2022年7月29日 星期五 齐鲁晚报

“骗子用假人脸盗刷女子数十万”“滴滴违法收集用户个人信息(包括人脸识别信息1.07亿条)被罚款80.26亿元”……最近,与人脸识别有关的话题频频成为热点。在“刷脸”越来越普及的今天,这些案例不禁令人深思:我们进行人脸识别是增加了额外的保障,还是不必要的安全隐患?针对这个问题,作为相关领域内的专业学者,重庆邮电大学高新波教授对人脸识别技术过去的发展历程、当下如何应对破解和挑战、未来将如何发展等作了详细介绍。

银行人脸识别系统被攻破,漏洞如何补?

专家:可采用『可见光+红外』双模摄像头或者多模验证方式来弥补

不法分子利用“换脸”攻击人脸识别系统

据高新波教授介绍,目前投入应用的人脸识别系统的图像采集方式有两种,一种是上传二维图像到系统,系统在特征空间里通过比对该图像和系统中注册的人脸图像以作识别。这种方案较为简便,但它的漏洞在于任何人使用符合条件的二维人脸图像,都可以被认证成功。例如,2019年就有几位小学生用打印的照片,“破解”了丰巢快递柜的刷脸取件功能。

所以,像银行这样的金融单位就会使用第二种人脸采集方案,即采集人脸图像的同时进行活体验证,以确保验证者为真人,防止他人恶意盗用照片。具体来说,就是要求采集人脸信息期间,用户按指令做眨眼、张嘴等动作。

活体检验的一大漏洞在于,系统假设这张脸和活体属于同一个人。如果李四带上了张三的面具,人脸识别系统检测到了张三的脸,同时李四完成了活体检测所需的动作,这种情况下系统就无法识别这个“本我”其实是李四而不是张三。此前有新闻报道,斯坦福大学的研究者发明了通过软件进行表情移植的“换脸”技术。最近的新闻中,不法分子就是利用类似的“高科技”来攻击人脸识别系统,盗刷银行卡的。

出现这样的漏洞,我们应该如何应对?

高新波介绍,我们可以采用“可见光+红外”双模摄像头的识别方式,即以可见光检测到人的表观,以热红外探测人脸的热量分布。只有光学人像和热红外温度分布图皆与个人保持一致,才能通过身份的辨识。这么一来,即使有人使用软件换脸、戴面具或长得相像,也无法冒名顶替了。

再者,也可以采用双模或者多模的验证方式,在人脸识别之外,加上虹膜、指纹、指静脉、掌纹、声纹等不同角度的验证方式,这样至少能够弥补下单一识别技术的漏洞。

关于有些面貌相似的人(如双胞胎)可以互相进行人脸认证,高新波教授说,理论上,识别面貌相似的人会增加识别难度,降低准确率,但并非无法做到。现实中那些长得十分相像的人,他们的父母或者熟悉的人仍然能分辨出来,说明这些面孔还是有区别的,人工智能肯定也可以识别出来。我们需要做的是加强对系统的训练,如采集大量的双胞胎人脸数据作为训练样本,让神经网络训练时专门把他们区分开,加大识别力度。

视频监控“匿名化”可以保护个人隐私

有关人脸信息被泄露的新闻,引起了大众对个人隐私安全的担忧。我们如何更好地保护相关隐私呢?

高新波说,这是个很关键的话题,大数据隐私保护是我们始终在思考的研究方向。最近在做一个保护个人隐私的视频监控系统,即在视频监控里实现“匿名化”。匿名化的方案有两种,一种是系统对人脸做变形处理,处理后的面孔人类无法辨认,只有机器仍可识别(A站在镜头前,电脑记录下来的却是不存在的Z)。通过如此“捏造”匿名人脸,可以保护隐私。

另一种是“换脸”,即在数据库内造出一个和现有人脸都有差距的面孔替换某个人,然后把原有的人脸用水印等方式嵌入其中。当需要追溯某个人的时候,通过技术就可知道这个人是谁;一般的系统没有这个技术,他们所能看到的就不是本人了。

那么,有方法可以让人能识别而机器不能识别吗?

高新波说,现在有一类新的技术叫做“对抗学习”,即在脸上贴特殊的贴片,干扰机器识别,这些贴片被称为对抗样本。如果将来要保护个人隐私不被过度采集的话,可能会应用贴片一类的东西,一旦我们贴在脸上,电脑、监控等就不能识别了,这个技术现在也有人在做。而且,这些贴片可以设计得比较小,方便现实生活里其他人辨认,只有电脑无法辨认。

为什么贴个东西电脑就无法辨认?因为人工智能的“可解释性”很差。换句话说,我们只知道它们能识别,但它们到底怎么识别却难以言说,因为它们所“深度学习”的,是神经网络设计出来的“特征”,人类根本无法理解这些特征。所以,科学家发现,有时在一幅图上添一点东西,电脑便难以识别,所以我们可以利用这个特点来拓展对抗样本的用途。

其实,人脸识别领域中,值得研究的地方还有很多。但保护隐私是目前最关键的问题。归根到底,我们还是希望科学技术被用于造福人类,而不是用来制造麻烦。

专家说法

应规定哪些单位有权进行人脸采集和识别

我国个人信息保护法中,人脸信息被列入生物识别信息的一种,被当作敏感信息进行保护。然而,有法学界人士认为,现行个人信息保护法对较为特殊的人脸信息没有单独的保护措施。人脸作为长期外露的一项生物特征,极易被获取,应加大保护力度。

2020年,山东济南、天津等地出现售楼处安装监控探头,提取并识别到访客户人脸信息的事件之后,一些看房者被迫戴头盔看房,以保护人脸。彼时,人脸信息的安全问题引起了诸多人的警觉。

清华大学法学院教授劳东燕一直认为,有必要将生物识别信息单独立法予以保护。“现行法律将人脸信息的特别保护主要寄托在个人同意环节上,这意味着,个人在知情同意后就要承担一切后果。但是,作为个人,可能根本不清楚同意后要面临怎样的风险和后果;此外,很多场景下,人们是被迫同意的,如果不同意,就无法正常使用服务。显然,不应该让个人承担全部的风险与责任。”劳东燕说。

中国政法大学传播法研究中心副主任朱巍则认为,人脸信息作为生物识别信息的一种,在个人信息保护法和民法典中都已有明确规定,人脸信息的保护原则,与其他个人敏感信息所遵循的原则没有不同,个人信息主体享受的权利也是一样的。“立新法的意义不大。更重要的是由有关部门制定出详细清单,规定哪类单位、在何种场景下有权进行人脸采集和识别。我认为,现在离对人脸信息前端采集设备进行重新登记、备案和审批的工作,已经不远了。”朱巍说。

扫码下载齐鲁壹点
找记者 上壹点

编辑:彭传刚 美编:继红 组版:侯波

延伸阅读

系统六度被“撞开” 这个责任谁来担

近日,一起事关人脸识别的一审判决引发社会关注。此案中,李某接到一通自称是警方打来的电话,在对方提供的网站上下载了两个App,又按对方要求到银行办了一张借记卡,并向该卡转账40余万元。当李某发现卡上的钱被转走后,才意识到上当了。李某认为,在其受骗过程中银行也有一定责任,遂以“借记卡纠纷”为由将银行告上法庭。

一审法院认为,李某在受骗过程中,操作存在明显过错,而银行完整履行了人脸识别、手机验证码确认和人工电话确认的义务,判其无责。

判决一出,引发了各界人士的讨论。

值得注意的是,此案中,李某的人脸信息被诈骗者轻易获得,并成功“撞开”人脸识别防护系统达6次之多。

人脸识别还安全吗?

2021年6月19日10时30分,身在北京的李某接到自称“陈警官”的电话,称她的护照在黑龙江省哈尔滨市涉嫌非法入境,要求李某向哈尔滨公安机关报案。“陈警官”确切知晓李某的身份证号码,使李某信以为真。随后,电话被转接到自称是哈尔滨市公安局“刘警官”的手机上。“刘警官”提供的网址显示,李某涉嫌一桩反洗钱案,通缉公告上李某的身份证号和户籍信息均准确无误。

为了“洗清罪名”,李某按照“刘警官”的要求,下载了“公安防护”和“瞩目”两款手机应用。在“瞩目”上,李某与“刘警官”共享了手机屏幕,以“确保”是本人操作。在“刘警官”指导下,李某设置了呼叫转移和短信转发,将自己手机来电和短信都转移到“刘警官”的手机上。

“刘警官”以“清查个人财产”为由,要求李某办理银行卡。李某在附近银行办理了借记卡,同时开通了网上银行和手机银行,随后将个人积蓄转到新办的借记卡上,共42.9万元。

察觉出不对的李某登录手机银行发现,借记卡中的存款不翼而飞,随后向公安机关报案。民警调查时发现,诈骗者在转账过程中,6次“撞开”人脸识别系统,6次操作均显示“活检成功”。

“可能是活化软件。”一位曾参与某国有商业银行人脸识别安全验证项目的人士说,在拿到一段人脸录像后,用活化软件对人脸进行建模,有可能“骗开”人脸识别系统。“在录像中,受害者极有可能已经做出过眨眼、张嘴、摇头等人脸识别系统经常要求受试者做出的动作。”

银行应承担什么责任?

李某一案中,一审判决银行无责,引发了一些不同意见。李某的爱人马某是此案中李某的代理人。马某在银行系统工作,他认为,银行定下的“人脸识别+短信验证码”的验证模式,其目的是确保由用户本人亲自操作转账。李某在完全不知情的情况下,被诈骗人员从账户中转走钱,银行应当承担保管不力的责任。

清华大学法学院教授劳东燕对记者表示,银行完全无责的说法,她也不认可。劳东燕认为,去银行办理存款等,如果不同意采集人脸就办不了相应业务。“也就是说,人脸识别是银行引进的一套系统,银行和科技公司是风险的共同制造者,当然应当承担一部分责任。此外,从预防的效果来看,让银行承担一部分责任,有助于倒逼金融系统提升安全等级,查补漏洞。”

一审法院在判词中称,李某在受骗过程中“过错明显”。对此,有人认为,这是一起典型的电信诈骗案,银行和个人储户都没有过错,个人储户只是受害者。朱巍告诉记者,人脸识别并不是绝对安全,诈骗者和守卫者都在发展之中,不能认定银行有过错;但他同时认为,如果说个人储户“过错明显”,也不成立。“个人储户因看到对方掌握自己准确的身份证号和户籍信息,才信以为真,这与前一段时间一些存储个人信息的服务器被攻破有关。”朱巍坚持认为,储户是受害者,不是过错方。

上述银行人士告诉记者,“活检”是为了区别真的人脸和仿制品,如果诈骗者通过对李某的人脸信息建模,骗开识别系统,且骗开了6次,那“活检”就形同虚设。“也许在法律上,银行使用短信验证码和人工电话等多种途径进行身份验证,已尽到义务。但在技术上,‘活检’这一关的漏洞还是很明显的。”该人士告诉记者,李某错在不应设置电话呼叫转移和短信转发,接不到银行的验证码和人工电话,人脸识别就成了唯一的验证手段。“应该尽可能地使用多重验证方式,避免只用一种。”该人士说。

综合法治日报、北京科技报

报料电话:(0531)85193700 13869196706 欢迎下载齐鲁壹点 600多位在线记者等你报料
报纸发行:(0531)85196329 85196361 报纸广告:(0531)85196150 85196552 85196557 差错投诉:(0531)85193700 发行投诉:4001176556 (0531)85196527 邮政投递投诉:11185 全省统一零售价:1元
刊号:CN37-0003 邮发:23-55 广告许可证:鲁工商广字01081号 地址:济南泺源大街2号 大众传媒大厦 邮编:250014 大众华泰印务公司(大众日报印刷厂)印刷