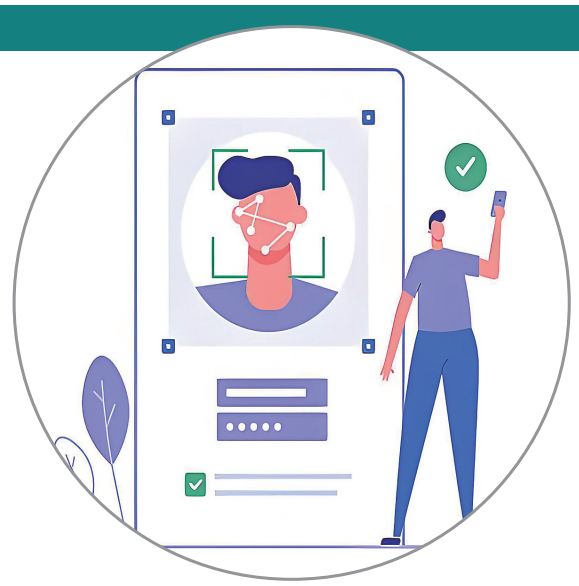
2025年4月24日 星期四
责任校对 王 曈
责任编辑 李昕也
技术编辑 崔 敏

手机非法植入『虚拟相机』 轻松骗过『人脸识别』

近日，一起“帮助网约车司机非法改装手机”的刑事案件再次引发了对AI技术滥用的关注——犯罪嫌疑人通过非法改装“虚拟相机”应用程序，再结合AI换脸技术，便帮助被封号司机绕过了网约车平台的人脸识别。

在主流的社交平台、短视频平台及电商渠道中，潜藏着大量宣称可“规避人脸识别”的灰色服务。值得警惕的是，这些服务商声称，“任何平台的人脸识别都能‘直接过’”。



通过为手机植入“虚拟相机”应用程序，替换本地手机相机，再利用AI换脸技术合成一段动态验证视频，当平台调取摄像头进行人脸识别验证时，屏幕中的人脸就自动被替换成了这段合成视频。

调查 “过脸教程”现身多平台 为灰色服务引流

“网约车远程刷脸教程”“替换系统相机”“网约车过脸”“苹果安卓均可，全平台通用”……在多个社交、短视频平台上，有着不少宣称可“规避网约车人脸识别”的账号。

这些账号所发布的视频演示了在滴滴、高德打车、货拉拉、哈啰顺风车、阳光车主等多个网约车平台上操作一款“虚拟相机”应用程序，从而通过人脸识别的过程。

例如，在一条短视频中，当手机摄像头被遮挡住的同时，点击进入名为“阳光车主”的平台人脸识别界面，人脸识别框内仍出现了逼真的人像视频，并顺利通过该系统。这些账号多留有联系方式，为进一步的“灰色服务”引流，在评论区，还有网友留言称可提供“代注册”服务，可以批量生成“合规司机”身份，帮助被封号司机“作弊”。

在淘宝、闲鱼等电商平台上，有大量店铺提供“虚拟相机工具”“硬改摄像头”相关服务，用于社交中的“虚拟视频”、电商“无人直播”等需求，在宣传中多以“虚拟相机插件、替换本地相机、硬改摄像头”等字眼出现。

进一步咨询发现，不少商家所售服务“鱼目混珠”，当被询问能否“破解平台人脸识别”时，其表示平台链接中虽没有，但可以换平台交易。

记者联系上了一位淘宝商家，咨询“破解人脸识别”服务，该商家声称，只需对手机进行刷机并远程操作安装一款“虚拟相机”应用程序，安装成功后，不仅是网约车平台，任何需要人脸识别的平台都能“直接过”，整个服务费用为1500元。

拆解 人脸识别“直接过”怎么做到的？

平台人脸识别究竟是如何被“技术破解”的？

中国信通院人工智能研究所安全治理部主任石霖表示，这主要是采取了一种叫作“注入攻击”的方式，原理是对手机终端“越狱”并安装“注入程序”，当开启人脸验证后，程序识别到与相机数据采集相关的关键函数后，使用工具将自定义视频或图像注入目标进程，绕过物理相机的数据流，对真实环境进行“隔离”，从而“欺骗”平台程序。整个流程需要当事人“配合”提供几张不同角度的人脸照片并深度伪造软件处理。

当前，破解人脸识别验证的黑色产业链频频现身，甚至许多软件代码已经开源。那么，是否真如服务商所说，该技术或令所有含“人脸识别”功能的平台陷入“破防”风险？是否存在数据泄漏风险？

石霖表示，单一的安全防范手段不足以“100%”应对攻击手段，平台通常采用多种手段交叉叠加的方式提升安全能力，也取得了较好的效果。比如：

目前银行常采用对App代码进行“混淆加密”的加固方式，让攻击者找不到注入的突破口；

再如，现在的智能手机上安全防护能力已经达到一定的标准，也会经常进行安全监测，如果发现手机上被安装了注入工具，或者手机“越狱”（通过技术手段解除厂商对设备操作系统的限制）了，就会提示相应的安全风险；

再配合“多因子认证”方式，除了人脸也需通过账号密码、短信验证码等方式开启认证。

此外，即便是手机端侧存在被破解风险，这类技术手段也很难入侵平台后台的风控系统，造成更大的数据泄露损失。

风险 规避人脸识别构成犯罪 需警惕AI换脸滥用

AI换脸技术在带来便利和机遇的同时，也衍生出新型法律风险。

近日，上海市静安区检察院办理的一起提供侵入、非法控制计算机信息系统程序、工具的刑事案件中，犯罪嫌疑人刘某就是通过非法改装11部手机，利用AI换脸技术合成动态验证视频，为被平台封禁账号的网约车司机提供规避人脸识别的服务，非法获利1万余元，被判处有期徒刑一年，缓刑一年，并处罚金5000元，没收违法所得及犯罪工具。

利用AI换脸技术破解平台认证，并非个案。2022年，广东五名男子使用AI换脸伪造“眨眼”“摇头”等活体视频破解人脸识别验证，7000条至60000余条不等，非法获利人民币40万元至120万余元不等，最终被宣判非法获取计算机信息系统数据罪。

广东金轮律师事务所合伙人褚亭丽律师表示，当前，AI换脸技术存在被滥用的现象，可能引发肖像权侵权、公民个人信息权益侵害等民事纠纷，甚至涉嫌构成诈骗罪、非法侵入计算机信息系统罪或本案所涉的提供侵入、非法控制计算机信息系统程序、工具罪等刑事犯罪。

据南方都市报