ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.13, No.34, Dec. 2017
E-mail: eduf@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

浅谈“刷脸识别”的伦理问题

刘莹[1,2]

(1.中国人民大学信息学院,北京 100872;2.北京达因军惠网络技术有限公司,北京 100013)

摘要:“以貌取人”的时代到来了,通过“刷脸”的业务应用呈爆炸式增长。苹果公司近期宣布iPhone X手机使用“刷脸”方式了;去银行ATM取款可通过刷脸方式;进机场及火车站,要通过人脸核验;通过“刷脸”就可以畅通无阻的进入小区等。“刷脸”无处不在,这是一个大数据共享、开放的“刷脸”时代,只要我们带着一张脸,我们无时无刻都被暴露在“第三只眼”的监视之下,因此,“刷脸”技术带来了个人隐私保护的隐忧,也带来了个别组织对“人脸”数据的滥用或垄断的担心,特别是由“刷脸”带来的产品的安全性与责任问题并对传统伦理观带来了新挑战。

关键词:伦理问题;刷脸;人脸识别技术

中图分类号:TP18　　文献标识码:A　　文章编号:1009-3044(2017)34-0185-03

DOI:10.14004/j.cnki.ckt.2017.3883

“以貌取人”的时代到来了,通过“刷脸”的业务应用呈爆炸式增长,苹果公司近期宣布iPhone X手机使用“刷脸”方式了;去银行ATM取款可通过刷脸方式;进机场及火车站,要通过人脸识别核验;在网上进行证券开户,需进行刷脸人证核验识别比对;上网进行购物可通过“刷脸”进行支付;没有携带有效身份证入住酒店,可通过“刷脸”入住;没带小区钥匙,通过“刷脸”就可以畅通无阻的进入小区;走在大街上,闯了红灯,也可以通过抓拍、比对、识别人脸,把人给找出来等等……;这真是一个“刷脸”的时代,无论你走到哪里,只要一张脸,就可以把你的身份信息识别出来,把人从中识别出来;这是一个大数据共享、智能、开放的“刷脸”时代,只要我们带着一张脸,我们无时无刻都被暴露在“第三只眼”的监视之下,因此,“刷脸”技术带来了个人隐私保护的担忧,也带来了个别组织对“人脸”数据的滥用或垄断的担心,特别是由“刷脸”带来的产品的安全性与责任问题并对传统伦理观带来了新挑战。

1 何谓“刷脸”技术?有何局限性?

“刷脸”识别技术是基于人的脸部特征,对输入的人脸图像或者视频流进行分析。判断识别过程:首先判断是否存在人脸,如果存在人脸,则进一步的分析每个脸的位置、大小和各个主要面部器官的位置信息。并根据这些信息,进一步提取、分析每个人脸中所蕴涵的身份特征,并将其与已知的人脸进行对比,从而判定人脸的身份。

而人脸身份的判定结果是根据两张人脸比对相同率的高低计算来确定的。每个人脸识别厂商根据算法不同、识别准确率的不同在不同的使用环境下推荐其不同的识别阈值。所谓阈值:就是判别同一个人的标准值;即当比对识别两张照片的结果值大于或等于阈值时,即可判定这两张人脸为同一人;当比对识别两张照片的结果小于阈值时,即可判定这两张人脸为不是一个人;而每个人脸识别厂商推荐的阈值中,都会存在所谓的误识率。因此说现在人脸识别技术还不能达到通过“刷脸”的方式精确的100%判别为同一人。

虽然现在有的公司或媒体称:人脸识别依赖面部3D构型,绝大部分化妆不会改变人脸的3D轮廓;人脸识别技术是处理大量来自面部的数据信息,比如说面部结构、五官、肌肉等,还有的公司号称正在研发眼纹识别技术等等……但人脸识别的过程是较复杂的过程,难免或多或少的在人脸抓取、分析、识别的过程中存在一些其局限性。例如:① 抓取人脸时带不带口罩、帽子、围巾、墨镜或眼镜等都会影响其人脸比对的识别率;② 对整容过或在化浓妆时的人脸判别也会影响其识别率;③ 而对相似的两张人脸的判别误识率是比较高的(例如:双胞胎姐妹或兄弟、包括极其相似的两人):本人曾在公司做过这样的实验:用不同的厂商的人脸比对识别的算法,把人脸识别的阈值设置不同,比对判别的结果也会不同;当阈值设置较高时,比对判别的误识率较低,但对于抓拍人脸的质量要求就较高;当阈值设置较低时,而比对判别的误识率也较高,如果是极为相似的两个人,比对识别通过率就较高。因此,人脸识别技术还存在一些其局限性,不可能达到100%的准确无误的判别。

2 “刷脸”业务的主要应用

1) “刷脸支付”业务:随着苹果公司近期宣布iPhone X手机支持“刷脸”。使“刷脸”话题又一次在网上火爆起来,许多人甚至一夜未眠—怕“脸”被借刷。在苹果公司的光环下,“刷脸”支付业务有可能很快在大家身边更快的流行起来了。其实“刷脸”业务的应用并不是什么新鲜事,例如:天坛公园厕所取厕纸必须进行刷脸,刷一次只出60厘米长的纸,十分钟之内不能重复刷脸拿纸,目的是防止个别人多次重复取纸。“刷脸”支付也已经不是什么新鲜事情,百度公司是最早布局“刷脸”支付的互联网公司,而在2015年汉诺威IT博览会(CeBIT)上,马云在现场演示“刷脸支付”,更引爆社交网络。再到京东在今年6月,宣布金融内部测试“刷脸支付”及8月底京东金融推出“刷脸支付”,并推广到线下。这样互联网“BAJ”公司都已经入场“刷脸支付”领域,“支付”比“登录”或天坛公园“刷脸”取纸的业务应用更加复杂,因“刷脸支付”距离资金更近,安全性要求更高。

收稿日期:2017-10-15

作者简介:刘莹(1975—),女,山东莱芜人,技术经理,研究生,研究方向为管理科学与工程。

另一方面,“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:白天和晚上的光线不同、不同人群面对摄像头的角度和姿势各异,识别难度更高。而“刷脸”支付如造成经济损失谁来负责?是否有明文的法律规范?

2)“刷脸取款”业务:今年九月份,建设银行陕西省分行已开通“刷脸取款”业务,客户首先在ATM上通过输入手机号验证身份确认开通“刷脸取款”业务后,即可使用的“刷脸取款”,最快仅需几十秒。开通后,首先在ATM机上点击“刷脸取款”,输入银行预留手机号码,注视屏幕上方的摄像头,输入取款金额就会吐出钞票。其实银行“刷脸”取款的技术背后也是人脸识别,通过机器自动抓取人的现场人脸照片,然后再与银行已采集的可信照片进行对比,最后输入电话号码或身份证号进行身份确认,输入账号密码即可完成取款。但在“刷脸”取款时,对抓取人脸时有其要求:对整容时进行削骨等操作幅度太大时,那很有可能出现人脸核验失败,这时候需要用户重新更新身份证照片信息等。另一方面,当是双胞胎的两个人或极相似的人时,而“刷脸取款”无需携带银行卡,只需要知道手机号和身份证号,“刷脸”验证就可以取款成功。这样就会出现安全隐患,当卡还在卡主人身上,资金不翼而飞,出现这种情况的经济损失,谁来买单?而最近,“刷脸取款”银行业务已在目前包括招行、农行、建行、汇丰等多家银行,已经在ATM机和手机银行客户端实现了其功能。

3)“刷脸”其他业务应用:“刷脸考勤”这项应用应该比较成熟并且大范围内应用。公司的每一位员工需在手机上下载公司的APP管理系统,当员工到达公司后(即进行位置定位),连接公司WIFI,然后登陆APP系统对准脸部进行拍照,自己做出记录,即可完成考勤。“刷脸”门禁系统:在小区的大门上安装了“刷脸”核验机,首先要进行小区业主人脸的采集,当每次业主进行小区时,进行刷脸核验、比对成功后即可进入小区。“刷脸进站”:在兰州、柳州火车站等及国内很多机场都已经开始采用“刷脸”核验技术。“刷脸”无证入住酒店:在酒店前台的“刷脸”核验设备上,到店顾客可以直接点击触摸屏上的“未携带身份证件”,输入身份证号码,屏幕跳出摄像头,人脸识别后,即可直接办理入住,整个过程不到1分钟,就这样将“刷脸入住”带入了公众视野。“刷脸”业务还有很多很多,就不在这一一列举。

“刷脸”这项听上去高大上的技术,正在迅速扩张壮大起来,正在向我们的百姓公众生活走来。当前“刷脸”识别技术还面临一些挑战,从外界环境与条件来看,用户在进行人脸抓拍过程中的姿态、光照、遮挡、图片清晰度等都会影响到效果;从人自身的变化看,从小到老,会发生一些变化,识别变化会比较困难。另外对于双胞胎或极为相似的两人也很难识别。例如:伦敦警方最近试用了一种新的面部识别系统,但是他们犯了一个令人十分尴尬的错误。在诺丁山狂欢节上,警方使用这项技术搜寻嫌疑人时,发生了大约35次错误的身份匹配,并且其中一人被“错误地”逮捕。因此,下一步人脸识别技术需要提升自身应对攻击和复杂环境的能力,动态监控的精准度还需要提升;另外还需要提升识别运行速度,增进用户体验,不能让正在进行“刷脸”识别的用户等太久。

3 “刷脸”引起的个人隐私伦理问题

随着互联网与各种智能设备的普及,“刷脸”业务呈爆炸性增长,“刷脸”业务随处可见,则有可能在人们不知不觉间就会被采集到,更加重了公众的心理顾虑。如今的“刷脸”技术随还未完全成熟,差错率和安全性还有待检验。而且虽然人脸是“弱隐私”,但生物特征是独一无二的。人类的生物特征数据库如果一旦被泄露或盗取,风险后果可能比信息泄露还要大。

“人脸”信息应该是最容易被采集到的,人脸信息在人们不知不觉中就会被采集走。现在处于大数据、人工智能、数据共享时代,无论你走到哪,通过人脸信息很快就会把的身份信息分析出来,随之而来的人们生活轨迹、日常爱好、个人隐私就都会被挖掘出来。因此,“人脸”数据来了个人隐私保护的隐忧,也带来了个别组织对数据的滥用或垄断的担心,特别是人类自由可能被侵犯,由此产生了“刷脸”时代人类的自由与责任问题并对传统伦理观带来了新挑战。

人脸识别技术为数据的采集提供了方便的技术手段,而大数据共享形成了从“人脸信息”到“身份信息”再到“个人隐私”的一个全方位的监控,构成了立体天罗地网的关系网。利用现代智能技术,可以在无人的状态下每天24小时全自动、全覆盖地全程监控,毫无遗漏地监视着人们的一举一动。在随处可见的人脸抓拍设备,我们的一切活动都被智能设备时时刻刻盯梢着,跟踪着,让人真正感受到被天罗地网所包围,一切行为和思想都暴露在“光天化日、朗朗乾坤”之下,就像未穿衣服行走在大街上。而我们的人脸信息,以数据编码的形式保留下来,它可通过互联网快速传遍各种组织世界并存储于数据云端,易传播,易存储,一旦进入网络就很难于彻底清除,因此也就容易永久保存,不易消逝。 就这样,只要我们带着一张脸走到哪,就无时无刻的被监控着、被跟踪着。

随着数据共享时代的来临,,数据成了一种土地、资本、能源等传统资源之外的一种新资源, 数据成了一种新资源独立的客观存在,这种新资源已成为这个时代的标志, 成了物质世界、精神世界之外的一种新的信息世界。因此,数据的所有权、知情权、采集权、保存权、使用权以及隐私权等,就成了每个公民在大数据时代的新权益,这些权益的滥用也必然引发新的伦理危机。而人脸生物信息数据的使用应该谨慎,类似的还有虹膜、指纹等生物特征信息,生物特征是世界独一无二的,一旦丢失将不可挽回,如果这些后台数据被攻击截获、被泄露,被不法分子利用,那么后果不堪设想。

“刷脸”技术带来的第一大伦理危机是个人隐私权问题。通过我们的人脸信息,可知例如人脸面部特征、年龄、性别等,再通过大数据共享,进一步可知个人身份信息、健康状况、收入水平、家庭成员、教育程度……,只要是我们不愿意公布的,都可以看作是个人隐私。在大数据共享时代,传统的数据保护举措不再有效,那些传统的限制条件也不再存在,因此对隐私保护形成了巨大的挑战。

个人稳私权的伦理问题首先涉及的是人脸信息采集权的问题。我们出门都会带着一张脸,而且大多情况不会进行遮挡。而人脸信息的采集技术非常成熟,人脸采集设备在大街小巷随处可见,在你不知不觉的时候,也许只需一两秒的时间就会把你的人脸信息采集完成。而从人脸信息就可以分析到你的身份信息、生活轨迹信息等等,都在我们不知情的情况下被记录和储存下来。

个人稳私权的伦理问题另外一个重要问题是人脸信息的使用。虽然人脸信息属于“弱隐私”,但也是人类独一无二的生物特征。人脸信息一旦被上传互联网,则会立即被永久性地保存下来,就像白纸染上墨迹一样,我们很难彻底清除。而人脸信息与其他数据进行交叉、重组、关联等操作,就会把个人的大量

稳私信息被挖掘出来。而人脸是人类辨别个体不同的最直观最有效的方法之一,也许有一天你上网查询信息时,发现你的人脸照片在其中,而且标注大量的个人稳私信息。或许有一天你走在大街上,成了名人,莫名其妙的被人指点、谈论。

大量的人脸数据也意味着巨大的风险,需要有一个合理的法律条文和道德底线为基础,如何将人脸识别集成到人们生活领域。使这些数据即可为我们带来经济效益和社会效益,又可以有效的保护我们的个人稳私。

首先,我们要坚持伦理底线。人脸信息随时随的在我们的生活中产生、传输、存储和使用,所以我们在人脸数据的采集、使用中必须遵循一定的伦理规范,确保他人的人脸信息不被盗取和不受侵犯。

其次,我们就加强立法工作。人脸识别技术是一种新技术,我们的时代也因此迅速迈入"刷脸"时代。但是,由于人脸识别技术发展过快,原来诸多法律、法规面对现有的人脸识别技术都显得无能为力,因此必须重新立法,对人脸数据的采集、使用、储存和删除各个环节都有一定的法律约束。对非法使用人脸信息的"黑科技"进行打击,并要求数据挖掘者、数据使用者承担其相应的法律责任。此外,由于互联网技术,人脸数据可以永久被存储,这有可能给他人个人隐私带来伤害,因此应该立法规定数据的存储、使用期限,数据存储者负责到期信息删除用来保护当事人的权益等。

最后,我们要有一个开放的共享态度。我们身处在互联网、刷脸、人工智能、大数据时代。人脸识别技术是这个社会经济需求和科技内逻辑两种合力的推动下出现的,因此都有其发展的必然性。我们保持开放和共享的态度,让人脸信息资源发挥其最大的价值,让我们的时代数据信息资源更加丰富。

对"刷脸"识别技术,我们既要对其充满信心,用开放、包容的态度来看待其中不尽完善的地方,也要保持理性、审慎的姿态应对"刷脸时代"的到来。在想让全民共享人脸识别技术的成果时,我们遇到了从前没遇到的行为轨迹、隐私保护、行为预测、人性自由等诸多问题。我们要加快建立健全人脸识别技术使用统一标准,我们应制定和遵循新伦理及规范制度,使人脸识别技术更好地为人们生活服务。

参考文献:

[1] 黄欣荣.大数据时代的伦理隐忧[N]. 大众日报,2015.
[2] 黄欣荣.大数据时代的思维变革[J]. 重庆理工大学学报,2014.
[3] 邱仁宗.大数据技术的伦理问题[J]. 科学与社会, 2014.
[4] 彭颖. "刷脸"消费时代来临了吗? [N].南方日报, 2017.
[5] 王乾. 论大数据分析的方法论意义[J].武汉科技大学, 2015.

(上接第180页)

$$y(t+k)=e(t)+f(y(t+k-1),\cdots,y(t+1),y(t),\cdots,y(t+k-n_y),y(t+k-1),\cdots,v(t),u(t-1),\cdots,u(t+k-n_u)),(k=0,1,\cdots,N_p) \quad (2)$$

在上述公式当中,$e(t)=y(t)-\hat{y}(t)=y(t)-f(y(t-1),\cdots,y(t-n_y),u(t-1),\cdots,u(t-n_u))$为模型误差修正项,$u(t+k-n_u),\cdots,u(t-1)$主要是表示对已知过去时刻的控制向量。除此之外,$v(t),\cdots,v(t+k-1)$主要表示为待定量,对现在以及未来时刻的控制向量进行表示,在这种情况下,一旦当$k\geq N_U$的时候,$v(t+k)=v(t+k-1)=\cdots=v(t+N_U-1)$。

3 基于免疫算法的滚动优化措施

在针对电厂过热气温进行智能预测控制的时候,要根据实际情况采取有针对性措施对其进行滚动优化。通过实践可以看出,滚动优化的根本目的是为了能够针对每一采样时刻进行有效控制,从控制量的容许区对其进行操作,只有保证满足③和④的前提条件下,才能够从中选择出最优控制量序列,促使控制性能指标能够达到最优化标准和要求[4]。

$$u_{min}\leq u(t+k)\leq u_{max},0\leq k\leq N_u-1 \quad (3)$$

$$-\Delta u_{max}\leq \Delta U(t+k)\leq \Delta U_{max},0\leq k\leq N_u-1 \quad (4)$$

4 结束语

在当前现代社会发展过程中,越来越多的科学技术被广泛应用到各个行业当中,特别是很多行业已经逐渐朝着智能化、技术化方向发展。电厂过热气温控制也可以利用智能预测控制方法对其进行控制,这样能够最大限度保证对电厂过热气温进行有效控制,将其本身的性能作用发挥到最大。

参考文献:

[1] 吕剑虹, 陈来九. 预测控制在热工控制中的应用前景[J]. 动力工程, 2016(2).
[2] 朱红霞, 沈炯, 王培红等. 基于免疫遗传算法的模糊优化控制及其仿真研究[J]. 东南大学学报:自然科学版, 2016(1).
[3] 王东风, 韩璞. 基于免疫遗传算法优化的气温系统变参数PID控制[J]. 中国电机工程学报, 2015(9).
[4] 陈来九. 热工过程自动调节原理和应用[M]. 北京: 水利电力出版社, 2016.