# 人脸识别技术迎井喷期 专家:完善标准保护隐私

资本加速涌入 金融和安防成“先锋”应用领域

人脸识别技术商用迎来“井喷期”

专家建议完善相关行业标准保护用户隐私

近期，“刷脸”成为了热词，人脸识别技术不断进入大众视野。苹果新机iPhone X具备“刷脸”解锁功能，并且可运用到Apple Pay以及各种需要身份验证的App中；首个“刷脸”支付的商用试点也在杭州一家肯德基餐厅开启；一些银行正尝试启用自动取款机“刷脸”取款功能；高铁检票、宾馆入住也在使用“刷脸”技术……

人脸识别已经在人们衣食住行的各个领域发力，迎来运用的“井喷期”，其中，金融和安防等行业成为应用“先锋”领域。随着人脸识别技术的商用场景不断扩充，市场潜力巨大，资本嗅到商机纷纷涌入。来自前瞻产业研究院的数据显示，2016年我国人脸识别行业市场规模已超过10亿元，预计到2021年将达到51亿元左右。

“刷脸”时代带来巨大市场

刷脸进站、刷脸取款、刷脸支付、刷脸报到……随着人脸识别技术的日渐成熟，“刷脸”时代正在到来。在业内人士看来，人脸识别技术正在不断突破各个行业应用的“阈值”，带来日趋丰富的应用场景。

“随着深度学习算法登场，人脸识别精度相比五年前已有大幅飞跃。”360公司副总裁、人工智能研究院院长颜水成说，各种设备拍摄人脸所提取的信息会结成数据对，不断积累的海量数据成为反哺技术完善的“充足养料”。

蚂蚁金服生物识别技术负责人陈继东说，近年来得益于深度学习的迅速发展，我们可以基于神经网络让机器模拟出人类大脑的学习过程，并通过卷积神经网络模型和海量的图片数据进行训练。生物识别从以前70%、80%的准确率提升至近两年的99.6%甚至99.7%，具备商用条件。同时，在支付场景中人脸识别技术的误识率已经达到十万分之一。

旷视科技副总裁谢忆楠告诉记者，人脸识别技术主要有三大应用方向，一种为1：N认证，判断某个体是否为特定群体中的一员，用于人员出入管理和城市安防，包括公安抓捕逃犯、小区门禁启用刷脸系统，以及一些商家的VIP管理等。

另一种为1：1认证，即证明本人与证件信息是统一的，主要应用于需要实名制验证的场景。南航今年6月在河南南阳机场启用的“刷脸登机”，武汉火车站和广州南站启用的“刷脸进站”，即属于此类。

第三种是活体检验，证明是真人在操作业务，进而做账户许可授权。中信银行的ATM和移动客户端可以进行远程身份认证，海通证券可以远程开户，滴滴平台则可以查验驾驶者是否为注册司机。

人脸识别正在慢慢从线上走到线下，在无人零售、快捷支付、酒店入住等场景中亮相。资本看准其中的商机，纷纷入局。今年7月，商汤科技宣布完成4.1亿美元B轮融资。上海依图科技与北京旷视科技完成了C轮融资，金额分别为3.8亿元人民币与1亿美元。来自前瞻产业研究院的数据显示，2016年我国人脸识别行业市场规模已超过10亿元，预计到2021年将达到51亿元左右。

商业应用场景不断丰富

《经济参考报》记者了解到，人脸识别技术在金融上的应用呈爆发式增长态势。从我国自主研发的全球首台具有人脸

识别功能的ATM机通过验收，到互联网企业蚂蚁金服、京东、苏宁等推出“刷脸支付”应用，再到传统银行如招商银行试点人脸识别应用……支付、取款、贷款等金融领域的应用走到了其他领域应用的前面。

今年9月，“刷脸”在金融上的应用赚足了眼球。在苹果新机发布会上，iPhone X具备“刷脸”解锁功能成为了关注焦点，苹果称这一功能可运用到Apple Pay；金融科技公司蚂蚁金服与肯德基共同对外宣布“刷脸支付”进入商用试点阶段，这是刷脸支付从线上走到线下，首次真正落地到商业场景的消费中。

在杭州万象城肯德基的KPRO餐厅里，《经济参考报》记者看到不少消费者尝试了“刷脸支付”：在自助点餐机上选好餐，进入支付页面，可选择继支付宝、微信移动支付选项后的新选项“刷脸支付”，然后进行人脸识别，大约需要1-2秒，再输入与支付宝账号绑定的手机号，确认后即可支付，过程不到10秒。

在难度系数极高的城市安防领域，人脸识别也在大显神通。以往人脸识别技术只能处理数百人级别的数据比对，但现在已经发展到上万人甚至更高量级的数据比对，且突破拍摄角度不正、光线变化复杂、分辨率低等不利条件，帮助公安机关迅速抓捕逃犯。

记者获悉，人脸识别公司旷视科技已为多地公安系统提供了实时警情数据服务，其中直接协助警方破获案件1032起，抓获、控制的在逃人员超2000人。重庆市某公安分局使用商汤科技的人像比对系统，在40个工作日内辨认出69名嫌疑人，相比人工效率提升200倍。

在人脸识别技术到来之前，指纹识别、虹膜识别等生物特征识别方式已经在生活中得到广泛运用。不过受访人士表示，相比较而言，人脸识别最大的优点在于“非接触性”，这可以大大提升系统响应速度，提高使用便捷度，同时避免指纹等接触式识别产生的疾病传播等卫生隐患。

此外，“非配合、非侵入”式特征，意味着可以在不需要使用者配合的情况下采集到数据，这有利于公安在安防等领域的应用。

人脸识别技术还越来越用于娱乐。面部识别解锁功能成为平板电脑“卖点”、智能相册可通过识别人脸进行照片分类、“美颜”类APP自动识别人脸并为其“化妆”……例如，一款火爆的“FACE U”软件，可以将用户头像“变成”大圣、兔子等形象，与朋友圈、微博等社交平台的朋友互动。

业内人士认为，智能家居将会是未来人脸识别的应用场景之一，智能防盗门在主人站在门口时才会打开，智能电视能识别你是谁，并推送给你常看的节目，甚至服务机器人也可以根据对象身份的不同提供相应的服务。未来人脸识别技术会让用户信息的深度挖掘成为可能，商家可以对会员的购买行为进行分析，进而有针对性地安排商业布局或促销活动。

技术准确度突破可期

专家认为，未来，人脸识别技术还会继续突破。一方面，准确度、安全性会继续提升，针对整容、双胞胎等特殊情况的处理能力也在提升。另一方面，人脸识别能够处理的数量级也会继续扩大。当技术已经进步到可以在上亿张照片的数据库中提取、比对某张人脸时，则应用场景会逐步扩大。

据颜水成介绍，通常人脸识别包含以下环节：相机或者专业设备先采集到图片，人脸检测技术定位图片中的人脸，然后从中再定位诸如眼角、鼻尖、嘴角、脸部轮廓线等特征，进行包括光线补偿或者遮挡物剔除等校正。再用深度学习算法进行身份特征提取，跟数据库中的人脸特征做比对，以识别人脸身份。

业内人士认为，其中的技术关键在于通过不同脸部图像上的特征关键点和面部表情网，找出彼此之间的关联，最终判定这些图像是否为同一个人。但人脸是变化的，不同角度、不同妆容都能影响特征关键点的抓取。

此外，“刷脸支付”是在线下公共设备和开放环境下进行，真实场景复杂多变，且安全性要求更高。生物识别技术对人们的生活带来更多便利还是挑战？

疑惑一：“刷脸”如何确保精准度？

在衡量人脸识别能力时，很多公司都会宣称其准确率超过“99%”。对此，长期研究机器学习的西安交通大学电信学院特聘教授、国家“千人计划”专家龚怡宏表示，这里的准确率指的是在一些世界知名人脸数据库比对中取得的成绩

，但在现实运用中，这种准确度要大打折扣。

商汤科技联合创始人杨帆也认为，这些准确度是在一定前置条件下取得的，但现实应用场景复杂多变，人群样本更大，不同光线、姿态、分辨率等条件都可能给机器识别带来困难。

不过，这也不代表技术要达到100%准确率才可以使用。“世界上没有完美的技术，任何技术都是有错误率和瑕疵的，但是如果在特定的场景下，技术的准确度能够满足要求、错误带来的风险可以承受，那它就是有价值的。”颜水成说。

苹果方面介绍，新机iPhone X的面容ID功能利用由点阵投影器、红外镜头和泛光感应元件组成的先进原深感摄像头系统，在A11仿生强劲动力的支持下可绘制面谱并识别面容。该功能会投射30000多个肉眼不可见的红外光点，然后将得到的红外图像和点阵图案传输给神经网络，创建用户脸部的数学模型，再将这些数据发送至安全隔区，以确认数据是否匹配。而且，用户的样貌随着时间而改变，技术也能随之进行调整适应。

蚂蚁金服介绍，支付宝在肯德基KPRO的点餐机上配备了3D红外深度摄像头，在进行人脸识别前，会通过软硬件结合的方法进行活体检测，来判断采集到的人脸是否是照片、视频或者软件模拟生成的，避免各种人脸伪造带来的身份冒用情况。

疑惑二：双胞胎、过度化妆和整容能分辨吗？

“人脸的角度、光线、表情、年龄、化妆、遮挡、照片质量等会影响我们的判断，并且随着数据库样本增大，两个不同人长得像的概率会快速上升。”陈继东提出了生物识别技术面临的难题，不过，他认为深度学习会让计算机更聪明，能克服这些困难。

颜水成表示，面对双胞胎或者整容前后等特殊情况，机器能否识别，要看具体情况。比如整容幅度过大，机器无法识别是有可能的。此外，脸部信息也会随着年龄增长而改变。如果到了机器无法识别的程度，使用者只需去系统更新脸部照片就可解决。

为了提高识别率，不少应用场景都需要用户采用除人脸识别技术外的双重验证。陈继东表示，交叉验证方式进一步提升识别率，即使是双胞胎也“判若两人”。在金融等对误识别率容忍极低的领域中，单一识别要素即使精准度再高仍然会有漏网之鱼，因此需要结合多因子综合验证。目前人脸识别准确率已远超肉眼，而且有活体检测算法来判断采集到的人脸信息是否为照片、视频等冒充。“即便出现账户被冒用的极小概率事件，支付宝也会通过保险公司全额赔付。”

疑惑三：用户隐私如何保护？

有专家指出，人脸特征与指纹、虹膜相比，是一个具有弱隐私的生物特征。例如，很多人都会发自拍照，也是相对公开的特征。如何保证用户数据安全尤为关键。

据媒体报道，在一个名为“你的脸就是大数据”的项目中，俄罗斯摄影师叶戈尔·茨韦特科夫在圣彼得堡用了6周时间拍摄100名地铁乘客的人脸照片，之后利用人脸识别工具比对俄罗斯最大社交网站VK（VKontakte）上的5500万用户，找到了大约70名乘客的个人资料。

如何防范类似的隐私泄露风险？旷视科技副总裁谢忆楠表示，旷视在采集到照片后会对照片进行脱敏处理，只提取照片特征，而非照片本身，即使这些特征在传输过程中被窃取，也无法还原出照片，过程是不可逆的。

陈继东说，目前支付宝已经对人脸识别技术进行了加密、脱敏的技术防范，可以将人脸信息变成一个不可逆的数字信息，不能还原、比对。

苹果方面介绍，其所有保存的面容信息都被保护在安全隔区内，以确保数据安全无虞。同时，所有处理都在设备上进行，不会发生在云端，以充分保护用户隐私。面容ID只有在用户注视iPhone X时才会为它解锁，并采用特别设计，可防止被照片或面具假冒的人脸欺骗。

相关行业标准有待完善

专家普遍认为，人脸识别技术的市场潜力巨大，技术要求高安全性、高准确率、高可用性、高实时性，但目前人脸识别技术还没有一个行业标准，用户隐私安全也亟待保障，建议制定并完善行业标准。

在中科院计算技术研究所研究员山世光看来，经过多年发展，人脸识别近几年确实取得了突破式发展，完成了一些以前“不可能完成的任务”。但用户隐私也值得关注，即用户的照片是如何传输和保存的，有没有在未经允许的情况下被保存或拷贝。相关应用如何设计人脸识别系统，确保用户数据不被盗用，目前看起来还不明确。“人脸识别技术逐渐走向成熟，应用越来越多，人脸识别技术的各类标准，包括保护公民隐私的标准应尽快出台。”山世光说。

华为集团从事模式识别的技术人员田女士说，人脸数据很难更改，“例如，我们不可能因为一次人脸数据被盗就去整容来更改我们独有的生物密码。因此，当下很多技术都在突破活体检测，如用‘眨眨眼’‘张张口’来进一步确认”。

杨帆表示，人脸识别是一条很长的产业链，保护用户隐私不仅需要靠公司的自律，更需要在政府引导下建立起整个行业的统一标准，共同筑起保护用户隐私的行业堤坝。

颜水成说，人脸识别更广泛运用的基础在于进一步提升识别准确率和安全性，而大量数据作为深度学习的养料是必不可少的。以后，人脸识别采集设备会越来越多，会积累大量的数据，但这些数据如果变成一个个数据孤岛，就无法使人脸识别技术得到提升，建议在数据的共享和开放上加大引导力度，促进技术发展。

来源：经济参考报

责任编辑：张岩

表决结果：同意票3票；反对票0票；弃权票0票。

原料：牛肉10克、香菇1朵、鸡蛋1个、葱花适量、大米粥1小碗、盐1克、玉米粒适量。

当前文章：http://www.fdpju.cn/article/20171013_7411.pdf

发布时间：2017-10-22 02:00:46

小时代 小产权房 非诚勿扰 香港金像奖 命运石之门 奇博少年 悲惨世界 少年医王 翻译官 花果山