2023年7月3日 星期一 策划:李婷 责编:余强 美编:孟宪东 TIANJINDAILY 天津日报

AI换脸拟声 规范迫在眉睫

最近一段时间,“AI”成为网络热词。从德国媒体用AI生成“舒马赫专访”内容并发表引发巨大争议,到“AI孙燕姿”一夜爆红,再到利用“AI换脸”10分钟诈骗400万元……随着人工智能进一步发展,原本用在影视和广告领域的“AI换脸拟声技术”被一些不法分子用来实施电信网络诈骗,网上甚至还有人专门出售“AI换脸拟声”软件和教程。规范“AI换脸拟声技术”,迫在眉睫。

■ 本报记者 韩爱青

现状

技术门槛变低 被滥用频现

近来,网络上一些热度较高的新闻似乎都与“AI换脸拟声”有关。一名男性特效师将自己的脸替换到影视片段中,生成跟女星亲吻视频;一名网络博主在地铁拍的日常生活照,遭不怀好意之人使用AI技术“一键脱衣”……因“AI换脸拟声”引发的侵权事件年来屡屡发生:去年年底,杭州互联网法院审理了一起因“AI换脸”App利用深度合成算法侵害他人肖像权的案件;歌手林俊杰曾因个人肖像被用“AI换脸”技术制作了大量“鬼畜”视频起诉短视频博主;有人利用“AI换脸”技术传播对演员刘昊然带有侮辱性的视频、截图。

除了引发侵权问题,“AI换脸拟声技术”还被一些不法分子用来实施电信网络诈骗,福州的郭先生10分钟被骗走430万元,安徽的何先生被骗245万元……我市尚未对外公布有利用“AI换脸拟声技术”诈骗的案例,但警方一直对外进行相关防骗提示。

“AI换脸拟声技术”究竟是一项什么样的技术?其适用领域是哪里?“在人工智能领域,AI换脸不算什么新鲜事。”天津科技大学人工智能学院副院长张贤坤告诉记者。这项技术最早可以追溯到2016年,当时一家名为DeepFake的网站发布了一款“DeepFakeLab”的软件,可以实现逼真的换脸效果。“AI换脸指应用人工智能(AI)技术,通过人脸特征建模,用深度学习的方法把人脸的部分特征复制到另外一个人的脸上,并使得后者看起来更像,相当于把一个人的脸换成另外一个人的脸。”张贤坤说,这项技术原来主要用于电影、电视和广告等领域,让其中的特效更加逼真,提高观众的观看体验。如有高难度动作需要替身时,可以先让替身实际参与拍摄后,再用“AI换脸技术”进行后期合成,这样一来,不仅简单方便,还能获得很好的拍摄效果。

张贤坤认为,随着人工智能技术的不断发展和完善,特别是计算机算力的提升,现在的“换脸”效果更加逼真,在电影、电视、广告和游戏领域得到了广泛的应用。近年来,随着深度学习等人工智能技术的快速发展,特别是生成式对抗网络GAN(一种深度学习模型)的广泛应用,AI合成的产品和服务越来越多,除了利用“AI换脸”外,还可以“换声”。技术门槛变低,便出现被滥用的情况。

记者在调查中发现,有不少可供免费下载的软件,这类软件一般都是有固定的视频或者图片模板,只要上传人脸照片便可轻松实现“换脸”。记者尝试在手机软件下载程序中搜索“AI换脸”,一下子搜索出四五十款。记者选择了一款有24万人下载的软件,从自己手机里随意选取了一张正面照,上传到软件给出的视频模板中,不到一分钟就自动生成换脸视频,毫无违和感,并且可以保存在自己的手机里、分享到社交平台上。如果还想体验高级功能,比如更多的模板、更快更好的效果,可以每个月花费10多元钱,解锁会员功能。

AI还可以合成或克隆声音。记者在电商平台上搜索“AI拟声”,有多家店铺提供服务。其中一家店铺写着“AI孙燕姿、周杰伦、林俊杰,AI克隆自己”。记者从店铺客服处了解到,花28元就能购买一款软件,安装在手机、电脑等电子设备上,再按照教程操作,就可以轻松将自己唱歌的声音AI合成歌手的声音,相似度达到98%,“非常简单,一学就会。”客服人员说。

天津师范大学法学院焦艳玲教授介绍,2019年,一款手机应用程序“ZAO”发布后一时风靡全网,用户只要将自己的照片上传至应用程序,就可以对影视剧中人物换脸,引发了是否侵权的争议。然而由于当时《中华人民共和国民法典》和《中华人民共和国个人信息保护法》均未出台,该应用程序是否构成侵权、违法的问题并没有定论,只是基于该程序存在保护用户隐私协议不规范、数据泄露风险的安全问题,被工业和信息化部约谈并要求整改。

而近期比较火的“AI孙燕姿”与应用程序“ZAO”的情况相似,都是借助人工智能生成新作品,只不过前者的目的是“换声”,后者的目的是“换脸”。两者都需要对人工智能模型进行信息“投喂”和训练,这就需要取得训练的素材,比如大量的人脸图像和个人语音。

“人脸图像和语音看似普通,却蕴含一个人独一无二的生物特质——人脸特征信息和声纹信息,这些都属于生物识别信息,可以永久和唯一地识别个人身份。”焦艳玲说,我国于2020年和2021年分别颁布实施《中华人民共和国民法典》和《中华人民共和国个人信息保护法》,两部法律都对使用生物识别信息进行了详细规定。后者明确规定生物识别信息为敏感个人信息,对此类信息的收集、存储、使用、加工等限定了严格的条件——只有具有特定的目的和充分的必要性,并采取严格保护措施的情形下才能处理此类信息,且处理时必须取得信息主体单独以及明示的同意。2021年,最高人民法院发布了《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》,对信息处理者违反法律、行政法规的规定或者双方的约定使用人脸识别技术,处理人脸信息、基于人脸识别技术生成的人脸信息所引起民事案件的审判进行了全面规定。对自然人声音的保护,依据《中华人民共和国民法典》第1023条,可以参照适用肖像权保护的相关规定。未经同意使用他人图像和声音进行AI创作,其行为已经构成了对个人生物识别信息的侵权,可以依据上述法律规范要求行为人承担侵权责任,这一点是没有争议的。如果在特定场景下实施“AI换脸拟声”,例如对不雅视频中的人物进行换脸,造成个人社会评价降低,还会构成名誉权的侵权。

另外,2022年12月,国家多部门联合发布的《互联网信息服务深度合成管理规定》,对我国境内应用深度合成技术提供互联网信息服务做出了全面规范。第六条规定:“任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律和行政法规禁止的信息,不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律和行政法规禁止的活动。深度合成服务提供者和使用者不得利用深度合成服务制作、复制、发布、传播虚假新闻信息。转载基于深度合成服务制作发布新闻信息的,应当依法转载互联网新闻信息稿源单位发布的新闻信息。”

近日,包头警方公布“和好友语音聊天10分钟被骗430万元”的案件,正是利用深度合成技术侵害他人合法权益的真实写照。根据《中华人民共和国刑法》规定,利用“AI换脸拟声”骗取他人财产的行为还构成了侵犯公民个人信息罪。2022年12月26日,最高人民法院发布指导性案例192号,明确使用人脸识别技术处理的人脸信息以及基于人脸识别技术生成的人脸信息属于《中华人民共和国刑法》所规定的“公民个人信息”。窃取或者以其他方法非法获取上述人脸识别信息,情节严重的,构成侵犯公民个人信息罪。

“在如此全面的法律规定面前,利用‘AI换脸拟声’实施违法行为的情况仍然屡屡发生,反映出核心问题并不在立法层面,而在于法律的执行层面以及公民的意识层面。”焦艳玲认为,加大对违法行为的预防和监管是目前首要的任务。同时,网络服务平台应尽责审查,通过提升技术手段,加大对违法视频的审查力度。公众则应注意对个人图像和语音的保存和保护,并加强对“AI换脸拟声”危害的认识,多渠道辨别视频人物的真实性。

调查

网售软件 就可轻易实现

出路

专家呼吁 首要加大预防监管

人工智能专家:

“AI换脸”识别软件将很快出现

那么该如何辨别“AI换脸拟声”视频中人物的真实性呢?张贤坤认为,“AI换脸拟声”技术被滥用,涉及人工智能技术的伦理问题。虽然“AI换脸拟声”如今可以做到以假乱真,但假的就是假的,通过计算机很容易就能辨别出来。例如,一般情况下视频是每秒24帧以上,这是人眼分辨的极限,高清视频可能达到每秒60帧,数值越高,视频流畅度就越高。“AI换脸”是在每一帧不同的位置切入人脸,由于速度快,人眼难以识别,计算机却可以进行图片比对,未来应该很快会出现多种识别“AI换脸”图片或者视频的应用软件。

在目前尚无相关软件可用的情况下,人们也可以靠关注细节来辨别真人和“AI换脸”假人。“我们都知道外人很难区分双胞胎,但是其家人是很容易认出他(她)们的,也就是说即使是双胞胎,如果仔细观察也有细微差别。至于‘AI换脸’的假人,我们可以通过对比原照片和换脸照片寻找是否有明显差异,也可以观察人脸的眼睛、嘴、鼻子等细节,例如,‘AI换脸’的假人脸部线条不够柔和、眼眶和嘴巴太大或太小、整体脸部比例不协调。另外,也可以通过慢进拉长视频间隔,发现不同时间点上画面间是否存在瑕疵来辨别真伪。”在张贤坤看来,“AI换脸”技术更加关注的是人脸位置,还可以通过视频前后背景等其他位置破绽识别真假。

提醒:

■ **如何防骗?**

张贤坤特别指出,一般来说“AI换脸”的假人牙齿边缘过于整齐,眼睛瞳孔颜色不一样,反射光源不一致;正常人一般2到10秒眨一次眼,每次眨眼用时0.1至0.4秒,但假人眨眼频率不正常;假人在视频通话时,视频会有跳动、闪烁的画面,通话不顺畅。

■ **如何避免被冒用身份信息去诈骗身边人?**

焦艳玲介绍,首要就是保护好个人信息。不轻易提供人脸、指纹等生物信息,尽量不在社交平台发布正面照片或者视频;不要把身份证、银行卡的照片存在手机里,不要轻易在社交软件上透露年龄、工作、个人所在地等信息,及时卸载和注销不常用的手机App。