A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques

Shoroog Albalawi[1], Lama Alshahrani[2], Nouf Albalawi[3], Reem Kilabi[4], A'aeshah Alhakamy[5]
Faculty of Computers and Information Technology,
Master of Artificial Intelligence at University of Tabuk, Saudi Arabia[1,2,3,4,5]
Industrial Innovation & Robotics Center (IIRC) and Faculty of Computers and Information Technology,
Department of Computer Science at University of Tabuk, Saudi Arabia[5]

***Abstract*—Biometric authentication is becoming more prevalent as it allows consumers to authenticate themselves without entering a physical address or a personal identification number. Thus, a simple finger gesture or a glance at a camera can still prove one's identity. In this review, we explain in detail how the concept of authentication and the various types of biometric techniques is used for user identification. Then, we discuss the various ways these techniques can be combined to create a truly multimodal authentication system. For a more organized approach, our overview is classified into two main categories based on human biometric traits. First, the physiological traits include fingerprint, facial, iris/retina, hand, and finger-vein. Second, the behavioral traits includes voice, signature, and keystroke recognition systems. Finally, we offer a comprehensive comparison of selected methods and techniques and focus on three criteria: algorithms, merits, and drawbacks. Based on this comparison, we provide insight into our future research in iris recognition, by which we combine several artificial intelligence algorithms to develop our system.**

Keywords*—Biometric authentication; physiological traits; behavioral traits; facial recognition; iris recognition; voice recognition; signature

I. Introduction

Authentication is a security function that involves providing and checking the proof of the person's identity, the message sender, the software, the logical server, or the device. Different identification methods have been proposed for exchanging safety-related information [1], [2], [3], [4], faced with the logical evolution of international regulations; new technological solutions are gradually being implemented. Among these technologies, biometrics is the most relevant technology to reliably and rapidly identify and authenticate a person, based on their unique biological characteristics.

Biometric authentication uses a person's biological characteristics to verify their identity and ensure secure access to an electronic system. The biometric technologies are based on how each person can be identified distinctly through one or more biological characteristics, such as fingerprint, hand morphology, retina and iris, voice, DNA, or signatures. In general, biometrics can be classified into two categories: physiological traits, and behavioral traits, as shown in Fig. 1. Biometric authentication is the application of these biometric technologies to identify a person as part of a user validation process to access a system.

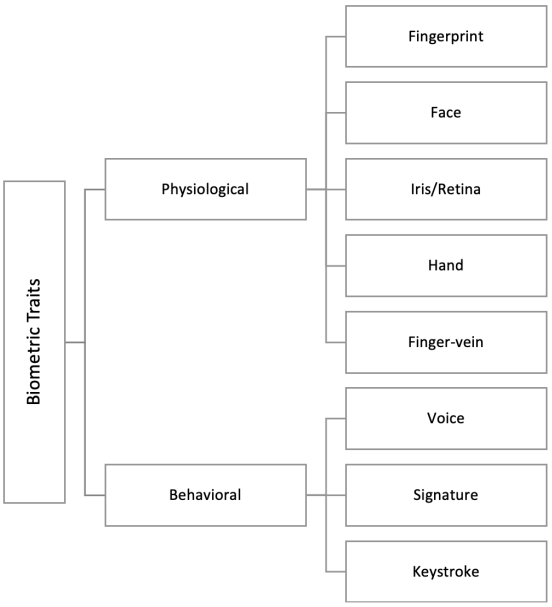

Fig. 1. Classification of Biometric Traits.

The motivations and potential benefits that drive our research are the convenient use of this approach in different systems around the world. Our future project involves using iris recognition methods in airports for fast and accurate authentication. The objective is to identify the human iris and link the data together by using artificial intelligence (AI) techniques to extract a passenger's information, such as flight number, dedicated gate, seat number, departure and arrival times, travel bag weight, how many kilos are reserved for travel bags, vaccination status, and chronic disease diagnosis (e.g., diabetes, high blood pressure).

Because different types of information can be extracted from the human iris, from our point of view, we believe the following methods better fit for our future work. (1) The edge detection algorithm is used to localize the iris and select the most important features. The system can then be segmented

and localized by using the fuzzy algorithms and the edge detection. (2) statistical features extraction methods are then used to extract the characteristics of human iris. (3) The feature space is then divided into classes, and the extracted features are trained parallel to partition the features into these classes using Principal component analysis (PCA). (4) The Support vector machines (SVMs) algorithm is then used to classify the new images in the database according to their classes to pinpoint the traveler's identity.

In this work, we present a review of biometric authentication methods and techniques that ease the way people interact with systems and how their identity influences governmental and private systems. Section III introduces physiological biometrics, and the behavioural biometrics are presented in Section IV. In these sections, we briefly discuss and list the most common biometrics, such as the facial, iris, fingerprint, voice, and signature recognition techniques. We also depict, the typical design steps of each system and its applications to provide a thorough description.

II. Biometrics Recognition Systems

Biometric technologies are used to secure a wide range of electronic communications or to connect to a computer or smartphone. Biometric authentication systems compare the human biometric data to be authenticated with the biometric database. If the two samples are matched, the authentication is then confirmed and access is granted. This process is sometimes part of a multifactor authentication system. Thus, the smartphone user can connect using their secret code such as a personal identification number [PIN] and add an iris scan. Generally, biometric identifiers are classified into physiological or behavioral characteristics; see Fig. 1.

Human biopsies are related to the various physiological characteristics of the human body such as fingerprints, facial features, iris, retina recognition, and DNA. Behavioral biometrics are related to a behavioral pattern, like the rhythm of a person typing, or how they use their fingers or look at the camera.

III. Physiological Biometrics

Physiological or static biometrics use physical characteristics, such as fingerprint or facial recognition, etc. to unlock cell phones, log into bank accounts, or complete transactions. However, the main types of static biometrics used to verify a person's identity are fingerprint recognition, facial recognition, iris recognition, etc.

A. Fingerprint Recognition

The fingerprint is one of the oldest forms of biometric authentication, and mobile platforms use this technology widely. It was originally popularized by Apple's Touch ID. A fingerprint reader analyzes a person's fingerprint and compares it to the finger's stored digital pattern during authentication. Fingerprint recognition may change if the finger is wet or dirty. An attacker cannot replicate a person's fingerprint because of its vividness; however, it can be used to create a 3D model or a fake image.

Fingerprint authentication is based on the concordance between the registration or signature file obtained during enrollment and the file obtained during authentication. Several methods are used to recognize fingerprints, such as locating minutiae and processing textures. The process of extracting minutiae involves using the template comparing to the image digitization and minutiae extraction, as shown in Fig. 2.

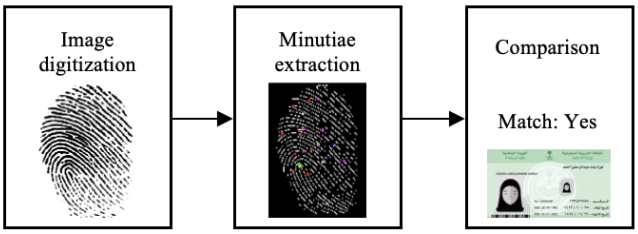

Fig. 2. Fingerprint Authentication Process: (1) Image Digitization, (2) Minutiae Extraction and (3) Comparison to the Templates.

The image digitization step consists of digitizing the fingerprint, filtering unnecessary features (e.g., scars), and determining information useful to the system. To detect the endpoints and crossing points of ridges, known as minutiae, a fingerprint skeleton is created using complex algorithms in order to make each line of the imprint, with a length from 5 to 8 pixels and a thickness of 1 pixel. Fig. 3 shows the creation of a fingerprint skeleton.

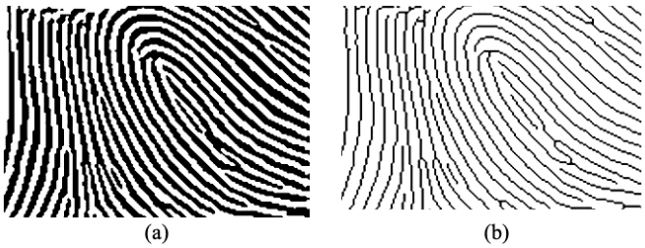

Fig. 3. Fingerprint Skeleton Creation.

The minutiae allows the extraction step to determine the signature of the fingerprint using different algorithms. The template used to characterize the fingerprint is based on a minimum number ranging from 12 to 14 minutiae, although this number can be higher as needed to establish a reliable comparison. In fact, it is possible to identify one fingerprint among several million fingerprints with this minimum of correctly identified and localized minutiae.

Finally, the comparison of two minutiae's, corresponding to two fingers to be compared, constitutes the identity verification system. To determine whether two minutiae's extracted from two images correspond to the same fingerprint, it is necessary to adopt a comparison system that is insensitive to any translations, rotations, or deformations, which systematically affect the fingerprints. From two extracted minutiae's, the system should be able to give a similarity or correspondence index of 0% if the fingerprints are totally different, and 100% if the fingerprints are from the same image.

Fingerprint recognition algorithms are sensitive to the image quality. The pretreatment step is therefore necessary before

performing the following steps. The quality of fingerprint images depends on several factors, such as contact with the probe, quality of the probe, and depth of ridges/bifurcations. Generally, preprocessing consists of smoothing, contrast enhancement, spatial/frequency domain filtering. Today, several techniques are used to solve the problems associated with fingerprints recognition.

A comprehensive overview of the patterns and techniques used in fingerprint recognition depends on the minutiae-based technique. [5]. Peralta, et al. [6] described the various aspects of fingerprint authentication and identification with respect to the minutiae-based matching algorithm. Fingerprint authentication utilizing minutiae extraction technique are discussed by Sharma, et al. [7] who covered all related systems and processes. Unimodal and multi-modal biometrics techniques were summarised by Delac and Grgic [8] including pros and cons for each model.

B. Facial Recognition

facial recognition is a technique used to identify/verify human identity based on their facial features. facial recognition can be performed from photos or video recordings. To develop a system with robust facial recognition, four steps are taken under consideration: (1) facial detection, (2) feature extraction, and (3) feature classification, and (4) feature matching. The face detection step involves identifying the human face in the image, and the feature extraction step involves extracting the feature vectors for the identified facial. The feature extraction step is considered the most crucial step in the facial recognition process. The results can then be compared and classified according to a certain criterion to identify the features of the image. These steps are illustrated in Fig. 4.

There are three major approaches to automatic face recognition by computer: global feature approach (facial-based recognition), local feature approach (constituent-based recognition), and hybrid approaches.

1) Global methods: The global approach is commonly used to identify facials using the entire image without taking into account the a face's local physiological features, such as the eyes and mouth.

The global algorithms are based on statistical properties and are usually quick to implement. However, they are sensitive to various factors such as lighting conditions and facial expression. Some of these algorithms are principal component analysis (PCA), linear discriminant analysis (LDA), support vector machine (SVM), and neural network (NN).

In this context, Sugandi, et al. [9] have proposed a facial recognition method based on PCA and backpropagation NN. Each facial image in the training is represented exactly by a linear combination of eigenfaces. This method is performed in three stages. In the first step, facial detection is performed using Haar-like features. In the second step, the authors use the AdaBoost learning algorithm to select the most important features. Finally, the backpropagation NN is used for the recognition process. In their work, the authors demonstrated that using 5 data facial images with each data are taken 100 times than usual, the experimental result showed the satisfactory result with 87.5% recognition rate.

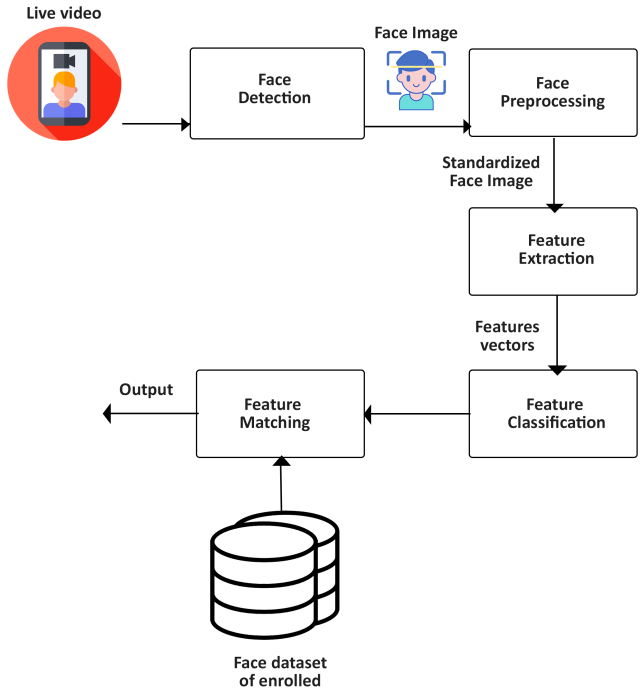

Fig. 4. Facial Recognition Structural Steps: (1) Facial Detection, (2) Feature Extraction and (3) Facial Recognition.

A study conducted by Anusha, et al. [10] showed that the weight of the image when compared with the test images can be used to identify the facials. With the same objective, Shen, et al. [11] pa method that uses both the, (1) PCA algorithm to get the feature space of the training set and then trains to identify the projected facial and (2) Fisher linear discriminant (FLD) algorithm to obtain the fusion feature space and then to train and recognize the projected facial in the feature space. Their study proved that the algorithm based on the FLD and PCA features can outperform the existing facial recognition methods.

Luabibi, et la. [12] proposed a four-phase approach for facial recognition. The first step is the localization of the facials, and the second involves extracting the features, and the third one is the classification, and the fourth phase is the back propagation algorithm to identify the facials.

The LDA method is a numerical technique that can be used to classify and improve the data representation. The resulting combinations are usually used as linear classifiers. This algorithm cuts each facial into a linear combination before classifying it. The resulting sets of new dimensions are called fisherfaces after the LDA method. Due to its complexity, the LDA algorithm is not as effective as other methods.

Bhattacharyya, et al. [13] proposed a method that involve grouping images of the same class and different classes. The resulting set of facials is then classified according to the closest training images. The study's results revealed that the proposed algorithm is significantly better than the existing methods. Lu, et al. [14] combined both the direct LDA and Fractional LDA techniques, and algorithms can be used for small sample sizes.

It can also classify the facials according to the closest training images. Results of the experiments on two databases supported the effectiveness of the proposed algorithm.

SVM's are commonly used in machine learning to solve problems related to discrimination and regression. Although they are not as efficient as some of the most popular algorithms, their potential is still very promising. In their study, Jin, et al. [15] proposed an algorithm based on a modified SVM learning scheme that uses the SVM and particle swarm optimization techniques. The results of the experiments showed that the proposed method has better accuracy than the existing methods.

In addition, Jose, et al. [16] presented a review of the techniques used for 2D facial recognition using the SVM technique. The authors analyzed the recognition results according to the techniques used to extract information such as facial features, pattern classifiers, and databases. A new method that uses the SVM algorithm to detect the facials in grayscale images was presented by Ignas et al. [17]. They then identifed the faces using the sizes and positions of the eyes and lips.

Also, Javed [18] used the PCA and SVM to build for building a facial recognition model. The authors [19] presented an overview of the effective use of machine learning, particularly regarding using SVMs in facial recognition. Therefore, the authors give an extensive survey of facial recognition and its applications.

Artificial Neural Networks (ANNs) are systems comprising of several interconnected processing units. They can perform various computational tasks based on the input data. In computer vision, an NN is composed of several processing units known as neurons. These components can learn and adapt to different tasks in order to classify the data.

Deep learning (DL) is an AI method that learns by itself. It is inspired by the human brain. The goal of DL is to learn and recognize different words and facials in an image. For example, DL can detect the letters in text before recognizing a face. In their work, Hassan, et al. [20] detailed the various approaches used in facial recognition and provided a thorough analysis of their results. They also introduced hybrid algorithms that can be used for extracting and classifying facial features.

Convolutional Neural Networks (CNNs) are commonly used in facial recognition. They are typically complex and require a high amount of processing power and storage space to perform their intended applications. In this area, Liu, et al. [21] tried to improve the performance of CNNs by introducing a block called the squeeze-and-excitation algorithm. The proposed algorithm has fewer parameters and can be more suitable for various applications.

2) Local methods: These are also called the geometrical, local characteristics, or analytical methods. This approach involves in applying transformations in specific places of the image, most often around the characteristic points (i.e., corners of the eyes, mouth, and nose). Attention is given to small local details, and the approach avoids the noise generated by aspects such as hair, eyeglasses, hats, and beards.

However, the difficulty of these methods arises when it taking into consideration several views of the facial and the lack of precision in the extraction phase of the points, which constitute their major drawback. Specifically, the methods start by extracting the local facial features such as the nose, eyes, and mouth; and the method then use their geometry and/or appearance as input to the classifier. Hence, we can distinguish two practices:

- The first practice is based on the extraction of entire regions of the facial; it is often implemented with a global facial recognition approach.
- The second practice extracts particular points from different characteristic regions of the facial, such as the corners of the eyes, mouth, and nose.

Among these approaches, we can list the hidden Markov model (HMM) and the elastic bunch graph matching algorithm (EBGM). An HMM is a statistical model in which the modeled system is assumed a Markov process with unknown parameters. Unlike a classic Markov chain, where the transitions have taken are unknown to the user but the states of execution are known, in an HMM, the states of execution are unknown to the user. HMMs are currently among the most widespread models of form recognition. They then were established in speech recognition and written recognition.. However, when using HMMs, the structure of the facial is considered as distinct regions, described by characteristic vectors.

In this context, Alhadi, et al. [22] studied three different methods to extract feature vectors from HMMs: discrete cosine transform, discrete wavelet transform, and PCA. The results of the experiments revealed that combining these methods improved the models' recognition performance. In addition, a state-of-art HMM model applied to facial recognition problems in the review [23]. In this work, the authors have presented the evolution of HMM use from the early 1990s to the present day; this makes it easier for new researchers to understand and adopt the HMMs more easily for facial recognition.

In 1997, Wiskott, et al. [24] proposed a graph matching algorithm commonly used in computer vision. This algorithm makes it possible to recognize objects in an image by using a graphic representation extracted from other images. This approach extracts a set of characteristics using a data structure called a packet graph [25]. Furthermore, Jaiswal [26] presented a method for recognizing human facials that uses the concept of a graph matching algorithm known as EBGM. The proposed method achieves high recognition rates for both the facial and the image graphs.

3) Hybrid methods: Hybrid methods pair the advantages of global and local methods by combining the detection of geometric (or structural) characteristics with the extraction of local characteristics. They make it possible to increase the stability of the recognition performance during changes in pose, lighting, and facial expressions. Local feature analysis and Gabor wavelet extracted features (such as EBGM) are typical hybrid algorithms [27], [28], [29].

C. Iris / Retina Recognition

The ability to identify the facial using the iris is one of the most accurate and secure methods for biometric identification. Unlike the hands and facial, the iris is a protected internal

organ and is therefore less, and therefore less likely to be damaged. The user must fix a digital camera that scans the iris of a person from a distance of 30 to 60 cm and directly acquires iris drawing. Then, this drawing is compared to a computerized personal identification file to identify the person.

An iris recognition system is a type of biometric system that uses images of human irises to identify people. It features two main processes: localization and segmentation. Images of the iris are determine and analyzed to extract its biometric signature. However, the image processing operations are divided into four stages: localization, segmentation, encoding, and classification. The diagram in Fig. 5 shows the methodology steps and sequential processing of the proposed iris recognition system.

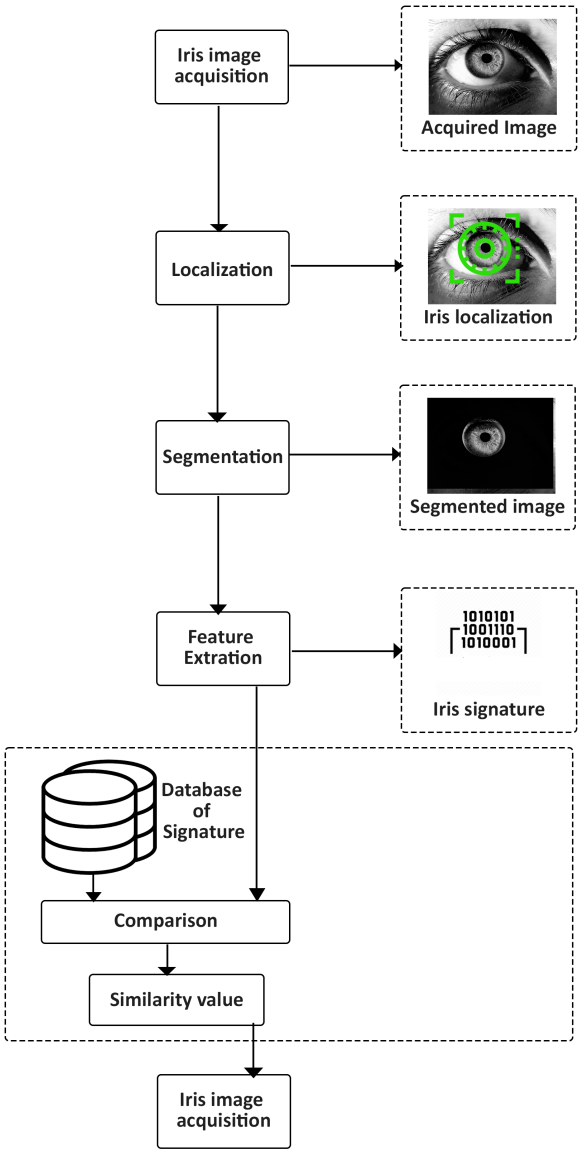

Fig. 5. The Architecture of the Iris Recognition System which Include; (1) Image Acquisition, (2) Iris Localization, (3) Segmentation and (4) Feature Extraction.

1) Iris Recognition: A new approach for the recognition of the human iris was developed by Fernando, et al. [30]. It uses the SIFT feature transformation to extract the characteristic features and then matches two images. Experiments with the BioSec database show that the SIFT approach achieves better performance than the existing matching methods.

A novel approach for deep learning that aims to improve the accuracy of the recognition of the iris using a more simplified framework was presented by wang and Kumar [31]. It utilizes residual network learning and dilated convolutional kernels to improve the training process. An unsupervised network approach can greatly simplify the network and provide better performance than state-of-the-art algorithms for iris recognition. It also eliminates the need for upsampling and downsampling layers. The results of our experiments demonstrate the applicability of our approach to improve the accuracy of iris recognition.

Furthermore, a new generalizability method for the recognition of the iris is introduced by Adamović, et al. [32], which performed on the two CASIA databases. The results of the experiments demonstrated the system performs as expected. The generalizability method can significantly reduce the computational costs of the system, which in turn makes the method suitable for practical applications. The goal is to achieve a classification accuracy of almost perfect. The method also eliminates the possibility of generating an image from a template.

2) Retina Recognition: The retina is a region of the eye that consists of four layers of cells. The arrangement of these cells is unique and provides a high level of recognition. This technology is well-suited for high-security applications because it can achieve a recognition rate of around 90% compared to other methods. The idea for retinal identification and unique vascular pattern was first introduced by two ophthalmologists, Dr Carleton Simon and Dr. Isodore Goldstein in 1935 [33].

A new method for retina recognition based on a fractal dimension was also presented by Sukumaran, et al. [34]. The authors of the study compared the accuracy of this technology with the commercially available ones. The experimental results of the method revealed that it produces high accuracy and low computational cost.

With the same objective, Tuama and George [35] proposed a personal identification system using the vascular diagram of the human retina. This system is composed of four stages. First, the prepocessing technique is used to extract the retinal image from the background and to remove noisy areas from the retinal image. Then, wavelet transforms 2D and adaptive thresholding were used to extract the blood vessels. Next, the system performs feature extraction and filtration. Finally, the matching step is used for the retina recognition. Experimental results on three publicly available databases (DRIVE, STARE, and VARIA) have demonstrated that the proposed method is better than several existing techniques.

IV. Behavioral Biometrics

Behavioral biometrics analyze a person's unique habits and movements to create a behavioral pattern. Like static biometrics, behavioral biometrics adds another layer of security to

verify a person's identity. Accordingly, this technology uses motion sensors and AI to identify unique behaviors, such as how a phone is held. These technologies are is widely regarded as the last frontier in security [36], [37].

A. Keystroke Dynamics Recognition

Stroke rhythm analyzes a person's typing rhythm on digital devices (e.g., smartphones) to create a form of human digital footprint or signatures. Gaines, et al. [38] first proposed this technology when they created the first automated dynamic keystroke recognition systems [39].Major contributions have notably evaluated the fuzzy logic [40], NNs, [41], [42], and different pattern recognition techniques (e.g., Bayes classifier) [43], [44].

B. Signature Recognition

The recognition of a signature can be accomplished by analyzing a large number of discriminative variables: (i) global characteristics such as writing time or the number of touches on the tablet with the pen, and/or (ii) local characteristics such as the position of certain curvatures or the instantaneous speed. A pressure-sensitive pencil-shaped reader and a digital tablet usually acquire a signature.

Developing a robust facial recognition system involves three basic steps: (1) preprocessing, (2) feature extraction, and (3) signature matching and classification. Before the algorithm can be used for facial recognition, the preprocessing step involves removing background noise and refining on the signature. The signature recognition system architecture is presented in Fig. 6. Feature extraction is the next step in the recognition process. It involves extracting the various features of the human signature, such as the Walsh coefficient, grid, and texture. The signature recognition step matches the various features of the human signature to template signature databases.

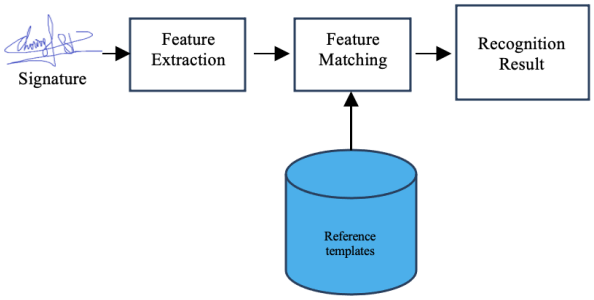

Fig. 6. Signature Recognition System Architecture that begins with Feature Extraction, then Matches these Features with a Reference Template and Finally Obtains the Recognition Result.

The best-known comparison techniques use a HMM [45], or a dynamic programming approach [46], [47].The International Graphonomic Society (IGS) research community, particularly the Scribens team, proposed the most important contribution to handwritten signature verification [48]. In this area, Jain, et al. [46] proposed to use a new measure of dissimilarity based on the alignment of characteristic vector sequences by dynamic time warping. This technique represents the most recent work in manual signature verification

C. Voice Recognition

Voice recognition is a process that uses the sounds produced by a person's vocal tract and the shape of their nose, mouth, and larynx to identify their voice. Analyzing a person's voice is a strong authentication method, but illness (e.g., the common cold, bronchitis) and background noise can distort the voice and disrupt authentication. The architecture of an automatic voice recognition system is represented in Fig. 7.

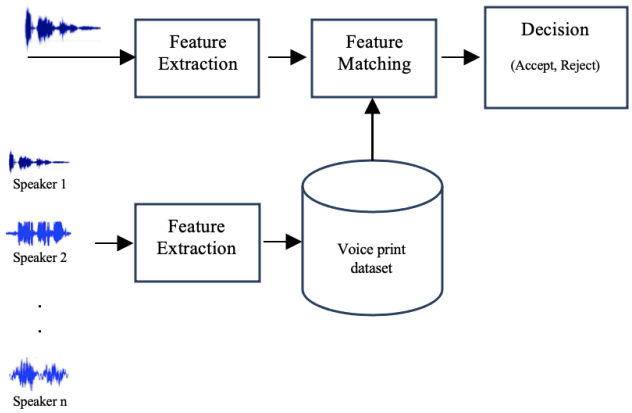

Fig. 7. Voice Recognition System Architecture that Includes Feature Extraction, Feature Matching and Decision-making based on the Voice Print Dataset.

However, the applications of speech recognition are diverse and each system has its own architecture and operation mode. In 1987, the Worlds of Wonder Company first marketed speech recognition via a doll named Julie [49]. For its voice recognition algorithm, Texas Instruments used a digital signal processing system that could recognize eight different sentences.

In addition, voice recognition has been studied for many years to help people with disabilities [50], [49], [51]. People without mobility can control an electric wheelchair through voice commands [52].

V. Discussion and Comparison

In this section, we provide a summary and discussion of the review and outline different methods of biometric authentication. We select and compare some of these methods and observe each method's algorithms, advantages and disadvantages. The study of limitations is key to improving in the future work, and we must highlight them to build our own methodology.

It is crucial to acknowledge that each method is not excluded from the others. These techniques can be combined with one another or used in different parts of the whole process to achieve the desired realism.

To explore each technique and compare these methods, we established criteria to recognize the major differences and how

they affect the final outcome. The major differences in aim, accuracy, and robustness among methods make concluding the compression challenging.

Therefore, based on the information provided in each study we attempted to distill the most useful information to write this section. We believe this effort will be helpful as a future reference for our work and that of others regarding usability, performance and more. Thus, the criteria are as follows:

- **Method.** The fundamental calculations and algorithms essential for the system's methodology and structure.
- **Merit.** The advantages the system provides, including the accuracy of the result under the previous criteria.
- **Drawbacks.** The system's limitations based on the required data, assumptions, and outcomes. Future work usually starts by discussing and discovering these drawbacks and then attemptting to solve them.

We could cover more criteria, but doing so requires insight into and evaluation of each system, which is outside the scope of the current review. We might approximate for the time and effort for the rendering and processing, but the result would be untrustworthy without any quantitative data.

An overview of these criteria to compare the previous methods from selected papers are presented in Table I. These papers were chosen based on two factors: (1) significance in their field, (2) ability to offer insights for our future work.

VI. Open Problem and Proposed Methodology

Biometric identification is a process that uses sensors to measure a person's biological characteristics. The data these devices collect then can be compared to information stored in a database. In addition to fingerprints and eyes, biometrics such as facial recognition and hand geometry have been studied and used. Eye biometrics offer the highest level of accuracy and individuality.

Iris recognition is a biometric technique that allows recognition of a person by observing their iris. Generally, the iris recognition system includes a series of steps: (i) image acquisition; (ii) iris preprocessing, including localization and segmentation; (iii) feature extraction; and (iv) matching and classification. The diagram in Fig. 8 shows the methodology steps and sequential processing of the proposed iris recognition system.

For passenger identification at an airport, we propose an iris recognition system that performs the feature extraction method and the PCA algorithm to extract and select the most important statistical features of the human iris. In addition, this system performs a supervised classification process using the SVM algorithm to identify a person's identity. The proposed system will be applied to a collection of human iris databases, such as the CASIA iris database.

This system consists of two main phases: the preprocessing phase and the classification phase. In the preprocessing phase, the system will acquire the required human iris image. The iris's features will be processed to obtain information using the statistical feature extraction method. Next, these features

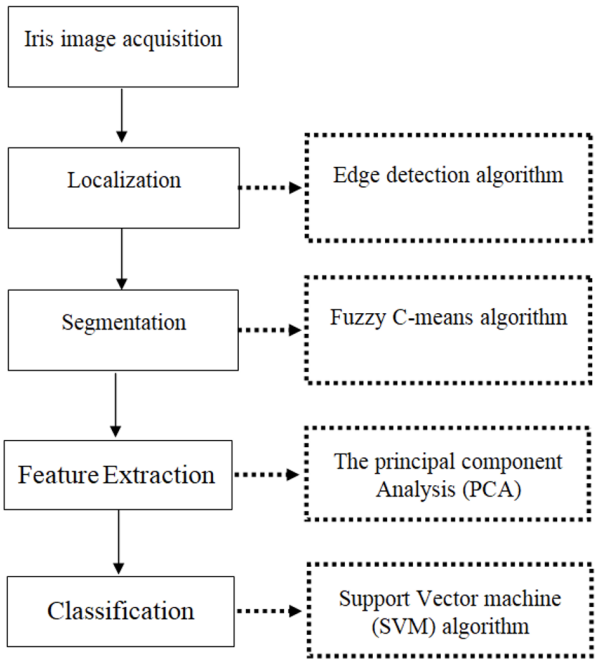

Fig. 8. Methodology Steps for Our Future Implementation in Iris Recognition System.

will be refined using the PCA reduction technique and will be the input to the SVM algorithm for classifiying human iris.

Once the iris's image is acquired, image-processing techniques are used to extract the iris, construct biometric signature, and finally find its identity. However, the acquired image must have a minimum resolution and quality to ensure the characteristics necessary for representation and identification have been obtained. Therefore, efficient segmentation of these regions is necessary.

Iris localization is one of the most important steps in an iris recognition system because it determines the matching accuracy. This step mainly localizes the boundaries of the iris, which are the inner and outer boundaries of the iris and upper and lower eyelids. To do this, edge detection techniques can be used to localize the iris in the original image. After acquiring the image, the iris should be isolated. As a first step, a series of image enhancement operations such as filtering, contrast enhancement, and histogram equalization type can be applied. The goal is to enhance the quality of the image and then apply iris segmentation operations.

The processing set necessary to extract the iris from its environment defines the iris segmentation: pupil, sclera, eyelids, eyelashes, and specular reflections. This is the most difficult step in the recognition system because it affects the system's performance.

Segmentation approaches are based on detection by fuzzy algorithms such as the fuzzy c-means algorithm. In this step, the iris is segmented in details. The encoding consists of extracting the iris's most discriminating and relevant characteristics, which are required for its identification.

To do this, the statistical features are extracted from the iris

TABLE I. COMPARISON OF PREVIOUS METHODS FROM THE SELECTED PAPERS THAT WE COVERED FOCUSING ON THREE CRITERIA: ALGORITHMS, MERIT AND DRAWBACKS

Research	Method	Merit	Drawbacks
		PHYSIOLOGICAL BIOMETRICS	
		Fingerprint Recognition Methods	
Borra, et al. [5]	-Minutiae based approach. -Pattern recognition. -Wavelet.	High accuracy rate.	-No noisy/encrypted images, -Slow performance due to three levels of split texture -Fails to determine real humans sometimes.
Peralta, et al. [6]	-Minutiae-based local matching -Correlation-based matching -Indexing	-Simplicity -Distortion tolerance.	Expensive computation, slow and depend on the skin situation.
Sharma, [7]	Minutiae based matching.	Widely used and familiar.	Affected with wet or dry skin.
Delac, et al. [8]	-Unimodal biometric systems -Multimodal biometric system.	Reliability due to use the combination of different biometric strength.	-Noisy Scanned data. Difficulty in the data gained from humans. -Biometric sign can expose to forgery.
		Facial Recognition	
Budiet, et al. [9]	-PCA -Back Propagation Neural Network.	-No Correlated Features, -High Performance, -Reduce Overfitting, -Improved Visualization, -No user action: not very intrusive, No physical contact.	Independent variables become less interpretable, -Data standardization is must before PCA, -Information Loss.
Anusha, et al. [10]	PCA	-Not intrusive, done from a distance, -Inexpensive technique. -Several characteristic features	-More suited for authentication than for identification purposes. -User perceptions and civil liberty.
Shen, et al. [11]	-PCA -FLD .	-Reduced Overfitting. -Improved Visualization.	-Data standardization before PCA. -Information Loss.
Morooj, et al. [12]	-PCA -Backpropagation NN	-Removes Correlated Features. -Improves Algorithm Performance	-Independent variables become less interpretable, -Information Loss
Bhattacharyya, et al. [13]	LDA	-Objective evaluation. -small set of features for classification purposes. -Overcomes the limitation of PCA by applying the linear discriminant criterion.	-Singular within-class scatter matrix due to small size sample. -Difficulty differentiating identical twins. Sensitive to changes such as beard and glasses.
Jin, et al. [15]	-PSO -SVM	Effective in high dimensional spaces.	-Not suitable for large data sets. -Premature convergence of PSO leading to stagnate in local optimum. -Environmentally sensitive technology.
Jose, et al. [16]	SVM	Effective in high dimensional spaces.	Not suitable for large data sets.
Ignas, et al. [17]	-SVM -Gaussian kernel for grayscale.	Effective in high dimensional spaces	-Not suitable for large data sets. -No Noisy data. -No Overlapped classes.
Mahnoor, [18]	-PCA -SVM	Effective in high dimensional spaces	-Not suitable for large data sets. -No Noisy data. -No Overlapped classes.
Jaiswal, et al. [26]	EBGM.	Insensitive to lighting variation -Rigid, and deformable matching.	More complicate procedure.
		Iris/Retina Recognition	
Fernando, et al. [53]	SIFT	- Stable in lighting and perspective variations. -Locality. -Resistant to occlusion and crowding -No prior segmentation. - Distinctiveness. -Quantity, generate many features.	-Complicated Mathematically. .High computation cost. .Not effective for low powered devices.
Poursaberi, et al. [54]	-Wavelet-based texture Hamming distance of minimum and harmonic mean	-Efficiency: close to real-time performance. -Extendable -Robust High accuracy. -Iris does not change over time	-Acquiring an image requires proper alignment and positioning. -Result affected by pupil size change.
Félix, et al. [55]	Facial key-point detection, Integro-differential operator (IDO) Mathematical morphology	-No intimate contact with the reader. -More robust than voices.	-Hard to use. -Difficulty integrating with other systems
Vahid, et al. [56]	Pattern Recognition Approach.	-Higher average for matching performance. -Convenient for people who wear glasses. -Low chances of a false positive.	-The eye position can be problematic. -Expensive specialized devices.
Sukumaran, et al. [57]	Fractal dimension using box counting Pattern Recognition Approach	-Most reliable biometric technology -Unique data points	-Serious health risk, infrared light beam. -Very large false rejection rate
Saba, et al. [58]	-Vascular diagram of the human retina -Pattern Recognition Approach	-Very accurate. -Impossible to forge a retina. -Low error rate. -Low false rejection rate -Low false acceptance rate.	-Inconvenient for people who wear eyeglasses. -Uncomfortable for some users. -Retina biometric devices.
		BEHAVIORAL BIOMETRICS	
		Keystroke Dynamics Recognition	
Gaines, et al. [38]	Examine the probability distribution of time to pressed/relaxed each key while typing on keyboard.	-Ergonomic. -Uniqueness. -Low Implementation and Deployment Cost. -Transparency and Noninvasiveness. -Increase Password Strength and Lifespan. -Replication Prevention -Additional Security. -Continuous Monitoring and Authentication	-Person's physical condition is important. -Lower Accuracy. -Lower Permanence .

Signature recognition			
Jain, et al.[46]	Behavioral biometrics based on person's handwriting	-Ergonomic. -Highly resistant to impostors. -Enrollment is intuitive and fast. -Fast response -Low storage needed. -Native language don't matter. -Little time of verification.	-Depend on the emotional state. -Difficult to use. -Large template. -High Cost -Vary over time.
Voice recognition			
Simpson, et al. [52]	Arduino, HM2007 Voice recognition module and Motors.	-More natural and easier- -Faster than typing -Can be done over the phone- No specialized equipment -Not intrusive, Low computing power	-Not reliable. Sensitivity to environment variations.

image, and the linear dimensionality reduction technique PCA is used to refine the features. Therefore, the iris encoding process constitutes representing the iris's signature. The encoding or feature extraction step is unique for each iris, regardless of dimensional variations or rotations created during the iris acquisition. This information then will be used to classify the iris.

VII. Conclusion and Future Work

Biometrics involves studying physical characteristics to identify human. With information technology and digitization, these techniques have undergone major development. Generally, biometrics can be applied to individuals who have voluntarily shared information with the biometric system, which must control them based on characteristics such as their fingerprint or voice. This step represents the enrollment procedure. This biometric information is then transformed into a digital file called a signature or template, using a specific algorithm that retains and encrypts the characteristic elements of the digitized image. This signature is then archived and compared with the person's characteristics during the control.

In this paper, we presented a detailed review of biometric systems and compared them to find the best methods and algorithms for our future work. We summarized the notion of authentication and authentication technologies and focused on biometric authentication methods. In addition, we briefly discussed the most common biometrics (i.e., face, iris, voice, signature, and fingerprint recognition techniques) and the different ways to combine them to obtain multimodal systems. Finally, we presented the typical design steps of each system and biometric applications. Consequently, the process automation, particularly the measure of characteristics such as the iris, the shape of the face or hand, the voice, the speed of typing or pressing keys, the dynamics of signature represent some challenges that can be develop in the authentication system.

After collecting all this information, we will present a hybrid approach that combines SVM-based classification and AI techniques to perform advanced iris recognition. The first step involves developing an edge detection algorithm that selects the most important features. The fuzzy and edge detection algorithms are then used to segment and localize the system. The extracted features are then divided into classes using the PCA algorithm. The proposed methodology will be used to identify passengers at an airport in our future work.

References

[1] C. Otti, "Comparison of biometric identification methods," in *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2016, pp. 339–344.

[2] A. Sumalatha and A. B. Rao, "Novel method of system identification," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. IEEE, 2016, pp. 2323–2328.

[3] M. Ortega, M. G. Penedo, J. Rouco, N. Barreira, and M. J. Carreira, "Retinal verification using a feature points-based biometric pattern," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, pp. 1–13, 2009.

[4] C. D. Byron, A. M. Kiefer, J. Thomas, S. Patel, A. Jenkins, A. L. Fratino, and T. Anderson, "The authentication and repatriation of a ceremonial tsantsa to its country of origin (ecuador)," *Heritage Science*, vol. 9, no. 1, pp. 1–13, 2021.

[5] S. R. Borra, G. J. Reddy, and E. S. Reddy, "A broad survey on fingerprint recognition systems," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2016, pp. 1428–1434.

[6] D. Peralta, M. Galar, I. Triguero, D. Paternain, S. García, E. Barrenechea, J. M. Benítez, H. Bustince, and F. Herrera, "A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation," *Information Sciences*, vol. 315, pp. 67–87, 2015.

[7] M. Sharma, "Fingerprint biometric system: a survey," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 5, no. 7, pp. 743–747, 2014.

[8] K. Delac and M. Grgic, "A survey of biometric recognition methods," in *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine*. IEEE, 2004, pp. 184–193.

[9] B. Sugandi, I. Dewita, and R. P. Hudjajanto, "Face recognition based on pca and neural network," in *2019 2nd International Conference on Applied Engineering (ICAE)*. IEEE, 2019, pp. 1–5.

[10] P. Anusha, K. L. Prasad, G. R. Kumar, E. L. Lydia, and V. S. Parvathy, "Facial detection implementation using principal component analysis (pca)," *Journal of Critical Reviews*, vol. 7, no. 10, pp. 1863–1872, 2020.

[11] S. Shen, C. Zhang, R. Xiao, W. He, and N. Zhang, "Research on face recognition based on pca and fld," in *2019 3rd International Conference on Data Science and Business Analytics (ICDSBA)*. IEEE, 2019, pp. 479–481.

[12] M. K. Luaibi and F. G. Mohammed, "Facial recognition based on dwt–hog–pca features with mlp classifier," *Journal of Southwest Jiaotong University*, vol. 54, no. 6, 2019.

[13] S. K. Bhattacharyya and K. Rahul, "Face recognition by linear discriminant analysis," *International Journal of Communication Network Security*, vol. 2, no. 2, pp. 31–35, 2013.

[14] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using lda-based algorithms," *IEEE Transactions on Neural networks*, vol. 14, no. 1, pp. 195–200, 2003.

[15] J. Wei, Z. Jian-Qi, and Z. Xiang, "Face recognition method based on support vector machine and particle swarm optimization," *Expert Systems with Applications*, vol. 38, no. 4, pp. 4390–4393, 2011.

[16] J. A. C. Moreano, N. L. S. Palomino, and A. C. L. Casa, "Facial recognition techniques using svm: A comparative analysis," *Enfoque UTE*, vol. 10, no. 3, pp. 98–111, 2019.

[17] I. Kukenys and B. McCane, "Support vector machines for human face detection," in *Proceedings of the New Zealand computer science research student conference*. Citeseer, 2008, pp. 226–229.

[18] M. Javed, *Building a Facial Recognition Model using PCA & SVM Algorithms*. Medium, 2020.

[19] Y. M. Riyazuddin, S. MahaboobBasha, J. K. Reddy, and S. Naseera-Banu, "Effective usage of support vector machine in face detection," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 3, pp. 1336–1340, 2020.

[20] R. J. Hassan, A. M. Abdulazeez *et al.*, "Deep learning convolutional neural network for face recognition: A review," *International Journal of Science and Business*, vol. 5, no. 2, pp. 114–127, 2021.

[21] W. Liu, L. Zhou, and J. Chen, "Face recognition based on lightweight convolutional neural networks," *Information*, vol. 12, no. 5, p. 191, 2021.

[22] M. W. F. F. H. Alhadi, "Support vector machines for human face detection," in *IASTED International Conference on Computational Intelligence*. Citeseer, 2005, pp. 4–6.

[23] P. Corcoran and C. Iancu, *Hidden Markov Models in automatic face recognition-A review*. IntechOpen, 2011.

[24] L. Wiskott, N. Krüger, N. Kuiger, and C. Von Der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 19, no. 7, pp. 775–779, 1997.

[25] ——, "Face recognition by elastic bunch graph matching," *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, vol. Chapter 11, pp. 355–396, 1999.

[26] S. Jaiswal, "Comparison between face recognition algorithm-eigenfaces, fisherfaces and elastic bunch graph matching," *Journal of global research in computer science*, vol. 2, no. 7, pp. 187–193, 2011.

[27] H. Cho, R. Roberts, B. Jung, O. Choi, and S. Moon, "An efficient hybrid face recognition algorithm using pca and gabor wavelets," *International Journal of Advanced Robotic Systems*, vol. 11, no. 4, p. 59, 2014.

[28] S. Shan, P. Yang, X. Chen, and W. Gao, "Adaboost gabor fisher classifier for face recognition," in *International Workshop on Analysis and Modeling of Faces and Gestures*. Springer, 2005, pp. 279–292.

[29] H. Cho, R. Roberts, B. Jung, O. Choi, and S. Moon, "An efficient hybrid face recognition algorithm using pca and gabor wavelets," *International Journal of Advanced Robotic Systems*, vol. 11, no. 4, p. 59, 2014.

[30] V. R.-A. J. O.-G. Fernando Alonso-Fernandez, Pedro Tome-Gonzalez, "Iris recognition based on sift features," *International Conference on Biometrics, Identity and Security (BIdS)*, pp. 1–7, 2009.

[31] K. Wang and A. Kumar, "Toward more accurate iris recognition using dilated residual features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3233–3245, 2019.

[32] S. Adamović, V. Miškovic, N. Maček, M. Milosavljević, M. Šarac, M. Saračević, and M. Gnjatović, "An efficient novel approach for iris recognition based on stylometric features and machine learning techniques," *Future Generation Computer Systems*, vol. 107, pp. 144–157, 2020.

[33] C. Simon, "A new scientific method of identification," *New York state journal of medicine*, vol. 35, no. 18, pp. 901–906, 1935.

[34] M. P. S. Sukumaran, "Retina recognition based on fractal dimension," *International Journal of Computer Science and Network Security (IJCSNS)*, pp. 1–7, 2009.

[35] S. A. Tuama and L. E. George, "Retina recognition based on texture analysis: Building a system for individual recognition based on vascular retina pattern," *LAMBERT Academic Publishing (LAP)*, pp. 1–7, 2016.

[36] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass, "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–11.

[37] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research," *Information & Computer Security*, 2022.

[38] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, *Authentication by keystroke timing: Some preliminary results*. Rand Corp Santa Monica CA, 1980.

[39] S. Bleha, C. Slivinsky, and B. Hussien, "Computer-access security systems using keystroke dynamics," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 12, no. 12, pp. 1217–1222, 1990.

[40] W. G. De Ru and J. H. Eloff, "Enhanced password authentication through fuzzy logic," *IEEE Expert*, vol. 12, no. 6, pp. 38–45, 1997.

[41] T. Ord and S. M. Furnell, "User authentication for keypad-based devices using keystroke analysis," in *Proceedings of the second international network conference (INC-2000)*, 2000, pp. 263–272.

[42] M. S. Obaidat and B. Sadoun, "Verification of computer users using keystroke dynamics," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 27, no. 2, pp. 261–269, 1997.

[43] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation computer systems*, vol. 16, no. 4, pp. 351–359, 2000.

[44] J. A. Robinson, V. Liang, J. M. Chambers, and C. L. MacKenzie, "Computer user verification using login string keystroke dynamics," *IEEE transactions on systems, man, and cybernetics-part a: systems and humans*, vol. 28, no. 2, pp. 236–241, 1998.

[45] R. S. Kashi, W. Turin, and W. L. Nelson, "On-line handwritten signature verification using stroke direction coding," *Optical Engineering*, vol. 35, no. 9, pp. 2526–2533, 1996.

[46] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern recognition*, vol. 35, no. 12, pp. 2963–2972, 2002.

[47] B. Wirtz, "Stroke-based time warping for signature verification," in *Proceedings of 3rd International Conference on Document Analysis and Recognition*, vol. 1. IEEE, 1995, pp. 179–182.

[48] I. G. S. (IGS), "chemin de polytechnique montréal (québec)," http://www.scribens.polymtl.ca/, accessed: 2021-11-30.

[49] K. Tang, R. Kamoua, V. Sutan, O. Farooq, G. Eng, W. C. Chu, and G. Hou, "Speech recognition technology for disabilities education," *Journal of Educational Technology Systems*, vol. 33, pp. 173 – 184, 2004.

[50] J. Noyes and C. Frankish, "Speech recognition technology for individuals with disabilities," *Augmentative and Alternative Communication*, vol. 8, no. 4, pp. 297–303, 1992. [Online]. Available: https://doi.org/10.1080/07434619212331276333

[51] J. Schönbächler, "Le traitement de la parole pour les personnes handicapées," *Travail de séminaire*, 2003.

[52] R. Simpson and S. Levine, "Voice control of a powered wheelchair," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 10, no. 2, pp. 122–125, 2002.

[53] F. Alonso-Fernandez, P. Tome-Gonzalez, V. Ruiz-Albacete, and J. Ortega-Garcia, "Iris recognition based on sift features," in *2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS)*. IEEE, 2009, pp. 1–8.

[54] A. Poursaberi and B. N. Araabi, "Iris recognition for partially occluded images: methodology and sensitivity analysis," *EURASIP Journal on Advances in Signal Processing*, vol. 2007, pp. 1–12, 2006.

[55] F. Fuentes-Hurtado, V. Naranjo, J. A. Diego-Mas, and M. Alcañiz, "A hybrid method for accurate iris segmentation on at-a-distance visible-wavelength images," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, pp. 1–14, 2019.

[56] V. Nazmdeh, S. Mortazavi, D. Tajeddin, H. Nazmdeh, and M. M. Asem, "Iris recognition; from classic to modern approaches," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2019, pp. 0981–0988.

[57] S. Sukumaran and M. Punithavalli, "Retina recognition based on fractal dimension," *IJCSNS Int J Comput Sci and Netw Secur*, vol. 9, no. 10, pp. 66–7, 2009.

[58] S. A. Tuama and L. E. George, *Retina Recognition Based on Texture Analysis: Building a system for individual recognition based on vascular retina pattern*. LAP LAMBERT Academic Publishing, 2016.