Efficient Fine-Grained Website Fingerprinting via Encrypted Traffic Analysis Using Deep Learning: The BurNet Approach

* 基于深度学习加密流量分析的高效细粒度网站指纹识别方法

摘要—细粒度网站指纹识别（Website Fingerprinting，WF）技术能让潜在攻击者通过分析经 TLS 等安全协议保护的网络流量，推断出受害者正在访问的受监控网站中的具体网页。目前大多数研究聚焦于以网站为粒度的指纹识别，通常将网站首页作为指纹识别的代表。细粒度网站指纹识别可揭示更多用户隐私，如在线购物习惯、视频观看偏好等，也可用于网络审查。但由于同一网站内网页极为相似，如何准确且高效地进行细粒度网站指纹识别仍是一个待解决的问题。在本文中，我们提出了 BurNet，这是一种基于卷积神经网络（CNNs）的细粒度网站指纹识别方法。为了提取相似网页之间的差异，我们引入了“单向突发”这一全新概念，它是与一条 HTTP 消息相对应的数据包序列。BurNet 以单向突发序列而非双向数据包序列作为输入，这使其适用于本地和远程攻击场景。BurNet 利用 CNNs 构建了一个强大的分类器，通过精巧的架构设计，在提升分类准确率的同时降低了训练的时间复杂度。我们从两个知名网站收集了真实数据集，并开展了大量实验来评估 BurNet 的性能。封闭世界评估结果显示，在两种攻击场景下，BurNet 的表现均优于现有方法。在更贴近现实的开放世界环境中，BurNet 在二元分类任务中能够达到 0.99 的精确率和召回率。在训练效率方面，BurNet 也优于其他基于 CNNs 的同类方法。

***Index Terms*—细粒度网站指纹识别；加密流量；单向突发；卷积神经网络**

I. Introduction

With the prevalent adoption of the Transport Layer Security (TLS) protocol across websites, the proportion of web traffic encrypted by security protocols has been on a continuous upward trend [1]. For instance, Google has implemented security measures to protect 95% of its products and services [2]. Website fingerprinting (WF) through encrypted traffic analysis empowers potential attackers to identify the websites visited by victims. Existing studies typically operate at the website-level granularity, using website homepages as representatives for fingerprinting. However, we assert that fine-grained WF, which aims to recognize specific webpages within a designated website, can expose more user privacy. This includes details such as the products users view on online shopping platforms or the videos they watch on YouTube. Additionally, network administrators can utilize fine-grained WF for web censorship, like restricting access to certain pages on popular websites. Table I presents a comparison of existing WF methods. Designing an effective fine-grained WF method is a formidable challenge. Firstly, accurately identifying encrypted network flows corresponding to different webpages is extremely difficult. Webpages on the same website share more similarities compared to the index pages of different websites [3], making it hard to distinguish them based on encrypted traffic. Secondly, it is nontrivial to develop a WF method that is applicable to diverse attack scenarios. Attackers can be positioned at various points along the network path from victims to web servers, resulting in different capabilities to obtain network traffic. The third challenge

Identify applicable funding agency here. If none, delete this.

manual feature selection.

II. Ease of Use

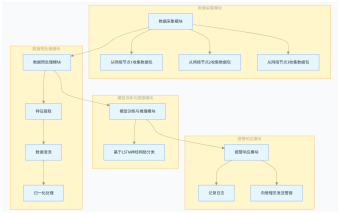

图 1: Example of a figure caption.

某研究团队在 CIFAR-10 图像分类数据集上，使用三种典型卷积神经网络模型（AlexNet、VGG16、ResNet-50）进行了实验。研究者记录了各模型的训练时间、模型参数量、测试准确率以及适合边缘设备部署的可行性（以“高”“中”“低”评价）。结果如下：

表 I: 不同卷积神经网络模型在 CIFAR-10 数据集上的实验结果

模型名称	训练时间（分钟）	参数量（M）	测试准确率	边缘部署可行性
AlexNet	22	61	83.6%	高
VGG16	45	138	89.4%	中
ResNet-50	60	25.6	91.7%	低

在本次实验中，针对 CIFAR - 10 图像分类数据集使用 AlexNet、VGG16 和 ResNet - 50 三种典型卷积神经网络模型进行测试，得到了不同维度的实验结果，具体分析如下：

1. 准确率方面：从实验数据可知，AlexNet 的测试准确率为 83.6%，VGG16 的测试准确率为 89.4%，而 ResNet - 50 的测试准确率达到了 91.7%。通过对这三个模型准确率的数值比较，ResNet - 50 在准确率方面表现最优。在深度学习模型的性能评估中，准确率是一个关键指标，它直观反映了模型对数据分类的正确性程度。ResNet - 50 凭借其独特的网络结构，例如残差块的设计，有效地解决了深度神经网络在训练过程中的梯度消失和梯度爆炸问题，使得模型能够学习到更加复杂和抽象的特征，从而在 CIFAR - 10 数据集上实现了最高的分类准确率。

2. 适合部署到资源受限的边缘设备方面：边缘设备通常具有有限的计算资源、存储资源和能源供应。在衡量模型是否适合部署到边缘设备时，模型的参数量和训练时间等因素至关重要。AlexNet 的参数量为 61M，训练时间为 22 分钟，且边缘部署可行性评价为高；VGG16 参数量达 138M，训练时间 45 分钟，边缘部署可行性为中；ResNet - 50 参数量 25.6M，训练时间 60 分钟，边缘部署可行性低。尽管 ResNet - 50 参数量相对不是最大，但训练时间长且边缘部署可行性评价为低。综合来看，AlexNet 具有相对较少的参数量以及较短的训练时间，其边缘部署可行性被评价为高，所以 AlexNet 最适合部署到资源受限的边缘设备上。较少的参数量意味着模型在存储和计算时所需的资源更少，较短的训练时间也减少了在边缘设备上进行模型更新或微调时的资源消耗。

3. 性能与部署可行性之间的平衡方面：性能方面主要参考测试准确率，部署可行性则综合考虑参数量、训练时间以及给定的可行性评价。VGG16 的测试准确率为 89.4%，处于较高水平，其参数量为 138M，训练时间 45 分钟，边缘部署可行性评价为中。与 AlexNet 相比，VGG16 虽然在部署可行性上稍逊一筹，但在性能（准确率）上有明显提升；与 ResNet - 50 相比，VGG16 在性能上略低，但在部署可行性方面更具优势。因此，VGG16 在性能与部署可行性之间取得了较好的平衡。它既能够在图像分类任务中达到较高的准确率，展现出良好的性能，同时在资源需求和部署的难易程度上也处于可接受的范围，对于一些对性能有一定要求且资源并非极度受限的边缘设备应用场景具有较高的适用性。