ICS 35.240.15
UNSPSC 43.23.15
CCS L 70

团 体 标 准

T/UNP XXXX—2024

人脸识别模型设计生成系统技术规范

Technical specification for face recognition model design and generation system

（征求意见稿）

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国联合国采购促进会 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。

本文件由武汉莫问科技有限公司提出。

本文件由中国联合国采购促进会归口。

本文件起草单位：武汉莫问科技有限公司、武汉小菠菜科技有限公司、武汉万事莱文化科技有限公司、武汉吉客威睿数字科技有限公司、武汉深夜数字艺术传播有限公司。

本文件主要起草人：李儒日、戴冬竹、邓梦云、陈书敏、张晨胜、钱文蔚。

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”。

人脸识别模型设计生成系统技术规范

1 范围

本文件规定了人脸识别模型设计生成系统的系统架构、功能要求、性能要求、数据要求、安全要求、运维管理、评价与改进。

本文件适用于人脸识别模型设计生成系统的开发，设计和应用。

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 38671 信息安全技术 远程人脸识别系统技术要求

GB/T 39335 信息安全技术 个人信息安全影响评估指南

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

基于自然人的面部特征对该个体的自动识别。

[来源：GB/T 38671—2020，3.1.2，有修改]

3.2

人脸样本 face sample

在人脸特征项提取之前的人脸特征特性的模拟表示或数字表示。

4 系统架构

4.1 人脸识别模型设计生成系统架构包括应用层、支撑层、网络层、硬件层、运维层和安全层。其中应用层包括系统登录、系统参数设置、人脸采集管理、客户端管理、人脸识别管理、系统数据管理、在线客服、系统管理等功能，系统框架图见图1。

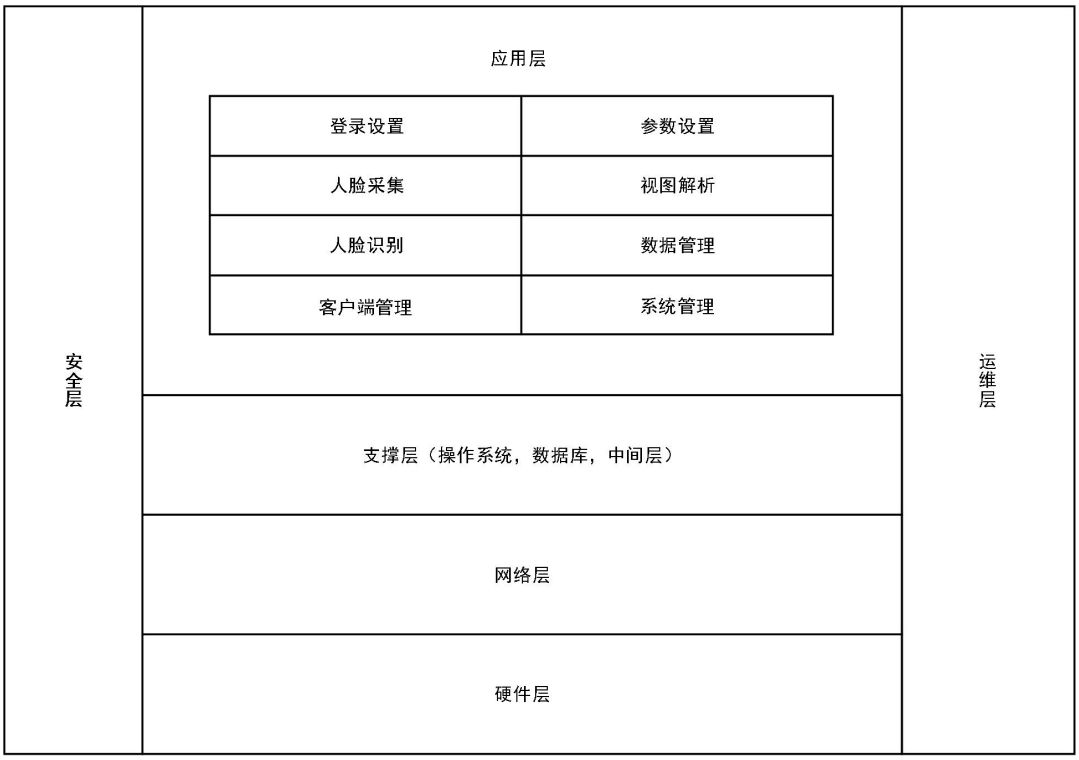

图 1　人脸识别模型设计生系统架构图

4.2　各模块功能如下：

a）　应用层：包括登录设置、参数设置、人脸采集、人脸识别、数据管理、客户端管理、系统管理；

b）　支撑层：提供系统运行所需的支撑服务；

c）　网络层：搭建数据传输通道，实现系统内外数据的交互；

d）　硬件层：为系统运行提供基础物理设备，如计算机设备及配件，保障系统正常运转；

e）　运维层：负责系统运行维护，确保系统安全、稳定，持续优化运维工作；

f）　安全层：保障系统安全，包括访问控制、隐私保护、审计、数据加密及备份恢复等。

5　功能要求

5.1　登录设置

5.1.1　人脸识别模型设计生成系统登录功能要求如下：

a）　支持用户名、密码和验证码的输入验证，仅当三者同时正确时，用户才能成功登录系统。用户名和密码在注册时设定，验证码随系统刷新自动显示，确保登录的安全性，防止非法用户访问系统；

b）　登录失败时，系统应提示“登陆失败，请重新登陆！”，并提供“确定”和“取消”按钮，方便用户操作；

c）　设置登录失败次数限制，当用户连续登录失败达到预设次数时，人脸识别模型设计系统应暂时锁定该用户的账号，不应让其继续登录，并提示用户账号已被锁定，应等待一段时间后才能再次尝试登录；

d）　人脸识别模型设计系统应记录每次登录失败的详细信息，包括登录时间、用户账号、登录 IP 地址、失败原因等。

5.1.2　人脸识别模型设计生成系统应支持多种注册方式，并符合以下要求：

a）　应支持现场注册或非现场注册；

b） 应支持人脸样本批量注册；
c） 宜满足单个用户注册多张人脸样本的需求；
d） 宜支持不同图像源的人脸注册，例如实时采集相片或已存储的相片等；
e） 可支持一种或多种采集设备采集的人脸样本；
f） 注册过程中，能与用户进行适当交互，例如提醒用户配合，提示注册成功等。

5.2 参数设置

人脸识别模型设计生成系统参数设置功能要求如下：
a） 人脸识别颜色设置：能调整人脸识别过程中的颜色参数，如白平衡、镜像、水平、垂直方向的颜色设置，以及可选颜色模式；
b） 人脸跟踪信息设置：包括人脸跟踪的开启与关闭，以及相关参数的调整，如 LED 状态（长亮、闪烁、关闭），曝光、抖动的自动或手动设置（手动设置可选择快门速度，如户外、慢、快等模式，以及频率 50 Hz 或 60 Hz），USB 带宽的自动或默认设置，同时支持对当前参数配置的加载、保存操作。

5.3 人脸采集

5.3.1 数据处理者收集人脸识别数据采集的要求如下：
a） 采集人脸识别数据时，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进行删除并确保不可恢复；
b） 应采用数据主体主动配合的措施收集人脸识别数据；应在识别过程中持续告知数据主体，并通过语言、文字等向数据主体进行提示；
c） 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。

5.3.2 人脸识别模型设计生成系统应自动判别采集对象位置，依据采集对象身高和距离自动调节采集设备。

5.4 视图解析

人脸识别模型设计生成系统应具备视图解析功能，并符合以下要求：
a） 应进行人脸检测；
b） 应进行人脸特征项提取；
c） 应对样本进行质量判断并给出判断结果，对质量判断未通过的人脸样本可提示重新采集；
d） 根据应用需求，可对人脸目标进行跟踪。

5.5 人脸识别

人脸识别模型设计生成系统的人脸识别管理要求如下：
a） 在人脸识别过程中，对人脸状态进行标记，如正常、打马赛克、面具、眼镜、帽子、动物脸、卡通脸、换场景、背景模糊等，方便用户对识别结果进行分类和统计分析；
b） 对不同的场景和遮挡情况，人脸识别模型设计生成系统应有识别能力，通过对各种人脸状态的识别和处理，提高系统在复杂环境下的准确性和可靠性。

5.6 数据管理

5.6.1 数据查询

支持对人脸识别过程中的数据进行查询，可根据时间范围（开始时间和结束时间）、姓名、源ID、比分等条件进行比中/未比中记录查询，查询结果应显示比对时间、采集图像、底图图像、姓名、获取时间等详细信息。

5.6.2 数据对比

提供图像对比功能，显示现场照片和底库照片，并给出比分，同时展示用户信息（如姓名、注册时间、性别、出生日期、国籍等）和详细信息，支持从文件打开或打开摄像头获取图像进行对比，用户可设置重复阈值（0～1）进行比对验证，并查看比对结果。

5.6.3 数据储存

5.6.3.1 人脸识别模型设计生成系统应具备数据存储功能，当人脸参考存储在人脸识别模型设计生成系统内时，应符合以下要求：

a) 支持人脸参考存储到人脸注册数据库，并返回人脸参考标识符；
b) 每个用户的人脸参考对应唯一人脸参考标识符；
c) 支持人脸参考标识符删除操作，删除后该标识符及对应人脸参考失效；
d) 支持人脸参考标识符查询操作，并确认人脸参考标识符及对应人脸参考是否有效。

5.6.3.2 当人脸参考存储在人脸识别系统外（例如用户令牌）时，人脸识别系统应能获取并使用人脸参考。

5.6.4 数据使用

数据处理者使用人脸识别模型设计生成系统数据的要求如下：

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；

注：可更新指当特定人脸特征泄漏或作废时，同一人脸图像可提取与该特征不同的人脸特征；不可逆指无法从人脸特征恢复出对应的人脸图像。不可链接指同一人脸图像提取的不同人脸特征之间不具备关联性。

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；

注：本地人脸识别是在终端设备中进行人脸识别数据收集、使用等处理活动的过程，该方式中人脸识别数据的处理均在终端设备完成。远程人脸识别是在终端设备收集人脸识别数据，在服务器端使用人脸识别数据的过程，该方式中人脸识别数据的处理在终端设备和服务器端分别进行。

d) 应对人脸识别数据使用行为进行审计。

5.7 客户端管理

5.7.1 服务地址配置

对摄像机人脸识别过程的客户端程序进行管理，包括设置程序名称、特征提取服务URL、对比服务URL、通知服务URL等。

5.7.2 参数保存

提供保存功能，将配置好的客户端参数进行保存。

5.8 系统管理

人脸识别模型设计生成系统应具备人脸识别管理功能，并符合以下要求：

a) 日志管理：应支持授权用户对日志进行查询和导出等；
b) 权限管理：应支持配置用户操作权限；
c) 接口配置：应对应用开放接口、协议接口、硬件接口等进行配置；
d) 用户管理：可进行用户信息的增加、修改、删除、查询、停/启用等；
e) 在线客服管理要求如下：
   1) 用户在使用人脸识别模型设计生成系统过程中，可随时与在线客服进行实时沟通，咨询问题、寻求帮助或反馈意见；
   2) 客服应提示用户留下联系方式，在问题无法及时解决时，进行后续跟进处理。

6 性能要求

6.1 人脸检测精度

人脸检出率不应低于90%，人脸误检率不应大于5%。

6.2 响应时间

人脸识别模型设计生成系统响应时间符合以下要求：

a) 人脸验证时，人脸识别模型设计生成系统平均响应时间不应大于 2 s；
b) 人脸辨识时，人脸识别模型设计生成系统平均响应时间不应大于 2 s。

6.3 可靠性

无故障工作时间应至少达到500000 h。

6.4 兼容性

人脸识别模型设计生成系统兼容性符合以下要求：

a) 应兼容不同配置的服务器；
b) 应兼容不同操作系统；
c) 应兼容不同浏览器；
d) 应兼容主流硬件平台。

7 数据要求

7.1 数据传输

数据处理者应采取双向身份鉴别、数据完整性校验、数据加密等措施保障人脸识别数据传输安全。

7.2 数据公开

数据处理者提供、公开人脸识别数据的要求如下：

a) 除非经数据主体单独同意或书面同意，不应公开人脸识别数据；
b) 不宜向第三方提供或委托处理人脸识别数据。因业务确需提供或委托处理的，应符合的安全要求包括但不限于：
    1) 按 GB/T 39335 规定的要求对数据接收方开展安全评估，并通过合同等方式约定提供或委托处理的目的、期限、方式、保护措施等，并对数据接收方的处理活动进行监督；
    2) 在提供或委托处理前，单独告知数据主体人脸识别数据向数据接收方提供或委托的目的数据接收方身份，接收方数据安全能力、数据类别、可能产生的影响等相关信息，并征得数据主体单独同意或书面同意；
    3) 数据接收方应按约定处理人脸识别数据，不应超出约定目的、方式等处理人脸识别数据，不应转委托；数据接收方应采取安全措施保障所处理的人脸识别数据安全；委托不生效、无效、被撤销或终止的，数据接收方应将人脸识别数据返还，并予以删除，不应保留或恢复。
c) 因合并、分立等原因转移人脸识别数据的，应向数据主体告知数据接收方的身份、联系方式；数据接收方应继续履行数据处理者的保护义务；数据接收方变更处理目的、处理方式的，应重新向数据主体告知并取得数据主体单独同意或书面同意；没有数据接收方或未取得数据主体单独同意或书面同意的，应删除人脸识别数据并确保不可恢复。

7.3 数据加密

人脸识别模型设计生成系统数据加密要求如下：

a) 应对存储和传输的数据进行加密处理；
b) 应采取双向身份鉴别、数据完整性校验、数据加密等措施保障人脸识别数据传输安全；
c) 在系统运行中出现致使信息丢失或致使系统无法运行的故障时能进行信息恢复，备份和恢复应。

7.4 数据删除

数据处理者在发生以下情况时，应在15日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、无法实现或者为实现处理目的不再必要；

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。

8 安全要求

8.1 访问控制

访问控制要求如下：

a） 建立访问控制策略，通过对主、客体设置敏感标记，实现对用户、设备、应用程序等不同主体不同粒度的访问控制机制；

注：系统中有两类主体：一类是特权用户，包括系统管理员、系统安全员和系统审计员；另一类是处理专门事务的系统进程。系统中的客体是指主体所能操作的对象，包括作为图像处理、数据存储的对象和为用户服务的进程。前者主要包括：已登记人脸模板、人脸采集样本、识别结果；后者主要包括：系统管理员操作进程、数据库操作进程、安全员操作进程、审计员操作进程。

b） 人脸识别模型设计生成系统的用户应有唯一标识，支持通过用户名和密码进行身份鉴别。采用用户名和密码认证的密码的长度应不少于 8 个 ASCII 字符，并由数字、字符和特殊符号组成。

8.2 个人信息保护

人脸识别模型设计生成系统应对用户人脸模板等公民个人隐私信息进行保护，包括但不限于以下功能：

a） 无关联保护：应防止通过应用程序或数据库关联到存储的人脸模板数据；
b） 机密性保护：应防止非授权用户对人脸模板数据的访问。

8.3 安全审计

生成审计记录（记录应包含事件发生的时间、事件类型和主体身份），对审计数据按权限进行分级访问控制。

9 运维管理

9.1 基本要求

人脸识别模型设计生成系统的运行和维护，包括系统及其运行环境的运行维护、数据维护等要求。人脸识别模型设计生成系统运行维护基本要求包括但不限于：

a） 对系统、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；
b） 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；
c） 建立知识库，收集、积累、共享和使用运行维护数据和经验，持续改进运行维护服务。

9.2 日常维护

人脸识别模型设计生成系统日常维护包括但不限于：

a） 人脸识别模型设计生成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、木马人侵等风险，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模型设计生成系统的监控指标、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；

注：运行环境状态包括底层资源的统一监控，如计算机处理器利用率、数据库运行状态、系统负载等。

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） 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；
e） 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；

f） 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。

10 评价与改进

依据第5章～第9章的要求确定系统的评价内容，定期开展系统功能、性能、数据、安全、运维方面的评价，审查不合格项，并有针对地采取纠偏措施。