RZ Family

Partner/Craftwork Face recognition Demo run guide

Introduction

This application note explains how to run the face recognition demonstration provided by Craftwork, a Renesas Ready partner of RZ/V.

Target Devices

RZ/V2L series

Contents

1. What is Face recognition? 2

2. How Face recognition Works 2

3. About the methof of Face recognition 2

3.1 Classification by operation method 2

3.2 Classification by technical aspects 3

4. Introduction of Craftwork Face recognition 3

4.1 Summary 3

4.2 Processing steps and performance 4

5. Setup guide of Face recognition demo application 5

6. Operational guide of Face recognition demo application 8

Revision history 14

1. What is Face recognition?

Face recognition is a technology that extracts and analyzes facial features to identify specific individuals. It identifies individuals by comparing images or videos captured by a camera with information stored in a database. Compared to other biometric authentication methods such as fingerprint recognition, vein recognition, and iris recognition, face recognition offers the advantage of being non-contact, which enhances hygiene, and it is user-friendly as it allows authentication even when carrying items. It is increasingly being adopted in various fields, including security systems for access control, smartphone unlocking, and surveillance cameras.

In addition to the above, there are also methods that do not require personal identification or authentication. These face recognition detect where a person's face is located in an image and identify attributes such as gender, age, and expressions like smiling. In recent years, this technology has become widely used in marketing research, particularly in the retail sector.

2. How Face recognition Works

The face recognition process described here consists of the following three major steps.

1.Face detection

Detects only human faces in the image captured by the camera.

2.Feature extraction

Feature values are extracted from the face detected in ‘1’ above. In addition to the position and shape of the eyes, nose, and mouth, facial regions (contours) and, with the recent evolution of AI, information such as skin texture and wrinkles are also subject to extraction, improving authentication accuracy.

3.Matching check (Collation)

The features obtained in ‘2’ above are matched with the features in the pre-registered database of faces. If a matching face is found, the individual is authenticated; if not, the authentication fails. The system sets a certain threshold, called “similarity,” and authentication is successful only when the threshold is exceeded. The SDK allows the user to set the similarity value, but setting it to a low value increases the success rate but decreases the accuracy of authentication.

3. About the method of Face recognition

3.1 Classification by operation method

In operation, there are two types of face recognition systems: edge type and cloud type, and this system uses the edge type.

✓Features of Edge type

The major advantage of the edge type, where face recognition is installed in an edge device (in this case, RZ/V2L), is the speed of authentication. There are no delays caused by cloud processing or large data transfers, and highly accurate face recognition can be performed in real time. In addition, even when accessing external data on the network, matching is performed with minimal data, so communication costs can be reduced while maintaining high speed.

✓ Features of Cloud type

Since there is no need for an edge device (dedicated terminal), ordinary cameras installed in smartphones and tablets can be used, and there is no need to manage and maintain the system in-house. On the other hand, authentication takes time, and if the Internet is interrupted, the system itself becomes unavailable. Furthermore, since facial photos are personal data, measures must be taken to prevent information leaks and security risks due to hacking.

3.2 Classification by technical aspects

Technically, there are two methods of face recognition: Visual-based 2D authentication and 3D authentication that uses an IR (infrared camera) in combination.

✓2D authentication

The system can be configured with a standard RGB camera, thus reducing costs. This system uses 2D authentication, and RZ/V2L can simplify the system and provide a high-speed, highly accurate face recognition solution. For the detection of “spoofing” by smartphones and other devices, which has been in increasing demand recently, the system detects whether a person is a real person or not by extracting reflections and lens distortions of the panel surface in the captured image.

✓3D authentication

IR (infrared camera) enables highly accurate impersonation detection through authentication in dark environments and 3D detection of depth such as facial irregularities. However, the combined use of RGB and IR cameras results in higher costs and limits the size of the final product.

4. Introduction of Craftwork Face recognition

4.1 Summary

This section describes the “Face Detection/Face Recognition Model” offered by Craftwork, as RZ Ready partner. (Company URL https://craft-server.co.jp/service/ai-solution/)

This solution implements the company's uniquely designed and trained face detection/face recognition AI model in DRP-AI, the RZ/V2L's HW accelerator, to provide face recognition that can operate on actual devices.

✓Business model

- This is a partner-made solution and will be charged for.
- Currently, Craftwork is considering opening a GitHub where related software will be posted in the future. As for the immediate operation, if you would like to receive a trial SD image file, please send an application mail to the following mail address. Craftwork will provide you with the SD image as soon as possible, but please understand that we may decline your request depending on the situation.

  Mail to: ai_info@craft-server.co.jp
- Please fill in following information

  Subject: Face Recognition Demo

  Message: Company name, Your name, Purpose of use

✓Main functions and features

- Support for multiple face detection and face recognition
- Multiple attributes can be detected for face detection (whether or not a mask is worn, face orientation, etc.)
- Authentication is possible even when masks are worn.
- Biometric identification using a single-lens camera (to avoid impersonation in photos and videos)
- High-performance, lightweight model optimized for DRP-AI for edge applications
- Complete SDK available for immediate use

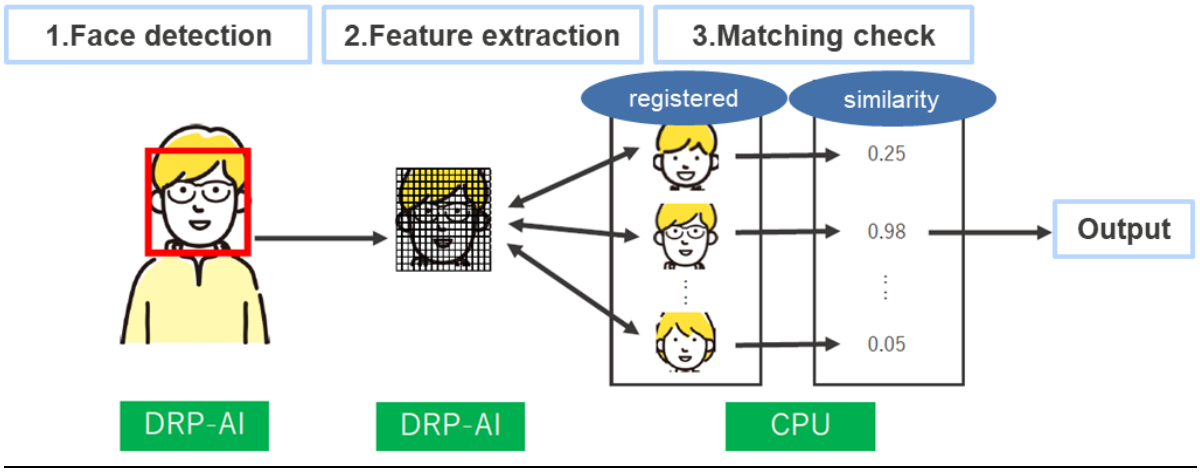
✓Usage Scenes

- Surveillance Cameras Detecting Suspicious Persons
- Access control systems

- Hands-free authentication
- Privacy protection processing by facial filtering
- Biometric authentication for personal devices
- User authorization functions for equipment that should be restricted to limited users, etc.

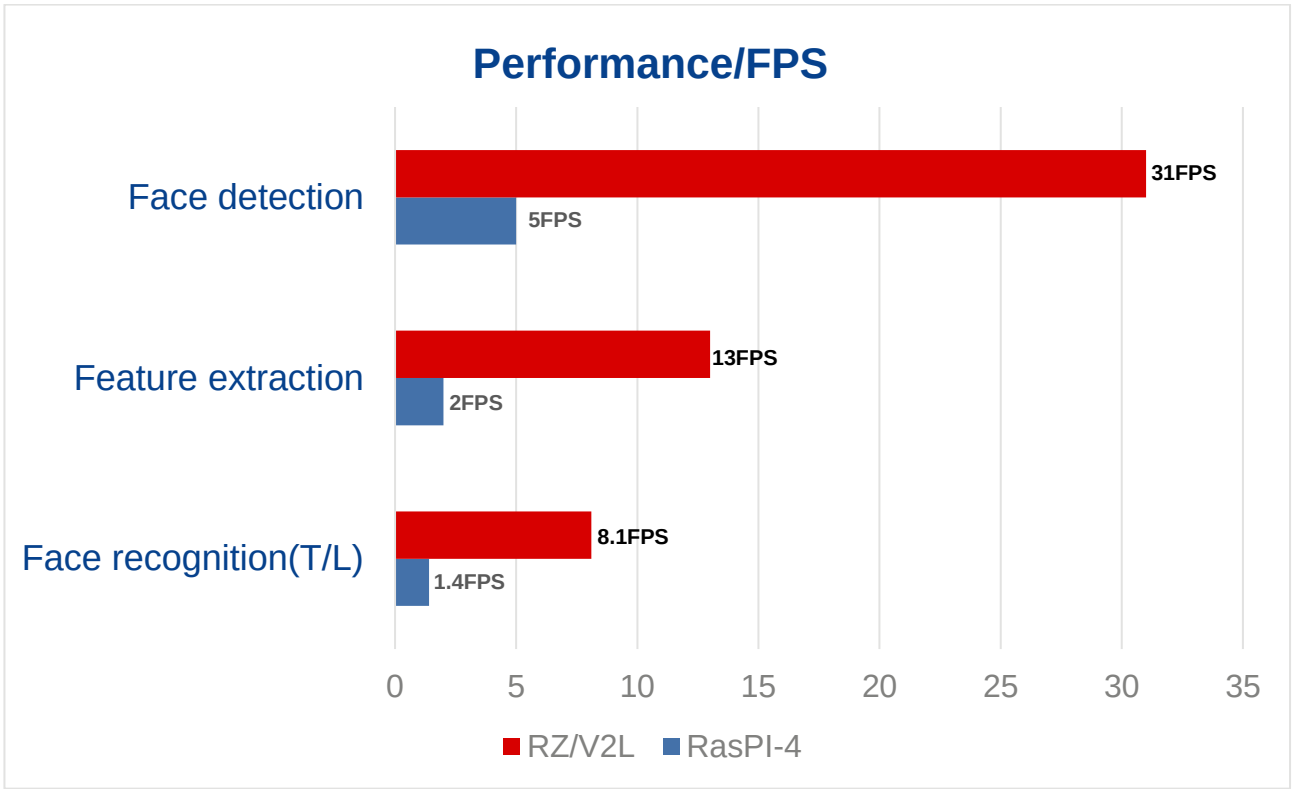
4.2 Processing steps and performance

✓Processing steps from face detection to face recognition



✓Performance

Performance of processes executed by DRP-AI compared to Raspberry Pi-4



5. Setup guide of Face recognition demo application

5.1 Setup procedures

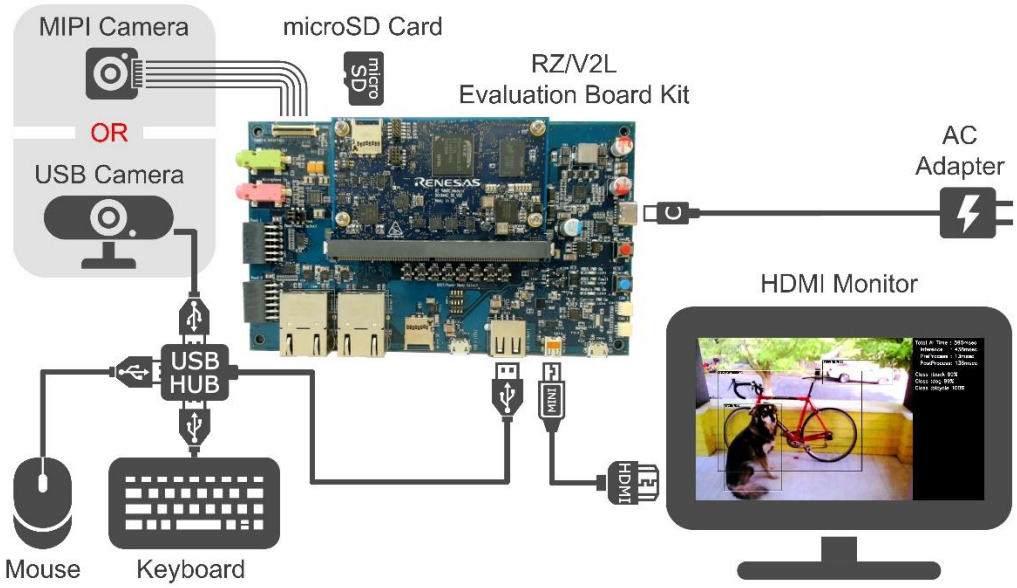
① Prepare SD card. (32GB Micro SD card)
② Extract the downloaded file rzv2l_evk_facerecog_yyyyymmdd.tar.gz. (yyyymmdd is a date string) The unzipped file will be rzv2l_evk_xxxxx.ddi file. (The xxxxxx part is an identification string, which is different for each user.)
③ Insert the SD card ① into the Linux PC.
④ Copy the file rzv2l_evk_xxxxx.ddi extracted in ② to the Linux PC and restore the SD image using the dd command. Command execution example: (when the sd card is mounted on /dev/sdb)

```
sudo dd bs=4M if=./rzv2l_evk_xxxxx.ddi of=/dev/sdb conv=fsync status=progress
```

Replace the xxxxxx part of rzv2l_evk_xxxxx.ddi with the actual file name.

/dev/sdb should be the name of the device on which the SD card is mounted.

⑤ Insert the SD card into the RZ/V2 EVK. Also, connect HDMI Monitor, AC Adapter, USB Camera, and USB mouse.



Above figure taken from RZ/V2L AI Applications Demo How to Use Guide/Overview
https://renesas-rz.github.io/rzv_ai_sdk/latest/

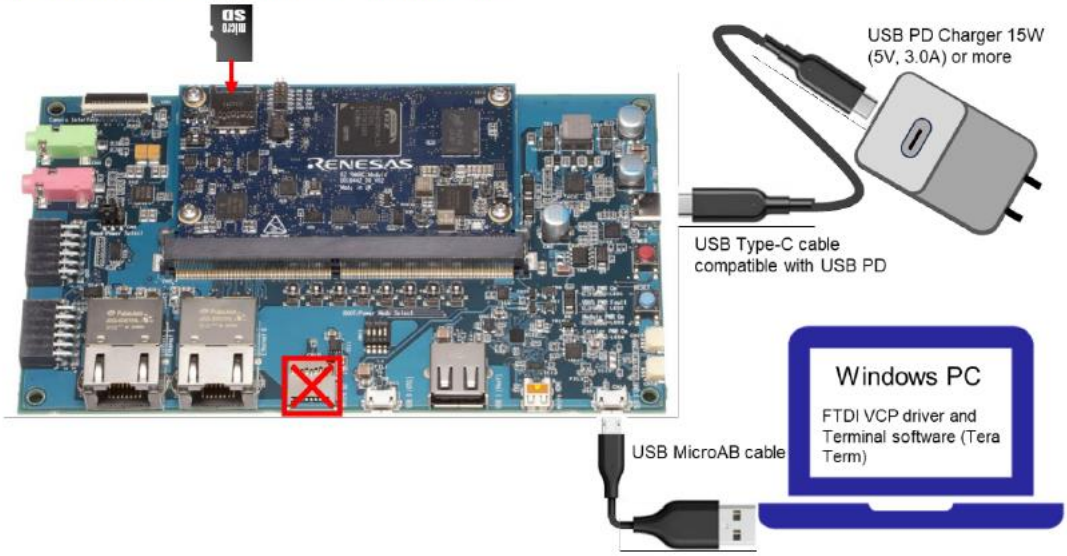
⑥ Set SW11 of RZ/V2L EVK to eSD boot.
Reference source : SMARC EVK of RZ/V2L Linux Startup Guide(R01US0617EJ0103)
8. Appendix
- 8.4 How to boot from eSD

8.4.2 Set SMARC EVK board for eSD boot

Change the switches to eSD boot on the carrier board acting on SW11 (SW11-1 ON, SW11-2 ON, SW11-3 OFF, SW11-4 ON)

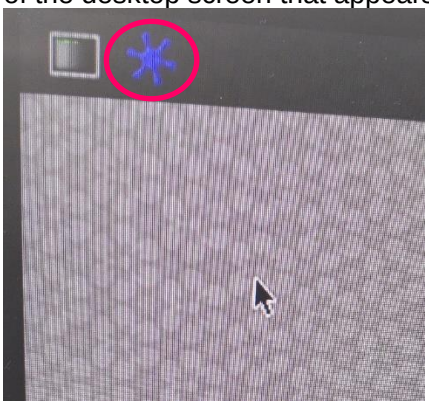
Change SW1 on the module to select micro SD card slot (SW1-1 ON, SW1-2 ON):

Please insert the micro SD card in the SOM module slot.

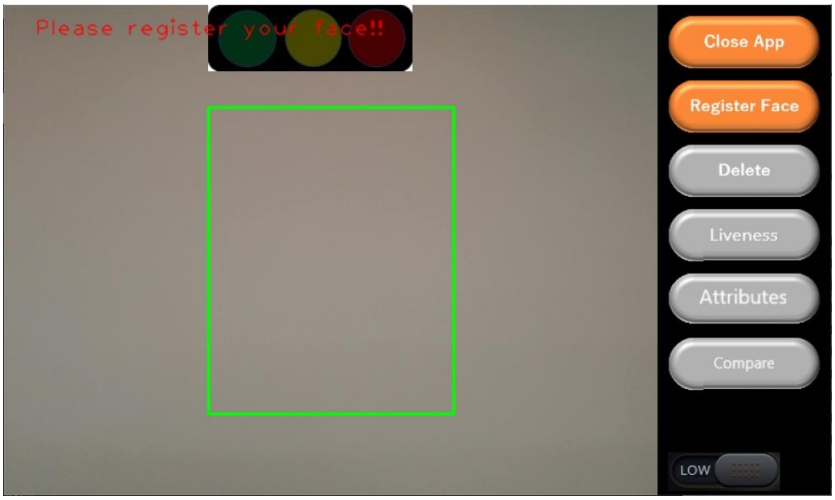


⑦ Turn on the RZ/V2L EVK and confirm that it can start up.

⑧ Click with the mouse on the second blue icon from the left that appears in the upper left corner of the desktop screen that appears.



⑨ After that, confirm that the following demonstration screen is displayed.

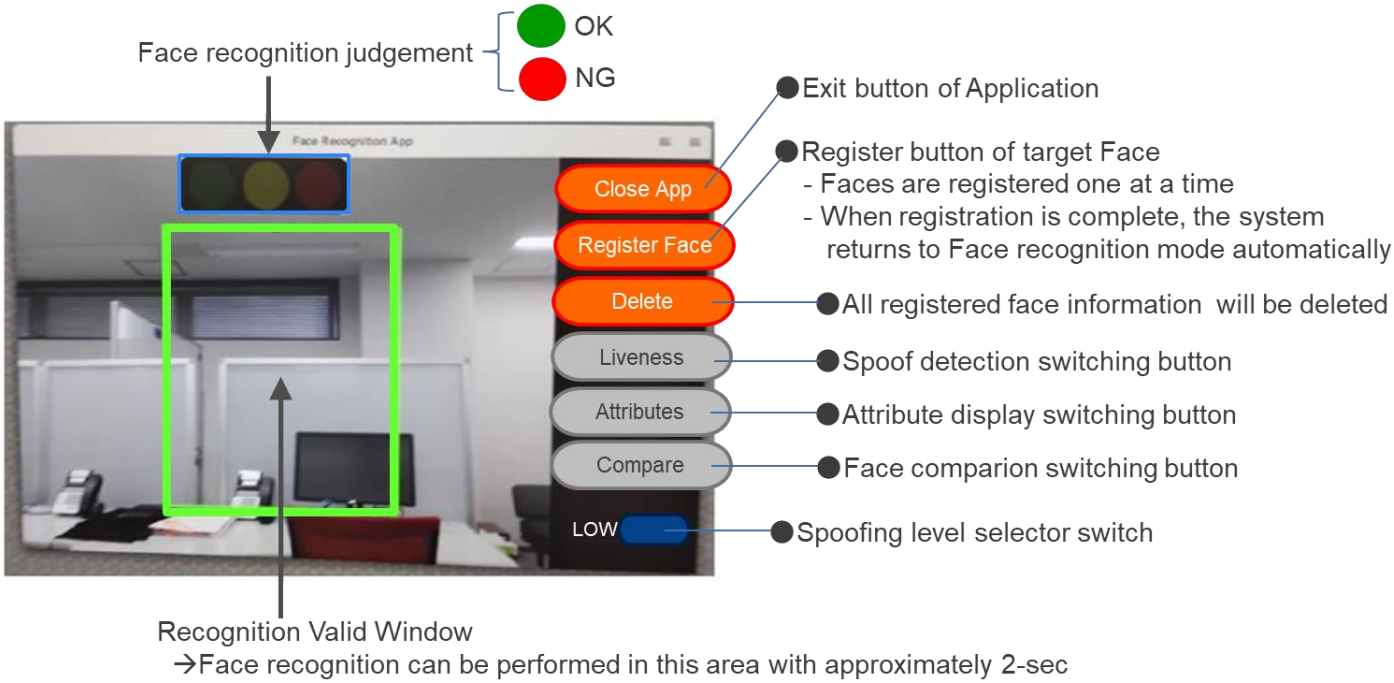


When the above screen appears, setup is complete.

How to operate the demo application with the SDK is explained in the next section.

6. Operational guide of Face recognition demo application

6.1 Explanation of UI



① Authentication Area

This is the area where face recognition is enabled.

If the face is projected for about 2 seconds so that it fits in this area, face recognition can be performed.

② Exit button

Click this button to exit the application.

③ Face registration button

Click this button to enter the face registration mode.

When one face is registered, the application returns to the face recognition mode.

④ Erase button

Clicking this button deletes all registered faces.

⑤ Spoofing detection on/off button

Clicking this button toggles the spoofing detection on and off.

When on, the button turns orange.

⑥ Organ point display on/off button

Clicking this button toggles the organ point display on and off.

When on, the button turns orange.

⑦ Authentication judgment signal

Blue lights up when the face is successfully authenticated.

Red lights up if the face is not authenticated.

⑧ Face comparison on button

When clicked, the screen for measuring the similarity of two faces will be displayed.

⑨ Spoofing level switch button

Toggles the level of spoofing criteria.

When set to HIGH, the spoofing criteria become more stringent.

6.2 How to launch the application

Click the right side of the icon displayed in the upper left corner of the desktop screen (red frame in the figure below) to start the application.

It takes a few seconds to launch the application, so please wait a moment after clicking the icon.

6.3 Authentication Procedure

① Click the Face Registration button.

② Project the face you wish to register so that it fits into the authentication area.

The facial features will be registered in the database.

③ Project the face so that it fits into the authentication area and keep it there for about 2 seconds.

④ When the blue light of the authentication judgment signal turns on, the authentication is successful. If the face is not authenticated, the red light turns on.

If you wish to authenticate again, once again, do not project your face into the authentication area, wait about 2 seconds in that state, and then perform step ② again.

6.4 Authentication screen

If the detected face does not fit in the authentication area, the color of the rectangle will be gray.

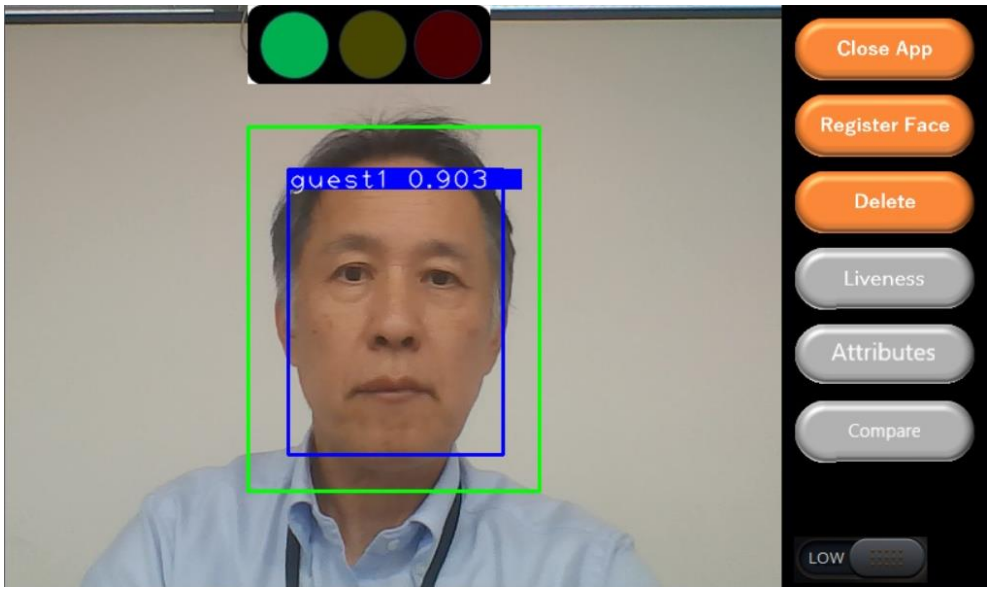
If the detected face is within the authentication area and is being authenticated, the color of the rectangle will change according to the similarity as follows.

- When the similarity is less than 0.2 : Gray
- When the similarity is between 0.2 and 0.5* : Red
- When the similarity is greater than 0.5* : Blue

* The color of the color changes depending on the set authentication thresholds.

The values shown are the default values for the thresholds.

During authentication, the similarity is displayed above the face rectangle (see figure below).

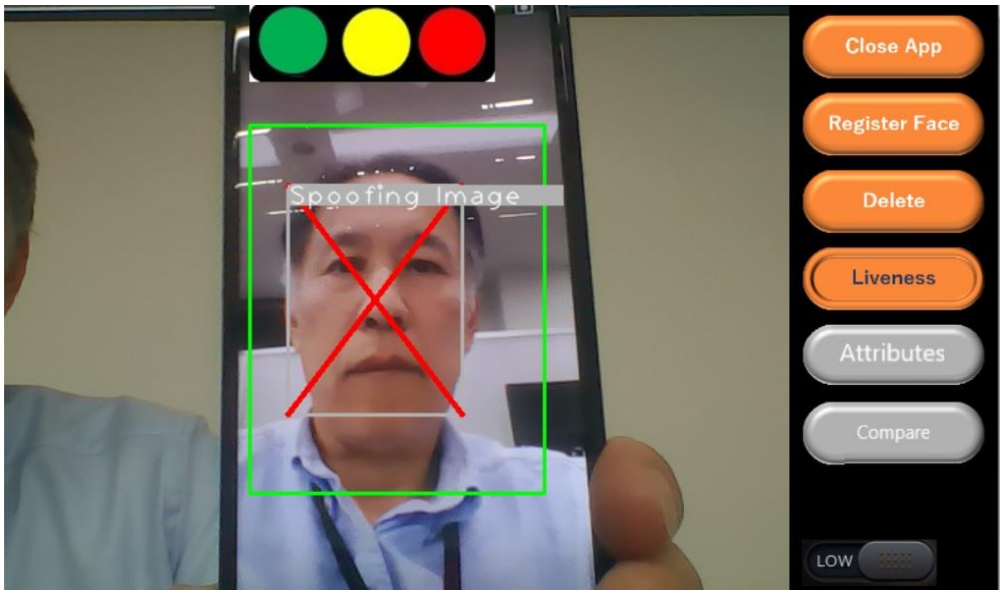


6.5 Authentication Screen with Spoofing Detection On

When the Spoofing On/Off button (“Liveness” button) is turned ON, spoofing detection is enabled.

When spoofing detection is enabled, if a face is projected into the authentication area, spoofing detection will be performed before authentication.

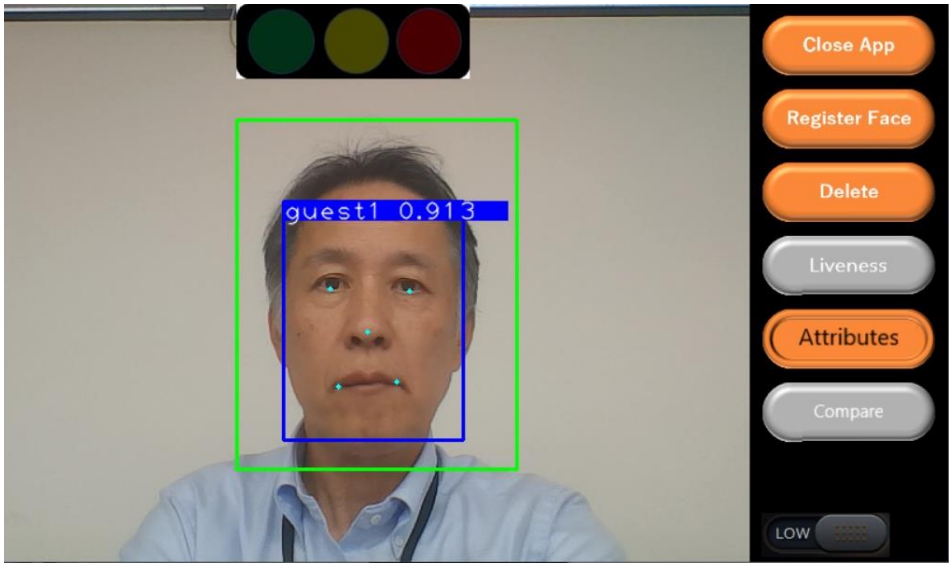
The spoofing detection process will run for a few seconds, and if the result is determined to be spoofing, the screen will look like the one below.



If the spoofing detection is passed, the authentication result will be displayed as described above.

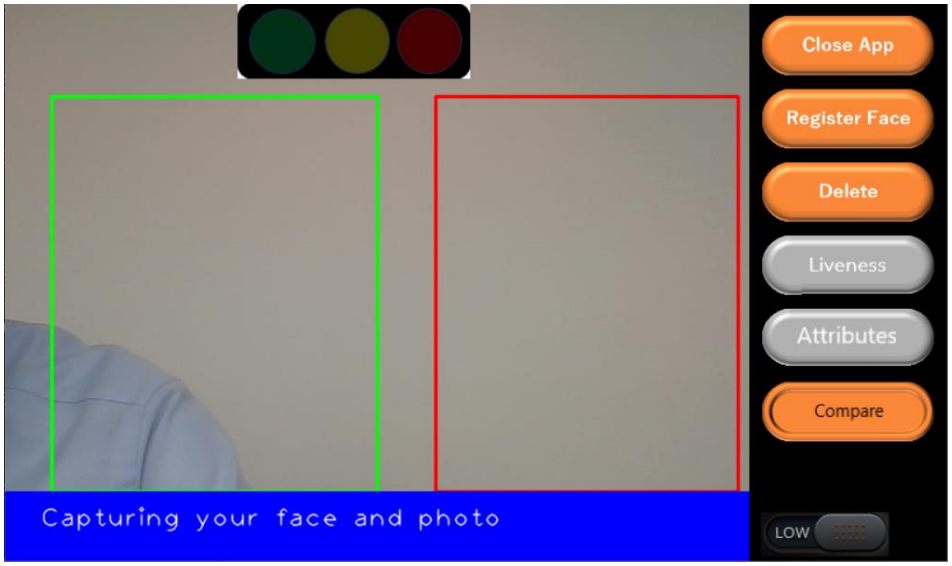
6.6 Screenshot with organ point display on

Clicking on the “Attribute” button will display the positions of the eyes, nose, and mouth as dots, as shown in the following screen.



6.7 Screen when face comparison is on

When you click on the Face Comparison button (“Compare” button), a green frame and a red frame will appear, as shown in the following screen. Here you can measure the similarity between two faces.



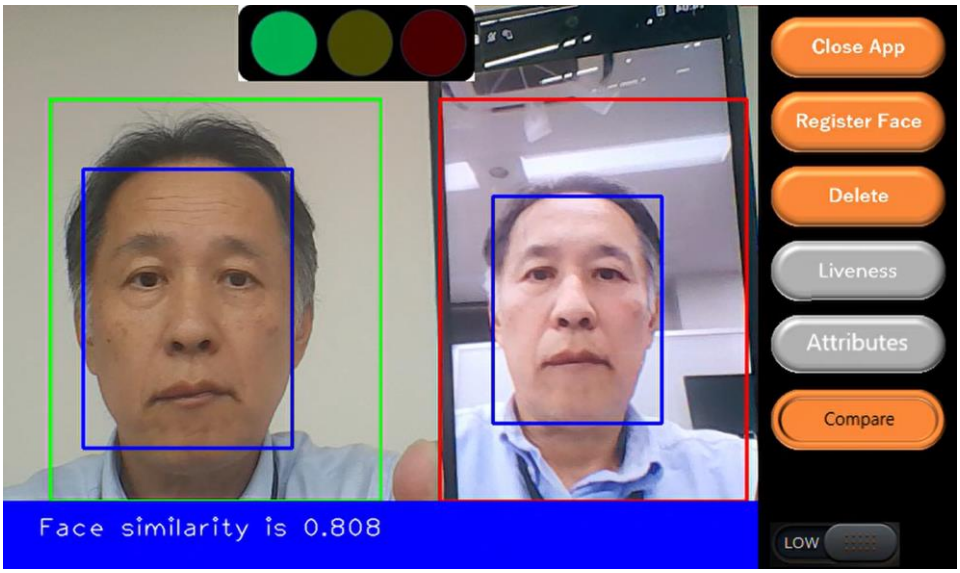
Display the face images to be compared in the respective frames.

Once a face is detected, the similarity of the faces is measured and the results are displayed.

The similarity is displayed as a numerical value at the bottom of the screen as shown below.
The closer the value is to 1.0, the more similar two faces are.

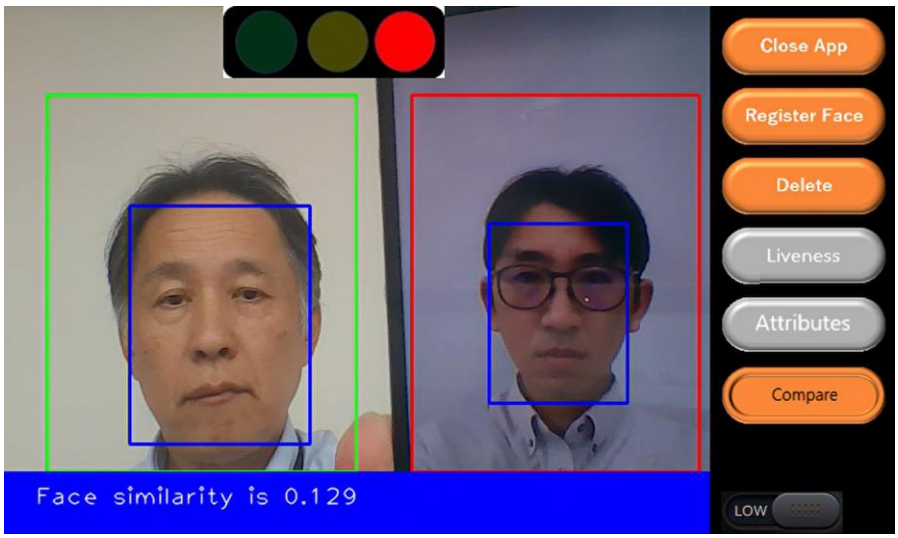
If the similarity is 0.5 or higher, it is displayed as a green light, as shown in the following screen.

Translated with www.DeepL.com/Translator (free version)



If the similarity is less than 0.4 to 0.5, a yellow light is displayed.

If the similarity is less than 0.4, a red light is displayed as shown in the following screen.



When face comparison is finished, face comparison is automatically turned off.

These are the instructions for the Face Recognition Demo Application Operation Guide.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Oct.28.24	-	First release

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan

www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.