REVIEW OF VARIOUS BIOMETRIC AUTHENTICATION TECHNIQUES

Shyam Sankar
Undergraduate, Department of Computer Science Engineering
SRM Institute of Science and Technology,
Kattankulathur, Tamil Nadu, India
shyamsankar11102000@gmail.com

Abstract: Biometrics refers to the measurements and calculations related to the physical and Behavioural characteristics of human beings. Biometric traits unique enough to exclusively identify a person are used to construct biometric identification/verification systems that selectively grants access based on the success of the recognition process. This review article studies characteristics like uniqueness, permanence, expense, accuracy, convenience and vulnerability exhibited by various biometric traits and the latest advancements in the applications of the same.

Keywords: Biometrics, pattern recognition, computer vision, Behavioural biometrics, physiological biometrics.

I. INTRODUCTION

Identification of a person is key to enable restricted access. Identification can be performed by using something that a user knows, something that a user has or something that a user is. Biometrics are something that a user is. Biometric systems use the unique characteristics of the human body or the Behavioural characteristics of a person for identification. The use of biometric traits as a method of authentication dates back to prehistoric times. Fingerprints on clay tablets in ancient Babylon used for business transactions and handprints used as evidence for criminal investigations in the Qin Dynasty during BC 200s are just some of the examples. In 1881, Juan Vucetich an Argentine anthropologist and police official started a collection of fingerprints of criminals in Argentina and used it to successfully identify a criminal[1]. Biometric technology has come a long way ever since. The advancements in computer processing has led the way to automated biometric recognition systems implemented extensively from smart phones to bank transactions[2]. Biometrics holds the edge against other identification when it comes to the fast and user-friendly experience, being non-transferrable and its application in fields like forensics, healthcare, voter registration etc. However issues associated with biometrics like scalability, privacy and vulnerability to attacks are still being addressed to this day.

Some of the characteristics discussed in this review article are:

1) Uniqueness: is the measure of characteristic difference of a biometric trait that enables identification of one individual from the others.
2) Permanence: is the measure of how time sensitive the biometric trait is. The factors considered include ageing, diseases that can modify the characteristic features of the biometric trait.
3) Convenience: is the measure of how user-friendly the biometric identification process is.
4) Expense: is the measure of how costly the infrastructure required for setting up the biometric system is.
5) Accuracy: is the measure of how precise the biometric authentication is.
6) Vulnerability: is the measure of how susceptible the biometric system is to imitation and other forms of attacks.

II. TYPES OF BIOMETRICS

A. Physiological biometrics

Physiological biometric authentication systems use the unique physical measurements of the human body for identification. Physiological biometrics is the most widely used type of biometrics with applications ranging from fingerprint and face recognition in smart phones to vein and retina recognition in various high-security facilities.
Physiological biometric traits are also used in forensic science in identifying dead bodies and identifying criminals from DNA samples and fingerprints left around in a crime scene[3]. Physiological biometric traits discussed in this paper are DNA fingerprinting, ear biometrics, iris recognition, retina recognition, face recognition, fingerprint recognition and vein recognition.

B. Behavioural biometrics

Behavioural biometric authentication systems use the unique Behavioural traits and habits exhibited by human beings for identification. Behavioural biometrics are vulnerable to imitations, however with an anti-fraud solution, Behavioural biometrics can be highly secure with the advantage of being user-friendly. Reference [4] gives a detailed insight into the application of Behavioural biometrics like keystroke dynamics in the verification of the user in an unobtrusive manner. Behavioural biometric traits discussed in this paper are gait recognition, keystroke dynamics, speaker recognition and signature recognition. Biometric systems can also be classified into unimodal and multimodal depending on the number of biometric traits used for authentication. Unimodal biometric systems are biometric systems that use a single Behavioural or physiological trait for authentication. Multimodal biometric systems use more than one biometric trait to perform authentication. Multimodal biometric systems have the advantage of having better accuracy, enhanced security and are less vulnerable to spoof attacks.

III. PHYSIOLOGICAL BIOMETRICS.

1. DNA Fingerprinting/DNA Profiling

DNA (Deoxyribonucleic acid) fingerprinting is the identification of an individual on the basis of characteristics derived from the genetic code that comprises the structure of the DNA molecule. Although more than 99% of the DNA between two individuals is identical, the rest of the DNA possesses characterized regions (polymorphic markers) that are unique enough to be used for identification. The use of genetic coding finds its most popular application in forensic investigations, parentage testing and identification of human remains. The most commonly used method is to use Short Tandem Repeats (STRs) to create a DNA Fingerprint. As of 2017, the number of regions observed for STR analysis has increased from 13 to 20 that contribute to increased accuracy [5]. With the advent of technology, the amount of samples needed for doing analysis has decreased. A DNA analysis that used to take several weeks to process has reduced to less than an hour. There is also research on models to predict a description of a person including complicated facial features from DNA sequence information. This method is called DNA phenotyping[6].

2. Ear Biometrics

Ear biometrics refers to the biometric technique that uses the geometrical features of the structure of the ear for identification. Ear detection and recognition is one of the most reliable means to identify an individual especially when used to construct multimodal biometric systems combining other recognition techniques (Eg: Face Recognition). Also the fact that the ear undergoes only negligible changes with age is advantageous [7]. Reference [8] proposes a method of ear biometrics that uses sound reflecting from the ear to measure the shape of the ear canal. The shape of the ear canal is unique and this method of measurement is unaffected by accessories like earrings. An earbud-type device is used to transmit sound and the sound reflected from the ear canal is used to determine the shape of the ear canal. The proposed method is user-friendly, accurate and impregnable to presentation attacks. Reference [9] introduces an end-to-end deep neural network model that employs feature reconstruction and style reconstruction losses to generate frontal face image with ear image as the input. The Generative Adversarial Network (GAN) based model was trained and tested using the ear and face pairs dataset, FERET and MULTI-PIE. The face images generated by the model from ear images were assessed using face recognition techniques with the original face images. The reconstructed images were found to have astonishing similarities to the original images.

3. Eyes - Iris Recognition

Iris recognition refers to the method of using the spatial pattern of the coloured portion of the eye located in front of the lens and behind the cornea for identification. Iris recognition is a highly unique and reliable form of biometric authentication; however the only drawback is the limited measurability. Iris recognition systems can be spoofed by using cosmetic contact lenses. Contact lenses can be designed to both evade a system to avoid getting detected as well as to pose as another person. Reference [10] investigates the effects of ocular diseases that affect the geometry or tissue structure of the eye. 2996 iris images from 230 distinct eyes were analysed using four independent iris recognition algorithms. Ocular diseases can cause a change in geometrical patterns from the enrolment state, thus it is advisable that the person undergo visual inspection before enrolling for biometrics. Reference [11] proposes the use of a modified LAMSTAR Artificial Neural Network for iris identification and achieves a recognition rate of more than 99% on the CASIA iris database. The LAMSTAR neural network is a modified version of Kohonen SOM modules. The paper also suggests that pre-processing steps like segmentation and normalization has a huge role to play in increasing the accuracy of the classifier. Reference [12] presented a state-of-the-art open source iris recognition system that features a fast and accurate CNN-based segmentation and a fusion of OSPAD-2D and OSPAD-3D for iris presentation attack detection all of which can be implemented on a low resource platform supporting Python. The paper proposes an implementation on Raspberry Pi that amounts for a total cost of less than 75 USD.
4. Eyes - Retina Recognition

The human retina is a thin layer of tissue made up of neural cells that lines the back of the eye. Retina recognition is a biometric technique that takes advantage of the pattern of blood vessels that supply the retina with blood. Unlike iris recognition, retinal scan requires the cooperation of the individual being subject to scan as it requires the individual to look through an eyepiece that employs a low energy infrared light to capture the retinal image. However, the retina recognition system is very difficult to spoof because of the location of the retina. Retinal scan is also popular in the medical diagnosis front because of its ability to detect diseases that have an observable effect on the retina like cataract, AIDS, syphilis etc. Reference [13] introduced a model for biometric retina identification using neural networks. The paper discussed the process of image acquisition, feature extraction and classification in detail. Retinal scan images are converted into grayscale images and are fed as input to a neural network for classification. The proposed model achieved an accuracy of 97.5% which was the highest during the period. Recently proposed models have achieved higher accuracies and performance rates along with methods to avoid spoof attacks. Reference [14] proposes a biometric retina recognition system that addresses the high cost and sophisticated equipment requirement for capturing retinal scans. Unlike other retinal scan techniques that use near-infrared light, the proposed method uses signals acquired from the visual spectrum to capture retinal images using off-the-shelf camera systems.

5. Face Recognition

Face recognition is a biometric technique that analyzes the patterns in facial textures to identify a person. Although highly popular as an authentication technique in computers and mobile platforms, face recognition has lower accuracy compared to other biometric techniques. Data for facial recognition can be acquired easily in a non-invasive manner. Digital cameras to 3D sensors capable of capturing rigid features of the face can be used for data acquisition. Reference [15] proposes the use of a head pose estimation algorithm to use only frontal view images of face for identification. This method has proved an increase in 35% for the face detection rate and an increase of 9% of face recognition accuracy. The paper also proposes the use of IR facial images to monitor fever in the subject by temperature estimations, thus exploring the application of biometrics in the healthcare sector. Reference [16] introduces a night time face recognition technique that uses a thermal image to map the person’s identity to a database of visible face imagery. The method is being developed by the U.S Army Research Laboratory for real time application for identifying persons of interest during night time missions.

6. Fingerprint Recognition

Fingerprint recognition is a biometric technique that identifies individuals based on the unique patterns produced by the frictional ridges and valleys or the location and direction of minutiae points of skin on our fingertips. Fingerprint can be acquired mainly using four types of sensors - optical, capacitive, ultrasound and thermal. Fingerprints are durable throughout life; however injuries or loss of collagen due to ageing can cause a decrease in fingerprint quality. Fingerprint based biometrics are also vulnerable to spoofing attacks (also called presentation attacks) where fingerprints can be forged using materials like silicone, gelatine or latex. Reference [17] proposes an end to end spoof detection network that shows significant improvement in cross sensor, cross material and cross dataset performance. The network uses DenseNet for feature computation and global fingerprint image features along with local patch based image features. Reference [18] created the L3-SF database of synthetic fingerprints obtained by training a CycleGAN to transform real fingerprints from PolyU and handcrafted seed images into realistic fingerprints with dynamic ridge maps, sweat pores and scratches. The database also showed similar performance when compared with real fingerprint databases. The aim of this work is to encourage fingerprint recognition researches set back due to legal issues protecting the privacy of biometric data. An alternative to fingerprint recognition is palm recognition. Palm recognition uses the patterns in the entire surface area of the palm for authentication. Multimodal biometric recognition that combines fingerprint and palm recognition is more accurate than when they are used individually in a unimodal setup.

7. Hand Geometry Recognition

Hand geometry recognition refers to the biometric technique that uses the measurements along different dimensions of the human palm and fingers to establish identity. Hand geometry is not as unique as fingerprint, iris, retina etc. and hence not suitable for one-to-many comparisons, however, hand geometry can be accurate as a verification system or when being used as a complimentary biometric technique in a multi-modal biometric system. Hand geometry is time sensitive, geometrical features of the hand can undergo changes due to ageing or a significant amount of weight gain. Many experts in the field consider hand geometry as an outdated biometric technique because it has fewer numbers of unique characteristics and a relatively unstable permanence when compared to other popular biometric techniques.

8. Vein Recognition

Vein recognition or vascular biometrics refers to the biometric technique that uses the unique vascular patterns of a human palm or finger to identify a person. Deoxidised haemoglobin circulating through the veins is capable of absorbing near infra-red light. This property is used to produce an image showing the vein pattern in a palm/finger. Vein recognition is accurate, fast, and secure and does not require any contact with the system.
Palm vein recognition is more accurate when compared to finger vein recognition because more patterns are used as features for identification. Vein recognition systems require blood flow through the palm/finger and because the veins are located below the skin, it is almost non-spoofable. Reference [19] proposes a palm vein verification model that used Two-Dimensional Discrete Wavelet Transform (2-D DWT) for feature extraction, Principal Component Analysis (PCA) for feature reduction and Particle Swarm Optimization (PSO) for feature selection. A wrapper model was used to select relevant features based on metaheuristic optimization technique. The paper compares the accuracy provided by K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Decision Tree (DT) and Naive Bayes for classification. SVM produced the best results because of the similarity in the method of splitting data with PCA. Reference [20] proposes Histogram of Oriented Physiological Gabor Responses (HOPGR), a finger vein specific local feature descriptor. HOPGR involves two phases. The first phase focuses on extracting prior information by analysing the directional characteristics of finger vein patterns in an unsupervised manner. The second phase uses physiological gabor filter banks to extract responses and orientation. The proposed method performs better than most of the state-of-the-art methods in finger vein recognition.

### TABLE 1: CHARACTERISTICS EXHIBITED BY PHYSIOLOGICAL BIOMETRICS

<table>
<thead>
<tr>
<th>Biometric Technique</th>
<th>Uniqueness</th>
<th>Permanence</th>
<th>Convenience</th>
<th>Expense</th>
<th>Accuracy</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA Fingerprinting</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Ear Biometrics</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Eyes - Iris Recognition</td>
<td>High</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Eyes - Retina Recognition</td>
<td>High</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Face Recognition</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Hand Geometry Recognition</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Vein Recognition</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Reference [21] proposes PSVNet, an end-to-end deep learning network designed to reduce the amount of training samples required for accurate palm vein authentication. The proposed method uses an encoder-decoder network to learn domain specific features. This is followed by stacking inception layers used to generate palm vein feature sets. PSVNet uses a siamese convolutional neural network trained with a triplet loss function designed to learn the distance metric between positive, negative and anchor embeddings.

### IV. BEHAVIOURAL BIOMETRICS

**A. Gait Recognition**

Gait refers to the style and speed of walking. Gait recognition is the biometric technique that analyzes the unique movement of different body parts to identify a person. Gait recognition is non-intrusive and very difficult to imitate. The different techniques involved in the measurement and analysis of gait are [22]:

1) **Temporal and spatial parameters**: Spatial parameters are step length and stride length. Temporal parameters are the number of steps per unit time, speed and single limb support
2) **Kinematics**: uses marker systems to measure the position of joints and segments during each phase of movement.
3) **Markerless gait capture**: is a non-intrusive method of measuring of body joint positions from a sequence of images using colour cameras and depth sensors.
4) **Pressure measurement**: analyzes the pressure distribution, contact area, center of force movement and symmetry between sides for a comprehensive gait analysis.
5) **Kinetics**: analyses the muscle activity and soft tissue resistance to measure the ground reaction force at each joint.
6) **Dynamic electromyography**: analyzes significant muscle activity during movement.

Reference [23] introduces Incremental Learning of Gait Covariate Factors (iLGaCo), the first incremental learning approach of covariate factors for gait recognition where the model can be updated with new data without retraining the new data and the old data, but instead performing a shorter training process with the new data and a subset of the old data. The method tackles the forgetting problem in an efficient way with limited storage and low computational cost using a small memory for the previous samples and a weighted loss function for the learning process. Reference [24] introduces JointsGait, an unobtrusive model based gait recognition method of extracting gait information from human body joints. JointsGait uses 18 2-D joints as input to extract spatio-temporal features rather than silhouettes. This method has proved to outperform appearance based methods especially in the case of clothing variations. Then Joints Relationship Pyramid Mapping (JRPM) is proposed to map spatio-temporal gait features into a discriminative feature space according to human body structure and walking habit. Reference [25] proposes a method that uses inertial sensors like gyroscopes and accelerometers in smartphones to collect gait data under unconstrained conditions. A hybrid network combining Deep Convolutional Neural Networks (DCNN) and Deep Recurrent Neural Network (DRNN) was used for robust inertial gait feature representation.
B. Keystroke Dynamics/Typing Biometrics

Keystroke dynamics refers to the biometric technique that uses the detailed timing information regarding the typing pattern, rhythm and speed of keystrokes as characteristics to identify a person. The most commonly used metrics for keystroke dynamics are dwell time and flight time. Dwell time is the amount of time that a key is pressed and flight time is the idle time between releasing a key and pressing a key. Keystroke dynamics can be analysed without intruding the user's activity and can be measured using a standard keyboard. However, rhythm and typing patterns can be affected by mood changes, illness, medicine consumption etc., thus making it difficult to identify the user. Reference [26] introduces Wearable-Assisted Continuous Authentication (WACA), a continuous user authentication technique based on keystroke dynamics, which relies on built-in sensors of a wearable to acquire data and performs authentication procedure on a periodical basis in an unobtrusive manner. WACA on testing against real data, achieved low error rate and was also capable of identifying insider threats. Reference [27] introduces a method of identifying individuals below the age of 15 from keystroke dynamics with a success rate of more than 90%. This can prevent children from accessing inappropriate and predatory websites. The paper also suggests the future prospects of a multi-modal authentication system using mouse dynamics (identification using timing, movement direction and clicking information) and keystroke dynamics. Reference [28] introduced the algorithm, Instance-based Tail Area Density (ITAD) metric that significantly reduces the number of keystrokes required to identify users. A fused matching score constructed by weighing the monographs and digraphs with feature importance, in combination with ITAD produced a performance better than most of the previous state-of-the-art methods. Reference [29] introduced a method that uses keystroke and mouse dynamics for identifying an insider threat by exploiting the natural increase in stress level of a human being while performing an illegal action. Mouse dynamics is a new biometric technique that uses the patterns of operating a mouse to identify the user. Mouse dynamics enables high accuracy when used in combination with keystroke dynamics as a multimodal biometric system. The study showed that there is a significant increase in speed of pressing keys and buttons when under stress which can be successfully analyzed to detect an imposter.

C. Speaker Recognition

Speaker recognition refers to the biometric technique that identifies a person from the characteristics exhibited by his/her voice. The term speaker recognition is mainly used to refer to two types of processes: speaker identification and speaker verification. Speaker identification is the method of identifying a person by comparing against the entire database i.e. a one-to-many (1:N) approach. Speaker verification is the method verifying whether the person is who he claims to be i.e. a one-to-one (1:1) approach. Speaker verification is the most commonly used of the two. Speaker recognition systems can also be text dependent, text independent or text prompted. Speaker recognition is not the most reliable biometric authentication technique since identity recognition can be affected by diseases like common cold that can affect the voice. Also, speaker recognition systems are vulnerable to voice imitation by another person. Reference [30] explores the effect of adding pitch and voice quality features like jitter and shimmer to a Convolutional Neural Network (CNN) model for Automatic Speech Recognition (ASR). The proposed model uses pitch and voice features with Mel-Frequency Spectral Coefficients (MFSCs) to train CNN with Gated Linear Units (GLUs).

D. Signature Recognition

Signature recognition is a biometric technique that uses the style and unique characteristics of a person’s signature for identification and verification. Signatures have been used as a proof of identity and as a legally binding mark in legal contracts for a very long time. Data for signature recognition is acquired popularly in two ways [31]:
1) Static/off-line: Signatures are made on a paper or a similar kind of material. The hand-written signature is digitized using a camera or optical scanner.
2) Dynamic/On-line: Signatures are made using a pen or a finger on a screen of a tablet, smartphone or similar devices.

Signatures are very easy to replicate, however the minute characteristics observed by feature engineering algorithms like pressure, stroke and direction are very difficult though not impossible to replicate.

<table>
<thead>
<tr>
<th>Biometric Technique</th>
<th>Uniqueness</th>
<th>Permanence</th>
<th>Convenience</th>
<th>Expense</th>
<th>Accuracy</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gait Recognition</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Keystroke Dynamics</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Signature Recognition</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

V. CONCLUSIONS

Biometric systems have undergone massive development in the past decades. Passwords and proximity cards are being replaced by automated biometric authentication systems.
In 2018 alone, the global biometric system market has accounted for revenue of 21.8 billion USD of which mobile biometric technologies brought in more than 20 billion. Apart from smartphone users, biometric authentication systems are also being used in airports, banks, military bases, high security prisons etc. This indicates the user friendly, fast and accurate nature of biometrics. Emerging trends in biometric technology like cloud-based biometric identification is capable of increasing the accuracy and reducing the infrastructure needed thus mitigating the “expensive” tag that the technology carries. New and innovative biometric traits are being discovered and the accuracy and secure nature of the existing biometric technologies are being tested and improved.

REFERENCES


