基于边缘计算的支持多密钥的加密图像检索

李颖莹[1,2]，马建峰[1,2]，苗银宾[1]

（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071； 2. 陕西省网络与系统安全重点实验室，陕西 西安 710071）

摘 要：针对现有加密图像检索方案未考虑不同密钥加密图像集的情况，基于局部敏感哈希、安全近邻及代理重加密技术提出了基于边缘计算的支持多密钥的加密图像检索系统（包含基础方案和改进方案）。所提方案不但提高了图像查询效率、精度，而且降低了查询用户的额外计算开销。安全性分析表明，所提基础方案仅可抵抗已知密文攻击，而所提改进方案可抵抗已知背景攻击。基于实际数据集的实验性能测试表明，所提方案在实际应用场景中是可行的。

关键词：多密钥；局部敏感哈希；代理重加密；已知密文攻击；已知背景攻击

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020086

Encrypted image retrieval in multi-key settings based on edge computing

LI Yingying[1,2], MA Jianfeng[1,2], MIAO Yinbin[1]

1. School of Cyber Engineering, Xidian University, Xi’an 710071, China

2. Shaanxi Key Laboratory of Network and System Security, Xi’an 710071, China

Abstract: Aiming at the fact that the existing encrypted image retrieval schemes do not consider different keys to encrypt images, a multi-key encrypted image retrieval system based on edge computing (including basic scheme and enhanced scheme) based on local sensitive hashing, secure nearest neighbor and proxy re-encryption technologies was proposed. The retrieval efficiency and accuracy were improved and the extra computational cost of query users was reduced. Security analysis shows that the basic scheme can only resist the known ciphertext attack, while the enhanced scheme can resist the known background attack. The experimental performance test based on the real-world dataset shows that the proposed schemes are feasible in practical application scenarios.

Key words: multi-key, locality sensitive hashing, proxy re-encryption, known ciphertext attack, known background attack

1 引言

随着图像设备如数码相机、智能手机迅速更新换代，以及各种图像应用层出不穷，图像数据呈爆炸式增长趋势，大大增加了用户本地数据计算和存储负担。资源受限的用户借助云计算服务将数据外

收稿日期：2020–01–06；**修回日期**：2020–03–26

基金项目：促进海峡两岸科技合作联合基金资助项目（No.U1405255）；陕西省科技统筹创新工程计划基金资助项目（No.2016KTZDGY05-06）；中央高校基本科研业务费基金资助项目（No.JB191506）；国家自然科学基金资助项目（No.61702404, No.61702105, No.U1804263, No.61972094）；陕西省自然科学基金资助项目（No.2019JQ-005）；中国博士后科学基金资助项目（No.2017M613080）

Foundation Items: The Key Program of NSFC Grant (No.U1405255) , Shannxi Science & Technology Coordination & Innovation Project (No.2016KTZDGY05-06) , Fundamental Research Funds for the Central Universities (No.JB191506), The National Natural Science Foundation of China (No.61702404, No.61702105, No.U1804263, No.61972094) , The Natural Science Foundation of Shannxi Province (No.2019JQ-005) , China Postdoctoral Science Foundation Funded Project (No.2017M613080)

包至云服务器。但是在万物互联的时代，仅依靠以云计算为代表的集中式计算模式不足以支持海量数据处理，不能有效解决服务负载、传输带宽等问题，无法满足数据实时性处理需求。因此，以边缘计算为代表的分布式计算模式应运而生，为海量移动设备提供最近端服务，相比以云计算为代表的集中式计算模式节省了大量计算、传输和存储成本。但另一方面，外包至边缘计算节点的图像数据由于脱离了用户的实际掌控而面临隐私泄露问题。为此，用户将加密后的图像数据外包至边缘计算节点。尽管加密算法能在一定程度上保证图像数据安全，但会影响图像检索在密文上的应用。

传统的明文图像检索主要采用基于文本的图像检索（TBIR, text-based image retrieval）和基于内容的图像检索（CBIR, content-based image retrieval）2 种方法。其中，基于文本的图像检索方法是用文本对图像进行人工标记，受人为主观影响导致查询准确率低。基于内容的图像检索方法用图像本身的颜色、纹理和形状信息客观描述图像内容，大大提高了查询准确率。目前，如何在密文上应用明文 CBIR 技术是加密图像检索研究的重点之一。Lu 等[1-2]提出基于 CBIR 的加密图像检索方案，并用同态加密算法保护图像特征向量；Zhang 等[3]利用同态加密和属性基加密技术实现大规模加密图像检索；Xia 等[4]基于词袋模型和地球移动距离设计了一个安全 CBIR 方案。尽管基于同态加密和可搜索加密技术可以实现加密图像检索[5-7]，但是如果将这些支持单密钥的传统图像检索方案直接应用到实际多密钥场景中，查询用户必须生成多个陷门。例如，在电子医疗系统中，医生想要查询其他 3 个医院的医疗图像库。如图 1(a)所示，这 3 个医院的医疗图像库由各自密钥加密，通过系统认证的医生需要发送 3 个查询请求才能达到检索目的。当系统中医院数目增多时，医生实现检索目的所需的计算开销和通信开销随之增多。如果医生只需要生成一个查询请求就可以检索其他所有医院的医疗图像库，如图 1(b)所示，用户只需生成一个查询陷门即可查询不同密钥加密的图像集，这将大大减小用户的计算与通信开销。

然而，已有的加密图像检索方案[1-2,4-12]大多不支持多密钥加密图像检索，仅有的支持多密钥加密图像检索的方案[3,13]由于涉及复杂的安全多方计算和同态加密技术，导致实用性受到影响。因此，需要设计一种支持多密钥的加密图像检索方案，解决以下关键问题：1) 所有外包至边缘服务器的数据都应进行加密，使服务器无法根据密文获取明文相关信息；2) 每个图像查询用户应该以尽可能低的开销查询不同密钥加密的图像，以便实现云端数据共享；3) 检索结果应满足查询要求，检索时间应满足实时性需求，以保证方案的准确性和高效性。

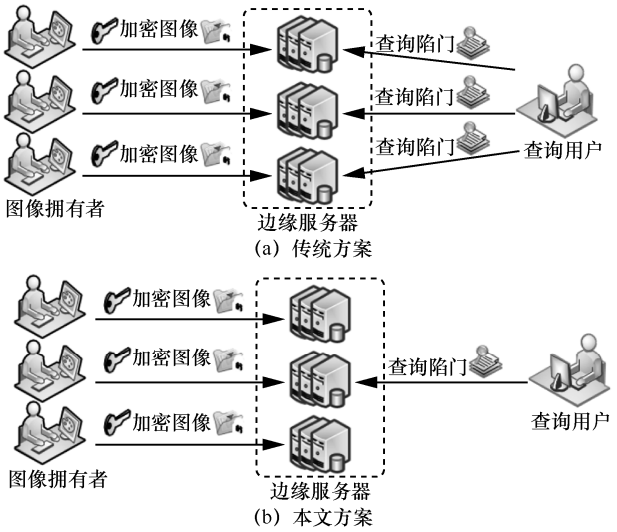


图 1　方案背景比较

为解决以上问题，本文基于局部敏感哈希算法、安全近邻算法及代理重加密等技术提出了基于边缘计算的支持多密钥的加密图像检索方案。局部敏感哈希算法在生成索引时将相似图像映射到同一个桶中，能有效减小图像检索时间，保证方案的高效性。安全近邻算法利用随机向量分裂和可逆矩阵加密向量，可快速实现图像相似度的安全计算，保证方案的安全性和准确性。代理重加密技术能够帮助代理服务器进行不同加密密钥密文之间的转换，将拥有者加密的密文转换成查询用户可解密的形式，以此减少多拥有者/多密钥场景下查询用户的开销。边缘计算具有低时延、高可用、高实时的优势，能克服云计算模式中因数据迁移、网络传输造成过多带宽资源消耗的不足，为用户提供高质量服务。本文基于这些算法和技术提出基于边缘计算的、支持多密钥的加密图像检索方案，其具有以下特点。

1) 多密钥场景。提出了一种多密钥场景下的加密图像检索方案，查询用户仅需生成一个查询陷门即可对不同密钥加密的图像进行检索，比传统方案更实用，用户计算负担更小。

2) 访问控制。实现了对图像查询用户的访问控制，边缘服务器重加密图像加密密钥后，用户只能用合法分配的私钥解密。密钥中心为每个查询用户分发不同的私钥，即使其他用户窃取查询结果，也不能解密出明文。

3) 高安全性。在用图像特征向量的内积表示图像之间的相似度时，所提方案在特征向量中加入了冗余项，以此提高了服务器端相似度计算的安全性。

2 相关工作

密文检索主要涉及文本领域和图像领域。关于文本检索的多密钥场景，Yin 等[14]利用随机密钥为不同数据建立索引，同时用户选择其他随机密钥生成陷门而不影响密文匹配，减少了密钥管理复杂度，但不支持细粒度访问控制。Sun 等[15]利用属性基加密和代理重加密技术设计了支持细粒度访问控制的密文检索方案，且支持数据用户的属性撤销，避免了用户与拥有者直接交互。不同于密钥和数据一一对应，Miao 等[16]针对共享型数据的多密钥场景，利用多重签名技术提出了高效可验证的关键字检索方案，可抵抗选择关键字攻击，后来又扩展到连接多关键字模型[17]，提出既支持连接多关键字又可进行结果验证的高效检索方案，能够抵抗离线关键字猜测攻击。

上述方案都是针对文本检索的研究，图像不像文本那样可用关键字进行准确唯一标记，从而导致基于关键字的密文检索方案无法直接应用于图像领域。Lu 等[1]提出了基于 CBIR 的加密图像检索方案，允许图像进行相似性匹配，但是没有考虑明文图像和加密图像之间的距离变化。针对这一问题，Lu 等[8]采用了保序加密和 Min-hash 方案，但是该方案局限于用视觉单词描述图像特征。Zhang 等[9]利用同态加密性质解决了距离变化问题，并用欧氏距离作为图像相似性度量，然而同态的使用大大增加了方案计算开销。为减小计算开销，Xia 等[10]基于图像的全局特征利用局部敏感哈希算法构建索引，实现了高效的加密图像检索。Yuan 等[11]基于多项式性质提出了支持访问控制的加密图像检索方案，并设计了安全 k-means 外包算法。

尽管以上方案实现了加密图像检索，甚至具有高效率和访问控制功能，但是这些方案均针对单密钥场景，无法满足实际需求中的多密钥场景。Liang 等[12]针对多个查询用户设计了多密钥非对称内积加密算法，为不同查询用户分发不同密钥，同时利用全局优化和高斯分布提高密钥安全性和空间利用率，但是该方案不支持在多个密钥加密的图像集上检索。Shen 等[13]和 Zhang 等[3]分别利用安全多方计算和多密钥同态加密提出了支持多拥有者-多用户的加密图像检索方案，尽管前者通过简化欧氏距离计算方法，后者借助并行计算模式来减小计算开销，但方案的实用性仍受计算和通信开销影响。为减小开销，王祥宇等[18]通过设计轻量级密钥转换协议来实现多用户加密图像检索方案。此外，文献[19-21]提出了多密钥背景下的可搜索加密方案，但是尚未实现图像检索。

针对已有方案绝大多数不支持多密钥加密的图像检索或者多密钥加密的图像检索方案效率较低的问题，本文结合局部敏感哈希算法、安全近邻算法和代理重加密技术，利用边缘计算模式数据就近处理原则，提出基于边缘计算的支持多密钥的图像检索方案。表 1 给出了本文方案与其他方案的比较。从表 1 可以看出，本文方案能同时满足多密钥场景、访问控制、已知背景攻击安全和高效率这 4 个要求。

表 1 本文方案与其他方案的比较

方案	多密钥加密图像	访问控制	已知背景攻击安全	高效率
文献[3]方案	√	√	√	×
文献[9]方案	×	×	√	×
文献[10]方案	×	×	×	√
文献[11]方案	×	√	√	√
文献[12]方案	×	√	√	√
文献[13]方案	√	×	√	×
文献[18]方案	√	×	√	√
本文方案	√	√	√	√

注：√表示支持，×表示不支持。

3 预备知识

本文方案主要运用基于双线性对的代理重加密技术解决多密钥转换问题，应用局部敏感哈希算法提高检索速度，其中哈希函数属于 p 稳态局部敏感哈希函数。本节分别介绍代理重加密和局部敏感哈希的相关定义。

定义 1 双线性对[22]。设 G,G_T 是 2 个阶为素数 p 的乘法循环群，g 是 G 的一个生成元。双线性对 $e: G\times G\to G_T$ 有以下性质。

1) 可计算性。存在一个有效算法可计算 e。

2) 双线性。对任意 $u,v\in G$ 和 $a,b\in\mathbb{Z}_p$，都有 $e(u^a,v^b)=e(u,v)^{ab}$。

3)非退化性。$e(g,g)\neq 1$。

定义 2　代理重加密[23]。一个代理重加密方案由算法 KeyGen、ReKey、Encrypt、ReEncrypt、Decrypt 构成。

1) $(\mathrm{pk}_i,\mathrm{sk}_i)\leftarrow\mathrm{KeyGen}(1^\kappa)$。输入安全参数 κ，为用户 i 输出公私钥对 $(\mathrm{pk}_i,\mathrm{sk}_i)$。

2) $\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}\leftarrow\mathrm{ReKey}(\mathrm{pk}_\mathrm{A},\mathrm{sk}_\mathrm{A},\mathrm{pk}_\mathrm{B},\mathrm{sk}_\mathrm{B})$。输入 Alice 的公私钥对 $(\mathrm{pk}_\mathrm{A},\mathrm{sk}_\mathrm{A})$ 和 Bob 的公私钥对 $(\mathrm{pk}_\mathrm{B},\mathrm{sk}_\mathrm{B})$，输出代理重加密密钥 $\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$，其中，Alice 为委托者，Bob 为被委托者。

3) $c_i\leftarrow\mathrm{Encrypt}(\mathrm{pk}_i,m)$。输入用户 i 的公钥 pk_i 和消息 m，输出密文 c_i。

4) $c_\mathrm{B}\leftarrow\mathrm{ReEncrypt}(\mathrm{rk}_{\mathrm{A}\to\mathrm{B}},c_\mathrm{A})$。输入代理重加密密钥 $\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$ 和 Alice 的密文 c_A，输出 Bob 可解密的密文 c_B。

5) $m\leftarrow\mathrm{Decrypt}(\mathrm{sk}_i,c_i)$。输入用户 i 的公钥 sk_i 和密文 c_i，输出消息 m 或错误符号 $\perp$ 表示 c_i 不合法。

定义 3　p 稳态局部敏感哈希[24-25]。给定距离 R、cR，概率值 P_1、P_2，其中 $c>1$，$P_1>P_2$，称函数族 $\mathcal{H}$ 是 (R,cR,P_1,P_2) 敏感。对任意 2 个 d 维向量 $\boldsymbol{u},\boldsymbol{v}\in\mathbb{R}^d$ 和任意函数 $h\in\mathcal{H}$。

1) 如果 $\|\boldsymbol{u}-\boldsymbol{v}\|\leqslant R$，则 $\Pr[h(\boldsymbol{u})=h(\boldsymbol{v})]\geqslant P_1$。

2) 如果 $\|\boldsymbol{u}-\boldsymbol{v}\|\geqslant cR$，则 $\Pr[h(\boldsymbol{u})=h(\boldsymbol{v})]\leqslant P_2$。

此处，函数 h 为 p 稳态局部敏感哈希函数，形如 $h_{a,b}(\boldsymbol{v})=\left\lfloor\dfrac{\boldsymbol{a}\boldsymbol{v}+b}{r}\right\rfloor$，其中，$\boldsymbol{a}$ 是每维服从 p 稳态分布的 d 维向量，b 是一个服从 $[0,r)$ 均匀分布的实数，r 是一个常数。

4　系统模型、威胁模型及安全目标

4.1　系统模型

本文方案包括 4 个实体，即密钥生成中心、图像拥有者、图像查询用户和边缘服务器，系统模型如图 2 所示。完全可信的密钥生成中心负责系统初始化和密钥分配，图像拥有者将加密图像、加密密钥密文和加密索引上传到边缘服务器存储，查询用户将查询陷门发送给边缘服务器，边缘服务器则根据陷门匹配加密索引获取候选图像集列表，然后重加密候选图像集对应的密钥密文，最后将密钥和候选图像集作为检索结果返回给查询用户。

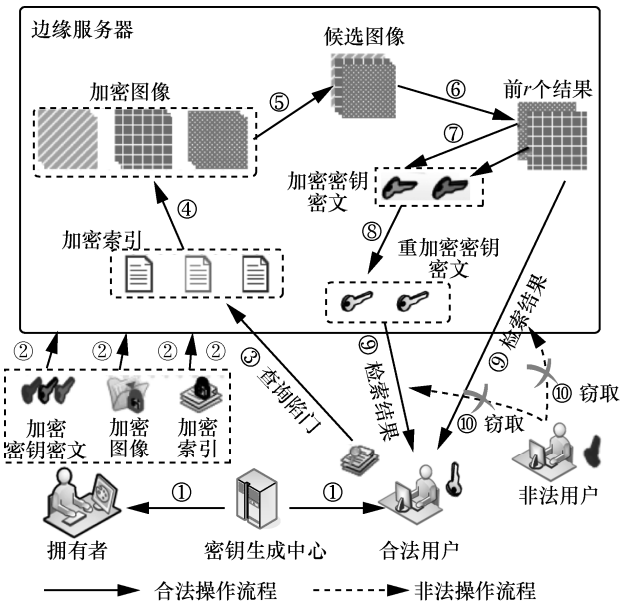


图 2　系统模型

1) 密钥生成中心。为图像拥有者和查询用户生成密钥。如图 2 中①所示。

2) 图像拥有者。加密图像集和图像加密密钥，计算转换密钥，构建加密索引，最后将加密图像、加密密钥密文和加密索引上传给边缘服务器。如图 2 中②所示。

3) 图像查询用户。加密查询图像的特征向量，生成查询陷门发送给边缘服务器。如图 2 中③所示。

4) 边缘服务器。根据查询用户发送的陷门和拥有者发送的加密图像、加密索引进行查询，对图像加密密钥进行重加密，最后将搜索结果和重加密密钥密文返回给用户。如图 2 中④～⑨所示。另外，图 2 中⑩表示没有密钥的非法用户即使窃取检索结果也不能解密出明文。

4.2　威胁模型

在本文方案中，假设边缘服务器是半可信的，即服务器会诚实且正确地执行协议，同时也会积极获取加密图像的明文信息。此外，假设图像拥有者和查询用户是可信的，且查询用户和服务器之间不会相互合作。根据服务器可获得的知识将攻击模型总结为以下 2 种。

已知密文攻击模型[26]。服务器只知道从图像拥有者端外包而来的加密图像集和加密索引以及来自图像查询用户的查询陷门。

已知背景攻击模型[27]。与已知密文攻击模型相比，服务器拥有更多背景知识，如额外获得一些查询陷门对应的明文、图像明文等。

4.3 安全目标

基于 4.2 节定义的威胁模型，本文安全目标主要是防止半可信服务器从图像密文集、索引集、密钥密文集、陷门和内积计算结果中获取有效信息。

1) 图像隐私。服务器从加密图像集中不能解密明文图像，也不能获取明文图像相关信息。

2) 索引隐私。服务器不能解密加密索引表，更不能解密索引表中的特征向量。

3) 密钥隐私。服务器在进行重加密操作时，不能获取拥有者和查询用户的私钥，也不能解密图像加密密钥。

4) 陷门隐私。服务器根据陷门无法得知查询图像的明文信息，也不能判断陷门之间的关系。

5) 内积计算隐私。服务器从加密向量内积计算结果中无法知道明文向量内积值，同时应用统计分析也不能获取任何明文信息。

5 支持多密钥的加密图像检索方案

由于不同拥有者的图像加密密钥不同，致使查询用户不能用同一个陷门查询图像集。如果将支持单密钥的传统图像检索方案直接应用于实际多密钥场景，会为用户带来额外开销；而且传统云计算模式在数据存储、传输方面消耗大量带宽资源，无法满足实时处理数据的需求。为解决这些问题，本节提出基于边缘计算的支持多密钥的加密图像检索方案。方案利用代理重加密技术实现图像加密密钥的密文转换，应用局部敏感哈希算法提高检索速度，再用安全近邻算法提高检索精度和安全性，基于边缘计算模式节约数据在服务器和终端设备之间的传输链路资源。

5.1 方案定义

在对本文方案进行详细描述之前，给出方案定义。首先，定义方案中用到的符号，如表 2 所示。

表 2 符号定义

符号	定义
$M=\{m_i\}_{i=1}^{n}=\{M_i\}_{i=1}^{w}$	明文图像集
$C=\{c_i\}_{i=1}^{n}=\{C_i\}_{i=1}^{w}$	加密图像集
$K=\{k_i\}_{i=1}^{w}$	图像加密密钥集
$I=\{I_i\}_{i=1}^{w}$	安全索引集
$\Lambda=\{\Lambda_i\}_{i=1}^{w}$	重加密密钥集
TD	陷门

其次，定义本文方案主要包含的 7 种算法。

1) $(\mathcal{G},\Gamma,k,\mathrm{sk},\mathrm{pk})\leftarrow\mathrm{KeyGen}(1^{\kappa})$。给定安全参数 κ，密钥生成中心输出系统参数 $\mathcal{G}$ 和 Γ、图像加密密钥 k、私钥 sk 和公钥 pk。

2) $C\leftarrow\mathrm{ImgEnc}(k,M)$。图像拥有者用加密密钥 k 加密明文图像 M，输出密文图像 C。

3) $\Lambda\leftarrow\mathrm{KeyTrans}(k,\mathrm{pk},\mathrm{sk})$。图像拥有者将图像加密密钥 k 加密成 k'，并生成转换密钥 $\mathrm{TK}_{\mathrm{UID}}$，输出重加密密钥 Λ。

4) $I\leftarrow\mathrm{IndexGen}(\Gamma,M)$。图像拥有者用参数 Γ 对明文图像 M 的特征向量进行预处理并加密特征向量，输出加密索引 I。

5) $\mathrm{TD}\leftarrow\mathrm{TrapdoorGen}(\Gamma,m_q)$。图像查询用户利用参数 Γ 对查询图像 m_q 的特征向量进行预处理并加密特征向量，输出查询陷门 TD。

6) $R\leftarrow\mathrm{Search}(C,\Lambda,I,\mathrm{TD})$。边缘服务器根据查询陷门 TD 匹配索引集 I，在图像密文集 C 中搜索符合查询要求的密文，将密文结果对应的拥有者密钥 k' 重加密成 k'_{UID}，输出检索结果 R。

7) $M'\leftarrow\mathrm{ImgDec}(R,\mathrm{sk})$。图像查询用户用自己的私钥 sk 解密出图像加密密钥，进一步解密出明文图像。

5.2 方案描述

本节从 7 个阶段描述本文方案的具体步骤，即密钥生成阶段 KeyGen、图像加密阶段 ImgEnc、密钥转换阶段 KeyTrans、索引生成阶段 IndexGen、陷门生成阶段 TrapdoorGen、检索阶段 Search 和图像解密阶段 ImgDec。其中，除密钥生成阶段外其他 6 个阶段流程如图 3 所示。

5.2.1 密钥生成阶段

$(\mathcal{G},\Gamma,k,\mathrm{sk},\mathrm{pk})\leftarrow\mathrm{KeyGen}(1^{\kappa})$。密钥生成中心输入参数 κ，输出双线性对参数 $\mathcal{G}=(G,G_T,e,p,g)$ 和秘密参数 $\Gamma=\{\boldsymbol{s},\boldsymbol{A}_1,\boldsymbol{A}_2,\{h_k\}_{k=1}^{\lambda},\{\psi_j\}_{j=1}^{L},\{\varphi_j\}_{j=1}^{L}\}$，其中，$\boldsymbol{s}$ 为一个 $d+1$ 维随机二值向量，$\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 为 2 个 $(d+1)\times(d+1)$ 维随机可逆矩阵，$\{h_k\}_{k=1}^{\lambda}$ 为 λ 个哈希函数，$\{\psi_j\}_{j=1}^{L}$ 为局部敏感哈希函数族，$\{\varphi_j\}_{j=1}^{L}$ 为 L 个哈希表的加密函数。密钥生成中心为拥有者分配图像加密密钥 $k=\{k_i\}_{i=1}^{w}$ 和公私钥对 $(\mathrm{sk}_{\mathrm{o}},\mathrm{pk}_{\mathrm{o}})$，满足 $\mathrm{pk}_{\mathrm{o}}=g^{\mathrm{sk}_{\mathrm{o}}}$，为 u 个用户分配公私钥对 $\{\mathrm{sk}_i,\mathrm{pk}_i\}_{i=1}^{u}$，身份为 UID 的用户分配到公私钥对 $(\mathrm{sk}_{\mathrm{UID}},\mathrm{pk}_{\mathrm{UID}})$，满足 $\mathrm{pk}_{\mathrm{UID}}=g^{\mathrm{sk}_{\mathrm{UID}}}$。需要说明图像拥

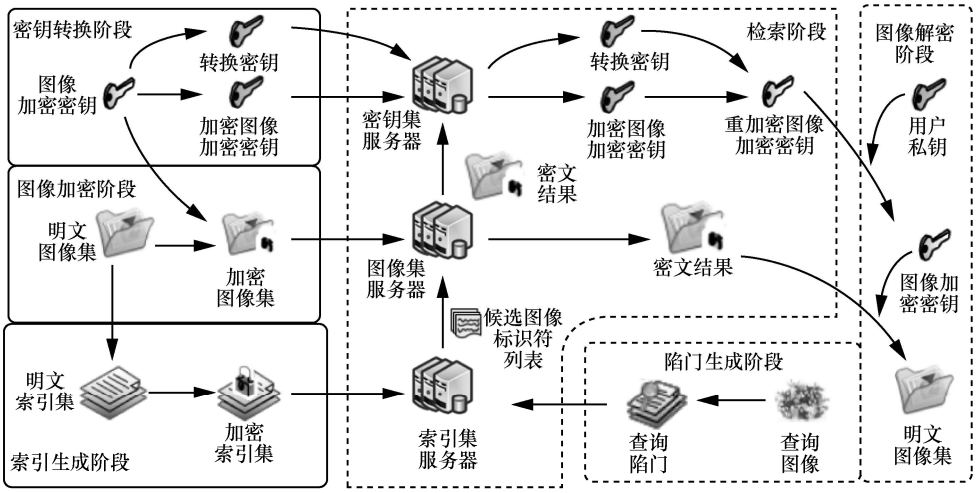


图 3 方案执行流程

有者知道查询用户的公私钥。

5.2.2 图像加密阶段

$C \leftarrow \mathrm{ImgEnc}(k, M)$。图像拥有者利用图像加密密钥 k_i 将明文图像集 M_i 加密成密文图像集 C_i，将 w 个不同密钥加密的密文图像集 $C=\{C_i\}_{i=1}^{w}$ 发送给边缘服务器存储。

5.2.3 密钥转换阶段

$\Lambda \leftarrow \mathrm{KeyTrans}(k, \mathrm{pk}, \mathrm{sk})$。图像拥有者首先将图像加密密钥 k_i 加密成 $k_i' = (\mathrm{pk}^{\varepsilon_i}, k_i F^{\varepsilon_i})$，其中，$\varepsilon_i$ 为随机数，F 为双线性对，即 $F=e(g,g)$。接着为 UID 的用户计算转换密钥 $\mathrm{TK}_{\mathrm{UID}} = g^{\frac{\mathrm{sk}_{\mathrm{UID}}}{\mathrm{sk}_{\mathrm{o}}}}$，则 k_i 对应的重加密密钥为 $\Lambda_i = \{k_i', \mathrm{TK}_{\mathrm{UID}}\}$。最后，$w$ 个重加密密钥组成 $\Lambda = \{\Lambda_i\}_{i=1}^{w}$ 发送给边缘服务器。

5.2.4 索引生成阶段

$I \leftarrow \mathrm{IndexGen}(\Gamma, M)$。索引生成阶段分两步完成，第一步为生成未加密的索引表，第二步为加密索引表。

1) 生成未加密的索引表。对于图像集 M_i 中每幅图像 $m_{i,t}$，先提取特征向量 $\boldsymbol{f}_{i,t} = (\boldsymbol{f}_{i,t_1}, \boldsymbol{f}_{i,t_2}, \cdots, \boldsymbol{f}_{i,t_d})$，其中 $t \in [1, n_i]$，n_i 为 M_i 所含图像总数。然后将 λ 个哈希函数 $h_1, h_2, \cdots, h_\lambda$ 作用于向量 $\boldsymbol{f}_{i,t}$，得到 λ 个哈希值 $\psi(\boldsymbol{f}_{i,t}) = \{h_k(\boldsymbol{f}_{i,t})\}_{k=1}^{\lambda}$。接着将 L 个 $\psi(\cdot)$ 作用于 $\boldsymbol{f}_{i,t}$，构造 L 个哈希表，即为未加密索引表，表中每个桶的值为 $\mathrm{BKT}_{i,j}^{b} = \psi_j(\boldsymbol{f}_{i,t})$，其中 $j \in [1, L]$，$b \in [1, N_{i,j}]$，$N_{i,j}$ 为第 j 个哈希表中桶的数目。如表 3 所示，图像 $m_{i,t}$ 的特征向量 $\boldsymbol{f}_{i,t}$ 和其相应图像信息标识符 $\mathrm{ID}(m_{i,t})$ 共同存储在哈希表中。第 j 个表有 $N_{i,j}$ 个哈希桶，同一个哈希桶中的图像是相似的。

2) 加密索引表。用函数 $\varphi(\cdot)$ 加密桶值 $\mathrm{BKT}_{i,j}^{b}$，用文献[28]中安全近邻算法加密特征向量。具体地，将 d 维图像特征向量 $\boldsymbol{f}_{i,t} = (\boldsymbol{f}_{i,t_1}, \boldsymbol{f}_{i,t_2}, \cdots, \boldsymbol{f}_{i,t_d})$ 扩展成 $d+1$ 维向量 $\overline{\boldsymbol{f}}_{i,t} = (\boldsymbol{f}_{i,t}, \|\boldsymbol{f}_{i,t}\|^2)$，再根据随机二值向量 $\boldsymbol{s}$ 将 $\overline{\boldsymbol{f}}_{i,t}$ 分裂成两部分 $\overline{\boldsymbol{f}}_{i,t}^{a}$ 和 $\overline{\boldsymbol{f}}_{i,t}^{b}$。分裂规则为，对于 $l \in [1, d+1]$，当 $\boldsymbol{s}[l]=0$ 时，有 $\overline{\boldsymbol{f}}_{i,t}^{a}[l] = \overline{\boldsymbol{f}}_{i,t}^{b}[l] = \overline{\boldsymbol{f}}_{i,t}[l]$；否则，为 $\overline{\boldsymbol{f}}_{i,t}^{a}$ 和 $\overline{\boldsymbol{f}}_{i,t}^{b}$ 随机赋予正值，使其满足 $\overline{\boldsymbol{f}}_{i,t}^{a}[l] + \overline{\boldsymbol{f}}_{i,t}^{b}[l] = \overline{\boldsymbol{f}}_{i,t}[l]$。接着用随机可逆矩阵 $\boldsymbol{A}_1^{\mathrm{T}}$ 和 $\boldsymbol{A}_2^{\mathrm{T}}$ 分别乘 $\overline{\boldsymbol{f}}_{i,t}^{a\mathrm{T}}$ 和 $\overline{\boldsymbol{f}}_{i,t}^{b\mathrm{T}}$，可得加密后的特征向量 $\boldsymbol{f}_{i,t}' = (\boldsymbol{A}_1^{\mathrm{T}} \overline{\boldsymbol{f}}_{i,t}^{a\mathrm{T}}, \boldsymbol{A}_2^{\mathrm{T}} \overline{\boldsymbol{f}}_{i,t}^{b\mathrm{T}})$。表 4 给出加密后的第 j 个哈希表。L 个加密后的哈希表构成索引表 I_i。拥有者将 w 个 M_i 生成的索引表 $I = \{I_i\}_{i=1}^{w}$ 发送给边缘服务器。

表 3　　第 j 个哈希表

桶值	图像信息
$\mathrm{BKT}_{i,j}^{1}$	$(\mathrm{ID}(m_{i,1}), \boldsymbol{f}_{i,1}), (\mathrm{ID}(m_{i,12}), \boldsymbol{f}_{i,12}), (\mathrm{ID}(m_{i,35}), \boldsymbol{f}_{i,35}), \cdots$
$\mathrm{BKT}_{i,j}^{2}$	$(\mathrm{ID}(m_{i,7}), \boldsymbol{f}_{i,7}), (\mathrm{ID}(m_{i,24}), \boldsymbol{f}_{i,24}), (\mathrm{ID}(m_{i,67}), \boldsymbol{f}_{i,67}), \cdots$
⋮	⋮
$\mathrm{BKT}_{i,j}^{N_{i,j}}$	$(\mathrm{ID}(m_{i,16}), \boldsymbol{f}_{i,16}), (\mathrm{ID}(m_{i,28}), \boldsymbol{f}_{i,28}), (\mathrm{ID}(m_{i,49}), \boldsymbol{f}_{i,49}), \cdots$

表 4　　加密后的第 j 个哈希表

加密桶值	图像信息
$\varphi(\mathrm{BKT}_{i,j}^{1})$	$(\mathrm{ID}(m_{i,1}), \boldsymbol{f}_{i,1}'), (\mathrm{ID}(m_{i,12}), \boldsymbol{f}_{i,12}'), (\mathrm{ID}(m_{i,35}), \boldsymbol{f}_{i,35}'), \cdots$
$\varphi(\mathrm{BKT}_{i,j}^{2})$	$(\mathrm{ID}(m_{i,7}), \boldsymbol{f}_{i,7}'), (\mathrm{ID}(m_{i,24}), \boldsymbol{f}_{i,24}'), (\mathrm{ID}(m_{i,67}), \boldsymbol{f}_{i,67}'), \cdots$
⋮	⋮
$\varphi(\mathrm{BKT}_{i,j}^{N_{i,j}})$	$(\mathrm{ID}(m_{i,16}), \boldsymbol{f}_{i,16}'), (\mathrm{ID}(m_{i,28}), \boldsymbol{f}_{i,28}'), (\mathrm{ID}(m_{i,49}), \boldsymbol{f}_{i,49}'), \cdots$

5.2.5 陷门生成阶段

$\mathrm{TD} \leftarrow \mathrm{TrapdoorGen}(\Gamma, m_q)$。与索引生成阶段类似，查询用户首先提取查询图像 m_q 的特征向量 $\boldsymbol{f}_q = (\boldsymbol{f}_{q_1}, \boldsymbol{f}_{q_2}, \cdots, \boldsymbol{f}_{q_d})$，然后用 $\psi_j(\cdot)$ 计算桶值 BKT_j，$j \in [1, L]$，用 $\varphi(\cdot)$ 加密桶值为 $\{\varphi(\mathrm{BKT}_j)\}_{j=1}^{L}$。接着用户将 $\boldsymbol{f}_q$ 扩展为 $\overline{\boldsymbol{f}}_q = (-2\boldsymbol{f}_q, 1)$，对于 $l \in [1, d+1]$，若 $\boldsymbol{s}[l] = 0$，则为 $\overline{\boldsymbol{f}}_q^a$ 和 $\overline{\boldsymbol{f}}_q^b$ 随机赋予正值，使其满足 $\overline{\boldsymbol{f}}_q^a[l] + \overline{\boldsymbol{f}}_q^b[l] = \overline{\boldsymbol{f}}_q[l]$；否则，$\overline{\boldsymbol{f}}_q^a[l] = \overline{\boldsymbol{f}}_q^b[l] = \overline{\boldsymbol{f}}_q[l]$。再随机选取正数 $\delta \in \mathbb{R}^+$，用 $\boldsymbol{A}_1^{-1}$、$\boldsymbol{A}_2^{-1}$ 分别乘以 $\overline{\boldsymbol{f}}_q^{a\mathrm{T}}$、$\overline{\boldsymbol{f}}_q^{b\mathrm{T}}$，得到加密查询向量 $\boldsymbol{f}_q' = (\delta \boldsymbol{A}_1^{-1} \overline{\boldsymbol{f}}_q^{a\mathrm{T}}, \delta \boldsymbol{A}_2^{-1} \overline{\boldsymbol{f}}_q^{b\mathrm{T}})$。最后 $\{\varphi(\mathrm{BKT}_j)\}_{j=1}^{L}$、$\boldsymbol{f}_q'$ 和用户身份 UID 组成陷门 $\mathrm{TD} = \{\{\varphi(\mathrm{BKT}_j)\}_{j=1}^{L}, \boldsymbol{f}_q', \mathrm{UID}\}$ 发送给边缘服务器，由边缘服务器进行检索。

5.2.6 检索阶段

$R \leftarrow \mathrm{Search}(C, \Lambda, I, \mathrm{TD})$。检索阶段分两步完成，第一步为计算相似度，第二步为重加密密钥。

1)计算相似度。边缘服务器接收到查询陷门 TD 后，首先在索引表里找到与陷门桶值相同的桶，桶里面的图像即为候选图像集。然后计算候选图像集的特征向量与查询图像特征向量之间的内积值，计算过程如式(1)所示。

$$\begin{aligned} &\boldsymbol{f}_q'^{\mathrm{T}} \boldsymbol{f}_{i,t}' = \\ &(\delta \boldsymbol{A}_1^{-1} \overline{\boldsymbol{f}}_q^{a\mathrm{T}})^{\mathrm{T}} \boldsymbol{A}_1^T \overline{\boldsymbol{f}}_{i,t}^{a\mathrm{T}} + (\delta \boldsymbol{A}_2^{-1} \overline{\boldsymbol{f}}_q^{b\mathrm{T}})^{\mathrm{T}} \boldsymbol{A}_2^{\mathrm{T}} \overline{\boldsymbol{f}}_{i,t}^{b\mathrm{T}} = \\ &\delta \overline{\boldsymbol{f}}_q \overline{\boldsymbol{f}}_{i,t}^{\mathrm{T}} = \delta(\left\| \boldsymbol{f}_{i,t} \right\|^2 - 2\boldsymbol{f}_q \boldsymbol{f}_{i,t}^{\mathrm{T}}) = \delta(\left\| \boldsymbol{f}_q - \boldsymbol{f}_{i,t} \right\|^2 - \left\| \boldsymbol{f}_q \right\|^2) \end{aligned} \tag{1}$$

边缘服务器依次计算候选列表中每幅图像 $m_{i,t}$ 与查询图像 m_q 的内积值，根据内积值大小排序选出前 r 个最相似的加密图像。

2)重加密密钥。边缘服务器根据 r 个加密图像对应的密钥密文 k_i' 及用户身份 UID 对应的转换密钥 $\mathrm{TK}_{\mathrm{UID}}$ 计算 $e(\mathrm{pk}^{\varepsilon_i}, \mathrm{TK}_{\mathrm{UID}})$，计算过程如式(2)所示。

$$\begin{aligned} &e(\mathrm{pk}^{\varepsilon_i}, \mathrm{TK}_{\mathrm{UID}}) = e(g^{\mathrm{sk}_o \varepsilon_i}, g^{\frac{\mathrm{sk}_{\mathrm{UID}}}{\mathrm{sk}_o}}) = \\ &e(g, g)^{\varepsilon_i \mathrm{sk}_{\mathrm{UID}}} = F^{\varepsilon_i \mathrm{sk}_{\mathrm{UID}}} \end{aligned} \tag{2}$$

边缘服务器将 r 个加密图像和对应的重加密密钥作为检索结果返回给查询用户。

5.2.7 图像解密阶段

$M' \leftarrow \mathrm{ImgDec}(R, \mathrm{sk})$。收到检索结果的查询用户用其合法私钥 $\mathrm{sk}_{\mathrm{UID}}$ 计算加密密钥，如式(3)所示。

$$\frac{k_i F^{\varepsilon_i}}{(F^{\varepsilon_i \mathrm{sk}_{\mathrm{UID}}})^{\frac{1}{\mathrm{sk}_{\mathrm{UID}}}}} = \frac{k_i F^{\varepsilon_i}}{F^{\varepsilon_i}} = k_i \tag{3}$$

得到图像加密密钥 k_i，用来解密出相应明文图像。若用户无合法私钥 $\mathrm{sk}_{\mathrm{UID}}$，则不能解密重加密密钥密文，更不能解密图像密文。

本节介绍的方案主要利用代理重加密技术完成密钥转换，借助局部敏感哈希算法提高检索效率，应用安全近邻算法计算内积提高检索精度，其中内积计算方法只能保证唯密文安全，不可抵抗已知背景攻击。如若敌手获得一组明密文对 $(\boldsymbol{f}, \boldsymbol{f}')$ 和一组陷门明密文对 $(\boldsymbol{f}_{q'}, \boldsymbol{f}_{q'}')$，以及明文图像子集 P，计算内积 $\boldsymbol{f}_{q'}'^{\mathrm{T}} \boldsymbol{f}' = \delta(\left\| \boldsymbol{f} \right\|^2 - 2\boldsymbol{f}_{q'} \boldsymbol{f}^{\mathrm{T}})$，由此获得随机数 δ 取值，进而可判断检索结果中其他图像与查询图像明文之间的关系。针对这一问题，下面对此方案（基础方案）做出改进，使其能够抵抗已知背景攻击。

6 改进方案

为使本文方案能够抵抗已知背景攻击，对相似度计算方法进行改进，在特征向量中添加部分冗余项，其他步骤不变。虽然添加冗余项会影响检索精度，但为提高安全性，本文方案可以适当妥协。下面对需改动的阶段进行说明，对无影响的 ImgEnc、KeyTrans 和 ImgDec 阶段不予说明。

KeyGen 将 $d+1$ 维随机二值向量 $\boldsymbol{s}$ 扩充成 $d+\alpha+1$ 维，$(d+1)\times(d+1)$ 维随机可逆矩阵 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 也扩充成 $(d+\alpha+1)\times(d+\alpha+1)$ 维，另外增加 α 维随机向量 $\boldsymbol{\eta}$ 组成冗余项。其余参数不变。

IndexGen 针对特征向量加密过程，将 d 维特征向量 $\boldsymbol{f}_{i,t} = (\boldsymbol{f}_{i,t_1}, \boldsymbol{f}_{i,t_2}, \cdots, \boldsymbol{f}_{i,t_d})$ 扩展成 $d+\alpha+1$ 维向量 $\tilde{\boldsymbol{f}}_{i,t} = (\boldsymbol{f}_{i,t}, \left\| \boldsymbol{f}_{i,t} \right\|, \boldsymbol{\eta})$，其中 $\boldsymbol{\eta} = (\eta_1, \eta_2, \cdots, \eta_\alpha)$。随机分裂和矩阵加密步骤与基础方案一致，得出加密后的向量 $\hat{\boldsymbol{f}}_{i,t} = (\boldsymbol{A}_1^{\mathrm{T}} \tilde{\boldsymbol{f}}_{i,t}^{a\mathrm{T}}, \boldsymbol{A}_2^{\mathrm{T}} \tilde{\boldsymbol{f}}_{i,t}^{b\mathrm{T}})$。

TrapdoorGen 针对查询图像 m_q 的特征向量加密过程，将 d 维特征向量 $\boldsymbol{f}_q = (\boldsymbol{f}_{q_1}, \boldsymbol{f}_{q_2}, \cdots, \boldsymbol{f}_{q_d})$ 扩展成 $\tilde{\boldsymbol{f}}_q = (-2\boldsymbol{f}_q, 1, \boldsymbol{\beta})$，其中 $\boldsymbol{\beta}$ 为 α 维的随机二值向量。后续随机分裂和矩阵加密步骤与基础方案一致，得到加密后的查询向量 $\hat{\boldsymbol{f}}_q = (\delta \boldsymbol{A}_1^{-1} \tilde{\boldsymbol{f}}_q^{a\mathrm{T}}, \delta \boldsymbol{A}_2^{-1} \tilde{\boldsymbol{f}}_q^{b\mathrm{T}})$。

Search 向量内积计算形式变化为

$$\hat{\boldsymbol{f}}_q^{\mathrm{T}}\hat{\boldsymbol{f}}_{i,t}=$$
$$(\delta\boldsymbol{A}_1^{-1}\tilde{\boldsymbol{f}}_q^{a\mathrm{T}})^{\mathrm{T}}\boldsymbol{A}_1^{\mathrm{T}}\tilde{\boldsymbol{f}}_{i,t}^{a\mathrm{T}}+(\delta\boldsymbol{A}_2^{-1}\tilde{\boldsymbol{f}}_q^{b\mathrm{T}})^{\mathrm{T}}\boldsymbol{A}_2^{\mathrm{T}}\tilde{\boldsymbol{f}}_{i,t}^{b\mathrm{T}}=$$
$$\delta\tilde{\boldsymbol{f}}_q\tilde{\boldsymbol{f}}_{i,t}^{\mathrm{T}}=$$
$$\delta(\left\|\boldsymbol{f}_{i,t}\right\|^2-2\boldsymbol{f}_q\boldsymbol{f}_{i,t}^{\mathrm{T}}+\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}})=$$
$$\delta(\left\|\boldsymbol{f}_q-\boldsymbol{f}_{i,t}\right\|^2-\left\|\boldsymbol{f}_q\right\|^2+\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}) \tag{4}$$

由式(4)可以看出，改进方案中内积计算结果比基础方案多出了冗余项 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$。这将提高内积计算结果的安全性，7.1 节会给出具体分析。

7　方案分析

本节将分析所提方案的安全性及理论性，同时使用真实数据集进行实际性能测试。

7.1　安全性分析

本文方案能够达到所提的安全目标，具体分析如下。

1) 图像隐私。本文采用传统对称密钥加密算法加密图像，图像隐私的安全性依赖于加密算法，安全的加密算法能有效防止图像隐私泄露。

2) 索引隐私。对于索引表中的加密桶值 $\varphi(\mathrm{BKT}_{i,j}^b)$，边缘服务器如果没有解密密钥就不会得到明文桶值。对于索引表中存储的特征向量，随机分裂、矩阵相乘、补充冗余项都保护了特征向量隐私。如果边缘服务器想要获得明文特征向量，就需要知道随机向量 $\boldsymbol{s}$ 和随机矩阵 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$ 的值。由于服务器无法得知这些信息，那么索引表中的特征向量也就无法被破解。

3) 密钥隐私。虽然服务器根据重加密密钥可以控制查询用户的访问，但是从中解密出图像拥有者私钥 sk_{o} 和图像查询用户私钥 $\mathrm{sk}_{\mathrm{UID}}$ 依赖于离散对数困难问题的解决。没有 $\mathrm{sk}_{\mathrm{UID}}$ 的服务器无法从计算结果 $F^{\varepsilon_i\mathrm{sk}_{\mathrm{UID}}}$ 中获得图像加密密钥 k。同样，没有被授权的用户因为没有合法的公私钥也无法解密出图像加密密钥。

4)陷门隐私。与索引隐私相同，只要不泄露随机向量 $\boldsymbol{s}$ 和随机矩阵 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$，查询向量就不会被泄露。另外，随机数 δ 的引入保证了陷门之间没有关联，使边缘服务器无法通过陷门判断每次查询图像是否相同。

5)内积计算隐私。虽然边缘服务器根据计算结果可知图像间的相似度，但是由于 δ 和 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 的存在无法恢复出图像之间的距离。另外，为体现冗余项的干扰作用，2 个冗余项 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 有相同取值的可能性应小于 $\frac{1}{2^\gamma}$，即对每一个 $\boldsymbol{f}_{i,t}$，$\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 至少有 2^γ 个不同取值。而 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 的总数不大于 $\mathrm{C}_\alpha^{|\boldsymbol{\beta}|}$，其中 $|\boldsymbol{\beta}|$ 为 $\boldsymbol{\beta}$ 中 1 出现的次数。当 $\frac{\alpha}{|\boldsymbol{\beta}|}=2$ 时 $\mathrm{C}_\alpha^{|\boldsymbol{\beta}|}$ 值最大。即 $\mathrm{C}_\alpha^{|\boldsymbol{\beta}|}\geqslant\left(\frac{\alpha}{|\boldsymbol{\beta}|}\right)^{|\boldsymbol{\beta}|}=2^{|\boldsymbol{\beta}|}$，当 $\alpha=2\gamma$，$|\boldsymbol{\beta}|=\gamma$ 时，有 $\mathrm{C}_\alpha^{|\boldsymbol{\beta}|}\geqslant 2^\gamma$，因此每个 $\boldsymbol{f}_{i,t}$ 至少含有 2γ 个冗余项，每个 $\boldsymbol{f}_q$ 从中随机选取一半的冗余项。为尽可能不影响排序结果的精确性，$\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 应服从正态分布。令随机向量 $\boldsymbol{\eta}$ 的每一维 η_i 服从均匀分布 $\mathrm{U}(\mu'-\zeta,\mu'+\zeta)$，可知均值和方差分别为 μ' 和 $\frac{\zeta^2}{3}$。根据中心极限定理，对于 γ 个独立同分布随机变量 η_i，其和近似服从正态分布 $\mathrm{N}\left(\gamma\mu',\gamma\frac{\zeta^2}{3}\right)$。令 $\mu=\gamma\mu'$，$\sigma^2=\gamma\frac{\zeta^2}{3}$，也就是 $\mu'=\frac{\mu}{\gamma}$，$\zeta=\sqrt{\frac{3}{\gamma}}\sigma$，有 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 服从正态分布 $\mathrm{N}(\mu,\sigma^2)$。此时，方案的精确性和安全性随 σ^2 变化而变化，σ^2 越大，安全性越高，精确度越低；σ^2 越小，安全性越低，精确度越高。更具体的证明可参考文献[29]。此外，根据内积计算形式，可以证明在已知背景攻击模型下对于多项式时间敌手，加密图像集和查询陷门是安全的。

定理 1　对于多项式时间敌手，内积计算在已知背景攻击模型下可保证加密图像集和陷门安全。

在已知背景攻击模型中，敌手可接触加密图像集、加密索引表和陷门集，获取其他背景知识，如一组明密文对和陷门明密文对，以及明文图像子集。假设敌手为 $\mathcal{A}=\{C,T,P,(\boldsymbol{f},\hat{\boldsymbol{f}}),(\boldsymbol{f}_{q'},\hat{\boldsymbol{f}}_{q'})\}$，其中，$C=\{\hat{\boldsymbol{f}}_1,\hat{\boldsymbol{f}}_2,\cdots,\hat{\boldsymbol{f}}_n\}$ 为加密向量集，$T=\{\hat{\boldsymbol{f}}_{q_1},\hat{\boldsymbol{f}}_{q_2},\cdots,\hat{\boldsymbol{f}}_{q_s}\}$ 为陷门集，$P=\{\boldsymbol{f}_1,\boldsymbol{f}_2,\cdots,\boldsymbol{f}_w\}$ 为明文向量集，$(\boldsymbol{f},\hat{\boldsymbol{f}})$ 为一组明密文对，$(\boldsymbol{f}_{q'},\hat{\boldsymbol{f}}_{q'})$ 为一组陷门明密文对。需要说明的是，即使敌手知道加密特征向量集 C，也无法知道 P 中明文特征向量对应的密文形式，更无法得知 P 和 C 之间的对应关系。

证明　图像向量之间的相似度可由式(5)度量。

$$\hat{\boldsymbol{f}}_q^{\mathrm{T}}\hat{\boldsymbol{f}}_i=\delta(\left\|\boldsymbol{f}_i\right\|^2-2\boldsymbol{f}_q\boldsymbol{f}_i^{\mathrm{T}}+\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}) \tag{5}$$

敌手将 $(\boldsymbol{f},\hat{\boldsymbol{f}})$ 和 $(\hat{\boldsymbol{f}}_{q'},\boldsymbol{f}_{q'})$ 代入式(5)，可得

$$\hat{\boldsymbol{f}}_{q'}^{\mathrm{T}}\hat{\boldsymbol{f}}=\delta(\|\boldsymbol{f}\|^2-2\boldsymbol{f}_{q'}\boldsymbol{f}^{\mathrm{T}}+\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}) \tag{6}$$

其中，δ 和 $\boldsymbol{\beta}\boldsymbol{\eta}^{\mathrm{T}}$ 均未知，且加密后的特征向量不会泄露明文特征向量信息，即使已知明文向量集 P，敌手在多项式时间内也无法暴力破解。因此在已知背景攻击模型下，敌手无法获得加密数据集和陷门的明文形式。

证毕。

需要说明的是，为了实现高效加密图像检索方案，有必要泄露最少的信息给边缘服务器。例如边缘服务器很容易知道在同一个哈希桶中的图像是相似的，同样也知道检索结果里的图像是相似的。如果想要避免这些信息泄露，可以采用文献[30]中的方案。但考虑到其复杂度过高，效率低下，且远未达到实用程度，本文暂不解决这些问题。

7.2　性能分析

下面分别从理论和实际性能 2 个方面与文献[13]方案（MIPP, multiple image owners with privacy protection）对比，论证本文方案（基础方案、改进方案）的可行性。理论分析涉及计算开销和存储开销。实际性能主要对 KeyGen、KeyTrans、IndexGen、Search 这 4 个阶段以及检索精度进行仿真实验。

7.2.1　计算开销分析

表 5 给出了 3 种方案的理论计算开销对比。本文主要考虑了几种比较耗时的密码运算，即群 Z_p 指数运算、群 G 指数运算、群 G_T 指数运算、双线性对运算 E、哈希运算 H、矩阵运算 M'、M'' 以及 MIPP 中群指数运算 G_q 和加法运算 $G_q^{'}$。另外，图像加解密采用传统对称加解密算法，在此不予分析。

表 5 中，w 表示图像拥有者个数，d 表示提取出的特征向量维数，d' 表示基础方案中加密特征向量维数，d'' 表示改进方案中加密特征向量维数，n 表示图像总数，L 表示哈希表个数，λ 表示哈希函数个数，r' 表示检索结果中来自不同密钥加密的图像种类，符号“—”表示不存在。

由表 5 可看出，在 KeyGen 阶段，密钥生成时间随图像加密密钥个数增加而增加，方案改进前后向量维数增多使密钥生成时间也增多。在 KeyTrans 阶段，密钥转换时间受密钥个数影响，密钥个数越多，密钥转换时间越多。但方案改进前后，该阶段计算开销保持一致。在 IndexGen 阶段，索引生成时间与图像总数呈正相关，特别是改进方案中矩阵维数增加，因此改进方案的索引生成时间比基础方案多。在 TrapdoorGen 阶段，考虑一个用户的一次查询，陷门生成时间主要受矩阵计算、哈希计算以及特征向量维数影响。在 Search 阶段，计算开销主要受向量维数或加密密钥个数影响。根据以上几个阶段的分析，改进方案比基础方案计算开销增大或者保持一致，主要是因为特征向量维数增大，但以此为代价可换来安全性的提高。由于 MIPP 没有进行密钥转换，因此只列出了其他 4 个阶段。可以看出，MIPP 每个阶段的计算开销与群指数运算密切相关，而本文方案只有 2 个阶段的开销受群指数运算影响。

7.2.2　存储开销分析

表 6 给出了 3 种方案的理论存储开销对比。其中 $|G|$、$|G_T|$、$|Z_p|$、$|Z_q|$、$|G_p|$ 和 $|G_q|$ 分别表示群 G、G_T、Z_p、Z_q、G_p 和 G_q 中元素的长度。同计算开销分析一致，图像加解密算法在此不予分析。另外，服务器将检索结果传给查询用户后即可删除检索结果，因此也不考虑检索阶段的存储开销。

表 6 中，w 表示图像拥有者个数，d 表示提取

表 5　3 种方案的理论计算开销对比

方案	KeyGen	KeyTrans	IndexGen	TrapdoorGen	Serach
基础方案	$2G+rZ_p+2d'^2$	$(w+2)G+wG_T$	$(\lambda LH+2M')n$	$\lambda LH+2M'$	$2d'^2n+r'E$
改进方案	$2G+rZ_p+2d''^2$	$(w+2)G+wG_T$	$(\lambda LH+2M'')n$	$\lambda LH+2M''$	$2d''^2n+r'E$
MIPP	$(2+3d)wG_q$	—	$ndpG_q$	dpG_q	$n(2G_q+G_q^{'})$

表 6　3 种方案的理论存储开销对比

方案	KeyGen	KeyTrans	IndexGen	TrapdoorGen
基础方案	$2\|G\|+(w+2)\|Z_p\|+2d'(d'+1)+(L+1)d$	$(w+1)\|G\|+w\|G_T\|$	$2d'n\|Z_p\|$	$2d'\|Z_p\|$
改进方案	$2\|G\|+(w+2)\|Z_p\|+2d''(d''+1)+(L+1)d$	$(w+1)\|G\|+w\|G_T\|$	$2d''n\|Z_p\|$	$2d''\|Z_p\|$
MIPP	$w\left(d\|Z_q\|+\|Z_p\|\right)+\|G_p\|$	—	$2n\|G_q\|$	$2\|G_q\|$

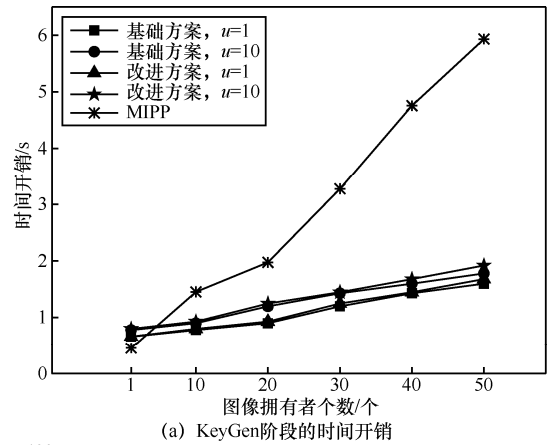
出的特征向量维数，d' 表示基础方案中加密特征向量维数，d'' 表示改进方案中加密特征向量维数，n 表示图像总数，L 表示哈希表个数，符号“—”表示不存在。

由表 6 可以看出，在 KeyGen 阶段，需要存储公私钥、图像加密密钥以及系统秘密参数。假设用户个数为 1，存储开销随图像拥有者个数和特征向量维数增加而增加。在 KeyTrans 阶段，存储开销随图像拥有者个数增长而增长。该阶段存储开销在方案改进前后不变。在 IndexGen 阶段，索引存储开销和图像总数呈正相关。当给定图像个数时，图像特征向量的维数会影响索引存储开销。在 TrapdoorGen 阶段，考虑一个用户的一次查询，陷门存储开销主要受向量维数影响。根据以上 4 个阶段的存储开销分析可以看出，改进方案比基础方案的存储开销大是由特征向量维数增加造成的，但增加的维数与图像明文特征向量维数对比可以忽略。与 MIPP 对比，本文方案存储开销受较多因素影响，但从后续实验可看出本文方案存储开销是可接受的。

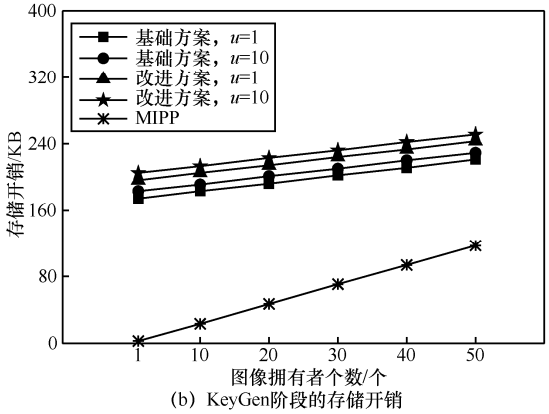
7.2.3　实际性能

为测试本文方案的实际性能，基于 Corel100 数据集[31]，从每一类中分别取 20、40、60、80、100 幅图像组成 2 000、4 000、6 000、8 000、10 000 幅图像，并提取图像的 CLD 特征[32]。实验环境为 PC 机（i5-4590 主频 3.3 GHz，内存为 4 GB，操作系统为 Win7 64b），实验工具采用 Python2.7。图 4~图 8 展示了本文方案在 KeyGen、KeyTrans、IndexGen、Search 这 4 个阶段以及检索精度上与 MIPP 的比较。由于本文着重研究加密图像检索方法，而不是图像加密方法，且陷门生成本质上为索引生成 n=1 的情况，因此文中没有测试 ImgEnc、ImgDec 和 TrapdoorGen 这 3 个阶段的开销。

在 KeyGen 阶段，假设一个拥有者对应一个加密密钥，从图 4(a)可看出，MIPP 的时间开销增幅最大。基础方案和改进方案的时间开销非常接近，说明特征向量维数变化对时间开销影响很小。特别地，当用户个数分别为 1 和 10 时，改进方案生成 50 个密钥所需时间分别为 1.7 s 和 1.9 s 左右。图 4(b)中本文方案存储开销增长缓慢。特别地，当用户个数分别为 1 和 10 时，改进方案生成 50 个密钥所需存储空间分别为 243 KB 和 251 KB 左右。虽然维数增多导致开销增长，但同时也提高了方案的安全性。

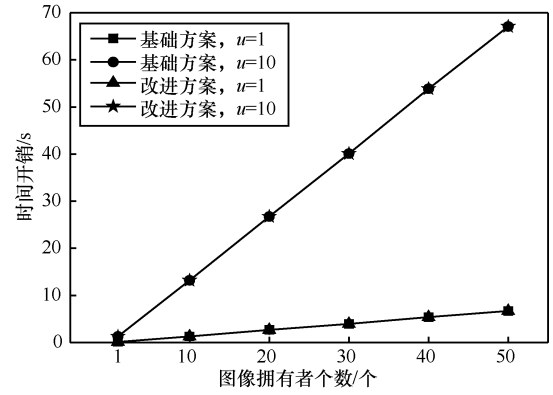


(a) KeyGen阶段的时间开销

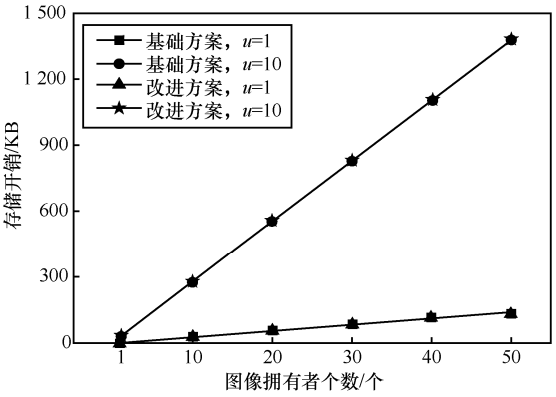


(b) KeyGen阶段的存储开销

图 4　KeyGen 阶段



(a) KeyTrans阶段的时间开销



(b) KeyTrans阶段的存储开销

图 5　KeyTrans 阶段

在 KeyTrans 阶段，仅考虑本文方案开销，如图 5 所示，特征向量维数变化不影响基础方案和改进方案的开销。随着用户数增加，需要的转换密钥相应增加。特别地，当用户个数分别为 1 和 10 时，转换 50 个密钥所需时间分别为 8 s 和 68 s 左右，所需存储空间分别为 160 KB 和 1 400 KB 左右。为实现多密钥场景，密钥转换时间和存储开销随密钥个数增多是不可避免的。但这只是一次性操作，相比于图像加密所带来的巨额开销是可接受的。

在 IndexGen 阶段，如图 6 所示，时间开销和存储开销随图像总数增多而增加。本文方案索引生成时间开销明显少于 MIPP，存储开销增加是因为存储了加密向量。方案改进前后增长趋势接近，说明向量维数增加带来的影响很小。特别地，当图像总数为 10 000 幅时，方案改进前后生成索引所需时间分别约为 117 ms 和 123 ms，所需存储空间分别约为 10.5 MB 和 11.5 MB。

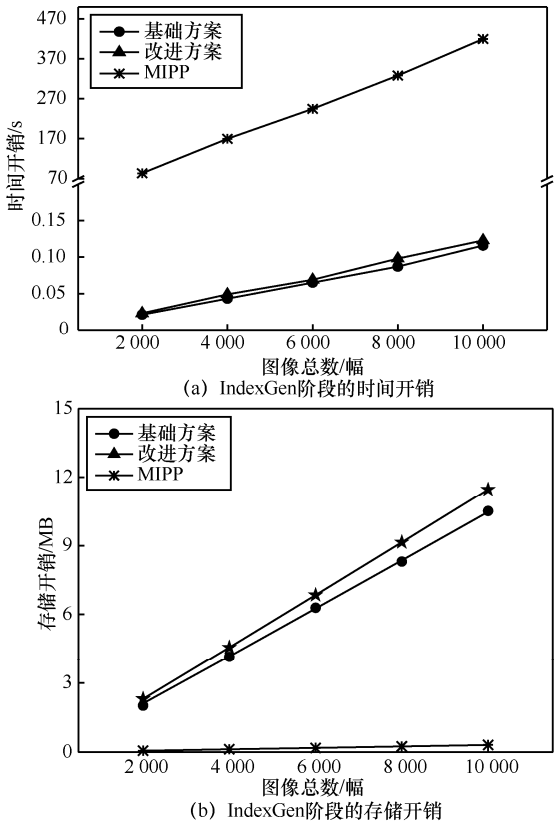


图 6 IndexGen 阶段

在 Search 阶段，仅考虑检索时间开销，如图 7 所示。方案改进前后的时间开销很接近，说明向量维数变化不会明显影响检索时间。随图像总数增加，检索时间增长趋势不明显，这是因为局部敏感哈希有效缩短了检索时间。随着拥有者数量增多，导致服务器需要做更多的密钥转换，本文方案时间开销多于 MIPP。尽管如此，本文方案在多密钥场景下搜索 10 000 幅图像仅耗时 0.26 s，这是可接受的。

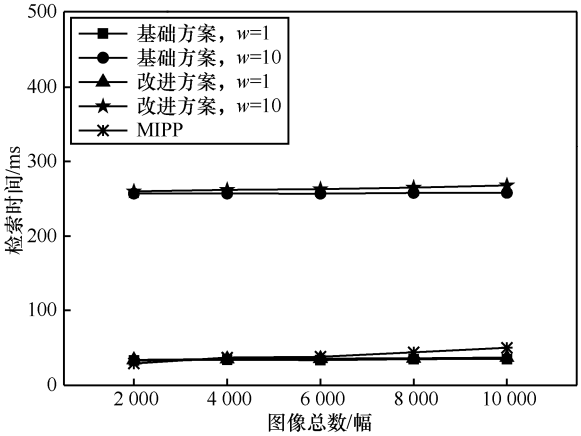


图 7 Search 阶段

本文方案采用的精度计算方式为 $p=\frac{r'}{r}$，其中 r 为返回检索结果数目，r' 为返回结果中正确的图像个数，即与查询图像同类的图像个数。边缘服务器返回 10 000 幅图像的前 r 个检索结果得到的检索精度随图像总数的变化情况如图 8 所示。随着 r 的增大，检索精度逐渐下降。与明文下的检索精度相比，加密算法导致密文检索精度下降。基础方案与改进方案的检索精度变化曲线接近，说明冗余项的增加在提高方案安全性的前提下没有明显降低检索精度。由于 MIPP 为提高检索效率简化了欧氏距离计算方法，导致其检索精度很低，这将严重影响 MIPP 的实用性。

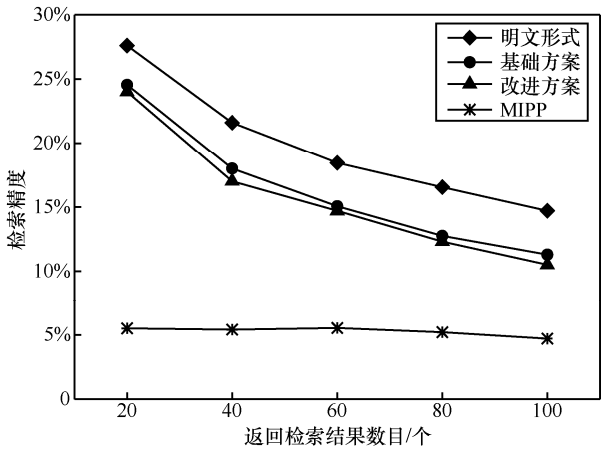


图 8 检索精度

综上所述，虽然本文方案时间开销和存储开销

受图像加密密钥个数和用户个数影响较大，但是对于实现多密钥场景来说，这是不可避免的。同时，为了提高方案安全性，加入冗余项之后的改进方案比基础方案性能稍有恶化，但是依然在可接受的范围内。因此，本文方案在实际应用中是可行的。

8　结束语

本文针对边缘计算环境下的图像隐私安全问题，借助于边缘计算低时延、高可用、高实时的优势，设计了一种支持多密钥的加密图像检索方案。应用局部敏感哈希算法对图像进行了预处理，提高了检索速度。利用安全近邻算法加密图像特征，使边缘服务器可以直接计算图像之间的相似度并排序，提高了检索精度。同时利用代理重加密技术进行密钥转换，管理用户访问不同加密密钥加密的图像集。方案分析表明，本文方案达到了安全目标，可抵抗已知背景攻击，并且在实际应用中是可行的。进一步研究工作将会结合实际需求对方案的查询功能进行扩展。

参考文献：

[1] LU W J, VARNA A L, SWAMINATHAN A, et al. Secure image retrieval through feature protection[C]//Proceedings of 34th Internet Conference on Acoustics, Speech and Signal Processing. Piscataway: IEEE Press, 2009: 1533-1536.

[2] LU W J, VARNA A L, WU M. Confidentiality-preserving image search: a comparative study between homomorphic encryption and distance-preserving randomization[J]. IEEE Access, 2014(2): 125-141.

[3] ZHANG L, JUNG T, LIU K B, et al. PIC: enable large-scale privacy preserving content-based image search on cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2017, 28(11): 3258-3271.

[4] XIA Z H, ZHU Y, SUN X M, et al. Towards privacy-preserving content-based image retrieval in cloud computing[J]. IEEE Transactions on Cloud Computing, 2018, 6(1): 276-286.

[5] ZHENG P J, HUANG J W. An efficient image homomorphic encryption scheme with small ciphertext expansion[C]//Proceedings of 21st ACM Internet Conference on Multimedia. New York: ACM Press, 2013: 803-812.

[6] QIN Z, YAN J B, REN K, et al. Privacy-preserving outsourcing of image global feature detection[C]//Proceedings of Global Communications Conference. Piscataway: IEEE Press, 2014: 710-715.

[7] QIN Z, YAN J B, REN K, et al. Towards efficient privacy-preserving image feature extraction in cloud computing[C]//Proceedings of Internet Conference on Computational Geometry. Piscataway: IEEE Press, 2014: 497-506.

[8] LU W J, SWAMINATHAN A, VARNA A L, et al. Enabling search over encrypted multimedia databases[C]//Proceedings of IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics. Bellingham: SPIE, 2009: 725418.

[9] ZHANG Y, ZHOU L, PENG Y F, et al. A secure image retrieval method based on homomorphic encryption for cloud computing[C]//Proceedings of 19th Internet Conference on Digital Signal Processing. NewYork: ACM Press, 2014: 269-274.

[10] XIA Z H, XIONG N N, VASILAKOS A V, et al. EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing[J]. Information Sciences, 2017, 387: 195-204.

[11] YUAN J W, YU S C, GUO L K. SEISA: secure and efficient encrypted image search with access control[C]//Proceedings of 34th Internet Conference on Computer Communications. Piscataway: IEEE Press, 2015: 2083-2091.

[12] LIANG H H, ZHANG X P, WEI Q H, et al. Secure image retrieval with multiple keys[J]. Journal of Electronic Imaging, 2018, 27(2): 023032.

[13] SHEN M, CHENG G, ZHU L, et al. Content-based multi-source encrypted image retrieval in clouds with privacy preservation[J]. Future Generation Computer Systems, (2018-05-09)[2020-01-06]. doi.org/10.1016/j.future.2018.04.089.

[14] YIN H, QIN Z, ZHANG J X, et al. Secure conjunctive multi-keyword search for multiple data owners in cloud computing[C]//Proceedings of 22nd Internet Conference on Parallel and Distributed Systems. New York: ACM Press, 2016: 761-768.

[15] SUN W H, YU S C, LOU W J, et al. Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(4): 1187-1198.

[16] MIAO Y B, MA J F, LIU X M, et al. VKSE-MO: verifiable keyword search over encrypted data in multi-owner settings[J]. Science China Information Sciences, 2017, 60(12): 1-15.

[17] MIAO Y B, MA J F, LIU X M, et al. VCKSM: verifiable conjunctive keyword search over mobile e-health cloud in shared multi-owner settings[J]. Pervasive and Mobile Computing, 2017, 40: 205-219.

[18] 王祥宇, 马建峰, 苗银宾. 高效隐私保护的多用户图像外包检索方案[J]. 通信学报,2019,40(2):31-39.
WANG X Y, MA J F, MIAO Y B. Efficient privacy-preserving image retrieval scheme over outsourced data with multi-user [J]. Journal on Communications, 2019, 40(2):31-39.

[19] SUN S F, LIU J K, SAKZAD A, et al. An efficient non-interactive multi-client searchable encryption with support for boolean queries[C]//European Symposium On Research in Computer Security. Berlin: Springer, 2016: 154-172.

[20] HAMLIN A, SHELAT A, WEISS M, et al. Multi-key searchable encryption, revisited[C]//IACR International Workshop on Public Key Cryptography. Berlin: Springer, 2018: 95-124.

[21] SHANKAR K, LAKSHMANAPRABU S K, GUPTA D, et al. Adaptive optimal multi key based encryption for digital image security[J]. Concurrency and Computation: Practice and Experience, 2018: e5122.

[22] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[23] ATENIESE G, FU K, GREEN M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security, 2006, 9(1): 1-30.

[24] ANDONI A, INDYK P. Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions[C]//Proceedings of 47th Symposium on Foundations of Computer Science. New York: ACM Press, 2006: 459-468.

[25] DATAR M, IMMORLICA N, INDYK P, et al. Locality-sensitive hashing scheme based on p-stable distributions[C]//Proceedings of 20th Symposium on Computational Geometry. New York: ACM Press, 2004: 253-262.

[26] DELFS H, KNEBL H, KNEBL H. Introduction to cryptography: principles and applications[M]. Berlin: Springer, 2002.

[27] LIU K, GIANNELLA C, KARGUPTA H. An attacker's view of distance preserving maps for privacy preserving data mining[C]//Proceedings of European Conference Principles of Data Mining and Knowledge Discovery. Berlin: Springer, 2006: 297-308.

[28] WONG W K, CHEUNG D W, KAO B, et al. Secure kNN computation on encrypted databases[C]//Proceedings of 28th Internet Conference on Management of Data. New York: ACM Press, 2009: 139-152.

[29] CAO N, WANG C, LI M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.

[30] CHOR B, GOLDREICH O, KUSHILEVITZ E, et al. Private Information Retrieval[C]//Proceedings of 36th Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1995: 41-50.

[31] WANG J Z, LI J, WIEDERHOLD G. SIMPLIcity: semantics-sensitive integrated matching for picture libraries[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2001, 23(9): 947-963.

[32] MANJUNATH B S, OHM J R, VASUDEVAN V V, et al. Color and texture descriptors[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2001, 11(6): 703-715.

[作者简介]

李颖莹（1995− ），女，陕西汉中人，西安电子科技大学博士生，主要研究方向为数据隐私保护、云计算安全。

马建峰（1963− ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为计算机系统安全、移动与无线安全、系统可生存性和可信计算。

苗银宾（1988− ），男，河南驻马店人，博士，西安电子科技大学讲师，主要研究方向为应用密码学、无线网络安全。