Facial Recognition User Manual

Murugappan Mahalingam
Application Analyst (E3)
12/1/22

Contents

Overview

The Face authentication application uses image pre-processing, anti-spoofing checking and System-on-a-chip matrix acceleration engine embedded to extract the face features of the user. These face features are then stored during enrolment of a new user or compared during authentication to determine whether the user is valid.

Application Architecture

Facial Enrolment Application (FEA)

Facial Enrolment, runs neural network algorithm and stores encrypted faceprints on database. A faceprint is a set number of points which is represented as mathematical transformation of the user's face. saves encrypted facial features to local database (ADM_FACEPRINTS.tbl). Stored encrypted faceprints are matched with enrolled faceprints later during authentication. For best performance, enrol under normal lighting conditions and look directly at the device. During the enrolment process, device will send a status hint in green (successful) or in red (unsuccessful) to the call-back provided by application.

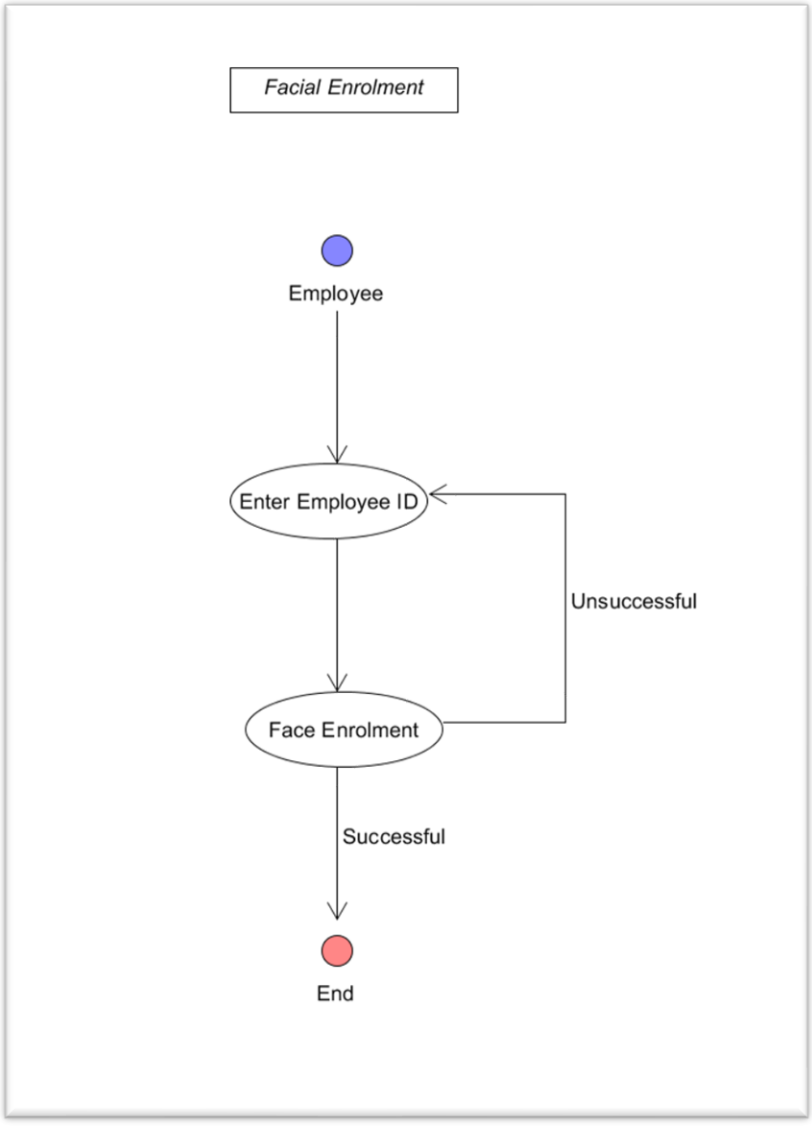


Figure 1: Facial Enrolment Flow Diagram

Facial Authentication Application (FAA)

For every authentication attempt, runs neural network algorithm, generates faceprints and compares them to all enrolled faceprints in database. Finally, returns whether the authentication was forbidden or allowed with enrolled user id. During the authentication process, device will send a status hint in green (successful) or in red (unsuccessful) to the call-back provided by application.

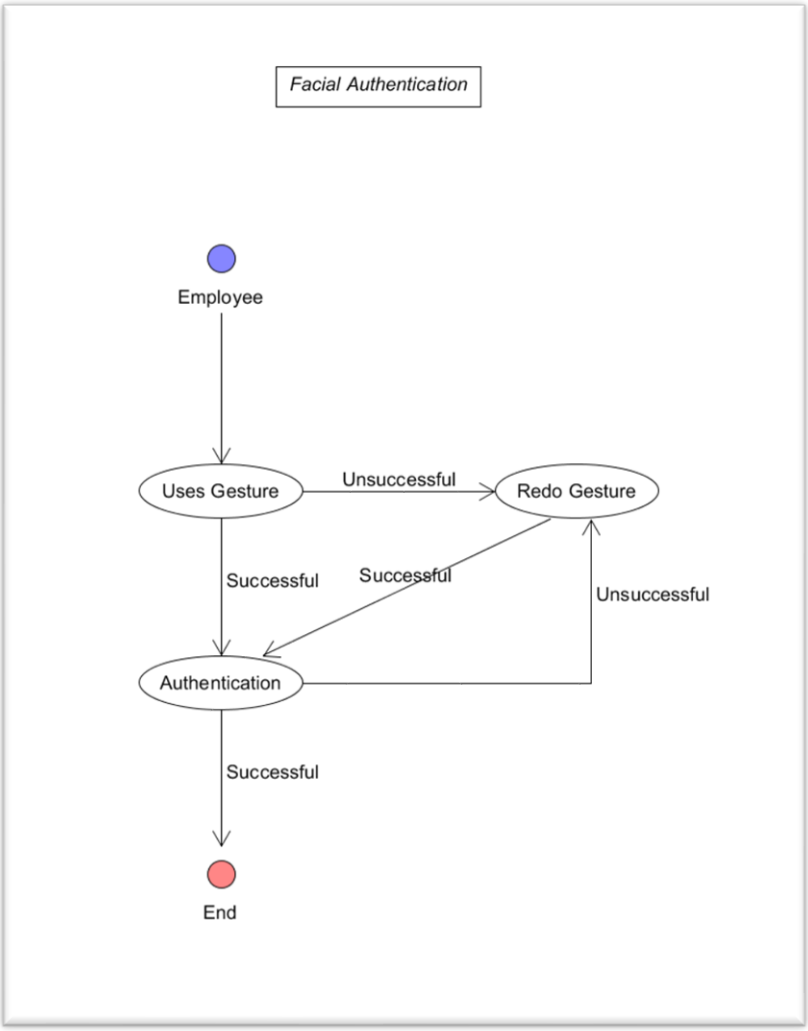


Figure 2: Facial Authentication Flow Diagram

Setting up the F455/F450 Camera [Firmware Update]

Note: This only has to be done once and it can be done in one computer.

Step 1:

Install rsid_sdk_v0.25.0_signed_win64 found in the camera_update folder.

Step 2:

Open Command prompt, plug in the camera and run the following.

Step 3:

Update firmware to version 3.1.0.29 first with the following command:

rsid-fw-update.exe --file <bin path> [--port <COM#>] [--force-version] [--force-full] [--interactive / --auto-approve]

Command Example:

rsid-fw-update.exe --file "C:\Git_Projects\projects\ ENVIS_Facial \camera_update\F450_3.1.0.29_SKU1_SIGNED.bin" --port COM5 --force-version

Note: Do not run the update via the realsense application as it may fail since this is a forced update. Please use the cmd

Note: Typically, the ports are either COM3 or COM5, check by opening up the Realsense ID viewer application and clicking on the Log tab

Step 4:

Update firmware to version 4.3.0.8200 first with the following command:

rsid-fw-update.exe --file <bin path> [--port <COM#>] [--force-version] [--force-full] [--interactive / --auto-approve]

Command Example:

rsid-fw-update.exe --file "C:\Git_Projects\projects\ENVIS_facial\ camera_update \F450_4.3.0.8200_SKU1_SIGNED.bin" --port COM5 --force-version

Note: Do not run the update via the realsense application as it may fail since this is a forced update. Please use the cmd

Note: Typically, the ports are either COM3 or COM5, check by opening up the Realsense ID viewer application and clicking on the Log tab

Setting up the Database (ailanthus)

Step 1:

Open database folder from SSMS

Step 2:

Make sure Ailanthus Database Exists in the database

Step 3:

Run the query set in adm_faceprint.sql

Setting up the Application

Step 1:

Open facial_authentication package.

Step 2:

Run Installation.bat

Step 3:

Start PSMS

Step 4:

Run enrolment.bat to see if it works

Note: Command prompt will show the error. The error is usually an instruction to rectify the issue.

Step 5:

Close enrolment.bat

Step 6:

Run authentication.bat to see if it works.

Note: it will fail to open if there are no facial prints in the database.

Note: Command prompt will show the error. The error is usually an instruction to rectify the issue.

Step 7:

Close authentication.bat

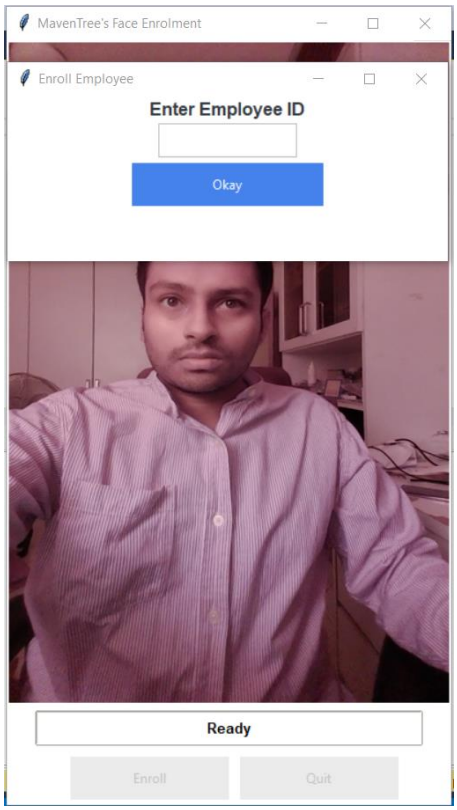
Using the Enrolment.bat

Step 1:

Double Click Enrolment.bat

Step 2:

A command prompt and Camera GUI will appear.



Step 3:

Enter Employee ID and pose for the camera.

Note: This only needs to be done once per employee.

Step 4:

When Successful, a green message will appear and the transaction can be seen in the database table created (adm_faceprint).

Step 5:

Close the application

Note: Enrolment and authentication cannot be run at the same time. The camera can only work one application at a time.

.

Using the Authentication.bat

Step 1:

Double Click Authentication.bat

Step 2:

Upon connecting to the server, the camera application and command prompt will open up.

Step 3:

Open up ETC. [http://localhost:8080/psms/mcs/ETC.xhtml?mode=facial]

Step 4:

Use Gestures to begin/trigger authentication.

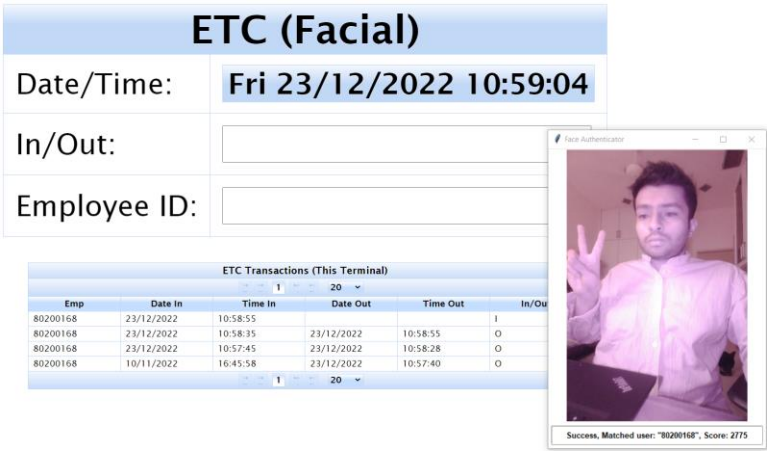
Point Index finger up to trigger IN

V-Sign to trigger OUT

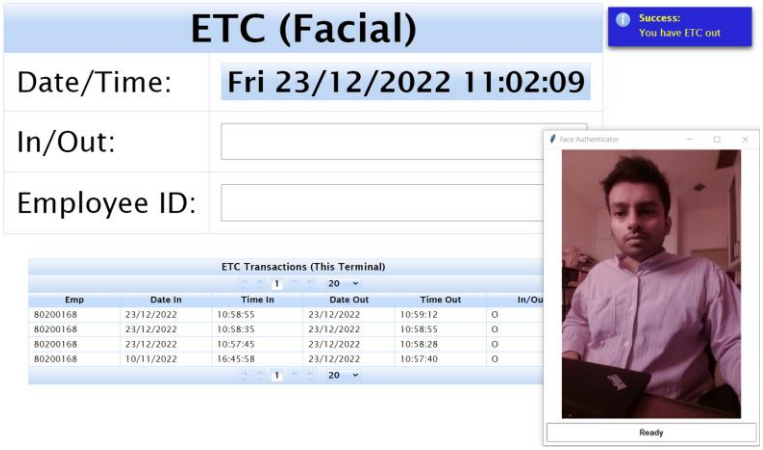
Note: Both left or right hands can be used for triggering authentication

Step 5:

Upon successful triggers, authentication will begin. When Authentication is successful, employee id and match confidence score will appear in the GUI.



Followed by the transactions in ETC.



Troubleshooting

Scenario 1: What to do when authentication works on the GUI but nothing appears on ETC?

Refresh the ETC Page and you will see this (Active clients connection: 1) in the command prompt. This means the connection has been established between the etc and application.

←[35;1m[2022-12-2 10:06:21,753] [Thread-8] [socket_handler.py :0126] [DEBUG] Checking client heartbeat...←[0m

←[35;1m[2022-12-2 10:06:21,756] [Thread-1] [socket_handler.py :0131] [DEBUG] Sending PING to [6727a391-0967-40ca-af37-d15cb7516ee5] ←[0m

←[1;36m[2022-12-2 10:06:21,759] [Thread-1] [socket_handler.py :0140] [INFO] Active clients connection: 1←[0m

Scenario 2: What to do the application is not connected to the server?

Open environment_config.ini file in the facial_authentication folder. Change the ACTIVE_ENV to whichever server you are using.

Then restart the application.

Example: ACTIVE_ENV=local to ACTIVE_ENV=dev

```
[INIT]
ACTIVE_ENV=local

;Step 2: Configure the different environment settings below
; Follow the format of the following [SampleConfig] section below to declare the specific environment configurations
;[SampleConfig]
;database.dbname=unitTest
;database.user=root
;database.password=

[local]
restapi.GET_FACEPRINT_URL=http://localhost:8080/ailanthus/faceprint/get-faceprints-json
restapi.ADD_FACEPRINT_URL=http://localhost:8080/ailanthus/faceprint/add-faceprints-json
restapi.PING_URL=http://localhost:8080/ailanthus/faceprint/ping
authentication.some_value=1234

[dev]
restapi.GET_FACEPRINT_URL=http://titan-dev:8080/ailanthus/faceprint/get-faceprints-json
restapi.ADD_FACEPRINT_URL=http://titan-dev:8080/ailanthus/faceprint/add-faceprints-json
restapi.PING_URL=http://titan-dev:8080/ailanthus/faceprint/ping
authentication.some_value=1234

[qas]
restapi.GET_FACEPRINT_URL=http://titan-qas:8080/ailanthus/faceprint/get-faceprints-json
restapi.ADD_FACEPRINT_URL=http://titan-qas:8080/ailanthus/faceprint/add-faceprints-json
restapi.PING_URL=http://titan-qas:8080/ailanthus/faceprint/ping
authentication.some_value=8000

[app]
restapi.GET_FACEPRINT_URL=http://titan-app:8080/ailanthus/faceprint/get-faceprints-json
restapi.ADD_FACEPRINT_URL=http://titan-app:8080/ailanthus/faceprint/add-faceprints-json
restapi.PING_URL=http://titan-app:8080/ailanthus/faceprint/ping
authentication.some_value=6666

[station_1]
GET_FACEPRINT_URL=http://localhost:8080/hello
ADD_FACEPRINT_URL=http://localhost:8080/world
PING_URL=http://localhost:8080/hi

[station_2]
GET_FACEPRINT_URL=http://localhost:8080/goodbye
ADD_FACEPRINT_URL=http://localhost:8080/world
PING_URL=http://localhost:8080/bye
```