|  |  |  |
| --- | --- | --- |
| 学号： | 22009290060 |  |
| 姓名： | 王舒贤 |

**《计算机安全导论》**

**课程报告**

|  |  |
| --- | --- |
| **学 号：** | 22009290060 |
| **姓 名：** | 王舒贤 |
| **班 级：** | 2203013 |
| **指导教师：** | 张志为 |
| **日 期：** | 2024/11/21 |

计算机科学与技术学院

概要

人工智能（AI）走进人们生活已经不是什么稀罕事，ai的滥用也是不可避免的，最近，网上出现了很多雷军骂人的视频…

正文

随着ai对我们生活的影响越来越深，使用ai来便利我们的生活也变得越来越常见。其中，ai声音作为应用技术比较成熟，使用门槛比较低的技术被广泛应用。人类的声音，作为情感表达和交流的核心元素，正逐渐成为人工智能技术模拟的目标。AI模拟人声音不仅在技术上突破了多项难题，更在社会、文化及伦理等层面引发了广泛的讨论。本文将从多个角度探讨AI模拟人声音的技术背景、应用前景以及由此带来的思考。

AI模拟人声音，通常通过语音合成技术实现。最早的语音合成系统，基于规则的拼接方式，将语音单元（如音节或词素）拼接成语音。随着深度学习和神经网络技术的引入，语音合成的质量和自然度得到了极大的提升。现在，许多AI语音系统已经能够模仿特定个体的声音，甚至在情感、语气和语调上表现得近乎完美。

目前，基于神经网络的语音合成模型，如WaveNet、Tacotron等，利用大量的语音数据进行训练，能够生成非常自然且富有情感的声音。通过模拟语音波形、频谱图以及声道模型，AI能够重建出一个人的声音特征，包括音色、节奏、语调、停顿等细微差异。这使得AI不仅能够模拟标准化的语音，还能够精准地模仿特定人的个性化声音。

“国庆期间上网被‘雷军’骂了整整七天”？“雷军”语音包，你是真的火了！据悉，这个假期，短视频平台上涌现了大量“雷军”的发言视频，涉及堵车、调休、游戏等热门话题，不仅言辞犀利，还频频爆粗口。这些视频无一例外都是通过AI配音生成的。目前，相关短视频已被平台陆续下架。

记得之前“Are you ok”火的时候，包括雷军在内，大家都很喜欢这种幽默风趣的作品，但这次的内容不一样了。“雷总，最近你怎么在骂人”“每次都是开屏暴击”，这些询问和讨论也在雷军的社交账号留言区下刷屏，对此，雷军回复了三个愤怒表情。不只是雷军，但凡是正常人，都不愿意和这样的虚假AI配音沾边。

这事直接反映出大家对玩梗的边界感认知，即“过度玩梗”，“低俗梗”，一般的语音内容比如有趣的调侃，科普大家可以喜闻乐见，但是加上“用小米SU7撞人”，“评价某某厂商产品低劣”就是在利用语音本人的身份恶意制作“低俗梗”，“烂梗”，或许部分人觉得没什么，只是在开玩笑而已，新的东西成不了大气候，但是合成的内容中，还不乏具有辱骂和诽谤性质的。这样的内容，即使再可乐再好玩，也改变不了其侵犯当事人肖像权、名誉权等正当权益的本质问题，是赤裸裸的违法行径。

可以创作的内容太过混乱，你要是拿它来朗读有色小说，这要是传到熟人耳朵里，会留下什么印象？找谁说清楚？今天我们调侃雷军，可当我们自己身陷其中，恐怕就笑不出来了

AI生成的假视频、假录音，可能只需要一个软件，甚至是几秒钟时间，造假成本可谓极低，同时，违法越轨成本也并不高。那在猎奇、流量和利益的驱动下，生成式AI被滥用，便是一个能看到的必然结果。若要扭转这一情况，必须要把生成式AI关进法律的“笼子”里，使其可管控、守规矩，存在于道德伦理可接受的范围内。

前不久，国家互联网信息办公室起草了《人工智能生成合成内容标识办法（征求意见稿）》，明确指出，人工智能生成合成内容标识包括显式标识和隐式标识，且不得恶意删除、篡改、隐匿标识。未对生成合成内容进行标识造成严重后果的，由网信等有关主管部门按照有关法律、行政法规、部门规章的规定予以处罚。

这种AI语音只是一个开始。科幻片中实时AI模仿语音降临时，你还能保护好自己吗？

我去了解了相关技术，主要是**GPT-SoVITS语音合成模型**

GPT-SoVITS是一款开源的[语音合成模型](https://so.csdn.net/so/search?q=%E8%AF%AD%E9%9F%B3%E5%90%88%E6%88%90%E6%A8%A1%E5%9E%8B&spm=1001.2101.3001.7020" \t "_blank)，结合了深度学习和声学技术，能够实现高质量的语音生成。其独特之处在于支持使用参考音频进行零样本语音合成，即使没有直接的训练数据，模型仍能生成相似风格的语音。用户可以通过微调模型，进一步提升其性能，以适应特定的应用需求。是一个相对而言体量较小，具备完整的图形化ui，学习门槛极低的模型，只需要约5分钟的声音原始数据，就可以获得效果不错的训练结果，训练过程很快，等待时间少，不容易出错。

上手门槛如此之低，带来了诸多伦理和社会问题。

**虚假信息的传播与误用**  
AI模拟人声音最直接的挑战之一是其在虚假信息传播中的潜在风险。通过模拟名人、政治人物或普通人的声音，恶意分子可以制作虚假音频，进行诈骗、传播假新闻或进行其他欺诈行为。由于声音是个体身份的重要特征，AI能够模仿他人声音的能力使得识别真假变得更加困难。

**隐私问题与授权**  
当AI可以模拟一个人的声音时，这个声音是否属于这个人本身？如果某个声音被未经授权地模拟，是否侵犯了个人的隐私权或肖像权？这引发了关于个人身份、声音版权以及如何有效保护个人权益的问题。例如，某人可以在未授权的情况下用AI生成一个名人的声音，这是否构成了对该名人声音的侵权行为？

**声音代替真实沟通的风险**  
随着AI模拟声音技术的普及，人们可能开始依赖机器合成的声音进行交流，尤其是在孤独或高压力的环境中。长期依赖这种非人类的互动方式可能会导致人与人之间的疏离，削弱人类社会中真正的情感联结。尤其在心理健康领域，虽然AI能够模拟安慰的语气，但其缺乏真实人类的情感和共鸣，可能难以为需要帮助的人提供深层次的情感支持。

**道德责任与信任问题**  
当AI开始模拟个体的声音时，相关的道德责任如何界定？如果AI生成的声音造成了伤害或误导，责任应由谁来承担？是开发者、使用者，还是AI本身？这些问题考验着我们对AI技术的信任和理解。尤其是在模拟人的声音涉及到敏感话题（如政治、法律等领域）时，这种技术可能会被滥用，进而影响公众对科技的信任。

小白兔在家里终于听到了妈妈的声音，可是，那真的是妈妈么？