Exploring the Landscape: A Comprehensive Survey on Biometric-Based Identification System

Aparna Shukla[1] , Vandana Bhattacharjee[2] and Jaya Pal[3]

[1]Department of Computer Science & Engineering,Birla Institute of Technology Mesra, Ranchi
[2]Department of Computer Science & Engineering,Birla Institute of Technology Mesra, Ranchi
[3]Department of Computer Science & Engineering,Birla Institute of Technology Mesra, Ranchi
a.shukla@bitmesra.ac.in, vbhattacherjee@bitmesra.ac.in and jayapal@bitmesra.ac.in

Abstract

In response to the rapid rise of electronic crimes, establishing a robust user authentication system has become imperative for access control and safeguarding private data. Human biometrics, including face, fingerprint, palm, iris scanning, facial features, signature, and voice, furnish a reliable security level for both personal and public utilization, surpassing traditional methods like passwords. This paper explores biometric identification systems, addressing techniques. It briefly reviews various modalities, analyzing their strengths and limitations. The examination extends to identification methods, covering feature extraction, matching algorithms, and performance evaluation parameters are discussed, emphasizing recent advancements like multi-modal biometrics and deep learning. The paper concludes with future research directions in biometric identification systems, including developing more accurate and robust techniques, improving data quality, and addressing ethical and legal issues.

Keywords: Statistics; Data science; Biometrics; Capitalize the first word of each keyword.

1. Introduction

Today, the foremost priority revolves around personal identification, signifying the link between an individual and their identity. This connection manifests through processes known as authentication (or verification) and identification (or recognition)[1]. Authentication involves validating a claimed identity, posing the question, "Am I truly who I assert to be?" On the other hand, identification entails acknowledging an individual within the system's enrolled database, answering the query, "Who am I in this context?"

Conventional methods that do not rely on an individual's inherent attributes for personal identification include knowledge-based and token-based identification systems. The former utilizes personal information possessed by the individual, such as a PIN or password, for the identification process. In contrast, the latter relies on information physically carried by the individual, such as a driver's license, credit card, ID card, and other personal documents.

Security systems have evolved through various trends, starting from reliance on knowledge-based elements like PINs to possession-based elements such as driving licenses. More recently, there has been a shift towards the emerging trend of identification based on intrinsic attributes, namely biometrics, or combinations of two or more of these factors. The biometric trend emerges as a potential solution to address the shortcomings associated with knowledge-based and token-based authentication systems.

Traditional security systems for human identification fall short of delivering on their security promises due to inherent issues. These approaches face serious challenges, such as the potential loss, theft, or forgetfulness of tokens, and the susceptibility of PINs or passwords to easy guessing or forgery. As a result, these shortcomings significantly degrade the system's performance [2]. Traditional identification systems cannot make sufficiently distinctive judgments to differentiate between a genuine individual and an imposter. Therefore, there is a pressing need for a reliable, robust, and secure identification system. The emergence of "biometrics" addresses these challenges by providing a strong foundation for a secure identification system where traditional methods falter. With biometrics, there is no requirement to carry or remember anything, offering a promising alternative to overcome the limitations of traditional security systems [3].

The contributions of this paper are manifold:

- To delve into the foundational aspects of biometric systems, covering essential information such as the basic operational processes inherent in any biometric system.
- To explore various biometric modalities, discussing their advantages, disadvantages, application domains, and existing challenges.
- To examine performance evaluation metrics for assessing biometric system efficacy.

This survey paper evaluates the effectiveness of biometric systems. It also catalogs available datasets for popular biometric modalities. The paper is structured as follows: Section 2 outlines general biometric system stages and modes. Section 3 delves into comparative analyses of biometric modalities and the necessity of Multibiometrics systems. Section 4 introduces various techniques and devices for biometric data acquisition, followed by a discussion of feature extraction techniques in the literature in Section 5. Section 6 examines performance parameters for evaluating biometric system efficiency, and finally, Section 7 concludes the paper.

2. Biometric System

In recent decades, numerous security measures for personal identification have been introduced. However, their effectiveness has come into question as the misuse of technological advancements has led to a significant increase in unethical activities.

Biometrics, an emerging technology, is widely accepted in addressing identification challenges[2]. It has positioned itself as a robust alternative to traditional security systems by mitigating longstanding issues associated with the conventional approaches. With substantial advancements in the field of identification systems, biometric systems have become increasingly prevalent over the last few decades. Biometric technologies are increasingly becoming the foundation of a broad spectrum of highly secure identification and personal verification solutions..

2.1 Overview of Biometric System

The term "Biometric" is derived from the Greek words "Bio" (life) and "Metric" (to measure), signifying "A life to measure" [5]. In the realm of Information Technology, biometrics refers to the science and technology of measuring distinct physiological or behavioral traits in humans for identification purposes. Physiological traits are associated with the physical structure or composition of the body, including fingerprint, face, hand, iris, etc., while behavioral traits encompass the actions performed by an individual, such as gait, signature, and more.

Biometrics revolutionize the process of recognizing individuals based on their unique characteristics such as the face, fingerprint, iris, handwritten signature, gait, and keystroke, surpassing traditional methods such as passwords and PINs[3][4]. Such systems find extensive use in diverse applications, including civilian and government settings like ATMs, border checkpoints, surveillance, security, computer/network security, and financial transactions [8]. Private companies are increasingly adopting biometric solutions to enhance security and safeguard confidential and employee-related information from unauthorized access.

Biometric systems simplify personal identification by recognizing patterns in an individual's physiological or behavioral traits. The process involves acquiring a biometric identifier, extracting discriminative features, and comparing them with enrolled templates in a database to make the final identification decision.

Biometric systems simplify personal identification by recognizing patterns in an individual's physiological or behavioral traits. This involves acquiring a biometric identifier, extracting discriminative features, and comparing them to enrolled templates in a database for the final decision. This advanced identification technique is preferred due to its accuracy and reliability

Figure 1 illustrates the generic structure of biometric systems, consisting of four key stages that operate sequentially to reach the system's final decision [6][9].

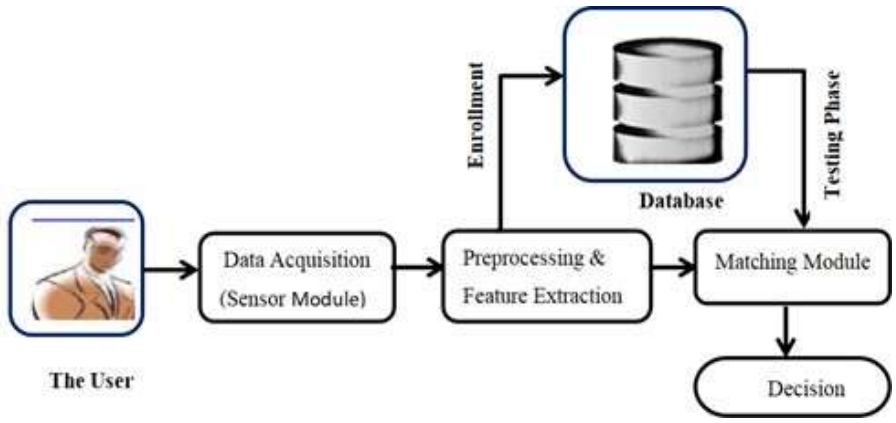


Figure 1: A Generic Structure of a Biometric Identification System

Four vital modules of any biometric system are:

- *Data Acquisition*

The Data Acquisition Module (Sensor Module) serves as a bridge between the user and the biometric system. It captures biometric information using electronic sensors, like fingerprint sensors, converting it into a digital format crucial for subsequent system processes. This stage is pivotal, often incorporating quality checks due to its impact on the overall system performance.

- *Preprocessing and Feature extraction*

The acquired biometric data may contain anomalies, necessitating preprocessing before actual operations. This involves stages like missing data imputation, smoothing, normalization, and segmentation to isolate the relevant biometric trait. After enhancing data quality, application-specific features are extracted, varying based on the biometric traits used. These features are then sent to either the enrollment phase for database storage or the matching phase for individual identification.

- *Matching*

After extracting relevant features from the captured biometric identifier, the matching process involves comparing these features with pre-stored templates in the database to generate matching scores. Similarities or dissimilarities (distance scores) can result, where a higher score in similarities indicates a closer match, while in dissimilarities, a lower score suggests a closer match between the query and templates.

- *Decision*

In the conclusive stage of the biometric system, user identification occurs based on the matching score from the matching module. The claimed identity is either accepted as a genuine user or rejected as an imposter user.

2.2 Biometric System Operating Modes

The biometric system operates in two modes, as shown in Figure 2: enrollment and testing (verification/identification).

- ***Enrollment Phase***

During the enrollment phase, the extracted features vector set from the person's biometric trait called templates are stored digitally in the system's database. Biographic information (e.g., name, PIN, address) that distinguishes the user is also included. This phase, illustrated in Figure 2a, serves to register a new user or update an existing user's templates. Quality checks are implemented to ensure the input trait's quality. To address security and privacy concerns, templates are often stored in encrypted form in sensitive applications.

- ***Testing Phase***

In addition to enrollment, the testing phase of a biometric system serves one of two fundamental asks depending on the application context: verification (Figure 2b) or identification (Figure 2c). The term "recognition" is often used interchangeably with "identification."

- ***Verification (1:1): Am I who I claim to be?***

Verification is a binary classification task determining the authenticity of a claimed identity based on a one-to-one mapping with a new query feature vector set (e.g., "Does this biometric trait belong to Ravi?") in the following manner.

Given a feature vector set X_f and claim identity I, the task is to determine if $(I,\ X_f)$ belongs to the "Genuine" class c_1 or "Imposter" class c_2. Let X_I be the stored template analogous to the identity I . In this case, $X_f$is matched against X_I using a similarity function (S) and a predefined threshold ∂, leading to the decision rule given by equation 1.

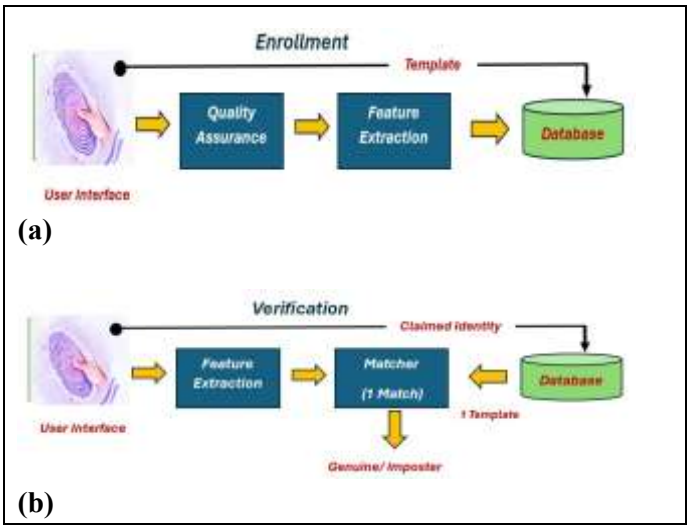
$$(I, X_f) \in \begin{cases} c_1 & if\ S(X_f, X_I) \geq \partial \\ c_2 & otherwise \end{cases} \qquad (1)$$

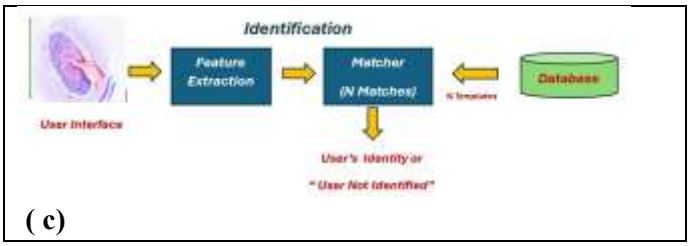
- ***Identification (1:N): Who am I***

In identification mode, a one-to-many mapping occurs between a new query feature vector set and all other stored templates in the database to determine the authenticity of the claim as genuine or imposter in the following manner:

Given a feature vector set X_f and claim identity I_k, k={1,2,…,N},where $I_1, I_2, \ldots, I_N$ are the classes enrolled in the database. We must ascertain whether $(I,\ X_f)$ belongs to the "Genuine" class or reject the sample if no correct class is identified, resulting in the decision rule specified by equation 2.

$$(I, X_f) \in \begin{cases} I_k & if\ max\left(S(X_f, I_k)\right) \geq \partial \\ Reject & otherwise \end{cases} \qquad (2)$$





(c)

Figure 2 Biometric System Modes (a) Enrollment (b) Verification (c) Identification

2.3 Historical Background and Significance of Biometric System

The earliest known reference to the term "biometrics" appeared in a 1981 article in The New York Times [10]. While humans have employed biometric methods, "automated" biometric technologies emerged with computer development. The earliest mention of non-automated biometrics dates back to prehistoric hand ridge patterns found in Nova Scotia's picture writing[10].

Biometrics, the study of human metrics, has ancient roots, tracing back to prehistoric times. Techniques for recognizing individuals based on physical or behavioral traits have existed for centuries. Facial recognition, an early and fundamental biometric, has been used since the dawn of civilization to distinguish between known and unknown individuals. However, "automated" biometric technologies emerged with computer development.

Table 1 highlights key historical moments in biometrics development.

Table 1: Time Line of Biometrics

Time Line	Description
500 BC	The first fingerprints recorded were used in ancient China on clay seals.
1800S	In the 1800s, notable progress in biometrics occurred with the rise and fall of the Bertillon system, the inception of Henry's fingerprint classification system, and the establishment of dedicated fingerprint databases.
1858	Sir William Herschel, a member of the Civil Service of India, pioneered the development of the first standardized hand image system.
1870	Alphonse Bertillon introduced "Bertillonage" or anthropometry, a system for identifying individuals through body measurements, physical descriptions, and photographs.
1892	Sir Francis Galton's fingerprint study proposed a 10-finger classification system, and his minutiae-based identification approach remains in use today.
1896	Bengal Police's Sir Edward Henry collaborated with Sir Francis Galton to create an efficient fingerprint classification and storage method.
1900s	In the 1900s, major biometric breakthroughs included iris and hand geometry for identification, and the rise of facial recognition.
1903	The New York Civil Service Commission introduced applicant fingerprinting, which was later adopted by the state prison system. In 1904, fingerprint bureaus were established by the St. Louis police and the U.S. Penitentiary.
1907	The Palm System developed by Hungarians was used in criminal cases.
1921	FBI establishes a fingerprint analysis department.
1936	Ophthalmologist Frank Burch initially suggested employing iris patterns for identification.
1960	Swedish professor Gunnar Fant's model explained the physiological aspects of acoustic

	speech production, aiding speaker recognition.
1969	FBI sought automation for fingerprint identification due to the overwhelming manual process. NIST identified challenges in scanning and comparing minutiae.
1970	Researchers Goldstein, Lesk, and Harmon automated facial recognition using 21 markers, computed manually in the 1970s and Dr. Joseph Perkell expanded acoustic speech production understanding with motion X-rays.
1974	First-hand geometry recognition systems emerged, serving time tracking, identification, and access control.
1975	FBI funding for minutia scanners led to a prototype reader, that stored only fingerprint minutiae due to high digital storage costs.
1976	Texas Instruments led the development of the first speaker recognition system, subjected to testing by MITRE and the US Air Force.
1980	To study and promote speech processing a group was formed refer as NIST Speech group that conduct annual evaluations for industry advancement.
1985	David Sidlauskas patented the concept of hand geometry identification.
1988	The Los Angeles County Sheriff's Department, specifically the Lakewood Division, employed video images for database searches. Furthermore, researchers Sirovich and Kirby employed principal component analysis in facial recognition, illustrating that fewer than 100 values were necessary for a normalized facial image approximation.
1991	Turk and Pentland found residual error applicable to facial detection using eigenfaces, enabling real-time automated recognition, despite environmental constraints.
1992	The Biometric Consortium established by NSA, involving government agencies, private industry, and academics to enhance biometric testing, interoperability, and standards.
1993	The FERET (Face Recognition Technology Evaluation) from '93 to '97 evaluated face recognition prototypes, fostering their commercial transition.
1994	In 1994, Dr. John Daugman patented iris recognition, a forerunner of modern solutions. Lockheed Martin triumphed in the IAFIS competition for fingerprint identification. ECOWARE Ltd., later acquired by Lockheed Martin, developed the first system supporting fingerprints and palm prints. In the same year, IN-SPASS, a biometric implementation based on hand geometry data, was introduced to enable eligible travelers to bypass immigration lines at select US airports but was discontinued in 2004.
1996	The Atlanta Olympic Games employed hand geometry for Olympic Village access, enrolling 65,000+ people, and processing one million transactions over four weeks. Additionally, in 1996 the NSA funded NIST for yearly speaker recognition evaluations.
1997	The NSA sponsored the Human Authentication API, the first standard for commercial biometric interoperability, laying the foundation for future standardization protocols.
1999	The International Civil Aviation Organization studied biometric technology compatibility with MRTD inspection processes to assess its potential as an international standard. Concurrently, the FBI's open-set fingerprint identification system, IAFIS, addressed information exchange challenges.
2000S ***In the 21st century, biometrics has advanced significantly, with faster and more efficient systems, growing social acceptance of facial recognition, and common mobile biometric solutions.***	
2000	The inaugural FRVT tested multiple commercial biometric systems on a large scale. The FBI and West Virginia University introduced the first Biometric Systems bachelor's program, though it wasn't accredited.
2001	The facial recognition system during the 2001 Super Bowl produced twelve false positives and no true positives.
2002	ISO formed a biometric subcommittee for standardization promoting data exchange. M1 Technical Committee on Biometrics (US Technical Advisory Group) developed

	ANSI standards. FBI's Next Generation IAFIS developed requirements for a national palm print service.
2003	The US National Science & Technology Council formed a Biometrics Subcommittee, overseeing research, development, policy, outreach, and global collaboration. ICAO adopted a biometric data integration blueprint for passports, favoring facial recognition. The European Biometrics Forum aimed to make the US a global biometric industry leader.
2004	The US-VISIT program integrated biometrics like digital photos and inkless fingerprints for visa holders. Simultaneously, the Department of Defense implemented ABIS, employing iris images, voice samples, DNA, and mugshots to identify national security threats. President Bush's Homeland Security Presidential Directive 12 mandated federal government employees and contractors to have identification cards with two fingerprints. In 2004, California, Rhode Island, and Connecticut established palm print databases for law enforcement.
2008	In 2008, Google introduced voice search in BlackBerry and Nokia phones using the Google Mobile app, later added to the iPhone in November. Additionally, the DoD and FBI began developing next-gen databases encompassing fingerprints, palm, face, and iris data.
2009	Hungary introduces biometric passports, while Hitachi pioneers a finger vein scanner.
2010	In March 2010, Google Voice Search beta integrated into YouTube, offering automatic captions for English-speaking hearing-impaired users. Biometrics aided in identifying a terrorist involved in 9/11 planning.
2011	In 2011, Siri was introduced, providing iPhone users with voice-controlled digital personal assistance. During the same year, the CIA utilized DNA and facial recognition to authenticate Osama bin Laden's remains with a 95% certainty.
2013	Touch ID, introduced by Apple, was featured on the 5S, 6, 6+ phones, iPad Air 2, and Mini 3.
2014	A vein scanner is showcased at a Hungarian Stadium.
2015	Microsoft introduced Cortana as its rival to Siri, a personal productivity assistant that responds to voice commands and utilizes machine learning.
2016	Hungary implements biometric ID cards, and Windows Hello in Windows 10 offers secure facial or fingerprint sign-in.
2017	Israeli researchers authenticate signatures with wearables like smartwatches. BioWatch develops a fully functional wearable secured by wrist vein patterns for payments, access control, and more. In IoT, biometrics support identity in homes, workplaces, and automobiles. Smart speakers like Amazon Echo and Google Home offer voice biometrics opportunities. Jaguar and Land Rover patent a biometric system for car access with facial and gait recognition, while other automakers integrate sensors into vehicle parts.
2018	In 2018, the first MasterCard Biometric Card combined chip technology with fingerprints for in-store purchases. Byton introduced an electric vehicle with integrated face biometrics, unlocking the door and loading the driver's profile upon sitting, enabling control through gestures and voice commands.
2020S	Biometric authentication is set to fully integrate in the 2020s, driven by high security. Applications with difficult-to-counterfeit traits are advancing, boasting over 99% effectiveness in hardware scanners. Improved algorithms and emerging options like heart rate and gait detection may lead to a passwordless society by 2030. The global biometric market revenue is expected to rise steadily, promising an exciting future for this technology with a rich history.

Advancements in computer technology and image processing techniques in the 20th century led to the development of additional modalities like facial recognition, iris recognition, and voice recognition. These modalities offer distinct advantages, including high accuracy, convenience, and resistance to forgery.

The significance of biometric-based systems lies in their ability to provide reliable and secure identification methods. Traditional identification methods, such as passwords or PINs, can be easily compromised, leading to unauthorized access or identity theft. Biometric systems address these concerns by utilizing unique traits that are difficult to duplicate. Biometric identification systems strike a balance between security and privacy, offering robust identification solutions for diverse sectors such as law enforcement, access control, and financial services.

3. Biometric Modalities

Every human being is naturally endowed with numerous physiological or behavioral characteristics that can be deemed as biometric identifiers. Any human characteristics chosen as biometric identifiers must adhere to the seven factors introduced by [11].

3.1 Pre-requisites of Good Biometrics

Biometric identifiers are unique and measurable characteristics employed to identify and describe individuals. The use of biometric identifiers is application-dependent. In other words, certain biometrics may be more suitable than others depending on specific levels of security and convenience [9]. No single biometric stands out significantly for all possible applications [11]. Biometric identifiers establish a significant and strong link between the user and their identity [14][15]. Choosing a specific biometric for a particular application requires considering and assigning weight to several factors [5][8][12], as outlined below in Table 2 :

Table 2: Seven Pillars of Biometric System

1	Universality	The extent to which the biometric trait is present in all individuals.
2	Uniqueness	The degree of distinctiveness of the biometric trait within individuals, minimizes the chance of false matches.
3	Permanence	The stability and consistency of the biometric trait over time.
4	Collectability	The ease with which the biometric trait can be measured or captured.
5	Performance	The speed and efficiency of the biometric system in terms of enrollment, identification, and verification.
6	Acceptability	The willingness of individuals to use and adopte the biometric system.
7	Circumvention	For enhanced security, a system should be more resistant to identity management system circumvention.

3.2 Types of Biometrics

Biometric modalities are commonly categorized into physiological or behavioral characteristics, as depicted in Figure 3[13]. Physiological biometrics comprise recognition through hand, face, ear, eye, fingerprint, and DNA. Behavioral biometrics are linked to an individual's conduct, covering various aspects such as typing rhythm (keystroke), signature, and voice, among others[8].

Physiological biometrics involve measuring features directly from parts of the human body, extracted using specific equipment and techniques. On the other hand, behavioral biometrics pertain to measurements derived from human actions[13]. In terms of acquisition, behavioral biometrics require measurements taken over a specific period, which is a crucial factor. These modalities capture and analyze specific traits or patterns to establish a person's identity.

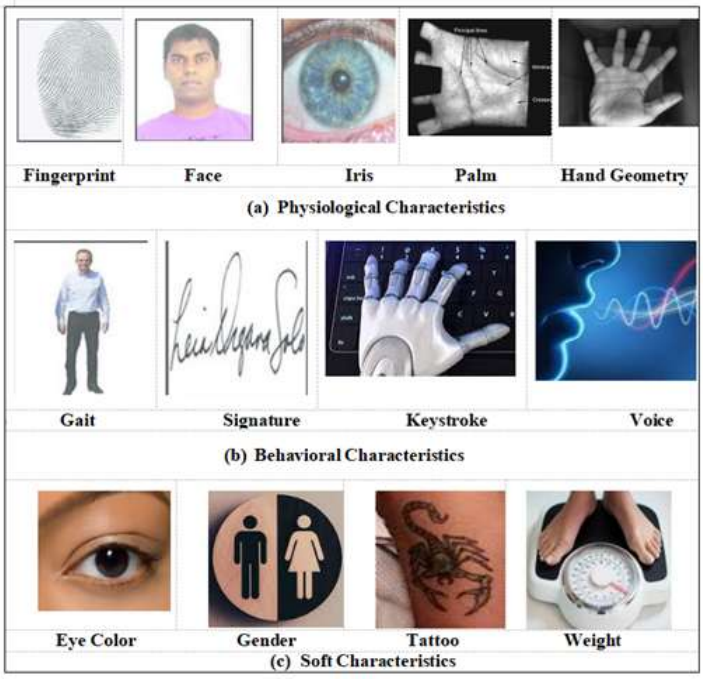


Figure 3: Biometric Modalities: (a) Physiological (b) Behavioral, (c) Soft Biometrics

3.2.1 Physiological Biometric Modalities

Human physiological characteristics encompass fingerprint, hand geometry, iris, retina, DNA sequence, heartbeat, finger surface, finger knuckle point, and various other traits. Moreover, the predominant technologies in commercial biometrics rely on the measurement of physiological features, which remain stable and unchanged over time.

Below are some widely accepted popular biometric identifiers:

- *Face:*

The human face stands out as a highly natural and robust biometric identifier, attributed to its inherent ability to recognize fellow beings through facial expressions. Consequently, it has been a captivating subject for researchers for centuries [16]. Because of the nonlinear arrangement of human faces, they can be viewed as a complex pattern recognition problem and constitute a developing area of research in computer vision applications [17].

Face recognition systems utilize the spatial relationships among facial features and global appearance. They operate in verification and identification modes. Verification compares a query face with a template, while identification maps a query face to multiple stored templates, revealing its identity by comparing it against the entire database of face templates. In instances where the test individual is absent from the database, the Face Recognition Vendor Test (FRVT2002) [18] addresses this scenario. The query face is compared to every stored face template, with computed scores ranked numerically. If the highest score exceeds a preset threshold, an alarm is triggered.

In less than ideal conditions, face recognition system accuracy may be affected by factors such as lighting, facial expressions, pose, occlusion, and time delay, posing challenges despite its success in controlled environments. [19].

- *Fingerprint:*

Fingerprints, emphasized for 5000 years, stand as a historically reliable biometric for identification[20]. Originating from friction ridges on fingertips, their convenience and high accuracy have been utilized throughout history. These distinct patterns, formed during fetal development, ensure individuality, making fingerprints a robust tool in forensics for distinguishing between genuine individuals and impostors[21].

Fingerprint recognition, the oldest and widely recognized biometric method is a modern, digitized version of the traditional ink-and-paper system employed by law enforcement for identification.

Fingertip skin has raised ridges and valleys, creating unique patterns known as fingerprints for biometric recognition. Key features include arches, loops, and whorls, depicted in Figure 4. The core (center point) and delta (divergence point) act as recognition features, aiding in aligning and matching fingerprints. However, it's crucial to acknowledge that not all fingerprints may exhibit these features. [22].

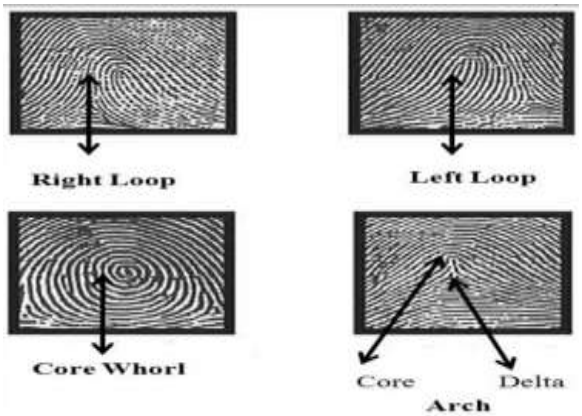


Figure 4: Fingerprint pattern: Loop, Whorl, and Arch [28]

In fingerprint recognition, "*minutiae*", refers to minor features causing disruptions in ridge flow: classified into endings and bifurcations, where ridges stop or split [18][22] as shown in Figure 5. In such systems, a high-quality image is collected using optical, silicon, or ultrasound sensors. In the optical sensor, the user places her/his finger on the platen and a laser light illuminates the fingerprint, reflecting off ridges and converting it to a digital signal.

Moreover, the mapping of extracted fingerprint features can be achieved through three methods: ridge, correlation, and minutiae.

i. Ridge feature-based fingerprint matching involves acquiring ridges using an innovative method.

ii. Fingerprint matching based on correlation overlays two fingerprint images, evaluating the relationship between equivalent pixels.

iii. Fingerprint matching based on minutiae stores a plane containing pixel points, which are compared and matched with the corresponding set of points in the template.

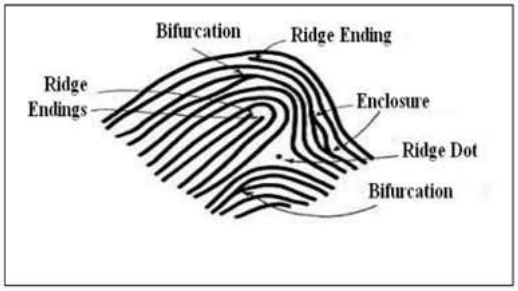


Figure 5: Minutiae [28]

The finger knuckle print is valuable for individual characterization, serving as another biometric approach that has shown significant expansion for specialists in recent years[23].

- *Hand Geometry:*

Human hands offer rich textures for early identification, including fingerprints, palmprints, finger surfaces, nails, and knuckle points. Hand geometry, particularly, stands out as a strong, simple, accessible, and cost-effective biometric gaining attention from researchers.

Hand geometry systems, with the longest implementation history, were patented by David Sidlauskas in 1985, becoming commercially available the following year. The 1956 Olympic Games implemented hand geometry systems to regulate and secure physical access to the Olympic Village (NSTS, 2006).

After a certain age, each person's hand maintains a distinct and unchanging shape. Hand-based identification relies on extracting features like finger length, width, and area, offering accuracy despite environmental factors. This method is cost-effective as hand images can be easily captured using webcams or smartphones, serving as an alternative to traditional biometric scanners. [9] [24] [25].

- *Palmprint:*

Similar to fingerprint and hand geometry, palm-print is a biometric extracted from the human hand with rich features, making it effective for identification based on distinguishable characteristics[25].

In general, a palm-print includes:

- Principal lines: The heart line, life line, and head line.
- Regions: Finger-root (I), inside region (II), and outside region (III).
- Datum points: End-points and their mid-points across the palm.

Additional features:

- Geometry features: Width, length, and area of the palm.
- Wrinkle features: These lines, distinct from principal lines, are thinner and more irregular, classified as coarse wrinkles and fine wrinkles.
- Delta point features: The palm-print exhibits a delta-like region defined as the center.
- Minutiae features: Resemble features found in fingerprints.

- *Iris:*

Certainly, the iris is a minimally invasive biometric trait gaining attention for personal identification. Positioned between the black pupil and white sclera, the human iris exhibits intricate details, including coronas, stripes, freckles, crypts, and furrows, making it highly accurate and distinctive [26][27].

A user's cooperation is crucial in iris-based identification systems, requiring proper positioning of the iris in the specified location relative to the camera's focal plane and controlled brightness for optimal results. Renowned for its reliability, government agencies often employ this highly secure biometric system in high-security environments.

- *Ear:*

Ear biometrics is a promising passive method for person identification. This biometric recognition analyzes the shape of the outer ear, ear lobes, and bone structure using both 2D and 3D methodologies. A sensor captures a side profile image, and an algorithm locates and isolates the ear from surrounding elements using color and depth analysis. It accounts for variations in skin tone, ear size, shape, hair occlusion, and earrings[28]. Unlike the face, it remains unaffected by expressions and makeup. However, hair presence and changes in brightness can pose challenges, addressed by researchers using thermogram imagery [29].

- *DNA:*

DNA, or Deoxyribonucleic Acid, serves as a one-dimensional unique code defining individuality. Its distinctive patterns allow for identification through hereditary variations, prominently used in forensic applications for person identification.

Two DNA profiles are compared: one from the crime scene and another from a suspect. If unmatched, the suspect is unlikely the source. If matched, further verification is needed to confirm the sample's source. The number of loci compared determines significance. The probability of exact matches in ten or more loci between different individuals is one in one billion, excluding identical twins.While reliable and secure, DNA-based identification systems have limitations. They cannot be used for online identification, and identical twins may share the same DNA sequencing.

Table 3 elaborates on the comparative analysis of the strengths, weaknesses, common application areas, and current challenges of some popular physiological biometric modalities.

Table 3: Comparative Analysis of Physiological Biometric Features

S. NO	Physiological Feature	Strengths	Weakness	Applications	Current Challenges
1	Face	• Non-intrusive and user-friendly. • Suitable for large-scale identification.	• Vulnerable to variations in lighting and pose. • Potential for false positives and negatives.	• Security systems, • Mobile devices, • Surveillance, • Access control.	• Ensuring accuracy across diverse demographics. • Addressing ethical concerns related to privacy and surveillance
2	Fingerprint	• High accuracy and reliability. • Established and widely adopted.	• Susceptible to wear, damage, or latent prints. • Some people may have difficulty providing clear fingerprints.	• Law enforcement, • Border control, • Smartphones, • Access control.	• Dealing with latent prints. • Improving resistance against spoofing techniques.
3	Hand Geometry	• Non-intrusive and easy to use. • Stable over time for most individuals. •	• Limited distinctiveness for some users. • Vulnerable to intentional variations. •	• Physical access control systems. •	• Enhancing accuracy for diverse hand shapes and sizes. • Improving resistance against spoofing.
4	Palmprint	• Unique Patterns and difficult to forge. • Can be combined with other biometrics.	• Limited acceptance compared to fingerprints. • Sensitivity to variations in hand	• Access control. • Identity verification.	• Sensitive to hand orientation and varied acceptance.

			orientations.		
5	Iris	• High accuracy and stability over time. • Resistance to changes in lighting conditions.	• Requires specialized hardware. • Vulnerable to occlusions.	• High-security environments, • Access control.	• Cultural hesitations related to eye scanning. • Improving performance in unconstrained environments.
6	Retina	• High accuracy and uniqueness. • Difficult to replicate.	• Invasive and requires proximity for scanning. • Health and safety concerns for some users.	• High-security environments. • Critical infrastructure	• Limited acceptance due to invasiveness and health concerns.
7	Ear	• Unique Structure: Ears have distinct features. • Stable Over Time: Ear shape remains relatively constant.	• Hair presence: Hair on the ear can pose challenges • Environmental Factors: Brightness changes may affect the accuracy.	• Security Access: Used for person identification in secure environments. • Forensic Applications: Assist in criminal investigations.	• Hair interference • Environmental Sensitivity.
8	DNA	• Boasts the utmost precision. • The likelihood of two individuals possessing identical DNA profiles is less than one in a hundred billion.	• The sample collection is a time-consuming process. • Provides a lot of info but has privacy problems and needs lots of storage. • Results can be affected by contamination. • Expensive, Poor convenience, and no quick matching.	• Proving guilt or innocence. • Physical and network security	• Privacy concerns, lengthy analysis, high costs, potential sample contamination, and limited real-time applications are challenges with DNA.
9	Vein Pattern	• Difficult to spoof due to the internal nature of veins. • Stable and unique patterns.	• Requires specialized imaging devices. • Limited public acceptance.	• Limited adoption; potential in secure environments.	• Developing cost-effective and user-friendly devices. • Addressing concerns related to medical data privacy.

These summaries provide insights into the strengths, weaknesses, applications, and challenges associated with various physiological biometric features. It's important to note that ongoing research and technological advancements aim to address these challenges and enhance the overall effectiveness of biometric systems.

3.2.2 Behavioral Biometric Modalities

Individual behavioral traits, derived from sociological behaviors like gait, signature, lip motion, body language, and handwriting, serve as biometric features for personal identification, as discussed in this section.

- *Signature:*

Each person's unique signature style serves as a distinct biometric characteristic, offering a reliable mode of biometric recognition. The initial signature recognition system was developed by North American Aviation in 1965. Signatures, long used in government for legal and commercial transactions, evolved from offline to online systems, incorporating dynamic signature concepts [30] [31].

Signature verification utilizes a specialized pen or tablet connected to a computer to analyze both the visual image and the signing process. Behavioral characteristics like size, duration, speed, pressure, and stroke directions are extracted during data acquisition, forming an enrollment template for future comparisons. Signatures are categorized as online (captured electronically with dynamic features) and offline (processed from saved images). Dynamic signatures, a widely used biometric, require multiple samples for accurate verification, offering security in forensic applications. [32].

- *Gait:*

Individuals' walking styles, or gait, differ and can serve as a biometric for personal identification. Though collecting gait data is less convenient, it is considered trustworthy. Factors like mood or injury can affect an individual's gait, posing concerns. However, favorable results, achieving a 95% recognition rate, have been reported in gait-based identification systems [33].

- *Voice:*

Voice or speaker biometrics relies on an individual's voice for identification, incorporating features influenced by the vocal tract's physical structure and behavioral characteristics. It serves as both a behavioral and physiological biometric, taking into account vocal tract and facial features. Voice recognition systems encompass text-dependent, where users speak a set phrase, and text-independent, which requires no specific phrase. While text-dependent systems enhance accuracy through repeated passphrase enrollment, text-independent systems offer increased security against abuse, albeit with greater design complexity [28]. Recognition involves transforming sound waves into feature vectors, comparing them for similarity without direct voice comparison, and determining a match based on pattern analysis [34].

- *Handwriting:*

Handwriting, a widely used behavioral biometric, is primarily applied in forensic document examination for person identification. Both online [35] and offline [36] handwriting methods have been introduced to ascertain individual handwriting traits [37]. Extracting features from a handwritten document involves analyzing the shape and size of letters, pen strokes, loops, and crossed lines.

- *Keystroke:*

Keystroke biometrics verifying individual identity through typing rhythm, accommodates both trained and amateur typists, enhancing security when used with passwords. It can verify users at log-on or continually monitor. Although not uniquely individual, it offers adequate discriminatory data for identity authentication [38]. Keystroke, a behavioral biometric, varies among individuals. Monitoring keystrokes can be unobtrusive,

revealing distinctive patterns [8].

Keystroke biometric system implementations are cost-effective and user-friendly compared to other biometrics [39]. Features, based on time durations and neural networks, facilitate identity association. Commercial systems leveraging these dynamics are emerging [40][41]. However, susceptibility to user mood and fatigue makes them less robust.

The comparative analysis of the strengths, weaknesses, common application areas, and current challenges of some popular behavioral biometric modalities is tabulated as in Table 4:

Table 4: Comparative Analysis of Behavioral Biometric Features

S. NO	Behavioral Feature	Strengths	Weakness	Applications	Current Challenges
1	Signature	• Behavioral aspects add a layer of security. • Capture unique characteristics of the signing process.	• Vulnerable to variations in signing habits. • Requires dynamic signature data for accuracy.	• Document authentication, • Financial Transactions.	• Developing standardized metrics for signature dynamics • Addressing variations due to fatigue or health conditions.
2	Gait	• Non-intrusive and can be captured at a distance. • Difficult to spoof as it involves a unique pattern.	• Affected by changes in footwear or walking surface. • Limited accuracy in unconstrained environments.	• Security systems, • Surveillance, • Access control.	• Improving accuracy in unconstrained environments. • Addressing ethical concerns related to surveillance
3	Voice	• Non-intrusive and can be captured remotely. • Offers natural and convenient user interaction.	• Susceptible to environmental noise and variations in speech. • Vulnerable to voice mimicking or replay attacks.	• Phone authentication, • Voice assistants, • Security Systems.	• Enhancing accuracy in noisy environments. • Improving resistance against voice spoofing.
4	Handwriting	• Unique individual characteristics, • Non-intrusive.	• Susceptible to variations, • Forgeries	• Document authentication, • Signature verification access.	• Increased digital communication reduces reliance, • Potential security concerns, • Adaptability to evolving technology.
5	Keystroke	• Continous authentication during user interaction.	• Sensitive to changes in typing behavior.	• Computer access. • Online	• Balancing security with user convenience.

		• Non-intrusive and transparent to the user.	Limited accuracy for short text inputs.	Authentication	• Addressing variations in typing behavior over time.

3.2.3 Soft Biometric Modalities

Biometric systems automatically identify individuals based on physiological or behavioral features like fingerprints, faces, gaits, and keystrokes. These systems can be either single (unimodal) or multimodal, addressing issues such as non-universality and sensor noise. While multimodal systems offer enhanced reliability, they often require extensive verification time, causing user inconvenience.

Soft biometrics enhance biometric systems by incorporating ancillary information like gender, blood group, height, weight, age, ethnicity, and eye color. This additional data, collected during enrollment, aids in distinguishing genuine individuals from impostors in the identification phase, reducing manual intervention and enhancing overall system performance [42].

Soft biometric features alone are indistinct and unreliable, making them insufficient for identity verification. However, when integrated with primary biometric systems, they significantly enhance overall performance [43], as documented in various literature [44] [45].

3.3 Comparison of Biometric Modalities

A comparison study of the most widely adopted traits is presented in Table 5 categorized them into High (H), Medium (M), and Low (L) perception levels., focusing on the characteristics of biometric entities[46].

Table 5: Comparison of Biometric Modalities based on Characteristics of Biometric Modalities

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facialthermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

3.4 Unimodal and Multimodal Biometrics

A biometric security system identifies an individual based on their physiological or behavioral features, such as fingerprints and facial characteristics.

These systems can be broadly categorized as either unimodal or multimodal biometric systems. Unimodal biometric systems utilize a single source of biometric features, like fingerprints, iris scans, or palm prints, to establish an individual's

identity. On the other hand, multimodal biometric systems employ multiple sources of biometric information, such as combining face and ear features, fingerprints, and palm prints, or integrating two fingerprints (like left and right index fingers). Multimodal systems have gained widespread popularity over unimodal counterparts [4].

3.4.1 Limitations of Unimodal Biometric Systems

In the early stages of the biometric era, single-identifier-based systems, known as 'unimodal biometric systems,' emerged, offering enhanced security over traditional methods. However, each physiological and behavioral trait has its limitations, and technical issues such as noisy sensors during enrollment and environmental effects can compromise system integrity. These drawbacks, identified by [8] [47] as accuracy, scalability, security, and privacy issues, underscore the need for more robust solutions in the advancing digital age.

Limitations of unimodal biometric systems include susceptibility to interclass similarities, such as difficulties in distinguishing identical twins in facial recognition. Inaccurate matching, especially for identical twins, poses a challenge, as cameras may struggle to differentiate between subjects. Additionally, unimodal biometrics are vulnerable to spoof attacks, allowing for data forgery or imitation, as seen in fingerprint recognition where rubber fingerprints can be used to deceive the system. These limitations underscore the need for more robust and multimodal biometric solutions[49][50].

3.4.2 Multibiometrics Biometric Systems

Multibiometrics leverages two or more traits, such as facial images, fingerprints, iris scanning, hand geometry, and voice recognition, to identify individuals. Biometric systems use single or multiple sensors to measure these characteristics[51]. For enhanced accuracy, systems like face and iris combination exemplify multibiometrics, addressing the limitations of unimodal biometrics and improving overall performance.

Multibiometrics systems effectively tackle non-universality concerns inherent in unimodal systems, gaining widespread adoption in both governmental and civilian applications[52].

Multibiometrics encompasses multisensors, multiple algorithms, instances, samples, and multimodal approaches. In multisensors, multiple cameras capture diverse facial angles for a single trait. Multiple algorithms, like minutiae and texture processing for fingerprints, reduce hardware costs but increase complexity. Multiple instances involve various instances of the same modality, matching multiple fingerprint images or irises. Multisamples acquire multiple images of the same trait, like different fingerprint portions or facial angles. In multimodal, diverse modalities are combined, necessitating both hardware and software systems for processing[53].

Multibiometrics enhances identification reliability by combining information from various modalities. Fusion occurs at different levels: the sensor level integrates raw data from multiple sensors, the feature level fuses acquired data feature vectors, the matching level integrates match scores from different classifiers, and the decision level consolidates outcomes from multiple classifiers [48][54].

Figure 6 depicts the block diagram of fusion levels in a Multibiometrics system.

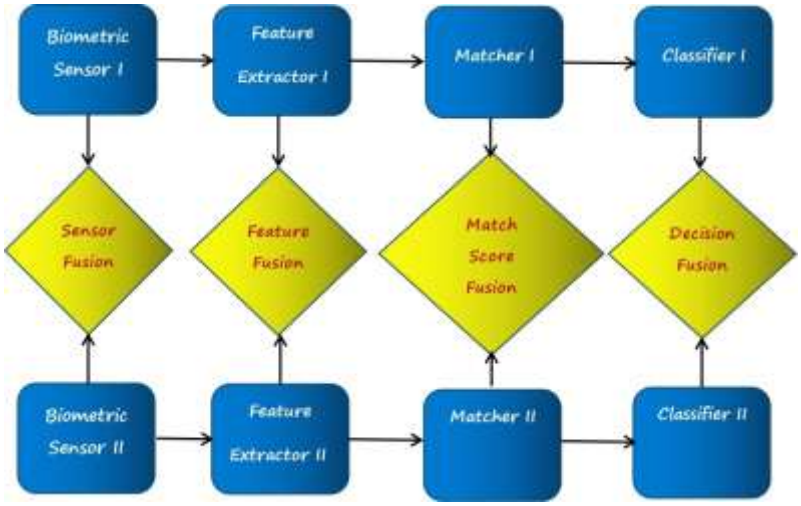


Figure 6: Multibiometrics Fusion Levels

A multimodal system has three different operational modes: serial, parallel or hierarchical. In serial mode, also called cascade mode, each methodology is assessed sequentially, reducing overall acknowledgment time.

Parallel mode processes information simultaneously from multiple modalities, with the final decision based on combined results. Whereas, multiple classifiers are organized into a tree structure, with a preference for hierarchical mode in scenarios with a large number of classifiers. Current multimodal biometric systems typically operate in either sequential or parallel mode, addressing issues like missing or noisy biometric data.

4. Biometric Data Acquisition and Feature Extraction

4.1 Biometric Data Acquisition

Biometric Data Acquisition is the collection of individuals' physiological or behavioral traits (e.g., fingerprints, facial features) for identification. Specialized sensors capture this data during enrollment or authentication in biometric systems.

Table 6 depicts the comprehensive overview of Biometric data acquisition techniques and devices along with the challenges, and considerations.

Table 6: Comprehensive Overview of Biometric Data Acquisition: Techniques and Devices, Challenges, and Emerging Technologies.

Biometric Modality	Techniques and Devices	Challenges and Considerations	Emerging Technologies
Face	3D cameras, infrared sensors, RGB cameras	Illumination variations, occlusions, privacy concerns	Deep learning for facial recognition, emotion-based recognition
Fingerprint	Optical sensors, capacitive sensors, ultrasonic sensors	Skin conditions, spoofing with fake fingerprints	3D fingerprint imaging, sweat-based biometrics
Hand	3D hand scanners,	Size and shape variations,	Thermal hand recognition, vein-based

Geometry	image-based systems	hygiene concerns	hand biometrics
Palm-Print	Contact and non-contact scanners	Image distortion, environmental factors	Multi-spectral palmprint recognition, 3D palmprint analysis
Iris	Near-infrared cameras, CCD cameras	Reflections, occlusions, non-uniform illumination	Multispectral imaging, mobile iris recognition
Retina	Retinal scanning devices	Invasive nature, hygiene concerns	Contactless retina scanning, mobile retinal recognition
Ear	2D and 3D ear scanners	Position variations, occlusions	Soft biometrics for ear recognition, earprint-based authentication
DNA	DNA sequencing devices	Privacy concerns, ethical considerations	Rapid DNA analysis, DNA computing for biometrics
Vein Pattern	Infrared light, near-infrared light	Environmental factors, image quality	Vein pattern recognition with NIR spectroscopy, contactless vein imaging
Signature	Digitizing tablets, stylus pens	Variability in writing style, forgeries	Behavioral signature analysis, dynamic signature recognition
Gait	Video cameras, motion sensors	Clothing variations, view angle changes	Deep learning for gait analysis, wearable sensor technology
Voice	Microphones, digital signal processing	Background noise, voice imitation	Behavioral voice recognition, anti-spoofing techniques
Handwriting	Digitizing tablets, pressure-sensitive pens	Variability in writing style, forgeries	Online signature verification,
Keystroke	Keyboards, typing pattern analysis	Variability in typing behavior, user cooperation	Continuous authentication, adaptive models

4.2 Biometric Feature Extraction and Representation

Biometric feature extraction involves the selection or enhancement of essential characteristics in a sample. This process typically relies on specific algorithms, with the method varying based on the type of biometric identification employed. It is the process of capturing and encoding distinctive characteristics from biometric data for subsequent analysis and comparison. This crucial step in biometric systems helps convert raw data into compact and discriminative templates for efficient matching.

Effective feature extraction is critical for accurate and efficient biometric identification. Table 7 elaborates on the most prominent feature extraction and representation approaches of some core biometric modalities.

Table 7: Some Common Biometric Feature Extraction Methods and Techniques

Biometric Modality	**Feature Extraction Methods**	**Representation Techniques**
Fingerprint [6]	Minutiae points, Ridge patterns	Minutiae-based templates, Ridge flow patterns
Face [55]	Eigenfaces, Local Binary Patterns (LBP)	Face vectors, LBP histograms
Iris [56]	Phase-based methods, texture analysis	Iris codes, Gabor wavelets
Hand Geometry [57]	Finger lengths, hand shape analysis	Geometric features, hand geometry codes
Palmprint [58]	Crease patterns, texture analysis	Palmprint features, wavelet transform
Retina [61][62]	Blood vessel patterns, shape, and pigmentation	Vascular tree, vascular graph, and statistical measures

Vein Pattern [59]	Near-infrared imaging, pattern analysis	Vein patterns, texture features
DNA [63]	DNA sequence analysis, SNP identification	Unique genetic code or numerical representation
Voice [60]	Mel-frequency cepstral coefficients (MFCC)	Voiceprints, spectrogram
Handwriting [64]	Stroke features, directionality, size, pressure.	Graphical representation, statistical measures
Signature [30]	Speed, pen pressure, pen tilt	Dynamic features, pressure distribution
Keystroke [38]	Key press timing, key hold time, flight time	Timing vectors, statistical features

5. Deep Learning Implication in Biometric System

Advances in deep learning and machine learning have also influenced feature learning, allowing systems to automatically extract discriminative features from raw data. In this segment of the paper, we showcase a researcher's exploration into the latest developments in utilizing deep learning frameworks for biometric recognition.

The face has become a extensively studied and popular biometric, especially in recent years. Its applications range from security cameras in airports and government offices to everyday uses like cellphone authentication, as demonstrated by the iPhone's Face ID. In the past, recognition involved various hand-crafted features such as LBP, Gabor Wavelet, SIFT, HoG, and sparsity-based representations [65][66][67][68][69]. Recognition involves both 2D and 3D face versions [70], with a predominant emphasis on 2D face recognition. A significant challenge lies in the face's vulnerability to changes over time, including aging or external factors such as scars or medical conditions [71].

Many studies utilize deep learning for face recognition. This survey provides a summary of some of the most notable endeavors in face verification and/or identification.

In 2014, Taigman and his team presented an early deep-learning approach for face recognition in their paper, DeepFace [72]. It achieved state-of-the-art accuracy on the LFW benchmark [73], approaching human performance under unconstrained conditions for the first time (DeepFace: 97.35% vs. Human: 97.53%). Trained on 4 million facial images, this work marked a significant milestone in face recognition, inspiring many researchers to adopt deep learning for this purpose. In the same year, Sun et al. introduced DeepID, a face verification method that utilized features from the last hidden layer of a deep convolutional network trained on approximately 10,000 face identities[74].

Several studies explore generative models for face image generation. A noteworthy model is Progressive-GAN [75], where Karras and his team introduced a framework that incrementally expands both the generator and discriminator of GAN. This technique allows the model to learn and generate high-resolution, realistic images. Several other studies have been suggested for face recognition.

In [76] Darlow et al. introduced MENet, a deep learning-based fingerprint minutiae extraction algorithm, showing promising results on FVC datasets. In [77], Tang et al. presented FingerNet, another deep-learning model for fingerprint minutiae extraction, incorporating feature extraction, orientation estimation, and segmentation to estimate minutiae maps. In [78], Lin and Kumar suggested a multi-view deep representation, using CNNs, for contactless and partial 3D fingerprint recognition. In [79], the authors create a deep learning framework for fingerprint texture learning, achieving verification accuracies of 100%, 98.65%, 100%, and 98% on PolyU2D, IITD, CASIA-BLU, and CASIA-WHT databases, respectively. In [80], Lin and Kumar suggested a multi-Siamese network for accurate matching of contactless and contact-based fingerprint images.

In [81], Kim and team introduced a fingerprint liveness detection method using statistical features learned from a deep belief network (DBN), achieving high accuracy on LivDet2013 test datasets. In [82], Nogueira and colleagues proposed

a convolutional neural network model for detecting fingerprint liveliness (real or fake), achieving 95.5% accuracy in the 2015 fingerprint liveness detection competition. In [83], Minaee and team introduced an algorithm for fingerprint image generation using a generative model, an extension of GAN called "Connectivity Imposed GAN".

In [84], Minaee and team showed that features extracted from a pre-trained CNN on ImageNet can achieve high accuracy in iris recognition, marking a pioneering application of deep learning in this field. In [85], Gangwar and Joshi introduced an iris recognition network based on a convolutional neural network, providing robust, discriminative, and compact results with very high accuracy, particularly excelling in cross-sensor recognition of iris images.

In [86], Xin and team introduced an early palmprint recognition approach using a deep learning framework. They built a deep belief network through top-to-bottom unsupervised training, achieving robust accuracy on the validation set. In [87], Zhao and collaborators introduced a unified deep convolutional feature representation for hyperspectral palmprint recognition. In [88], Shao and Zhong presented a few-shot palmprint recognition model utilizing a graph neural network. Palmprint features from a convolutional neural network are transformed into nodes in the GNN, with edges representing similarities between image nodes.

Ear recognition, an emerging field, is expected to witness a growth in biometric recognition studies. Despite lagging behind face, iris, and fingerprint recognition in popularity, ear recognition faces challenges due to limited dataset sizes. Zhang et al. [89] introduced few-shot learning methods to enable networks to rapidly learn image recognition with limited training data. Dodge et al. [90] proposed transfer learning for unconstrained ear recognition. Emersic et al. [91] introduced a deep learning-based averaging system to tackle overfitting in small datasets. In [92], the authors presented the first publicly available CNN-based ear recognition method, experimenting with diverse strategies and architectures for optimal configurations.

Before the advent of deep learning, i-vector systems [93] were prevalent in speaker recognition, utilizing factor analysis to represent speaker and channel variabilities in a low-dimensional space. Recently, there's a rising inclination towards incorporating deep learning in speaker recognition. During this period, the introduction of d-vector in [94] aimed to tackle text-dependent speaker recognition using neural networks. Numerous papers delve into end-to-end approaches employing neural networks. In [95] and [96], neural networks handle pairs of speech segments, classifying match/mismatch targets. In [97], the author suggests the Generalized end-to-end (GE2E) loss, which is similar to triplet loss, for text-dependent speaker recognition, employing an in-house dataset.

Numerous studies investigate deep learning applications in fingerprint [98][99], iris [100][101][102], palmprint [103][104][105], ear [106][107], voice [108][109][110][111], signature [112], gait recognition [113][114], and more. Ongoing research and technological advancements aim to improve the robustness and security of biometric feature extraction methods

6. Performance Evaluation and Benchmarking

Evaluating biometric systems is crucial to assess their accommodation of unique properties. Examining performance metrics for verification and identification systems aids in judging their appropriateness for specific applications.

6.1 Metric for Evaluating Biometric System Performance

6.1.1 Verification Performance Metrics

Pattern recognition systems may encounter two errors: False Acceptance Rate (FAR) and False Rejection Rate (FRR). When feature vectors show similarity, a matching score is generated. For dissimilarity, if the score is below (above) the threshold, the feature vectors are considered matched.

- *False Acceptance Rate(FAR) or False Match Rate (FMR):*

False Acceptance Rate (FAR) measures the likelihood of the system incorrectly matching an input pattern to a non-matching template in the database. It depends on the specified threshold and is given by:

$$FAR=\frac{M}{N}\times 100\ \% \qquad (3)$$

Where, N represents unique instances of imposter matches and M denotes the count of individuals incorrectly identified as genuine matches.

- *False Rejection Rate (FRR) or False Non-Match Rate (FNMR):*

The framework's failure to detect a match between data and a template is reflected in the False Rejection Rate (FRR). FRR assesses the proportion of valid inputs inaccurately dismissed, indicating the chance of mistaking a genuine user for an imposter.

$$FRR=\frac{M}{N}\times 100\ \% \qquad (4)$$

Where N denotes unique valid matches performed, and M represents cases mistakenly rejected as imposter matches.

- *Equal Error Rate (ERR):*

EER, also known as the Crossover Error Rate (CER), quantifies the point where acknowledgment and rejection errors balance. Evaluated using the ROC curve, it swiftly compares device accuracy, with lower EER indicating higher precision.

- *Accuracy (A):*

If T is the threshold yields the minimum average False Acceptance Rate (FAR) and False Rejection Rate (FRR) across various thresholds, the accuracy at θ can be defined as:

$$A=\left(100-\frac{FAR_T+FRR_T}{2}\right)\times 100\ \% \qquad (5)$$

Where, FAR_T and FRR_T represent Acceptance Rate and Rejection Rate at a specific threshold. The optimal threshold is the one that maximizes accuracy by balanci
ng these two rates.

- *Receiver Operating Characteristics (ROC):*

The ROC plot visually illustrates the trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR). It showcases the system's discriminative power, aiding in comparing biometric system performance effectively.

6.1.2 Identification Performance Metrics

Evaluation of an identification system involves analyzing performance through metrics like Correct Recognition Rate (CRR) and examining the genuine versus non-genuine (imposter) best match graph.

- *Correct Recognition Rate (CRR):*

Also known as Rank 1 accuracy, it is the ratio of correct top best matches to the total matches in the query set. Specifically, if M correct matches are found in a test set of N images, the CRR is expressed as:

$$CRR=\frac{M}{N}\times 100\ \% \qquad (6)$$

- *Genuine Vs Imposter Best Match Graph (GvI Graph):*

GvI visually represents the separation between genuine and non-genuine matching scores for all probe images by plotting their best genuine and imposter scores, allowing for visual analysis of the score separation

6.2 Datasets and Evaluation and Protocols for Benchmarking

Biometric datasets and evaluation protocols are essential for benchmarking the performance of biometric systems. These datasets contain biometric samples, such as fingerprints or facial images, and the evaluation protocol outlines the procedures and metrics used to assess the accuracy and effectiveness of biometric identification algorithms. The benchmarking process helps compare and improve the performance of different biometric systems, ensuring reliable and standardized evaluations in the field.

Benchmarks are categorized into specific areas based on the addressed (sub)problem and the adopted evaluation protocol. For instance- FVC-onGoing offers diverse benchmarks for assessing recognition algorithms. Each benchmark uses a isolated dataset that remains unchanged over time. Any new datasets will create separate benchmarks or new versions of existing ones, and comparisons will only be made on the same data.

Some popular biometric modalities and their datasets are listed in table 8.

Table 8: Popular Biometric Modalities's Datasets

Biometric Modality	Database Name	Database Size (Number of Images)
Fingerprint	• FVC Fingerprint[115] • Poly U High Resolution Fingerprint [116] • CASIA Fingerprint[117] • NIST Fingerprint [118]	• FVC2002(DB1,DB2,DB3) • FVC2004(DB4) • 1480 • 20,000(500 subjects) • 258 Latent Fingerprints
Face	• Yale Face Database [119] • CMU Multi-PIE [120,121] • LFW(Labeled Faces in the Wild Database) [73] • Poly U NIRFD Database[122] • VGGFace 2[123] • Casia Web Faces [124] • MS-Celeb[125] • Celeb-A [126] • MegaFace[127]	• 5760 • >750000 • >13000 • 34000 • 3.31 million from 9131 subjects • 453,453 • 10 million face images • >200K • 1 million images from 690K identities
Iris	• CASIA-Iris-1000[128] • UBIRIS [129] • IIT Delhi iris database[130] • ND-CrossSensor-Iris-2013[131] • Mobile Iris Challenge Evaluation (MICHE)[132]	• 20,000(1000 subjects) • UBIRIS.v1 (1877) and UBIRIS.v2 (11000) • 2240 (224 subjects) • LG2200(116,564) and LG4000(29,986[676 subjects]). • 3732 (92 subjects)
Palmprint	• PolyU dataset [133] • CASIA Palmprint[134] • IIT Delhi palmprint[135] (hand images)	• 6000(500 subjects) • 5502(312 subjects) • 235 subjects
Ear	• IIT Ear Database [136] • AWE Ear Database [137]	• 471 • 1000

	• UERC Ear Database[138] • WPUT Ear Dataset [139]	• 11804 • 2071
Voice	• NIST SRE[140] • SITW[141] • VoxCeleb[142]	• SRE 2016 and SRE 2018 (2 popular datasets) • Recordings of 299 speakers with an average of 8 different sessions per person • VoxCeleb1 (100,000 utterances for 1,251 celebrities) and VoxCeleb2 (millions utterances for 6,112 identities)
Signature	• ICDAR 2009 Signature[143] • SVC2004[144] • Offline GPDS-960 Corpus [145]	• NFI-offline (authentic signatures-100, forged signatures-33) and NLDCC-online (signature files: online-1953 , offline-1953) • Signature -100 sets(each set contains 20 genuine signatures) and 20 skilled forgeries. • 960 subjects(authentic signatures-24, forgeries signature-30)
Gait	• CASIA Gait Database [146] • Osaka Treadmill Dataset[147]	• Casia 4 Subsets: Dataset A (standard dataset), Dataset B (multi-view gait dataset), Dataset C (infrared gait dataset), and Dataset D (gait and its corresponding footprint dataset). • 4007 subjects (4 subsets): dataset A: Speed variation, dataset B: Clothes variation, dataset C: view variations, and dataset D: Gait fluctuation.

7. Conclusion and Future Perspect

In this data-driven age, where data is being abundantly generated and utilized for important decisions, a robust user authentication system is very important for access control and safeguarding private data. Security systems have evolved through various trends, moving from reliance on possession-based components like driver's licenses to knowledge-based components like PINs. The tendency to identify people based on their inherent qualities—biometrics, for example—or on combinations of two or more of these elements has gained traction in recent times. The biometric movement presents itself as a viable remedy for the drawbacks of token- and knowledge-based authentication methods. Human biometrics, including face, fingerprint, palm, iris scanning, facial features, signature, and voice, provide a dependable security level for personal and public use, surpassing traditional methods like passwords. This paper provides a comprehensive overview of biometric identification systems delving into the foundational aspects of biometric systems, covering essential information such as the basic operational processes inherent in any biometric system. It briefly reviews various modalities, analyzing their strengths and limitations. The examination extends to identification methods, covering feature extraction, matching algorithms, and performance evaluation parameters are discussed, emphasizing recent advancements like multi-modal biometrics and deep learning. The paper also extensively looks into the application of deep learning in biometric systems, such as the DeepFace face recognition model which was trained on 4 million facial images and achieved 97.35% accuracy which is only 0.18% less than that achieved by human. Deep generative models have also been used by researchers for face image generation. Ear recognition is an emerging field, and the number of biometric recognition studies involving ears may be on a ride in the future, however, the constraint is in limited dataset sizes. Nevertheless, there is a plethora of biometric system related problem areas for the future researcher and there is huge scope due to the advancement in deep learning approaches like transfer learning, few shot learning, semi supervised learning to name a few. The paper concludes with future research directions in biometric identification systems, including developing more accurate and robust techniques, improving data quality, and addressing ethical and legal issues

Acknowledgments

Please add the acknowledgments to colleagues and funding agencies here.

Conflicts ofInterest

The authors declare no conflict of interest.

Author Contributions

The authors must include the CRediT- Contributor Role Taxonomy considering each author contribution for the paper, using the following roles (for more information, access https://credit.niso.org/): **Conceptualization:** XXXX, T.K.; YYYYYY, G.M. **Data curation: Formal analysis: Funding acquisition: Investigation: Methodology: Project administration: Software: Resources: Supervision: Validation: Visualization: Writing - original draft: Writing - review and editing:**

References

1. B. Miller, "Vital signs of identity [biometrics]," *IEEE Spectr*, vol. 31, pp. 22–30, 1994,
2. Jain Anil, and Hong Lin, and Pankanti Sharath, "Biometrics Identification," *Communication of the ACM*, vol. 43, no. 2, pp. 90–98, 2000.
3. Unar J. A., Seng W. C., and Abbasi A., (2014). *A review of biometric technology along with trends and prospects*, Pattern Recognition, 47(8), 2673-2688.
4. Ross, A., Nandakumar, K. and Jain, A.K., (2008). *Introduction to multibiometrics*. In Handbook of biometrics, Springer, Boston, MA, 271-292.
5. Jain Anil, Hong Lin, and Pankanti Sharath, (2000a). *Biometrics Identification*, Communication of the ACM, 43(2), 90-98.Communication of the ACM, 43(2), 90-98.
6. Jain A. K., Flynn P., and Ross A., (2008). *Handbook of Biometrics*, Springer Verlag US, 1-556.
7. Kaur, Gagandeep, Gurpreet Singh, and Vineet Kumar. "A review on biometric recognition." *International Journal of Bio-Science and Bio-Technology* 6.4 (2014): 69-76.
8. Jain A. K., Ross A., and Prabhakar S., (2004a). *An introduction to biometric recognition,* IEEE Transactions on Circuits and Systems for video technology, 14(1), 4 – 20.
9. Jain A. K., Ross A., and Nandakumar K., (2011). *Introduction to Biometrics*, Springer Publishing Company.
10. J. L. Wayman, "The scientific development of biometrics over the last 40 years," 2007.
11. Jain A. K., Bolle R., and Pankanti S., (1999a). *Biometrics: Personal Identification in Networked Society,* Kluwer Academic Publishers Book,
12. Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric recognition: Security and privacy concerns." *IEEE security & privacy* 1.2 (2003): 33-42.
13. Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7. Institute of Electrical and Electronics Engineers Inc., pp. 5994–6009, 2019. doi: 10.1109/ACCESS.2018.2889996.
14. Marcel S., Nixon M. S., and Li S. Z., (2014). *Handbook of Biometric Anti-SpoofingTrusted Biometrics under Spoofing Attacks*, Advances in Computer Vision and Pattern Recognition-Springer, 1-279.
15. Zhang D., and Kong W. K., (2003). *Online palm print identification,* IEEE Transaction on Pattern Analysis and Machine Intelligence, 25(9), 1041-50.

16. Jain, A.K. and Kumar, A., (2012). *Biometric recognition: an overview*, In Second generation biometrics: The ethical, legal and social context, Springer, Dordrecht, 49- 79

17. Abate A.F., Nappi M., Riccio D., and Sabatino G., (2007). *2D and 3D face recognition: A survey*, Pattern recognition letters, 28(14), 1885-1906.

18. Phillips P., Grother P., Micheals R., Blackburn D., Tabassi E., and Bone M., (2002). *Face Recognition*, Vendor Test: Evaluation Report.

19. Ko T., (2005). *Multimodal biometric identification for large user population using fingerprint, face and iris recognition*, In 34th Applied Imagery and Pattern Recognition Workshop (AIPR'05), pp. 6 pp. -223, doi: 10.1109/AIPR.2005.35.

20. Berry J. and Stoney D.A., (2001). *The history and development of fingerprinting,* Advances in fingerprint Technology, Second Edition, 13-52

21. Pankanti S., Prabhakar S., and Jain A. K., (2001). *On the individuality of fingerprints*, IEEE Conference on Computer Vision and Pattern Recognition, 805–812

22. S.A. Abdulrahman, W. Khalifa, M. Roushdy, A.-B.-M. Salem, Comparative study for 8 computational intelligence algorithms for human identification, Comput. Sci. Rev. 36 (2020) 100237.

23. C. Champod, C.J. Lennard, P. Margot, M. Stoilovic, Fingerprints and Other Ridge Skin Impressions, CRC Press, 2004.

24. Kukula E., and Elliott S., (2001). *Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance*, In Proc. of 35th Annual International Carnahan Conference on Security Technology, 83 – 88.

25. Kumar A., Wong D. C. M., Shen H. C., and Jain A. K., (2003). *Personal verification using palmprint and hand geometry biometric*, *In International Conference on Audioand Video-Based Biometric Person Authentication*, Springer, Berlin, Heidelberg, 668- 678.

26. Zhu Y., Tan T., and Wang Y., (2000a). *Biometric personal identification based on iris patterns,* Proceeding 15th International Conference on Pattern Recognition, 2, 801-804.

27. Daugman J., (1999). *Recognizing persons by their iris patterns,* Information Security Technical Report, Elsevier, 3(1), 33-39

28. Rahul D Chaudhari, Ashok A Pawar, Rakesh S Deore, 2013, The Historical Development of Biometric Authentication Techniques: A Recent Overview, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 02, Issue 10 (October 2013).

29. Burge M. J., and Burger W., (1998). *Ear biometrics,* In Jain, Anil K., Bolle R., and Pankanti S., *Biometrics: Personal Identification in Networked Society,* Kluwer Academic, 273-286.

30. Kholmatov A., (2003). *Biometric identity verification using on-line & off-line signature verification*, Master's thesis, Sabanci University.

31. Morita H., Sakamoto D., Ohishi T., Komiya T., and Matsumoto T., (2001). *On-line signature verifier incorporating pen position, pen pressure, and pen inclination trajectories*. In AVBPA, 318–323.

32. L.G. Hafemann, R. Sabourin, L.S. Oliveira, Offline handwritten signature verification literature review, in: 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2017, pp. 1–8.

33. James B. H. A., Mark S. N., and John N. C., (2001). *Automatic gait recognition by symmetry analysis*, In AVBPA, 272–277.

34. K., Amjad & Aithal, Sreeramana. (2022). Voice Biometric Systems for User Identification and Authentication – A Literature Review. International Journal of Applied Engineering and Management Letters. 198-209. 10.47992/IJAEML.2581.7000.0131.

35. Malaviya A., and Liliane P., (1993). *A fuzzy online handwriting recognition system:FOHRES*, 2nd International Conference on Fuzzy Set Theory and Technology, 1-15.

36. Zhu Y., Tan T., and Wang Y., (2000b). *Biometric personal identification based on handwriting*, Proceeding 15th International Conference on Pattern Recognition, ICPR, 2, 797-800.

37. Srihari S. N., Cha S. H., Arora H., and Sangjik L., (2001). *Individuality of handwriting: A validation study*, Proceedings of the Sixth International Conference on Document Analysis and Recognition, 106-109.

38. C. Wu et al., Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array, Mater. Today 21 (3) (2018) 216–222.

39. Bergadano F., Gunetti D., and Picardi C., (2002). *User authentication through keystroke dynamics*, ACM Transactions Information System Security, 5(4), 367–397.

40. Bhattacharyya D., Ranjan R., Alisherov F., and Choi M., (2009). *Biometrics Authentication: A Review*", International Journal of u- and e – Service, Science and Technology, 2(3), 13-28.

41. Jain, A., Bolle, R. and Pankanti, S. (2002) Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, Forth Printing.

42. Jain A.K., Dass S.C., and Nandakumar K., (2004b). *Soft Biometric Traits for Personal Recognition Systems*, in Proceedings of the International Conference on Biometric Authentication, 3072, 731–738.

43. Jain A. K., and Park U., (2009). *Facial marks: Soft biometric for face recognition*, in Proceedings of the IEEE International Conference on Image Processing (ICIP '09), 37– 40.

44. Jain A. K., Dass S. C., and Nandakumar K., (2004c). *Can soft biometric traits assist user recognition?* International Society for Optical and Photonics, 5404, 561–572.

45. Park U., and Jain A. K., (2010). *Face matching and retrieval using soft biometrics*, Information Forensics and Security, 5(2), 406–415.

46. Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. *Advances in user authentication*. Cham, Switzerland: Springer International Publishing, 2017.

47. Gad R., El-Fishawy N., El-Sayed, A., and Zorkany M., (2015). *Multi-Biometric Systems: A State-of-the-Art Survey and Research Directions*, International Journal of Advanced Computer Science and Applications (IJACSA), 6(6), 128-138.

48. MUHTAHIR O. Oloyede & GERHARD P. Hancke, (2016). Unimodal and Multimodal Biometric Sensing Systems: A Review. IEEE Access. Volume 4, pg-7532-7555. 10.1109/ACCESS.2016.2614720.

49. M. Mittal and B. Garg, ‘‘Secure identity using multimodal biometrics,’’ Int. J. Inf. Technol. Knowl., vol. 7, no. 2, pp. 20–25, 2014.

50. M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, ‘‘‘A study of users’ acceptance satisfaction biometric systems,’’ in Proc. IEEE Int. Carnahan Conf. Secur. Technol.(ICCST), Oct. 2010, pp. 170–178.

51. H. Jaafar and D. A. Ramli, ‘‘A Review of Multibiometric System with Fusion Strategies and Weighting Factor,’’ Int. J. Comput. Sci. Eng. (IJCSE), vol. 2, no. 4, pp. 158–165, Jul. 2013.

52. C. Prathipa and L. Latha, ‘‘A survey of biometric fusion and template security techniques,’’ Int. J. Adv. Res. Comput. Eng. Technol., vol. 3, no. 10, pp. 3511–3516, 2014.

53. M. Ghayoumi, ‘‘A review of multimodal biometric systems: Fusion methods and their applications,’’ in Proc. IEEE/ACIS 14th Int. Conf. Comput. Inf. Sci. (ICIS), Jun./Jul. 2015, pp. 131–136.

54. R. Brunelli and D. Falavigna, ‘‘Person identification using multiple cues,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 17, no. 10, pp. 955–966, Oct. 1995.

55. M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Maui, HI, USA, 1991, pp. 586-591, doi: 10.1109/CVPR.1991.139758.

56. Daugman, John. "How iris recognition works." *The essential guide to image processing*. Academic Press, 2009. 715-739.

57. Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, 2003 . *Guide to biometrics*. Springer Science & Business Media, NY.https://doi.org/10.1007/978-1-4757-4036-3.

58. Lu, G., Zhang, D., Kong, W.K., Wong, M. (2008). A Palmprint Authentication System. In: Jain, A.K., Flynn, P., Ross, A.A. (eds) Handbook of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-71041-9_9.

59. Y. Wang, Y. Fan, W. Liao, K. Li, L. -K. Shark and M. R. Varley, "Hand vein recognition based on multiple keypoints sets," 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 2012, pp. 367-371, doi: 10.1109/ICB.2012.6199778.

60. Reynolds, D.A. and Rose, R.C., 1995. Robust text-independent speaker identification using Gaussian mixture speaker models. *IEEE transactions on speech and audio processing*, *3*(1), pp.72-83.

61. Ross, A. and Jain, A., 2003. Information fusion in biometrics. *Pattern recognition letters*, *24*(13), pp.2115-2125.

62. Meghana, K. and Manjula, G. P. and Ramya, G. and Eswari, Veluru and Puneeth, G. J., Retina Based Biometric Recognition System (November 20, 2020). Compliance Engineering Journal, Volume 11, Issue 7, 2020, Page No: 119-126.

63. Butler, J.M., 2005. *Forensic DNA typing: biology, technology, and genetics of STR markers*. Elsevier.

64. Plamondon, R. and Srihari, S.N., 2000. Online and off-line handwriting recognition: a comprehensive survey. *IEEE Transactions on pattern analysis and machine intelligence*, *22*(1), pp.63-84.

65. Weihong Deng, Jiani Hu, and Jun Guo. In defense of sparsity based face recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 399–406, 2013.
66. Qiong Cao, Yiming Ying, and Peng Li. Similarity metric learning for face recognition. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 2408–2415, 2013.
67. John Wright, Allen Y Yang, Arvind Ganesh, S Shankar Sastry, and Yi Ma. Robust face recognition via sparse representation. *IEEE transactions on pattern analysis and machine intelligence*, 31(2):210–227, 2008.
68. Meng Yang, Lei Zhang, Jian Yang, and David Zhang. Regularized robust coding for face recognition. *IEEE transactions on image processing*, 22(5), 2012.
69. Dong Yi, Zhen Lei, and Stan Z Li. Towards pose robust face recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 3539–3545, 2013.
70. Ajmal Mian, Mohammed Bennamoun, and Robyn Owens. An efficient multimodal 2d-3d hybrid approach to automatic face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 29(11), 2007.
71. Unsang Park, Yiying Tong, and Anil K Jain. Age invariant face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 32(5), 2010.
72. Yaniv Taigman, Ming Yang, Marc’Aurelio Ranzato, and Lior Wolf. Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1701–1708, 2014.
73. Labeled faces in the wild. http://vis-www.cs.umass. edu/lfw/.

74. Yi Sun, Xiaogang Wang, and Xiaoou Tang. Deep learning face representation from predicting 10,000 classes. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1891–1898, 2014.

75. Tero Karras, Timo Aila, Samuli Laine, and Jaakko Lehtinen. Progressive growing of gans for improved quality, stability, and variation. *arXiv preprint arXiv:1710.10196*, 2017.

76. Luke Nicholas Darlow and Benjamin Rosman. Fingerprint minutiae extraction using deep learning. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 22–30. IEEE, 2017.
77. Yao Tang, Fei Gao, Jufu Feng, and Yuhang Liu. Fingernet: An unified deep network for fingerprint minutiae extraction. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 108–116. IEEE, 2017.
78. Chenhao Lin and Ajay Kumar. Contactless and partial 3d fingerprint recognition using multi-view deep representation. *Pattern Recognition*, 83:314–327, 2018.
79. Raid Omar, Tingting Han, Saadoon AM Al-Sumaidaee, and Taolue Chen. Deep finger texture learning for verifying people. *IET Biometrics*, 8(1):40–48, 2018.
80. Chenhao Lin and Ajay Kumar. Multi-siamese networks to accurately match contactless to contact-based fingerprint images. In *International Joint Conference on Biometrics (IJCB)*, pages 277–285. IEEE, 2017.
81. Soowoong Kim, Bogun Park, Bong Seop Song, and Seungjoon Yang. Deep belief network based statistical feature learning for fingerprint liveness detection. Pattern Recognition Letters, 77:58–65, 2016.
82. Rodrigo Frassetto Nogueira, Roberto de Alencar Lotufo, and Rubens Campos Machado. Fingerprint liveness detection using convolutional neural networks. *IEEE transactions on information forensics and security*, 11(6):1206–1213, 2016.
83. Shervin Minaee and Amirali Abdolrashidi. Finger-gan: Generating realistic fingerprint images using connectivity imposed gan. *preprint, arXiv:1812.10482*, 2018.
84. Shervin Minaee, AmirAli Abdolrashidi, and Shervin Minaee, Amirali Abdolrashidiy, and Yao Wang. An experimental study of deep convolutional features for iris recognition. In *signal processing in medicine and biology symposium*, pages 1–6. IEEE, 2016.
85. Abhishek Gangwar and Akanksha Joshi. Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition. In *2016 IEEE International Conference on Image Processing (ICIP)*, pages 2301–2305. IEEE, 2016.
86. Zhao Dandan Pan Xin, Pan Xin, Luo Xiaoling, and Gao Xiaojing. Palmprint recognition based on deep learning,2015.
87. Shuping Zhao, Bob Zhang, and CL Philip Chen. Joint deep convolutional feature representation for hyperspectral palmprint recognition. *Information Sciences*, 489:167–181, 2019.
88. Huikai Shao and Dexing Zhong. Few-shot palmprint recognition via graph neural networks. Electronics Letters, 55(16):890–892, 2019.

89. Jie Zhang, Wen Yu, Xudong Yang, and Fang Deng. Few-shot learning for ear recognition. In *Proceedings of the 2019 International Conference on Image, Video and Signal Processing*, pages 50–54. ACM, 2019.
90. Samuel Dodge, Jinane Mounsef, and Lina Karam. Unconstrained ear recognition using deep neural networks. *IET Biometrics*, 7(3):207–214, 2018.
91. Ziga Emersic, Dejan Stepec, Vitomir Struc, Peter Peer, Anjith George, Adii Ahmad, Elshibani Omar, Terranee E Boult, Reza Safdaii, Yuxiang Zhou, et al. The unconstrained ear recognition challenge. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 715–724. IEEE, 2017.
92. Ziga Emersic, Dejan Stepec, Vitomir Struc, and Peter Peer. Training convolutional neural networks with lim ited training data for ear recognition in the wild. In *International Conference on Automatic Face & Gesture Recognition*, pages 987–994. IEEE, 2017.
93. Najim Dehak, Patrick J Kenny, R´eda Dehak, Pierre Dumouchel, and Pierre Ouellet. Front-end factor analysis for speaker verification. *IEEE Transactions on Audio, Speech, and Language Processing*, 19(4):788–798, 2010.
94. Ehsan Variani, Xin Lei, Erik McDermott, Ignacio Lopez Moreno, and Javier Gonzalez-Dominguez. Deep neural networks for small footprint text-dependent speaker verification. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2014.
95. Georg Heigold, Ignacio Moreno, Samy Bengio, and Noam Shazeer. End-to-end text-dependent speaker verification. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2016.

96. Shi-Xiong Zhang, Zhuo Chen, Yong Zhao, Jinyu Li, and Yifan Gong. End-to-end attention based text-dependent speaker verification. In *Spoken Language Technology Workshop (SLT)*, pages 171–178. IEEE, 2016.
97. Li Wan, Quan Wang, Alan Papir, and Ignacio Lopez Moreno. Generalized end-to-end loss for speaker verification. In *International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2018.
98. Branka Stojanovi´c, Oge Marques, Aleksandar Ne˘skovi´c, and Sne˘zana Puzovi´c. Fingerprint roi segmentation based on deep learning. In 2016 24th Telecommunications Forum (TELFOR), pages 1–4. IEEE, 2016.
99. Yanming Zhu, Xuefei Yin, Xiuping Jia, and Jiankun Hu. Latent fingerprint segmentation based on convolutional neural networks. In Workshop on Information Forensics and Security (WIFS), pages 1–6. IEEE, 2017
100. Gerald O Williams. Iris recognition technology. In 1996 30th Annual International Carnahan Conference on Security Technology, pages 46–59. IEEE, 1996.
101. Yao Wang. Iris recognition using scattering transform and textural features. In signal processing and signal processing education workshop, pages 37–42. IEEE, 2015.
102. Zijing Zhao and Ajay Kumar. Towards more accurate iris recognition using deeply learned spatially corresponding features. In IEEE International Conference on Computer Vision, pages 3809–3818, 2017.
103. David Zhang, Wangmeng Zuo, and Feng Yue. A comparative study of palmprint recognition algorithms. ACM computing surveys (CSUR), 44(1):2, 2012.
104. Mahdieh Izadpanahkakhk, Seyyed Razavi, Mehran Gorjikolaie, Seyyed Zahiri, and Aurelio Uncini. Deep region of interest and feature extraction models for palmprint verification using convolutional neural networks transfer learning. Applied Sciences, 8(7), 2018.
105. Zhihuai Xie, Zhenhua Guo, and Chengshan Qian. Palmprint gender classification by convolutional neural network. IET Computer Vision, 12(4):476–483, 2018.
106. Fevziye Irem Eyiokur, Dogucan Yaman, and Hazım Kemal Ekenel. Domain adaptation for ear recognition using deep convolutional neural networks. iet Biometrics, 7(3):199–206, 2017.
107. Samuel Dodge, Jinane Mounsef, and Lina Karam. Unconstrained ear recognition using deep neural networks. IET Biometrics, 7(3):207–214, 2018.
108. Clark D Shaver and John M Acken. A brief review of speaker recognition technology. 2016.
109. Daniel Garcia-Romero, David Snyder, Gregory Sell, Daniel Povey, and Alan McCree. Speaker diarization using deep neural network embeddings. In International Conference on Acoustics, Speech and Signal Processing, pages 4930–4934. IEEE, 2017.
110. Yun Lei, Nicolas Scheffer, Luciana Ferrer, and Mitchell McLaren. A novel scheme for speaker recognition using a phonetically-aware deep neural network. In International Conference on Acoustics, Speech and Signal Processing, pages 1695–1699. IEEE, 2014.
111. Georg Heigold, Ignacio Moreno, Samy Bengio, and Noam Shazeer. End-to-end text-dependent speaker verification. In International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016.
112. Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Exploring recurrent neural networks for on-line handwritten signature biometrics. IEEE Access, 6:5128–5138, 2018.
113. Cheng Zhang, Wu Liu, Huadong Ma, and Huiyuan Fu. Siamese neural network based gait recognition for human identification. In International Conference on Acoustics, Speech and Signal Processing. IEEE, 2016.
114. Munif Alotaibi and Ausif Mahmood. Improved gait recognition based on specialized deep convolutional neural network. Computer Vision and Image Understanding, 164:103–110, 2017.
115. Fvc fingerprint dataset. http://bias.csr.unibo.it/ fvc2002/.
116. PolyU fingerprint dataset. http://www4.comp.polyu. edu.hk/~biometrics/HRF/HRF_old.htm.

117.Casia fingerprint dataset. http://biometrics. idealtest.org/dbDetailForUser.do?id=7.

118.Michael D Garris and R Michael McCabe. Fingerprint minutiae from latent and matching tenprint images. In *Tenprint Images", National Institute of Standards and Technology*. Citeseer, 2000.

119.Extended yale face database b (b+). http://vision.ucsd.edu/content/ extended-yale-face-database-b-b.

120.The cmu multi-pie face database. http: //www.cs.cmu.edu/afs/cs/project/PIE/MultiPie/ Multi-Pie/Home.html.

121.Ralph Gross, Iain Matthews, Jeffrey Cohn, Takeo Kanade, and Simon Baker. Multi-pie. *Image and Vision Computing*, 28(5):807–813, 2010.

122.Polyu nir face database. http://www4.comp.polyu.edu. hk/~biometrics/polyudb_face.htm.

123.Vggface2.http://www.robots.ox.ac.uk/~vgg/data/ vgg_face2/.

124.Dong Yi, Zhen Lei, Shengcai Liao, and Stan Z Li. Learning face representation from scratch. *arXiv preprint arXiv:1411.7923*, 2014.

125.Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He, and Jianfeng Gao. Ms-celeb-1m: A dataset and benchmark for large-scale face recognition. In *European Conference on Computer Vision*, pages 87–102. Springer, 2016.

126.Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. Deep learning face attributes in the wild. In *Proceed ings of the IEEE international conference on computer vision*, pages 3730–3738, 2015.

127.Ira Kemelmacher-Shlizerman, Steven Seitz, D Miller, and Evan Brossard. The megaface benchmark: 1 million faces for recognition at scale. In *IEEE Conference on Computer Vision and Pattern Recognition*, 2016.

128.Casia iris dataset. http://biometrics.idealtest.org/ findTotalDbByMode.do?mode=Iris.

129.Ubiris iris dataset. http://iris.di.ubi.pt/.

130.Iit iris dataset. https://www4.comp.polyu.edu.hk/ ~csajaykr/IITD/Database_Iris.htm.

131.Lg iris. https://cvrl.nd.edu/projects/data/.

132.Maria De Marsico, Michele Nappi, Daniel Riccio, and Harry Wechsler. Mobile iris challenge evaluation (miche)-i, biometric iris dataset and protocols. *Pattern Recognition Letters*, 57:17–23, 2015.

133.Polyu palmprint dataset. https://www4.comp.polyu. edu.hk/~biometrics/MultispectralPalmprint/MSP. htm

134.Casia palmprint dataset. http://www.cbsr.ia.ac.cn/ english/Palmprint%20Databases.asp.

135.IIT palmprint dataset. https://www4.comp.polyu.edu. hk/~csajaykr/IITD/Database_Palm.htm.

136.Ajay Kumar and Chenye Wu. Automated human identification using ear imaging. *Pattern Recognition*, 45(3):956–968, 2012.

137.Awe ear dataset. http://awe.fri.uni-lj.si/home.

138.Ustb ear dataset. http://www1.ustb.edu.cn/resb/en/ visit/visit.htm.

139.Dariusz Frejlichowski and Natalia Tyszkiewicz. The west pomeranian university of technology ear database– a tool for testing biometric algorithms. In *International Conference Image Analysis and Recognition*, pages 227–234. Springer, 2010.

140.Alvin F Martin and Mark A Przybocki. The nist speaker recognition evaluations: 1996-2001. In *2001: A Speaker Odyssey-The Speaker Recognition Workshop*, 2001.

141.Aaron Lawson. The speakers in the wild (sitw) speaker recognition database. In *Interspeech*, pages 818–822, 2016.

142.Arsha Nagrani, Joon Son Chung, and Andrew Zisserman. Voxceleb: a large-scale speaker identification dataset. *arXiv preprint arXiv:1706.08612*, 2017.

143.Icdar svc 2009. http://tc11.cvc.uab.es/datasets/ SigComp2009_1.

144.Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. Svc2004: First international signature verification competition. In *International conference on biometric authentication*, pages 16–22. Springer, 2004.

145.Francisco Vargas, M Ferrer, Carlos Travieso, and J Alonso. Off-line handwritten signature gpds-960 corpus. In *International Conference on Document Analysis and Recognition*, volume 2, pages 764–768. IEEE, 2007.

146.Casia gait database. http://www.cbsr.ia.ac.cn/ users/szheng/?page_id=71.

147.Osaka gait database. http://www.am.sanken.osaka-u. ac.jp/BiometricDB/GaitTM.html.

i