Evaluating Fingerprint, Face, and Iris Authentication

Amelie Ferrell, Griffin Danner-Doran, Ife Adetunji, Naif Alkaltham, and Roneet Arora

CSEC 472 - Authentication

Professor Yidan Hu

December 14, 2023

Abstract

Due to the many issues with existing password systems, biometrics have been proposed as an alternative for use in digital authentication. Of these proposed biometric systems, fingerprint, 2D face, and iris authentication have emerged as the most promising methods for widespread use. However, to determine which method is most suitable for practical widespread deployment, we analyzed each according to accuracy, security, cost, and usability through a review of 28 pieces of existing literature. During the literature review, we further explored accuracy as it changes over time to assess each system's viability in the long run. From our research, we concluded that despite having worse usability and cost when compared to the other methods, the impressive accuracy, accuracy over time, and security of iris authentication meant that it was the best biometric method for universal deployment. In future studies, we could evaluate the three methods using the additional metrics of algorithm efficiency and privacy or we could investigate 3D face authentication as another potential biometric method.

Introduction

As we continue to increase our reliance on technology, digital authentication is essential and ubiquitous in our modern lives, securing access to our bank accounts, personal data, phones, and in the near future, appliances like our fridges. Yet despite the importance of security in digital authentication, most systems still rely on a method that has barely advanced since it was created: the password. Passwords suffer from a myriad of weaknesses from a human and technological standpoint, both of which have only gotten worse over the years. Humans are bad at remembering passwords, so rather than risk being locked out of password-protected accounts [27] we opt to make our passwords easy to remember, which makes them extremely easy for attackers to guess. Even worse, faced with an increasing number of accounts, we reuse these same weak passwords across different applications with minimal variations, allowing for multiple accounts to be compromised if just one is. Taken together with the increased performance of modern dictionary and brute force attacks, not to mention phishing attacks, our passwords are only becoming more vulnerable by the day. However, even with these known faults in security, the low cost and complexity of password systems result in them being the de facto standard for digital authentication.

As the risks of password-dependent digital authentication have continued to increase, biometrics have been proposed to either supplement or completely replace passwords. Biometric authentication systems allow users to be authenticated using only their physical or behavioral characteristics, which eliminates many weaknesses inherently found in passwords. Well-chosen biometrics are naturally unique among users, but are also somewhat permanent, meaning that they form a unique, unforgettable biological password. Among the many biometric systems proposed to replace passwords, fingerprint, 2D face, and iris biometrics have emerged as the most suitable forms of biometric authentication [1][2] for widespread use. These biometrics can

be collected with a camera or scanner small enough to fit in a mobile device like a phone or laptop, as opposed to more complex biometrics like retina scans which need specialized hardware [3] to implement. Furthermore, these biometrics can run quickly and efficiently on these mobile devices, meaning that they do not add any complexity to the login process. Fingerprint and face authentication algorithms have already proven feasible for commercial applications and practical iris authentication algorithms for mobile devices have shown promising results [21]. Despite this speed, ease of use, and comparatively low cost, these methods show high levels of accuracy [1].

Well-studied biometrics have already seen widespread adoption, with fingerprint scanners and facial recognition technology increasingly common in security systems and consumer electronics alike. However, the increased presence of biometrics has come along with new attacks against these systems. Fingerprints have long been known to be copyable [16], 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. Even with liveness checks, advanced attacks like silicone fingers, fake head models, or even patterned contact lenses [22] have emerged as potential threats, highlighting the need for truly secure biometric systems. Furthermore, the software and hardware solutions needed to combat these attacks often come into conflict with the biometric systems' practicality. Despite the main purpose of biometric authentication being security and accuracy, the cost and usability of a biometric method are often equally important when it comes to mass deployment. As a result, it is important to identify the strengths and weaknesses of each biometric type before making a blanket recommendation for the best option for general usage.

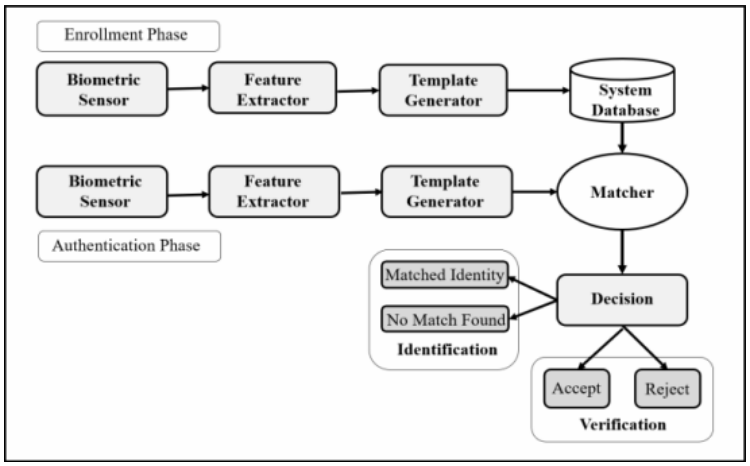
The goal of this study is to evaluate each of the three selected biometric authentication mechanisms - fingerprint, 2D face, and iris - on their suitability for practical deployment. To that end, we conducted a literature review where each biometric method was analyzed using the metrics of accuracy, security, cost, and usability, with accuracy further explored to focus on its reliability over time. An emphasis in this analysis was additionally placed on the scalability of the method for widespread use. Using the results of this review, we evaluated the three methods and came to a conclusion on which is the most effective and realistic biometric authentication to implement on a large scale as the "standard" biometric authentication method.

Background and Related Works

Biometrics

All biometric authentication systems require two broad phases. The first phase is enrollment which only happens once, and the second is recognition, which occurs whenever a user needs to authenticate. 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 from the user in the sensor module, then this data is processed and sent to the feature extraction module. The feature extraction module then 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, which tends to take longer than recognition as it gathers multiple sets of data to build a more complete template. During recognition, after the new template is created, it is compared to the 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 user according to the tolerances of the algorithm [6].



[6, fig. 2] Diagram of the biometric authentication process.

Fingerprint Authentication

Fingerprint authentication is the oldest biometric system, with the unique attributes of fingerprints discovered nearly 200 years ago and used in various forms of fingerprint identification in the past century [16]. 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 and remove any RGB-based noise. Next, the image is binarized; The ridges of the fingerprint are represented with a black pixel, and the valleys are represented with a white pixel. Then, each pixel is assigned either a 0 or 1, although the digit that is assigned to each color can differ between algorithms. Finally, the image is thinned such that each ridge is exactly 1 pixel wide [7].

Despite extensive study, no clear superior method for fingerprint extraction has emerged, so there is a wide variety of techniques used for feature extraction. The algorithm in [7] offers a technique that uses a Sobel operator for edge detection after thinning and then uses

cross-numbering for feature extraction. In this method, each ridge pixel is assigned a number 0-4 based on its adjacent ridge pixels, with the feature numbers corresponding to an isolated point, ending point, connecting point, bifurcation point, and crossing point respectively. The algorithm used in [8] is based on Mindtct, a feature extraction algorithm from the open-source NIST biometric image software. This method analyzes 2 x X slices of pixels to identify ridge endings and ridge bifurcations [25]. In the algorithm proposed in [13], the authors use the commercial deep learning fingerprint extractor Verifinger SDK to identify minutiae, then apply a minutiae pair algorithm as shown in [13, Fig. 2]. Here, all minutiae are paired together and the distance, relative orientation, and types of each pair are combined to create a binary template feature vector.

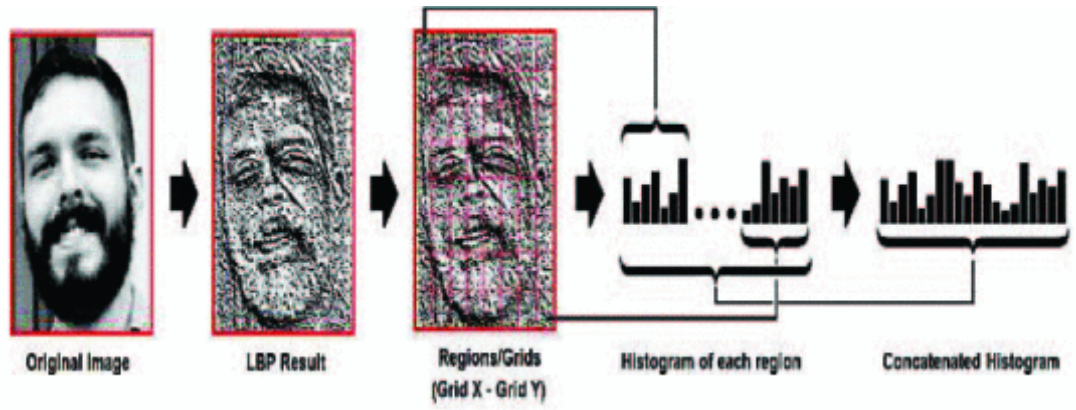
[13, Fig. 2] Illustration of the metrics calculated for a minutiae-pair.

Face Authentication

Facial authentication 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 authentication 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 [18]. Where most algorithms differ is the feature extraction and template encoding process, which then affects how comparison occurs during the recognition phase. Some algorithms like Apple's FaceID collect tens of thousands of points to

create a detailed 3D map of the face that includes depth data [4], but our study focuses on 2D authentication methods. These methods tend to use pattern recognition or machine learning to identify features, which are then encoded into a template using methods such as LBP(Local Binary Patterns) as shown in [9, Fig. 4].

Since face authentication encapsulates a variety of features that could be used for authentication, there are equally a variety of methods proposed within our study. For the technique in [17], the authors found success with a principal component analysis (PCA) algorithm, a form of eigenface, combined with a Partial Least Squares(PLS) algorithm. This was used to improve face accuracy when detecting makeup by correlating features between makeup and non-makeup faces. The approach in [18] is completely different, as it uses the Viola-Jones method pattern classification algorithm on downscaled images for face detection, then uses a modified version of the same method to identify features for extraction. The authors of this paper also use LBP to handle illumination normalization. The authors of [23] introduce the Mobiface algorithm, which uses lightweight deep learning. Mobiface uses bottleneck and residual bottleneck convolutional blocks for feature extraction, with images being downsampled over the process to reduce computational complexity.



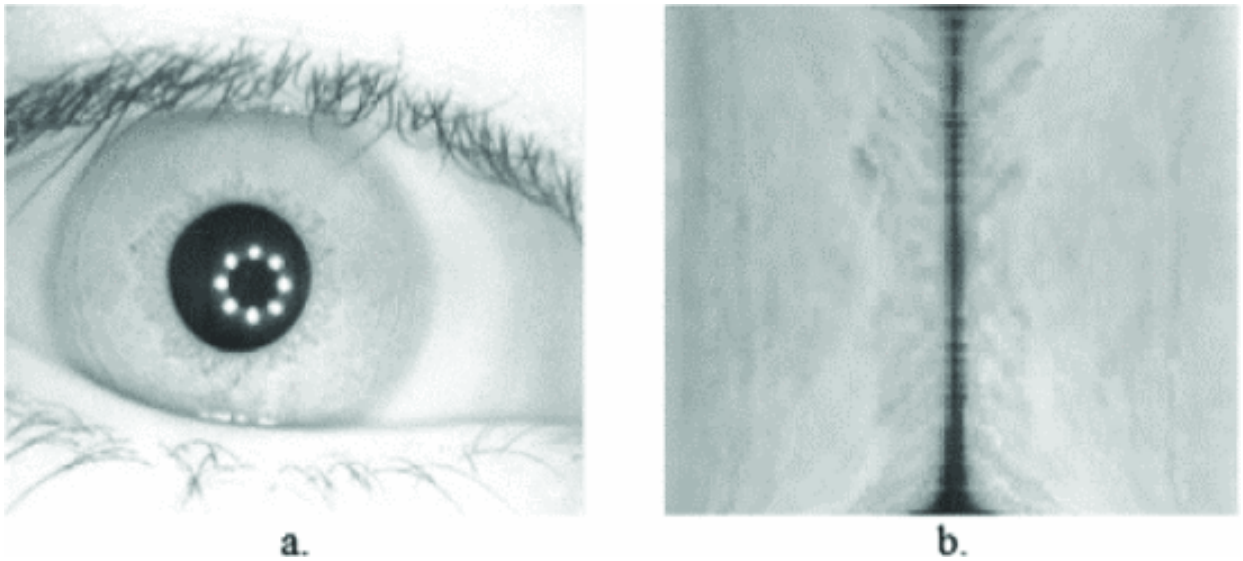
[9, Fig. 4] Diagram of an LBP encoding system using histograms for template generation.

Iris Authentication

Iris authentication involves identifying the colored ring around the eye's pupil. The patterns in the iris form uniquely for each person, even among family members [10]. These patterns also stay the same for a person's entire life [2][12]. Similar to face and fingerprint authentication, 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/localization, 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, resulting in images such as seen in [10, Fig. 7]. At this stage, algorithms may take varying approaches to feature extraction, with most creating a binary code to represent the iris feature template [11][19].

Given the specificity of the biometric in iris authentication, the methods researched for this paper varied less than fingerprint and face. The iris recognition method in [10] uses a thresholding algorithm to determine the iris boundary using histogram equalization, then normalizes the image to a standard size while removing noise like eyelashes. Finally, features are classified and extracted using a 177-layer Resnet CNN(Convolutional Neural Network) with a Softmax classifier. For the algorithm in [11], the authors use a negative database storage scheme on top of the OSIRIS-V4.1 algorithm, the latest version of the open-source BioSecure project. OSIRIS-V4.1 localizes the iris using a least squares method, uses Daugman's rubber sheet model for normalization, and uses 2D-Gabor filters of different resolutions and orientations to create the final iris code [26]. For the last algorithm, the authors of [21] use a lightweight CNN that uses two convolutional blocks with two and four layers respectively. The first block extracts low-level features to normalize and isolate the iris, then the second block extracts deep features for template generation and comparison.



[10, Fig. 7] a. Original iris image; b. Image after processing

Research questions

The first and most important requirement of an authentication system is that it can securely identify users. This task consists of both accurately identifying correct users and accurately detecting and rejecting invalid users, particularly users attempting to impersonate a

valid user by forging their biometric features. To address these elements of each mechanism, we asked the question:
Q1: What are the security concerns (i.e. accuracy and resistance to impersonation) of each type?

One area of particular interest to us regarding accuracy was the permanence of each biometric type. Given that our goal with this paper is to recommend a single authentication type for general use, we wanted to make especially sure that our selected biometric can accurately identify a person over long periods of time, resulting in the question:

Q2: How do changes in an individual's physical features over time affect the reliability of fingerprint, face, and iris authentication? And among these, which method consistently delivers the most accurate results?

Finally, while accuracy and security are extremely important to use a biometric authentication mechanism, even a perfect method will not be widely adopted if it is hard to use and/or prohibitively expensive. To evaluate the actual feasibility of implementing each authentication mechanism, we looked at the cost of each mechanism as well as its ease of use. This evaluation resulted in the question:

Q3: What are the usability and cost propositions of each type? In other words, how viable is it to introduce this biometric type into everyday technology?

Methods

To start our literature review and gain a general understanding of our topic, we looked for related papers that discussed the advantages and disadvantages of fingerprint, face, and iris authentication. Given the broad scope of each biometric, these papers provided specific methods and techniques that directly showcase the weaknesses and strengths within each authentication system. Once we had a sufficient understanding of each method, we returned to the papers with the four key metrics of accuracy, security, cost, and efficiency in mind. To evaluate the characteristics of fingerprint authentication as well as potential implementations, we analyzed papers [1][2][6][7][8][12][13][14][15][16][24][25][28]. To evaluate the strengths and known weaknesses of face recognition as it is used in biometric authentication schemes, we reviewed papers [1][2][4][6][9][12][15][16][17][18][23]. Finally, 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][21][22][26].

After evaluating and understanding each method, we also assessed the application techniques of these biometric methods to understand how environmental factors, like time and lighting, might impact their performance. To assess these factors and the adaptability of these technologies, we referenced these key papers, [1][2][6][8][10][12][13][15][17][18][21], where

environmental factors like time and lighting were discussed or played an impactful role on the performance of a proposed method. This aspect of the literature review was crucial for understanding the practical effectiveness of the biometric authentication methods. Our analysis highlights the significance of environmental factors in the use of biometric systems, suggesting pathways for the development of more reliable and efficient authentication methods across various settings.

After the literature review, we finalized our research and discussed our analysis of the papers. Based on the findings in our review, we rated each biometric method across accuracy, security, accuracy over time, cost, and usability. Particularly, our evaluation for the ratings was based on which authentication methods best aligned with our criteria for potential large-scale adoption. That meant evaluating whether these biometric methods could succeed with widespread use and on commercial devices such as mobile phones and laptops. Afterward, we provided detailed explanations for our evaluation of each biometric authentication method, concluding with which method most met our expectations for extensive use. Given this conclusion, we then provided our recommendation for the biometric authentication method that is most suitable for real-world applications.

Findings

After discussing the results of our literature review, we created Table 1 to represent each biometric method rated across our key categories. In the following sections, each of the metrics - accuracy, security, accuracy over time, cost, and usability - is discussed in depth across the three biometrics to give insight into the ratings shown here. Overall, calculating the final score in Table 1 for each biometric places iris authentication as the best biometric method for widespread deployment, followed by fingerprint and then 2D face authentication. Despite its relatively high cost and somewhat cumbersome user experience, iris authentication's high accuracy, accuracy over time and security significantly outperforms the other biometric authentication methods that we reviewed. Consequently, we believe that iris authentication presents a secure form of biometric digital authentication that is flexible enough to be used in all kinds of commercial devices, offering a promising universal biometric system.

X	**Accuracy**	**Security**	**Accuracy over time**	**Cost**	**Usability**
Fingerprint	2	3	4	1	2
Face	3	5	3	1	1
Iris	1	1	1	4	3

Table 1. Rating of each biometric technique across the 5 explored metrics. Each category is rated on a scale of 1 to 5 where 1 = exceptional and 5 = substandard.

Accuracy

Using the specific methods proposed in several papers from the literature review, we constructed Table 2 to compare the best-case accuracies of three different methods for each of the three biometrics. For the sake of comparison, these values are taken from the theoretical best-case accuracies for each method since not all methods had a prototype implementation. Fingerprint methods were tested on FVC2002 Database 2 [8][13] or an equivalent database [7], while the iris methods were tested on some variation of the CASIA database [10][11][21]. However, the face authentication methods did not have a consistent testing set [17][18] and only one presented testing data across multiple databases [23], so its accuracy results are taken from its self-identified "challenging" database to match the similar language used in [18].

Our review found that fingerprint authentication has a wide variety of different techniques with varying accuracies, but in the best case, one was able to achieve an EER of .86% [8]. This high accuracy comes from the precise measurement of minutiae on the fingerprint. Since fingerprints are almost completely unique between people and can contain up to 80 distinct minutiae [16], when taken correctly they provide a very clear set of features that can be mathematically analyzed to distinguish between users. The largest risk to fingerprint accuracy comes from the difficulty of getting a perfect fingerprint, with most rejections occurring due to environmental factors like sweat or dirt obscuring minutiae [12]. Though more accurate than face authentication, ultimately fingerprints provide fewer distinguishing features than the iris, resulting in a lower accuracy than iris authentication.

Similarly, face authentication also has a wide variety of methods, though they tend to be less accurate than fingerprint authentication. Of the three proposed methods that we researched, the most accurate method displayed an EER of 2% [18]. While face authentication has many more potential features to analyze since it can look at RGB, geometric shapes, key feature patterns, and spacing among other methods, this can be an issue as some people may have similar features [2]. Unlike iris and fingerprint patterns, human faces do not develop randomly, meaning that family members, especially twins, may have similar key features depending on the method used. As a result, face authentication methods are more likely to accept invalid users than the other two biometrics, leading it to have the lowest accuracy of the three methods.

Of the three observed methods, iris authentication was by far the most consistent, with all three of the explored methods having an accuracy above 90%. The best method was able to achieve an extremely low EER of .03% [21], exploiting the extreme detail and variation of the iris. Not only is the iris far more detailed than fingerprints, with over 200 features [20] with which to distinguish users, but it is far more unique than face features or even fingerprints. Iris features are completely unique between people, including family members and twins [2]. Even on the same person, the left and right eye have different iris features [10] meaning that any given user could potentially have two completely different iris templates. Combined with the precise

machine learning techniques observed in multiple proposed methods, the iris proves to be the most accurate method analyzed in this study.

Technique	Type	EER	GAR	FAR/FMR	FRR/FNMR
Blockchain-based cross numbering[7]	finger	-	82.55%	-	-
Mindtct[8]	finger	.86%	-	1.32%	-
Minutiae-pair[13]	finger	8.25%	-	-	-
Partial-least squares[17]	face	-	80.5%	-	-
Viola-Jones + LBP[18]	face	2%	-	-	-
MobiFace[23]	face	-	91.3%	-	-
CNN with softmax classifier[10]	iris	-	96.67%	-	-
NDBIris[11]	iris	.6%	98.94%	.01%	-
Lightweight CNN[21]	iris	.03%	-	-	-

Table 2. Performance of three different proposed algorithms for each biometric type. EER, GAR, FAR/FMR, and FRR/FNMR were evaluated based on the data available from each proposed algorithm.

Security

Fingerprints have long been known to be copyable, with ink-based and latent-print copying methods used by police for decades [16]. Adversarial attacks have only expanded upon these methods, growing to include silicone or resin-based fake fingers, photo-based spoofing, and advanced print-lifting techniques, all of which have been successfully used to fool commercial fingerprint authentication systems [24][28]. These techniques are particularly effective since fingerprint recognition requires contact, which leaves prints that can be accurately copied and later used to spoof a valid user. While some proposed solutions integrate other biometrics [16] to form a multi-modal system, these methods often require additional hardware and ultimately do not address the issues with fingerprint authentication itself. Far more promising are a variety of software-based liveness and spoof detection techniques that integrate machine learning to identify valid fingerprints. One proposed technique uses an automatically adapting SVM (Support Vector Machine) classifier to identify and reject fake fingerprints created using a variety of materials including glues, resins, gels, and silicone. It was able to achieve an average EER of around 10 - 20% against most attacks [28], with the adaptive feature allowing it to improve its performance when encountering novel spoofing techniques. Another

software-based technique specifically targeted photo-based spoofing, which is the easiest technique to execute since it does not require physically accessing a victim's device or the victim's finger. This method uses a lightweight CNN to tell if a photo is real or presented and was able to achieve an EER of .97% [24] against multiple photo presentation attack types while remaining efficient enough for mobile deployment. Overall, while fingerprint spoofing attacks continue to grow more complex, exploiting the reproducible nature of fingerprints, many promising liveness techniques have emerged to combat them. As a result, fingerprint authentication maintains a reasonable level of security, being less secure than iris authentication but much more secure than face authentication.

Of the three methods evaluated in this study, 2D face authentication is particularly vulnerable to static presentation attacks. Since a standard 2D face authentication system typically takes only a single picture of a user from a short distance away, it is extremely easy to spoof the system with a printed or electronically displayed photo. As a result, many variations of liveness checks have been proposed to combat photo presentation attacks, with liveness checks usually split into two categories. The first category is active liveness checks, which often require a video of the user performing a predefined action like blinking. However effective, these methods take significant computational resources to be able to recognize such actions and are thus only used in cloud based applications [4]. Another type of active liveness check might require the user to move the authenticating device around their head to prove dimensionality, but this generally requires a gyroscope to verify movement and thus would not be feasible for devices like laptops and stationary face scanners, reducing its potential for widespread application. As a result, most modern face recognition systems have instead opted to use passive liveness checks, which do additional processing on the single image of the user. Since 2D analysis methods have proved ineffective, most modern systems use 3D depth analysis for liveness detection. This is often done by using structured light cameras, which are fairly expensive, to detect the depth of a user and confirm they are not a picture. However, despite increasing the cost of the system, these systems can still be fooled by presentation attacks, with one study achieving a 48.44% success rate against these mixed systems using a single 2D image of a user [4]. This proves that even with extensive, and expensive, security measures, 2D face authentication systems prove extremely insecure against presentation attacks. Ultimately, with a lack of cost-effective or practical defensive techniques and the highest vulnerability to spoofing, 2D face authentication is by far the least secure biometric method explored in this study.

Due to the small size of the iris and the contactless nature of iris authentication, iris images of a potential target user are harder to obtain than face images or fingerprints. Furthermore, given the high image quality needed for successful authentication, iris authentication is inherently much less susceptible to spoofed presentation attacks than the other two methods. However, despite the reduced risk, presentation attacks are still feasible against iris authentication [5] if proper liveness techniques are not used. Much like fingerprint

authentication, many promising machine learning-based solutions can significantly reduce the impact of presentation attacks without adding additional hardware costs or reducing the usability of the system. One such technique is a proposed liveness system that uses a lightweight deep learning architecture designed for mobile applications. This technique exploited the small loss of detail in spoofed iris attacks to achieve an excellent EER of .33% against various advanced presentation attacks, including printed images, patterned contact lenses, and even cadaver eyes [22]. While not the only approach to liveness detection, this technique demonstrates that due to the highly precise and detailed nature of iris authentication, software based solutions can almost entirely eliminate the security risk of presentation attacks without significant reductions to usability or cost. As a result, iris authentication proves to be more secure than face or fingerprint authentication.

Accuracy over time

Despite the high accuracy of fingerprint authentication in ideal conditions, in practice, it suffers heavily from environmental factors. Since fingerprint authentication requires physical contact, this can include the buildup of substances like dirt, sweat, or grease on the scanner. These substances can also be present on the finger itself, with additional obscuring factors including cuts, burns, and other injuries [12] or even simply wrinkles in the finger ridges. Such factors can significantly reduce the accuracy of fingerprint recognition, as it uses a relatively limited source of features to identify a user. As discussed above, nearly all fingerprint recognition algorithms determine authentication based on minutiae extracted from a black-and-white version of the fingerprint image. These obscuring factors can completely erase or change the shape of the fingerprint, significantly altering the minutiae extracted. For example, a small paper cut across your finger changes the type of minutiae for every single ridge it crosses and a burn might completely erase whole sets of minutiae from your fingerprint. As a result, these seemingly small environmental changes can significantly increase the chance of a false rejection from the system, making it much harder for a valid user to be accurately identified. Furthermore, since we use our fingers almost constantly to hold and touch physical objects, the chance of injury or contamination is much higher than for the face or iris, meaning these kinds of false rejections occur much more frequently. Finally, fingerprints change with age even in healthy individuals [2], meaning they do not have the permanence we desire in a biometric system. Overall, the relative ease of obscuring the minutiae examined by fingerprint authentication combined with the high chance of environmental changes to fingerprints means that of our three systems, fingerprint authentication has the worst accuracy over time.

While face authentication algorithms have been making gains in accuracy since their inception, they also tend to struggle with environmental changes to a user's face. This can include lighting, makeup, face angle, and sometimes even clothing. However, unlike fingerprinting which can only use the minutiae of the finger and nothing more, facial recognition methods can use a far greater number of features to maintain accuracy even in the presence of

obscuring factors. Facial identification methods like the Viola-Jones method can identify the core features of a human face, primarily the nose, mouth, and eyes, and create an accurate bounding box around it [18]. This allows for the correct isolation of a face even at a slight angle or with clothing like hats and scarves. Furthermore, lighting issues can be addressed with encoding strategies like LBP [18], which help normalize images from an illumination standpoint and ensure that images under different lighting conditions are processed with the same accuracy. Even makeup, which fundamentally changes the appearance and key features of a human face, can be detected and accounted for with somewhat decent accuracy using correlation mapping [17]. As a result, while environmental factors do moderately reduce the accuracy of face authentication systems, there are techniques to mitigate their impact that can reduce the occurrence of false rejections in a variety of environmental conditions. With that said, faces are also subject to significant changes as a result of aging, especially for younger people, which likewise reduces its permanence as a biometric marker. Altogether, despite suffering much more meaningful impacts from environmental changes than iris authentication, the increased information density of the face allows for face authentication techniques to handle such issues more effectively than fingerprint authentication.

In contrast, iris authentication remains very accurate over long periods and suffers minimal reductions to its accuracy as a result of environmental factors. Due to its location on the body, the iris is much less prone to injury than the finger or face and shows a high degree of permanence since its patterns remain stable for a person's entire life [2][10][12]. Additionally, iris recognition inherently adjusts for some environmental factors. Since the iris and the eye as a whole are partially obscured by the eyelids and eyelashes, the removal of these noise features has been a part of the iris extraction process since it was first proposed. All modern iris recognition algorithms include some form of normalization, which extracts the iris into a standardized form without noise features [10][21], meaning these obstructing features have no significant impact on accuracy. However, iris authentication is not completely immune to environmental changes. Though iris data is gathered more precisely than the other biometrics, since the user needs to get close to a camera and look right at it, lighting still presents a potential problem for iris authentication. While changes in lighting have the additional effect of dilating the pupil, thus changing the size of the iris, many proposed iris recognition algorithms implement machine learning to improve their normalization techniques to account for this with almost no reduction in accuracy [21]. As a result, iris authentication proves extremely accurate over time, with robust algorithms able to account for the vast majority of environmental factors.

Cost

As a result of its long history of being used for authentication/identification and its widespread deployment in consumer electronics, fingerprint authentication is incredibly cheap to implement on devices of any size. Laptops and stationary fingerprint authenticators can use very cheap fingerprint scanners [12] that use a variety of methods such as optical, capacitive, or

ultrasonic sensors. For modern phones and tablets, no additional hardware is required at all since their cameras can function as fingerprint scanners with the proper software implementation [15]. As a result, widespread adoption of fingerprint authentication would incur little to no costs for consumers and minimal costs for manufacturers.

Face authentication is even easier to implement than fingerprint authentication. It can be done only using currently available hardware [1] since all it needs is a picture of the user, with nearly every modern camera capable of capturing a user's face in an acceptably high quality. However, it should be noted that unlike fingerprint and iris authentication, which can use software-based liveness detection to achieve sufficient security outcomes, should depth-based liveness be implemented, additional hardware would be needed. As discussed in the security analysis, this form of liveness detection combats static picture spoofing attacks using structured-light-based cameras [4]. This requires additional hardware since the camera needs to be capable of projecting and reading infrared light. As a result, if these liveness detection systems were implemented on all consumer devices, they would incur noticeable costs to consumers and manufacturers. Given the high costs and the surprisingly poor security outcomes of such liveness checks, we do not recommend using them in a purely 2D face system, which is why they are not included in the price rating for face authentication.

Iris authentication has the highest base cost of the three methods to implement on a global scale. While it only needs a camera, iris authentication requires a clear, high-resolution image of the user's eye to correctly authenticate them [12][20]. Given the small size of the iris and the somewhat difficult process of accurately capturing the eye due to its reflective nature, iris authentication requires a higher camera quality than face or fingerprint authentication. While the average camera quality in commercial devices continues to improve rapidly, meaning that this requirement will be less prohibitive in the near future, a current global deployment of iris authentication would moderately increase prices for consumers as manufacturers add more expensive cameras to make their devices compatible with iris authentication.

Usability

One of the reasons fingerprint authentication is so widespread today is because it is incredibly simple to use. A user merely needs to touch the registered finger to the scanner for a very short time while the fingerprint image is taken [12]. With modern systems, the image can be taken instantly, meaning the user does not need to present their finger for an extended period of time. However, fingerprinting is the only biometric mechanism of the three discussed in this study which requires physical contact. As a result, a user needs to completely remove any obtrusive clothing, such as gloves, before attempting to authenticate. Furthermore, to prevent the environmental issues discussed previously, the user may also need to clean their hands or the scanner before use, which could be difficult to do if the necessary materials (ex. water) are not

easily accessible. Both factors potentially add more time to the recognition process, reducing the convenience of the system as compared to simple face authentication.

Face authentication is similarly easy to use, with the user only needing to look at the camera while a picture is taken [18]. This process is increasingly efficient with modern cameras, as they can quickly and automatically identify a face before the picture is taken. This lets them focus on the user's face, reducing the chance of a blurry picture and the amount of time a user needs to get an acceptable picture for face authentication. While obstructive pieces of clothing like sunglasses or masks may need to be removed before authenticating, this does not significantly reduce the convenience of the system. Furthermore, since face authentication is fully contactless [12] there is no need to clean the camera before use, improving its convenience relative to fingerprinting.

Of the 3 systems we analyzed, iris authentication is by far the least usable. Similar to the other systems, obtrusive items like glasses may need to be removed to improve the accuracy of the process, but this does not significantly impact the convenience of the system. Instead, the primary usability concern for iris authentication is that due to the small size of the iris and the need for a very high-quality image of the eye to provide accurate feature analysis and comparison, a user must get very close to the camera. Furthermore, current cameras are generally not programmed to automatically identify and focus on irises within an image, so the user needs to remain relatively still for a few seconds during the authentication process [12]. Taken together, these two factors mean that iris authentication takes both more time and more effort than the other systems. Though iris authentication is contactless, where the user does not have to physically touch a sensor, the user may become uncomfortable by holding still for too long or by having to put their eye right next to the camera.

Conclusion

Based on our thorough analysis of all three biometric authentication methods, we have identified relevant information concerning each method's viability as a widespread authentication mechanism. In our analysis of fingerprint authentication, we found that it struck a balance between cost, accuracy, usability, and security with its accuracy over time being a little below average. For cost, the fingerprint method is fairly cheap as cameras can be used for fingerprint authentication on mobile devices and fingerprint scanners generally do not cost much money. Although fingerprint authentication is usually a very accurate method, its accuracy diminishes over time due to environmental factors such as sweat, dirt, or injury. It also happens to be very easy to use but it is not overly secure as it has been known to be easily copyable. Similarly, 2D face authentication is also cheap to implement and very easy to use. However, it lacks accuracy and overall security. In terms of security, this authentication method is very weak since it is extremely susceptible to static presentation attacks. Furthermore, even the introduction of 3D liveness detection cannot significantly mitigate this risk, which is why many systems tend to

favor a fully 3D solution. Although 2D face authentication and fingerprint authentication have cheap implementation and are easy to use, their weaknesses in security and accuracy over time are ultimately why we do not recommend these methods for widespread use.

After evaluating each biometric method over our criteria list, we found that iris authentication provides the best biometric method because of its significant advantage in accuracy, accuracy over time, and security. Where this method falls short is that it is more costly due to the need for a high-quality camera that will provide a high-resolution image of the iris. Iris authentication is also not as easy to use compared to fingerprint and face, because the user must remain still and close to a camera for a few seconds. However, iris authentication is a very accurate method that is not largely affected by environmental factors. Iris are not typically prone to injuries and they are not affected by age which makes this authentication system accurate over time. Many algorithms in these systems also utilize machine learning to curb any environmental factors such as differences in lighting. The security in these systems is also an advantage for this authentication method. Although presentation attacks are feasible with iris authentication, it is not as susceptible to these spoofed attacks given that a high image quality is needed for successful authentication and many spoofed attacks miss details that can be detected by machine learning liveness checks. Commercial biometrics currently trend towards fingerprint and face authentication but as the cost of high-quality cameras go down and become standard on consumer mobile devices, iris authentication will become more commonly used. Therefore, as these technologies develop, it seems that iris is the best biometric authentication method and should be considered the best candidate for a universal biometric system.

Future works

In future studies, we could further generalize our conclusions by including additional contemporary biometric techniques in our evaluation. As mentioned in the background section, face authentication can be implemented using 2D and 3D methods. For our evaluation, we did not fully explore 3D face authentication outside of the context of liveness detection due to its need for significant additional hardware, which was a disqualifying factor for our initial biometric choices. However, unlike other hardware-dependent biometrics like retina scans, 3D face authentication has proved mobile capable with applications like Apple's FaceID. While only a feature in expensive high-end devices, it seems that the hardware required for 3D face authentication may be cheaply available in the near future, potentially allowing for widespread deployment. As such, it might be worth analyzing to determine how it compares to the methods studied here.

Alternatively, we could examine our existing methods using additional metrics. In our evaluation, we did not directly study privacy/data security and algorithm efficiency as a part of our criteria. However, multiple papers referenced in this study contained elements relating to the encryption of stored biometrics or cancelable biometric techniques. It seems feasible that a

further extension of this study could look at the privacy implications of each biometric type, which play a key role in the long-term viability of a biometric system. While the algorithm efficiency of each biometric type was not explored here beyond its ability to run efficiently on mobile devices, it may be worth exploring further given that each proposed method had its upsides and downsides in terms of computational complexity and runtime. Furthermore, efficiency is a particularly relevant metric should we want to evaluate different biometric techniques for use in low-resource IOT devices like fridges and doorbells. As a whole, an extension of this study could further explore 3D face authentication methods, as well as evaluate each biometric algorithm in terms of efficiency and an analysis of the privacy/security that each provides.

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.

[21] G. Odinokikh, M. Korobkin, I. Solomatin, I. Efimov and A. Fartukov, "Iris Feature Extraction and Matching Method for Mobile Biometric Applications," 2019 International Conference on Biometrics (ICB), Crete, Greece, 2019, pp. 1-6, doi: 10.1109/ICB45273.2019.8987379.

[22] J. E. Tapia, S. Gonzalez and C. Busch, "Iris Liveness Detection Using a Cascade of Dedicated Deep Learning Networks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 42-52, 2022, doi: 10.1109/TIFS.2021.3132582.

[23] C. N. Duong, K. G. Quach, I. Jalata, N. Le and K. Luu, "MobiFace: A Lightweight Deep Learning Face Recognition on Mobile Devices," 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS), Tampa, FL, USA, 2019, pp. 1-6, doi: 10.1109/BTAS46853.2019.9185981.

[24] E. Marasco and A. Vurity, "Fingerphoto Presentation Attack Detection: Generalization in Smartphones," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 4518-4523, doi: 10.1109/BigData52589.2021.9672054.

[25] C. Watson et al., “User’s Guide to NIST Biometric Image Software (NBIS),” 2007,. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7392.pdf.

[26] N. Othman, B. Dorizzi, and S. Garcia-Salicetti, “OSIRIS: An open source iris recognition software,” Pattern Recognition Letters, vol. 82, pp. 124–131, Oct. 2016, doi: https://doi.org/10.1016/j.patrec.2015.09.002.

[27] D. Ziegler, M. Rauter, C. Stromberger, P. Teufl and D. Hein, "Do you think your passwords are secure?," 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 2014, pp. 1-8, doi: 10.1109/PRISMS.2014.6970600.

[28] A. Rattani, W. J. Scheirer and A. Ross, "Open Set Fingerprint Spoof Detection Across Novel Fabrication Materials," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2447-2460, Nov. 2015, doi: 10.1109/TIFS.2015.2464772.