

开题报告填写要求

一、开题报告作为毕业设计（论文）答辩委员会对学生答辩资格审查的内容之一。此报告应在指导教师指导下，由学生在毕业设计（论文）工作前期内完成，经指导教师签署意见及所在专业审查后生效；

二、开题报告内容必须用黑色签字笔工整书写或按教务处统一设计的电子文档标准格式（可从教务处网页上下载）打印，禁止打印在其它纸上后剪贴，完成后应及时交给指导教师签署意见；

三、开题报告内有关“学院（系）”、“专业”等名称的填写，应写中文全称；学生的“学号”要写全，不能只写最后几位数字。

四、学生毕业后开题报告随同毕业设计（论文）一同在院（系）
归档。

湖南大学

毕业设计(论文)开题报告

(全日制本科生)

课 题 名 称 基于深度学习的短视频

版权保护系统

课 题 类 别 设计 ☒ 论文 ☐

专 业 、 班 级 信息安全 1801

学 生 林慧鸣

学 号 201808060101

指 导 教 师 廖鑫

二〇二三年 1 月

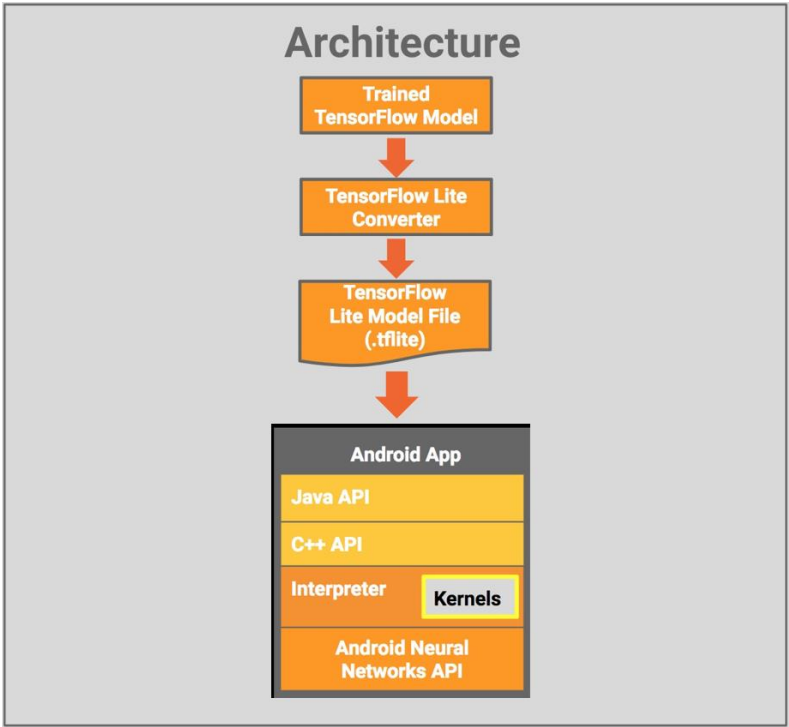
<p>一、 本课题设计（研究）的目的</p> <p>在移动互联网时代，短视频成为目前互联网中传播能力较广的媒体技术。然而短视频类新型社交平台盗版视频猖獗，版权侵害问题愈演愈烈，严重阻碍了短视频的发展，短视频版权保护需求日益增加。</p> <p>在版权保护过程中，传统的短视频版权保护系统对于短视频传输中的保护能力较差，不仅无法实时提取版权信息，而且常常造成加入版权信息后的短视频内容异常，或传播后的短视频无法准确提取版权信息。数字水印是一种用于保护版权的技术，目前，已有研究提出性能较好的基于深度学习的跨介质数字水印算法，但并没将这些算法应用在短视频的版权保护中。为了解决上述问题，本课题拟面向移动设备，结合深度学习数字水印技术，将版权信息嵌入视频中，旨在提供实时可靠的视频版权保护方案，研究并实现一个实时短视频版权保护系统。</p>
<p>二、设计（研究）现状和发展趋势</p> <p>数字水印是为保护数字媒体内容的版权而开发的主要技术之一。它将多媒体媒体内容所有者的信息或指纹隐藏在媒体内容中，通过提取这些信息可识别媒体内容的所有权，或跟踪数字媒体内容的分发情况。</p> <p>基于深度学习的数字水印方法由于其视觉上不可感知性高，鲁棒性强，已取得了不错的进展，能保证在视觉上不可感知，且可以对抗各种组合攻击（噪声、JPEG 压缩、裁剪等）。</p> <p>在短视频中加入数字水印可以确立版权所有者、认证多媒体来源的真实性、识别购买者、提供关于数字内容的其它附加信息、确认所有权认证和跟踪侵权行为。它在篡改鉴定、数据的分级访问、数据跟踪和检测、商业和视频广播、Internet 数字媒体的服务付费、电子商务认证鉴定等方面具有十分广阔的应用前景。</p> <p>大部分深度学习数字水印论文在针对个别攻击的鲁棒性上还不够理想，设计一个实用的鲁棒水印方法非常重要；针对不可微压缩的问题成为了一大难点，其解码的准确率还需要继续提升；在针对不可感知性的提升中，将传统方法的某些策略应用到网络中是一个值得研究的方向。</p> <p>当前，针对 StegaStamp 的研究比较成熟，内容分为自适应和弱自适应两类，弱自适应是在图表的背景嵌入，不触及前景区域，自适应包括区域嵌密和基于深度学习的整体嵌密。</p>

<p>区域嵌密如果使用传统模板的方法（如 Screen Shooting 中的方法），精准定位嵌密区域，提取时使用手动设计，由于 hand-crafted 是人为手动设计特征，依照人类视觉的特点对什么样的特征敏感，什么样的特征不敏感来提取图像中有区分能力的特征，因此提取出来的特征每一维往往都有具体的物理含义。深度学习模板的方法（如 DeepTemplate）采用纯学习方法，设计特征提取的 rule，一般是一个 model，人为设计的部分是 model 结构以及学习 rule，至于模型参数则需要通过学习得到，训练完成后得到一个具体的 model，而特征则需要通过这个 model 去对图像或视频进行提取，但是得到的特征往往无法解释每一维具体的物理含义。以及视觉重要性网络+区域嵌密的方法（如 Viscode）</p> <p>基于深度学习的整体嵌密，包括有噪声层，数据驱动，3D 光渲染，人眼闪烁等方法。</p> <p>StegaStamp 是基于深度学习，使用噪声层的扰动训练，具有端到端的框架和纠错抗干扰机制，我们可以对其深度学习模型进行改进，并部署到移动端中。</p>
<p>三、设计（研究）的重点与难点，拟采用的途径（研究手段）</p> <p>1、 平台搭建：</p> <p>框架使用 Tensorflow Lite 平台，pycharm 软件；UI 设计使用 Flutter 平台，idea 软件，语言使用 python，dart；Tensorflow Lite 和 Flutter 通过 tflite API 进行连接。</p> <p>2、 设计重点：</p> <p>设计的水印方法思想来源于 StegaStamp 的论文，训练好编码器，检测器，解码器的神经网络并构建模型，使用编码器用于单张图片水印信息的嵌入，使用检测器进行检测，解码器进行纠错并解码。在训练解码器的时候，模拟真实的图像质量退化模型对嵌入信息的图像做变换，检测器和编码/解码系统一起训练，使解码系统能够自动适应检测器的定位误差来代替手动的选择模拟噪声强度，最终达到解码系统的鲁棒性与图像质量之间的平衡。</p> <p>由于视频是连续的图像（图像序列）组成的，通过对图像数字水印的研究可以推广到将视频每一帧进行分解并嵌入信息（例如 python 的 opencv 可以将视频分割成图像）提取时按每帧图片提取的流程提取水印信息，进而实现短视频数字水印版权保</p>

护的效果。

3、功能实现：

使用 python 实现 StegaStamp 提出的数字水印算法，改进使其适用于视频文件，使用 tensorflow 训练好神经网络的模型，然后使用 Tensorflow Lite converter 将其转换为 Tensorflow Lite 模型文件(.tflite)。最后将这个文件在开发移动端程序的时候嵌入到程序的内核中去，这样就可以在安卓移动端实现嵌入水印和提取水印的操作。



4、需求测试：

利用案例测试水印信息的鲁棒性，例如增加对视频的压缩和屏摄等干扰；测试嵌入后视频与原视频的相似度以及提取水印的准确率；模拟真实案例测试水印嵌入以及检测流程，比如能否实现嵌入所有信息，能否实时提取水印信息等。

四、设计（研究）进度计划

- | | |
|--------------------------|-------------|
| 1. 阅读论文，熟悉相关知识与术语与所需要的技术 | 1. 01-1. 19 |
| 2. 尝试设计短视频版权保护系统并能够顺利运行 | 1. 20-2. 20 |
| 3. 尝试将系统部署到手机端 | 2. 21-3. 20 |
| 4. 完善系统并且进行相应的场景与需求测试 | 3. 21-4. 20 |
| 5. 撰写毕业论文并进行最后修改 | 3. 31-5. 15 |
| 6. 准备答辩 PPT 与相关材料 | 5. 16-6. 03 |

二、主要参考资料（参数）：

[1] Tancik M, Mildenhall B, Ng R. Stegastamp: Invisible hyperlinks in physical photographs[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 2117-2126

[2] .Liu J, Ke Y, Zhang Z, et al. Recent advances of image steganography with generative adversarial networks[J]. IEEE Access, 2020, 8: 60575-60597.

[3] Zhang C, Benz P, Karjauv A, et al. Udh: Universal deep hiding for steganography, watermarking, and light field messaging[J]. Advances in Neural Information Processing Systems, 2020, 33: 10223-10234.

[4] Fu J, Zhu B, Cui W, et al. Chartem: Reviving chart images with data embedding[J]. IEEE Transactions on Visualization and Computer Graphics, 2020, 27(2): 337-346.

[5] Zhang P, Li C, Wang C. Viscode: Embedding information in visualization images using encoder-decoder network[J]. IEEE Transactions on Visualization and Computer Graphics, 2020, 27(2): 326-336.

[6] Song K, Liu N, Gao Z, et al. Deep restoration of invisible QR code from TPVM display[C]//2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW). IEEE, 2020: 1-6.

[7] Chen K, Yi F, Jia J, et al. Real time robust Invisible Hyperlinks in Physical Photographs based on embodied AI platform[C]//2020 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). IEEE, 2020: 271-274.

[8] Deng Y, Jia J, Zhu D, et al. FaceCode: An Artistic Face Image with Invisible Hyperlink[C]//International Forum on Digital TV and Wireless Multimedia Communications. Springer, Singapore, 2020: 63-72.

[9] Jia J, Gao Z, Chen K, et al. RIHOOP: Robust Invisible Hyperlinks in Offline and Online Photographs[J]. IEEE Transactions on Cybernetics, 2020.

Li L, Bai R, Zhang S, et al. Screen-Shooting Resilient Watermarking Scheme via Learned Invariant Keypoints and QT[J]. Sensors, 2021, 21(19): 6554.

指导教师意见

签名：

月

日

教研室（学术小组）意见

院（系）意见

教研室主任（学术小组组长）（签章）：

月日

院长（教学主任）（签章）：

月日