

人脸识别突飞猛进 更要看好“我们的脸”

在国内,进入高铁站、机场过安检、入住宾馆或到单位签到时使用人脸识别系统已是普遍的事了。但奇怪的是,近来国外媒体时有人脸识别系统患上“脸盲症”的报道。近日,英国大都会警察局被曝其部署的人脸识别系统准确率仅达到2%。而美国民权组织在使用亚马逊面部识别系统时,扫描所有535位美国国会议员的面部照片,结果其中28人竟被识别成了罪犯。如此误差引起了人们的质疑,以及对警方使用该系统的担忧。

人脸识别是AI技术发展较快、应用较多的一个领域,国内警方的人脸识别系统屡屡精准识别逃犯,国外警方的人脸识别准确率为何如此之低?究竟是评价标准不同,还是技术上真有差别?

隐私忧虑或限制技术发展

对于中外人脸识别效果的巨大差异,航天科工智慧产业发展有限公司系统总体部专家何东昌在接受媒体采访时解释,首先是国外的国情问题。有些国家认为,人脸识别存在隐私问题,甚至对视频监控技术的应用都有一定限制。例如在英国,面部识别和追踪技术就曾引发巨大争议,英国各界甚至发起一项“请警方停止用摄像头进行面部识别”的抗议活动。类似情况在美国也有发生,如亚马逊公司

利用云计算平台、人工智能技术帮助警方使用人脸识别技术,美国公民自由联盟对此提出了抗议。

“国内人脸识别应用已相当广泛,并积累了相当多的实战经验,在人脸图像采集、预处理以及特征选取等方面的工程优化也做得很好。”何东昌说,除国情外,在国际上我国的人脸识别技术确实发展比较快。

美国国家标准与技术研究院组织的人脸识别算法测

试FRVT2018结果显示,我国公司再度摘得桂冠。该测试以评测标准的严谨性、一致性和全面性著称。在测试中,我国的人脸识别算法在千万分之一的误报下,达到识别准确率95.5%,成为当时全球业界在此项指标下的最好水平。

清华大学媒体大数据认知计算研究中心主任王生进教授介绍,当前人脸识别有三种应用模式:1:1人脸识别、1:N人脸识别、M:N动态布控。

1:1识别的本质是计算

机对当前人脸与人像数据库进行快速人脸比对,并得出是否匹配的过程,“刷脸”登机、验票、支付都属此类;1:N是在海量的人像数据库中找到当前用户的人脸数据并进行匹配,即从N个人脸中找出1个目标;M:N是通过计算机对场景内所有人进行面部识别,并与人像数据库进行动态人脸比对,能应用于黑名单监控、VIP客户管理系统、校园人脸识别系统等多种场景。



■相关链接

人脸识别技术知多少

目前,国内外人脸识别技术发展速度加快,技术路径也比较多。何东昌介绍,主流的人脸识别技术基本上可归结为五类。

其中,基于模板匹配方法是将待处理的人脸图像直接与数据库中所有模板进行匹配,选取匹配最相似的模板图像作为待处理图像的分类。不过,由于数据库中每个人的模板图片数量有限,不可能涵盖现实中所有的复杂情况,简单的模板匹配只利用了相关信息,对背景、光照、表情等非相关信息非常敏感。因此,该方法只适用于理想条件下的人脸识别,并不适合应用于实际场景。

基于几何特征的方法,即人的面部有形状和大小都不相同的部件,如鼻子和嘴巴等。通过对这些部件形状的对比、部件间位置的检测,从而实现人脸识别。与基于模板匹配方法相似,形状、距离等信息并不能表达出图像中的姿态、表情等非线性因素,导致该方法的可靠性和有效性较低。

基于神经网络的方法直接使用图像像素点作为神经网络的输入,通过模拟人脑神经元工作机制,可学习到其他方法难以实现的隐性人脸特征表示。而且神经网络拥有非线性激活函数,使得网络对人脸图像中的非线性因素和关系有一定的表达能力。

基于稀疏表示的人脸识别方法中,稀疏表示用的“字典”直接由训练所用的全部图像构成,无需经字典学习。

最后一种是基于深度学习的人脸识别方法。其核心内容是逐层训练的网络结构,每层使用的是自编码神经网络,自编码神经网络主要包括对数据编码和解码两部分内容。通过编码、解码实现对输入数据的无监督学习,辨识能力随数据增长逐步提高。

(本版综合)

保护“刷脸”信息需多管齐下

在信息即价值的时代,个人隐私信息的商业价值日益凸显。在人脸识别技术火爆的同时,社会上出现了是否会侵犯隐私,人脸是否能被“假冒”的担忧和质疑。对此,何东昌认为,目前国内,从消费电子领域到安保、网络支付、金融等领域都在逐步引入人脸识别,但新技术有“双刃剑”属性,应防范其中潜藏的安全隐患。

特别是在“刷脸”过程中,用户的姓名、性别、年龄、职

业,甚至用户在不同情境状态下的情绪等大量信息都被采集并储存。这些信息如果得不到妥善保管而被泄露,用户个人隐私就处在“裸奔”状态。“因此,面对刷脸产生的个人隐私问题,我们必须多角度共同保护。目前在人脸识别技术领域,我国尚无相应的安全监管机制,应及早未雨绸缪,预先防范。”何东昌说。

微软总裁兼首席法务官布拉德·史密斯也在其博客中表示,考虑到这项技术被滥用

的可能性和广泛的社会影响,政府在人脸识别方面的立法似乎显得尤为重要。

“看好我们的脸”,公民应多一些戒备与防范意识,企业多一些技术层面的保障措施,监管也需要及时跟进。业内人士建议,政府应从管理者角度,通过立法方式强化面部识别领域的监管力度,保障公民个人信息安全;相关行业、企业应提升应用软件等载体及储存设备的安全技术水平,提升网络安全意识,避免公民隐

私信息泄露或遭非法转卖;非必要的隐私数据不应采集。当前,人脸识别技术的开发仍有巨大拓展空间,国家有必要在数据共享和开放上加大引导力度,促进技术发展。另一方面,人脸识别技术在逐渐走向成熟,应用将越来越多,识别技术的各类标准,特别是保护公民隐私的标准应尽快出台;相关行业及企业需担负起社会责任,主动积极地规范行业标准,自觉维护采集、储存的公民隐私数据安全等。

大开眼界

糕点师制作眼镜蛇蛋糕

近日,美国糕点师切尔茜·怀特制作了一只外形酷似眼镜蛇的蛋糕,该蛋糕长1米多,表面喷成棕金色,有着逼真的蛇鳞,蛇头昂然挺立,龇着利齿,细节刻画得非常生动。



无人驾驶汽车长着大眼睛

无人驾驶汽车的原理主要是通过各种传感器来确定周围障碍物,进而执行行驶决策。近日捷豹路虎的未来交通部门在无人驾驶汽车前方设计了一双大眼睛,它不是传感器,而是汽车对障碍物意识的直观表现。



智能缝纫机

日本车乐美公司近日推出了一款智能缝纫机,无需专业技能,普通用户仅仅通过手机App就能完成刺绣创作。

这款智能缝纫机最大工作范围为102mm x 102mm,适用于DIY包包,桌巾上的小型刺绣图案。具有接入点模式,即使没有无线网络也能使用。