

实施满月,记者实测发现

由AI技术合成”



【实测】

使用4款深度合成技术应用软件体验AI换脸时
有的会弹出个人信息保护指引
有的想解锁高级功能先买会员

说起深度合成技术就不得不提最广为人知的AI换脸技术。

名为“zao”的AI换脸软件在2019年横空出世,其宣传卖点“仅需一张照片,出演天下好戏”,用户可以将经典影视角色或爱豆视频替换成自己的照片,并能分享到微博、微信等平台。该款软件的蹿红,使得AI换脸技术迅速攻占人们的视野。但在蹿红后不久,其用户协议上的“霸王条款”备受网友质疑,用户质疑点在于使用APP换脸时所上传的个人静态和动态图片是完全免费,不可撤销、永久、可转授权和可再许可的,相当于将肖像权卖给平台。时至今日,该款软件已销声匿迹,取而代之的是“一键换脸”“AI换脸秀”“FacePlay(秀脸)”等AI换脸软件。

此次《互联网信息服务深度合成管理规定》实施要点之一,是深度合成服务提供者提供合成成人声、仿声、人脸生成、人脸替换等服务可能导致公众混淆或者误认的,应当在生成或者编辑的信息内容的合理位置、区域进行显著标识,向公众提示深度合成情况。如今《规定》施行已满一个月,实施情况如何呢?新快报记者通过下载安卓、苹果应用商店下载量靠前的AI换脸软件进行实测。

记者下载了“一键换脸”“AI换脸秀”“FacePlay(秀脸)”“AI换脸”等四款深度合成技术应用软件,使用软件前均出现了大同小异的提醒:“视频换脸技术类似视频版PS技术,利用人脸图像和视频结合。人脸照片在视频合成后会立即删除,不会保留你的人脸照片和数据。”“请确保你使用的照片获得本人授权同意,严禁使用未获得本人授权同意的照片,如因照片未授权对他人肖像权造成侵犯所产生的法律责任由本人承担。”

测试的一款软件有免费使用次数,消耗了免费使用次数则需要进行付费。例如FacePlay应用程序可以进行初步体验,如果想解锁高级功能,需要支付17元的周会员,或者128元的半年会员。在体验AI换脸时,有个人信息保护指引弹出,其中明确“我们会遵循AI换脸隐私政策收集、使用信息,但不会仅因同意本AI换脸隐私政策而采取强制捆绑的方式收集信息;相册、文件读写权限均不会默认开启,只有经过明示授权才会在为实现功能或服务时使用,不会在功能服务不需要时通过您授权的权限收集信息。”在进行AI换装时,也有提示表明,系统不会保留人脸照片和数据,需确保使用的照片获得本人授权。

在记者测评的几款AI换脸软件中,只有2款软件“AI换脸秀”和“FacePlay”在生成视频后有明显的水印标识提示“视频由AI技术合成”。

【建议】

广州市政协委员、广州仲裁委员会仲裁员谭国戬:
视频发布平台要核实用户身份信息
对监测涉诈异常账号应当重新核验

成年人看到AI换脸的视频尚且真假难辨,对于中老年人来说无疑是摆在面前的“天堑”。根据中国互联网络信息中心发布的第50次《中国互联网络发展状况统计报告》显示,截至2022年6月,我国网民规模为10.51亿。网民的年龄结构显示,50岁及以上网民群体占比为25.8%,60岁及以上网民群体占比为11.3%,由此估算老年网民群体数量达到1.18亿人。此外,《报告》显示互联网应用也在持续发展。其中,短视频增长最为明显,截至2022年6月,我国短视频用户规模达9.62亿,较2021年12月增长2805万,占网民整体的91.5%。

提高风险意识和信息保护意识

老年人该如何提高防诈骗意识呢?广州市政协委员、广州仲裁委员会仲裁员谭国戬建议,日常生活中,市民应当积极参与防诈骗活动,了解防诈骗知识。同时,提高风险意识和信息保护意识,不随意填写个人信息,避免被不法分子利用。另外,要提高家中老人、小孩的防范意识,提醒他们在遇到类似情况时应和家人确认,切勿贸然转账。谭国戬说,倘若受骗,市民可求助于所在街道/镇司法所、公共法律服务站、村/社区法律顾问、律师事务所、12345政府服务热线等,也可及时向公安机关报案,向网信部门等主管部门举报诈骗信息。市民还可以及时向相关平台进行反馈和举报,使得诈骗信息获得及时的处理。另外,市民可通过诉讼的途径维护自身权益。

针对上文提到小芝的案例,北京浩天(广州)律师事务所合伙人张万隆则表示,“使用未经授权的视频进行AI换脸将涉嫌侵犯他人的肖像权或著作权人的信息网络传播权、著作权人的保护作品完整

权,相关权利人可要求平台下架视频并追究侵权人的法律责任,有权要求侵权人对自己赔礼道歉,并且赔偿因侵权行为给受害人造成的损失。”

应用商店要落实上架审核责任

谭国戬同时提到,虚假视频的发布责任应当归属于视频发布者和视频发布的平台。平台负有风险防控责任、侵权责任、未转通知和未采取必要措施的责任,平台承担核实用户真实身份信息、对监测识别的涉诈异常账号应当重新核验、对设立移动互联网应用程序办理许可或者备案手续、履行合理注意义务、协助公安机关办理电信网络诈骗案件依法调取证据提供技术支持和协助等责任。

谭国戬表示,建议深度合成服务提供者制定和公开管理规则、平台公约,完善服务协议,落实真实身份信息认证制度。采取技术或者人工方式对输入数据和合成结果进行审核,建立用于识别违法和不良信息的特征库。发现利用深度合成服务制作、复制、发布、传播虚假信息的,应当及时采取辟谣措施,保存有关记录,并向网信部门和有关主管部门报告。设置便捷的用户申诉和公众投诉、举报入口并及时反馈处理结果。

同时,应用程序分发平台如互联网应用商店等应当落实上架审核、日常管理、应急处置等安全管理责任,核验深度合成类应用程序的安全评估、备案等情况。网信部门和电信主管部门、公安部门依据职责对深度合成服务开展监督检查和防诈骗的宣传、教育力度,如在短视频平台设置安全弹窗,提醒用户在观看营销内容和涉及支付的视频时提高警惕。

●知多D

《互联网信息服务深度合成管理规定》当中明确指出,深度合成技术是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术,包括但不限于:

(一)篇章生成、文本风格转换、问答对话等生成或者编辑文本内容的技术;(二)文本转语音、语音转换、语音属性编辑等生成或者编辑语

深度合成技术

音内容的技术;(三)音乐生成、场景声编辑等生成或者编辑非语音内容的技术;(四)人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等生成或者编辑图像、视频内容中生物特征的技术;(五)图像生成、图像增强、图像修复等生成或者编辑图像、视频内容中非生物特征的技术;(六)三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术。



■软件弹窗提示“严禁使用未获得本人授权同意的照片”。



■使用“AI换脸秀”软件生成的视频,视频左上角有标识“视频由AI技术合成”。



■使用“一键换脸”软件生成的AI换脸视频截图。