

# T/GDAF

## 广东省公共安全技术防范协会团体标准

T/GDAF ×××—20××

### 人像识别产品测试流程规范

Specification for testing process of portrait recognition products

(征求意见稿)

2023-09-01

××××—××—××发布

××××—××—××实施

广东省公共安全技术防范协会 发布



# 目 次

前言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 文档要求 .....	2
4.1 一般要求 .....	2
4.2 测试计划要求 .....	2
4.3 测试记录要求 .....	2
4.4 测试结果要求 .....	3
5 机构要求 .....	3
5.1 合规资质 .....	3
5.2 质量控制和过程规范 .....	3
5.3 数据保护和隐私保护 .....	3
5.4 专业报告和沟通能力 .....	3
6 人员要求 .....	3
6.1 技术背景 and 知识 .....	3
6.2 测试经验和技能 .....	3
6.3 数据保护和隐私意识 .....	3
7 流程规范 .....	4
7.1 测试计划设计 .....	4
7.2 测试用例设计 .....	4
7.3 测试工作准备 .....	5
7.4 测试执行 .....	5
7.5 测试结果 .....	7

## 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这些专利的责任。

本文件由广东省公安厅办公室科技信息化处提出。

本文件由广东省公共安全技术防范协会归口。

本文件起草单位：

本文件主要起草人：

# 人像识别产品测试流程规范

## 1 范围

本文件适用于人像识别产品,为人像识别产品的测试流程提供方法。规定了人像识别产品测试流程。

## 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 25000.51-2016 就绪可用软件产品的质量要求和测试细则

GB/T 26238—2010 信息技术 生物特征识别术语

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

GB/T 41819-2022 信息安全技术 人脸识别数据安全要求

GA/T 893—2010 安防生物特征识别应用术语

GA/T 1756-2020 公安视频监控人像/人脸识别应用技术要求

## 3 术语和定义

GB/T 26238—2010和GA/T 893—2010界定的以及下列术语、定义和缩略语适合于本文件。

### 3.1

**人像识别** vision Human visual recognition

通过人脸信息,人体体态等人体特征判断人物的过程。

### 3.2

**人脸检测** face detection

对于给定的静态图像或动态图像,判断其中是否存在人脸。如果存在,确认人脸具体的位置和大小。

### 3.3

**人体检测** human body detection

基于业界领先的AI技术准确地检测出图片或视频中的人体,并返回高精度的人体矩形框坐标。

### 3.4

**误识率** false acceptance rate

不同人像的匹配分数大于给定阈值,从而被认为是相同人像的比例。

### 3.5

**误拒率** false rejection rate

相同人像的匹配分数小于给定阈值,从而被认为是不同人像的比例。

### 3.6

**识别正确率** Recognition accuracy

相同人像的匹配分数大于给定阈值,从而被认为是相同人像的比例。

### 3.7

**误识次数** Number of false identifications

本该匹配失败的人像被判断为匹配成功人像的次数。

### 3.8

**误拒次数** Number of false rejection

本该匹配成功的人像被判断为匹配失败人像的次数。

### 3.9

**类间测试** Interclass test

不同目标人物进行人像识别的测试。

### 3.10

**类内测试** In class test

同一目标人物进行人像识别的测试。

## 4 文档要求

### 4.1 一般要求

4.1.1 依据 GB / T 25000. 51-2016 就绪可用软件产品的质量要求和测试细则，测试文档一般包含：

- a) 测试计划；
- b) 测试说明；
- c) 测试结果（报告）。

4.1.2 每个测试文档都应包括：

- a) 标题；
- b) 修订历史；
- c) 目录；
- d) 该文档正文中引用的文档的标识符；
- e) 有关作者和审查者的信息。

### 4.2 测试计划要求

#### 4.2.1 资源

- a) 明确测试活动所需要的人力资源；
- b) 明确测试执行所需的工具和环境资源。

#### 4.2.2 进度

- a) 规定资源环境准备进度；
- b) 规定文档编制进度；
- c) 规定测试执行。

### 4.3 测试记录要求

- a) 测试目标；
- b) 详细实施步骤；
- c) 实施结果结论；
- d) 执行人员记录；
- e) 执行时间记录。

#### 4.4 测试结果要求

- a) 执行结果的汇总;
- b) 发现的异常清单;
- c) 实施结果结论;
- d) 执行人员;
- e) 执行地点;
- f) 执行时间。

### 5 机构要求

#### 5.1 合规资质

测试机构应该具备相关的合规资质和认证,符合国家和行业的测试标准和要求。应该具备至少一项相关的测试认证或资质证书,如ISO 17025认可证书、CNAS认可证书等。

#### 5.2 质量控制和过程规范

测试机构应该建立有效的质量控制和过程规范,确保测试工作的可靠性和一致性。包括确立标准化的测试流程和规范化的测试方法,制定相应的测试计划和测试用例,进行测试结果的评估和分析。

#### 5.3 数据保护和隐私保护

考虑到人像识别产品测试涉及到用户的个人隐私和数据安全,测试机构需要具备相关的数据保护和隐私保护措施。测试机构应该建立保密协议和数据安全管理制度,确保测试过程中的数据安全和隐私保护。

#### 5.4 专业报告和沟通能力

测试机构应该能够提供专业的测试报告,并能够清晰、准确地向项目方或委托方进行测试结果的沟通和解释。他们应该具备良好的沟通和协调能力,与项目组成员、开发人员等进行有效的合作和交流。

### 6 人员要求

#### 6.1 技术背景和知识

测试人员应该具备相关的技术背景和知识,了解人像识别的基本原理、算法和技术。他们应该熟悉常见的人像识别算法和工具,理解其应用场景和限制。

#### 6.2 测试经验和技能

测试人员应该具备一定的测试经验和技能,包括测试计划编写、测试用例设计、测试环境搭建、问题分析和解决。

#### 6.3 数据保护和隐私意识

考虑到人像识别涉及到个人隐私和数据安全等重要问题,测试人员需要具备数据保护和隐私意识。他们应该严格遵守相关法律法规,尊重用户隐私权,妥善处理测试数据,并确保数据的安全性和保密性。

7 流程规范

人像识别产品的测试流程如图1:

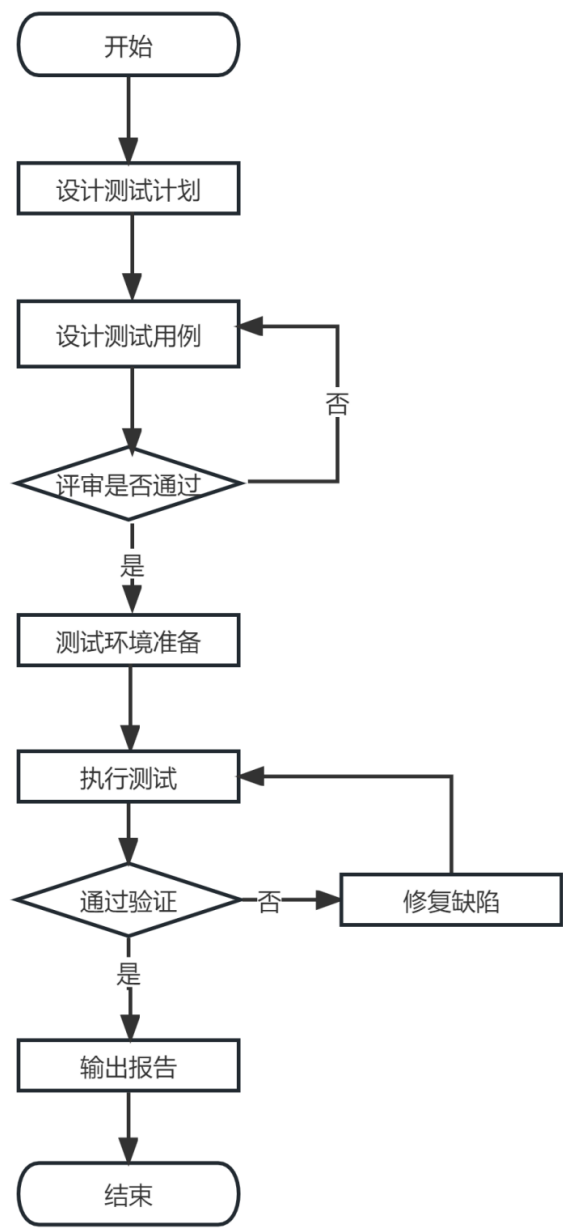


图1 测试流程图

7.1 测试计划设计

测试前应制定详细测试计划, 测试计划从测试环境设计、测试对象的组成、测试对象的通行方式、测试流程等方面进行具体规定, 指导测试的进行。

7.2 测试用例设计



7.2.1 测试用例设计，应遵循基于测试需求，充分覆盖兼顾效率的原则，必须保证覆盖测试需求的基础上能有效率的得到执行；

7.2.2 测试用例设计，应体现测试遵循标准的质量特性和所使用的测试方法，测试结果的评判准则等因素，确保测试的过程符合标准和规范；

7.2.3 测试用例设计，必须考虑可执行性和可再现性，若存在自定义的输入项，需恒定输入内容，预置条件清晰、预期结果明确，测试项步骤描述简洁清晰，确保能被测试执行人员所理解和执行，同时保证测试过程中发现的缺陷的可再现性。

### 7.3 测试工作准备

根据测试计划的要求，准备测试人力、工具资源，此外，人像识别产品的测试数据资源应满足以下要求：

- a) 测试对象的通行方式应从测试数据库中，选择被测系统人群的典型通行方式；
- b) 测试宜从标准数据库选取图片、视频录像，可补充应用现场测试。如为第三方测试，则应选取符合相关标准要求的测试数据集；
- c) 在利用视频录像进行测试的情况下，应保证视频录像的播放速度与录制速度相同；
- d) 在无法采用视频录像方式测试时，可在同一现场环境下搭建测试平台，多次测试的视频源应一致。

### 7.4 测试执行

基于已建立的数据库导入到待测试的人像识别系统中，根据系统对应功能对系统完成人像识别过程。

#### 7.4.1 功能性

- a) 人像检测：导入图像或视频，检测图像或视频中的人像，并对其进行框选和标识；
- b) 人像特征提取：查看是否能够将检测到的人像转换为独特的数字特征，用于后续的比对和匹配；
- c) 人像比对：将两张或多张人像图片进行比对和匹配，判断它们是否属于同一个人；
- d) 人像搜索：在大规模人脸数据库中进行快速搜索，找到目标人物的相关信息；
- e) 人像追踪：对视频流中的人像进行实时跟踪，实现对目标人物的追踪和监控；
- f) 数据统计查询：对人像数据库中的数据进行汇总、整理和查询；
- g) 系统管理维护：对人像识别系统进行管理和维护，包括用户权限、数据备份、故障处理等方面。

#### 7.4.2 识别准确率

从测试数据库中选取原始图像集，进行人像识别，统计识别出的误识、误拒及正确识别的数量，计算误识率、误拒率和识别正确率。

##### a) 误识率

不同人像的匹配分数大于给定阈值，从而被认为是相同人像的比例，简单地说就是“把不应该匹配的人像当成匹配的人像”的比例。

$$\text{误识率} = \frac{\text{误识次数}}{\text{类间测试总次数}} = \frac{\text{本该匹配失败的人像判为匹配成功的次数}}{\text{不同人识别的总次数}} \times 100\%$$

##### b) 误拒率

相同人像的匹配分数小于给定阈值，从而被认为是不同人像的比例，简单地说就是“把应该相互匹配的人像当成不能匹配的人像”的比例。

$$\text{拒识率} = \frac{\text{误拒次数}}{\text{类内测试总次数}} = \frac{\text{本该匹配成功的人像判为匹配失败的次数}}{\text{同一个人识别的总次数}} \times 100\%$$

### c) 识别正确率

相同人像的匹配分数大于给定阈值，从而被认为是相同人像的比例，简单地说就是“正确将相互匹配的人像识别出来”的比例。

$$\text{识别正确率} = \frac{\text{正识次数}}{\text{测试总次数}} = \frac{\text{本该匹配成功的人像判为匹配成功的次数}}{\text{测试总次数}} \times 100\%$$

## 7.4.3 安全性

参考《GB/T 41819-2022 信息安全技术 人脸识别数据安全要求》和《GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》，从数据采集规范安全性测试。

- a) 查看收集人像识别数据时，是否向数据主体告知人脸人像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；
- b) 查看收集年满 14 周岁未成年人的个人信息前，是否征得未成年人或其监护人的明示同意；不满 14 周岁的，是否征得其监护人的明示同意；
- c) 查看未取得数据主体单独同意收集的人像是否立即删除并确保不可恢复；
- d) 当数据主体不同意收集人像识别数据的，是否拒绝数据主体使用基本业务功能；
- e) 查看自动采集个人信息的频率是否实现产品或服务的业务功能所必需的最低频率；
- f) 是否采用需要数据主体主动配合的措施收集人像识别数据；在识别过程中是否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；
- g) 是否提供处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式；
- h) 个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则是否合理。

## 7.4.4 数据保护

从数据传输和数据存储规范数据保护测试。

- a) 参考 GB/T 41819-2022 信息安全技术 人脸识别数据安全要求，应查看是否采用物理或逻辑隔离方式分别存储人像识别数据和个人身份信息等；
- b) 查看是否在使用人像识别数据识别自然人身份后立即删除用于识别的人像；
- c) 以任意非常规方法修改所要求的数据，如直接进入数据库内修改，修改后在系统内访问该数据，查看系统是否识别；
- d) 查看系统的日志内每条数据是否记载操作者/发起者；
- e) 查看系统的日志内每条数据是否记载接收者；
- f) 验证所收集数据的授权情况，确保收集的数据不会被未经授权的人或机构获取和利用；
- g) 查看所提交的指定数据是否加密，脱敏显示数据是否可复制，进入数据库查看敏感数据是否加密；
- h) 验证日志是否需要解密才能查看，敏感信息如姓名、手机、IP 是否均被脱敏处理；
- i) 在用户使用前，验证是否能判定用户的授权是否正确且唯一；
- j) 查看登录页面是否有双重身份认证；
- k) 修改密码查看系统是否对口令进行限制，同一账号连续输入多次错误口令，查看是否锁定账号；
- l) 修改用户系统权限，执行修改后相关权限，系统不会因用户的权限的改变造成混乱；
- m) 验证安装文件是否能防止被反编译并被篡改；

- n) 查看是否针对用户进行分级分权管理，分为超管角色、业务角色与普通用户角色；
- o) 当进行远程管理时，是否采取必要措施、防止鉴别信息在网络传输过程中被窃听。验证日志是否需要进行解密才能查看，敏感信息如姓名、手机、IP 是否均被脱敏处理。

## 7.5 测试结果

### 7.5.1 功能性测试结果

- a) 不存在系统缺陷严重性等级为致命和严重的缺陷；
- b) 系统缺陷严重性等级为一般性的错误数量：不超过全部用例数的 5%；
- c) 缺陷严重性等级见表 1，以上 a) 和 b) 同时满足时，该人像识别系统是可用的，否则为不可用。

表1 缺陷严重性等级划分准则

等级	缺陷严重性等级	说明
1	致命	1) 系统或程序引起死机； 2) 系统崩溃、意外退出； 3) 程序死循环、数据库发生死锁； 4) 因错误操作导致的程序中断； 5) 功能不可使用或错误、数据计算错误； 6) 与数据库连接错误、数据通讯错误。
2	严重	1) 功能未实现或实现错误； 2) 数据计算错误、产生错误结果； 3) 数据通讯错误、程序接口错误； 4) 数据库的表、业务规则、缺省值未加完整性等约束条件； 5) 数据约束错误、数据输入输出错误； 6) 程序流程不合理； 7) 功能设计不符合业务场景； 8) 接口不完备； 9) 状态不正确。
3	一般	1) 打印内容、格式错误； 2) 简单的输入限制未放在前台进行控制； 3) 删除操作未给出提示； 4) 操作界面信息错误（包括数据窗口内列名定义、含义是否一致）； 5) 数据库表中有过多的空字段。
4	建议	1) 界面不规范； 2) 辅助说明描述不清楚、提示窗口文字未采用行业术语； 3) 输入输出不规范； 4) 长时间操作未给用户提示； 5) 可输入区域和只读区域没有明显的区分标志； 6) 控件没有对齐、标点符号丢失或不正确； 7) 就功能、操作、校验、说明等方面，提出建议性的改进要求。

### 7.5.2 识别准确率

- a) 误识率小于等于 5%；
- b) 误拒率小于等于 5%；

- c) 识别正确率大于等于 90%;
- d) 以上 a)、b)和 c)同时满足时, 该人像识别系统是可用的, 否则为不可用。

7.5.3 安全性、数据保护

- a) 不存在高危漏洞;
- b) 不存在中危漏洞;
- c) 低危漏洞数量: 小于或等于 3 个;
- d) 漏洞严重性等级见表 2, 以上 a)、b)和 c)同时满足时, 该人像识别系统是可用的, 否则为不可用。

表2 漏洞严重性等级划分准则

等级	漏洞严重性等级	说明
1	高危	1) 发现存在重大漏洞或弱点, 可能导致未经授权的访问、系统被入侵或数据泄露等严重后果; 2) 存在严重的隐私保护问题, 例如未经许可获取、存储或传输用户的个人身份信息, 可能导致个人隐私泄露; 3) 发现系统容易遭受面部假冒攻击, 即通过使用他人的面部特征来欺骗识别系统, 破坏身份认证的有效性。
2	中危	1) 部分数据存储或传输过程中存在潜在的安全风险; 2) 存在一些弱密码、未加密的敏感数据或使用不安全的认证机制; 3) 安全设置或配置方面存在一些疏漏, 可能被攻击者利用; 4) 存在一些已知的但尚未公开的安全漏洞, 需要尽快修复。
3	低危	1) 存在一些较为常见的安全配置问题, 但风险相对较小; 2) 存在一些潜在的安全风险, 但恶意攻击的可能性较低; 3) 存在一些较为次要的安全漏洞, 但对系统整体安全性的影响较小。