TC260-PG-2023XX

网络安全标准实践指南

—车外画面局部轮廓化处理效果验证

（征求意见稿 v1.0-202301）

全国信息安全标准化技术委员会秘书处

2023 年 01 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、国家计算机网络与信息安全管理中心、中国汽车工业协会、中国科学院自动化研究所、广州广电计量检测股份有限公司、北京清华亚迅电子信息研究所、上海市北数所安全研究院、广州小鹏汽车科技有限公司、岚图汽车科技有限公司等单位的技术支持。

摘　要

汽车在运行过程中采集到的车外画面（包含道路、建筑、行人、车辆等内容）是重要的数据资源，可用于汽车数据处理者改进自动驾驶算法。由于车外画面中可能包含人脸、车牌等信息，汽车制造商、自动驾驶算法提供商、出行服务企业等汽车数据处理者收集获取车外画面时，需要按照法律法规、国家标准等要求在汽车内部对人脸、车牌完成局部轮廓化处理后再向车外传输。

为帮助有关单位落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《汽车数据安全管理若干规定（试行）》等政策法规要求，本实践指南给出了人脸、车牌局部轮廓化处理的效果验证方法，可为汽车数据处理者及有关机构验证局部轮廓化处理效果提供参考。

目　录

1 范围

本实践指南给出了验证车外画面进行人脸、车牌局部轮廓化处理效果的流程、方法及验证标准。

本实践指南适用于汽车数据处理者对车外画面进行人脸、车牌局部轮廓化处理效果的自行验证，也适用于第三方机构对局部轮廓化处理效果的验证。本实践指南给出的验证方法仅适用于判别人脸、车牌的局部轮廓化处理效果。

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 41871　信息安全技术　汽车数据处理安全要求

3 术语和定义

3.1 验证方

验证人脸、车牌局部轮廓化处理效果的组织。

3.2 车外画面

汽车向车外采集的视频、图像数据。

3.3 局部轮廓化处理

将视频、图像中包含人脸、车牌等信息的区域删除，或者将这些区域替代为无法关联个人信息主体且不可复原的其他图像的过程。

3.4 测试道路

覆盖专用测试道路、普通城市道路、高速公路和停车场等场景的道路集合。

4 验证流程

验证方按以下流程开展验证：

a) 验证方将待验证车辆置入其指定的测试道路，确定待验证车辆是否满足附录A中相关要求；

b) 验证方打开待验证车辆网络连接功能，接入验证方移动终端热点，移动终端内置流量抓取工具对车辆进行数据采集，确保车内数据从唯一指定链路（如Wi-Fi方式）对外传输；

注：流量抓取工具可以是验证方专用测试工具，也可以是商用或开源网络抓包软件，常用抓包软件如Wireshark、tcpdump等。

c) 验证方人员随车进行实时监测，使接入移动终端热点的待验证车辆在测试道路的三种场景下进行行驶和驻车测试，每个道路场景各对应早、中、晚三种不同光照条件，共计9轮，每轮测试时长持续不少于30分钟；

d) 验证方在每轮行驶测试完成后，触发汽车的车外画面上传条件，从上传数据中实时提取车外画面及局部轮廓化区域位置信息，得到9组待验证样本；

注：局部轮廓化区域位置信息格式见附录B。

e) 验证方将提取的待验证样本导入开展效果验证的实验室计算环境，按本文件第5章对获取的局部轮廓化处理画面进行人脸、车牌检测；

注：实验室计算环境，一般是指部署有高性能服务器或计算机，可用于搭建基于机器学习或视频图像处理的程序，以便于开展自动化机器算法检测和人工检测的环境。

f) 验证方根据机器算法检测和人工检测结果，按本文件第6章给出验证结论。

5 效果验证方法

验证方按照以下方法开展验证：

a) 通过检测算法及人工肉眼检测相结合的方式对向车外传输的车外画面进行效果验证（算法选取方式见附录C）：

1） 对每一幅图片或每一个视频文件，使用5种不同的人脸检测算法分别进行验证；对任一图片或视频，若有2种及以上算法检测出人脸信息，则认为该样本未通过验证；

2） 对每一幅图片或每一个视频文件，使用5种不同的车牌检测算法分别进行验证；对任一图片或视频，若有2种及以上算法检测出车牌信息，则认为该样本未通过验证；

3） 从所有车外画面中进行抽取，图像每10幅随机抽取一幅，视频每10秒随机抽取一帧，对所有抽取的样本，以人工肉眼检测的方法验证是否残留人脸或车牌；人工肉眼检测发现残留，若经度量确认残留的人脸宽超过20像素，或车牌高度高于10像素的，则认为该样本未通过验证。

b) 从所有已完成局部轮廓化处理的画面中进行抽取，图像每10幅随机抽取一幅，视频每10秒随机抽取一帧，对所有抽取得到的样本，读取其相应的位置信息文件，以便于后续检测；通过检测算法及人工肉眼检测相结合的方式对局部轮廓化区域及其周围进行检测，验证是

否没有五官、面部皮肤等人脸残留，没有字母、汉字、数字等车牌残留。若检出残留的，则认为该样本未通过验证。

6 验证结论

验证方按照以下步骤给出验证结论：

a) 针对9组待验证样本，分别统计按本文件5a)验证时的未通过样本数量，计算未通过验证样本数量占全部按5a)进行验证样本总数的比例，记为“未通过率A1”、……、“未通过率A9”，计其中最大值为“未通过率A”；

b) 针对9组待验证样本，分别统计按本文件5b)验证时的未通过样本数量，计算未通过验证样本数量占全部按5b)进行验证样本总数的比例，记为“未通过率B1”、……、“未通过率B9”，计其中最大值为“未通过率B”；

注：计算数量时，每幅图片、每个连续视频都记为1个样本。

c) 按以下标准形成验证结论：

1） 未通过率A和未通过率B有一项大于10%的，结论为未通过；

2） 未通过率A和未通过率B均不大于10%，结论为通过；

3） 被验证方未能按照本文件附录A要求进行验证准备，无法正常完成验证流程的，结论为未完成。

附录 A

（规范性）

验证准备事项

验证方进行验证前，对车外画面进行人脸、车牌局部轮廓化处理的汽车数据处理者应配合验证方进行以下准备：

a) 提前准备用于验证的实车车辆：

1） 车辆应具备与在售或即将销售车辆一致的视频传感器参数、数据处理流程和能力，保证车辆的数据采集、车内处理、向外传输等基本功能正常；

2） 开启可供外部接入的调试接口或远程调试功能；

3） 开启接入访问本地文件的权限；

4） 支持上传流量集中获取。

注：例如配置或改造网络路由规则使汽车统一采用Wi-Fi方式对外传输数据。

b) 向验证方提供必要的技术和人员支持：

1） 开启车辆所有涉及数据采集、车内处理、向外传输的功能；

2） 提供汽车数据上传触发条件；

3） 支持验证方完成设备访问车端系统，导出待验证样本；

4） 支持验证方访问业务系统，根据车辆VIN码、IP等信息导出待验证样本；

5） 支持验证方进行上传流量分析、提取车外画面。涉及传输通道加密的，由被验证方提供验证所需的加密证书，

或临时信任验证方提供的验证证书，或暂停传输通道加密，或从上传位置（近场访问车端系统内）和接收位置（远程访问云平台）取得上传的车外画面；涉及上传数据自身加密的，由被验证方提供解密方式。

附录 B

（规范性）

已处理画面的位置信息文件格式

已处理画面的位置信息应以如下形式提供：

a) 每个已处理画面文件应附带一个位置信息文件；

b) 位置信息文件中的每一行代表一幅图像或视频中一帧图像的局部轮廓化区域的位置信息；

c) 若已处理画面为图像，其附带的位置文件中应仅有一行内容；

d) 若已处理画面为视频，其附带的位置文件中可有多行内容，每一行代表该视频每秒钟第一帧图像中局部轮廓化区域的位置信息；视频中没有进行局部轮廓化的时间，对应行应留空；

e) 若一幅图像中仅存在一个局部轮廓化区域，其对应的一行位置信息应包括局部轮廓化区域所有像素点横坐标的最小值和最大值、纵坐标的最小值和最大值、区域类型（人脸为0，车牌为1）五个数字，五个数字以逗号分隔，并在前后加括号；

注1：人脸/车牌局部轮廓化区域不规则时，其附带的位置信息可解析为局部轮廓化区域的外接矩形，即以区域内所有像素点横、纵坐标的最小值所在点为左上顶点，区域内所有像素点横、纵坐标的最大值所在点为右下顶点的矩形。该矩形可作为人脸/车牌标注框，辅助机器算法对已处理画面进行检测。

注2：图像坐标系一般以水平方向向右为x轴正方向，垂直方向向下为y轴正方向。

示例：

对于一幅包含一个车牌局部轮廓化区域的图像，其车牌局部轮廓化区域内所有像素点横坐标的最小值、最大值分别为x1、x2，纵坐标的最小值、最大值分别为y1、y2，则其位置信息记为：(x1, x2, y1, y2, 1)。

f) 若一幅图像中存在多个局部轮廓化区域，应按照局部轮廓化区域内像素横坐标的最小值进行排序，并以从小到大的顺序，在位置信

息文件对应行中列出e)中要求的每个局部轮廓化区域位置信息，每个位置信息间应以空格分隔。

示例：

一幅包含了两个人脸和一个车牌局部轮廓化区域所对应的一行位置信息可能是： (21, 54, 64, 101, 0) (191, 243, 18, 35, 1) (512, 691, 678, 881, 0)。

附录 C

（规范性）

选取人脸、车牌检测算法的指南

C.1 本实践指南所述人脸、车牌检测算法应：

a) 能在主流的测试数据集上获得较好效果。

注1：本条所述较好效果在人脸检测方面是指，至少可在WIDER Face数据集，结果与实际人脸交并比大于0.5计为检测出人脸时，高、中、低难度的mAP（mean Average Precision，平均精度均值）值分别不低于0.90、0.95、0.96。

注2：本条所述较好效果在车牌检测方面是指，至少可在CCPD以及CRPD数据集，结果与实际车牌交并比大于0.7计为检测出车牌时，mAP值不低于0.95。

b) 能在覆盖场景较全面的自建数据集上获得较好效果。

注3：本条所述自建数据集建设见C.2。

注4：本条所述较好效果在人脸检测方面是指，结果与实际人脸交并比大于0.5计为检测出人脸时，mAP值不低于0.95。

注5：本条所述较好效果在车牌检测方面是指，结果与实际车牌交并比大于0.7计为检测出车牌时，mAP值不低于0.95。

C.2 自建检测数据集

自建人脸、车牌检测数据集均应：

a) 数据集内图像不少于10000幅；

b) 场景丰富，覆盖城镇街道、高速公路、路边停车场地、地上和地下停车场等；

c) 属性多样，覆盖不同目标、尺度、遮挡、光照、角度等；

d) 覆盖c)中两种及以上属性的图像不低于总数据的50%；

e) 覆盖b)中任意一场景和c)中一项属性组合的图像总数不低于100幅；

f) 自建人脸检测数据集时，整体难度参照WIDER Face数据集的中等难度进行制作；

g) 自建车牌检测数据集时，整体难度参照CRPD数据集的难度进行制作。