ICS 35.040.50
CCS L81

团　体　标　准

T/CIQA xxx - 2023

AI 鉴定通用规范

AI Qualification General Specification

2023-XX-XX 发布　　2023-XX-XX 实施

中国出入境检验检疫协会　发 布

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》给出的规则起草。

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。

本文件由中国出入境检验检疫协会奢侈品行业标准化技术委员(CIQA/TC15)提出并归口。

本文件起草单位：图灵深视（北京）科技有限公司、图灵深视（杭州）科技有限公司、浙江阿里巴巴闲鱼网络科技有限公司、北京传祁拍拍网络科技有限公司、大连津如珠宝有限公司、中奢鉴（北京）科技发展有限责任公司。

本文件主要起草人：唐平中、李俊、李佳、李志恒、于冰洁、刘明伟、张琛、祁伟伟、游静波、潘佳琳。

AI 鉴定通用规范

1 范围

本文件规定了电子商务中产品的 AI 鉴定算法数据处理流程、目标检测、图片质量评估、目标分类、集成、准确率评估等相关技术，以及鉴定报告的具体规范。

本文件适用于具有计算机视觉，深度学习能力的公司获取数据、进行模型训练、搭建人工智能鉴定系统。

注：本文件适用的部分电子商务产品包括：奢侈品品牌的箱包、腕表、鞋履、服装、珠宝玉石等，详情见附录 A。

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 5721.28—2001 信息技术 词汇 第 28 部分：人工智能 基本概念与专家系统

GB/T 5721.34—2006 信息技术 词汇 第 34 部分：人工智能 神经网络

3 术语、定义和缩略语

3.1 术语和定义

GB/T 5721.28—2001、GB/T 5721.34—2006 界定的以及下列术语和定义适用于本文件。

3.1.1

人工智能 Artificial Intelligence

一门交叉学科，通常视为计算机科学的分支，研究表现出与人类智能（如推理和学习）相关的各种功能的模型和系统。

[GB/T 5271.28—2001,定义 28.01.01，有修改]

3.1.2

机器学习 Machine Learning

功能单元通过获取新知识或技能，或通过整理已有的知识或技能来改进其性能的过程。

[GB/T 5271 .31—2006,定义 31.01.02]

3.1.3

深度学习 Deep Learning

深度学习是机器学习的分支，是一种以人工神经网络结构对数据进行表征学习的算法。

[T/SIA 006—2018，定义 2.3]

3.1.4

神经网络 Neural Network

由加权链路且权值可调整连接的基本处理元素的网络，通过把非线性函数作用到其输入值上使每个单元产生一个值，并把它传送给其他单元或把它表示成输出值。

注 1：虽然某些神经网络旨在模拟神经系统中神经元的功能，但大多数神经网络用于人工智能以实现连接模型。

注 2：非线性函数的例子是阈值函数、sigmoid 函数以及多项函数。

3.1.5

计算机视觉 Computer Vision

功能单元获取、处理和解释可视化数据的能力。

3.1.6

目标检测 Object Detection

找出图像中所有感兴趣的目标（物体），确定它们的类别和位置的过程。

3.1.7

目标分类 Object Classification

对图像中的目标进行分类的过程。

3.1.8

数据增强 Data Augmentation

一种通过让有限的数据产生更多的等价数据来人工扩展训练数据集的技术。

3.1.9

对抗生成网络 Generative Adversarial Net

是一种深度学习模型，通过框架中的生成模型和判别模型的互相博弈学习产生相当好的输出。

3.1.10

语义分割 Semantic Segmentation

通过查找像素，识别图像中存在的内容以及位置。

3.1.11

人工智能鉴定 Artificial Intelligence Authentication

通过以计算机视觉为主的人工智能技术，对商品和证照的制作工艺和印刷字体等进行客观的真伪鉴别的过程。

3.1.12

鉴定点 Authentication Feature

是指 AI 鉴定或者人工鉴定关注的商品的特殊部位，这些部位正品和仿品存在可分辨差异，详情见附录 A。

3.1.13

训练数据 Train Data

数据挖掘过程中用于数据挖掘模型构建的数据。

3.1.14

真标签 True Label

符合正品工艺的待鉴定物品标注为真。

3.1.15

假标签 False Label

不符合正品工艺的待鉴定物品标注为假。

3.2 缩略语

下列缩略语适用于本文件。

AI：人工智能 （Artificial Intelligence）

NN：神经网络 （Neural Network）

GAN：对抗生成网络 （Generative Adversarial Net）

IOU ：交并比（Intersection over Union）

YOLO：一种目标检测方法（You Only Look Once）

SKC: 库存颜色单位（Stock Keeping Color）

4 性能要求

4.1 时效性

上传图片后系统在 10s 内应给出鉴定结果。

4.2 智能性

AI 鉴定整个技术（除了拍照）应由计算机完成，无需人干预，并保证准确率大于 90%。

4.3 鲁棒性

在不同拍摄环境、拍摄角度下，图片应清晰，同一个鉴定点多次测试，系统应在 95%以上的概率给出一致的结果。

4.4 准确性

在符合相应图片质量要求前提下，AI 鉴定结果的准确率仅对所提供的图片做判断，且应不低于人工鉴定师在无实物的情况下只看图片得出的鉴定结果的准确率，最低准确率应高于 90%。

5 图片信息要求

图片信息库应符合如下要求：

a） 收集的图片需要确保清晰，最短边分辨率应高于 400 个像素值，且鉴定点无遮挡；

b） 同时有真假商品的图片，图片来自于合作的各大商家，且均被授权使用；

c） 单张图片大小应不低于 500k。

6 硬件

硬件应符合如下要求：

a）训练设备（服务器）需有显卡，且显存大小至少 16G；

b）训练设备（服务器）具有操作系统，能安装主流的深度学习框架，支持编程软件使用；

c）部署设备需要保证网络畅通，长时间处于联网状态。

7 相关人员要求

从事 AI 鉴定系统开发人员应具备：

a）了解电子商务、质量安全、消费权益等相关的法律法规知识；

b）对商品的鉴定有一定的专业知识；

c）了解人工智能技术，具有计算机视觉专业知识，了解深度学习，对目标检测，目标分类有相关研究；

d）了解显卡，服务器部署方法。了解深度学习相关框架，使用方法；

e）具有代码能力，了解至少一门编程语言。

8 训练数据要求

8.1 数据增强

数据增强不仅可以解决类别数据不均衡的问题，还可以提升算法在不同场景下的鲁棒性，防止因输入图片细微的光照改变、角度变换造成鉴定得分的巨大差异。常见数据增强方法如下：

a）传统数据增强方法：通过平移（随机上下左右移动 30%以内）、旋转（旋转角度主要包括 0°~30°、90°和 180°）、颜色变换（调整对比度、亮度）等操作将图像场景多样化；

b）深度学习增强方法：通过对抗生成网络生成以假乱真的图片来扩充缺失数据。

8.2 训练数据处理

在数据成为训练数据前，应完成如下处理流程：

a） 将数据以品类、品牌或系列为单位进行整合，同时将无效数据（非品类、品牌、系列、非鉴定点）清洗出去；

b） 经过 a） 步骤后，将符合要求的图片数据交由品牌方和具有中检资质认证的鉴定师进行复核，每张图得到可靠的真假标签；

c） 将得到可靠的标签（真、假标签）后的数据进行鉴定点标注，标注图片中具有鉴定信息区域的位置和鉴定点名称；

d） 经过 c）步骤后得到的图片用于检测模型的算法训练和优化；

e) 使用 c）步骤的标注信息将图片按照鉴定点割取出来，仅使用具有鉴定信息的区域和真假标签进行鉴定模型的训练和优化。

如图 1 所示，表示了数据所经历的三个最主要的处理过程。

图 1 算法训练数据处理流程

9 AI 鉴定系统

9.1 AI 鉴定系统模块

如图 2 所示，AI 鉴定算法模块应包含目标检测、图像质量评估、目标分类、集成四个模块。

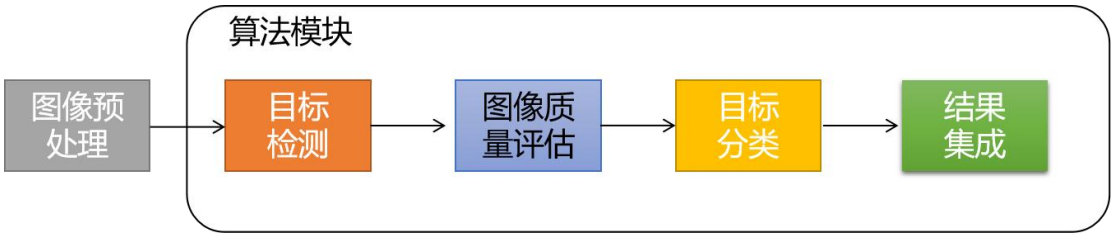

图 2 AI 鉴定算法模块流程图

9.2 目标检测

9.2.1 必要性

目标检测的任务是通过深度学习方法找出图像中的目标物体，确定它们的类别和位置。AI 鉴定整个算法流程中引入目标检测，不仅可以判断输入图片是否含有鉴定点，确定鉴定点的具体名字，还可以精准地定位到鉴定点所在位置。

图 3 为目标检测的一个结果示例图，检测到一个目标，预测类别为“包”,置信度为 0.813，位置用红色矩形框框出。将目标精准的定位出来既可以检测输入图片鉴定点是否正确，亦可根据位置信息将目标切割出来，防止复杂背景对鉴定结果造成干扰。

图 3 目标检测结果示例图

9.2.2 训练数据量要求

经过 8.1 数据增强和 8.2 训练数据处理后，训练数据量应达到以下条件：

a) 各鉴定点的数据量在 1000 张以上;

b) 正样本（有标注图片）和负样本（没有鉴定意义的图片）比例控制在 5:1。

9.2.3 准出条件

AI 鉴定的目标检测算法应具备以下几点：

a) 为确保 AI 鉴定结果的实时性，目标检测算法应在 1S 内出结果；

b) 为确保目标检测区域的精确度，算法的 IOU 应高于 0.7；

c) 目标检测算法的准确率应大于 0.95；

d) 目标检测算法的召回率应大于 0.9。

9.3 图像质量评估

9.3.1 必要性

基于项目本身数据特征，在鉴定点拍摄时，可能会存在模糊、反光、图片过小等问题，将这类图片输入分类网络中会大大影响鉴定结果的准确性。因此，针对图片质量的判断模型很有必要。如图 4 所示，图像质量评估模型可利用语义分割技术，该技术对每个像素点逐个进行分类判断，黑色部分代表图片中的模糊区域，其中得分越高，代表该张图片越模糊。

图 4 部分模糊拒鉴结果示例图

9.3.2 训练数据要求

图像质量评估模型训练数据包括两大类，符合鉴定要求的图片数据和不符合鉴定要求的图片数据。

a) 符合鉴定要求的图片：像素值高且目标最长边大于 224 个像素值，鉴定信息完整，没有遮挡的鉴定点图片。

b) 不符合鉴定要求的图片：图片模糊，反光，最长边小于 224 个像素值，存在遮挡，非鉴定区域等情况的鉴定点图片。

9.3.3 准出条件

图像质量评估模型应具备以下条件：

a) 为确保 AI 鉴定结果的实时性，图像评估算法应在 1S 内出结果；

b) 图像评估模型的结果和人为感知符合度应高于 95%。

9.4 目标分类

9.4.1 目标分类网络

经过 9.2 目标检测和 9.3 图像质量评估合格后的鉴定点图片，输入到分类网络中，进行真假鉴定。目标分类网络通过深度学习方法，判断一张图片属于真类别还是假类别。图 5 为目标分类结构示例图，输入一张合格的鉴定点图片，通过隐藏层提取特征，最终层输出真假类别。

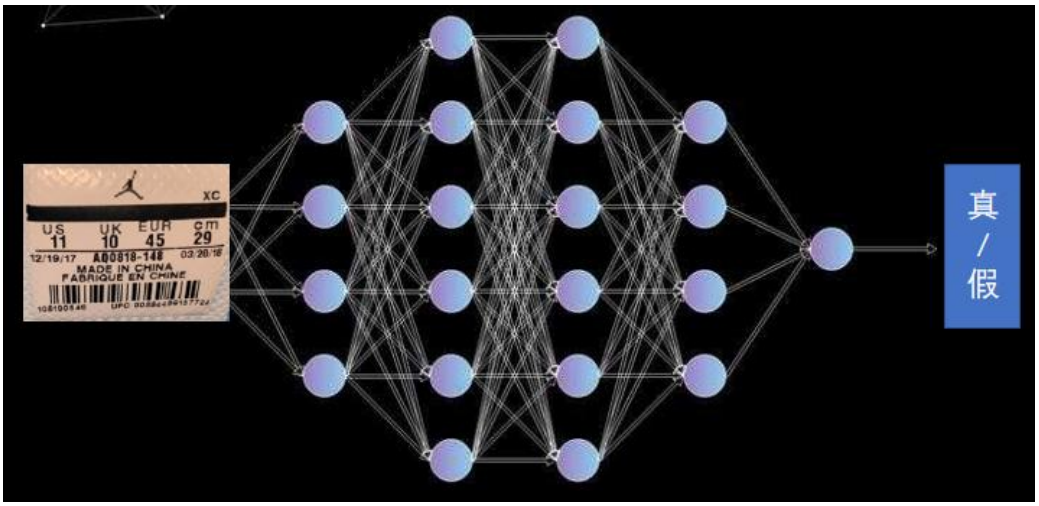

图 5 目标分类结构示例图

9.4.2 训练数据量要求

经过 8.1 数据增强和 8.2 训练数据处理后，应达到以下数量的要求，才能得到一个可使用的真假分类模型。

a) 各个鉴定点的数据量在 2000 张以上；

b) 单个鉴定点的真假数据量相差不要超过 500 张；

c) 鉴定点数据应包括该品类 80%的 SKC；

d) 根据标注信息将鉴定点区域割取下来，排除背景等无关信息的干扰，进行分类模型的训练。

9.4.3 准出条件

目标分类模型应具备以下条件：

a) 为确保 AI 鉴定结果的实时性，分类算法应在 1S 内给出结果；

b) 各鉴定点的真假分类准确率应高于 90%。

9.5 结果集成

9.5.1 必要性

通过考虑各个鉴定点结果和得分，设计集成逻辑，给出整个商品鉴定结果。集成可以提

升最终鉴定结果准确率和鲁棒性。

9.5.2 集成方案

集成应考虑并确定如下因素：

a）根据鉴定师意见，以及算法准确率，确定每个鉴定点的权重；

b）确定最少拍摄鉴定点数，每个鉴定点的重要性，以及哪些鉴定点的拍摄必不可少；

c）针对单个鉴定点，多个方法给出的结果，进行集成。

9.5.3 准出条件

集成应达到如下效果：

a）明确给出最终鉴定结果；

b）对单个鉴定结果进行集成后准确率有所提升。

10 鉴定报告

如图 6 所示，鉴定报告应包括以下信息：

a）整体鉴别结论：告知待鉴别商品是否符合正品工艺或无法鉴别，符合正品工艺为真，不符合正品工艺为假；

b）鉴别品牌：展示待鉴别商品的品牌；

c）鉴定报告出具机构：鉴定报告中要显示出具该报告的机构，若有多个机构，应全部列出

d）鉴定详情：显示各个鉴定点的检测结果和鉴定得分，其中单鉴定点得分越高，代表该鉴定点跟正品工艺符合程度较高。

图 6　鉴定报告示例图

11 整体鉴定准出条件

11.1 测试数据准备

为保证测试结果的客观公正性，测试样本的选择应符合以下条件：

a) 每个品牌最少准备真假各 500 个测试样本，且样本清晰无遮挡，涵盖该品牌的所有款式；

b) 假数据中要包括高仿、低仿，真数据要注意平衡经典款和中古款之间的数据量；

c) 由品牌方和资深鉴定师确保真假标签的准确性。

11.2 整体鉴定准确率统计

根据集成逻辑进行整体集成后，最终得到待鉴定目标的真假。准确率的计算方式如下：

a) 真数据的样本总量为 A_t，AI 鉴定测试结果为真的数据量为 B_t，则真数据的准确率 acc_t 按公式(1)计算：

$$acc_t = \frac{B_t}{A_t} \tag{1}$$

b) 假数据的样本总量为 A_f，AI 鉴定测试结果为真的数据量为 B_f，则假数据的准确率 acc_f 按公式(2)计算：

$$acc_{\mathrm{f}} = \frac{B_{\mathrm{f}}}{A_{\mathrm{f}}} \tag{2}$$

c）统计所有样本中无法鉴定的数据，记为 C，无法鉴定率 d 按公式(3)计算：

$$d = \frac{C}{A_{\mathrm{t}} + A_{\mathrm{f}}} \tag{3}$$

11.3 准出条件

a）真假数据整体鉴定准确率应大于 92%;

b）真假整体鉴定准确率相差应小于 5%，否则准确率有明显的倾向性，不能达到准出要求；

c）无法鉴定率应小于 10%。

12 国内外标准情况与有关法律法规和强制性标准的关系

a）本文件是为解决会员单位实际问题而提出的，经查新，国内外目前均无该专业内容要求的标准。

b) 本文件与有关的现行法律、法规和强制性国家标准无冲突和交叉。

c) 本文件是填补现行标准体系的空白。

d）本文件中数据获取需相关符合国家相关法律法规

附录 A
（规范性）

（部分）产品鉴定点要素如表 A.1 所示。

表 A.1 （部分）产品鉴定点要素

类别	关键要素	辅助要素
箱包类	皮签、五金刻字、拉链、防伪标、黑标等具有重要鉴定意义的鉴定点符合品牌方的制作工艺。	皮质、油边和走线等符合品牌方的制作工艺。
腕表类	表盘、表背和表把等具有重要鉴定意义的鉴定点符合品牌方的制作工艺。	配件和附件等符合品牌方的制作工艺。包括保卡、盒子、证书、钻卡以及表带刻字等。
鞋履类	鞋标、背胶、走线、鞋盒侧标和鞋盒钢印等具有重要鉴定意义的鉴定点符合品牌方的制作工艺。	配件和附件等符合品牌方的制作工艺。包括鞋撑、吊牌等。
衣服类	吊牌、水洗标和领标等具有重要鉴定意义的鉴定点符合品牌方的制作工艺。	配件和附件等符合品牌方的制作工艺。包括衣袋二维码、摆织标和 LOGO 刺绣等。
珠宝玉石类	材质、密度和折射率、等具有重要鉴定意义的鉴定点符合该类珠宝玉石的工艺。	透光性和荧光反应 等符合该类珠宝玉石的工艺。