信息，如图2所示，计算出root($\mathcal{T}$)′。最后，对计算出的根节点利用式(6)进行签名验证。

$$e(g^{H(\mathrm{root}(\mathcal{T})\|\mathrm{Time})}g^{\theta},\sigma_{\mathrm{root}})=P \tag{6}$$

如果式(6)成立，表明搜索结果是正确的。随后，BCN将验证结果通知给IU，IU对图像密文进行解密，从而获得感兴趣的k个明文图像。

如果式(6)不成立，BCN将此信息通知IU和IO。作为响应，IO首先检查所有相关的数据更新日志，包括更新内容和时间戳等，对比这些更新记录与默克哈希树的最后更新时间，以确定是否存在未及时更新的情况。若确认问题源于更新的滞后，则由IO重新生成默克哈希树$\mathcal{T}'$，从叶节点开始，包括所有被认为已更新的数据块。将$\mathcal{T}'$发送给CS，并重新生成根节点签名σ'_{root}发送至BCN。如果不是由于未及时更新产生的验证失败，IO可以责令CS更换验证未通过的图像。若错误由CS的行为如数据丢失、篡改或未及时更新引起，IO有权对CS进行追责。接着，CS会重新搜索并将新的搜索结果返回给IU，IU在收到结果后将再次进行验证，直至验证成功并接收最终搜索结果。

4.8　图像更新

图像更新过程包括数据的删除、新增和替换，

其中图像替换操作可视为删除和新增的组合操作。本文方案重点讨论图像删除和新增操作。

图像删除操作需要移除图像本身及其对应的索引，并删除 4-MHT 中的相应叶节点。对于 4-MHT 叶节点的删除操作，被删除的节点将用 NULL 值替代，随后重新计算该节点的哈希值，并更新从该节点到根节点路径上的所有节点。此外，根节点需要根据当前时间进行重新签名并上传至 BCN。通常情况下，当删除的节点数为 m' 时，最坏情况下需要重新计算的节点数为 $m'\log_4 m$。

图像新增操作涉及图像本身的加密计算、图像索引的加密处理以及向 4-MHT 中添加新的节点并更新根节点的签名。4-MHT 节点的新增操作分为 2 种情况：第 1 种情况是新增的图像数量 m' 不会引起 4-MHT 层数的增加，此时，更新的节点数在最坏情况下为 $m'\log_4 m$；第 2 种情况是新增节点数导致 4-MHT 层数增加 1 层，此时，最坏情况下需要更新的节点数为 $m'(\log_4 m + 1)$。

5　搜索正确性和安全性分析

本节分析方案的搜索正确性和安全性。

5.1　搜索正确性

搜索正确性是指方案中对加密后的查询和索引进行搜索，可以得到和明文搜索同样的结果。

从图像中提取的原始特征向量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 经过扩展、转换和加密后得到安全索引矩阵 $E(\boldsymbol{X})$ 和安全查询矩阵 $E(\boldsymbol{Y})$。已知图像间的相似性是由其特征向量间的欧氏距离决定的，其欧氏距离越小，相似性越高。因此，本文方案的搜索正确性，取决于 $E(\boldsymbol{X})$ 和 $E(\boldsymbol{Y})$ 的距离排序与 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的欧氏距离排序是一致的。

定理 1　给定查询向量 $\boldsymbol{y}$，$\boldsymbol{y}$ 和每个索引向量 $\boldsymbol{x}$ 的欧氏距离排序结果和加密后的安全矩阵 $E(\boldsymbol{Y})$ 及 $E(\boldsymbol{X})$ 的距离排序结果一致。

证明　首先，将向量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的欧氏距离表示为 eDist($\boldsymbol{x}$,$\boldsymbol{y}$)。$E(\boldsymbol{Y})$ 和 $E(\boldsymbol{X})$ 的距离则由 Dist($E(\boldsymbol{X})$, $E(\boldsymbol{Y})$) 表示，由式(5)可知

$$\mathrm{Dist}(E(\boldsymbol{X}),E(\boldsymbol{Y})) = \left\lceil \frac{-\mathrm{sum}(E(\boldsymbol{X}) \circ (E(\boldsymbol{Y})))}{p^2} \right\rfloor_{q_2}$$

其中，p 是系统参数，将式(2)和式(4)中的 $(p\boldsymbol{X} + \boldsymbol{R})$ 和 $(p\boldsymbol{Y}^{\mathrm{T}} + \boldsymbol{R})$ 分别看作一个整体，表示为 $\boldsymbol{X}'$ 和 $\boldsymbol{Y}'$，则式(2)和式(4)可表示为

$$E(\boldsymbol{X}) = \boldsymbol{X}' \times \boldsymbol{K} \tag{7}$$

$$E(\boldsymbol{Y}) = \boldsymbol{K}^{-1} \times \boldsymbol{Y}' \tag{8}$$

接着，将矩阵 $\boldsymbol{X}'$、$\boldsymbol{K}$、$\boldsymbol{K}^{-1}$、$\boldsymbol{Y}'$ 表示为行向量或行向量的转置形式，如式(9)和式(10)所示。

$$E(\boldsymbol{X}) = (\boldsymbol{x}_1 \quad \cdots \quad \boldsymbol{x}_n)^{\mathrm{T}} \times (\boldsymbol{k}_1 \quad \cdots \quad \boldsymbol{k}_n) \tag{9}$$

$$E(\boldsymbol{Y}) = (\boldsymbol{k}'_1 \quad \cdots \quad \boldsymbol{k}'_n)^{\mathrm{T}} \times (\boldsymbol{y}_1 \quad \cdots \quad \boldsymbol{y}_n) \tag{10}$$

计算 $\mathrm{sum}(E(\boldsymbol{X}) \circ E(\boldsymbol{Y}))$

$$\begin{aligned}
&\mathrm{sum}(E(\boldsymbol{X}) \circ E(\boldsymbol{Y})) = \\
&\mathrm{sum}(((\boldsymbol{x}'_1 \quad \cdots \quad \boldsymbol{x}'_n)^{\mathrm{T}} \times (\boldsymbol{k}_1 \quad \cdots \quad \boldsymbol{k}_n)) \circ \\
&\qquad ((\boldsymbol{k}'_1 \quad \cdots \quad \boldsymbol{k}'_n)^{\mathrm{T}} \times (\boldsymbol{y}'_1 \quad \cdots \quad \boldsymbol{y}'_n)) = \\
&\mathrm{sum}\begin{pmatrix} \boldsymbol{x}'_1\boldsymbol{k}_1\boldsymbol{k}'_1\boldsymbol{y}'_1 & \cdots & \boldsymbol{x}'_1\boldsymbol{k}_n\boldsymbol{k}'_1\boldsymbol{y}'_n \\ \vdots & & \vdots \\ \boldsymbol{x}'_n\boldsymbol{k}_1\boldsymbol{k}'_n\boldsymbol{y}'_1 & \cdots & \boldsymbol{x}'_n\boldsymbol{k}_n\boldsymbol{k}'_n\boldsymbol{y}'_n \end{pmatrix} = \\
&\boldsymbol{x}'_1\boldsymbol{y}'_1 + \boldsymbol{x}'_2\boldsymbol{y}'_2 + \boldsymbol{x}'_3\boldsymbol{y}'_3 = \\
&\mathrm{sum}(\boldsymbol{X}' \circ \boldsymbol{Y}')
\end{aligned} \tag{11}$$

由此，可得

$$\begin{aligned}
&\mathrm{Dist}(E(\boldsymbol{X}),E(\boldsymbol{Y})) = \\
&\left\lceil \frac{-\mathrm{sum}(\boldsymbol{X}' \circ \boldsymbol{Y}')}{p^2} \right\rfloor_{q_2} = \\
&-2r(\boldsymbol{x} \cdot \boldsymbol{y}) + r\sum_{i=1}^{n} x_i^{\,2} + r\sum_{i=1}^{n} y_i^{\,2} + \sum_{k=N+4}^{n^2-(N+4)} r_k + \\
&\left\lceil \frac{\boldsymbol{R} \times \boldsymbol{R}}{p^2} + \frac{\boldsymbol{X} \times \boldsymbol{R} + \boldsymbol{R} \times \boldsymbol{Y}^{\mathrm{T}}}{p^2} \right\rfloor_{q_2} = \\
&r\left(\sum_{i=1}^{n} x_i^{\,2} + \sum_{i=1}^{n} y_i^{\,2} - 2(\boldsymbol{xy})\right) + r + \sum_{k=N+4}^{n^2-(N+4)} r_k = \\
&r(\mathrm{eDist}(\boldsymbol{x},\boldsymbol{y}))^2 + \sum_{k=N+4}^{n^2-(N+4)} r_k
\end{aligned} \tag{12}$$

即安全矩阵之间的距离等于原始向量的欧氏距离的 r 倍加上一个干扰项 $\sum_{k=N+4}^{n^2-(N+4)} r_k$。其中，$r$ 和 r_k 都是由 IU 自行选择的随机数，在同一次搜索过程中不变。因此，r 和 r_k 不会影响最终 Dist 的排序结果，即 Dist($E(\boldsymbol{X})$, $E(\boldsymbol{Y})$) 的排序结果和 eDist($\boldsymbol{x}$,$\boldsymbol{y}$) 的排序结果保持一致。证毕。

5.2　安全性

本节根据 3.3 节给出的安全性目标，证明方案的索引和查询的安全性、查询的不可链接性以及搜索结果的可验证性。

5.2.1　*索引和查询的安全性*

本文方案中，查询矩阵与索引矩阵采用相同的加密策略。因此，以索引矩阵的加密为例来分析证明索引和查询的安全性。定理2用于证明加密的索引矩阵无法恢复明文索引，从而确保索引安全性。

定理2　如果LWE问题是困难的，从$E(\boldsymbol{X})$中恢复$\boldsymbol{X}$在计算上是不可行的。

证明　分别在已知密文模型和已知背景模型下证明。

1) 已知密文模型

本文方案中，对索引矩阵$\boldsymbol{X}$的加密如式(2)所示，即$E(\boldsymbol{X})=(p\boldsymbol{X}+\boldsymbol{R})\times\boldsymbol{K}$。其中$\boldsymbol{X}$和$\boldsymbol{R}$都是大小为$n\times n$的矩阵。矩阵($p\boldsymbol{X}$+$\boldsymbol{R}$)与另一个$n\times n$的矩阵$\boldsymbol{K}$的乘积，可以表示为$n^2$个$n$维向量的点积，具体为

$$\begin{aligned}E(\boldsymbol{X})_{11}&=p\boldsymbol{x}_1\boldsymbol{k}_1+\boldsymbol{r}_1\boldsymbol{k}_1\\E(\boldsymbol{X})_{12}&=p\boldsymbol{x}_1\boldsymbol{k}_2+\boldsymbol{r}_1\boldsymbol{k}_2\\&\vdots\\E(\boldsymbol{X})_{ij}&=p\boldsymbol{x}_i\boldsymbol{k}_j+\boldsymbol{r}_i\boldsymbol{k}_j\\&\vdots\\E(\boldsymbol{X})_{nn}&=p\boldsymbol{x}_n\boldsymbol{k}_n+\boldsymbol{r}_n\boldsymbol{k}_n\end{aligned}\tag{13}$$

其中，$E(\boldsymbol{X})_{ij}$表示矩阵的第i行第j列的元素，$\boldsymbol{x}_i$表示矩阵$\boldsymbol{X}$的第i行，$\boldsymbol{r}_i$表示矩阵$\boldsymbol{R}$的第i行，$\boldsymbol{k}_j$表示矩阵$\boldsymbol{K}$的j列。

接着，将$p\boldsymbol{x}_i$表示为$\boldsymbol{x}'_i$，将$\boldsymbol{r}_i\boldsymbol{k}_j$表示为$r'_i$，则式(13)中的$n^2$个等式可以表示为

$$E(\boldsymbol{X})_{ij}=\boldsymbol{x}'_i\boldsymbol{k}_j+r'_i\tag{14}$$

其中，$1\leqslant i\leqslant n$，$1\leqslant j\leqslant n$。因此，从安全矩阵$E(\boldsymbol{X})$中恢复$\boldsymbol{X}$就变成了定义2中的LWE问题。而且，密钥$\boldsymbol{K}$对敌手来说是未知的，因此从$E(\boldsymbol{X})$中恢复$\boldsymbol{X}$是比解LWE问题更困难的。

根据定义2，求解LWE问题是困难的，因此在已知密文模型中从加密索引矩阵中恢复原始索引矩阵在计算上也是不可行的。

2) 已知背景模型

在已知背景模型中，敌手能从背景信息中分析并获取除密文外的附加信息，例如少量的明文查询。在已知密文模型中已经证明改进的基于LWE的安全kNN算法可以防止敌手直接从密文中得到明文索引信息，Yao等[6]提出了一种线性分析攻击，该攻击并不从密文直接恢复原始数据，而是利用欧氏距离重构数据。在本文方案中，线性分析攻击指的是从Dist中试图获取明文索引和查询。具体来说，给定索引矩阵$\boldsymbol{X}$和查询矩阵$\boldsymbol{Y}$，敌手可以试图构造如式(15)所示的等式。

$$\mathrm{Dist}(\boldsymbol{X},\boldsymbol{Y})=r(\mathrm{eDist}(\boldsymbol{x},\boldsymbol{y}))^2+\sum_{k=N+4}^{n^2-(N+4)}r_k\tag{15}$$

式(15)中有2n+2个未知数，即2个n维向量$\boldsymbol{x}$、$\boldsymbol{y}$和随机数r，$\sum_{k=N+4}^{n^2-(N+4)}r_k$（随机数之和，在此整体当作一个随机数）。由于敌手可以获取查询向量$\boldsymbol{y}$、因此未知数的个数可以降为n+2。在Yao等[6]提出的攻击中，如果敌手可以获取大于n个查询，就可以构造n个等式并通过求解来恢复出$\boldsymbol{x}$。但在本文方案中，每次构造等式时都会引入不同的随机数r和$\sum_{k=N+4}^{n^2-(N+4)}r_k$，因此要想恢复$\boldsymbol{x}$是很困难的。所以，即使敌手可以获取$n$个查询向量，仍然面临着构造$n$个等式来求解3$n$个未知数（即$\boldsymbol{x}$、$n$个随机数$r$、$n$个随机数$\sum_{k=N+4}^{n^2-(N+4)}r_k$）的问题，从而免受线性分析攻击的影响。因此，本文方案也可保证已知背景模型下的索引安全。证毕。

5.2.2　*查询的不可链接性*

定理3　敌手无法区分任意2个安全查询矩阵是否提取自同一图像。

证明　在查询生成阶段，假设从一幅图像中提取查询向量$\boldsymbol{y}$，随后再定义2个查询向量$\boldsymbol{y}_1$和$\boldsymbol{y}_2$，假设$\boldsymbol{y}_1=\boldsymbol{y}_2=\boldsymbol{y}$。在向量扩展阶段，IU选择不同的随机数来将它们扩展为$\boldsymbol{y}'_1$和$\boldsymbol{y}'_2$，然后将它们填充进查询矩阵$\boldsymbol{Y}_1$和$\boldsymbol{Y}_2$。在查询加密阶段，IU选择不同的随机矩阵$\boldsymbol{R}_1$和$\boldsymbol{R}_2$进行如下加密。

$$\begin{aligned}E(\boldsymbol{Y}_1)&=\boldsymbol{K}^{-1}\times(p\boldsymbol{Y}_1+\boldsymbol{R}_1)\\E(\boldsymbol{Y}_2)&=\boldsymbol{K}^{-1}\times(p\boldsymbol{Y}_2+\boldsymbol{R}_2)\end{aligned}\tag{16}$$

在向量扩展和查询加密阶段分别引入了不同的随机数和随机矩阵，因此获得的加密矩阵$E(\boldsymbol{Y}_1)$和$E(\boldsymbol{Y}_2)$是不同的。敌手从而无法判断$E(\boldsymbol{Y}_1)$和$E(\boldsymbol{Y}_2)$为从同一图像生成的安全索引矩阵。因此，本文方案可以保证查询的不可链接性。证毕。

5.2.3　*搜索结果的可验证性*

本文方案通过4-MHT来生成图像的完整性证明，并对4-MHT的根节点进行签名来确保搜索结果的可验证性。引理1和定理4用于证明搜索结果的可验证性。

引理 1　如果存在一个$(t,q_H,q_\sigma,\varepsilon)$-敌手$\mathcal{A}$（$\mathcal{A}$最多对哈希预言机进行$q_H$次查询，$q_\sigma$次签名查询，并在$t$时间后，以至少$\varepsilon$的概率输出有效伪造）采用自适应选择消息攻击攻破根节点签名方案，则可以构造模拟器(t',ε')-$\mathcal{B}$（$\mathcal{B}$在t'时间后以至少ε'的概率）求解q_σ-共谋攻击算法（CAA）问题[32]，其中，$\varepsilon' \geqslant (\frac{q_\sigma}{q_H})^{q_\sigma} \cdot \varepsilon$且$t' = t$。

证明　模拟器$\mathcal{B}$要完成如下挑战：给定g是群$\mathbb{G}$的生成元，计算g^θ，$h_1,\cdots,h_{q_\sigma} \in \mathbb{Z}_q$，以及$g^{\frac{1}{h_1+\theta}},\cdots,g^{\frac{1}{h_{q_\sigma}+\theta}}$，计算$g^{\frac{1}{h+\theta}}$其中$h \notin \{h_1,\cdots,h_{q_\sigma}\}$。

$\mathcal{B}$将公钥设置为g^θ，作为签名者来回答$\mathcal{A}$的哈希查询和签名查询。挑战分为如下4个阶段。

S1：$\mathcal{B}$准备q_H个哈希查询的回复$\{w_1,w_2,\cdots,w_{q_H}\}$，$h_1,\cdots,h_{q_\sigma}$随机分布在回复集合中。

S2：$\mathcal{A}$对$c_j(1 \leqslant j \leqslant q_H)$进行哈希查询。$\mathcal{B}$将查询结果$w_i$发给$\mathcal{A}$。

S3：$\mathcal{A}$对w_i进行签名查询。如果$w_i = h_j$，$\mathcal{B}$返回$g^{\frac{1}{h_j+\theta}}$给$\mathcal{A}$，否则查询终止。$\mathcal{A}$在这一步成功的概率为$P \geqslant \frac{q_\sigma}{q_H}$。

S4：$\mathcal{A}$终止查询并输出一对消息签名$\{c^*,\sigma^*\}$。c^*的哈希值$H(c^*) = w_l$且$w_l \notin \{h_1,\cdots,h_{q_\sigma}\}$。由于$\{c^*,\sigma^*\}$是合法伪造的，所以等式$e(g^{H(c^*)} \cdot g^\theta,\sigma^*) = e(g,g)$成立。

因此，$\sigma^* = g^{\frac{1}{w_l+\theta}}$。$\mathcal{B}$将$\{w_l,\sigma^*\}$作为挑战的输出。$\mathcal{B}$的执行时间和$\mathcal{A}$相同，即$t' = t$。最终，$\mathcal{B}$成功的概率为$\varepsilon' \geqslant (P)^{q_S} \cdot \varepsilon = (\frac{q_S}{q_H})^{q_S} \cdot \varepsilon$。证毕。

定理 4　如果根节点签名是不可伪造的，则任何敌手都无法通过伪造图像或图像完整性的证明信息来以显著优势通过搜索结果验证。

证明　根据引理1，如果存在可以攻破根节点签名方案的敌手，则q_σ-CAA困难问题能被解决。但已知q_σ-CAA问题是(t,ε)困难的，因此根节点签名是不可伪造的。证毕。

此外，根节点签名存储在不可篡改的区块链上，依托区块链的分布式的特征，使签名更加可靠，进一步确保了完整性验证的准确性。区块链使得各方共同参与，一旦数据由于非IO原因造成损坏或丢失，则可向CS进行追责和索赔，也促使CS能够更加诚实地完成自己的存储和搜索任务。

6　性能分析

本文方案的性能通过理论和实验2个方面进行分析。在理论分析部分，本文方案与3个典型的安全图像搜索方案（自适应可验证隐私保护医学图像检索（AVPMIR, adaptive verifiable privacy-preserving medical image retrieval）方案[17]、安全可验证的多密钥图像搜索（SVMIS, secure and verifiable multi-key image search）方案[9]、基于隐私保护阈值的图像检索（PTIR, privacy-preserving threshold-based image retrieval）方案[24]）在计算和存储成本方面进行了比较。在实验分析中，在真实数据集上评估了本文方案的搜索准确性、关键算法的效率和存储开销。

6.1　理论分析

本文方案及AVPMIR方案[17]、SVMIS方案[9]、PTIR方案[24]都基于安全kNN算法，实现了安全性与效率的平衡。因此，将本文方案与这3个典型的方案进行对比分析。

首先从索引加密、查询加密以及搜索3个方面分析本文方案的计算成本。

1)索引加密：IO从每幅图像中提取的索引向量的维数为N，将其扩展并转换为$n \times n$的特征矩阵，其中$n = \left\lceil \sqrt{N+4} \right\rceil$。索引矩阵加密的时间复杂度主要由大小为$n \times n$的安全索引矩阵与同等大小的密钥矩阵$\boldsymbol{K}$的乘法决定，该操作的计算代价为$O(n^3)$，为方便比较，用$N$代替$n$，则计算代价表示为$O(N^{\frac{2}{3}})$。假设有$m$幅图像索引需要加密，总的计算代价为$O(mN^{\frac{2}{3}})$。

2) 查询加密：IU加密查询的方法与IO加密索引的方法基本相同。安全查询矩阵的大小也是$n \times n$，因此查询加密的时间复杂度也为$O(n^3)$，也即$O(N^{\frac{2}{3}})$。

3)搜索：CS的搜索过程主要涉及安全查询矩阵和安全索引矩阵之间的哈达玛积运算，该操作的时间复杂度为$O(n^2)$，即$O(N)$。若图像总数为m，即安全索引矩阵的总数为m，则云服务器执行一次搜索的时间复杂度为$O(mN)$。

本文方案与3个典型方案的计算代价比较如表2所示。搜索主要考虑安全的相似度搜索算法的计算代价，不考虑具体的传统搜索算法。其中m是图片总数，N是特征向量维数。在这些关键算法中，本文方案相较于其他方案具有更低的时间复杂度，尤其是处理高维特征图像时，有效减少了计算资源的消耗。

表2 计算代价比较

方案	索引加密	查询加密	搜索
AVPMIR	$O(mN^2)$	$O(N^2)$	$O(mN)$
SVIMIS	$O(mN^2)$	$O(N^2)$	$O(mN)$
PTIR	$O(mN^3)$	$O(N^3)$	$O(mN^2)$
本文方案	$O(mN^{\frac{2}{3}})$	$O(N^{\frac{2}{3}})$	$O(mN)$

接着，从安全索引、安全查询和密钥3个方面分析本文方案的存储成本。图像的安全索引为一个大小是$n \times n$的矩阵，其存储代价为$O(n^2)$，m幅图像总的存储代价为$O(mn^2)$，即$O(mN)$。安全查询矩阵和密钥矩阵同样都是$n \times n$的矩阵，其存储代价也为$O(n^2)$，即$O(N)$。

本文方案与3个典型方案的存储代价比较如表3所示。由表3可明显看出，本文方案中安全索引、安全查询以及密钥的存储代价都有所减少。尤其是通过将向量转换为矩阵的方式，将密钥大小从N^2减少到N，显著降低了存储需求。因此，本文方案在安全索引和查询的存储成本以及在密钥管理上具有明显优势。

表3 存储代价比较

方案	安全索引	安全查询	密钥
AVPMIR	$O(mN)$	$O(N)$	$O(N^2)$
SVIMIS	$O(mN)$	$O(N)$	$O(N^2)$
PTIR	$O(mN^2)$	$O(N^2)$	$O(N^2)$
本文方案	$O(mN)$	$O(N)$	$O(N)$

最后，分析搜索结果验证相关的计算代价。表4对本文方案使用的4-MHT和传统方案中的2-MHT进行比较，包括IO生成4-MHT时的哈希运算次数（生成）、IO删除m'幅图像时的哈希运算次数（删除）、IO新增m'幅图像时的哈希运算次数（增加）、BCN验证时所需哈希运算次数（验证）以及CS返回辅助信息的节点数（辅助信息）。在IO生成4-MHT时，需要$\frac{4}{3}n$次哈希运算，而传统的2-MHT需要约$2n$次哈希运算，这表明4-MHT在生成过程中比2-MHT需要更少的哈希运算。IO删除m'幅图像时的哈希运算次数在最坏情况下为$m'\log_4 m$次，而在2-MHT中则需要$m'\mathrm{lb}\, m$次。IO新增m'幅图像时，如果新增图像数不会引起验证树的层数增加（情况1），则哈希运算次数在最坏情况下为$m' + m'\log_4 m$次，而在2-MHT中则需要$m' + m'\mathrm{lb}\, m$次；如果引起验证树层数增加一层（情况2），则所需哈希运算次数为$m' + m'(\log_4 m + 1)$次，相应的在2-MHT中则需要$m' + m'(\mathrm{lb}\, m + 1)$次。在BCN验证时，对于单幅图像，4-MHT需要$\log_4 m$次哈希运算，而2-MHT需要$\mathrm{lb}\, m$次哈希运算，显然4-MHT更为高效。当CS在返回必要的节点以验证数据完整性时，2-MHT需要返回$\mathrm{lb}\, m$个节点，而4-MHT则需要返回$3\log_4 m$个节点。尽管4-MHT返回节点数更多，但该操作只涉及CS和BCN之间的通信，不影响用户设备的性能。综合考虑设备存储、计算以及带宽需求，选择4-MHT在本文方案中可提供更高的效率。此外，本文方案使用的高效短签名方案不依赖特殊的哈希函数，与传统的BLS签名方案[33]相比，显著提升了根节点的验证效率。

6.2 实验分析

本文方案用Python实现，并通过CIFAR-10[34]、Fashion-MNIST[35]、Caltech-256[36]3个真实数据集来评估搜索准确性，效率分析仅在CIFAR-10数据集上进行。CIFAR-10数据集包含10个类别的RGB彩色图像，每个类别选择1 000幅图像进行测试；

表4 验证相关操作成本比较

方法	生成	删除	新增		验证	辅助信息
			情况1	情况2		
2-MHT	$2n$	$m' + m'\mathrm{lb}\, m$	$m' + m'\mathrm{lb}\, m$	$m' + m'(\mathrm{lb}\, m + 1)$	$\mathrm{lb}\, m$	$\mathrm{lb}\, m$
4-MHT	$\frac{4}{3}n$	$m' + m'\log_4 m$	$m' + m'\log_4 m$	$m' + m'(\log_4 m + 1)$	$\log_4 m$	$3\log_4 m$

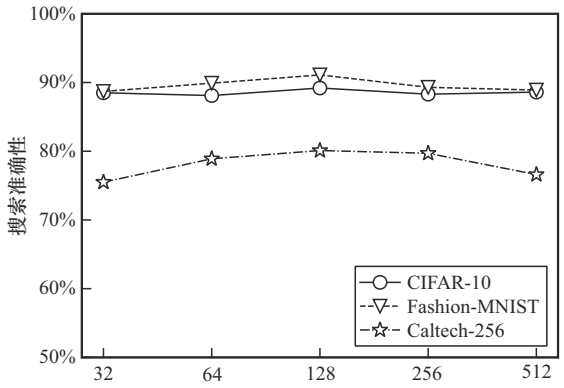
Fashion-MNIST 数据集包含 10 个类别的灰度图像，每个类别选取 1 000 幅图像进行测试；Caltech-256 数据集包含 256 类图像，每类约有 80 幅图像。搜索阶段的实验是在配备 Intel Core i7-7700 CPU（3.60 GHz）和 64 GB RAM 的服务器上完成的，旨在模拟云计算环境中的计算和存储能力。索引和查询加密以及验证相关算法都是在配置较低的 Intel Core i5-7400 CPU（3.00 GHz）和 8 GB RAM 的个人计算机上进行，以模拟端设备的性能条件。

6.2.1　准确性

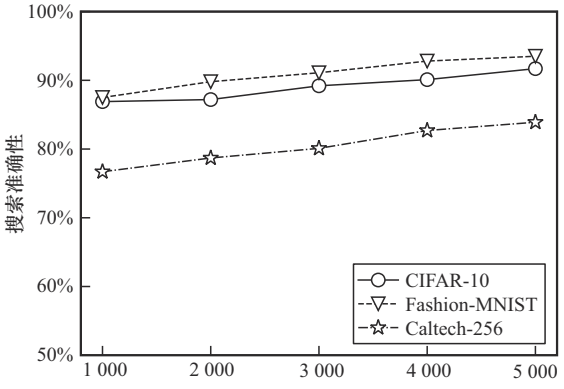
搜索准确性由准确率（precision）表示和评估。

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \times 100\% \tag{17}$$

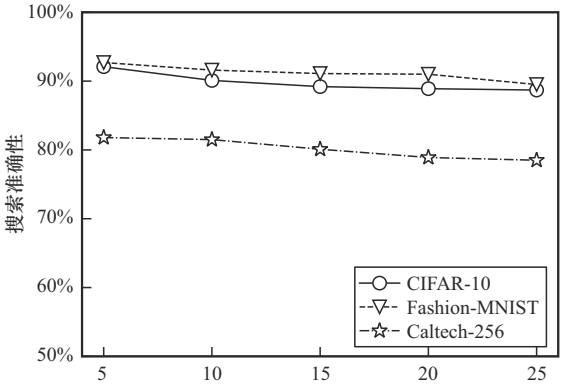
其中，TP 表示搜索结果中与查询图像属于同一类别的图像数量，FP 表示搜索结果中与查询图像不属于同一类别的图像数量。实验评估搜索准确性与图像总数 m、返回图像数 k 以及提取特征向量维数 N 之间的关系。通过 ResNet50 提取图像特征向量，并采用主成分分析（PCA, principal component analysis）技术，将特征向量维数降至 32、64、128、256、512，以便进行评估。图 4 为不同条件下图像搜索准确性的变化。如图 4(a) 所示，当图像总数 m 设置为 3 000 幅，返回图像数 k 固定为 15 时，搜索准确性在各个数据集上均在 N=128 时达到最高的搜索准确性。原因是如果特征向量维数过高，虽然保留了更多的原始信息，但也会包含更多的冗余或噪声信息，导致搜索时的准确性下降。而如果特征向量维数过低，则可能会丢失重要的特征信息，导致无法很好地表示图像特征，进而影响搜索准确性。在图 4(b) 中，返回图像数 k 为 15，特征向量维数 N 为 128，搜索准确性随返回图像数的增加而提高。这是因为随着图像数的增加，从这些图像中提取的特征向量能更全面地反映整体图像库的特征，从而提升搜索准确性。在图 4(c) 中，图像总数 m 设置为 3 000 幅，特征向量维数 N 为 128。随着返回图像数 k 的增加，搜索准确性有所下降。主要原因是在 m 固定的情况下，增加 k 会导致搜索结果中包含更多得分较低的图像，从而影响整体的搜索准确性。从图 4 整体来看，Caltech-256 数据集的搜索准确性较低，主要原因在于其类别数较多且每个类别的图像数量相对较少。尽管该数据集中的图像质量较高，但由于类别较多且每个类别的样本不足，模型难以有效学习每个类别的特征，因此在搜索过程中容易出现不同类别之间的混淆。此外，较少的类别内图像数量使得每个类别的特征提取不够充分，进一步影响了搜索准确性。



(a) m=3 000, k=15时搜索准确性



(b) k=15, N=128时搜索准确性



(c) m=3 000, N=128时搜索准确性

图 4　不同条件下图像搜索准确性的变化

6.2.2　计算代价

本节详细测试方案中几项关键算法的运行时间，具体包括索引加密、查询加密、搜索过程以及

搜索结果验证。计算代价部分仅涉及时间消耗，在各个数据集上运行时间相当，因此仅在CIFAR-10数据集上进行测试。

图5为在不同特征向量维数N和图像总数m条件下加密索引矩阵所需时间。根据6.1节的分析，索引加密的时间复杂度为$O(mN^{\frac{2}{3}})$。当N设置为64、128、256时，相应的n值为9、12、17。图5表明，随着特征向量维数N和图像总数m的增加，加密索引矩阵所需时间都会相应增加。比如当N设置为128时，加密10 000个索引矩阵仅需0.35 s，总体加密时间极短。

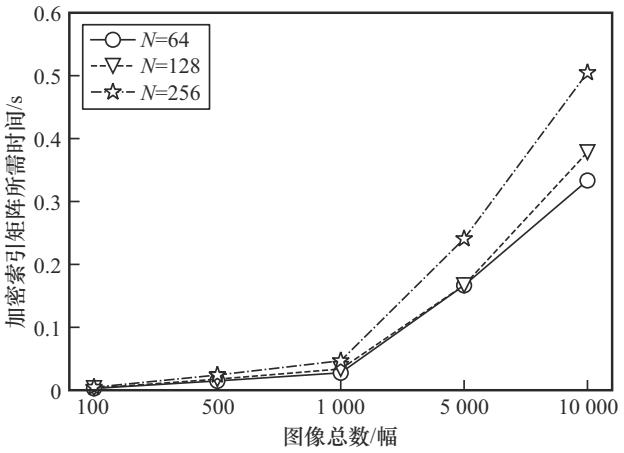


图5　在不同特征向量维数N和图像总数m条件下加密索引矩阵所需时间

图6为不同特征向量维数N和图像总数m对加密查询矩阵所需时间的影响。从图6中可以看出，加密查询矩阵所需时间随着向量维数N的增加而增加，但与图像总数无关。这与查询加密的时间复杂度$O(N^{\frac{2}{3}})$表现一致。当$N=128$时，生成一个安全索引矩阵仅需0.038 ms，这显示了本文方案在处理速度上的高效性。

图7为在不同特征向量维数N和图像总数m条件下，CS执行搜索任务的时间变化。显然，特征向量维数N越大，搜索时间越长。而且当特征向量维数N固定时，随着搜索图像总数的增加，搜索时间也会逐步增加。这与6.1节中的分析相符合，即搜索算法的时间复杂度为$O(mN)$，显然搜索时间与图像总数m和向量维数N成正比。比如当提取向量的维数为128时，CS执行10 000幅图像的搜索仅需0.12 s。

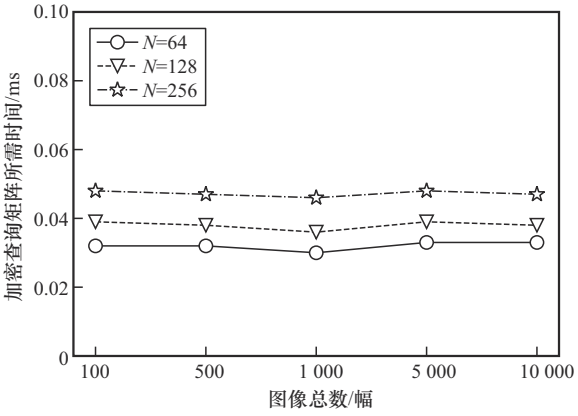


图6　不同特征向量维数N和图像总数m对加密查询矩阵所需时间的影响

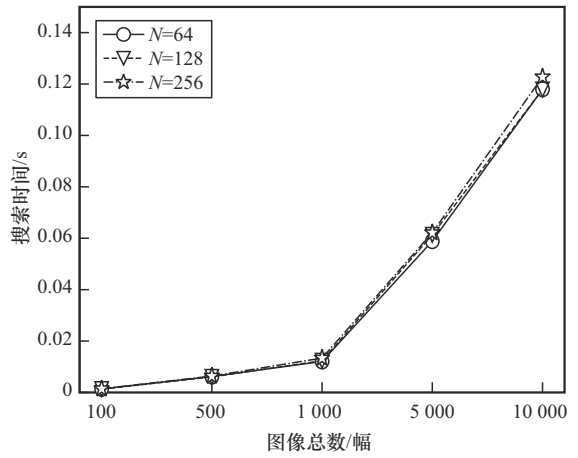
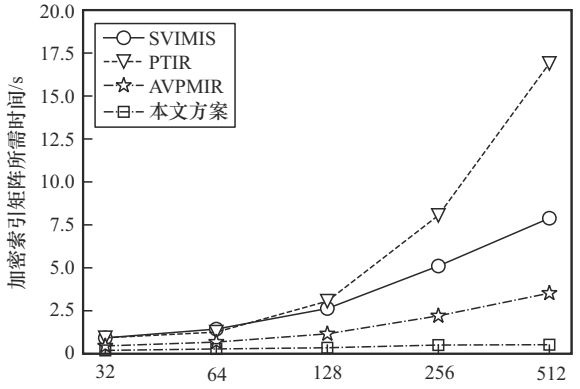


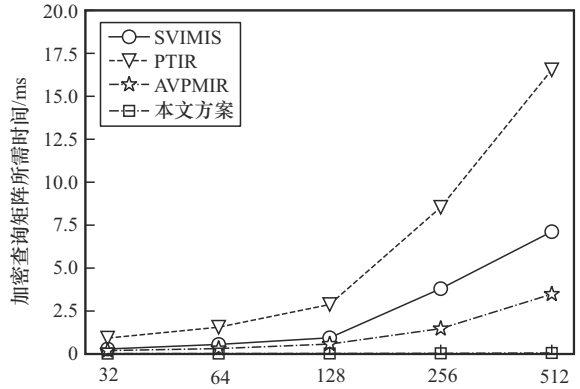
图7　在不同特征向量维数N和图像总数m条件下，CS执行搜索任务的时间变化

图8为4个方案的主要算法（索引加密、查询加密、搜索）在不同特征向量维数下的计算开销。图8(a)对比了本文方案和其他3个典型方案在不同特征向量维数条件下的索引加密的时间消耗，其中图像总数m固定为10 000。从图8(a)可以看出，随着特征向量维数的增加，各个方案的加密索引矩阵所需时间均呈现显著增长趋势，但本文方案在3种向量规模下均表现出最低的加密索引矩阵所需时间。图8(b)对本文方案和2个典型方案在不同特征向量维数N条件下的加密查询矩阵所需时间进行对比。从图8(b)中可以观察到，随着特征向量维数N的增加，各个方案的加密查询矩阵所需时间均逐渐增长。但本文方案的加密查询矩阵所需时间始终保持最低，因此，在物联网环境中，本文方案可以确保性能较低的轻量级设备便捷地生成安全查询。图8(c)对比了各个方案在不同特征向量维数N条件下的搜索时间，图像总数固定为10 000。随着特征

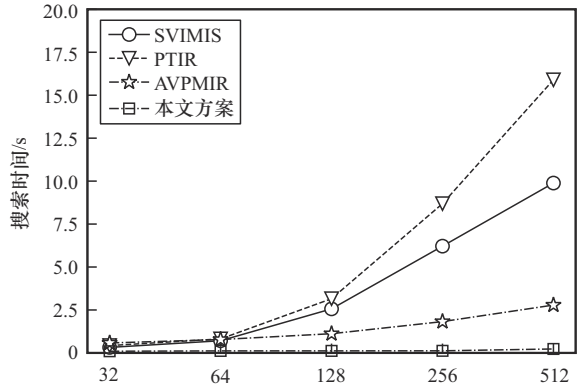
向量维数N的增加，3种方案的搜索时间均有所增加，但本文方案的搜索时间始终最低，并且随着图像总数的增加，其增长幅度显著低于其他方案，体现出更好的扩展性。



(a) 索引加密时间对比



(b) 查询加密时间对比



(c) 搜索时间对比

图8　4个方案的主要算法（索引加密、查询加密、搜索）在不同特征向量维数下的计算开销

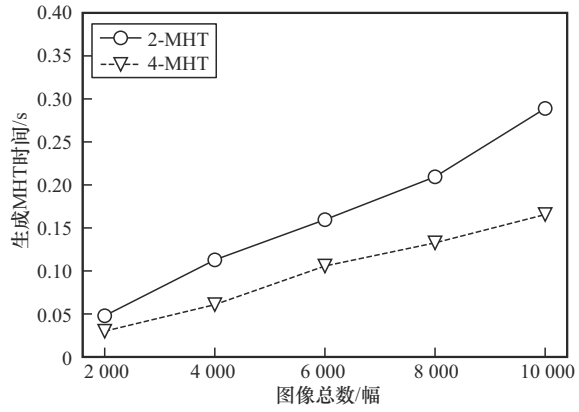
总体来说，本文方案在主要算法上的计算开销均优于其他3种方案，尤其在大规模数据集和轻量级设备环境下展现了更优的性能和扩展性。

验证过程中，首先测试IO生成4-MHT的时间，选择256位安全哈希算法（SHA-256, secure hash algorithm 256-bit）。如图9(a)所示，随着图像总数的增加，生成MHT的时间也相应增长，这主要是因为更多的图像意味着更多的叶节点以及更高的树高度，从而导致哈希运算次数的增加。但整体来看，4-MHT在生成阶段的表现仍优于传统的2-MHT。例如，当文件总数为10 000时，生成所需的4-MHT仅需0.16 s。

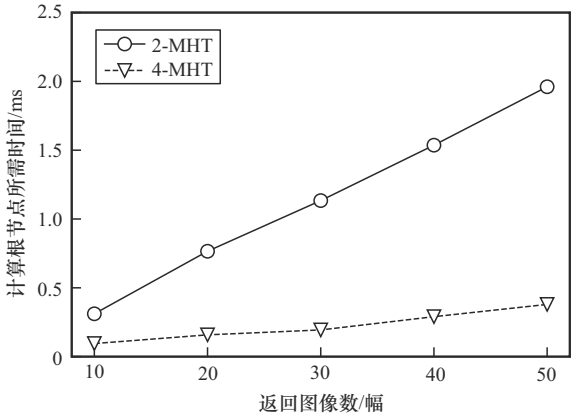
图9(b)和图9(c)分别展示了在不同的返回图像数m'和不同的图像总数m条件下，计算根节点所需时间。具体来说，图9(b)显示了图像总数固定为5 000幅，返回图像数从20幅增加到50幅，计算根节点所需的时间逐渐增加，原因是相应的验证路径增加导致了更多的哈希运算次数，但是在4-MHT中的计算时间仍然比2-MHT时间少。图9(c)中，当返回图像数固定为30幅时，图像总数从2 000幅增至10 000幅，根节点生成时间略有上升，这是由于默克哈希树的大小和验证路径都会随图像总数的增加而增长。但是，4-MHT的性能依然优于2-MHT。假设图像总数为5 000幅且返回50个检索结果，CS计算根节点的时间仅约为0.38 ms。

在生成根节点之后，BCN执行根节点签名验证的时间是固定的，本文方案采用短签名算法以提高效率，相较于传统方案中常用的BLS签名表现更佳。如表5所示，签名验证时间仅需要19.83 ms。在大规模图像检索场景下，虽然区块链的时延和吞吐量可能会影响整体系统性能，但本文方案通过采用短签名算法，BCN验证根节点签名的时间消耗仅为验证传统BLS签名的45%左右，相较于传统方案有了明显的改善。这一改进有效降低了区块链操作中的时延，尤其在签名验证过程中减少了时间开销。本文方案采用混合存储方法，即将图像数据本身存储在云服务器上，BCN只存储和验证图像根节点的签名，因此存储在链上的数据量相对图像总数而言较少，有助于减轻BCN的负担，提高处理速度并减少网络负载。总体来说，本文方案平衡了网络性能和数据安全，为大规模图像检索提供了可行的解决方案。

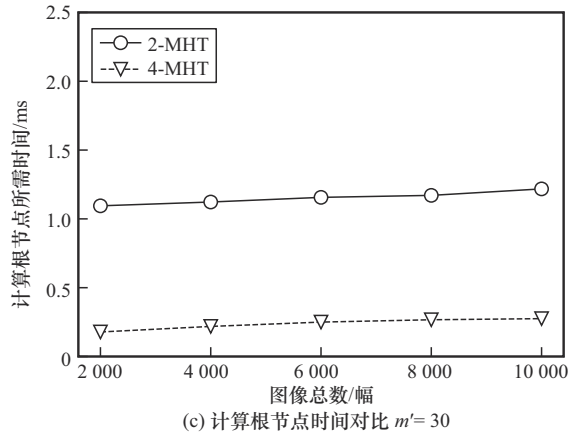
此外，在IO签名阶段，由于未使用特殊的复杂哈希函数，本文方案仅需11.12 ms即可完成对根节点的签名，这一性能对物联网设备十分友好。



(a) 生成MHT时间对比



(b) 计算根节点时间对比 m = 5 000



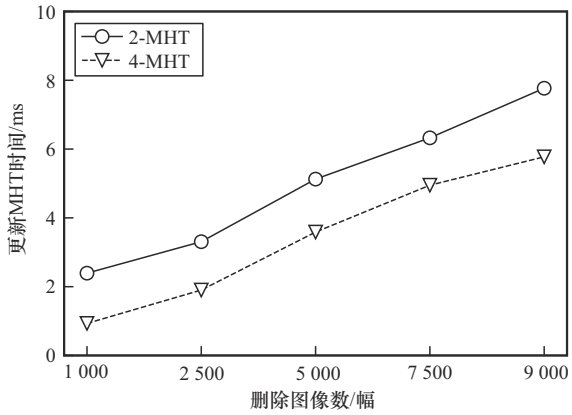
(c) 计算根节点时间对比 m'= 30

图9　验证相关算法性能

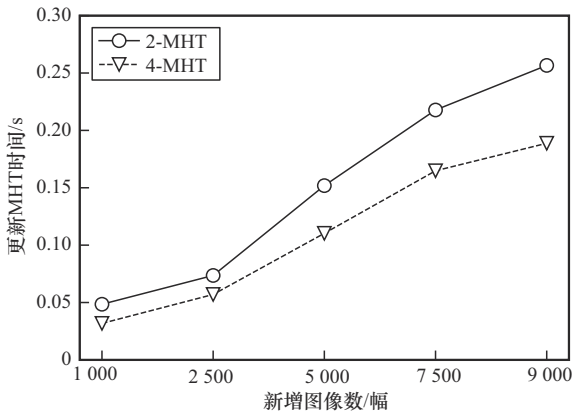
表5　　**方案签名时间对比**

方案	密钥生成时间/ms	签名时间/ms	验签时间/ms
BLS	11.60	37.31	43.11
本文方案	11.59	11.12	19.83

图10为图像更新（删除和新增）时，IO更新MHT的时间变化。假设原有图像数为10 000幅，删除和新增图像数均分别设置为1 000、2 500、5 000、7 500和9 000幅。从图10(a)可以看出，随着删除图像数的增加，2-MHT的更新时间明显高于4-MHT的，说明2-MHT在删除图像时的计算开销更大。图10(b)显示，与删除图像时的结果一致，2-MHT在新增图像时的更新时间也比4-MHT的更长。总体来说，图像更新时间在4-MHT上较2-MHT更低，其主要原因是同样数量的图像生成4-MHT的层高更低。由于4-MHT的每个内部节点可以拥有更多的子节点，其树结构相对更扁平。当增加图像数量时，4-MHT能够容纳更多的节点而无须增加树的高度，避免频繁增加层级，尤其在大规模数据量的情况下，4-MHT比2-MHT更稳定且更高效。



(a) 删除图像时更新MHT时间对比



(b) 新增图像时更新MHT时间对比

图10　图像更新（删除和新增）时，IO更新MHT的时间变化

6.2.3　存储代价

本节测试了不同图像数量和特征向量维数下的安全索引矩阵$E(\boldsymbol{X})$、安全查询矩阵$E(\boldsymbol{X})$和密钥$\boldsymbol{K}$的存储成本。

表6为特征向量维数N为128时本文方案的存储成本。结果表明，$E(\boldsymbol{X})$的存储成本随图像数量的增加而上升，因为每幅图像都会生成一个$E(\boldsymbol{X})$进行

存储。而 $E(\boldsymbol{Y})$ 和 $\boldsymbol{K}$ 的大小都固定为 1.28 KB，不受图像数量影响，因为它们都是 $n \times n$ 的矩阵，其尺寸由 $n = \left\lceil \sqrt{N+4} \right\rceil$ 决定，与图像数量无关。

表 6　特征向量维数 N 为 128 时本文方案的存储成本

m	$E(\boldsymbol{X})$/KB	$E(\boldsymbol{Y})$/KB	$\boldsymbol{K}$/KB
1 000	9.02	1.28	1.28
5 000	43.03	1.28	1.28
10 000	87.62	1.28	1.28

表 7 为在 5 000 幅图像组成的图像集上本文方案的存储成本。可以观察到，$E(\boldsymbol{X})$、$E(\boldsymbol{Y})$ 和 $\boldsymbol{K}$ 的大小均随 N 增加，因为当图像数量固定时，包括 $E(\boldsymbol{X})$ 在内，其尺寸都是随着特征向量维数 N 的增加而增大，因为矩阵的维数 n 直接受到 N 的影响。因此，在实际应用中，可以根据设备的存储能力和处理能力选择合适的特征向量维数，以确保整个系统的高效运行。

表 7　在 5 000 幅图像组成的图像集上本文方案的存储成本

N	$E(\boldsymbol{X})$/KB	$E(\boldsymbol{Y})$/KB	$\boldsymbol{K}$/KB
64	26.01	0.78	0.78
128	43.03	1.28	1.28
256	82.03	2.44	2.44

7　结束语

为了应对云辅助物联网环境中图像安全检索的挑战，本文提出了一种可验证的安全图像检索方案。利用 CNN 模型生成低维索引和查询，有效提升了检索准确性。通过改进的基于 LWE 的安全 kNN 算法增强了索引和查询的安全性，使生成的安全索引矩阵和安全查询矩阵能够在已知背景模型下抵抗线性分析攻击。与现有方案相比，本文方案显著减少了索引、查询和密钥的存储需求，从而提高了通信和计算效率。此外，由分布式不可篡改的区块链替代传统的第三方审计中心，结合 4-MHT 和高效的短签名算法实现了搜索结果验证，并为验证失败提供了有效的处理措施，减轻了用户的计算负担。安全性分析和理论复杂度的比较验证了本文方案在保证索引和查询安全性的同时提高了检索效率。实验结果进一步证明了本文方案在物联网环境中的实用性。

参考文献：

[1] LI X Q, YANG J S, MA J W. Recent developments of content-based image retrieval (CBIR)[J]. Neurocomputing, 2021, 452: 675-689.

[2] WAN J, WANG D Y, HOI S C H, et al. Deep learning for content-based image retrieval[C]//Proceedings of the 22nd ACM International Conference on Multimedia. New York: ACM Press, 2014: 157-166.

[3] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceedings of the Proceeding 2000 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2000: 44-55.

[4] LU W J, SWAMINATHAN A, VARNA A L, et al. Enabling search over encrypted multimedia databases[C]//Proceedings of the Media Forensics and Security. Piscataway: IEEE Press, 2009: 404-414.

[5] WONG W K, CHEUNG D W, KAO B, et al. Secure kNN computation on encrypted databases[C]//Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. New York: ACM Press, 2009: 139-152.

[6] YAO B, LI F F, XIAO X K. Secure nearest neighbor revisited[C]//Proceedings of the 2013 IEEE 29th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2013: 733-744.

[7] BRAKERSKI Z, GENTRY C, HALEVI S. Packed ciphertexts in LWE-based homomorphic encryption[C]//International Conference on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2013: 1-13.

[8] YUAN J W, TIAN Y F. Practical privacy-preserving MapReduce based K-means clustering over large-scale dataset[J]. IEEE Transactions on Cloud Computing, 2019, 7(2): 568-579.

[9] LI Y Y, MA J F, MIAO Y B, et al. Secure and verifiable multikey image search in cloud-assisted edge computing[J]. IEEE Transactions on Industrial Informatics, 2020, 17(8): 5348-5359.

[10] KHAN S, ABBAS H, IQBAL W. Verifiable privacy-preserving image retrieval in multi-owner multi-user settings[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2024, 8(2): 1640-1655.

[11] LU X Q, PAN Z K, XIAN H Q. An integrity verification scheme of cloud storage for Internet-of-things mobile terminal devices[J]. Computers & Security, 2020, 92: 101686.

[12] XIA Z H, WANG X H, ZHANG L G, et al. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2594-2608.

[13] ANJU J, SHREELEKSHMI R. A faster secure content-based image retrieval using clustering for cloud[J]. Expert Systems with Applications, 2022, 189: 116070.

[14] SHEN M, CHENG G H, ZHU L H, et al. Content-based multi-source encrypted image retrieval in clouds with privacy preservation[J]. Future Generation Computer Systems, 2020, 109: 621-632.

[15] KUMAR S, PAL A K, ISLAM S H, et al. Secure and efficient image retrieval through invariant features selection in insecure cloud environments[J]. Neural Computing and Applications, 2023, 35(7): 4855-4880.

[16] YANG T F, MA J F, MIAO Y B, et al. MU-TEIR: traceable encrypted image retrieval in the multi-user setting[J]. IEEE Transactions on Services Computing, 2023, 16(2): 1282-1295.

[17] LI D, LÜ Q G, LIAO X F, et al. AVPMIR: adaptive verifiable privacy-

preserving medical image retrieval[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(5): 4637-4651.

[18] ZHANG Y, ZHUO L, PENG Y F, et al. A secure image retrieval method based on homomorphic encryption for cloud computing[C]// Proceedings of the 2014 19th International Conference on Digital Signal Processing. Piscataway: IEEE Press, 2014: 269-274.

[19] WANG Y, CHEN L Q, WU G, et al. Efficient and secure content-based image retrieval with deep neural networks in the mobile cloud computing[J]. Computers & Security, 2023, 128: 103163.

[20] GE C P, SUSILO W, BAEK J, et al. A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 2907-2919.

[21] HU B L, ZHANG K, GONG J Q, et al. Designated server proxy re-encryption with Boolean keyword search for e-health clouds[J]. Journal of Information Security and Applications, 2024, 83: 103783.

[22] LI X, XUE Q H, CHUAH M C. CASHEIRS: Cloud assisted scalable hierarchical encrypted based image retrieval system[C]//Proceedings of the IEEE INFOCOM 2017 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2017: 1-9.

[23] ZHU D, ZHU H, WANG X Y, et al. An accurate and privacy-preserving retrieval scheme over outsourced medical images[J]. IEEE Transactions on Services Computing, 2023, 16(2): 913-926.

[24] SONG L, MIAO Y B, WENG J, et al. Privacy-preserving threshold-based image retrieval in cloud-assisted Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(15): 13598-13611.

[25] GU Q, XIA Z H, SUN X M. MSPPIR: Multi-source privacy-preserving image retrieval in cloud computing[J]. Future Generation Computer Systems, 2022, 134: 78-92.

[26] 李颖莹, 马建峰, 苗银宾. 基于边缘计算的支持多密钥的加密图像检索[J]. 通信学报, 2020, 41(4): 14-26.
LI Y Y, MA J F, MIAO Y B. Encrypted image retrieval in multi-key settings based on edge computing[J]. Journal on Communications, 2020, 41(4): 14-26.

[27] 宋甫元, 秦拯, 张吉昕, 等. 基于访问控制安全高效的多用户外包图像检索方案[J]. 网络与信息安全学报, 2021, 7(5): 29-39.
SONG F Y, QIN Z, ZHANG J X, et al. Efficient and secure multi-user outsourced image retrieval scheme with access control[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 29-39.

[28] ZHANG S B, LIU Q, WANG T, et al. FSAIR: fine-grained secure approximate image retrieval for mobile cloud computing[J]. IEEE Internet of Things Journal, 2024, 11(13): 23297-23308.

[29] LIU Z P, WANG S, LIU Y. Blockchain-based integrity auditing for shared data in cloud storage with file prediction[J]. Computer Networks, 2023, 236: 110040.

[30] 陈建伟, 王姝妤, 张美平, 等. 基于区块链且可验证的智能电网多维数据聚合与分享方案[J]. 通信学报, 2024, 45(1): 167-179.
CHEN J W, WANG S Y, ZHANG M P, et al. Blockchain-based and verifiable multidimensional data aggregation and sharing scheme for smart grid[J]. Journal on Communications, 2024, 45(1): 167-179.

[31] MERKLE R C. A certified digital signature[C]//Proceedings of the Advances in Cryptology. Berlin: Springer, 2007: 218-238.

[32] ZHANG F G, SAFAVI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]///Proceedings of the 7th International Workshop on the theory and Practice in Public Key Cryptography. Berlin: Springer, 2004: 277-290.

[33] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319.

[34] KRIZHEVSKY A, HINTON G. Learning multiple layers of features from tiny images[R]. 2009.

[35] XIAO H, RASUL K, VOLLGRAF R. Fashion-MNIST: a novel image dataset for benchmarking machine learning algorithms[J]. arXiv Preprint, arXiv: 1708.07747, 2017.

[36] GRIFFIN G, HOLUB A, PERONA P. Caltech-256 object category dataset[R]. 2007.

[作者简介]

郭佳琦（1990– ），女，陕西宝鸡人，西安电子科技大学博士生，主要研究方向为云计算安全、应用密码学。

马智（1994– ），男，博士，陕西西安人，西安电子科技大学讲师，主要研究方向为操作系统、形式化验证和嵌入式软件。

王文胜（1993– ），男，博士，河北衡水人，西安电子科技大学讲师，主要研究方向为自动机理论、时序逻辑、可信人工智能。

田聪（1981– ），女，博士，陕西渭南人，西安电子科技大学教授、博士生导师，主要研究方向为软件安全、智能软件开发方法、可信软件基础理论与方法。

段振华（1948– ），男，博士，陕西咸阳人，西安电子科技大学教授、博士生导师，主要研究方向为形式化方法、可信软件基础理论与方法。