Multimodal Biometrics in Consumer Mobile Device: a Step Toward IoT Security

Karthik Karunanithi
California State University, Fullerton
karthikknidhi@csu.fullerton.edu

Yu Liu
California State University, Fullerton
liuyuxisu@csu.fullerton.edu

Daniel Kim
California State University, Fullerton
dan.kim@csu.fullerton.edu

Jacob Biloki
California State University, Fullerton
jbiloki@csu.fullerton.edu

Reliable user authentication is a standing challenge in mobile device and IoT security, and biometrics is often perceived as a promising solution. The goal of our project is to deliver the benefits of multimodal biometrics, or identifying users based on multiple biometric traits (e.g, face and ear, face and fingerprint) simultaneously, to consumer mobile devices and to IoT platforms.

We see multimodal biometrics as a financially sustainable approach that implements secure authentication in IoT technologies. This is because multimodal biometrics can significantly increase security without significantly increasing device manufacturing costs or requiring additional hardware; most mobile and many IoT devices already integrate cameras and fingerprint sensors for acquiring different types of biometrics such as faces, fingerprints, ears. Our project provides the missing piece: a viable approach for consolidating the biometric data acquirable with these existing sensors in order to increase the overall recognition accuracy of the system.

Multimodal biometric systems are more secure than the state-of-the-art mobile/IoT biometric systems based on a single biometric modality. This is because a multimodal system challenges attackers to spoof multiple biometric traits in order to bypass authentication, which is significantly more challenging than spoofing a single trait. Further, if the identifying information in one biometric modality is distorted by uncontrolled conditions (e.g., a face image where the visibility of the face features is poor due to dim lighting) a multimodal system can compensate for that lack of information by using identifying information from other modalities.

We have explored techniques for implementing a multimodal biometric system based on face, fingerprint, and ear on a mobile device (i.e., Samsung Galaxy S7 phone) and then extending it to IoT platforms. We choose these biometrics because they can be readily acquired using the existing mobile camera and fingerprint scanner technologies available on many mobile and IoT devices. We then statistically combined features from these biometric modalities in ways in which maximizes recognition accuracy in uncontrolled conditions in which mobile and IoT devices typically operate (e.g., poorly lit settings and dirty fingers, which can degrade the recognition accuracy).

Our algorithm works as follows: first we extract the Linear Binary Pattern (LBP) and Histogram of Oriented Gradients (HOG) features from the face, fingerprint, and ear biometrics. We then concatenate the extracted sets of features and apply Principal Component Analysis (PCA) in order to reduce the size of the combined features to scale it to the mobile/IoT devices' memory. Finally, we apply different classifiers including Supporting Vector Machines (SVMs), Neural Networks, and Hidden Markov models in order to classify the featureset as belonging to

a particular user. The performance of the different classifiers is compared under different conditions including poor lighting of face images, varying angles of the fingerprint images, and angles at which the ear image is taken. Different classifiers may perform best in different conditions, which is a phenomenon we are planning to investigate.

Our current preliminary success rate is 94.36% and 97% for face and fingerprint recognition, respectively under controlled conditions. This evaluation was conducted on the Face94 database and the Indian Institute of Technology Rural Fingerprint Database. However, biometrics recognition faces serious challenges is real-life situations. The facial recognition on dataset we collected under uncontrolled environment (including lighting, camera angles and facial emotion variations) on Samsung Galaxy S5 is only 73%. Similar unsatisfactory results were achieved when tested on dataset we collected using Futronic F588H fingerprint scanner. These results clearly reveal the deficiencies of single-biometric systems and are a strong motivator for the multimodal approach.

Our next step is to construct a database of face, fingerprint, and ear images captured using a mobile/IoT device in uncontrolled conditions and to evaluate our three-biometric scheme using this data. The goal of the evaluation is to ensure that our multimodal scheme yields recognition accuracy of at least 5% over the face-only, fingerprint-only, and ear-only single-biometric schemes as well as over the two-biometric face-fingerprint, face-ear, and fingerprint-ear schemes.

We are hoping that our results will show that multimodal biometrics, although ready for integration with mobile devices and IoT, is an underused method which facilitates sustainable development of mobile and IoT security.