

基于访问控制安全高效的多用户外包图像检索方案

宋甫元¹, 秦拯¹, 张吉昕², 刘羽¹

(1. 湖南大学信息科学与工程学院, 湖南 长沙 410082;

2. 湖北工业大学计算机学院, 湖北 武汉 430068)

摘要: 由于公有云不是可信的实体, 通过公有云提供图像检索服务时, 它可能会窃取图像数据的敏感信息。近年来, 密文图像检索方法被提出, 用于保护图像隐私。然而, 传统的隐私保护图像检索方案搜索效率较低, 且无法支持多用户场景。因此, 提出一种基于访问控制安全高效的多用户外包图像检索方案。该方案采用一次一密和矩阵变换方法, 实现基于欧几里得距离(简称欧氏距离)相似性的密文图像检索, 并利用矩阵分解和代理重加密, 实现多用户外包图像检索。采用局部敏感哈希算法构建索引, 提高密文图像检索效率。特别地, 提出一种基于角色多项式函数的轻量级访问控制策略, 该策略能够灵活设定图像访问权限, 防止恶意用户窃取隐私信息。安全性分析论证了所提方案能够保护图像和查询请求的机密性; 实验结果表明所提方案能够达到高效的图像检索。

关键词: 图像检索; 可搜索加密; 隐私保护; 访问控制

中图分类号: TP309

文献标识码: A

DOI: 10.11959/j.issn.2096-109x.2021076

Efficient and secure multi-user outsourced image retrieval scheme with access control

SONG Fuyuan¹, QIN Zheng¹, ZHANG Jixin², LIU Yu¹

1. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

2. School of Computer Science, Hubei University of Technology, Wuhan 430068, China

Abstract: In the cloud-based image retrieval services, the cloud server may not be fully trusted in which may arise privacy concerns. Some privacy-preserving image retrieval schemes have been proposed to protect image privacy. However, the traditional privacy-preserving image retrieval schemes have some weaknesses, such as inefficient and single-user setting. Therefore, an efficient and secure multi-user outsourced image retrieval (EMIR) scheme with

收稿日期: 2020-12-03; 修回日期: 2021-01-18

通信作者: 秦拯, zqin@hnu.edu.cn

基金项目: 国家自然科学基金(61772191, 61902123, 62002112, 62002106); 长沙市科技计划项目(kq2004025, kq2004027); 湖南省科技计划重点资助项目(2015TP1004, 2018TP1009, 2020JJ5085, 2018TP3001)

Foundation Items: The National Natural Science Foundation of China (61772191, 61902123, 62002112, 62002106), The Science and Technology Projects of Changsha (kq2004025, kq2004027), The Science and Technology Key Projects of Hunan Province (2015TP1004, 2018TP1009, 2020JJ5085, 2018TP3001)

论文引用格式: 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.

access control was proposed. EMIR utilized matrix decomposition and proxy re-encryption to achieve multi-user outsourced image retrieval. By leveraging the techniques of one-time pad and matrix transformation, EMIR supported efficient and secure image retrieval based on Euclidean distance similarity in a privacy-preserving manner. In addition, EMIR applied locality sensitive hashing (LSH) to build searchable indexes in a privacy-preserving manner, which could improve the image retrieval performance. Specifically, a lightweight access control strategy by using role-based polynomial function was designed to authorize the legality of the query user. Security analysis shows that EMIR can protect the confidentiality of the images and the queries. The extensive experiments demonstrate that EMIR achieves efficient image retrieval.

Keywords: image retrieval, searchable encryption, privacy-preserving, access control

1 引言

图像检索是一种基于内容（如图像特征、图像纹理等）在大规模图像数据集上高效搜索的技术^[1]，在诸多领域已经有广泛的应用，如图像识别、目标检测等。一方面，随着移动设备以及无线通信的快速发展，图像数据规模呈爆炸性增长趋势，然而，大规模图像数据的存储以及检索需要耗费巨大的存储资源和计算开销。另一方面，随着云计算的普及与应用，越来越多的企业将大规模图像数据外包到云平台上，这样既可以享受云平台强大的计算能力和充足的存储空间，缓解本地的存储和计算压力，也可以更好地面向公众提供图像检索服务^[2]。在基于云计算的图像检索中，数据拥有者将本地的图像外包到云平台上，用于提供图像检索服务。查询用户发送图像查询请求给云平台，期望获取存储于云平台中所匹配的图像，当云平台收到查询用户的查询请求后，云平台检索存储的图像，并返回匹配的查询结果给查询用户。然而，图像中可能包含丰富的敏感信息，如患者的医疗影像、用户的地理位置等。如果数据拥有者直接将未加密的图像外包到云平台上，云平台出于利益将会窃取其中的敏感数据，从而导致隐私信息泄露。另外，恶意用户可能会伪装成合法用户访问数据，这将带来敏感图像隐私泄露问题。因此，亟须研究一种云计算环境下基于访问控制策略的安全外包图像检索方案，防止用户的图像隐私信息和查询请求被窃取。

为了保护用户的图像隐私信息和查询请求，在外包图像数据和发送查询请求前，数据拥有者和查询用户采用加密算法加密各自的图像数据集和查询请求^[3]。尽管图像加密能够保护图像隐私，

但在密文环境下，图像检索的准确率和效率将会受到极大的影响。传统的可搜索加密方案难以支持多用户环境下的大规模图像检索^[4]。因此，针对多用户场景下，如何进行高效的大规模密文图像检索仍然是一个挑战。

目前，已有研究者展开了隐私保护图像检索的研究^[1,3,5]。为了保护图像隐私，一些工作基于同态加密^[6]和安全多方计算^[7]提出了隐私保护图像检索方案。然而，传统的加密算法效率较低，限制了图像检索的速度。为了提高图像检索效率，Li 等提出了基于 R-tree 的索引构建方法^[8]，但是该方法会降低图像检索的准确率。另外，现有的图像检索方案仅能支持单用户图像检索^[9-11]，但现实应用中需要面向多用户提供图像检索服务。另外，用户可能不是诚实可信的，一些恶意用户会伪装成合法用户窃取图像中的隐私信息，从而导致图像隐私泄露风险。因此，数据拥有者需要针对外包图像数据设置访问控制策略，认证查询用户的访问权限，保障图像数据的安全。

针对以上问题，本文提出一种面向多用户高效且安全的外包图像检索方案。本文的主要贡献可以归纳为如下几点。

(1) 本文基于局部敏感哈希算法，提出了一种安全高效的外包图像检索方案，该方案可以实现快速的密文图像搜索。

(2) 本文基于角色多项式函数，设计了一种轻量级的访问控制策略，实现了查询用户的授权认证，防止恶意用户窃取图像隐私。另外，本文采用代理重加密方法，实现了多用户场景下的密文图像搜索。

(3) 安全性分析表明本文的方案能够在定义的威胁模型下保护外包图像、检索结果和查询请

求的隐私。实验结果表明本文的方案在大规模真实图像数据集下能够达到高效的图像检索。

2 准备知识

2.1 访问控制

访问控制是指用户能够对自身的文件、数据设定权限，只有授权的用户才能访问数据。一种通用的访问控制机制是基于用户角色设定访问控制策略。本文利用基于角色的多项式函数设计了一种轻量级的访问控制策略，其中，多项式函数的根可以用多项式函数的系数表示。本文采用通用的 Vieta 函数^[12] $g(x) = c_n x^n + \dots + c_1 x + c_0 = c_n (x - x_n) \dots (x - x_1)$ 表示基于角色的多项式函数，其中， c_i 表示 x^i 的系数， $x_1, \dots, x_n$ 表示多项式函数 $g(x)$ 的根。特别地，本文假设用户的角色可以用一个整数 z_i 表示，那么只有与 z_i 相关的文件才能被用户访问。对于一个设定权限的数据集，假设可访问数据集的角色集合为 $\delta = \{z_1, z_2, \dots, z_k\}$ ，只有当用户的角色属于集合 δ 时，用户才可以访问该数据集。因此，访问控制策略可以用多项式函数 $g(s) = \prod_{z_i \in \delta} (s - z_i) = \sum_{i=0}^k \hat{z}_i s^i$ 表示。为了达到访问控制的目的，数据拥有者需要设定可访问数据集的角色作为多项式函数的根。也就是说，判断一个用户是否能访问数据集等价于判断用户的角色是否为多项式函数的根。本文设计的访问控制策略定义如下。

定义 1 访问控制策略。对于一个数据集 D ，给定可访问数据集的角色集合 $\delta = \{z_1, z_2, \dots, z_k\}$ ，一个基于角色的多项式函数可被构造为 $g(s) = \prod_{z_i \in \delta} (s - z_i) = \hat{z}_k s^k + \dots + \hat{z}_0 = \sum_{i=0}^k \hat{z}_i s^i$ ，其中， $\hat{z}_k = 1$ ， $\hat{z}_{k-1} = -\sum_{i=1}^k z_i$ ， $\hat{z}_0 = (-1)^k \prod_{i=1}^k z_i$ 。那么用户能够访问该数据集 D ，当且仅当用户的角色是多项式函数 $g(s)$ 的根。

2.2 局部敏感哈希

局部敏感哈希是一种哈希算法，主要运用在高速海量数据的快速近似查找与检索，效果极其显著。近似查找是指比较数据点之间的距离或者相似度。局部敏感哈希的主要思想是根据高维向量之间的距离判定哈希值概率，当两向量距离很

近，那么设计一种哈希函数计算两向量的哈希值，使二者哈希值相同的概率较大。同时，若两向量之间的距离较远，它们哈希值相同的概率较小。本文给出局部敏感哈希定义如下。

定义 2 局部敏感哈希。给定一族哈希函数 H ， H 是一个从欧式空间 S 到哈希编码空间 U 的映射， dist 表示两点的欧式距离。对于任意 $x, y \in S$ ，如果以下两个条件都满足，则称该哈希函数满足 (r_1, r_2, p_1, p_2) 性^[3]。

- (1) 若 $\text{dist}(x, y) \leq r_1$ ，则 $\Pr[h(x) = h(y)] \geq p_1$ 。
- (2) 若 $\text{dist}(x, y) \geq cr_2$ ，则 $\Pr[h(x) = h(y)] \leq p_2$ 。

3 系统模型、威胁模型及设计目标

3.1 系统模型

本文的系统模型如图 1 所示，主要包含 4 个实体：云服务器、数据拥有者、查询用户、可信机构。

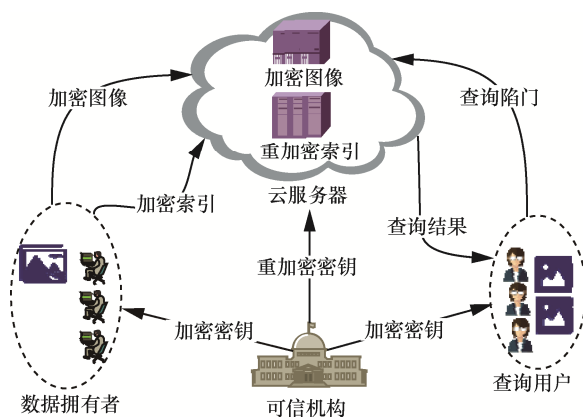


图 1 系统模型
Figure 1 System model

(1) 数据拥有者

数据拥有者是图像数据的所有者。在外包图像之前，数据拥有者先用对称加密算法（如 AES）加密图像数据集，并把图像特征向量提取出来，构建加密的检索索引，然后，数据拥有者把加密索引和加密图像数据集上传到云服务器上。此外，数据拥有者为图像数据集设定访问策略，用于认证查询用户的访问权限。

(2) 云服务器

云服务器具备充足的存储空间和强大的计算能力，主要负责存储数据拥有者的图像数据，并为查询用户提供图像检索服务。

(3) 查询用户

查询用户根据查询图像生成相应的查询陷门，并将加密的查询陷门提交到云服务器。云服务器收到查询请求后，进行密文图像检索，并返回匹配的密文图像给查询用户。

(4) 可信机构

可信机构负责初始化系统安全参数，生成加密密钥和重加密密钥，并分发给数据拥有者、查询用户以及云服务器。

3.2 威胁模型

本文的威胁模型中，可信机构和数据拥有者是完全可信的。云服务器是半可信的，云服务器会按照设计的协议执行图像检索算法。然而，云服务器对存储于其中的图像数据和用户的查询请求非常好奇，可能会出于利益窃取用户的图像数据和查询请求。查询用户部分是可信的，部分是半可信的，需要通过访问控制策略认证用户的访问权限。根据云服务器拥有的知识^[13]，本文主要考虑以下两种攻击模型。

(1) 已知明文攻击：云服务器能够获取图像数据集中的部分明文-密文对。

(2) 已知背景攻击：相较于已知明文攻击，云服务器拥有更强的攻击能力。云服务器能够提取图像数据集中特定加密图像的统计特征，利用统计分析推测出图像特征向量，甚至加密图像对应的明文图像。

3.3 设计目标

本文的目标是设计一种云计算环境下高效且安全的多用户外包图像检索方案。特别地，本文所提的方案需要达到以下几点需求。

(1) 多用户

本文所提的方案应支持多数据拥有者多查询用户场景下的外包图像检索，并且数据拥有者和查询用户之间无须共享对称密钥，查询用户可以使用随机生成的密钥加密查询陷门。

(2) 隐私保护

图像内容、特征向量、查询请求以及查询结果的隐私信息应该被保护，云服务器不能够窃取它们的隐私数据。此外，陷门不可链接，云服务器不能够推测两个或者多个检索结果是否与同一个查询请求匹配。

(3) 高效性

本文所提出的方案在陷门生成、索引构造、图像检索过程中的时间开销应较低，且不能降低图像检索的准确率。

4 多用户图像检索方案设计

本节介绍提出的基于访问控制安全高效的多用户外包图像检索方案。在图像检索方案中，本文利用主成分分析方法提取图像的特征向量，并对图像的 Fisher 矢量进行降维。另外，本文采用欧氏距离相似性衡量两图像所对应特征向量之间的相似度，从而为查询图像匹配到与之相似的图像。本节首先介绍密文图像检索方案的构造细节，然后分析密文图像检索方案的正确性。

4.1 多用户图像检索方案

本文的多用户图像检索方案包括 4 个算法：密钥生成、索引构建、陷门生成、图像搜索。

4.1.1 密钥生成

给定一个安全参数 λ ，可信机构首先随机生成一个 $(n+3+k) \times (n+3+k)$ 正交矩阵 $\mathbf{M}$ ，将该矩阵与其对应的转秩矩阵 $\mathbf{M}^T$ 作为密钥。对于数据拥有者，可信机构利用 QR 分解方法生成一个正交矩阵 $\mathbf{M}_{Q_1}$ 和一个上三角矩阵 $\mathbf{M}_{Q_2}$ ，即 $\mathbf{M} = \mathbf{M}_{Q_1} \mathbf{M}_{Q_2}$ 。可信机构将密钥 $\mathbf{M}_{Q_1}$ 发送给数据拥有者，将重加密密钥 $\mathbf{M}_{Q_2}$ 分发给云服务器。类似地，对于查询用户，可信机构也采用 QR 分解方法生成一个正交矩阵 $\mathbf{M}_{S_2}^T$ 和一个上三角矩阵 $\mathbf{M}_{S_1}^T$ ，即 $\mathbf{M}^T = \mathbf{M}_{S_1}^T \mathbf{M}_{S_2}^T$ 。可信机构将密钥 $\mathbf{M}_{S_2}^T$ 发送给查询用户，将重加密密钥 $\mathbf{M}_{S_1}^T$ 发送给云服务器。此外，对于数据拥有者，可信机构随机生成一个对称密钥 K ，并利用对称加密算法（如 AES）加密图像数据集。与此同时，可信机构随机生成一个置换 π ，并将置换 π 分发给数据拥有者和查询用户。

4.1.2 索引构建

在索引构建过程中，主要分为两个阶段：构建哈希桶和建立索引。第一步构建哈希桶，利用局部敏感哈希算法，将相似的图像（即哈希值相同的图像）放到同一个桶内。通过局部敏感哈希算法，可以过滤掉不相似的图像，极大地减少图像检索的搜索空间，提高图像检索效率。第二步

提取图像特征向量，建立并加密索引。

(1) 构建哈希桶。在哈希桶构建过程中，利用哈希函数 H 哈希所有图像的特征向量，并根据哈希值构建哈希桶。其中，对于图像数据集中的每一个特征向量 $\{F_1, F_2, \dots, F_m\}$ ，本文采用哈希映射可得 l 维的哈希向量，即 $H(F_i) = (h_1(F_i), h_2(F_i), \dots, h_l(F_i))$ 。则哈希桶值相同的图像可以归类为相似图像。令 $\{BKT_b\}_{b=1}^N$ 表示一系列哈希桶的集合，其中 N 表示哈希桶的数量。为了避免图像特征向量隐私泄露，本文采用单向哈希函数 ϕ 映射哈希桶中的每个桶的哈希值，其中哈希函数 ϕ 由可信机构生成。

(2) 建立索引。在索引建立过程中，数据拥有者首先利用主成分分析方法提取图像的特征向量 $F_i = (f_{i,1}, f_{i,2}, \dots, f_{i,n})$ 。然后，数据拥有者将图像特征向量 F_i 扩充为 $n+3+k$ 维向量，如式(1)所示。

$$\hat{F}_i = (\alpha f_{i,1}, \alpha f_{i,2}, \dots, \alpha f_{i,n}, \alpha \left(-\sum_{j=1}^n f_{i,j}^2 \right), 1, \hat{z}_0, \dots, \hat{z}_k) \quad (1)$$

其中， α 为一次一密随机正数， $\{\hat{z}_i\}_{i=0}^k$ 为基于角色的多项式函数 $g(s)$ 的系数。随后，数据拥有者基于置换 π 将扩充后的向量 $\hat{F}_i$ 进行随机置换（置换过程中，分别对前 $n+1$ 个数置换，以及后 $k+2$ 个数置换），即 $\tilde{F}_i = \pi(\hat{F}_i)$ 。置换完成后，数据拥有者用自己的密钥 M_{O_i} 对每一个置换向量进行加密，如式(2)所示。

$$\text{Enc}_{M_{O_i}}(\tilde{F}_i) = \tilde{F}_i M_{O_i} \quad (2)$$

接着，数据拥有者将加密的图像和索引（特征向量和哈希桶）外包到云服务器中。当云服务器收到加密的特征向量时，云服务器利用可信机构分解的重加密密钥（上三角矩阵 M_{O_2} ）转换加密的特征向量，如式(3)所示。

$$\text{Enc}_M(\tilde{F}_i) = \text{Enc}_{M_{O_i}}(\tilde{F}_i) M_{O_2} \quad (3)$$

通过索引转换的方式，云服务器可以将不同密钥系统下的查询陷门和索引转换为相同密钥系统下的陷门和索引，从而实现多用户在密文环境下进行欧式距离相似度的比较。

4.1.3 陷门生成

在陷门生成过程中，查询用户首先提取出查询图像对应的特征向量 $Q = (q_1, q_2, \dots, q_n)$ ，并计算

查询图像对应的哈希桶值 $BKT_Q = H(Q)$ 。同时，

为了保护查询图像哈希桶值的机密性，查询用户同样使用可信机构生成的单向哈希函数 ϕ ，将哈希桶值 BKT_Q 映射为 $\phi(BKT_Q)$ 。然后，查询用户将查询图像的特征向量 Q 扩充为式(4)。

$$\hat{Q} = (\beta q_1, \beta q_2, \dots, \beta q_n, \beta, \gamma, 1, s, s^2, \dots, s^k) \quad (4)$$

其中， β, γ 为一次一密随机正数， s 表示查询用户的角色值。随后，与索引置换类似，查询用户利用置换函数 π 将扩充向量 $\hat{Q}$ 置换为 $\tilde{Q} = \pi(\hat{Q})$ 。置换结束后，查询用户用自己的密钥 $M_{S_2}^T$ 加密置换向量，得到查询陷门，如式(5)所示。

$$T_Q = M_{S_2}^T \tilde{Q} \quad (5)$$

查询用户将查询陷门和查询图像的哈希桶值 $\{T_Q, \phi(BKT_Q)\}$ 一起提交给云服务器，用于密文图像检索。

4.1.4 图像搜索

在图像搜索中，当云服务器收到查询用户发送的查询陷门及哈希桶值时，云服务器首先对查询用户的合法性进行认证。根据定义 1，云服务器计算查询用户的角色值 s ，并根据角色值 s 是否符合基于角色的多项式函数的根来判断用户的访问权限，即判断等式 $g(s) = \sum_{i=0}^k \hat{z}_i s^i = 0$ 是否成立。

当该等式成立时，说明查询用户的角色满足数据拥有者设定的访问控制策略。

然后，云服务器根据查询图像的哈希桶值 $\phi(BKT_Q)$ 寻找到与查询图像相似的图像。通过局部敏感哈希的方式，云服务器能够快速过滤掉不相似的图像，并在相似图像的桶内进行密文检索，能够极大地缩小密文图像的搜索空间。为了实现多用户的图像检索，云服务器需要利用重加密密钥，将查询用户的查询陷门进行转换，从而使查询陷门和索引是在相同密钥下加密所得。也就是说，云服务器利用重加密密钥 $M_{S_1}^T$ 将查询陷门转换为式(6)。

$$T'_Q = M_{S_1}^T T_Q \quad (6)$$

云服务器利用欧氏距离相似性方法计算与查询图像哈希值相同的图像，并对这些图像按照欧氏距离相似度高到低进行排序。排序完成后，云服务器将前 k 个相似图像返回给查询用户，即

图像数据集中与查询图像相似的 top- k 图像。满足访问控制策略的查询用户再利用可信机构发送的密钥 K 解密图像, 得到明文图像。

4.2 方案的正确性分析

本文提出的多用户外包图像检索方案能够根据加密索引与加密陷门的内积, 正确计算并返回 top- k 相似图像。本节给出方案正确性分析, 定理如下。

定理 1 正确性。在多用户外包图像检索方案的密文图像检索中, 对于两幅图像对应的特征向量 $\mathbf{F}_i, \mathbf{F}_j$, 云服务器可以通过对应的加密索引和加密陷门之间的内积大小关系, 确定两特征向量与查询图像对应的特征向量 $\mathbf{Q}$ 之间欧氏距离的大小关系。也就是说, $\text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q \geq \text{Enc}_M(\tilde{\mathbf{F}}_j) \circ T'_Q$ 等价于 $\text{dist}(\mathbf{F}_i, \mathbf{Q}) \leq \text{dist}(\mathbf{F}_j, \mathbf{Q})$ 。

证明 由于密钥 $\mathbf{M}$ 为正交矩阵, 则 $\mathbf{M}\mathbf{M}^T = \mathbf{I}$, 其中 $\mathbf{I}$ 表示单位矩阵。重加密索引与重加密陷门的内积可表示为式(7)和式(8):

$$\text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q = \text{Enc}_{M_O}(\tilde{\mathbf{F}}_i) \mathbf{M}_{O_2} \mathbf{M}_{S_1}^T T'_Q = \tilde{\mathbf{F}}_i \mathbf{M} \mathbf{M}^T \tilde{\mathbf{Q}} = \tilde{\mathbf{F}}_i \circ \tilde{\mathbf{Q}} \quad (7)$$

$$\text{Enc}_M(\tilde{\mathbf{F}}_j) \circ T'_Q = \text{Enc}_{M_O}(\tilde{\mathbf{F}}_j) \mathbf{M}_{O_2} \mathbf{M}_{S_1}^T T'_Q = \tilde{\mathbf{F}}_j \mathbf{M} \mathbf{M}^T \tilde{\mathbf{Q}} = \tilde{\mathbf{F}}_j \circ \tilde{\mathbf{Q}} \quad (8)$$

由于本文有置换 $\tilde{\mathbf{F}}_i = \pi(\hat{\mathbf{F}}_i)$ 和 $\tilde{\mathbf{Q}} = \pi(\hat{\mathbf{Q}})$, 则等式 $\tilde{\mathbf{F}}_i \circ \tilde{\mathbf{Q}} = \hat{\mathbf{F}}_i \circ \hat{\mathbf{Q}}$ 成立。从而式(7)可以等价转换为式(9)。

$$\text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q = \alpha\beta \sum_{w=1}^n f_{i,w} q_w - \frac{1}{2} \alpha\beta \sum_{w=1}^n f_{i,w}^2 + \gamma + g(s) \quad (9)$$

根据定义 1, 查询用户能够访问图像数据, 当且仅当查询用户的角色是多项式函数 $g(s)$ 的根, 即 $g(s)=0$ 。因此, 等式 $\text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q = \alpha\beta \sum_{w=1}^n f_{i,w} q_w - \frac{1}{2} \alpha\beta \sum_{w=1}^n f_{i,w}^2 + \gamma$ 成立。故而, 明文索引与明文陷门的欧式距离的比较关系如式(10)所示。

$$\begin{aligned} \text{dist}^2(\mathbf{F}_i, \mathbf{Q}) - \text{dist}^2(\mathbf{F}_j, \mathbf{Q}) &= \\ \sum_{w=1}^n (f_{i,w} - q_w)^2 - \sum_{w=1}^n (f_{j,w} - q_w)^2 &= \end{aligned}$$

$$\begin{aligned} &\frac{2}{\alpha\beta} \sum_{w=1}^n \left(\alpha\beta f_{j,w} q_w - \frac{1}{2} \alpha\beta f_{j,w}^2 + \gamma \right) - \\ &\frac{2}{\alpha\beta} \sum_{w=1}^n \left(\alpha\beta f_{i,w} q_w - \frac{1}{2} \alpha\beta f_{i,w}^2 + \gamma \right) = \\ &\frac{2}{\alpha\beta} \{ \text{Enc}_M(\tilde{\mathbf{F}}_j) \circ T'_Q - \text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q \} \end{aligned} \quad (10)$$

由于 $\alpha > 0$ 且 $\beta > 0$, 可得 $\text{Enc}_M(\tilde{\mathbf{F}}_i) \circ T'_Q \geq \text{Enc}_M(\tilde{\mathbf{F}}_j) \circ T'_Q \Leftrightarrow \text{dist}(\mathbf{F}_i, \mathbf{Q}) \leq \text{dist}(\mathbf{F}_j, \mathbf{Q})$ 。因此, 定理 1 的正确性证毕。

5 方案安全性分析

本节分析方案的安全性, 其中包括图像安全性、索引和查询陷门的机密性、以及查询陷门的不可链接性。

5.1 图像安全性

由于本文提出的基于访问控制的多用户外包图像检索方案中, 数据拥有者在外包图像数据集之前, 首先采用 AES 对所有图像进行加密, 然后将加密的图像数据集发送给云服务器。因此, 云服务器无法窃取图像数据, 从而图像安全性得到保证。

5.2 索引和查询陷门的机密性

对于已知明文攻击模型, 本方案可以保护索引的机密性, 分析如下: 数据拥有者的索引将会按照 $\text{Enc}_{M_O}(\tilde{\mathbf{F}}_i) = \tilde{\mathbf{F}}_i \mathbf{M}_{O_1}$ 加密后上传给云服务器。云服务器收到加密索引后, 云服务器利用重加密密钥, 将加密索引转换为 $\text{Enc}_{M_O}(\tilde{\mathbf{F}}_i) = \text{Enc}_{M_O}(\tilde{\mathbf{F}}_i) \mathbf{M}_{O_2} = \tilde{\mathbf{F}}_i \mathbf{M}_{O_1} \mathbf{M}_{O_2}$ 。如式(3)所示, 加密函数中, 云服务器只拥有重加密密钥 $\mathbf{M}_{O_2}$ 中的 $(n+3+k)^2$ 个元素, 然而 $\tilde{\mathbf{F}}_i$ 和 $\mathbf{M}_{O_1}$ 中分别含有 $n+3+k$ 和 $(n+3+k)^2$ 个未知元素, 总共含有 $n^2 + k^2 + 2nk + 7n + 7k + 12$ 个未知变量。然而, 云服务器只拥有 $n+3+k$ 个函数方程。根据 Yuan 等^[14]提出的基于误差学习 (LWE, learning with error) 问题, 方程不可解的安全性已得到论证。因此, 云服务器从密文 $\text{Enc}_M(\tilde{\mathbf{F}}_i)$ 中恢复明文 $\mathbf{F}_i$ 是一个 LWE 问题。即使云服务器拥有部分明-密文对, 它也不能够还原出明文 $\mathbf{F}_i$, 索引的机密性得到保护。同理, 查询陷门的机密性在已知明文攻击模型下也能够得到保护。

对于已知背景攻击模型，本方案同样可以保护索引的机密性，分析如下：图像索引构建过程中，经过了扩充和置换操作。首先，本文针对特征向量进行扩充，在扩充后的向量 $\hat{\mathbf{F}}_i = (\alpha f_{i,1}, \alpha f_{i,2}, \dots, \alpha f_{i,n}, \alpha(-\sum_{j=1}^n f_{i,j}^2), 1, \hat{z}_0, \dots, \hat{z}_k)$ 中，方案中加入了一次一密的随机数 α ，即使云服务器统计特征向量的词频和分布，它也不能够恢复出特征向量 $\mathbf{F}_i$ 。其次，对于图像数据集中的任意特征向量 $\mathbf{F}$ ，假设特征向量集合 $\mathbf{A}_F = \mathbf{F}^T \mathbf{F}$ 成立，那么存在无限的正交矩阵对 $\{\mathbf{A}, \mathbf{A}^T\}$ ，使得等式(11)成立。

$$\mathbf{A}_F = \mathbf{F}^T \mathbf{F} = \mathbf{F}^T \mathbf{I} \mathbf{F} = \mathbf{F}^T \mathbf{A}^T \mathbf{A} \mathbf{F} = (\mathbf{A} \mathbf{F})^T (\mathbf{A} \mathbf{F}) \quad (11)$$

由于等式(11)中包含无限的正交矩阵 $\mathbf{A}$ ，那么必定存在无限的矩阵 $\mathbf{A} \mathbf{F}$ 。也就是说，图像的特征向量集合 $\mathbf{A}_F$ 有无穷多种组合形式。因此，即使云服务器获取了部分明-密文对，以及分析特征向量的统计信息，它也不能够还原图像的特征向量。因此，在已知背景攻击模型下，本方案能够保护索引的机密性。同理，查询陷门的机密性在已知背景攻击模型下也可以得到保护。

(3) 查询陷门的不可链接性

本方案能够实现查询陷门的不可链接性，分析如下：一方面，查询图像的特征向量扩充为 $\hat{\mathbf{Q}} = (\beta q_1, \beta q_2, \dots, \beta q_n, \beta, \gamma, 1, s, s^2, \dots, s^k)$ ，其中 β, γ 两者都是一次一密的随机数。对于同一张查询图像而言，每次扩充时， β, γ 都不一样，云服务器无法从两个扩充后的向量中，推测出他们是否来自同一张查询图像的特征向量。另一方面，本方案对于扩充后的查询向量进行了随机置换，即 $\tilde{\mathbf{Q}} = \pi(\hat{\mathbf{Q}})$ 。特征向量的特征点位置发生了随机变换，云服务器无法通过分析特征向量中的特征点，判断查询图像对应的查询陷门。因此，本方案能够保证查询陷门的不可链接性。

6 方案性能分析

本节首先分析方案的复杂度，包括计算复杂度和通信复杂度，然后，在真实图像数据集和模拟数据集上进行实验评估。

6.1 复杂度分析

本文所提方案的计算复杂度与已有的方案^[15]

计算复杂度的对比如表1所示。本文假设安全参数 λ 的长度为 $|\lambda|$ ，图像数据集的大小为 m ，哈希桶中图像的数量为 $L (L < m)$ ，图像的特征向量维度为 n ， k 表示云服务器返回结果中 top- k 图像数量。

表1 计算复杂度对比
Table 1 Comparison of computational cost

方案	计算复杂度		
	索引构建	陷门生成	图像搜索
EPIR 方案	$O(mn^2)$	$O(n^2)$	$O(mn^2)$
EPIRM 方案	$O(2mn^2)$	$O(n^2)$	$O(2mn^2)$
本文方案	$O(2Ln^2)$	$O(n^2)$	$O(2kn^2)$

此外，本方案的通信复杂度与已有方案的通信复杂度对比如表2所示。

表2 通信复杂度对比
Table 2 Comparison of communication cost

方案	通信复杂度		
	索引构建	陷门生成	图像搜索
EPIR 方案	$2nm \lambda $	$2n \lambda $	$2nm \lambda $
EPIRM 方案	$2nm \lambda $	$2n \lambda $	$2nm \lambda $
本文方案	$2nL \lambda $	$2n \lambda $	$2nk \lambda $

6.1.1 计算复杂度

首先，分析本文提出的方案的计算复杂度，并与现有的方案 EPIR 和 EPIRM^[15]进行了比较，对比结果如表1所示。在本方案中，本文采用局部敏感哈希算法将相似图像归类到同一个桶内，当查询用户图像的哈希值与某哈希桶的哈希值相同时，说明该哈希桶中的图像比其他哈希桶中的图像更相似。云服务器只需要检索该哈希桶中的图像，并返回 top- k 的相似图像给查询用户。通过这种方式，本文方案可以极大地降低图像检索空间，提高索引构建效率和图像搜索效率。在索引构建过程中，本文方案只需要执行哈希桶中图像特征向量的加密操作。如式(2)和式(3)所示，索引构建阶段需要执行正交矩阵与特征向量的加密和重加密操作，两者均为矩阵与向量的乘法运算。因此，索引构建的计算复杂度为 $O(2Ln^2)$ 。然而，在 EPIRM 中，云服务器需要对整个图像数据集进行检索并构建索引，其索引构建的计算复杂度为 $O(2mn^2)$ 。在陷门生成过程中，如式(5)所示，查询用户只需要执行一次矩阵与向量的乘法运算。

因此, 陷门生成的计算复杂度为 $O(n^2)$ 。在图像搜索过程中, 云服务器需要计算重加密索引与重加密陷门之间的内积, 并返回 $\text{top-}k$ 相似图像。因此, 图像搜索的计算复杂度为 $O(2kn^2)$ 。然而, 对于 EPIRM 而言, 其图像检索是遍历整个图像数据集, 并返回前 k 个最相似的图像, 图像检索的计算复杂度为 $O(2mn^2)$ 。

6.1.2 通信复杂度

由于在索引构建和陷门生成过程中, 数据拥有者和查询用户都是执行矩阵与向量的乘法运算。因此本方案的索引构建的通信开销为 $2nL|\lambda|$, 陷门生成的通信开销为 $2n|\lambda|$ 。在图像搜索过程中, 云服务器需要执行向量与向量的内积运算, 其通信开销为 $2nk|\lambda|$ 。

6.2 实验评估

本文分别在真实数据集和模拟数据集上进行了测试。本文使用 Java 实现了所提的方案, 同时也实现了对比方案 EPIR 和 EPIRM, 并与之进行了性能对比。实验测试环境为 Intel E3-1225 v5 @3.30 GHz 的处理器, 32.0 GB 内存, Windows 7 操作系统。此外, 本文使用 ORL (olivetti research laboratory) 人脸数据集^[16]测试检索准确率, 并生成了 10 000 个多维数据向量作为仿真实验数据集。假设图像特征提取的 Fisher 向量维度为 4 096。本文实验结果包括两方面: 检索准确率和计算开销。

6.2.1 检索准确率

为了在真实数据集 ORL 上测试本方案的准确率, 本文分别选用了主成分分析 (PCA, principal component analysis) 和直方图表示法 (EHD, edge histogram descriptor) 提取特征向量。本文采用两种应用广泛的精度衡量方式: 平均精度 (MAP, mean average precision)^[17]和 $\text{top-}k$ 精度 ($k\text{-P}$)^[5], 测试本文方案的图像检索准确率。

由图 2 可知, 当特征向量维度高于 PCA-512 时, 图像检索的平均精度非常高。在特征向量为 PCA-4096, 平均精度可达 94.5%。当特征向量维度低于 PCA-512 时, 平均精度迅速下降。从图 3 可以看出, 当选择 EHD 为特征向量提取算法, 且返回图片数量范围在 [20, 100] 时, $\text{top-}k$ 精度均高

于 90%, 最高精度可达 96.1%。因为密文图像搜索结果是基于明文图像特征向量的欧氏距离相似度排序的, 所以图像搜索的准确率不受特征向量加密算法影响, 而是取决于图像特征提取的算法。

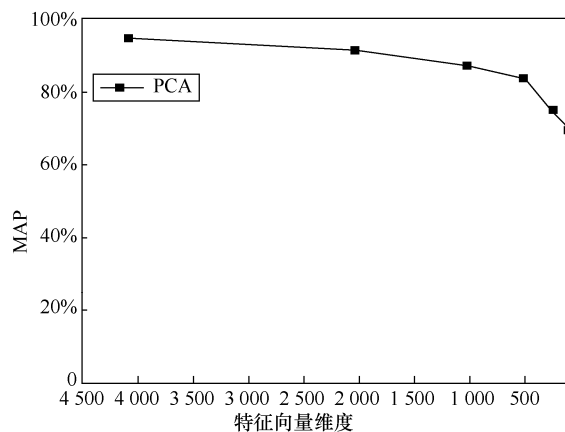


图2 不同特征向量维度下的平均精度
Figure 2 MAP with different feature vector dimensions by PCA

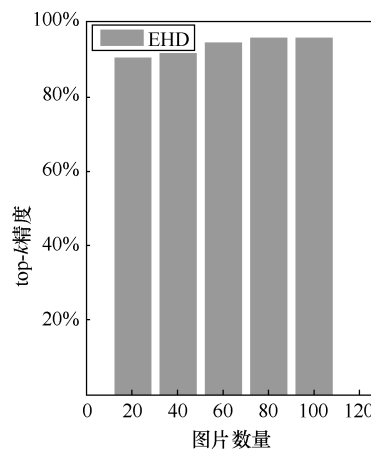


图3 不同图片数量下 top-k 精度
Figure 3 top-k precision with different k by EHD

6.2.2 计算开销

在计算开销方面, 本文对比了所提出的方案与 EPIR 和 EPIRM 的时间开销。

(1) 索引构建计算开销

在索引构建过程中, 本文方案主要包括两个阶段: 构建哈希桶和建立索引。首先, 数据拥有者采用局部敏感哈希算法将相似图像归并到同一个哈希桶内, 过滤掉不相似图像。通过这种方式, 本文方案可以极大地降低图像搜索空间, 迅速定位到与查询图像相似的哈希桶。其次, 数据拥有

者扩充特征向量, 置换扩充后的特征向量, 并利用自己的密钥加密置换后的向量, 具体如式(1)和式(2)所示。云服务器接收到加密索引后, 再根据相应的重加密密钥对索引进行转换, 并将转换后的索引存储在云服务器中。从图4可以看出, 在不同特征向量维度下, 本文方案在索引构建上的时间开销均比EPIR和EPIRM更低。因为本文方案采用了局部敏感哈希算法, 极大地减少了图像索引构建数量, 且构建的特征向量维度低于对比方案的特征向量维度。而且EPIR和EPIRM引入了 $2n$ 维随机误差向量和 $m-1$ 个随机数, 增加了特征向量的维度, 使矩阵乘法运算的时间开销更大。从图5也可以看出, 针对不同的图像数据量, 本文方案在索引构建方面, 性能优于EPIR和EPIRM。

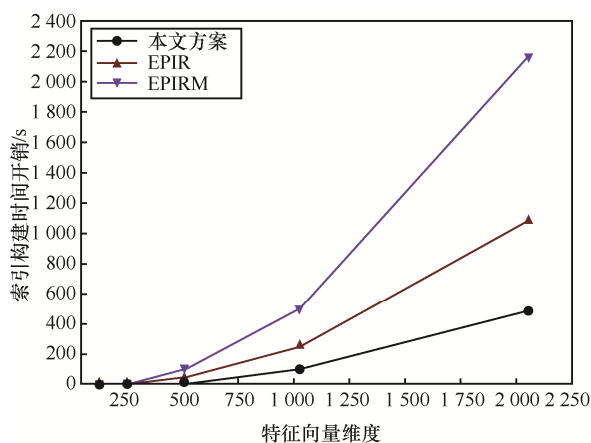


图4 特征向量维度变化下的索引构建时间开销
Figure 4 Running time of index build with different feature vector dimension

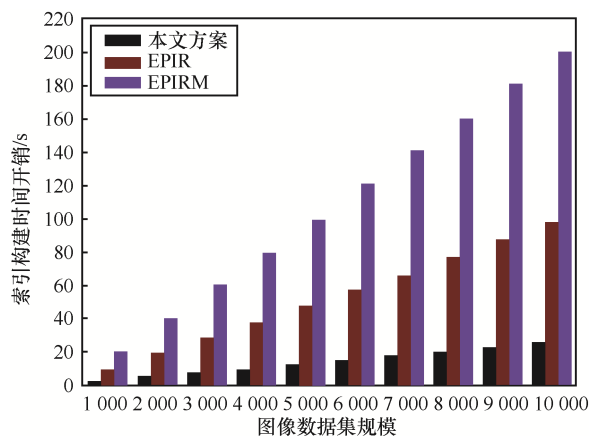


图5 图像数据集规模变化下的索引构建时间开销
Figure 5 Running time of index build with different number of images

(2) 陷门生成计算开销

在陷门生成过程中, 查询用户先扩充查询图片的特征向量, 如式(4)所示。扩充完成后, 查询用户利用置换函数, 随机扰动扩充向量的位置。然后, 查询用户用自己的密钥加密向量生成查询陷门, 如式(5)所示。从图6可以发现, 随着特征向量维度的增加, 陷门生成的时间开销呈线性递增趋势, 且本方案比EPIR和EPIRM效率更好。因为本方案只引入了两个随机数, 而EPIR和EPIRM引入了 $m-1$ 个随机数和一个 $2n$ 维随机误差向量。

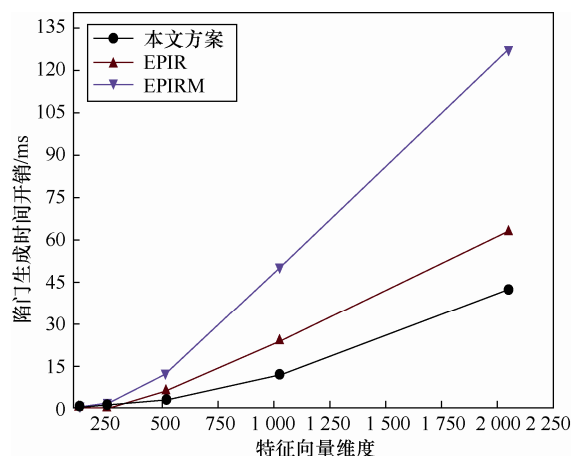


图6 特征向量维度变化下的陷门生成时间开销
Figure 6 Running time of trapdoor generation with different feature vector dimension

(3) 图像搜索计算开销

在图像搜索过程中, 本文采用欧氏距离相似性衡量密文索引与查询陷门的相似度。此外, 本文采用局部敏感哈希算法找出与查询请求相似的图像, 并根据欧氏距离相似度返回 $\text{top-}k$ 图像给查询用户。由图7可知, 本文的方案在特征向量维度增加时, 图像搜索时间开销低于EPIR和EPIRM, 且三者都呈线性递增趋势。由图8可知, 本文方案的时间开销略低于EPIR和EPIRM。因为本文方案利用了局部敏感哈希算法聚类相似的图像, 并将相似图像存放于同一个哈希桶中, 云服务器只需要检索与查询图像对应的哈希桶中的图像, 而不用遍历整个图像数据集。因此, 本文方案对于密文环境下高维特征向量和大规模图像数据集的检索是高效的且满足现有图像检索的强安全性和高准确率需求。

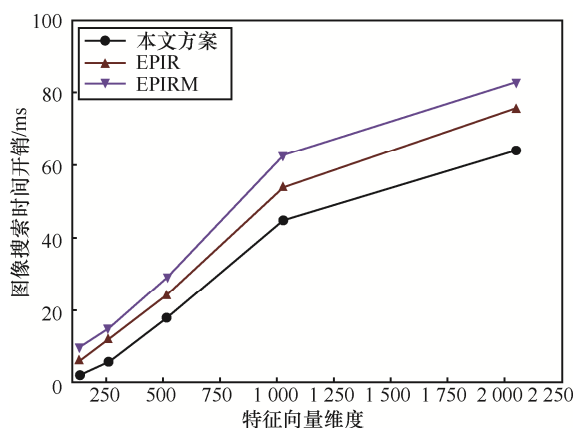


图7 特征向量维度变化下的图像搜索时间开销
Figure 7 Running time of image search with different feature vector dimensions

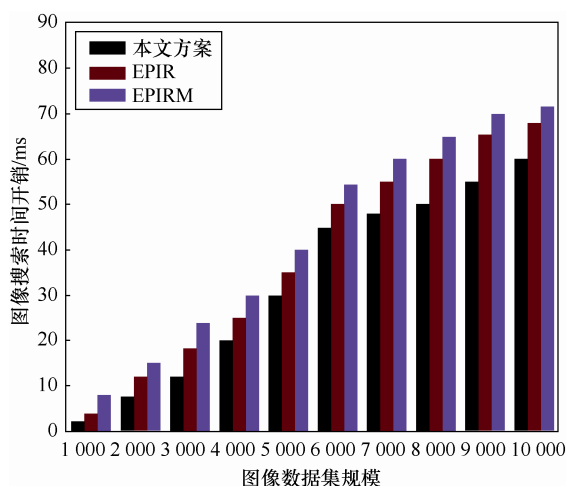


图8 图像数据集规模变化下的图像搜索时间开销
Figure 8 Running time of image search with different number of images

7 结束语

针对多用户场景下外包图像检索的效率和隐私保护问题, 本文提出了一种基于访问控制安全高效的多用户外包图像检索方案。该方案采用矩阵正交分解性质, 将对称密钥分解为用户的加密密钥和云服务器的重加密密钥, 并利用代理重加密方法, 实现了多用户环境下外包图像检索。本文利用局部敏感哈希算法构建索引, 极大地降低了图像搜索空间。同时, 本文基于角色多项式函数提出了一种轻量级的访问控制策略, 用于设定图像的访问权限, 防止恶意用户窃取图像隐私。安全性分析证明了本文的方案能够达到已知明文攻击和已知背景攻击下的安全。大量的实验结果

表明本文的方案对于高维特征向量和大规模图像数据集, 在计算效率方面优于现有的密文图像检索方案。

参考文献:

- [1] SHASHANK J, KOWSHIK P, SRINATHAN K, et al. Private content based image retrieval[C]//Proc. Of IEEE CVPR. 2014: 1-8.
- [2] SONG F Y, QIN Z, LIU Q, et al. Efficient and secure k-nearest neighbor search over encrypted data in public cloud[C]//Proc of IEEE ICC. 2019: 1-6.
- [3] XIA Z, XIONG N N, VASILAKOS V A, et al. EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing[J]. Information Sciences. 2017, 387: 195-204.
- [4] ZHOU K, REN J. Passbio: privacy-preserving user-centric biometric authentication[J]. IEEE Transactions on Information Forensics Security. 2018, 13(12): 3050-3063.
- [5] LI X, XUE Q, CHUAH M C. Casheirs: cloud assisted scalable hierarchical encrypted based image retrieval system[C]//Proc of IEEE INFOCOM. 2017: 1-9.
- [6] SHEN M, CHENG G, ZHU L, DU X, et al. Content-based multi-source encrypted image retrieval in clouds with privacy preservation[J]. Future Generation Computer Systems. 2020, 109: 621-632.
- [7] JUNG T, LI X, WAN M. Collusion-tolerable privacy-preserving sum and product calculation without secure channel[J]. IEEE Transactions on Dependable and Secure Computing. 2014, 12(1): 45-57.
- [8] YUAN J, YU S, GUO L. SEISA: Secure and efficient encrypted image search with access control[C]//Proc of IEEE INFOCOM. 2015: 2083-2091.
- [9] ZHENG Y, LU R, GUAN Y, et al. Achieving efficient and privacy-preserving exact set similarity search over encrypted data[J]. IEEE Transactions on Dependable and Secure Computing. 2020.
- [10] FU Z, HUANG F, SUN X, et al. Enabling semantic search based on conceptual graphs over encrypted outsourced data[J]. IEEE Transactions on Services Computing, 2016, 12(5): 813-823.
- [11] XU L, YUAN X, WANG C, et al. Hardening database padding for searchable encryption[C]//Proc of IEEE INFOCOM. 2019: 2503-2511.
- [12] SHU J, JIA X, YANG K, et al. Privacy-preserving task recommendation services for crowd sourcing[J]. IEEE Transactions on Services Computing, 2021, 14(1): 235-247.
- [13] ZHANG C, ZHU L, XU C, et al. TPRR: A trust-based and privacy-preserving platoon recommendation scheme in VANET[J]. IEEE Transactions on Services Computing, 2019.
- [14] YUAN J, TIAN Y. Practical privacy-preserving MapReduce based k-means clustering over large-scale dataset[J]. IEEE Transactions on Cloud Computing, 2017, 7(2): 568-579.
- [15] WANG X, MA J, LIU X, et al. Search in my way: Practical outsourced image retrieval framework supporting unshared key[C]//Proc of IEEE INFOCOM. 2019: 2485-2493.
- [16] PENG Z, JIA Y, LIU H, et al. Maximum entropy subspace clustering network[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021.
- [17] YUE Y, FINLEY T, RADLINSKI F, et al. A support vector method for optimizing average precision[C]//Proc of ACM SIGIR. 2007: 271-278.

[作者简介]



宋甫元（1991-），男，江西上饶人，湖南大学博士生，主要研究方向为隐私保护、数据安全、应用密码学。



张吉昕（1987-），男，湖北武汉人，湖北工业大学讲师，主要研究方向为人工智能、知识图谱、异常行为分析与恶意代码分析。



秦拯（1969-），男，湖南长沙人，湖南大学教授、博士生导师，主要研究方向为云计算安全、隐私保护、图数据管理与应用。



刘羽（1994-），女，湖南邵阳人，湖南大学博士生，主要研究方向为应用密码学、图像加密。