

隐私保护的图像内容检索技术研究综述

吴颖¹, 李璇^{1,2,3}, 金彪¹, 金榕榕¹

(1. 福建师范大学数学与信息学院, 福建 福州 350100;

2. 福建省网络安全与密码技术重点实验室, 福建 福州 350100;

3. 数字福建大数据安全技术研究所, 福建 福州 350100)

摘要: 随着智能设备与社交媒体的广泛普及, 图片数据的数量急剧增长, 数据拥有者将本地数据外包至云平台, 在云服务器上实现数据的存储、分享和检索。然而, 图像数据含有大量有关用户的敏感信息, 外部攻击者和不完全可信的云服务器都试图获取原始图像的内容, 窥探用户隐私, 造成严重的隐私泄露风险。回顾了近年来隐私保护需求下图像内容检索技术的研究进展, 总结了应用于该技术的图像加密算法, 包括同态加密、随机化加密和比较加密, 围绕这3种密码技术, 详细分析和比较了典型的解决方案, 并介绍了索引构造的改进策略。最后, 总结和展望了未来的研究趋势。

关键词: 隐私保护; 图像内容检索; 可搜索加密; 云计算安全

中图分类号: TP391.41

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019035

Survey on the privacy-preserving content based image retrieval

WU Ying¹, LI Xuan^{1,2,3}, JIN Biao¹, JIN Rongrong¹

1. College of Mathematics and Informatics, Fujian Normal University, Fujian 350100, China

2. Fujian Provincial Key Lab of Network Security & Cryptology, Fujian 350100, China

3. Digital Fujian Big Data Security Technology Institute, Fujian 350100, China

Abstract: With the widespread popularity of smart devices and social media, the number of image data is exponentially increasing. The data owners tend to outsource the local data to the cloud servers, where data is stored, shared and retrieved. However, the content of users' image data contains a lot of sensitive information, which may be exposed to the attackers and the incomplete trusted cloud servers, resulting in a serious risk of privacy leakage to users. The research progress of the content-based image retrieval technology under the privacy-preserving in recent years were reviewed, and the key image cryptographic technology were summarized, including homomorphic encryption,

收稿日期: 2018-12-11; 修回日期: 2019-01-08

通信作者: 李璇, jessiel24@163.com

基金项目: 国家自然科学基金资助项目 (No.61872090, No.61872086); 福建省自然科学基金资助项目 (No.2017J05099)

Foundation Items: The National Natural Science Foundation of China (No.61872090, No.61872086), The Natural Science Foundation of Fujian Province (No.2017J05099)

论文引用格式: 吴颖, 李璇, 金彪, 等. 隐私保护的图像内容检索技术研究综述[J]. 网络与信息安全学报, 2019, 5(4): 14-28.

WU Y, LI X, JIN B, et al. Survey on the privacy-preserving content based image retrieval[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 14-28.

randomized encryption and comparative encryption. Around these techniques, the typical solutions are analyzed and compared in detail, and the improvement strategies of index construction are introduced. Finally, the future research directions are discussed.

Key words: privacy-preserving, content-based image retrieval, symmetric searchable encryption, cloud computing security

1 引言

随着云计算技术的发展和大数据信息时代的到来,越来越多的数据拥有者选择将本地设备上的数据外包给云服务器,以减少本地存储资源和计算资源的消耗^[1]。一些主流的社交网络(如 Facebook 和 Flickr 等运营商)也利用用户上传的数据实现行为广告、用户偏好分析等目的^[2]。由于互联网上存在大量恶意用户,同时“诚实但好奇”的云服务提供商也并不可信,导致外包数据的隐私性和安全性引发了人们的担忧^[3]。近年来,数据隐私成为业内用户和研究者普遍关注的问题,隐私保护计算成为信息安全领域和其他相关领域的热门研究方向,广泛应用于生物信息识别^[4]、医疗诊断^[5]、监控视频匹配^[6]等多个领域。

为了防止隐私泄露,数据加密技术被广泛应用于外包数据的隐私保护计算。用户可以选择在本地端对涉及隐私的数据进行加密后上传云端,然后由云服务器在密文上实现更新、搜索和计算等操作。隐私保护的图像内容检索(PPCBIR, privacy-preserving content based image retrieval)是隐私保护计算的一个重要方向,能够帮助用户实现外包图像的安全检索。随着各大社交网络、云存储应用的流行,每天有数以亿计的数字图像被上传和存储。基于内容的图像检索(CBIR, content based image retrieval)可以帮助人们从互联网海量的图像中迅速找到自己感兴趣的图像。CBIR 把检索的关键放在图像内容自身的特征,对图像进行分析,建立图像特征描述符并存入图像特征库,当用户提供查询图像的特征向量时,云端通过计算特征向量与图像特征库中各个特征的相似度,

按照相似性大小进行排序后输出检索结果^[7]。由于图像数据可能含有大量有关用户的敏感信息(如人脸、家庭环境等),为了避免个人隐私泄露,用户可以在上传敏感图像前对其加密,但加密操作会导致明文领域的 CBIR 技术不再可用。为了解决这个问题,近年来研究者提出了许多 PPCBIR 方案,在不向云服务器透露敏感信息的情况下,支持加密域上的图像内容检索。

2 隐私保护的图像内容检索

2.1 PPCBIR 方案的实体

PPCBIR 方案一般涉及 3 类实体:图像所有者、图像查询者以及云服务器。

图像所有者:提取待上传图像的特征向量,构造安全的可搜索索引,用密钥将图像特征加密成密文,并将密文特征和安全索引外包给云服务器。部分方案中,图像所有者还承担授权查询用户和制定访问策略的任务。

图像查询者:由图像所有者授权可在云服务器检索其上传图像的合法用户。在请求检索图像时,图像查询者提取查询图像的特征,并加密成密文,将密文特征作为查询陷门提交给云服务器。在接收到查询结果后,使用图像所有者共享的密钥对其解密。

云服务器:存储密文图像特征和安全索引,并处理来自图像查询者的检索请求,按照访问策略执行检索任务。面对受保护的大规模多媒体数据时,云服务器应具有对受保护数据进行搜索和计算的能力。

2.2 PPCBIR 方案的关键环节

实现 PPCBIR 方案的关键环节有两点:图像

特征的保护和密文域的相似性度量。

1) 图像特征的保护

该环节需要提取原始图像特征,使用密码算法对特征加密保护,并保证经过加密处理的图像特征描述符可以用于后续的检索操作。图像特征包括全局特征和局部特征。全局特征是从整体上描述一幅图像,包括颜色直方图^[8]、形状特征^[9]和纹理特征^[10-11]等信息。局部图像特征是用带权重的局部特征向量集合表示一幅图像,较为常用的局部图像特征提取算法有尺度不变特征变换^[12](SIFT, scale-invariant feature transform)、局部聚合向量^[13](VLAD, vector of locally aggregated descriptors)、局部二值模式^[14](LBP, local binary patterns)等。提取特征之后,为了提高检索效率,通常使用视觉词袋^[15](BoVW, bag of visual-words)、局部敏感哈希^[16](LSH, locality-sensitive hashing)、主成分分析^[17-18](PCA, principal component analysis)等技术对提取的特征进行降维。

原始图像特征可以在明文上提取,也可以在密文上提取。明文上提取特征的过程较为简单,由用户在本地上独立从原始图像上提取特征。但当提取图像特征的计算量较大时,由于终端用户的资源有限,用户会考虑将此过程中复杂的计算部分外包给云服务器处理,由双方协作完成图像特征的提取。考虑到云端是“诚实但好奇”的,用于计算特征的外包数据需进行保护,以避免泄露图像或特征的内容,因此提出了密文域的特征提取算法^[19-23]。在图像特征提取完成后,用户对特征加密,并将其发送给云服务器,以用于后续基于密文特征的检索。

2) 密文域的相似性度量

相似性度量是 PPCBIR 实现图像检索的重要环节,通过实现密文之间的相似度比较,从而完成密文图像的检索。由于数据加密后往往打乱了原始明文的统计特性,密文域上的相似性度量较为困难,设计时需综合考虑数据加密和特征提取

这两个环节所使用算法的特点,设计出能够在加密域上实现的相似性度量方案,以实现密文之间的相似度计算和排序。常用的距离计算有欧式距离、L1 距离、汉明距离等,为了得到相似性的排名结果,还可以利用最高有效位(MSB most significant bit)、安全 KNN^[24](secure K-nearest neighbor)、安全多方计算(secure multi-party computation, SMC)等算法进行度量。

由于密文距离计算的复杂度较高,如果采用对查询图像和数据库中图像两两之间计算密文距离,会造成极低的检索效率。要提高密文图像的检索效率,还需要设计有效的索引结构和检索优化方案。

当有权限的图像查询用户发送查询请求和查询门限给云服务器后,云端在不知道原始图像特征内容的情况下,在密文上执行检索操作,并将得到的查询结果返回给用户。

PPCBIR 方案的基本步骤如图 1 所示。表 1 列出了典型 PPCBIR 方案的关键环节。

3 PPCBIR 的数据加密技术

数据加密是实现 PPCBIR 的关键技术环节,通过隐藏数据语义内容,实现保护数据隐私的目的^[25]。在隐私保护的图像检索中,为了不向云服务器泄露敏感信息,用户需要在将图像上传至云服务器前加密图像特征。

为了达到 PPCBIR 中图像检索的需求,需要寻求合适的加密方式,使密文能够被处理,且保证密文下的操作结果近似等于明文下的操作结果。在 PPCBIR 的研究中,常用的加密技术包括同态加密(HE, homomorphic encryption)、随机化加密和比较加密。下面具体介绍这 3 种密码算法的原理,并简要说明其在 PPCBIR 中的应用。

3.1 同态加密

同态加密算法允许在密文域上对加密数据进行计算,计算过程不会泄露数据的原始内容^[26]。

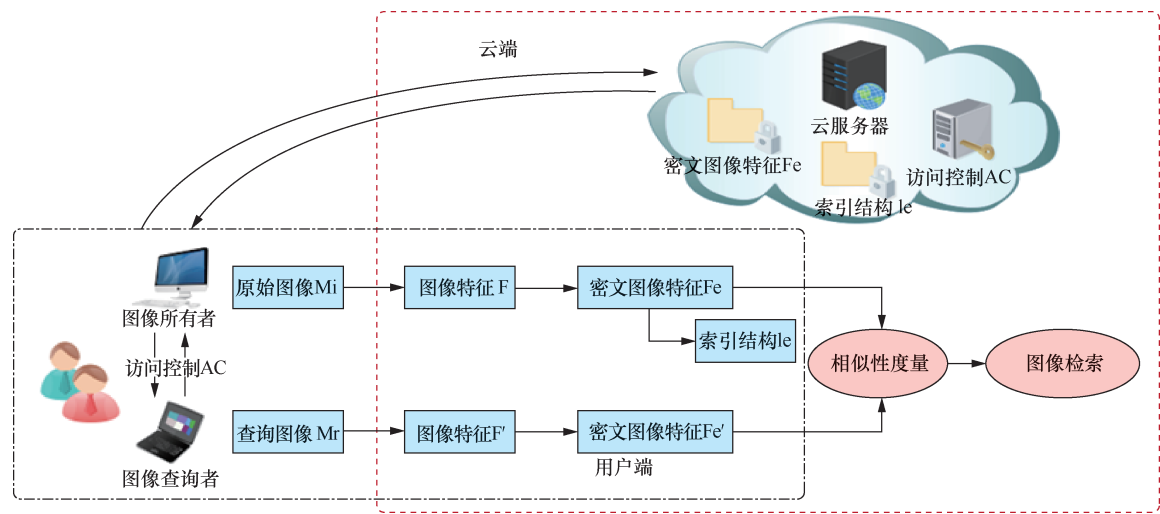


图 1 PPCBIR 技术框架

方案	特征/索引	加密算法	相似性度量算法
Zhang ^[31]	低级特征→局部保留投影	Paillier	欧氏距离→MSB
Bellafqira ^[32,34]	小波子带直方图	Paillier	L1 距离
Lu ^[37]	视觉特征	平面随机化	汉明距离
		随机投影	L1 距离
		随机化一元编码	L1 距离
Shen ^[57]	SIFT 特征	Jung ^[58]	欧氏距离→SMC
Ferreira ^[59]	颜色/纹理	像素行位移	汉明距离
Cheng ^[60,61]	DCT 系数直方图	DCT 系数置乱	曼哈顿距离
Han ^[62]	DCT 系数差分特征→LBP	DCT 系数置乱	曼哈顿距离
Huang ^[63]	VLAD	Wong ^[24]	内积计算
Huang ^[64]	PoV	类混淆	SVM 分类器
Zou ^[50]	SIFT 特征→LSH	比较加密	欧式距离
Zhu ^[65]	LSH	AES	内积计算
Zhu ^[66]	LSH	安全线性规划转换	EMD 距离
Xia ^[67,68]	LSH	Wong ^[24]	内积计算

持有密钥的用户对密文计算结果解密后，可以直接得到明文上的相应计算结果。同态加密分为部分同态加密（SHE，somewhat homomorphic encryption）和全同态加密（FHE，fully homomorphic encryption）。部分同态加密包括加法同态和乘法同态，分别支持密文域上的明文加法计算和明文乘法计算，经典算法有 RSA、ElGamal、Paillier 同态加密等^[27]。全同态加密可以同时支持密文域的加法和乘法计算，从而满足密文域的任何计算需求，但其

复杂度高和资源消耗很大。所以隐私保护计算的研究者目前更多将精力放在 SHE 的应用上，SHE 也被广泛用于隐私保护的图像处理^[28-29]。

Paillier 加密^[29]是隐私保护图像处理中最常用的加法同态加密算法，其加解密过程如下。

密钥生成：随机选择两个大素数 p 和 q ，满足 $\gcd(pq, (p-1)(q-1)) = 1$ ，选择一个随机整数 $g, g \in \mathbb{Z}_N^*$ ，计算

$$N = p \cdot q$$

(1)

$$\lambda = \text{lcm}(p-1, q-1) \quad (2)$$

其中, 公钥 $PK = \{N, g\}$, 私钥 $SK = \{\lambda\}$ 。

加密算法: 对数据进行加密

$$c = E_{PK}(m, r) = g^m \cdot r^N \bmod N^2 \quad (3)$$

m 是明文, c 是密文, r 是用户随机选择的整数。

解密算法:

$$m = D_{SK}(c, \lambda) = \frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N \quad (4)$$

隐私保护的图像内容检索中, 由于涉及密文域上图像相似度的度量计算, 同态加密算法的性质能够为其提供很好的技术支持。使用同态加密算法加密初始图像或图像特征, 再利用其支持密文域加法和数乘的特性, 实现密文域上的有效检索^[30-34]。

3.2 随机化加密

随机化加密的原理是在原始数据中增加随机噪声或者对其进行随机变换, 使数据使用者无法从随机化干扰后的数据中获得原始数据的详细内容。随机化加密效率高, 适用于数据量大、冗余度高的图像数据加密^[35-36]。

近年来, 一些研究者将随机化加密方法应用于 PPCBIR 中^[37-38]。由于随机数加密的安全性源于其对明文统计特性的破坏, 如何在密文域上完成明文图像的相似性度量, 构建有效的 PPCBIR 方案, 是面临的主要挑战。目前, 基于随机化加密的 PPCBIR 方案中, 主要思想是将需要保护的图像或其特征看作多维的向量, 对向量的多个分量分别进行加密处理, 定义合适的向量距离, 使数据加密前后的距离保持不变, 从而通过计算加密后的索引向量与待查询向量之间的距离, 完成密文域上的相似度排序, 实现图像检索。下面简要介绍基于随机矩阵变换的随机化加密算法^[38]。

提取一组特征向量 $\mathbf{f} = (f_1, f_2, \dots, f_l)^T$, 拓展为如下形式。

$$\tilde{\mathbf{f}} = (f_1, \dots, f_l, \|\mathbf{f}\|_2^2)^T \quad (5)$$

其中, $\|\mathbf{f}\|_2^2 = \sum_{i=1}^l f_i^2$ 。随机选择一个 $(l+1) \times (l+1)$ 维的可逆矩阵 $\mathbf{R}$, 对 $\tilde{\mathbf{f}}$ 做矩阵变换。

$$\mathbf{f}' = \mathbf{R}^T \cdot \tilde{\mathbf{f}} \quad (6)$$

$\mathbf{f}'$ 是转换之后的特征向量。这里, $\mathbf{R}$ 作为图像所有者和图像查询者的安全密钥。具体转换过程为

$$\mathbf{f}' = \text{SecureTransfrom}(\mathbf{R}, \mathbf{f}) = \mathbf{R}^T \cdot (f_1, \dots, f_l, \|\mathbf{f}\|_2^2)^T \quad (7)$$

这种安全转换方法可以防止特征向量的信息泄露, 同时支持相似度计算, 被广泛应用于隐私保护下的安全距离度量工作^[39]。

3.3 比较加密

基于请求的比较加密 (request-based comparable encryption) 是一种对称加密算法, 具有如下性质: 当且仅当给定一个与明文相关联的令牌时, 该机制允许将加密后的密文与其他密文进行比较。比较加密是 Furukawa 等^[40-41]基于原有的保序加密 (OPE, order-preserving encryption) 做出的改进算法。

Agrawal 等^[42]提出的 OPE 算法, 特点在于在密文上保留了明文的原有顺序, 对于一些涉及顺序信息的查询操作, 可以直接应用于加密数据, 且加密后不会影响系统查询、更新等功能^[43-46]。对 OPE 的相关研究^[47-48]中发现, OPE 存在的问题: 如果某个范围内的所有数据都被一个 OPE 加密, 那么攻击者很有可能通过获取密文的顺序得到原始的信息。Furukawa 等^[40-41]针对 OPE 存在的这一问题, 提出了一种基于请求的比较加密。它不仅可以实现密文下的数值比较, 也能保证数值的安全。Furukawa 在文献[41]中提出了改进方案, 减少了密文的长度。之后 Chen 等^[49]提出了一种基于滑动窗口的方法, 使比较加密的效率得到提高。下面简要介绍基于请求的比较加密。

比较加密算法由 4 个部分组成: 参数生成、数据加密、令牌生成和数据比较。

1) 参数生成: 给定安全参数 $\kappa \in \mathbb{N}$ 和范围参

数 $n \in \mathbb{N}$ ，输出参数 $param$ 和主密钥 $mkey$ 。其中， n 包括在 $param$ 内。

$$(param, mkey) = Gen(\kappa, n) \quad (8)$$

2) 数据加密：给定参数 $param$ 、主密钥 $mkey$ 和明文 $num(0 \leq num < 2^n)$ ，输出密文 $ciph$ 。

$$ciph = Enc(param, mkey, num) \quad (9)$$

3) 令牌生成：给定参数 $param$ ，主密钥 $mkey$ 和明文 $num(0 \leq num < 2^n)$ ，输出令牌 $token$ 。

$$token = Der(param, mkey, num) \quad (10)$$

4) 数据比较：给定参数 $param$ 、两个待比较密文、 $ciph$ 、 $ciph'$ 和令牌 $token$ ，输出结果为-1、1或0。

$$Cmp(param, ciph, ciph', token) \in \{-1, 1, 0\} \quad (11)$$

定义 1 假设有两组明文数据： $num = \sum_{i=1}^{n-1} b_i 2^i$ ，

记为 $(b_0, \dots, b_{n-1})$ ， $b_i \in \{0, 1\}$ ； $num' = \sum_{i=1}^{n-1} b'_i 2^i$ ，记为

$(b'_0, \dots, b'_{n-1})$ ， $b'_i \in \{0, 1\}$ 。如果对于所有的 $\kappa \in \mathbb{N}$ ， $n \in \mathbb{N}$ ， $0 \leq num, num' < 2^n$ ，有 $param, mkey, token, ciph$ 和 $ciph'$ 满足

$$\begin{aligned} (param, mkey) &= Gen(\kappa, n) \\ token &= Der(param, mkey, num) \\ ciph &= Enc(param, mkey, num) \\ ciph' &= Enc(param, mkey, num') \end{aligned} \quad (12)$$

$$Cmp(param, ciph, ciph', token) = \begin{cases} -1, & num < num' \\ 1, & num > num' \\ 0, & num = num' \end{cases} \quad (13)$$

则认为比较加密满足完整性。

Zou 等^[50]把比较加密用于图像特征的加密和比较中，主要思想是使用比较加密算法对原始图像及由特征向量生成的索引进行加密处理，原始图像特征得到保护，通过得出密文域上的顺序信息以实现密文比较，比 Lu 等^[51]基于 OPE 的方案具有更高的安全性。

4 基于同态加密的 HE-PPCBIR 方案

在 PPCBIR 领域中，许多研究者利用同态加密的特性设计了密文图像上的检索方案。本节介绍基于同态加密的 PPCBIR (HE-PPCBIR) 研究成果。

4.1 基于同态加密的特征提取

特征提取是 PPCBIR 的第一步，在实际操作过程中，往往面对多维度的图像数据库，当图像特征的提取过程较为复杂时，由于用户能够利用的本地计算资源有限，庞大的计算任务给终端用户带来沉重的负担。许多研究者把图像特征提取的任务外包给云服务器，要求云服务器在不知道图像数据原始内容的情况下，也能进行特征提取的计算。

尺度不变特征变换 (SIFT, scale-invariant feature transform)^[12]是一种用于检测和描述图像局部特征的常用算法，其特征具有尺度旋转不变性，在计算机视觉和模式识别领域被广泛应用。Hsu 等^[19]讨论了安全 SIFT 外包问题，首次利用同态加密的 Paillier 算法研究了加密域中隐私保护的 SIFT，方案允许只对部分涉及隐私的区域进行加密。然而，Hsu 的解决方案在计算上难以处理，在加密数据比较中引入了非常大的计算复杂度，每个比较都需要遍历任意两个阈值之间一半的纯文本空间；另外，从隐私的角度来看，如果通过选择较小的明文域来降低比较协议的复杂性，则会破坏安全性，是不安全的。针对 Hsu 等提供的思路，一些研究者在处理安全 SIFT 外包问题上做出了许多拓展。Wang 等^[20]考虑了基于形状特征提取的安全性和隐私保护的 SIFT 外包计算问题，分别采用同态加密和 Yao 混淆电路协议^[52]提出了两种不同安全级别的方法；Li 等^[21]分析了系统抵抗恶意攻击的能力，因为高级的恶意攻击会在尺度空间中破坏图像特征，发现使用凸松弛方法可以有效地去除 SIFT 的关键点，同时为了隐藏去除 SIFT 关键点的痕迹，将大量的伪 SIFT 关键点注入之前经过处

理的图像中, 使失真最小化。

以往的解决方案都存在一个共同的局限性: 为了对密文进行操作, 不小心破坏了原 SIFT 特征的顽健性和特殊性; 无法进行很好的图像相似度匹配; 缺乏对原始图像特征提取算法关键特征的保存进行全面的分析和评价。

Wang 等^[22]提出了分布式的隐私保护 SIFT 计算外包协议。该协议将图像随机分割成两个部分, 分别分配给两个独立的半诚实的云服务器, 利用同态加密和 Yao 混淆电路^[52], 进行安全关键点的比较, 实现 SIFT 特征的安全外包计算。Yao 混淆电路是一种两方安全计算的方案, 可以实现任意函数的安全计算^[53-54]。在计算 SIFT 特征的过程中, 把双方的隐私计算输出记为 V_1 和 V_2 , 通过使用 Huang 等提出的方法^[55], 对各个关键部分的计算结果都做了一次比较函数 $f(V_1, V_2)$ 的计算, 双方可以推导出各自的输入和输出结果, 但无法获得对方任何的输入信息。该方案能比较完整地保留 SIFT 的关键特性, 但仍有进一步降低 SIFT 计算和通信成本的空间, 尤其是它不能消除边缘响应, 导致检测到的关键点对小噪声不稳定。Hu 等^[23]在研究中对 Wang 等^[22]的方案做了更具体的优化, 先对原始图像做随机分割, 再把特征提取计算分别分布到两个独立的基于批处理安全乘法协议 (BSMP) 和基于批处理安全比较协议 (BSCP) 的云服务器上, 并利用同态加密技术协作生成密文域的 SIFT 描述符。数据查询者可以从两个服务器生成的加密 SIFT 描述符中恢复真实的特征描述符, 但无法获取原始图像的任何信息。

4.2 基于同态加密的安全图像检索

本节介绍基于同态加密的 HE-PPCBIR 方案, 从特征信息和算法两个层面对各方案进行综述, 并比较分析其特点。

Lu 等^[30]在研究综述中总结了 HE-PPCBIR 的相关工作, 给出了一种基于加性同态加密的

PPCBIR 方案。图像拥有者使用加法同态加密算法对图像特征进行保护后, 上传至云服务器的加密图像特征库 f 。图像查询者在检索图像时, 可以根据不同的安全需求, 选择将查询图像特征 q 以密文或者明文形式上传给云服务器: 以密文形式查询时, 查询用户需要参与图像特征相似度的安全计算过程; 以明文形式查询时, 用户无须参与, 最后在结果中加入噪声, 以提高安全性。方案虽然可行, 但牺牲了搜索精度, 且大大增加了用户的计算和存储开销, 不适合于实际应用。同时, 该文介绍了采用完全同态加密方法, 服务器可以直接在密文上计算查询图像特征和图像库中加密特征之间的相似度距离, 无须用户直接参与。但该方法的计算量很大, 在距离排序时, 为了避免距离大小信息的泄露, 也需要用户的参与进行解密和排序。

Zhang 等^[31]的方案着重研究了图像检索的安全性能, 首先提取低级的图像特征向量, 再利用局部保留投影 (LPP, locality preserving projections) 将特征向量降维得到一个 49 维的特征向量, 之后进行特征向量加密、密文下的相似度距离排名等操作。其中采用 Paillier 加密算法加密特征向量, 欧式距离作为计算距离的方法。为了避免距离计算结果泄露, 使用最高有效位 (MSB, most significant bit) 度量距离计算结果, 记 $b_{ij} = 2^i + d_i - d_j$ 最高有效位 $b_{ijMSB} = 2^{-i}[b_{ij} - (b_{ij} \bmod 2^i)]$, 之后计算加密后的 b_{ijMSB} 。

$$[b_{ijMSB}] = [2^{-i}[b_{ij} - (b_{ij} \bmod 2^i)]] = ([b_{ij}][b_{ij} \bmod 2^i]^{-1})^{2^{-i}} \quad (14)$$

其中, $[b_{ij}] = [2^i + d_i - d_j] = [2^i][d_i][d_j]^{-1}$ 。

这里, 服务器需要通过与用户进行两次交互计算 $[b_{ij} \bmod 2^i]$ 的值。

$$\begin{aligned} [b_{ij} \bmod 2^i] &= [(d_i \bmod 2^i - r_i \bmod 2^i) \bmod 2^i] \\ &= ([d_i \bmod 2^i][r_i \bmod 2^i]^{-1}) \bmod 2^i \quad (15) \end{aligned}$$

最后, 用户解密 $[Z] = [b_{ijMSB} + h] = [b_{ijMSB}][h]$ (h 为 k bit 的随机数), 服务器根据 b_{ijMSB} 的值,

检索到 K 幅最相似的图像返回给用户。该方案保证了图像检索过程的安全性, 但忽略了整体计算开销和通信开销的问题。

Lu^[30]和 Zhang^[31]都使用了同态加密技术加密特征向量, 直接在密文域上计算特征之间的相似度距离, 在检索过程能够达到较高的安全性, 但二者都需要用户与服务器的频繁交互, 且同态加密计算复杂, 不可避免地造成了繁重的计算和通信开销。Bellafqira 等^[32]在避免客户和服务器之间交互的方向上减小通信开销, 他们在工作中使用了 Paillier 加密图像, 并在加密域上提取基于小波变换的全局图像特征, 安全 CBIR 的计算^[33]都由云服务器执行, 避免了客户和服务器之间的额外通信, 但检索效率和精度不高。之后 Bellafqira 等^[34]对该工作进行了扩展, 提出了计算加密离散小波变换 (SDWT, secure image discrete wavelet transform) 的方法, 利用两个云服务器进行共享加密的直方图计算, 与文献[32]方案相较, 安全性和检索精度上都有提升, 但同态加密和特征提取过程产生的计算问题仍没有得到解决。

Zhang 等^[56]的多层级同态加密方案 (PIC) 考虑了多用户场景下 PPCBIR 中密钥的分发和管理。方案中引入了密钥代理 (KA), 首先由一个完全可信的密钥发布中心 (TP) 随机选择密钥, 拆分密钥后分配给用户, 加密时, 从用户到 KA 再到云服务器进行分级加密, 在每一级加密过程中, 利用该级对应的密钥更新获得的密文。为加快搜索进程, 方案中还设计了 MapReduce 框架, 通过将搜索过程设计为一级搜索和二级搜索, 通过任意数量的 mappers 和一个 reducer 可以完成在簇中找到 KNN 的搜索。特征向量和查询向量的密文分配给 mappers 进行同态操作和密钥修改以生成距离密文。然后, 这些内容被发送到 KA 方的 reducer 进行解密并对距离排名。该方案较好地保护了密钥的安全, 避免了用户和云服务器之间

的直接交互, 但一定程度上产生了额外的计算开销。Shen 等^[57]针对现有的大多数 PPCBIR 方案只针对一个图像拥有者的局限性, 设计了一种可支持多个图像共享用户的安全检索模型。在特征的加密环节采用 Jung 等^[58]提供的计算协议, 可以在半诚实的模型下有效保护数据隐私。

由于同态加密算法本身具有较高的计算复杂度, 现有的大部分基于同态的图像安全检索方案虽然可以满足更高级别的安全需求, 但繁重的计算通信开销问题依然是今后相关研究中所面临的关键问题。

5 基于随机化加密的 RE-PPCBIR 方案

随机化加密是通过对原始数据加入随机扰动或者进行随机变换, 以隐蔽数据的原始信息, 但并非完全抹去数据内容, 数据使用者依然可以使用处理后的数据进行后续的操作。在基于随机化加密的 PPCBIR 方案 (RE-PPCBIR) 中, 利用随机化加密的性质对图像特征进行保护, 并在加密过程中保留计算特征相似度时需要的信息。本节介绍近年来 RE-PPCBIR 的研究成果。

在设计 RE-PPCBIR 方案时, 不同的图像视觉特征可以采取不同的随机化方法, 以达到更好的特征保护效果。图像的视觉特征包括全局特征和局部特征。全局图像特征是从整体上描述一幅图像, 提取全局特征的过程是基于区域或整个图像执行的, 利用颜色、形状、纹理和空间布局等信息获取图像描述符, 通过全局描述符的比较进行图像检索。局部图像特征是用带权重的局部特征向量集合表示一幅图像, 较为常用的局部图像特征提取算法有 SIFT^[12]、VLAD^[13]、LBP^[14]等。基于全局特征的图像检索操作方便, 计算开销较小, 但检索精度不高。基于局部特征的图像检索在计算上较为复杂, 但往往具有更好的顽健性及更高的检索精度。

本节从随机化加密图像特征的角度, 分别对 Lu

等提出的 3 种特征保护方案^[37]、IES-CBIR 方案^[59]、DCT 系数随机置乱方案^[60-62]以及基于安全 KNN 算法^[24]的 RE-PPCBIR 方案^[63-66]的加密过程进行综述。

Lu 等^[37]提出的 PPCBIR 方案利用随机数加密技术,引入了 3 种距离保持机制对图像视觉特征进行加密,目的是保持图像特征加密前后的近相似性,这 3 种机制分别为:位平面随机化、随机投影和随机化一元编码。

1) 位平面随机化

位平面随机化先将特征向量的所有分量值二进制化,再对同一层位平面采用流密码与伪随机序列异或,最后计算相对应的密文位平面之间的汉明距离,来衡量图像特征的相似性。

2) 随机投影

随机投影通过对数据做矩阵变换来隐藏原始数据的信息。设 $\mathbf{f}$ 和 $\mathbf{g}$ 均是 n 维的特征向量,选取一个 $m \times n$ 的高斯随机矩阵 $\mathbf{R}$ 作为密钥,对 $\mathbf{f}$ 进行随机化加密,即

$$E(\mathbf{f}) = \mathbf{R} \cdot \mathbf{f} = [r_1 \cdot \mathbf{f}, \dots, r_m \cdot \mathbf{f}] \in \mathbb{R}^m \quad (16)$$

然后计算密文特征向量 $E(\mathbf{f})$ 与 $E(\mathbf{g})$ 之间的欧氏距离,即

$$\begin{aligned} d(E(\mathbf{f}), E(\mathbf{g})) &= \sum_{i=1}^m |r_i \cdot \mathbf{f} - r_i \cdot \mathbf{g}| \\ &= \sum_{i=1}^m \|r_i\|_2 \cdot \|\mathbf{f} - \mathbf{g}\|_2 \cdot |\cos(\theta_i)| \\ &= \|\mathbf{f} - \mathbf{g}\|_2 \cdot \sum_{i=1}^m \|r_i\|_2 \cdot |\cos(\theta_i)| \\ &\approx c \cdot \|\mathbf{f} - \mathbf{g}\|_2 \end{aligned} \quad (17)$$

3) 随机化一元编码

随机化一元编码的基本思想是使用流密码异或加密和置乱加密技术隐藏原始特征向量的信息,再将加密后的向量随机投影到低维空间。由于加密过程使用相同的密钥,加密前后的汉明距离保持不变,通过计算低维空间上向量之间的汉明距离,可以实现加密域上的图像检索。

Lu 等^[37]提出的 3 种方法操作简单,适用于密

文域图像检索工作中对大部分特征向量的保护和相似性的计算。方案存在一些缺陷:①其安全性仅针对视觉特征,未能描述在半诚实的云环境下的抗攻击能力;②面对海量且高维的图像库图像,其产生的巨额计算和通信成本不容忽视,检索效率低。Ferreira 等^[59]针对颜色信息和纹理信息设计了一种可以支持 CBIR 的特征保护方案 IES-CBIR。在 IES-CBIR 检索方案中,用户对颜色信息进行确定性加密,同时对纹理信息进行概率加密,加密颜色特征以提高安全性,加密纹理特征以实现图像的安全检索,这样分开加密可以避免用户的直接干预,使密文图像检索的整个过程在云服务器上执行。

IES-CBIR 的检索过程为:首先,服务器对每个加密图像和 HSV (hue saturation value) 颜色通道构建一个表示图像的颜色直方图(每个图像产生 3 个直方图);然后,服务器从授权用户接收查询请求的陷门,提取其特征向量,通过直方图交集比较数据库中 k 个最相似的图像;最后,查询用户接收到来自服务器的排序结果,使用图像所有者授权的解密密钥恢复出原始图像信息。

Lu^[37]和 Ferreira^[59]等的 RE-PPCBIR 方案存在同样的问题:①原始图像的加密独立于特征的提取和加密,很容易给用户带来额外的计算成本,不适用于海量的高维图像数据库;②加密算法都是针对图像像素的置乱或位移等操作,不能保证 JPEG 文件大小的保存和格式的兼容性。

为了克服这些局限性,近年来,有一些研究者针对 JPEG 图像,利用加密前后 DCT 系数直方图的不变性,提出了基于随机化加密的 JPEG 加密图像检索方案。Cheng 等^[60]采取 DCT 系数随机置乱^[61]的方法加密 JPEG 图像,由于 DCT 系数包含了图像的特征信息,在加密域上保留其分布特性,可以实现相似图像的安全检索。下面简要描述 DCT 系数随机置乱的过程。

已知一幅彩色的 JPEG 图像可以由 Y、U 和 V 这 3 个色彩空间构成，设每个空间中任一 8×8 像素块的 DCT 系数为 $C_{i,j}(m,n)$ ，其中， m 和 n 是每一像素块中 DCT 系数的位置坐标。对于给定的 m 和 n ，图像所有者根据密钥决定置乱的方式，在频率相同的位置上移动 DCT 系数，加密结果可以保持 JPEG 格式的兼容性。转换公式如下。

$$F_{ij} = \frac{C_i C_j}{4} \sum_{m=0}^7 \sum_{n=0}^7 f_{mn} \cos\left(\frac{(2m+1)i\pi}{16}\right) \cos\left(\frac{(2n+1)j\pi}{16}\right) \quad (18)$$

当 $i, j = 0$ 时， $C_i, C_j = \frac{1}{\sqrt{2}}$ ，否则 $C_i, C_j = 1$ 。

在图像检索阶段，服务提供者利用 DCT 系数直方图不变性，计算出每个分量各个频率位置上的 DCT 系数直方图，再对 3 个分量加权距离排名得到搜索结果。该方案不需要特征的提取和加密，一定程度上减少了服务器的计算负担。方案的缺陷在于：加密后的图像文件大小增加，另外增加了服务器的存储和通信成本，此外，明文图像的信息是部分可见的，在安全性方面存在威胁。韩威等^[62]的方案中也研究了基于 DCT 系数的 JPEG 加密图像检索。与 Cheng^[60]的方案不同的是，韩威的方案需要云服务器在图像密文上提取 DCT 系数差分特征以及 LBP (local binary patterns) 特征，比较特征距离确定图像的相似度，不过由于 DCT 变换消除了图像的冗余信息，提取特征的过程较为简单，减少了用户与云服务器的交互，但是泄露部分明文信息，安全威胁仍然存在。

基于安全 KNN^[24]的检索方法也是目前图像安全检索常用方法，使用数据随机化将图像特征加密后，可以支持在密文特征上计算特征之间相似度的 KNN 排名。在构建 PPCBIR 结构时采用安全 KNN 算法，可以很好地达到特征保护和相似度度量的目的。安全 KNN 算法的原理是使用随机矩阵对特征向量进行乘法变换，并通过计算加密域上索引向量与查询向量间的“内积相似

度”，完成原始数据的相似度比较，实现安全 KNN 算法。下面简单介绍安全 KNN 算法的过程。

算法 1 有 2 个 l 维的特征向量 p 和 q ， S 是一个长度为 $l+1$ 的位向量， M_1 和 M_2 表示 $(l+1) \times (l+1)$ 的可逆矩阵。

加密特征向量的过程如下。

1) 给 p 增加一个 $-0.5\|p\|^2$ 的分量，扩展成 $l+1$ 维，根据 S 向量中对应分量值的情况，把 p 分割成两个随机向量 $\{p', p''\}$ 。通过矩阵乘法分别把 p' 、 p'' 变换成向量 $M_1^T p'$ 和 $M_2^T p''$ ，作为加密后的密文数据。这里的密钥为 $\{S, M_1, M_2\}$ 。

2) 给 q 增加一个值为 1 的分量，扩展成 $l+1$ 维。随机生成一个正整数 r ，给 q 加扰动，根据 S 向量中对应分量值的情况，把 q 分割成两个随机向量 $\{q', q''\}$ 。与第 1) 步的加密过程相反，将 q' 和 q'' 通过乘法矩阵变换成向量 $M_1^{-T} q'$ 和 $M_2^{-T} q''$ 作为密文。这里的密钥为 $\{S, M_1^{-1}, M_2^{-1}\}$ 。

计算密文相似度的过程为

$$\{M_1^T p', M_2^T p''\} \cdot \{M_1^{-T} q', M_2^{-T} q''\} = p' \cdot q' + p'' \cdot q'' = -0.5r(\|p\|^2 - 2p \cdot q) \quad (19)$$

未加密时 p 和 q 的相似度距离为 $\|p_i\|^2 - 2p_i \cdot q + \|q\|^2$ 。由于 $\|q\|^2$ 和 $-0.5r$ 是已知的常数，密文特征向量间内积的比较等同于明文特征向量 p 和 q 间欧式距离的比较，从而实现了密文域上的特征向量相似度比较。

Huang 等^[63]使用 VLAD 作为图像描述符^[13]，采用基于投影的双线性二进制码 (BPBC, bilinear projection-based binary codes) 将 VLAD 转化为低维的二进制码，结合了安全 KNN 方案计算查询特征向量与图像库中图像特征的相似性。Huang 等^[64]也采用 PCA^[17-18]降低特征维度，计算出 PoV 的值表示特征向量，以此掩盖特征数据的真实信息。在查询完成后设计了关联反馈的机制，通过查询用户与云服务器的交互，在云服务器中训练 SVM 分类器，以达到更高的检索性能。为了防止

不可信云服务器在反馈机制中学习到用户的查询意图, 查询用户需要在上传之前引入混淆类别, 虽然一定程度上可以干扰云服务器的判断, 但用户在选择混淆类的过程中已经不可避免地向云服务器透露了一些敏感信息, 因此该方案关联反馈机制的安全性还有待进一步优化。

6 基于比较加密的 CE-PPCBIR 方案

比较加密是一种对称加密算法, 允许密文之间进行大小的比较, 可用于构建 PPCBIR 方案, 实现密文域的相似度量。与同态加密相比, 比较加密的计算和检索开销较小。本节对基于比较加密的 PPCBIR 方案 (CE-PPCBIR) 进行介绍。

Lu 等^[51]提出了基于 OPE 的 PPCBIR 方案。方案采用词袋模型构建索引, 使用视觉词汇表示特征, 训练视觉单词表, 再使用分层聚类的方法生成词汇树, 构建出倒排索引。图像所有者提取一幅图像的特征向量后, 对其做 OPE 加密, 将加密的倒排索引和密文图像发送给云服务器。云服务器接收到来自图像查询者的查询请求后, 通过计算两组视觉词汇之间的 Jaccard 距离评价图像的相似度。由于 OPE 会泄露词频之间的大小关系, 敌手很容易通过密文的大小关系推断出明文数值的所在范围, 因此在实际应用中的安全性不高。

Zou 等^[50]使用比较加密设计了 PPCBIR 方案。该方案使用 LSH 构建图像的树索引结构, 索引结构通过比较加密保护, 利用比较加密的性质实现密文域的相似度量计算。下面详细介绍 Zou 等^[50]的 CE-PPCBIR 方案, 以说明比较加密在安全图像检索中的应用。

图像所有者先提取图像 SIFT 特征, 通过 LSH 降维, 得到散列后的特征向量 $\vec{h}_i (1 \leq i \leq n)$, 特征维数为 m 。计算模值 $|\vec{h}_i|$, 根据模值大小进行排序, 以中间值作为根节点, 构建树形索引结构。采用比较加密算法, 使用主密钥 $mkey$ 对索引结构

加密得到 $Ciphtree$, 同时用密钥 SK 加密图像, 将密文图像及其安全索引上传给云服务器。云服务器返回对应的 ID 给图像所有者。

使用比较加密算法对基于 LSH 构建的树状索引加密时, 分为生成令牌 (Gentoken) 和生成密文 (GenCiph) 两个步骤进行。

1) $Gentoken(\vec{h}_i, mkey)$: 假设散列后的特征向量为 $\vec{h}_i = (v_{i1}, v_{i2}, \dots, v_{im})$, 将 v_{ij} 的值当成二进制的比特串, 即 $v_{ij} = (b_0, b_1, \dots, b_{u-1}) := \sum_{0 \leq w \leq u-1} (2^w b_w)$, 令 $b_u = 0$ 。

随机选择 3 个散列函数 $Hash_1, Hash_2, Hash$: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^k$, 执行

$$\begin{aligned} d_w &= Hash_1(mkey, b_u, b_{u-1}, \dots, b_w) \\ token_{ij} &= (d_{ij1}, d_{ij2}, \dots, d_{iju}) \end{aligned} \quad (20)$$

最后, 输出特征向量 $\vec{h}_i$ 的令牌。

$$token_i = (token_{i1}, token_{i2}, \dots, token_{im}) \quad (21)$$

其中, $w = u, u-1, \dots, 1; 1 \leq i \leq n, 1 \leq j \leq m$ 。

2) $GenCiph(param, v_{ij}, token_i, r)$: 输入随机数 r , 令牌 $token_i$ 和特征向量的比特串 $v_{ij} = (b_0, b_1, \dots, b_{u-1})$, 然后对 $\vec{h}_i$ 的每个分量 v_{ij} 进行加密操作, 算法如下。

$$f_w = Hash_3(d_{w+1}, r) + Hash_2(mkey, d_{w+1}) + b_w \quad (22)$$

第 i 个特征向量的第 j 维加密为

$$Cf_{ij} = (f_{ij0}, f_{ij1}, \dots, f_{ij(u-1)}) \quad (23)$$

加密后的特征向量为

$$Ch_i = (r, (Cf_{i1}, Cf_{i2}, \dots, Cf_{im}), |\vec{h}_i|) \quad (24)$$

输出密文特征 Ch_i 。

检索时, 图像查询者将加密处理后的查询特征 Ch' 发送给云服务器, 云服务器使用比较加密算法, 计算

$$C_{ij} := b_{ij} - b'_j \quad (25)$$

其中, b_{ij} 为 Ch_i 上第 i 个向量的第 j 维, b'_j 为 Ch' 上第 j 维向量。 Ch_i 与 Ch' 之间的欧式距离计算如下

$$\begin{aligned} ed_i^2 &= (b_{i1} - b'_1)^2 + (b_{i2} - b'_2)^2 + \dots + (b_{im} - b'_m)^2 \\ &= \sum_{j=1}^m (C_{ij})^2 = \sum_{j=1}^m (v_{ij} - v'_j)^2 \end{aligned} \quad (26)$$

云服务器比较 ed_i^2 与阈值 num ，如果 $ed_i^2 < num$ ，返回 Ch_i ，找到对应的密文图像和密文特征向量集合 C_k ，将 C_k 发送给图像所有者。图像所有者收到 C_k 后使用密钥 SK 对其解密，与查询用户达成协议后，将解密的结果发送给查询用户。

该方案比基于 OPE 的 PPCBIR 安全性更高，一方面，敌手通过密文向量的模值推断出每一维向量值的概率可以忽略不计；另一方面，云服务器不知道标签 $token$ 的值，避免了“诚实且好奇”的云端自行比较图像库的图像，导致对用户隐私造成威胁。方案的局限性在于需要图像所有者、查询用户和云服务器的频繁交互，其应用场景受到限制。

7 PPCBIR 的索引结构优化

为了提高 PPCBIR 方案的检索效率，研究者开始关注 PPCBIR 索引结构的优化问题。

一些研究人员提出了基于局部敏感哈希 LSH^[16] 的 PPCBIR 方案。LSH 算法是一种针对海量高维数据的快速最近邻查找算法，基本思想是：原始数据空间中的两个相邻的数据点通过相同的 LSH 函数进行映射或投影变换后，在新的空间中仍保持相邻（即被映射到同一个桶内）的概率很大，同时，不相邻的数据点被映射到同一个桶的概率很小。研究者利用 LSH 的特性，将经过随机化处理后的特征映射到低维的空间，使在低维空间的特征也能保持原有的相似程度。利用散列后的特征向量构建的安全索引，可以使存储资源得到有效利用，同时，由于将原本高维空间的数据比较转化为低维空间的数据比较，大大提高了检索效率。

Zhu 等^[65] 采用散列函数簇 $g = (h_1, \dots, h_\lambda)$ 把图像的一个多维特征向量映射成 λ 维的向量 $g(f_i) = [h_1(f_i), h_2(f_i), \dots, h_\lambda(f_i)]$ ，同时生成随机矩阵 R ，通过随机化变换对特征向量进行加密

保护。

$$f'_i = R^T \cdot (f_{i1}, \dots, f_{i\lambda}, \|f_i\|_2^2)^T \quad (27)$$

所有特征 $\{f_i\}_{i=1}^n$ 采用聚类方法聚成 n 个散列桶 $\{BKT_j\}_{j \in [1, n]}$ 。为了隐藏散列桶的散列值，使用密钥 k 对其执行 AES 加密，得到 $E(k, BKT_j)$ 。同时，以散列桶为关键词，构建出安全索引。图像所有者把密文图像和安全索引上传至云服务器保存。

被授权的查询用户需要把查询图像的明文发送给图像所有者，由图像所有者提取特征 f_q 并加密为 f'_q 后，与查询特征对应的加密散列值 $E(k, g(f_q))$ 返回给查询用户。

$$E(k, g(f_q)) = E(k, [h_1(f_q), h_2(f_q), \dots, h_\lambda(f_q)]) \quad (28)$$

查询用户请求检索服务时，需要发送 f'_q 和 $E(k, g(f_q))$ 给云服务器，云服务器通过安全索引表搜索到其所在散列桶内所有相似图像 ID，以及相应的密文特征，通过内积计算出图像库的待检索图像与查询图像之间的相似度距离。

$$f_q^T \cdot f'_i = (rR^{-1} \cdot (-2f_{q1}, \dots, -2f_{q\lambda}, 1)^T)^T \cdot R^T \cdot (f_{i1}, \dots, f_{i\lambda}, \|f_i\|_2^2)^T = r(\|f_q - f_i\|_2^2 - \|f_q\|_2^2) \quad (29)$$

在安全索引的构建中，为了提高相似图像的碰撞概率，还建立了多张散列表，对于一个查询请求，从所有的散列表中找到对应的散列桶，然后逐一比较查询图像与散列桶中图像集图像间的相似度。

Zhu 等^[66] 设计了两个阶段的 PPCBIR 结构框架，支持全局特征和局部特征的搜索：第一阶段利用 LSH 对图像数据库进行预过滤，缩小搜索范围；第二阶段设计了安全线性规划转换（SLP, secure linear programming），可以实现密文下的 EMD 距离度量，方案的局限性在于局部特征的维度较大，在得到相对精确的搜索结果的同时，牺牲了大量的时间成本。Xia 等^[67] 基于上述 LSH 安全索引构造方式，设计了 Two-Layer-Index 双层索引结构，索引的顶层是利用基于 p 稳定分布的

LSH 构建的散列表, 作为预筛选层, 底层是 One-One Map 一对一索引, 用于对与查询图像的相似度计算和得分排名, 双层索引结构使检索效率得到显著提升。方案的不足之处在于: ①为了达到更高的检索效率, 牺牲了一定的准确度; ②图像的相似度信息被泄露。例如, 构建预筛选层的同时, 云服务器很容易判断出同一散列桶中的图像是相似的。在 Xia 等的另外一项工作^[68]中, 在 PPCBIR 中考虑了不诚实用户的问题, 首次构建了密文域上的水印协议。水印与图像查询用户关联且唯一, 可被追踪, 能够阻止授权查询用户对检索图像的非法复制和分发。方案存在一些方面需要改进: ①该水印协议未能达到理想的顽健性; ②一个小的参数 α 会导致可用的水印数量被限制。

8 结束语

隐私保护的图像内容检索技术 PPCBIR 为图像数据的外包存储和检索中存在的隐私问题提供了解决办法, 密文检索策略在“诚实但好奇”云服务器环境下能够得到广泛应用。本文围绕 PPCBIR 的主要技术和关键环节, 对该领域近年来的研究成果进行了综述, 在关键密码技术方面, 总结了应用于 PPCBIR 的图像加密算法(包括同态加密、随机化加密和比较加密)。按照使用的密码技术不同, 分类回顾了近年 PPCBIR 的研究进展, 并介绍了为提高检索效率采用的检索结构优化方案。

结合当前 PPCBIR 的研究进展, 未来对 PPCBIR 研究的重点如下。

1) 大数据环境下, 从海量的图像数据中快速且准确地挖掘出用户所需信息的相关工作, 已经成为当前的研究热点。而加密域图像检索的研究还处于起步阶段, 面对大规模的图像数据库, 如何在隐私保护的前提下实现有效甚至高效的大规模图像检索, 是未来 PPCBIR 面临的挑战。

2) 加密技术是实现图像数据隐私保护的主要解决手段, 但基于对称密码模型中可能存在密钥泄露的问题, 且尚未有方案考虑到图像用户自身携带恶意信息的情况。当图像查询用户的查询请求中携带恶意内容时, 云服务器需要考虑如何识别和拦截。同时, 设计面向数据检索的轻量级图像加密算法, 减少资源有限的客户端的计算量, 也是当前的迫切需求。

3) 图像特征的有效程度会影响最终的检索性能, 在提取图像特征时需要考虑特征维度大小对检索性能的影响。针对多维的图像特征计算, 设计更加安全、高效的轻量级搜索模式, 也是未来重要的研究方向。

参考文献:

- [1] KAMARA S, LAUTER K. Cryptographic cloud storage[C]// International Conference on Financial Cryptography and Data Security, Berlin: Springer Berlin Heidelberg, 2010:136-149.
- [2] LEON P, UR B, SHAY R, et al. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising[C]//Sigchi Conference on Human Factors in Computing Systems, 2012:589-598.
- [3] NAIMIA I, WESTREICH D J. Big data: a revolution that will transform how we live, work, and think[J]. Mathematics & Computer Education, 2014, 47(17):181-183.
- [4] LAGENDIJK R L, BARNI M. Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation[J]. IEEE Signal Processing Magazine, 2013, 30(1):82-105.
- [5] RUPA C. Privacy preservation of ROI of medical image using squint pixel and PLSB hiding technique[C]//International Conference on Virtual System & Multimedia. IEEE, 2017:1-5.
- [6] DUFAUX F. Video scrambling for privacy protection in video surveillance - recent results and validation framework[J]. Proceedings of SPIE-The International Society for Optical Engineering, 2011, 8063:307-314.
- [7] GUDIVADA V N, RAGHAVAN V V. Content based image retrieval systems[J]. Computer, 1995, 28(9):18-22.
- [8] SMITH J R, CHANG S F. Tools and techniques for color image retrieval[J]. Proc. of SPIE(The International Society for Optical Engineering) 1996, 2670:32-42.
- [9] JAIN A K, VAILAYA A. Image retrieval using color and shape[J]. Pattern Recognition, 1996, 29(8):1233-1244.
- [10] DUNN D, HIGGINS W E, WAKELEY J. Texture segmentation using 2D Gabor elementary functions[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1994, 16(2):0-149.
- [11] MANJUNATH B S, MA W Y. Texture features for browsing and retrieval of image data[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996, 18(8):837-842.

- [12] LOWE D G. Distinctive image features from scale-invariant keypoints[J]. *International Journal of Computer Vision*, 2004, 60(2): 91-110.
- [13] JEGOU H, DOUZE M, SCHMID C, et al. Aggregating local descriptors into a compact image representation[C]//*IEEE Conference on Computer Vision and Pattern Recognition*. 2010: 3304-3311.
- [14] YANG B, CHEN S. A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image[J]. *Neurocomputing*, 2013, 120(10):365-379.
- [15] SHEKHAR R, JAWAHAR C V. Word image retrieval using bag of visual words[C]//*IAPR International Workshop on Document Analysis Systems*. 2012: 297-301.
- [16] DATAR M, IMMORLICA N, INDYK P, et al. Locality-sensitive hashing scheme based on p-stable distributions[C]//*Twentieth Symposium on Computational Geometry*, ACM, 2004:253-262.
- [17] TIPPING M E, BISHOP C M. Probabilistic principal component analysis[J]. *Journal of the Royal Statistical Society Series B (Statistical Methodology)*, 1999, 61(3):611-622.
- [18] JOLLIFFE I T. Principal component analysis[J]. *Journal of Marketing Research*, 2002, 87(100):513.
- [19] HSU C Y, LU C S, PEI S C. Image feature extraction in encrypted domain with privacy-preserving SIFT[J]. *IEEE Trans Image Processing*, 2012, 21(11):4593-4607.
- [20] WANG S M, NASSAR M, ATALLAH M, et al. Secure and private outsourcing of shape-based feature extraction[M]. *Information and Communications Security*. Springer International Publishing, 2013: 90-99.
- [21] LI Y M, ZHOU J T, CHENG A, et al. SIFT keypoint removal and injection via convex relaxation[J]. *IEEE Transactions on Information Forensics & Security*, 2016, 11(8):1722-1735.
- [22] WANG Q, HU S S, REN K, et al. Catch me in the dark: effective privacy-preserving outsourcing of feature extractions over image data[C]//*IEEE International Conference on Computer Communications(INFOCOM)*. 2016:1-9.
- [23] HU S S, WANG Q, WANG J J, et al. SecSIFT: privacy-preserving outsourcing computation of feature extractions over encrypted image data[J]. *IEEE Transactions on Image Processing*, 2016, 25(7):3411-3425.
- [24] WONG W K, CHEUNG D W, KAO B, et al. Secure KNN computation on encrypted databases[C]//*ACM Sigmod International Conference on Management of Data*. 2009:139-152.
- [25] 卓力, 龙海霞, 彭远帆, 等. 加密域图像处理综述[J]. *北京工业大学学报*, 2016, 42(2):174-183.
ZHUO L, LONG H X, PENG Y F, et al. Image processing in encrypted domain: a comprehensive survey[J]. *Journal of Beijing University of Technology*, 2016, 42(2):174-183.
- [26] FONTAINE C, GALAND F. A survey of homomorphic encryption for nonspecialists[J]. *Eurasip Journal on Information Security*, 2007, 2007(1):1-10.
- [27] PAILLIER P, POINTCHEVAL D. Efficient public-key cryptosystems provably secure against active adversaries[C]//*International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*. Springer-Verlag, 1999:165-179.
- [28] MATTON S, MOURET G, BOCQUET R, et al. Sub-image homomorphic filtering technique for improving facial identification under difficult illumination conditions[C]//*International Conference on Systems, Signals & Image Processing, Iwssip*, 2006: 439-473.
- [29] LI L, EL-LATIF A A, NIU X. Elliptic curve elgamal based homomorphic image encryption scheme for sharing secret images[J]. *Signal Processing*, 2012, 92(4):1069-1078.
- [30] 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.
- [31] ZHANG Y, ZHUO L, PENG Y, et al. A secure image retrieval method based on homomorphic encryption for cloud computing[C]//*International Conference on Digital Signal Processing*. IEEE, 2014:269-274.
- [32] BELLAFQIRA R, COATRIEUX G, BOUSLIMI D, et al. Content-based image retrieval in homomorphic encryption domain[C]//*International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2015:2944-2947.
- [33] QUELLEC G, LAMARD M, CAZUGUEL G, et al. Wavelet optimization for content-based image retrieval in medical databases[J]. *Medical Image Analysis*, 2010, 14(2):227-241.
- [34] BELLAFQIRA R, COATRIEUX G, BOUSLIMI D, et al. An end to end secure CBIR over encrypted medical database[C]//*Engineering in Medicine and Biology Society*. IEEE, 2016:2537.
- [35] AHMED E D H, KALASH H M, ALLAH O S F. An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption[J]. *Informatica*, 2007, 31(1):121-129.
- [36] TONG X J, CUI M G. Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation[J]. *Science China(Information Sciences)*, 2010, 53(1):191-202.
- [37] LU W J, VARNA A L, SWAMINATHAN A, et al. Secure image retrieval through feature protection[C]//*IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2009:1533-1536.
- [38] XIA Z H, ZHU Y, SUN X, et al. A similarity search scheme over encrypted cloud images based on secure transformation[J]. *International Journal of Future Generation Communication & Networking*, 2013, 6(6):71-80.
- [39] 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.
- [40] FURUKAWA J. Request-based comparable encryption[C]//*European Symposium on Research in Computer Security*. Springer Berlin Heidelberg, 2013:129-146.
- [41] FURUKAWA J. Short comparable encryption[C]//*International Conference on Cryptology and Network Security*. Springer, Cham, 2014:337-352.
- [42] AGRAWAL R, KIERNAN J, SRIKANT R, et al. Order preserving encryption for numeric data[C]//*ACM SIGMOD IntConf on Management of Data*. 2004:563-574.
- [43] LEE S, PARK T J, LEE D, et al. Chaotic order preserving encryption for efficient and secure queries on databases[J]. *IEICE Transactions on Information and Systems*, 2009, 92(11):2207-2217.
- [44] BOLDYREVA A, CHENETTE N, LEE Y, et al. Order-preserving symmetric encryption[C]//*International Conference on Advances in Cryptology-eurocrypt*, 2009:224-241.
- [45] LIU D X, WANG S L. Nonlinear order preserving index for encrypted database query in service cloud environments[J]. *Concurrency & Computation Practice & Experience*, 2013, 25(13): 1967-1984.
- [46] GAO Y Q, MIAO M X, WANG J F, et al. Secure approximate nearest neighbor search over encrypted data[C]//*IntConf on Broad-*

- band & Wireless Computing. IEEE, 2015:578-583.
- [47] POPA R A, REDFIELD C M S, ZELDOVICH N, et al. CryptDB: protecting confidentiality with encrypted query processing[C]//ACM Symposium on Operating Systems Principles 2011, Cascais, Portugal, DBLP, 2011:85-100.
- [48] TANG Q. Privacy preserving mapping schemes supporting comparison[C]//2010 ACM Workshop on Cloud Computing Security Workshop. 2010:53-58.
- [49] CHEN P, YE J, CHEN X F. Efficient request-based comparable encryption scheme based on sliding window method[J]. Soft Computing, 2016, 20(11):4589-4596.
- [50] ZOU Q, WANG J F, YE J, et al. Efficient and secure encrypted image search in mobile cloud computing[J]. Soft Computing, 2017, 21(11): 2959-2969.
- [51] LU W J, SWARMINATHAN A, VARNA A, et al. Enabling search over encrypted multimedia databases[C]//Media Forensics and Security. International Society for Optics and Photonics, 2009: 725411-725418.
- [52] YAO A C. How to generate and exchange secrets[C]//Foundations of Computer Science, Symposium on. IEEE, 2008:162-167.
- [53] 申立艳, 陈小军, 时金桥, 等. 隐私保护集合交集计算技术研究综述[J]. 计算机研究与发展, 2017, 54(10):2153-2169.
- SHEN L Y, CHEN X J, SHI J Q, et al. Survey on private preserving set intersection technology[J]. Journal of Computer Research and Development, 2017, 54(10):2153-2169.
- [54] LINDELL Y, PINKAS B. A proof of security of yao's protocol for two-party computation[J]. Journal of Cryptology, 2009, 22(2): 161-188.
- [55] HUANG Y, EVANS D, KATZ J, et al. Faster secure two-party computation using garbled circuits[C]//Usenix Conference on Security. USENIX Association, 2011:35-35.
- [56] 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. IEEE, 2015:1-1.
- [57] SHEN M, CHENG G, ZHE L, et al. Content-based multi-source encrypted image retrieval in clouds with privacy preservation[J]. Future Generation Computer Systems, 2018:1-13.
- [58] JUNG T, LI X Y, WAN M. Collusion-tolerable privacy-preserving sum and product calculation without secure channel[J]. 2015, 12(1):45-57.
- [59] FERREIRA B, RODRIGUES J, LEITAO J, et al. Towards an image encryption scheme with content-based image retrieval properties[J]. Lecture Notes in Computer Science, 2015: 311-318.
- [60] CHENG H, ZHANG X, YU J, et al. Encrypted JPEG image retrieval using block-wise feature comparison[J]. Journal of Visual Communication & Image Representation, 2016, 40:111-117.
- [61] CHENG H, ZHANG X, YU J. AC-coefficient histogram-based retrieval for encrypted JPEG images[J]. Multimedia Tools and Applications, 2015, 75(21):13791-13803.
- [62] 韩威, 申铭, 徐彦彦, 等. 一种云环境下 JPEG 图像的安全检索方法[J]. 计算机应用研究, 2017(4):1239-1243.
- HAN W, SHEN M, XU Y Y, et al. Secure JPEG image retrieval method under cloud environment[J]. Application Research of Computers, 2017(4):1239-1243.
- [63] HUANG K, XU M, FU S J, et al. Efficient privacy-preserving content-based image retrieval in the cloud[C]//International Conference on Web-Age Information Management. Springer International Publishing, 2016:28-39.
- [64] HUANG Y, ZHANG J, PAN L, et al. Privacy protection in interactive content based image retrieval[J]. IEEE Transactions on Dependable & Secure Computing, 2018:1-1.
- [65] ZHU Y, SUN X M, XIA Z H, et al. Enabling similarity search over encrypted images in cloud[J]. Information Technology Journal, 2014, 13(5):824-831.
- [66] ZHU Y, SUN X M, XIA Z H, et al. Secure similarity search over encrypted cloud images[J]. International Journal of Security & Its Applications, 2015, 9(8): 1-14.
- [67] 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, 2015, 6(1): 276-286.
- [68] 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 & Security, 2016, 11(11):2594-2608.

[作者简介]



吴颖 (1995-), 女, 福建漳州人, 福建师范大学硕士生, 主要研究方向为隐私保护。



李璇 (1984-), 女, 湖北黄石人, 博士, 福建师范大学副教授, 主要研究方向为云数据安全与隐私保护。



金彪 (1985-), 男, 安徽六安人, 博士, 福建师范大学讲师, 主要研究方向为信息安全。



金榕榕 (1998-), 女, 江西南昌人, 主要研究方向为计算机视觉和图像处理。