你还敢随便发照片吗？

“刷脸时代”如何保护我们的脸

央视3·15曝光人脸识别滥用

如今，我们已进入“刷脸”时代。购物刷脸支付、手机刷脸解锁，进小区时刷脸开门……越来越多的事情可以用人脸识别技术来解决。

刷脸验证是否都能够通过换脸视频进行？换脸技术是否存在安全隐患？人们需要注意哪些？

□东方今报·猛犸新闻记者 周兰 ■见习记者 刘旭/文图

换脸视频通过刷脸验证？专业人士：聚识率和误识率数值不同

为什么地铁和门禁的刷脸验证用换脸视频即可通过？伴随着AI技术的发展，用户的隐私和数据保护有哪些要求？人们使用刷脸设备应该需要注意哪些地方？带着这些问题，记者采访了全球移动互联网企业专业人士，关于AI换脸和刷脸验证，该专业人士进行了回答。

当下人们热衷的换脸视频及换脸软件，都属于AI换脸领域。其技术已达到普及，基本操作为用户上传照片，将静态的图片生成动态的表情，或是将相貌融合到影片中，这些都是通过人像的切割、定位、识别、云端处理、视频帧截取以及学习生成最终实现换脸。APUS技术专家表示，人脸代表了一个人的身份即生物特征或是社会属性的身份，如果换张脸，可能侵犯肖像权、诽谤等不安全因素会发生。

技术专家介绍，从最早的美颜，到现在换脸可能更多地运用在漫画脸或者虚拟人物中，以及安防领域。关于换脸视频通过刷脸验证，是因为刷脸验证在不同场景和领域的要求分为不同等级。人脸识别需要采集人脸到数据库，通过与模型库里的人脸进行识别和匹配，从而定位并反馈结果。而采集的人脸模型库分为人口库和公安库，比如小区门禁的人脸采集为人口库，金融支付是公安库，公安库的照片具有一定要求，不可外部传播。此外，人脸识别技术在不同领域是不一样的使用场景，在民生领域有两个数值，分别为聚识率和误识率。聚识率即当机器识别到不是本人后，后面的动作将停止。误识率即识别错误，将A识别为B。“这两个数值在金融和民生领域是不一样的，民生领域对误识率要求更低一些，我了解到的情况是民生领域做得好的误识率能够做到一万次可能就错一次，达到万分之一。比如地铁刷脸检票，如果聚识率过高的话会造成排队拥堵。而在金融领域，聚识率的数值会高一些，一旦识别错误，损失会很大。一般在3个点或5个点以下就可以。不同领域系数不能一概而论，每家算法不一样的话数值也不一样。”技术专家表示，人脸识别除了识别人像外，还会做活体检测，方式很多，有根据指令做出动作比如点头眨眼等，还有通过红外线传感器、3D光等识别是平面的照片还是立体的脸部形态，3D结构光严格意义上安全性更高些。

AI换脸流行背后存在隐患 你还敢随便发照片吗？

AI换脸给人们带来欢乐的同时也造成了隐患，生活中也能找到相关案例。据相关报道，南京女子小李的大学同学通过QQ向她借钱3000元，对方打过来一段只有四五秒的视频电话，小李看到确实是本人后便放心转账。她在第二次转账时发现异常，再次拨通对方电话才得知同学账号被盗，警方判断那段视频很可能被人换了脸。还有杭州“人脸识别第一案”等。

此外，AI换脸还涉及肖像权，同时信息的泄露也存在一定的社会风险。APUS技术专家说，“换脸”有风险，核心个人信息被泄漏，甚至被贩卖，威胁财产安全和人身安全。

制作换脸视频首先需要用手机号动态验证码进行验证登录。用户如果想要下载或分享换脸视频，则需要进行验证确认所使用的照片的确是用户本人，而验证的方式则是在摄像头前进行眨眼、扭头、张嘴等指示动作。本质上已经搜集了用户面部的识别信息，而这是一个用户最核心的个人信息。个人信息一旦被比对之后，如果落到坏人的手里，有可能涉及财产安全和人身安全的问题。如果在支付场景，比如现在很多银行APP和支付宝或微信，用户为方便直接脸部扫描，同样也需要个人的面部信息。

在国内和海外，人们对用户隐私和数据保护都有很强的诉求，AI对数据保护和用户隐私有哪些要求？对此，技术专家认为，数据保护和用户隐私是一个对所有行业都适用的领域，所有公司不要超限搜集用户隐私，用户有知情权和删除的权利。目前国家法律法规还不够完善，因此在提供人脸、指纹等隐私数据采集的时候一定要清晰地知道被用到哪里，以及采集方的公信力，避免人的信息用到不法之地。目前国家的相关法律也在逐渐完善的过程中，网络安全、消费者权益等法案的出台以及网安等监管机构也在不断地采取措施等。

■律师分析

有关换脸视频的做法 可能涉及侵犯公民个人隐私

河南春屹律师事务所主任张少春律师表示，首先，有关换脸视频的做法，可能涉及侵犯公民个人隐私，《民法典》第一千零三十二条规定自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。其次，《刑法修正案(九)》增设帮助信息网络犯罪活动罪，针对明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通信传输等技术支持，或者提供广告推广、支付结算等帮助的行为独立入罪。也就是说，如果商家给犯罪分子提供类似换脸视频，涉嫌协助作案，可能被以该罪追究刑事责任。

■链接

个人信息保护法 将对人脸识别等作出专门规定

人脸识别等新技术的应用和发展，给个人信息保护带来许多新挑战。

在今年的“3·15”晚会上，多家商户被曝光在未告知或征得同意的情况下获取客户的人脸识别信息进行商用，而整个采集过程中，消费者都“蒙在鼓里”。这样一来，也就难以举证存在违法收集、使用个人信息的情形，给消费者维权带来难度。

即使确定存在违法行为需要删除个人信息，如何确认是否彻底删除？个人信息案件的执行，也将是留给未来的一个课题。

数字经济时代，技术应用如何在与消费者选择权的平衡中寻求边界，这是人脸识别技术应用中更为核心的问题。值得关注的是，个人信息保护法正在制定中，对处理包括人脸等个人生物特征在内的敏感个人信息作出专门规定，要求只有在具有特定目的和充分必要性的前提下，方可处理敏感个人信息，并在事前进行风险评估。希望个人信息保护法能够对个人信息进行全方位保护。

如何防范AI换脸诈骗？

面对利用AI人工智能等新型手段的诈骗，我们要牢记以下几点：

01 多重验证，确认身份

目前，AI换脸难以肉眼区分。因此，在涉及钱款时，尽量通过电话询问具体信息，确认对方是否为本人。

02 保护信息，避免诱惑

加强个人信息保护意识，对于不明平台发来的广告、中奖、交友等链接提高警惕，不随意填写个人信息，以免被骗子“精准围猎”。

03 相互提示，共同预防

做好家中老人的宣传防范工作。提醒老年人在接到电话、短信时，要放下电话，再次拨打家人电话确认，不要贸然转账。

“讲课、看片、答辩、点评、体验”五步教学法，消防小哥哥为幼儿上了一堂“走心”安全课

□东方今报·猛犸新闻首席记者 夏萍 实习生 王晓娜

为切实做好幼儿园消防宣传教育工作，全面掀起幼儿园消防安全教育高潮，不断提升广大师生应对火灾事故的能力，4月13日，商丘市民权县消防救援大队工作人员走进辖区幼儿园组织开展消防安全演练，为辖区幼儿园创造一个稳定的消防安全环境筑起坚固的防火墙。

演练开始前，民权县消防救援大队工作人员首先用通俗易懂的语言向小朋友提问：“如果发生火灾了，小朋友们要怎么报警？”“打电话，119！”“如果家里垃圾桶起火了，但爸爸妈妈都不在家，你会怎么办？”“我会把没用的衣服弄湿盖到火上，然后把火踩灭……”小朋友们都非常积极，现场氛围十分活跃。

为了让小朋友们高效、牢固地学懂、学会消防安全知识，消防工作人员分别针对幼儿、教师不同的社会身份进行播放，尤其是幼儿观看的视频，根据幼儿的年龄特点，贴近生活并结合本园实际，精心挑选出合适的教育片。片中的典型案例、实际场景的生动演示深深吸引了幼儿。宣传人员还以“讲课、看片、答辩、点评、体验”五步教学方法，对如何有效预防、如何快速报警、如何安全逃生、如何正确灭火等“四类重点”内容进行言传身教，让小朋友熟练掌握火灾预防、自救逃生等基本知识和技能。之后开展的消防安全逃生演练活动达到了预期的效果。①

主编：王栋梁 责编：徐战方 美编：康永红 版式：朱永华 校对：刘天保