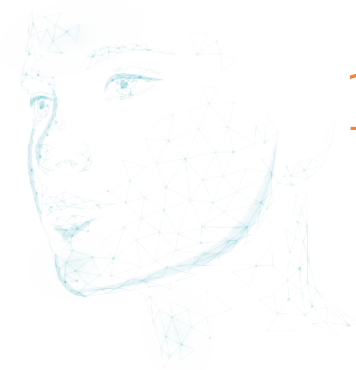
“秒变”小丑！记者体验“AI换脸”


记者体验“AI换脸”秒变“小丑”。记者 苗雪未 通讯员 李栋 摄



“AI换脸”火了！最近，中国香港警方破获一起诈骗案——某公司职员在参加一场“多人视频会议”后被骗走2亿港元。在这场会议中，只有受害者是“真人”，其他“参会同事”都是诈骗分子用“AI换脸”冒充的。网友们纷纷感慨：“这下，眼见也不一定为实了”。

“AI换脸”的门槛高不高，涉及哪些“黑科技”？它可能会导致哪些法律风险，受害者又该如何维权？除了“换脸”，AI还有哪些妙用？3月11日，记者来到宁波头部IT企业——国研软件股份有限公司（以下简称国研软件），探秘“AI换脸”背后的技术原理。

1 记者“秒变”小丑

“AI换脸”有多神奇？国研软件行业应用研发部高级工程师孙一帆向记者演示这项应用。只见摄像头“捕捉”记者的面部神态后，把记者的脸“秒变”为小丑的脸。由记者“换脸”而成的小丑，还会跟随记者的表情“开口大笑”。它也能把记者“换脸”成孙一帆本人，出现两位“孙一帆”同框的画面。

“这款‘AI换脸’应用来自Github代码开源平台，通过深度学习算法，精准识别视频中的人脸图像，并提取出眼睛、鼻子、嘴巴等关键特征，再将其与素材库里的图像进行匹配、替换、融合。只需上传你的一张照片，就能快速换脸，但效果不够逼真。要想提升效果，至少需输入4000-6000张照片。”孙一帆介绍。

这样看来，通过“AI换脸”进行视频会议诈骗，要么是“吃准”了视频会议的参与者无需频繁变换表情，只需一张照片“换脸”就能“糊弄”过去；要么就是骗子已“潜伏”多日，收集大量当事人同事的面部照片，以做到以假乱真。可见，保护个人信息安全迫在眉睫。

那么，我们该如何分辨“AI换脸”和真人？网传的“捏鼻子”等方法靠谱吗？

孙一帆告诉记者，这种做法可以参考，但并不绝对奏效。“目前的AI算法，都是基于完整的面部照片，‘捏鼻子’意味着面部有遮挡，如果AI训练时遮挡的数据不够，就可能‘露马脚’。但如果训练的数据充分，或采用更健全的算法，也可能破解这一痛点。这种情况下，最好询问对方彼此都知道的问题，以确认身份。”孙一帆说。

至于网友们关心的“是否会被‘AI换脸’拿来做刷脸支付？”孙一帆认为，目前还无需担心，因为现有的“刷脸支付”“刷脸门禁”，并不支持“AI换脸”所需的虚拟摄像头采集功能。但保护人脸数据等个人信息安全，仍需技术开发方、APP运营方、监管方等相关机构建立更严格的标准和规范。

2 “AI换脸”有哪些法律风险？

如今，“AI换脸”的应用层出不穷，有人用它“复活”已去世的亲人，以寄托思念；有人将它用于电商直播，以“提升主播颜值”；更有人拿明星照片“换脸”剪辑视频……然而，企业或个人在使用“AI换脸”时，稍有不慎就可能在违法的边缘“试探”。

浙江素豪律师事务所律师孙央指出，“AI换脸”可能涉及的法律风险有以下几种——

一是，著作权侵权风险。企业可能在已有的视频或图片中，将人脸进行替换。而其使用的视频或图片等素材，他人可能享有著作权，如果未经著作权人同意擅自使用这些素材，将侵犯著作权。

二是，肖像权侵权风险。《民法典》第1019条规定，未经肖像权人同意，不得制作、使用、公开肖像权人的肖像。如果没有经过他人同意，将他人的人脸用来制作短视频或其他作品，可能会侵犯肖像权。

此前，杭州物联网法院曾审理过一起因“AI换脸”APP利用深度合成算法侵犯他人肖像权的案件。原告楼某某是一位古风汉服模特，发现被告运营的“AI换脸”APP，使用了其拍摄的古风造型视频模板，供其他用户“换脸”生成新视频。最后，法院判决被告向楼某某赔礼道歉，并赔偿损失5000元。

三是，名誉权侵权风险。《民法典》第1024条规定，民事主体享有名誉权，任何组织或者个人不得以侮辱、诽谤等方式侵害他人的名誉权。如果在AI换脸视频中，将他人人脸替换的行为构成对他人名誉的贬损，可能构成对名誉权的侵犯。

同时，针对人脸信息被“盗用”至“AI换脸”应用等问题，《中华人民共和国个人信息保护法》为侵害人脸识别信息的行为，规定了罚款、吊销营业执照、损害赔偿等行政、民事乃至刑事责任，以增强对违规使用人脸识别技术、侵害人脸识别信息的行为的威慑力。

如果发现“AI换脸”侵犯了自己的权益，该如何维权？

孙央律师建议，受害人首先要保留证据，通过截图、证据保全等方式保存侵权视频或图片；如果是在某个平台上发现被侵权，可以向平台运营者投诉，要求删除侵权视频或图片；最后，可以向人民法院提起诉讼，维护自己的合法权益。

3 如何让AI“为我所用”？

技术的进步绝非“洪水猛兽”。要想让AI作为一种生产力工具，既需要完善的监管体系，也有赖于千行百业的从业者，加强合理使用AI的能力。

以国研软件为例，该公司将AI技术用于农贸市场的数字化改造，研发出能自动“识别”蔬果的智慧溯源秤，从而追溯每一件菜品的“前世今生”，助力宁波保障“菜篮子”安全。为提升工作效率，该公司IT技术人员还用上了一款“小研机器人”，既能辅助写代码，又能方便新员工快速入职。

“我们的‘小研机器人’对接阿里的‘通义千问’大语言模型，能运用Python、Java等多种语言帮忙生成代码，解放IT人士的生产力；我们还将企业的规章制度导入系统，如出差流程、报销流程等，方便大家一键查询，省去人力沟通成本。”国研软件政务应用研发部高级工程师毛校军告诉记者。

在宁波，“AI+行业”的案例层出不穷。比如，浙江九为健康联合华为打造九为盘古中医药大模型，借AI提升中医药研发效率；宁波薄言信息打造“垂直行业版ChatGPT”，为得力等本土企业提供“智慧升级版AI电商客服”；多家外贸企业运用AI跨语言和外商交流，增加接订单的效率。

毛校军表示，灵活使用AI的能力，或将成为未来人才的核心竞争力。

记者 严瑾 通讯员 李栋

央视报道“AI换脸”应用。 视频截图