《人工智能视觉隐私保护 第2部分：技术应用指南》

（征求意见稿）编制说明

# 1、工作简况

根据根据新一代人工智能产业技术创新产业联盟（暨中关村视听产业技术创新联盟）2020年标准制修订计划的安排，由海信集团控股股份有限公司牵头制定团体标准《人工智能视觉隐私保护 第2部分：技术应用指南》的制定任务。

新一代人工智能产业技术创新战略联盟AI标准工作组由新一代人工智能产业技术创新战略联盟于2018年批准成立。工作组的任务是：面向我国的人工智能数据的隐私保护需求，联合国内企业和科研机构，制（修）订由AI技术应用涉及到的数据隐私安全共性技术标准，为人工智能产品与应用提供规范健全的数据隐私保护标准，服务于智能家电、智能音响、边缘计算设备、服务架构等涉及用户数据隐私的AI产业应用。

计算机视觉技术在近些年中得到了迅速发展，并应用于诸多领域，如产品交互方案实现、安防、智能制造、医疗诊断、自动驾驶等。但对视觉类数据（包括视频和图像等）的隐私保护手段仍不完善，视频视觉数据作为一种包含大量可视信息的媒介，其海量信息中蕴藏着高价值密度的敏感信息，一旦泄露会对企业、用户造成重大影响和困扰。为了推动技术应用落地、同时满足用户隐私保护需求，数据隐私保护组开展了人工智能视觉隐私保护系列标准的研制工作。已制定团体标准《人工智能视觉隐私保护 第1部分：通用技术要求》从安全技术、风险评估以及安全管理三大维度，对AI视觉隐私保护系统提出要求，2020年12月31日发布实施。

《人工智能视觉隐私保护 第2部分：技术应用指南》给出了视觉数据的保护目标和措施，提供了人工智能视觉隐私保护技术应用过程中的管理措施指南。本标准适用于组织规范企业对海量的视觉数据下针对隐私保护标准措施的规范使用，也适用于网络安全相关主管部门、第三方评估机构等组织开展视觉隐私数据的安全监督管理、评估。

# 2、制定过程

2020年6月AI隐私工作组第11次会议通过《人工智能视觉隐私保护 第2部分：技术应用指南》提案，2020年11月标准正式立项，计划编号为2020111003。2022年6月在AI第19次标准会议数据隐私保护组会议上，条件采纳M1593（即WD5.2），要求根据工作组意见做修改，形成征求意见稿。

自2020年12月第13次会议，决议采纳M1355提案，并形成草案N1282后，工作组召开了6次（2021年3月、2021年6月、2021年8月、2021年10月、2021年12月、2022年3月、2022年6月）全体会议，主要形成以下会议决议：

1. 标准需覆盖视觉隐私保护算法的基本要求与算法保护性能评价指标、结构化数据和非结构化数据要求；
2. 按GB/T 20000.7要求将标准调整为指南标准；
3. 增加隐私保护技术方法分类；
4. 按视觉隐私数据的生命周期，形成AI视觉脱敏、加密、去标识、数据追溯等技术方法的指导和评价指标；
5. 按照GB/T 1.1-2020的要求，编制标准文本并形成征求意见稿。

本部分起草单位：海信集团控股股份有限公司、山东大学、深圳龙岗智能视听研究院、美的集团(上海)有限公司、中国海洋大学、天津大学、上海商汤智能科技有限公司、云从科技集团股份有限公司、翼健（上海）信息科技有限公司、上海数字电视国家工程研究中心有限公司、北京邮电大学、西安电子科技大学、北京大学。

本标准主要起草人：陈维强、高雪松、刘琚、张世雄、区志财、魏志强、李克秋、张淯易、李亚锋、魏文应、唐剑、刘秀龙、徐浩、李军、周禾、顾凌晨、刘晓玺、王雪静、邵宸、刘常昱、吕林、黎俊良、殷惠清、陆月明、朱辉、田永鸿、王荣刚、牟小峰、蒋慧、吴庚、温浩、尹建华、左金鑫、鲁昱、赵雪圻、陶键源、李若尘。

# 3、标准编制原则和确定标准主要内容的论据，若标准中涉及专利，则应列出相关专利的目录及其使用理由。

## 3.1编制原则与确定内容的依据

《人工智能视觉隐私保护 第2部分：技术应用指南》是对视觉隐私数据保护算法做出最适合的建议和最佳的科学操作指导。目前，针对视觉数据保护算法的度量缺乏统一的标准及行业性建议。现存的安全性要求都是从算法本身的衡量指标角度出发，过于笼统。视觉隐私数据保护算法的种类有很多，每一个算法重点保护的对象不同，不同算法产生的代价与带来的保护收益不同导致准确度与性能差异很大。这些差异导致本文件无法产生准确统一的安全性与可用性约束条件。因此，本文件抽象出所有视觉隐私保护算法的共性，针对算法的性能以及代价不同进行了统一的定性，其理念和原则广泛适用于视觉隐私数据保护算法。

《人工智能视觉隐私保护 第2部分：技术应用指南》给出了视觉数据的保护目标和措施，提供了人工智能视觉隐私保护技术应用过程中的管理措施指南。本文件只涉及视觉隐私数据保护的技术与处理，现阶段仅暂应用于家庭监控视频中，但其技术特征可向城市、社区等场景应用延伸。隐私数据是指数据中直接或间接蕴含的，涉及个人或组织的，不宜公开的，需要在收集、存储、查询和分析、发布过程中加以保护的信息，而视觉隐私数据在隐私数据的基础上具有视觉特征，包括视频、图像等。本文件中，对保护视觉隐私数据的算法技术提出基本建议，它们符合用户对视觉隐私数据广义上的认知，同时本文件也对隐私数据算法的性能提出基本建议。

## 3.2 处理专利技术的基本策略

本标准不涉及专利问题。

# 4、主要试验或验证的分析、综述报告，技术经济论证，预期的经济效果

标准中所涉及的隐私保护技术已在具有视觉采集功能的终端显示设备、家庭安防监控设备等产品上进行验证测试。通过验证，结合产品实际特性，同时兼顾产品性能及隐私保护要求，给出视觉隐私保护算法评价指标及参考值：平均精度均值（宜达到25%以上）、结构相似性（不宜低于0.50）、内核感知距离（不小于8）、峰值信噪比（不宜低于30dB）、信息隐藏容量（在保证不失真的情况下越大容量越高）、每秒传输帧数（不宜低于30dB）、元任务类别与样本数。标准通过技术指标达成系统特性、推荐了可选技术路线，可作为生产或应用厂家的技术方案，既能确保视觉信息在产品上有效应用、又可确保隐私受到保护。

同时标准研制也结合行业调研的方式同步开展，对推荐技术指标调研其行业典型应用值，并结合测试结果给出最终推荐建议值。如实时性指标中的25FPS，即是参考国内行业内摄像头典型技术参数及处理最低值25FPS。可引导相关厂家的技术落地、实施，促进行业进步、技术发展，推动视觉隐私保护产业上下游的发展。

# 5、采用国际标准或国外先进标准的目的、意义和一致性程度，我国标准与被采用标准的主要差异及其原因；以及与国际、国外同类标准水平的对比情况

目前，国内外尚无人工智能视觉隐私保护技术应用的相关标准化技术文件。

# 6、与我国有关的现行法律、法规和相关强制性标准的关系。

符合现有法律法规和强制性标准。