International Journal of Engineering in Computer Science

**E-ISSN:** 2663-3590
**P-ISSN:** 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2024; 6(2): 131-152
Received: 03-07-2024
Accepted: 17-08-2024

**Sundws Mustafa Mohammed**
Department of Anaesthesia, Technical College of Health, Sulaimani Polytechnic University, Iraq

**Shahlaa Mashhadani**
Department of Computer, College of Education for Pure Sciences Ibn Al-Haitham, University of Baghdad, Iraq

**Oday Ali Hassen**
Department of Information Technology, Ministry of Education, Wasit Education Directorate, Kut, Iraq

**Corresponding Author:**
Department of Information Technology, Ministry of Education, Wasit Education Directorate, Kut, Iraq

# Human biometric identification: Application and evaluation

**Sundws Mustafa Mohammed, Shahlaa Mashhadani and Oday Ali Hassen**

**DOI:** https://doi.org/10.33545/26633582.2024.v6.i2b.136

## Abstract

Biometric detection methods are an integral part of human identification systems, which allow the examination of specific individuals for forensic purposes. For criminal identification and general analyzes of human characteristics, investigative authorities use these methods. This paper presents a variety of perspectives and aspects of human characteristics as they relate to biometrics, and furthermore, the many aspects associated with biometric applications are highlighted in this paper. Biometrics applications rely heavily on human aspects, such as training AI models with a high degree of learning and training processes, which in turn trains the entire model to reflect human views and traits in terms of human characteristics, such as face, fingerprint, lip, or iris, Or the palm of the hand, or even the tongue, which is part of the human identification system. In today's world, technological equipment has taken over control tasks previously performed by humans and automation has spread into almost every aspect of life. An increasingly urgent need has arisen for a trustworthy personal identification system to verify users' identities before granting them access to restricted areas or rejecting counterfeiters. As a direct result of this. For example, when an unauthorized person gains access to the password, traditional verification methods that rely on passwords are vulnerable to hacking. Therefore, for the purpose of individual identification, many biometric methods have been designed by different academics. One example of a biometric feature is one that does not require tokens or saving. Physiological or behavioural characteristics of an individual are used by biometrics-based personal identification systems for the purpose of recognition where speech, handwriting, keystrokes, etc. are behavioral traits, while fingerprints, faces, and hand geometry are physiological traits. The increasing need to establish and verify trustworthy personal identity in many public and private sectors has led to tremendous development in biometric authentication technology in recent years. This manuscript also covers a wide range of topics related to biometric applications, opening many potential areas for use in human trait detection and assessment, ultimately improving the overall performance and accuracy of existing systems. In order to accurately identify humans, the paper details several aspects of human traits. This research also provides a comparative analysis and evaluation of several proposed biometric identification methods as well as documents their potential applications and rejection of fraudsters.

**Keywords:** Authentication, biometric, features extraction, biometrics, human identification, cloud biometrics, biometric physiological, biometric behavioural

## Introduction

When a live thing's characteristics are studied in order to train and assess several essential aspects, this process is called biometric analysis. The analytics of many aspects from the human perspective or even internal parts are made possible by biometric applications, which have a number of views [1, 2]. Biometrics refers to techniques that automatically identify or verify people by analyzing their unique behavioral or physiological traits. Recognizing a person's face, detecting a smile, speaking their name, identifying their hand geometry, iris, DNA sequence, signature, fingerprint (dactylogram), or retina are all examples of biometric technology [3, 4]. A biometric authentication program has already provided identity to almost 1.2 billion people in low- to middle-income nations.

There are four main types of biometric detection algorithms: knowledge-based, feature-invariant, template matching, and appearance-based. Each kind is an essential part of an identification system. There are two parts to the recognition process: training and evaluation [12, 13].

The training step involves feeding the algorithm examples of the images it needs to learn, and it creates a unique model for each of those images. The evaluation process involves comparing the model of a newly learnt test image to all the models within the database. After that, in order to find out if the recognition is activated, the nearest matching model is obtained. In this step, a set of Eigen-objects, or basis features, are formed using a series of face photos and a statistical method called simulated annealing. Combinations of these typical features can be seen in any human face [14, 15].

Biometrics refers to the study and practice of identifying individuals based on their unique physiological and behavioral traits. Biometric authentication is gaining traction in many fields, including banking, aviation, financial transactions, and more. Figure 1 shows a block schematic of the biometric recognition system. Two components, enrolment and testing, are the backbone of such a system. Database storage of the template occurs during the enrollment procedure. Also, while testing is going on, the collected templates are compared with the data from the people. The matching software uses an appropriate algorithm to compare the input and template and estimate the distance between them. This is the result that was expected to be achieved.

In order to employ biometric features recognition to facilitate human identification, users must first upload a photo of the subject into the system. The system will then reprocess the picture, removing noise and other undesired aspects [8, 9]. The next step is for the system to use the image's landmarks, including factors like the distances between the eyes, length the jaw line, etc., to determine the image's classification. The system then displays the results of its search across the database, which it had previously determined to be an ideal match. The current method of fingerprint identification, which is straightforward and quick to perform, can be hindered by the usage of latent fingerprints, which are not always available at the crime scene. Thieves nowadays are so cunning that they seldom leave a trace, such as a fingerprint, at a crime site. An automated image processing algorithm and a face database were both part of this system, which could compare the face feed to the database's existing face records. The effectiveness of this system depends on two components: detection and recognition. In references [10, 11]. The following Figure. 1, a, b. shows the basic stages of the biometric recognition system.

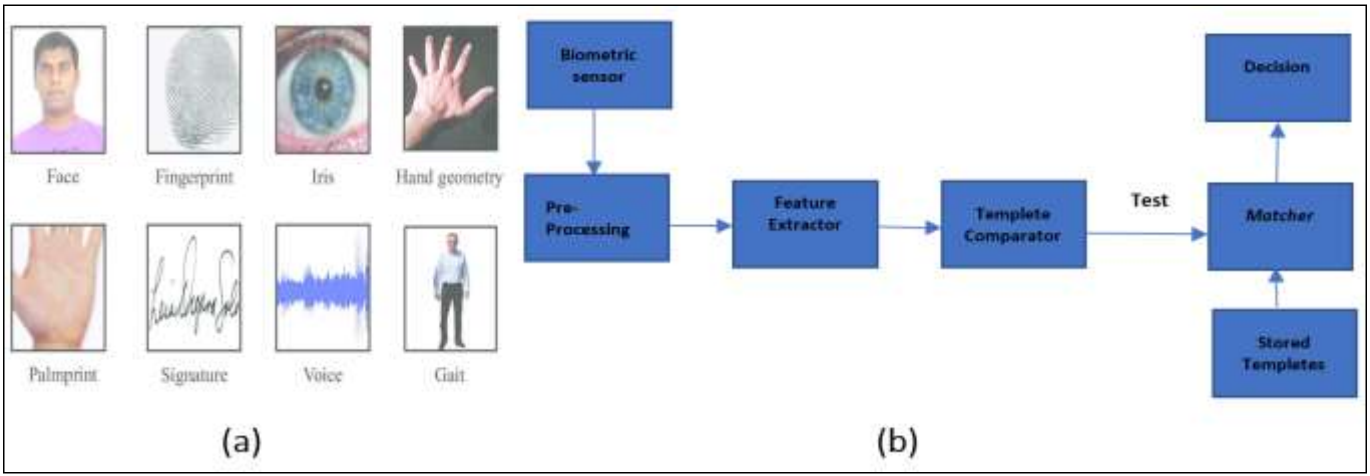


**Fig 1:** a, b: shows the basic stages of the biometric recognition system.

The first building piece, the sensor, gathers data from the outside world and functions as a link between the system and the actual environment. It is versatile and can adapt to many applications, but vision-based picture capture systems are a good fit. The second block is responsible for preprocessing, which involves improving the input picture and removing artifacts from the sensor. The subsequent section is responsible for extracting key attributes. The optimal extraction of the correct characteristics is essential at this step. In order to create a template, one uses either image features or a vector of numbers that have certain characteristics. An extracted collection of similar features from the source is combined to form a template. Templates for decreasing file size and preserving claimer identity Eliminate elements of biometric measures that are not necessary for comparison algorithms. Assorted Types of Biometric Traits:

The Physiological consists of Face, Fingerprint, Hand geometry , Iris, DNA, retina scan, Ear Acoustic Authentication, Eye Vein Recognition, Facial Recognition, Finger Vein Recognition, Footprint and Foot Dynamics, Body Odor Recognition, Palm Print Recognition, Palm Vein Recognition, Skin Reflection, Thermography Recognition and the Behavioral, Keystroke dynamic, Sign: Texture, Voice: Speech based Signals, Gait: Motion Detection, Speaker Recognition, Lip Motion.

also and phases advanced to pattern recognition beings are needed to distinguish friend from foe for survival and identification has been always critical for him; so these days have been tried to mechanization the identification or authentication systems. “These developments have been based on the needs of society and the world” [1]. A need for improvements which in caused to reduce fraud, enhance security and accelerate the routines issues. In the past, in order to identify the crime and the criminal, fingerprints and portraits detecting procedures were used but these days a mechanized system is established to do so. Biometric technology can be divided into two general categories. Figure 2. Explain this.

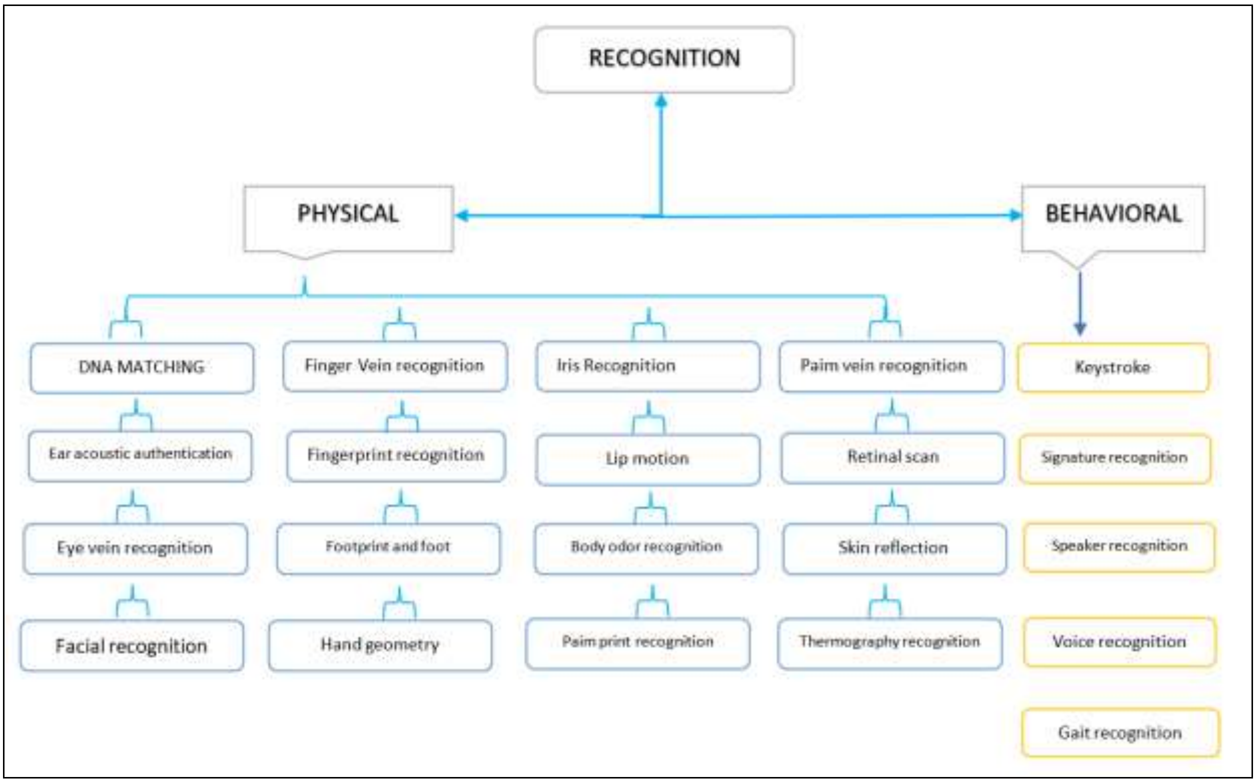


**Fig 2:** Shows the basic stages of the biometric recognition system behaviour and Physiological.

**Biometric methods based on Physiological and Behavioral:** Are facial recognition and fingerprint security features anything you've used on a mobile device? Physiological biometrics have been utilized in your case.

Conversely, you may have unknowingly come into contact with behavioral biometrics; for instance, certain internet accounts may record your typing activity. Biometrics is the science and practice of identifying and verifying people using their distinctive physical attributes. In person or online, these distinct traits can be utilized to identify and verify individuals.

Biometrics encompasses a wide range of topics and classifications; for further information, see our Biometric Encyclopedia. However, in this article, we will be discussing the applications of behavioral and physiological biometrics in relation to online security, with an emphasis on their distinctions.

Here we will go over the basics of behavioral biometrics, physiological biometrics, and how they vary from one another.

Therefore, we will explain each of them in detail as follows and Figure. 3. Explain this.

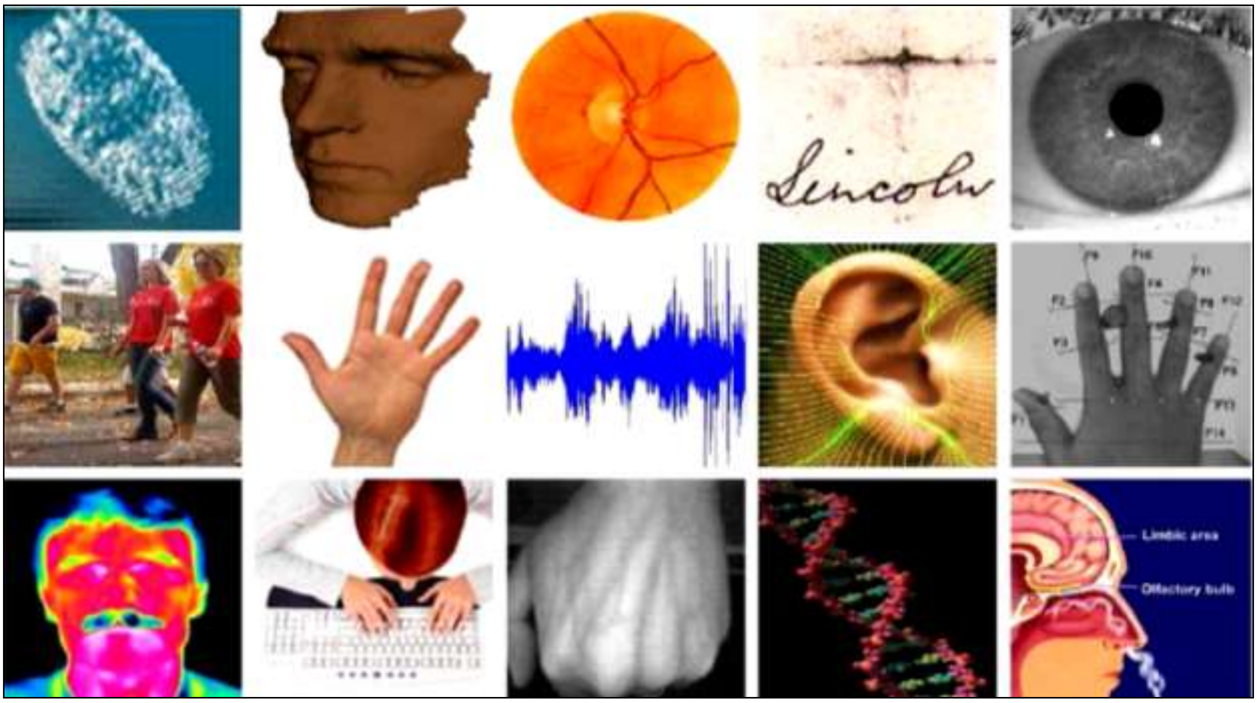


**Fig 3:** Among the biometrics that are most commonly employed.

### Biometric methods based on Physiological

A person's physiological qualities are associated with their bodily make-up. The authentication process makes use of a wide range of physiological features associated with humans, such as vascular patterns, fingerprints, iris, retina, and face and hand geometry. The vast majority of these detections rely on visual cues. Physiological biometrics, also known as static biometrics, are the particular measurements, features, and proportions of your body. Your vein patterns, fingerprints, and retina are almost unchangeable, which is why we refer to them as static. This method from authentication include from:

### Finger Prints pattern Recognition

is a mark created by a human finger's friction ridges. One significant technique in forensic science is the extraction of partial fingerprints from a crime scene. Fingerprints left on metal or glass surfaces are caused by the combination of grease and moisture on the finger. The peaks of the skin's friction ridges can be used to transfer ink or other substances to a smooth surface, such paper, in order to intentionally imprint a full fingerprint. Although fingerprint cards also usually capture parts of the lower joint regions of the fingers, fingerprint records normally contain impressions from the pad on the final joint of fingers and thumbs.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster.

It may also be defined as "Fingerprints: impressions left on surfaces by a human finger's friction ridges." [3] Two fingerprint matching is one of the most used and dependable biometric methods. Fingerprint matching merely takes into account a fingerprint's visible characteristics.

Two methods exist for detecting fingerprints: vision-based pattern matching for identification, and detection of minutiae (such as ridge endings, bifurcations, dots, or islands; see Fig. 4.

The automated process of matching an input fingerprint with a stored fingerprint pattern in order to identify human characters is known as fingerprint recognition. Even though fingerprint recognition has been around for a while, it is currently among the most used biometrics.

As a result of the fingertip's elevated lines (ridges) and indented parts (furrows), a fingerprint might be created. There are three distinct designs that the ridges and furrows might take on: loops, whorls, and arches. After extending outward, the loop returns inward.

Four distinct groupings of whorls make up fingerprint patterns:

a) Flat (circles with equal diameters),
b) Central pocket loop - a whorled-end loop.
c) A double loop is made up of two loops that form an S-shaped pattern.
d) Unintentional loop with an uneven form.

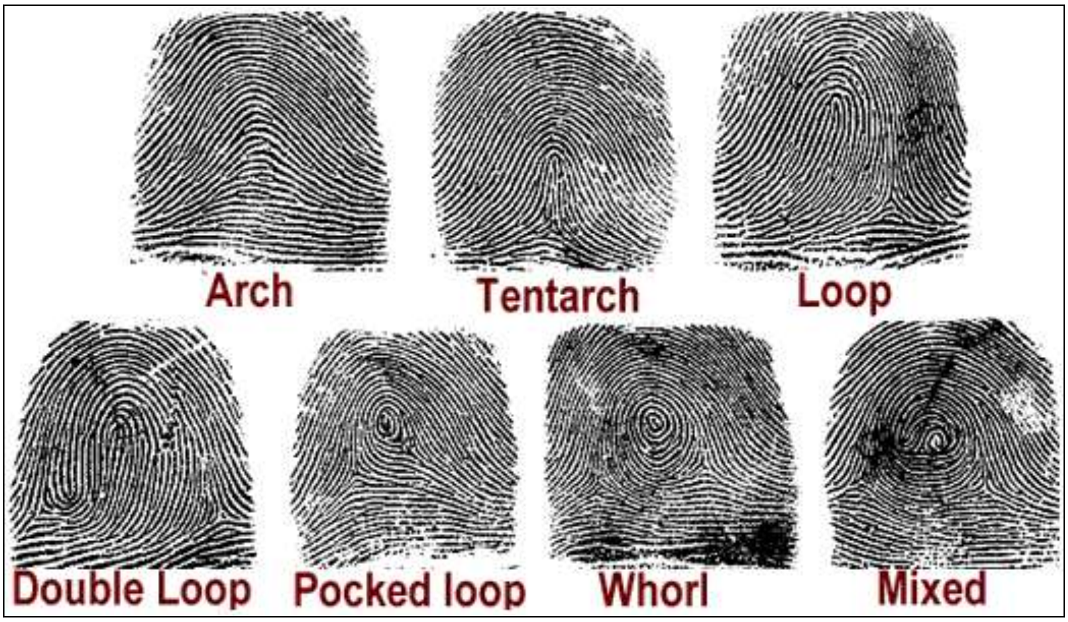


**Fig 4:** Seven predefined classes of Fingerprint Recognition Patterns of type minutiae**.**

Pattern matching analyzes two pictures to determine their similarity, whereas minutiae based approaches rely on the detection of location and orientation for minutiae.

### 1. One can read a fingerprint using methods that rely on optical, capacitance, thermal, or ultrasonic principles [1].

a) Optical methods depend on recording the digital picture created by light reflection at the spots where ridges meet the surface of the sensor. To read fingerprints optically, all you need is a light source, a light sensor, a surface to touch, and a capture device—a charge-coupled device (CCD), a CMOS camera, or even just a webcam - to record the image.
b) A silicon chip with a grid of capacitive plates is the key component of capacitive fingerprint sensors. The finger shapes one side of the capacitor plate, while the other side has a little metallization region on the chip. The ridges on a fingertip are very capacitive since they are so close to neighboring pixels when pressed on a chip's surface. The capacitance is smaller in the valleys because they are relatively far from the pixels.
c) The ultrasonic technique involves placing the user's finger on a piece of glass, which the sensor then moves to detect the whole fingerprint, using high-frequency

sound waves for monitoring the surfaces of the finger. A window of the ultrasonic head is touched with the fingertip. A ring-shaped matrix of electro-acoustic transducers, one, two, or more may be found within the head. The ultrasonic fingerprint acquisition technique relies on the transmission of ultrasonic waves in the direction of the finger and the subsequent detection of their echo.

d) Thermography is most effective for revealing previously unseen fingerprints. Heating paper to temperatures between 220 and 300 degrees Celsius can reveal latent print impressions that are rich in eccrine and sebaceous substances, according to the research. Under irradiation in the 505 nm region, the latent prints may be seen on this heated paper substrate.

**2. The fingerprint detecting method has several advantags**

a) One of these is that it is quite unique.
Fingerprints are unique to each individual.
The fingerprints of twins who are identical, who have th e same genetic makeup, are unique.

b) That is why fingerprints are such a reliable form of iden tification.

c) Fingerprint patterns, or ridges, are hardwired from the moment of conception and do not change throughout a person's life, with the exception of severe injuries.

d) Unless you're an amputee, your fingerprints are readabl e and may be used for authentication purposes even wit hout a token.

e) This method has gained a lot of acceptance.

**3. The Fingerprint Attendance System's disadvantages**

a) Fingerprints that have been damaged can't be recognized.

b) Deployment is not always cheap.

c) There is a risk of fingerprint data theft.

d) Designed more for office workers than those who operate in the field.

e) Compared to facial recognition technologies, accuracy is lower.

f) Compared to facial recognition systems, it is not as efficient.

**4. Falsified fingerprint reproduction is a constraint due to the fact that fingerprints are noisy and distorted due to dirt and twisting. Additionally, there are individuals who feel uncomfortable putting their fingers where others have already touched.**

**Iris Recognition**

Iris Recognition refers to a biometric technique that uses distinctive patterns seen in the ring-shaped area around the pupil of the eye to identify individuals. Since each iris is distinct from the next, they are the perfect biometric verification tool.

Although iris recognition is still a rather uncommon kind of biometric identification, in the years to come we may anticipate seeing greater use of it. One area that is anticipated to advance with increased usage of Iris Recognition is immigration control, as a safety precaution and a reaction to the global danger of terrorism.

Iris recognition is a widely sought-after technique of identification, particularly in fields like border control and law enforcement, because it is a very robust biometric with a fast search speed against big datasets and is extremely resistant to false matches. Iris Recognition is a powerful and incredibly dependable technique for precisely identifying people.

Figure 5. shows the colored circular region that encircles the pupil, which is the iris of the eye. No two iris patterns are the same. Even in the same individual, no two irises will ever be identical.

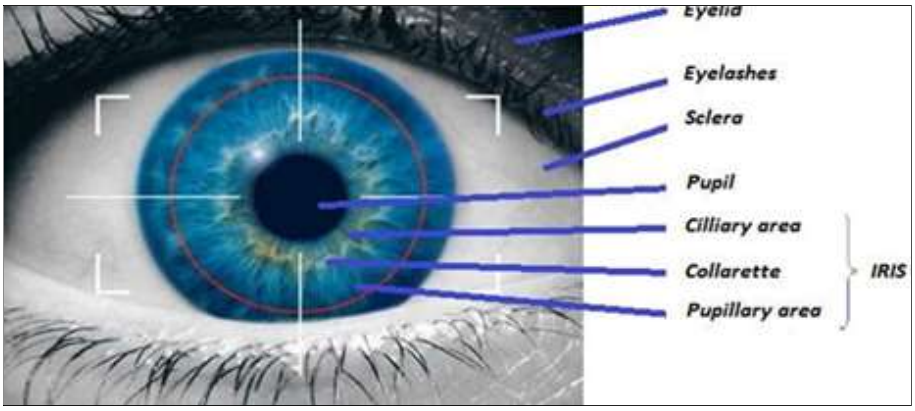


**Fig 5:** Iris recognition.

Various methods for iris recognition may include acquiring images, locating them, segmenting them, and then matching them. A high-frame-rate camera or video-capturing equipment can be utilized to obtain the high-resolution iris picture needed for authentication purposes. Performing the localization phase follows the acquisition of the iris picture. This method identifies the iris region of an image. The iris/sclera (outer) border and the iris/pupil (inner) boundary are two circles that may be used to approximate this [3]. Segmentation, the next step after iris localization, is dividing the input iris picture into many parts. The last stage after iris segmentation and localization is pattern matching using database templates.

Iris patterns do not alter with time, making this method of person authentication quite precise. Due to the need for precise alignment and orientation during iris image acquisition, this approach is not ideal for easy insertion. Results may also be impacted by the fact that pupil size changes in response to changes in lighting.

Identification of human visual nerve characteristics using deep analytics of iris patterns is what iris detection and subsequent recognition is all about [22, 23]. This is seen in Figure. 6.

**Fig 6**: Iris Recognition.

For the purpose of evaluating human qualities and identifying citizens, iris recognition is being used by several governments.

Iris development starts in the third month of embryonic development and is nearly complete by the eighty-first month. We are able to extract similar characteristics from iris due to its complex look and structure (pattern). Although imaging the iris's surface is not very challenging, it is nevertheless something to think about thoroughly. The likelihood of mistake increases, for instance, when working with images that have had their contrast, resolution, and focus adjusted, or when viewing them through eyes whose rotation angles are off. It is also possible to discover identification using this strategy.

The color and texture of an individual's iris can vary greatly from person to person. Therefore, scanning an individual's iris is a suitable means of identification. A scan of the eye's colored region is used in the technique [7]. Iris picture (Figure. 7).

**Fig 7:** Iris image.

**Geometry of the Hand and Palm Print**

Arrays of geometric measurements taken from the hand, such as the circumference, palm diameter, and finger breadth and length, are used by hand geometry based identification systems. For the aim of authentication, vision-based methods are used. Like any other biometric method, it involves acquiring images, extracting features, and matching templates. The methods used to capture images for hand biometrics may be either contact-type or guided, with the former requiring a flat surface upon which to rest the hand and the latter using pegs to direct its positioning, or platform-free and non-contact. Limited and dependent on human interaction. Methods that limit the range of motion for the hands by using a flat surface and either pegs or pins Open and centered on human interaction. A platform is still necessary for peg-free circumstances. No boundaries and no physical touch. situations in which the capture of hand images does not need the use of any platform or pegs [4]; hence, no touch is necessary. Fig. 8: explain hand geometry.

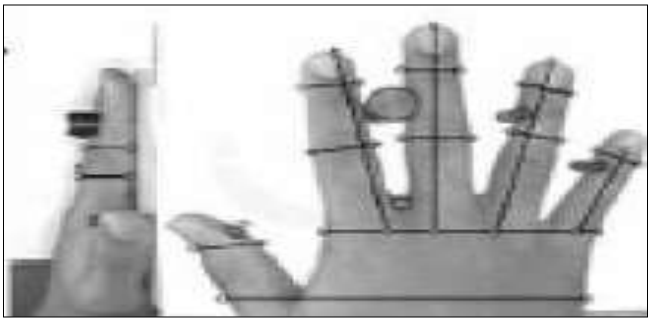


**Fig 8:** Hand Geometry**.**

The dark lines that make up palm prints indicate the ridges and peaked areas of the friction-ridden skin. There are two main approaches to matching: one uses minutiae-based techniques that rely on the position, orientation, and direction of minutiae points, while the other uses ridge-based characteristics such sweat pores, spatial qualities, and geometrical characters. It is possible to utilize capacitive, optical, or ultrasonic sensors, similar to the fingerprint approach. Figure 9. explain Palm Print for biometric detection.

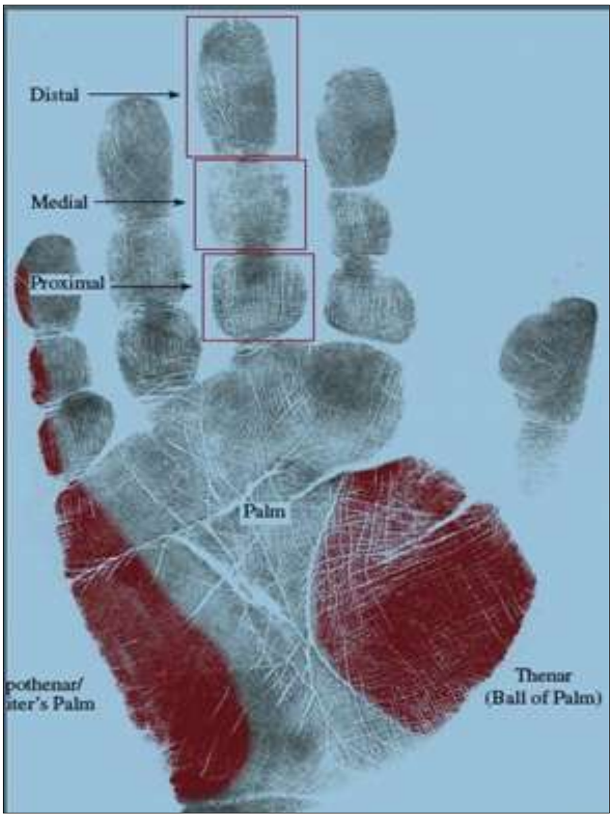


**Fig 9:** Palm Print for biometric detection.

For the purpose of hand geometry recognition, a CCD camera is employed to capture the essential features of the hand. Images of the hand are captured in both the vertical and horizontal planes using this technique, and then they are processed. A number of picture points and lines are presumed to be relevant throughout this procedure. You can find out how long, wide, and thick each finger is using the points and lines. Afterwards, the data is saved in a database by the identification system. It is only after this data is checked with the input data that the individual may be identified. Workers can safely use the geometric approach since it is insensitive to dirt and grime. This approach is well-suited for use in access control systems, and it has the added benefit of not involving the police or criminal justice system, which is a major draw for many potential users. They say it's inefficient since it can't distinguish between several images of people's hands and can only verify the identification of a single person, rendering search apps useless.

### Retina Recognition

Retinal recognition is a biometric method that identifies a person based on the distinct patterns on their retina. The layer of blood vessels at the back of the eye is called the retina. The eye is placed in front of the apparatus at a distance of up to one meter (8 cm) for capture. The task requires the user to align a succession of markers that are visible via the eyepiece. For the scanner to record the retinal pattern, the eye must be optically focused. Near infrared (NIR) light at 890 nm scans the retina to identify the distinct blood vessel pattern. The uniqueness of the blood vessel patterns is used by retina recognition. Commercial development of it began in the middle of the 1970s. According to Sandia Laboratory, less than 1.0% of rejections were incorrect.

For the human eye, retina is analogous to film for a camera. It converts light into electrical impulses thanks to its millions of photoreceptors.

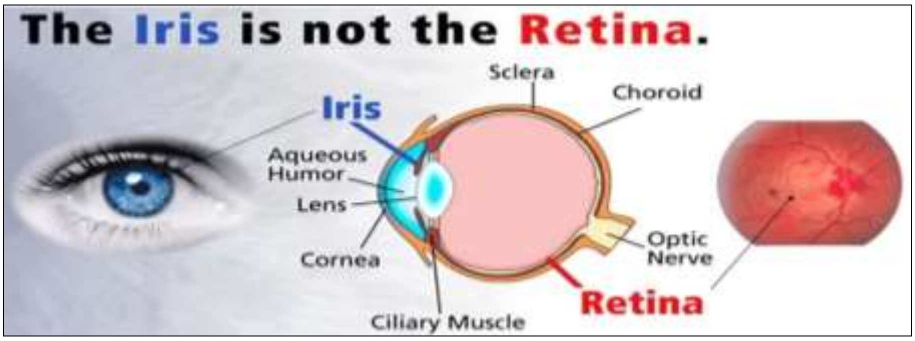


**Fig 8:** Human Retina

A retina-based identification method makes advantage of the retina's distinctive arrangement of blood vessels. Since the retina is located on the back of the eye, it remains steady throughout a person's lifespan despite not being directly visible. The need for an infrared light source to enlighten the retina is further justified for this reason. One benefit of infrared light is that the retina's blood vessels absorb it at a far higher rate than the rest of the eye's tissue. And then the scanning gadget takes all that reflected light and processes it. Acquiring, processing, matching, and representing an image in template form are all steps in the retina scanning process. Compared to other biometric methods, the template size is quite little, typically 96 bytes.

For retina scans, patients need to take their spectacles off, bring their eye close to the scanner, focus on a fixed spot, and hold still for around 10 to 15 seconds while the scan takes place [5].

### Hand or finger Vein Recognition

Vein matching, also known as vascular technology or finger vein biometrics, is a biometric authentication method that examines the patterns of blood veins that are visible through the skin's surface. This method uses near-infrared light to shine on a person's fingers in order to take pictures of the veins inside their hand. It is nearly hard to counterfeit as a result. Furthermore, the presence of blood in the veins during identification verifies that the person being identified is real and living, not a fraudster.

A user's hand vascular patterns are the primary focus of vein identification systems. Vein authentication technology provides a high degree of accuracy in comparison to other biometric systems since the user's veins are situated inside the human body, making them impossible to copy.

A series of near-infrared light-emitting LEDs create a picture by penetrating the skin of the hand and causing the light to be absorbed by the blood vessels. The biometric device's database is built from many templates that are created from this digital picture. Templates may be created using a variety of variables, such as the locations of vessel branches, vein thickness, and branching angles. Both contacting and non-contacting types of vascular imaging equipment are possible. The advantage of the non-contacting technique is that the person providing the biometric data doesn't even have to touch the sensor. This is useful in situations when extreme cleanliness is required, including in operating rooms for medical procedures, or when people are afraid to touch biometric sensors [6]. Fig.11. explain Hand Vascular Pattern.

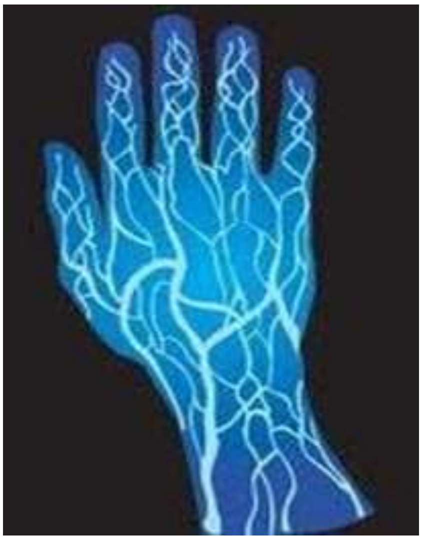


**Fig 11:** Map of the Blood Vessels in the Hand.

A novel approach to person identification using vessel images is introduced. Access control systems operating under network coverage can benefit from this approach (Fig. 12). Registration, data collection, and recognition were the two phases of this investigation. Using near-infrared imaging, the registrar phase gathers N pictures of various people's hands as part of the core curriculum. In order to create adaptive samples, the pictures undergo pre-processing, feature extraction, and modeling. The neural network is then employed for verification. Image detection threshold, edge detection, edge removal, skeleton extraction vessel, resolution improvement employing morphological functions make up the preprocessing in the approach that is being described. Following the application of the wavelet transform to image and statistical feature extraction, the necessary vectors must be created in the feature extraction stage for comparison in the authentication step. Actually, this technology has introduced a new era in identification technology, and the CCD camera can only acquire a picture by means of a hand vein (vein Pattern) [5].

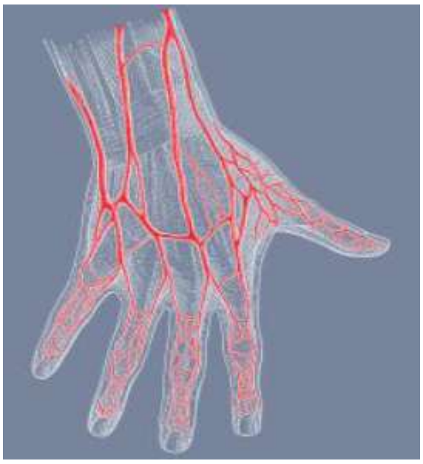


**Fig 12:** The condition of the vessel.

### Facial recognition

Facial recognition identifies human faces using biometrics and technology, usually through artificial intelligence. It maps the characteristics of the face from an image or video, then looks for a match by comparing the data with a database of recognized faces.

By mapping facial traits from a picture or video and then comparing the data with a database of recognized faces, facial recognition technology enables the identification of a human face using biometrics.

a) Although facial recognition technology may be used to confirm identification, privacy concerns are also raised. Here's how it functions:
   Software is provided with a minimum of one video or photograph displaying a person's face.
b) A facial signature is a map of a person's facial characteristics made by software by scanning photos and videos. This contains information about their exact position of eyes, scars, and other facial features.
c) The user's face signature is compared to a database using facial recognition technologies.
   Tens of millions or perhaps billions of photos may be found in numerous databases nowadays.

Whether or whether the facial signature matches anything in the system's database is determined by the face recognition software.

Certain systems could further compute a score for accuracy or provide substitutes.

One definition of facial recognition software is an application that can verify an individual's identity using only a photograph or video clip. Facial feature mapping is the foundation of this technique. Facial feature mapping includes measurements of things like eye-to-nose ratio, nose width, jaw line length, and more. In order to quantify these spots, which are called nodal points, a numerical code is generated, thereby establishing a unique fingerprint for each person. A face in the database is represented by this fingerprint. Facial recognition systems that are automated employ both 2D and 3D methods. See figure 13.

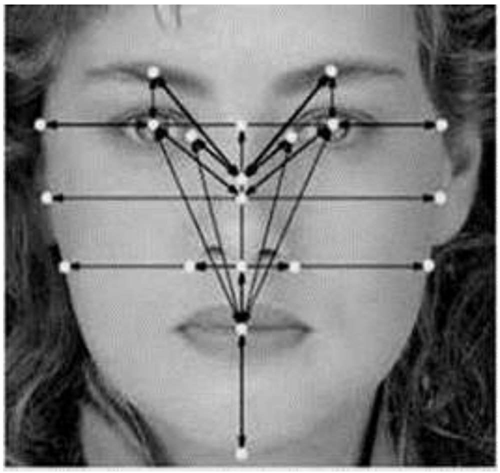


**Fig 13:** Face nodes

Figure 14. Shows an example of face recognition in action, which involves identifying a human face based on its characteristic lines and other characteristics. The training of the soft computing algorithms is based on the distinct and individual structures of each face. References [18, 19].

**Fig 14:** Recognition of Faces.

It's possible to use edge, corner, and pixel evaluations to find a face, and these can be used to make predictions about faces for a variety of purposes [20, 21].

### A) 2D Facial Recognition

2D facial recognition technologies detect faces by comparing digital pictures, such as those obtained by the camera containing a facial recognition authentication terminal, biometric tablet, as well as smartphone, to a database of previously captured photographs. This is the most often used sort of face recognition technology since it is less costly and simpler to apply than other approaches.

The 2D face recognition technique is built using a mathematical model that extracts information from digital images in order to distinguish face nodal points with their distances in a human face, such as the size of the eyes or nose. This sort of software for facial recognition as well as algorithm works through comparing face traits inside a picture to those in existing data sets, allow it to create an individual's identification with accuracy.

The Eigenfaces algorithm, 2D Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and other approaches are utilized in 2D facial identification. Each one of these face recognition systems has distinct qualities and advantages. See figure 15.

**Fig 15:** 2D facial recognition technologies.

### B) 3D Facial Recognition

Three-dimensional face recognition (3DFR) has become a powerful tool for identifying individuals based on their faces. There are two main schools of thought when it comes to recognizing techniques: the conventional and the modern. While the latter mostly use deep learning to do 3DFR end-to-end, the former often extract unique face characteristics (e.g., global, local, and hybrid features) for matching.

One of the biggest issues with face recognition is its sensitivity to facial expressions. This is solved by the geometric framework for 3D face identification that is shown here. Facial expressions, being an intrinsic feature of the human face, are more challenging to manage than external variables such as lighting or posture. When doing facial recognition in the wild, this issue becomes much more apparent.

The curvature of the nose, chin, and eye sockets areas where the face's underlying hard tissue and bone are most noticeable are utilized by 3D image recognition algorithms in real-time face identification. You may use this method to identify a topic from various perspectives since it relies on depth and an axis of measurement that is unaffected by illumination. See Fig. 16.

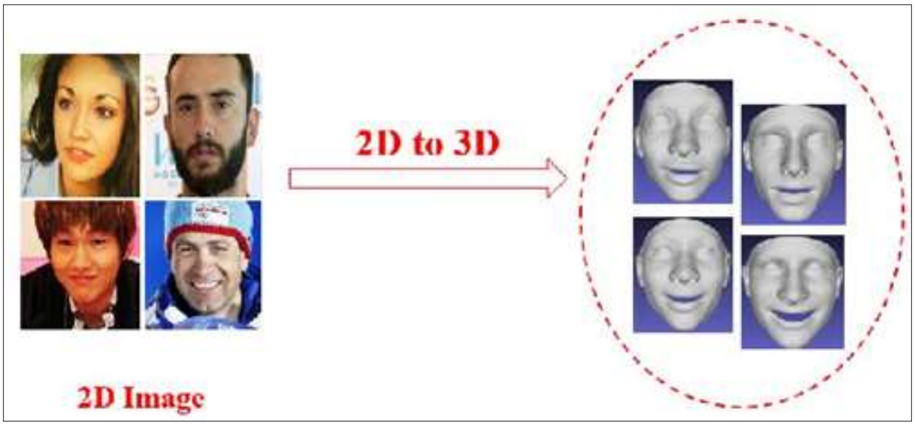


**Fig 16:** The features of 3D recognition.

### Biometric methods based on Behavioral

Behavioral biometrics is a method of user authentication that collects data from the user's actions. It stands in contrast to physical biometrics, which focuses on physically identifiable information (such as fingerprints and facial recognition) to evaluate human qualities.

Each user is associated with a certain set of behavioral attributes, which are known as behavioral biometrics. By analyzing a user's actions in the past, behavioral biometrics can detect fraudulent activity and confirm their identity. Companies may offer a better secure experience for clients with behavioral biometrics, which is passive as it doesn't need any activity from the user. Behavioral biometrics, its applications, classifications, and advantages in the context of cybersecurity will be covered in this blog.

It can also be divided Behavioral biometric technique has four main sections:

a) The Sensor Block: is in charge of collecting biometric data.

b) The Extracting Features Block: works with the data collected to determine its vector features.

c) The Comparing Block: Its job is to check the earned vector against predefined templates.

d) If you want to accept or reject identification, you'll find it in the decision block.

Biometrics is the study of human characteristics with the aim of developing reliable methods of personal identification. It is anticipated that this approach will outperform more conventional ways in the past. The system's performance in real-world scenarios may be measured by comparing the ratio of false positives to false negatives, or FAR and FRR, respectively. To be used in the system as biometric features, a biometric identifier has to meet certain criteria:

a) Distinctness: In their own special way, every single person stands out from the crowd.
b) Obtaining responsibility: the capability might be obtained rapidly and without requiring intensive processing for every single instance.
c) Capable of high resolution: two people are inherently indistinguishable from one another.
d) Sustainability: Persistence across time and life events; the extracted characteristics do not change. Here we shall introduce some of the most popular biometrics, in accordance with Figure 17.

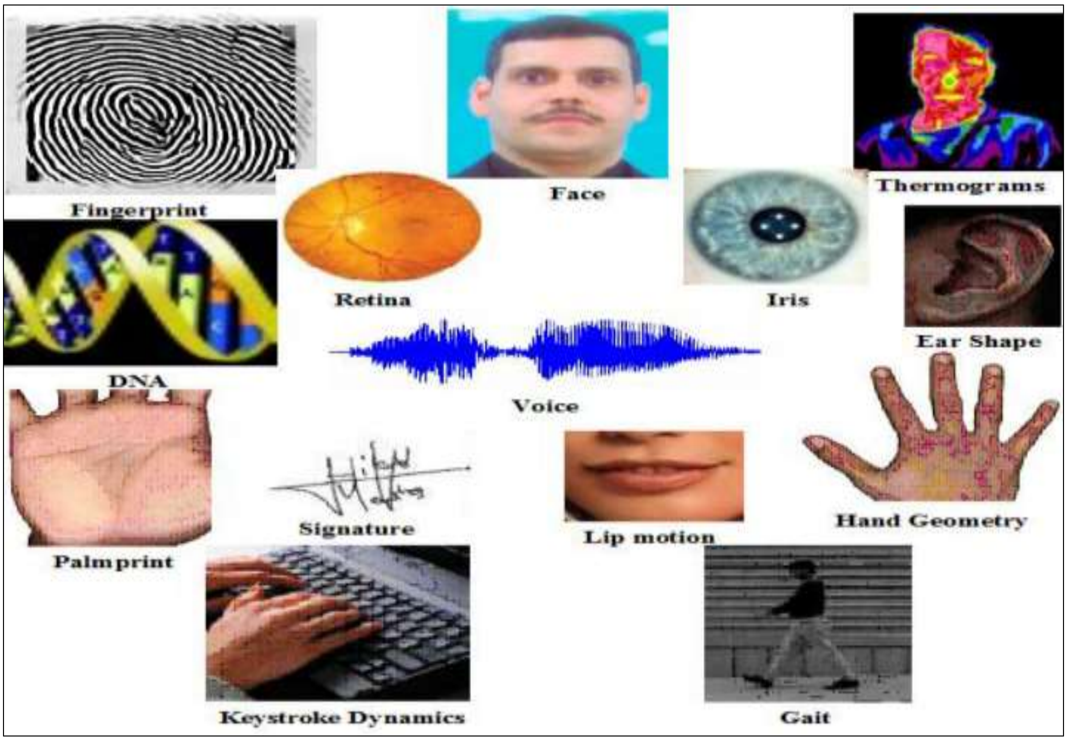


**Fig 17:** Behavioral, physiological biometrics.

### Recognition of Dynamic Signatures

A dynamic signature is a form of biometric authentication that makes use of the physical and behavioral traits that a person displays when signing a name or other word.

There is a difference between dynamic signature devices and electronic signature capture systems, the latter of which is used to take a picture of the signature and is prevalent in places where businesses collect them to authorize transactions.

In order to analyze a person's handwriting, dynamic signature recognition makes use of many features. These traits are gathered via touch-sensitive technology, including digital tablets or personal digital assistants, and their use and significance differ among vendors.

Everyday life relies on people's signatures to authorize monetary transactions, legal papers, contracts, and more. At one point in this procedure, the outside look of the signature was the main concern. One way to look at it is as comparing signatures. Users can accomplish real-time signature capture using dynamic signature recognition by writing their signature on a digital tablet that is often linked to a personal computer to perform processing and verification [22]. Timing, writing pressure, and speed are all behavioral characteristics that are intrinsic to signing. Duplicating a signature's visual look is very easy, but duplicating its behavioral qualities is quite challenging. Typical examples of dynamic data utilized for recognition purposes include x and y coordinates, pressure, azimuth, inclination, velocity, and acceleration. For the sake of comparison, this data is utilized. **Fig.17.** Signature Recognition.

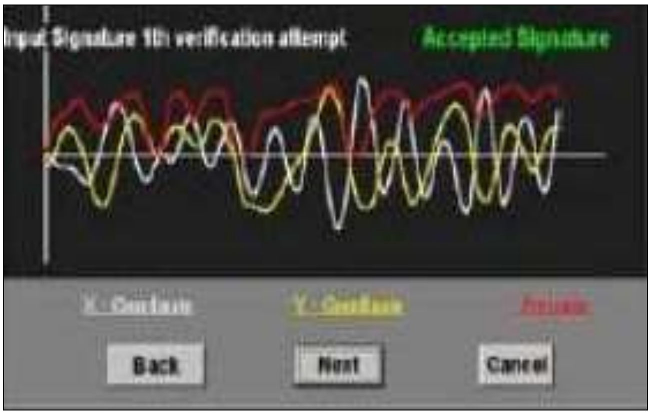


**Fig 18:** Signature pattern Recognition.

To authenticate a user's identity on a computer, dynamic signature verification technology employs the behavioral biometrics of a handwritten signature. To do this, data on the signature process's shape, velocity, stroke, pen pressure, and time is analyzed. See Figure 19.

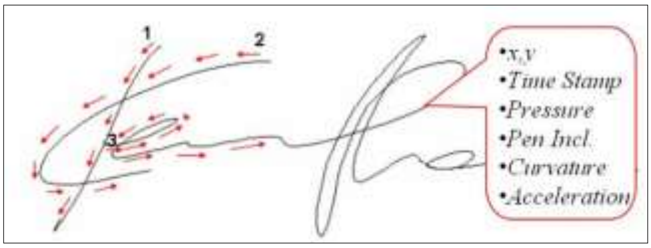


**Fig 19:** Biometrics Research Group.

Wet signatures, electronic signatures, digital signatures, and clickwrap signatures are the four most common types of signatures utilized in commercial settings. One or more of these ways may be required when you sign significant documents or agree to a contract, depending on the circumstances.

Though it's simple to fake a signature, imposters have a hard time trying to "mimic" the behavioral patterns that are intrinsic to signing, which is the main advantage of Signature Recognition. Signature Recognition, in contrast, has a greater mistake rate, especially when the signs' behavioral traits are contradictory.

Static approaches are regarded as two-dimensional images devoid of time-dependent information that serve as a signature. As a result, the signature may be verified using its static, time-invariant features. Consequently, the process of recognizing signatures turns into a routine pattern recognition procedure. Since the signature pattern will inevitably change, this method's signature verification procedure may be restricted to identifying and mapping the region of significant changes [6].

Rather than comparing the signature after it has been made, the sign dynamics recognition is dependent on the dynamics of the signature being made. The pressure, direction, acceleration, and length of the strokes—as well as the number and duration of the strokes—are used to assess dynamics. The most evident and significant benefit of this is that by glancing at a previously created signature, a fraudster cannot learn how to write the signature. The trademark dynamics are recorded using a variety of devices. These are either specialized gadgets or conventional tablets.

The technique for detecting signatures examines the user's writing style. This approach evaluates the pen pressure change mode as well as the case of written instructions in X and Y. Motion and pressure sensors are either within the pen or beneath the paper to perform this. The sensor has accomplished pressure, direction, and speed, as previously described. Next, as the data are being processed, a simultaneous vector is made, and the data from the two vectors are contrasted. The two primary categories of signature recognition techniques are dynamic (online) and static (offline). Tablets record pressure and 2D coordinates [11, 21], see figure 20.

**Fig 20:** A Signature taken using Tablet

Three-dimensional motions can be recorded with specialized writing instruments. There are two main drawbacks of tablets. Initially, the digitalized signature that is produced appears distinct from the typical user signature. Second, the user does not see what they have previously typed when they sign. To view the signature, he or she must glance at the computer monitor [4, 37]. For many (inexperienced) users, this is a significant disadvantage. Certain special pens function similarly to regular pens; they may be used to write on paper and contain an ink cartridge.

**Pattern Recognition by voice**

Machines and programs with voice or speaker recognition capabilities may take in and process spoken instructions or dictation. With the proliferation of AI and smart assistants like Siri and Alexa from Apple and Amazon, voice recognition has become more popular and widely used.

Customers can now ask for things, set reminders, and do other basic chores with the simple voice of their voice thanks to voice recognition technologies.

With the use of automated speech recognition (ASR) software, voices may be recognized and differentiated. To get the most out of their speech-to-text conversion, users of some ASR applications have to teach the software to identify their voice. Automatic speech recognition systems analyze the tempo, intonation, and pattern of a speaker's voice.

The terms voice recognition and speech recognition are sometimes used interchangeably, however there is a significant difference between the two. While speech recognition analyzes the content of spoken words, voice recognition detects who is speaking.

Two factors allow for the possibility that a person's voice might be a biometric characteristic. First of all, the voice is a physiological phenomenon that arises from the operation of the vocal tract. Also, it's a character flaw that manifests itself in the form of an accent in one's voice. When you add these two things together, it becomes quite difficult to mimic someone else's voice precisely. Sound, in the form of human speech, may be transformed into electrical impulses using voice recognition technology. In order to facilitate authentication, these signals are encoded. With the use of a microphone, the spoken words or phrases are recorded. In order to calculate the likelihood ratio, input speech samples are compared with enrolled models. Fig.20. Signal from Voice Recorded by Sensor

**Fig 21:** Signal from Voice Recorded by Sensor

Recognition systems should also take into account the natural variations that occur in a person's voice as they age. Also, intruders can acquire access control by recording the voices of authorized users and then running the recording through the verification procedure. During the verification process, speech recognition systems will require users to repeat a series of randomly generated words in order to prevent illegal access using recording device

Due to the massive volume of data that needs processing, the computing cost is rather significant. As seen in **Figure 22.** More and more, voice recognition systems are focusing on signals analytics, which include training and prediction of speech pitch and volume [24, 25]. Many different types of criminal investigations and human characteristic identification employ this method [26].

**Fig 22:** Voice Recognition.

When using the speech recognition technique, it modifies the data before comparing it with the reference set. Its association with a particular text is fading as identification by speech technologies grow. Although "sound spectrogram" devices are used by contemporary technologies, most people still picture oscilloscopes and speech frequencies when they think about voice recognition. Actually, a sound spectrogram is a graph that displays the time in seconds on the horizontal axis and the frequency of the sound on the vertical axis. In this scenario, a unique graph will be created for every sound or voice. Using colors and shadows to display the graph, the gadget enhances accuracy and acoustic sound quality. Small things, like flu-like voices, can have a big impact on the sound and make it hard to make out details because speaking is an ever-changing process. However, aspects like accent, word stress, and speech pace little impact this procedure. The speaker authentication mechanism is depicted in Figure 23, which provides an overview.

**Oday Ali Hassen, Shahlaa Mashhadani and Iptehaj Alhakam SUJPS 2022 (November), Vol., No., p.p.:**

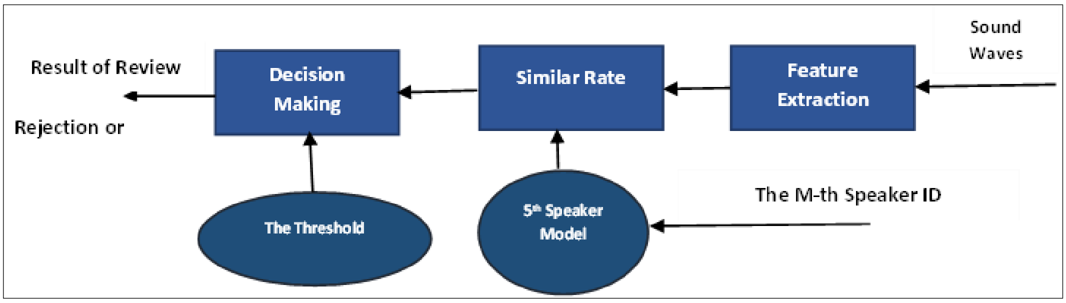


**Fig 23**: An outline of methods for recognizing speaker

**Tongue Biometric recognition**

A novel biometric authentication technology, a tongue print is both distinctive and difficult to fabricate due to the fact that no two prints are identical.

In biometrics, a person is instantly identified by comparing their unique physical or behavioral traits to a database of records from a large number of other individuals. One way this is accomplished is by employing a biometric scanning equipment, such as a tongue-print scanner, which records the user's unique biometric information and then digitizes it for computer analysis and verification. This kind of identification provides a more solid guarantee [2]. The shape and texture of the exposed tongue carry information known as a tongue print.

The tongue's physiological surface roughness and geometric form are quite consistent [3]. Unlike other forms of identification, the tongue is both clearly visible for examination and well shielded from environmental factors, making it exceedingly difficult to alter or fabricate [4].

Research has shown that even identical twins' tongues don't look exactly like each other, adding to the uniqueness of each individual tongue print [5]. There are static and dynamic authentication features provided by the tongue. Biometric identification systems that involve tongue prints are thus rapidly expanding in popularity [6]. A tongue print identification system has been the focus of study for the last ten years.

When it comes to biometric identification, tongue prints are really handy. The study's technique is straightforward and easy for dentists to use regularly. Further validation of the results and identification of additional tongue traits for application in forensics and biometric authentication processes would necessitate large-scale investigations.

Figure 24 shows the human tongue, which has a distinct form and characteristics that make it a potential underutilized biometric item. What follows is a representation of human characteristics based biometric identification using the tongue.

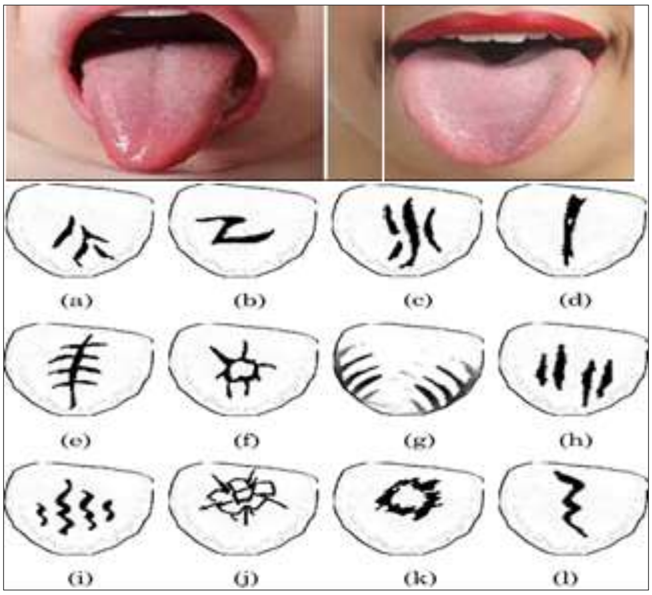


**Fig 24:** shows the human tongue

**Recognition by Gait**

The person is identified from a database by the system after it evaluates the walking characteristics, height, pace, and silhouette. Because it is less noticeable than fingerprints or retinal scanners, this method is more practical in public areas.

In the intriguing field of gait identification research, people are identified by studying video sequences of them walking. It's a non-invasive biometric technique that uses a person's walking pattern to identify them at a distance without requiring their involvement [93]. See figure 25 explain human gait.

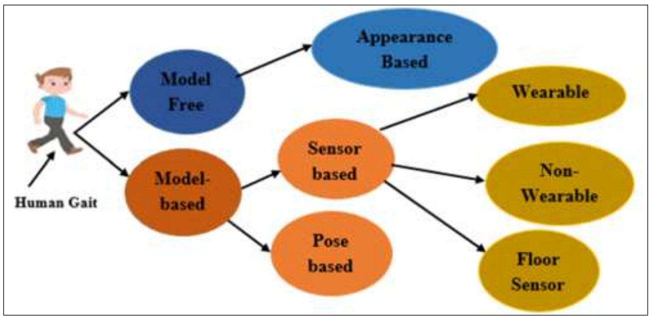


**Fig 25:** Explain human gait cycle.

Many different settings have found uses for gait recognition systems, including security, medical examinations, identity management, and access control. These systems need a complex combination of technological, operational, and definitional options. a variety of techniques are employed in clinical gait analysis, such as:

a) Computerized video cameras to depict action in slow motion.
b) In order to track movement on camera, markers are applied to the skin.
c) A platform with sensors that monitor the force of a footstep and the length of a stride.
d) Electrodes applied to the skin for the purpose of tracking muscular activity.

One distinct advantage to gait recognition is that it can record gait remotely, without the subject's knowledge or permission, which is a huge plus. The gait recognition system uses automated motion feature extraction to verify the identification of the moving subject.

Gait is thus a novel biometric that provides significant operational advantages over several other biometrics such as face, fingerprint, iris etc. Unlike traditional biometrics like fingerprint, gait does not require the active cooperation of the subjects.

One reason for doing gait analysis is that it is a kind of behavioral biometry. When it comes to physiological biometry, systems can only handle data collected at a certain moment in time.

The proposed method comprises three stages: pre-processing, feature extraction, and recognition; there have been many attempts to identify individuals based on their gait in video images, and these methods can be broadly categorized into two groups: statistical approaches and model based approaches. According to the results of this method's evaluation, the preparation step often consists of executing a basic background removal algorithm without any significant effort being done. The suggested technique for person-from-gait identification makes use of pre-processing to get a good idea of the backdrop and for object detection, a novel approach based on fuzzy sets, and a new algorithm based on Warping Dynamic Time for the recognition phase. This is seen in Figure 26.

**Fig 26**: illustrate gait analysis.

**3. System for Biometric Assessment and Identification**

Particularly in the more outward features of a human being, such as the iris and fingerprints, the topic of human identification is currently expanding into one of the most expansive study domains in which scientists have handled and achieved extremely powerful findings. Consequently, there was a discrepancy between the precision of the findings and the discrepancy, and even the expense, which became crucial in the application during a period when the world was preoccupied with material concerns and expense. Table 1. show the distinctions between several forms of human identification.

**Table 1:** With Different Biometrics, We Consider Accuracy, Cost, and Other Considerations.

| Biometric Technology | Accuracy | coast | Devices required | Social acceptability |
|---|---|---|---|---|
| And | High | High | Test equipment | Low |
| Iris recognition | High | High | Camera | Medium-low |
| Retinal Scan | High | High | Camera | Low |
| Facial recognition | Medium-low | Medium | Camera | High |
| Voice recognition | Medium | Medium | Microphone telephone | High |
| Hand Geometry | Medium-low | Low | Scanner | High |
| Fingerprint | High | Medium | Scanner | Medium |
| Signature recognition | Low | Medium | Optic pen touch panel | High |

## 4. Biometric System Component

Qualities, both observable and explicable in terms of conduct. Biometric technology encompasses a wide range of methods that consistently identify individuals by their unique set of observable physiological or behavioral traits. Biometrics has its origins in a field that is thousands of years old. It follows that the biometric system's components are not universal but rather type-specific, responding to differences in user profile and operational difficulties. Here are the figures that demonstrate this: 26, 27, 28, 29

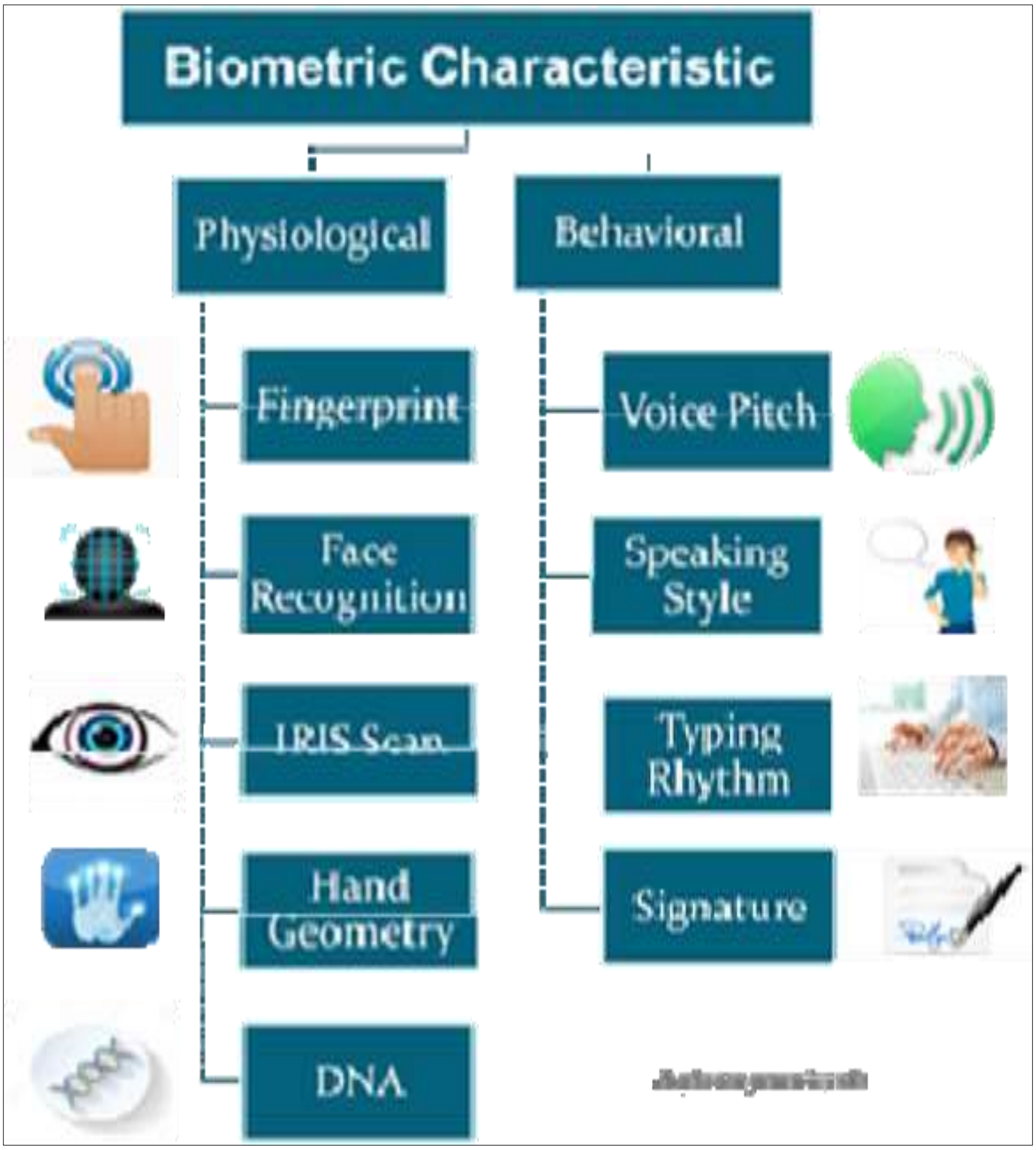


**Fig 27**: Biometric Components

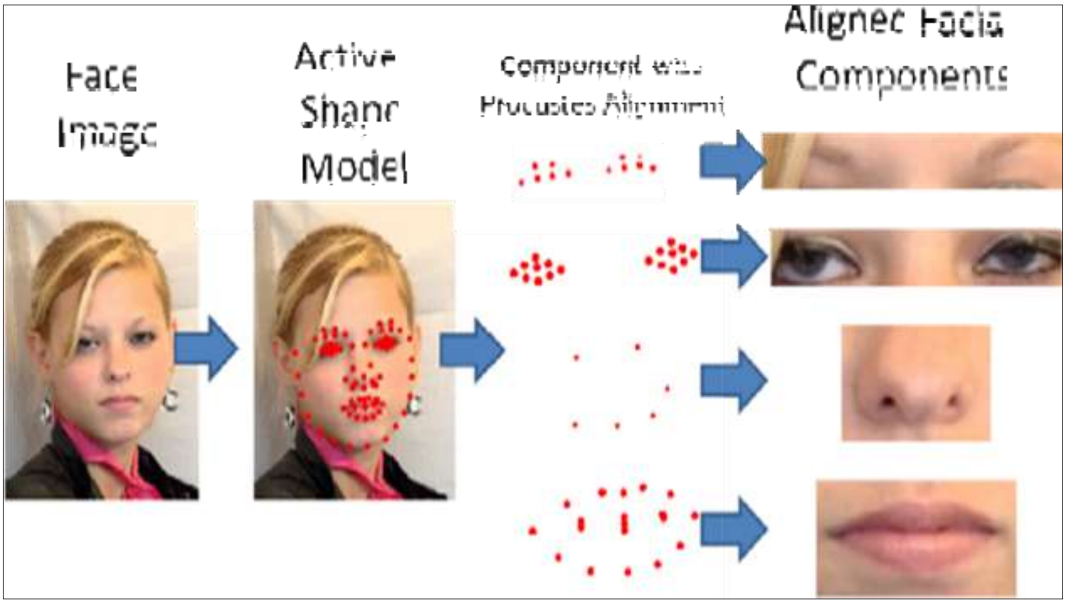

Face Image
Active Shape Model
Component with Procrustes Alignment
Aligned Facial Components

**Fig 28:** Biometric Components.

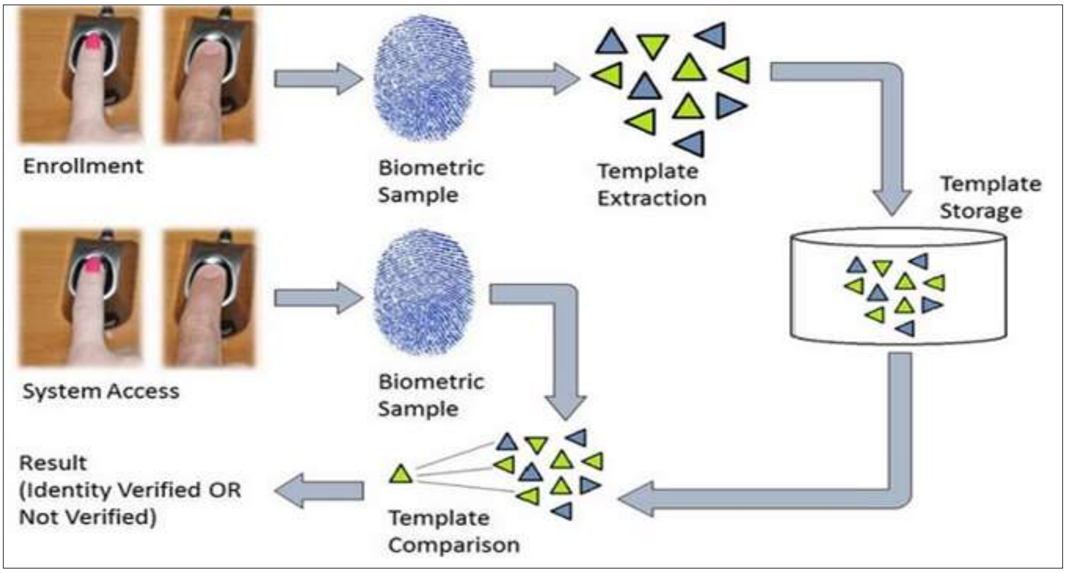


**Figure- 29**: Biometric Components.

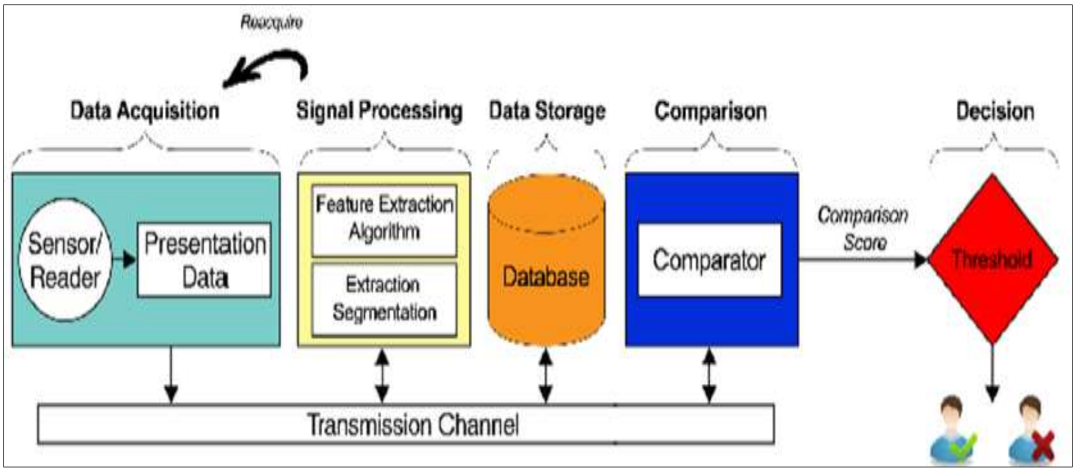


**Fig 30**: Biometric Components.

## 5. Biometric Benefits

One reliable method of protecting sensitive information stored in digital formats is biometric authentication. When compared to more conventional forms of verification, it offers superior safety and convenience. Privacy issues, false positives, and expensive prices are some of the downsides.

Benefits of biometric indicators:

a) The difference between them and passwords is that they are associated with a specific person.
b) You won't have to worry about carrying or remembering anything with them, making them quite convenient.
c) They are quite resistant to fraud in terms of security.
d) Accurate Identification
e) Ease of Use
f) Resistance to Forgery
g) Security
h) Scalability

## 6. Applications

**a) In forensic science**, a database is used to match the features of a deceased person or convicted offender. Even with skewed data, certain programs may still find a face that looks close to a given one. Gomes, Lee.

**b) Authentication systems:** It is an authentication job, and it involves checking the database of all enrolled claimants to make sure no one is claiming using more than one identification for every newly enrolled application. Gomes, Lee.

**c) Surveillance:** It's likely that the field of surveillance is the one interested in facial recognition the most. For obvious reasons, recognition of faces is the ideal biometric worldwide video data used in identification applications, and video is the preferred medium for surveillance due to the abundance and variety of information it carries.

**d) Pervasive Computing**: Although pervasive or universal computing is not yet economically viable, it is anticipated to become an important arena in which face recognition will play a significant role.

Biometric applications are multi-faceted, serving many purposes in the analysis of human characteristics, both external and internal. Biometrics refers to techniques that automatically identify or verify people by analyzing their unique behavioral or physiological traits. Technologies that use biometrics include:

1) Face Recognition
2) Face Smile Detection
3) Voice Recognition
4) Hand Geometry Identification
5) Iris Identification
6) DNA Sequence Matching
7) Signature Recognition
8) Finger Print (dactylogram) Identification
9) Retina Identification

## 7. Evaluation

Consideration of safety measures is essential prior to using biometric authentication. Many different kinds of biometric authentication methods have been covered in this article. Here we shall assess several methods and determine the level of safety. The efficacy of any biometric authentication method may be evaluated using a number of criteria. Following is a description of these elements [28-30]. Table 1 shows the evaluated vales of various evaluation techniques.

### Factors of Evaluation

Consideration of safety measures is essential prior to using biometric authentication. Many different kinds of biometric authentication methods have been covered in this article. Here we shall assess several methods and determine the level of safety. The efficacy of any biometric authentication method may be evaluated using a number of criteria. Following is a description of these elements [28-30]. Table 1 shows the evaluated vales of various evaluation techniques.

**FAR (False Acceptance Rate) and FMR (False Match Rate):** FAR and FMR: The likelihood that the system mistakenly reports an accurate match between the pattern entered with a nonmatching pattern within the database when, in fact, there is no such match. The percentage of matches that do not match is quantified. Because they are frequently employed to prohibit particular behaviors by forbidden individuals, these systems are crucial.

**FRR (False Reject Rate) or FNMR (False Non-Match Rate):** The likelihood that the system reports a failure of matching between the input pattern with the matching templates in the database inaccurately. It calculates the percentage of valid inputs that are rejected.

### Relative Operating Characteristic (ROC)

In general, the method of matching makes a judgment based on some parameters (for example, a threshold). In biometric systems, the FAR and FRR are often trade-off factors that may be changed. The ROC plot is created by plotting the FAR and FRR values while altering the variables indirectly. The Detection Error The trade-off (DET), which is derived using normal deviation scales on both axes, is a frequent version. This more linear graph highlights the differences between greater performance (fewer mistakes).

### Equal Error Rate (EER)

There is parity between the acceptance and rejection error rates. It is easy to see the effects of changing FAR and FRR when using ROC or DET charting. It is usual practice to utilize the ERR when comparing two systems quickly. Retrieved from the ROC plot by locating the point where the FAR and FRR values are equal. When the EER is low, it means the system is very accurate.

### Failure to Enroll Rate (FTE or FER)

The inputted percentage of data is considered incorrect and is not entered into the system. Failure to enroll occurs when the sensor receives data that is deemed invalid or of substandard quality.

### Failure to Capture Rate (FTC)

In automated systems, the FTC refers to the likelihood that a biometric trait will not be detected by the system even when it is supplied correctly.

### Template Capacity

Its definition is the largest number of data sets that can be entered into the systems.

### Results of Evaluation

A tabular style is used to display the assessments of different methodologies with respect to the aforementioned factors.

### Finger Print Technology

Technology based on fingerprints: Because moisture has a major impact on capacitance, it also affects the fingerprint bit map that is acquired from the scanner. Because of this, individuals with abnormally wet or dry figures have issues using these silicon figure print readers, as bitmaps produced by them are of insufficient quality.

### Face Recognition Technology

Technology for Facial Recognition: While facial recognition systems are becoming better, they still haven't met my expectations. A better algorithm for face location is required. In many cases, the present software either fails to detect the face altogether or locates "a face" in the wrong location. This degrades the outcome. Additionally, the algorithms have trouble differentiating between extremely similar people, such as identical twins, and re-enrollment is necessary for each major hair or beard style change. spectacles further complicates things. You can deceive it with a photo and it won't even need to touch a human if you don't have any countermeasures in place. Facial mimics provide the basis of liveness detection in most cases. It is requested that the user grin or blink. You may say the individual is "alive" if the picture updates correctly.

### Technologies of Iris

I Due to its one-of-a-kind characteristics, creating an artificial copy of an iris is an extremely challenging task. Some believe that the iris, which has strong connections to the brain, is among the first bodily components to decompose after death. As a result, if the iris liveness detection is functioning as it should, it should be exceedingly difficult to fabricate an artificial iris in order to fraudulently circumvent the biometric devices.

### Techniques for Hand Geometry

To use it properly, one must ensure that their hand is properly positioned, that they have included guidance markings, and that the units are installed at a comfortable height for the majority of people. Because the silhouette of the hand form is all that matters, noise elements like dirt and oil aren't a big deal. A vast data set is not generated by hand geometry. Thus, given a big enough dataset, hand geometry might not be able to differentiate between individuals well enough. In many cases, the hand template is just 9 bytes in size. Those kinds of systems are completely unfit for identifying purposes. Application at a lesser degree of security is demonstrated.

### Retina Geometry

The most significant issue with the retina scan is how invasive it is. A retina scan requires an intrusive procedure that you must undergo on your own. It is necessary to guide the laser light via the cornea or edge. Retinal scanners are also not straightforward to use. The individual being scanned must adhere to the operator's instructions, which need expertise. Retinal scanning devices, on the other hand, are supposedly accurate and employed in situations requiring high levels of security.

### Method for Voice-Recognition Speakers

The biggest benefit of speaker verification systems, according to speaker recognition technique (voice), is that they don't necessitate any specialized and costly hardware. You may utilize it from a distance using your phone as well. Background noise is a major issue that reduces accuracy, although a high sample rate isn't necessary. Because it relies on behavioral traits, it might be adversely impacted by one's present physical and emotional state.

### Technique for Verifying a Signature

No two people's signatures are ever exactly same. Since this is the case, there needs to be some wiggle room in the data collected from a person's signature. In terms of signature dynamics systems, the majority primarily check the dynamics. The resultant signature is completely ignored by them. A small number of systems assert that they can validate not just the signature dynamics but also the final signature appearance. From what we've seen, the acceptable signature can appear quite different from the master template if the system doesn't check the resultant dynamics vs. signature. Because decision-makers typically place a premium on writing swiftly, it is theoretically feasible to successfully counterfeit a signature, even if the resultant signature is noticeably different. The data acquired during the signing procedure is around 20 KB in size. The size of the master template might range from a few kilobytes to around 90 bytes, depending on the number of signatures used. Signature recognition struggles with match discrimination when the master template size is rather large, making it unsuitable for anything other than verification. While manufacturers claim a crossover rate of about 2% for signature dynamics biometric devices, our own experience has shown that this is far lower. The following table. 2 shows an analysis of the evaluation results.

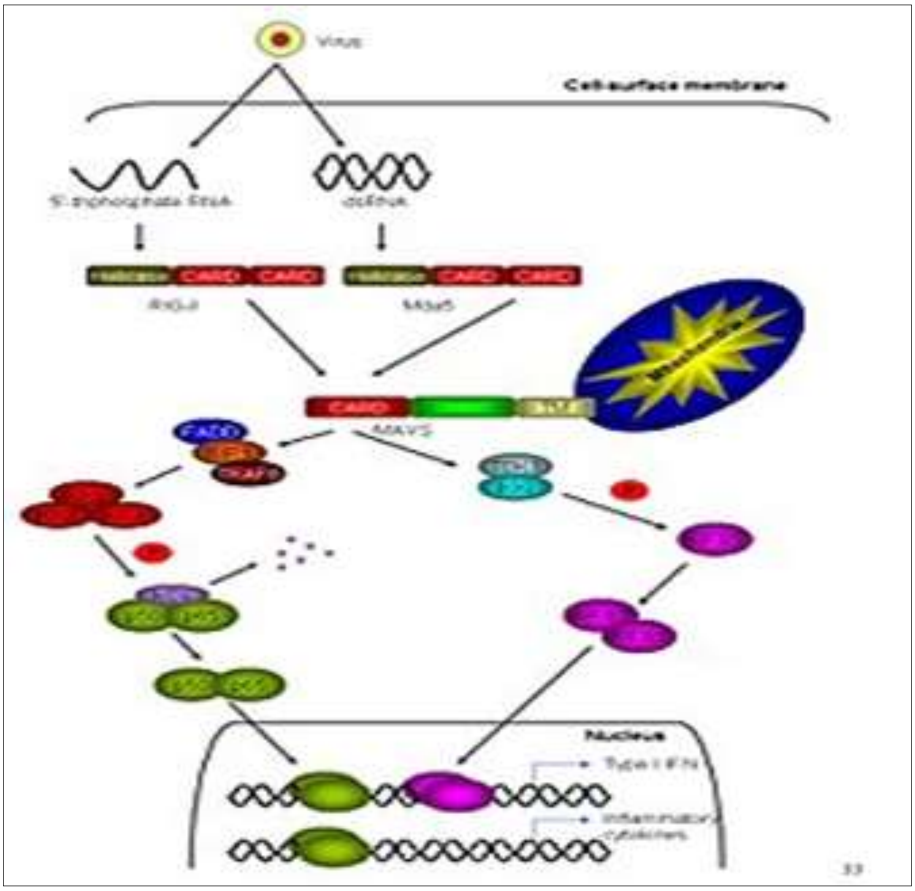
**Table 2:** Assessment of Biometric Methods

| Biometric | EER | FAR | FRR | Subjects | Comments |
|---|---|---|---|---|---|
| Face | NA | 1% | 10% | 37437 | Varied light, indoor outdoor |
| Finger print | 2% | 2% | 2% | 2500 | Rotation and exaggerated skin distortion |
| hand geometry | 1% | 2% | 2% | 129 | With rings and improper placement |
| Iris | .01% | .94% | .99% | 1224 | Indoor environment |
| keystrokes | 1.8% | 7% | .1% | 15 | During 6 months period |
| Voice | 6% | 2% | 10% | 30 | Text dependent and multilingual |

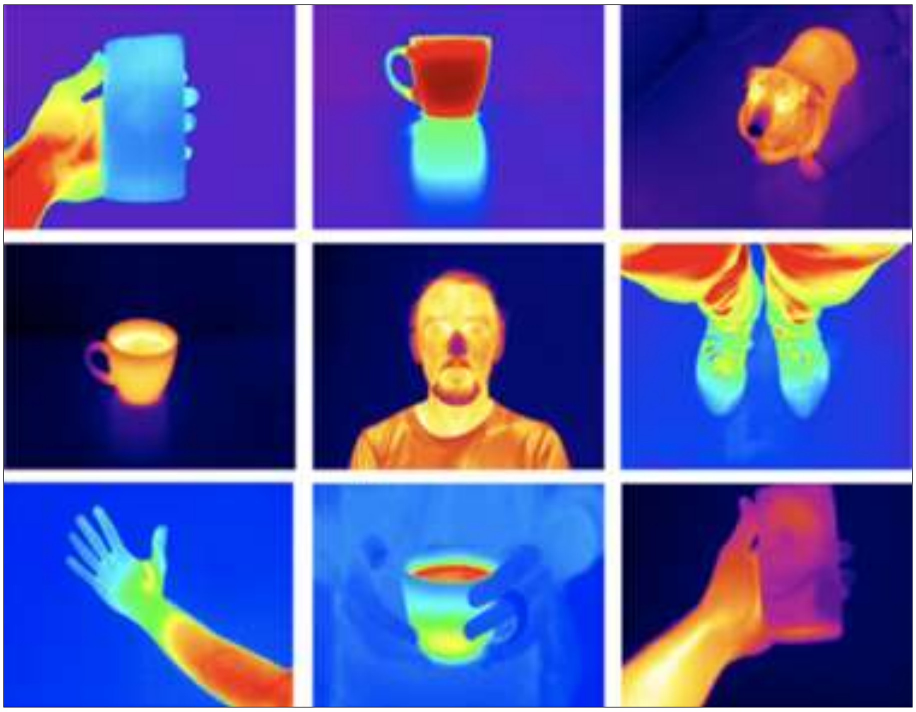
## 8. Other Techniques

Some other available techniques for biometric authentication are described below.

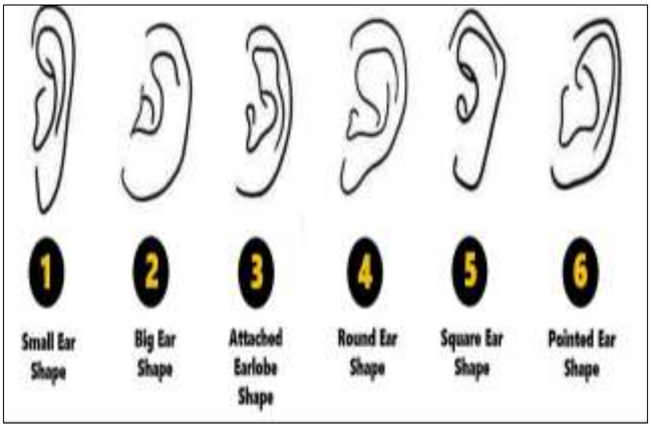
**1. DNA:** DNA sampling is somewhat invasive and needs a sample of tissue, blood, or another body fluid. This capturing technique still needs to be improved. To yet, DNA analysis is not yet automated enough to be classified as a biometric technology. It is now feasible to analyze human DNA in ten minutes. It could become more important as soon as technology develops to the point where DNA can be linked automatically and in real time. Since the use of biometric DNA is already widely used in criminal detection, it will continue to be used in law enforcement for the foreseeable future [2, 4, 16].



**Thermal imaging:** The vein geometry of the hand is comparable to this technique. In order to create a picture of the vein pattern in the wrist or face, it additionally makes use of an infrared light source and camera [17].

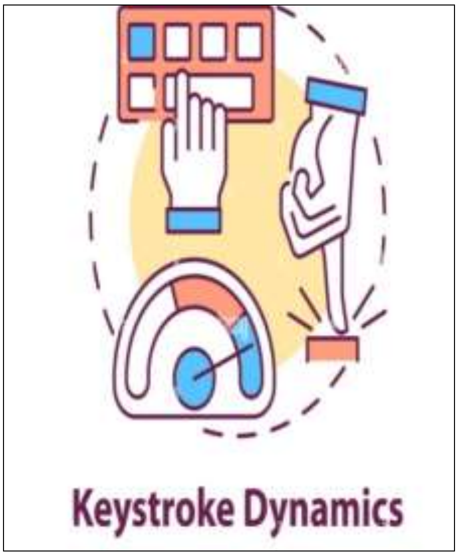


**Ear Shape**: Wherever ear marks are discovered at crime scenes, the ability to identify individuals based on their ear shape is utilized by law enforcement. It is yet unclear if this technology will find its way into access control applications. Otophone, made by the French firm ART Techniques, is an ear shape verifier. A lighting unit and cameras that take two pictures of the ear are housed in a telephone-style handset [4, 18].



**Body Odor Sensor:** An electronic nose can detect a broad variety of odors thanks to its array of smell sensors. A state-of-the-art data processing approach is essential for dependable electronic nose systems. Machine learning is one of the most important methods used in electronic nose design

**Keystroke Dynamics**: A technique that can handle both professional typists and the occasional novice with just two fingers on the keyboard is keystroke dynamics, and it uses a person's typing rhythm to confirm their identity. Systems can either check the user's identity when they log in or keep tabs on a Biometrics Systems 32 typist all the time. Since a software package is all that is required to implement these systems, the cost should be minimal [12, 35].



**Fingernail Bed:** The American firm AIMS is working on a technology that can scan the skin tissue directly beneath a fingernail. Skin that is rich in blood vessels is arranged in almost parallel rows to form this tongue-and-groove pattern. A key metric used by the AIMS system is the distance from these parallel dermal structures, which are represented as thin channels [30].

**Discussion**

Physical human characteristics are substantially harder to fabricate than security codes, passwords, and hardware keys, which is why biometric authentication is quite dependable. It is possible to misplace, have stolen, duplicate, or forget a token such a smart card, ID card, magnetic stripe card, or physical key. It is possible to forget, disclose, or watch a password. Furthermore, in today's lightning-fast digital world, individuals are expected to memorize a plethora of passwords and Personal Identification Numbers (PINs) for various online accounts, including but not limited to: bank accounts, ATMs, E-Mail, wireless, phones, websites, and more. For many uses, biometrics offers the prospect of inexpensive, quick, accurate, and easy verification. Biometric systems are transformed into tele-biometric systems when they are interconnected with telecommunication technologies. The two primary processes are testing and enrollment.

**Conclusion**

Since biometrics authentication technology has just recently been used for commercial purposes in the public sphere, it is considered a novel technological development. Biometrics technology has several uses, one of which is in security systems. It offers precise answers to issues with identification and detection. Enhanced security, efficient authentication, less fraud, and ease of use and implementation are just a few of its many positive aspects that may enhance human life. Additionally, there is no need to spend money on a password manager or token generator. Contrarily, there are several unresolved issues with biometrics security systems, including data privacy, bodily privacy, and religious objections. After considering all of this, it is clear that all of this emerging technology will unquestionably improve and simplify our lives. Methods involving biometric location and dataset preparation are integral to human identification, which allows for the research of individual persons for quantifiable purposes. Criminal distinguishing proofs and general evaluation of human qualities are two areas where study professionals use these approaches. This study outlines datasets that incorporate natural aspects of EEG data, and it indicates numerous assessments and perspectives on human traits related to biometrics. A person's inherent characteristics, such as their brain waves, can be used for identification purposes. The many foci associated with biometric applications are also highlighted in this article.

Biometrics provides an unquestionable and trustworthy approach. When dealing with important data, the technique really shines. This approach has several potential uses, one of which is the electronic election. Determination and authentication can be carried out in several methods, such as via fingerprints, signature, face, eye scan, voice, etc. All banking, financial, and passport activities, among others, might benefit from this new technology and science, we hope.

Biometric identity is very reliable because it is much harder to fake physical traits than security codes, passwords, hardware keys, sensors, fast processing equipment, and a lot of memory space. However, the system is pricey. Some of the uses for biometric-based identity are network and desktop access, single-password application login, data protection, remote utilization of resources, security for transactions, and Web security. Personal identification processes that are strong can help e-commerce and e-government live up to their prospects. People are already using these technologies to do safe online banking, investing, and other financial activities. They are also useful for store sales, law enforcement, health and social services, and more. To make sure that only authorized people can access big business networks, biometric technologies will likely be very important. They will also be used at the point of sale to protect all kinds of digital material, like in Digital Rights Management as well as Health Care settings. Biometrics is expected to be used in almost every part of the business and our daily lives. It can be used by itself or with other technologies like smart cards, encryption keys, and digital signatures. Like, biometrics are used in some school programs, like lunch programs in Pennsylvania and a school the library in Minnesota. Verification of yearly pass holders at an amusement park, speaker verification for TV home shopping, Internet banking, and users' authentication in a number of social services are some other current uses [4].

## References

1. Liu Z, Yan JQ, Zhang D, Tang QL. A tongue-print image database for recognition. International Conference on Machine Learning and Cybernetics. 2007 China;4:2235-2238.
2. Diwakar M, Maharshi M. An extraction and recognition of tongue-print images for biometrics authentication system. International Journal of Computer Applications. 2013;61(3).
3. Jeddy N, Radhika T, Nithya S. Tongue prints in biometric authentication: A pilot study. Journal of Oral and Maxillofacial Pathology. 2017;21(1):176.
4. Kaur G, Singh D. A novel biometric system based on hybrid fusion speech, signature, and tongue. International Journal of Computer Applications. 2015;119(7).
5. Musa OA, Elsheikh TE, Hassona ME. Tongues: Could they also be another fingerprint? Indian Journal of Forensic Medicine and Toxicology. 2014;8(1):171.
6. Mousavinasab Z, Azari S. A review on biometric systems. 2007.
7. Amiri A, Fathi M, Taheri R. Provide a new approach for identification of individuals based on gait improved DTW algorithm and fuzzy sets. Fourth Iranian Conference on Machine Vision and Image Processing. 2007.
8. Jain A, Bolle R, Pankanti S, eds. Biometrics: personal identification in networked society. Springer Science & Business Media. 1999;479.
9. Ross A, Jain A, Pankanti S. A prototype hand geometry-based verification system. In: Proceedings of 2nd conference on audio and video-based biometric person authentication. 1999:166-171.
10. Zhao S, Wang YD, Wang YH. Biometric identification based on low-quality hand vein pattern images. International Conference on Machine Learning and Cybernetics. 2008;2:1172-1177.
11. Антипов РС, Мартыненко ТВ. E-mail: 380713347428@ yandex.ru, tatyana.v.martynenko@ gmail.com. Научное издание. 144.
12. Mehrabian H. Identification based on iris image analysis (Doctoral dissertation, Master Thesis in Electrical Engineering). 2007.
13. Bhattacharyya D, Ranjan R, Alisherov F, Choi M. Biometric authentication: A review. International Journal of u- and e-Service, Science and Technology. 2009;2(3):13-28.
14. Thorat SB, Nayak SK, Dandale JP. Facial recognition technology: An analysis with scope in India. arXiv preprint arXiv:1005.4263. 2010.
15. Joshi MP, Uppal RS, Kaur L. Development of vision-based iris recognition system. International Journal of Advanced Engineering Sciences and Technologies. 2011;6:277-281.
16. de-Santos-Sierra A, Sánchez-Avila C, Del Pozo GB, Guerra-Casanova J. Unconstrained and contactless hand geometry biometrics. Sensors. 2011;11(11):10143-10164.
17. Róka A, Csapó Á, Reskó B, Baranyi P. Edge detection model based on involuntary eye movements of the eye-retina system. Acta Polytechnica Hungarica. 2007;4(1):31-46.
18. Sridevi E, Aruna B, Sowjanya P. An exploration of vascular biometrics. Freshman Engineering Department, KL University, India. 2011.
19. Sierro A, Ferrez P, Roduit P. Contact-less palm/finger vein biometrics. In: 2015 International Conference of the Biometrics Special Interest Group (BIOSIG). 2015:1-12.
20. Indovina M, Dvornychenko V, Tabassi E, Quinn G, Grother P, Meagher S, Garris M. ELFT Phase II-an evaluation of automated latent fingerprint identification technologies. National Institute of Standards and Technology. 2009.
21. Ross AA, Nandakumar K, Jain AK. Handbook of multibiometrics. Springer Science & Business Media. 2006;6.
22. Pankanti S, Prabhakar S, Jain AK. On the individuality of fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2002;24(8):1010-1025.
23. Gaur S, Shah VA, Thakker M. Biometric recognition techniques: A review. International Journal of Advanced Research in Electrical, Electronics and

Instrumentation Engineering. 2012;1(4):282-290.

24. Jain AK, Kumar A. Biometric recognition: An overview. Second Generation Biometrics: The Ethical, Legal and Social Context. 2012:49-79.
25. Abdulhussien AA, Hassen OA, Gupta C, Virmani D, Nair A, Rani P. Health monitoring catalogue based on human activity classification using machine learning. International Journal of Electrical and Computer Engineering. 2022;12(4):3970.
26. Jain AK, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security. 2006;1(2):125-143.
27. Najm H, Ansaf H, Hassen OA. An effective implementation of face recognition using deep convolutional network. Journal of Southwest Jiaotong University. 2019;54(5).
28. Jain AK. Second generation biometrics. 2012.
29. Fenker SP, Bowyer KW. Analysis of template aging in iris biometrics. Computer Society Conference on Computer Vision and Pattern Recognition Workshops. 2012:45-51.
30. Saini K, Dewal ML. Designing of a virtual system with fingerprint security by considering many security threats. International Journal of Computer Applications. 2010;3(2):25-31.
31. Fenker SP, Bowyer KW. Analysis of template aging in iris biometrics. In: Computer Society Conference on Computer Vision and Pattern Recognition Workshops; 2012. p. 45-51.
32. Suganthy M, Ramamoorthy P, Krishnamoorthy R. Effective iris recognition for security enhancement. International Journal of Engineering Research and Applications. 2012;2(2):1016-9.
33. Fancourt C, Bogoni L, Hanna K, Guo Y, Wildes R, Takahashi N, *et al*. Iris recognition at a distance. In: International Conference on Audio-and Video-Based Biometric Person Authentication. Berlin, Heidelberg: Springer Berlin Heidelberg; 2005. p. 1-13.
34. Kumar A, Wong DC, Shen HC, Jain AK. Personal verification using palmprint and hand geometry biometric. In: Audio-and Video-Based Biometric Person Authentication: 4th International Conference, AVBPA; Guildford, UK, June 9–11, 2003. Proceedings 4. Berlin: Springer Berlin Heidelberg; 2003. p. 668-78.
35. Brockly M, Elliott SJ, Guest RM, Blanco-Gonzalo R. Human-biometric sensor interaction. 2015.
36. Kaur S. Speaker verification using LabVIEW. International Journal of Computer Applications. 2011;21(4):8.
37. National Science and Technology Council. Biometrics in government post−9/11: Advancing science, enhancing operations. 2008.
38. Sanchez-Reillo R, Sanchez-Avila C, Gonzalez-Marcos A. Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2000;22(10):1168-71.
39. Ansaf H, Najm H, Atiyah JM, Hassen OA. Improved approach for identification of real and fake smile using chaos theory and principal component analysis. Journal of Southwest Jiaotong University. 2019;54(5).
40. Zhang D, Kong WK, You J, Wong M. Online palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2003;25(9):1041-50.
41. Hassen OA, Abu NA, Abidin ZZ, Darwish SM. A new descriptor for smile classification based on cascade classifier in unconstrained scenarios. Symmetry. 2021;13(5):805.
42. Lin CL, Fan KC. Biometric verification using thermal images of palm-dorsa vein patterns. IEEE Transactions on Circuits and Systems for Video Technology. 2004;14(2):199-213.
43. Chen H, Bhanu B. Shape model-based 3D ear detection from side face range images. In: Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)-Workshops; 2005. p. 122.
44. Jain A, Hong L, Bolle R. On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1997;19(4):302-14.
45. Wayman JL. Fundamentals of biometric authentication technologies. International Journal of Image and Graphics. 2001;1(1):93-113.
46. Ross A, Dass S, Jain A. A deformable model for fingerprint matching. Pattern Recognition. 2005;38(1):95-103.
47. Matsumoto T, Matsumoto H, Yamada K, Hoshino S. Impact of artificial "gummy" fingers on fingerprint systems. In: Optical Security and Counterfeit Deterrence Techniques IV. 2002;4677:275-89.
48. Hong L, Jain A. Integrating faces and fingerprints for personal identification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1998;20(12):1295-307.
49. Hassen OA, Abu NA, Abidin ZZ, Darwish SM. Realistic smile expression recognition approach using ensemble classifier with enhanced bagging. Computers, Materials & Continua. 2022;70(2).
50. Ross AA, Govindarajan R. Feature level fusion of hand and face biometrics. In: Biometric Technology for Human Identification II; 2005. p. 196-204.
51. Abiyev RH, Altunkaya K. Neural network-based biometric personal identification. In: Frontiers in the Convergence of Bioscience and Information Technologies; 2007. p. 682-7.
52. Bhattacharyya D, Ranjan R, Alisherov F, Choi M. Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology. 2009;2(3):13-28.
53. Jain AK, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security. 2006;1(2):125-43.
54. Hassen O, Abu N, Abidin Z. Human identification system: A review. International Journal of Computer Business Research (IJCBR). 2019;9:1-26.
55. Jain AK, Pankanti S, Prabhakar S, Hong L, Ross A. Biometrics: A grand challenge. In: Proceedings of the 17th International Conference on Pattern Recognition (ICPR); 2004. p. 935-42.
56. Paranjape RB, Mahovsky J, Benedicenti L, Koles Z. The electroencephalogram as a biometric. In: Canadian Conference on Electrical and Computer Engineering; 2001.
57. Ravi KVR, Palaniappan R. A minimal channel set for individual identification with EEG biometric using genetic algorithm. In: International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007); 2007. p. 328-32.
58. Darwish SM, El-Zoghabi AA, Hassen OA. A modified walk recognition system for human identification based

on uncertainty eigen gait. International Journal of Machine Learning and Computing. 2014;4(4):346.

59. Shreya S, Chatterjee K. Latent fingerprint and iris fusion for enhancement of performance of human identification system. Expert Systems with Applications. 2024;235:121208.
60. Aljanabi RA, Al-Qaysi ZT, Ahmed MA, Salih MM. Hybrid Model for Motor Imagery Biometric Identification. Iraqi Journal For Computer Science and Mathematics. 2024;5(1):1-12.
61. Carvalho M, Brás S. Addressing intra-subject variability in electrocardiogram-based biometric systems through a hybrid architecture. Biomed Signal Process Control. 2024;87:105465.
62. Singh KK, Barde S. A Feasible Adaptive Fuzzy Genetic Technique for Face, Fingerprint, and Palmprint Based Multimodal Biometrics Systems. J Curr Sci Technol. 2024;14(1).
63. Hassen OA, Abo NA. HAAR: An Effectual Approach for Evaluation and Predictions of Face Smile Detection. Int J Comput Bus Res (IJCBR). 2017;7(2):1-8.
64. Greco M, Eldridge M, Banks E, Halámková L, Halámek J. Metabolite monitoring concept for the biometric identification of individuals from the skin surface. Analyst. 2024.
65. Hassen OA, Abo NA. HAAR: An Effectual Approach for Evaluation and Predictions of Face Smile Detection. Int J Comput Bus Res (IJCBR). 2017;7(2):1-8.
66. Shende P, Shinde S, Wadhwa L, Waghulde K, Pande A, Sonawane A, Shaikh A. Soft computing approach for feature extraction of palm biometric. Multidiscip Sci J. 2024;6(4):2024049.
67. Пуріш СВ, Лобачев МВ. Gait recognition methods in the task of biometric human identification. Вісник сучасних інформаційних технологій. 2023;6(1):13-25.
68. Zhuravlov D, Polshakova O. Detection of face spoofing attacks on biometric identification systems. Адаптивні системи автоматичного управління: міжвідомчий науково-технічний збірник. 2023;(1)42.
69. Garea-Llano E, Morales-Gonzalez A. Framework for biometric iris recognition in video, by deep learning and quality assessment of the iris-pupil region. J Ambient Intell Human Comput. 2023;14(6):6517-6529.
70. Haq HBU, Saqlain M. Iris detection for attendance monitoring in educational institutes amidst a pandemic: A machine learning approach. J Ind Intell. 2023;1(3):136-47.
71. Alghamdi M, Angelov P, Alvaro LP. Person identification from fingernails and knuckles images using deep learning features and the bray-curtis similarity measure. Neurocomputing. 2022;513:83-93.
72. Kuroda SI, Nakaya-Kishi Y, Tatematsu K, Hinuma S. Human olfactory receptor sensor for odor reconstitution. Sensors. 2023;23(13):6164.