高效隐私保护的多用户图像外包检索方案

王祥宇[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：传统的隐私保护的图像检索方案会带来较大的计算量和通信开销，且在多用户场景下无法保护图像特征向量和查询请求的隐私。为此，提出了多用户场景下高效隐私保护的基于内容的图像检索方案。该方案利用隐私保护的欧式距离比较技术对图像特征向量进行相似度排序并返回 top-k 结果。同时，设计的高效密钥转换协议允许每一个检索用户使用自身的私钥生成查询请求，并检索不同数据拥有者生成的加密图像。安全分析表明，图像检索过程中，用户个人隐私以及云端数据安全都可以得到保护，且基于实际数据集的性能分析表明提出的图像检索方案在实际应用中是高效可行的。

关键词：基于内容的图像检索；多用户；隐私保护；密钥转换协议

中图分类号：TN918.4

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019023

Efficient privacy-preserving image retrieval scheme over outsourced data with multi-user

WANG Xiangyu[1,2], MA Jianfeng[1,2], MIAO Yinbin[1]

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

2. Shaanxi Key Laborary of Network and System Security, Xidian University, Xi’an 710071, China

Abstract: The traditional privacy-preserving image retrieval schemes not only bring large computational and communication overhead, but also cannot protect the image and query privacy in multi-user scenarios. To solve above problems, an efficient privacy-preserving content-based image retrieval scheme was proposed in multi-user scenarios. The scheme used Euclidean distance comparison technique to rank the pictures according to similarity of picture feature vectors and return top-k returned. Meanwhile, the efficient key conversion protocol designed in proposed image retrieval scheme allowed each search user to generate queries based on his own private key so that he can retrieval encrypted images generated by different data owners. Strict security analysis shows that the user privacy and cloud data security can be well protected during the image retrieval process, and the performance analysis using real-world dataset shows that the proposed image retrieval scheme is efficient and feasible in practical applications.

Key words: content-based image retrieval, multi-user, privacy-preserving, key conversion protocol

1 引言

随着数码相机、智能手机、医疗影像设备等成像设备的发展，图像数量呈爆炸性增长。从大规模图像数据集中检索特定的图像在疾病检测与诊断[1]、网上购物和社交网络[2]等许多实践领域受到越来越多的关注。

但是，每个图像由成千上万个特征点组成，大规模图像检索业务给许多公共服务组织或公司带

收稿日期：2018−04−04；**修回日期**：2018−07−26

基金项目：促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.2016TZC-G-6-3）；国家自然科学基金青年基金资助项目（No.61702404）

Foundation Items: The Key Program of NSFC Grant (No.U1405255), The Shaanxi Science & Technology Coordination & Innovation Project(No.2016TZC-G-6-3), The National Natural Science Foundation of China (No.61702404)

来巨大的资源消耗。例如，即使患者已经离开，医院也需要存储患者的所有医疗图像；社交媒体平台需要将所有用户的照片存储在他们的相册中。随着云计算的发展，许多企业和组织目前更愿意在公有云平台上托管他们的数据和服务，这样既可以节省基础设施投入，也能更好地提供服务。但是，由于许多图像中包含敏感信息，将图像直接外包给公有云可能会导致隐私泄露甚至引起法律纠纷[3]。

为了解决这一问题，Shashank 等[4]提出了一种基于内容的图像检索（CBIR, content-based image retrieval）方案，该方案保护了查询图像的隐私，但是图像数据集是未加密的，导致数据集内容直接暴露给云服务器。为此，Lu 等[5]首次在加密图像域上构建了隐私保护的 CBIR 方案。该方案通过提取视觉词汇来表示图像，使用 Jaccard 相似度来评估 2 个图像之间的相似性，并采用保序加密和最小散列算法来保护视觉词的信息，但该方案仅适用于视觉词表示的图像检索算法，其准确度比基于 Fisher 向量的图像检索算法低 20%以上[6-7]。尽管基于同态加密的方案可以保证检索准确度，但是通常会产生很大的时间和存储开销[8-10]。为了实现高效准确的 CBIR 方案，Xia 等[11]一方面采用安全 k 近邻（kNN，k-nearest neighbors）算法[12]来保护特征向量，使云服务器能够高效地对检索结果进行排序；另一方面在牺牲检索准确度的前提下使用局部敏感散列建立双层索引来提高检索效率。Yuan 等[13]同样使用安全 kNN 算法来保护 Fisher 向量[6-7]，并通过 K-means 聚类算法提高大规模数据检索效率，该方案对加密图像的检索效率和准确率接近明文图像检索的性能。但是，由于安全 kNN 算法使用对称密钥加密，在多用户场景下，各个用户可以相互解密查询请求，这带来了极大的隐私泄露威胁。为此，Zhang 等[14]使用一种多级同态加密协议设计了一个支持多用户的图像检索系统，每个用户使用不同的私钥加密查询请求，保证了隐私性，但是该方案带来了巨大的通信开销和计算开销。

为了实现一个高效隐私保护的多用户图像检索方案，需要解决以下关键挑战：1) 所有图像特征向量都应加密，检索过程应以非交互方式完成，所有存储和大部分计算应外包给公有云平台，且要求公有云平台无法获取图像、特征向量和检索结果的隐私信息；2) 每个用户应该持有不同的加密密钥，这样即使用户的请求被截取了，也无法获得请求内容；3) 每个用户要能够对云端存储的所有图像进行检索，以便满足大规模数据共享的需求。

本文提出的方案很好地满足了以上需求，表 1 显示了本文的方案与文献[13-14]方案的对比情况。可以看到，与这种方案相比，本文的方案具有更低的存储要求和计算量，同时还能满足多用户需求。

表 1　　3 种方案的开销对比

方案	存储开销	通信开销	计算开销	支持多用户
SEIS 方案[13]	低	低	低	否
PIC 方案[14]	非常高	非常高	中等	是
本文方案	非常低	低	非常低	是

2　系统模型、安全威胁模型及设计目标

2.1　系统模型

如图 1 所示，所提方案主要考虑 5 个实体：云服务器（CS，cloud server）、数据拥有者（DO，data owner）、检索用户（SU，search user）、密钥转换中心（KCC, key conversion center）和可信代理（TA,

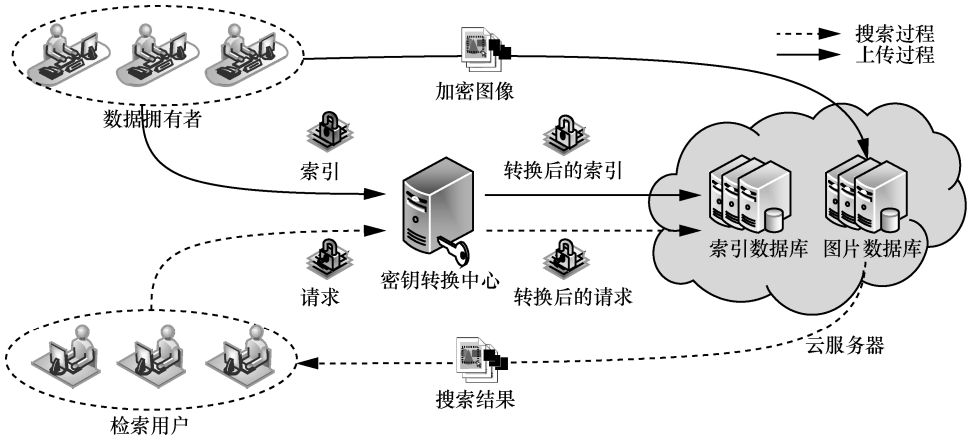

图 1　系统模型

trusted agent）。

1) DO 是图像数据的拥有者，在外包图像之前先把图像特征提取出来构建加密检索索引，然后把密文索引和使用对称加密算法（如 AES）加密的图像一起提交到 CS。

2) CS 拥有大量的存储空间和计算资源，为用户提供存储和计算服务。

3) SU 根据所需检索的图像内容生成检索请求提交给 KCC，并从 CS 得到检索结果。

4) KCC 是独立的第三方，拥有一定的计算能力，为其他实体提供密钥转换服务，包括索引和查询请求的转换。

5) TA 是可信的第三方，给系统中的各个实体分配密钥。

2.2　安全威胁模型

在提出的方案中，CS 和 KCC 是“好奇而诚实”的，即 CS 和 KCC 将遵循给定的协议来执行服务，但它可能会分析用户的数据以获取额外的敏感信息。DO 和 SU 被认为是诚实的，并且不会与 CS 及 KCC“勾结”。KCC 是独立的第三方，其不会与任何一方“合谋”。这些假设与大多数关注公共云中加密数据检索的现有相关工作一致[12-15]。根据云服务器的可用信息，在数据的隐私保护方面考虑以下 2 种威胁模型。

1) 已知密文模型。CS 只能访问所有加密的图像，加密的可检索索引和加密的检索请求。CS 不能对图像数据集进行学习，可检索索引中的特征向量信息对 CS 也是保密的。

2) 已知背景模型。在这个更强的威胁模型中，CS 拥有已知密文模型中的所有信息[12-15]。另外，CS 可以提取数据集中特定加密图像的统计信息，如检索频率，甚至可以获知数据集中的一些图像，但是不知道图像的明文–密文对。

2.3　设计目标

1) 高效性。系统必须满足高效性，即具备很低的通信和计算开销，同时具有高准确度。

2) 多用户。系统必须支持多个用户同时对云服务器的图像集进行安全检索，即在检索过程中，用户无法获取其他用户的请求信息，也无法获得索引内容。但是，用户可以对 CS 上的所有图像进行检索，这使本文方案可以实现大规模多源数据共享。

3) 隐私保护。为了保证用户数据的隐私不被泄露给云服务器，必须满足下列隐私需求。

① 图像安全性：提出的方案必须保证原始图像数据集对 CS 保持机密，同时对 SU 是可用的。这可以使用对称加密（即 AES 等）来解决，下文中不再叙述。

② 索引和请求机密性：必须保证 CS 不能通过索引或请求来推断出图像的内容[注1]。

③ 查询请求的不可链接性：在检索过程中，攻击者不应该能够判断 2 个或多个检索是否来自同一个检索请求。

3　图像检索方案设计

本节首先提出一种高效的单用户图像检索方案。随后，为了支持多用户图像检索，提出了一个多用户密钥转换协议，从而实现多用户图像检索。表 2 定义了要使用到的符号，另外定义 2 个描述符。

表 2　　符号含义

符号	意义
$\boldsymbol{M}_{Oi}$	数据拥有者的用户密钥
$\boldsymbol{M}'_{Oi}$	数据拥有者的转换密钥
$\boldsymbol{M}_{Ui}$	检索用户的用户密钥
$\boldsymbol{M}'_{Ui}$	检索用户的转换密钥
$E_{M}(\cdot)$	使用密钥 $\boldsymbol{M}$ 加密
$SK=\{\boldsymbol{M},\boldsymbol{M}^{-1}\}$	加密密钥
$\vec{I}_i=\{d_1,d_2,\cdots,d_m\}$	图像索引
$\vec{Q}=\{q_1,q_2,\cdots,q_m\}$	查询请求

定义 1　对任意 $x\in\mathbb{R}$，$\lfloor x\rceil$ 表示最接近 x 的整数，$\lfloor x\rceil_h$ 代表 $\lfloor x\rceil$ 模 h。

定义 2　对任意向量 $\vec{\boldsymbol{V}}$ /矩阵 $\boldsymbol{M}$，$|\max(\vec{\boldsymbol{V}})|$（$|\max(\boldsymbol{M})|$）表示其中元素绝对值的最大值。

3.1　单用户图像检索方案

在图像检索方案中，使用主成分分析（PCA，principal components analysis）[15]算法对图像的 Fisher 矢量[6-7]进行降维，作为相似度匹配的依据，并使用欧式距离来衡量相似度。为了实现数据隐私保护，引入了隐私保护的欧氏距离比较技术 [16]。通过该技术，可以以一种安全的方式比较 2 个加密向量与同一向量之间欧氏距离的大小。该技术的细节

注1　本文不考虑访问权限的控制问题，即假设对于所有检索到的结果，SU 都可以解密。访问控制可以通过基于属性的加密技术在所提方案上进行扩展。

在图像检索方案中进行介绍。

单用户图像检索方案主要包括 4 个算法：密钥生成(KeyGen)、索引生成(IndexBuild)、查询生成(QueryGen)和图像检索(ImSearch)，具体如下。

1) KeyGen 算法。TA 随机选择一个 $2m\times 2m$ 的可逆矩阵 $\boldsymbol{M}$，并生成加密密钥 $\mathbf{SK}=\{\boldsymbol{M},\ \boldsymbol{M}^{-1}\}$，然后通过安全信道将 SK 分发给 DO 和 SU，其中 $\boldsymbol{M}^{-1}$ 为 $\boldsymbol{M}$ 的逆矩阵。

2) IndexBuild 算法。首先，对于每一个图像，DO 首先提取出特征向量 $\vec{\boldsymbol{I}}_i=\{d_1,d_2,\cdots,d_m\}$，将其使用同样比例化为整数（例如，同时乘以 10 000）。然后，DO 将 $\vec{\boldsymbol{I}}_i$ 扩展为 $2m$ 维，如式(1)所示。

$$\vec{\boldsymbol{I}}_i=\{d_1,d_2,\cdots,d_m,-\frac{1}{2}\sum_{j=0}^{m}d_j^2,\alpha_1,\cdots,\alpha_{m-1}\} \tag{1}$$

其中，$\alpha_1,\alpha_2,\cdots,\alpha_{m-1}\in\mathbb{Z}_p$ 是由 DO 随机选择的整数，整数 p 代表数值范围。完成扩展之后，DO 对每一个索引 $\vec{\boldsymbol{I}}_i$ 进行加密，如式(2)所示。

$$E_{\boldsymbol{M}}(\vec{\boldsymbol{I}}_i)=(\Gamma\vec{\boldsymbol{I}}_i+\vec{\varepsilon}_i)\times\boldsymbol{M} \tag{2}$$

其中，$\Gamma\in\mathbb{Z}_h, h\gg p\gg 2|\max(\vec{\varepsilon}_i)|$，$\vec{\varepsilon}_i\in\mathbb{Z}_p^{2m}$ 是 DO 为每一个索引 $\vec{\boldsymbol{I}}_i$ 生成的随机误差向量。加密完成后，DO 公布系统参数 Γ 并将 $E_{\boldsymbol{M}}(\vec{\boldsymbol{I}}_i)$ 发送给 CS。

3) QueryGen 算法。给定一个查询请求 $\vec{\boldsymbol{Q}}=\{q_1,q_2,\cdots,q_m\}$，SU 首先将其扩展为 $2m$ 维，如式（1）所示。

$$\vec{\boldsymbol{Q}}=\{\gamma q_1,\gamma q_2,\cdots,\gamma q_m,\gamma,\beta_1,\beta_2,\cdots,\beta_{m-1}\} \tag{3}$$

其中，$\beta_1,\beta_2,\cdots,\beta_{m-1}\in\mathbb{Z}_p$ 是随机整数，$\gamma\in\mathbb{Z}_p$ 是一个随机正整数。然后，SU 将检索请求 $\vec{\boldsymbol{Q}}$ 加密为

$$E_{\boldsymbol{M}^{-1}}(\vec{\boldsymbol{Q}})=\boldsymbol{M}^{-1}(\Gamma\vec{\boldsymbol{Q}}^{\mathrm{T}}+\vec{\varepsilon}_q) \tag{4}$$

其中，$\vec{\varepsilon}_q\in\mathbb{Z}_p^{2m}$ 是 SU 为 $\vec{\boldsymbol{Q}}_i$ 生成的随机的误差向量。加密完成后，SU 把检索请求 $E_{\boldsymbol{M}^{-1}}(\vec{\boldsymbol{Q}})$ 发送给 CS。

4) ImSearch 算法。在收到 $E_{\boldsymbol{M}^{-1}}(\vec{\boldsymbol{Q}})$ 后，CS 根据请求与索引的欧式距离对图像进行排序检索。给定检索请求 $-E_{\boldsymbol{M}^{-1}}(\vec{\boldsymbol{Q}})$ 和密文索引 $E_{\boldsymbol{M}}(\vec{\boldsymbol{I}}_a)$、$E_{\boldsymbol{M}}(\vec{\boldsymbol{I}}_b)$、$\vec{\boldsymbol{Q}}$ 与 $\vec{\boldsymbol{I}}_a$，$\vec{\boldsymbol{I}}_b$ 之间的欧式距离可以通过式(5)~式(7)进行比较。

$$\mathrm{Comp}_{ia}=\left[\frac{E_{\boldsymbol{M}^{-1}}(\vec{\boldsymbol{Q}})E_{\boldsymbol{M}}(\vec{\boldsymbol{I}}_a)}{\Gamma^2}\right]_h=$$

$$\left[\sum_{j=1}^{m}\gamma(q_jd_{aj}-\frac{1}{2}\sum_{j=1}^{m}d_j^2)+\sum_{j=1}^{m-1}\alpha_j\beta_j+\frac{\vec{\varepsilon}_i\vec{\varepsilon}_q^{\mathrm{T}}}{\Gamma^2}+\frac{\vec{\boldsymbol{Q}}\vec{\varepsilon}_q^{\mathrm{T}}+\vec{\varepsilon}_i\vec{\boldsymbol{I}}_a^{\mathrm{T}}}{\Gamma}\right]_h=$$

$$\sum_{j=1}^{m}\gamma(q_jd_{aj}-\frac{1}{2}\sum_{j=1}^{m}d_j^2)+\sum_{j=1}^{m-1}\alpha_j\beta_j=$$

$$-\frac{\gamma}{2}(\mathrm{Dis}\{\vec{\boldsymbol{Q}},\vec{\boldsymbol{I}}_a\}-\sum_{j=1}^{m}q_j^2)+\sum_{j=1}^{m-1}\alpha_j\beta_j \tag{5}$$

$$\mathrm{Comp}_{ib}=-\frac{\gamma}{2}(\mathrm{Dis}\{\vec{\boldsymbol{Q}},\vec{\boldsymbol{I}}_b\}-\sum_{j=1}^{m}q_j^2)+\sum_{j=1}^{m-1}\alpha_j\beta_j \tag{6}$$

$$\mathrm{Comp}_{ab}=\mathrm{Comp}_b-\mathrm{Comp}_a=\frac{\gamma}{2}(\mathrm{Dis}\{\vec{\boldsymbol{Q}},\vec{\boldsymbol{I}}_a\}-\mathrm{Dis}\{\vec{\boldsymbol{Q}},\vec{\boldsymbol{I}}_b\}) \tag{7}$$

式(5)~式(7)的正确性取决于一个事实，即 $\Gamma\gg 2|\max(\vec{\varepsilon}_i)|,\Gamma\gg 2|\max(\vec{\varepsilon}_q)|$。由于 γ 是一个正整数，若 Comp_{ab} 是一个正数，则 $\vec{\boldsymbol{Q}}$ 与 $\vec{\boldsymbol{I}}_a$ 的欧式距离更小，即 $\vec{\boldsymbol{Q}}$ 与 $\vec{\boldsymbol{I}}_a$ 更相似；否则，$\vec{\boldsymbol{Q}}$ 与 $\vec{\boldsymbol{I}}_b$ 更相似。通过这种方法，CS 可以根据检索请求，对所有图像的相似度进行排序，然后返回前 K 个结果。

3.2 多用户密钥转换协议

为了在多用户图像检索场景下满足用户隐私需求，要保证不同的 DO/SU 无法解析其他 DO/SU 的索引内容/查询内容，因此他们持有的密钥应该不同。与此同时，要保证每一个 SU 能够对 CS 中存储的所有索引进行检索。由于使用对称加密方案，CS 接收到的查询与索引必须使用相同密钥加密才能完成欧式距离比较。为了满足以上需求，设计了一个多用户密钥转换协议。

3.2.1 密钥分配

首先，TA 随机选择一个 $2m\times 2m$ 的可逆矩阵 $\boldsymbol{M}$，则加密密钥 $SK=\{\boldsymbol{M},\ \boldsymbol{M}^{-1}\}$，其中 $\boldsymbol{M}^{-1}$ 为 $\boldsymbol{M}$ 的逆矩阵。对于每一个数据拥有者 DO_i，生成用户密钥 $\boldsymbol{M}_{Oi}$ 以及转换密钥 $\boldsymbol{M}'_{Oi}$，满足 $\boldsymbol{M}=\boldsymbol{M}_{Oi}\boldsymbol{M}'_{Oi}$。同样地，对于每一个检索用户 SU_i，生成用户密钥 $\boldsymbol{M}_{Ui}$ 以及转换密钥 $\boldsymbol{M}'_{Ui}$，满足 $\boldsymbol{M}^{-1}=\boldsymbol{M}'_{Ui}\boldsymbol{M}_{Ui}$。通过安全信道，将 $\boldsymbol{M}_{Oi}$、$\boldsymbol{M}_{Ui}$ 分发给对应的 DO_i、SU_i，将转换密钥 $\boldsymbol{M}'_{Oi}$、$\boldsymbol{M}'_{Ui}$ 分发给密钥转换中心 KCC。

3.2.2 密钥转换协议

密钥转换协议如图 2 所示，在 IndexBuild 算法中，DO 将使用 $\boldsymbol{M}_{Oi}$ 加密的索引发送 KCC，KCC 根据 $\boldsymbol{M}'_{Oi}$ 将加密密钥转换为主密钥 $\boldsymbol{M}$。在 QueryGen 算法中，同样使用类似方法将请求加密密钥转换为 $\boldsymbol{M}$，这样，CS 就可以对所有由主密钥加密的索引进行检索。具体过程如下。

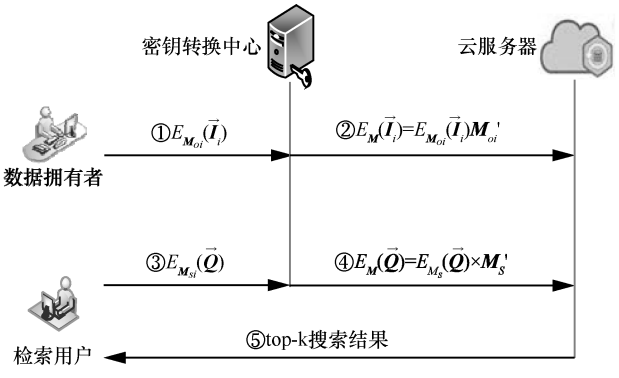

图 2　密钥转换协议

1) 给定特征向量 $\vec{I}_i=\{d_1,d_2,\cdots,d_m\}$，DO 依旧将 $\vec{I}_i$ 扩展为 $2m$ 维。完成扩展之后，DO 将每一个索引 $\vec{I}_i$ 加密为

$$E_{M_{Oi}}(\vec{I}_i)=(\Gamma\vec{I}_i+\vec{\varepsilon}_i)M_{Oi} \tag{8}$$

加密完成后，DO 将 $E_{M_{Oi}}(\vec{I}_i)$ 发送给 KCC。

2) 在收到 $E_{M_{Oi}}(\vec{I}_i)$ 后，KCC 对其进行密钥转换，如式(9)所示。

$$E_M(\vec{I}_i)=E_{M_{Oi}}(\vec{I}_i)M'_{Oi} \tag{9}$$

转换完成后，KCC 把转换后的密文索引发送给 CS。

3) 给定一个查询请求 $\vec{Q}=\{q_1,q_2,\cdots,q_m\}$，SU 首先将其扩展为 $2m$ 维，然后加密为

$$E_{M_{Ui}}(\vec{Q})=M_{Ui}\ (\Gamma\vec{Q}^T+\vec{\varepsilon}_q) \tag{10}$$

加密完成后，SU 把检索请求 $E_{M_{Ui}}(\vec{Q})$ 发送给 KCC。

4) KCC 收到密文检索请求 $E_{M_{Ui}}(\vec{Q})$ 后，对其加密密钥进行转换

$$E_{M^{-1}}(\vec{Q})=M'_{Ui}E_{M_{Ui}}(\vec{I}_i) \tag{11}$$

转换完成后，将 $E_{M^{-1}}(\vec{Q})$ 发送给 CS。

5) 在收到检索请求 $E_{M^{-1}}(\vec{Q})$ 后，CS 根据请求与索引对图像进行排序，然后返回前 K 个结果。

4　方案安全性分析

本节对提出方案的安全性进行分析。首先，定义并证明本文所使用加密方案的安全性；然后，根据第 3 节中提出的隐私需求对本文的图像检索方案进行安全性分析；最后，分析多用户密钥转换协议的安全性。

4.1　安全性定义

本文提出的图像检索系统中使用的加密方案由 Yuan 等[16]基于误差学习（LWE，learning with error）问题[17]提出，安全性已经得到证明。下面简要回顾该方案的安全性证明，以便进行后续的方案安全性分析。

定义 3　LWE 问题：给定一个维数 $m\geqslant 2$，模数 $h\geqslant 2$，和一个 $\mathbb{Z}_h$ 上的概率分布 χ。给定（$\vec{\alpha}_i\in\mathbb{Z}_h^m$，$\beta_i\in\mathbb{Z}_h$）的任意多个抽样

$$\beta_i=\vec{V}\vec{\alpha}_i^{\mathrm{T}}+\varepsilon_i \tag{12}$$

其中，误差 $\varepsilon_i\in\chi$。以不可忽略的概率恢复矢量 $\vec{V}$ 在计算上是不可行的。

推论 1　若 LWE 问题是困难的，则对于一个敌手来说，从本文使用的加密方案加密的 $E_M(\vec{I}_i)$ 或 $E_{M^{-1}}(\vec{Q})$ 中恢复明文在计算上是不可行的。

证明　在本文的加密方案中，每一个索引 $\vec{I}_i$ 的加密方式为

$$E_M(\vec{I}_i)=(\Gamma\vec{I}_i+\vec{\varepsilon}_i)M \tag{13}$$

由于索引 $\vec{I}_i$ 和请求 $\vec{Q}$ 的加密方式类似，因此简便起见，只使用 $\vec{I}_i$ 来进行证明。在 $E_M(\vec{I}_i)$ 中，$\vec{I}_i$ 和都是 $\vec{\varepsilon}_i$ 都是 $2m$ 维的向量，他们与 M 的乘积可以认为是 4 m^2 次 $2m$ 维的向量内积

$$\begin{aligned}&E_M(\vec{I}_i)(1)=\Gamma\vec{I}_i\times M(1)^{\mathrm{T}}+\vec{\varepsilon}_iM(1)^{\mathrm{T}},\\&\vdots\\&E_M(\vec{I}_i)(2m)=\Gamma\vec{I}_iM(2m)^{\mathrm{T}}+\vec{\varepsilon}_iM(2m)^{\mathrm{T}}\end{aligned} \tag{14}$$

其中，$E_M(\vec{I}_i)(j)$ 是 $E_M(\vec{I}_i)$ 的第 j 个元素，$M(j)$ 是 M 的第 j 列，$1\leqslant j\leqslant 2m$。将 $\Gamma M(j)^T$ 定义为 $M(j)'$，$\vec{\varepsilon}_iM(j)^T$ 定义为 ε_i'，得到了（$M(j)'$，$E(\vec{I}_i)(j)$）的 $2m$ 个样本

$$E_M(\vec{I}_i)(j)=\vec{I}_iM(j)'+\varepsilon_i',1\leqslant j\leqslant 2m \tag{15}$$

因此，从密文 $E_M(\vec{I}_i)$ 中恢复 $\vec{I}_i$ 就成为了定义 2 中给出的 LWE 问题。而该问题被认为是计算不可行的。另外，由于方案中的 M 是秘密密钥，敌手不可获得，因此实际上 $M(j)'$ 对于对手来说也是不可得的。这使得从本文的方案中恢复 $\vec{I}_i$ 比 LWE 问题更困难。下面分析本文使用的加密方案 2 种不同威胁模型下的安全性。

1) 已知密文模型。在这个模型下，由于 CS

只能得到加密索引 $E_M(\vec{I}_i)$ 和加密请求 $E_M(\vec{Q})$ 的访问权，根据推论 1，CS 从其中恢复明文是计算不可行的。

2) 已知背景模型。Yao 等[18]对安全 kNN 这类欧式距离保持算法提出了线性分析攻击。该攻击能够成功的前提是 CS 要获得足够多的明–密文对。在已知背景模型下，CS 虽然能获得一些明文图像样本，但他并不知道明–密文对。即使 CS 获得一些图像的明文密文对，本文中使用的特征提取算法参数及 PCA 的降维参数是不公开的，因此 CS 无法从图像中得出对应的特征向量 $\vec{I}_i$，因此无法完成线性分析攻击。

4.2 图像检索方案安全性

下面根据 3.3 节提出的隐私保护需求从三方面对图像检索方案进行分析。

1) 图像安全性：本文提出的方案中，原始图像数据集是使用 AES 进行加密的，故图像的安全性可以得到很好的保证。

2) 索引和请求机密性：在本文方案中，检索索引 $E_M(\vec{I}_i)$ 和查询请求 $E_{M^{-1}}(\vec{Q})$ 都是加密的，该加密方式的安全性已经在上文进行了证明，因此，索引和请求机密性可以得到保证。

3) 查询请求的不可链接性：在本文的方案中，每一个请求 $E_{M^{-1}}(\vec{Q})$ 都设置了不同的随机数 $\gamma,\beta_1,\beta_2,\cdots,\beta_{m-1}\in\mathbb{Z}_p$。这些随机数保证了即使是相同的图像，其生成的请求都是不同的。另外，在加密过程添加的误差向量进一步加大了请求的差异性。

4.3 多用户密钥转换协议安全性

在多用户密钥转换协议中，加密密钥 SK 被分解成用户密钥和转换密钥，分别分配给 DO/SU 和 KCC。在本文方案中，KCC 与系统中的其他实体是不共谋的，所以 DO/SU 和 KCC 都无法获得 SK。这样，在索引生成/查询生成阶段，DO/SU 使用用户密钥对数据进行加密，每个由于用户密钥是相互独立的，即使用户截获了其他人的检索索引 $E_{M_{Oi}}(\vec{I}_i)$/查询请求 $E_{M_{Ui}}(\vec{Q})$，也无法将其解密从而获得原始数据。另外，KCC 只有转换密钥，同样无法解密用户的索引/查询请求。最后，由于 CS 存储的索引和收到的查询请求都是用 SK 加密的，因此 CS 可以对所有图像进行检索，满足功能需求。

5 方案性能分析

本节对提出的多用户图像外包检索方案的性能进行分析。为了对方案性能进行仿真，本文使用 Python 实现了本文提出的方案。为了更好地进行性能比较，同样用 Python 实现了 SEIS[11]作为对比方案。测试环境为 Ubuntu 16.04 LTS 操作系统，3.3 GHz Intel Core(TM)处理器，4 GB RAM。本文使用著名的 INRIA Holidays 数据集[15]进行准确度测试，该数据集同样用于很多其他图像检索工作的仿真[6-7,11,14]。这里设提取的 Fisher 向量的维度为 4 096。

5.1 检索准确度

为了验证方案的检索准确度，选择了文献[18-19]这 2 个明文图像检索方案和 SEIS 作为对比方案。这里采用的准确度测试指标为应用广泛的平均精度（MAP，mean average precision）[19]。

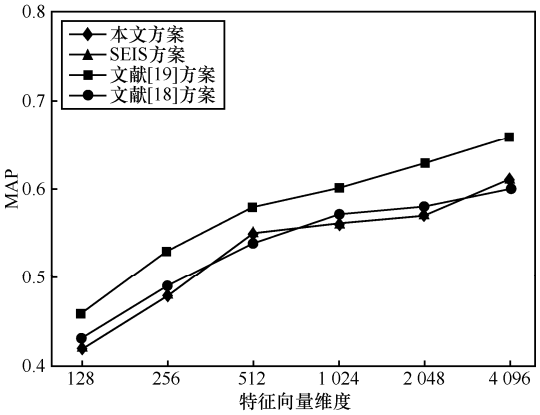

图 3 不同特征维度下检索准确度对比

从图 3 可以看出，本文方案与文献[18-19]这 2 种明文方案的准确度接近。由于本文方案与 SEIS 采用相同的特征向量提取方式，因此准确度相同。可以看到，当特征向量维度小于 512 时，准确度增长明显，特征向量维度大于 512 时，准确度趋于平缓。因此，推荐使用大于 512 的特征向量维度。

5.2 存储和通信开销分析

本文方案的存储开销以及通信开销与已有方案的对比如表 3 所示。

表 3 存储和通信开销对比

方案名称	索引存储开销/bit	通信开销/bit
SEIS	$4mn\|e\|$	$4mn\|e\|$
单用户方案	$2mn\|e\|$	$2mn\|e\|$
多用户方案	$2mn\|e\|$	$4mn\|e\|$

1) 存储开销：定义 $|e|$ 为索引或查询向量中元素的位宽，一般为 64 bit。假设有 n 个图像存储在

云服务器中，每个图像的索引向量 $\vec{I}_i$ 为 m 维。在本文提出的方案中，每个索引向量 $\vec{I}_i$ 会被扩展为 $2m$ 维向量并加密，由于多密钥方案并没有对云端存储的索引做改变，所以单用户和多用户方案的索引存储开销均为 $2mn|e|$。而在 SEIS 方案中，每个索引向量 $\vec{I}_i$ 除了被扩展为 $2m$ 维向量，在加密过程中还被分裂成 2 个，因此存储开销为 $4mn|e|$。

2) 通信开销：在单用户和多用户方案中，检索请求都被加密为 $2m$ 维向量。不同的是，单用户方案的请求直接发送到 CS 进行检索；而多用户方案中的请求需要先发送到 KCC 进行密钥转换，然后再发送给 CS。因此，单用户方案的通信开销为 $2mn|e|$，而多用户方案为 $4mn|e|$。由于 SEIS 方案中每个查询请求被加密为 2 个 $2m$ 维向量，所以 SEIS 方案的通信开销为 $4mn|e|$。

综上所述，本文提出的 2 种方案存储开销均优于 SEIS，只有 SEIS 的一半。单用户方案的通信开销为 SEIS 的一半，多用户方案的通信开销与 SEIS 相同。

5.3　计算开销分析

本节对比本文提出的方案和 SEIS 的各个算法的算法复杂度，然后对它们的运行时间进行仿真。为了方便描述，使用 DOT_{2m} 来定义 2 个 $2m$ 维向量的内积操作，即：给定 2 个向量 $\vec{A}=\{a_1,a_2,\cdots,a_{2m}\}$ 和 $\vec{B}=\{b_1,b_2,\cdots,b_{2m}\}$，它们之间的一个内积操作为 $\vec{A}\vec{B}^{\mathrm{T}}=\sum_{j=1}^{2m}a_jb_j$。由于计算开销与 DOT_{2m} 操作相比十分微小，忽略单个的加法操作和取模操作。为了实现满足多用户检索需求，在单用户方案基础上加入了密钥转换协议，为了更好地比较单用户与多用户方案的计算开销，使用 KeyTrans 算法来指代密钥转换过程。

计算复杂度对比如表 4 所示。在本文的方案中，IndexBuild 过程的算法复杂度为 $2mn\mathrm{DOT}_{2m}$，如式(2)所示，在加密过程中每个索引向量都需要内积一个 $2m\times 2m$ 矩阵，这相当于进行了 $2m\mathrm{DOT}_{2m}$ 操作，那么加密 n 个索引花费 $2mn\mathrm{DOT}_{2m}$ 操作。在 SEIS 中，每个索引向量首先被分裂成 2 个向量，然后 2 个向量分别内积 $2m\times 2m$ 矩阵进行加密，因此加密 n 个索引花费 $4mn\mathrm{DOT}_{2m}$ 操作。如式(4)所示，QueryGen 过程中的加密方式与 IndexBuild 中类似，单用户方案需要 $2m\mathrm{DOT}_{2m}$ 操作来进行查询加密，而 SEIS 需要 $4m\mathrm{DOT}_{2m}$ 操作。值得注意的是，为了实现满足多用户检索需求，多用户方案加入了 KeyTrans 过程。如式(9)和式(11)所示，每转换一个索引（查询）该算法执行 $2m\mathrm{DOT}_{2m}$ 操作，因此多用户方案同样需要 $4m\mathrm{DOT}_{2m}$ 操作。ImSearch 过程中，如式(5)所示，CS 使用查询向量 $E_M(\vec{Q})$ 对每一个索引 $E_M(\vec{I}_i)$ 进行内积操作，在本文方案中，算法复杂度为 $n\mathrm{DOT}_{2m}$ 操作。由于在加密时进行了向量分裂，SEIS 的算法复杂度为 $2n\mathrm{DOT}_{2m}$。

表 4　　计算复杂度对比

算法名称	IndexBuild 算法	QueryGen 算法	KeyTrans 算法	ImSearch 算法
SEIS	$4mn\mathrm{DOT}_{2m}$	$4m\mathrm{DOT}_{2m}$	—	$2n\mathrm{DOT}_{2m}$
本文方案	$2mn\mathrm{DOT}_{2m}$	$2m\mathrm{DOT}_{2m}$	$2m\mathrm{DOT}_{2m}$	$n\mathrm{DOT}_{2m}$

图 4 绘制了特征维数从 128 到 4 096，图像数量为 20 000 时，IndexBuild 算法的运行时间。可以看到，所有方案的运行时间都随着维度的增长而增长。单用户方案运行时间约为 SEIS 的一半，多用户方案运行时间与 SEIS 类似，这与理论分析一致。从图 5 可以看出，当特征向量维度为 512 时，各种方案 IndexBuild 的运行时间随着图像数量的增加线性增长。其中，单用户方案的运行时间约为 SEIS 的一半，多用户方案运行时间与 SEIS 类似。

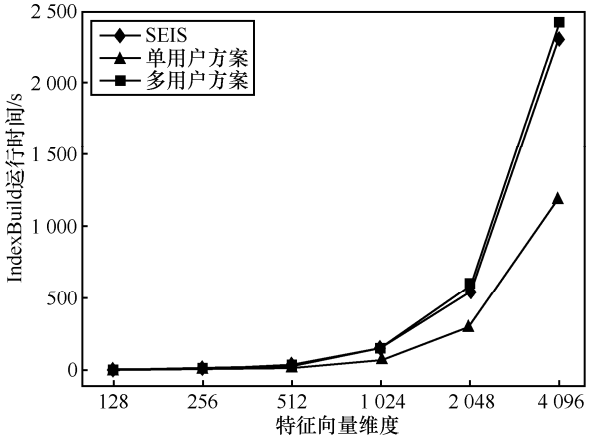

图 4　不同特征维度下 IndexBuild 运行时间

图 6 绘制了特征向量维度从 128 到 4 096 时，QueryGen 算法的运行时间。从图中可以看到，所有方案的运行时间都随着维度的增长而增长。本文的单用户方案运行时间约为 SEIS 的一半，多用户方案运行时间与 SEIS 类似，查询生成时间小于 150 ms，可以满足高效性需求。

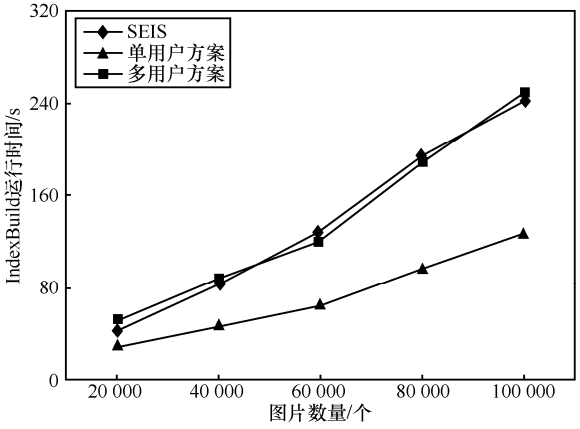

图 5 不同图像数量下 IndexBuild 运行时间

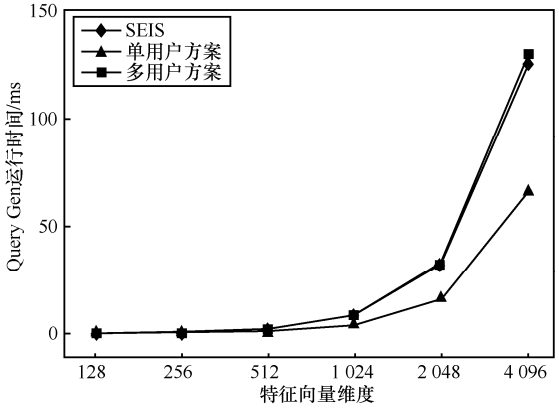

图 6 不同特征维度下 QueryGen 运行时间

从图 7 可以看出，当特征向量维度为 512 时，各种方案 ImSearch 的运行时间随着图像数量的增加线性增长。与 IndexBuild 一样，单用户方案的运行时间约为 SEIS 的一半。因为密钥转换导致的时间消耗，多用户方案运行时间与 SEIS 类似，对 10 万个图像的检索时间不到 200 ms。

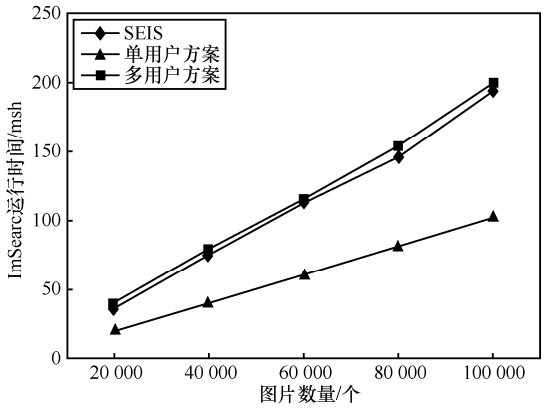

图 7 不同图像数量下 ImSearch 运行时间

图 8 绘制了特征维数从 128 到 4 096，图像数量为 10 000 时，ImSearch 算法的运行时间。可以看到，所有方案的运行时间都随着维度的增长而增长。单用户方案运行时间约为 SEIS 的一半，多用户方案运行时间与 SEIS 类似。

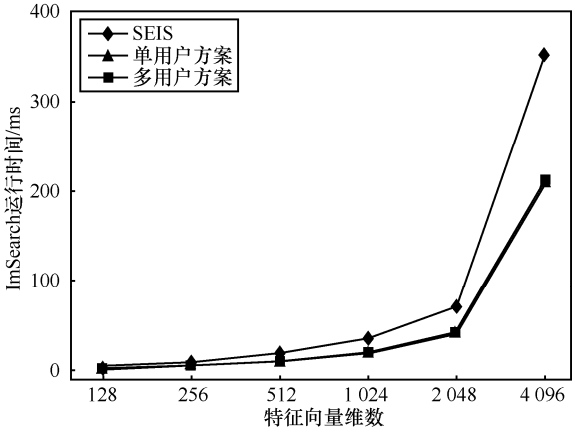

图 8 不同特征维度下 ImSearch 运行时间

6 结束语

为了高效地解决多用户图像检索系统的隐私保护问题，本文首先提出了一种高效隐私保护的单用户图像检索方案。该方案可以达到与明文方案接近的检索准确度，与 SEIS 相比，其存储开销、通信开销和计算开销均降低了一半。另外，为了满足多用户图像检索需求，本文提出了一个多用户密钥转换协议。通过该协议，数据拥有者或检索用户可以使用自己独有的密钥加密检索索引或请求，保证了索引或请求的隐私性。同时，检索用户可以对云服务器上的所有图像进行检索，保证了大规模多源数据的共享。严格的安全性分析表明本文方案可以满足用户隐私保护需求。基于真实数据集上的实验验证了本文方案的高效性，使用本文提出的方案对 10 万张图像进行检索的时间不到 200 ms。因此，本文所提方案在实际的多用户场景中是可行的和高效的。

参考文献：

[1] FISCHER B, BROSIG A, DESERNO T M, et al. Structural scene analysis and content-based image retrieval applied to bone age assessment[C]//Proc Society of Photo-Optical Instrumentation Engineers Conference Series. 2009, 7260:726004-726011.

[2] MISHRA N, SILAKARI S. Image Mining in the Context of Content Based Image Retrieval: A Perspective[J]. International Journal of Computer Science Issues, 2012, 9(4):121-132.

[3] BO C, SHEN G, LIU J, et al. Privacy.tag: privacy concern expressed

and respected[C]// Proc. ACM International Conference on Embedded Networked Sensor Systems (SenSys'14). 2014:163-176.

[4] SHASHANK J, KOWSHIK P, SRINATHAN K, et al. Private Content Based Image Retrieval[C]//IEEE Conference on Computer Vision and Pattern Recognition (CVPR'14). 2014:1-8.

[5] LU W, SWAMINATHAN A, Varna A L, et al. Enabling search over encrypted multimedia databases[C]//Media Forensics and Security I. 2009:725418.

[6] PERRONNIN F, LIU Y, SANCHEZ J, et al. Large-scale image retrieval with compressed Fisher vectors[C]// Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR'10). 2010:3384- 3391.

[7] DOUZE M, RAMISA A, SCHMID C. Combining attributes and Fisher vectors for efficient image retrieval[C]// Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR'11). 2011:745-752.

[8] HSU C Y, LU C S, PEI S C. Secure and robust SIFT[C]// Proc. ACM International Conference on Multimedia (MM'09). 2009:637-640.

[9] ZHANG Y, SUN X, WANG B. Efficient algorithm for k-barrier coverage based on integer linear programming[J]. China Communications, 2016, 13(7): 16-23.

[10] ZHENG P, HUANG J. An efficient image homomorphic encryption scheme with small ciphertext expansion[C]//ACM International Conference on Multimedia. 2013, 24(3):803-812.

[11] XIA Z, 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.

[12] WONG W K, CHEUNG D W, KAO B, et al. Secure kNN computation on encrypted databases[C]//International Conference on Management of Data. 2009:139-152.

[13] YUAN J, YU S, GUO L. SEISA: Secure and efficient encrypted image search with access control[C]//IEEE Conference on Computer Communications. 2015: 2083-2091.

[14] ZHANG L, JUNG T, FENG P, et al. PIC: enable large-scale privacy preserving content-based image search on cloud[C]//International Conference on Parallel Processing. 2015:949-958.

[15] JEGOU H, DOUZE M, SCHMID C. Hamming embedding and weak geometric consistency for large scale image search[C]//Proc European Conference on Computer Vision. 2008:304- 317.

[16] YUAN J, TIAN Y. Practical privacy-preserving mapreduce based k-means clustering over large-scale dataset[J]. IEEE Transactions on Cloud Computing, 2017, PP(99):1-1.

[17] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6):1-40.

[18] XIAO X, LI F, YAO B. Secure nearest neighbor revisited[C]// Proc. IEEE International Conference on Data Engineering. 2013:733-744.

[19] YUE Y, FINLEY T, RADLINSKI F, et al. A support vector method for optimizing average precision[C]//Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR'07). 2007:271-278.

[作者简介]

王祥宇（1994− ），男，内蒙古巴彦淖尔人，西安电子科技大学博士生，主要研究方向为数据安全、云安全、大数据隐私保护。

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。