

公共场所人脸识别分级分类应用指南

Guidelines for facial recognition classification application in public places

2024-04-02 发布

2024-07-01 实施

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 1

 4.1 合理性原则 1

 4.2 良性发展原则 2

 4.3 权责一致原则 2

 4.4 安全性原则 2

 4.5 未成年人保护原则 2

5 分级分类方法 2

 5.1 人脸识别公共场所分类 2

 5.2 人脸识别风险评估 3

 5.3 公共场所人脸识别应用风险分级 5

6 应用方法 5

 6.1 概述 5

 6.2 应用主体条件 6

 6.3 实施环节及措施 6

 6.4 不同应用等级建议采取的措施 7

附录 A（资料性） 常见的应用人脸识别的公共场所分类说明 10

参考文献 14

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由上海市经济和信息化委员会提出并组织实施。

本文件由上海市人工智能标准化技术委员会归口。

本文件起草单位：上海华东电信研究院、上海市质量和标准化研究院、上海依图网络科技有限公司、上海商汤智能科技有限公司、上海市人工智能行业协会、公安部第三研究所、上海人工智能实验室、上海市大数据中心、上海计算机软件技术开发中心、中国社科院、同济大学、上海交通大学、华东师范大学、支付宝(中国)网络技术有限公司、上海云从汇临人工智能科技有限公司、中电金信数字科技集团有限公司、上海说以科技有限公司。

本文件主要起草人：彭莉、常永波、徐雷、张正敏、赵春昊、宋方方、戴宇欣、朱婕、陈俊琰、刘彩霞、谢芳艺、刘晶晶、沈涛、段伟文、陈吉栋、袁梦、石念、陈曦、蒋慧、宋剑锋、瞿晶晶、梁满、陈敏刚、陈文捷、陈玉珑、张志忠、许源、张哲煜、林冠辰、彭晋、李军、杨清、陈森。

公共场所人脸识别分级分类应用指南

1 范围

本文件提供了公共场所人脸识别分级分类应用的基本原则、分级分类的方法，以及应用方法。
本文件适用于公共场所新建人脸识别系统的分级分类应用，已建人脸识别系统可参照执行。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

人脸识别 face recognition

以人面部特征作为识别个体身份的一种个体生物特征识别方法。人脸识别包括人脸验证和人脸辨识。
[来源：GB/T 38671—2020，3.1.2，有修改]

3.2

公共场所 public places

提供公众使用或公众有权访问的空间。

3.3

个人人脸信息处理者 personal face information processor

人脸识别活动中自主决定处理目的、处理方式的组织、个人。

3.4

个人信息主体 personal information possessor

个人信息所标识或者关联的自然人。

[来源：GB/T 35273—2020，3.3]

3.5

使用主体 use subject

使用人脸识别系统的组织、个人。

3.6

实施主体 implementation subject

研发、生产、集成人脸识别系统的组织、个人。

3.7

人脸识别应用 face recognition applications

应用人脸识别进行人员管理、安全防范等特定目的的过程。

4 基本原则

4.1 合理性原则

合理性原则包括但不限于：

- a) 最小必要：只收集满足人脸识别目的所需的最小范围的信息，不收集与人脸识别目的无关的个人信息；
- b) 目的明确：遵循合法、正当、必要和诚信原则明确应用目的，并采取对个人权益影响最小的方式实现应用目的；
- c) 一致性：个人信息的收集、使用目的与结果必须一致，不能随意改变。

4.2 良性发展原则

良性发展原则包括但不限于：

- a) 公开透明：人脸识别系统宜在民众充分知情的情况下建设和应用；
- b) 准入控制：开展人脸识别业务的主体具备保障个人人脸信息数据安全的能力。

4.3 权责一致原则

个人人脸信息处理者在人脸识别系统建设和应用过程中明确并承担相应责任，若无法履行则不启动相关工作。

4.4 安全性原则

安全性原则包括但不限于：

- a) 事前考虑：项目实施前宜预先评估安全风险及合规问题；
- b) 事中保障：项目执行阶段设立有效的安全保障机制，具备应对各种安全风险的安全能力，采用充分的安全措施和技术手段以防范可能出现的风险；
- c) 事后追溯：建立完整的项目审计追溯机制，覆盖项目实施完成和使用过程。

4.5 未成年人保护原则

个人人脸信息处理者在必须处理不满十四周岁未成年人的个人人脸信息时，宜事先取得未成年人父母或者其他监护人的同意，并采取严格保护措施、制定专门的个人信息处理规则、履行更高标准的告知义务。

5 分级分类方法

5.1 人脸识别公共场所分类

公共场所应用人脸识别的常见应用场景可分为社会管理、行业应用、其他三类，各场景可依照行业类别进一步细分，见表 1。

- a) 社会管理包括公共安全、司法、政务、公共服务、交通以及其他具有社会管理属性的细分场景（见表 A.1）。
- b) 行业应用包括金融、医疗、教育、建筑、房地产、商业、娱乐等细分场景（见表 A.2）。
- c) 其他，包括社区和园区等细分场景（见表 A.3）。

注1：其他应用场景主要涉及利用人脸识别技术实现人员管理、安全防范等目的的应用场景。

注2：社区是人们进行居住、生活等活动的特定区域；园区是满足从事某种特定行业生产和科学实验需要的标准性建筑物或建筑物群体，包括工业园区、产业园区、物流园区、都市工业园区、科技园区、创意园区等。

表1 常见的应用人脸识别的公共场所分类

| 应用场景 | 细分场景 |
|------|------|
| 社会管理 | 公共安全 |
| | 司法 |
| | 政务 |
| | 公共服务 |
| | 交通 |
| | 其他 |
| 行业应用 | 金融 |
| | 医疗 |
| | 教育 |
| | 建筑 |
| | 房地产 |
| | 商业 |
| | 娱乐 |
| | 其他 |
| 其他 | 社区 |
| | 园区 |

5.2 人脸识别风险评估

5.2.1 风险评估要素

5.2.1.1 公共场所实施人脸识别时宜充分考虑以下风险要素：

- a) 应用目的风险。通过人脸识别应用的目的进行体现，对于有多个应用目的的项目，选取最高值作为本项风险值；
- b) 底库规模风险。通过人脸识别系统可识别的人脸数量，即底库规模体现，底库规模越大风险相对越高；
- c) 覆盖密度风险。通过人脸采集设备的布局密度体现，密度越高风险相对越高；
- d) 管理水平风险。通过人脸识别使用主体的管理科学程度体现，管理科学规范水平越高风险越低；
- e) 网络环境风险。通过人脸识别系统接入网络的方式体现，接入的网络安全性越高风险相对越低。

注1：底库规模指系统存储的可识别的人脸图像特征信息的数据库大小，单位为“人”，每个单位可能包括多个特征信息。

注2：覆盖密度是指人脸采集设备的分布密度，单位为“路每平方公里”，即每平方公里安装了多少路人脸采集设备。

5.2.1.2 各项风险要素宜采用的取值范围可参考表 2～表 6。

表2 应用目的风险评估表

| 风险要素：应用目的 | 风险值参考取值范围 |
|-----------|-----------|
| 安全防范 | 1～3 |

表2 应用目的风险评估表（续）

| 风险要素：应用目的 | 风险值参考取值范围 |
|-----------|-----------|
| 人员管理 | 2~4 |
| 商业分析 | 3~5 |
| 娱乐体验 | 4~5 |

表3 底库规模风险评估表

| 风险要素：底库规模（人） | 风险值参考取值范围 |
|--------------|-----------|
| 0~1000 | 1~2 |
| 1000~10000 | 2~3 |
| 10000及以上 | 3~5 |

表4 覆盖密度风险评估表

| 风险要素：覆盖密度（路每平方公里） | 风险值参考取值范围 |
|-------------------|-----------|
| 0~50 | 1~2 |
| 50~100 | 2~3 |
| 100以上 | 3~5 |

注：覆盖密度计算方法为计划安装的摄像头总路数除以公共场所的总面积，面积不足1平方公里的按1平方公里算。

表5 管理水平风险评估表

| 风险要素：管理水平 | 风险值参考取值范围 |
|-----------|-----------|
| 第三级 | 1~3 |
| 第二级 | 2~4 |
| 第一级 | 3~5 |

注：管理水平风险宜考虑的因素包括政策和制度、机构和人员管理、风险管理等方面，GB/T 20269—2006 中6.1~6.3给出了管理水平从第一级到第三级的风险评估要点。

表6 网络环境风险评估表

| 风险要素：网络环境 | 风险值参考取值范围 |
|-----------|-----------|
| 政府专网或离网 | 1~3 |
| 局域网 | 2~4 |
| 公网 | 3~5 |

5.2.2 综合风险值评估

综合风险值计算方法见公式(1)。

$$R = 0.28M + 0.17D + 0.12F + 0.23G + 0.20W \dots\dots\dots (1)$$

式中：

R ——综合风险值；

M ——应用目的风险值；

D ——底库规模风险值；

F ——覆盖密度风险值；
 G ——管理水平风险值；
 W ——网络环境风险值。

5.3 公共场所人脸识别应用风险分级

公共场所人脸识别风险从低到高可划分为A、B、C、D、E五个等级。

建议结合5.1人脸识别的场所分类结果和5.2应用人脸识别的综合风险值，按照图1得出公共场所人脸识别应用风险等级。

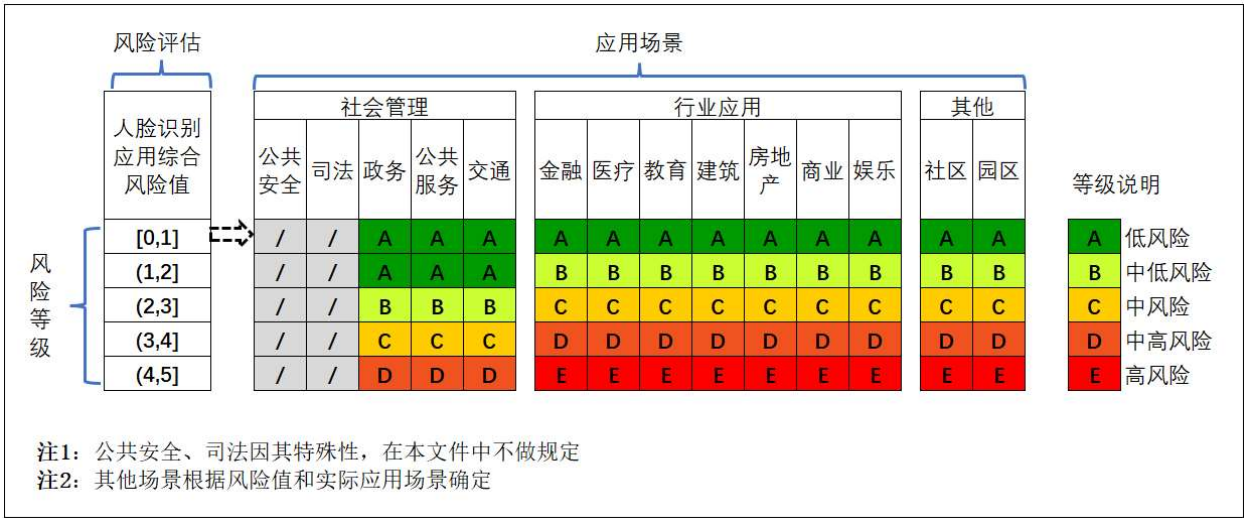


图1 公共场所人脸识别应用风险等级划分索引图

6 应用方法

6.1 概述

6.1.1 根据应用人脸识别的风险等级，实施的人脸识别系统宜参照 GB/T 20269—2006、GB/T 22239—2019、GB/T 22240—2020 要求完成相应等级的安全设计和实施防护措施。

6.1.2 公共场所人脸识别应用宜遵循最小必要原则，具体分级如下：

- a) A 级（低风险）：认可使用。适用于低风险的场景，或法律、法规、强制标准中已有规定的允许使用人脸识别的应用场景；
- b) B 级（中低风险）：允许使用。适用于中低风险场景，宜提供至少一种可选择的替代方案或组合应用方案，包括但不限于证件识别、锁具、密码等非生物特征识别方案；
- c) C 级（中风险）：适度使用。适用于中风险场景，不宜将人脸识别作为唯一的方案，宜提供至少一种可选择的替代方案或组合应用方案，包括但不限于证件识别、锁具、密码等非生物特征识别方案；
- d) D 级（中高风险）：审慎使用。适用于中高风险场景，非必要不使用，若必须使用则通过优化要素风险降低风险等级后使用，且不宜将人脸识别作为出入的唯一的方案，宜提供至少一种可选择的替代方案或组合应用方案，包括但不限于证件识别、锁具、密码等非生物特征识别方案；
- e) E 级（高风险）：不建议使用。适用于高风险场景，不建议使用人脸识别系统。

6.2 应用主体条件

6.2.1 使用主体

- 6.2.1.1 人脸识别系统的使用主体具有良好的信用情况。
- 6.2.1.2 组织并采用合法、合适的方式，获得人脸识别对象的正式同意授权。
- 6.2.1.3 在公共场所的显著位置，告知设置人脸识别采集点位的提示标识。
- 6.2.1.4 宜参照GB/T 20269—2006 建立和实施涵盖多个关键领域的分等级管理要求。
- 6.2.1.5 宜采用必要的安全技术确保系统和数据安全，并建立相应的应急预案对使用中的危险行为进行溯源。

6.2.2 实施主体

- 6.2.2.1 人脸识别系统实施主体一般包含集成商和系统供应商两类。
- 6.2.2.2 宜通过质量管理体系认证和信息安全管理体系认证，并取得符合国家或行业要求的信息安全管理体系相关资质证书，以及根据业务需求所需的其他特定资质证书。
- 6.2.2.3 人脸识别系统信息安全工程管理要求参考 GB/T 20282—2006 的规定。

6.2.3 其他服务提供方

其他服务提供方管理参考GB/T 32914—2016的规定。

6.3 实施环节及措施

6.3.1 描述

人脸识别应用涉及收集、传输、存储、使用、共享转让公开披露、删除等环节。应用人脸识别逐一考虑这些环节可采取的技术措施，以及各环节的个人信息主体、使用主体、人脸识别系统技术提供者或设备供应商等主体的权限和责任。

6.3.2 收集

收集个人人脸信息的基本原则是目标明确、公开透明、自主选择、授权同意。且满足最小必要原则，仅收集与业务直接相关的个人人脸信息。收集不满十四周岁未成年人个人人脸信息的，宜取得未成年人的父母或者其他监护人的同意和授权。

6.3.3 传输

传输个人人脸信息宜进行去标识化处理和采用加密等安全措施，遵循最小必要原则，与其他个人信息进行隔离传输。

6.3.4 存储

- 6.3.4.1 存储个人人脸信息宜进行去标识化处理和采用加密等安全措施，不存储原始个人人脸信息，仅存储个人人脸摘要信息，并与其他个人信息进行隔离存储。
- 6.3.4.2 根据不同应用场景设置个人人脸摘要信息的最高存储时限，该时限小于必要使用时长，授权人签署的授权时间小于该时限。
- 6.3.4.3 个人人脸摘要信息超出存储期限后，及时删除或做匿名化处理。
- 6.3.4.4 允许个人信息主体对存储的个人人脸摘要信息进行查询、变更、删除等操作。

注：个人人脸摘要信息是对个人人脸信息进行关键信息提取并编码后形成的信息，具有不可逆的特性，即无法通过个人人脸摘要信息反向推导获取个人人脸信息。

6.3.5 使用

6.3.5.1 个人人脸信息处理者确保个人人脸信息使用过程安全、透明，可进行角色分类设置和有限授权，确保相关操作保留痕迹可溯源。

6.3.5.2 个人人脸信息使用宜在授权人授权范围内使用，不超出个人授权的范围，使用目的与授权人签署的授权目的一致。当个人人脸信息使用目的变更时，告知并征得授权人的重新授权。

6.3.5.3 个人人脸信息处理者保障个人人脸信息在使用过程中不被泄露和篡改。

6.3.5.4 个人人脸信息的使用主体可通过授权的方式允许授权人对其个人人脸信息进行查询、变更、删除等操作，并确保过程安全。

6.3.5.5 对个人人脸信息进行展示宜遮挡重要部位信息，例如双眼等，并参考 GB/T 35273—2020 中 7.2 的要求，展示过程中个人人脸信息不宜与被展示人的其他个人信息关联展示。

6.3.6 共享、转让、公开披露

6.3.6.1 个人人脸信息处理者在进行个人人脸信息共享、转让、公开披露前宜进行影响评估，及时无遗漏地向个人信息主体告知相关信息并获得授权同意。

6.3.6.2 个人人脸信息处理者对个人人脸信息进行共享、转让、公开披露宜参照 6.3.5。

6.3.7 删除

6.3.7.1 删除个人人脸信息时，操作的及时性、主动性、安全性、完整性等是需要重点考虑的。

6.3.7.2 在分析结束后、到达授权时限或责任主体破产且无法合法合理转让个人人脸信息到其他个人人脸信息处理者时，个人人脸信息处理者宜及时删除个人人脸信息。

6.3.7.3 当个人信息主体发现个人人脸信息处理者进行违法违规操作时要求删除个人人脸信息的，个人人脸信息处理者宜及时删除。

6.4 不同应用等级建议采取的措施

6.4.1 A 级（低风险场景）

A级应用建议采取的措施包括：

- a) 风险管理：进行基本的风险管理，针对关键系统资源定期进行风险分析和评估；
- b) 抗攻击能力：至少在算法和模型层面具备主动抵御各种攻击的能力；
- c) 安全管理制度：建立日常管理活动中常用的安全管理制度；
- d) 安全管理机构：设立系统管理员等岗位，并定义各个岗位的职责，并为各岗位配备相关人员；
- e) 安全管理人员：指定或授权专门的部门或人员负责人员录用；
- f) 安全计算环境：对登录的用户进行身份识别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- g) 环境和资源：对物理环境划分不同等级安全区域，编制详细的资产清单；
- h) 监督和检查管理：有措施防止对信息处理设备的滥用，防止发生侵犯软件版权，定期进行安全管理检查和评估，对系统使用进行实时监测，对异常使用可启动应急响应。

6.4.2 B 级（中低风险场景）

在满足A级应用基础上，建议采取的措施包括：

- a) 风险管理：采用规范方法进行风险评估，建立风险管理的监督机制和管理程序；
- b) 抗攻击能力：至少在算法、模型和系统层面具备主动抵御各种攻击的能力；

- c) 安全管理制度：制定网络安全工作的总体方针和安全策略，对安全管理活动中的主要管理内容建立安全管理，对日常人员或操作人员执行的日常管理操作建立操作流程；
- d) 安全管理机构：设立网络安全管理工作的职能部门，设立系统管理员、审计管理员和安全管理员等岗位，并根据实际情况为各岗位配备专职或兼职专业人员；
- e) 安全管理人员：指定或授权专门的部门或人员负责人员录用，对被录用人员的身份、安全背景、专业资格或资质等进行审查；
- f) 安全计算环境：对登录的用户进行身份识别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- g) 环境和资源：对不同安全保护等级的安全区域进行标记管理；
- h) 监督和检查管理：制定加密控制规则，形成制度化的检查和改进措施。

6.4.3 C级（中风险场景）

在满足B级应用基础上，建议采取的措施包括：

- a) 风险管理：建立风险管理质量管理体系，进行独立审计，对关键区域或部位进行威胁分析和评估；
- b) 抗攻击能力：至少在算法、模型、系统和硬件层面具备主动抵御各种攻击的能力，对攻击行为进行监测；
- c) 安全管理制度：制定网络安全工作的总体方针和安全策略，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
- d) 安全管理机构：成立指导和管理网络安全工作的委员会或领导小组，设立网络安全管理工作的职能部门，设立系统管理员、审计管理员和安全管理员等岗位，并根据实际情况为各岗位配备专职专业人员；
- e) 安全管理人员：指定或授权专门的部门或人员负责人员录用，对被录用人员的身份、安全背景、专业资格或资质等进行审查，并与被录用人员签署保密协议；
- f) 安全计算环境：对登录的用户进行身份识别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，采用口令、密码技术、生物技术等两种或者以上组合的鉴别技术对用户进行身份鉴别；
- g) 环境和资源：实施不同等级安全区域的隔离管理，对重要数据的介质必须加密存储；
- h) 监督和检查管理：持续改进安全策略依从性检查过程。

6.4.4 D级（中高风险场景）

在满足C级应用基础上，建议采取的措施包括：

- a) 风险管理：针对风险管理活动实施全面质量管理，建立风险管理和质量管理体系，进行独立审计，对关键区域或部位进行威胁分析和评估；
- b) 抗攻击能力：至少在算法、模型、系统和硬件层面具备主动抵御各种攻击的能力，对攻击行为进行监测，并建立系统抗攻击自我优化的能力；
- c) 安全管理制度：制定网络安全工作的总体方针和安全策略，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
- d) 安全管理机构：成立指导和管理网络安全工作的委员会或领导小组，设立网络安全管理工作的职能部门，设立系统管理员、审计管理员和安全管理员等岗位，并为各岗位配备专职专业人员；

- e) 安全管理人员：指定或授权专门的部门或人员负责人员录用，对被录用人员的身份、安全背景、专业资格或资质等进行审查，并与被录用人员签署保密协议，从内部人员中选拔从事关键岗位的人员；
- f) 安全计算环境：对登录的用户进行身份识别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，采用口令、密码技术、生物技术等两种或者以上组合的鉴别技术对用户进行身份鉴别；
- g) 环境和资源：对物理安全的保障有持续的改善，对极为重要数据的介质可以使用数据隐藏技术进行存储；
- h) 监督和检查管理：持续改进安全策略依从性检查过程。

6.4.5 E级（高风险场景）

根据 6.1.2 中的 e) 项，高风险场景不建议使用人脸识别系统。

附 录 A

(资料性)

常见的应用人脸识别的公共场所分类说明

人脸识别常用的公共场所描述见表A.1～表A.3。

表A.1 公共场所分类说明表（社会管理）

| 细分场景 | 应用目的 | 必要性分析 | 替代方案 |
|------|---|---------------------------|--|
| 公共安全 | a) 在公共安全管理过程中可运用人脸识别系统辅助社会公共安全管理活动，对犯罪活动进行追踪、取证。具体应用可包括但不限于重要公共场所的公共安全视频监控、大型演出比赛等人票核验、移动警务、酒店入住登记。 b) 本细分场景下人脸识别系统使用目的可为安全防范、身份验证和人员管理。 | 个人人脸信息可与身份信息强相关且和行踪轨迹有关联。 | 本场景通常涉及重要的公众利益，此处人脸识别系统的应用通常难以被替代。 |
| 司法 | a) 在司法执行过程中可运用人脸识别系统辅助狱所内的管理。具体应用可包括但不限于狱所内人员管理、在押人员寻踪、智能点名等。 b) 本细分场景下人脸识别系统的主要目的可为身份验证和人员管理。 | 个人人脸信息可与身份信息强相关且与行踪轨迹有关联。 | 本场景涉及重要的公众利益，此处人脸识别应用通常难以被替代。 |
| 政务 | a) 在政府行政过程中可运用人脸识别系统辅助进行社会管理，使得政务更加便利和现代化。具体应用可包括但不限于应急响应、城管执法、政府办事身份核验（本地和远程）。 b) 本细分场景下人脸识别系统的主要目的可为身份验证。 | 个人人脸信息可与身份信息有强关联。 | 本场景涉及公众利益和重要个人利益，此处人脸识别通常可用其他生物识别信息或身份证件替代。 |
| 公共服务 | a) 在公共服务场景中可利用人脸识别辅助管理人员，避免匿名导致的公德暂失。具体应用可包括但不限于免费取厕纸、共享雨伞处利用人脸登记领取、垃圾分类居民行为监控、养老金领取管理、办税认证等。 b) 本细分场景下人脸识别系统的主要目的可为身份验证、人员管理。 | 个人人脸信息与身份信息弱相关。 | 本场景大多涉及较少的个人、公众利益。此处人脸识别通常可用证件、账号密钥、手机扫码等方式替代。 |
| 交通 | a) 在交通场所运用人脸识别系统辅助验票通关安检等环节顺利进行。具体应用可包括但不限于驾乘人员身份核验、闯红灯行人身份识别、机场人包绑定安检、城市轨道交通刷脸支付等。 b) 本细分场景人脸识别系统的主要目的可为安全防范和身份验证。 | 个人人脸信息可与身份信息有强关联。 | 本场景涉及公众利益和个人利益。此处人脸识别通常可用证件或者其他生物识别信息替代。 |
| 其他 | 社会管理中用到人脸识别的其他场所，利用人脸识别进行人员进出管理、安全管理、身份核验、行为分析、便民服务等。 | 根据具体的场景可进行具体分析。 | 根据具体的场景可进行具体分析。 |

表A.2 公共场所分类说明表（行业应用）

| 细分场景 | 应用目的 | 必要性分析 | 替代方案 |
|------|---|----------------------------|--|
| 金融 | a) 在金融行业中可利用人脸识别系统进行身份验证，便于进行与金融、支付相关的活动。具体应用可包括但不限于金融办事中利用人脸进行身份核验（本地/远程）、刷脸支付。 b) 本细分场景下人脸识别系统的主要目的可为身份验证。 | 个人人脸信息可与身份信息强相关且与财产信息有关联。 | 本场景大多涉及重要个人利益。此处人脸识别通常可用证件或者其他生物识别信息替代。 |
| 医疗 | a) 在医疗行业中可利用人脸识别系统进行身份验证，便于进行与医疗、就诊相关的活动。具体应用可包括但不限于无需证件单用人脸进行挂号、问诊、买药、医疗区无关人员管控等。 b) 本细分场景下人脸识别系统的主要目的可为身份验证。 | 个人人脸信息与身份信息强相关及与健康生理信息有关联。 | 本场景大多涉及重要个人利益。此处人脸识别通常可用证件或者其他生物识别信息替代。 |
| 教育 | a) 在课堂教学中可利用人脸识别系统辅助教学以及教学活动管理。具体应用可包括但不限于利用人脸和图像识别收集分析师生行为、在普通考试中进行人证核验和人脸上课点名。 b) 本细分场景下人脸识别系统的主要目的可为身份验证、人员管理。 | 个人人脸信息与身份信息强相关。 | 本场景大多涉及较少个人利益，部分具体应用甚至有损害个人利益的行为。此处人脸识别通常可用证件或者其他生物识别信息替代。 |
| 建筑 | a) 在建筑环境中可运用人脸识别系统进行辅助管理，具体应用可包括：对内部人员进行管理并且防止未经授权人员的进入，保障工地安全，工人考勤，关键责任人实时在岗，通过记录考勤辅助进行人力成本和效率分析等。 b) 本细分场景下人脸识别系统的主要目的可为人员管理、身份验证和行为安全。 | 个人人脸信息可与身份信息强相关。 | 本场景大多涉及较少个人、公众利益。此处人脸识别通常可用证件、智能手环或其他智能终端替代。 |
| 房地产 | a) 在房地产环境中可运用人脸识别系统辅助进行物业管理、房地产经营等。具体应用形式包括：对内部人员进行管理并且防止未经授权人员的进入、在取得用户授权的前提下，通过人脸识别进行身份确认等。 b) 本细分场景下人脸识别系统的主要目的可为人员管理和身份验证。 | 个人人脸信息可与身份信息强相关。 | 本场景大多涉及较少个人、公众利益。此处人脸识别通常可用证件或者其他生物识别信息替代。 |
| 商业 | a) 在商业场所或各种软硬件中可利用人脸识别技术进行行为分析、会员身份验证以及其他人脸识别应用相关体验。具体应用可包括但不限于人证核验或活体检测、收集分析顾客行为、演出比赛实名购票验票提防黄牛、景区健身房等会员刷脸进入、内容智能识别、人脸相关增强现实（AR）服务。 b) 本细分场景下人脸识别系统的主要目的可为商业分析、身份验证、人员管理。 | 个人人脸信息与身份信息弱相关或不相关。 | 本场景大多涉及个人利益，部分具体应用甚至有损害个人利益的行为。此处人脸识别通常可用证件或者其他生物识别信息替代。 |

表 A.2 公共场所分类说明表（行业应用）（续）

| 细分场景 | 应用目的 | 必要性分析 | 替代方案 |
|------|---|---------------------|--|
| 娱乐 | a) 在休闲娱乐场所采集个人人脸信息实现娱乐、统计客流量、分析顾客面部情绪等目的。具体应用包括进行AI换脸、面部情绪分析、会员管理、客流分析、年龄识别等。 b) 本细分场景下人脸识别系统的主要目的可为娱乐体验、统计客流量、分析顾客面部情绪。 | 个人人脸信息与身份信息弱相关或不相关。 | 本场景大多涉及个人利益，部分具体应用甚至有损害个人利益的行为。此处人脸识别通常可不使用。 |
| 其他 | 行业应用中用到人脸识别的其他场所，利用人脸识别进行业务分析、人员管理、客流分析、身份核验、客户行为分析、表情分析、VIP服务等。 | 根据具体的场景可进行具体分析。 | 根据具体的场景可进行具体分析。 |

表A.3 公共场所分类说明表（其他）

| 细分场景 | 应用目的 | 必要性分析 | 替代方案 |
|------|---|---------------------------|--|
| 社区 | <p>a) 在社区场景中可利用人脸识别进行对于人员进行身份核实和管理。具体应用可包括可但不限于住宅楼栋、公共活动中心、物业办公室、车库出入口、安防中心控制室、重要设备机房以及住宅楼栋顶层平台处的监控、小区业主出入口的监控和小区楼栋以及主出入口处的门禁、来访人员管理、对不同身份的人提供人性化服务等。</p> <p>b) 本细分场景下人脸识别系统的主要目的可为安全防范、身份验证。</p> | 个人人脸信息与身份信息弱相关，可与行踪轨迹有关联。 | 本场景监控类人脸识别应用难以被替代，但是门禁类可用其他证件、账号密钥等方式替代。 |
| 园区 | <p>a) 在园区场景中可利用人脸识别系统辅助进行园区管理。具体应用包括：园区门禁无感通行；访客系统；公共卫生防范系统；园区人脸识别机器人测体温、面对面沟通服务等；园区智慧停车系统刷脸快速找车；园区安全防范、园区支付刷脸系统等。</p> <p>b) 本细分场景下人脸识系统的主要目的为身份验证、安全防范、智能支付等。</p> | 个人人脸信息与身份信息弱相。 | 本场景安全防范类人脸识别应用难以被替代，其他如门禁类、刷脸找车等可用其他证件、账号密钥、刷二维码等方式替代。 |

参 考 文 献

- [1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
 - [2] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
 - [3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
 - [4] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
 - [5] GB/T 32914—2016 信息安全技术 信息安全服务提供方管理要求
 - [6] GB/T 35273—2020 信息安全技术 个人信息安全规范
 - [7] GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求
-