

AttFaceMasker 人脸隐私保护专家

钟乐轩 冯玉琴 肖邦媛 冀星宇 蓝梦萍
桂林电子科技大学人工智能学院 广西桂林

DOI:10.12238/ems.v7i6.13830

[摘 要] 随着深度学习等人工智能领域的迅猛发展，人脸识别技术已实现了显著的突破。利用人脸属性来进行身份识别的技术得到了越来越广泛的应用，例如社区、学校等场所的门禁系统、银行柜台的身份验证、犯罪嫌疑人的侦察等。然而，利用人脸识别技术收集到的众多人脸数据，其中包含了用户的敏感信息，倘若这些信息不慎外泄，用户的隐私将受到重大侵害。本文基于人脸隐私的保护与人脸面部属性的修改，提出一种行之有效的人脸隐私增强框架——AttGAN 面部属性编辑框架，助力人脸隐私保护技术的发展。

[关键词] 深度学习；人脸识别；面部属性编辑

1 引言

深度学习等领域的快速进步极大地促进了人脸识别技术的发展。其中的生物识别系统积累了大量的面部图像数据，用于识别个人身份。然而，这些面部图像中蕴含着用户的敏感信息，一旦泄露，将严重威胁用户的隐私安全。面部图像中的面部特征（如发型、衣着、性别等软生物特征属性）容易被机器自动检测出来，并可能被用于其他商业用途，从而导致功能的不当扩展，或者与其他数据库匹配，引发隐私泄露等安全问题。

因此，提供可靠的技术解决方案来应对由于人脸隐私泄露而造成的风险、问题具有重要意义，这能够在保护个人的身份效用并保留主要的身份特征以保持个人身份用于支持人脸识别，与此同时保护人脸图像的属性隐私。

2 项目总体设计

AttFaceMasker 人脸隐私保护专家的框架包含三个核心

部分：编码器和解码器、基于目标图像的分类器与鉴别器、重建学习。其中，编码器将原始图像转换为潜在空间，解码器则在潜在空间的基础上加入目标属性或原始属性，进行解码并转换为图像。编码器与解码器的结合能够很好地实现对单张图片（单个模型）中多个属性的操作和编辑修改，避免了需要对大量图片（模型）进行训练以编辑各项属性来实现某一任务的问题。基于目标图像的分类器能够对解码器生成的目标图像进行多属性分类约束，从而规避修改编辑相关性极高的属性所造成的不可预测变化问题，保证属性编辑的相对正确性。此外，分类器的训练采用有监督学习。重建学习则基于潜在空间增加原始属性并进行解码，其目标是使潜在空间包含足够多的信息，同时让解码器通过潜在空间实现较好的重建。基于该框架，本项目希冀实现在图像的众多属性中，实现对目标属性的修改，抑或对目标属性的删除，与此同时保留大量的原始面部属性，以此来保护个人面部隐私。

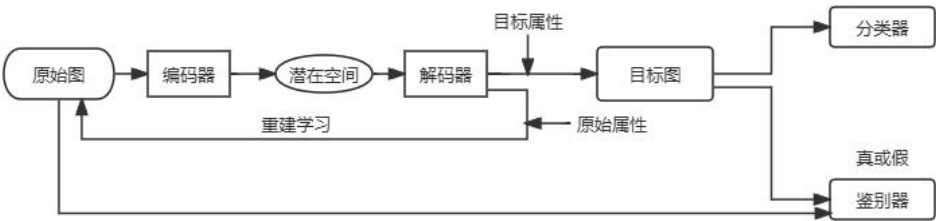


图 1 项目的框架图

3 项目创新性以及优势

本项目基于人脸隐私保护与人脸面部属性修改，创新性地提出了一种有效的人脸隐私增强框架，将编码器、解码器、

基于目标图像的分类器与鉴别器、重建学习等多种技术有机融合，构建了一个融合多种技术的框架。这种多技术融合的创新架构能够更全面、更有效地实现人脸隐私保护。与传统

方法需要对大量图片（模型）进行训练才能编辑各项属性来实现某一任务相比，本项目创新性地实现了在单张图片（单个模型）中对多个属性的操作和编辑修改，大大提高了人脸隐私保护的效率和灵活性。本项目兼顾了人脸隐私保护与人脸识别功能的平衡，不仅能够有效保护个人面部隐私，还能保留人脸识别系统的身份效用，具有很高的实用价值。在当

今信息高度发达的社会环境中，个人信息的保护尤为重要。该项目针对人脸隐私保护这一关键问题进行探索和开发，具有一定的前瞻性，能够有效应对并缓解数据信息泄露可能导致的安全问题，从而推动智能技术的发展和应用的拓展，随机编辑人脸属性样例如下：



(a) 增加面部皱纹数量 (b) 人物肤色变白 (c) 增加眼睫毛数量
(d) 唇色由红变白并增加胡子 (e) 人物肤色变暗

图 (a) ~ (e)

4 总结

在当今高度信息化的社会环境下，计算机视觉和图像处理、深度学习、多媒体等技术及其应用得以快速发展，人脸识别技术也因此得到了广泛应用。与此同时，随着人工智能应用的大范围普及，包括人脸图像在内的个人信息被大量采集与使用，导致这些个人信息的获取变得更加容易。然而，大量因人脸识别而收集的人脸数据中包含了用户的个人隐私信息，一旦泄露，将给用户的隐私带来重大风险。

探索和开发保护人脸图像隐私的技术显得尤为关键和紧迫，这不仅能够有效应对并缓解数据泄露可能导致的安全问题，还能促进智能技术的发展和应用的拓展，具有重大的现实意义。本 AttFaceMasker 人脸隐私保护专家采用的编码器、解码器、分类器、鉴别器和重建学习相结合的框架，可以保留众多面部属性并修改对应属性，保护用户的个人人脸面部隐私，同时保留人脸识别系统的身份效用。

【参考文献】

[1] 岳猛, 姚志强. 人脸隐私增强计算模型优化方案[J].

福建电脑, 2024, 40 (02): 17-21. DOI: 10.16707/j.cnki.fjpc.2024.02.004.

[2] 徐欣桐. 面向人脸识别的图像隐私保护方法研究[D]. 南京理工大学, 2023. DOI: 10.27241/d.cnki.gnjgu.2023.001523.

[3] 廖冰冰. 人脸图像隐私保护技术研究[D]. 长春工业大学, 2023. DOI: 10.27805/d.cnki.gccgy.2022.000033.

[4] 刘回归. 基于面部语义建模的人脸匿名技术研究[D]. 杭州电子科技大学, 2023. DOI: 10.27075/d.cnki.ghzdc.2022.000653.

[5] 何昱雯. 基于生成对抗网络的图片隐私保护算法研究与实现[D]. 北京邮电大学, 2019.

[6] 肖红梅, 王伟珍, 房媛. 基于生成对抗网络的女上装图像属性编辑[J]. 服装学报, 2024, 9 (01): 42-47.

课题项目: 广西壮族自治区 2024 年大学生创业实践计划立项项目“AttFaceMasker 人脸隐私保护专家”项目成果, 项目编号: 202410595421.