Evaluating Iris, Face, and Fingerprint Authentication

Introduction:

Importance:

While passwords have long been the de facto standard for digital authentication, widespread bad habits among password holders combined with the increasing complexity of password attacks have significantly reduced the security of such a system. Recently, biometrics have been proposed to either supplement or completely replace password-based authentication systems. Among the many proposed biometric systems, iris, face, and fingerprint biometrics have emerged as the most efficient forms of biometric authentication[1][2]. These biometrics can be done with a camera or scanner small enough to fit in a phone, as opposed to more complex biometrics like retina scans which need specialized hardware[3] to implement. Despite this ease of use and comparatively low cost, these methods show high levels of accuracy[1].

Motivation:

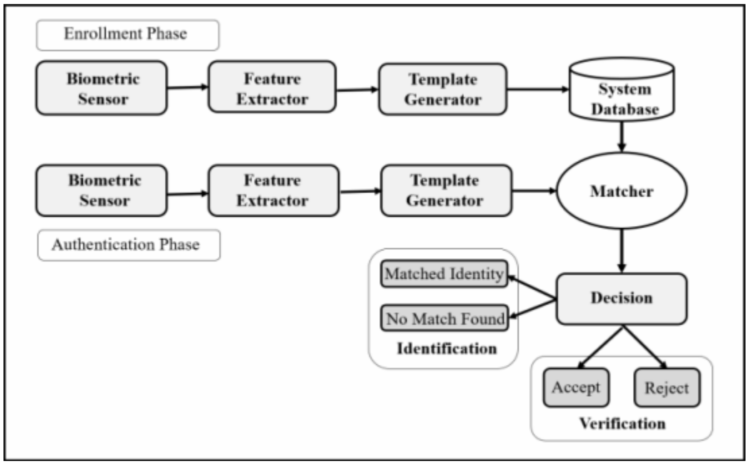
Well-studied biometrics have already seen widespread adoption, with fingerprint scanners and facial recognition technology increasingly common in consumer electronics like laptops and phones. However, this increased presence has come along with new attacks against these systems. Fingerprints have long been known to be copyable, but recent attacks have emerged showing that given an image of sufficient quality both face[4] and iris[5] biometrics can be fooled if proper liveness checks are not put into place. Furthermore, the cost and ease of use of each type must also be considered given that these qualities often take precedence over accuracy or security when it comes to mass production. Overall, it is important to identify the strengths and weaknesses of each biometric type before making a blanket recommendation for the best option for general consumer usage.

Goal:

The goal of this project is to evaluate each of the three most commonly used biometric authentication mechanisms for their accuracy, security, ease of use, and cost. Using this evaluation, we will come to a conclusion on which is the most effective and realistic one to implement on a large scale as the “standard” biometric authentication method.

Background:

All biometric authentication systems require 2 broad phases. The first is enrollment, second is recognition. These phases can be further broken down into four modules. These are the sensor module, feature extraction module, matching module, and decision module. The target biometric is captured in the sensor module, then this data is processed and sent to the feature extraction module. The feature extraction module extracts the biometric features/characteristics that are unique to the individual, which is used to create a template that represents the trait profile of the individual. These are the only modules used for enrollment. During recognition, a new template is created and compared to other stored templates in the matching module. Typically a score will be generated with how close the templates resemble each other, which is used in the decision module to either accept or reject the scanned trait according to the tolerances of the algorithm[6].



(Source 6 Figure 2)

Fingerprint authentication is the oldest biometric system, with the unique attributes of fingerprints discovered 200 years ago and used in various forms of fingerprint identification in the past century. The basis for unique fingerprint biometrics is the somewhat random pattern of ridges and valleys that make up a human fingerprint. These patterns form distinct shape groups called minutiae, which make up the data points for recognition. While previously such a comparison was done visually, digital fingerprinting uses a more exact process. First, the fingerprint is grayscaled to accentuate the minutiae. Next, the image is binarized such that 1 represents a white pixel aka valley and 0 represents a black pixel aka ridge. Finally, the image is thinned such that each ridge is 1 pixel wide. Here, different algorithms may do additional processing such as edge detection[7], while others move directly into minutiae extraction[8]. The resulting minutia data forms the template used for recognition or enrollment purposes.

Facial recognition is a more recent development than fingerprinting and has seen significant advancements in recent years. One major factor in this growth has been the demand for convenient biometric authentication methods in modern smartphones. As a result of this demand, facial recognition algorithms have grown increasingly robust and efficient, especially through the use of machine learning. Face recognition follows the standard biometric phases, but has a vast number of different approaches to feature extraction and template generation. Face detection is the one common element between these algorithms, and involves detecting an individual face from a live feed or an image. Where most algorithms differ is the feature extraction and template encoding process, which then affects how comparison occurs during the recognition phase. Some algorithms do a geometric mapping of the face using key points like the nose and eyes, while others like Apple's FaceID collect tens of thousands of points to create a more detailed map of the face. Others used machine learning algorithms to identify the face, which generally involves training an algorithm to convert the face image to an encoded pattern, such as a binary pattern[9]. These data points then form the template used for the individual.

Iris recognition involves identifying the colored ring around the eye's pupil. The patterns in the iris form uniquely for each person, even among family members. These patterns also stay the same for a person's entire life[2]. Similar to facial recognition, there are many techniques used to evaluate iris biometric data. However, there are a few steps that remain consistent between algorithms, all of which follow the standard biometric phases. Once the image of the iris is captured, it undergoes iris segmentation, where the boundary between the iris and pupil is identified[10]. Once the iris is extracted from the picture, it undergoes normalization. Normalization scales the image to a standard size and orientation for feature extraction, then does some initial processing to remove noise components like the eyelids and eyelashes from the image. At this stage, algorithms may take varying approaches to feature extraction. Some methods use filters to create a binary representation of the iris image, while others use a real-valued feature vector[11]. As with the other methods, the extracted features are then used to create the templates for recognition or enrollment.

Research questions:

- What are the security concerns (i.e. accuracy and resistance to impersonation) of each type?
- How do changes in an individual's physical features over time affect the reliability of iris, face, and fingerprint authentication? And among these, which method consistently delivers the most accurate results?
- What are the efficiency and cost propositions of each type? In other words, how viable is it to introduce this biometric type into everyday technology?

Method:

- **Literature Review:**
    - Gather related papers discussing the advantages and disadvantages of iris, face, and fingerprint authentication.
        - To evaluate the characteristics of fingerprint authentication as well as potential implementations, we analyzed papers [1][2][7][8][12][13][14][15][16].
        - To evaluate the strengths and known weaknesses of face recognition as its proposed utility in biometric authentication schemes, we reviewed papers [1][2][4][6][9][12][15][16][17][18].
        - To evaluate the advantages as well as known limitations of iris biometrics in practical use cases, we studied papers [1][2][3][5][6][10][11][12][15][16][19][20].
    - Examine the aspects of efficiency, security, cost, and user experience for each authentication method.
    - Assess the application techniques of these biometric methods to understand how environmental factors like time and lighting might impact their performance.
        - We assessed the application techniques of these biometric methods by analyzing papers to understand how environmental factors like time and lighting might impact their performance. Key references for this assessment included [1][2][6][8][10][12][13][15].
    - Analyze the literature to understand how these authentication methods can be used individually or in tandem.
        - To analyze how these authentication methods can be used individually or in tandem, we referred to [2][4][7][9][12][14][16][18][19][20].

- **Primary Data Collection:**
    - Design a survey to gauge user opinions on the experience and practicality of each biometric authentication method to supplement the literature review, particularly relating to the ease of use for each method.
    - Distribute the survey to a select group of individuals and gather their responses.
    - Analyze the survey data to identify trends, user preferences, and any potential challenges.

- **Finalization:**
  - Based on the literature review and survey results, rank each biometric method according to time efficiency, security, cost, and user experience.
  - Evaluate which authentication method aligns best with our criteria for potential large-scale adoption.
  - Provide detailed conclusions and recommendations for the most suitable biometric authentication practices for real-world applications.

Preliminary findings:

- Fingerprint recognition is very cheap and efficient to implement on small devices[1] like a phone, especially since a high-quality camera can function as a fingerprint scanner[15]. However, while its accuracy in ideal conditions is high, in practice its accuracy is highly dependent on environmental factors(sweat, dirt, etc)[12]. Furthermore, not everyone can provide a valid fingerprint due to injury or disease, and fingerprints change with age even in healthy individuals[2]. Finally, without the addition of liveness checks, this authentication protocol is highly susceptible to impersonation since fingerprint copying techniques have a long history of success, particularly by law enforcement[16].
- Face recognition is cheap to implement using currently available hardware[1] and provides a fast, contactless recognition phase[12][18]. However, despite gains in recognition accuracy, face recognition still struggles to adapt to slight changes in a user’s face (ex lighting, makeup, angle)[17] as well as aging, leading to both false authentication and false rejection. It also still struggles to handle twins[2] or people with very similar features, which is a major security risk. As a result, it tends to have a lower accuracy than iris or fingerprint authentication[15]. Additionally, with a high-quality image of a target, 2D face recognition is easy to fool and with proper setup, a 2D image can even fool a 3D scan without sufficient liveness checks[4].
- Iris biometrics are the most long-lasting and permanent[2][10] of the three biometrics we analyzed. Iris recognition also has a higher accuracy than the other techniques as well as an efficient, contactless recognition phase[1][10][11][15][19]. However, this accuracy comes at a cost, as iris recognition requires a clear, high-resolution image to correctly authenticate a user[12][20]. Consequently, iris recognition appears to be the most expensive biometric of the three to deploy on a large scale, as it requires a higher mean camera quality than face or fingerprint recognition. Additionally, like the other biometrics, some sort of liveness is required to prevent impersonation using static images of a user[5].

References:

[1] Z. V. Boriev, S. S. Sokolov, and A. P. Nyrkov, “Review of modern biometric user authentication and their development prospects,” *IOP Conference Series: Materials Science and Engineering*, vol. 91, p. 012063, Aug. 2015. doi:10.1088/1757-899x/91/1/012063.

[2]S. M. R. Bagwan, G. Gupta and S. B.Thigale, "Robust Multi-Bio-Metric Authentication Framework in Face and Iris recognition," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-10, doi: 10.1109/INOCON57975.2023.10100996.

[3]N. K. Shaydyuk and T. Cleland, "Biometric identification via retina scanning with liveness detection using speckle contrast imaging," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, USA, 2016, pp. 1-5, doi: 10.1109/CCST.2016.7815706.

[4]Z. Wu, Y. Cheng, J. Yang, X. Ji and W. Xu, "DepthFake: Spoofing 3D Face Authentication with a 2D Photo," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 917-933, doi: 10.1109/SP46215.2023.10179429.

[5]H. Shahriar, H. Haddad and M. Islam, "An Iris-Based Authentication Framework to Prevent Presentation Attacks," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 2017, pp. 504-509, doi: 10.1109/COMPSAC.2017.60.

[6]S. K. Choudhary and A. K. Naik, "Multimodal Biometric Authentication with Secured Templates — A Review," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 1062-1069, doi: 10.1109/ICOEI.2019.8862563.

[7]D. Pawade, A. Sakhapara, M. Andrade, A. Badgujar and D. Adepu, “Implementation of Fingerprint-Based Authentication System Using Blockchain,” In Soft Computing and Signal Processing - Advances in Intelligent Systems and Computing, vol 900. pp. 233 -242, Jan 2019, doi:10.1007/978-981-13-3600-3_22.

[8]X. Yin, S. Wang, M. Shahzad and J. Hu, "An IoT-Oriented Privacy-Preserving Fingerprint Authentication System," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11760-11771, 15 July 15, 2022, doi: 10.1109/JIOT.2021.3131956.

[9]S. Singh, S. C. K. Chintalacheruvu, S. Garg, Y. Giri and M. Kumar, "Efficient Face Identification and Authentication Tool for Biometric Attendance System," *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, 2021, pp. 379-383, doi: 10.1109/SPIN52536.2021.9565990.

[10]T. Le-Tien, H. Phan-Xuan, P. Nguyen-Duy and L. Le-Ba, "Iris-based Biometric Recognition using Modified Convolutional Neural Network," 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 2018, pp. 184-188, doi: 10.1109/ATC.2018.8587560.

[11]D. Zhao, W. Luo, R. Liu and L. Yue, "Negative Iris Recognition," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 112-125, 1 Jan.-Feb. 2018, doi: 10.1109/TDSC.2015.2507133.

[12]I. Ahmed and A. Asghar, “Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare”, IJRAI, vol. 13, no. 7, pp. 1–12, Jul. 2023.

[13]W. Yang, S. Wang, K. Yu, J. J. Kang and M. N. Johnstone, "Secure Fingerprint Authentication with Homomorphic Encryption," 2020 Digital Image Computing: Techniques and Applications (DICTA), Melbourne, Australia, 2020, pp. 1-6, doi: 10.1109/DICTA51227.2020.9363426.

[14]Y. Liu et al., "Secure and Efficient Online Fingerprint Authentication Scheme Based On Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 564-578, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3103546.

[15]A. A. Pawle and V. P. Pawar, “A study of different biometric authentication techniques in cloud computing,” *International Journal of Engineering Research and*, vol. V6, no. 05, pp. 944–951, May 2017. doi:10.17577/ijertv6is050575.

[16]S. M. R. Bagwan, S. Kumar and S. B.Thigale, "Face, Iris, and Fingerprint based Robust Biometric Authentication System," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-8, doi: 10.1109/INOCON57975.2023.10101122.

[17]G. Guo, L. Wen and S. Yan, "Face Authentication With Makeup Changes," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 5, pp. 814-825, May 2014, doi: 10.1109/TCSVT.2013.2280076.

[18]Q. Tao and R. Veldhuis, "Biometric Authentication System on Mobile Personal Devices," in IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 4, pp. 763-773, April 2010, doi: 10.1109/TIM.2009.2037873.

[19]C. Rathgeb, F. Breitinger, H. Baier and C. Busch, "Towards Bloom filter-based indexing of iris biometric data," 2015 International Conference on Biometrics (ICB), Phuket, Thailand, 2015, pp. 422-429, doi: 10.1109/ICB.2015.7139105.

[20]S. Joy, R. Baby Chithra, A. S. Bale, N. Ghorpade, S. N. Varsha and A. S. Naidu, "A Comparative Study on Recent Trends in Iris Recognition Techniques," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1521-1525, doi: 10.1109/ICEARS53579.2022.9752355.