Press Release – 08/25/2023

Contact Information
Symisc Systems
https://symisc.net
https://pixlab.io
https://faceio.net
Vincent Garnier
contact@symisc.net
Mrad Chams
chm@symisc.net
PixLab Support
support@pixlab.io
FACEIO Support
support@faceio.net
PixLab Privacy Officer
privacy@pixlab.io

PixLab Unveils Cutting-Edge Deep-Fake Detection & Presentation Attacks Prevention SDK for Biometrics Authentication Applications

PixLab, **a leading provider of advanced image and video analysis solutions, is thrilled to announce the integration of its state-of-the-art Deep-Fake detection & Presentation Attacks Prevention newest Machine Learning based, Software Development Kit (SDK) into the FACEIO facial authentication, biometric web framework.**

This groundbreaking Deep-Fake detection model is set to redefine the standards of online security and authentication.

Deep fake have indeed emerged as significant challenges in the realm of biometric authentication.

To address this, FACEIO has pioneered a **Liveness detection system (documented here)** capable of identifying deep fake videos through smartphone or laptop detection mechanisms. For a more in-depth understanding, including visual examples of attempted spoofs, you can explore our detailed announcement here.

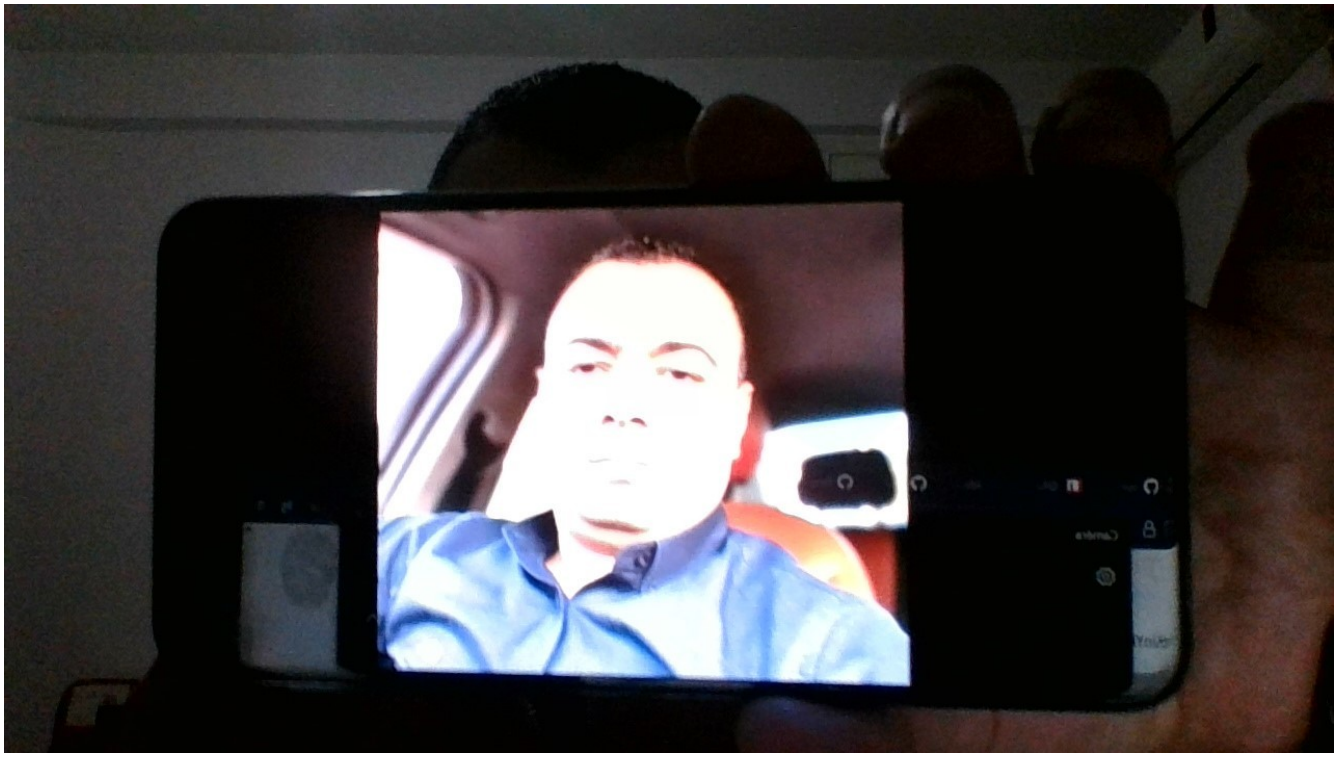
Our Face Anti-Spoofing feature, designed to combat Smartphone & Print Attacks from static images or video streams, require **only a single frame to operate**, and is available starting from the Business Plan tier.

Once activated, you can manage the *Face Anti-Spoofing Security Option* directly from the *Application Manager*'s Security Tab within the FACEIO Console.

Key Highlights:

- **Advanced Machine Learning**: PixLab's newly developed model employs sophisticated machine learning algorithms to scrutinize facial images, ensuring genuine user authentication and warding off potential spoof attacks.
- **Exclusive Availability**: Recognizing the premium value of this advanced security feature, PixLab has made it exclusively available starting from the Business Plan tier on FACEIO. Interested users can explore the pricing details and benefits at FACEIO Pricing.
- **User-Centric Approach**: The system is designed with user convenience in mind. Once activated, the Face Anti-Spoof engine autonomously screens out deep fake and presentation attacks, ensuring a seamless and secure user experience.
- **Single Frame, Passive Anti-Spoof Detection**: FACEIO's integration goes beyond active checks. **The SDK require only a single frame to operate, with no action on the user side unlike the previous implementation.**

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



When activated, **this feature is engineered to counteract Smartphone & Print Attacks originating from static visuals or video feeds with the `fioErrCode.PAD_ATTACK` error code being raised to your application if such attacks are detected**.

That is, the system will ensure that is presented with a **live (real) person** during each authentication or enrollment operation. This is to effectively **thwart presentation attacks, commonly referred to as Deep-Fakes or Face Spoofing attempts**. In biometrics, liveness detection determines whether the presented face is genuine and from a live individual at the capture point, or a counterfeit from a deceptive artifact or non-living body part.

Enabling Deep-Fake & Face Spoofing Prevention On Your FACEIO Application

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 Deep-Fake Prevention for.**
4. Navigate to the **SECURITY** tab from the manager main view.
5. Once the target application selected. **Activate** the ***Protect Against Deep-Fakes & Face Spoof Attempts*** security option as shown below.:

6. You're all set. Upon a new user enroll or authenticate on your application, the deep-fake prevention engine shall be triggered to filter out spoof & presentation attacks. Upon an attack is detected, the `fioErrCode.PAD_ATTACK` error error code is raised, and you should act accordingly such as banning this user depending on your policy**.**

A Word from PixLab: "We recognize the evolving challenges in the digital landscape, especially with the rise of deep fakes and sophisticated spoofing techniques. Our primary goal with this integration is to provide our users with an unmatched level of security without compromising on user experience. We're confident that this enhancement to FACEIO will set a new benchmark in biometric authentication," said *Mrad Chams*, CTO, PixLab.

About PixLab: PixLab is at the forefront of biometric technology, dedicated to providing innovative solutions for a digital age. With a commitment to excellence and user security, PixLab continues to push the boundaries of what's possible in online authentication.

For media inquiries, please contact: *Vincent Garnier,* Community Manager, Email: [contact@pixlab.io]