

## 不要拒绝进步

记得上世纪90年代,汽车遥控器发明前,如果手拿重物,要想打开车门确实是件麻烦事。进入21世纪,轻按遥控器的按钮代替了把钥匙插进锁眼旋转的复杂动作。而现在,大多数汽车都装备了无钥匙进入系统,开车门变得更加轻松而潇洒。

如果仔细观察,你会发现,我们身边这样的技术进步比比皆是。当你自如地应用这些先进技术,享受这些科技带给你的快乐和便捷时,不要忘了,这些新技术在刚诞生时,曾经被大多数人拒绝。汽车遥控器刚出现时曾被认为会增加汽车被盗的风险,导致给汽车安装上机械的排挡锁和方向盘锁曾在十几年前的中国非常流行。数码相机

的出现,也让一些摄影爱好者质疑,他们固执地相信只有胶片相机才能拍出最出色的画面,甚至为此囤积大量的胶卷。

本期要介绍的人脸识别技术也面临推广的瓶颈,抛开目前成本较高不谈,大多数人对实体钥匙的信赖让这项技术平民化还有很长的路要走。有人认为人脸识别遇到光线太暗的地方就会失效,有人认为整容后就无法识别,还有人认为生物特征信息的采集会泄露公民的隐私给社会造成混乱。但不管怎样,科技的发展不是传统守旧意识可以阻挡的。尽管新技术会有这样那样的不足,但是毕竟这是科技的进步,我们没有理由拒绝。

## 人脸识别:将让钥匙成为历史

■本报记者 童岱

美国大片《碟中谍4》中的这些场景肯定让你印象深刻:目标人物出现在人头攒动的火车站,特工的眼镜将看到的人脸信息自动搜集并比对分析,迅速锁定其行踪;迎面而来的美女杀手让特工的手机发出嘀嘀的报警声,上面显示的是杀手姓名和信息……这便是人脸识别技术。

11月14日,记者走进清华大学电子工程系教授苏光大的实验室,这里摆放了多种人脸识别识别仪器设备,体验了一把这早已不是科幻的技术,但仍让人感觉很新鲜。

## 不到两秒便能确定身份

在实验室的一角,记者看到一台类似于摄像机、电子扫描机和电脑组合的设备,这是二代身份证人脸识别系统。按苏光大的要求,记者站在摄像机前,将自己的二代身份证贴在电子扫描机上,不到两秒的时间,记者的视频头像、身份信息以及身份证上的照片都被录入并显示在一旁的电脑屏幕上,并伴有语音提示:“身份核实,比对成功。”

说起来很简单,通过一台计算机,把一张人脸和身份信息对应起来。“人脸识别技术,是利用电子设备对人的脸部特征信息进行身份识别,是生物识别技术的一种。”苏光大说,人脸识别的过程其实并不复杂。首先是检测人脸,通过计算机判断输入图像中是否存在人脸,存在的话便显示出其位置和大小。然后是定位面部特征,对识别出的每张人脸,都会记录五官细节及其脸部轮廓信息。最后一步便是人脸比对,根据已定位的面部特征与数据库中的的人脸比对相关信息,判断其身份。

由于人脸识别系统信息的存储方式,仍是以计算机能识别的数字或代码为主,和其他电脑信息一样会受到黑客的威胁。不过只要对存储的人脸信息加密,即使是黑客盗走了“人脸”,也难以识别和利用。这就决定了人脸识别具有传统身份鉴定方式所欠缺的安全性、保密性,而且很方便。

具备了这些特点,人脸识别技术也让全球的巨头们趋之若鹜。Facebook(社交网络)在其网站上引入了人脸识别功能并收购了一家脸部识别网站;谷歌也接连收购了两家做面部识别的公司;英特尔还发布了以机器视觉为核心的感知计算软件开发工具包……这表明,人脸识别正在摆脱“非主流”,这项技术所展现的世界,或许将比Google Glass(和智能手机具备同样功能的)更有型。

## “我用不着钥匙开门了”

11月15日,和往常一样,汉王科技产品部副总经理石践到公司上班,走到办公室所在的楼层门禁,他站在普通电话机大小的人脸识别门禁处,头像随即显示在门禁的小屏幕上,内置的识别系统扫描了他的脸部特征确认后,门禁便自动打开,识别过程只用了一秒。

接着,石践走到办公室门前,门锁处有一个手机大小的屏幕,上面有个内置摄像头,他按了一下门锁上方的黑色按钮并看着摄像头,头像便显示在屏幕上,1秒不到,办公室门便自动开启。

“正像你刚才看到的一样,进入办公大楼后,我用不着钥匙开门了。”石践告诉《中国科学报》,目前国内已经有许多企业开始使用上述人脸识别门禁考勤系统,在国内的人脸识别门禁考勤市场上,汉王的产品已占到了70%,在汉王出口的人脸识别门禁考勤产品中,销往美国的比例占到了25%。

而石践办公室门上的人脸锁,则是汉王目前正在推进的项目,在今年各地举办的安防展会上,这个装置吸引了众多眼球。这个装置支持人



苏光大教授实验室内的二代身份证人脸识别系统,不到两秒便能对拍摄的人像和证件作出比对。

本报记者童岱摄影

“以后我们到家开门时,不再再在包里翻来翻去找钥匙,对着门口的人脸识别系统“刷脸”确认身份,便可进门。“这不是科幻,而是技术上已实现的现实,现在的阻力在于成本和老百姓对人脸识别的认知度,这个阻力我预计3~5年便能解除。”清华大学电子工程系教授苏光大说。



人脸识别的优势在于定位面部特征,五官细节及脸部轮廓信息是关键识别信息。汉王科技供图

脸、密码和钥匙三合一开锁,用户可以按自身习惯选择,操作起来也挺方便。

同时,锁体上的摄像头还附带拍照功能,每一位试图进入办公室的人员都会被拍照留档,照片最高存储量达到100张可以实现循环存储,也可以随时用U盘将存储的照片进行保存。尝试强行进门的人员,如果其脸部特征没有提前录入人脸锁,尝试三次开锁之后,识别系统便会发出警报。

“人脸锁的耗电量我们也尽可能地做到最低,现在只需要四节五号电池可以保证一年时间的使用。”石践说,人脸锁的适用场所不会局限于办公大楼、机要室、财务室等办公场所,个人住所将来也可以用得到。

值得一提的是,以往的人脸识别门禁考勤总是需要大型计算机的协助才能完成,但汉王在2008年开始上市的人脸通产品,已经将比对过程从PC平台转移到指甲盖大小的芯片上,这也使得成本价格正在趋向于平民化的路线。

## 人脸识别门禁锁靠谱吗?

说到民用,人脸识别的安全性到底如何?苏光大告诉《中国科学报》,人脸识别门禁若是用在

个人住所中,比用钥匙开门更便捷,安全性同样也得到了提高,犯罪分子不可能像从前那样复制钥匙或是通过开锁工具进门盗窃或抢劫。“要知道,现在一般的门锁,很难有开锁公司开不了的,小偷们也在与时俱进,许多复杂的安全防盗门在他们眼里也不是太大的难题。”

对此,也有人提出质疑,对于人脸识别门禁,如果犯罪分子通过其他渠道拿到居民的照片,是否也能达到开门的目的。

对此,中国科学院自动化研究所博士张小博表示,这就涉及到防伪功能。人脸识别技术做得不过硬的话可能有两方面的问题,一方面是活体比对系统是否完善,通常而言,门锁中无论是嵌入计算机还是芯片,都可以利用三维成像技术比对预存的人脸信息,从而防止用照片就能开门的笑话。安防行业使用的人脸识别系统大多数是动态识别,是通过监控摄像头进行动态采集实时图像与数据库预存的模型进行比对,如果多次比对失败,便会实时启动报警预案。

另一方面,便是恶劣光线问题。早期的人脸识别技术,对于光线过暗,或者是亮度太大,都会导致人脸比对失败。但近红外人脸识别技术可以解决这个问题。

## 延伸阅读

■本报记者 童岱

早期的刑侦案件中,办案人员会让目击者将嫌疑人的面部特征,向画师描述,再由画师依描述所绘制的素描图来协助破案。素描对嫌疑犯相貌的还原程度,与目击者的描述能力以及画师绘画的能力相关,有时会出现较大误差。

但现在,只要嫌疑犯出现在任何公共场所的摄像头下,利用人脸识别技术,几秒钟就能用计算机比对并核实身份。

## 将手绘变为计算机语言

1989年,清华大学电子工程系教授苏光大和他的团队受公安部委托,承担了名为“GA计算机人像组合技术”的研究项目,他们利用计算机将人脸分为头发、脸型、眉毛、眼睛、鼻子、嘴巴这六个区块,每个区块设置不同的类型,这样一来,通过目击者挑选,工作人员将区块组合成嫌疑人的脸,从而帮助破案。

与过去素描肖像相比,这种利用计算机组合的人脸图像能更快速的成像,也更容易对图像进行修改和微调。1994年,武汉市公安局利用该技术破获了持枪抢劫特大案件,这也成为我国利用人像组合破获的首起成功案例。此后,这项技术也成为公安部门的必备装备。

“二代身份证的出现,是拓展人脸识别技术的一个契机。”苏光大说,对于警方而言,根据

## 国内人脸识别始于协助破案



重庆枪击哨兵案案犯周克华踩点监控图像,头像只有3×4像素,苏光大将其重建成像。

二代身份证上的人像就可以构建规模巨大的人像数据库。

2008年1月,根据公安部门提供的身份信息,苏光大团队建立了国内首套千万级数据库的人脸识别系统。如今,这个数据库的人数已经过亿。警方在侦破案件时,通过监控摄像头得到的嫌疑犯画面图像,便可以从数据库中迅速比对其身份信息,确定其窝藏地点,加快破案速度。

## 超分辨率技术解决“看不清”

然而,在公安部门实际的破案过程中,常常



案犯周克华(左为重建像) 苏光大供图

会遇到视频监控场景中的人脸图像分辨率非常小,这也让办案人员常常陷入困境。为了使模糊人脸图像得到清晰度的重建,2010年7月底,苏光大完成的“数字影像资料处理及检验技术”通过了公安部的验收。令他没想到的是,这项技术很快得到了应用。

2010年12月,苏光大接到一通不寻常的电话,内蒙古准格尔刑警队的警员在电话中寻求帮助,他们手中的犯罪嫌疑人人脸图像模糊,无法辨认。

“当时他们传给我的那张图像是由路边的监控摄像头拍到的,像素非常低,等我将在图中人像

## 正在被改变的生活方式

多年以来,人脸识别技术在应用层面被“困”在安防领域,而这几年,相机、电视以及互联网公司的频繁介入,这项技术越来越“亲民”。

如果你手边有尼康、索尼等日系的相机,使用时,会发现相机对于笑脸的识别,以及根据脸部区域进行对焦会非常方便,所以说,你就早体验过了人脸识别。

智能电视作为家庭娱乐的终端设备,在智能交互方面也用上了人脸识别。石践说,包括联想、海尔、海信等公司出品的智能电视,其人脸识别的技术核心都是汉王提供的。一家三口可以将自己的脸部特征通过内置在电视中的摄像头录入,然后整理出自己喜欢的频道。再次使用的时候,摄像头会对坐在正前方的用户进行人脸识别分辨出是哪位用户,然后用户就可以立刻观看自己喜欢的节目了。

手机自然也不会例外,被Facebook收购的Face.com最近也在App Store中推出了应用人脸识别的手机拍照应用KLIK。这款应用所主打的并不是丰富的滤镜功能,而是社交分享功能,它能够在拍照过程中就自动将拍摄对象的身份从画面中识别出来,并且迅速分享到用户关联的Facebook等社交网站的账户。

到银行ATM机取款的方式将来或许也会发生变化。我们常看到这样的新闻:犯罪分子通常抢劫受害人的银行卡并逼问出新密码后,会在ATM机取走钱款。苏光大透露,国家相关部门正在和银行系统酝酿一个计划,一旦实现,这将杜绝这种犯罪途径。这个计划是将个人的银行卡信息和二代个人身份证结合起来,ATM机也将装载人脸识别系统,用户想在ATM机上取款,用身份证就可以实现,取款过程中,ATM机上的摄像头将实时记录取款人的脸部特征,并迅速比对其身份证上的照片,核实身份后方可取款,如果核实失败,将无法取款。

## 无法回避的隐私问题

2011年,Facebook将人脸识别功能引入欧洲市场。网站扫描了用户上传的数亿张照片,对用户和好友建立了人脸特征数据库。根据这一数据库,用户未来在上传新照片时,Facebook将会自动提示是否根据其中的用户名标注标签。随后开始被欧洲各国的消费表示不满,今年9月底,面对欧盟官员的压力,Facebook承诺在欧洲市场去除网站使用的人脸识别技术和功能。

苏光大认为,包括人脸识别在内的生物识别技术,若是用于维护公共安全,比如机场、海关、公安部门等,只要相关部门注重对采集的生物特征信息保密,合法使用,侵权的可能性较小。

张小博则表示,只要是采集公民的生物特征信息,就存在信息泄露的风险,尤其在民用这一块,国家有必要出台或完善相关的法律法规,保障公民的个人信息安全。已经进入立法阶段的中国《个人信息保护法(草案)》中,将所有能识别的个人信息都列为保护范畴,甚至包括了个人图像和声音。无论如何,珍惜你手中的钥匙吧,或许用不了几年了。

## 人脸识别亮相奥运会安防

放大后才发现,人像的像素是4×6,肉眼完全无法辨认。”苏光大说,当时他将这张人像放入他们研发的软件中进行了电脑复原、重建头像,准格尔警方依据重建后的高清晰度头像,很快便破了内蒙古准格尔旗凶杀案。

公安部A级通缉犯周克华同样也是一个典型案例。苏光大说,周克华在重庆作案后,他就受到重庆警方的邀请去协助破案。根据重庆警方提供的视频信息,他将放大的犯罪嫌疑人的头部模样进行了重建还原,破案后,两者头像对比,误差同样很小。

## 人脸识别亮相奥运会安防

国内在人脸识别领域的权威机构,除了清华大学,还有中科院自动化研究所和中科院计算技术研究所。自“9·11”事件,2004年伦敦地铁爆炸案等恐怖袭击发生后,国内的学者们开始关注公共安全领域。经过多年的积累和沉淀,人脸识别技术终于在2008年奥运会上有了大型应用,这也成为这项技术在国内应用的里程碑式事件。

当时,北京奥组委对开幕式、闭幕式入场进行了实名制管理,入场券持有者需要提交个人近照,在入场验票时利用人脸识别技术进行实名制身份认证。当时,技术提供方便是清华大学的苏光大团队和中科院自动化研究所以及其他单位合作完成。

## 生物识别有些啥?

■曾笑生

早期的人类过着穴居生活时,为了防备野兽的袭击,有时会推动巨石挡住洞口,这个时期,人便是“钥匙”。随着时间的推移,粗陋的木栓成为最早期的锁具,并逐渐演变成了更为结实的金属锁栓,随着簧片的发明和机械加工工艺的不断提升,各种制式的锁具便诞生了出来,为了打开它们,需要特定的钥匙。

到了现在,无论你是否曾注意到,锁具和钥匙正在被包括人脸识别在内的生物识别技术所带来的改变而淘汰。



## 指纹识别——安全指数:★★★

由于指纹具有终身不变性、唯一性、方便性,使得指纹识别已几乎成为生物特征识别的代名词。许多单位和部门门禁、考勤系统都已得到应用,就连笔记本电脑、手机、汽车等都已有了应用的指纹识别。

但其缺点也很显著,手指多汗、有灰尘或是磨损严重,都使得识别时难以成像,影响通过率。甚至有不少白领为了早上多睡会儿,还在中关村的一些小店里仿制了自己的指纹膜,20来块钱就可以搞定,这也造成了用人单位的烦恼。当然,最新的生物射频指纹识别技术可以解决防伪的问题,只是成本又成了问题。



## 静脉识别——安全指数:★★★★

静脉识别是根据血液中的血红素有吸收红外线光的特质,将具红外线感应度的小型照相机对着手指进行摄影,即可将沿着血管的阴影处摄出图像来。比对时,同存储在识别仪器中静脉特征值比,采用复杂的匹配算法对静脉特征进行匹配,从而对个人进行身份鉴定,确认身份。

其最突出的优点在于静脉隐藏在身体内部,被复制或盗用的几率很小。使用时也不用接触仪器,使用者心理抗拒性低,受生理和环境因素的影响也低,所以安全指数很高。但是,随着年龄增长,静脉识别是否会发生根本性的变化暂无定论。



## 虹膜识别——安全指数:★★★★★

由于人类的虹膜结构组成复杂且具有唯一性,虹膜又被称为“第二指纹”。人的虹膜在岁左右就基本发育完全,进入相对稳定期。虹膜识别技术将虹膜的可视特征转换成512个字符的Iris Code(虹膜代码),存储后可供后期识别所用。除了唯一性的优点外,虹膜识别技术还具有稳定性、防伪性、识别准确等特点。

这些优势也使得虹膜识别成为安防领域最为推崇的生物识别技术之一。有一个有趣的例子,2003年3月18日,阿布扎比(阿拉伯联合酋长国之一)宣布世界上第一套国家级的虹膜追踪与国界控制系统开始启用。这套系统从2001年开始建设,它的目的是对阻止所有被阿布扎比所驱逐的游客及其他人员进入阿布扎比。在以前没有这套系统的时候,由于被驱逐的人员中多数是阿拉伯人,许多都拥有“大胡子”的面相特征,海关检查人员很难区分哪些是被驱逐的人。通过使用这套系统,非法入境的情况得到很好的控制。

人脸识别及上述三种识别方式,是生物识别中目前应用最广的四个类别,此外,还有DNA识别、语音识别、行走步态识别等。

由于这些人体特征是人体所固有,这些生物密钥无法复制、被盗或被遗忘。这些使得生物识别相比传统的身份鉴定方法更安全、更方便。