计算机科学
COMPUTER SCIENCE

基于SecureCNN的高效加密图像内容检索系统

卢雨晗, 陈立全, 王宇, 胡致远

引用本文

卢雨晗, 陈立全, 王宇, 胡致远. 基于SecureCNN的高效加密图像内容检索系统[J]. 计算机科学, 2023, 50(9): 26-34.

LU Yuhan, CHEN Liquan, WANG Yu, HU Zhiyuan. Efficient Encrypted Image Content Retrieval System Based on SecureCNN [J]. Computer Science, 2023, 50(9): 26-34.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400033

基于 SecureCNN 的高效加密图像内容检索系统

卢雨晗　陈立全　王　宇　胡致远
东南大学网络空间安全学院　南京 210000
(Lyh_230701@163.com)

摘　要　随着智能设备的快速发展,云上的基于内容的图像检索技术(CBIR)越来越受欢迎。但在半诚实的云服务器上进行图像检索存在泄露用户隐私的风险。为了防止个人隐私遭到泄露,用户外包图像给云之前会对其进行加密,但现有的明文域上CBIR方案对于加密图像数据的搜索是无效的。为了解决这些问题,文中提出了一个基于近似数同态的高效加密图像内容检索方案,在保护用户隐私的情况下,能够快速实现以图搜图,且无需用户的持续交互。首先使用近似数同态神经网络对图像集进行特征提取,可以保证网络模型的参数和图像集数据不会泄露给云服务器。其次,提出了一种新的神经网络分治方法,该方法可以减少同态加密乘法深度和提高模型运行效率;利用分级可导航小世界(HNSW)算法构造索引,实现高效图像检索。此外,使用同态加密保障图像数据传输过程的安全性,使用对称加密算法保证存储阶段的安全性。最后,通过实验对比和安全性分析证明了该方案的安全性和效率。实验结果表明,该方案是IND-CCA的,且在保证图像私密性的前提下,其同态加密的乘法次数最多为3次,在检索精度上远超过现有方案,在检索时间复杂度方面比现有方案高出至少100倍,实现了检索精度和效率的兼顾。

关键词:近似同态;基于内容的图像检索技术;神经网络;分级可导航小世界图算法;高效检索
中图法分类号　TP391.41

Efficient Encrypted Image Content Retrieval System Based on SecureCNN

LU Yuhan,CHEN Liquan,WANG Yu and HU Zhiyuan
School of Cyberspace Security,Southeast University,Nanjing 210000,China

Abstract　With the rapid development of smart devices,content-based image retrieval technology(CBIR) on the cloud is becoming increasingly popular. However,image retrieval on a semi-honest cloud server carries the risk of compromising user privacy. To prevent personal privacy from being compromised,users encrypt their images before outsourcing them to the cloud,but existing CBIR schemes on plaintext domains are ineffective for searching encrypted image data. To solve these problems,an efficient encrypted image content retrieval scheme based on approximate number homomorphism is proposed in the paper,which can quickly achieve image search without continuous user interaction while protecting user privacy. Firstly,feature extraction of image sets using approximate number homomorphism neural network can ensure that the parameters of the network model and the image set data are not leaked to the cloud server. Secondly,a new neural network partitioning method is also proposed to reduce the homomorphic encryption multiplication depth and improve the model operation efficiency,and also construct the index using hierarchical navigable small world(HNSW) algorithm to achieve efficient image retrieval. In addition,homomorphic encryption is used to guarantee the security of image data transmission process and symmetric encryption algorithm is used to guarantee the security of storage stage. Finally,the security and efficiency of the scheme are proved by experimental comparison and security analysis. Experimental results show that the scheme is IND-CCA,and the number of multiplications of homomorphic encryption in this scheme is at most 3 times while guaranteeing the image privacy,which far exceeds the existing schemes in terms of retrieval accuracy and at least 100 times higher than the existing schemes in terms of retrieval time complexity,achieving a balance of retrieval accuracy and efficiency.

Keywords　Approximately homomorphic,Content-based image retrieval,Neural Network,Hierarchical navigable small world algorithm,Efficient search

到稿日期:2023-04-05　返修日期:2023-07-07
基金项目:国家重点研发计划(2020YFE0200600);国家自然科学基金(62002058)
This work was supported by the National Key R&D Program of China(2020YFE0200600) and National Natural Science Foundation of China(62002058).
通信作者:陈立全(Lqchen@seu.edu.cn)

1 引言

随着智能成像设备的快速发展，图像的数量与日俱增。不少用户看重云服务器高效和智能的基于内容的图像检索服务[1]，选择将图像外包至云服务器。尽管云服务器在图像存储和检索大规模数据方面展现了巨大的业务和技术上的优势，但在图像数据的安全保障方面也带来了新的挑战：倘若云服务器不诚实，它将可能使用户的隐私遭到泄露。例如 2019 年，据 Securityaffairs 报道[2]，全球有 600 个未受保护的医学影像归档和通信系统暴露于互联网中，泄露的数据大约有 4 亿。大量信息泄漏事件[3-4]警示人们必须注意互联网中的隐私保护。要解决隐私安全问题，用户可以将图像加密后上传至云服务器，然而现有的图像检索方案对于加密图像数据的搜索是无效的。

为了检索加密图像，许多学者提出了基于密文的图像检索方案。Wang 等[5]提出了一种基于 CBIR（Content Based Image Retrieval）的加密图像搜索方案，该方案允许图像相似性匹配。但是，该方案没有考虑明文图像和加密图像之间距离的变化。Agrawal 等[6]提出使用保序加密（Order-Preserving Encryption，OPE）的方法对图像进行检索，保序加密可以实现加密前后特征顺序不变的保序功能，但安全性得不到保障。为了提高加密图像的安全性，Furukawa[7]提出了基于请求的可比较加密（Convergent Encryption，CE），可比较加密在保序加密的基础上提供了一定程度的安全性，但它的密文长度太长。后续有一些学者[8-9]在可比较加密的基础上进行改进，提高了比较效率，降低了密文长度，但终端计算能力有限，且这些加密方法大多使用尺度不变特征变换[10]（Scale-invariant Feature Transform，SIFT）、归一化直方图特征[11]和离散余弦变换系数[12]（Discrete Cosine Transform，DCT），选择的特征相对简单，有时并不能完全代表整张图像的特征，可能导致密文检索准确率低。

为了解决加密图像检索现存的问题，有学者提出了同态加密图像检索的方法。同态加密的方法很好地解决了加密条件下数据运算的问题，在密文检索领域得到了广泛的使用。2016 年，Dowlin 等[13]将卷积神经网络（Convolutional Neural Network，CNN）的安全推理阶段与同态加密算法结合起来构建了 CryptoNets 神经网络模型，并使用 MNIST 数据集进行训练。然而 CryptoNets 在激活层使用了近似函数来替代，导致密文模型的准确率低于明文模型。为了降低同态加密方案的开销，文献[14]提出使用稀疏多项式改进 CryptoNets 结构，加速推理过程，使用低次近似多项式替代 CNN 中常用的激活函数，并通过实验进行验证。Juvekar 等[15]使用同态加密和混淆电路技术设计了一个低延迟的安全神经网络推理系统，并在 VGG（Visual Geometry Group）网络中实现了密文运算。但是，它需要用户和服务器之间不断通信。此外，当同态运算的次数变多时，该方案会消耗巨大的内存空间。上述方案虽然在提高特征的准确度和模型的训练效率方面有很大的进展，但它们需要在本地构建检索索引，且大多数方案使用的是 BGV（Brakerski-Gentry-Vaikuntanathan）和 BFV（Brakerski-Fan-Vercauteren）同态加密方案。许多神经网络算法需要对像素值进行归一化处理，而这些方案只能处理 0～255 范围内的像素值但不能进行浮点数运算。同时，为了实现同态加密下的神经网络激活层的功能，上述方案主要采用两种方法：近似函数替代和混淆电路。使用近似函数会导致模型准确率下降且乘法次数消耗大，而混淆电路则会带来高通信成本。因此，这些方案不适用于神经网络的分类问题，需要寻找能够处理同态浮点数运算的加密方法，构建保证一定安全性的图像检索方案。

为了提高同态加密神经网络模型的准确度，减少图像上传者的计算成本和提高检索速率，本文提出了一种基于同态近似安全推理的密文检索算法。参考 splitNN[16]，本文将神经网络进行分治，分成线性运算（卷积层、全连接层和归一层）和非线性运算（激活层），分别在两个服务器上运行，能够在保证整体方案安全性的条件下，使密文网络模型的准确度与明文模型近似，且能在大幅度提高运行效率的同时尽可能减少通信轮数。在本文方案中，只有经过授权获得认证的用户才能进行图像的查询。

综上所述，本文的主要贡献如下：

1）本方案使用 CKKS（Cheon-Kim-Kim-Song）和对称加密对图像进行加密，因此图像所有者可以安全地将图像外包给云服务器。

2）本方案将神经网络模型分治（线性模块和非线性模块）运算，解决了密文条件下使用近似函数替代带来的模型准确率下降和使用混淆电路造成通信成本高的问题，可以更好地提高安全推理的速率和模型的准确性。

3）在图像检索模块，HNSW（Hierarchical Navigable Small World，HNSW）算法通过对图网络进行不同程度的抽取简化，得到不同层级的快速网络，具有效率高、检索快的优点。本方案采用 HNSW 算法能够很好地提高图像检索的准确度和效率。

本文第 2 章回顾了与文章相关的一些研究；第 3 章介绍了文章的系统架构和使用的算法；第 4 章对整体方案进行实验的评估；第 5 章进行系统的性能分析；第 6 章进行系统的安全性分析；最后总结全文并展望未来。

2 相关工作

2.1 基于 CKKS 的近似同态加密方案

CKKS 近似数同态加密算法是由 Cheon 等 4 位韩国研究者[17]于 2017 年提出的近似计算同态加密算法，其具体构造基于 BGV 方案，是基于 RLWE（Ring-Learning With Errors）难题的全同态加密方案。CKKS 不同于以往同态加密算法中追求的明文与解密结果完全一致，它进行近似计算，允许误差，放宽了对准确性的限制。CKKS 方案最大的优势是能直接对双精度浮点类型的实数甚至复数进行编码、加密和运算，适用于深度学习中机器学习算法的浮点数运算。

CKKS 算法运算的流程如图 1 所示，先对消息进行编码，再加密，接着在密文空间进行一些运算后再解密，最后解码成运算后的结果。

CKKS 的主要思想是将加密噪声视为近似计算过程中

发生错误的一部分，即用私钥 sk 对消息 m 得到密文 c，得到：

$$\langle c, sk\rangle = m + e \pmod q \tag{1}$$

其中，e 代表插入的小错误，以保证有误差学习(LWE)、环-LWE(RLWE)和 NTRU(Number Theory Research Unit)困难假设的安全性。只要 e 足够小，那么就可以用近似算法代替原消息。同时，CKKS 在加密前对消息乘以一个比例因子(Scale)，使得近似误差呈线性增长而不是指数增长，从而减少了加密噪声造成的精度损失。此外，CKKS 通过对密文进行乘法运算后进行缩放，可以将密文最大模量所需的比特大小降至 $O(\eta \log d)$，这能有效地对指数、对数和三角函数等超越函数的泰勒级数展开进行近似求值。

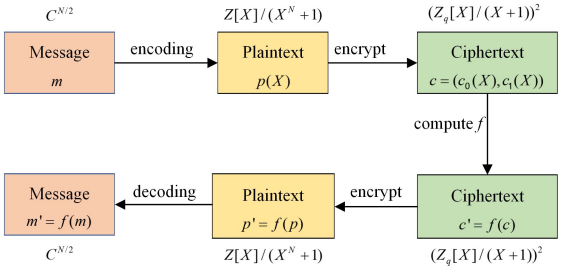


图 1 CKKS 加解密过程

Fig. 1 CKKS encryption and decryption process

在对 CKKS 算法验证的实验中，在一台运行在 2.9 GHz 处理器的 Intel Core i5 上对 14 位精度的密文同时进行 4 096 个槽的并行乘法大约需要 0.45 s，平均每个槽 0.11 ms。CKKS 适用于大数据云计算的环境，因为它允许在单个密文中加密大量信息，能够并行计算。

因此本文提出的同态加密神经网络模型选择使用 SEAL 库的 CKKS 算法来解决近似数运算问题。

2.2 基于图的 HNSW 检索算法

最近邻搜索算法(K-Nearest Neighbor Search, K-NNS)被广泛应用于机器学习算法以及数据库的特征匹配，然而其复杂性随着存储元素数量的增加呈线性增长，这使得它不适用于大规模数据库。此外，普通的最近邻算法的精确解只有在数据维度较低的情况下才能提供可观的搜索速度[18]。

为了解决这一问题，许多学者提出了改进算法，例如近似近邻搜索[19](K-Approximate Nearest Neighbor, K-ANNS)、局部敏感哈希[20]和产品量化[21](Product Quantization, PQ)。然而，在低维数据下，这些算法性能仍存在显著下降的情况。

2018 年 Malkov 等[22]提出了基于图的 HNSW 检索算法。HNSW 算法具有更好的基于对数复杂度的缩放能力，按照不同尺度分离链接，并使用高级启发式算法来选择邻居。性能评估表明，HNSW 算法的通用度量空间方法明显优于以前仅适用于向量空间的开源最新方法。

HNSW 利用多层的图结构来完成图的构建和检索，它将节点划分成不同层级，贪婪地遍历来自上层的元素，直到达到局部最小值，然后切换到下一层，以上一层中的局部最小值作为新元素重新开始遍历，直到遍历完最底层。如图 2 所示，搜索从顶层的一个元素开始(红色)，红色箭头显示算法从入口点到查询的方向(绿色)。HNSW 检索算法如算法 1 所示。

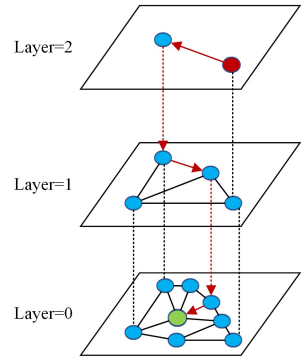


图 2 HNSW 检索过程(电子版为彩图)

Fig. 2 HNSW retrieval process

算法 1 HNSW 检索算法

输入：查询元素 q，输入点 ep，离 q 最近的元素个数返回 ef，层数 lc

输出：ef 最接近 q 的邻居

```
1. v ← ep// 已访问元素集
2. C ← ep // 候选集
3. W ← ep // 最近邻居的动态列表
4. while |C|>0
5.     c ← extract nearest element from C to q
6.     f ← get furthest element from W to q
7.     if distance(c,q)>distance(f,q)
8.         break // all elements in W are evaluated
9.     for each e ∈ neighbourhood(c) at layer l_c// update C and W
10.    if e ∉ v
11.        v ← v∪ e
12.        f ← get furthest element from W to q
13.    if distance(e,q) < distance(f,q) or |W|<ef
14.    C ← C∪e
15.    W ← W∪e
16.    if |W|>ef
17.        remove furthest element from W to q
18. return W
```

HNSW 算法在一层中寻找最近邻居 ef 是通过在搜索过程中保留一个动态列表，此列表里包含 ef 最近已找到的元素，通过计算列表中最近的先前未计算的元素的邻域，在每一步更新列表，直到计算列表中每个元素的邻域。

HNSW 算法提供了出色的性能，同时具有鲁棒性强的特点，能够适应实际的应用。

基于图的 HNSW 检索算法在向量检索的评测中表现较为优异，算法效率高，可以用于本文提取的特征向量的索引构建的检索模块中。

3 基于内容的同态加密检索方案

3.1 基于内容的同态加密检索架构

本节描述所提基于内容的同态加密检索系统的架构，系统架构由 5 个实体组成，即云服务器(计算服务器和存储计算服务器)、(多个)查询用户、(多个)图像所有者和证书发放中心，详细架构如图 3 所示。

计算服务器(Linear Computing Server)：拥有预训练的同态神经网络模型，承担线性层和归一化层的安全计算。

存储计算中心(Storage & Nonlinear Computing Cen-

ter)：拥有对称密钥 Key，负责非线性层的计算，与计算服务器共同响应用户对加密图像的查询；存储加密图像集，构建并保存索引。

图像所有者(User)：拥有图像集，将图像集加密后经转发路由转发至存储计算服务器。

图像检索者(Query User)：获取检索权限，将加密图像上传至云端进行检索。

转发路由(Store Keys and Forward Route)：存储和管理密钥，验证检索用户的权限，发送用户 ID 和公钥给授权用户；作为转发路由转发需要存储和计算的数据至存储计算服务器。

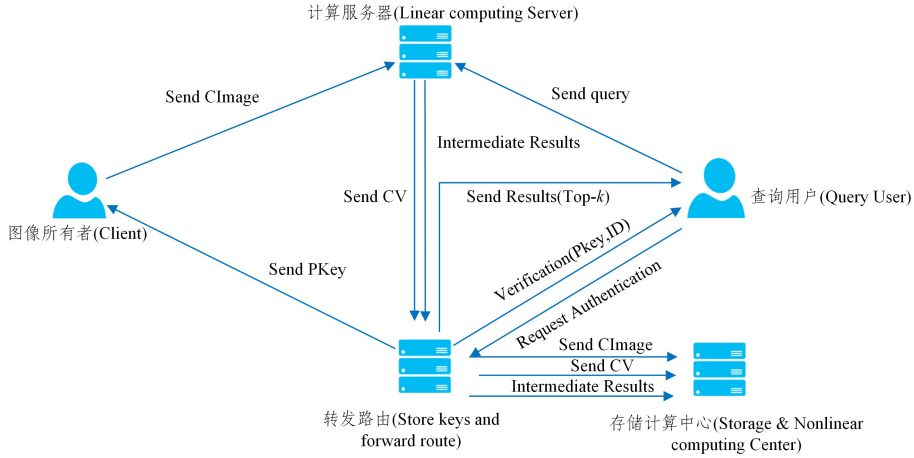


图 3 基于内容的同态加密检索架构

Fig. 3 Content-based homomorphic encryption retrieval architecture

首先，图像所有者将图像集加密后发送至计算服务器，同时将加密图像集经转发路由发送至存储计算服务器，存储计算服务器保存加密图像集。计算服务器进行神经网络的线性部分安全推理，将线性结果交由转发路由，由转发路由解密然后再次用对称密钥加密结果发送至计算存储服务器，计算存储服务器进行神经网络的非线性部分推理。计算服务器得到加密特征集后交由转发路由，转发路由对其进行解密并再次使用对称加密，然后转发至计算储存中心，由计算存储服务器构建和保存图索引。

当检索用户需要检索图像时，用户首先向证书发放机构发送请求，机构验证用户身份后，向用户发送公钥和专属的用户 ID。用户将检索图像加密后上传至计算服务器，由计算服务器和存储计算服务器计算出加密特征向量，计算存储服务器通过特征向量对图索引进行检索得到用户请求的相似图像集并通过转发路由返回至用户。

在本文方案中，图像所有者、转发路由是完全可信的，而服务器是半诚实的。其中存储计算服务器与外界隔离，只能与转发路由进行沟通，且存储计算服务器存储的信息都进行了对称加密，防止信息泄露。

为了更好地描述系统各个模块之间的关系，文中定义了一系列符号，其对应的描述如表 1 所列。

表 1 符号与其描述

Table 1 Symbols and their descriptions

符号	描述
Image	明文图像
CImage	密文图像
query	查询图像序列
Skey	同态加密私钥
Pkey	同态加密公钥
CV	加密的特征向量
Node	索引节点
index	图像特征索引
PI	明文图像序列号
Result()	返回的检索结果

为了提高密文推理阶段的模型训练准确性，同时降低乘法深度，我们将网络模型进行分治，从 Relu 层截断分为两个网络模块，不包含 Relu 的网络模块(卷积层、全连接层和归一化层)在计算服务器上运行，Relu 网络模块(激活层)在计算存储服务器上运行，如图 4 所示。

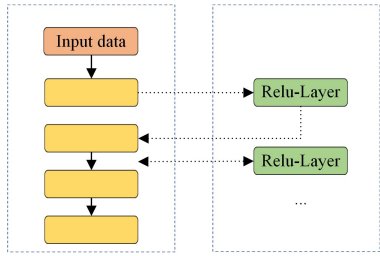


图 4 网络模块

Fig. 4 Network module

3.2 近似数同态加密神经网络实现

本文中神经网络模型的参数都已经进行了预训练，在近似数同态加密神经网络中只执行推理阶段。CKKS 算法只支持有限次数的乘法，并且随着神经网络深度的增加，乘法的次数也会增加，而乘法深度的增加会导致密文扩张和推理阶段效率低下。因此，只有优化神经网络结构，才能尽可能增加神经网络结构的深度。同时，CKKS 加密参数应尽可能小，才能加快密文图像安全推理的速度。

3.2.1 密文线性层实现

神经网络的线性层主要为卷积层、全连接层和 BN 层。卷积层和全连接层的明文计算公式都可以简单表示为：

$$y_{\text{out}} = w_i \cdot x_i + b_i \tag{2}$$

其中，y_{out} 为线性层的输出，w_i 为对应层的权重，x_i 为输入，b_i 为偏移量。

由上述公式可知，神经网络的线性层主要运算方式为加法和乘法，在近似数同态运算中是能够直接实现的。因此，

密文条件下的卷积层和全连接层计算公式为：

$$Ciphertext(y_{out})=ciphertext(w_i \cdot x_i+b_i) \tag{3}$$

$Ciphertext()$表示 CKKS 的加密函数，$encode()$为 CKKS 下的编码函数。通过这样的运算就能实现线性层从明文运算转化为密文计算的过程。

BN 层由 Ioffe 等[23]于 2015 年提出，通过数据归一化将每层神经网络的神经元输入的分布调整至均值为 0、方差为 1 的标准正态分布，用于解决神经网络中深度越大收敛越慢的问题。

$$\begin{cases}\mu_B \leftarrow \dfrac{1}{m}\sum\limits_{i=1}^{m} x_i \\ \sigma_B^2 \leftarrow \dfrac{1}{m}\sum\limits_{i=1}^{m}(x_i-\mu_B)^2 \\ \hat{x}_i \leftarrow \dfrac{x_i-\mu_B}{\sqrt{\sigma_B^2+\varepsilon}} \\ y_i \leftarrow \gamma x_i+\beta \equiv BN_{\gamma,\beta}(x_i)\end{cases} \tag{4}$$

其中，μ_B 是每批数据的均值，σ_B^2是每批数据的方差。γ 和 β 是最合适神经网络的分布，为了实现密文条件下的批量归一化，需要提前保存神经网络训练时的方差和均值的参数，即 $variance$和 $mean$。因此，得到密文条件下的批量归一化公式为：

$$\hat{y}=\gamma \cdot \frac{x_i-mean}{\sqrt{variance+\varepsilon}}+\beta \tag{5}$$

通过上述公式就能将明文形式的归一化层转化为密文条件下的运算。

3.2.2 近似数同态加密神经网络结构

本方案使用 MNIST 数据集和 CIFAR-10 数据集来对明文训练后的神经网络模型进行同态安全神经网络推理。同态加密安全神经网络推理在进行一次密文乘法运算时会消耗一次乘法次数。由于方案对激活层进行单独计算，因此安全神经网络推理所需的最大乘法次数将在激活层后清零再重新计算。

针对 MNIST 数据集，本方案设计了 10 层神经网络，选择全连接层的输出作为密文图像的特征向量。表 2 列出了用于提取 MNIST 数据集深度神经网络的参数，整个推理过程需要消耗的乘法次数最大为 3。

表 2 MNIST 数据集网络参数

Table 2 MNIST dataset network parameters

	网络层	描述	参数	乘法深度
1	Conv1	输入图像大小 28×28，卷积核尺寸 5×5，步数 1，卷积核个数 20，卷积输出 24×24×20	卷积核权重，偏移量	1
2	BN1	输入 24×24×20，输出 24×24×20	方差，均值，γ，β	2
3	Relu1	激活层	—	清零
4	Average pool1	池化窗口大小 2×2，输出 12×12×20	—	1
5	Conv2	卷积核尺寸 3×3，步数 1，卷积核个数 50，卷积输出 10×10×50	卷积核	2
6	BN2	输入 10×10×50，输出 10×10×50	方差，均值，γ，β	3
7	Relu2	激活层	—	清零
8	Average pool2	池化窗口大小 2×2，输出 5×5×50	—	1
9	Flatten	将多维数组扩展为一维数组	—	1
10	FC1	输入 1250，输出 500	全连接层权重，偏移量	2
11	softmax	—	—	3

同样，针对 CIFAR-10 数据集，本文构建了一个 11 层的神经网络结构，该神经网络的具体参数如表 3 所列。

表 3 CIFAR-10 数据集网络参数

Table 3 CIFAR-10 dataset network parameters

	网络层	描述	参数	乘法深度
1	Conv1	输入图像大小 32×32×3，卷积核尺寸 5×5，步数 1，卷积核个数 32，卷积输出 28×28×32	卷积核权重，偏移量	1
2	Relu1	激活层	—	清零
3	BN1	输入 28×28×32，输出 28×28×32	方差，均值，γ，β	1
4	Average pool1	池化窗口大小 2×2，输出 14×14×32	—	2
5	Conv2	卷积核尺寸 3×3，步数 2，卷积核个数 64，卷积输出 6×6×64	卷积核	3
6	Relu2	激活层	—	清零
7	BN2	输入 6×6×64，输出 6×6×64	方差，均值，γ，β	1
8	Average pool2	池化窗口大小 2×2，输出 3×3×64	—	2
9	Flatten	将多维数组扩展为一维数组	—	2
10	FC1	输入 576，输出 128	全连接层权重，偏移量	3
11	Relu3	激活层	—	清零
12	softmax	—	—	1

整个推理过程需要消耗的乘法次数最大为 3。本文的神经网络模型改进乘法次数与其他同态加密网络模型的对比如表 4 所列。本文方案和对比模型均采用 SEAL 库中的同态加密算法，可以看出，相较于其他网络，本方案显著减少了密文神经网络的乘法次数。

表 4 乘法深度对比

Table 4 Multiplication depth comparison

网络	深度	原始次数	改进后的次数
MNIST	10	9	3
CIFAR-10	11	10	3
CryptoDL[24]	14	14	14
Ref. [25]	13	12	10

3.3 基于图的 HNSW 索引构建

通过上述密文神经网络的推理，就能获得同态的密文特征向量。由于密文形式的特征向量不具备检索能力，因此在计算服务器得到密文特征向量后，计算服务器会将其发送至计算存储服务器进行存储，同时计算服务器还将解密特征向量并建立基于图的 HNSW 检索索引用于在线阶段的图像检索，具体索引构建方案和检索方案如算法 3 和算法 4 所示。

算法 3 检索构建算法

输入：计算服务器：加密图像特征 $\mathbf{CV}=\{cv_1,\cdots,cv_n\}$

输出：计算存储服务器：索引 index

计算存储服务器：

While：

提取密文特征向量：$\mathbf{CV}=\{cv_1,\cdots,cv_n\}$

Return **CV** to 计算储存服务器

End

计算存储服务器：

1. 解密密文特征向量 $\mathbf{V}=\mathrm{dec}(\mathbf{CV})$

2. 计算解密后特征向量的 KNN 结点 Node=HNSW(**V**)

3. 计算 index=Node+PI(Image)

4. 存储 index

算法 4 图像检索算法

输入：图像特征向量的 HNSW 图 G'

输出：密文相似图像集{CImage$_i$，1≤i≤500}

计算服务器：

计算检索图像的密文特征向量 $\mathbf{CV}'$

Return $\mathbf{CV}'$ to 计算存储服务器

计算存储服务器：

1. 解密检索密文特征向量 **V**=dec(**CV**)

2. 计算特征向量的 HNSW-KNN 结点 Node′=HNSW(**V**)

3. 计算结点 Node 和 Node′之间的余弦相似值

Cosine Similarity=Similar(Node，Node′)

Return min(PI(Image$_i$))

4. Send CImage$_i$ to 查询用户

4 实验结果

本文使用 MNIST 数据集和 CIFAR-10 数据集来验证所提出的同态加密检索方案的准确性、效率和安全性。

MNIST 数据集：MNIST 数据集来源于美国国家标准与技术研究所(National Institute of Standards and Technology，NIST)，该数据集包括 250 人手写的数字图片，图像为 28×28。训练集一共包含 60000 张图像和标签，而测试集一共包含 10000 张图像和标签。

CIFAR-10 数据集：CIFAR-10 数据集是由 Hinton 的学生 Alex Krizhevsky 和 IIya Sutskever 整理的一个用于识别常见物体的数据集，该数据集一共包含 10 个类别的 RGB 图像，分别为：飞机(airplane)、汽车(automobile)、鸟类(bird)、猫(cat)、鹿(deer)、狗(dog)、蛙(frog)、马(horse)、船(ship)和卡车(truck)。数据集的图像尺寸为 32×32×3，数据集中一共有 50000 张训练图像和 10000 张测试集图像。

在对密文图像进行推理的过程中，本方案将 the poly modulus degree 设置为 4096，最大模数长度设置为 109 比特，scale 设置为 225，最多可支持 3 次乘法。

本章分别评估了特征提取、索引构建和图像检索的性能。在特征提取的过程中，测量了模型训练的准确率、加密时间、模型运行时间和内存空间；在索引构建期间，测量了索引构建时间、索引构建内存和索引存储量；在检索阶段，使用检索消耗时间作为评估指标。

4.1 模型准确率

本节采用 MNIST 数据集和 CIFAR-10 数据集作为训练集，对 3.2 节的网络模型进行训练，并比较明文和密文条件下不同模型测试集的准确度。

表 5 模型测试集准确率分析

Table 5 Accuracy analysis of model test set

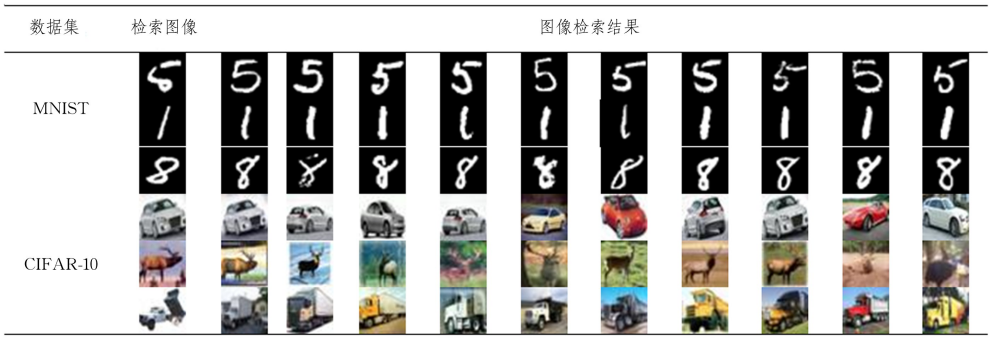
网络	明文模型准确率	密文模型准确率
MNIST	0.99049	0.99049
CIFAR-10	0.76590	0.76589
Manto[26]	0.91990	0.91200
Delphi [27]	0.91980	0.85360

4.2 检索准确率

在图像检索数据集构建上，本方案选择来自 MNIST 数据集和 CIFAR-10 数据集的 20000 张图像构成的两个数据集，分别用这两个图像集经过同态加密神经网络推理后得到的特征向量来构建特征向量索引，验证所提索引算法的正确性和有效性。选择两个特征向量之间的余弦相似性来作为特征向量相似性的衡量标准，并通过索引返回用户要求的 Top-k 张相似图像。这里随机选择 6 张图像作为检索图像，其检索结果如表 6 所列。

表 6 Top-10 检索图像结果

Table 6 Top-10 search image results



本文使用精确率评估方案的图像检索正确程度，图像检索精确率 Precision 的定义如下：

$$Precision=\frac{\text{Number of similar images retrieved}}{\text{Total number of retrieved images}} \tag{6}$$

$$Recall=\frac{\text{Number of similar images retrieved}}{\text{Total number of similar images in the dataset}} \tag{7}$$

高精确度意味着使用的检索算法的检索性能高，本文方案在 MNIST 和 CIFAR-10 数据集上的表现如图 5 和图 6 所示。

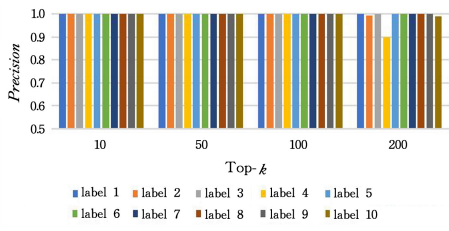


图 5 MNIST 数据集各标签的准确率

Fig. 5 Accuracy of each label in MNIST dataset

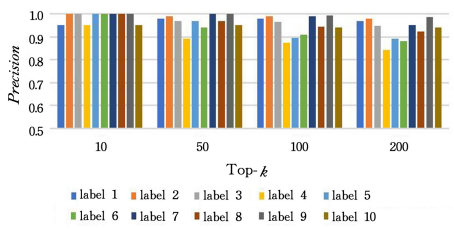


图 6 CIFAR-10 数据集各标签的准确率

Fig. 6 Accuracy of each label in CIFAR-10 dataset

从图中可以看出，在 Top-k=10，50，100 时，在 MNIST 数据集上，所提算法的检索准确率都为 100%，在 Top-k=200 时，除了第二个标签的检索准确率为 99.5%外，其他标签的检索准确率都为 100%。在 CIFAR-10 数据集上，Top-k=10，50，100，200 时，所提算法各标签的检索准确率都高于 68.5%。

图 7 给出了检索 Top-k 和 Recall 之间的关系，可以看出，随着 Top-k 的增加，召回率也在逐步上升，最终 MNIST 数据集的召回率接近 1，而 CIFAR-10 数据集的召回率为68.85%。

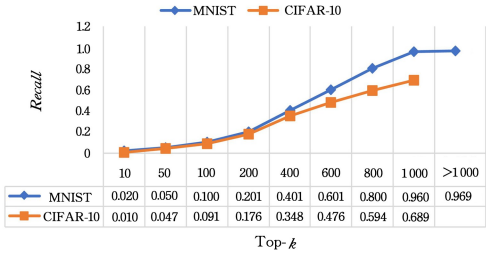


图 7 Recall 与 Top-k 之间的关系

Fig. 7 Relationship between Recall and Top-k

在使用相同数据集的情况下，本方案与其他文献进行对比的详细情况如图 9 所示。

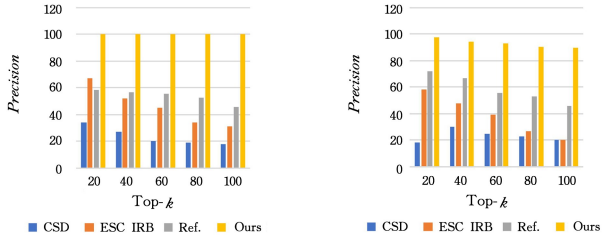


图 8 检索精度对比

Fig. 8 Search accuracy comparison

从图 8 可以看出，在 MNIST 数据集上，其他方案[25,28-29]的准确度均低于 70%，而本文方案准确率接近 100%；在 CIFAR-10 数据集上，本方案的准确率至少为 89%，比其他方案更高。

5 性能分析

5.1 效率分析

本文方案采用 CKKS 同态加密算法和对称加密算法对原始图像进行加密，分别从加密效率、模型运行效率、通信量与其他类似工作的对比进行方案效率分析，具体如表 7 所列。

表 7 效率对比

Table 7 Efficiency comparison

网络	同态加密时间/s	对称加密时间/s	运行时间/s	推理内存/GB	通信轮数
MNIST	2.229	0.001	0.1678	3.0	2
CIFAR-10	6.791	0.004	0.2012	4.7	3
Ref.[30]	—	—	1.4690	—	—
SCI_{HE}[31]	147.200	—	41.1000	5.9	n
Cheetah[32]	39.100	—	16.0000	0.5	n

在加密效率方面，本方案同态加密 MNIST 数据集需要 2.229s，加密 CIFAR-10 需要 6.791s，所耗费时间远远少于对比方案。

在模型运行效率方面，本方案对 MNIST 数据集和 CIFAR-10 数据集中一张图片的推理时间分别为 0.168 s 和 0.201 s，远远快于对比模型的推理速度，其中，本文方案较 Ref.[30]快至少 7 倍，较 SCI_{HE} 快至少 204 倍，较 Cheetah 快至少 79 倍。

从通信量来看，本文方案的通信轮数相较于其他使用混淆电路和同态的网络显著减少。

5.2 索引构建效率

本文使用的基于图的 HNSW 检索算法构建索引的效率测试结果如表 8 所列。

表 8 索引构建效率对比

Table 8 Index construction efficiency comparison

网络	索引构建时间(10000 images)/s	索引构建内存/GB	索引存储量/GB
MNIST	0.3859	0.0604	1.960
CIFAR-10	0.4637	0.4713	1.960
Ref.[33]	421.5000	—	—
Ref.[34]	0.8546	—	34.550
Ref.[35]	56.4000	—	—

将本文的索引算法与其他方案进行比较。从表 8 可以看到，本文使用的索引比其他的索引构建效率更高。其他索引时间至少为 0.85 s，对应的索引大小也超过了 20MB，与本方案的索引构建时间 0.46 s 和 0.39 s、索引构建内存 1.96 MB 形成鲜明对比。

5.3 检索效率

本文使用的基于图的 HNSW 检索算法检索效率测试结果如表 9 所列，使用 Top-k=10，50，100，200 这 4 种类型的 Top-k 来评估检索算法，每一类型进行 10 次检索实验，取其平均值。

表 9 索引检索效率对比

Table 9 Index retrieval efficiency comparison

类别	网络	平均检索时间/ms
Top-k=10	MNIST	0.197
	CIFAR-10	0.199
	CLD	22.900
	CSD	25.700
	EHD	19.800
	SCD	23.800
	Ref.[34]	38.100
Top-k=50	MNIST	0.196
	CIFAR-10	0.196
Top-k=100	MNIST	0.196
	CIFAR-10	0.297
Top-k=200	MNIST	0.199
	CIFAR-10	0.299

从表 9 可以看出本方案的索引检索效率几乎不随检索图像数量的增加而提高，同时本方案比现有的方案检索效率要高至少 100 倍，这表明所提方案具有良好的检索效率。

6 安全性分析

本章讨论如何使用方案来保障神经网络参数的安全性以及保证图像特征不被反推，从而保障数据的隐私，同时证明本方案是 IND-CCA(INDistinguishability under Chosen Ciphertext Attack)的。

1)隐私泄露分析：在安全推理和图像查询的过程中，神经网络的参数和检索图像信息不会被泄露。

本方案使用近似同态加密模型权重参数，使用近似同态加密和对称加密图像信息。同态加密的算法的安全性取决于 CKKS 算法，其安全性依赖于 RLWE 难题；对称加密的安全性依赖于对称密钥的保密。因此，在安全推理的过程中，神经网络的参数和检索图像的信息都不会被泄露。

2)攻击性分析：在图像检索的过程中，即使攻击者获得图像特征向量也不能反推出图像所属类别。

服务器对图像进行特征提取得到的特征值一直是以同态密文的形式存在的，CKKS 算法基于 RLWE 难题，根据 RLWE 假设，RLWE 保证加密后的信息是均匀分布、不可区分的，所以加密后的特征向量包含的特征值是无法区分的。因此，在图像检索的过程中，即使攻击者获得图像特征向量也不能反推出图像所属的类别。

3)安全假设分析：在图像检索的过程中，加密图像检索方案是 IND-CCA。

加密图像检索系统可能会受到攻击者 A 的攻击，攻击过程为：

1)攻击者 A 获得系统的公钥；

2)攻击者 A 选择一系列明文或加密图像对系统进行查询，系统将加密或解密结果返回至攻击者 A，得到：$\{(V_1, CV_1),(V_2, CV_2),\cdots,(V_n, CV_n)\}$。

3)攻击者 A 输出 V_i'，如果 $b=b'$，则攻击成功。

假设查询图像 Q 的密文特征向量为 $\boldsymbol{V}_i'$，图像 X 的密文特征向量为 $\boldsymbol{b}=\boldsymbol{b}'$。根据式(3)，本文的神经网络模型线性层均使用加密的图像输入与加密的预训练模型权重和偏移量来运算，加密消息 $c=m+e(\mathrm{mod}\ q)$，所有消息 c 都包含一个附加的错误 e，即加密和解密的结果均是近似数。即使使用相同的密钥对同一张图像进行多次线性计算也会产生不同的结果，因此 N 次猜测的概率为 $1/n$。所以攻击者 A 的优势为：

$$A_{\mathrm{Adv}}(A)=\left|Pr(\boldsymbol{b}'=\boldsymbol{b})-\frac{1}{2}\right|=\left|\left(\frac{1}{2}+\frac{1}{n}\right)-\frac{1}{2}\right|=\frac{1}{n}$$

因此攻击者 A 的攻击优势为多项式时间，可以忽略不计。所以本方案是 IND-CAA 安全的。

结束语 本文主要研究云环境下具有隐私保护能力的安全图像检索方案。该方案实现了一个同态近似神经网络和分治 CNN 模型，使本文提出的框架能够安全有效地推理卷积神经网络。文章进一步使用了分级可导航小世界图算法，使服务器能够准确高效地比较两张图像。实验结果表明，本文提出的方案能够在保证用户隐私的前提下，对图像进行准确、高效的检索。通过与现有方案进行比较，本文方案实现了超越现有同类加密图像检索方案至少 100 倍的高效检索，且在检索精度上超过了现有方案。然而，尽管神经网络的训练被移交到了云服务器上，但同态加密计算本身具有复杂性，导致近似同态网络推理时间的增加无法避免。在今后的工作中，本方案将从 CKKS 算法出发，通过优化算法来缩短网络推理的时间，进一步提高加密图像推理效率。

参 考 文 献

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

[2] HE Y, CHEN L, NI Y, et al. Privacy protection scheme for edge computing based on function encryption[C]// 2021 International Conference on Networking and Network Applications(NaNA). IEEE, 2021: 131-135.

[3] LIU W, WU D J. Research progress on privacy protection of medical information[J]. Software, 2020, 41(5): 74-79.

[4] 2020 Data Breach Incident Report in the U. S. Healthcare Industry [EB/OL]. www. mchz. com. cn.

[5] WANG H, XIA Z, FEI J, et al. An AES-based secure image retrieval scheme using random mapping and BOW in cloud computing[J]. IEEE Access, 2020, 8: 61138-61147.

[6] AGRAWAL R, KIERNAN J, SRIKANT R, et al. Order preserving encryption for numeric data[C]// Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. 2004: 563-574.

[7] FURUKAWA J. Request-based comparable encryption [C]// European symposium on research in computer security. Berlin: Springer, 2013: 129-146.

[8] CHEN P, YE J, CHEN X. Efficient request-based comparable encryption scheme based on sliding window method[J]. Soft Computing, 2016, 20: 4589-4596.

[9] ZOU Q, WANG J, YE J, et al. Efficient and secure encrypted image search in mobile cloud computing[J]. Soft Computing, 2017, 21: 2959-2969.

[10] QIN Z, YAN J, REN K, et al. Towards efficient privacy-preserving image feature extraction in cloud computing[C]// Proceedings of the 22nd ACM International Conference on Multimedia. 2014: 497-506.

[11] FENG Q, LI P, LU Z, et al. DHAN: Encrypted JPEG image retrieval via DCT histograms-based attention networks[J]. Applied Soft Computing, 2023, 133: 109935.

[12] ZHANG C, LI J, WANG S, et al. An encrypted medical image retrieval algorithm based on DWT-DCT frequency domain[C]// 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications(SERA). IEEE, 2017: 135-141.

[13] GILAD-BACHRACH R, DOWLIN N, LAINE K, et al. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy[C]// International Conference on Machine Learning. PMLR, 2016: 201-210.

[14] CHOU E, BEAL J, LEVY D, et al. Faster cryptonets: Levera-

ging sparsity for real-world encrypted inference[J]. arXiv:1811.09953,2018.

[15] JUVEKAR C,VAIKUNTANATHAN V,CHANDRAKASAN A.{GAZELLE}:A low latency framework for secure neural network inference[C]// 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018:1651-1669.

[16] PERETEANU G L,ALANSARY A,PASSERAT-PALMBACH J. Split HE:Fast secure inference combining split lear-ning and homomorphic encryption[J]. arXiv:2202.13351,2022.

[17] CHEON J H,KIM A,KIM M,et al. Homomorphic encryption for arithmetic of approximate numbers[C]// Advances in Cryptology-ASIACRYPT 2017:23rd International Conference on the Theory and Applications of Cryptology and Information Security. Springer International Publishing,2017:409-437.

[18] GALLEGO A J,RICO-JUAN J R,VALERO-MAS J J. Efficient k-nearest neighbor search based on clustering and adaptive k values[J]. Pattern Recognition,2022,122:108356.

[19] LI W,ZHANG Y,SUN Y,et al. Approximate nearest neighbor search on high dimensional data—experiments,analyses,and improvement[J]. IEEE Transactions on Knowledge and Data Engineering,2019,32(8):1475-1488.

[20] BELARBI M A,MAHMOUDI S,BELALEM G,et al. A New Comparative Study of Dimensionality Reduction Methods in Large-Scale Image Retrieval[J]. Big Data and Cognitive Computing,2022,6(2):54.

[21] THAKUR N,REIMERS N,LIN J. Domain adaptation for memory-efficient dense retrieval[J]. arXiv:2205.11498,2022.

[22] MALKOV Y A,YASHUNIN D A. Efficient and robust approximate nearest neighbor search using hierarchical navigable small world graphs[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence,2018,42(4):824-836.

[23] IOFFE S,SZEGEDY C. Batch normalization:Accelerating deep network training by reducing internal covariate shift[C]// International Conference on Machine Learning. PMLR,2015:448-456.

[24] HESAMIFARD E,TAKABI H,GHASEMI M. Cryptodl:Deep neural networks over encrypted data[J]. arXiv:1711.05189,2017.

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

[26] CHENG K,FU J,SHEN Y,et al. Manto:A Practical and Secure Inference Service of Convolutional Neural Networks for IoT[J]. IEEE Internet of Things Journal,doi:10.1109/JIOT.2023.3251982.

[27] SRINIVASAN W Z,AKSHAYARAM P,ADA P R. DELPHI:A cryptographic inference service for neural networks[C]// Proceedings of 29th USENIX Security. 2019:2505-2522.

[28] 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.

[29] WANG Z,QIN J,XIANG X,et al. A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing[J]. Multimedia Systems,2021,27:403-415.

[30] LEE J W,KANG H,LEE Y,et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network[J]. arXiv:2106.07229,2021.

[31] RATHEE D,RATHEE M,KUMAR N,et al. CrypTFlow2:Practical 2-party secure inference[C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020:325-342.

[32] HUANG Z,LU W,HONG C,et al. Cheetah:Lean and Fast Secure {Two-Party} Deep Neural Network Inference[C]// 31st USENIX Security Symposium(USENIX Security 22). 2022:809-826.

[33] HASSAN A,LIU F,WANG F,et al. Secure content based image retrieval for mobile users with deep neural networks in the cloud[J]. Journal of Systems Architecture,2021,116:102043.

[34] WANG Z,QIN J,XIANG X,et al. A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing[J]. Multimedia Systems,2021,27:403-415.

[35] 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,2020,109:621-632.

LU Yuhan, born in 1999, postgraduate. Her main research interests include image security retrieval and so on.

CHEN Liquan, born in 1976, Ph.D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include information security, cryptography and network security protocol, etc.

(责任编辑:何杨)