ICS 35.240
CCS L71

DB31

上　海　市　地　方　标　准

DB 31/T 1554—2025

人脸识别系统工程建设规范

Specification for engineering construction of face recognition system

2025-03-26 发布　　2025-07-01 实施

上海市市场监督管理局　　发 布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语、定义和缩略语 2
4　建设总体要求 3
5　建设方案要求 4
6　建设要求 5
7　信息安全要求 9
8　工程技术检验要求 10
9　系统验收要求 11
10　系统运维要求 11
附录 A（资料性）　人脸识别系统的应用结构 12
附录 B（资料性）　人脸识别系统的人脸数据来源与典型应用场景 13
附录 C（资料性）　人脸信息安全管理机制 14
参考文献 15

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。

本文件与DB31/T XXXX—202X 《人脸识别系统工程验收规范》关联使用。

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：公安部第三研究所、上海市质量和标准化研究院、上海市人工智能行业协会、上海市公安局治安总队、上海华东电信研究院、上海计算机软件技术开发中心、上海骏聿数码科技有限公司、杭州臻稀生物科技有限公司、上海依图网络科技有限公司、杭州锘崴信息科技有限公司、蚂蚁金融服务集团、海康威视数字技术（上海）有限公司、上海商汤智能科技有限公司。

本文件主要起草人：刘彩霞、谢芳艺、张正敏、焦志皓、刘丹丹、钟俊浩、沈涛、陈曦、周迅、常永波、彭莉、陈敏刚、白雪松、马玉、阮系真、赵春昊、李帜、林冠辰、同刚、俞凯。

引　言

人脸识别作为一种使用便捷的非接触式生物特征识别技术，在安防、金融、教育、旅游、零售等多个领域得到了广泛应用。已经大量部署的各类人脸识别系统在宾旅馆业人员入住身份管理、民航旅客身份核验、铁路旅客身份核验、金融业务远程支付、重点区域人脸动态布控、企事业单位日常考勤等工作中发挥了重要作用。尤其是在2017年底中共中央总书记习近平在主持中共中央政治局就实施国家大数据战略的第二次集体学习时明确提出推动实施国家大数据战略以来，大数据、云计算、人工智能等新兴技术快速崛起，人脸识别系统也随之快速发展成为集成大数据、云计算、信息安全等多领域技术的一种典型规模化人工智能综合应用，并由此带来涉及各种产品应用模式、各类行业领域、各种应用场景的人脸数据库智能交互、联网接入智能应用、人脸数据安全保障及系统整体管理与运维等建设应用问题。

2020年3月6日发布、2020年10月1日正式实施的GB/T 35273—2020《信息安全技术个人信息安全规范》国家标准规定了开展收集、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。该标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，规范个人信息控制者在收集、存储、使用、共享、转让、公开、披露等信息处理环节中的相关行为，旨在控制个人信息非法收集、滥用、泄漏等乱象，最大限度地保障个人的合法权益和社会公共利益。最高人民法院审判委员会2021年6月8日发布、2021年8月1日正式施行的《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》（法〔释〕〔2021〕15号），进一步明确了在审理使用人脸识别技术处理个人信息相关民事案件过程中的侵权行为界定标准。2023年8月08日，国家互联网信息办公室根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国信息保护法》等法律法规，起草了《人脸识别技术应用安全管理规定（试行）》（征求意见稿），旨在规范人脸识别技术应用，保护个人信息权益及其他人身和财产权益。上海市市场监督管理局2024年4月02日发布了DB31/T 1467—2024《公共场所人脸识别分级分类应用指南》，该标准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，已于2024年7月01日正式实施。

上海作为国际化大都市，其各项社会管理工作亟需人脸识别等生物识别科技手段辅助进行人员身份验证和身份辨识，在无序建设使用人脸识别系统存在诸多不确定性风险的背景下，本文件以DB 31/T 1467—2024明确的公共场所人脸识别分类分级应用主体的合规性为前提对人脸识别系统工程建设进行标准化规定。

本文件与上海市地方标准DB31/T XXXX—202X《人脸识别系统工程验收规范》配套使用，共同促进上海市人脸识别系统的工程建设管理、工程检验与验收，助力保障人脸数据采集、使用的合法合规性。

人脸识别系统工程建设规范

1 范围

本文件规定了人脸识别系统工程的建设总体要求、建设方案要求、建设要求、信息安全要求、工程技术检验要求、系统验收要求以及系统运维要求。

本文件适用于上海市采用人脸识别技术进行人员身份验证或身份辨识的各类人脸识别系统的设计、建设、验收和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 26237.5 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

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 31488 安全防范视频监控人脸识别系统技术要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35290 信息安全技术 射频识别（RFID）系统安全技术规范

GB/T 35678 公共安全 人脸识别应用 图像技术要求

GB 37300 公共安全重点区域视频图像信息采集规范

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

GB/T 38671 信息安全技术 远程人脸识别系统技术要求

GB/T 40694.5 信息技术 用于生物特征识别系统的图示、图标和符号 第5部分：人脸应用

GB/T 41772 信息技术 生物特征识别 人脸识别系统技术要求

GB/T 41819 信息安全技术 人脸识别数据安全要求

GB 50057 建筑物防雷设计规范

GB 50311 综合布线系统工程设计规范

GB 50343 建筑物电子信息系统防雷技术规范

GB 50348 安全防范工程技术标准

GA 450 台式居民身份证阅读器通用技术要求

GA/T 1093 出入口控制人脸识别系统技术要求

GA/T 1126 近红外人脸识别设备技术要求

GA 1153 手持式居民身份证阅读器

GA/T 1154.4 视频图像分析仪 第4部分：人脸分析技术要求

GA/T 1324 安全防范 人脸识别应用 静态人脸图像采集规范

GA/T 1325 安全防范 人脸识别应用 视频图像采集规范

GA/T 1326—2017 安全防范 人脸识别应用 程序接口规范

GA/T 1755—2020 安全防范 人脸识别应用 人证核验设备通用技术要求

DB 31/T 1240.2　公共数据共享交换工作规范　第2部分：平台接入技术要求
DB 31/T 1467—2024　公共场所人脸识别分级分类应用指南
DB 31/T XXXX—202X　人脸识别系统工程验收规范

3　术语、定义和缩略语

3.1　术语和定义

GB/T 35273、GB/T 41819界定的以及下列术语和定义适用于本文件。

3.1.1

人脸数据　face data

以电子或其他方式记录的、能够藉以识别特定自然人身份或反映特定自然人活动情况的人脸图像、人脸视频、人脸样本、人脸参考、人脸特征项或人脸特性的通称。

[来源：GB/T 37036.3—2019，3.3，有修改]

3.1.2

人脸识别系统　face recognition system

对特定自然人进行人脸验证或人脸辨识，以提供人脸识别应用服务的信息系统。

[来源：GB/T 41722—2022，3.2，有修改]

3.1.3

人脸关联数据　face related data

与人脸数据对应的个人信息。

注：包括但不限于姓名、身份证件号码等身份数据、拍摄时间地点等活动轨迹数据及联系方式等档案数据。

[来源：GB/T 41786—2022，3.2.29，有修改]

3.1.4

人脸信息　face information

人脸识别系统产生或关联的信息。

注：包含但不限于人脸数据和人脸关联数据、系统输出的人脸识别结果、智能分析结果等。

3.1.5

人脸数据主体　face data subject

人脸数据所标识或关联的自然人。

3.1.6

人脸信息控制者　face information controller

有权限决定人脸数据处置目的、方式等的组织或个人。

注：包括系统使用者、系统实施者、系统运维者及系统管理者。

3.2　缩略语

下列缩略语适用于本文件。

FAR：错误接受率（False Acceptance Rate）
FRR：错误拒绝率（False Rejection Rate）
FPIR：错误接受辨识率（False Positive Identification Rate）
FNIR：错误拒绝辨识率（False Negative Identification Rate）
LDER：活体检测错误率（Liveness Detection Error Rate）
PADER：呈现攻击检测错误率（Presentation Attack Detection Error Rate）

UPS：不间断电源（Uninterruptible Power Supply）
URL：统一资源定位系统（Uniform Resource Locator）
Web：全球广域网（World Wide Web）

4 建设总体要求

4.1 主体资质

人脸识别系统的建设和使用主体应具有良好的信用，并应按照GB/T 20269建立和实施了信息系统安全管理，宜取得信息安全管理体系相关资质证书。通过集成商或系统供应商进行人脸识别系统工程实施的，工程实施主体宜具备信息安全管理体系相关资质证书。

4.2 风险评估

4.2.1 人脸识别系统建设主体应对人脸识别用途、技术应用、数据安全进行风险评估，保障人脸识别用途的合法性、人脸识别技术应用的正当性、人脸生物特征数据的安全性。

4.2.2 在公共场所建设人脸识别系统时，建设使用主体应按照 DB31/T 1467—2024 中 5.2 的要求按照应用目的风险、底库规模风险、覆盖密度风险、管理水平风险、网络环境风险等 5 个风险要素对相应公共场所的人脸识别应用进行风险等级评估。当综合风险值评估结果对应等级为 E 级（高风险场景）时，系统的建设使用主体应终止人脸识别系统工程建设规划；当综合风险值评估结果对应等级为 A 级（低风险场景）、B 级（中低风险场景）、C 级（中风险场景）、D 级（中高风险场景）时，系统的建设使用主体应分别按照 DB31/T 1467—2024 中 6.4.1、6.4.2、6.4.3、6.4.4 的要求采取相应措施后再启动人脸识别系统工程建设事宜。

4.3 设计评审

人脸识别系统工程建设主体在建设前应预先自行进行建设方案设计或委托具备资质能力的专业机构进行建设方案设计，设计完成后应组织专家对建设方案进行专业技术评审。

4.4 人脸识别比对数据源合规

4.4.1 人脸识别系统应使用个人单独同意提供的个人各类证件表面照片、芯片内数字照片或自建数据库人脸照片等作为比对数据源。法律、行政法规规定不必取得个人同意的除外。

4.4.2 使用人脸识别技术验证个人身份、辨识特定自然人的，宜优先使用国家人口基础信息库、国家“互联网+”可信身份认证平台、国家网络身份认证公共服务等权威渠道。

4.5 人脸识别用户知情权合规

4.5.1 使用人脸识别技术处理人脸信息应取得个人的单独同意或者依法取得书面同意。法律、行政法规规定不必取得个人同意的除外。

4.5.2 使用不满十四周岁未成年人人脸信息的，应取得未成年人的父母或者其他监护人的单独同意或者书面同意。

4.5.3 宾馆、银行、车站、机场、体育场馆、展览馆、博物馆、美术馆、图书馆等经营场所中，个人自愿选择使用人脸识别技术验证个人身份的，应确保个人充分知情并在个人主动参与的情况下进行，验证过程中应以清晰易懂的语音或者文字等方式即时明确提示身份验证的目的。

4.6 人脸识别使用场所合规

4.6.1　不应在旅馆客房、公共浴室、更衣室、卫生间及其他可能侵害他人隐私的场所安装图像采集、个人身份识别设备。

4.6.2　宾馆、银行、车站、机场、体育场馆、展览馆、博物馆、美术馆、图书馆等经营场所，除法律、行政法规规定应使用人脸识别技术验证个人身份的，不应以办理业务、提升服务质量等为由强制、误导、欺诈、胁迫个人接受人脸识别技术验证个人身份。

4.6.3　不应在商务楼宇、居民社区等物业管理区域使用人脸识别技术验证个人身份作为出入建筑物的唯一方式。个人不同意通过人脸信息进行身份验证的，物业服务企业等建筑物管理人应提供其他合理、便捷的身份验证方式。

4.6.4　在公共场所安装图像采集、个人身份识别设备，应为维护公共安全所必需，应遵守国家有关规定，应设置显著提示标识。

4.6.5　在公共场所、经营场所使用人脸识别技术远距离、无感式辨识特定自然人，应为维护国家安全、公共安全或者为紧急情况下保护自然人生命健康和财产安全所必需，并由个人或者利害关系人主动提出。

5　建设方案要求

5.1　工程概况

工程概况应包含以下内容：

a）　人脸识别用途及目的；

b）　人脸识别系统建设必要性分析；

c）　人脸识别模式。

注：人脸识别模式包括1:1、1:N、n:N等模式及同时兼具以上两种及以上的混合模式。

d）　拟使用的人脸识别比对数据源；

e）　人脸识别系统联网应用方式；

f）　人脸识别系统安装场所现场勘察结果及合规性分析。

5.2　设计说明

设计说明应包含以下内容。

a）　人脸识别系统应用结构及功能业务流程。常规应用结构及功能业务流程参见附录A。

b）　人脸识别系统与相关主要设备的技术指标。

c）　设备选型及其功能、性能、安全性相关的标准符合性证明材料。

d）　人脸信息处理方式。

e）　人脸信息安全性保障制度。

f）　个人信息保护影响评估事项，包括但不限于：

1）　是否符合法律、行政法规的规定和国家标准的强制性要求，是否符合伦理道德；

2）　处理人脸信息是否具有特定的目的和充分的必要性；

3）　是否限于实现目的所必需的准度、精度及距离要求；

4）　采取的保护措施是否合法有效并与风险程度相适应；

5）　发生或者可能发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、非法利用的风险以及可能造成的危害；

6）　可能对个人权益带来的损害和影响，以及降低不利影响的措施是否有效。

5.3　运维管理

运维管理应包含以下内容：

a） 日常管理责任人员信息；

b） 应急处置预案；

c） 巡检方案；

d） 故障解决方案。

6 建设要求

6.1 系统集成

需接入指定管理平台的人脸识别系统应支持接口协议调整，并应支持通过特定接口协议被指定管理平台集成和调用。

6.2 人脸数据获取

6.2.1 人脸识别系统的人脸数据获取应符合 GB/T 35273 中个人信息的收集相关要求。

6.2.2 应仅采集与实现人脸识别系统的应用业务功能有直接关系的人脸信息。

6.2.3 应满足自动采集所必需的最低频率与间接获取最少数量的人脸信息。

6.2.4 应用于非社会公共安全或非司法目的时，应采用需要人脸数据主体主动配合的措施。

6.2.5 应用于非社会公共安全或非司法目的时，应告知被收集者（包含人脸数据主体、人脸信息控制者）获取人脸数据及人脸关联数据的规则，应包括但不限于收集者信息、收集目的、人脸数据类型和数量、处理方式、存储时间等信息，并征得被收集者明示同意。

6.2.6 获取的人脸数据与人脸关联数据应包括但不限于证件信息、凭证信息、离线人脸采集设备获取的人脸数据、在线人脸采集设备获取的人脸数据、离线存储的数据库获取的人脸数据、远程数据库或云数据库获取的人脸数据、第三方数据库获取的人脸数据等；具体数据来源及其典型应用场景见附录 B。

6.2.7 应将人脸数据与人脸关联数据采用唯一的个人信息标识进行绑定，应支持数据获取过程的可追溯性。

6.2.8 应在获取人脸数据后按人脸信息安全管理机制自动删除人脸原始图像、图片、视频，经过匿名化处理的人脸信息除外。

6.2.9 应在获取人脸关联数据后按人脸信息安全管理机制自动删除残留个人敏感信息，应包括但不限于个人身份信息、手机号、证件号、个人财产信息等。

6.2.10 用于社会公共安全防范的人脸识别系统的静态人脸图像采集应符合 GA/T 1324 的要求，视频人脸图像采集应符合 GA/T 1325 的要求，重点区域视频图像信息采集应符合 GB 37300 的要求。

6.3 人脸数据格式

用于社会公共安全防范的人脸识别系统的人脸图像数据格式应符合 GB/T 35678 的要求。其他人脸识别系统的人脸数据格式应符合 GB/T 26237.5 的要求。

6.4 程序接口

用于社会公共安全防范的人脸识别系统的程序接口应符合GA/T 1326的要求，其他人脸识别系统的程序接口应符合管理方的要求。

6.5 设备选型

6.5.1 应依据应用场景和使用模式选择符合 GB/T 31488 的视频监控人脸识别系统、符合 GA/T 1755—

2020 的人证核验设备、符合 GA/T 1093 的出入口控制人脸识别系统、符合 GA/T 1126 的近红外人脸识别系统、符合 GB/T 37036.3—2019 的人脸识别移动设备、符合 GB/T 38671 的远程人脸识别系统或符合 GB/T 41772 的人脸识别系统。

6.5.2 需同时采集人员居民身份证信息等关联数据的，选用的台式居民身份证阅读器应符合 GA 450 的要求，选用的手持式居民身份证阅读器应符合 GA 1153 的要求。

6.5.3 需同时采集人员护照、驾驶证、工作证、学生证、社保卡、出入门禁卡信息等关联数据的，选用的识读设备应符合 GB/T 35290 的基本级要求。

6.5.4 选择按照国家有关规定列入网络关键设备和网络安全专用产品目录的图像采集设备、个人身份识别设备时，应审核其是否由具备资格的机构认证合格或者经检测确认符合相关国家标准强制性要求的证明文件。

6.6 人脸解析

6.6.1 人脸识别系统应能进行人脸检测。

6.6.2 人脸识别系统应能进行人脸特征提取，且符合下列要求：

a） 关联个人信息标识；

b） 生成可更新、不可逆、不可链接的人脸特征；

c） 支持对图像中两眼间距小于或等于60像素的人脸提取特征；

d） 人脸特征提取成功率大于或等于99.99％。

6.6.3 人脸识别系统应能对采集的人脸数据进行质量判断，并对质量判断结果不通过的人脸数据主体进行重新采集。

6.6.4 用于社会公共安全防范的人脸识别系统，宜能对人脸目标进行跟踪。

6.6.5 用于社会公共安全防范的人脸识别系统，宜具有人脸属性分析和属性描述功能，且符合下列要求：

a） 可描述属性包括但不限于年龄段、佩戴的附属物（包含口罩、眼镜）、是否有胡须等；

b） 对于眼间距小于或等于60像素的人脸，平均属性分析准确率应大于或等于85％，单项属性分析准确率应大于或等于75％；

c） 具备人脸属性分析功能的设备至少符合GA/T 1154.4的相关要求。

6.7 人脸数据存储

6.7.1 人脸识别系统应按人脸信息安全管理机制设定人脸信息存储规则。

6.7.2 除法定条件或者取得个人单独同意外，不应保存人脸原始图像、图片、视频，经过匿名化处理的人脸信息除外。

6.7.3 人脸信息存储规则应符合下列要求：

a） 采用物理或逻辑隔离方式分别存储经过匿名化处理的人脸数据与人脸关联数据；

b） 采用国产商用密码算法对规定的人脸信息进行加密存储，且存储介质应授权可控；

c） 因特定管理目的确需存储匿名化处理的人脸数据与人脸关联数据时，支持经授权后查询和删除；

d） 人脸验证或人脸辨识后，自动删除证件原始图像、人脸图像等带有个人身份信息的人脸数据；

e） 具备人脸数据库关联的系统，支持人脸特征项存储到人脸数据库，并返回人脸参考标识符；

f） 在供电电源掉电或更换电池时，已存储的匿名化处理的人脸数据与人脸关联数据不丢失。

6.7.4 人脸识别系统应具备数据备份和容灾备份功能。

6.8 人脸注册(仅适用于关联使用人脸数据库的系统)

6.8.1　人脸识别系统应具有人脸注册功能。
6.8.2　人脸识别系统宜支持现场注册或导入图像进行单张或批量人脸注册。
6.8.3　人脸识别系统宜支持调用人脸数据库并进行人脸注册。
6.8.4　人脸识别系统宜支持远程采集或导入图像进行人脸注册。
6.8.5　人脸识别系统宜支持单个用户注册多张人脸图像。
6.8.6　人脸识别系统宜支持不同数据来源或不同采集设备的人脸注册。
6.8.7　人脸识别系统宜支持给出注册过程提示。
6.8.8　当使用符合 GA/T 1755—2020 中 5.1.3.2 目标集要求的人脸图像进行人脸注册时，人脸注册成功率应大于或等于 99 %。

6.9　人脸验证（仅适用于具备 1:1 人脸识别模式的系统）

6.9.1　人脸识别系统应具有人脸验证功能。
6.9.2　人脸识别系统应将通过采集获取的人脸特征项与证件读取或与数据库预注册获取的人脸特征项进行 1:1 比对,并给出比对相似度与人脸验证结果。
6.9.3　人脸识别系统应支持以导出或上传方式输出比对相似度得分与人脸验证结果。
6.9.4　在使用符合 GA/T 1755—2020 中 5.1.3 测试数据库要求进行测试时，在同一设定阈值条件下，人脸验证性能应符合表 1 的要求。

表1　人脸验证性能要求

测试数据库规模	性能要求	应用场景示例
千量级	当FAR≤0.1 %时，FRR≤2 %。	附B 表B.1中对应的人脸验证
	当FAR≤0.01 %时，FRR≤3 %。	
十万量级	当FAR≤0.001 %时，FRR≤3 %。	附录B 表B.1中对应的人脸验证
	当FAR≤0.0001 %时，FRR≤5 %。	
注：测试数据库包括个人数据的目标集和探测集，一般规模量级以N来衡量。其中N为目标集中不重复的测试人员数量，M为探测集中的测试人脸图像数量，M≥10 N。		

6.9.5　人脸验证时，人脸识别系统的平均响应时间应小于或等于 2 s。

6.10　人脸辨识（仅适用于具备 1:N 或 n:N 人脸识别模式的系统）

6.10.1　人脸识别系统应具有人脸辨识功能。
6.10.2　人脸识别系统应将通过获取的人脸特征项与人脸数据库中的人脸特征项进行 1:N 比对，并给出比对相似度与人脸辨识结果，其中人脸辨识结果先确定候选者列表长度，并排序输出候选者列表。
6.10.3　在 1:N 人脸比对模式下，人脸识别系统应将给定小规模的人脸数据库的人脸特征项与已存储或调用的人脸数据库中的人脸特征项进行 n:N 比对，并给出相似度与人脸辨识结果，其中人脸辨识结果应先确定人员名单与候选者对应关系及列表长度，并排序输出按人员名单形成的候选者列表。
6.10.4　人脸识别系统应支持以导出或上传方式输出比对相似度与人脸辨识结果。

6.10.5　在使用符合 GA/T 1755—2020 中 5.1.3 测试数据库要求进行测试时，在同一设定阈值条件下，人脸辨识性能应符合表 2 的要求。

表2　人脸辨识性能要求

测试数据库规模	列表长度（K）	性能要求	应用场景示例
千量级 （闭集测试）	1，5，10	当FPIR≤0.1 %时，FNIR≤5 %。	附录B 表B.1中对应的人脸辨识
		当FPIR≤0.01 %时，FNIR≤10 %。	
千量级 （开集测试）	1，5，10	当FPIR≤0.1 %时，FNIR≤5%。	附录B 表B.1中对应的人脸辨识
		当FPIR≤0.01 %时，FNIR≤10 %。	
注1：测试数据库包括个人数据的目标集和探测集，一般规模量级以N来衡量；其中N为目标集中不重复的测试人员数量，M为探测集中的测试人脸图像数量，M大于或等于10 N。 注2：闭集测试是测试人脸图像的人员确定为隶属于人脸数据库中的人员，且和已包含在人脸数据库内的人脸图像不同；开集测试是指测试人脸图像对应的人员不一定隶属于人脸数据库中的人员。 注3：列表长度K，指的是前K命中率，如K=1，表示首位命中率；K=5，表示前五位命中率。			

6.10.6　人脸辨识时，使用千量级数据库进行测试条件下，人脸识别系统的平均响应时间应小于或等于 3 s。

6.11　人脸防伪检测

6.11.1　人脸识别系统宜具备人脸防伪检测功能。

6.11.2　人脸识别系统宜支持活体检测。

6.11.3　人脸识别系统应能防静态纸质图像、静态电子图像、动态电子图像的二维假体及三维塑料面具、三维纸张面具、三维硅胶面具、三维树脂头模等人脸照片、人脸视频、仿真人脸面具、仿真人脸头模假体呈现攻击，其他防假体呈现攻击方式可参见 GB/T 41987—2022。

6.11.4　使用二维假体及三维塑料面具、三维纸张面具进行假体攻击时，在同一设定阈值条件下，PADER 小于或等于 1 %时，LDER 应小于或等于 5 %。

6.12　系统管理

6.12.1　人脸识别系统应支持设置阈值，包括但不限于质量判断阈值、人脸比对的相似度阈值。

6.12.2　人脸识别系统应具有故障提示功能，出现故障时能给出故障提示。

6.12.3　人脸识别系统应具有中文交互界面。

6.12.4　人脸识别系统应具有日志管理功能，能提供日志记录和追溯人脸数据的处理过程，包括但不限于设备标志、识别时间、个人信息标识、识别结果等信息。

6.12.5　人脸识别系统应具有用户管理功能，经授权后能对用户信息进行增加、修改、删除、查询、停止/启用等操作。

6.12.6　人脸识别系统应具有权限管理功能，能对人脸信息控制者、人脸数据主体、系统使用主体与系统实施主体等角色配置权限。

6.12.7　人脸识别系统应具有接口配置功能，支持对应用开发接口、协议接口、硬件接口等进行配置。

6.13　应用接口

6.13.1　人脸识别系统应具备应用开放接口，包括但不限于提供人脸注册服务、人脸验证服务、人脸辨识服务、人脸防伪检测服务、人脸解析服务等人脸应用服务；应用程序接口应符合 GA/T 1326—2017 中 5.4 的相关要求。

6.13.2　人脸识别系统应具备联动控制接口，应包括但不限于防盗报警系统、出入口控制闸机、门禁考勤机、酒店自助入住终端、消防控制系统等。

6.13.3　人脸识别系统应具备数据库关联接口，应具备数据支撑能力，表字段数量、长度和数据类型等应符合数据库类型接入要求。

6.14　联网接入（仅适用于具备联网应用需求的系统）

6.14.1　前置机交换接入方式

人脸识别系统应通过人脸数据库表或应用交互文件目录进行数据交换，各接入端应通过桥接方式获取人脸数据库表内容或文件，并向前置的人脸数据库表或前置文件目录推送数据；涉及公共场所视频图像联网的，应符合GB/T 28181的相关要求。

6.14.2　服务接口交换接入方式

人脸识别系统应以Web服务作为系统与各接入端之间数据获取和推动的接口，在代理业务系统提供的Web服务，应对外隐藏该Web服务的真实URL，应使用代理URL访问业务系统的真实Web服务以达到数据交换目的。

6.14.3　共享交换

人脸识别系统的共享交换应提供统一服务调用接口和数据共享方式。接入上海市数据共享交换平台的人脸识别系统应符合DB31/T 1240.2的相关要求。

6.15　施工安装

6.15.1　人脸识别系统的管理子系统、数据服务设备、集成应用系统等相关管理与应用组件应设置在独立控制室，应具备对各系统操作、记录、显示及集成地理信息应用控制功能。

6.15.2　应部署有线、无线通讯方式；应具备交换机的，支持路由功能和三层交换功能。

6.15.3　人脸识别系统应用于公共场所的，应在显著位置设置明显的人脸识别应用警示标志；使用人脸识别的图示、图标和符号应符合 GB/T 40694.5 的相关要求。

6.15.4　人脸识别系统的综合布线符合 GB 50311 和 GB 50348 的规定，重点部位布设线缆应采用暗敷方式，前端布线标准应不低于超五类线缆。

6.15.5　人脸识别系统宜采用独立集中供电模式。

6.15.6　人脸识别系统宜配备 UPS 电源。

7　信息安全要求

7.1　概述

面向社会公众提供人脸识别技术服务的，相关技术系统应符合GB/T 22239的网络安全等级保护第三级及以上要求，并采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。

7.2 人脸信息安全管理机制

7.2.1 人脸识别系统使用主体应制定人脸数据的管理规定、处置规则与处理权限等安全管理制度。
7.2.2 具有数据库的人脸识别系统应设置专门的人脸信息保护机构或保护责任人，应明确对应的职责要求。
7.2.3 人脸识别系统使用主体应针对人脸数据泄露、篡改、丢失、损毁或被非法获取、非法利用等安全风险，制定应急预案与相应的处理措施。
7.2.4 人脸识别系统使用主体应建立保障人脸数据主体权利的机制，保障人脸数据主体的知情同意、授权、人脸数据处理等方面权利，并及时响应相应的请求。
7.2.5 针对社会管理及重点行业应用的人脸识别系统，使用主体应建立与相关主管部门的上报备案机制，确保人脸数据安全合规性。
7.2.6 人脸识别系统使用主体应每年对图像采集设备、个人身份识别设备的安全性和可能存在的风险进行检测评估，并根据检测评估情况改进安全策略，调整置信度阈值，采取有效措施保护图像采集设备、个人身份识别设备免受攻击、侵入、干扰和破坏。
7.2.7 人脸信息安全管理机制可参照附录C进行设置。

7.3 人脸数据安全

7.3.1 人脸识别系统的人脸数据安全应符合GB/T 41819中相关要求。
7.3.2 不宜采集与提供服务无关的人脸信息，确需采集的，应在15 d内删除或者进行匿名化处理。
7.3.3 应采用国产商用密码算法加密存储人脸数据。
7.3.4 应对身份标识信息、人脸特征序列数据等敏感信息采用加密机制和身份鉴别授权机制管理，确保其不被非授权的访问、修改或删除。
7.3.5 应在传输过程中对人脸数据进行完整性与机密性保护。
7.3.6 在人脸信息安全管理机制中发生异常情况时，应在15 d内删除人脸数据并确保不可恢复。
7.3.7 应依据人脸数据更新策略，使用已通过人脸验证或人脸辨识的不可逆人脸数据替换数据库中对应人员的原有人脸数据。

7.4 安全防护

7.4.1 应对提出人脸识别相关应用要求的用户进行身份鉴别。
7.4.2 应在人脸信息比对失败时返回比对失败信息，记录失败时间并予以告警。
7.4.3 应采取I/O接口屏蔽、网络资源访问控制等入侵检测和防御等措施保护人脸信息安全。
7.4.4 应对人脸识别结果输出和识别记录导出提供完整性保护和机密性保护。
7.4.5 使用移动终端或远程工作时，应建立信息安全必要保护措施。
7.4.6 应具有安全审计功能，产生审计记录，并严格限制未经授权用户访问。

8 工程技术检验要求

8.1 人脸识别系统应在安装调试完成后进行为期7 d～30 d的试运行，经试运行达到设计、使用要求，并获建设单位认可后，应出具试运行报告。

8.2 人脸识别系统建设和使用主体应在工程竣工验收前，依据本文件第6章和第7章的相关要求，按照DB 31/T XXXX—202X中第7章的试验方法对人脸识别系统的功能、性能及信息安全管理要求进行工程技术检验。

9 系统验收要求

工程技术检验合格后，应按DB 31/T XXXX—202X的要求进行系统验收。

10 系统运维要求

10.1 应建立人脸识别系统运行维护保障的长效机制，设授权的专人负责日常管理及人脸数据安全管理。

10.2 应制定人脸识别系统应急处置预案和故障解决方案，出现故障时及时修复，一般情况修复时间应在2 h内，期间存储的人脸数据不应丢失。

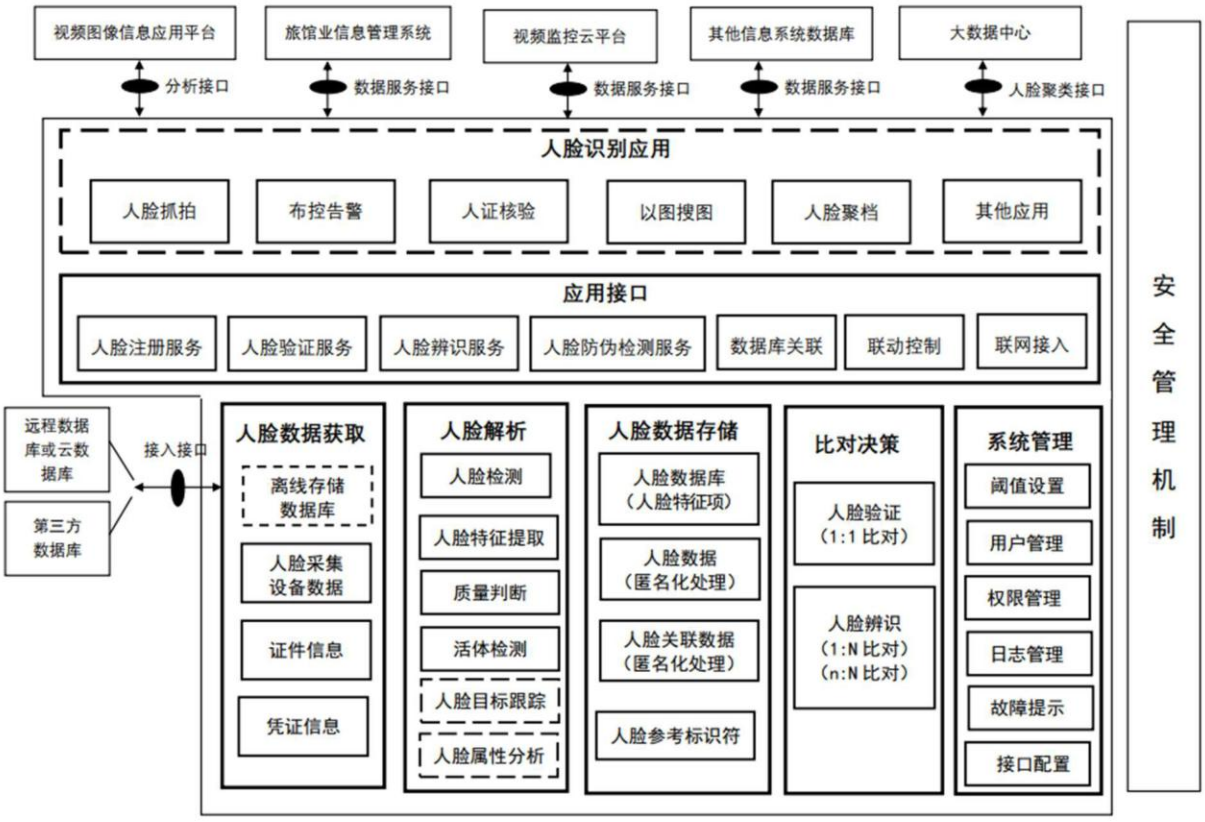
10.3 重点单位重点部位人脸采集设备前端抓拍图像效果，出现图像偏移、模糊等情况时应及时检修校正。

10.4 应进行例行巡检，保障系统软件正常运行。

10.5 应对数据进行定期巡检，确保数据的可用、准确、完整、安全。

附 录 A
（资料性）
人脸识别系统的应用结构

人脸识别系统的应用结构如图A.1所示。



图A.1 人脸识别系统的应用结构

附 录 B
（资料性）
人脸识别系统的人脸数据来源与典型应用场景

人脸识别系统的人脸数据来源与典型应用场景详见附表B.1。

表B.1 人脸识别系统的人脸数据来源与典型应用场景

类型	数据来源	典型应用场景
现场 人脸验证	采集对象需配合采集人脸图像，采用人脸确认比对方式识别。	银行柜台业务办理、社保实名认证、场馆安保管理、演出比赛人票核验、酒店入住登记等。
远程 人脸验证	图像采集现场无人工监管，应有活体检测要求。	金融网络远程开户、社保网络实名认证、远程考场考生身份核验、征信报告自助打印、城市轨道交通刷脸支付等。
配合式 人脸辨识	采集对象主动配合采集人脸图像。 根据安全等级需要，可有活体检测要求。	无卡门禁考勤、访客查询登记等。
非配合式 人脸辨识	采集图像时，采集对象处于不知情的非配合状态。	追逃布控、黑名单人员视频监控、客户识别迎宾服务等。
n:N 人脸辨识	输入一组图片数据与数据库中另一组图片数据交叉比对，返回相似度较高的图片对，供后续分析使用；或采集两人及以上人群人脸信息，与数据库中图片数据交叉比对。	嫌疑人名单检索的多个人脸数据库的交叉比对等。

附 录 C
（资料性）
人脸信息安全管理机制

人脸信息安全管理机制宜包括安全管理制度和规程、安全管理机构、数据安全防护等级定级、安全事件处置和应急响应等，具体安全参考项详见附表C.1。其中，安全防护等级是基本级时，宜对存储介质进行格式化，或使用专用的工具在存储区域填入无用的信息进行覆盖；安全防护等级是增强级时，宜采用物理方式销毁存储介质，销毁后人脸数据应不可恢复。

表C.1 人脸信息安全管理机制的安全参考项

安全管理区域	安全参考项	安全防护等级	
		基本级	增强级
安全管理制度和规程	1）根据人脸数据安全防护等级要求制定安全管理策略，包括但不限于采集策略、加解密策略、脱敏策略、溯源策略、存储策略、使用策略、销毁策略等。	●	●
	2）制定安全管理规章制度和操作规程。	○	●
	3）指定或授权专人负责策略和规章制度的文档管理。	●	●
	4）形成由管理策略、管理规章制度、操作规程、记录表单等构成的安全管理制度体系。	○	●
安全管理机构	1）明确人脸数据安全管理主要负责人及其职权范围，对人脸数据安全负全面领导责任。	●	●
	2）明确内部涉及人脸数据处理工作的发生安全事件的处罚机制。	○	●
	3）对接触、使用和管理人脸数据的相关人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	●	●
	4）加强对内部人员外部人员和外协人员的安全管理，不应进行非授权操作，不应泄露、篡改、丢失和滥用数据。	●	●
数据安全防护等级定级	1）以书面形式说明数据安全防护等级，以及确定等级的理由。	●	●
	2）将数据分级备案材料报主管部门备案。	○	●
	3）定期评审数据安全防护等级，如需要变更数据等级，应依据变更审批流程执行变更。	○	●
安全事件处置和应急响应	1）及时向安全管理部门报告所发现的人脸数据的安全弱点和可疑事件。	●	●
	2）明确人脸数据的安全事件报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	●	●
	3）制定人脸数据安全事件应急响应机制、管理规范和流程，以及应急预案，包括应急处理流程、系统恢复流程等内容，明确人员分工，并定期开 展应急演练。	●	●
	4）发生安全事件后，根据应急响应机制进行处置。	●	●
注：●表示必选；○表示可选。			

参 考 文 献

[1] GB/T 41786—2022 公共安全 生物特征识别 术语
[2] GB/T 41987—2022 公共安全 人脸识别应用 防假体呈现攻击测试方法
[3] DB 31/T 1240.1 公共数据共享交换工作规范 第1部分：平台建设和运行管理要求