新华每日电讯

本刊编辑：雷琨　刘新华　王小舒

邮箱：lihl_mrdx@163.com

新华视界 引力波 科技专刊

13版

2017年3月24日　星期五

人脸识别，这么容易就被骗？

本报记者尹平平　实习生孙楠

人脸识别，这项几年前还只是在科幻电影里才能看到的技术，已经开始逐渐进入我们的生活了：现在手机上的支付宝等不少APP，登录时都需要“人脸识别”；在银行的自助终端机办理一些简单的业务，也需要“人脸识别”确认是否是本人操作；有些公司或写字楼的门禁，已经不再靠刷卡，而是靠“刷脸”；甚至连北京天坛公园的厕所取厕纸，都需要“人脸识别”，以便节约……

这项新鲜的人工智能技术，在很多方面都让人感觉到更方便并且更安全了：你可以猜出来或者窃取我的密码，但这张脸是我自己的，你总偷不走吧？

然而，不久前的“央视3·15”晚会却提醒大家：并非如此。晚会现场，主持人仅用一张照片，而不是用自己的脸，对着镜头，就轻松进入了一个需要人脸识别认证才能登录的APP。

虽然目前的人脸识别通常需要操作者眨眼、张嘴或转头，以便证明是“活的人”而不是“死的照片”，可是通过一些P图软件，照片也能“活”起来，照片也能眨眼、张嘴或转头。甚至，就像“央视3·15”晚会时主持人操作的那样，可以给自己换一张脸。而在晚会现场，这些通过P图软件处理过的“照片脸”或者“假脸”，都被现场演示的人脸识别系统一路绿灯地轻松放行。

这令很多观众瞠目结舌。在微博、微信朋友圈等社交媒体上，不少人都表示“再也不敢信刷脸登录了”，庆幸自己“幸亏还没开通过刷脸支付的功能”，甚至还有人埋怨：“为什么不早说？干嘛非等3·15才爆出来？”

“人脸识别”真的“笨”到连活人和照片都分不清吗？它到底是更安全还是更危险呢？这项正在兴起并开始广泛应用的人工智能技术，我们到底是该接受，还是拒绝呢？《新华每日电讯》记者带着这些问题，采访了人脸识别和互联网安全领域的技术人员。

▲人脸识别技术的应用在国内日益广泛。2016年10月12日，一名女孩在杭州云栖大会会场一展台内体验“扫脸付”生物识别支付技术。该次杭州云栖大会由杭州市政府与阿里巴巴集团主办。　新华社资料照片

怎么区分真人和假脸？

很多人工智能技术，都是基于计算机系统的深度学习来实现的，人脸识别也不例外。

人脸识别系统的深度学习，首先是对人脸进行逐层的特征分类，每一层都会对某种信息进行分类、优化，然后将信息传递到下一层。比如，第一层可能会寻找简单的边线；第二层可能会寻找可以形成长方形或圆形等简单形状的边线集合；第三层可能会识别眼睛和鼻子等特征……第五、第六层以后，神经网络会将这些特征结合在一起，让机器可以根据训练数据集，达到拥有自我学习的能力，最终掌握“人脸”的概念。

深度学习神经网络的层数越多，它能表达的信息也就越复杂。目前，我国在人脸识别上的前沿技术团队，已经可以做到将人脸信息分为1000层以上的神经网络。而数据越多，人脸识别的效果就会越精确。

早期的人脸识别系统，之所以会把照片当成人脸，是因为它学习的“教材”就是照片。既然是从照片上学习到人脸的信息，自然就会把照片当成人脸。“因为它本身没有太强的信息甄别能力。”360企业安全移动应用事业部总经理赵刚向记者解释道，“现存的许多人脸识别系统只是强调它的学习能力，它的分辨是基于你教授的内容和信息，你教它什么，它就学习什么。”

把照片当成大活人，这太危险了。因此，现在几乎所有人脸识别系统要做的第一步，就是确认正在识别的对象，是一个人，而不是照片。所以要求你眨眼、张嘴或扭头。简言之，就是验证“你”是“活的你”。这在业界被称为“活体检测”。接下来才是第二步：确定待验证的人脸，与用户此前预留在系统人脸数据库中的人脸，是同一张人脸，即人脸的识别和比对。简言之，就是验证“活的你”是“数据库中记载的你”。

但就像“央视3·15”晚会上主持人演示的那样，图片处理软件也可以让照片“活”起来。面对这些“动图”，我们用肉眼很容易就看出来了，可是号称“人工智能”的人脸识别系统，难道就“懵圈”了吗？

并非如此。人脸识别系统的学习，并不是拿到文凭，毕业以后，就再也不学习的“一锤子买卖”。它一直处于不断学习的过程当中。遇到动图照片的“假脸攻击”，技术人员就要让系统学习新的内容，告诉它什么样的脸即使能动，也不是活体，从而增强人脸识别系统的甄别能力。

“一般来说，合成图像中的人脸，和原有的真脸相比，会存在众多不匹配的情况。再精心的PS，在光线分布、色调均匀度、贴图周边处理方面，都难免会存在微小的不自然。在假脸和真脸之间的衔接区域，也会留下‘合成痕迹’，如模糊处理、涂抹等。”商汤科技计算机视觉研究员吴立威告诉《新华每日电讯》记者，“这些不匹配的情况，通过我们人脸识别系统，基于大数据训练的深度学习模型，都可以一一找出来。即便是那些人眼根本察觉不到的头发丝般细微的瑕疵。”

既然可以合成图像，也就可以合成视频，“央视3·15”晚会上主持人的“换脸”就是其中一种。但合成的视频，仍会带有光线、色调不自然等“合成痕迹”。

此外，吴立威表示，合成视频攻击，往往通过用手机摄像头翻拍提供合成视频的屏幕来实现，此时的屏幕图像与真实人脸就会存在如显示屏幕边缘、屏幕亮度、屏幕反光、摩尔纹、像素点纹理、镜头畸变等差异，可以被不断更新的算法识别出来。

“总的来说，只要给予足够多的人脸攻击大数据样本，机器就能够自主地学习到伪造图像或合成视频中的瑕疵，最终就能得到对于这些攻击的分辨能力。并且，随着学习数据的不断增多，深度学习系统也会一天比一天强大，让各种各样的换脸无可遁形。”吴立威说。

“刷脸”能做支付的唯一凭证吗

“在我们看来，主持人在‘3·15’晚会上展示的‘攻击’，已经是‘上古时代’的‘攻击手法’了，业内主要的技术团队早就已经可以防护了。”旷视科技互联网市场运营总监伞璐笑着对记者说。

“3·15”晚会的展示，只是把人脸识别领域的反攻击工作和黑客的较量从幕后搬到了台前。伞璐介绍说，他们早在2015年底，就针对线上身份验证服务，设立了专门的活体攻防团队。这个攻防团队平均每天过滤掉的攻击次数达到52342次。而“央视3·15”晚会上主持人演示的，确实是最常见的攻击方法，但只是他们每天要面对的攻击中的一小部分，并且在目前的碰撞试验阶段，就已能够防护住了。

小视科技首席算法官倪冰冰告诉记者，无论是通过图像处理软件做的屏幕翻拍、虚拟人脸，还是像电影中常见的那种高仿人脸面具等攻击，虽然表面看似真实，“但是一旦数学变幻到某个特定的特征空间，马脚就露出来了。”倪冰冰介绍说，他们非常重视反欺诈技术的研发和产品迭代，团队的核心成员当中，有一半以上都参与其中。

然而，即使技术人员们做出如此这般的承诺，上周李砚去银行办事，还是遇到了一件让她哭笑不得的事情。

李砚小两口计划近期休年假到境外旅游，办签证时需要提供银行卡一年的消费流水单。李砚夫妇的账，都是汇总到李砚爱人名下的银行卡里，李砚的爱人工作很忙，让李砚拿着他的银行卡和身份证去银行代办。银行卡密码，是小两口结婚时就已经“共享”过的，李砚此前帮爱人代办类似业务也不是一次两次了。午休时，李砚找了个身材魁梧的男同事，陪她一起去银行办事。

以往打印银行卡消费流水，都是要到柜台由银行柜员办理的。现在，打印流水这种“小事”，可以到一个自助终端机上，在工作人员的引导下，半自助完成，不需要取号排队。李砚按照机器的操作要求，刷了爱人的银行卡、身份证，输入了密码之后，下一步安全认证拦住了她：人脸识别。

人脸识别的主要目的是：确保是本人操作。可因为银行卡是爱人的，李砚是代办，她无法通过人脸识别这一关。以往在柜台操作，如果代办，代办人也需要出示自己的身份证，由柜员审核通过即可。可是在自助终端机上操作，没有这么一步，李砚向银行工作人员咨询，对方表示爱莫能助，只能由本人办理，才能通过“刷脸”这关。

正在李砚和工作人员交涉时，李砚的同事探身过来，想知道发生了什么。这时，自助终端机上的人脸识别系统捕捉到了李砚同事的脸，竟然通过了验证，打印出了消费流水。“什么鬼？”李砚忍不住叫出来，“为什么他能验证通过？他不是我老公啊！”

李砚给记者看了她爱人与这位同事的照片，除了面部都比较富态以外，五官轮廓都不像。“这就是所谓的人脸识别吗？我怎么觉得一点都不安全，反而更危险了呢？”

这是人脸识别的通过率和误识率的问题。根据《新华每日电讯》调查，目前人脸识别企业普遍的方式是，在保证正确识别和正确拒绝通过率情况下，尽可能降低误识率。但误识率就像误差一样，很难避免。

目前主要的人脸识别团队都能做到将通过率控制在95%左右。也就是说用户在刷脸时，20次中通过19次，有1次需要重新刷或者停止交易，或者转用人工方式进行二次排查。

李砚在银行自助终端机上的操作，仍然是在银行工作人员的指导和监督下完成的。虽然靠同事“刷脸”通过了验证，但一旁的工作人员并没有把打印出的消费流水给她，而是等她爱人事后带着身份证来领取的。

2015年12月，央行发布了《中国人民银行关于改进个人银行账户服务加强账户管理的通知》，通知指出：“提供个人银行账户开立服务时，有条件的银行可探索将生物特征识别技术和其他安全有效的技术手段作为核验开户申请人身份信息的辅助手段。”自此，人脸识别在金融领域的实名认证应用场景中实现了快速落地，但这只是一种“辅助手段”。

“在任何涉及人身、财产安全的应用场景中，从来不会仅仅把人脸识别作为唯一的账户验证手段。”伞璐对记者强调道，“人脸识别技术的价值是为信息安全做加法，通过和传统的用户安全认证方式相加，打造‘静态验证+动态验证’的立体防护体系。”

“人脸识别不可能是一个包打天下的东西。它可以作为一个安全的补充，但是不能对它寄太高希望，把它当成唯一的认证手段。”360企业安全移动应用事业部总经理赵刚表示，“即使是其他的生物认证，比如指纹、虹膜甚至静脉识别，都只是多一层防护，但是这些防护都不是万无一失的。**没有哪一项可以称得上绝对安全。任何安全防护都有攻克方式，只是时间和成本的问题。**”

人脸识别只能用于安全认证？

赵刚认为，**对于人脸识别，盲目地信任肯定是不可取的态度，但是也不能因为它目前存在的问题，就将其一棍子打死。**

实际上，作为一项逐渐深入到我们生活当中的人工智能技术，人脸识别的作用，也不仅限于各种终端账号登录的安全认证方式。

虽然互联网金融领域的人脸识别是几乎每个人都能接触到的，但更广泛使用人脸识别技术的却是安保领域。比如，在抓捕逃犯时，通过人脸识别系统，可以协助在数据库或者监控视频中锁定目标，并跟踪对方行迹，这样能够提高破案效率或者做及时有效的智能预警。

人脸识别还可以用于一些商业上的数据分析，比如研究逛商店的人的消费偏好。根据商店监控录像捕捉到的人脸信息，可以统计出一段时间内，各个柜台前站的人的数量和时长，以此来评判哪个产品是热销产品。针对具体的客户，也可以测绘出他的逛街路线，了解他的消费喜好，从而通过其他方式更有针对性地进行营销。

现在珍爱网、世纪佳缘等大型的婚恋网站，也都引入了人脸识别技术。一方面，可以保证注册会员信息的真实可靠；另一方面，也可以通过放你喜欢的明星照片，来搜索出“合眼缘”的异性，再辅之以其他方面的大数据分析，帮助会员更高效地找出心仪的另一半，实现“人工智能相亲”。

商汤科技人脸识别团队表示，他们的合作伙伴中，有不少是直播平台。现在不少直播APP可以在直播的同时，给主播添加帽子、头饰、眼镜等卡通效果，这就是基于人脸识别和AR技术实现的，系统要先定位你脸部五官的位置，然后再给相应的位置“穿戴上”相应的配饰，增加娱乐互动效果。

个别面膜企业，也引入了人脸识别技术。通过让用户“刷脸”，测量脸部大小，为用户提供面膜尺寸，和对用户的肌肤年龄、性别等属性进行分析。P图软件就更不用说了，通过人脸检测和关键点检测，在图像中精准定位人脸和五官位置，从而进行人像美白、五官美化等精准修容的操作。

由此可见，我们的面部信息也是一项重要的个人信息。可是在这个信息安全面临极大考验的时代，人们总难免会担心“面部信息的安全”，毕竟自己的脸天天都暴露在光天化日之下，不能像密码一样秘而不宣。有些小心谨慎的人，不仅对人脸识别技术产生怀疑，连自己和家人的照片，都不敢发在社交媒体上，唯恐被坏人利用。

在赵刚看来，加强防范意识固然是必要的，但没必要过度担心从而因噎废食。“对于一项人们还不够了解的新的技术，无论是盲目的信任，还是因为一些现存的瑕疵就恐惧或者拒绝，都将对这个行业和技术发展产生打击。提早去了解它，适度地利用它，并且保持警惕，让安全成为你生活的一部分，而不是绊脚石，才是正确的态度。”

中国深渊科考取得世界级突破

中科院深渊科考队历时68天、航行7929海里，在深海地震探测、水下滑翔机下潜等方面取得多项世界级突破

新华社北京3月23日电(记者董瑞丰、刘诗平)记者从中国科学院获悉，中科院深渊科考队23日已返回海南三亚。科考队历时68天、航行7929海里，赴马里亚纳海沟挑战者深渊和雅浦海沟，在深海地震探测、水下滑翔机下潜、深海采样等方面取得多项世界级突破。

据中科院深海科学与工程研究所介绍，科考队使用我国自主研发的深海海底地震仪，在马里亚纳海沟挑战者深渊完成了两条万米级人工地震剖面测线，使我国成为世界上首个获取万米级海洋人工地震剖面数据的国家。

我国自主研发的海翼号水下滑翔机3次突破水下滑翔机的世界下潜深度记录，最大下潜深度达6329米。我国自主研发的海斗号自主遥控水下潜水器5次下潜进入万米深度，并在10886米深处着底，突破万米级长距离微细光纤传输及控制的技术瓶颈，在我国首次实现万米海底的巡航遥控和实时视频影像传输播放。

据了解，科考队还在雅浦海沟7884米深度获取一尾深海狮子鱼样品，这是目前我国在深海获取的鱼类样品的最大深度。采用我国研发的深海摄像机在挑战者深渊8152米深度记录了狮子鱼的活动，这是目前国际上发现的鱼类生存的最大深度。

此外，科考队使用自主研发装备，20次进入挑战者深渊大于10800米的海底，获得大量样品和影像资料，未来将有助于科学界对万米海斗深渊的研究。其中，采集的近2800毫升保压气密水样，是国际上首次在万米深度获得的保压气密水样。

国产可穿戴机器人助截瘫者重新行走

新华社上海电(记者龚雯)近视患者戴上一副眼镜就可以像正常人一样看书，那是否可以让无法行走的截瘫患者穿上一套外骨骼机器人，就可以像普通人那样迈步行走?科技的快速发展，让一切皆有可能。

记者采访获悉，我国自主研发的商用化外骨骼机器人Fourier　X1近期在上海对外发布，主要针对下半身瘫痪的患者，帮助他们实现坐、站、行走、上下楼梯等基本功能，也被称为“可穿戴机器人”。

值得一提的是，这款机器人通过19个不同的传感器，11个分布式CPU模块，能够“感知”患者在步行中的变化，“思考”患者的意图。如果患者走动的重心、步态偏差比较大，超出设定范围，机器人会采取自动关停、报警等安全措施，设备停止之后人不会直接摔倒，而是处于固定暂停状态。

虽然这套机器人重达20公斤，但实际使用过程中，重量会转移到患者脚底的金属板上。在充满电的情况下，外骨骼机器人可以行走7小时左右。

有报告预测，未来5年广义康复机器人的年复合增长率约为37%，其中外骨骼机器人年复合增长率为47%，远高于其他类别的医疗机器人的平均增速。预计到2020年，全球外骨骼机器人的市场将超过18亿美元。

首批机器人警察将走上迪拜街头

机器人警察在街头巡逻?这即将在阿拉伯联合酋长国成为现实。

“今日俄罗斯”电视台网站20日援引多名阿联酋官员的话报道，阿联酋首批机器人警察将于今年5月在迪拜上岗。迪拜警察局技术创新部主任阿德南·阿里此前透露，准备今年先把机器人警察部署在迪拜旅游景区，到2020年再拓展至更多街区。

即将上岗的机器人型号最早是在2015年10月海湾信息技术展上发布的。该款机器人掌握多项语言技能，可扫描识别周围的人，民众可通过其触摸屏进行报警、缴纳交通罚款等。

迪拜警察局未来塑造中心主任阿卜杜拉·本·苏丹告诉阿联酋《海湾新闻报》，“我们正寻求今后让更多机器人承担警察职责。到2030年，我们热切期盼让机器人警察数量达到(迪拜)总警力的大约25%”。

据迪拜警察局智能服务部总指挥哈立德·纳赛尔·拉祖齐介绍，迪拜警方还希望到2030年，让全部警察局建筑物的电力供应50%靠自给自足。此外，警方还将引入更多“智能机制”，例如让其中一个警察局完全无需配备警员。　**(杨舒怡)据新华社微特稿**