2022.4.15 星期五
责编:杨成 美编:江佳锁 组版:丁亚平
现代快报+

合成技术频频伪造出逼真视频

多地现“变脸”诈骗，警惕你的脸被盗刷

一段视频、一段语音未必是真人拍摄或者录制。在你不知道的手机App后台、支付界面、门禁闸机，或许有人正在盗刷你的脸……去年以来，多地发生“变脸”诈骗案。记者调查发现，随着深度合成技术迅猛发展、落地场景激增，一些不法分子趁机牟利。音频、视频等合成技术滥用，对人脸、声纹、指纹等个人敏感信息保护形成挑战。

新华社发

合成动态视频一个2至10元 竟能注册手机卡、支付账户

近日，陈先生来到浙江省温州市公安局瓯海分局仙岩派出所报案，称自己被“好友”骗了近五万元。经过警方核实，骗子用了AI换脸技术，利用陈先生好友阿诚社交平台上先前发布的视频，截取了面部视频画面并进行了“换脸”，从而对陈先生进行了诈骗。

2021年4月，安徽省合肥市警方在公安部“净网2021”专项行动中打掉一个犯罪团伙，该团伙利用人工智能技术伪造他人人脸动态视频，为黑灰产业链提供注册手机卡等技术支撑。

在警方抓捕现场，几名犯罪嫌疑人正用电脑将一张张静态照片制作为人脸动态视频。模拟制作出来的动态人物不仅能做点头、摇头等动作，还可完成眨眼、张嘴、皱眉等丰富表情，效果极为逼真。

在嫌疑人的电脑里，警方发现了十几个G的公民人脸数据，人脸照片和身份证照片分门别类存放在一个个文件夹里。“身份证正反面照片、手持身份证照片、自拍照等，被称为一套。”民警介绍，成套照片被称为“料”，出售照片的人被称为“料商”，这些“料”在网上已转手多次，而“料”的主人却毫不知情。

犯罪嫌疑人马某交代，由于制作简单，一个视频价格仅为2至10元，“客户”往往是成百上千购买，牟利空间巨大。

近年来，类似案件在浙江、江苏、河南等多地发生。浙江衢州中级人民法院的一份刑事裁定书披露：张某、余某等人运用技术手段骗过支付宝人脸识别认证，并使用公民个人信息注册支付宝账户，非法获利数万元。

这些案件的作案流程颇为雷同：不法分子非法获取他人照片或有偿收购他人声音等“物料”，仅需少量音视频样本数据，便可合成媲美真人的伪造音视频，用来实施精准诈骗，侵害他人人身和财产安全，或销售、恶意传播技术换脸不雅视频等，造成肖像权人名誉受损。

网络“叫卖”合成软件教程 风险背后存技术漏洞、治理短板

据合肥市公安局包河分局网安大队民警王祥瑞介绍，前述案件中8名犯罪嫌疑人多为社会闲散人员，有的连高中都没有读完。他们按照网购教程下载软件，花几个月便“自学成才”。

记者在网上联系到一位售卖相关教程的卖家。卖家介绍，全套软件及教程售价有400元、800元两档，800元的为高阶版本，“过人脸成功率超高”。记者在演示视频中看到，照片上传至软件后，标注出五官位置，调整脚本参数，一张脸便动了起来。“五官参数随教程送上，照抄即可。”据介绍，这些伪造视频不仅通过率高，人工审核都难辨真假。

“目前公众对照片等静态信息易被篡改已有所警惕，但对视频、声音等动态信息内容仍持有较高信任度。”清华大学人工智能研究院基础理论研究中心主任朱军说，深度合成技术飞速演进，让“眼见不再为实”，破解身份核验的难度会越来越低、耗时将越来越短。

专家担心，尽管针对深度合成技术的识别技术不断迭代、检测手段持续增强，但依然没能跑赢“伪造”技术升级的速度。浙江大学网络空间安全学院院长任奎说，随着合成技术应用门槛的进一步降低，合成内容已模糊真实与伪造的边界。

北京智源人工智能研究院安全创新中心执行主任田天认为，新型伪造方法层出不穷，网络传播环境日趋复杂，检测算法存在漏洞缺陷等，反深伪检测难度越来越大。

法律规定相对滞后，也给不法分子留下可乘之机。中伦律师事务所合伙人陈际红说，目前法律规定，禁止利用信息技术手段伪造等方式侵害他人的肖像权，但技术如何使用算合理使用，哪些情形下应禁止使用等，没有具体规定；收集或收购个人声纹、照片，使用人脸、指纹、DNA、虹膜等个人生物信息等行为，在哪些范围内构成犯罪、将面临怎样的惩罚，需要司法裁判进一步给出明确指引。

规制合成技术滥用 别再让公众为“脸面”担忧

保护人脸、指纹、声纹等敏感信息，不再担忧信息“裸奔”损害个人隐私、财产、名誉等，是公众的共同期待。

我国首个国家层面的科技伦理治理指导性文件《关于加强科技伦理治理的意见》近日印发，凸显技术伦理治理的重要性紧迫性。在今年的最高法工作报告中，包括人脸安全在内的个人信息安全等多次被提及。

陈际红表示，打击“变脸”诈骗犯罪，应从技术的合法使用边界、技术的安全评估程序、滥用技术的法律规制等方面予以规范，提高技术滥用的违法成本。

中国工程院院士、信息技术专家邬贺铨提出，针对深度合成技术滥用现象，应以技术规制技术，利用技术创新、技术对抗等方式，提升和迭代检测技术的能力。

技术规制之外，针对技术滥用暴露的风险治理应当体系化、完善化。“要构建数据集质量规范、根据应用场景对相关技术进行风险分级分类管理，明确设计开发单位、运维单位、数据提供方的责任。”国家工业信息安全发展研究中心副总工程师邱惠君说。

专家提醒，针对花样翻新的“变脸”诈骗，公众要提高防范意识，不轻易提供人脸、指纹等个人生物信息给他人，不过度公开或分享动图、视频等；网络转账前要通过电话、视频等多种沟通渠道核验对方身份。一旦发现风险，及时报警求助。

据新华社