舟山晚报
2023年10月30日 星期一 责任编辑 陈海维 版式设计 张赟

警惕AI“深度伪造” 接陌生电话时建议先“变声”

专家：人体生物特征易被“移花接木” 电话、视频聊天时需加强防范与甄别

“以前我们说‘眼见为实’，但随着技术发展，不法分子的技术手段也在更新，造出‘假人说假话’，有时让人防不胜防，必须要注意鉴别和防范。”近日，于深圳举行的世界数字城市大会“生物特征识别技术应用论坛”上，国家特聘专家陈友斌教授在接受本报全媒体记者专访时谈到：“人脸识别技术已经落地各项应用，由此引发的个人隐私泄露等问题也日渐突出，人脸识别技术应用安全管理势在必行。”

AI换脸、声音合成 “好友”以假乱真骗走钱财

“如今，社会生活中的不少业务都可以在线上进行，金融方面如开户、开卡、理财、信贷；民生方面如申领社保、修改密码、开庭、办案；商务方面如谈判、签约、公证等，然而你有没有想过，屏幕上出现的那个人，是否真的是你以为的那个人？人工智能大时代下，这一点特别需要警惕。”陈友斌说。

前不久，包头警方就通报了一起利用AI实施诈骗的案件：福州市某公司法人代表郭先生10分钟内被骗430万元。据通报，郭先生的一位“好友”突然通过微信视频联系他，称自己的一位客户朋友在外地竞标，需要430万元保证金，且需要公对公账户过账，想要借郭先生公司的账户走账。基于对好友的信任，加上已经视频聊天核实了身份，郭先生没有核实就直接分两笔把430万元转到了对方指定的银行卡上。事后，郭先生拨打好友电话才知道被骗，原来不法分子通过智能AI换脸和拟声技术，伴装成好友对他实施了诈骗。

“不法分子用视频对讲的方式模拟受害者朋友的声音，看起来，人也是这个人，声音也是他的声音，但其实根本就不是他朋友所为。”陈友斌说。

无独有偶。2022年2月，有位陈先生到派出所报案，称自己被“好友”诈骗了近5万元。经警方核实，诈骗分子利用陈先生某好友在社交平台发布的视频，截取其面部画面后利用“AI换脸”合成，制造陈先生与“好友”视频聊天的假象骗取其信任，从而实施诈骗。

今年10月7日，国家金融监督管理总局北京监管局发布风险提示称，有不法分子非法获取个人信息，通过计算机算法仿真合成受骗者亲人、领导同事或公职人员的肖像面容与声音，冒充上述人员身份行骗；在获得受害者信任后使用事先准备好的套路话术向受害人发送银行卡转账、虚拟投资理财、刷单返利等诈骗信息，并利用视频通话，语音轰炸等手段进一步降低受害者的防备心，受害者往往在短时间内难以察觉异样，一旦听信诈骗分子的骗术并完成转账，对方便杳无音讯。

AIGC数字人？自然人？ 人体生物特征或被“深度伪造”

“不法分子通过AI换脸和拟声技术，伴装熟人实施诈骗。”陈友斌介绍，我国在人脸识别这一领域的应用排在世界前列，因而人脸识别的风险和隐私保护必须引起关注。

“在镜头前面的那个人，他是不是一个真实的自然人？人是不是真实的？证件是不是真的？人证是不是一致？需要远程核身的手段。”陈友斌介绍，出现在伪造图像或者伪造视频中，借助AI技术生成或者伪造的人称为“AIGC数字人”。它可以是真实世界不存在的人，也可以是对真实世界存在的人的伪造。而“自然人”是出现在真实图像或者真实视频中，且存在于真实世界的人。

据了解，目前在广深两地，生产和销售虚拟数字人的企业已达上千家，由AI技术创建的“数字人”具有高度逼真的外观和自然的语言交互能力，能够与用户进行实时对话互动，甚至达到“不仔细看看不出来”的逼真程度。

作为多年从事图像识别与人工智能领域研究的专家，陈友斌提醒：“人脸、声纹、指纹、虹膜、签名等是最常用的人体生物特征，即便是自然人，但是否他本人此时此刻就在那个地方，还是别人移花接木把他粘到那里去？也需要鉴别。”

陈友斌介绍，与传统技术相比，“AI换脸”的破坏力不仅在于“伪造”，更在于“深度”。“诈骗分子一般会先对公众在网络上发布的各类信息进行大数据分析，包括社交媒体上的个人数据、工作信息、人际关系等，研究他们的日常生活习惯、工作习惯、资产状况等，然后结合要实施的骗术，通过AI技术对人群进行筛选，从而确定要实施诈骗的目标人群，锁定诈骗对象。”

警惕声纹造假 接陌生电话“变个声音再说”

陈友斌介绍，“深度伪造(Deep Fake)”是一种基于深度学习的多媒体篡改与合成技术，主要包括图像、语音、视频和文本的伪造及篡改等，在视频通话、视频会议中，模仿目标人物去欺骗另外一个人。“深度伪造发展得非常快，这个技术最早用于好莱坞拍电影时去模拟一些现实中拍不到的部分，后来被不法分子所利用，让人脸图片的嘴巴动起来、眼睛眨起来，还能摇头晃脑的，还有换脸等，现在这类模型非常多。”

他告诉记者，这种深度伪造技术在不改变身份的情况下，可以对人脸进行年龄、性别、种族的改变，并且操纵口部或者表情；还可以通过人脸迁移、交换、堆叠等方式，以“换脸也换表情”“换脸不换表情”等多种方法混合来改变身份。“实时交互式的深度伪造将合成映射到现在的时刻，针对实时交互式的应用场景，如在线会议中使用虚假身份窃取信息或扰乱秩序，或在视频通话中模仿目标人物去欺骗另一端的用户等。”

陈友斌提醒：特别需要注意的是，声音的信息也可以通过提取“声纹”来进行造假。

什么是“声纹”呢？陈友斌介绍，人类语言的产生是人体语言中枢与发音器官之间一个复杂的生理物理过程，发声器官——舌、牙齿、喉头、肺、鼻腔在尺寸和形态方面每个人的差异都很大，所以任何两个人的声纹图谱都有差异。现在大家都常接到很多陌生人打来的广告电话，殊不知在和陌生人说话的过程中，不知不觉就把自己的声纹泄露了。

“不法分子可能通过不同的人向你打电话‘轮番轰炸’，也许他们的目的根本不是为了推销，而是获取你的声纹、生活习性和社会关系，进而实施诈骗。”陈友斌介绍，语音时长会影响声纹识别的精度，有效语音时长越长，算法得到的数据越多，精度也会越高。

因此，他提醒：“不熟悉人工智能科技的老年人尤其需要提高警惕，包括年轻人也一样，接到陌生电话千万不要多说话，实在必须说话时可以捏着鼻子、变个声音跟他说，否则经过一段时间的数据学习，不法分子就可能会利用你的声纹信息和讲话习惯等，合成你的声音、换成你的脸，在你的社交网络里进行诈骗。”

细心留意AI伪造“蛛丝马迹” 多渠道确认不轻信视频内容

如何防范AI深度伪造诈骗？陈友斌提醒：“如果这个人跟你很熟，你跟他多交互对话几次，就可以发现问题了。”

据了解，以银行业务为例，是需要通过图像、语音、自然语言处理再加上交互对话来完成金融业务，最大限度减小风险。而普通人也可以通过多种核对的方式来发现AI深度伪造的“蛛丝马迹”。

他介绍，因为人脸合成的素材大多使用的是睁眼照片，所以“缺少眨眼”可以被视为是合成视频的“特征”之一，此外合成视频还可能存在口型和发音不同步、情绪不符合、某个地方不自然或者不衔接、牙齿和嘴唇纹理不清，耳朵不对称等情况。AI拟声、AI换脸包装作伪后的通话，虽能逼真地模仿原始人物的语言和行为，但仍充满破绽，例如眨眼频率过低、眼睛移动不协调、面部表情不自然、语句不连贯等——这些都是“数字人”的特点。

以下防范口诀比较好记：电话回拨再确认，视频不可轻易信；私人问题记得问，答不上来不可信；眨眼能破AI面孔，关键时刻要常用。

据悉，国家网信办8月8日发布的《人脸识别技术应用安全管理规定（试行）(征求意见稿)》，也从公共场所、经营场所、可能侵害他人隐私的场所等作出了要求。

有关部门也提醒：要提高信息保护意识，特别警惕需要录入个人信息的非正规软件；在开启“定位服务”、输入身份证号或是录入“人脸识别信息”“指纹识别信息”等个人生物信息时一定要慎之又慎；发现APP过度、强制收集个人信息时及时向有关部门投诉举报。此外，妥善设置个人社交账户的浏览权限，不过度公开或分享涉及个人信息的动图、视频等，对不明平台发来的链接提高警惕，不轻易向陌生人开启手机屏幕共享。

据广州日报