UNISOC FaceID User Guide

适用产品信息	SC9863A\SC9832E\SC7731E\UMS312\UMS512(T)
适用版本信息	Android 10.0\Android 9.0\Android 8.1
关键字	FaceID

声明

本文件所含数据和信息都属于紫光展锐所有的机密信息，紫光展锐保留所有相关权利。本文件仅为信息参考之目的提供，不包含任何明示或默示的知识产权许可，也不表示有任何明示或默示的保证，包括但不限于满足任何特殊目的、不侵权或性能。当您接受这份文件时，即表示您同意本文件中内容和信息属于紫光展锐机密信息，且同意在未获得紫光展锐书面同意前，不使用或复制本文件的整体或部分，也不向任何其他方披露本文件内容。紫光展锐有权在未经事先通知的情况下，在任何时候对本文件做任何修改。紫光展锐对本文件所含数据和信息不做任何保证，在任何情况下，紫光展锐均不负责任何与本文件相关的直接或间接的、任何伤害或损失。

请参照交付物中说明文档对紫光展锐交付物进行使用，任何人对紫光展锐交付物的修改、定制化或违反说明文档的指引对紫光展锐交付物进行使用造成的任何损失由其自行承担。紫光展锐交付物中的性能指标、测试结果和参数等，均为在紫光展锐内部研发和测试系统中获得的，仅供参考，若任何人需要对交付物进行商用或量产，需要结合自身的软硬件测试环境进行全面的测试和调试。

版本历史

版本	日期	备注
V1.0	2020/1/2	初稿

目录

图目录

1 前言

1.1 范围

本文档主要介绍了人脸解锁功能的原理、功能限制以及常见问题分析。

本文档的使用人员包括：

FaceID 开发人员、测试人员以及对外合作的开发人员以及客户。

1.2 缩略语

名称	全称	定义
FaceID	face identification	人脸识别,人脸认证
TEE	Trusted Execution Environment	可信执行环境

2 FaceID 原理简介

2.1 原理简介

UNISOC FaceID 功能主要是指进行一比一的人脸认证，即为了解决两个人是否为同一个人的问题；应用上是作为人脸解锁进行使用，人脸解锁分为注册和解锁两个阶段。注册阶段读入人脸图片进行信息提取，存储人脸模板信息；解锁阶段读入人脸图片进行信息提取，判断是否是真实人脸，并与录入阶段存储的人脸信息进行匹配，符合要求则解锁成功，反之则解锁失败。

2.2 流程简介

2.2.1 数据预处理

如图 2.1，预处理过程可以简单分为三个步骤，人脸检测、人脸关键点检测、人脸标准化，其中人脸检测是从图片中找出人脸；人脸关键点检测在上一步中找到的人脸上确认人脸的特征点信息；然后根据特征点信息，将人脸部分归一化成固定方向与尺寸的图像作为输入给人脸识别模块。

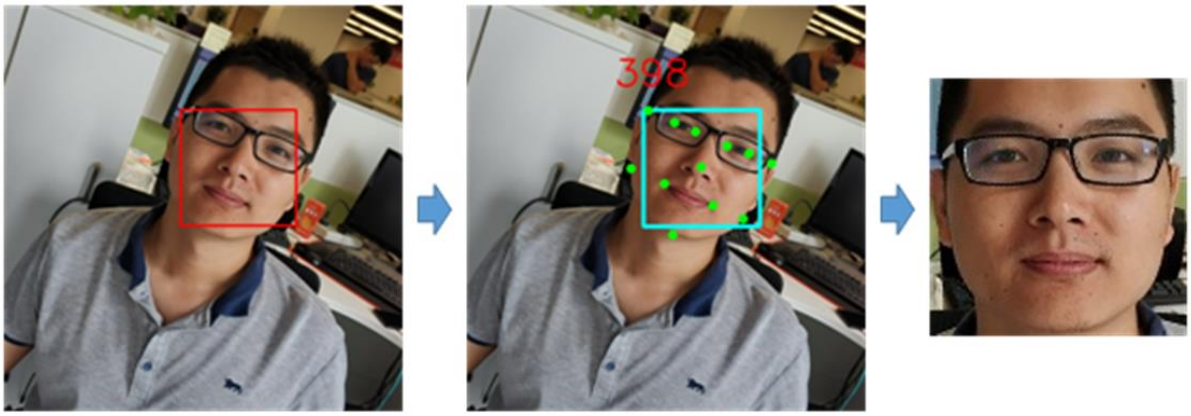

图 2.1 数据预处理过程

2.2.2 活体检测模块

人脸活体检测的目标是检测手机人脸认证系统的验证用户是真实活体在操作，以抵御照片、视频等手段的攻击，保障用户的利益。

目前版本的人脸活体检测原理为识别人眼眨眼这一生理特征，通过这一特征来判断是否是真实活体在操作。判断人眼眨眼的算法首先精确提取一些人脸的关键点位置（比如眼睛的轮廓点），精确定位眼睛的位置；然后采用机器学习的方法，基于大量人脸样本训练识别人眼状态的识别器。通过上述的方法判断用户是否有眨眼这一的生理动作。该版本人脸活体检测可以有效防止照片类的假脸攻击。

2.2.3 人脸识别模块

如图 2.2，人脸识别模块拿到预处理给出的人脸图片，直接输入给深度神经网络 CNN 进行特征提取，最终提取出人脸高维特征向量；如果是注册过程则会将特征信息存储下来备份，如果是解锁过程，则将新提取的特征与注册过程中存储的特征进行匹配，如果相似度比较高，则认为是同一个人，否则不是同一个人。

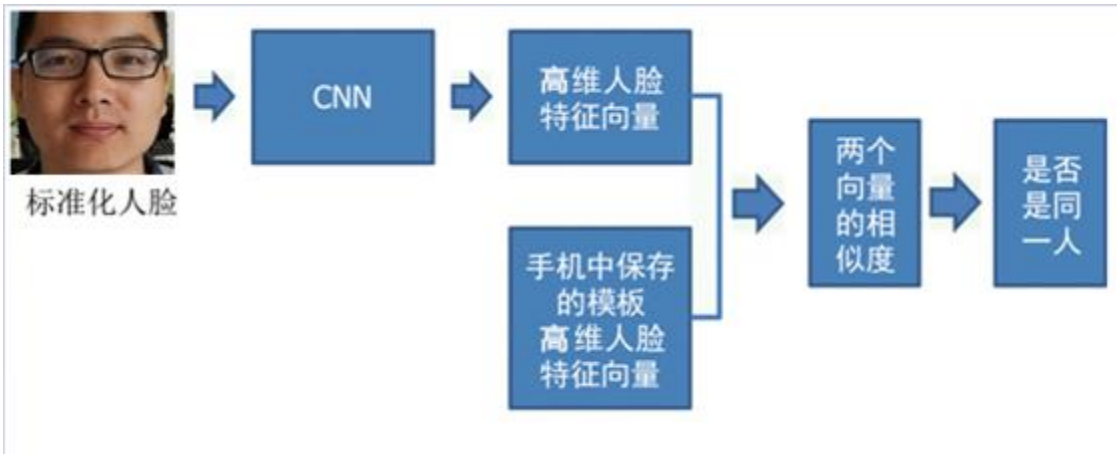

图 2.2 人脸识别过程

3 FaceID 功能限制

3.1 人脸录入阶段

3.1.1 关于人脸位置

需要结合 UI 窗口的位置，在 UI 窗口内部适当位置录入。

3.1.2 关于人脸姿态

人脸在图像平面的旋转角度：[-5°, 5°]

人脸绕颈旋转的角度：[-5°, 5°]

人脸垂直方向的角度（低头、抬头）: [-10°, 30°]

3.1.3 关于遮挡

不接受对人眼和嘴巴进行遮挡，比如墨镜、口罩都是不接受的，所以请保持面部清洁，以防解锁时降低成功率。

3.1.4 关于闭眼

不允许录入的时候处于闭眼状态。

3.1.5 关于光线

对于过暗、过亮或者逆光的环境录入会降低解锁成功率，不建议在这种环境下进行录入;加入了光照条件的限制，过暗或者逆光都是无法录入的。

3.1.6 关于照片/视频录入

不允许这种方式的录入。

3.1.7 关于多人的录入

不允许在 100cm 内的多人同时在界面的录入，在 100cm 外的人将会被忽略。

3.1.8 关于录入流程

当前的录入机制是两姿态(正脸，抬头)录入，后续逐渐会更新到单姿态（正脸）录入的方式。

3.2 人脸解锁阶段

3.2.1 关于解锁距离

一般情况下支持 30-100cm 范围内解锁。

3.2.2 关于人脸姿态限制如下：

人脸在图像平面的旋转角度：[0°, 360°)

人脸绕颈部的角度（人脸水平旋转角度）: [-30°, 30°]

人脸垂直方向的角度（低头、抬头）: [-30°, 30°]

3.2.3 关于人脸遮挡

不接受对人眼和嘴巴进行遮挡，比如墨镜、口罩都是不接受的，所以请保持面部清洁，以防解锁时降低成功率。

3.2.4 关于闭眼

不允许解锁的时候处于闭眼状态。

3.2.5 关于光线

对于过暗、过亮或者逆光的环境解锁会降低解锁成功率，不建议在这种环境下进行解锁。

3.2.6 关于表情

对于适度的表情可以解锁，过于夸张的表情有可能会降低解锁成功率。

3.2.7 关于视频解锁

无法防止这种欺骗。

3.2.8 关于人脸在画面中位置

对于部分人脸不在图像内的情况，解锁不会成功。

3.2.9 关于多人解锁

多人解锁时，只有最大人脸会启动解锁。

4 FaceID 常见问题分析

4.1 常见问题分析

4.1.1 是否符合功能限制？

请对照功能限制部分，确认使用或者测试方式是否满足设计需求

4.1.2 人脸录入困难

请确定光照环境是否符合要求，并参考人脸录入界面的提示操作。

如果需要进一步定位分析，请帮忙 dump 人脸录入数据供研发分析。

4.1.3 解锁容易失败

“曝光是否合适？人脸是否在图像内？”可使用 Camera 的预览功能进行初步判断，其他限制请参考功能限制部分的解锁限制见 3.2。

如果需要进一步定位分析，请帮忙 dump 人脸解锁和录入的数据供研发分析。

4.1.4 解锁速度较慢或者安全级别不足

由于不同芯片平台的硬件性能差异较大，解锁速度和解锁安全性之间需要平衡，不同平台的用户体验会有差异。

4.1.5 如何查看版本号？

方式一：用 adb 命令查询：adb logcat | grep "LIBVER" 查看 FACEID_CreateHandle 后面的版本号；

方式二 :通过 ylog 查询 :开启手机 dump log 功能 ,然后使用手机进行一次注册或者解锁 ,将 ylog dump 出来，在 log 中搜索关键字"LIBVER" 查看 FACEID_CreateHandle 后面的版本号；

4.1.6 如何 dump 人脸录入数据？

4.1.6.1 对于 SC9863A\SC9832E\SC7731E 项目

操作步骤如下：

```
adb root
adb remount
```

adb shell setprop persist.save.enrollface 1 （Android 8.1，Android 9.0 dump 每一帧录入数据，分析录入困难的问题时打开）

adb shell setprop persist.save.enrollface 2 （Android 8.1，Android 9.0 dump 录入成功的数据，分析解锁问题时与 dump 解锁数据的命令一起打开）

adb shell setprop persist.vendor.faceid.dump 1 （android 10）

数据都会存入如下手机目录中：

/data/vendor/faceid(android9.0) /data/system/users/0/facedata(android 8.1)
/data/vendor_de/0/facedata (android10)

adb pull /手机目录 ./本地目录

注意：注册数据文件名带有“e*.yuv”字样

4.1.6.2 对于 UMS312\UMS512(T)项目

操作步骤如下：

a) 如果 adb root; adb remount 可以成功：修改手机内/vendor/etc/init/storageproxyd_androidp.rc 文件，重启手机后执行步骤 b）

将 vendor.plaintext 服务的注释去掉：

start vendor.plaintext
service vendor.plaintext /vendor/bin/sprdstorageproxyd -f plaintext -d /dev/trusty-ipc-dev0 -p /data/vendor/sprd_ss -r /dev/block/mmcblk0rpmb
class late_start
group system
seclabel u:r:tee:s0

如果 remount 不成功，则打开终端执行如下命令，不要关闭命令窗口，执行步骤 b）

adb shell /vendor/bin/sprdstorageproxyd -f plaintext -d /dev/trusty-ipc-dev0 -p /data/vendor/sprd_ss -r /dev/block/mmcblk0rpmb

b) dump 开关设置

adb root
adb remount

adb shell setprop persist.save.enrollface 1（Android 8.1，Android 9.0 dump 每一帧录入数据，分析录入困难的问题时打开）

adb shell setprop persist.save.enrollface 2（Android 8.1，Android 9.0 dump 录入成功的数据，分析解锁问题时与 dump 解锁数据的命令一起打开）

adb shell setprop persist.vendor.faceid.enrollface 1 （Android10.0 dump 每一帧录入数据，分析录入困难的问题时打开）

adb shell setprop persist.vendor.faceid.enrollface 2 （Android10.0 dump 录入成功的数据，分析解锁问题时与 dump 解锁数据的命令一起打开）

录入数据都会存入手机目录中: /data/vendor/sprd_ss

注意：注册 yuv 数据文件名带有“enroll*.yuv”字样

4.1.7 如何 dump 人脸解锁数据？

4.1.7.1 对于 SC9863A\SC9832E\SC7731E 项目

操作步骤如下：

adb root
adb remount

adb shell setprop persist.save.authicateface 1 （Android 8.1 , Android 9.0）

adb shell setprop persist.vendor.faceid.dump 1 （Android 10.0 ）

数据都会存入如下手机目录中：

/data/vendor/faceid(android9.0) /data/system/users/0/facedata(android 8.1)
/data/vendor_de/0/facedata (android10)

adb pull /手机目录 ./本地目录

注意：解锁数据文件名带有 “a*.yuv”字样

4.1.7.2 对于 UMS312\UMS512(T)项目

操作步骤如下：

a) 如果 adb root; adb remount 可以成功：修改手机内/vendor/etc/init/storageproxyd_androidp.rc 文件，重启手机后执行步骤 b）

将 vendor.plaintext 服务的注释去掉：

start vendor.plaintext
service vendor.plaintext /vendor/bin/sprdstorageproxyd -f plaintext -d /dev/trusty-ipc-dev0 -p /data/vendor/sprd_ss -r /dev/block/mmcblk0rpmb
class late_start
group system

seclabel u:r:tee:s0

如果 remount 不成功，则打开终端执行如下命令，不要关闭命令窗口，执行步骤 b）

adb shell /vendor/bin/sprdstorageproxyd -f plaintext -d /dev/trusty-ipc-dev0 -p /data/vendor/sprd_ss -r /dev/block/mmcblk0rpmb

b) dump 开关设置

adb shell setprop persist.save.authicateface 1 （Android9.0）

adb shell setprop persist.vendor.faceid.authicateface 1 （Android 10.0）

解锁数据都会存入手机目录中: /data/vendor/sprd_ss

注意：解锁数据文件名带有 “auth*.yuv” 字样

4.1.8 人脸解锁调试 log 开关

如果需要 UNISOC 工程师帮忙定位问题 ,需要在 userdebug 版本复现问题并抓取相应 log 和图片数据，在抓取 log 之前需要输入如下命令以方便定位问题：

adb shell setprop persist.vendor.faceid.log 4