



Abstract

Weak passwords and rudimentary authentication systems have been a top concern for both businesses and individual users for some time now. Last year, a data breach investigations report by Verizon claimed that over 0% of the total number of breaches leveraged stolen or weak passwords. As a result, companies have been investing on a multitude of ways to strengthen password security and improve the authentication process for both clients/users and employees. One of these ways is biometric authentication. Currently, most of the general population's experience with biometric authentication is done through mobile devices such as Apple's FaceID and TouchID and Android fingerprint readers. They are often marketed as convenient and secure alternatives to common 4- or 6-digit user passcodes.

Research Design & Data Collection

The scope of this project will focus on four types of biometric data: fingerprints, faces, voices, irises, and retinas. The scope was narrowed to these four based on time constraint and prevalence of available data. These four types of biometrics signatures are very popular and utilized the most for current authentication systems that use biometrics.

Due to the approval process for human subjects' protection and time constraints, the researcher did not perform tests to acquire new data and will instead incorporate data across other studies. Because of this, the sample size of the research will vary (some test results will have 30000+ subjects while others may only have several hundreds).

Signature	Cost (Average range)	Performance		Collectability Observations
		FAR	FRR	
Voice	\$40 - \$150	1.6%	7%	Impacted by mental and biological state of the user (voice is sufficiently different when distressed or speaking with nasal congestion)
Fingerprints	\$50 - \$300	1%	1.5%	Impacted by moisture/oil and fingertips that were sufficiently shaved from physical labor. Minimal impact from positioning. Susceptible to spoofing in lab setting.
Face	\$250 - \$650	2%	6%	Impacted by facial similarities, lighting, and positioning. Impacted by skin color.
Iris	\$350 - \$1500	.0001%	.56%	Impacted from movement (closed eyelids, off-axis gazes). Rare impact by iris inflammation or any other disease that effects the iris.

Table1. Consolidated Results

Introduction & Research Objective

Introduction

When it comes to biometric technologies, the particular methods that are used to gather the appropriate biometric signatures for authentication varies greatly in performance, cost, and collectability. As technology improves and additional research is performed, an increased number of biometric signatures utilized for authentication are emerging with improved effectiveness. Businesses and individual users who are interested in implementing a biometric authentication system must consider the types of signatures and accompanying technology before committing to biometric as an alternative to traditional authentication methods. Because of this, there is great interest in discerning the differences between various biometric signatures and technology..

Research Objective

The primary objective of this research is to evaluate biometric authentication and evaluate the various authenticating methods performed by current biometric technologies. A meta-analysis will be conducted for selected biometric authentication methods to determine which is most suitable for the needs of a business and individual users

Hypothesis

After reviewing several studies, the expected result from performing an evaluation between all four methods should show that fingerprint scanners as the most effective biometric authentication currently available for any one user or entity. Fingerprints are sufficiently unique which is important for authentication and the cost of fingerprint scanners should be similar in prices to voice recognition, adequately cheaper than facial recognition, and substantially cheaper than retina/iris scanners. Fingerprint scanners also appear to have higher collectability as they are not as impacted by factors such as poor lighting or poor positioning (facial recognition or iris scanner).

Results

Summarization of results:

- Facial and voice recognition have terrible relative FRR.
- Face recognition is just awful apparently.
- Iris Scanners are ridiculously accurate.
- Fingerprint scanners are extremely cheap.

Discussion

Things to consider:

- Relative Performance
- FAR vs FRR
- Accuracy vs Cost
- Role of Collectability

Conclusions

The objective of this project was to determine which, among the four biometric authentication methods selected, would best suit the needs of an individual or an organization based on performance. After consolidating, analyzing, and evaluating the data, the only conclusion that can be made is that... it depends. The reason for this is because none of the four biometric methods are heads and shoulders above the rest in all the categories that matter. Iris scanners are the most accurate in terms of FAR and FRR but they are also the most expensive, and voice recognition is cheap but its accuracy is awful relative to the other methods. That being said, fingerprint and iris scanners are the only two options in terms of performance.

Figure 1 Example of a low-price iris scanner with limited features



IriShield-USB MK 2120U Iris Scanner

The IriShield USB MK 2120U is a ready-to-use single iris capture camera. The compact camera is powered via USB port. Its low power consumption and mobile OS support makes it suitable for use with smartphones, tablets or other handheld devices. Each eye is illuminated by infrared LED, thus irises can be captured in various indoor and outdoor environments. The captured iris images are compliant with ISO/IEC 19794-6 standard.

Our Price: \$190.00

Figure 2 Example of a high-price iris scanner with added features



CMITech EMX-30

The EMX-30 is a fully hands-free, dual iris imager intended for desktop, countertop and kiosk enrollment and authentication applications. This lightweight and compact system operates at a stand-off distance range of 32 to 35 cm. The EMX-30 features a simple and intuitive user interface, making it easy to use and integrate, even for subjects with minimal acclimation.

Our Price: \$1,265.00

Contact

Phone: 808-385-2201
Name: Irvin Cabreros
Organization: University of Hawaii at West Oahu
Email: irvinjay@hawaii.edu

References

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3), 13-28.

El-Abed, M., & Charrier, C. (2012). Evaluation of Biometric Systems. *New Trends and Developments in Biometrics*, 149-169

Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J. L., & Danilcheva, A. (2018). Recent advances in biometric technology for mobile devices. In 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS) (pp. 1-11). IEEE.

Phillips, P. J., Martin, A., Wilson, C. L., & Przybocki, M. (2000). An introduction evaluating biometric systems. *Computer*, 33(2), 56-63.