Vehicle Cybersecurity

Facial Recognition
Basic Security Requirements

Version 1.1

Version Date: November 14, 2019

UNCONTROLLED COPY IF PRINTED

FORD CONFIDENTIAL

Revision History

Date	Version	Created/Modified By	Notes
11/4/2019	1.0	QZOU2	Initial Version
11/6/2019	1.1	ALIN13	Edit to include additional requirements and English translation

Table of Contents

1 Introduction

1.1 Executive Summary

This document provides high level basic security requirements for facial recognition technology utilized in vehicle.

1.2 Purpose of Document

The purpose of this document is to outline several key basic security requirements for facial recognition which includes regulatory requirements/recommendations (aka GB/GBT). This document shall be considered a general guide unless specified as a requirement.

The document will focus on the following areas:

- General security requirements (通用安全要求)
- Face feature **capture module** security requirements (人脸特征捕获模块的安全要求)
- Face feature **storage module** security requirements (人脸特征存储模块的安全要求)
- Face feature **comparison module** security requirements (人脸特征比较模块的安全要求)
- Secure face image data transmission requirements (安全的人脸图像数据传输要求)
- System log security requirements (系统日志安全要求)

1.3 References

This section contains references to regulatory requirements/recommendations and international standards/references, which affect the requirements presented in this specification.

The terms related to security in these documents should all be met.

Reference Title	Document Name
GB/T 26238-2010	信息技术 生物特征识别术语 Information technology biometrics terminology
GB/T 35273-2019	信息安全技术 个人信息安全规范 (征求意见稿) Information Security Technology Personal Information Security Specification
GB/T 37036.1-2018	信息技术 移动设备生物特征识别 第 1 部分：通用要求 第 7 章：安全要求 Information technology - Biometrics of mobile devices - Part 1: General requirements Chapter 7: Safety requirements
GB/T 37036.3-xxxx	信息技术 移动设备生物特征识别 第 3 部分：人脸 (征求意见稿) 第 9 章：安全要求 Information technology Biometrics for mobile devices Part 3: Faces (Draft for comment) Chapter 9: Safety requirements
ISO_IEC_30107-1_2016	Information technology Biometric presentation attack detection Part 1:Framework 信息技术生物识别表示攻击检测第 1 部分：框架
GB/T xxxxx-xxxx	信息安全技术 基于可信环境的远程人脸识别认证系统技术要求(征求意见稿) 第 8 章： 安全要求 Information Security Technology Technical Requirements for Remote Face Recognition and Authentication System Based on Trusted Environment (Draft for Comment) Chapter 8: Security Requirements
Research & Vehicle Technology - PD	Image Recognition Feature Level Specification 图像识别功能等级规范

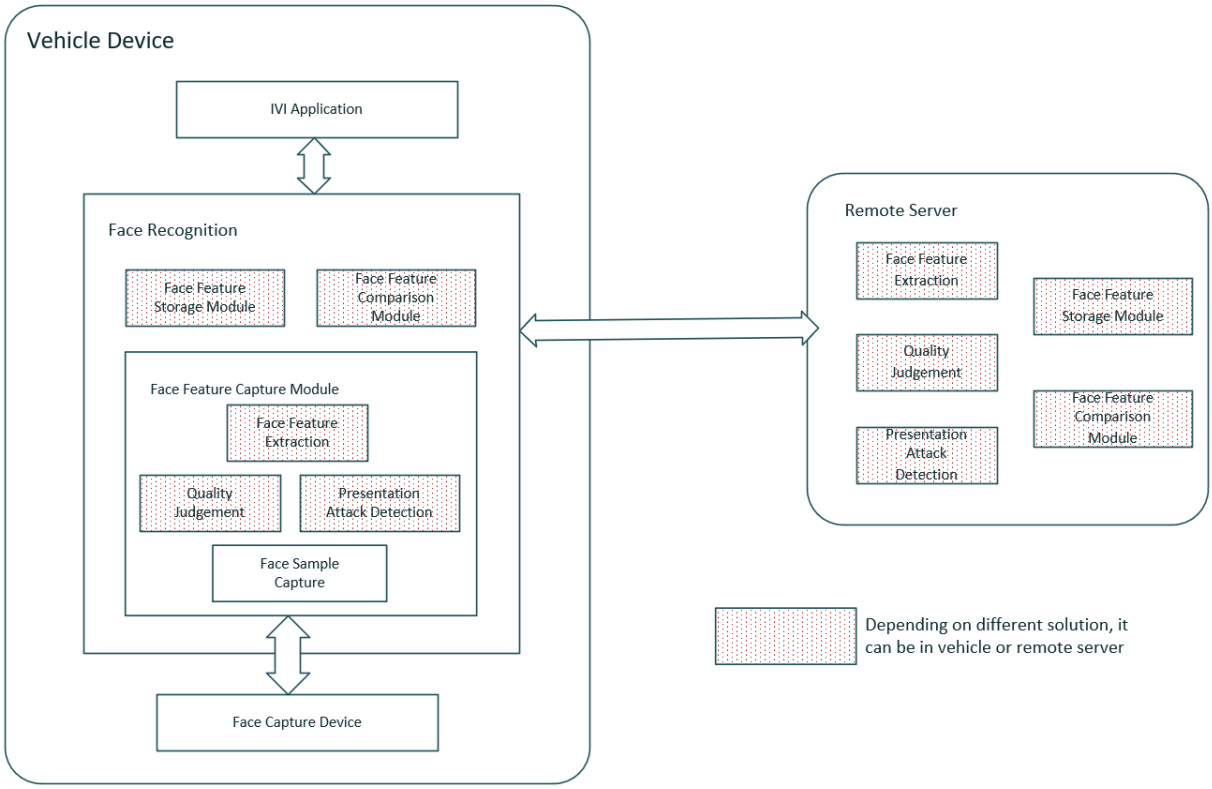
1.4 Terminology and Abbreviations

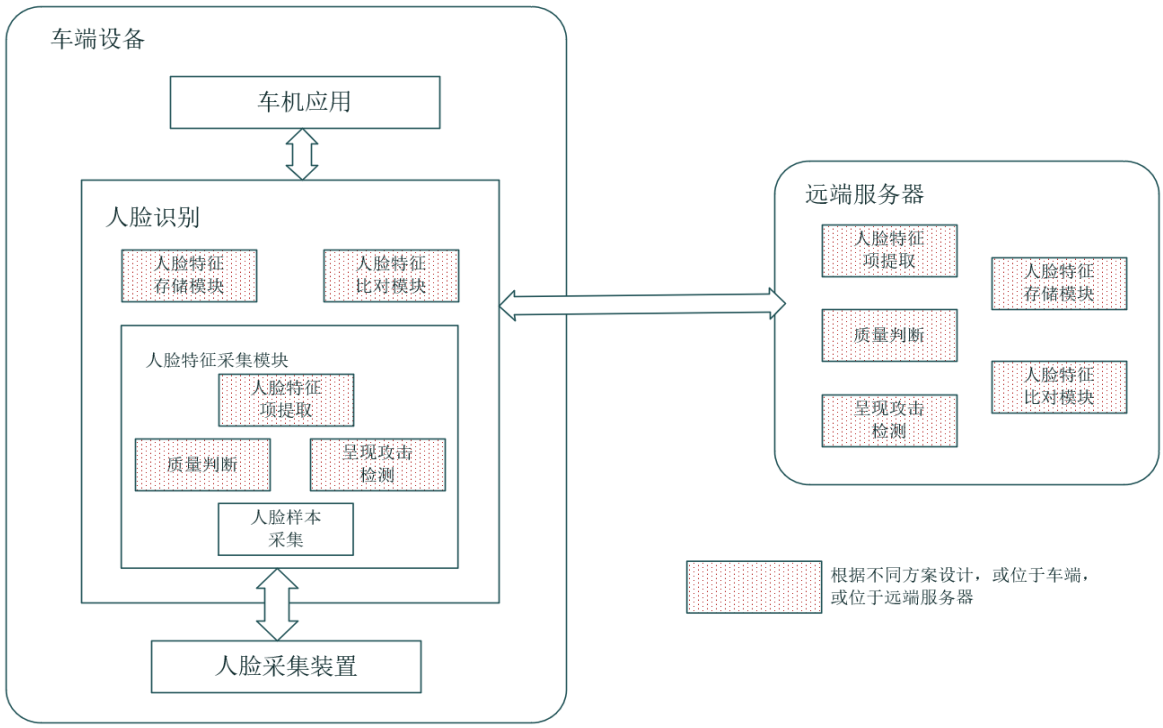
Term	Description
Artefact	Artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns 呈现生物特征或合成生物特征图案副本的人造物体或表示
Liveness	Quality or state of being alive, made evident by anatomical characteristics, involuntary reactions or physiological functions, or voluntary reactions or subject behaviors 存活的质量或状态，通过解剖特征，非自愿反应或生理功能，或自愿反应或受试者行为而明显
Liveness detection	Measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture 测量和分析解剖特征或非自愿或自愿反应，以确定是否从捕获点处存在的活体对象中捕获了生物特征样本
Normal presentation	Interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system 生物特征捕获主体与生物特征数据捕获子系统之间的交互以生物特征系统的策略所预期的方式进行
Presentation attack	Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system 向生物识别数据捕获子系统的演示，旨在干扰生物识别系统的运行
Presentation attack detection (PAD)	Automated determination of a presentation attack 自动确定演示攻击
Presentation attack instrument (PAI)	Biometric characteristic or object used in a presentation attack 演示攻击中使用的生物特征或对象
Facial recognition	The process of identifying an individual based on the characteristics of the individual's face 基于个体的人脸特征，对个体进行识别的过程
Face characteristic	The distinguishing and repeatable feature information can be extracted from the individual's face information, so as to achieve the purpose of automatic identification 可以从个体的人脸信息中提取出的有区别的、可重复的特征信息，从而达到个体自动识别的目的
Face data	This standard is a general term for face samples, face references, face features, or face features at any stage of processing 本标准对处于任何处理阶段的人脸样本、人脸参考、人脸特征项或人脸特性的通称
Face capture device	Device for collecting face recognition feature information and converting it into adult face collection sample 收集人脸识别特征信息并将其转换成人脸采集样本的装置
Face sample	Representation of simulated or digital facial features obtained from a face acquisition device 从人脸采集装置获得的模拟的或数字的人脸特征的表示
Face feature	A numeric value or marker extracted from a face sample for comparison 从人脸样本中提取的，用于比对的数值或标记
Face probe	Face data input to the algorithm and compared with face reference data 输入到算法的、与人脸参考数据进行比对的人脸数据

Term	Description
Face template	The set of reference facial feature items, the set of stored facial feature items, can be directly compared with the facial feature items of the face probe sample 参考的人脸特征项的集合，已存储的人脸特征项的集合，可直接与人脸探针样本的人脸特征项进行比对
Face reference	One or more stored face samples, face templates, face recognition models, etc. belonging to the biometric data body for comparison 用于比对的、属于生物特征数据主体的一个或多个已存储的人脸样本、人脸模板或人脸识别模型等
APFAR	Attack presentation false acceptance rate 呈现攻击误判率
APNRR	Attack presentation non-response rate 呈现攻击无响应率
BPFRR	Bona fide presentation false rejection rate 善意呈现误判率
BPNRR	Bona fide presentation non-response rate 善意呈现无响应率
FAR	False acceptance rate 错误接受率
FRR	False rejection rate 错误拒绝率
SE	Secure element 安全元素
REE	Rich execution environment 丰富的执行环境
TEE	Trusted execution environment 受信任的执行环境

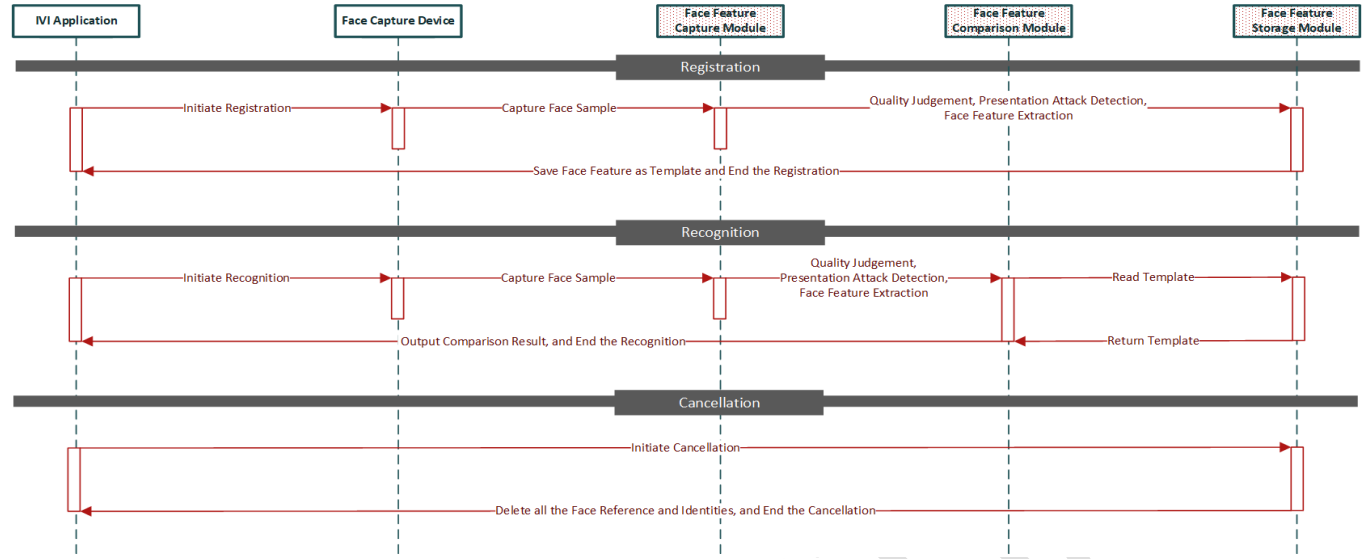
2 Facial Recognition Architecture and High Level Flow

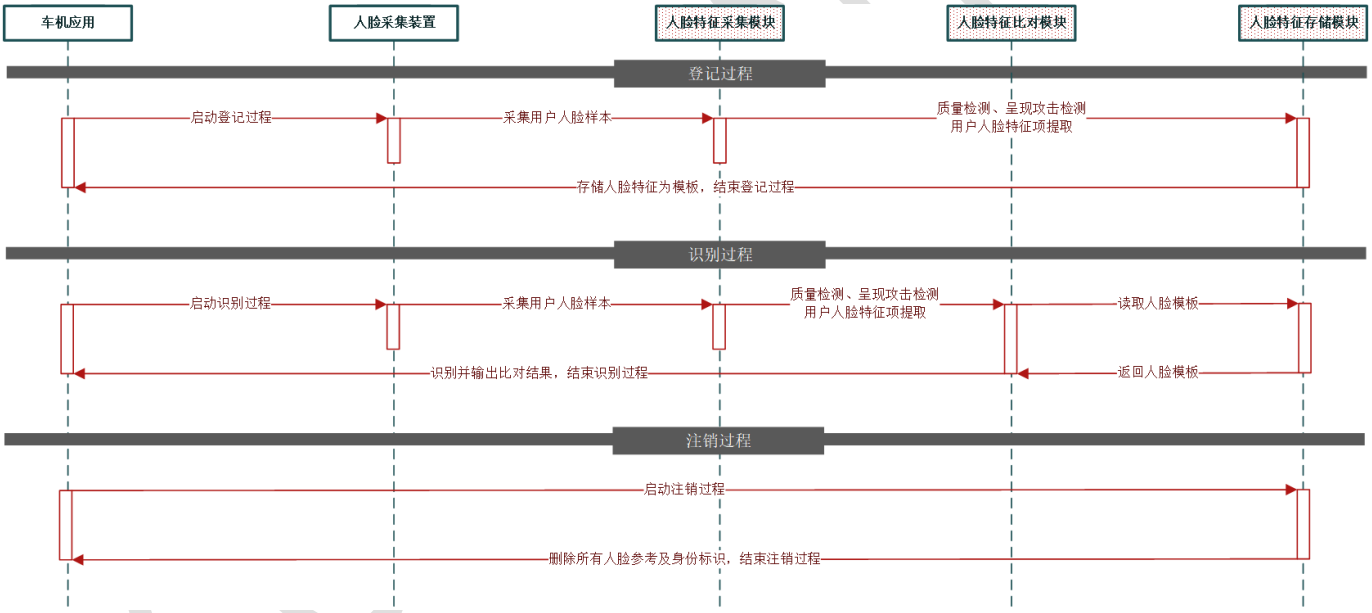
2.1 Architecture



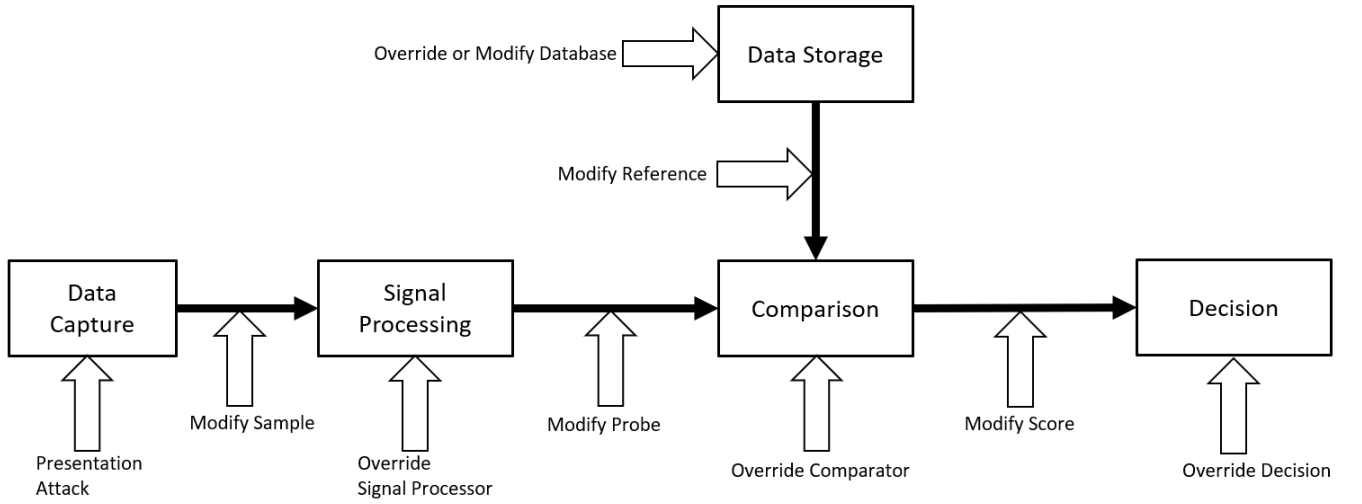


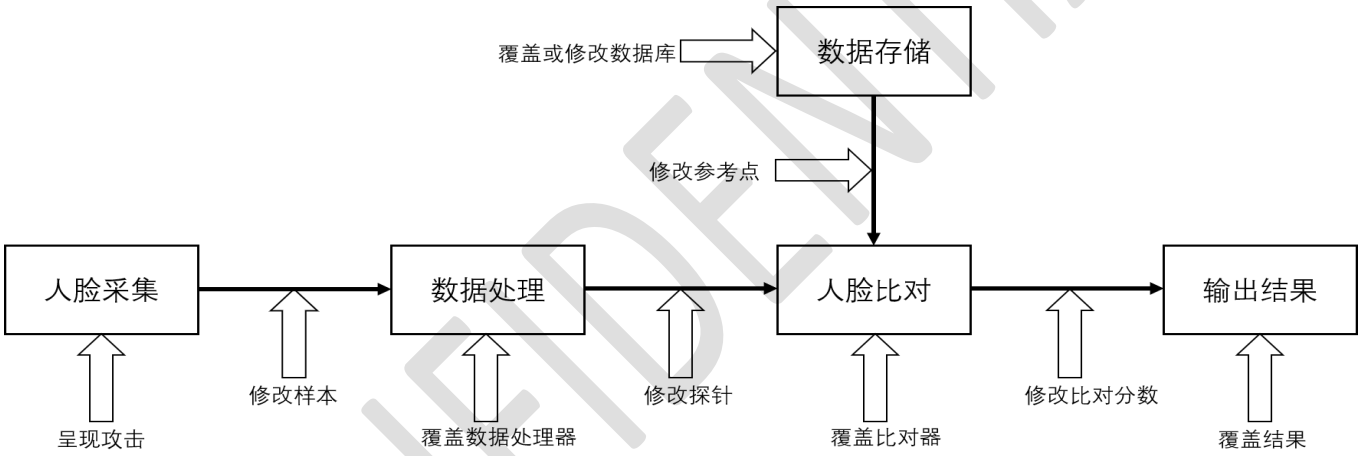
2.2 High Level Flow





3 Facial Recognition Process and Attack Type





Presentation Attack	Description
Print attack	The attacker uses someone's photo. The image is printed or displayed on a digital device. 攻击者使用某人的照片。 图像在数字设备上打印或显示
Replay/video attack	A more sophisticated way to trick the system, which usually requires a looped video of a victim's face. This approach ensures behavior and facial movements to look more 'natural' compared to holding someone's photo. 一种更复杂的欺骗系统的方法，通常需要循环播放受害者面部的视频。 与拿着某人的照片相比，这种方法可确保行为和面部动作看起来更“自然”
3D mask attack	During this type of attack, a mask is used as the tool of choice for spoofing. It's an even more sophisticated attack than playing a face video. In addition to natural facial movements, it enables ways to deceive some extra layers of protection such as depth sensors. 在这种类型的攻击过程中，将掩码用作欺骗的首选工具。 这比播放人脸视频还要复杂。 除了自然的面部移动外，它还可以欺骗一些额外的保护层，例如深度传感器

4 Security Requirements

4.1 General security requirements

人脸识别功能模块基本安全要求包括但不限于：(The basic security requirements of the face recognition function module include but are not limited to:)

- 应具备有效的安全机制，确保当前操作人员拥有合法权限完成用户登记、更新和注销；宜采取适当的机制和程序，在用户登记过程中确认当前登记者的真实身份; (Effective security mechanisms should be in place to ensure that current operators have legal authority to complete user registration, update and cancellation; appropriate mechanisms and procedures should be in place to confirm the current identity of the current registrant during the user registration process;)
- 在运行时宜具备运行环境的检查能力，检查范围可包括移动设备系统是否被非法用户获取管理员权限、程序运行环境是否可信等,在发现运行环境异常时应具备相应处理措施，如提示用户安全风险、关闭应用等；(It is advisable to have the inspection capability of the operating environment during operation. The scope of the inspection may include whether the mobile device system is authorized by an unauthorized user, whether the program running environment is trusted, etc., and when the operating environment is abnormal, the corresponding processing measures should be provided, such as prompting the user to be safe. Risk, closing applications, etc.;)
- 应采取安全验证措施确保只有具备调用权限的调用方才能调用该模块；(Security verification measures should be taken to ensure that only the caller with the call permission can call the module;)
- 应采取安全加固措施提升自身安全防护水平，如：(Safety reinforcement measures should be taken to improve the level of safety protection, such as:)
    - 代码混淆、重新编译、加壳保护、修改指令调用顺序等；(Code obfuscation, recompilation, pack protection, modify instruction call order, etc.;)
    - 在运行时自身代码和文件完整性检查；(Source code and file integrity check at runtime)
    - 自身代码防注入处理。(Code injection prevention processing)
- 应具备有效的安全机制，确保人脸特征样本采集、质量判断、呈现攻击检测、人脸特征项提取和传输过程中的用户特征数据的机密性和完整性；(Effective security mechanisms should be in place to ensure the confidentiality and integrity of user profile data during face feature sample collection, quality judgment, presence attack detection, face feature extraction and transmission;)
- 应及时清除未通过质量判断的用户人脸特征样本，并确保其不可恢复；(User face feature samples that fail quality judgment should be cleared in time and ensured that they are unrecoverable)
- 生物特征项提取结束后应及时清除用户的人脸特征样本，并确保其不可恢复 (After the biometric item is extracted, the user's face feature sample should be cleared in time and ensure that it is unrecoverable.)

4.2 Face feature capture module security requirements

- 宜设置人脸特征采集超时处理机制，即在设置的有效时长内，如无法采集到符合质量要求的且通过呈现攻击检测的人脸样本时，模块自动退出运行；(It is advisable to set the face feature collection timeout processing mechanism, that is, within the set effective time, if the face sample that meets the quality requirements and is detected by the attack detection cannot be collected, the module automatically exits the operation;)
- 应保护用户输入的敏感数据或采集到的用户人脸数据；(User-entered sensitive data or collected user face data should be protected;)
- 远程识别模式中，车端设备如支持 TEE 或者 SE 等可信环境时，宜结合可信环境增强人脸特征采集模块的安全性，包括但不限于：(In the remote identification mode, when the vehicle end equipment supports a trusted environment such as TEE or SE, it is better to enhance the security of the face feature collection module in combination with a trusted environment, including but not limited to;)
    - 宜使用位于可信环境中的人脸采集装置对用户的人脸样本进行采集；(It is advisable to collect the user's face samples using a face acquisition device located in a trusted environment;)
    - 宜在可信环境中对采集的用户人脸样本进行质量判断、呈现攻击检测和人脸特征项提取；(It is advisable to perform quality judgment, presentation attack detection and face feature extraction on collected user face samples in a trusted environment;)

- 宜通过可信环境中的可信交互界面实现与用户之间的交互；(It is advisable to interact with users through a trusted interaction interface in a trusted environment;)
- 宜在可信环境中存储所涉及的密钥，如与远端服务器之间进行安全通讯时所涉及到的密钥。(It is advisable to store the key involved in a trusted environment, such as the key involved in secure communication with the remote server.)

- 本地识别模式中，人脸特征采集模块应通过可信环境进行安全保护。(In the local recognition mode, the face feature collection module should be secured by a trusted environment)
- 呈现攻击检测性能要求应满足下表要求 (The performance requirements for attack detection should meet the requirements of the following table.)

攻击类型(Attack type)	性能要求 (Performance requirements)		
	BPFRR/APFR	APNRR	BPNRR
二维呈现攻击类型 2D rendering attack type	在 APFAR 为 3%时， BPFRR 应＜3%	计算速率 1s 的情况下 APNRR 应＜5%	计算速率 1s 的情况下 BPNRR 应＜3%
三维呈现攻击类型 3D rendering attack type	在 APFAR 为 5%时， BPFRR 应＜5%	计算速率 1s 的情况下 APNRR 应＜5%	计算速率 1s 的情况下 BPNRR 应＜3%

4.3 Face feature storage module security requirements

- 远程识别模式中，人脸特征存储模块安全要求包括但不限于：(In the remote identification mode, the face feature storage module security requirements include but are not limited to;)
  - 应对用户人脸参考进行去标记操作或脱敏处理，并应与用户身份标识信息分库保存；(The user face reference should be de-marked or desensitized, and should be saved with the user identity information;)
  - 宜采用加密的方式在人脸特征存储模块中存储用户的人脸参考。(The user's face reference should be stored in the face feature storage module in an encrypted manner.)
- 本地识别模式中，应结合可信环境采取有效的安全方式对用户的人脸数据的本地存储进行安全保护。(In the local identification mode, the local storage of the user's face data should be secured in an effective and secure manner in combination with the trusted environment.)

4.4 Face feature comparison module security requirements

- 远程识别模式中，移动设备如支持 TEE 或 SE 等可信环境，宜结合可信环境增强人脸特征比对模块的安全性，如在可信环境中存储并使用安全通讯所涉及的密钥，使用可信交互界面向用户展示识别决策结果等。(In the remote identification mode, if the mobile device supports a trusted environment such as TEE or SE, it is better to enhance the security of the face feature comparison module in combination with a trusted environment, such as storing and using the key involved in secure communication in a trusted environment. Use a trusted interface to show users the results of identifying decisions, etc.)
- 本地识别模式中，人脸特征比对模块安全要求为：(In the local recognition mode, the face feature comparison module security requirement is:)
  - 人脸特征比对模块一般是以软件的形式在移动设备中实现，应采取有效的安全措施确保该模块的安全性，并采取有效的安全措施确保比对过程中所使用的用户人脸数据以及识别决策结果的保密性和完整性，不被窃取或篡改；(The face feature comparison module is generally implemented in a mobile device in the form of software. Effective security measures should be taken to ensure the security of the module, and effective security measures are taken to ensure the user face data used in the comparison process and Identify the confidentiality and integrity of decision-making results without being stolen or tampered with;)
  - 比对结束后，按照 GB/T 35273-2017 信息安全技术个人信息安全规范 规定来处理用户人脸特征数据和比对过程中所产生的其他临时数据(After the comparison, the user's face feature data and other temporary data generated during the comparison process are processed in accordance with the GB/T 35273-2017 information security technology personal information security specification.)
  - 应在可信环境中如 TEE 或 SE 实现人脸特征比对模块。(Face feature comparison module should be implemented in a trusted environment such as TEE or SE)

4.5 Face data transmission security requirements

- 远程识别模式中：(Remote identification mode:)

- 在将采集到人脸数据传输到远端服务器时，应采取有效的安全方式对人脸数据进行安全保护，确保其保密性和完整性；(When transmitting the collected face data to the remote server, the face data should be securely protected in an effective and secure way to ensure its confidentiality and integrity.;)
- 从移动设备中传输人脸数据到远端服务器进行比对并返回识别决策结果，应采取有效的安全方式对传输的人脸数据以及识别决策结果进行安全保护，确保其保密性和完整性，不被窃取或篡改。(Transmitting face data from the mobile device to the remote server for comparison and returning the recognition decision result, the effective transmission method should be adopted to securely protect the transmitted face data and the recognition decision result to ensure confidentiality and integrity. Being stolen or tampered with)
- 采用满足数据传输安全策略相应的安全控制措施，如安全通道、可信通道、数据加密等。(Adopt appropriate security control measures to meet data transmission security policies, such as secure channels, trusted channels, data encryption, etc.)
- 具备在构建传输通道前对两端主体身份进行鉴别的能力。(Ability to identify both body identities before building a transmission channel)
- 具备对传输数据的完整性进行检测的能力以及相应的恢复控制措施。(Ability to detect the integrity of transmitted data and corresponding recovery control measures)
- 支持数据真实性检测，应采用国家规定的签名密码算法及组合算法鉴别数据的来源。(Support data authenticity detection, should use the national signature cryptography algorithm and combination algorithm to identify the source of data)

4.6 Facial recognition system log security requirements

- 日志安全要求包括但不限于：(Log security requirements include but are not limited to:)
  - 日志记录中不应出现明文的人脸数据、密钥信息或其他安全相关的参数等；(Clear face data, key information, or other security-related parameters should not appear in the log record;)
  - 应采取安全措施对日志信息做完整性保护，如数字签名等；(Security measures should be taken to protect the log information integrity, such as digital signatures, etc.;)
  - 应具备授权管理机制，对日志记录的增加、删除、修改的操作权限进行管理。(Should have an authorization management mechanism to manage the operation rights of adding, deleting, and modifying log records.)

5. Appendix

5.1 Secure Environment Security Requirements

若设备支持可信执行环境或安全单元等安全环境，在生物特征采集、存储和比对过程中(If the device supports a secure environment such as a trusted execution environment or security unit, in the process of biometric collection, storage and comparison)

- 宜使用位于可信执行环境中的生物特征采集模块对用户的生物特征样本进行采集；(User biometric samples should be collected using a biometric acquisition module located in a trusted execution environment;)
- 宜在可信执行环境中对采集的用户生物特征样本进行质量判断，呈现攻击检测和生物特征项提取；(It is advisable to perform quality judgment on the collected user biometric samples in a trusted execution environment, presenting attack detection and biometric item extraction.;)
- 如果生物特征存储和比对模块在移动设备中实现，应在可信执行环境中实现生物特征存储和比对；(Biometric storage and comparison in a trusted execution environment if the biometric storage and comparison module is implemented in a mobile device)
- 宜使用可信执行环境或安全单元中的安全服务，如安全加解密服务、安全时钟服务、随机数服务等；(It is advisable to use security services in a trusted execution environment or security unit, such as security encryption and decryption services, secure clock services, random number services, etc;)
- 应通过可信执行环境中可信交互界面实现与用户之间的交互；(Interaction with users should be achieved through a trusted interaction interface in a trusted execution environment;)
- 应在可信执行环境或安全单元中存储所涉及的密钥；(The key involved should be stored in a trusted execution environment or security unit;)

- 如需与位于富执行环境的生物特征采集模块或移动应用进行数据交互时，应具备有效的安全机制验证富执行环境中交互对象的合法性，数据交互过程中宜采用安全通道机制以保证交互数据的完整性和机密性。(If you need to interact with the biometric collection module or mobile application located in the rich execution environment, you should have an effective security mechanism to verify the legality of the interactive objects in the rich execution environment. In the data interaction process, a secure channel mechanism should be adopted to ensure the interaction data. Integrity and confidentiality)

5.2 Security Audit Requirements

5.2.1 数据安全审计(Data Security Audit)

安全审计功能应按以下要求产生审计数据：(The security audit function should generate audit data according to the following requirements:)

- 为下述可审计事件产生审计记录：(Generate audit records for the following auditable events:)
  - 审计功能的开启和关闭；(Audit function on and off;)
  - 使用身份鉴别机制；(Use identity authentication mechanism;)
  - 系统管理员、安全管理员、审计管理员和一般操作员所实施的操作；(Operations performed by system administrators, security administrators, audit administrators, and general operators;)
  - 其他与系统安全有关的事件或专门定义的可审计事件；(Other system security related events or specially defined auditable events;)
  - 伪造人脸图像；(Forged face image;)
  - 人脸假体面具仿冒；(Face prosthetic mask counterfeiting;)
  - 伪造特征数据或篡改识别结果数据、用户属性数据、配置管理数据；(Forging feature data or tampering with recognition result data, user attribute data, configuration management data;)
  - 企图保存人脸图像；(Attempting to save a face image;)
  - 非授权保存特征数据；(Unauthorized saving of feature data;)
  - 非授权进行数据库操作。(Unauthorized database operations)
- 审计记录至少应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；(The audit record should at a minimum include: the date and time of the event, the user, the type of event, the success of the event, and other audit-related information;)
- 日志记录中不应出现明文形式的人脸特征模板、私钥、对称密钥及其它安全相关的参数。(Face feature templates, private keys, symmetric keys, and other security-related parameters in clear text should not appear in the log record.)
- 审计功能部件应能将可审计事件与发起该事件的用户身份相关联。(The audit feature should be able to associate an auditable event with the identity of the user who initiated the event)
- 对于身份鉴别事件，审计记录应包含请求的来源（例如：设备标识符）。(For identity authentication events, the audit record should contain the source of the request (for example: device identifier))

5.2.2 安全审计审阅 (Security Audit Review)

根据对安全审计的不同要求，安全审计查阅分为：(According to the different requirements of security audit, security audit review is divided into:)

- 审计功能部件应为管理员提供查看日志所有信息的能力。(The audit feature should provide administrators with the ability to view all information about the log)
- 审计功能部件应以适于阅读和解释的方式向阅读者提供日志信息。(The audit function should provide the log information to the reader in a manner suitable for reading and interpretation.)

5.2.3 安全审计事件选择 (Security Audit Event Selection)

审计功能部件应可根据下列属性选择或排除审计事件集中的可审计事件：(The audit feature should be able to select or exclude auditable events from the audit event set based on the following attributes:)
用户标识、事件类型、主体标识、客体标识等。(User ID, event type, subject ID, object ID, etc.)

5.2.3 安全审计事件存储 (Security Audit Event Storage)

根据对安全审计的不同要求，安全审计事件存储分为：(According to the different requirements of security audit, security audit event storage is divided into:)

- 受保护的审计踪迹存储：审计踪迹的存储受到应有的保护，能检测或防止对审计记录的修改；（Protected audit trail storage: The storage of audit trails is protected as intended to detect or prevent modification of audit records:）
- 防止审计数据丢失：在审计踪迹存储记满时，应能够阻止除由管理员发起的以外的所有审计事件的发生；（Prevent audit data loss: When audit trail storage is full, it should be able to block the occurrence of all audit events except those initiated by the administrator;）
- 审计数据的可用性确保：在意外情况出现时，能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击时，确保审计记录不被破坏（The availability of audit data ensures that changes to audit records can be detected or prevented in the event of an unexpected situation, and that audit records are not destroyed when audit storage is full, storage fails, or storage is compromised）

5.2.3 安全审计日志保护 (Security Audit Log Protection)

- 审计功能部件应定期对审计日志做数字签名等完整性保护运算。（The audit function should periodically perform digital signatures and other integrity protection operations on the audit log.）
- 完整性保护运算的对象是从上次签名后加入的所有审计日志条目以及上次签名的结果。（The object of the integrity protection operation is all the audit log entries added since the last signature and the result of the last signature）
- 对审计日志签名的时间周期应是可配置的。（The time period for signing the audit log should be configurable）
- 对审计日志签名的事件应写入审计日志中，审计日志签名结果应包含在其中。（Events signed to the audit log should be written to the audit log, and the audit log signature results should be included）