Apple In My Eyes (AIME): Liveness Detection for Mobile Security Using Corneal Specular Reflections

Muhammad Mohzary[1] Khalid J Almalki[1] Baek-Young Choi[1] Sejun Song[1]
[1]School of Computing and Engineering, University of Missouri - Kansas City, MO, USA
Emails: [1]{kjaf3f, mm3qz, choiby, songsej}@umsystem.edu

***Abstract*—In this paper, we present a novel *software-based* face Presentation Attack Detection (PAD) method named "Apple in My Eyes (AIME)" using screen display as a challenge and corneal specular reflections as a response for authenticating the liveness against presentation. To detect face liveness, AIME creates multiple image patterns on the authentication screen as a challenge, then captures meaningful corneal specular reflection responses from user's eyes using the front camera, and analyzes the reflective pattern images using various lightweight Machine Learning (ML) techniques under a subsecond level delay (200 ms). We demonstrate that AIME can detect various attacks, including digital images displayed on the phone or tablet, printed paper images, 2D paper masks, videos, 3D silicon masks, and 3D facial models using VR. AIME liveness detection can be applied for various contactless biometric authentication accurately and efficiently without any costly extra sensors.**

***Index Terms*—Presentation Attack Detection, Liveness Detection, Anti-spoofing.**

I. Introduction

Biometric features such as fingerprint, face, iris, hand geometry, voice, and gait, have become increasingly popular in many mobile security applications for the automated recognition and authentication of individuals. Due to the recent global pandemic caused by COVID-19, the quest for touchless and non-invasive physiological biometric authentication methods such as facial recognition grows swiftly. However, vulnerability to Presentation Attacks (PA) (a.k.a spoofing) poses a significant hurdle to its usability, security, and privacy. The liveness detection against spoofed artifacts (e.g., photos, videos, or masks) is one of the most challenging tasks as it cannot conclusively assess the physical presence in unsupervised environments. Although several methods have been proposed for tackling PA with motion challenges and 3D mapping [1], most of them require expensive depth sensors (e.g., iPhone Face ID) and fail to detect replaying and sophisticated 3D reconstruction attacks. Furthermore, as the quality of PA instruments (e.g., hyper-realistic masks, 3D reconstruction, and printing technologies) improves and the difficulty (in time, expertise, equipment, cost) of generating PAs decreases, achieving reliable PA Detection (PAD) with the existing method alone remains challenging. In this paper, we present a novel *software-based* face PAD approach named "Apple in My Eyes (AIME)" using screen display as a challenge and corneal specular reflections for authenticating the liveness against presentation. As illustrated in Figure 1 (a), when a user attempts to authenticate, AIME creates multiple image patterns on the authentication screen in different frequencies and sequences as a challenge and captures meaningful corneal specular reflection responses from user's eyes using the front camera. We design and develop various lightweight Machine Learning (ML) techniques to identify reflective patterns and perform authentication, including eye image acquisition, reflection image augmentation, super-resolution, and feature extraction. We also create two ML datasets, including facial data for identity verification and corneal reflection data for learning liveness authentication. We compose them in a lightweight ML package to achieve under a subsecond level delay (200 ms) for the entire task. We have implemented AIME in Android, iOS, and web apps to be used as a complementary liveness detection module for multi-factor contactless biometric authentication. We have conducted experiments on various devices by collecting over a thousand eye and corneal reflection images under different conditions, including daylight, dark, indoor, outdoor wearing glasses, and gaits (laying, sitting, walking, and standing). We demonstrate that AIME can detect various attacks, including digital images displayed on the phone, printed paper images, 2D paper masks, videos, 3D silicon masks, and 3D facial models using VR. The experimental results in accuracy and performance show that AIME is effective and efficient in detecting the liveness against sophisticated PAs.

II. AIME Architecture

The principal objective of AIME is to detect a presented face's liveness by challenging and sensing the reflective corneal patterns. AIME consists of Challenge and Collection (CC), Pattern Detection (PD), Feature Extraction (FE), and Data Training (DT), as illustrated in Figure 1. The CC module in Figure 1 (a) consists of challenge and face detection functions. CC is responsible for displaying a sequence of image patterns on the screen as challenges and capturing a facial image using the front camera. The facial recognition system uses the captured facial image for identity verification. The PD module consists of Facial Landmark Detection (FLD), Reflection Localization (RL), and Super-Resolution (SR), as illustrated in Figure 1 (b). PD is responsible for extracting reflective pattern images from the detected facial landmark (eyes) and generating high-resolution reflection images. FLD function in AIME is accountable for detecting right and left eyes from facial images. RL is responsible for locating the reflection images from the extracted eye images. We use

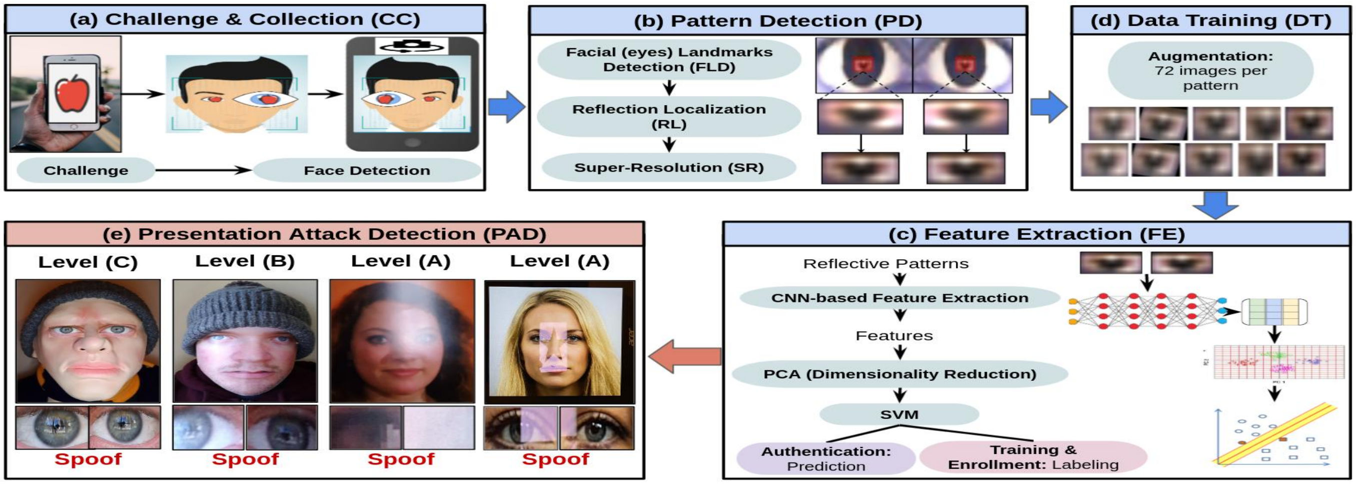
(a) Challenge & Collection (CC)
Challenge
Face Detection
(b) Pattern Detection (PD)
Facial (eyes) Landmarks Detection (FLD)
Reflection Localization (RL)
Super-Resolution (SR)
(d) Data Training (DT)
Augmentation: 72 images per pattern
(c) Feature Extraction (FE)
Reflective Patterns
CNN-based Feature Extraction
Features
PCA (Dimensionality Reduction)
SVM
Authentication: Prediction
Training & Enrollment: Labeling
(e) Presentation Attack Detection (PAD)
Level (C)
Level (B)
Level (A)
Level (A)
Spoof
Spoof
Spoof
Spoof

Fig. 1. The Block-diagram of AIME Presentation Attack Detection Method.

manual annotation software called VGG Image Annotator (VIA) to annotate corneal reflection in eye reflection images. Then, we train a MobileNetV2 model to perform this task. After we extract the reflective pattern from eye images, we use Super-Resolution Convolutional Neural Network (SRCNN) to recover HR corneal images from LR images and enhance their perceptual quality to recognize small reflective pattern regions. The FE module in Figure 1 (c) consists of CNN-based Feature Extraction (CNN-FE), Principal Component Analysis (PCA), and Support Vector Machine (SVM) models. FE module is responsible for learning a new set of deep learning features from reflective pattern images using a pre-trained VGG-16 model. CNN-FE returns the last max-pooling layer's output (layer-13) by removing the final three fully connected layers from VGG-16. Then, FE reduces the dimensionality of the extracted features into a lower-dimensional space using PCA. It is also responsible for labeling the classification model at the training and enrollment stages and making predictions for authentication. We use the SVM model with Radial Basis Function (RBF) kernel to classify the lower-dimensional features obtained from PCA. The DT module in Figure 1 (d) is accountable for creating patterns, augmenting reflection images in different reflective conditions, and generating datasets. We have collected eye reflection images from diverse environments, including daylight, darkness, indoor, outdoor, wearing glasses, and various postures (lying, sitting, walking, and standing). We have used the AIME app to collect facial images using different types of challenge patterns of shapes, letters, numbers, and colors. We have built a dataset of 1,300 eye reflection images for training the reflection location learning. We have created a dataset of 1080 reflection pattern images for the initial training by augmenting 72 images from every 15 patterns for classification in the Support Vector Machine (SVM) model.

III. Evaluations

We carried out extensive experiments using AIME implementation in Android, iOS, and web applications to evaluate AIME's performance and accuracy under real-world scenarios. Following the Fast Identity Online (FIDO) alliance [2] recommendations, we evaluate all three Presentation Attack Instruments (PAI) categories, including level A (immediate), level B (moderate), and level C (difficult) attacks. We prepare videos and digital images displayed on tablet, printed paper images, 2D paper masks, 3D silicon masks, and 3D facial models using VR. Figure 1 (e) shows that AIME can detect level A, B, and C attacks with realistic silicone masks with covered eyes.

IV. Conclusions

AIME is the first PAD using human corneal reflection as a challenge-response for mobile device security to the best of our knowledge. We designed and built multiple Machine Learning (ML) functions to identify reflective patterns and perform authentication, including eye image acquisition, reflection image augmentation, super-resolution, feature extraction, and classification. We have built a lightweight ML package for Android, iOS, and web applications. AIME can be used either as a stand-alone human liveness detection app or for various mobile and IoT device apps as a complementary software solution for touchless biometric systems. We have demonstrated that AIME provides an accurate and efficient PAD using only a front-facing camera, without using any infrared or depth sensors through extensive experiments under diverse conditions.

References

[1] B. M. Chrzan, "Liveness detection for face recognition," *Master's thesis*, 2014.

[2] S. Schuckers, G. Cannon, E. Tabassi, M. Karlsson, and E. Newton, "Fido biometrics requirements," *Population*, vol. 5, pp. 2–1, 2019.