



团 体 标 准

T/UNP XXXX—2025

人脸识别检测自动处理系统技术规范

Technical specification for automatic processing system of face recognition detection

（征求意见稿）

2025 – XX – XX 发布

2025 – XX – XX 实施

中国联合国采购促进会 发 布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语 1

 3.1 术语和定义 1

 3.2 缩略语 1

4 系统架构 1

5 功能要求 3

 5.1 用户标识创建 3

 5.2 人脸图像采集 3

 5.3 人脸图像处理 3

 5.4 人脸图像质量判断 3

 5.5 活体检测 3

 5.6 人脸数据管理 3

 5.7 用户鉴别 4

6 性能要求 5

 6.1 人脸注册 5

 6.2 人脸验证 5

 6.3 注册失败率 5

 6.4 识别性能 5

 6.5 活体检测防范能力 5

 6.6 防假体呈现攻击失败率 5

 6.7 响应时间 5

7 数据要求 6

 7.1 数据收集 6

 7.2 数据使用 6

 7.3 数据删除 6

 7.4 数据存储 6

8 安全要求 6

 8.1 用户身份验证 6

 8.2 数据传输 6

 8.3 访问控制 7

 8.4 数据脱敏 7

 8.5 用户权限 7

 8.6 操作日志 7

9 运行维护 7

9.1 基本要求 7

9.2 例行维护 7

9.3 响应支持 7

9.4 优化改善 8

10 评价改进 8

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。

本文件由中国联合国采购促进会提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

为助力中国企业参与国际贸易,推动企业高质量发展,中国联合国采购促进会依托联合国采购体系,制定服务于国际贸易的系列标准,这些标准在国际贸易过程中发挥了越来越重要的作用,对促进贸易效率提升,减少交易成本和不确定性,确保产品质量与安全,增强消费者信心具有重要的意义。

联合国标准产品与服务分类代码(UNSPSC, United Nations Standard Products and Services Code)是联合国制定的标准,用于高效、准确地对产品和服务进行分类。在全球国际化采购中发挥着至关重要的作用,它为采购商和供应商提供了一个共同的语言和平台,促进了全球贸易的高效、有序发展。

围绕UNSPSC进行相关产品、技术和服务团体标准的制定,对助力企业融入国际采购,提升国际竞争力具有十分重要的作用和意义。

本文件采用UNSPSC分类代码由6位组成,对应原分类中的大类、中类和小类并用小数点分割。

本文件UNSPSC代码为“43.23.15”,由3段组成。其中:第1段为大类,“43”表示“信息技术广播和电信”,第2段为中类,“23”表示“软件”,第3段为小类,“15”表示“特定于业务功能的软件”。

人脸识别检测自动处理系统技术规范

1 范围

本文件规定了人脸识别自动检测处理系统的系统架构、功能要求、性能要求、数据要求、安全要求、运行维护、评价改进。

本文件规定了人脸识别自动检测处理系统的设计、建设与运维。

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 41786 公共安全 生物特征识别 术语

3 术语、定义和缩略语

3.1 术语和定义

GB/T 41786—2022界定的术语和定义适用于本文件。

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)

UID: 用户身份证明 (User Identification)

4 系统架构

4.1 人脸识别检测自动处理系统框架由客户端、服务器端、安全传输通道组成。其中客户端进行人脸信息采集，经安全传输通道传输，在服务器端远程进行比对。系统架构如图 1 所示。

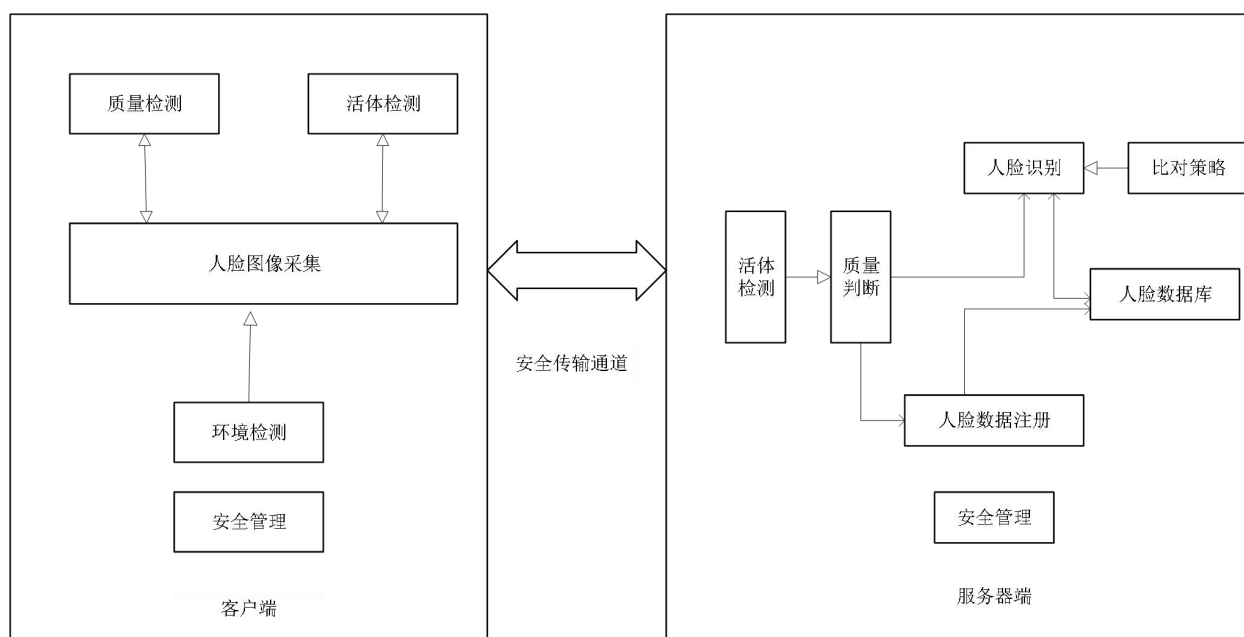


图1 人脸识别检测自动处理系统

4.2 客户端由以下模块组成，包括：

- 环境检测：对人脸采集的环境条件进行检测，判断人脸特征采集所处的环境是否满足采集要求，从而决定是否启动人脸采集；
- 人脸图像采集：对输入的图片或者视频等样本数据进行分析处理，提取满足质量条件的人脸图像，进行人脸特征提取和比对；
- 活体检测：对采集主体是否为活体人脸、是否受到假体人脸攻击进行检测和判断。条件允许时，可在客户端判断人脸比对对象是否为真实有效的人脸。活体检测不通过则不进行下一步处理；
- 质量检测：对人脸图像的质量进行判断，输出质量最佳的人脸图片进行后续的特征建模与比对。人脸质量检测不通过则不进行下一步处理；
- 安全管理：对客户端密码、配置参数、用户数据等敏感数据等进行安全管理。

4.3 服务器端由以下模块组成，包括：

- 活体判断：对客户端活体人脸检测过程中采集的信息进行二次判断，结合客户端检测结果，完成最终活体判断；
- 质量判断：对上传到服务器端的生物特征信息的质量进行判断；
- 人脸数据注册：通过人脸模板登记过程，实现用户原始人脸图像或用户特征数据与用户标识之间绑定关系的建立；
- 人脸数据库：对人脸数据进行生命周期管理，数据内容包括人脸特征模板、人脸辅助信息、用户属性数据、人脸比对数据等；

注1：人脸特征模板主要用来存储人脸的特定信息，以便计算机能够快速、准确的进行生物特征比对。

注2：辅助信息主要用于活体检测或多模态检测。

注3：用户属性数据主要用于用户检索，包括用户标识UID、姓名等。

e) 人脸识别：

- 人脸验证：将样本特征序列与注册的模板特征序列进行比对，确定两张人脸是否为同一个人；
 - 人脸辨识：将样本特征序列与一定范围内的已登记模板特征序列进行比对，根据比对得分进行排序，找出最为相似的已登记模板特征序列，从而确认用户身份。
- 比对策略：基于用户信息、客户端信息等不同条件，设置不同环境下的比对策略；
 - 安全管理：服务器端密码管理、安全审计、授权访问等安全管理功能；

- h) 安全传输通道：客户端与服务器端应建立数据传输通道的安全策略和规程，通过安全控制措施实现数据传输安全。

5 功能要求

5.1 用户标识创建

在用户注册时，系统应引导用户通过一个安全的流程创建唯一的用户标识（UID），该过程包括：

- a) 确认用户同意隐私政策和服务条款；
- b) 收集必要的个人信息，如姓名、联系方式等，用于建立用户档案；
- c) 使用高强度算法生成不可预测且唯一的 UID。

5.2 人脸图像采集

采集人脸图像时应符合以下要求：

- a) 检查环境条件是否适宜拍摄高质量的人脸图像，例如光线强度、背景复杂度等；
- b) 引导用户调整位置，使得人脸位于最佳拍摄范围内；
- c) 自动检测并聚焦于人脸区域，确保捕捉到清晰的人脸轮廓；
- d) 在不影响用户体验的前提下，宜快速完成图像抓取。

5.3 人脸图像处理

采集完成后，系统应对图像进行处理，并符合以下要求：

- a) 应用滤波器去除噪声，提高图像质量；
- b) 调整对比度和亮度，使面部特征更加明显；
- c) 统一所有人脸图像大小；
- d) 应支持预处理操作，比如旋转校正、遮挡物移除等。

5.4 人脸图像质量判断

人脸图像处理完成后，应对人脸图像质量进行判断，判断内容包括但不限于：

- a) 人脸图片的模糊程度；
- b) 人脸图片的明暗程度；
- c) 人脸图片的人脸角度；
- d) 人脸图片的完整程度。

5.5 活体检测

5.5.1 主动配合式活体检测

应支持根据检测主体的主动式反应进行活体人脸检测，通过指令要求用户进行相关动作并判断人脸的真实有效性，指令包括但不限于：

- a) 点头、抬头、左右转头、张嘴、眨眼等；
- b) 唇语、说指定的数字或者文字等。

5.5.2 被动交互式活体检测

应支持检测主体无需主动配合动作模式下的活体人脸检测，包括但不限于以下方式：

- a) 可见光下根据主体的脸部细节微小变化判断是否为活体；
- b) 根据检测主体接收特定波段光源照射后产生的反馈，进而判断是否为活体。

5.6 人脸数据管理

5.6.1 人脸数据注册

人脸数据注册方式包括现场注册、远程注册两种方式。

5.6.2 人脸数据注销

人脸数据注销符合以下要求：

- a) 注销参与者是有关闭意愿的用户本人；
- b) 在注销前对授权注销者进行身份验证；
- c) 注销后，存储器中的人脸数据应销毁，不应重复使用，下次使用应重新采集。

5.6.3 人脸数据注册加载

人脸数据注册加载应符合以下要求：

- a) 建立不同数据源、不同安全域之间采集数据加载安全策略、加载方式和访问控制机制；
- b) 确保人脸数据加载过程中的数据正确性和一致性；
- c) 确保人脸数据加载过程中数据的安全保护；
- d) 记录并保存人脸数据加载过程中人脸等个人信息数据的处理过程。

5.7 用户鉴别

5.7.1 人脸验证

人脸验证具备以下功能：

- a) 进行人脸验证时，应给出 UID；
- b) 根据所给用户身份标识信息，检索出该用户的人脸模板；
- c) 执行数据包验证功能，检验用户人脸模板的完整性；
- d) 将实时采集并生成的人脸样本特征与所检索出的该用户的人脸模板进行比对，产生用于用户验证的比对相似度值；
- e) 根据比对阈值输出人脸识别判定；
- f) 人脸验证后应清除残留信息。

5.7.2 人脸辨识

人脸辨识应符合以下要求：

- a) 将实时采集的并生成的人脸样本特征与已存贮的人脸模板逐一进行比对，产生用于人脸辨识的比对相似度值；
- b) 根据比对阈值输出人脸识别判定；
- c) 人脸辨识后应清除残留信息。

5.7.3 防伪造

系统应检测并防止用户使用伪造的鉴别数据，包括但不限于：

- a) 防复制伪造：检测或防止对当前用户识别数据的复制和非授权保存；
- b) 防照片伪造：检测或防止使用照片伪造识别图像；

注：打印的普通人脸照片、纸质高清人脸照片、手机屏幕重放的人脸照片攻击。

- c) 纸质面具伪造：检测或防止使用绝大多数人脸纸质面具的仿冒行为；
- d) 上述攻击或非授权操作事件时应取消服务，并产生报警。

5.7.4 决策反馈保护

人脸识别决策反馈保护满足以下要求：

- a) 根据人脸识别决策策略，返回人脸识别比对结果，并保护反馈结果的完整性；
- b) 识别过程中，应避免提供给用户的反馈信息泄露用户的人脸特征信息数据；
- c) 应返回是否通过信息，不反馈识别分数，防止爬山攻击。

5.7.5 鉴别失败

5.7.5.1 失败判定

系统在识别过程中，当出现以下情形时判断为识别失败，包括：

- a) 设备故障：人脸采集器故障，不能成功捕捉图像；
- b) 像质障碍：捕捉的人脸图像质量不适于生成人脸模板或生成人脸样本超时断开；

- c) 终端操作超时断开；
- d) 数据库故障：人脸数据库故障且在规定尝试次数内未能消除；
- e) 尝试超次：对人脸验证与人脸辨识，应分别设定警告次数值，连续警告次数大于该阈值时视作失败。

5.7.5.2 失败处理

人脸识别失败的处理应符合以下要求：

- a) 制定识别失败返回值表；
- b) 在出现识别失败情况时，返回对应的错误代码或错误值；
- c) 针对识别失败记录事件日志；
- d) 制定明确的识别失败处理策略，进行警告与报警；
- e) 针对不同识别失败原因进行相应处理。

5.7.5.3 警示与报警

系统的警告与报警满足以下要求：

- a) 进行人脸验证时，如用户不是所给身份标识信息或其他用户身份信息的持有者、用户已被删除或在进行人脸辨识时，已存贮的人脸模板中无用户的候选者，应给出警告信息；
- b) 检测出伪造识别图像、识别数据，或复制、非授权保存图像、数据、非活体人脸或非授权数据库操作时，应给出报警信息。

6 性能要求

6.1 人脸注册

系统人脸注册失败率应不大于1%。

6.2 人脸验证

当错误接受率为0.1%时，错误拒绝率应不大于5%。

6.3 注册失败率

具有人脸辨认模式的识别系统，注册失败率应不大于0.1%。

6.4 识别性能

人脸识别性能应符合下列要求：

- a) 人脸辨认模式：FAR 不大于 1%时，FRR 不大于 5%；
- b) 人脸确认模式：FAR 不大于 0.1%时，FRR 不大于 2%。

6.5 活体检测防范能力

6.5.1 正常通过率

系统活体检测正常通过率应不小于95%。

6.5.2 攻击拒绝率

系统活体检测攻击拒绝率应不小于99%。

6.6 防假体呈现攻击失败率

识别系统的防假体呈现攻击失败率应符合下列要求：

- a) 防人脸照片攻击失败率不大于 5%；
- b) 防人脸视频攻击失败率不大于 5%。

6.7 响应时间

6.7.1 呈现攻击检测关闭条件下，人脸识别响应时间应不大于 1 s。

6.7.2 呈现攻击检测开启条件下，人脸识别响应时间应不大于 3 s。

7 数据要求

7.1 数据收集

数据处理者收集人脸识别数据的要求如下：

- a) 收集人脸识别数据时，应向数据主体告知人脸识别数据的相关事项，包括但不限于数据处理者的名称和联系方式、个人信息保护负责人的姓名和联系方式、处理规则、必要性依据等，并征得数据主体单独同意或书面同意；未取得数据主体单独同意收集的人脸图像应立即删除并确保不可恢复；
- b) 数据主体不同意收集人脸识别数据的，不应拒绝数据主体使用基本业务功能；
- c) 应采用需要数据主体主动配合的措施收集人脸识别数据；
- d) 应在识别过程中持续告知数据主体验证目的，并通过语言、文字等向数据主体进行提示；
- e) 应仅收集生成人脸特征所需的最小数量、最少图像类型的人脸图像；
- f) 应采取安全措施保证人脸识别数据的真实性、完整性和一致性，防止人脸识别数据在收集过程中泄漏或篡改。

7.2 数据使用

数据处理者使用人脸识别数据的要求如下：

- a) 应在使用人脸识别数据识别自然人身份后立即删除用于识别的人脸图像；
- b) 人脸特征应具有可更新、不可逆、不可链接的特性；
- c) 在本地和远程人脸识别方式均适用时，应优先使用本地人脸识别；
- d) 应对人脸识别数据使用行为进行审计。

7.3 数据删除

数据处理者在发生以下情况时，应在15 d内删除人脸识别数据并确保不可恢复：

- a) 人脸识别数据处理目的已实现或无法实现；
- b) 人脸识别数据存储时间达到数据主体单独同意或书面同意的存储期限；
- c) 数据主体撤回同意或明示停止使用；
- d) 数据处理者停止提供人脸识别业务；
- e) 数据主体一年未使用数据处理者提供的产品或服务；
- f) 法律、行政法规规定的其他情形。

7.4 数据存储

数据存储符合以下要求：

- a) 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；
- b) 人脸数据和人脸关联数据不应使用图片、明文等直接图像文件或简单编码方式直接存储；
- c) 人脸数据和人脸关联数据的使用应能配置使用期限，到期应采取自动删除相关数据、匿名化处理、去标识化处理等方式进行处理。

8 安全要求

8.1 用户身份验证

- 8.1.1 设备或识别系统的登录密码应具备不低于 8 位的复杂度，且包含数字、字母或特殊字符。
- 8.1.2 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。
- 8.1.3 宜具有密码、数字证书和生物特征识别等多种身份验证方式。

8.2 数据传输

8.2.1 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。

8.2.2 远程识别系统联网应用时，应采用端到端加密或传输通道加密的传输安全策略。

8.3 访问控制

8.3.1 应对非授权设备连接识别系统的行为进行检查或限制，以允许或拒绝数据进出。

8.3.2 应对识别系统内部设备连接到外部网络的行为进行检查或限制，以允许或拒绝数据进出。

8.4 数据脱敏

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。

8.5 用户权限

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。

8.6 操作日志

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。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。操作日志应不可更改或删除。

9 运行维护

9.1 基本要求

人脸识别系统的运行和维护，包括应用软件及其运行环境的运行维护、数据维护等要求。系统运行维护基本要求包括但不限于：

- a) 设立运行维护团队，负责系统的日常运维和管理，确保系统运行的安全性和稳定性；
- b) 对应用软件、数据及运行环境进行调研和分析，确定运行维护要点，制定系统运行维护规程；
- c) 明确运维人员的岗位职责，保证权限清晰、各司其职、个人信息安全及应用系统正常运行；
- d) 运维人员按照规程进行运维操作，关键操作由上级主管监督执行；
- e) 规范系统运行维护管理和流程，提高系统的安全性和稳定性，降低运维成本和风险；
- f) 建立知识库，收集、积累、共享和使用运行维护数据和经验，以持续改进运行维护服务。

9.2 例行维护

人脸识别系统应用软件及其运行环境和数据的例行维护包括但不限于：

- a) 人脸识别系统应具备自检能力，包括系统完整性、功能有效性的校验，并能防御软件被篡改、木马入侵等风险，运维人员应定期查验系统自检结果；
- b) 应定期检查人脸识别系统的监控指标、运行状态及其运行环境状态，对于系统的异常情况和故障，应及时进行预警、排查、修复、回溯及备案；
- c) 定期进行人脸识别系统的性能优化或调整，确保系统的性能和响应速度；
- d) 制定运维人员的权限管理方案，避免越权操作，确保系统的安全性和人脸识别主体数据隐私性；
- e) 抽样检查人脸识别主体身份信息，人脸识别数据等关键业务数据的真实性、有效性、完整性及数据之间的一致性，防止数据错误影响业务的正常开展；
- f) 制定系统备份和恢复方案，包括但不限于安装包，数据及模型参数文件等备份及恢复，确保系统数据的可靠性和完整性；
- g) 系统的运维手册和使用说明书应及时更新和完善。

9.3 响应支持

响应支持包括服务受理、故障诊断与解决处理、主体请求、新功能上线等，要求包括但不限于：

- a) 受理服务请求，包括故障请求和非故障请求，根据故障解决方案、系统监控分析、日志分析等进行故障定位及排查；
- b) 执行故障解决方案，检测、监控、跟踪处理效果，将处理经验和建议纳入维护文档；
- c) 建立保障人脸识别主体权利的机制和渠道，保障其知情同意、获取人脸识别数据处理情况、撤回同意、注销账号、投诉、获得及时响应等方面的权利，并及时响应其相关请求；
- d) 新功能上线过程中，做好配置更新、权限分配、数据初始化、安全检查和功能使用培训等工作。

9.4 优化改善

系统优化改善包括系统功能、性能及数据的优化以及系统的升级发布，要求包括但不限于：

- a) 系统功能存在缺陷或业务需求发生变化，应根据实际需要进行软件功能修改、完善和新增开发；
- b) 因业务量增加、系统数据冗余及安全威胁等，应对系统、数据及运行环境进行优化和改进；
- c) 对于具备二次开发能力的人脸识别系统，其二次开发接口符合如下要求：
 - 1) 不应将修改人脸识别数据标识作为开发接口提供给二次开发使用；
 - 2) 二次开发不应影响系统自检功能和自检结果。
- d) 系统升级发布：
 - 1) 系统升级应取得人脸识别系统所有者的明示同意，所有者不同意时，人脸识别系统应能正常工作；
 - 2) 应制定发布计划、制作发布包并实施发布，并对发布结果进行确认，发布失败时执行回退；
 - 3) 升级发布不应影响系统自检功能、自检结果及人脸识别主体数据安全；
 - 4) 升级发布后，应进行配置更新、权限分配、数据初始化及安全检查等工作；
 - 5) 系统升级发布后，应进行人脸识别系统的版本管理和控制。
- e) 系统的优化与升级，不应导致人脸识别系统使用的目的、方式、范围或规则等发生变化。

10 评价改进

依据第5章～第9章规定的要求，定期开展人脸识别检测自动处理系统的功能、性能、数据、安全、和运行维护方面的评价，审查不合格项，并有针对性地采取纠偏措施并持续改进。
