FACEIO's LIVENESS DETECETION ML MODEL

PixLab | symisc systems

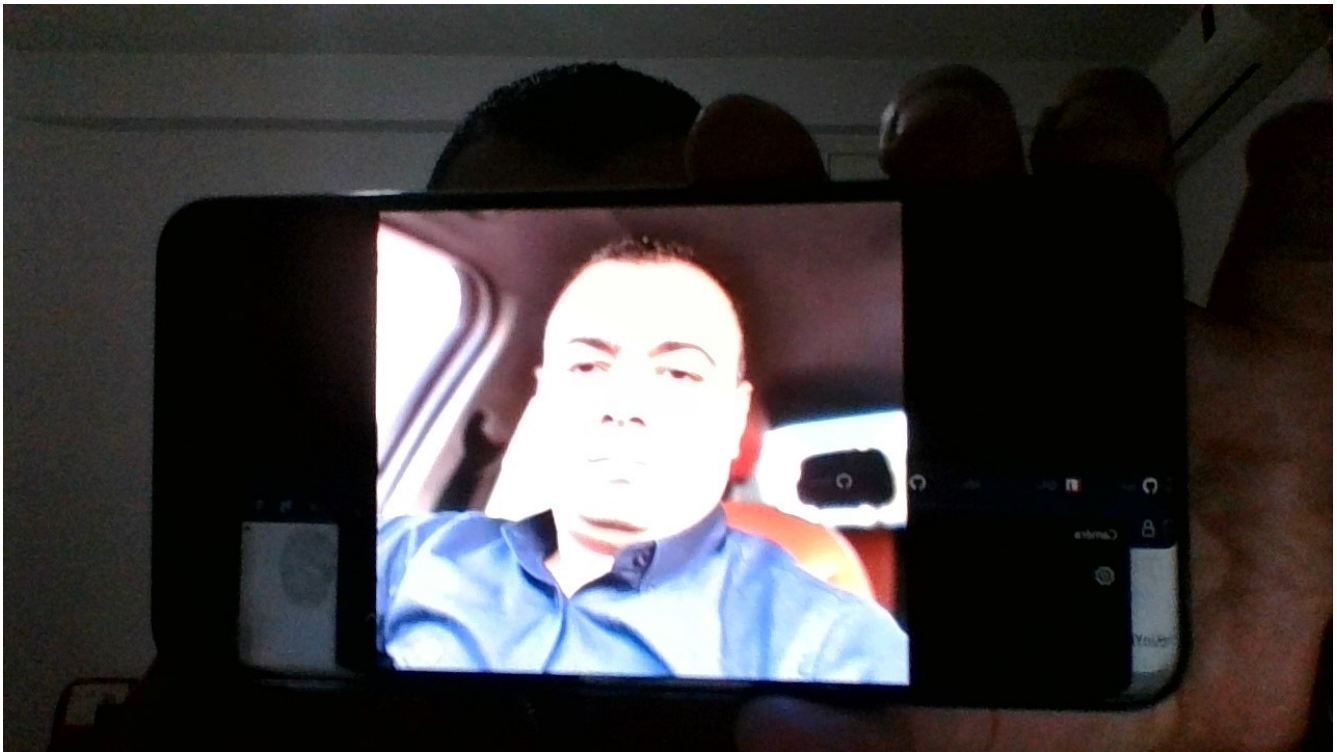
FACEIO

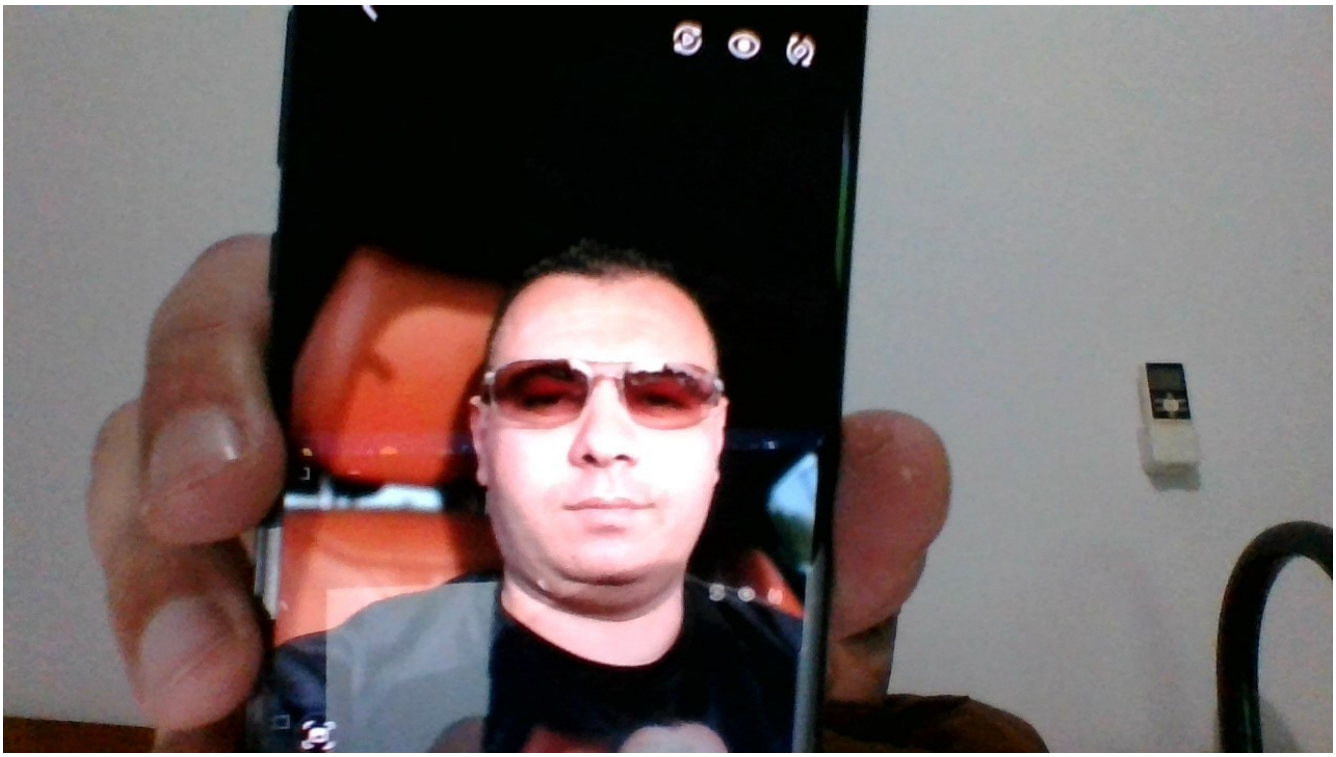
Customer ID: 1357669C

Liveness detection in biometrics is the ability of a system to detect if the target face is real from a live person present at the point of capture or fake from a spoof artifact or lifeless body part.

PixLab's Liveness detection implementation uses Machine Learning approach that analyze face images - after they are collected from the input camera stream whether during Authentication or Enrollment - to verify if the source is coming from a fake representation.

***Example of Spoof ATTACKS deterred by our ML model*:**





Enabling Liveness Detection on your FACEIO Application

Please note that Liveness detection is a resource intensive operation, therefore it is available on the ENTERPRISE PLANS, and up. To activate this feature, please follow these straightforward steps:

1. **Connect to your account via the FACEIO Console first.**
2. From the console main view, visit the *Application Manager* .
3. **Select the target application for which you want to enable Liveness Detection for.**
4. Navigate to the **SECURITY** tab from the manager main view.
5. Once the target application selected. **Activate** the ***Perform Liveness Detection During Authentication & Enrollment*** security option as shown below.:

6. You're all set. Upon a new user enroll or authenticate on your application, the Liveness detection engine shall be triggered to filter out spoof & presentation

attacks. Upon an attack is detected, the `fioErrCode.PAD_ATTACK` error code is raised, and you should act accordingly such as **banning this user** depending on your policy.