ICS 35.240
CCS L 80

团　体　标　准

T/CFEII 0010—2023

人脸识别应用
三维假体人脸分类分级规范

Facial recognition applications—
Specification for classification and grading of 3D fake face

2023 - 08 - 21 发布　　2023 - 08 - 21 实施

中国电子信息行业联合会　发布

全国团体标准信息平台

全国团体标准信息平台

目　　次

前　　言 II
引　　言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　概述 2
5.1　呈现攻击流程 2
5.2　三维假体人脸使用原则 2
6　三维假体人脸分类 2
7　三维假体人脸分级 3
附 录 A （规范性） 人脸识别应用防假体攻击测试三维假体人脸选取比例 4
附 录 B （资料性） 三维假体人脸分级测试方案 5

全国团体标准信息平台

前　言

本标准按照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。

本标准由中国电子信息行业联合会提出并归口。

请注意本标准的某些内容可能涉及专利，本标准的发布机构不承担识别专利的责任。

本标准起草单位：国家工业信息安全发展研究中心、国家语音及图像识别产品质量检验检测中心、杭州海康威视数字技术股份有限公司、小视科技（江苏）股份有限公司、北京清飞科技有限公司、武汉莫问科技有限公司、上海商汤智能科技有限公司、上海依图网络科技有限公司、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、北京尊冠科技有限公司、北京智游网安科技有限公司、罗克佳华科技集团股份有限公司、大同市数字政府服务中心、北京信源电子信息技术有限公司大同分公司、北京信源电子信息技术有限公司吉安分公司。

本标准主要起草人：朱倩倩、刘永东、李美桃、王晶晶、王升国、杨帆、李双、种国双、高云龙、倪邦杰、乔思渊、魏宇飞、王新秀、李儒日、李佳秾、赵春昊、林冠辰、郭建领、李世勇、黄贵玲、韩云、薛学琴、周永修、 韩杰、马国斌。

全国团体标准信息平台

引　言

近年来，伴随着基础设施的改善和算法识别准确率的提升，人脸识别凭借非接触、非侵扰、采集简单等特性，在赋能实体经济、促进产业转型、改善社会民生、提升生活质量等方面得以广泛应用。然而，人脸识别在高速发展、改变生产生活方式的同时，也暴露出一些安全问题，其中假体人脸呈现攻击是一种常见的安全风险。与二维假体人脸相比，三维假体人脸呈现攻击风险更大。目前三维假体人脸作为人脸呈现攻击的一种呈现攻击工具，其在保障呈现攻击检测安全性中发挥了重要作用，但三维假体作为呈现攻击工具，并没有统一的分类分级规范，导致各个单位和检验检测机构的测试结果不在同一测试基准上，一定程度上阻碍了人脸识别行业的高质量发展。

本文件提出了三维假体人脸分类分级规范，明确了三维假体人脸的分类和分级要求。通过对三维假体人脸分类分级的细化，有效规范检验检测机构、技术开发方和技术应用方等开展人脸识别系统防三维假体人脸攻击的测试，提升人脸识别系统的防呈现攻击能力，保障人脸识别应用安全。

全国团体标准信息平台

全国团体标准信息平台

人脸识别应用 三维假体人脸分类分级规范

1 范围

本文件规定了三维假体人脸分类和分级要求。

本文件适用于检验检测机构、技术开发方和技术应用方等开展人脸识别系统防三维假体人脸呈现攻击的测试。

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 35678—2017 公共安全 人脸识别应用 图像技术要求

GB/T 37036.8—2022 信息技术 移动设备生物特征识别 第8部分：呈现攻击检测

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 41815.1—2022 信息技术 生物特征识别呈现攻击检测 第1部分：框架

3 术语和定义

GB/T 37036.8—2022、GB/T 41815.1—2022 界定的以及下列术语和定义适用于本文件。

3.1

人脸识别应用 face recognition applications

使用人脸识别技术来确认特定自然人或特定自然人身份的过程。

3.2

三维假体人脸 3D fake face

冒充真人身份的三维人脸仿冒品，是一种呈现攻击工具（PAI）。

3.3

活体检测 liveness detection

对解剖学特征、无意识或有意识的反应的度量和分析，以确定采集到的人脸样本是否来自采集端有生命特征的人。

[来源：GB/T 41772—2022，3.18]

3.4

威胁程度 threat level

在给定攻击者的知识能力、熟练程度、环境资源的情况下呈现攻击工具（PAI）威胁能力的度量。

3.5

相似度 similarity

两个生物特性相似程度的一个实数，数值越大两个生物特性越相似。

3.6

反射率 reflection

某一个波长照射在假体人脸上的反射能量与入射能量的比率。

3.7

色容差 color tolerance

在单一光源下，假体人脸与对应被采集者的关键特征点的颜色偏差。

4 缩略语

下列缩略语适用于本文件。

2D：二维（Two Dimensions）

3D：三维（Three Dimensions）

NIR：近红外（Near Infrared Radiation）

PAD：呈现攻击检测（Presentation Attack Detection）

PAI：呈现攻击工具（Presentation Attack Instrument）

RGB：光学三原色（Red Green Blue）

5 概述

5.1 呈现攻击流程

呈现攻击一般分为定向呈现攻击和非定向呈现攻击。定向呈现攻击的实施者一般为生物特征识别假冒者，目的是以特定对象为目标进行攻击；非定向呈现攻击的实施者一般为生物特征识别掩饰者，不需要知晓特定的被攻击者生物特征，目的是为了掩饰自身的真实身份或特征。本文件主要讨论定向呈现攻击的一般流程，见图1。活体检测是PAD的子集，是保障人脸识别系统安全性的重要环节。

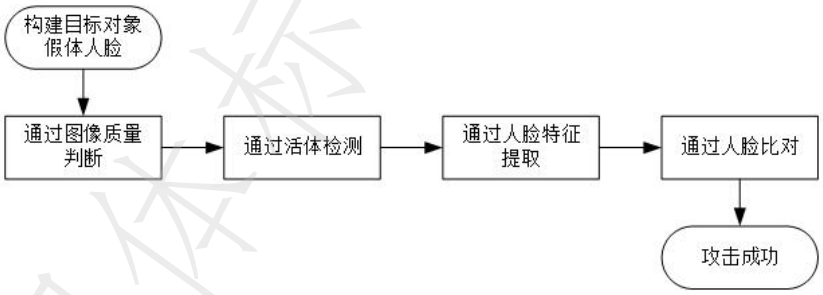


图1 定向呈现攻击流程

5.2 三维假体人脸使用原则

对人脸识别系统实施呈现攻击的威胁程度与测试人员的技能、呈现方式（如距离、角度、移动）、光线条件、配饰（如围巾、眼镜、帽子）等外部因素相关，本文件旨在评估测试用三维假体人脸质量的威胁程度，该因素是直接影响人脸识别系统呈现威胁程度的内部因素。

在呈现攻击检测中，一般情况下使用更多的假体人脸类型进行更多的测试次数，可以增加测试的准确性。鉴于假体人脸作为一种人工制品，其材料和材料混合物的种类繁多，因此在假体人脸分类分级的基础上，结合应用场景的安全风险程度，选取相应比例威胁程度等级的假体人脸作为PAI进行防假体攻击检测。人脸识别应用防假体攻击测试三维假体选取比例应符合附录A的要求。

6 三维假体人脸分类

根据三维假体类型、材质类型、裁剪类型和形态类型对三维假体人脸进行分类，具体类型见表1。

表1 三维假体人脸分类

三维假体类型	材质类型	裁剪类型	形态类型
仿真人脸面具	硅胶、砂岩、树脂、乳胶、石膏、泡沫、石英砂、陶瓷、纸质、布质等	抠洞、不抠洞	——
仿真人脸头模	硅胶、砂岩、树脂、乳胶、石膏、泡沫、石英砂、纸质、布质等	——	静态、动态
注 1：抠洞指抠除眼睛、鼻子、嘴巴等部位。 注 2：静态指面部五官不具备动作能力；动态指面部五官具备动作配合能力。			

7　三维假体人脸分级

在人脸识别应用中，一般在使用摄像头拍摄及采集人脸图像的同时，结合各类活体检测技术，判断图像是否来自真人，有效防范三维假体等类别的攻击，保证人脸信息的真实有效性。

常见的活体检测技术有 RGB 活体检测、NIR 活体检测、3D 活体检测、动作活体检测、光线活体检测等。RGB 活体检测主要通过人脸的外观图像特征及底层纹理特性进行活体判断；NIR 活体检测主要通过不同材质对近红外光的反射率差异进行活体判断；3D 活体检测主要通过 3D 结构光或 TOF 原理获取物体的深度信息或距离信息进行活体判断；动作活体检测主要通过指令动作的配合及图像特征进行活体判断，指令动作包括但不限于点头、摇头、张嘴、眨眼等；光线活体检测又称炫彩活体检测，主要通过屏幕颜色变化采集人脸不同反射颜色信息进行判断。

根据三维假体人脸对人脸识别系统威胁程度，三维假体人脸共分为基本级和增强级两个等级。一般情况下，二维图像相似度越高，人脸比对的通过率越高；色容差越小、工艺精度误差越小，RGB 活体检测和人脸比对的通过率越高；近红外光反射率差越小，NIR 活体检测通过率越高；三维数据误差小，3D 活体检测通过率越高。各等级的要求见表 2，三维假体人脸分级测试方案见附录 B。

表 2　三维假体人脸分级要求

对象	指标	分级要求	
		基本级	增强级
三维假体人脸	色容差	色容差小	色容差小
	工艺精度误差	工艺精度误差小	工艺精度误差小
	二维图像相似度	二维图像相似度高	二维图像相似度高
	近红外光反射率差异	—	近红外光反射率差异小
	三维数据误差	—	三维数据误差小

附 录 A
（规范性）
人脸识别应用防假体攻击测试三维假体人脸选取比例

人脸识别应用防假体攻击测试三维假体人脸选取比例见表 A.1。

表 A.1 人脸识别应用防假体攻击测试三维假体人脸选取比例

序号	三维假体人脸选取比例（增强级：基本级）	典型应用场景
1	2:8	公园、居民小区等使用人脸识别技术核对人员身份
2	5:5	机场、火车站使用人脸识别技术认证比对，或入户门开锁
3	8:2	移动智能终端、应用程序使用人脸识别技术实现解锁、支付等功能

全国团体标准信息平台

附 录 B
（资料性）
三维假体人脸分级测试方案

B.1 测试环境

除特殊规定外，测试环境要求室内环境，环境温度为15℃～35℃，光照强度为3001x～30001x，色温为4000K～5000K。

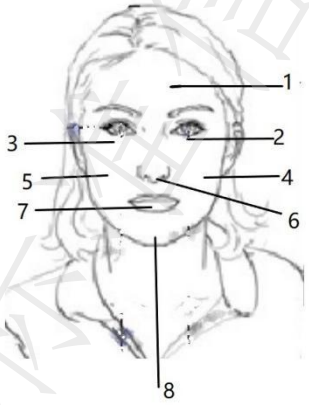
B.2 测试工具

温湿度计、光照计、色温照度计、色差仪、人脸比对平台、高光谱成像仪。

B.3 三维假体人脸测试

B.3.1 色容差

假体人脸与对应被采集者的 8 个关键特征点（额头、左下眼睑、右下眼睑、左侧面颊、右侧面颊、鼻尖、嘴唇、下巴）色容差见图 B.1。若 8 个特征点的色容差值都不大于 7SDCM，则判定结果为色容差小，否则判定结果为色容差大。色容差测试结果判定见表 B.1。



注:
1 表示额头（中） 2 表示下眼睑（左）
3 表示下眼睑（右） 4 表示左面颊
5 表示右面颊 6 表示鼻尖
7 表示嘴唇 8 表示下巴

图 B.1 人脸关键特征点

表 B.1 色容差测试结果判定

假体人脸/被采集者	特征点位置	测试结果	判段方法	判定结果
001-SZ/001	额头	ΔE=6.41SDCM	ΔE≤7SDCM	色容差小
	左下眼睑	ΔE=6.90SDCM		
	右下眼睑	ΔE=6.53SDCM		
	左侧面颊	ΔE=5.79SDCM		
	右侧面颊	ΔE=6.60SDCM		
	鼻尖	ΔE=6.97SDCM		

	嘴唇	ΔE=5.29SDCM		
	下巴	ΔE=6.68SDCM		
002-SZ/002	额头	ΔE=6.79SDCM	ΔE＞7SDCM	色容差大
	左下眼睑	ΔE=11.59SDCM		
	右下眼睑	ΔE=4.82SDCM		
	左侧面颊	ΔE=8.20SDCM		
	右侧面颊	ΔE=6.00SDCM		
	鼻尖	ΔE=4.79SDCM		
	嘴唇	ΔE=4.71SDCM		
	下巴	ΔE=6.36SDCM		

注： ΔE 表示色容差。

B.3.2 工艺精度误差

查看采集数据的工艺精度误差和制作假体人脸的工艺精度误差。若采集工艺精度误差ΔA≤0.1mm和制作工艺精度误差ΔB≤0.1mm，则判定结果为工艺精度误差小，否则判定为工艺精度误差大。工艺精度评估结果判定见表 B.2。

表 B.2 工艺精度评估结果判定

采集工艺精度误差	制作工艺精度误差	判段方法	判定结果
ΔA≤0.1mm	ΔB≤0.1mm	ΔA≤0.1mm 且ΔB≤0.1mm	工艺精度误差小
ΔA＞0.1mm	ΔB≤0.1mm	ΔA＞0.1mm 或ΔB＞0.1mm	工艺精度误差大
ΔA≤0.1mm	ΔB＞0.1mm		
ΔA＞0.1mm	ΔB＞0.1mm		

注： ΔA 表示采集工艺精度误差，ΔB 表示制作工艺精度误差。

B.3.3 二维图像相似度

假体人脸与对应被采集者在同一采集设备下正面拍摄两张分辨率不低于 1280*720 的彩色照片，应满足 GB/T 35678—2017 中人脸图像注册图像的要求。输入不少于 3 个主流国内外人脸比对平台测试，若人脸比对平台输出结果都为同一个人，则判定结果为二维图像相似度高，否则判定为二维图像相似度低。二维图像相似度测试结果见表 B.3。

表 B.3 二维图像相似度测试结果

序号	材质	性别	颜色	国内外人脸比对平台					
				A	B	C	D	E	F
1	硅胶	男	彩色	同一个人的可能性极高	同一个人的概率为78.62%	两张照片是同一个人	同一个人的可能性很高	同一人相似度 83%	同一个人

2	硅胶	女	彩色	同一个人的可能性极高	同一个人的概率为76.51%	两张照片是同一个人	同一个人的可能性很高	同一人相似度73.1%	同一个人
3	泡沫	女	彩色	同一个人的可能性极高	同一个人的概率为78.48%	两张照片是同一个人	同一个人的可能性很高	同一人相似度72.2%	同一个人
4	树脂	男	彩色	同一个人的可能性极高	同一个人的概率为82.88%	两张照片是同一个人	同一个人的可能性很高	同一人相似度63.3%	同一个人
5	树脂	男	彩色	同一个人的可能性极高	同一个人的概率为74.75%	两张照片是同一个人	同一个人的可能性很高	同一人相似度74%	同一个人
6	硅胶	女	彩色	同一个人的可能性极高	同一个人的概率为74.41%	两张照片是同一个人	同一个人的可能性很高	同一人相似度74.4%	同一个人
7	硅胶	男	彩色	同一个人的可能性较高	同一个人的概率为74.26%	两张照片是同一个人	同一个人的可能性很高	同一人相似度71.5%	同一个人
8	树脂	女	彩色	同一个人的可能性极高	同一个人的概率为74.95%	两张照片是同一个人	同一个人的可能性很高	同一人相似度79.7%	同一个人
9	树脂	男	彩色	同一个人的可能性极高	同一个人的概率为73.62%	两张照片是同一个人	同一个人的可能性很高	同一人相似度80.2%	同一个人
10	乳胶	男	彩色	同一个人的可能性极高	同一个人的概率为74.7%	两张照片是同一个人	同一个人的可能性很高	同一人相似度75.7%	同一个人
11	乳胶	女	彩色	同一个人的可能性极高	同一个人的概率为74.99%	两张照片是同一个人	同一个人的可能性很高	无识别	同一个人
12	树脂	女	白色	同一个人的可能性较高	同一个人的概率为74.74%	两张照片是同一个人	可能性一般	无识别	同一个人
13	布质	女	彩色	同一个人的可能性极高	同一个人的概率为84.09%	两张照片是同一个人	同一个人的可能性很高	同一人相似度52.9%	同一个人
14	树脂	女	铜色	同一个人的可能性极低	同一个人的概率为13.13%	两张照片不是同一个人	同一个人的可能性极低	无识别	不是同一个人
15	树脂	女	铜色	同一个人的可能性极低	同一个人的概率为1.56%	两张照片不是同一个人	同一个人的可能性极低	无识别	不是同一个人

B.3.4 近红外光反射率

假体人脸材料与对应被采集者皮肤在高光谱成像仪下的780nm~1100nm近红外反射率测试。若假体人脸与真实皮肤在红外波段的光反射波形一致，则判定为近红外反射率差异小，否则判定为近红外反射率差异大。假体人脸材料近红外反射率对比见图B.2，对应被采集者近红外反射率对比见图B.3,泡沫和硅胶材质假体人脸材料近红外光反射率测试结果判定见表B.4。

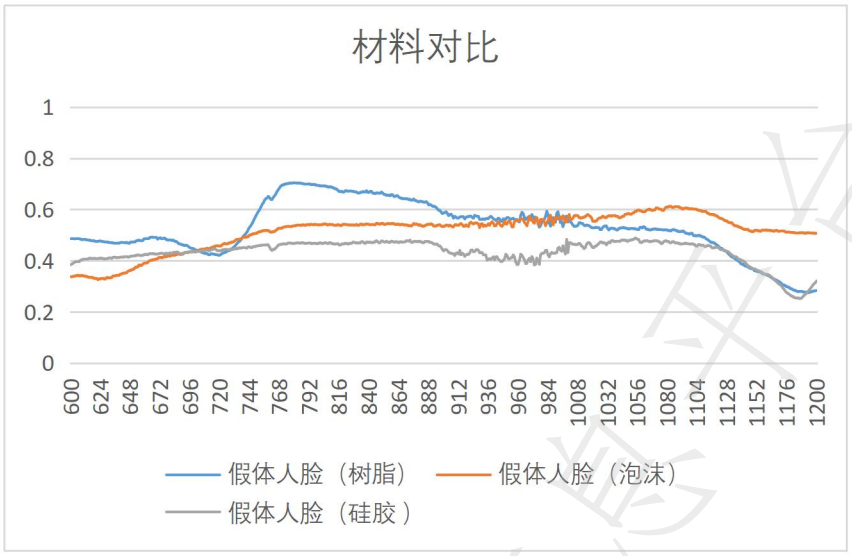


图 B.2　材料近红外反射率比对

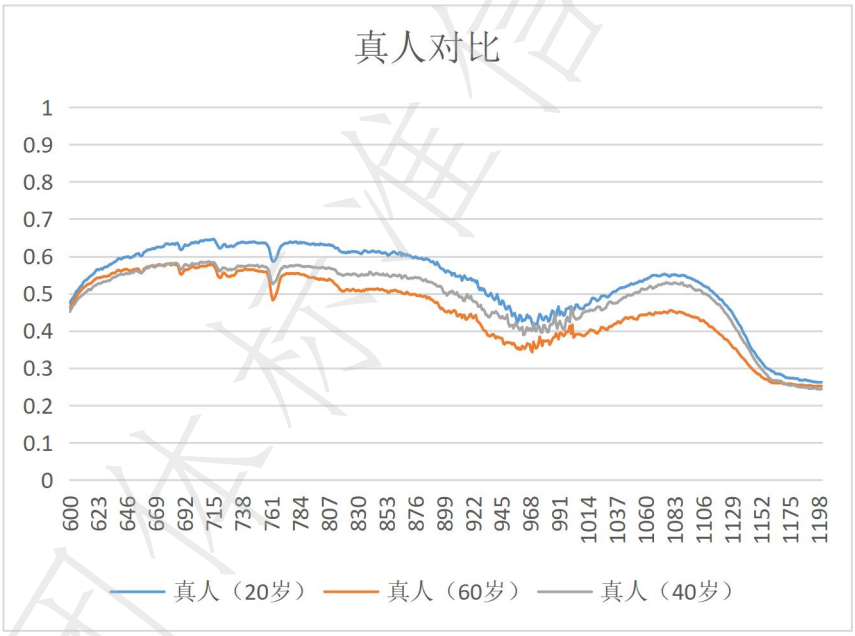
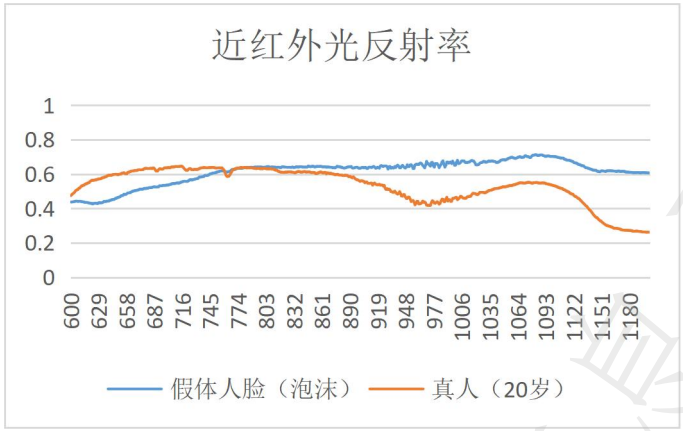
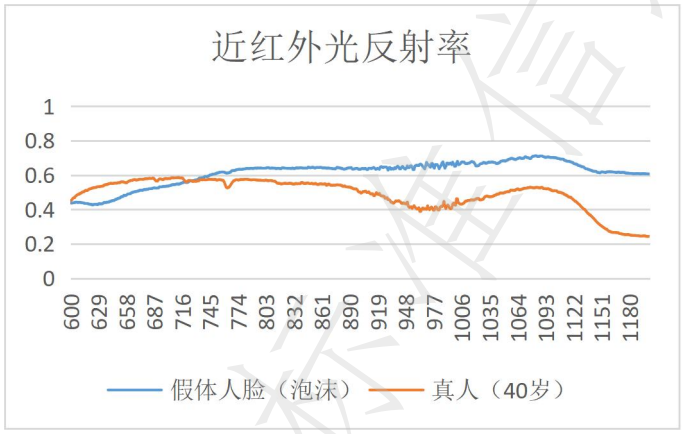
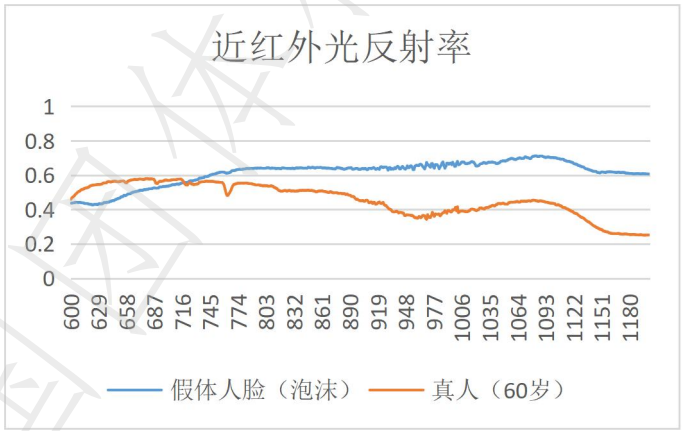
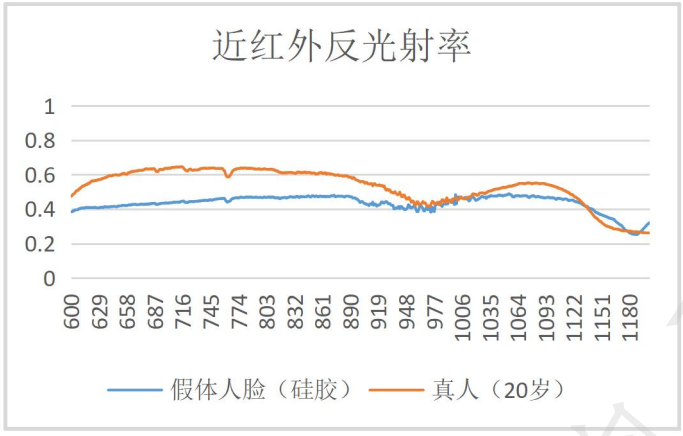
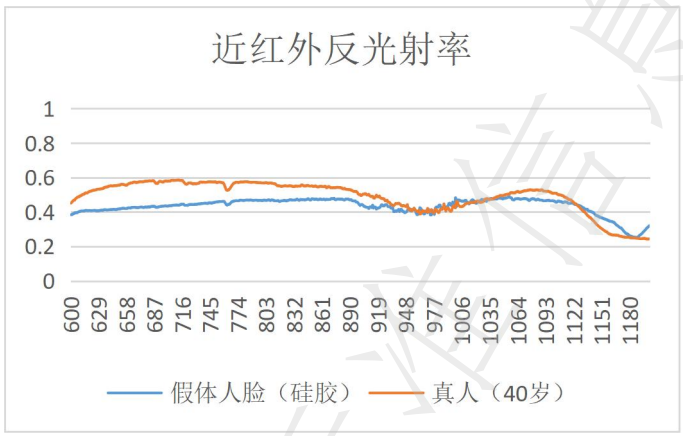
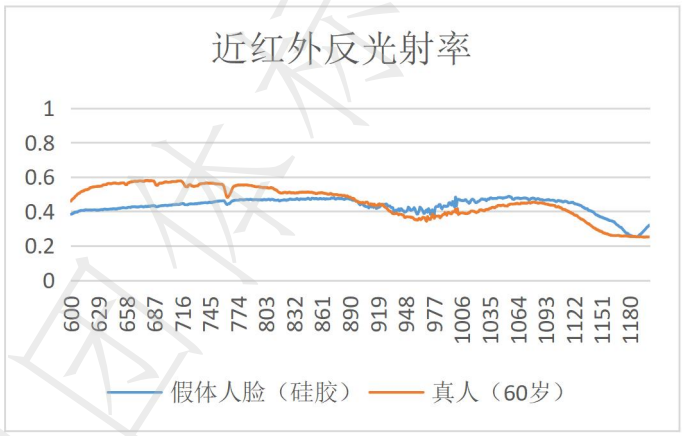


图 B.3　真人近红外反射率比对

表 B.4　近红外光反射率测试结果判定

假体材质	近红外反射率对比图	判段方法	判定结果
泡沫	  	近红外光谱波形不一致	近红外光反射率差异大

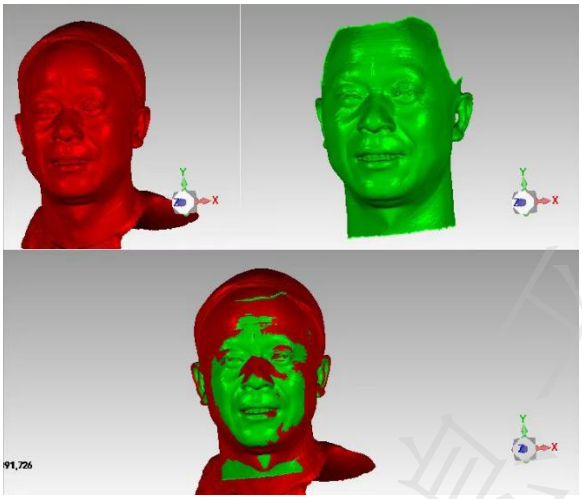
全国体育信息安全

硅胶	  	近红外光谱波形一致	近红外光反射率差异小

B.3.5 三维数据误差

假体人脸与对应被采集者用同一采集设备得到两组 3D 点云数据，利用 Geomagic Qualify 3D 偏差检测分析 3D 点云数据误差见图 B.4。若三维数据标准差 ΔC≤0.8mm，则判定为三维数据误差小，否则判定为三维数据误差大。

注： ΔC表示三维点云数据标准差



图B.4　3D点云数据比对

全国团体标准信息平台