智能网联汽车 生物识别标准化需求研究报告

汽标委智能网联汽车分标委

资源管理与信息服务标准工作组

2022 年 6 月

前　言

在此衷心感谢参加研究报告编写的各单位、组织及个人。

本报告编制过程中参考了行业很多研究成果，在此一并感谢。

组织指导：全国汽车标准化技术委员会智能网联汽车分标委

牵头单位：北京百度智行科技有限公司、中国汽车技术研究中心有限公司。

参与单位：上海商汤临港智能科技有限公司、重庆长安汽车股份有限公司、中国第一汽车集团有限公司、一汽解放汽车有限公司、宁波谦川科技有限公司、上海蔚来汽车有限公司、惠州市德赛西威汽车电子股份有限公司、上海集度汽车有限公司、安徽江淮汽车集团股份有限公司、华为技术有限公司、北京地平线信息技术研发有限公司、零束科技有限公司、博泰车联网科技（上海）股份有限公司、中汽院智能网联科技有限公司、上汽通用五菱汽车股份有限公司、长城汽车股份有限公司、东软集团股份有限公司、博世汽车部件（苏州）有限公司、岚图汽车科技有限公司、北京车和家汽车科技有限公司、联合汽车电子有限公司、厦门金龙联合汽车工业有限公司、通用汽车（中国）投资有限公司、赛力斯汽车有限公司、东风汽车集团有限公司技术中心、斑马网络技术有限公司。

参与人员：贾元辉、鞠伟男、张路、王诗萌、盛了、彭伟、夏方舟、刘丽萍、陶莹、范亦卿、董莉娜、付春晖、郑红丽、王淑琴、卢晶、杨继山、郭伟、张凯、吴优、吴羽熙、邱安崇、蔡静雯、杜秉权、

张丽平、夏文娟、张雷、隋琳琳、潘凯、纪嫣静、陶冶、王艳艳、张东海、田发景、裴峥、张强、唐秋阳、崔硕、覃永进、王鹏、辛泽鹏、卜长凯、吴祥东、吴甜甜、潘嘉汇、马钰嘉、夏春雷、张春旺、刘志腾、牛寅、申远、黄常军、李博、陈自函、陆萍、敖璘琳、郑方、李红林、满志勇、王琳。

目录

前　言 1

1　研究背景 1

1.1　概述 1

1.1.1　生物识别技术简介 1

1.1.2　生物识别技术分类 2

1.1.3　生物识别应用 4

1.2　汽车领域应用 5

1.3　研究范围 8

2　ICV 生物识别技术及应用 10

2.1　生物信息比对 10

2.1.1　场景说明 10

2.1.2　产业普及现况 11

2.1.3　技术原理 12

2.1.4　测评指标及方法 15

2.1.5　痛点分析及应对 16

2.2　乘员监测 18

2.2.1　驾驶员监测 18

2.2.2　乘客监控 25

2.2.3　生物存在检测 27

2.2.4　健康监测 35

2.3　智能交互 37

2.3.1 场景说明.....37
2.3.2 产业普及现况.....38
2.3.3 技术原理.....39
2.3.4 测评指标及方法.....44
2.3.5 痛点分析及应对.....45
3 生物识别信息安全风险分析及应对.....46
3.1 典型漏洞事件.....46
3.2 安全风险评估.....47
3.3 技术应对现况.....51
4 法律法规分析.....54
4.1 国内法律法规现况.....54
4.2 国外法律法规现况.....56
4.2.1 美国.....56
4.2.2 欧盟.....59
4.2.3 其他国家.....59
4.3 小结.....60
5 标准化分析.....61
5.1 国内标准体系分析.....61
5.1.1 基础通用.....64
5.1.2 产品通用规范.....65
5.1.3 应用编程接口.....66
5.1.4 数据交换格式.....67

5.1.5 样品质量.....70
5.1.6 测试方法.....70
5.1.7 行业应用.....72
5.1.8 安全与加密.....73
5.1.9 其他.....74
5.1.10 小结.....75
5.2 国外标准体系分析.....75
5.3 标准化建议.....78
5.3.1 产业发展建议.....78
5.3.2 标准制定建议.....79
5.3.3 标准化路线图.....80
6 总结与展望.....82
6.1 研究总结.....82
6.2 后续展望.....82
附录 A 术语定义.....84
附录 B 缩略语.....85
附录 C 隐私计算示例.....88
附录 D 引用文件.....91

1 研究背景

1.1 概述

1.1.1 生物识别技术简介

生物识别技术是指利用计算机和传感器等技术，对人体固有的生理特征和行为特征进行采集和处理，以实现个人身份识别或行为状态监控，最终为人体提供服务的一种技术。

传统的生物识别技术主要定义于“识别”和“鉴权”的应用范围，而广义上的生物识别技术，也包括动态实时地对生物信息进行采集和分析，以获取生物体状态信息并进一步辅助决策的应用。例如，使用人脸识别技术判断脸部表情变化、识别情绪；利用眼球追踪技术判断驾驶员是否分心、个人心理状况等；通过监测心率等信息以判断驾驶员的健康状况和注意力集中程度等。这些应用突破了传统身份识别的应用范围，是一种更广义范畴的生物识别技术应用。

在身份识别领域，生物识别系统是一种模式识别系统，通过将探测对象的固定物理特征与已存储的信息匹配比对以实现身份识别。系统主要由样本获取模块、特征提取模块、匹配模块和数据库模块等组成，典型应用框架可参考图 1。其中，样本获取模块获取生物物理特征信息并将其发送到系统进行进一步处理；特征提取模块提取样本的固定特征；匹配模块从探测样本中提取的特征与预存特征进行匹配，并返回匹配分数；数据库模块包含所有先前提取特征的数字表示，通常被称为模板。

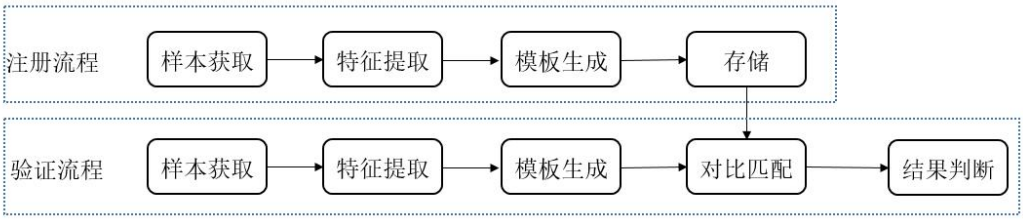


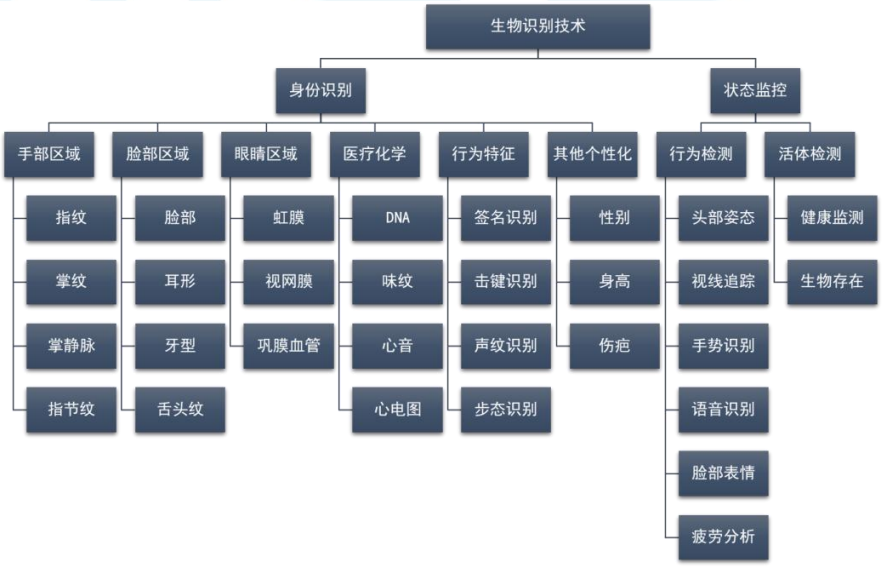
图 1　生物识别技术在身份识别场景的应用框架

在状态监控领域，应用框架相对简单，不需要注册流程。只需增加一个特征分类模块，将提取的特征按设定的条件进行分类，输出分类结果。典型应用框架可参考图 2。

图 2　生物识别技术在状态监控场景的应用框架

1.1.2　生物识别技术分类

生物识别技术从功能维度可以分为身份识别和状态监控两类。当前主流技术可参考图 3。



*根据公开资料整理

图 3　生物识别技术分类参考

身份识别在生物识别技术中应用最为广泛，其主要基于面部特征、

指纹、掌纹、视网膜、虹膜、步态等人体的固有生理特征和行为特征实现身份识别。基于生理特征的生物识别技术包括指纹识别、掌纹识别和面部识别等，其技术相对成熟、应用推广比较广泛。基于行为特征的生物识别技术包括签名识别、击键识别、声纹识别、步态识别等。其中，签名识别系统的可靠性易受时间和人员精神状态的影响；击键识别的准确性也会受到持续时间、出错频率及力度大小的影响。整体看，基于行为特征的身份识别尚处于初期研究阶段、应用仍相对较少。在生物识别领域，目前应用最为成熟的身份识别技术是人脸识别和指纹识别，其次则是虹膜识别、掌纹识别、语音识别等。据美国智库 Acuity Market Intelligence 统计，指纹识别技术占比为 58%，人脸识别技术占比 18%[1]。

状态监控在生物识别技术中的应用也比较多，如在车载应用中针对驾驶员及乘客的行为检测，包括头部姿态、视线追踪、手势识别、语音识别、脸部表情分析等，也有针对儿童或宠物等生物存在的检测提醒等。

目前，生物识别技术常用的模态包括人脸识别、指纹识别、掌纹识别、虹膜识别、声纹识别等，各识别技术的优缺点如表 1 所示。此外，随着生物识别技术的应用要求不断提升，单一的生物识别技术已经满足不了实际的应用需求，多模态混合生物识别逐渐成为生物识别领域未来的发展重点。

表 1　常见生物识别技术对比

生物识别技术	人脸识别	指纹识别	掌纹识别	虹膜识别	声纹识别
特征唯一性	中	高	中	高	低
特征持久性	中	高	中	高	低
准确性	中	高	中	高	低
可接受度	高	中	中	低	高
受攻击可能性	高	低	中	低	高
设备成本	中	中	高	高	低
不适用场景	光线不足、遮挡等	手指损伤、磨损等	手掌缺陷、生理变化等	眼睛受损、隐形眼镜、美瞳等	声带受损、噪音大等

资料参考：前瞻产业研究院[2]

1.1.3　生物识别应用

随着生物识别技术日趋成熟，物联网、云应用、智能设备等市场不断发展，生物识别技术在各领域得到广泛应用。在企业层面，生物识别技术主要用于电子商务、电子货币、考勤等；在实现政府职能方面，生物识别技术主要用于电子政务、户籍管理、社会福利、保险等；在公共安全领域，生物识别技术主要运用于公安刑侦追逃、罪犯识别、边防安全检查等；在信息安全领域，生物识别技术主要用于计算机和网络登录、文件加密和解密等；在场所进出方面，生物识别技术主要用于军事机要部门、金融机构的门禁控制和进出管理等。据前瞻产业研究院资讯，商业企业、政府职能和公共安全是生物识别技术主要需求方，合计占比达到 71%；银行及金融、教育所占比重也在 5%以上；其余领域占比稍小[3]。

在市场需求和技术创新的双重驱动下，生物识别技术在全球范围内取得了快速的发展。据 Frost&Sullivan 和中商情报网讯，全球生物识别市场规模从 2016 年的 126 亿美元上升至 2021 年的 286 亿美元，年均复合增长率为 17.8%。随着人工智能市场的加速发展，生物识别技术的应用领域将进一步扩大，预计 2022 年市场规模将达 340 亿美元[4]。

相对于全球市场来说，中国的生物识别市场占比仍较低，但随着中国经济的飞速发展，生物识别市场规模预期将会保持快速增长。据中商情报网讯，中国生物识别市场规模从 2016 年的 127 亿元增长至 2021 年的 326 亿元，年均复合增长率为 20.7%，预计 2022 年中国生物识别行业市场规模将增长至 400 亿元[5]。近年来，我国也密集出台相关法律法规和政策，以不断加强对生物识别行业的引导和支持。

1.2 汽车领域应用

智能网联汽车的快速发展，使得生物识别技术不仅仅局限于消费、医疗、家居等领域，也越来越适用于车载领域。当前，语音识别、手势识别、指纹识别、人脸识别、驾驶员疲劳监测等生物识别技术的应用已逐渐成为汽车智能化的重要方向。生物识别技术正在不断提高汽车的智能化程度、丰富驾驶环境的个性化功能，通过驾驶员智能监控等方式为用户驾驶提供了更便捷、更安全的驾乘体验。

车载生物识别，主要指通过摄像头、红外传感器、指纹传感器、麦克风等传感器对汽车内外生物体的相关数据进行采集，对其生理特征和行为特征进行分析与处理，实现对车内外生物体的身份识别、状

态监控、个性化服务等功能，使汽车具备一些类似生物的感知能力。

受限于安全、稳定、成本等因素，当前生物识别技术在汽车上的应用尚处于初级阶段，但随着消费需求的变化、技术的迭代发展以及汽车的智能化发展，各汽车厂商也准备将生物识别技术更广泛地整合到汽车应用中。据 Frost&Sullivan 发布的《2016-2025 全球汽车行业生物识别技术》报告预测，到 2025 年，近三分之一的汽车将配备生物传感器[6]。

生物识别技术在汽车领域的早期应用，主要集中在国外品牌的一些高档车型上。其中，宝马在 7 系、5 系等车型装载了手势识别功能；奔驰发布的新一代奔驰 CLA 轿车也将搭载手势识别系统；现代汽车途胜、胜达已量产搭载智能指纹识别开门系统；斯巴鲁的 DriverFocus 系统和凯迪拉克的 Super Cruise 智能驾驶系统都包含了人脸识别和驾驶员监控系统等。此外，欧盟起草并修订了法规(EU) 2021/1341 要求，自 2022 年 7 月 6 日起对车速超过 70 公里/小时的 M 类和 N 类新认证车型强制实施驾驶员注意力监测系统的搭载要求，2024 年 7 月 7 日起对所有新注册车型强制安装驾驶员注意力监测系统。驾驶员注意力监测系统可监测驾驶员的疲劳程度，在需要时向驾驶员提供视觉和声音警告，提高驾驶员的驾乘安全。

在国内市场，相对于传统车企，造车新势力对新技术的应用比较激进，在其车型上同时采用多项生物识别技术，极大提高了车辆的智能化水平。

事实上，车载生物识别技术的应用不仅局限于身份识别、驾驶员

监控、个性化服务等基本功能，还有着更广阔的应用潜力。随着生物识别技术的成熟，车载生物识别技术还可以帮助我们跟踪车上人员的健康状况和情绪变化，如监测车上人员的心跳、脑电波、脉搏等，通过这些技术建立身体监控模型，以判断驾乘人员疲劳程度、是否适合开车等。相信在不久的将来，越来越多生物识别技术将应用到汽车上。

智能网联汽车设计的重点在于用户安全和用户体验，因此大量车载应用程序都会收集用户的生物特征数据，以下为几个典型的应用场景：

驾驶员监测：主要通过面部识别检测技术来检测车内驾驶员的疲劳程度和身体状况，以及利用眼球追踪技术检测驾驶员是否分心，并判断其是否有能力从自动驾驶系统重新接管车辆，从而确保驾驶的安全性。

身份认证：基于安装在方向盘、B 柱、后视镜等临近主驾驶位置的指纹、面部、声线等识别设备，通过面部扫描、虹膜扫描、声纹识别、指纹跟踪等手段，确认驾驶员的身份，身份确认后可解锁车门、后备箱和车机系统。

健康监测：利用方向盘和安全带上的一系列传感器来监测驾驶员的健康状态，例如，安全带上的压电传感器捕捉呼吸、红外传感器测量体温、导电传感器测量心率。通过分析驾驶员心率、血压等信息，车辆可调整情绪照明系统，帮助减少压力或实现健康提醒。当监测到驾驶员出现医疗紧急情况时，车辆会发出语音提醒以提示驾驶员放慢车速，或主动拨打紧急求助电话。

个性服务：在车辆识别出用户身份之后，根据记忆功能对车辆进行个性化配置，如车内座椅、音乐、空调、导航等设备；通过人脸识别技术判断脸部表情变化以识别情绪，来播放不同的音乐。

生物存在检测：通过直接或间接感知技术，检测车内生物存在的情况，如检测车内是否有被遗留的儿童或宠物。当检测出车内有被遗留的生物时，系统将阻止车门上锁并发出警报以提醒驾驶员、乘客或者周围的人，以防止生物在车内发生意外。

未来汽车将逐渐实现多种生物识别技术融合的多模态生物识别功能，识别方式和应用场景也将越来越多样化，如行为测量（通过识别移动速度、力度、倾斜度等要素来预测车内乘员的进一步动作并进行验证）、DNA 识别、生物识别防盗器等。更人性化的车载交互功能也将随着技术的进步越来越多地应用到汽车上。

1.3 研究范围

生物识别技术能够在提升个人身份认证使用便捷性的同时有效地保证安全性，具有广阔的应用前景、巨大的社会效益和经济效益。生物识别技术多样，产业链较长，涉及生物识别算法厂商、芯片厂商、应用开发商、移动终端厂商、检测认证机构等多个角色。不同实现方案所采用的安全保障技术及验证方法参差不齐，可能给用户带来安全使用风险。因此，有必要通过制定相应的技术标准，引导产业健康良性发展和有序运行。

本研究将通过调研生物识别技术在汽车行业中的应用，对已量产或接近量产的典型应用功能下所应用的主要技术类型和标准化需求

进行分析；对暂未量产、尚处于开发阶段的生物识别技术探讨确定相应的概念、应用范围和应用前景，并尝试给出针对性的标准化建议。

2 ICV 生物识别技术及应用

2.1 生物信息比对

2.1.1 场景说明

（1）智能进入

智能进入场景，是指当车主准备开车门时，不需要插入钥匙或按遥控钥匙来开锁，而是通过有感或无感的交互过程完成开锁操作。这类场景涉及的技术主要包括 RFID、NFC、BLE/UWB 定位、指纹识别、人脸识别等。当未授权的人员接近车辆、触碰车辆、准备打开车门、已进入时，系统进行检测以识别并记录可疑人员，避免车主财产安全造成损失。

从应用场景可以看出，身份认证的准确性、安全性、稳定性直接决定了车辆的防盗系数和车主的财产安全。生物特征由于具有唯一性、稳定性、可采集性、伪造成本高等特点，因此适合用于车辆认证解锁的相关场景。例如：在门把手上设置触摸点，通过指纹识别的方式可实现身份认证，进而实现解锁功能；在车门附近安装摄像头，运用人脸识别技术，将探测到的人脸与已保存到的人脸特征进行比对，实现 1:1 甚至 1:N 的身份认证，进而对认证通过的身份授予各种车辆使用权限。

（2）车内付费

车内付费场景，是指通过识别车内的人脸、语音等相关信息，对产品或娱乐内容进行付费。主要应用场景包括车内点餐、车内购物、车内影音视频支付、车内交互付费服务等。

2.1.2 产业普及现况

近年来，在汽车领域推出的生物识别相关身份认证产品主要包括指纹识别、人脸识别解锁系统等，涉及的技术主要包括指纹识别和人脸识别。其中指纹识别技术和产品起步较早，在市场上占据主导地位，占比超过 1/3；随着深度学习和计算机视觉的快速发展，人脸识别技术及其产品在市场上的占比在逐年攀升。

具有指纹识别功能的车辆在市面上出现时间较早，在 2004 年，奥迪 A8 L 6.0 quattro 就推出了指纹扫描识别一触式发动机启动按钮，这类功能主要出现在高端车型中，且由于指纹识别的准确性容易受到光照、温度等因素的影响，通常只在车内配备。随着技术的进步和成本的降低，近年来开始在普通车型上普及。2019 年上市的北京现代第 4 代胜达上装有两个指纹模块，一个安装在门把手上，用于车辆解锁进入功能；另一个安装在车辆启动按键上，用于指纹录入和车辆启动功能。该产品基于电容传感器采集指纹信息，收集指纹信息后会将加密数据发送给系统，并在指纹成功认证后解锁汽车，具有准确性高、稳定性强等特点。

相比于指纹特征，人脸特征更加丰富，基于人脸特征可扩展的应用场景也更具发展潜力。人脸识别技术在交通、安防、金融支付等领域已普及多年，近期在汽车领域中的应用也开始涌现，新近上市的多款车型都具有人脸识别解锁功能。例如 2021 款凯迪拉克 XT4 推出人脸识别智能身份解锁系统，当用户靠近车辆时，通过近场蓝牙感应自动唤醒安装于 B 柱上的高清触摸屏，在高清双目红外摄像头、红外

成像技术及自适应补光系统等配合下，实现刷脸进入。同时该系统还融入了指纹解锁、密码信息等多重保障，提升汽车安全性。2021 款长安欧尚 X5 也推出了人脸识别系统，其将人脸识别设备安装在左后视镜，可实现车辆 1s 解锁。同时该车在车内也配备了人脸识别系统，用于实现车辆启动的身份认证。

2.1.3 技术原理

生物识别身份认证系统主要由生物特征采集、生物特征存储、生物特征比对三部分模块组成。功能的实现还涉及呈现攻击检测、样本质量控制、用户注册管理、数据加密传输等过程。出于对用户个人信息保护的目的，汽车安全场景中的生物识别过程及数据流转一般在车端完成。常见的技术架构可参考图 4。

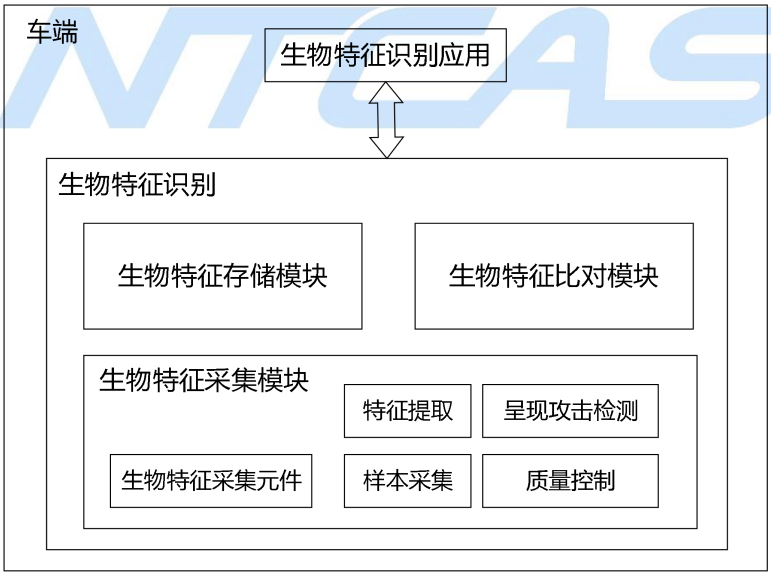


图 4　生物识别原理框图

2.1.3.1 指纹识别

目前，指纹识别技术主要有三种：光学识别、电容传感器识别和射频识别。

（1）光学识别

光学识别是利用光的折射和反射原理，将手指放在光学镜片上，光从底部射向三棱镜，并经棱镜射出，射出的光线在手指表面凹凸不平的线纹上折射的角度及反射光线明暗会不同。再通过 CMOS/CCD 投射，会在灰度图像上形成黑色的脊线（指纹图像中具有一定宽度和走向的纹线）和白色的谷线（纹线之间的凹陷部分），进而由指纹识别算法提取特征，然后与资料库比对判断是否一致。

光学识别的缺点在于该类型指纹模块对使用环境的温度、湿度都有一定的要求。且由于其只能采集到皮肤的表皮层信息，因此受手指表面是否干净影响较大。同时，光学识别容易被假指纹欺骗，稳定性和安全性都不是很高。

（2）电容传感器识别

电容传感器识别是利用硅晶元与导电的皮下电解液形成电场，指纹的高低起伏会导致二者之间的压差出现不同的变化，借此可实现准确的指纹测定。目前电容式指纹模块也分为划擦式与按压式两种，前者体积较小，但操作性较差，准确性相对较低；后者操作更加便捷，识别率也更高。

相比于光学识别，电容传感器识别对环境的适应能力更强，但其对手指干净程度的要求还是比较高，而且传感器表面使用硅材料，比较容易损坏。

（3）射频识别

射频传感器通过发射微量的射频信号，可以穿透手指的表皮层获取里层的纹路以获取信息。相比于前两种技术来说，射频传感器对手

指的干净程度要求较低，可以产生高质量的图像，识别精度较高。然而，射频传感器需要主动发射信号，所以功耗相对较高。目前该技术的实现成本较高、使用的厂商相对较少。

指纹活体检测可以电容传感器和射频识别为原理基础，通过电子信号感应识别对象的生物特征。进一步感知接触物体的导电性、热敏、指脉信号的强弱等，以检测指纹是否为照片、指套等假体。

2.1.3.2 人脸识别

人脸识别，是通过光学摄像头对人脸信息进行采集，对采集到的图像依次进行人脸检测、对齐、特征提取处理后，与数据库已注册的人脸特征进行比对以判断是否为同一个人。其中，人脸检测是将图像中的人脸用矩形框进行标注，剔除背景对后续环节的干扰；人脸对齐是通过旋转、平移、仿射变换等操作对检测到的人脸进行校正，减少由于采集时的角度变化对后续环节的影响；特征提取是通过算法提取特征信息，得到代表人脸的特征向量。

人脸活体检测的方法主要有三种：配合式活体检测、静默活体检测和双目活体检测，防伪等级依次提升。配合式活体检测最为常见，通过眨眼、张嘴、摇头、点头等配合式组合动作，使用人脸关键点定位和人脸追踪等技术，验证用户是否为真实活体操作；静默活体检测无需用户进行繁琐的脸部动作，只需要用户实时拍摄一张照片或一段人脸视频，即可进行真人活体校验，对用户通过显示器播放的人脸视频能进行严格校验识别，防止视频重放攻击；双目活体防伪检测采用“可见光+近红外”光电一体化的人脸活体检测技术，通过对不同光照

条件下的人脸皮肤反射的光谱信息进行分析分类、对异质人脸图像进行关联判断，有效区别出真实人脸皮肤和其他攻击材质的不同。可见光技术可实现人脸快速识别，近红外成像技术具有对可见光照不敏感、电子屏幕无法成像、可穿透墨镜成像等特点，可以更加有效地防止照片、视频、3D 面具等手段的攻击，具有较高的安全性。

2.1.4 测评指标及方法

测评主要有离线测试和实车（在线）测试两种。离线测试以客观评价为主，测评指标包括性能指标和安全指标两部分；实车测试主要以主观体验为主，测评指标主要为性能指标。

a) 离线测试

性能指标包括系统要求、系统性能和系统精度。系统要求包括最大、最小识别距离和最大注册人数；系统性能包括初始化时间、识别时间和识别角度范围；系统精度包括识别精度和活体精度两部分。

指纹识别中，系统精度包括指纹识别精度和指纹活体精度，活体精度包括 2D 纸张和 3D 指模或指套类的精度。测试方法主要是构建测试集，采集多人多种不同类型的指纹数据进行比较。

人脸识别，系统精度包括人脸识别精度和人脸活体精度，活体精度包括 2D 纸张面具和 3D 头模或头套活体精度。测试方法也主要以构建测试集为主。相比于指纹识别，人脸识别的测试集场景需要更为丰富，测试集中的人脸要覆盖不同光照、不同距离、不同角度的场景。

无论是指纹识别还是人脸识别，精度指标一般都用 FRR 和 FAR 评价，也有用 TPR 和 FPR 进行评价；活体精度要求一般采用 FRR 和

FAR 进行评价。两组指标的对应计算方式如下：

FRR =1- TPR =FN/(TP+FN)= (同人相似度<T)的数量/同人比较次数；

FAR=FPR= FP/(FP+TN)= (非同人相似度>T)的数量/非同人比较次数。

安全指标用于评价整个系统抵御外部攻击、保护数据隐私的性能，主要包括系统安全和个人隐私安全。系统安全隐患除了由识别算法导致的误匹配外，还包括注册阶段和识别阶段的外部攻击。注册阶段的主要攻击类型包括伪造身份通过审核、使用伪造特征进行注册、入侵数据库篡改已注册的生物特征信息等；识别阶段的主要攻击类型包括篡改特征处理器、篡改匹配器、传送攻击、重放攻击等。为保证系统安全性，一般要求系统使用加密手段对生物特征进行加密。为保证个人隐私安全，会进一步对加密手段进行限制，如要求加密算法具有不可逆性、不可链接性等。

b) 实车测试

实车测试主要针对实际体验场景进行测试，以真人实际体验测试为主，包括不同距离、不同角度、不同光照度进行测试。同时也需要验证响应时间、处理时间等技术指标。其中，精度指标通常会使用ACC，具体计算方式如下：

$$ACC=(TP+TN)/(TP+FN+TN+FP)$$

2.1.5 痛点分析及应对

使用场景中的痛点主要有以下几点：

a)摄像头成像痛点

采用摄像头的技术方案，无论是何种摄像头，外界光线等环境要素的变化，都可能导致整体画面过暗、过亮或阴阳脸等；也会由于用户佩戴眼镜、帽子、口罩等配饰，导致人脸的局部区域被遮挡，并因此导致在最终成像时出现无法识别人脸或者人脸特征点不清晰的情况，使得产品功能失效。

当前，为解决这一痛点，通常会通过硬件 ISP 或者软件 ISP 功能对画质成像进行调节。但类似试图修复画质的方法依然存在一定的局限性，特别是很难保证极端光线下的场景效果。未来，预期可通过多技术融合手段解决。

b)活体攻击痛点

人脸或者指纹识别应用于认证授权均面临着伪造、重放等被攻击的风险。相比人脸识别，指纹复刻和造假技术更简单、快捷。

为解决这一痛点，除了建立相关技术保护机制外，还应当通过针对性的测试来验证并最终提升相关产品的抗攻击能力。

c)构建测试集痛点

类似于产品抽样，构建测试集的方法既希望测试集的样本量足够多以尽量覆盖所有使用场景、又希望在构建测试集时能控制成本。然而，由于硬件原理、生物识别算法计算原理不同，行业很难构建公用测试集。

指纹识别的硬件原理单一且受到外界环境影响因素少，传感器选择较为单一，受光照因素影响较少，尚可以构建部分公用测试集；相

比之下，受传感器、模组、光照的影响，基于视觉的人脸识别在这方面的痛点更为明显。

为解决这一痛点，可以通过规范相关测试方法、明确对应的摄像头成像质量、规定验证时信息比对测试集方案来降低相关风险、减少痛点应对成本。

2.2 乘员监测

2.2.1 驾驶员监测

2.2.1.1 场景说明

在完全自动驾驶实现之前，驾驶员需要完全地或部分地参与到驾驶任务当中。执行驾驶任务要求驾驶员感知驾驶环境、完成驾驶决策和执行驾驶动作。驾驶分心会影响驾驶员对环境的感知和接管响应能力，导致驾驶员无法准确理解驾驶情境从而引起交通事故。根据公开资料，超过90%的道路事故是由人员本身犯错造成的，这些错误可以分为两类：违法与失误。

违法主要包括超速、醉驾、毒驾等违反法律或危险驾驶的行为。2019年上半年全国查处酒驾醉驾90.1万起，其中醉驾17.7万起，因酒驾醉驾导致死亡交通事故1525起。

驾驶失误主要由分心、疲劳或经验不足导致，这些情况并不违法但会严重影响驾驶安全。驾驶分心的原因主要有两种，一是视觉分心、二是认知分心。视觉分心体现在驾驶员的视线离开路面，转移到其它与驾驶无关的事物上，导致驾驶员对环境的感知能力降低，从而引起交通事故。认知分心体现在驾驶员思考其它与驾驶无关的事情或处于

走神的状态，导致驾驶员忽视关键道路要素、驾驶决策能力降低，从而引起交通事故。随着老龄社会的来临，驾驶员身体的突发状况也是发生事故的主要原因之一。

实际上，在日常驾驶中，几乎所有驾驶员都在接受一定程度上的驾驶员监测，比如：长时间连续驾驶后来自导航地图的休息提醒，或者来自同车乘员的状态观察及休息提醒。相比较于传统监测方式，基于生物识别技术的驾驶员监测功能显然更加准确有效。随着汽车驾驶自动化程度的逐步发展，驾驶员监测作为 ADAS 驾驶辅助及 L3 自动驾驶应用的一个重要功能，将发挥越来越明显的作用。

驾驶员监测，具体功能可包括监测驾驶员接管能力、监测并警示驾驶员疲劳或分心驾驶、监测驾驶员动作等。搭载于 L2 及以下驾驶自动化能力车型的驾驶员监测功能，主要用于判断驾驶员注意力状态，当驾驶员出现注意力不集中或疲劳状况时，及时发出警示；搭载于 L3 驾驶自动化能力车型的驾驶员监测功能，主要用于对车辆设计运行条件内驾驶员状态进行监测判断，评估驾驶员是否具备接管能力，作为自动驾驶系统是否可开启的判断条件。

疲劳监测，主要是对摄像头获取到的人脸进行识别并提取眼睛闭合度、眨眼、嘴巴闭合度等特征，进一步判断驾驶员的疲劳程度；注意力监测，主要是通过摄像头监测驾驶员的面部特征点、头部姿态和视线落点以判断驾驶员注意力状态；异常动作监测，主要是通过对摄像头获取到的人脸信息识别并提取图像中人脸嘴部、耳部及手部状态，来判断驾驶员是否有抽烟、打电话和喝水等异常动作。监测到以上驾

驶员异常情况后，可发出声光报警信息进行提醒，或与车辆的其它模块联动控制给出触觉提醒（如：空调、安全带等）。

2.2.1.2 产业普及现况

目前，驾驶员监测已成为国内智能座舱的重要发展方向，包括小鹏 P5、极氪 001、Alpha S、长安 UNI-T、智己 L7、零跑 S01、长城等均搭载了车内摄像头，通过软件算法可实现驾驶员监测。

由汽标委智能网联汽车分标委于 2021 年完成审查的推荐性国家标准《驾驶员注意力监测系统性能要求及试验方法》，主要对基于视觉识别的驾驶员注意力监测系统提出了明确的技术要求及测试方法。CNCAP（中国新车评价规程）作为中国最具影响力的第三方测评规程，于 2022 年 4 月发布 2022-2028 路线图，并计划于 2025 年版本中增加驾驶员监测功能的测试要求，以加速驾驶员监测功能的普及。

国外的驾驶员监测主要是把车辆的动态数据作为判断驾驶员分心和疲劳的判定依据。欧盟范围相关车企包括宝马、大众、奥迪等，均配备了以车辆动态数据为主要依据的疲劳报警方式，部分车型还加装了摄像头补充感知。欧盟 EU-771 法规，将驾驶员疲劳分为 9 个等级、并要求系统应具备识别 7 级及以上疲劳状态的能力。该法规计划于 2022 年 7 月配合 EU 2019/2144 实施，实施后将要求欧盟上市车辆具备驾驶员疲劳监测的功能。和国内标准相比，欧盟发布的 EU-771 法规测试方法更偏向于主观测试。

2.2.1.3 技术原理

早期的驾驶员监测系统大多是采用基于车辆行为特征的方法，近

些年随着深度学习技术的兴起，基于驾驶员行为表现的监测方法越来越成为市场主流。同时越来越多的研究者开始尝试把其他驾驶员相关的生理特征信号和传感器方式引入应用。

目前驾驶员监测有四种不同的技术方案：通过监测车辆信息间接监测驾驶员状态、基于生物传感器获取驾驶员生理指标进行直接监测、基于视觉传感器获取驾驶员行为信息进行直接监测和基于其他传感器的驾驶员监测方案。

（1）基于车辆信息的驾驶员监测方案

主要是通过对方向盘转角、方向盘握力/扭转力、加速度、制动踏板力、行车数据、驾驶时长等信息进行分析，实现对驾驶员驾驶行为的间接监测。该方案的理论基础是驾驶员疲劳程度加深或者分心时，不自主对车辆的控制能力变弱，并且反映在对车辆操控上的异常，如双手脱离方向盘、方向盘的大转动幅度次数增多、车辆越过车道线的频率更高等。通过这些异常情况的数据分析，进而推算驾驶员的疲劳程度及分心情况。

该方案优势为部署成本低，基于现有车辆的车身电子稳定系统控制单元所获取的信息即可部署，且资源占用率低。但由于该方案并不直接监控驾驶员，而是通过驾驶数据间接推测驾驶员状态，在急转弯、急加速等场景下，难以准确评估驾驶员状态，容易导致误报和漏报。

（2）基于生物传感器的驾驶员监测方案

主要是通过部署在方向盘或安全带上的电容传感器等对驾驶员生理指标数据进行分析，进而推断驾驶员当前状态。该方案的理论基础是人体处于疲劳等非正常状态时，心率、血压、皮电反映、皮肤温

度、脑电波、心电图信号检测(ECG)、脉搏信号检测、肌电图信号检测等生理特征指标与正常状态下有所不同。通过对异常指标的分析判断驾驶员的状态。例如：大脑皮层兴奋与抑制时，其脑电图上的表现不同，通过分析脑电图上的频率分布和波形，即可推测大脑活动的功能状态，从而推测是否存在心理疲劳。

该技术优点主要是准确率高。但由于传感器安装不便、驾驶员携带困难、整体部署成本较高等原因，目前在量产车型中尚未部署，仅在一些研究试验和学术论文中起到辅助验证的作用。

表 2　各种评测方法优劣性

评价方法	可靠性	实时性	灵敏度	侵入性	抗干扰性
方向盘转动情况检测	一般	好	一般	无	一般
车道偏离检测	一般	较好	一般	无	较强
Perclos 检测	高	好	较好	无	较强
嘴部状态检测	较高	一般	较好	无	较强
视线方向检测	一般	一般	一般	无	一般
EEG 信号检测	高	较好	好	有	强
ECG 信号检测	较高	较好	较好	有	较强
脉搏跳动检测	较高	较好	较好	有	较强
肌电图信号检测	较高	较好	较好	有	较强

（3）基于视觉传感器的驾驶员监测方案

主要是通过部署在方向盘、仪表盘或 A 柱等位置的光学摄像头、红外摄像头，获取驾驶员面部状态（如嘴部状态）、眼部状态（如眼睑闭合情况、视线情况）、头部姿态（如头部位置、姿势）、打哈欠、打电话、抽烟等行为的图像或视频信息，通过深度学习算法进一步分析，进而判断驾驶员当前状态，实现驾驶员监测的目标。

此方案的最大优势在于部署成本不高，一颗摄像头可同时满足舱

内多种监测需求。并且该方案技术较为成熟可靠、识别准确度高、监测实时性好，可根据驾驶员的不同感知程度，联合整车对驾驶员及时发出报警和提醒。若利用红外摄像头技术，在夜间仍可对驾驶员抓取清晰的图像，实现对驾驶员状态的全天候监测。

但该方案对摄像头的成像质量依赖较强，仅使用单个视觉特征的系统鲁棒性差，一旦出现遮挡或光照剧烈变化，很容易受到干扰。当驾驶员佩戴眼镜时，镜片上容易出现红外灯的光斑或出现车外事物的成像，当这些光斑或成像与驾驶员眼球重合时，摄像头获取准确眼球信息或面部信息的能力下降，从而导致系统识别准确率下降。

（4）基于其他传感器的驾驶员监测方案

对于酒驾、毒驾以及其他生命体征状态异常情况，可通过生物传感器或视觉传感器进行监测。

目前，此类方案准确率相对较差，例如，通过视觉传感器进行酒驾监测，可以识别驾驶员脸红等异样状态，从而进一步作出是否酒驾判断，但是驾驶员的个体差异导致通过视觉判断是否存在酒驾的可靠性不高。全身性的驾驶员状态监测系统（如超声、血流感应等）正在研究，通过与驾驶员整体健康监测的深度联动，可更精准地监测驾驶员状态，从而更准确地判断驾驶员的驾驶能力。

2.2.1.4 测评指标及方法

驾驶员监测的测评方法主要包括离线测试、台架测试和实车测试。离线测试和台架测试主要以客观评价为主，实车测试主要以主观体验为主。测评指标主要包括系统要求、系统性能和系统精度，系统要求

一般为功能要求；系统性能主要包括资源占用率、耐久测试、初始化时间等；系统精度主要是包括各个功能的精度要求。

a) 离线测试

离线测试通过采集不同光线、场景、道具和人员动作构建不同的测试集。针对测试集进行精度测试，常用的精度指标一般为 TPR、FPR 和 PRE 三个指标中的任意两个。计算方式如下：

$$TPR=TP/(TP+FN)$$

$$FPR=FP/(FP+TN)$$

$$PRE=TP/(TP+FN)$$

b) 台架测试

在台架上多人模拟相应不同动作（结合光线、眼镜、墨镜、配饰等因素），综合计算识别率，精度指标和离线测试相同。相比于离线测试，台架测试的测试方法和测试结果可再现，但台架测试设备复杂、更容易受场地因素影响。

c) 实车测试

常用的实车测试指标一般有两类。第一类为固定时间内误报次数，其主要从驾驶感受角度来控制整体系统的误报次数，其特点在于可以有效统计在一定正常驾驶时间内误报的个数；另一类为准确率 ACC，其计算方式如下：

$$ACC=(TP+TN)/(TP+FN+TN+FP)$$

但由于在实际应用过程中，很难精确统计负样本数量，即正常驾驶情况下不报警的个数，所以 ACC 可用性不好，通常会替换使用关

键成功指数 CSI(critical success index) ，其计算方式如下：

$$CSI = TP/（TP + FN + FP）$$

2.2.1.5 痛点分析及应对

无论上述何种技术原理，复杂场景的准确及时应对是驾驶监测系统应用中的一个难点。以基于摄像头的视觉方案为例，受限于摄像头的安装位置及强光、逆光、驾驶员墨镜等因素的影响，摄像头获取不到有效图像，导致驾驶员疲劳监测系统失效或者性能降低。同样，除视觉外的其他传感器也会受到一定的局限性。

和生物信息比对一样，测试集构建的数据规模和成本的矛盾点也是驾驶员监测验证的痛点之一。如何既能保证真实且丰富的驾驶场景，又能确保试验人员安全的数据采集，也是主要痛点。

针对上述痛点，在实际使用场景下，如何适时地给驾驶员有效的反馈，是重要的衡量指标。不仅需要算法的准确率高，还需要在预警策略的设计中加入更多人性化的考量。同时还能够引入更多维度的传感器或感知数据，配以符合算力需求的强大芯片，基于更符合驾驶员监管策略的交互设计，让系统与驾驶员之间建立更加充分的信任感。

2.2.2 乘客监控

2.2.2.1 场景说明

乘客监控主要是针对车舱内的乘客进行监测，一般应用场景包括乘客的疲劳、抽烟、打电话等行为监测，以及协同提供降低娱乐系统音量、打开车窗或者天窗等控制服务。

此外乘客监控还包括判断车内座位占用情况、乘客系安全带提醒

等功能。

2.2.2.2 产业普及现况

目前行业中基于摄像头的乘客监控类产品逐步上线，包括广汽、长城、长安在内的一些车企已发布相关产品。主要功能包括乘员人数检测、副驾驶及后排打电话降低音量控制、吸烟打开车窗控制等。以广汽 AION Y 为例，该车型能识别车内成员的年龄和情绪，并进一步智能推荐歌单；另外，该车型还有副驾通话自动降低音乐音量等功能。

2.2.2.3 技术原理

目前，乘客监控实现主要涉及两种技术：传统传感器方案和摄像头方案。传统传感器方案主要是通过座椅传感器、安全带传感器等对乘客状态进行基础识别、监测，但很难通过传感器监测相关乘客疲劳、打电话或者抽烟等异常状态；摄像头方案和驾驶员监测摄像头方案类似，主要通过安装在车内的摄像头（一般安装在内后视镜或阅读灯位置），对乘客进行监测。

传统传感器方案用来实现更为丰富的乘客监测功能会存在很多问题。例如，座位配备乘客分类系统的传感器通过感知乘客来判断是否需要打开该侧的安全气囊，这种功能的合理实现通常对座位上人员或者放在座位上物体的质量、位置和方式有一定要求。一些体型较小的乘客难以被传感器发现、一些重物又会误触传感器。

相比来看，摄像头方案能更准确地探测区分物体、人员，也可以通过一颗摄像头满足多个功能，例如座位探测、人员吸烟等情况，有效降低了整体成本。摄像头方案的不足之处在于计算机视觉技术的局

限性，例如，座椅遮挡导致视觉不可见、光线和畸变等因素造成视觉偏差。

2.2.2.4 测评指标及方法

摄像头方案乘客监控的性能指标和测评方法和驾驶员监测方式类似，可参考 2.2.1.4 章节。

2.2.2.5 痛点分析及应对

基于传统传感器的方案，识别准确率高、但痛点在于功能单一，若实现更丰富功能就必然要求安装更多数量传感器、导致成本上升。基于摄像头的方案，大部分情况下只要安装一个或两个摄像头就能覆盖全车场景和多个功能，但其对座椅位置识别准确率较低。

在成本可接受的情况下，不仅可以安装多个传感器来确保其稳定性，也可以通过多传感器融合的方式来弥补相关的不足。当成本受限时，可以通过调整安装传感器的位置或者摄像头的安装位置来覆盖重点区域。

2.2.3 生物存在检测

2.2.3.1 场景说明

研究表明当车内温度达到 35℃ 时，在阳光继续照射 20 分钟后，车内温度可以达到人体承受的临界水平（41℃）。若此时车内留有儿童（或宠物），由于儿童不具备采取有效行动的能力，如脱衣服、打开窗户等，其将面临严重的中暑甚至死亡的风险。因此，通过儿童存在探测（CPD, Child Presence Detection）技术检测车辆中的儿童，并提醒车辆用户或第三方服务，以降低车内滞留儿童中暑和死亡事件发

生的频率。

2.2.3.2 产业普及现况

宝马、通用等国际厂商很早就开始在其旗下的车型搭载应用儿童存在探测功能。近些年，国内主机厂也纷纷在新款车型上新增该功能，预估将在2023年前后实现大规模量产。

Euro-NCAP已将儿童存在探测配置纳入加分项，有力推动了汽车行业对儿童存在探测系统的装配率。在最新发布的C-NCAP（2022-2028）路线图中，儿童存在探测功能已被纳入2025版测试规程，2025版规程（初始期）间接感应与直接感应并行（只要有一种感应方式就可得分，且分值相同）；计划在2027版（过渡期）中加入增强警告，倾向于直接感应（直接感应得高分、间接感应得分不得超过直接感应）；计划在2029版（稳定期）中仅直接感应得分、间接感应不得分。

2.2.3.3 技术原理

生物存在探测手段主要可分为间接感应和直接感应两种。

间接感应，即利用打开车门、压力传感器或电容感应等信息，根据逻辑推断出车内是否存在滞留目标。该方法容易实现，不需要复杂的传感器和算法，但无法检测被遗留的是活体还是物体，并且需要考虑各种容易引起误报的开关门逻辑。因此，在准确率和误报率方面，该技术都存在较大的局限。

直接感应，即通过感知心跳、呼吸、运动或任何其他生命迹象来探测车内是否确切存在人的能力。目前的儿童生命体征检测技术有：

心冲击检测（心脏搏动和大动脉血液流动引起的身体周期性振动）、毫米波雷达检测（检测呼吸/心跳引起的儿童胸腔/腹腔振动）、超声波雷达（检测车内物体形状）、视觉方案（通过图像识别车内儿童或其它活体）。

心冲击检测技术和毫米波雷达检测技术可直接检测儿童生命体征，在很大程度上可以防止洋娃娃等人形物体引起的误报。毫米波雷达在工作时，通过发出的毫米波对目标进行照射并接收其回波，由此获得探测目标的距离、方向、速度等参数，通过连续对比这些参数，就可以得出车内有无物体在动。毫米波雷达通过检测儿童或宠物的心跳、呼吸时胸腔的浮动、儿童或宠物有无肢体动作来判断车内是否有儿童或宠物遗留。毫米波雷达的技术优势在于可以检测微小的物体移动，例如儿童或宠物的呼吸。根据波的传播理论，频率越高，波长越短，分辨率越高，探测距离越远。

视觉方案主要通过视觉对目标进行检测，通过连续比对和视觉检测得出车内有无物体在移动，并可以通过儿童或宠物的肢体和脸部特征进行识别。其优势在于，可以利用乘客感知摄像头同步解决儿童或宠物遗留问题，更集约利用整车成本；缺点在于，前排座椅、衣物或其他舱内物体的遮挡以及儿童或宠物的动作容易导致一些区域无法被正确识别和辨别，从而出现误报警和漏报警。为了弥补视觉技术方案在生命体感知、摄像头遮挡等条件下的不足，国内外一些新车 CPD 模块开始尝试毫米波雷达技术方案。

2.2.3.4 测评指标及方法

Euro-NCAP 对儿童存在探测系统提出了要求，并分别针对间接探测系统和直接探测系统提出了不同的测试方法。针对间接探测系统，主要基于不同场景设计测试用例，依据测试用例开展测试，根据探测结果对系统功能进行评估；针对直接探测系统，主要基于不同场景下的儿童假人状态设计测试用例，根据探测结果对系统功能进行评估。

Euro-NCAP 直接感应系统的评估基于车辆制造商提供的信息进行，车辆制造商需提供一份材料，详细说明系统如何确定儿童的存在，以及随后的警告规则，在提交材料和车辆评估之前，测试工具验证必须得到 Euro-NCAP 的批准。

（1）材料内容

车辆制造商应提供证明系统性能所需的所有必要信息，至少包括以下内容：

① 一般系统信息：

- 传感器类型和原理：wi-fi、RF、摄像头等；
- 传感器位置和 CPD 系统架构；
- 探测参数：运动、呼吸等；
- 探测覆盖区域，包括脚部空间和所有可选座椅；
- 临时/长期停用方法及要求（如适用）；
- 警告所需的 CPD 移动设备应用程序（如适用）。

② 传感数据：

- 呼吸监测输出数据；

- 运动监测输出数据；
- 触发阈值等信息；
- 外部干扰，例如阳光、电磁波、无线电波等。

③ 系统合规性证明：

- 感知和决策到警告激活的时间；
- 警告信号演示；
- 干预示范（如适用）。

④ 测试工具的验证情况（如适用）

OEM 和/或系统供应商需要提供详细的信息说明任何所用测试工具的验证情况。如果使用工具代替人类受试者，则验证数据需能够证明测试工具可以用作合适的人类替代物。

需要在车辆中对真人记录的输出与测试工具的输出进行直接比较，上述测试场景应与传感技术的“最坏情况”条件/主题的详细信息进行对比并一起提交。要求从新生儿到 6 岁左右的一系列人类受试者，以及年龄、体重和身高信息，以证明测试工具能涵盖人类受试者在该探测系统中的最坏情况。根据正在评估的参数，可能需要将儿童或相应的测试工具放置在适当的儿童约束系统（Child Restraint Systems, CRS）中。如果在测试工具的开发或 CPD 系统的验证中使用人类受试者，则必须遵守所有相关的道德和隐私准则。

（2）测试场景

直接感应系统必须能够对所有可能的用例做出正确响应，测试场景可以是室内（停车场）或室外，但需具备系统功能实现所需的条件，

例如手机信号和温度等（如适用）。儿童状态、毯子和遮阳帘要求如下：

①儿童被遗忘和故意遗留在后面

a) 后向 CRS 中的新生儿：

•睡在毯子/遮阳板下

b) 后向 CRS 中的一岁婴儿/儿童：

•睡在毯子下，四肢不动

•在毯子下醒来，肢体运动

c) 前向型 CRS 中的三岁儿童：

- 睡在毯子下，四肢不活动
- 在毯子下醒来，肢体运动

d) 前向型 CRS 中的六岁儿童：

- 睡觉时没有四肢运动
- 醒来时四肢运动

② 儿童进入解锁车辆

评估条件详述如下：

- 车门未上锁的停放车辆；
- 车门（任何车门）打开，受试者进入车辆，车门关闭（未上锁），但儿童锁激活；
- 触发传感器（直接或可能仅在一定延迟时间后）以检查车辆中是否有生物（包括脚部空间）；
- 确认儿童存在时，则必须触发初始警告。

（3）具体要求

系统可以单独或组合使用一系列参数来确定儿童存在情况和/或儿童分类，OEM 需证明该系统用于探测儿童呼吸或运动的各个参数如下：

①呼吸：睡眠儿童应使用以下呼吸频率：

- 新生儿 30bpm
- 一岁儿童 22bpm
- 三岁儿童 20bpm
- 六岁儿童 18bpm

②运动和姿态：需要一个尺寸和运动状态可以任意变化的儿童假人，并可以在 CRS 中进行如下活动：

- 头部：俯仰、翻转、侧倾
- 上下肢：挥手、踢腿、玩手等

③白天和黑夜：使用光学传感方法的系统（如摄像头）需要证明系统可以在各种照明条件下（例如白天和夜间）探测到儿童。

2.2.3.5 痛点分析及应对

间接检测技术的测评方法较为明确，按照需要报警和防止误报警的儿童遗留用车场景进行开关门、放置儿童、行车、锁车等不同流程。但间接检测需要客户严格按照相关方法来进行执行，一旦中间某个步骤和间接检测方案冲突就会有一定的误判出现。

基于门逻辑的车内生物检测，根据车辆的开关门逻辑判断车内是否有遗留物体，但该方法无法判断车内是否放置物品，更无法判断是

否有生命体，容易误报。

基于压力传感器的车内生物检测，根据预先设置的重量激活值，判断座椅上是否有儿童。但压力传感器的最小重量激活值不容易确定，不同儿童体型和重量差异较大，皮包、衣物等物体放在座椅上容易导致误判。

直接检测要求系统能识别在不同光照、儿童座椅类型、身体覆盖情况、儿童肢体运动状态和不同年龄等多种条件下的儿童生命体征。

基于毫米波雷达的车内生物检测，基于高频毫米波雷达实现车内人员检测，能够获取车内移动人员的准确检测信息。但毫米波雷达面临使用波段是否合法的问题。

基于双目摄像头的车内生物检测，通过对双目相机进行标定，获取座椅的点云信息，可以实现对座椅上的占用目标检测（包括车内的人员）。双目立体视觉能够同时获得 RGB 图像信息和深度信息，RGB 信息能够提供丰富的语义信息，深度信息有助于获取立体物体表面点云信息，对空间距高变化更为敏感。但双目立体视觉存在的缺陷是双目的深度信息获取依赖于 RGB 图像信息的配准，受到光照的影响比较大。

基于单目摄像头的车内生物检测，在 RGB 图像中实现人脸检测、人体检测、骨骼关键点检测。通过 RGB 图像信息能够获得丰富的语义信息(比如人脸、人体、骨骼关键点等)，再进行目标分类、跟踪和姿态识别。但该方案的不足是一般的 RGB 相机对遮挡物体无法根据语义信息进行判别。

基于红外相机的车内人员检测，根据不同的热像图，通过弹性束图匹配法(EBCM)的三维人脸识别算法判断并区分成人和小孩。红外相机能够获取丰富的驾乘人员面部信息，但是红外相机容易受到环境温度影响，三维人脸匹配算法使用的特征描述器维度信息较低，无法用来区分多个不同的人脸信息。

2.2.4 健康监测

2.2.4.1 场景说明

近年来，公共交通工具的乘员健康问题（如乘员疾病突然发作等）新闻不断见诸报端。而随着新冠肺炎疫情常态化防控的深入推进，公共交通工具作为社会运行的重要载体，乘员的健康状况监测成为新冠肺炎防控关口前移的重要手段。

乘客健康状况监测内容主要包括心率、呼吸频率、血压、血氧等，主要应用场景如下：

通过视觉、红外、挥发性有机物传感器等设备的综合分析，当乘客疾病突然发作时，车辆能够快速识别乘客发病情况并做出提醒。然后可进一步与高精地图系统联动，自动规划前往最近医疗机构的最快路线。同时与 V2X 系统等联动，广播推送该车有重病乘客，与道路信号灯、交通警察、急救中心等系统协同运作，从而实现重症患者的方便转运，减少等待时间。同时，急性病突然发作时，乘员健康监测系统也可以根据病种向车内其他乘客推送最合适的紧急救援方案。

在新冠肺炎常态化疫情防控期间，可通过车上集成的血氧传感器、红外热传感器、音视觉相机，精准定位发热、咳嗽等具有新冠肺炎症

状人员，同时可及时反馈至疾控中心、定点医院、当地政府等疫情处置责任主体，自主判断车辆是否应该停止运营，并为新冠肺炎疫情流行病学调查提供精准定位。

2.2.4.2 产业普及现状

目前用于车内健康监测的产品主要分为两类：一类是车辆出厂时自带的一些健康监测设备，如心率方向盘、智能座椅等；另一类是面向消费级的智能穿戴设备，如健康手表/手环等，这些设备可通过蓝牙传输的方式实现与车辆控制器的通信，实时传输相关生命体征数据。此外，还有一些技术手段，包括脑电波监测、视觉检测等，其相关产品尚处于研究开发阶段，量产应用车型中暂不常见。

2.2.4.3 技术原理

目前智能穿戴设备基本都包括心率监测的功能。常见的心率监测原理是基于 PPG（容积描记波）的方法，它使用光电式的检测方法将 LED 光源照射进入人体的皮肤组织，然后通过接收端的光电接收管来将接收到的光信号转换为电信号。由于皮肤组织内的血液流量随着脉搏的变化而周期性地变化，同时血液中的含氧血红细胞的比例也随着脉搏的变化而变化，因此它们对入射光的吸收程度也随着脉搏而呈现周期性的变化，体现在接收端就是接收到的电信号也随着脉搏而变化。通过算法可以解调出这个信号，从而估算出脉率，即心率。

视觉方法通过摄像头对多个皮肤区域进行采样，通过血液对不同波长的光的不同吸收率以及不同波长的光的皮肤穿透能力不同，从而计算出心率、血压等相关技术指标结果。另外通过多种传感器包括血

氧传感器、红外热传感器、音视觉相机等结合的方法来判断人体健康。

2.2.4.4 测评指标及方法

当前主要参考医疗相关的行业标准作为评价指标和评价方法。

2.2.4.5 痛点分析及应对

目前，在乘员健康监测方面，主要运用的传感器有视觉相机、红外相机等，同时基于超声波的非接触血流感应也处于研究阶段。而在系统的开发成本中，由于目前尚未大批量铺开，故系统的硬件成本存在进一步降低的空间；软件算法方面，对人体状态的进一步理解也需要大量的实际数据为支撑，丰富训练数据集，从而提高对人体所处状态的识别能力。

通过压力传感器/电容传感器等判断车内各个座位的使用情况，以及通过车内面向乘客的摄像头判断车内情况，都是目前主要的技术。前者硬件成本相对较高，虽然其可以比较高精度地判断人的位置，但是容易对重物相关的内容进行误报；摄像头方案在基于可见情况下的准确率更高，硬件成本更低，但是在不可见时的准确率比硬件传感器更低。

2.3 智能交互

2.3.1 场景说明

智能交互是指通过语音、手势、视线等方式，提升乘员对车舱系统的控制和调节体验的功能。

语音交互，是汽车座舱智能化的标志性功能，主要通过车内遍布各方位的收音装置，根据驾驶员及乘客的语音内容完成各类功能的启

动和调整。语音识别已可实现车窗、座椅、空调、香氛等车控功能，同时可实现车辆信息查询、生活信息查询和导航系统的智能语音识别、定位目的地和文字输入等功能。部分车企利用人工智能算法，可以实现与驾驶员、乘客的持续对话，实现更加精准和复杂的控制需求。

手势识别，主要通过车内各类传感器收集驾驶员手势动作，可实现通过手势控制车辆各类功能的目的。静态手势识别可实现车内前后排乘客对于空调调节、音量调节、音乐切歌等功能，甚至还包括了猜拳、动作识别等互动游戏；动态手势识别可实现页面翻页、视频切换、车窗控制等复杂功能。手势识别可提升隔空科技感，提高驾驶人机交互体验、驾驶的便利性和舒适度。

此外，智能交互还可以基于摄像头、雷达等传感器探测车外的生物信息实现各种交互功能。例如，车外交警手动指挥信号的识别、通过语音交互的物流取件等。

为了更加准确清晰地了解驾驶员及乘客意图，在实现语音、手势交互等基础功能外，通过“语音+图像”融合方案能准确识别乘员位置确定指令内容，实现多模语义理解、唇动检测、人声隔离等功能。最终实现更加负责、覆盖区域更加准确的交互功能，达成更加轻松、便捷、安全的人机交互体验。

2.3.2 产业普及现况

自 2011 年起，车载语音识别功能在国内的装车率逐年提升，现已成为多家车企新车型的“标准配置”。包括凯迪拉克、别克、福特、奇瑞、大众、上汽、蔚来、威马在内的国内外多个车型都搭载了语音

识别功能。汽标委正在制定推荐性国家标准《道路车辆 免提通话和语音交互性能要求及试验方法》，GB/T 36464.5-2018《信息技术 智能语音交互系统 第5部分：车载终端》也在推进修订中。标准的完善将进一步促进产品应用的规范化普及。

手势识别与视线识别则处于快速发展阶段，宝马、长城、长安、大众等多款车型已具备手势识别功能。2015年，宝马率先在车内新增基于3D TOF摄像头技术的手势控制功能，可识别6种预编程手势，包括手指顺时针滑动可提高音量、逆时针滑动则降低音量、指向中控台触摸屏中心可接听电话、手指滑向右侧拒绝接听电话等。

针对车外人员的智能交互功能也在逐渐发展，例如对交警的肢体行为和手势进行识别，但整体看，现阶段量产普及车型还较少。

2.3.3 技术原理

基于生物识别的智能交互，原理也是通过生物识别相关技术进行识别，并辅以语义分析等方法进行拓展和解析达到最终的交互目标。

（1）手势识别

手势识别，目前主要是采用摄像头视觉识别方案。通过兼容驾驶员监测摄像头、车舱监测摄像头或者额外布置的摄像头对驾驶员或者车舱内其他人员的手势进行识别。

汽车手势识别可分为简单手势和复杂手势两大类。简单手势识别仅能识别简单的上下左右或者挥动等二维手势；复杂手势识别可以通过3D摄像头和快速调制红外光源进行飞行时间测量，从而识别出包含有空间深度的三维手势。复杂手势识别能够支持车载手势识别系统

更多的动作，但同时在软件和硬件上的需求也比识别二维等简单手势要复杂的多，其中最难的地方便是如何将高精度的设备微小化，且不影响器件的发射功率、效率、感应灵敏度等。

从另一个角度，汽车手势识别还可以分为静态手势及动态手势。静态手势是指在发送指令的瞬间，手本身是静止的，智能算法只需要识别手部的静止姿态，就可以分别手势的类别。典型的算法一般包括：在图像帧中检测手部区域；对手部做跟踪并从原图中抠出手部图像或特征；分类网络预测静态手势置信度；后处理策略得到最终的手势指令。动态手势是指在发送指令的瞬间，手部除了姿态有特殊要求，手的运动也需要遵循事先预定好的规则。典型的算法流程一般包括：在连续图像帧中检测人手；对连续帧的人手做跟踪并抠出手部图像或特征；监测人手的运动状态（是否开始手势）；分类网络预测手势类别；后处理策略得到最终的手势指令。

（2）语音识别

语音交互所涉及的流程繁琐，涉及到从语言学到声学理论等多方面内容，同时在车端的使用需对特殊驾乘场景进行相应适配。结合大词汇量语音识别、自然语言理解、信息检索等技术提供特定领域内相对开放输入的语音识别服务，对用户的限制较为宽松，在所限定的领域内可以以自然语言的方式进行人机交互。

在语音交互在车端应用过程中，ASR（包含信号输入、特征提取以及音素选取等流程）、NLP（包含 NLU 与 NLG，涉及分词、文本向量化、文本分类、命名实体识别等处理）、TTS（包含文本预处理、

声学特征生成和声码器等，同时也是语音拟人化核心环节）成为三个关键环节。随着语音交互技术的成熟，语音识别准确率大幅提升，已为语音交互功能上车提供了技术验证与支持，因此智能 AI 科技企业开始纷纷加码语音交互在驾乘场景当中的应用与落地。

语音前端是音频信号处理的核心问题，也是车载语音识别和语义理解的重要预处理步骤。车内多声道扬声器的回声、路噪以及车内多人说话的相互干扰给车内语音采集带来极大挑战。基于麦克风阵列的语音前端，通过合理的定位、分离与提取，可以显著提升语音信号质量，是在车载环境下提升语音识别系统性能的有效手段。语音后端模块包括语音识别和自然语言处理两个模块。语音识别负责将输入的语音信号转化为文字信息，自然语言处理模块接收文字信息进行处理，并进一步分析其包含的意图信息。

（3）视线识别

学术界对视线的研究工作，已经持续了数十年时间，这期间学者们提出了大量的视线估计方法。通常来说，这些方法可以粗略的归类为 3 种：基于 3D 眼球模型的重建方法、基于 2D 眼睛特征的方法、基于人眼/脸外观特征的方法。由于人的眼睛结构的细节的多样性，每个人重建出来的各自的 3D 眼球模型是不一样的，因此，这种方法需要对每个人单独进行眼球参数的标定，例如虹膜半径，kappa 角（瞳孔中线与视轴的夹角）。眼球重建得到的视线预测值通常是比较准确的，但是这种方法往往依赖一些特定的设备，比如近红外摄像机等。基于 2D 眼睛特征的方法和 3D 重建的方法对额外设备的要求是相似

的，它直接使用检测到的眼部的几何特征，比如瞳孔中心，反光点来回归眼睛的注视点，它们也都不需要几何标定来将注视方向转换为注视点。

基于人脸/眼外观的方法不需要专用的设备，它通常使用现成的摄像头来获取人脸/眼图像，并从人脸/眼图像里来预测人眼视线。它的硬件设置比较简单，主要包含以下模块：

1)一个特征提取器，可以从图像里提取有效的视线特征。使用经典的图像处理方法，可以构建出这样的特征提取器。

2)一个回归器，用来学习特征到视线之间的映射。将高维的图像外观特征映射到低维的人眼视线。

3)大量的训练样本供回归函数学习，这些样本的搜集，通常会在个人标定上耗费大量的时间，然后针对每个人学习出特定于某个人的视线估计模型。当然，也有一些研究试图减少训练样本的数量，然而这同样会限制这类算法在实际应用中的使用场景。

近些年，随着深度学习技术在视觉领域的不断发展，基于深度学习的视线估计算法也逐步成为新的研究热点。和传统的视线算法相比，基于深度学习的方法的优势体现在以下方面：

1)可以从高维图像中提取更高级的视线特征。

2)更强大的拟合能力，对人脸/眼到视线的非线性映射拟合的更好。

这两点优势是基于深度学习的方法，比起传统的表观/特征学习方法更加可靠和准确。传统方法在头部运动时通常会出现较大的性能下降，而基于深度学习的方法，在一定程度上能够较好的处理头动情

况。同时，基于深度学习的方法还可以大幅提高在不同人的视线估计精度上的表现。这些改进，都很大程度上丰富了基于表观/特征的视线估计算法的应用场景。

（4）多模融合交互

多模语音算法需实现音视频的实时融合预测，需依赖 25fps 及以上帧率的视频，及实时的音频处理。

一个多模语音算法流程通常至少有两组输入：

一组是视频输入，摄像头数据需经过前置神经网络模块的实时处理，往往会首先需要在图像中进行人脸检测，在获得较为准确的人脸检测结果（人脸 ROI）之后，再运行人脸关键点检测算法。人脸关键点算法能够预测脸部的重要特征点的位置，如眼角，鼻尖，嘴角等。经验上，多模语音算法通常使用多个人脸关键点，其中有近 20 多个关键点用于描述唇部区域的定位特征点，使用数量较多的特征点能够在大角度侧脸的场景中，获得较好的唇部区域定位。在使用唇部关键点进行嘴部区域定位后，人脸区域会结合关键点相对标准脸的偏转角度进行仿射变换修正图像角度。唇部区域图像会结合时间戳被整理成视频数据，用于后续识别。

另一组是语音输入，在获取到原始信号及车机参考信号后，会通过语音前端模块进行降噪处理，再进行语音的特征提取，并获得实时流式的音频特征。

在视频数据和音频特征都准备好之后，多模语音算法会接收视频和语音数据进行联合预测。为了实现音视频同步，我们需要获取到准

确的音视频时间戳，通过时间戳实现语音和视频的严格对齐。由于音视频的帧率不一样，一个整数倍的帧率比例更容易让多模语音算法处理，一个通常使用的帧率是视频 25fps ，音频特征 100fps ，这样视频和音频能够以 1：4 的整数比例关系实现数据对齐。

一个成熟的多模语音系统会融合多个摄像头与多个麦克风的数据和结果，且在唇部遮挡或唇部质量不佳的条件下灵活切换单模语音和多模语音方案，将多模系统的性能优势发挥到极致的同时尽可能保障各个场景的基础性能。

2.3.4 测评指标及方法

（1）语音识别测试方法

语音识别测试可以分为单模语音测试和多模语音测试：

单模语音测试，主要通过人工嘴、音响声级计等工具配合语音测试素材、噪声搭建测试环境，根据人声声源调整音量和模拟车内噪声，通过不同语速及方言设置唤醒语料，确定唤醒率、唤醒音区准确率、识别率、人声隔离率、误识别率等参数。

多模语音测试方法参考单模测试，不同点主要在于多模语音需要算法回灌测试和真人实车测试。回灌测试是将测试数据直接送到算法模型，进行识别并输出识别结果，主要统计唤醒率、免唤醒命令词识别率、唤醒音区准确率、离线 ASR 识别率、识别音区准确率、多模人声隔离率、唇动检测准确率等参数。

（2）视觉识别测试方法

由于不同光线折射到人脸的阴影不同，不同年龄段人脸的纹理不

同，佩戴不同饰物、不同身高对人脸的遮挡，都会对算法识别结果产生一定影响，故将测试场景分为三个维度：光照、车控和模特。算法测试集分为三类：正样本测试集、自然驾驶测试集、专项负样本测试集。基于测试集和场景维度交叉完成测试，计算识别准确率和精确率。

2.3.5 痛点分析及应对

伴随语音交互等功能增加，如何保证降低驾驶员学习成本的同时正确响应车辆复杂功能控制成为人机交互急需解决的课题，频繁的误操作、误识别也会为驾驶安全性带来负面影响。多模交互是提升准确性和增加交互体验的解决方案之一，且不仅局限于单人多模输入，也可基于多人多模输入，将更有利于确定使用者真实意图。此外，语音识别涉及到语义关联和声源定位等技术。语义关联的痛点主要来自于某一个语义可以通过不同的表述方式或不同方言来表达，从而会导致部分语音识别失效。由于单个传感器无法定位声源，可能会因为接受到其他场景的语音导致误触发。该痛点不仅需要通过大量的数据训练来解决，还需要通过多种技术手段来补充融合。

另外，我国基于多模态 AI 芯片的语音控制解决方案供应商主要集中在互联网企业，虽然在概念上具有先进性，但在车规级、实用性、经济性上还有所欠缺。高优体验的智能交互需要多传感器交互并配合高算力芯片支持，也难免将带来车辆成本的提升。

建立相关智能交互场景的标准测试方法，有效拓展软硬件技术，不断提升各个场景下的应用效果，才是根本解决痛点的有效途径。

3 生物识别信息安全风险分析及应对

3.1 典型漏洞事件

（1）美国联邦政府系统指纹漏洞事件

在 2015 年，美国联邦政府人事管理办公室保存的 560 万个员工的指纹数据被黑客盗走。当时，所有的员工指纹数据都是存储在系统服务器数据库中，因此，黑客只要攻破服务器访问到数据库，就能够获取所有指纹数据。

（2）三星 Galaxy S10 手机屏下指纹漏洞事件

2019 年 10 月，根据《太阳报》消息，一对英国夫妇发现三星 S10 存在指纹识别漏洞，这部 S10 是男主送给女主的礼物，并第一时间给新机套上了网购的第三方「全包硅胶套」。然后女主回家录入指纹后，却发现男主也可以解锁手机甚至登陆银行 App。

首先这个「全包硅胶套」，是把手机正面和背面都用硅胶材质包裹起来，所以相当于在屏幕上增加了一层较厚的「硅胶膜」。

根据男主描述的时间线，女主应该是“戴手套”录入指纹，也就是说在录入过程中女主指纹与硅胶套纹路存在重叠的情况。

由此推断，当男主再进行指纹识别时，也会与硅胶套纹路有重叠，所以这可能是漏洞出现的原因，导致任何人都可以解锁手机。

（3）生物科技公司 Suprema 面部及指纹信息泄漏事件

2019 年 8 月，vpnMentor 的研究人员发现属于生物科技公司 Suprema 的一个数据库暴露在公网上，其中包含 100 多万人的生物识别数据，涉及英国大都会警察局、当地小型企业和各大政府机构收集

的面部和指纹识别信息。

Suprema 曾大力推销一款名为 BioStar 2 的生物识别软件，识别方式主要为面部识别和指纹识别，可帮助公司组织管理人员对特殊设施的访问。现 BioStar 2 已被近 6000 个组织采用，包括跨国公司、政府、银行和英国大都会警察局。

3.2 安全风险评估

基于对当前涉及生物识别信息车载应用的业务梳理，抽象概括形成三种业务场景，并利用 STRIDE 威胁建模的方式，对场景进行信息安全风险评估。

（1）生物识别信息以原始数据方式传输到云端进行识别验证

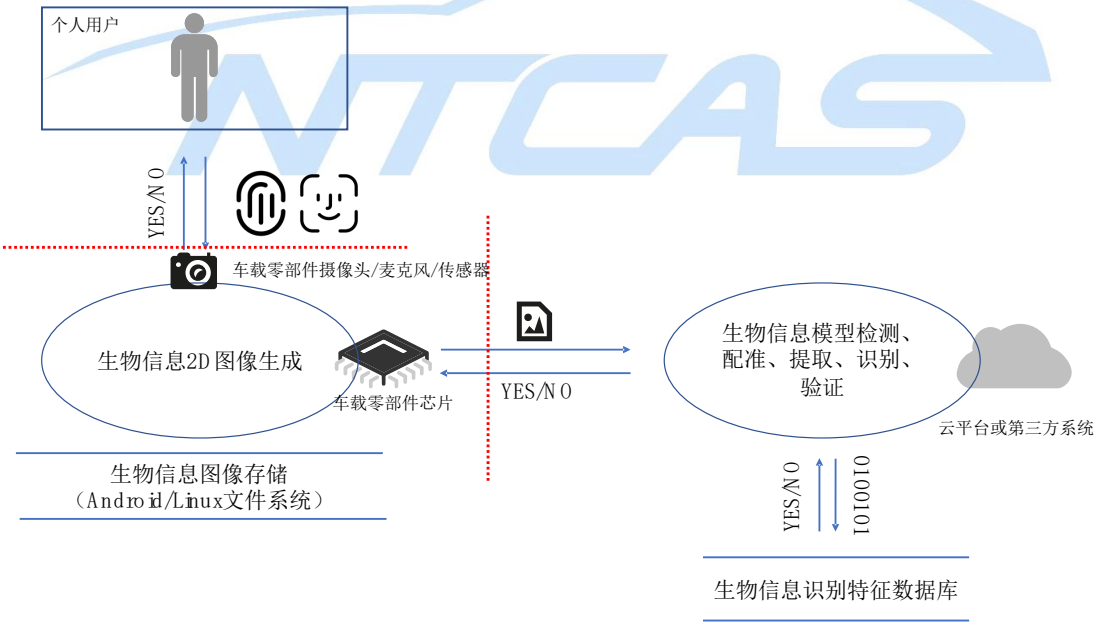


图 5　生物识别信息以原始数据方式传输到云端进行识别验证场景

场景说明：在本场景中，由于终端设备芯片算力、专利保护等问题，导致人脸、声纹等生物识别过程无法在终端完成，需要将生物识

别信息如图像文件或音频文件传输至云端或第三方后台系统进行识别验证。

表 3　场景一 STRIDE 分析

资产	威胁	风险
车载零部件芯片、云端系统、通信网络	Spooling 仿冒	恶意人员通过照片、头模、指纹贴膜、录音等方式仿冒用户的生物识别信息访问系统
	Tampering 篡改	恶意人员通过篡改云端返回给车端的验证结果，可能获得车端系统的访问权限
	Repudiation 抵赖	恶意人员通过篡改车端及云端系统的日志信息，实现对恶意行为的隐藏或抵赖
	Information Disclosure 信息泄露	由于车端或云端存储的信息泄露（如图像或音频原始数据，以及数据库的验证信息等），可能导致恶意人员获取用户的生物识别信息，从而实现对系统的非法访问，且这些用于登录的生物识别信息是无法更改的
	DoS 拒绝服务	由于系统对生物识别的验证次数有限制，或芯片算力及网络带宽的资源限制，可能导致恶意人员利用这些潜在漏洞发起拒绝服务攻击，从而使正常用户无法登陆和访问系统
	Elevation of privilege 提权	由于车端或云端系统的权限设置不当，可能导致恶意人员利用普通用户权限，访问到敏感数据，或非授权访问其他用户的数据（如临时用户访问车端存储的车主信息等）

（2）生物识别信息在本地进行提取后传输到云端进行识别验证

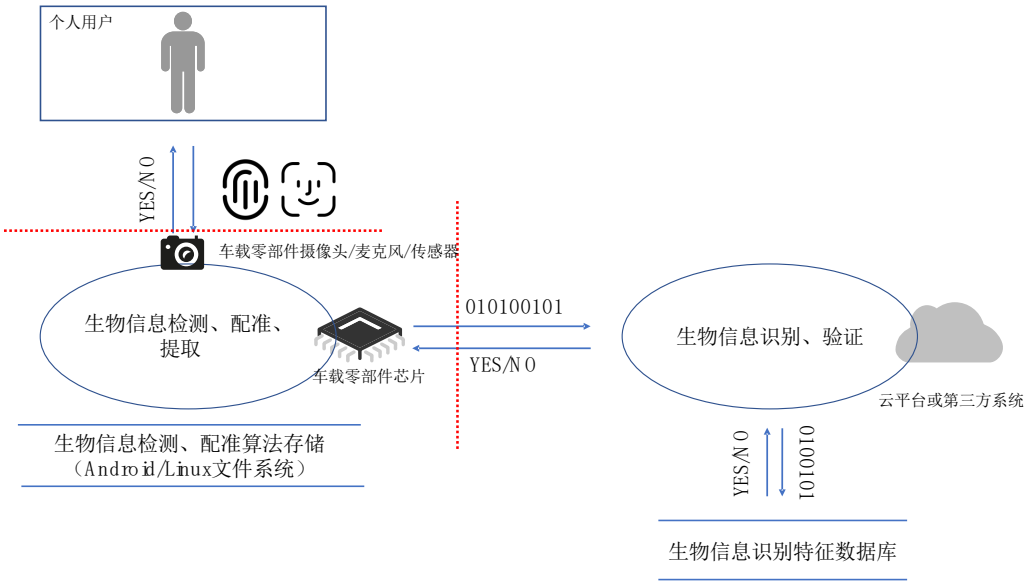


图 6　生物识别信息在本地进行提取后传输到云端进行识别验证场景

场景说明：在本场景中，由于终端设备芯片无法存储大量用户的验证数据，因此终端设备在对生物识别信息完成检测、配准和提取后，需要将提取出的相关数据传输至云端或第三方后台系统进行识别验证，在与云端的数据库进行比对识别后，返回验证结果给终端设备。

表 4　场景二 STRIDE 分析

资产	威胁	风险
车载零部件芯片、云端系统、通信网络	Spooling 仿冒	恶意人员通过照片、头模、指纹贴膜、录音等方式仿冒用户的生物识别信息访问系统
	Tampering 篡改	恶意人员通过篡改云端返回给车端的验证结果，可能获得车端系统的访问权限
	Repudiation 抵赖	恶意人员通过篡改车端及云端系统的日志信息，实现对恶意行为的隐藏或抵赖
	Information Disclosure 信息泄露	由于车端或云端存储的信息泄露（如车端存储的生物识别信息的提取数据，以及后台数据库的验证信息等），可能导致恶意人员获取用户的生物识别信息，从而实现对系统的非法访问，且这些用于登录的生物识别信息是无法更改的
	DoS 拒绝服务	由于系统对生物识别的验证次数有限制，或芯片算力及网络带宽的资源限制，可能导致恶意人员利用这些潜在漏洞发起拒绝服务攻击，从而使正常用户无法登陆和访问系统
	Elevation of privilege 提权	由于车端或云端系统的权限设置不当，可能导致恶意人员利用普通用户权限，访问到敏感数据，或非授权访问其他用户的数据（如临时用户访问车端存储的车主信息等）

（3）生物识别信息在本地完成识别验证

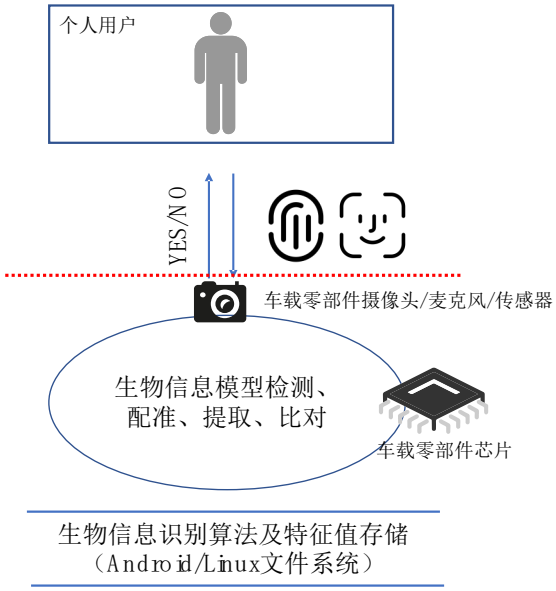


图 7　生物识别信息在本地完成识别验证场景

场景说明：

在本场景中，终端设备芯片完成全部生物识别信息的检测、配准、提取和比对过程，并返回比对结果给用户和其他系统。

表 5　场景三 STRIDE 分析

资产	威胁	风险
车载零部件芯片、云端系统、通信网络	Spooling 仿冒	恶意人员通过照片、头模、指纹贴膜、录音等方式仿冒用户的生物识别信息访问系统
	Tampering 篡改	恶意人员通过篡改生物识别系统 APP 给其他 APP 的比对结果，可能获得车端系统的访问权限（如在 Android 中劫持篡改进程间通信）
	Repudiation 抵赖	恶意人员通过篡改车端及云端系统的日志信息，实现对恶意行为的隐藏或抵赖
	Information Disclosure 信息泄露	由于车端存储的信息泄露（如车端存储的图像识别模型），可能导致恶意人员利用获取到的识别模型生成恶意的对抗样本，从而实现对车端系统的攻击或非授权访问
	DoS 拒绝服务	由于系统对生物识别的验证次数有限制，或芯片算力的资源限制，可能导致恶意人员利用这些潜在漏洞发起拒绝服务攻击，从而使正常用户无法登陆和访问系统
	Elevation of privilege 提权	由于车端系统的权限设置不当，可能导致恶意人员利用普通用户权限，访问到敏感数据，或非授

		权访问其他用户的数据（如临时用户访问车端存储的车主信息等）

综合上述三种场景的威胁建模分析结果，智能网联汽车生物识别信息的安全风险可以概括为：

(a) 利用伪造的生物识别信息，仿冒正常用户登录系统；

(b) 利用网络通信或进程间通信的漏洞，篡改验证结果；

(c) 删除或篡改日志信息，从而隐藏或抵赖恶意行为；

(d) 利用车端漏洞（如对芯片存储设备的数据提取分析）和云端漏洞（如远程执行漏洞或管理及人员漏洞）获取用户的生物识别信息或深度学习模型，进而实现对生物识别系统的精准欺骗，或根据截获的提取数据逆向还原出原始生物识别信息；

(e) 利用系统登录次数或计算和网络带宽资源限制，实现对生物识别系统的拒绝服务攻击；

(f) 利用系统权限配置漏洞，越权访问其他用户信息或敏感数据。

3.3 技术应对现况

在对生物识别数据合规应用前提下，企业还需要根据相关要求对生物识别数据进行高级别的安全防护。例如，将生物识别数据只保存在用户本人的终端设备上，而不是集中保存到企业的服务器上；将一个或多个生物识别数据保存到个人终端芯片的可信执行环境中；通过芯片硬件的安全机制保护数据安全性。

针对前面通过 STRIDE 威胁建模识别出的安全风险，企业应采取相应的技术手段规避或降低相关风险，例如可采取如下方式：

表 6　生物识别信息风险应对方案

风险	应对方案
利用伪造的生物识别信息，仿冒正常用户登录系统	1）通过可信执行环境或加密芯片对生物识别模型进行保护加固，防止被逆向分析或调试； 2）活体检测； 3）3D 结构光
利用网络通信或进程间通信的漏洞，篡改验证结果	1）识别验证前，建立车端与云端的双向可信连接，确保车端运行环境的安全可信； 2）对验证结果进行数字签名，防止其被篡改； 3）车端内部系统利用可信执行环境或加密芯片保护关键业务逻辑的运行，并通过安全可信的 API 确保进程间通信的安全； 4）高安全级别业务可在 Android/Linux 与可信执行环境操作系统之间使用非对称密钥的数字签名，确保关键数据不被篡改
删除或篡改日志信息，从而隐藏或抵赖恶意行为	1）利用可信执行环境隔离并加密存储日志信息，并对日志进行数字签名保护； 2）使用特定专用逻辑生成日志，并只能使用专用软件方可对日志进行正确读取
利用车端漏洞（如对芯片存储设备的数据提取分析）和云端漏洞（如远程执行漏洞或管理及人员漏洞）获取用户的生物识别信息或深度学习模型，进而实现对生物识别系统的精准欺骗，或根据截获的提取数据逆向还原出原始生物识别信息	1）车端利用可信执行环境或安全芯片保护生物识别模型，防止攻击者利用物理方式对其进行提取和逆向分析； 2）云端使用“零信任”架构，并严格遵循 ISO 27001 等标准，防止攻击者利用云端漏洞或社会工程学渗透至后台系统； 3）利用隐私计算技术实现“数据可用不可见”
利用系统登录次数或计算和网络带宽资源限制，实现对生物识别系统的拒绝服务攻击	1）使用细粒度的访问控制策略，精准的对重复使用同一套生物识别信息特征的访问进行登录次数限制； 2）使用 QoS（服务质量保证）或 Dedup（重复数据删除）技术确保识别信息的及时传输
利用系统的权限配置漏洞，越权访问其他用户信息或敏感数据	1）使用细粒度的访问控制，给不同应用程序分配不同的访问权限，并从存储计算资源、文件系统等层面进行隔离； 2）使用微内核技术，防止攻击者利用内核漏洞获得 root 权限； 3）使用形式化验证技术，确保微内核代码的安全性和可靠性

综合上述应对方案，可归纳一套结合车辆网络安全架构及隐私计

算技术的整体解决方案，通过车辆网络安全架构确保车端系统不被渗透攻击，同时又通过隐私计算技术确保在生物识别信息不出车的情况下，仍能满足模型优化及大数据分析等业务需求。

车辆网络安全架构整体上可分为车云协同机制和车端安全防护两部分，其中车云协同机制以车云可信验证及零信任等云安全技术构成，而车端安全防护则以车载芯片的可信执行环境及其安全操作系统为信任根基构建起一套从硬件层到内核层，直至应用层的可信安全体系。其中车载芯片的可信执行环境不仅可以成为车辆网络安全架构的可信根基，同时还作为隐私计算技术中机密计算的最佳实践方案，为保护生物识别信息以及深度学习模型等关键数据提供可信赖的技术支撑。

隐私计算技术包含了多个具体的技术路线，其在汽车行业应用的目的，是为了在车联网大数据分析及车辆状态监控等业务开展过程中，确保生物识别信息等个人敏感信息的安全性，同时又可以满足数据分析需求，保证分析结果的真实性及一致性。隐私计算技术大体上可分为基于密码学的算法技术（如多方安全计算、联邦学习、同态加密等），以及针对算法和计算过程安全性的安全防护技术（如机密计算、区块链等）两类。在实践中汽车企业应结合实际应用场景和数据类型选择恰当的技术方案落地，附录 C 列举了一套基于机密计算和联邦学习技术的隐私计算方案，便于汽车企业参考理解。

4 法律法规分析

4.1 国内法律法规现况

近年来，我国相继出台了相关政策文件，支持并规范生物特征识别产业的发展。

2016 年 3 月，十二届全国人大四次会议审查通过了《中华人民共和国国民经济和社会发展第十三个五年规划纲要》，其中明确指出支持新一代信息技术、生物技术等领域的产业发展壮大，重点突破人工智能技术，加快信息网络新技术开发应用。该规划的出台为生物特征识别技术和产业未来 5 年的发展规定了目标和方向。

2016 年 5 月，国家发展和改革委员会印发的《“互联网+”人工智能三年行动实施方案》（发改高技〔2016〕1078 号）连续三次提到“生物特征识别”：一是要进一步推进生物特征识别等关键技术的研发和产业化，为产业智能化升级夯实基础。二是建设满足多种生物特征识别的基础身份认证平台等基础资源服务平台，降低人工智能创新成本。三是鼓励安防企业与互联网企业开展合作，研发生物特征识别等多种技术的智能安防产品，推动安防产品的智能化、集约化、网络化。

2017 年 7 月，国务院发布的《新一代人工智能发展规划》（国发〔2017〕35 号）中指出经过多年的持续积累，我国的生物特征识别进入实际应用，一批龙头骨干企业加速成长，在国际上获得广泛关注和认可。同时，围绕社会综合治理、新型犯罪侦查、反恐等迫切需求，提出研发生物特征识别技术的智能安防与警用产品，建立智能化

监测平台的要求。

2017 年 12 月，工业和信息化部发布的《促进新一代人工智能产业发展三年行动计划（2018-2020 年）》（工信部科〔2017〕315 号）中明确表态，支持生物特征识别等技术创新，发展人证合一、视频监控、图像搜索、视频摘要等典型应用，拓展在安防、金融等重点领域的应用。到 2020 年，实现复杂动态场景下人脸识别有效检出率超过 97%，正确识别率超过 90%，支持不同地域人脸特征识别的目标。

2021 年 3 月，第十三届全国人民代表大会第四次会议通过《中华人民共和国国民经济和社会发展第十四个五年规划纲要》，其中明确提出加快壮大新一代信息技术、生物技术等产业，推动互联网、大数据、人工智能等同个产业深度融合，培育新技术、新产品、新业态、新模式。该规划出台为生物特征识别技术和产业未来 5 年的发展确定了目标和方向。

在数据安全层面，近年来，国家陆续出台多部法律法规，其强化个人信息、重要数据、汽车领域数据采集、处理等要求。

2016 年 11 月全国人大通过的《中华人民共和国网络安全法》明确个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

2021 年 6 月，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，明确数据活动的红线，在“数据主权、数据经营、数据交易”等方面，通过法律条文形式，

坚持保障数据安全与发展并重，鼓励研发数据安全保护技术，积极推进数据资源开发利用，推动数据时代的快速发展。

2021 年 8 月，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息，并规定了个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

2021 年 8 月，国家互联网信息办公室审议通过《汽车数据安全管理若干规定（试行）》，并经国家发展和改革委员会、工业和信息化部、公安部、交通运输部同意，予以发布，自 2021 年 10 月 1 日起施行。其中，将生物识别特征信息明确定义为敏感个人信息，并进一步规定汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

4.2 国外法律法规现况

4.2.1 美国

美国提出联邦层面的《国家生物识别信息隐私法案》，为企业生物识别数据使用树立规范；伊利诺伊州、德克萨斯州、华盛顿州、加利福尼亚州分别制定了专门处理保护消费者生物识别信息的法律；其他州选择将生物识别数据作为受消费者隐私或数据泄露通知法规保护的一类个人信息。

（1）2008 年，伊利诺伊州成为美国第一个通过立法的州，即生物识别信息隐私法案 (BIPA)，规范生物识别信息的收集和存储。该

法规将“生物识别标识符”的定义限制为“视网膜或虹膜扫描、指纹、声纹或手或面部几何扫描”。该法规进一步将“生物识别信息”定义为“任何信息，无论它是如何捕获、转换、存储或共享的，用于识别个人身份的生物特征”。

（2）2009 年，德克萨斯州制定了法律，要求在获取生物识别标识符并将其用于商业目的前，必须通知个人收集和同意。

（3）2017 年，华盛顿州通过了其生物识别隐私法规。它要求企业在“在数据库中注册或更改该个人生物识别标识符的使用之前须通知并获得该个人的同意”。华盛顿州法规中“生物识别”的定义比伊利诺伊州和德克萨斯州法规中使用的更广泛。华盛顿的法规将生物识别标识符定义为包括“通过自动测量个人生物特征生成的数据，例如指纹、声纹、眼睛视网膜、虹膜或其他用于识别特定个人的独特生物模式或特征”。

（4）2018 年 6 月 28 日，加利福尼亚州颁布《消费者隐私法》（California Consumer Privacy Act），该法保护加利福尼亚州居民收集或传输的个人信息，广义上包括生物识别信息。

（5）2021 年 7 月 9 日，纽约市《生物识别信息隐私法案》（Biometric Privacy Act）正式生效，对数据安全、知情告知及私人诉权等做出了较为详实的规定。该法案要求私人实体收集生物识别数据之前必须发布和张贴正式通知，并明确禁止私人实体将这些数据用于交易牟利目的。同时，该法还设立了一项私人诉讼权，使受害方能够要求终止侵害行为并获得赔偿。该法案 2018 年在纽约市议会提出，

经过多轮讨论，于2021年1月颁布，7月正式生效。法案主要聚焦于通过规范非公机构对生物识别数据的采集、储存、传输和使用，来确保其准确、安全和保护个人隐私。与已有法规相比，纽约市的《生物识别信息隐私法案》的主要特点在于：第一、法案规制的对象仅限于“私人实体”，包括个人、企业、商业机构等，并不适用于立法机构、政府、法院等公共部门；第二、对需要保护的生物识别信息界定较全面。该法案中的“生物标识”将视网膜或虹膜扫描、指纹、声纹、手部或脸部几何结构的扫描图像等都包括在内。“生物特征信息”则是指基于生物标识符而收集、转换、存储或共享的任何信息；第三、重视信息披露和告知。法案规定，收集、保留或使用客户生物识别信息的商业机构必须发布正式通知披露相关活动，确保客户充分知情；第四、法案禁止私人实体通过出售、租赁、交易或者其他方式从生物识别信息中获利；第五、法案专门规定了一项私人诉讼权，以保障信息主体的权利。个人可以对商业机构的不合规行为提起索赔，同时，如果商业机构不依照法规解决问题，个人也可以提起诉讼。企业的每次违规行为都将受到500至5000美元不等的法定处罚。

该法案严格程度属于比较适中，原则上并不禁止私营主体运用生物识别技术对公共主体则未加以具体规定，主旨还是希望能在保障公民隐私及自由与发挥人脸识别技术的公共服务优势方面寻求平衡。相较于欧盟“全面禁止”的倾向，美国的态度可能更趋于平衡和务实。

纽约市在生物识别信息保护方面的立法实践或可为类似的超大城市在规范数据权属关系及用户知情同意方式、个人信息收集、传输、

存储等数据管理规范、研究制定个人信息分级分类标准等方面建立健全相关法规体系提供参考，防止生物识别数据被滥采滥用。

4.2.2 欧盟

2018 年 5 月 25 日开始施行的欧盟《通用数据保护条例》（General Data Protection Regulation）第 4 条第 1 款将个人数据定义为 “任何指向一个已识别或可识别的自然人（‘数据主体’）的信息。” 第 4 条第 1 款定义“生物识别数据”为“通过对自然人的物理、生物或行为特征进行特定的技术处理而得到的个人数据。这类数据生成了自然人的唯一标识，比如人脸图像或指纹识别数据。

欧盟理事会提议的《人工智能法案》将使代表执法当局的人能够操作生物识别监控系统。该提案还扩展了系统的使用目的，包括防止对“关键基础设施”或个人“生命、健康或人身安全”的威胁。

2021 年 6 月，欧盟数据保护委员会（EDPB）和欧盟数据保护监督局（EDPS）发表联合意见，呼吁全面禁止在公共场所使用人工智能自动识别人脸、步态、指纹、DNA、声音和其他生物识别信号。

4.2.3 其他国家

阿联酋和新西兰分别出台《数据保护法》和《2020 年隐私法》，加强了对数据安全及个人隐私保护的规制建设；日本和新加坡分别完成了对本国《个人信息（数据）保护法》的修订，明确了个人数据权利及外部使用限制；加拿大出台的《数字宪章实施法案 2020》，提出了保护私营部门个人信息的现代化框架；印度《2018 个人数据保护法案（草案）》及巴西《通用数据保护法》都将生物信息纳入敏感个

人信息进行保护。

4.3 小结

随着新技术新应用的快速发展，以人脸识别为代表的人工智能技术得到了大规模应用。然而，生物识别数据披露的个人特征精确，且采集门槛较低、极易获取，一旦遭到泄露、篡改或非法共享，极易带来“身份盗窃”风险，且正在成为攻击者的主要目标。对此，各国政府纷纷出台相关法律法规，以规范生物识别数据的使用。

随着监管体系的日益完善，企业如何有效地做好合规应对，本文件尝试给出当前共识，仅供行业参考。

企业首先应建立一套包含顶层设计、组织架构、制度流程等内容的隐私保护体系，如参照 ISO 27701。进而在产品和服务设计开发过程中遵从法规标准中的相关内容，如《个人信息保护法》中的规定：“汽车数据处理者应当履行个人信息保护责任，充分保护个人信息安全和合法权益。开展个人信息处理活动，汽车数据处理者应当通过显著方式告知个人相关信息，取得个人同意或者符合法律、行政法规规定的其他情形。处理敏感个人信息，汽车数据处理者还应当取得个人单独同意，满足限定处理目的、提示收集状态、终止收集等具体要求或者符合法律、行政法规和强制性国家标准等其他要求。汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。”

5 标准化分析

5.1 国内标准体系分析

截止目前，国内围绕生物识别基础通用研究，已发布国家标准 50 余项、在研国家标准 40 余项。

表 7 国内生物识别基础通用标准列表（已发布）

标准号	标准名称	发布日期	实施日期
GB/T 16649.11-2019	识别卡 集成电路卡 第 11 部分：通过生物特征识别方法的身份验证	2019/8/30	2020/3/1
GB/T 26237.1-2010	信息技术 生物特征识别数据交换格式 第 1 部分：框架	2011/1/14	2011/5/1
GB/T 26237.2-2011	信息技术 生物特征识别数据交换格式 第 2 部分：指纹细节点数据	2011/12/30	2012/6/1
GB/T 26237.3-2011	信息技术 生物特征识别数据交换格式 第 3 部分：指纹型谱数据	2011/12/30	2012/6/1
GB/T 26237.4-2014	信息技术 生物特征识别数据交换格式 第 4 部分：指纹图像数据	2014/12/5	2015/5/1
GB/T 26237.5-2014	信息技术 生物特征识别数据交换格式 第 5 部分：人脸图像数据	2014/12/5	2015/5/1
GB/T 26237.6-2014	信息技术 生物特征识别数据交换格式 第 6 部分：虹膜图像数据	2014/12/5	2015/5/1
GB/T 26237.7-2013	信息技术 生物特征识别数据交换格式 第 7 部分：签名/签字时间序列数据	2013/12/31	2014/7/15
GB/T 26237.8-2014	信息技术 生物特征识别数据交换格式 第 8 部分：指纹型骨架数据	2014/9/3	2015/2/1
GB/T 26237.9-2014	信息技术 生物特征识别数据交换格式 第 9 部分：血管图像数据	2014/7/8	2014/12/1
GB/T 26237.10-2014	信息技术 生物特征识别数据交换格式 第 10 部分：手型轮廓数据	2014/7/8	2014/12/1
GB/T 26237.14-2019	信息技术 生物特征识别数据交换格式 第 14 部分：DNA 数据	2019/8/30	2020/3/1
GB/T 26238-2010	信息技术 生物特征识别术语	2011/1/14	2011/5/1
GB/T 28826.1-2012	信息技术 公用生物特征识别交换格式框架 第 1 部分：数据元素规范	2012/11/5	2013/2/1
GB/T	信息技术 公用生物特征识别交换格式框架	2020/4/28	2020/11/1

标准号	标准名称	发布日期	实施日期
28826.2-2020	第 2 部分：生物特征识别注册机构操作规程		
GB/T 29268.1-2012	信息技术 生物特征识别性能测试和报告 第 1 部分：原则与框架	2012/12/31	2013/6/1
GB/T 29268.2-2012	信息技术 生物特征识别性能测试和报告 第 2 部分：技术与场景评价的测试方法	2012/12/31	2013/6/1
GB/T 29268.3-2012	信息技术 生物特征识别性能测试和报告 第 3 部分：模态特定性测试	2012/12/31	2013/6/1
GB/T 29268.4-2012	信息技术 生物特征识别性能测试和报告 第 4 部分：互操作性性能测试	2012/12/31	2013/6/1
GB/T 30266-2013	信息技术 识别卡 卡内生物特征比对	2013/12/31	2014/7/15
GB/T 30267.1-2013	信息技术 生物特征识别应用程序接口 第 1 部分：BioAPI 规范	2013/12/31	2014/7/15
GB/T 30268.1-2013	信息技术 生物特征识别应用程序接口（BioAPI）的符合性测试 第 1 部分：方法和规程	2013/12/31	2014/7/15
GB/T 30268.2-2013	信息技术 生物特征识别应用程序接口（BioAPI）的符合性测试 第 2 部分：生物特征识别服务供方的测试断言	2013/12/31	2014/7/15
GB/T 32629-2016	信息技术 生物特征识别应用程序接口的互通协议	2016/4/25	2016/11/1
GB/T 32903-2016	信息技术 指静脉识别系统 指静脉图像数据格式	2016/8/29	2017/3/1
GB/T 33135-2016	信息技术 指静脉识别系统 指静脉采集设备通用规范	2016/10/13	2017/5/1
GB/T 33767.1-2017	信息技术 生物特征样本质量 第 1 部分：框架	2017/5/31	2017/12/1
GB/T 33767.4-2018	信息技术 生物特征样本质量 第 4 部分：指纹图像数据	2018/3/15	2018/10/1
GB/T 33767.5-2018	信息技术 生物特征样本质量 第 5 部分：人脸图像数据	2018/6/7	2019/1/1
GB/T 33767.6-2018	信息技术 生物特征样本质量 第 6 部分：虹膜图像数据	2018/6/7	2019/1/1
GB/T 33842.2-2017	信息技术 GB/T 26237 中定义的生物特征数据交换格式的符合性测试方法 第 2 部分：指纹细节点数据	2017/5/31	2017/12/1
GB/T 33842.4-2017	信息技术 GB/T 26237 中定义的生物特征数据交换格式的符合性测试方法 第 4 部分：指纹图像数据	2017/5/31	2017/12/1
GB/T	信息技术 GB/T 26237 中定义的生物特征	2018/3/15	2018/10/1

标准号	标准名称	发布日期	实施日期
33842.5-2018	数据交换格式的符合性测试方法 第 5 部分：人脸图像数据		
GB/T 33844-2017	信息技术 生物特征识别 用于生物特征十指指纹采集应用编程接口（BioAPI）	2017/5/31	2017/12/1
GB/T 34083-2017	中文语音识别互联网服务接口规范	2017/7/31	2018/2/1
GB/T 35783-2017	信息技术 虹膜识别设备通用规范	2017/12/29	2018/7/1
GB/T 35312-2017	中文语音识别终端服务接口规范	2017/12/29	2018/7/1
GB/T 36094-2018	信息技术 生物特征识别 嵌入式 BioAPI	2018/3/15	2018/10/1
GB/T 36460-2018	信息技术 生物特征识别 多模态及其他多生物特征融合	2018/6/7	2019/1/1
GB/T 37036.1-2018	信息技术 移动设备生物特征识别 第 1 部分：通用要求	2018/12/28	2019/7/1
GB/T 37036.2-2019	信息技术 移动设备生物特征识别 第 2 部分：指纹	2019/10/18	2020/5/1
GB/T 37036.3-2019	信息技术 移动设备生物特征识别 第 3 部分:人脸	2019/10/18	2020/5/1
GB/T 37036.4-2021	信息技术 移动设备生物特征识别 第 4 部分：虹膜	2021/4/30	2021/11/1
GB/T 37045-2018	信息技术 生物特征识别 指纹处理芯片技术要求	2018/12/28	2019/4/1
GB/T 37742-2019	信息技术 生物特征识别 指纹识别设备通用规范	2019/8/30	2020/3/1
GB/T 37743-2019	信息技术 智能设备操作系统身份识别服务接口	2019/8/30	2020/3/1
GB/T 38851-2020	信息技术 识别卡 集成指纹的身份识别卡通用技术要求	2020/7/21	2021/2/1
GB/T 40694.1-2021	信息技术 用于生物特征识别系统的图示、图标和符号 第 1 部分：总则	2021/10/11	2022/5/1
GB/T 40784.1-2021	信息技术 用于互操作和数据交换的生物特征识别轮廓 第 1 部分：生物特征识别系统概述和生物特征识别轮廓	2021/10/11	2022/5/1
GB/T 5271.37-2021	信息技术 词汇 第 37 部分：生物特征识别	2021/10/11	2022/5/1
SJ/T 11380-2008	自动声纹识别（说话人识别）技术规范	2008/3/10	2008/3/10

国内围绕生物识别信息安全领域研究，已发布国家标准 7 项、在

研国家标准 4 项。

表 8　国内生物识别信息安全标准列表（已发布）

标准号	标准名称	发布日期	实施日期
GB/T 35273-2020	信息安全技术 个人信息安全规范	2020/3/6	2020/10/1
GB/T 40660-2021	信息安全技术 生物特征识别信息保护基本要求	2021/10/11	2022/5/1
GB/T 38671-2020	信息安全技术 远程人脸识别系统技术要求	2020/4/28	2020/11/1
GB/T 38542-2020	信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架	2020/3/6	2020/10/1
GB/T 20979-2019	信息安全技术 虹膜识别系统技术要求	2019/8/30	2020/3/1
GB/T 37076-2018	信息安全技术 指纹识别系统技术要求	2018/12/28	2019/7/1
GB/T 36651-2018	信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架	2018/10/10	2019/5/1

将国内所发布生物识别相关标准进行分析，大概可区分为 8 类：基础通用、产品通用规范、应用编程接口、数据交换格式、样品质量、测试方法、行业应用和安全与加密。

5.1.1　基础通用

基础通用标准，主要对生物识别的基本词汇、术语及其定义、数据采集主体之间的交互以及生物特征识别系统的图示、图标和符号等方面进行相关的描述与界定。

GB/T 26238-2010 规定了与人的识别相关的生物特征识别领域的常用术语及其定义，不包括形态特殊术语，从而规范本领域术语的使用。

GB/T 40694.1-2021 规定了与生物特征识别注册、验证和/或辨识设备相关的一系列图标和符号。

GB/T 40784.1-2021 规定了通用生物特征识别系统的功能模块和组件，明确各组件的显著特征。同时结合生物特征识别相关的基础标准规定了通用的生物特征识别参考体系架构，支撑生物特征识别系统间的互操作性和数据交换。

GB/T 5271.37-2021 系统地描述了生物特征识别领域与人类的识别相关的概念，并协调现存的生物特征识别标准中使用的各种术语与优先术语，从而使此领域中术语的使用明晰化。

5.1.2 产品通用规范

产品通用规范标准，主要针对指静脉识别系统、虹膜识别设备、集成指纹的身份识别卡等通用类产品进行规范与界定。

GB/T 33135-2016 规定了指静脉识别系统中指静脉采集设备的技术要求、试验方法、质量评定程序、标志、包装、运输和贮存等。本标准适用于指静脉识别系统中指静脉采集设备的研制、生产和检验等。

GB/T 35783-2017 规定了虹膜识别设备的要求、试验方法、质量评定程序，以及标志、包装、运输和贮存。本标准适用于虹膜识别设备的研造、生产和检验等。

GB/T 36460-2018 规定了多模态及其他多生物特征融合方法。适用于生物特征融合，包括多生物特征识别特征类型、多实例、多传感器、多算法、决策级和分数级逻辑。

GB/T 37045-2018 规定了指纹处理芯片的组成、功能要求、处理流程和安全要求。适用于指纹处理芯片的设计、生产集成与应用，指

纹识别相关产品也可参考。

GB/T 37742-2019 规定了生物特征识别应用中指纹识别设备的要求、试验方法、质量评定程序、标志、包装、运输和贮存。适用于生物特征识别应用中指纹识别设备的研制、生产和检验等。

GB/T 38851-2020 规定了集成指纹的身份识别卡的基本组成、外观与结构、机械适应性、环境适应性、电特性与传输协议、通用流程与基本功能性能、命令、信息安全等要求。适用于指纹身份识别卡的研发、生产、检验和使用。

SJ/T 11380-2008 规定了声纹识别（说话人识别）的术语与定义、数据交换格式及应用编程接口，适用于各种计算机、网络和智能设备的声纹识别系统。该标准是我国第一个关于声纹识别（说话人识别）的标准，其颁布将很好地推动和规范我国的声纹识别产业的发展。

5.1.3 应用编程接口

应用编程接口标准，主要针对生物特征识别应用程序接口、生物特征识别应用程序接口的互通协议、指纹采集应用编程接口、中文语音识别互联网服务接口规范、中文语音识别终端服务接口规范等接口方面进行规范与界定。

GB/T 30267.1-2013 对生物特征识别系统内的标准接口定义了应用程序接口(API)和服务提供方接口(SPI)。生物特征识别系统支持来自多个供方的组件，并通过遵守本部分和其他国家标准，提供了组件之间的交互。

GB/T 32629-2016 规定了 BIP 消息的句法、语义和编码及 BioAPI 框架的架构和行为的扩展，以支持创建、处理、发送和接收 BIP 消息。

GB/T 33844-2017 规定了 BioAPI 应用如何与 BioAPI 框架相互作用以支持十指指纹采集（所有 10 个手指指纹的采集）。它规定并支持对大范围的身份认证管理和证书系统（该系统往往要求将十指指纹采集作为身份审核和背景检查过程的一部分）的部署。

GB/T 34083-2017 规定了中文语音识别服务系统在互联网环境下提供服务的能力范围、输入数据、输出数据、服务接口、接口返回值要求等。适用于基于互联网的中文语音识别服务系统接口的设计、开发和应用。

GB/T 35312-2017 规定了在终端设备（如移动电话、平板电脑无线音箱、车载导航仪等）上的中文语音识别系统所提供服务的功能集合包括服务系统能力范围输入/输出数据描述和服务接口的基本要求。适用于终端设备上的中文语音识别系统的设计和开发。

GB/T 36094-2018 定义的接口提供与此类生物特征识别模块直连，该接口定义综合考虑了接口提供的服务以及发送给生物特征识别模块的命令的报文格式和预期的来自这些模块的响应的报文格式。

GB/T 37743-2019 规定了为智能设备操作系统提供的身份识别服务接口。本标准适用于智能设备发行商定义并烧录设备身份识别信息，云服务提供商识别智能设备。

5.1.4 数据交换格式

数据交换格式标准，针对生物特征识别数据交换格式（包括框架、

指纹细节点数据、指纹型谱数据、指纹图像数据、人脸图像数据、虹膜图像数据、签名/签字时间序列数据、指纹型骨架数据、血管图像数据、手型轮廓数据、DNA 数据等）、公用生物特征识别交换格式框架（包括数据元素规范、生物特征识别注册机构操作规程）、指静脉图像数据格式、生物特征识别数据交换格式（包括框架、人脸图像数据、掌纹图像数据、指纹骨架数据、手形轮廓数据血管图像数据）等方面进行相关的规范与界定。

GB/T 26237.1-2010 规定了生物特征识别数据结构的用法概述、数据结构的类型、数据结构的命名思想及格式类型的编码方案。

GB/T 26237.2-2011 规定了 GB/T 26237 中基于细节点的指纹表示中所用到的概念和数据格式。

GB/T 26237.3-2011 规定了指纹型谱数据的定义、指纹型谱数据记录、指纹型谱数据卡格式、指纹型谱数据的存储形式，以及基于频谱的指纹数据的交换格式。

GB/T 26237.4-2014 规定了一个用来从一个或多个符合 ISO/IEC 19785-1 CBEFF 数据结构的指/掌纹图像区域进行存储、记录和传输信息的数据记录交换格式，可用来进行指纹图像数据的交换和比较。

GB/T 26237.5-2014 规定了一张/多张相片和人脸图像短视频流的存储、记录和传输的数据格式。规定了人脸图像拍摄时的场景约束、拍摄方法、数字人脸图像的存储格式、人脸图像拍摄的最佳范例。本部分适用于人脸图像数据的记录、存储和传输。

GB/T 26237.6-2014 规定了虹膜图像数据的交换格式，该格式主

要用于虹膜图像这一生物特征的注册、验证和识别系统。

GB/T 26237.7-2013 规定了动态签名/签字行为数据的概念和数据交换格式，该数据以时间序列形式利用诸如数字签名板或高级笔系统采集得到。

GB/T 26237.8-2014 规定了基于指纹型骨架模式的指纹识别数据交换格式，适用于自动指纹识别的各种应用领域。

GB/T 26237.9-2014 规定了血管生物特征图像的身份识别或身份验证技术所用的图像交换格式，可用于血管图像数据的交换和压缩。

GB/T 26237.10-2014 规定了生物特征识别领域中用于记录、储存和传输手型轮廓的数据交换格式。本部分规定了手型轮廓数据交换的内容、格式以及手型轮廓的计量单位。

GB/T 26237.14-2019 规定了一种用于 DNA 分型数据的交换格式。本部分适用于使用人类 DNA 来进行个体识别的 DNA 分型数据交换。

GB/T 28826.1-2012 规定了公用生物特征识别交换格式框架数据元素的术语和定义、符号和缩略语、结构、格式，以及格式之间的转换方式和符合性要求。

GB/T 28826.2-2020 规定了公用生物特征识别注册标识、注册机构、注册程序、注册申请和注册维护。适用于生物特征识别注册机构以及生物特征识别标识符申请、使用的相关方。

GB/T 32903-2016 规定了指静脉识别系统中指静脉图像的采集要求和数据格式，并给出了指静脉图像数据格式的具体示例。适用于指静脉识别系统中指静脉图像数据的采集、存储、交换和传输。

5.1.5 样品质量

样品质量标准，主要针对生物特征样本质量，包括框架、指纹图像数据、人脸图像数据、虹膜图像数据以及 DNA 数据进行了相关的描述与界定。

GB/T 33767.1-2017 规定了对任一或所有必要的生物特征样本类型，确立了规范中用到的和质量度量中使用的术语和定义，给出了生物特征质量分数的目的和解释，规定了生物特征数据交换格式中质量数据字段的格式和位置。

GB/T 33767.4-2018 针对指纹图像模态的质量方面，本部分确立了有助于指纹图像质量度量的规范、使用和测试的术语和定义、定义了指纹图像质量分数、识别或定义了指纹图像样本库，为算法开发人员和用户提供信息。

GB/T 33767.5-2018 规定了人脸图像质量指标定义、分类以及分析方法。本部分适用于人脸图像质量的分析。

GB/T 33767.6-2018 规定了用于量化虹膜图像质量的方法、用于生成虹膜图像的软硬件的规范性要求、用于衡量虹膜图像可用性的软硬件的规范性要求。

5.1.6 测试方法

测试方法标准，主要针对生物特征识别性能测试和报告、生物特征识别应用程序接口（BioAPI）的符合性测试、生物特征数据交换格式的符合性测试方法等方面进行相关的描述与界定。

GB/T 29268.1-2012 适用于以测试实验为基础的生物特征识别系统和算法的性能测试，该测试分析系统输出匹配得分和决策结果，而不涉及系统的算法或潜在的使用人群的生物特征分布情况。

GB/T 29268.2-2012 适用于生物特征识别系统和算法性能测试中的数据采集要求和建议、性能评价分析与报告，两种主要的性能评价类型为技术评价和场景评价。

GB/T 29268.3-2012 规定了描述表现模态间特定差异的通用方法，目的则是针对具体的生物特征模态，提出并定义各种方法，以实现特定的技术性能测试。

GB/T 29268.4-2012 适用于多供方生物特征识别系统的技术与场景评价的测试方法,其生物特征数据与交换格式标准的数据格式相一致。

GB/T 30268.1-2013 适用于符合 BioAPI(见 ISO/IEC19784-1)生物特征识别产品的符合性测试，规定了概念、框架、测试方法和准则。

GB/T 30268.2-2013 规定了 GB/T30267.1—2013 中定义的 BSP 的 5 个一致性子类将要执行本部分所有测试断言中的哪些子集，同时还规定了一些附加的断言，这些断言的执行取决于被测的软硬件实现是否满足 GB/T30267.1—2013 的可选特征。

GB/T 33842.2-2017 规定了指纹细节点数据交换格式的符合性测试方法的要素、测试断言和测试规程。针对指纹细节点数据格式结构的断言的测试，通过指纹细节点数据格式的每个字段的值的类型来判断内部一致性的断言的测试。

GB/T 33842.4-2017 规定了指纹图像数据交换格式，可用于一幅或多幅含有符合公用生物特征交换格式框架（CBEFF）的指纹图像的记录、存储和传输，其中每幅图像都应有相应的头记录包含与该图像相关元数据。建立了针对上述进制记录格式正确性的检查测试。

GB/T 33842.5-2018 规定了针对 GB/T 26237.5—2014 中定义的人脸图像数据交换格式的符合性测试方法的要素、测试断言和测试规程。 通过检测人脸图像数据每个字段的值的类型来检查内部一致性的符合性测试（对应于 ISO/IEC 29109-1:2009 中定义的类型 A 的级别 2）。

5.1.7 行业应用

行业应用标准，主要针对移动设备生物特征识别系统、卡上生物特征识别系统、社会保障卡生物特征识别系统等具体应用产品进行相关描述与界定。

GB/T 30266-2013 规范了在集成电路卡（ICC）内实施生物特征样本比对和返回决策的需求、卡内生物生物特征比对的安全策略，以及允许卡外预比对计算的命令和规则。

GB/T 16649.11-2019 规定了安全相关的行业间命令，用于在集成电路卡中通过生物特征识别方法进行个人身份验证。针对卡作为生物特征参考的载体和/或对持卡者的生物特征探针（卡上生物特征比对）进行验证的装置，本部分也给出了其使用的数据结构和数据访问方法。

GB/T 37036 已经发布了四个部分，第 1 部分通用要求、第 2 部分指纹、第 3 部分人脸、第 4 部分虹膜。GB/T 37036.1-2018 主要规

定了移动设备生物特征识别的技术架构、通用流程、功能要求和安全要求；GB/T 37036.2-2019 主要规定了应用于移动设备指纹识别系统的技术架构，规定了移动设备指纹识别的业务流程、功能要求、性能要求和安全要求；GB/T 37036.3-2019 主要规定了移动设备人脸识别系统的技术架构，规定了移动设备人脸识别的业务流程、功能要求、性能要求和安全要求；GB/T 37036.4-2021 主要规定了应用于移动设备虹膜识别的系统构成和业务流程，规定了移动设备虹膜识别系统的功能要求、性能要求和安全要求。

5.1.8 安全与加密

安全与加密标准，主要针对生物特征识别呈现攻击检测、个人信息安全规范、移动智能终端身份鉴别技术框架、生物特征识别身份鉴别协议框架等方面进行相关的描述与界定。

GB/T 35273-2020 规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。

GB/T 40660-2021 规定了生物特征识别信息的安全保护要求，包括生物特征识别系统的威胁和对策、生物特征信息和身份主体之间绑定的安全要求、应用模型以及个人信息保护要求等。

GB/T 36651-2018 规定了基于可信环境的生物特征识别身份鉴别协议框架，包括协议框架、协议流程、协议规则以及协议接口等内容。

GB/T 38542-2020 规定了统一的移动智能终端生物识别身份鉴别技术框架，规范移动智能终端上生物特征识别的处理流程、协议接

口、性能要求和信息安全，适用于基于生物特征识别的移动智能终端身份鉴别系统的设计、开发与集成。

GB/T 38671-2020 提出了以人脸识别为手段、以密码技术为保障的人脸识别系统，在远程可信环境中为信息系统提供用户身份标识与鉴别服务的安全框架，重点解决了前端可信环境、活体检测、服务端人脸库安全等关键环节的标准化问题。

GB/T 20979-2019 规定了采用虹膜识别技术进行身份识别的虹膜识别系统的结构、功能、性能、安全要求及等级划分。

GB/T 37076-2018 规定了采用指纹识别技术进行身份鉴别的指纹识别系统基本级和增强级的功能、性能、安全要求和等级划分。

5.1.9 **其他**

GB/T 38427.1-2019 规定了生物特征识别中人脸识别的流程、制作和应用过程以及防伪级别等技术要求。

JR/T0171-2020 主要将个人金融信息由高到低分为 C3、C2、C1 三个级别，人脸识别数据、指纹识别数据等个人生物识别信息属于 C3 级别，该标准明确要求金融业机构将用户个人信息外包提供给第三方时，不应委托或授权无金融业相关资质的机构收集人脸识别数据等个人生物识别信息。

JR/T 0164-2018 主要规定了移动金融服务场景中基于声纹识别的安全应用的功能要求、性能要求和安全要求等内容，不包括电话或网络电话（VoIP）中涉及声纹识别的应用场景。

QC/T 1058-2017《汽车用指纹识别装置》 主要规定了汽车用指

纹识别装置的术语和定义、原理、一般要求、技术要求、主要技术参数、试验方法、检验规则、标志、包装、运输、贮存。

5.1.10 小结

国内围绕生物特征识别标准化的工作逐渐展开，但当前主要还是依托 ISO/IEC 等国际标准化机构的前期标准进行国内转化为主，处于跟随状态。从所推进的领域来看，当前主要还是围绕通用的交换格式、接口、测试等方面展开，行业应用类的标准化研究目前主要聚焦在移动智能终端方面。随着智能网联汽车的发展，汽车已成为生物特征识别技术的重要应用领域，行业迫切需要针对车载生物识别技术的应用建立有针对性的标准体系，以指导生物识别技术在汽车行业的高效开发和规范应用。

5.2 国外标准体系分析

目前生物识别技术国际标准化工作主要在国际标准化组织（ISO）和国际电信联盟（ITU）展开。

ISO 中与生物特征识别技术较为相关的分委员会有生物特征识别分委会（ISO/IECJTC1/SC37）和信息安全技术分委会（ISO/IEC JTC1/SC27）。

ISO/IECJTC1/SC37 主要聚焦于生物特征识别系统和应用之间的互操作性和数据交换等标准化问题，秘书处由美国国家标准学会（ANSI）担任。目前 SC37 已发布与生物特征识别相关的标准有 120 余项，在研标准有 30 余项，主要包括下面几类标准:术语、生物特征识别应用程序接口（BioAPI）、数据交换格式及生物样本质量、生物

特征识别评估准则、性能测试和报告、司法和社会相关问题等。基于上述工作内容，SC37 主要分成 6 个工作组（WG1、WG2、WG3、WG4、WG5、WG6）。其中包括：WG1（生物特征识别术语）、WG2（生物特征识别应用程序接口）、WG3（生物特征数据交换格式）、WG4（生物特征识别系统技术实现)、WG5（生物特征识别测试与报告）和 WG6（生物特征识别与司法社会相关）。在业务上与 JTC1/SC17“卡及专用识别”、JTC1/SC27”信息技术安全技术”、ISO/TC8“银行、证券及其他金融业务”，以及国际工业生物统计学协会保持联系与合作。

ISO/IECJTC1/SC27 主要负责生物特征识别安全相关的标准化问题，如生物特征信息保护，生物特征识别安全测试和评估等，秘书处由德国标准学会（DIN）担任。主要分为 5 个工作组，其中 WG3 安全评估测试和规范工作组以及 WG5 身份管理和隐私保护技术工作组涉及到生物特征识别安全和身份认证。

此外，在金融服务技术委员会（ISO/TC68）和个人识别卡与安全设备分委会（ISO/IEC JTC1/SC17）也制定了一些与生物特征识别相关的标准，如将集成了生物特征识别技术的智能卡用于个人标识的技术规范。ISO/TC68 曾在 2008 年发布过一个生物特征识别相关标准《ISO 19092:2008 金融服务生物特征识别安全框架》，该标准目前已经修改采用为国家标准《GB/T 27912-2011 金融服务 生物特征识别安全框架》，主要规定了金融业使用生物特征识别鉴别人员身份的基本安全框架，描述了生物特征识别的主要技术类型并初步阐述了应用

时需考虑的问题[7]。

ITU 与生物特征识别标准相关的主要是 ITU-T SG17 安全标准工作组下设的 Q9 和 Q10 与生物特征识别技术相关。Q9 主要关注在通信应用环境中应用生物特征识别及其标准化工作。随着生物特征识别技术在电子商务、电子健康和移动支付领域中的广泛应用，该工作组同样关注生物特征数据的隐私保护、可靠性和安全性等方面的各种挑战。Q10 关注身份管理架构和机制，部分标准项目与基于生物特征识别身份认证相关。

伴随我国在生物特征识别技术研发和实际应用的快速发展，尤其是在基于移动设备的互联网金融领域的大规模应用，通过不断实践总结和迭代，在生物特征识别部分技术领域上如人脸识别、活体检测等已经在世界范围内取得了领先。在国际标准化工作上，我国也逐渐开始牵头部分标准的制订，如由中国牵头的 ISO/IEC 27553《移动设备生物特征识别身份认证安全要求》。

表 9　ISO 生物特征识别相关标准列表

标准类别	标准号	标准名称	实施日期
国际标准	ISO/IEC 2382-37	信息技术 协调一致的生物特征识别词汇	现行
国际标准	ISO/IEC 19794	信息技术 生物特征数据交换格式	现行
国际标准	ISO/IEC 39794	信息技术 可扩展的生物特征识别数据交换格式	现行
国际标准	ISO/IEC 19785	信息技术 通用生物特征交换格式框架	现行
国际标准	ISO/IEC 19784	信息技术 生物特征识别应用程序接口	现行
国际标准	ISO/IEC 24708	BioAPI 互通协议	现行
国际标准	ISO/IEC 24722	多模态及其他多生物特征识别	现行
国际标准	ISO/IEC 19795	多模态生物特征识别实现的测试	现行
国际标准	ISO/IEC 24709	生物特征识别应用程序接口的符合性	现行

		测试方法	
国际标准	ISO/IEC 29109	数据交换格式符合性测试	现行
技术报告	ISO/IEC TR30125	移动设备使用生物特征识别	
国际标准	ISO/IEC 30107-1	信息技术 生物特征识别呈现攻击检测 第一部分：框架	现行
国际标准	ISO/IEC 30107-2	信息技术 生物特征识别呈现攻击检测 第二部分：数据格式	现行
国际标准	ISO/IEC 30107-3	信息技术 生物特征识别呈现攻击检测 第三部分：试验和报告	现行
国际标准	ISO/IEC 21879	移动设备上的生物特征识别性能测试	现行
国际标准	ISO/IEC 24745	生物特征信息保护	现行
国际标准	ISO/IEC 19792	生物特征安全评估	现行
国际标准	ISO/IEC 19989	生物特征系统安全评估的准则和方法	现行
国际标准	ISO/IEC 17922	使用硬件安全模块的远程生物特征鉴别框架	现行
国际标准	ISO/IEC 24761	生物特征鉴别上下文环境	现行
国际标准	ISO/IEC DIS 27553	移动设备上使用生物特征识别进行身份认证的安全要求	制定中
国际标准	ISO/IEC 29100	信息技术 安全技术 隐私框架	现行
国际标准	ISO/IEC 29101	信息技术 安全技术 隐私架构框架	现行
国际标准	ISO 19092: 2008	金融服务生物特征识别 安全框架	现行

5.3 标准化建议

通过对智能网联汽车生物识别的政策、标准法规、技术及示范应用开展分析，并结合国内实际车联网、技术发展及应用现状研究，对产业发展及汽车领域标准化工作推进提出下述建议。

5.3.1 产业发展建议

（1）加强舱驾融通，推进与智能驾驶功能的融合交互

为了实现更安全的智能驾驶甚至自动驾驶落地，不仅需要对驾驶员监测系统的功能项进行必要拓展、对精度指标进行提升，还需要对相应的技术指标及测试方法进行标准化。驾驶员状态监测功能是自动驾驶应用落地过程中有效的安全保障，完善相应标准无论是对提升整车安全性还是用户体验都十分必要。建议行业建立联合工作平台进行

专题讨论和交流。

（2）完善标准体系，对应用场景标准迭代推进

智能网联汽车生物识别技术在有效提升便利性的同时，也存在着功能稳定性和用户隐私的风险。在已落地的智能网联汽车中，大部分功能聚焦在舱内主驾驶场景。今后整体网联汽车生物识别应用的趋势将会从主驾驶往全车多区多人过渡，如全车乘客监控系统、非人体识别（宠物）等。同时，关注焦点也将从安全概念越来越多的拓展到多模交互，如情绪识别、手势识别等。建议结合应用场景的拓展和技术路线的应用，分功能、分阶段进行相关场景研究和补充，保证研究既具有一定的落地性，也具备一定的前瞻性。根据智能网联汽车生物识别相关的技术和产业成熟度，制定有针对性的标准制定计划，迭代完善智能网联汽车生物识别的应用场景标准，进一步为相关法律法规的研究和制定提供参考和依据。

（3）持续推动新技术的有效落地

目前智能网联汽车生物识别技术的落地主要是图像识别，但在非车载领域同样存在其他生物识别技术路线，如深度信息 ToF 相机、毫米波雷达、指纹、声纹等。对于同类功能的车载应用落地是否存在更合适和高效的技术路线，建议行业持续深入探索。

5.3.2 标准制定建议

通过本文件 5.1.10 的分析发现，生物识别技术在汽车领域的标准化工作尚处于起步阶段。通过本文件第 2 章的分析发现，基于生物识别技术的车载应用正蓬勃发展，但严重缺乏标准指导。从场景看，当

前的车载应用主要包括生物识别比对类与生物识别监控类。结合行业发展需求及当前国内标准化现况，建议优先制定生物识别技术车载应用类标准。

（1）生物识别比对类

生物识别比对类标准，主要是对基于生物识别技术来进行身份比对的车载系统/功能进行技术标准研究，例如人脸识别技术、指纹识别技术、声纹识别技术等。按照不同场景在智能网联汽车领域的落地情况和需求迫切度，建议优先制定《智能网联汽车 生物识别认证系统技术要求及试验方法 第 1 部分：人脸》和《智能网联汽车 生物识别认证系统技术要求及试验方法 第 2 部分：指纹》两个标准。

（2）生物识别监控类

生物识别监控类标准，主要是对基于生物识别技术来对人员、婴儿、宠物等目标物体进行监控的车载系统/功能进行技术标准研究。例如驾驶员监测、乘员监测、车内儿童滞留检测等。按照不同场景在智能网联汽车领域的落地情况和需求迫切度，建议优先制定《驾驶员接管能力监测系统技术要求及试验方法》和《车内儿童存在检测系统技术要求及试验方法》两个标准。

5.3.3 标准化路线图

标准化路线图的制定主要考虑“成熟应用先行、产业急需先行、法律支撑先行”三点原则。同时为避免对技术创新和产业发展形成超前制约，重点标准要聚焦主要功能场景，优先制定行业落地成熟、各家对技术路线的实现达成主流共识的系统/功能模块产品类标准。考

虑到智能网联汽车领域生物识别产业的发展速度，未来可结合行业技术和应用的多样性发展，对标准路线图动态更新和进一步完善。

（1）第一阶段：（2022 年-2024 年）

聚焦现有技术能力、当前市场验证能力较为成熟的生物识别车载应用功能，尽快推进以下标准研究工作，通过行业规范化应用及有效监管提升智能汽车的便利性和可靠性。

——《智能网联汽车 生物识别认证系统技术要求及试验方法 第1部分：人脸》；

——《智能网联汽车 生物识别认证系统技术要求及试验方法 第2部分：指纹》；

——《驾驶员接管能力监测系统技术要求及试验方法》。

（2）第二阶段：（2024 年-2025 年）

关注虹膜识别、多模态识别等生物识别技术的行业研究及应用趋势，并同步观察国际标准体系走向，适时启动以下标准研究工作。

——《车内儿童存在检测系统技术要求及试验方法》；

——《智能网联汽车 生物识别认证系统技术要求及试验方法 第3部分：虹膜》。

（3）第三阶段：（2025 年→）

根据技术水平发展情况及行业应用进度，持续审视标准体系更新需求，并适时启动标准研究工作。

6 总结与展望

6.1 研究总结

本研究报告从智能网联汽车生物识别功能的应用场景、关键技术、产业普及现状、测评指标及方法、痛点及应对、法律法规以及标准体系等方面进行分析，根据研究结果分析智能网联汽车生物识别标准化需求并制定标准路线图供后续产业标准制定参考。从智能网联汽车、生物识别功能性能、信息安全、数据安全的需求入手，探索各个应用场景下的标准化需求，结合各领域的技术痛点和标准需求，展开整体研究工作。对于行业来说，通过制定不同场景下生物识别技术的标准化测评方法和指标，可促进产业普及与技术创新，同时引导行业健康良性发展、有序运行。对于消费者来说，生物识别的标准化为行业提供了更广阔的创新空间，同时也进一步提升了驾乘体验与个性化需求。

6.2 后续展望

随着汽车生物识别技术的发展与产业普及，智能网联汽车生物识别技术即将处于大规模商用阶段，并演化出更多的应用场景，将切实提升驾驶的安全性、可靠性、便利性。随着生物信息比对、驾驶员检测、生物存在检测、智能交互等应用场景在智能网联汽车上的量产使用，智能网联汽车分标委将与相关单位共同合作，继续推进该研究内容的完善，并基于本研究报告中的标准化建议，开展相关标准研究。同时，随着汽车生物识别技术的不断发展和创新，未来虹膜识别、声纹识别、步态识别等技术也将量产应用到生物信息比对场景中；手势识别等新兴技术也将更多应用到智能交互场景中；驾驶员监测技术也

将量产应用到L3级别的驾驶场景；汽车生物识别技术也将在数据合规的情况下应用到车外行人数据的采集场景中。未来，智能网联汽车分标委将与相关单位共同合作，在产业标准化共识基础上，通过标准工作支撑技术发展，不断迭代和研发相关技术并逐步完善相关标准体系的建设。

附录 A 术语定义

车载生物识别

主要指通过摄像头、红外传感器、指纹传感器、麦克风等传感器对汽车内外生物体的相关数据进行采集，对其生理特征和行为特征进行分析与处理，实现对车内外生物体的身份识别、状态监控、个性化服务等功能，使汽车具备一些类似生物的感知能力。

附录 B 缩略语

2D：二维（2-dimension）

3D：三维（3-dimension）

5G：第五代移动通信技术（5th Generation Mobile Communication Technology）

ACC：准确率（accuracy）

ADAS：高级驾驶辅助系统（Advanced Driving Assistance System）

AI：人工智能（Artificial Intelligence）

ANSI：美国国家标准学会（American National Standards Institute）

BioAPI：生物特征识别应用程序接口（Biometric Application Program Interface）

BLE：蓝牙低能耗（Bluetooth Low Energy）

CCD ：电荷耦合器件（Charge-coupled Device）

CMOS：互补金属氧化物半导体（Complementary Metal Oxide Semiconductor）

CPD：儿童存在探测（Child Presence Detection）

CRS：儿童约束系统（Child Restraint Systems）

CSI：关键成功指数（Critical Success Index）

DDAWS：驾驶员睡意和注意力警告（Driver Drowsiness and Attention Warning Systems）

DIN：德国标准学会 (Deutsches Institut für Normung e.V.)

ECG：心电图（electrocardiogram）

ECU：电子控制单元（Electronic Control Unit）

EEG：脑电波（Electroencephalogram）

FAR：误识率（False Acceptance Rate）

FN：假阴性（False Negative）

FP：假阳性（False Positive)

FPR：假正率（False Positive Rate）

FRR：拒识率（False Rejection Rate）

ICV：智能网联汽车（Intelligent Connected Vehicle）

IEC：国际电工委员会（International Electrotechnical Commission）

ISO：国际标准化组织（International Organization for Standardization）

ISP：图像信号处理（Image Signal Processing）

ITU：国际电信联盟（International Telecommunication Union）

L2：第二级（Level 2）

LDWS：车道偏离预警系统（Lane departure warning system）

NCAP：新车评估项目 （New Car Assessment Program）

NFC：近场通信（Near Field Communication）

PERCLOS：随时间推移瞳孔上眼睑闭合百分比（Percentage of Eyelid Closure over the Pupil Over Time）

RFID：射频识别（Radio Frequency Identification）

TN：真阴性（True Negative）

TOF：光飞行时间法（Time of flight）

TP：真阳性（True Positive）

TPR：真正率（True Positive Rate）

UWB：超宽带（Ultra Wide Band）

V2X：车对外界的信息交换（vehicle to everything）

附录 C 隐私计算示例

随着互联网、智能手机以及 Web3.0 技术和市场的日趋成熟和繁荣，隐私泄露问题早已成为全球各国争取所关注的重要问题，正如本文中所介绍的各国隐私法规的出台，极大的遏制住了隐私泄露问题的日益蔓延。但与此同时大数据、数据要素流通等技术又对数据产生了爆炸式的需求，而在这些海量数据中，隐私数据就像一块烫手的山芋，困扰着全球大数据产业和相关监管部门。

以密码学、数学和信息安全学等多门学科交叉形成的隐私计算技术，是目前公认的可以有效解决隐私数据保护和大数据分析之间矛盾的技术方案，实现数据可用不可见的目的。

隐私计算体系是由多个基础技术构建而成，用户可以结合数据特征、应用场景、计算平台等多种因素，选择不同的组合方案。这些基础技术包含同态加密（HE）、多方安全计算（MPC）、机密计算（CCA）、联邦学习（FL）、差分隐私（DP）、零知识证明（ZKP）、区块链技术以及传统的数据脱敏和假名化技术。

通过结合智能网联汽车生物识别技术的具体应用场景和零部件计算平台，我们认为可以通过结合机密计算和联邦学习技术构架一套可用于实际应用的智能网联汽车隐私计算方案。下图具体展示了智能网联汽车隐私计算解决方案的整体架构：

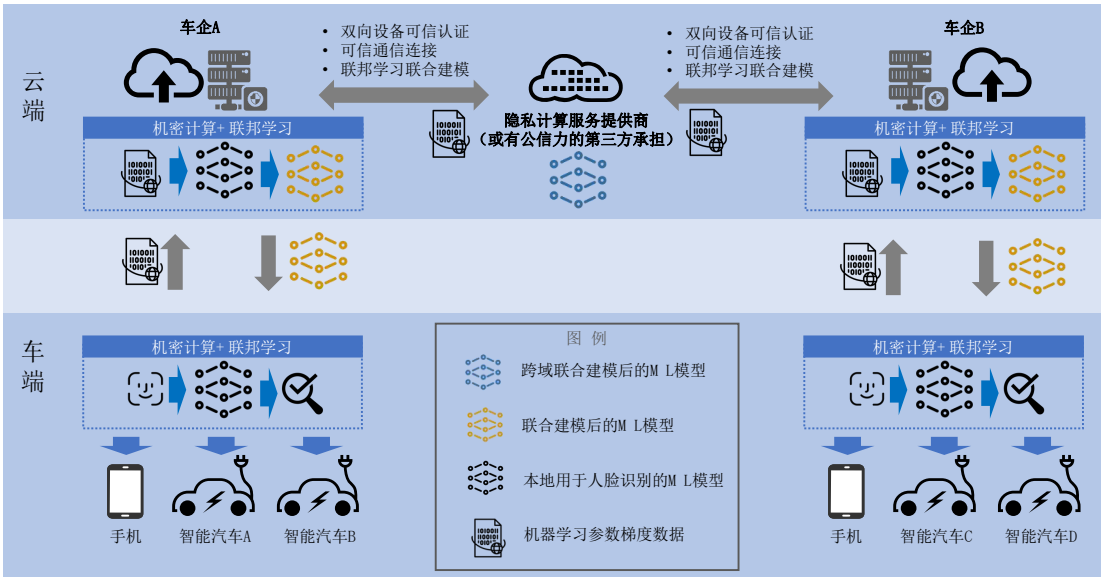


图 8　智能网联汽车隐私计算解决方案

解决方案简述：

● 机密计算最初源自于 2006 年 OMTP 工作组提出的“在一个智能设备上，除了一套通用多媒体操作系统之外，再提供一个完全隔离的安全操作系统，并通过其保护关键数据的安全”的架构，该架构被称为可信执行环境（TEE：Trusted Execution Environment）。ARM 公司自 V6 指令集开始支持的 TRUSTZONE 技术，就属于 TEE 架构。随着 ARM CPU 在移动互联网、物联网等领域的高速发展，TRUSTZONE 技术也在 V9 指令集中升级为机密计算（CCA：Confidential Compute Architecture）。由于车载芯片普遍使用 ARM CPU，因此，TRUSTZONE 或 CCA 将是智能网联汽车隐私计算技术的首选方案；

● 联邦学习（FL：Federated Learning）是进行分布式机器学习的过程中，各参与方可借助其他参与方数据进行联合建模和使用模型的技术。参与各方无需传递和共享原始数据资源，同时保

护模型参数，即在数据不出本地的情况下完成数据联合训练、联合应用、最终形成合法合规的机器学习模型；

● 通过车端及云端的机密计算体系，利用芯片硬件隔离和可信安全存储机制防止生物识别信息、机器学习模型、证书密钥等敏感数据的泄露，确保联邦学习过程及生物信息识别过程均在安全域中进行；

● 利用联邦学习技术，确保在模型训练过程中无需将生物识别信息传送至车外，同时又可以通过传递深度学习参数梯度，完成对深度学习模型的优化训练，从而实现在本地完成生物识别过程，同时又可以通过 CCA+FL 技术不断训练优化新模型的目的。

附录 D 引用文件

[1] 生物识别的未来 The Future of Biometrics，[R]，Acuity Market Intelligence.

[2] 2020 年全球生物识别行业市场现状及发展趋势分析进一步数字化、智能化发展，[R]，前瞻产业研究院.

[3] 2018 年生物识别技术行业应用市场现状与发展趋势分析，[R]，前瞻产业研究院.

[4] 2022 年全球生物识别市场规模及细分行业市场规模预测分析，[R]，中商情报网.

[5] 2022 年中国生物识别行业市场规模将达 400 亿 产业向着科技含量更高的方向发展，[R]，中商情报网.

[6] 2016-2025 全球汽车行业生物识别技术，[R]，Frost&Sullivan.

[7] 孙曦、冯春培、落红卫，生物特征识别国际标准化研究情况[J].金融电子化，2018(10)：60-61.