Biometric Authentication: Applications, Advantages, and Obstacles

California State University, Long Beach

CECS 378: Introduction to Computer Security Principles

Semester Project

11/17/2024

Abstract

Utilizing distinct physiological and behavioral characteristics to confirm user identities, biometric authentication has become an essential security feature in contemporary digital contexts. In contrast to conventional techniques like passwords or PINs, which are vulnerable to loss, theft, or abuse, biometrics offer a more dependable and convenient means of authentication. This study examines several biometric methods, such as vein scanning, facial recognition, and fingerprint recognition, highlighting how well they may improve security. Furthermore, the incorporation of biometrics into secure access control, financial systems, and mobile devices has greatly strengthened defenses against unwanted access. However, issues with data security, privacy, and the possibility of biometric spoofing make further research and development necessary. This research seeks to provide a thorough overview of biometric authentication's contribution to enhancing cybersecurity by analyzing existing developments and constraints and pointing out opportunities for further innovation.

Introduction

Strong authentication procedures are now more important than ever to guard against cyberattacks and illegal access due to the quick expansion of cloud computing, mobile apps, and internet services. Because of their susceptibility to brute-force, phishing, and hacker assaults, traditional authentication techniques like passwords and PINs are becoming less and less effective. Because of these drawbacks, people are looking for safer and easier-to-use substitutes, and biometric authentication is one promising option. To confirm a person's identification, biometric authentication uses distinctive physiological and behavioral traits like voice patterns, iris structures, face features, and fingerprints. Because biometric characteristics are intrinsically linked to the person, they are more secure and challenging to duplicate than standard credentials, which are susceptible to loss, theft, or sharing. The deployment of biometric systems is not without difficulties, nevertheless, despite its benefits. The dependability

of the technology is called into question by issues with privacy, data security, and the possibility of biometric spoofing, in which hackers try to mimic a user's biometric characteristic. In order to guard against abuse and guarantee user confidence, concerns about the handling and preservation of private biometric information must also be addressed. This paper explores the different forms, advantages, and disadvantages of biometric authentication as it is today. The paper attempts to give a thorough examination of how biometrics might enhance cybersecurity while also addressing the obstacles that need to be removed for broad adoption by examining current developments and practical applications.

Methodologies

Fingerprints are one of the first things that we can think of while talking about biometric authentication. In “Design and Implementation of Identity Authentication System Based on Fingerprint Recognition and Cryptography”, by fusing cryptography with fingerprint recognition, Feng Fujun and his colleague are able to design and implement the identity authentication system with a dual-layer security method (Feng et al., 2016). Three main goals guided the system's design: strong security, good dependability, and user-friendliness. C++ is the main programming language used in the software environment, which uses Visual Studio 2010 for development, Microsoft SQL Server 2008 for the database, and the Biokey SDK for integrating fingerprint functionalities. The URU4000B fingerprint scanner, renowned for its dependability in biometric authentication systems, is the hardware component that this component depends on. Basic user data, including username, password, email address, and phone number, are gathered during the system's registration procedure. Next, the user's fingerprint data is captured using a scanner. To improve security, all user information, including passwords, is encrypted using the MD5 hashing technique. The user inputs their username and password at the start of the authentication process, which is hashed using MD5 and compared to the database's stored hash. Once the password has been verified, the system moves on to fingerprint verification, which verifies the user's identification by comparing recently taken fingerprint data with

templates that have been recorded. According to performance evaluations, user convenience is ensured by the registration procedure taking about 10 seconds and the login process taking 15 seconds. False Rejection Rate (FRR) and False Acceptance Rate (FAR) were used to gauge reliability, and tests were run on both registered and unregistered users. A low FRR and zero FAR were shown in the results, demonstrating strong system reliability. By combining biometric verification with conventional credentials, a dual authentication technique greatly improves user authentication security while preserving an intuitive user interface.

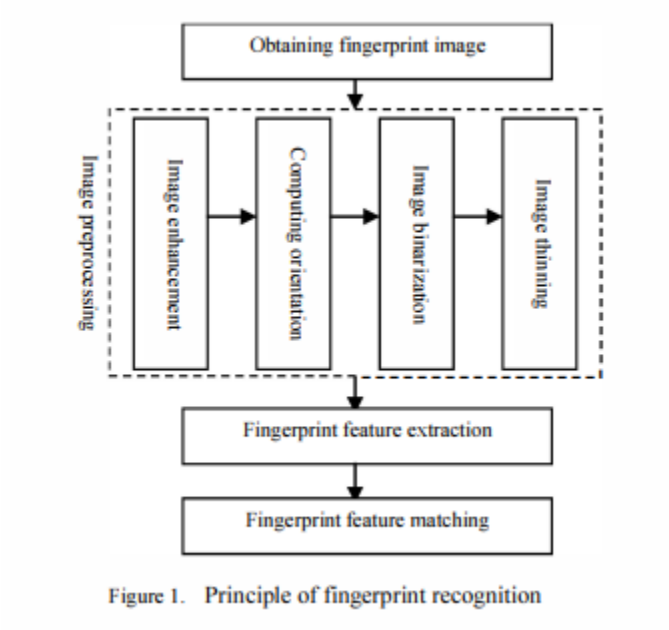


Figure 1. Principle of fingerprint recognition

Field	Type	Length	Remark
NAME#	Char	20	Name(key)
ID	Char	20	password
PHONENUM	Char	11	Telephone number
Email	Char	40	Email address
Fingerprint	text	20	Fingerprint template

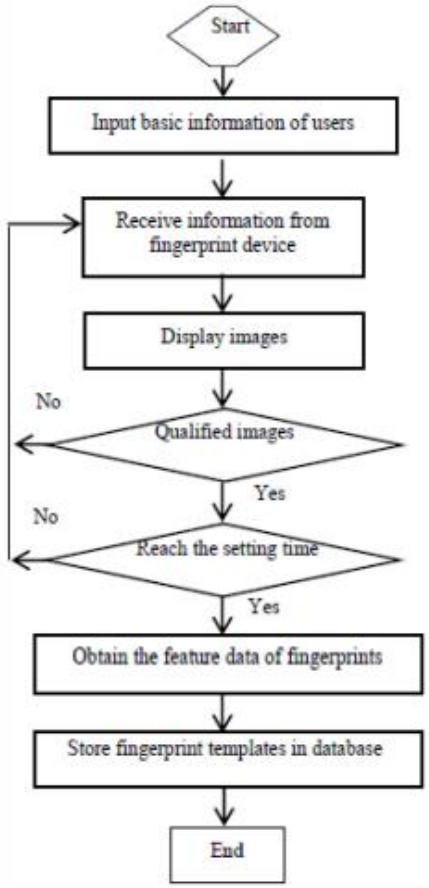


Figure 2. Procession of user register.

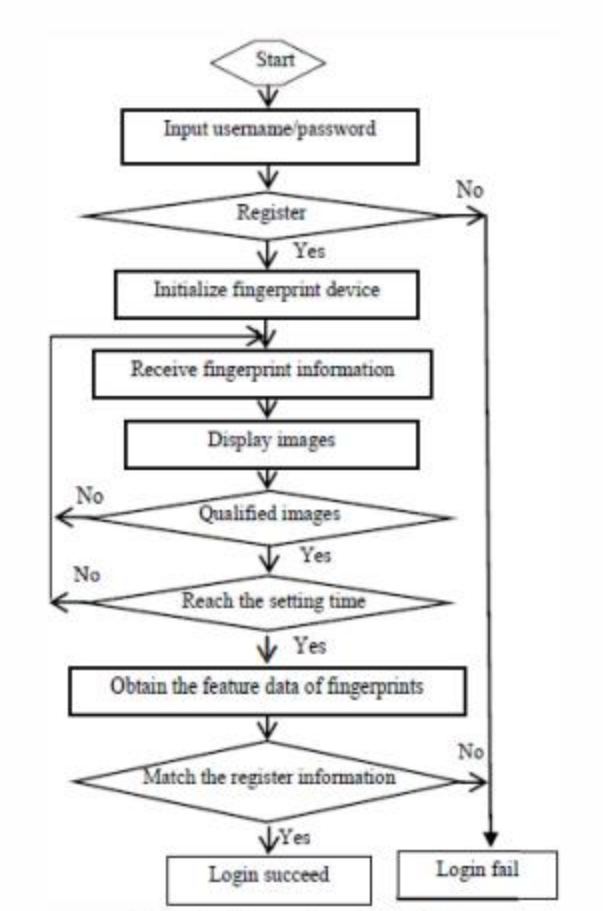


Figure 3. Procession of user login.

Even though fingerprints are used very popular these days, facial recognition is also another option that is widely used and more secure. In the "Personal based authentication by face recognition", Yung-Wei Kai and his team represent a Personal-Based Authentication System (PBAS) that integrates facial recognition with password validation to improve security and precision (Yung-Wei et al., 2008). Conventional facial recognition systems are susceptible to spoofing; however, PBAS mitigates this risk by incorporating passwords into the recognition procedure. This method entails sustaining a database that associates user faces with their passwords, which refines probable matches by excluding irrelevant candidates based on the input password, thereby enhancing the precision of

facial recognition. The technology utilizes Principal Component Analysis (PCA) to extract facial traits and map them into a "face space" for comparison. By minimizing the number of possible matches through password input, PBAS markedly improves the recognition rate. Experiments done on a proprietary facial database and a subset of the FERET database revealed that the integrated system surpassed conventional face-only approaches. For example, using five training photos, the recognition rate improved from 74.5% to 98.5% when passwords were employed, demonstrating the system's efficacy in integrating biometric and password authentication for enhanced security.

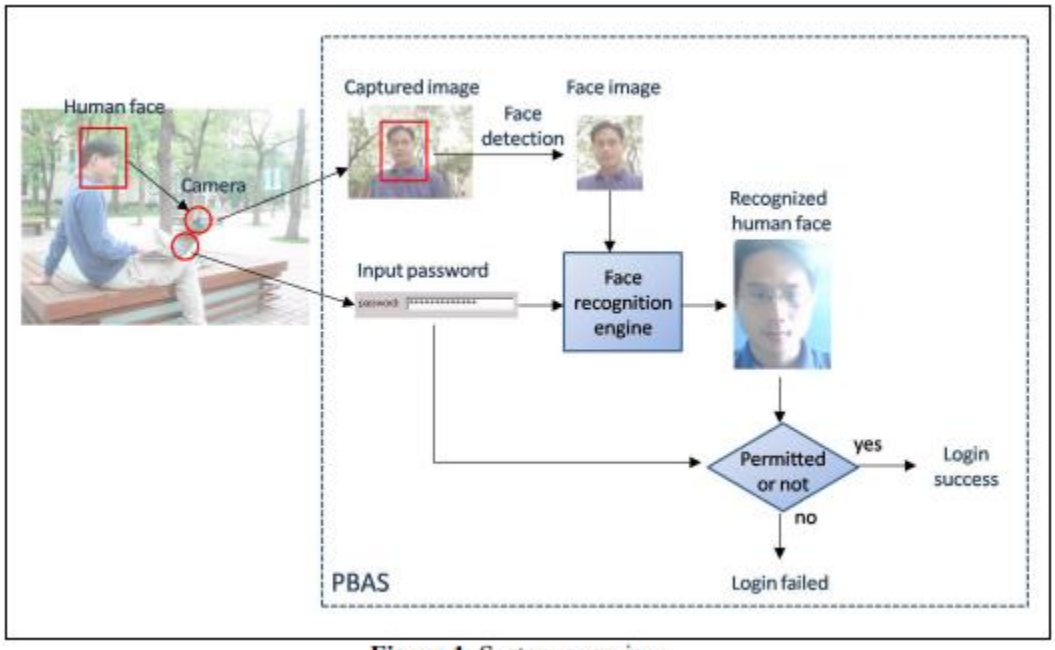


Figure 1. System overview

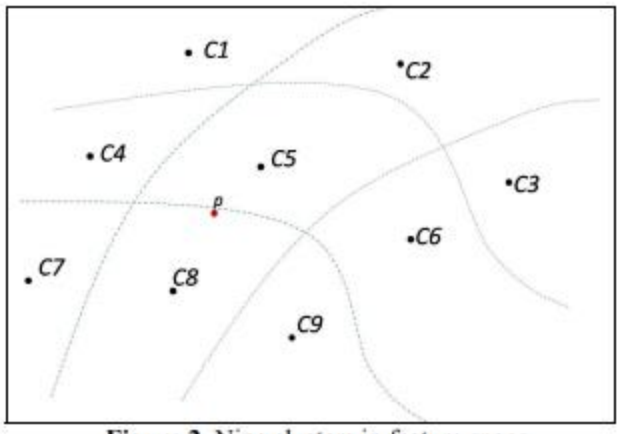


Figure 2. Nine clusters in feature space

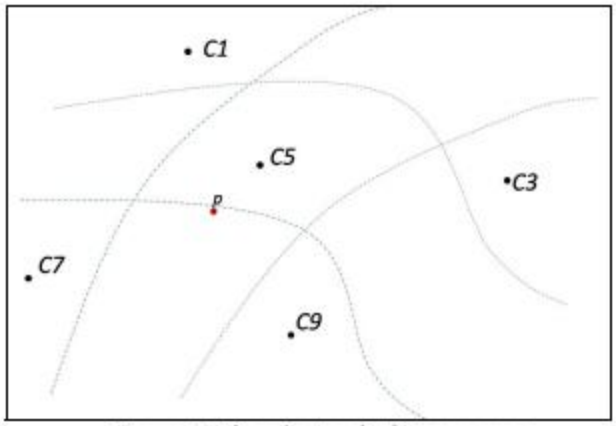


Figure 3. Five clusters in feature space

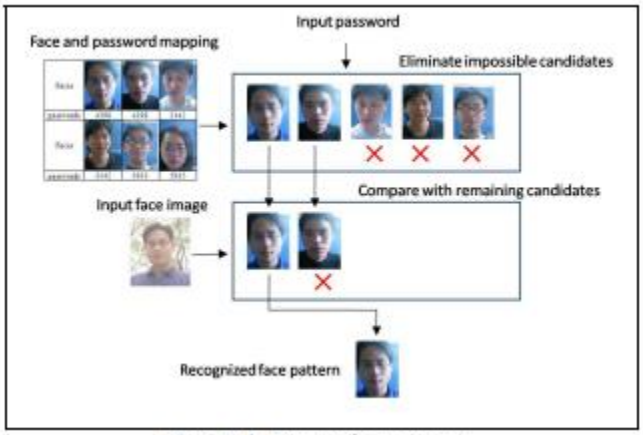


Figure 4. Integration process

Finally, one of the most advanced biometric authentications is using hand vein patterns. In the “Biometric Authentication System Using Dorsal Hand Vein Pattern”,

Anisha and her colleagues introduce a biometric authentication method utilizing the dorsal hand vein pattern for secure user identification (Anisha et al., 2020). The suggested technique employs a NoIR camera and a matrix of near-infrared (NIR) LEDs to capture vein patterns, which are distinctive and consistent across time. The system is constructed using a Raspberry Pi and utilizes OpenCV for image processing. The process entails acquiring a hand vein image by NIR imaging, which accentuates veins owing to the absorption characteristics of hemoglobin. The obtained image is subjected to pre-processing to improve quality, subsequently followed by feature extraction with a template matching method. This method contrasts the retrieved vein pattern with saved templates for user verification. The technology employs a contactless way to overcome the limitations of traditional biometric techniques, such as fingerprints or retinal scans, which can be affected by ambient conditions or human discomfort. The trials illustrate that this system offers a dependable and effective approach for secure authentication, particularly in scenarios where conventional biometric methods are inadequate.

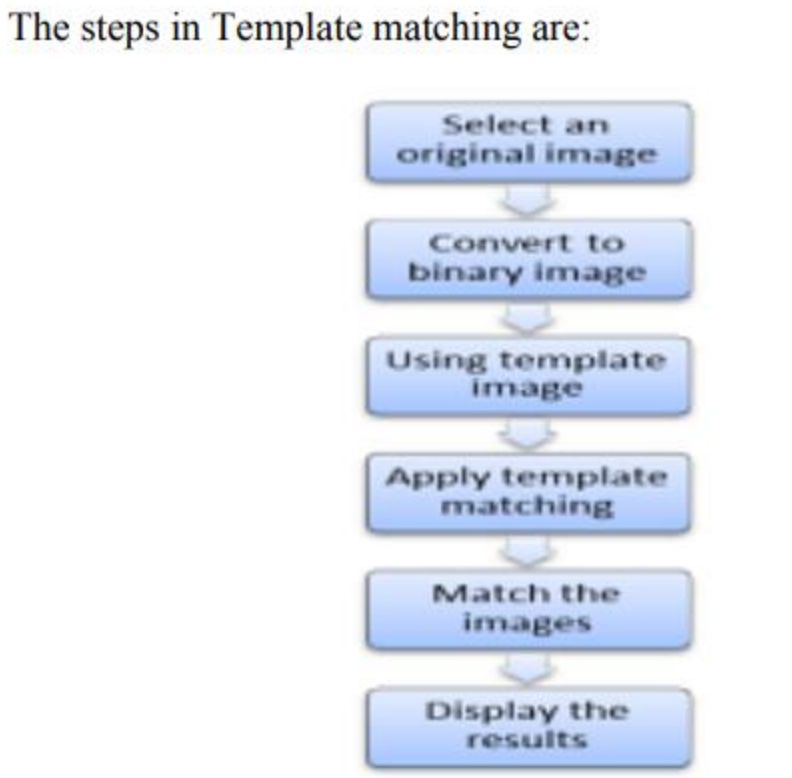


Fig. 1: Steps involved in template matching

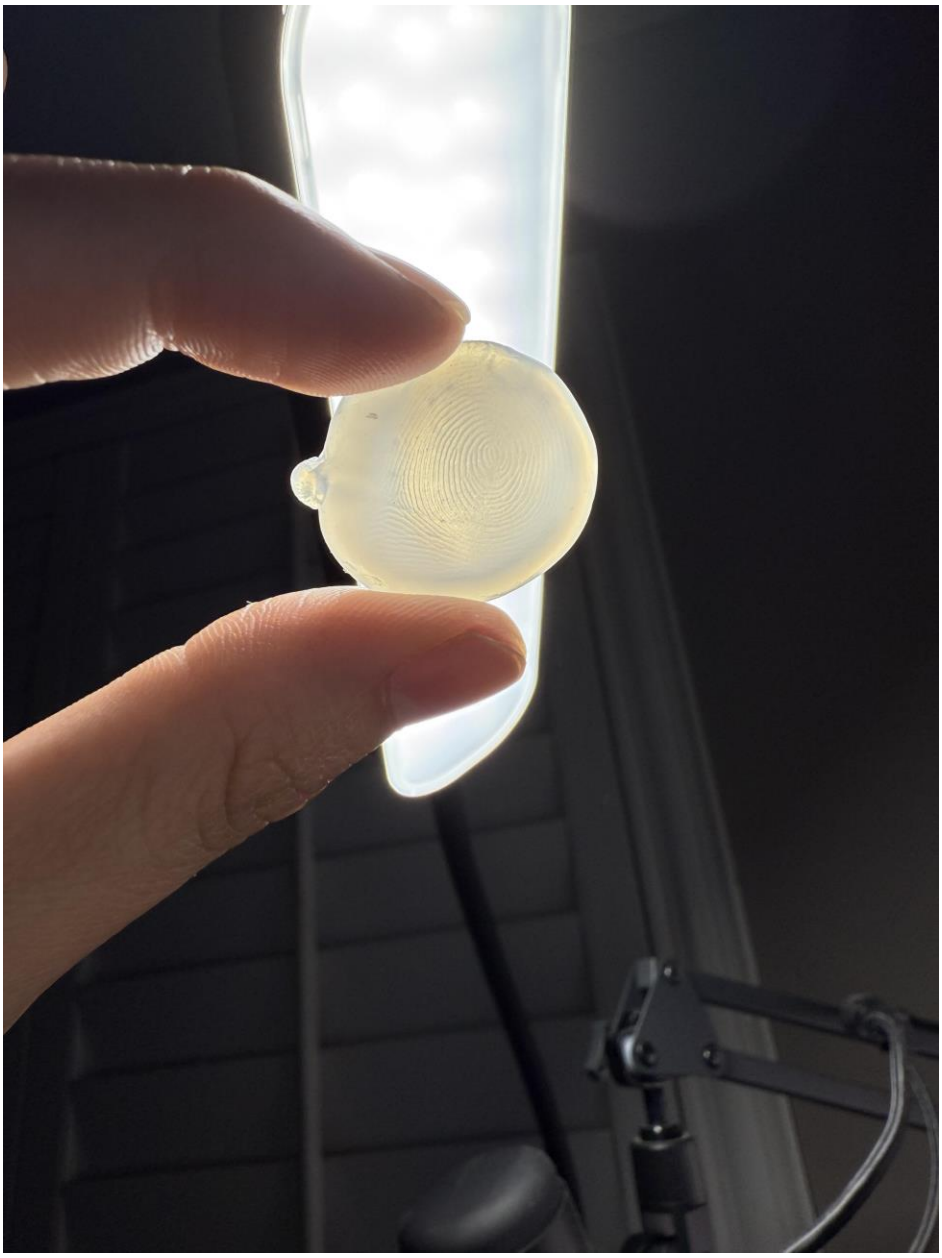
Result

Fingerprint, facial recognition, and vein pattern recognition each provide unique benefits for biometric authentication. Fingerprint systems offer enhanced security owing to the distinctiveness and permanence of fingerprints, assuring convenience since they cannot be misplaced or forgotten. When integrated with cryptographic techniques, they give dual-layer protection against identity theft. Facial recognition improves security by associating authentication directly with an individual's facial characteristics, rendering replication challenging. It can also be integrated with passwords for two-factor authentication, enhancing precision and protecting critical applications. Simultaneously, dorsal hand vein detection is distinguished by its contactless, non-invasive methodology, utilizing distinctive vein patterns beneath the skin that exhibit temporal stability. This method is impervious to dirt, wetness, or abrasions, rendering it exceptionally dependable. Furthermore, it employs safe Near-Infrared

(NIR) light to guarantee user comfort and is economically viable through the utilization of technologies like Raspberry Pi and OpenCV. Its adaptability and hygienic advantages render it suitable for secure applications, like financial transactions and mobile device verification, where security and reliability are critical.

Discussion

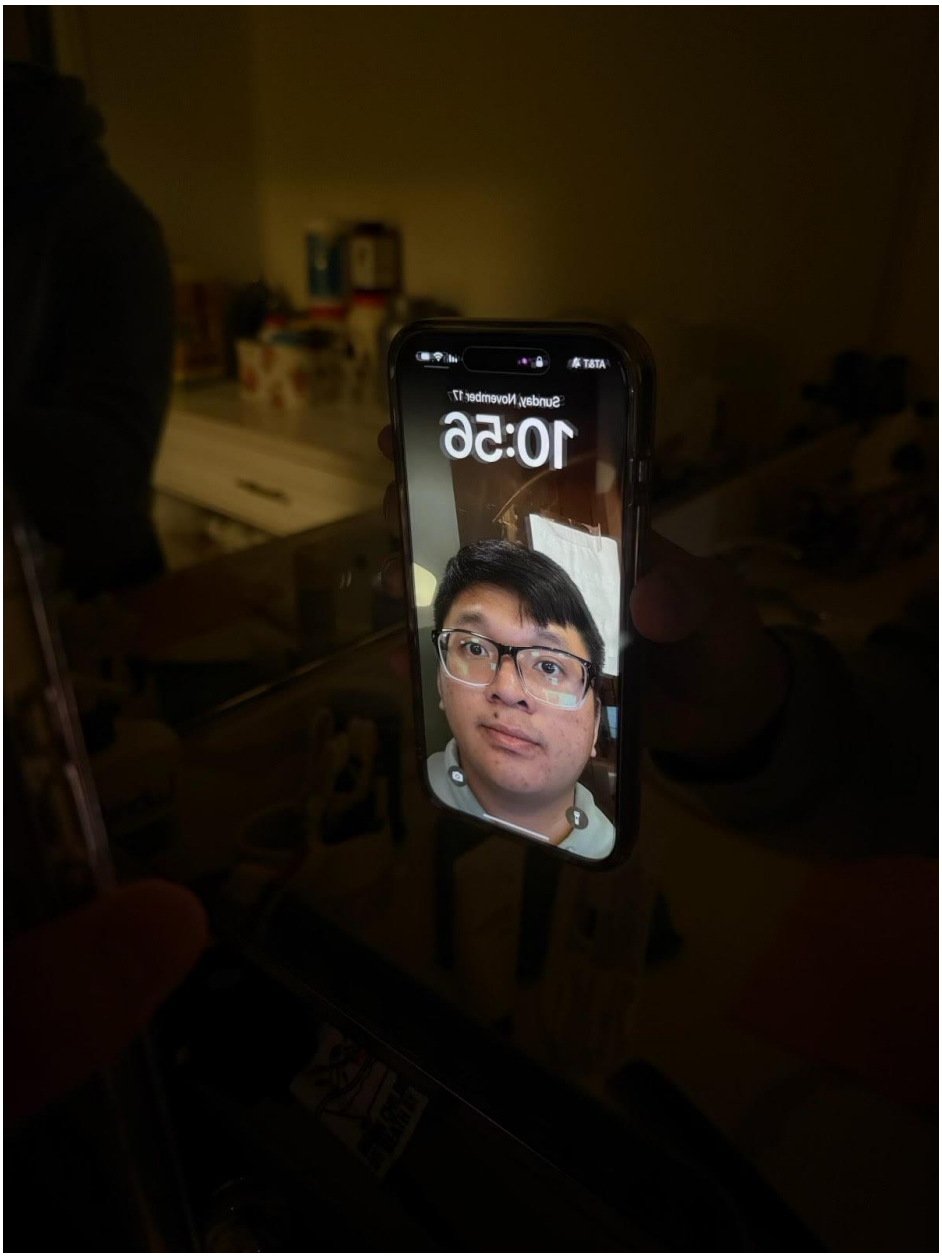
Even though all three of the methods for authentication – fingerprint, Face ID, and Vein Scanning – provide high security, they still have some drawbacks. A primary concern is security; fingerprints, in contrast to passwords, cannot be readily altered if compromised. The theft or replication of a fingerprint presents an enduring security threat, as the individual cannot merely "reset" their fingerprint. Moreover, fingerprint scanners may exhibit inaccuracies, including the inability to distinguish prints caused by dirt, dampness, or skin injury. This may result in irritation and accessibility challenges, especially for persons with specific physical problems or professions that impact their fingerprints. Moreover, fingerprint data retained on devices or servers may be susceptible to hackers, which raises privacy issues and the risk of misuse. These constraints underscore the necessity of augmenting fingerprint authentication with additional security protocols.



In the above picture, I have cloned my own fingerprint to see the fingerprint scanner can detect whether this is an artificial or a real fingerprint. Eventually, my fingerprint scanner cannot distinguish between which is real and which is unreal. Therefore, I can open my iPad with my clone fingerprint. Once our fingerprint is stolen, there is no way for us to change to a new one.

Face ID, however novel and convenient, possesses many downsides. A primary problem is privacy, as the system gathers and retains intricate face data, which might be exploited if compromised or inadequately disseminated. Security remains a concern; although

Face ID is mostly reliable, it can occasionally be deceived by photographs, masks, or individuals with similar appearances, particularly in less sophisticated versions. Environmental variables, such inadequate illumination or obscured sightlines, can diminish its trustworthiness, rendering it less reliable than alternative verification methods. Furthermore, Face ID may encounter difficulties with substantial alterations in look, such as the addition of a beard or the use of spectacles, possibly necessitating regular recalibration. Moreover, accessibility challenges emerge for individuals with face variations or disabilities, constraining its universality. These problems underscore the necessity for supplementary security measures in conjunction with Face ID.



In this picture, I used my own face to see if FaceID can detect whether this is my real face or is it just a picture. To my surprise, it can distinguish between a picture and a real person. iPhone X or above uses infrared light to scan our face. In above picture, we can see a tiny flashing purple light on top. This is an infrared light. It can help the phone to ensure that only the real person who owns this phone can unlock it.

Last but not least, vein scanning, although sophisticated and secure, also possesses some drawbacks. A significant constraint is its elevated cost, as the specialist apparatus necessary for vein imaging is costly to manufacture and sustain, rendering it less accessible for broad use. The technology may be influenced by external circumstances, such inadequate circulation, low temperatures, or specific medical conditions, which might modify vein patterns or diminish the device's capacity to capture them accurately. The necessity for direct contact or near proximity to the scanner presents hygienic issues, especially in public or communal settings. Moreover, although vein patterns are distinctive and difficult to duplicate, the storage and administration of vein data present privacy and security vulnerabilities, as any compromise of this sensitive biometric information could result in significant repercussions. These disadvantages highlight the necessity of reconciling the advantages of vein scanning with its practical constraints.

Conclusion

Modern biometric authentication systems utilize unique physiological features to verify users. Fingerprint recognition remains popular, while MD5 hashing and facial recognition are advanced methods. Yung-Wei Kai's Personal-Based Authentication System (PBAS) improves facial recognition accuracy by restricting matches using passwords. Advanced biometric methods like hand vein patterns and near-infrared imaging capture unique vein structures. However, each method has limitations, such as privacy concerns, environmental factors, sensitive data collection, lighting, and physical factors. Combining these systems with other security measures is essential for maximum safety. These limitations underscore the need for a comprehensive approach to biometric authentication.

Reference

Feng Fujun, Li Xinshe and Wang Litao, "Design and implementation of identity authentication system based on fingerprint recognition and cryptography," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 254-257, doi: 10.1109/CompComm.2016.7924704. keywords: {Fingerprint recognition;Cryptography;Reliability;Fingers;Electronic mail;Usability;Authentication;fingerprint recognition;cryptography;identity authentication;MD5},

A. Poojary, A. Chourasiya, K. Jha and S. Ranbhise, "Biometric Authentication System Using Dorsal Hand Vein Pattern," 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), Mumbai, India, 2020, pp. 1-3, doi: 10.1109/ICCDW45521.2020.9318632. keywords: {Veins;Biometrics (access control);Authentication;Feature extraction;Cameras;Skin;Pattern matching;Raspberry Pi;Open CV;Biometric;IR LEDs;No IR camera;Vein pattern},

Y. -W. Kao, H. -Z. Gu and S. -M. Yuan, "Personal Based Authentication by Face Recognition," 2008 Fourth International Conference on Networked Computing and Advanced Information Management, Gyeongju, Korea (South), 2008, pp. 581-585, doi: 10.1109/NCM.2008.167. keywords: {Face;Face recognition;Authentication;Principal component analysis;Cameras;Pattern recognition;Image recognition;authentication;face recognition},