The UNIVERSITY of OKLAHOMA
Gallogly College of Engineering
School of Computer Science

A Biometric Solution to Common Issues with Multi-Factor Authentication

Matt Kish, Cole Dalton, Chris Dalton, Blake Reynolds
CS4173 Fall 2023

Abstract

Abstract—In an era characterized by the ubiquitous presence of digital systems and networks, ensuring the security of user data and access is paramount. Multi-Factor Authentication (MFA) has become a pivotal safeguard, demanding multiple forms of user verification for access. Nonetheless, MFA deployment confronts a multitude of complex issues, spanning from user resistance and compatibility challenges to sophisticated phishing attacks and biometric vulnerabilities.

This project presents a rigorous exploration of an innovative solution to the multifarious challenges surrounding MFA. Our research endeavors to not only explain the primary causes of these issues but also to propose unique practical strategies that improve MFA's efficacy and user acceptance. These efforts aim to bolster digital security both at the organizational and individual levels.

This research approach leverages comprehensive literature reviews, empirical studies, and meticulous analyses of real-world MFA deployments. These methodologies provide an in-depth understanding of issues with MFA's and enable the formulation of mitigation strategies. A central tenet of this work underscores the imperative of educating and raising awareness among users, an element considered pivotal in catalyzing MFA adoption and diminishing security risks. give this more character.

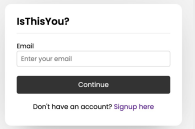
Index Terms—MFA, Multi-Factor Authentication, Biometrics, Security

Technical Details

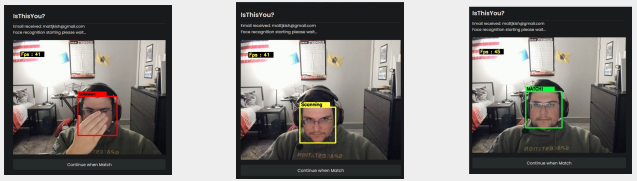
- Project addresses the need for robust MFA due to traditional authentication vulnerabilities.
- Combines facial recognition and signature comparison for enhanced security and user-friendly access.
- Core components: registration page for enrollment, login page for biometric authentication, success/failure feedback.
- preprocess.py captures and organizes facial images for user-specific recognition reference.
- webdeploy.py performs live facial authentication, matching real-time - images with stored references.
- Signature.py compares signature images using OpenCV, identifying similarities with a threshold of 130.
- Workflow: user registration, preprocessing of biometric data, login with facial and signature authentication.
- Outcome determines success/failure pages, guiding users accordingly.

Signature Comparison

Login Page



Process of the Facial Recognition



No Match | Scanning | Match

Experimental Implementation

- Development focus on Biometric Multi-Factor Authentication (MFA) system integrating facial recognition and signature comparison.
- Use of HTML-based interfaces supported by Python scripts, OpenCV libraries for facial recognition, and signature analysis.
- Utilization of SQL Azure Database for centralized storage of user registration data and biometric references.
- Methodology involves seamless registration, live facial recognition, and signature comparison during authentication.
- Specific performance metrics for facial recognition and signature comparison evaluation.
- Integration with SQL Azure ensures system robustness, scalability, and data security.
- Workflow covers user enrollment, real-time authentication, and feedback mechanisms.
- Targeting high accuracy rates (>90%), low processing times (<2 seconds), and minimal error rates (<5%) for system effectiveness.

Future Work

- Liveness detection and 3D face mapping for live face authentication
- Introduction of an account lockout feature after failed login attempts to mitigate brute-force attacks
- Integration of images directly into the SQL Azure Database for storage efficiency
- Unified signup page for streamlined user enrollment: name, email, facial recognition, and signature fields in a single HTML page
- Minimization of images captured during preprocessing while maintaining accuracy for reduced user effort
- Expansion of MFA capabilities to mobile applications for facial and signature recognition
- Improvement of accuracy over time by accepting the correct face after a set number of successful matches
- Commitment to continual innovation for a more secure, efficient, and user-friendly authentication system
- Future exploration in multimodal biometrics:
  - Advanced fusion techniques integrating diverse biometric modalities
  - Refinement of anti-spoofing measures to counter emerging security threats in multimodal biometric authentication

Conclusion

By implementing the use of two biometrics, our group has made a project that is extremely secure. Combining a physical biometric with a behavioral biometric makes it to where the user has to be identified by traits that are unique to that user. A facial recognition identifies the user by comparing the stored images to find a user that looks like the user trying to sign in. Once it finds a match, it will then move onto the signature to get the behavioral biometric. Since a signature is unique to a specific person, this makes it a good identifier to see if the user is who they say they are. Although our project is still not perfect and has some work to fix, instead of using a password, our project pairs facial recognition with a signature which makes it extremely secure in identifying and verifying that user.