

# 只要在人群中看你一眼 就永远记得你的脸

拿出手机购物,选好商品,在支付阶段却不用再输入密码,而是通过扫脸完成付款,这早已不是什么新科技。从马云在2015年3月CeBIT大会上的“刷脸”支付到微软推出的“刷脸”支付,关于人脸识别技术的讨论一直备受关注。也许你还不知道,目前计算机人脸识别的准确率已经高于人眼。

这种听上去极为酷炫的技术,在实践中非常“接地气”。相比于指纹、虹膜等许多其他生物识别技术,人脸识别更加容易大规模推广,因为几乎所有的用户都可以零成本参与。

本报记者 任志方

## 人脸就像 相貌上的指纹

在10年前,指纹识别还是一项新奇的技术,但现在许多手机的App都支持这种生物识别功能,甚至在千元机上都成为标配。在人脸识别的面前,指纹和密码都是小儿科。

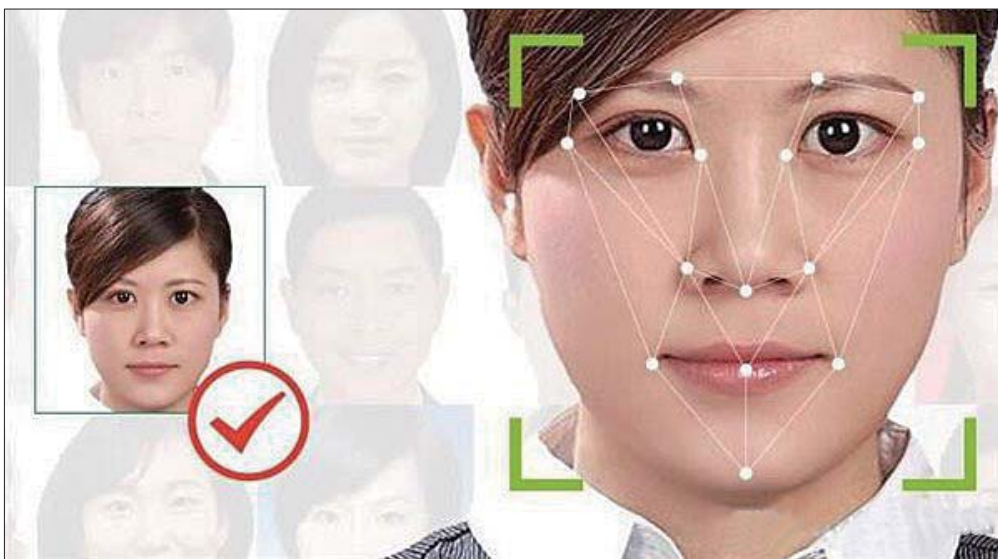
在生活中,如果有人说你长得像某个人,你可千万别相信,因为在这个世界上每张面孔都是独一无二的。在人脸识别技术面前,一对长相极为相似的双胞胎也有不同的特征。它会根据你的脸部特征产生一系列数字代码,只有你才能对应得上。人脸就像相貌上的指纹。

人脸识别技术研究始于20世纪60年代,但直到30年后,一些商业性的应用才逐渐进入市场。主要涉及移动互联网、智能硬件、公共安全、金融、监控、零售、娱乐等领域。在1996年上映的电影《碟中谍1》中,有这样一段情节,电影里追捕嫌疑人的探员汉纳威,在火车站利用同事传过来的目标人脸信息,通过隐形眼镜的系统识别迎面走来的所有行人,捕捉其脸部特征进而和数据库对接识别其身份信息,最终找到并抓捕嫌犯。电影里的桥段如今早已在现实生活中上演。人脸由于其易采集的特性,成为最易被接受的身份认证方式。

与可以数据化的代码不同,你的任何账号和密码只要通过验证都可以进行更改。而人脸识别数据则完全不同,人脸数据和指纹、虹膜等生物数据一样,改变成本非常高,甚至是不可更改的。近年人脸识别技术进步飞速,识别率达到99%以上,从而演变出来的功能也种类繁多并应用到各个领域。比如今年的高考和即将开始的司法考试,为了防止替考都应用了人脸识别技术。

就在7月12日,深圳机场的安检人脸识别系统正式投入使用,成为全国首家将人脸识别系统嵌入机场安检信息系统,实现两套系统一体化运行的机场。

这套系统通过安装在安检验证台后方的摄像头,在旅客到达验证台时迅速抓取脸部图像,并与旅客身份证件图像进行比对。当验证员人工读取旅客身份证件信息的同时,系统便可完成旅客脸部图像与身份证件图像的比对,并给出判别提示结果,辅助安检验证员完成对旅客乘机证件及身份的辨识。



## 需要辨认的 面孔越多越不灵

从识别能力来看,人脸识别技术有许多种。第一种是最初级的,也被称之为脸部探测。通常用于手机摄像头在拍照时对脸部自动对焦;第二种是脸部分类,分辨脸部肌理,比如微软或国内手机厂商推出的“刷脸”支付,能够判断的信息也有限。更高级的脸部识别技术有着更复杂的使用场景。比如马云说的“刷脸支付”,就涉及使用脸部识别技术进行用户身份核实。

分辨不同的面孔,对人来说,是我们通过眼睛获得视觉信息,信息经过大脑的处理被识别,然后分辨出眼前的是人、动物还是其他什么。这项看似简单的任务,对机器来说却并不容易实现。对计算机来讲,一幅图像信息,无论是静态的图片,还是动态视频中的一帧,都是一个由众多像素点组成的矩阵。比如一个1080p的数字图像,是一个由上千万个像素点组成的矩阵。机器需要在构成这些像素点的信息数据中,找出哪一部分数据是人脸,哪一部分是动物。

特征提取是实现人脸识别的关键一步,在这个步骤中系统通过一些数字来表征人脸信息,这些数字形成了一个人的脸部代码。常见的人脸特征分为两类,一类是几何特征,另一类是表征特征。几何特征是指眼睛、鼻子和嘴等面部特征之间的几何关系,如距离、面积和角度等。表征特征利用人脸图像的灰度信息,通过一些算法提取全局或局部特征。

这一步完成后就是人脸识别,即将提取到的特征与数据库中人脸的特征进行分类。而人脸识别又可以分为两大类:一类是确认,这是人脸图像与数据库中已存的该人图像比对的过程,回答你不是

是你的问题;另一类是辨认,这是人脸图像与数据库中已存的所有图像匹配的过程,回答你是谁的问题。两者之中,辨认要比确认困难,因为辨认需要进行海量数据的匹配。

之所以如此,是因为样本库的大小会影响识别精准度。如果样本库中只有一个样本,那么系统只需确认,这种1:1的对比精准度可以达到100%,但如果是1:N的对比,就会难很多,N的数值越大,难度系数越高,同时需要巨大的运算性能支持。换句话说,人工智能可以在数万张人脸中近乎完美地准确识别出你的脸,比人类更胜一筹。但是,如果人工智能面对百万张脸,人工智能不太达标。

## 识别不出来的1% 差在哪里

前面提到,人脸识别技术目前识别率达到99%以上,那么剩下的1%不准确在哪里?这就要说到复杂的技术要求和众多的限制条件下,造成的人脸识别失灵。

最简单的场景,如果想要区分双胞胎的人脸,依靠普通摄像头采集的二维图像或者视频几乎不可能。除非采用三维立体人脸识别,还要加很多限制条件。这类人脸识别技术,需要采集人脸的三维信息,一个普通摄像头是不够的。要么是两个普通摄像头加3D信息还原算法,要么专业的3D摄像头。但他们使用场景和条件约束非常多,所以很不常见。

人脸识别技术的关键在于通过不同脸部图像上眼睛、眉毛、鼻子、嘴巴、脸颊轮廓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。但是人脸是变化的,不同角度不同妆容都能影响特征关键点的抓取。如果只是简单的化妆,仅改变一些色彩,是不会对识别结果有很大影响。如果化妆

太过度,以至于人眼都觉得化妆后变了样,那机器也会产生误差。

## 谁会拥有 我们的“脸”

人脸识别如今已强大到这种地步,它可以用相机拍下面部信息,并存储到数据库中心,而这样做并不一定要事先获取你的同意。在我国,人脸识别已经用于反恐活动中,过去,不管是安检或者是警察破案时,对着视频只能人工识别犯罪嫌疑人,而今后这一现状将会被改变。目前我国的人脸识别技术水平已达到国际领先水平。此前,该技术已应用于国内一些重要会议之中,如APEC会议、全国两会、博鳌论坛等等。

但在商业领域,越来越多的社交应用也开始利用人脸识别技术,将用户的影像、照片和数据库中的各种资料联系起来。这种技术在带来便利的同时,也引发了人们对隐私泄露的担忧。

此前,Facebook因为未经用户允许而私自储存和使用用户的人脸识别数据而饱受诟病;而谷歌则因隐私政策和舆论压力而禁止谷歌眼镜使用人脸识别功能。在线上世界,互联网企业使用脸部识别技术的能力大大超越了在线下使用这项技术的水平。比如Facebook的新技术,专门用于在线图片的分析,能够在97.25%的识别中准确判断不同照片中是否出现的是一个人,而人类在同样的测试中正确率也只有97.5%。

在脸部识别技术准确率非常高的情况下,究竟是谁在掌握着我们的脸部数据?收集人脸数据,这桩生意所蕴含的可能性足够诱人。在可以预见的将来,人脸识别大规模应用已是趋势,但隐私保护、公共安全、商业应用三者之间的关系该如何处理,目前仍是个未解的难题。

【链接】

## 刷脸识网红 机器人还嫩点

6月30日,人机识别极限对抗大赛在杭州进行。决战双方是有着超强微观识物能力,人称“鬼才之眼”的王昱珩和人脸识别机器人“蜗可”。双方挑战的“道具”——50名青春靓丽的网络红人身着统一的服装站在舞台一边,舞台另一侧大墙上密密麻麻地贴着数百张网红的自拍照。

在公证员的见证下,观众从现场网红中随机抽取数位。对战双方需要对被选中者进行观察后,再从照片墙中挑出对应的照片。比赛共分三场且难度依次递进,前两个回合,双方打成平手。第三轮的“寻找网红童年照”却将人机双方置于极限挑战之中:十多年的成长蜕变足以让人的容貌发生巨大改变,辨识难度巨大。21分48秒,王昱珩率先按下按钮,提交答案。7分钟后,机器人“蜗可”也完成了识别。答案揭晓:王昱珩成功认出一位网红的童年照,并放弃辨认另一位,而此轮“蜗可”辨识的两位网红照片都出现差错。

赛后,王昱珩笑称事先并不知道比赛内容也未经彩排,“网红们的变化真的太大了。”人脸识别机器人“蜗可”的研发团队负责人陈继东则表示,人和机器各有所长,此次和人类最强大脑的PK,说明机器学习人类的大脑,“还有一段路要走。”

近两年,深度学习和大数据两项技术的相互作用,大大提高了人脸识别的准确率。生物识别智能开始进入商用,尤其是金融领域,成为数家互联网公司竞相追捧的香饽饽。在不久的将来,人脸识别技术或将逐步取代密码和手机短信校验码,用于互联网金融的身份验证基础平台。

资深专家陈继东表示,人脸识别的互联网级应用和金融级应用存在很大区别。“身份被盗用,直接导致财产的损失。”他指出,在金融行业,人脸识别技术的误识率要求非常高。“人脸识别的现实应用,不仅要做到在一堆照片中将同一个人识别出来,还需要将不同的人区分出来,这才是最难的一点。”陈继东强调,识别率和误识率应该综合起来看,尤其是在金融行业,必须把错误率设低。

研发人工智能机器人专家谢忆楠介绍,所谓深度学习,打个形象的比喻就是在“教小孩儿”。在深度学习的程序中,第一个步骤是人脸检测,即在一张照片中把人脸结构勾画出来。随后就要在人脸上进行关键点标注,这一步相当于“训练”程序学习观察人脸部特征。“这相当于一个监督式学习,我们会告诉机器人这个人到底是不是一个人。”久而久之,机器人会得出一些关键点参数。

谢忆楠举例说,人的两个瞳孔就是两个关键点,瞳距在判断人脸是否为同一人的过程中所占权重较高。众多关键点之间相互联系,形成一个统一的函数,该函数再对应不同人脸形成一个独有的数值。“每个人脸都有属于自己的数值”,谢忆楠说。以“蜗可”为例,它识别用户人脸是从二维图片中提取600多个关键点,进行交叉验证和动态识别。

(据《南方都市报》)

新知