T/SHSDAA

团　体　标　准

T/SHSDAA 001-2025

安全防范 主动配合式人脸识别系统技术要求

Security protection—Technical requirements for collaborative face recognition system

2025－10－29 发布　　2025－12－01 实施

上海安全防范报警协会　　发 布

目　　次

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。

本标准由上海安全防范报警协会提出，由上海安全防范报警协会标准化专业委员会归口。

本文件起草单位：公安部第三研究所、杭州海康威视数字技术股份有限公司、浙江大华技术股份有限公司、上海商汤智能科技有限公司、厦门立林科技有限公司、福建星网天合智能科技有限公司、厦门狄耐克智能科技股份有限公司、上海杰宝大王智能信息技术有限公司、上海永天科技有限公司、公安部安全防范报警系统产品质量监督检验测试中心、上海德梁安全检测有限公司。

本文件主要起草人：游寒旭、同刚、常东亮、姚光毅、戎玲、余永福、林善和、陆青、顾杰、薛梅子、王远春、苑剑沣、陈平、汤淳诚。

引　言

为进一步提升上海市智能安全防范系统中主动配合式人脸识别产品的建设水平，规范人脸识别技术的应用和实施，指导主动配合式人脸识别应用产品的设计、生产和检验，制定本文件。本文件提出了人脸识别系统的安全等级划分原则和方法，并对应安全等级对人脸识别应用产品分别提出了具有前沿性和引领性的功能、性能和信息安全要求。本文件结合上海市地方标准DB31/T 329（所有部分）《重点单位重要部位安全技术防范系统要求》，对展览馆、博物馆、危险化学品/放射性同位素集中存放场所、金融机构、公共供水、电力设施、中小学、幼儿园、托育机构、城市轨道交通、旅馆、商务办公楼、零售商业、党政机关、医疗机构、通信单位、枪支弹药生产、经销、存放、射击场所、燃气系统、公交车站和公交专用停车场库、港口、码头、监管场所、渡轮、游览船、寄递单位、游乐场所、养老机构、军工单位、大型活动场所、高校、化工企业、民用机场航站楼等重点单位重要部位采用的主动配合式人脸识别系统，提出了明确的安全等级要求，是本市智能安全防范系统建设和管理的重要技术依据。

安全防范 主动配合式人脸识别系统技术要求

1 范围

本文件规定了安全防范系统中的主动配合式人脸识别系统的分类、安全等级、功能要求、性能要求、信息安全要求以及重点单位重点部位安全等级要求。

本文件适用于安全防范系统中应用主动配合式人脸识别技术的出入口控制系统、人脸身份认证系统、电子巡查系统等系统产品和工程的设计、检测和验收，其他领域中的主动配合式人脸识别系统可参照执行。

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 41772—2022 信息技术 生物特征识别 人脸识别系统技术要求

GB/T 41786—2022 公共安全 生物特征识别 术语

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

GA/T 1093—2023 安全防范 人脸识别应用 出入口控制人脸识别技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 41786—2022、GA/T 1093—2023界定的以及下列术语和定义适用于本文件。

3.1.1

主动配合式人脸识别系统 collaborative face recognition systems

需要用户主动配合进入识别区域采集人脸图像，通过人脸辨识和/或人脸验证的识别方式对其身份进行识别并输出决策的装置和/或管理软件。

注：在安全防范系统中，主要包括使用人脸识别技术的出入口控制系统、人脸身份认证系统以及电子巡查系统。

3.1.2

数据主体 data subject

人脸识别数据所标识或关联的自然人。

[来源：GB/T 41819—2022, 3.4, 有修改]

3.1.3

人脸辨识 face identification

通过收集获得的人脸信息与信息系统存储的特定范围内人脸信息进行“一对多”比对，发现和识别具有特定身份的个人。

注：也称“人脸辨认”、“1:N人脸比对”。

3.1.4

人脸验证 face verification

通过收集获得的人脸信息与信息系统存储的特定人脸信息进行“一对一”比对，确认和核对两者是否为同一人。

注：也称“人脸确认”、“1:1人脸比对”。

3.1.5

人脸关联数据 data associated with face

人脸数据所标识个体的相关信息。

注： 包含但不限于身份数据、活动轨迹数据和档案数据。

3.1.6

现场图像 on-site image

在出入口现场采集的原始图像。

3.1.7

响应时间 response time

从采集现场图像开始，到完成人脸识别输出识别结果的时间。

注： 在人脸确认模式中，响应时间不包含通过协作输入单元读取或调用人脸图像/模板的时间。

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）

FER：注册失败率（Failure to Enroll Rate）

FRR：错误拒绝率（False Rejection Rate）

4 分类

4.1 根据识别模式不同，主动配合式人脸识别系统（简称系统）的人脸识别模式分为人脸辨识模式、人脸验证模式。

4.2 根据识别部分所在位置不同，系统分为本地识别系统和远程识别系统。本地识别系统的识别部分部署于本地端，远程识别系统的识别部分部署在管理服务端。

5 安全等级

5.1 一般要求

5.1.1 系统按照保护对象面临的风险程度和对防护能力差异化的需求，通过对系统中防假体呈现攻击能力、识别率、信息安全要求等进行区分，构建对应的安全等级。

5.1.2 系统按照防护能力分为四个安全等级，安全等级 1 为最低等级，安全等级 4 为最高等级。

5.2 安全等级的划分

5.2.1 等级 1：低安全等级

防范对象为基本不具备人脸识别知识，且仅使用常见、有限的工具实施破坏的攻击者。

注： 安全等级1的系统具有基本信息安全保护要求，满足最基本需求的识别率性能，能够抵御照片或视频等简易假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，几乎不会对安全防范系统保护的对象造成损失。

5.2.2 等级 2：中低安全等级

防范对象为仅具有少量人脸识别知识，懂得使用常规工具和便携式工具的攻击者。

注： 安全等级2的系统具有基本信息安全保护要求，满足较高的识别率性能，能够抵御照片和视频等简易假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，不会对安全防范系统保护的对象造成较大损失。

5.2.3 等级 3：中高安全等级

防范对象为熟悉人脸识别系统，可以使用复杂工具和便携式电子设备的攻击者。

注： 安全等级3的系统具有较高信息安全保护要求，满足最高的识别率性能，能够抵御照片、视频以及面具等假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，将会对安全防范系统保护的对象造成重大损失。

5.2.4 等级 4：高安全等级

防范对象为熟悉人脸识别系统，具备实施攻击的详细计划和所需的能力或资源，具有所有可获得的设备，且懂得替换人脸识别系统的部件方法的攻击者。

注： 安全等级4的系统具有较高信息安全保护要求，满足最高的识别率性能，能够抵御照片、视频、面具、头模等复杂精细工艺的假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，将会对安全防范系统保护的对象造成特别重大损失。

6 功能要求

6.1 明示告知/同意

明示告知/同意应符合表1中A的要求。

6.2 图像质量判断

图像质量判断应符合表1中B的要求。

6.3 防假体呈现攻击

防假体呈现攻击检测应符合表1中C的要求。

6.4 人脸注册

人脸注册应符合表1中D的要求。

6.5 人脸识别

人脸识别应符合表1中E的要求。

6.6 管理功能

管理功能符合表1中F的要求。

表1 系统功能要求

项目	序号	要求	安全等级			
			1	2	3	4
A 明示告知/同意	1	人脸数据及人脸关联数据收集应经数据主体授权同意，系统应当以显著方式、清晰易懂的语言真实、准确、完整地向数据主体告知下列事项： a)人脸信息的处理目的、处理方式(包括但不限于人脸图像的最小数量，提供数据应用范围等)，处理的人脸信息保存期限； b)处理人脸信息的必要性以及对数据主体权益的影响； c)数据主体依法行使权利的方式和程序。收集时应提供确认、取消等操作选项，获得数据主体同意体授权后进行收集人脸信息收集	M	M	M	M
	2	数据主体有权撤回同意，系统应当提供便捷的撤回同意的方式	M	M	M	M
	3	采用导入或其他方式进行批量人脸注册的系统，批量注册的人脸数据及人脸关联数据应经数据主体授权同意，并具有确认、取消等操作选项	M	M	M	M
	4	对人脸数据及人脸关联数据进行导出时，需经过系统管理员授权同意，并具有确认、取消等操作选项。对于导出的人脸数据及人脸关联数据应采用数据安全的保护措施	M	M	M	M
B 图像质量判断	5	当注册用图像的图像质量不符合系统注册要求时，拒绝注册后应给出给出明确提示原因	M	M	M	M
	6	当现场采集的人脸图像不满足系统要求时，本地端应给出可听/可视的提示	OP	M	M	M

表 1（续）

项目	序号	要求	安全等级			
			1	2	3	4
C 防假体呈现攻击	7	具有防假体呈现攻击能力，能够抵御不同类型假体人脸的呈现攻击。假体人脸应符合 GB/T 41987—2022 中附录A的要求。根据不同抵御能力，分为以下四个级别： ● 级别I：应能抵御人脸照片、人脸视频等2类人脸假体中的至少一种的呈现攻击； ● 级别II：应能抵御人脸照片、人脸视频等2类人脸假体的呈现攻击； ● 级别III：应能抵御人脸照片、人脸视频、人脸仿真面具等3类人脸假体的呈现攻击； ● 级别IV：应能检测包括人脸照片、人脸视频、仿真人脸面具、仿真人脸头模等在内的至少4类人脸假体的呈现攻击	级别I或以上	级别II或以上	级别III或以上	级别IV
	8	当检测到假体呈现攻击时，应给出可听/可视的受攻击提示	OP	OP	M	M
D 人脸注册	9	应符合 GA/T 1093-2023中5.7的要求	M	M	M	M
E 人脸识别	10	应符合GA/T 1093-2023中5.5的要求	M	M	M	M
	11	具有人脸验证识别模式的系统，用户证件信息读取方式应至少包含身份证读取	OP	OP	M	M
	12	当用户佩戴口罩时，应能进行人脸识别	OP	OP	OP	OP
	13	应能检测用户是否佩戴口罩，并给出相应的提示	OP	OP	OP	OP
F 管理功能	14	应符合GA/T 1093-2023中5.6的要求	M	M	M	M

注： M表示必选项，OP表示可选项。

7 性能要求

7.1 图像采集

图像采集应符合表2中A的要求。

7.2 识别距离

识别距离应符合表2中B的要求。

7.3 环境照度适应性

7.3.1 环境照度适应性应符合表 2 中 C 的要求。

7.3.2 室外应用的产品，宜符合以下要求：

a) 暗光识别：在10 Lux及以下的环境照度条件下，能够进行人脸识别；

b) 强光识别：在10000 Lux～100000 Lux的环境照度条件下，能够进行人脸识别；

c) 超强光识别：100000 Lux～200000 Lux及以上的环境照度条件下，能够进行人脸识别。

7.4 防假体呈现攻击失败率

防假体呈现攻击失败率应符合表2中D的要求。

7.5 存储容量

存储容量应符合表2中E的要求。

7.6 注册失败率

注册失败率应符合表2中F的要求。

7.7 识别准确率

识别准确率应符合表2中G的要求。

7.8 响应时间

响应时间应符合表2中H的要求。

表2 系统性能要求

项目	序号	要求	安全等级			
			1	2	3	4
A 图像采集	1	采集图像的水平分辨力	≥ 720 TVL	≥ 720 TVL	≥ 720 TVL	≥ 720 TVL
	2	采集图像的灰度等级	10级	10级	11级	11级
B 识别距离	3	人员人脸与图像采集设备采集点中心位置水平对齐后，能进行人脸识别的距离范围	0.3 m～ 1.2 m	0.3 m～ 1.2 m	0.3 m～ 1.2 m	0.3 m～ 1.0 m
C 环境照度适应性	4	在侧光、逆光、顺光条件下，系统满载（注册人数=系统声明容量）条件下，环境照度为10 Lux～10000 Lux时能进行人脸识别	M	M	M	M

表2（续）

项目	序号	要求	安全等级			
			1	2	3	4
D 防假体呈现攻击失败率	5	防人脸照片攻击失败率	≤5 %[1]	≤5 %	≤5 %	≤5 %
	6	防人脸视频攻击失败率	≤5 %[1]	≤5 %	≤5 %	≤5 %
	7	防仿真人脸面具攻击失败率	OP	OP	≤10 %	≤5 %
	8	防仿真人脸头模攻击失败率	OP	OP	OP	≤10 %
E 存储容量	9	系统注册人脸库（人脸模板）数量	根据实际应用声明	根据实际应用声明	根据实际应用声明	根据实际应用声明
	10	人脸识别记录数量是系统注册人脸库（人脸模板）数量的倍数	5倍或以上	5倍或以上	5倍或以上	5倍或以上
F 注册失败率	11	人脸辨识模式下的注册失败率(FER)	≤ 0.5 %	≤ 0.1 %	≤ 0.05 %	≤ 0.03 %
G 识别准确率	12	系统满载（注册人数=系统声明容量）条件下，人脸辨识模式下的识别准确率	FAR≤ 5 %且 FRR≤ 5 %	FAR≤ 3 %且 FRR≤ 5 %	FAR≤ 2 %且 FRR≤ 2 %	FAR≤ 1 %且 FRR≤ 2 %
	13	人脸验证模式下的识别准确率	FAR≤ 1 % 且FRR ≤2 %	FAR≤ 0.1 % 且FRR ≤2 %	FAR≤ 0.03 % 且FRR ≤2 %	FAR≤ 0.01 % 且FRR ≤2 %
H 响应时间	14	系统满载（注册人数=系统声明容量）条件下，呈现攻击检测关闭条件下，人脸识别响应时间	≤1 s	≤1 s	≤1 s	≤1 s
	15	系统满载（注册人数=系统声明容量）条件下，呈现攻击检测开启条件下，人脸识别响应时间	≤3 s	≤3 s	≤2 s	≤2 s
注1： M表示必选项，OP表示可选项。 **注2：** 5%[1]表示有相同编号的数字指标至少被选择一项						

8 信息安全要求

8.1 设备身份验证

设备身份验证应符合表3中A的要求。

8.2 用户身份验证

用户身份验证应符合表3中B的要求。

8.3 数据传输

数据传输应符合表3中C的要求。

8.4 访问控制

访问控制应符合表3中D的要求。

8.5 数据存储

数据存储应符合表3中E的要求。

8.6 数据脱敏

数据脱敏应符合表3中F的要求。

8.7 用户权限

用户权限应符合表3中G的要求。

8.8 操作日志

操作日志应符合表3中H的要求。

8.9 入侵检测和防御

入侵检测和防御应符合表3中I的要求。

表3 系统信息安全要求

项目	序号	要求	安全等级			
			1	2	3	4
A 设备身份验证	1	基本级：基于设备身份ID号、MAC地址等的合法性验证 增强级：基于数字证书的双向身份验证机制，并对证书集中管理	基本级	基本级	增强级	增强级
B 用户身份验证	2	基本级：设备或系统的登录密码应具备不低于8位的复杂度，包含数字、字母或特殊字符中的2种 增强级：设备或系统的登录密码应具备不低于10位的复杂度，密码不含用户名等，包含数字、字母和特殊字符，并要求定期更换	基本级	基本级	增强级	增强级
	3	基本级：登录不成功尝试次数超过设定最大次数时，应对非法身份仿冒连续攻击行为进行限制 增强级：1.满足基本级要求；2.配置当登录连接超时自动退出等措施	基本级	基本级	增强级	增强级

表3（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 用户身份验证	4	基本级：采用口令技术对用户进行身份验证 增强级：采用口令、数字证书或生物特征识别等两种或两种以上组合的鉴别技术对用户进行身份验证	基本级	基本级	增强级	增强级
C 数据传输	5	基本级：本地识别系统联网应用时，应采用校验技术保证通信过程中数据的完整性 增强级：本地识别系统联网应用时，应采用数据加密技术满足人脸数据和人脸关联数据在传输过程中的保密性	基本级	增强级	增强级	增强级
	6	基本级：远程识别系统联网应用时，应采用密码技术保证通信过程中数据的完整性 增强级：远程识别系统联网应用时，1.应采用端到端加密或传输通道加密的传输安全策略；2.具备在构建传输通道前对两端主体身份进行鉴别的能力；3.支持数据真实性检测，采用国密算法	基本级	增强级	增强级	增强级
D 访问控制	7	基本级：应能对非授权设备连接系统的行为进行检查 增强级：1.满足基本级要求；2.应能设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	基本级	基本级	增强级	增强级
	8	基本级：应能对系统内部设备连接到外部网络的行为进行检查 增强级：1.满足基本级要求；2.应能设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	基本级	基本级	增强级	增强级
E 数据存储	9	基本级：除法律、行政法规另有规定或者取得数据主体单独同意外，人脸数据和人脸关联数据应当存储于人脸识别设备内，不得通过互联网对外传输	基本级	基本级	基本级	基本级
	10	基本级：在采集和存储数据主体的原始证件图像、现场图像、人脸图像时，应遵循最小够用原则，根据实际应用需求，选择需要保存的最小数量、最少类型的图像	基本级	基本级	基本级	基本级

表3（续）

项目	序号	要求	安全等级			
			1	2	3	4
E 数据存储	11	基本级：人脸数据和人脸关联数据不应使用图片、明文或Base64等直接图像文件或简单编码方式直接存储 增强级：1.满足基本级要求；2.数据库存储的人脸数据和人脸关联数据应采用加密技术并分表，宜分区存储	基本级	基本级	增强级	增强级
	12	基本级：人脸数据和人脸关联数据的使用应能配置使用期限，到期应自动删除相关数据或匿名化处理或去标识化处理	基本级	基本级	基本级	基本级
F 数据脱敏	13	基本级：针对人脸数据和人脸关联数据的展示时，应采取匿名化等措施防止信息过量展示	基本级	基本级	基本级	基本级
G 用户权限	14	基本级：应具有用户权限管理，用户在授权范围内完成对人脸识别应用的登录、注册、编辑、存储、使用、查询、删除、备份等操作	基本级	基本级	基本级	基本级
H 操作日志	15	基本级：1.进行与人脸数据和人脸关联数据的相关操作（如编辑信息、导出数据、告警处理等）时，均应生成操作日志；2.操作日志应包含操作人员、操作时间、操作地址、操作行为等信息；3.操作日志应不能更改或删除 增强级：1.满足基本级要求；2.操作日志应至少保存6个月	基本级	基本级	增强级	增强级
I 入侵检测和防御	16	基本级：1.应关闭非必要的系统服务、默认共享和高危端口；2.应具有防御入侵的相关功能；3.宜安装恶意代码检测软件或具有配置相应的功能	基本级	基本级	基本级	基本级

9 本市重点单位重要部位安全等级要求

DB31/T 329（所有部分）《重点单位重要部位安全技术防范系统要求》标准覆盖的本市重点单位中，部署主动配合式人脸识别系统的重要部位的安全等级应符合表4的要求。

表4 本市重点单位重点部位安全等级要求

序号	重点单位	重要部位
1	展览馆、博物馆	等级3及以上：包括但不限于数据机房、监控室、一、二级风险展品/藏品的库区、库房、技术保护用房、需双人双锁管理的出入口及设计中规定的其他部位 等级2及以上：其他部位
2	危险化学品、放射性同位素集中存放场所	等级3及以上：包括但不限于数据机房、监控室、剧毒化学品仓库、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
3	金融单位	等级3及以上
4	公共供水	等级3及以上：包括但不限于数据机房、监控室、危化品加药间出入口、重要物资仓库出入口及设计中规定的其他重要部位 等级2及以上：其他部位
5	电力设施	等级3及以上：包括但不限于数据机房、监控室、重要物资仓库出入口及设计中规定的其他重要部位 等级2及以上：其他部位
6	中小学、幼儿园、托育机构	等级3及以上：包括但不限于数据机房、监控室、危化品存储实验室出入口及设计中规定的其他重要部位 等级2及以上：其他部位
7	城市轨道交通	等级3及以上：包括但不限于数据机房、监控室、重要物资仓库出入口、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
8	旅馆、商务办公楼	等级3及以上：包括但不限于数据机房、监控室、贵重物品寄存处及设计中规定的其他重要部位 等级2及以上：其他部位
9	零售商业	等级3及以上：包括但不限于数据机房、监控室及设计中规定的其他重要部位 等级2及以上：其他部位
10	党政机关	等级3及以上：包括但不限于数据机房、监控室、档案资料室、机要室、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
11	医疗机构	等级3及以上（包括但不限于数据机房、监控室、危化品存储仓库出入口、医疗废物集中存放场所出入口、需双人双锁管理的出入口及设计中规定的其他重要部位）
12	通信单位	等级3及以上：包括但不限于数据机房、监控室、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
13	枪支弹药生产、经销、存放、射击场所	等级3及以上：包括但不限于数据机房、监控室、枪支弹药库室出入口、档案（资料）室、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重要部位 等级2及以上：其他部位

表4（续）

序号	重点单位	重要部位
14	燃气系统	等级3及以上：包括但不限于数据机房、监控室、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
15	公交车站和公交专用停车场库	等级2及以上
16	港口、码头	等级2及以上
17	监管场所	等级3及以上：包括但不限于数据机房、监控室、警用装备室、档案资料室、需双人双锁管理的仓库出入口及设计中规定的其他重要部位 等级2及以上：其他部位
18	渡轮、游览船	等级2及以上
19	寄递单位	等级2及以上
20	游乐场所	等级3及以上：包括但不限于数据机房、监控室、重要动力机房出入口、需双人双锁管理的出入口及设计中规定的其他重要部位。 等级2及以上：其他部位
21	养老机构	等级3及以上：包括但不限于数据机房、监控室、档案资料室、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
22	军工单位	等级3及以上：包括但不限于办公、科研楼宇，企业的保密要害部位（如机要室、档案资料室等）中心机房、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
23	大型活动场所	等级3及以上：包括但不限于数据机房、监控室、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
24	高校	等级3及以上：包括但不限于数据机房、监控室、承担涉及国家机密项目（课题）的研究机构场所，机要室、档案室、国家实验室、国家重点实验室、高价值教学与科研设备存放场所，核、生、化、爆等实验室及危险品生产、使用、储藏场所，管制物品、贵重物品集中存放或生产、制作及销毁场所、需双人双锁管理的出入口及设计中规定的其他重要部位 等级2及以上：其他部位
25	化工企业	等级3及以上：包括但不限于危险化学品重大危险源安全监控场所、危化品仓库、剧毒品仓库、中心控制室、中心机房、化学化工实验室、易制爆易制毒物品仓库及中心机房及其他需双人双锁管理或多人组合进入的出入口 等级2及以上：其他部位
26	民用机场航站楼	等级3及以上

参 考 文 献

[1] 人脸识别技术应用安全管理办法（国家互联网信息办公室、中华人民共和国公安部令 第19号）

[2] GB/T 41772—2022 信息技术 生物特征识别 人脸识别系统技术要求

[3] GB/T 41786—2022 公共安全 生物特征识别 术语

[4] 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

[5] GA/T 1093—2023 安全防范 人脸识别应用 出入口控制人脸识别技术要求

[6] 本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（沪公技防[2023]1号）

[7] 本市安全防范涉及人脸识别应用产品及相关数据传输技术要求 技术解读

[8] DB31/T 329（所有部分） 重点单位重要部位安全技术防范系统要求