第17章

生物识别

基列人在以法莲人之前攻占了约但河。那些逃脱的以法莲人说，容我过去。基列人对他说，你是以法莲人吗？如果他说，不；他们对他说，现在说西伯列。他说西伯列，因为他想不出正确的发音。他们就拿住他，在约旦河边杀了他。那时，以法莲人四十两千人都被杀了。

– 士师记 12:5-6

17.1 简介

上面的引述可能是第一次记录在案的安全协议的军事用途，其中身份验证依赖于人的属性 在这种情况下是他的口音。 （在此之前没有那么正式的用途，例如以撒试图通过他的体毛来识别以扫但被雅各布欺骗了，或者实际上当人们通过他们的脸认出彼此时 - 我将在后面讨论。）

生物识别技术通过测量个体解剖学或生理学的某些方面（例如您的手部几何形状或指纹）、某些根深蒂固的技能或行为（例如您的手写签名）或两者的某种组合（例如您的声音）来识别人。

在 21 世纪，市场确实发生了翻天覆地的变化，自 2008 年本书第二版以来出现了三大变化。

1. 各州有很多大规模的生物识别公民身份项目，其中最大的一个项目可能是印度的Aadhaar项目，它已经记录了超过10亿人的虹膜密码和指纹。国际标准的生物识别旅行证件、为美国游客提供指纹的 US-VISIT 计划以及欧盟边境的人脸识别护照亭加快了国际旅行。

2. 自2012年以来,深度神经网络革命带来了人脸识别技术的巨大进步。这使得护照亭稳定地更快、更可靠,使大规模监控变得更容易,并引发了对隐私和人权的担忧– 特别是考虑到它在中国的部署。

3、自动指纹读取器不再是银行金库和福利院的小众产品,而是部署在数以亿计的手机上。现在人们将整个生命都保存在手机中,或者使用手机具有凭证的网络服务,因此人们需要依靠他们来阻止丢失或被盗的手机从烦恼变成灾难。

生物识别系统市场像火箭一样起飞,从 5000 万美元增长
1998 年增加到 2005 年的 15 亿美元 [997] 和 2019 年的 330 亿美元 [2038]。

我将首先描述计算机时代之前的生物识别技术 手写签名、面部特征和指纹 然后描述它们是如何实现自动化的,然后继续探索一些更现代的技术。

17.2 手写签名

古典中国使用手写签名,但雕刻个人印章被认为具有更高的地位;在中国、日本和韩国,它们仍然被用于严肃的交易活动。欧洲则相反:印章在中世纪时期就已经使用,但随着文艺复兴时期文字的传播,人们越来越多地只是写下自己的名字来表示对文件的认可。随着时间的推移,签名成为标准。每天,价值数十亿美元的合同仍然是通过手写签名签订的;这些将如何被电子机制取代仍然是一个现实的政策和技术问题。

手写签名是一种较弱的身份验证机制,因为它们很容易伪造,但由于它们的使用环境,它们几个世纪以来一直运行良好。一个重要因素是伪造责任。英国1882年汇票法规定,伪造的手写签名无效,这一规定在当时属于大英帝国的许多国家的法律中均有保留,例如加拿大和澳大利亚。在这些国家,手写签名对客户来说更好,因为银行承担了大部分风险,但 PIN 和电子令牌对银行来说可能更好 因此在很大程度上取代了它们。在法国和德国智能卡行业的游说下,欧洲也开始寻求电子签名。在美国,法律规定银行对其部署的电子系统负责,因此美国银行通常坚持使用芯片和签名卡,而不是使用芯片和 PIN。快递公司还收集手写签名作为收货证明,因为这是对所有收件人唯一有效的方式。因此,手写签名的验证仍然很重要。

现在,伪造签名被认为是真实签名的可能性主要取决于检查时的谨慎程度。许多商店的银行卡交易甚至不看样本就被接受

在卡上签名　如此之多以至于许多美国人甚至懒得在他们的信用卡上签名1。但即使勤奋的签名检查也不能将风险降低到零。一项实验表明,105 名专业文件检查员每人进行了 144 次成对比较,错误归因 6.5% 的文件。

同时,由 34 名未受过训练且教育水平相同的人组成的对照组在 38.3% 的时间内做错了 [1010],非专业人士的表现无法通过给予金钱奖励来提高 [1011]。专业人员犯的错误是业内持续讨论的主题,但被认为反映了审查员的先入之见 [198] 和背景 [587]。由于为这些测试的参与者提供了合理的笔迹样本而不仅仅是签名,因此可以公平地假设验证支票或送货收据上的签名性质的结果会更糟。

在大多数英语国家,大多数文件不需要通过特殊措施进行认证。签名的本质是签名者的意图,因此文盲在文件上的“X”是完全有效的。因此,电子邮件底部的明文名称具有完全的法律效力 [2042],除非有相反的具体规定。

例外情况来自各国不同的惯例和特殊规则。例如,用从非银行老客户借的钱在英国买房,手续是带护照等证件去律师事务所,在房产转让和贷款上签字合同,并让律师会签。

政府颁发的带照片身份证件的要求最初是由贷款人的保险公司提出的,并成为反洗钱法规的“了解你的客户”(KYC)条款;几个世纪以前,为了对财产交易征税,要求以书面形式购买房地产。

其他类型的文件(如专家证词)可能不必以特定方式计税。许多异常现象可以追溯到十九世纪,以及打字机的发明。一些国家要求机器书面合同在每一页上都有草签,而另一些国家则不需要;公约中的冲突仍然造成严重的问题。

在法庭案件中签名很少有争议,因为上下文大多清楚地表明谁做了什么。因此,这种薄弱的生物识别机制实际上在实践中运作良好　真正的问题来自于因国家和应用而异的大量程序规则。立法者做出了各种尝试来解决这个问题,并对电子文档施加统一的规则。

在第 26.5.2 节中,我讨论了 2000 年的全球和国家商业电子签名 (　ESIGN　) 法案,该法案使通过点击网页中的按钮签订的合同合法化,以及更重量级的欧洲 eIDAS 法规 (910/2014)要求所有成员国接受使用批准的产品制作的电子签名。这最初是为了帮助智能卡行业而设计的,但由于许多人和公司需要偶尔签署一些东西

1事实上,给小偷一个签名样本并不符合持卡人的利益　如果小偷在凭证上随机签名,真正的持卡人更容易否认它。
在卡上签名符合银行的利益,而不是客户的利益。

并且不想购买特殊硬件,最新法规现在允许在线签名服务公司在其云服务中生成被认为具有法律约束力的签名,即使客户手机或笔记本电脑的安全性可能还有很多不足之处.签名服务通常会生成带有机器签名的电子文档,我们应该假装是手写的;还有一个电子签名,由我们应该信任的服务提供商进行验证。

一个单独的主题是手写签名的自动识别,例如支票上的签名。这成为 1980 年代向银行出售支票处理设备的公司进行严肃生物识别研究的最早主题之一。在早期系统中,操作员会在屏幕上看到支票图像和客户的参考签名,然后做出决定。出于成本原因,这只针对几千美元以上的金额进行;较小的支票直接通过,由账户持有人提出异议。从 1990 年代初期开始,出现了标志性的平板电脑,不仅记录了曲线的形状,还记录了它的动态（手的速度,笔从纸上抬起的位置,等等）。这些被送货司机用来收集货物收据,也用于信用卡交易。自 1990 年代初以来,更好的产品可以将捕获的签名与之前登记的样本进行比较。

与警报一样,大多数生物识别系统都在错误接受率和错误拒绝率之间进行权衡,这在银行业中通常称为欺诈和侮辱率,在生物识别文献中称为类型 1 和类型 2 错误。许多系统都可以进行调整,使一个系统优于另一个系统。权衡取舍被称为接收器操作特性,这是雷达操作员首先使用的术语;如果你把雷达的增益调得太高,你会因为杂波而看不到目标,而如果它太低,你就根本看不到它。由操作员在曲线上选择合适的点。等错误率是指当系统被调整时,错误接受和错误拒绝的概率是相等的。对于基于平板电脑的签名识别系统,等错误率最多为1%;对于纯粹的光学比较,它是百分之几。这在支票处理中心等操作中并不是致命的,因为自动比较被用作过滤器来选择支票以供人工审查。但是,它在面向客户的应用程序（例如零售店)中是个阻碍。如果百分之一的交易失败,对客户的恶化将是不可接受的。因此,早在 1990 年代,英国银行就为生物识别设定了 1% 的欺诈率和 0.01% 的侮辱率目标,这超出了签名验证和指纹扫描的最先进水平　实际上仍然是 [719] .事实上,即使是平板电脑 1% 的相同错误率也是通过排除山羊而实现的　山羊是生物识别社区使用的一个术语,用于指代模板无法很好分类的人。

供应商通常将没有眼睛的人排除在虹膜扫描仪的统计数据之外,并将指尖磨损的体力劳动者排除在指纹统计数据之外。这可能导致欺骗性的性能声明并隐藏社会排斥问题。

一般来说,生物识别机制在有人值守的操作中往往更稳健,因为它们可以协助守卫而不是取代他们。

17.3 人脸识别

通过面部特征识别人是最古老的识别机制,至少可以追溯到我们早期的灵长类动物祖先。生物学家认为,我们认知功能的很大一部分已经进化为提供识别他人面部特征和表情的有效方法 [1604]。例如,我们非常擅长检测另一个人是否在看我们。

出于许多原因,人类识别面部的能力是一个重要的基准,其中之一就是对照片 ID 的依赖。驾照、护照和其他各种身份证件不仅直接用于控制进入机房,还用于引导大多数其他系统。用于访问系统的密码或智能卡的问题通常是一个过程的终点,该过程由该人在申请工作或开设银行账户时出示带照片的 ID 启动。

那么我们在通过照片 ID 识别陌生人方面有多好,而不是通过肉体识别朋友呢?

简单的答案是我们不是。威斯敏斯特大学的心理学家在连锁超市和银行的帮助下进行了一项有趣的实验 [1035]。他们招募了 44 名学生,并给他们每人发了四张信用卡,每张信用卡上都有不同的照片:

- 其中一张照片是“非常好”的照片。这是真实的,最近的;
- 第二个是“坏的,好的”。它是正品,但有点旧,学生现在有不同的衣服、发型或其他东西。换句话说,这是大多数人带照片的身份证件上的典型照片;
- 第三个是“好的,坏的”。从一堆大约一百张不同人的随机照片中,调查人员选择了一张最像主题的照片。换句话说,这就是犯罪分子用一叠偷来的牌可以得到的典型火柴;
- 第四个是“坏的,坏的”。它是随机选择的,只是它与受试者具有相同的性别和种族。换句话说,这是真正懒惰、粗心的罪犯会得到的典型匹配。

实验是在超市正常营业时间后进行的,但有经验丰富的收银员值班,并且了解实验的目的。每个学生使用不同的卡片多次经过结帐处。

结果发现,没有一个收银员能分辨出“好、坏”照片和“坏、好”照片之间的区别。事实上,他们中的一些人甚至分不清“好、好”和“坏、坏”之间的区别 。现在这个实验是在最佳条件下完成的,有经验丰富的员工 ,有充足的时间,而且如果卡被拒绝,不会有尴尬或暴力威胁。预计现实生活中的表现会更糟。事实上,许多商店不会将信用卡公司提供的捕获被盗卡的奖励传递给他们的收银员 。因此,即使是最基本的激励措施也不存在。然而,至少有两家尝试在信用卡上使用照片的银行经历了重大的

减少欺诈 [154]。结论是当时照片 ID 的好处基本上是它的威慑作用 [689]。

因此,也许人们不会在识别环境中有效地使用他们的面部识别技能,或者我们在社交环境中用来识别人的信息与我们通过查看单张照片获得的信息在大脑中的存储方式不同 .在任何情况下,认出路过的陌生人都比认出你认识的人难得多。据估计,错误识别是非法监禁的主要原因,20% 的证人在身份游行中犯了错误 [2044] 虽然不及将人脸与照片进行比较时近乎随机的结果那么糟糕,但仍不理想。

由于照片 ID 不适用于人类警卫,因此许多人已尝试使该过程自动化。尝试可以追溯到 19 世纪,当时 Francis Galton 设计了一系列用于面部测量的弹簧式“机械选择器”[738]。但是自动人脸识别实际上包含了很多独立的问题,其中大部分我们都没有机会对对象进行仔细的 3D 测量。自动护照检查亭可能是最简单的:拍摄对象在受控照明条件下直视相机,并将他们的脸与档案中的人脸进行比较。

在取证中,我们可能会尝试确定嫌疑人的面部是否与安全视频中的低质量记录相符。最难的是监视,我们可能想在机场扫描移动的人群,并试图找出数千名已知嫌疑人名单上的任何人。

人脸识别的早期应用通常只是安全剧院。 1998 年,伦敦纽汉姆区在大街显眼处放置了摄像机,并开展了一场公关活动,宣传他们的新计算机系统如何不断扫描人群中的面部,寻找数百名当地知名罪犯。他们报告的入室盗窃、入店行窃和街头犯罪显着减少,但后来承认他们在系统上只有 20 或 25 个恶棍的面孔,而且它从未认出他们中的任何一个 [1282]。 9/11 之后,许多地方都尝试过这样做。在佛罗里达州的坦帕,一个类似的系统在 2003 年被放弃,因为 ACLU 的信息自由请求发现它没有识别出任何恶棍 [1597]。波士顿洛根机场也尝试了人脸识别;对通过安检的乘客进行观察和匹配。该系统被发现是不切实际的,在错误匹配和错误警报之间没有有用的平衡 [316]。伊利诺伊州机动车管理局于 2003 年采用人脸识别技术来检测以假名申请额外驾驶执照的人 [663]。在这样的应用程序中,尝试检测不法行为可能是值得的,即使您只捕获了其中的四分之一。

作为基准,英国国家物理实验室 (NPL) 在 2001 年对多项生物识别技术进行的测试发现,人脸识别几乎是最差的;它的单次尝试等错误率几乎是 10% [1217]。

2005 年英国 Passport Oce 试验更接近现场条件,发现它只能识别 69% 的用户(并且只有 48% 的残疾参与者)[1920]。国际民航组织仍采用人脸识别作为护照和带有嵌入式芯片的身份证的标准;虹膜代码和指纹是可选的附加功能。典型的安装有一排展位,将实时照片和文件照片转发给人工操作员,人工操作员会收到疑似不匹配的警报。

然而,自从 2012 年神经网络革命开始以来,面部识别的性能有了显着提高,错误率下降了一个数量级。现在通过护照亭通常比 2010 年快得多,而且您不必总是摘下您的眼镜。但是数据呢?最好的可能来自 NIST 的面部识别供应商测试 (FRVT),该测试针对数以百万计的执法面部照片、监狱网络摄像头图像和野外照片测试产品,以进行 1:1 验证、一对多识别、面部变形检测和面部图像质量评估。根据 2018 年的报告,2013 年至 2018 年在准确性方面取得了巨大进步,这在很大程度上要归功于卷积神经网络 (CNN) 的采用。最准确的算法会在包含 1200 万个人的画廊中找到匹配的条目,错失率接近 0.1%;但在大约 5% 的图像中,识别成功的置信度较低,因此需要人工判断。一些算法正确地将侧视图照片与正面照片库相匹配;这种姿势不变性一直是人脸识别研究中长期寻求的里程碑。

存在可测量的种族偏见。美国开发的算法在亚裔、非裔美国人和美洲印第安人的一对一匹配中误报率明显更高,而在一对多匹配中,非裔美国女性的误报率最高。亚洲开发的算法对亚洲人和白人同样有效。剩余的错误在很大程度上是由于长期老化、面部受伤、图像质量差或拍摄中的第二张脸,例如印在 T 恤上的脸 [828]。

2018 年的一项研究将人脸识别算法与专业的法医人脸检查员、未经训练的超级识别者（非常有才华的人)以及随机的对照组进行了对比。它发现,两种类型的人类专家都明显优于对照组,并且 2015 年至 2017 年间开发的四个深度 CNN 识别出人类专家范围内的面孔,最近的得分高于法医专家的中位数。

然而,如果算法和人类专家一起工作,可以获得最好的结果 [1522]。

至于背后是什么,郭东和张娜在 2019 年发表的一篇调查论文探讨了深度学习在人脸图像分析和识别中的应用,并讨论了系统如何处理姿势、年龄、光照和表情的变化 [834]。大多数系统都是 CNN,但具有一系列适应性,例如,多个 CNN 在两个候选面孔的不同区域同时寻找不同类型的特征,自动编码器寻找共同的潜在特征以提供姿势鲁棒性;然后有各种融合、聚合和过滤。也可能有纠正化妆和面部表情的机制。在算法选择中存在复杂的权衡取舍,ROC 术语中的最佳算法花费的时间与图库大小成线性关系,这意味着半秒可以匹配 10m 个其他人脸;如果有三张或更多面部照片可用,则准确度可以翻倍,因为这使 CNN 能够考虑老化。但是视频图像的模糊仍然是一个严重的问题,将静止图像与视频匹配以及将可见光图像与近红外图像匹配也是如此。

人脸识别革命仍在继续,NIST 报告称,仅在 2018 年,一些算法的准确率就翻了一番。它也变得有争议。我们是否面临一个反乌托邦的未来,每个灯柱都有

一个带有嵌入式闭路电视的 5g 基站可以识别所有路人?突然之间,CCTV 从犯罪现场取证工具变成了实时人员识别和跟踪工具。这似乎是中国人的愿景;公司有训练相机,不仅可以识别个人,还可以识别群体,如果对象看起来是维吾尔族或藏族,分类器就会发出警报。在冠状病毒大流行期间,这种情况被强制戴口罩打断了,但之后无疑会恢复。俄罗斯一直在使用其摄像头发现违反冠状病毒检疫令的人,并声称已部署了 178,000 个摄像头 [1907]。即使在西方,我们是否会面临这样一个未来:警察不仅可以从已经跟踪道路车辆的自动车牌识别系统获得信息,还可以从跟踪行人的系统中获取信息?愤世嫉俗者会说,即使您戴着墨镜或口罩,手机位置历史记录也能正常工作,那有什么大惊小怪的?

但现在有些公司收集的人脸比执法部门多得多,因为他们不受法律限制,而且他们的服务帮助执法部门破获没有面部照片的人犯下的罪行。这些公司似乎准备提供更广泛的服务;它们有可能使增强现实眼镜的用户能够识别他们看到的大多数人 无论是地铁上迷人的陌生人,还是示威中的抗议者。你可以找到他们的名字、他们住在哪里以及他们在网上做什么。该公司的支持者评论说:“法律必须确定什么是合法的,但你可以禁止技术。当然,这可能会导致反乌托邦式的未来或其他什么,但你不能禁止它。” [897]。

政治和法律上的阻力已经开始。伊利诺斯州埃文斯顿的一个家庭发现,他们在 2005 年上传到 Flickr 的孩子的照片最终出现在一个名为 MegaFace 的数据库中,该数据库用于训练许多新的识别系统。这是违反伊利诺伊州法律的,现在有几起集体诉讼正在进行中。因此,社交媒体上的一些面部标记功能在伊利诺伊州(或德克萨斯州)不起作用 [898]。 2018 年,谷歌决定在其使用受到监管之前,不在其云平台中提供人脸识别 API。如果你用犯罪面部照片训练一个系统,它可以看着任何路人并说“这个强盗是最接近的匹配”。在警察喜欢触发的地方,可以杀人。 2019 年 5 月,旧金山禁止交通部门和执法部门等机构使用人脸识别。 2020 年 6 月,在全球范围内针对种族主义和有偏见的警察的抗议活动之后,亚马逊宣布暂停一年向执法部门提供其 Rekognition 人脸识别软件;他们的技术因错误识别有色人种而受到批评。美国公民自由联盟 (ACLU) 表明,亚马逊的系统将 28 名国会议员与被捕人员的面部照片进行了虚假匹配。 IBM 和微软也宣布他们将停止销售人脸识别产品 [2004]。由于技术现在是一种商品,四大的自我约束并没有阻止二线公司销售它。因此,四大巨头现在都在推动对人脸识别产品进行监管。法院已经介入:2020 年 8 月,伦敦上诉法院裁定,南威尔士警方使用面部识别违反了隐私权、数据保护法和平等法 [1592]。

最后,可以通过特殊硬件增强面部识别。 2017 年,Apple 在 iPhone X 上推出了它,其中一个点投影仪用数万个点在你的脸上绘制,然后一个摄像头读取它们。这涉及

化妆、一些太阳镜和面部毛发,据称错误接受率为百万分之一 而之前 iPhone 使用的指纹识别器的错误接受率为五万分之一。然而,我大孙女的 iPhone 可以被她的两个弟弟妹妹解锁,这是家庭的普遍问题 [526]。

17.4 指纹

自动指纹识别系统 (AFIS) 已经存在多年。
1998 年,它们占生物识别技术 5000 万美元销售额的 78%;到 20052 年,这一比例已降至 15.39 亿美元的 43.5%。AFIS产品会查看覆盖指尖的摩擦脊,并对脊的分支和端点等细节模式进行分类。有些人还观察脊部皮肤的毛孔[1213]。

多次独立发现使用指纹来识别人。马克吐温在 1883 年的密西西比河上的生活中提到了指纹,他声称是从一位当过监狱看守的法国老人那里了解到指纹的;他 1894 年的小说 Pudd nhead Wilson 使这个想法在美国流行起来。很久以前,在七世纪的中国法典中,指纹被接受为印章或签名的替代品,在八世纪的日本法典中,当一个不识字的男人想和他的妻子离婚时,指纹也被接受。几个世纪前,它们也在印度使用。随着显微镜的发明,1684 年英国植物学家 Nathaniel Grew 和 1686 年意大利的 Marcello Malpighi 提到了它们; 1691 年,爱尔兰伦敦德里的 225 名市民用他们的指纹签署了一份请愿书,要求威廉国王在城市被围困后给予赔偿。

1858 年,天文学家和殖民地地方官的孙子 William Her schel 在印度进行了第一次现代系统使用。他引入了手印和指纹来签署合同,停止冒充已故的养老金领取者,并防止有钱的罪犯付钱给穷人代为服刑。
1870 年代,日本的医疗传教士 Henry Faulds 独立发现了它们,并提出了利用犯罪现场的潜指纹来识别罪犯的想法。 Faulds 使指纹引起了查尔斯·达尔文的注意,达尔文反过来又促使弗朗西斯·高尔顿研究指纹。高尔顿在《自然》[738] 上写了一篇文章;这让他与退休的赫歇尔取得了联系,赫歇尔的数据使高尔顿相信指纹会贯穿人的一生。高尔顿继续收集更多的印刷品,并设计了一个方案来对它们的图案进行分类 [739]。 Chandak Sengoopta 讲述了印度的历史,他的书还指出指纹识别拯救了两个有点可疑的帝国制度,即契约劳工制度和鸦片贸易 [1701]。

这项技术的实际应用在很大程度上要归功于曾在孟加拉当过警察的爱德华·亨利爵士。他在 1900 年写了一本书,描述了他与助手 Azizul Haque 和 Hem Chandra Bose 开发的一种更简单、更可靠的分类,包括环、螺纹、拱形和帐篷,

2我没有 2019 年的可比数据,因为指纹技术现在与手机或 Aadhaar 等系统中的其他生物识别技术捆绑在一起。

这至今仍在使用。同年,他成为伦敦大都会警察局局长,这项技术由此传遍了世界 3。亨利真正的科学贡献是将高尔顿分类法发展成为一个索引系统。通过为嫌疑人的十个手指中的每一个手指是否都有螺纹（一种圆形图案)分配一位,他将指纹文件分成 1024 个箱子。通过这种方式,可以将必须搜索的记录数量减少几个数量级。与此同时,由于英国已停止将已定罪的重罪犯送往澳大利亚,人们认为有必要查明以前的罪犯,以便对他们判处更长时间的徒刑。

指纹基本上被世界警察用于两个不同的目的:识别人员身份（在美国主要用途)和犯罪现场取证（在欧洲主要用途）。

17.4.1 验证正面或负面的身份声明

在当今的美国 就像在 19 世纪的英国一样 不少罪犯在出狱后改名并搬到新的地方。犯者直来直去还好,逃犯累犯怎么办?美国警察历来使用指纹来识别被捕嫌疑人,以确定他们目前是否被其他机构通缉,他们是否有犯罪记录,以及他们之前是否以其他名字受到关注。 FBI 为此维护了下一代身份识别 (NGI) 服务系统;它每月查明大约八千名逃犯 [1809]。任何想要获得美国政府秘密或更高级别许可的人都必须接受 FBI 指纹检查,而且一些申请与儿童或老人一起工作的人也会接受检查。每天进行多达 100,000 张支票,大约有 100 万联邦、地方和州官员可以访问。有一种“回话”服务可以提醒雇主任何有许可的人触犯法律[1378];它还用于跟踪缓刑犯、假释犯和性犯罪者的再服刑。国土安全部的 IDENT 系统保存着 2 亿抵达美国港口的外国人的指纹;它将他们与在全球警察部队和情报部门的帮助下编制的坏人观察名单进行匹配。

这些是一种身份验证的示例 检查黑名单。另一种类型是系统检查身份声明,美国的主要应用是建筑入口控制和福利支付 [588]。

多年来,银行一直使用它们来识别印度和沙特阿拉伯等国家/地区的客户,由于文盲率高,墨水指纹的使用已经很普遍。印度现在有一个名为 Aadhaar 的国家系统,其中包含大多数居民的指纹和虹膜代码,最初旨在支持福利支付并确保没有人可以申请两次。它的使用也已成为许多其他交易的强制性要求。

3 在西班牙语版本的历史中,它们首先在阿根廷使用,并于 1892 年在阿根廷被判谋杀罪;而古巴于 1907 年成立了指纹局,击败了美国,美国于 1911 年在伊利诺伊州首次定罪。克罗地亚版本指出,阿根廷系统是由从达尔马提亚移民的胡安·武切蒂奇 (Juan Vucetich) 开发的。

德语版指的是布雷斯劳的浦肯野教授,他在 1828 年写了关于指纹的文章。成功真的有很多父亲!

在北美或欧洲,指纹从未用于验证银行客户的身份,但如果您在那里兑现支票但不是客户,一些美国银行确实会要求提供指纹。他们发现这可以减少大约一半的支票欺诈。有些人甚至对新客户进行了指纹识别,发现客户的抵触情绪低于预期,尤其是当他们使用扫描仪而不是墨水和纸张时 [716]。这些应用程序不是身份验证,而是试图识别甚至阻止后来证明是坏客户的客户 另一个例子是英国大型面包车租赁公司在您租用面包车时要求提供指纹。如果车辆没有归还,或者如果它被用于犯罪,指纹就会交给警察。因此,它们实际上是一个犯罪现场取证应用程序,我将在下一节中对此进行讨论。

那么自动指纹识别系统有多好呢?一个好的经验法则(如果有人可以这么说的话)是要验证身份声明,扫描一根手指可能就足够了,而要检查某人是否符合数百万重罪犯的黑名单,你最好扫描所有十个.美国国土安全部计划开始扫描每位到访访客的两个食指后,却被错误的匹配结果淹没了。数据库中有 6,000,000 个坏人,2004 年的误匹配率为 0.31%,漏匹配率为 4% [2027]。该程序改为“10 次打印”,每位参观者必须在三个连续扫描中出示每只手的四个手指,然后是两个拇指。欧盟将从 2020 年开始采用 4 指纹和面部识别相结合的方式;非居民既需要进入,也需要退出。

这都是关于假阴性和假阳性之间的权衡 接收器操作特性,如上一节所述。更好的系统每根手指的错误率略低于 1%。错误接受的发生是因为包含了降低错误拒绝率的特征 例如允许失真和特征选择的灵活性 [1610]。以足够高的概率发现返回的逃犯以阻止他们并以足够高的确定性来拘留他们(这意味着将错误警报保持在可管理的水平)需要匹配几根手指 也许十分之八。这确实会造成延误; UK Passport Oce 的一项研究发现,大约 20% 的参与者在进行 10 次打印时未能正确注册,并且 10 次打印验证花费了超过一分钟的时间 [1920]。这大概是我在 2010 年代飞进飞出美国时的经历。为每个人采集指纹的代价是,美国机场每 15 分钟要接待 300 名国际旅客,需要额外的 10 条工作移民通道。额外的建筑和设施成本淹没了硬件和软件上的任何花费。 (有关算法和系统的更多信息,请参阅 [973、1211、1213]。)

错误不是均匀分布的。许多人,如体力劳动者和抽烟斗的人经常损坏他们的指纹,年轻人和老年人都有模糊的指纹 [392]。自动化系统对于截肢者、有先天缺陷(例如多余手指)的人以及(罕见的)出生时根本没有传统指纹模式的人也有问题 [1120]。

小时候,我在切苹果的时候割破了左手的中指,留下了大约半英寸长的疤痕。当我将这根手指伸向联邦调查局 1989 年用于建筑物入口控制的系统时,我的伤疤使扫描仪崩溃了。 (十年后我再次尝试时,它工作正常。)

指纹识别系统可以通过多种方式受到攻击。一个老

骗子的伎俩是分散（或贿赂)为他指纹的警察,这样警察就会以错误的顺序拿手指,而不是在亨利系统下将手编入索引为“01101”,它可能变成“01011”,所以没有找到他的记录,他因初犯而得到较轻的判决 [1120]。

第一次引人注目的技术攻击发生在 2002 年,当时 Tsutomu Mat sumoto 及其同事表明可以使用烹饪明胶快速廉价地塑造和克隆指纹 [1246]。他测试了 11 种市售的指纹识别器,并轻松地骗过了所有的指纹识别器。这促使德国计算机杂志 C T 测试了在汉诺威 CeBIT 电子展上出售的许多生物识别设备 九个指纹识别器、一个面部识别系统和一个虹膜扫描仪。它们都很容易被愚弄 低成本的电容式传感器采用了一些简单的技巧,例如在手指扫描仪上呼吸以重新激活先前用户留下的潜在指纹 [1877]。隐藏的指纹也可以使用胶带重新激活或转移。

更昂贵的热扫描仪仍然可以被橡胶模压手指击败。

2013 年,Apple 在 iPhone 5S 上引入了指纹扫描仪,其他手机制造商竞相效仿。黑客适当地展示了攻击,2014 年 CCC 演示了德国国防部长的手指模型,该模型是根据照片创建的 [313]。手机上的扫描仪通常会在注册时存储 8-12 个部分打印件,并且会针对其中任何一个进行解锁,这使得扫描仪更有用,但也更容易受到攻击。 2016 年,Aditi Roy 及其同事发明了“masterprint”:一种可以戴在指尖上的假指纹,旨在匹配至少一个来自典型手指的部分指纹;它适用于 6% 的用户打印 [1625]。 2017 年,Apple 从指纹识别转向人脸识别,正如我上面所讨论的,但大多数 Android OEM 仍在使用指纹识别。 2019 年,事实证明,三星 S10 上的新型超声波扫描仪登记了屏幕保护膜而不是客户的手指,导致手机无法运行许多银行的应用程序 [466]。

还有其他角度。例如,圣贝纳迪诺枪手使用的是 iPhone 5C,这是最后一款没有扫描仪的手机;如果他使用的是更高版本,FBI 可以通过将其带到太平间并将其按在他的手指上,或者根据他的文件打印制作指尖模具来解锁它。随着政府机构收集越来越多的印刷品,它们的私密性将越来越低。

（中国人已经通过我在 2.2.2 节中讨论的 OPM 黑客获得了所有美国联邦雇员的指纹。)指纹系统也迅速扩展到低保证应用,从进入高尔夫俱乐部停车场到在学校自动借书图书馆。 （大多数欧洲国家/地区的隐私机构已禁止在学校使用指纹扫描仪;英国允许使用指纹扫描仪,这引起了注重隐私的父母的反对 [190]。)最新的转折来自 Mitre 项目,该项目开发了一种软件,可以从他们拍摄的照片中收集人们的指纹。在社交媒体上发帖;这些通常会显示足够详细的手指,以便与 FBI 数据库进行匹配 [321]。

指纹识别系统成功的最后一个原因是它们的威慑作用,这在福利支付中尤为明显。尽管用于验证福利申请者身份的廉价指纹读取器的错误率高达 5% [383],但事实证明它们是一种如此有效的方法

减少他们在九十年代在一个又一个地方被采用的福利名册 [1315]。

17.4.2 犯罪现场取证

指纹识别的第二个用途是犯罪现场取证 欧洲的主要应用。在犯罪现场发现的指纹与数据库记录进行匹配，任何匹配超过一定水平的指纹都被视为嫌疑人访问过犯罪现场的证据。他们往往足以靠自己定罪。在许多国家/地区，所有公民和所有外国居民都需要指纹。

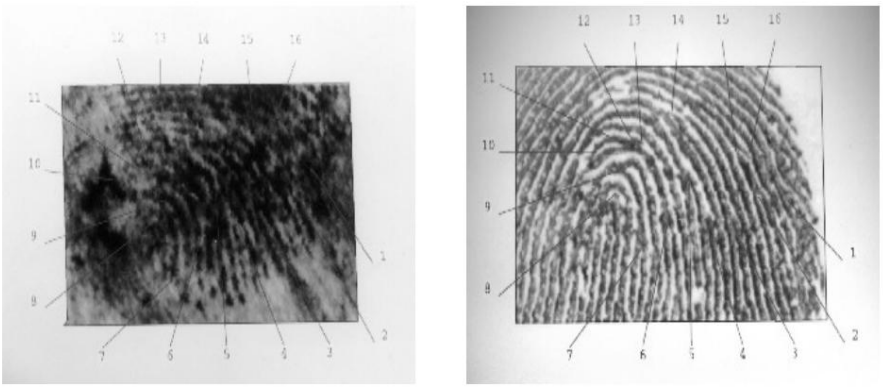
近年来，法医错误率变得极具争议，关键的限制是从犯罪现场拍摄的图像的大小和质量。质量和程序规则因国家/地区而异。

英国曾经要求指纹在 16 个点（相应的细节）上匹配，一位英国警察专家声称这只会偶然发生在 40 亿分之一到 100 亿分之一之间[1120]。

希腊接受 10 人，土耳其接受 8 人，而美国没有设定限制（而是对考试人员进行认证）。这意味着在美国，可以找到打印质量较差的火柴，但可以在法庭上公开挑战。

在英国，指纹证据几乎用了一个世纪都没有成功挑战； 16点指纹匹配被认为是悬而未决的证据。

McKie 案 [1273] 打破了法院的信心。苏格兰女警雪莉·麦基 (Shirley McKie) 因指纹匹配所需的 16 点而被起诉，并由苏格兰犯罪记录办公室的四名审查员核实。她否认那是她的指纹，并发现她在英国找不到独立的专家来支持她；该行业封闭的行列。她打电话给两位美国考官，他们出示了证明这不是身份证明的证词。犯罪现场和文件打印件并排显示在图 17.1 中。



(a) 犯罪现场打印 (b) 油墨印刷

图 17.1：McKie 案例中的脚印

她被无罪释放,这导致了一场持续多年的政治闹剧 [1272]。
第一个问题是针对她的案件的性质 [1273]。一些高级警官曾试图说服她做出虚假陈述,以解释在一起可怕的谋杀案现场出现被误认的印刷品的原因。她拒绝这样做导致她因伪证而被起诉,以此来诋毁她。她的无罪释放让人怀疑警方证词的可靠性,不仅针对她的具体案件,而且更普遍。被判犯有谋杀罪的男子在上诉后被宣告无罪,并起诉警方要求赔偿。政府对其他案件中可能还会有数十次上诉的前景感到恐慌,并以伪证罪起诉了四名指纹专家。那也没有任何进展。这个问题一次又一次地回到苏格兰议会。警察拒绝恢复雪莉·麦基的职务,涉事警察获得晋升,争吵变得越来越激烈。最终她从政府那里获得了 750,000 英镑的赔偿[189]。

该案例引发了专家对指纹识别价值的广泛讨论,并导致指纹证据在其他一些国家受到成功挑战 [760]。美国有两个引人注目的案例是 Stephan Cow ans 和 Brandon Mayfield。斯蒂芬·考恩斯 (Stephen Cowans) 于 1997 年因抢劫后枪杀一名警察而被定罪,但六年后,他辩称自己的指纹是误认,并存了足够的钱来对证据进行 DNA 检测,因此在上诉中被判无罪。 DNA 不匹配,这让波士顿和州警察重新分析了指纹,随后他们意识到这毕竟不是匹配的。布兰登梅菲尔德是俄勒冈州的一名律师,他被联邦调查局误认为是马德里爆炸案的肇事者之一,并被关押了两周,直到马德里警方逮捕了另一名指纹更匹配的男子。称他们的比赛“绝对无可争议”的联邦调查局同意在 2006 年向梅菲尔德支付 200 万美元。

在随后的一项研究中,心理学家伊蒂尔·德罗 (Itiel Dror) 向五名指纹检查员展示了一对指纹,告诉他们这些指纹来自梅菲尔德案,并询问他们 FBI 哪里出了问题。三位考官认为指纹不匹配并指出原因;一个不确定;并且有人坚持认为他们确实匹配。只有他是对的。这些指纹不是 Mayfield 套装,但在每一个案例中都是检验员本人在最近的一起刑事案件中匹配的一对 [586]。 Dror 与六位专家重复了这一过程,每人查看了八幅印刷品,他们在过去几年中对所有印刷品进行了真实检验。只有两位专家保持一致;其他四人在他们之间做出了六个不一致的决定。这些印刷品有一定的难度,只有一半的案例提供了误导性的上下文信息 [587]。

检察官和警察仍然向陪审团坚持法医结果没有错误,而 FBI 能力考试长期以来的错误率约为 1% [205],而误导性的上下文信息可将错误率推高至 10%,在某些情况下超过 50% .

四个评论是有序的。

· 如图 17.1 所示,指纹印记通常非常嘈杂,被污垢遮盖了。所以错误是很有可能发生的,而且在 McKie 案、Mayfield 案和

他们引起的普遍骚动。 Dror 的工作证实,发生错误识别的案例往往是困难的 [587]。

然而,法医文化只接受确定性。最大的法医组织国际鉴定协会认为,就“可能的、可能的或可能的鉴定应被视为……行为不当”作证。 [205]

- 即使如警方乐观主义者所声称的那样,16 个点出现错误匹配的概率为百亿分之一(1010) ,一旦将许多指纹相互比较,概率论就会开始发挥作用。一个在过去运行良好的系统,作为一个犯罪现场印刷品,可以手动将其与 157 名已知的当地窃贼的记录进行比较,一旦每年将数千份印刷品与数百万的在线数据库进行比较,该系统就会崩溃。不可避免的是,迟早会进行足够多的比赛以找到 16 分的不匹配。事实上,由于指纹数据库中的大多数人都是小罪犯,他们无法像雪莉·麦基那样进行坚决的辩护,如果没有其他冤案,我会感到惊讶。事情可能会变得更糟,因为欧洲警察部队现在将他们的生物识别数据库（包括指纹和 DNA)连接起来,以便警察部队可以搜索所有欧盟成员国的匹配项 [1905]。他们最终可能需要更强大的方法来处理误报。

- 认为任何安全机制都绝对可靠的信念会导致破坏其正确使用所需的自满和粗心大意。似乎没有考虑通过引入计算机匹配将所需的点数从 16 个增加到（比如说)20 个。十六岁是传统,没有人想挑战该系统或为被告专家提供公共资金。在英国,所有的专家都是警察或前警察,所以无论如何都没有独立的人可以雇用。即便如此,也可以使用多位专家的随机匹配;但是,如果指纹局不得不在大约 5-10% 的案件中告知辩方（例如)四位专家中的一位不同意,那么更多的被告将被宣告无罪。

- 绝对可靠的信念确保最终失败的后果将是严重的。与第 12.4.3 节中描述的 Munden 案例一样,它帮助破坏了关于自动取款机安全性的说法,安全机制是绝对可靠的假设导致程序、文化假设甚至法律涌现,以确保其最终失败将被拒绝尽可能长的时间,因此当它不能再被推迟时将产生真正的影响。在苏格兰的案例中,似乎出现了一种等级制度规避风险的文化,在这种文化中,审查员倾向于确认同事（尤其是资深同事)所做的鉴定。

当其中四人因伪证罪受审时,这种风险规避适得其反。

然而,即使我们确实有一个正确的匹配,它的含义并不总是很明显。可以使用胶带转移指纹,也可以使用最初为警察设计的技术制作模具。

所以有可能在犯罪现场发现指纹的嫌疑人是

被另一名罪犯陷害（或被警察陷害 大多数捏造案件涉及执法人员而不是其他嫌疑人 [254]）。即使恶棍没有被陷害，他也总是可以声称他是（陪审团可能会相信他）。

在美国，最高法院在其 Daubert 判决中认为，初审法官应筛选法医证据背后的原则和方法，以确保其相关性和可靠性 [516]。法官应该考虑参考的科学文献 在指纹的情况下，这是缺乏的，因为执法机构通常不愿意将他们的检查程序提交给严格的双盲测试。美国已经举行了多次涉及法医指纹证据的多伯特听证会，FBI 普遍占了上风[761]。然而，该局关于指纹检查零错误率的传统路线现在受到广泛嘲笑[1809]。

17.5 虹膜代码

我们现在从传统的识别人的方式转向现代和创新的方式。在实验室条件下测量时，通过眼睛虹膜中的图案识别人的错误率远远超过任何自动生物识别系统。最初的研究由能源部资助，该部门希望以最佳方式确保进入钚商店等场所，该技术现在用于从移民到福利的各种应用。机器可读旅行证件的国际标准要求使用照片，并允许使用指纹和虹膜。

就目前所知，每个人的虹膜都是独一无二的。它在视频画面中相当容易检测，不会磨损，并且通过角膜（角膜有自己的清洁机制）与外部环境隔离。虹膜图案包含大量的随机性，并且似乎具有指纹自由度数的许多倍。它是在怀孕的第三个月和第八个月之间形成的，并且（像指纹图案一样）似乎受到有限的遗传影响；形成它的机制似乎是混乱的。即使是同卵双胞胎（以及一个人的两只眼睛）的模式也是不同的，而且它们似乎在整个生命过程中都是稳定的。

Leonard Flom 和 Aran Safir 于 1987 年为虹膜识别系统的想法申请了专利，他们观察到每个虹膜都是不同的。 1993 年，约翰·道格曼 (John Daugman) 想出了如何让这个想法发挥作用，开发了信号处理技术，将虹膜图像中的信息提取到 256 字节的虹膜代码中。这涉及在瞳孔和虹膜外侧之间的多个同心环处进行的圆形小波变换（图 17.2）。生成的虹膜代码具有整洁的属性，即从同一虹膜计算的两个代码通常会在其 90% 的位中匹配 [517]。这比指纹扫描仪要简单得多，在指纹扫描仪中，对细节进行定位和分类是一项繁琐的计算任务。虹膜编码的速度和准确性，以及 Daugman 专利的到期，导致了许多商业虹膜识别产品 [1996]。虹膜代码提供任何已知验证系统中最低的错误接受率 在美国能源部和美国能源部进行的测试中为零

能源和不良贷款[1217]。等错误率已被证明优于百万分之一,如果准备容忍万分之一的错误拒绝率,那么理论上的错误接受率将低于万亿分之一。实际上,错误拒绝率明显高于此;很多事情,从睫毛到宿醉,都会导致相机看不到足够的虹膜。美国国防部在其 2002 年的现场试验中发现错误拒绝率为 6% [1258]； UK Passport Oce 试验发现正常用户为 4%,残疾用户为 9% [1920]。另一个问题是无法注册； Passport Oce 试验未能招募到 10% 的参与者,黑人用户、60 岁以上和残疾人的参与率更高。

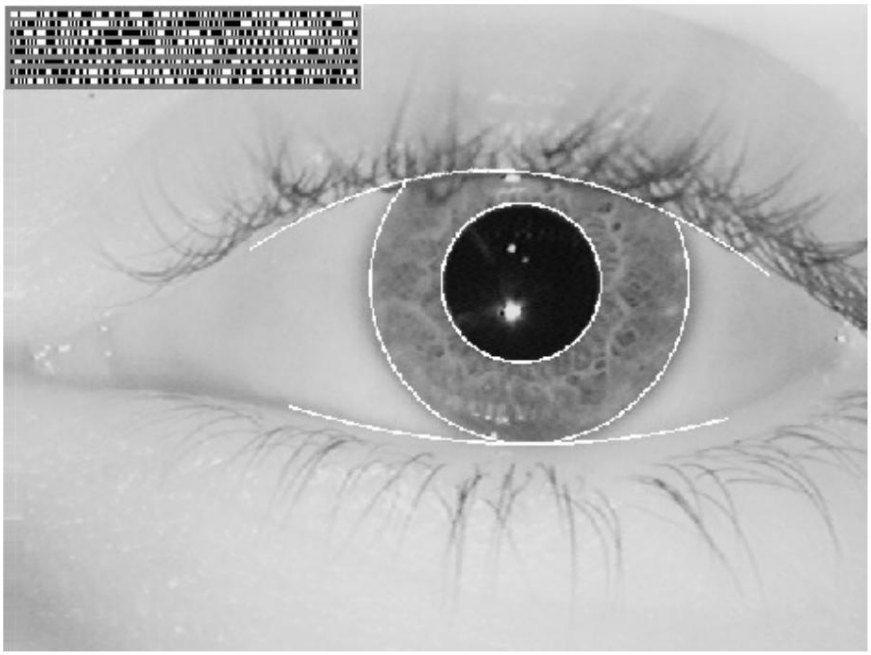


图 17.2：– 带有虹膜代码的虹膜（由 John Daugman 提供）

虹膜扫描的一个实际问题过去是在不太干扰的情况下廉价地获取图片。虹膜很小（不到半英寸）,需要具有数百个虹膜像素的图像。一个合作的对象可以把他的眼睛放在摄像机几英寸的范围内,最好的标准设备可以在两到三英尺的距离内工作。目前所有的虹膜扫描系统都使用红外线,当红外线照射到眼睛时,有些人会感到不舒服。鉴于更先进的相机,具有自动面部特征识别、平移和缩放功能,现在可以在航空公司乘客沿着走廊行走时偷偷捕捉他们的虹膜代码 [1240],并且在 2011 年关键专利到期后成本下降.

第一次大规模部署是在阿拉伯联合酋长国,它想追踪被驱逐出境的人,尤其是卖淫罪。几周后,被驱逐者会再次出现,他们会带着通过腐败获得的来自某些亚洲国家的新的、完全有效的护照。

自 2003 年部署以来,已导致超过 330,000 名人员被拘留

尽管有禁令或使用虚假文件试图进入该国。

最大的部署是印度的 Aadhaar 系统,所有居民都在该系统下进行了指纹和虹膜扫描。他们会得到一张带有 10 位数字的 Aadhaar 卡,验证者可以通过该卡在数据库中查找他们的个人资料。该项目的最初动机是让生活在贫困线以下并获得福利的 3 亿印度人能够进入城市寻找工作。以前福利只能在他们的城镇或村庄获得。

该系统在 2011 年至 2016 年期间招募了 10 亿人,并且所有虹膜代码都经过相互检查以确保唯一性。Aadhaar 现在在许多方面都是强制性的,收集到的指纹也可供警方用于犯罪现场取证。

对虹膜识别系统的可能攻击包括 至少在无人值守的操作中 一张目标虹膜的简单照片。有一些终端可以检测这种简单的假货,例如通过测量 hippus 瞳孔直径的自然波动发生在大约 0.5 Hz。但广泛销售的廉价终端不会这样做,如果活体检测变得普遍,那么攻击者无疑会尝试更复杂的技巧,例如在隐形眼镜上打印目标的虹膜图案。

使用时间最长的系统是阿联酋的系统,用于检测携带假证件返回的被驱逐者。典型的攻击是返回的被驱逐者在飞机上服用阿托品眼药水,放大她的瞳孔;如今,此类旅行者会被拘留,直到他们的眼睛恢复正常。至于 Aadhaar,主要的滥用和纠纷发生在系统周围,而不是通过它。 2019 年,一个热点问题是当局不愿在阿萨姆邦和其他边境地区登记穆斯林,这是试图将他们描绘成非法移民的更大政策的一部分。印度最高法院裁定,不得拒绝向未注册的人提供服务,但这并没有阻止注册成为开设银行账户、购买电话或 SIM 卡以及入学的实践要求。

尽管困难重重,但虹膜代码在某种意义上是最强大的生物识别技术,因为它们可以在适当的情况下向您保证,您面前的人与最初注册虹膜的人是同一个人。只有它们才能实现零错误接受的自动识别目标。

17.6 语音识别和变形

语音识别 也称为说话人识别 是从简短的话语中识别说话人的问题。语音识别系统关注的是转录语音并需要忽略语音特质,而语音识别系统则需要对它们进行放大和分类。有很多子问题,例如识别是否依赖于文本,环境是否嘈杂,操作是否必须实时以及是否只需要验证说话人或从大集合中识别他们。

与指纹一样,该技术可用于身份识别和取证。在法医音韵学中,任务通常是匹配录音电话

一些嫌疑人的谈话样本,例如炸弹威胁。典型的技术包括从频谱中过滤和提取特征;有关更多详细信息,请参阅 [1058]。一个更直接的生物认证目标是验证某些电话系统中的身份声明。

这些范围从电话银行到军事人员的身份识别,美国国家安全局维护着一个标准的测试数据语料库,用于评估说话人识别系统。在英国,寻求庇护者每周必须多次打电话 [1902]。此类系统倾向于使用呼叫者 ID 来确定人们的位置,并且还用于足球流氓等根据法院命令不得在特定时间前往特定地点的人。我个人使用的唯一系统是由我使用的其中一家银行运行的,当你更换手机时,它会通过他们的手机应用程序验证你的身份。但 2016 年,英国一家主要银行在手机应用程序中部署语音生物识别系统时感到尴尬,但第二年 BBC 的一名记者让他的异卵双胞胎模仿他的声音 [1744] 就把它搞砸了。

除了亲戚或恶棍可能设法模仿您的可能性外,还有一些强大的攻击。在 [730] 中描述了 1990 年代部署在美国 EP-3 飞机上的系统,该系统将截获的来自敌机和地面控制器的信息分解为四分之一秒的片段,然后将这些片段剪切和粘贴以提供新的、具有欺骗性的信息。与二十年后现在可以做的相比,那是原始的。现在网上有很多公众人物的视频似乎在说一些合适的话,而“Deepfake”编辑软件现在可以近乎实时地完成这种声音和图像变形。最近,犯罪分子使用 AI 冒充首席执行官的声音并下令支付 220,000 欧元:这种欺骗的受害者甚至不是机器,而是另一位高管 [1841]。

这可能是语音变形软件被用于真正欺诈的第一例;我们可以肯定这不会是最后一次。

17.7 其他系统

已经提出了许多其他生物识别技术 [1315]。打字模式在 1980 年代曾用于产品中,但似乎并不成功(打字模式,也称为击键动力学,在战时技术中有一个著名的先驱,即用拳头识别无线电报操作员,他们使用莫尔斯键)。静脉图案已在一两个系统中使用,但似乎并未广泛销售(在 NPL 试验中,静脉是最糟糕的 [1217])。手形几何在一些机场使用了一段时间,并且在 Bertillonage 系统中有一个历史性的前身,19 世纪的法国警察通过物理测量系统识别罪犯。

最近人们对文体学越来越感兴趣,文体学是一门根据作者的写作风格来识别作者(无论是文本还是代码)的科学。这至少可以追溯到一个世纪以前;年轻时,著名的密码学家威廉弗里德曼和他的妻子伊丽莎白一起被一位古怪的百万富翁聘用,研究培根是否写过莎士比亚。 (他们最终揭穿了这个想法,但在此过程中对密码学产生了兴趣。)计算机使运行成为可能

越来越微妙的统计测试和现代应用范围从试图识别发帖到网络犯罪市场和极端主义网络论坛的人到检测大学生的剽窃 [3]。研究人员表明,如果人们尝试 [318],他们可以改变他们的写作风格,足以击败简单的文体学。但大多数人不会这样做,并且通过更多的工作,通常可以检测到试图混淆的事实 [28]。文体学也延伸到代码;程序员可以从他们的编码风格中识别出来[370]。

其他提议包括面部温度图(面部表面温度图,源自红外图像)、耳朵形状、步态、唇纹和心电图。Bertillon 在 19 世纪的巴黎使用了耳朵的形状。也许在食品和饮料行业开发用于质量控制的数字鼻子的巨额投资可能会导致个人设备通过气味识别它们的主人。

最后一个生物特征值得一提 DNA。这已成为犯罪现场取证和确定子女抚养案件中父母身份的宝贵工具,但对于实时应用而言,它太慢且成本太高。作为基因型而不是表型,它的准确性受到同卵双胞胎发生率的限制:120 人中大约有一个白人有同卵双胞胎。还有一个隐私问题,因为可以从个人的 DNA 样本中重建越来越多的个人信息。存在重大程序问题,草率的实验室程序导致错误匹配。

并且还存在较大的数据质量问题;英国警方拥有世界上最大的 DNA 数据库,记录了近 600 万人,但其中约 50 万人的名字拼写错误甚至错误 [878]。

他们还因保留无辜者的 DNA 而受到法院判决,这些无辜者的 DNA 从被判无罪的嫌疑人到旁观者 [102]。适用于地方警务的流程并不总是在全国范围内扩展 从错误输入的记录到嫌疑人提供假名但由于未被起诉而从未被发现的小错误,与实验室错误一起累积,直到误报率变得严重操作和政治问题。在这种情况下,许多人担心 2019 年佛罗里达州的一名侦探设法获得了搜查私人 DNA 测试公司 GEDmatch 持有的所有数百万条记录的搜查令 [899]。

有趣的是,这是否会破坏较大的消费者 DNA 公司的业务,例如 23andMe 和 ancestry.com,足以让他们游说制定更严格的隐私法。

17.8 出了什么问题

与安全的其他方面一样,我们发现由于错误、失误和自满而导致的常见故障。在第 3.4.9 节中,我注意到一份报告称,为 83 个国家/地区的 5,700 家组织提供生物识别建筑入口控制系统的公司的在线数据库未受保护。优步第二次失去其在伦敦的营业执照,是因为他们未能阻止被禁止的司机重新注册,这要归功于照片检查错误 [310]。由于粗心的实验室程序,DNA 分型面临的主要问题是最初的假阳性率很高。这导致了有争议的法庭案件和司法不公。与指纹一样,任何被认为绝对可靠的系统都会

使它的操作员粗心到足以破坏它。

生物识别技术也像许多其他物理保护机制（警报、密封、篡改感应外壳……）一样，环境条件可能会造成破坏。噪音、污垢、振动和不可靠的照明条件都会造成损失。有些系统，如说话人识别，容易受到酒精摄入和压力的影响。环境假设的变化，例如从封闭系统到开放系统，从小系统到大系统，从有人照管到独立，从合作到顽固主体，从验证到识别，都可以破坏事物。

许多有趣的攻击更针对生物识别系统并适用于
超过一种类型的生物识别。

- 法医生物识别技术通常不会像人们想象的那样告诉我们。除了指纹或 DNA 样本可能是由警方植入的可能性外，它可能只是旧的。指纹的年龄无法直接确定，而且印在公共区域的指纹也说明不了多少。

  银行门上的印刷品比被抢劫的金库中的印刷品说明的要少得多。
  因此，在容易遭到抢劫的场所，清洁程序可能对取证至关重要。如果在银行柜台发现嫌疑人的指纹，并声称他三天前去过那里，他可能会因每天晚上都擦亮分行柜台而被定罪。用系统术语来说，新鲜度往往是一个关键问题，一些非常意外的东西会在“可信计算库”中找到它们自己。

- 新鲜感的另一个方面是，至少在理论上，大多数生物识别系统都可以使用适当的记录进行攻击。我们提到了直接攻击语音识别、通过隐形眼镜上的照片攻击虹膜扫描仪以及指纹模型。更简单的是，在像南非这样使用指纹来支付养老金的国家，一直流传着“泡菜罐中奶奶的手指”是她留给家人的最有价值的财产的故事。这里要吸取的教训是，生物特征认证设备的无人值守操作是很棘手的。大头钉并不总是直截了当的。虽然用好的指纹制作模具很容易 [406]，但人们随意留在门把手、啤酒杯等处的指纹通常太脏且太零碎，无法通过识别系统。但攻击绝对是可能的，而且肯定会发生。防御也是可能的；语音识别系统可能会要求你读出不可预知的挑战以阻止录音，而欧盟公民在英国退欧后用来申请在英国居留的应用程序的一个版本会随着手机屏幕上颜色的变化拍摄你的面部视频在你面前。

- 大多数生物识别技术并非对所有人都准确，并且无法像其他人一样可靠地识别某些人群（甚至根本无法识别）。老年人和体力劳动者的指纹通常有损坏或磨损；有顽固犯罪分子故意这样做的传统。黑眼睛和大瞳孔的人给出较差的虹膜代码。没有手指或眼睛的残疾人有被排斥的风险。（这就是 Aadhaar 同时使用虹膜和指纹的原因之一。）制作“X”的文盲更容易遭受签名伪造。

生物识别工程师有时会轻蔑地将此类对象称为“山羊”,但这是愚蠢和歧视性的。一个(或被认为是)社会倒退的生物识别系统 使残疾人、穷人、老年人和少数民族面临更大的冒充风险 应该受到有原则的抵制。它可能会因法律挑战而失败 [1552]。它也可能被假装残疾的恶棍打败。有时,对少数民族群体缺乏关注的行为过于粗暴,甚至是违法的。例如,在 2019 年,英国 Home Oce 部署了一款护照应用程序,尽管它知道它不适用于黑人 [1950]。

- 由此得出的一点是,系统可能容易受到串通攻击。爱丽丝开了一个银行账户,她的同伙贝蒂从中取款;然后爱丽丝抱怨盗窃并提供了一个无懈可击的不在场证明。除了简单地让贝蒂在她的指尖上留下橡皮印外,爱丽丝可能会自愿降低手写能力;通过提供几个略有不同的幼稚样本签名,她可以强制机器接受比平时更低的阈值。她可以花几个星期在她的花园里建一堵墙,然后把她的指纹平放,以降低指纹系统中的登记。她可能会在喝醉时注册语音识别系统。

- 下一个问题是强迫。如果你在中国被捕,自 2020 年 8 月起在香港被捕,警察会将你的手指放在手机上解锁。如果它使用面部识别,他们会按着你的头并将你的手机对准你;如果你想抵抗,你必须闭上眼睛,皱起你的脸 [1348]。

- 系统设计者往往不理解统计数据,而生日定理是一个很大的软肋。例如,数据库中有 10,000 个生物特征,大约有 50,000,000 对。因此,即使错误接受率仅为百万分之一,一旦注册人数超过 1000,出现至少一次错误匹配的可能性就会上升到一半以上 4。所以识别比验证要难得多。

实际结果是,当您试图依赖它作为证据时,为身份验证而设计的系统可能会失败。

- 当设计人员假设通过结合生物识别技术可以获得较低的错误率时,统计学的另一个方面开始发挥作用。但组合通常会提高错误接受率或错误拒绝率,同时使另一个更糟。如果你在家里安装了两个不同的防盗警报器,那么它们同时被击破的概率就会下降,而误报的数量会增加。

- 统计数据通常有些不平衡,因此除了生物特征通常超出正常参数范围的所谓“山羊”之外,可能还有特别容易模仿的“羔羊”和特别容易模仿的“狼”善于模仿别人。所以测试很重要

4 更准确地说,1177:当 N > p1.386/f 时,N 人数据库中的错误匹配配对变得更有可能,其中 f 是单个错误匹配率,此处为 106 [519]。
检查:1177 人进行 1177 x 1176 / 2 = 692,076 次配对,并且这些配对均未配对的概率为:0.999999692,076 = 0.500

在部署之前对大量和不同的人群进行彻底的系统。

- 许多供应商声称他们的产品保护隐私,因为存储的不是您的面部图像、指纹或虹膜,而是从中派生的模板,有点像单向散列,您不能从中获取被识别。有人认为,根据隐私法,生物识别数据不是个人数据,因此可以不受限制地传递。安迪·阿德勒 (Andy Adler) 驳斥了这些说法,他提出了一种有趣的针对人脸识别系统的爬山攻击。给定一个输出输入图像与目标模板有多接近的识别器,输入的人脸被连续改变以增加匹配。使用经过测试的系统,这会迅速生成可识别的目标图像 - 其打印输出将被接受为目标的面部 [24]。

  然后他展示了如何使用这种爬山技术来攻击其他生物识别技术,包括一些基于指纹的生物识别技术 [25]。

- 值得思考一下当人和计算机意见不一致时会发生什么。
  虹膜数据完全不是人类可以匹配的;大多数虹膜代码是从人眼不敏感的相位信息中导出的。

  但是,当警卫和程序对对象的脸是否与档案照片相符时会发生什么?心理学家建议,生物识别系统的使用方式应支持和增强人类认知,并在我们的社会规范范围内发挥作用 [586]。然而,我们工程师常常发现将用户视为必须适应我们的技术的麻烦更容易。这可能会降低人类的表现。例如,当一个自动指纹数据库提取出它认为最有可能的指纹并将其呈现给检查者时:他不会偏向于它吗?计算机不断地测试考官的警觉性,给他三个最好的匹配加上两个不佳的匹配,这不是更好吗,或者这会不会太烦人了?

- 最后,基督教原教旨主义者对生物识别技术感到不安。他们发现启示录 13 章 16 至 18 节谈到敌基督者:“他使众人,不分贫富贫富,自主的,为奴的,在右手上,或是在额上,受一个印记,叫人不得买或卖,除非有兽的印记或名字,或他名字的号码。

所以有一些不平凡的问题。但是生物识别技术现在已经成为主流,一个好的安全工程师需要知道如何恰当地使用它们。

17.9 总结

自古以来,人们就使用一种或另一种生物测量方法来识别人,传统方法是手写签名、面部特征和指纹。现在大规模部署了三个系统:我们手机上的指纹识别、印度和中东的虹膜识别

东方,以及面部识别 由于神经网络革命,面部识别变得更加准确。这些系统各有优势和劣势,而且错误率的统计数据可能非常困难。

当生物识别变得非常广泛时,在无人值守操作中伪造的风险可能会增加:在系统设计中必须考虑虹膜照片、指纹模型甚至是好的老式伪造签名。上下文很重要;如果能很好地融入社会和法律矩阵,即使是像手写签名验证这样的弱生物识别技术也能发挥作用。

生物识别技术通常在有人值守的操作中更强大,在这种情况下,通过良好的系统设计,人和机器的相对优势和劣势可以相互补充。法医使用存在问题,与十年前相比,法院甚至不再盲目信任指纹证据。从历史上看,许多生物识别系统通过威慑犯罪分子而不是实际识别他们来实现其大部分效果。尽管现在有通过人脸识别大规模识别人的前景,而且像俄罗斯和中国这样的威权国家正在这样做,但现在对于我们是否应该允许在民主国家大规模常规使用这项技术存在着严肃的争论。

研究问题

许多实际研究问题都与生物识别系统的设计或改进有关。 2019 年的热门话题是大规模监控闭路电视系统的可扩展性,以及由此引发的关于隐私、自治和主权的政策问题。鉴于面部识别技术仍在快速改进并寻找新的应用,争论可能会持续一段时间并推动相关主题的技术研究。

在为 2000 年第一版撰写本章时,我想到了一个想法,那就是给汽车装上仪表,以便通过驾驶员操作齿轮和离合器的方式来识别驾驶员。如果您的汽车认为它被盗了,它会打电话给控制中心,该中心会打电话给您进行检查。现在有研究表明,触觉系统的用户可以通过他们使用工具的方式来识别 [1478]。所以这是另一个想法。我们可以通过其他学到的技能来识别人类和 AI/ML 系统吗?例如,本章开头的引述 以法莲人因不会说希伯来字母“shin”而被发现并被杀害 实际上是关于人们在年轻时或成年后更难学会的一项技能.流利地使用当地方言的能力是区分内群体和外群体的最普遍和最发自内心的方式之一。酷酷的人群说着最新的俚语,跳着最新的舞。既然机器人和人类一样,拥有只能通过努力获得的技能,这是否会带来任何有趣的地方?

进一步阅读

标准的英国指纹史是由指挥官 GTC Lam bourne [1120] 讲述的,而印度的历史是由 Chandak Sengoopta [1701] 讲述的。

McKie 案例在 Ian McKie 和 Michael Russella [1273] 的一本书中有所描述。
Davide Maltoni、Dario Maio、Anil Jain 和 Salil Prabhakar 合着的一本关于自动指纹识别系统的很好的技术参考书 [1213]。至于面部识别，参见郭国栋和张娜[834]。虹膜代码的标准工作由 John Daugman [517] 完成。对于说话人识别取证，请参阅 Richard Klevans 和 Robert Rodman [1058]。

至于未来，美国国土安全部正在建立一个新的国土高级识别技术（HART)数据库，其中将包括多种形式的生物识别技术，从面部识别到DNA，并整合美国居民和外国人的记录； EFF [1196] 对政策影响进行了描述和讨论。生物识别取证中的错误反映在其他取证技术中；美国国家研究委员会 2009 年的一份报告显示，除 DNA 分析外，大多数法医方法在各个方面都不可靠，这不仅与基础科学技术有关，还与法医实践的分散性、缺乏标准和质量差有关治理[1413]。作为最近的一个例子，索菲·南丁格尔 (Sophie Nightingale) 和汉尼·法里德 (Hany Farid) 发现，一种通过接缝图案识别牛仔服装的常用方法远不及法医检查员多年来声称的那样可靠或可重复 [1447]。