机器视觉应用与 AI 产业—人脸识别

张运吉 (211300063、211300063@smail.nju.edu.cn)

(南京大学人工智能学院, 南京 210093)

摘要：人脸识别(Face Recognition)是一种依据人的面部特征(如统计或几何特征等)，自动进行身份识别的一种生物识别技术，又称为面像识别、人像识别、相貌识别、面孔识别、面部识别等。通常我们所说的人脸识别是基于光学人脸图像的身份识别与验证的简称。“人脸识别”在我们日常生活中随处可见，比如：大家进出校门、小区时候的人脸验证，网络上的各种人脸支付，登录 QQ 账号时的人脸识别等等。人脸识别是机器视觉的一种应用，本文将从行业背景、关键技术、应用实例和个人思考等四个方面来阐述人脸识别相关知识。

1 行业背景

人脸识别是一种基于人的面部特征的生物特征识别技术。近年来，人工智能技术在国内的应用遍地开花，科技巨头扎堆布局，很多资本开始青睐人脸识别，人脸识别技术逐步成熟，人脸识别在智慧城市、公共交通、公共安全和政府治理等场景中也得到了广泛的应用，显示出了显著的应用价值。2015 年来，我国也出台很多相关政策，推动人脸识别技术在中国更好的发展。

1.1 政策支持

2015 年以来，我国先后出台了《关于银行金融机构远程开立人民币账户的指导意见(征求意见稿)》、《安全视频监控人脸识别系统技术要求》、《信息安全技术网络人脸识别认证系统安全技术要求》等法律法规。为人脸识别技术在金融、安防、医疗等领域的应用和普及打下了坚实基础，扫清了政策障碍。

2017 年，人工智能首次写入国家政府报告，作为人工智能的重要细分领域，国家对人脸识别相关的政策支持力度在不断的加大；同年年 12 月，工信部发布《促进新一代人工智能产业发展三年行动计划(2018-2020 年)》，对提高人脸识别的有效检出率和正确识别率提出明确要求。人脸识别作为人工智能的一个重要细分领域，得到了国家政策的明显支持。

1.2 发展简史

人脸识别技术其实发展已久。早在 20 世纪 50 年代，人脸识别就被当作一个一般性的模式识别问题被研究了，当时主流技术主要基于人脸的几何结构特征，人工神经网络是当时别叫流行的分析工具，一直到 20 世纪 80 年代，这一阶段是人脸识别研究的初期，为以后的研究打下基础。20 实际 90 年代时人脸识别发展的高潮阶段，在这一阶段，人脸识别技术发展迅速，出现了很多经典的方法，例如 Eigen Face, Fisher Face 和弹性图匹配；并出现了若干商业化运作的人脸识别系统，比如最为著名的 Visionics（现为 Identix）的 FaceIt 系统。

直到现在，随着人脸识别研究的不断深入，研究者开始关注面对真实条件的人脸识别问题，主要包括以下四个方面的研究:1)不同的人脸空间模型，包括以线性判别分析为代表的线性建模方法、以 Kernel 方法为代表的非线性建模方法和基于三维信息的三维人脸识别方法。2)深入分析和研究影响人脸识别的因素，包括光不变人脸识别、姿势不变人脸识别和表情不变人脸识别。3)使用新的特征表示，包括局部描述符(Gabor Face, LBP Face 等)和深度学习方法。4)利用新的数据源，如基于视频的人脸识别、基于素描和近红外图像的人脸识别。

2 关键技术

一个人脸识别系统主要包括四个组成部分，分别为：人脸图像采集及检测、人脸图像预处理、人脸图像特征提取以及匹配与识别。

2.1 人脸图像采集及检测

人脸图像采集过程一般是通过摄像头等设备来获取的，不同的人脸图像通过摄像镜头采集得到，比如静态图像、动态图像、不同的位置、不同表情等，当采集对象在设备的拍摄范围内时，采集设备会自动搜索并拍摄人脸图像。

人脸检测就是把人脸图像中人脸的位置和大小等信息提取出来，主要是人脸图片上脸部特征点的坐标，主流的人脸检测方法基于以上特征采用 Adaboost 学习算法，Adaboost 算法是一种用来分类的方法，它把一些比较弱的分类方法合在一起，组合出新的很强的分类方法（第三次作业中介绍的集成学习方法）。人脸检测过程中使用 Adaboost 算法挑选出一些最能代表人脸的特征(弱分类器)，按照加权投票的方式将弱分类器构造为一个强分类器，再将训练得到的若干强分类器串联组成一个级联结构的层叠分类器，有效地提高分类器的检测速度。

2.2 人脸图像预处理

预处理是人脸识别过程中的一个重要环节。输入图像由于图像采集环境的不同，如光照明暗程度以及设备性能的优劣等，往往存在有噪声，对比度不够等缺点。另外，距离远近，焦距大小等又使得人脸在整幅图像中间的大小和位置不确定。为了保证人脸图像中人脸大小，位置以及人脸图像质量的一致性，必须对图像进行预处理。

人脸图像的预处理主要包括人脸扶正，人脸图像的增强，以及归一化等工作。人脸扶正是为了得到人脸位置端正的人脸图像；图像增强是为了改善人脸图像的质量，不仅在视觉上更加清晰图像，而且使图像更利于计算机的处理与识别。归一化工作的目标是取得尺寸一致，灰度取值范围相同的标准化人脸图像。人脸图像特征提取。

2.3 人脸图像特征提取

人脸识别系统可以利用的特征通常分为视觉特征、像素统计特征、人脸图像变换系数特征、人脸图像代数特征等。人脸特征提取是针对人脸的一些特征，又称人脸表示，它是对人脸特征建模的过程。

特征提取的方法有很多，常用的有 HOG，Dlib，CNN。接下里我展开介绍一下 CNN。

CNN，即卷积神经网络，简而言之，就是将输入的图像转化为一个向量表示。假设一个图片是 256 色的，那么可以将其转化为一个矩阵，每个像素点对应于矩阵中的一个元素。我们要做的就是识别这个矩阵的特征。用一个相对很小的矩阵在图片原始矩阵中从左到右，从上到下扫描一遍，每一个小矩阵块内，统计每种颜色出现的次数，以此来表达这个区域的特征。通过这一次扫描，得到一个由很多小矩阵区块组成的矩阵。这个矩阵比原始矩阵小一些，然后再重复扫描步骤，进行多次特征“浓缩”，最后将原始矩阵变成一个 1×1 的矩阵。而不同的图片，比如一个猫、一个狗或者一个熊，它们最后得到的这个数字会不同。

2.4 匹配与识别

提取的人脸图像的特征数据与数据库中存储的特征模板进行搜索匹配，通过设定一个阈值，当相似度超过这一阈值，则把匹配得到的结果输出。人脸识别就是将待识别的人脸特征与已得到的人脸特征模板进行比较，根据相似程度对人脸的身份信息进行判断。这一过程又分为两类：一类是确认，是一对一进行图像比较的过程，另一类是辨认，是一对多进行图像匹配对比的过程。

2.5 人脸识别的主要方法

基于几何特征的方法：几何特征可以是眼、鼻、嘴等的形状和它们之间的几何关系（如相互之间的距离）。这些算法识别速度快，需要的内存小，但识别率较低。

Belhumeur 提出的 Fisherface 人脸识别方法首先采用主成分分析（PCA）对图像表观特征进行降维。在此基础上，采用线性判别分析（LDA）的方法变换降维后的主成分以期获得“尽量大的类间散度和尽量小的类内散度”。该方法目前仍然是主流的人脸识别方法之一，产生了很多不同的变种，比如零空间法、子空间判别模型、增强判别模型、直接的 LDA 判 别方法以及近期的一些基于核学习的改进策略。

支持向量机使得学习机在经验风险和泛化能力上达到一种妥协，从而提高学习机的性能。支持向量机主要解决的是一个 2 分类问题，它的基本思想是试图把一个低维的线性不可分的问题转化成一个高维的线性可分的问题。通常的实验结果表明 SVM 有较好的识别率，但是它需要大量的训练样本，这在实际应用中往往是不现实的。而且支持向量机训练时间长，方法实现复杂，该函数的取法没有统一的理论。

基于 Hausdorff 距离(LHD) 的方法：心理学研究表明，人类在识别轮廓和灰度图像时一样快速和准确。LHD 是基于从人脸灰度图像中提取的线形图，它定义了两个线段集之间的距离。不同之处在于 LHD 不建立不同线段集之间的一一对应关系，能够适应线形图之间的微小变化。实验结果表明，LHD 在不同光照条件和不同姿态条件下都具有优异的识别性能，但在大表情情况下识别效果不佳。

3 应用实例

3.1 旷视科技

旷视科技创立于 2011 年，是一个人工智能产品和解决方案品牌。

旷视科技在金融、安防、零售领域都应用了人脸识别技术，发明了 Face++Financial，Face++Security，Face++BI 等垂直人脸验证解决方案；将人脸识别应用在互联网产品上，自己做研发，在美图秀秀、淘宝等互联网领域得到良好的应用；旷世与 OPPO、vivo、小米、诺基亚、荣耀、锤子等众多国内手机厂商合作，为这些手机安装人脸识别系统。

除了旷视之外，国内还有很多科技企业都在着重发展人脸识别技术。下图所示是一些重要公司比较占优的应用领域：

各公司实际领先的细分领域	
旷视科技	支付宝（刷脸登录）、园区门禁考勤、智能分析等商业应用；向机器人转型
商汤科技	主要提供 SDK、API 服务，拥有关键点贴图等商业应用（faceu、直播美化）；向 2B 应用转型
云从科技	银行、公安、机场、火车站等应用行业应用（农行超级柜台、建行校园 e 银行、广东省公安厅等）；继续深耕 2B 行业
依图科技	公安行业应用（福建省公安厅）；向智慧医疗转型

4 个人思考

4.1 好处

人脸识别技术是当下互联网时代中不可或缺的一部分，有很多好处，包括增加安全和保障，防止犯罪，减少人际交往，也为我们的日常生活带来了很多的便利。

执法机构用面部识别来追捕犯人或者寻找失踪的人，当面部识别与显示孩子几年后的样子的衰老软件相结合时，它甚至可以帮助找到失踪多年的人。当小偷进入商店时，企业主使用面部识别软件和安全摄像头来识别已知或可疑的小偷，这种先发制人的安全措施有助于防止入店行窃。

面部识别的便利性也超越了安全领域。不用现金或信用卡在商店购物，面部识别技术可以识别你的脸，并将商品记入你的账户。通过研究微妙的面部特征，在某些情况下它甚至可以帮助支持医疗工作，例如面部识别软件可以确定特定的基因突变是如何导致特定的综合症的，这项技术可能比传统的基因检测更快更便宜。

4.2 弊端

但技术是把双刃剑，人脸识别技术也带来了很多不可忽视的问题。

首先就是隐私问题，一些人不喜欢他们的脸被记录并存储在数据库中，以供未知的未来使用，与此同时，人们还担心面部识别数据的存储泄露，在国外，曾有黑客入侵银行、警察部门和国防公司去收集和使用面部扫描数据库。

人脸识别技术还为诈骗和其他犯罪提供了机会，不法分子也可以利用面部识别技术对无辜受害者实施犯罪，他们可以收集个人的个人信息，包括从面部扫描中收集并存储在数据库中的图像和视频，来实施身份欺诈。

4.3 如何对待

我们身为人工智能专业的研究者，要考虑到这不同的方面，权衡技术发展与社会影响．在努力发展人脸识别上，也要加强自己的社会责任心，造就一个更好的社会。

同时我认为政府需要尽快完善包括人脸识别在内的人体生物信息使用法律法规，采集人脸数据前须告知用途和可能风险，以保障公众知情权与选择权，防止企业过度收集和利用，对人脸数据存储权限做出明确规定，确保数据在采集、传输、使用和存储过程中的安全性，人脸数据应采取本地存储方式，禁止跨境流动，最后我们个人也要认识人脸数据的价值，增强隐私自我保护意识。

References:

[1] 人脸识别技术发展现状以及未来发展趋势 https://new.qq.com/rain/a/20201101A048PJ00

[2] 人脸识别长篇研究 https://zhuanlan.zhihu.com/p/105810423

[3] 百度百科：人脸识别 https://baike.baidu.com/item/%E4%BA%BA%E8%84%B8%E8%AF%86%E5%88%AB/4463435