Institute of Cyber Security for Society (iCSS)

ADAPTING TO MOVEMENT PATTERNS FOR FACE RECOGNITION ON MOBILE DEVICES

Matthew Boakes (M.J.Boakes@kent.ac.uk), Richard Guest (R.M.Guest@kent.ac.uk), Farzin Deravi (F.Deravi@kent.ac.uk)

University of Kent

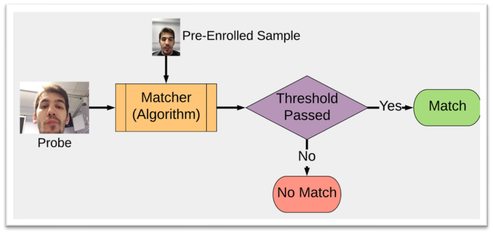
Introduction

- The continued increasing use of biometrics as a method of authentication is said to be on track to authenticate the vast majority of payments within the next ten years.
- This increase can be attributed to biometric authentication in mobile and smartphone devices, providing greater consumer access to the technology.
- Static biometric systems, such as eGates, can create a suitable environment for optimal operation and rely on a fixed decision threshold.
- However, we can not make the same environmental and operational scenario guarantees for mobile devices suggesting a more adaptive approach is required.

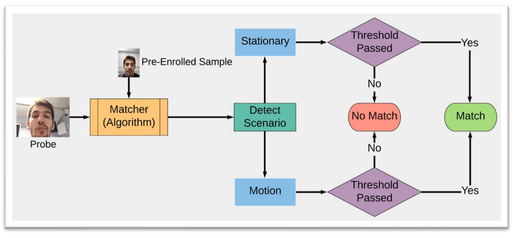
The Adaptive Decision Threshold

To solve this problem, we created the adaptive decision threshold whereby the system can dynamically alter the match score (similarity or dissimilarity) required based on the scenario.

Traditional



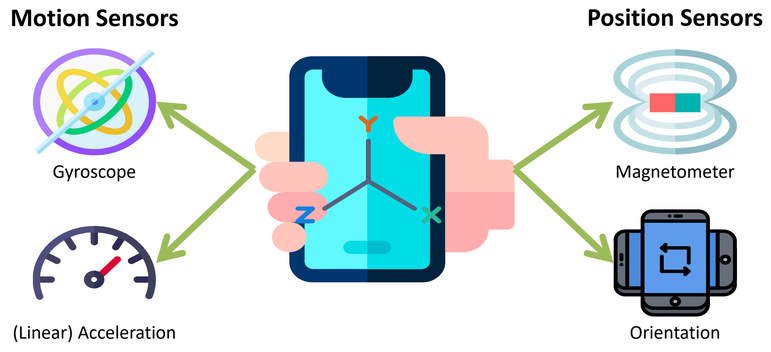
Adaptive



https://research.kent.ac.uk/cyber/

School of Engineering, University of Kent, Canterbury, Kent CT2 7NT, UK.

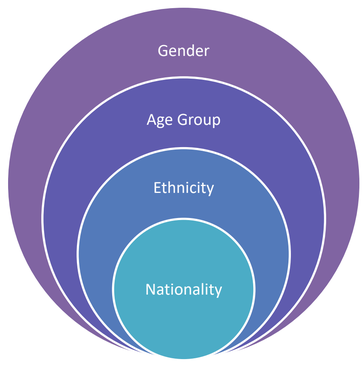
Automatic Scenario Detection



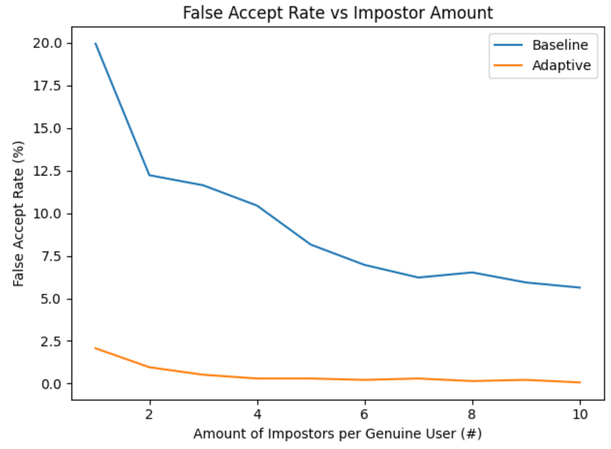
To create our scenario classifier for automatic scenario detection, we used two motion-based and two position-based sensors found within smartphone devices and a face quality metric score. We found that kNN had the highest accuracy when differentiating between scenarios.

Accuracy	Stationary vs Motion	Four Scenarios	Stationary	Motion
Cross-Val (F1-score)	0.99 (±0.01)	0.97 (±0.01)	0.98 (±0.01)	0.97 (±0.01)
Training	1.00	0.99	0.99	0.99
Testing	0.99	0.97	0.97	0.99

Tailored Impostors



To test the most out of the concept, we used a novel approach involving "tailored" impostors to select the most challenging group of impostors for testing based on demographic attributes. In other words, by testing against people who would appear most similar to the genuine user(s).



When testing the novel approach, we were able to achieve better results than using a static threshold (baseline) against the most "tailored" impostor(s). We trialled the biometric system offline against the "face_recognition" python library with data collected from smartphone devices.

Conclusions

- Presented a proof-of-concept for a novel adaptive approach to biometric authentication for a mobile device
- Proposed the creation of an extendable 'Adaptive Framework' altering the decision threshold based on the scenario
- Utilised smartphone sensors to create a scenario classifier
- **97%** testing accuracy for our four simple scenarios
- Showcased a method for choosing 'Tailored' Impostors for stress testing the approach using worst-case impostor data
- Demonstrated the proposal's potential merit, using data collected from a commercial device and an open-source face recognition algorithm
- Demonstrated the proposal's potential merit, using data collected from a commercial device and an open-source face recognition algorithm