**Biometrics –An emerging tool for personal Identification in Forensic**

**Kautuk Shrivastav**

Indian Army, India

Email-kautukshrivastavonweb@gmail.com

**Shantnu Singh Rathore**

Research Scholar

Department of Forensic Science

Guru Ghasidas Vishwavidyalaya

Bilaspur, Chhattisgarh, India

Email - rathore4n6@gmail.com

**First Author: Megha Yadav1**

Research Scholar

Department of Forensic Science

Guru Ghasidas Vishwavidyalaya

Bilaspur, Chhattisgarh, India

Email –meghaforensics@gmail.com

**\*Corresponding Author**

**Blessi N. Uikey**

Assistant Professor

Department of Forensic Science

Guru Ghasidas Vishwavidyalaya

Bilaspur, Chhattisgarh, India

Email -blessiuikey@gmail.com

**Dr. Chanchal Kumar**

Assistant Professor

Department of Forensic Science

Guru Ghasidas Vishwavidyalaya

Bilaspur, Chhattisgarh, India

Email -chanchalbiosgmail.com

**Abstract**

Accurate and reliable identification is of a vital concern in crime identification. Biometric system is an automated recognition system which utilised the various physiological and behavioural traits for personal identification. In the context of criminal justice system, Biometric technique became an important form of evidence. Biometric technique became more popular due to its liability and efficient nature. Due to the various recent advancement in the Biometric system, the technique is replacing the manual recognition methods used in criminal identification process. The Forensic Biometric system uses various characteristics such as Fingerprint, Iris, Retina, facial Markers, gait pattern, voice recognition, hand geometry, etc. The chapter explains the working of biometric system and their uses in forensic science.it will explore various biometric system and their uses and emerging trend in the biometric identifiers.

1. **Introduction**

A biometric system is a technology that uses the unique physical or behavioural characteristics for identification or confirmation of a person's identity [1]. Biometric is combination of technology and scientific authentication methods which is mainly based on anatomical and behavioural traits of humans. It is the science which deals with the identification of an individual. The term Biometrics is formed by two words − *Bio* which means life and *Metrics means* Measurements. Biometrics system can be described as a science of recognition and identification of humans through unique physical and behavioural traits. Each biometric characteristic that may distinguish between people is regarded as a biometric modality. The aim of the biometric technology is to establish the individuals’ identity. Associating an identity with and individual is known as personal identification which plays an important role in field of forensic science. Accurate identification of an individual helps in establishing an identity and these unique traits acquire at crime scene can be helpful after comparing with set from the data stored in Biometric system. This Biometric system is useful in real-time identification of an individual with a database of a complete set of information, and hence provides a forensic scientist with a proper result of comparison [2].

Biometric system automatically recognizes individual using biometric tool by taking the inputs through scanning devices and then supplied to the biometric detectors. The biometric system then checks the input from the database using algorithms and provides the result. Identification methods, a subject identity is determined based on the comparison of a biometric samples obtained from the subject earlier and stored in a database. Authentication methods are used for the confirmation of an individual’s claimed identity; in this case the comparison is made only with the stored biometric features that correspond to the claimed identity [3]. These characteristics can include fingerprints, iris scans, facial recognition, voice recognition, gait pattern, lip prints, odour, hand geometry, nail, knuckle etc. Biometric systems are commonly used for security and access control, such as unlocking Smartphone or accessing secure facilities, as they provide a high level of accuracy and are difficult to fake or replicate. However, they also raise important privacy and security concerns, as the biometric data collected must be carefully protected to prevent unauthorized access or misuse. The security field uses three different types of authentications: [4].

1. **Brief History of Biometrics**

The best example of identification is face to face recognition. Faces have been used by humans to distinguish between known (familiar) and unknown (unfamiliar) people ever since the dawn of civilisation. As with the increase in population and ease in migration the difficulty to recognise arises. The earliest record of occurrence of non- automated biometric system was found in the pre-historic image writing of

The earliest traces of biometrics date back to the Babylonian Empire where fingerprint and thumb impression were recorded for business transaction on clay tablet around 500 BC. But the first instance of a biometric identity system was documented in the 1800s in Egypt, while constructing the pyramids, clay slab with fingerprints of nearly 30000 years old have been found in Tutankhamen’s tomb in Egypt. The administrator started to keep records of worker by recording the physical and behavioural traits. Later the use of thumbprint was used as official seal on documents by Chinese emperors since 240 BC [5]. Joao de Barros the explorer reported that Chinese merchant use to take the palm print and footprint of children on the paper using ink to distinguish the children. During eighteenth century, many anatomical works appeared among which E.J. Purkinje’s contribution of 1823 was an important landmark in field of fingerprints. He published a treatise on diversity of ridge patterns and gave as system of classification of fingerprints. In 1858, W.J Hershel started using the fingerprints for official use for the first time on large scale. Alphonse Bertillon created a system for categorising and differentiating criminals using precise body measurements. The first system which focuses on meticulous measurements of different body parts. According to Bertillon some elements of the body remains constant or unchanging throughout the life such as size of skull or size and length of fingers. He developed a method of taking bodily measurements known as *Bertillonage* [6]. In 1890 Francis Galton based on his observations published his book emphasising on the individuality and permanence of fingerprints [7]. The fingerprint classification system given by Edward Richard Henry, Inspector General was adopted as means of identification in place of anthropometric system in March 1897. In 1901 fingerprints based criminal identification was officially introduces in England. The use of Henrys system with modification was started in 1902 by FBI and law enforcement agencies throughout U.S.

The New York state prison system started using Fingerprints systematically for criminal Identification throughout the country in 1903[8]. The Leavenworth Federal Penitentiary in Kanas and the St. Louis (Missouri) Police Department both started using Fingerprints in 1904. The American Army started utilising fingerprints around 1905. The U.S navy started adopting fingerprints two years later, and the Marine Corps followed a year later. More law enforcement agencies joined in on the use of Fingerprints as a form of personal identification during the course of following 25 years. Ophthalmologist Frank Burch presented the idea of using the iris pattern for identification and recognition of people in 1936. Some of the early research on automated facial recognition can be found in the 1960s at Panoramic Research in palo Alto, California [5][9].

A pioneer in the area of automated reasoning is Woody Bledsoe. He created a method known as man-machine facial recognition that made use of the feature extraction methodology; it was the first step towards leveraging distinctive biological traits to verify identity [10].

 Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago. The first known research publication on automated biometric recognition was published by Trauring in 1963 on fingerprint matching [11].

1. **Characteristics of an Ideal Biometric system**

The unique characteristics that can be used to authenticate the identity of the user can be done in three ways

1. Using PINS and passwords (something user knows, combination of word, numbers or symbols)
2. Using Cards (Something user has, special card, Keys, Identity cards)
3. Using anatomical/Behavioural trait (something the user is, Fingerprint, Footprints, Keystroke, voice)

It is crucial to comprehend the application needs and the application environment before choosing a certain biometric system. An ideal Biometrics must have all desirable characteristics that need to be considered before determining the suitability of biometric identifier i.e., whether the physiological or behavioural trait can be used in the biometric application. However, no one biometric system performs better than another [12]. When developing a biometric system, a lot of elements need to be taken into account, including tasks, user conditions, security risks, current data, user count, etc. If a certain biometric is utilized for security, it is also important to measure the degree of success. A biometric trait will accomplish lot of criteria’s, which includes Universality, permanence, acceptability, collectability, performance, circumvention. Etc. (13).

**A) The following seven characteristics are of importance for ideal biometrics.**

1. **Universality-** The characteristics or trait that each person will have. Every individual accessing the application must have the trait which can be used as identifier. The characteristics should be possessed by each individual we expect to enrol in the biometric system. The nature of the trait will be helpful in determining the rate of failure to enrol in the biometric system.
2. **Uniqueness-** The enrolled trait must have unique features that sufficiently separate the individuals from the user population. Example DNA, fingerprints.
3. **Permanence –** how well the trait resists changes over a period of time. The features of trait measurement must be constant over a period of time in all the conditions; it should not show the variability with change in condition.
4. **Measurability-** how easily the trait can measure efficiently without requirement of very big scanning devices as well as easy to record and measure.
5. **Performance** – How well the biometric system functions. The characteristics of biometric system explain speed and accuracy in the process of recognition and authentication.
6. **Acceptability:** How easily it is for user to accept the biometric system.
7. **Circumvention** – this refers how the trait can be artificially imitated to fool the system i.e., how easily the system can be fooled. This explains the how it can detect the altered artificial trait given to the system [14].
8. **Working of Biometric system**
9. As biometric is automated recognition system which is divided in two phases.
10. **Enrolment-**During the enrolment phase the biometric data of user is acquired and recorded in the data base. The process of enrolment is one time process, in this phase of enrolment, the measurements of the biometric trait is measured and recorded with personal identification details such as name, etc. age, sex etc. For enrolling the user in the biometric system, sensors are used.
11. **Recognition**-this is the second phase of biometric system, which is challenging phase. In this the identity of person claiming to be is determined. The biometric trait is re-acquired from the individual and compared with the database stored in the system. This phase must be accurate and quick [15].
12. **The working of Biometric system can be divided into mainly four components.**
13. **Sensor**- This is the first component of the biometric system which act as a interface between the computer system and real world. In this segment the patterns are recognised by using either image acquisition devices such as scanners or cameras in case of fingerprint, hand geometry, facial recognition, Iris, retina etc or movement-based acquisition devices such as microphone or platens to record voice, digital pads in case of Signature biometrics. The efficiency of the acquisition process in biometric system depends on the scanners used in the system. For various biometric sensors, the manner of capturing the raw biometric data varies such as 2-Dimensional image in case of Fingerprints, Face, Iris, retina etc, 1-dimensional amplitude, frequency and signals in voice recognition, locomotion, pen pressure, pen position and velocity in case of signature biometrics and chemical based sensors are used in case of DNA, odour biometric identifying systems [16][17].
14. **Feature Extraction**-In this segment, the raw biometrics data acquired through sensors is subjected to pre-processing before feature extraction. Before this quality assessment of the trait is performed in which it is determined whether the captured data is suitable for further processing or no. If the raw data is not of sufficient good quality, then the data is re-acquired or the failure alarm is generated alerting the system to produce suitable method of data input. After this the required biometric data is separated from the background noise through a process known as segmentation [18][19]. Finally, the segmented biometric data is process through quality enhancement algorithm in order to improve the quality of trait to minimize the noise in it. In this feature extraction process, compressed but communicative digital image of the acquired biometric trait is created known as *template.* This template will contain only prominent features that are discriminatory in nature which are essential for recognition (detecting minutiae points in fingerprint is the key feature extraction step in fingerprint biometric system [20].
15. **Data Base**- The biometric system database act as a hub of biometric information. During the enrolment phase, the feature extracted from the user in the form of raw biometric data is stored in data base along with the personal identity of the individual such as name, PIN, address, gender etc. The biometric data is then stored separately in centralise or decentralised data base based on the biometric system. The biometric data is broken into small fragments and the encrypted data is stored.
16. **Matcher** - In this segment of identification process, the questioned feature is compared against the store template in the database. [21]



1. **Types of Biometrics**
2. **Physiological Biometrics-**refers to the analysis of the physical characteristics feature of a person that are notably identified through five senses. These physiological characters are static in nature. These includes Fingerprints, Face biometrics, Iris biometrics, odour, DNA, etc.

**Physiological traits as Biometric Markers**

1. **Fingerprints**

Since 1896, fingerprints have been used, particularly for criminal identification, making them the oldest biometric approach and a pioneer in identity authentication. The central concept is centred on fingertips with skin that is corrugated. Flowing from one side of the finger to the other in ridges that resemble lines. These ridges have no flow ongoing and creates a pattern. The flow pattern results in a categorization pattern like arches, whorls and loops whereas the ridge flows discontinuity creates feature spots known as minutiae [22][23][24].

1. **Face biometrics**

A typical camera can be used to capture a face image. It is the most typical biometric for confirming identity. Holistic or global approach and feature-based approach are the two basic methods used to do face recognition

The feature-based method is based on the identification of specific fiducial spots on the face, such as those at the cheekbones, on the sides of the nose and mouth, at the eyes, etc., that are less prone to change[25].

The holistic method concurrently processes the complete face image without locating the individual points. The technology employed in this strategy can vary depending on whether neural networks, statistical analysis, or transformations are used. The holistic strategy has the advantage that it utilizes the entire face.

1. **Hand geometry**

The hand image is obtained using camera capturing from the top when the user places his/her hand on a desired surface. User hand can be aligned using reference marks or pegs. Two views are usually taken in a single image, the side view and the top view. The side view is usually captured by the top camera, using a side mirror. From the hand image, the fingers are located and the width, length, thickness, curvatures and their relative geometry measured When the user places his or her hand on the appropriate surface, a camera that shoots from the top captures the hand image[26]. Aligning the user hand can be done with pegs or reference markers. Typically, two viewpoints are captured in three views: the top, the side, and the single image. The top camera typically records the side view using a side mirror. The location of the fingers, as well as their width, length, thickness, curves, and measured relative geometry[27].

1. **Iris**

Typically, a monochrome camera with visible and near-infrared light (700-900nm) is used to capture the iris image. The iris, the coloured portion of the eye, is made up of trabecular meshwork, a type of tissue. The iris appears to be a layered mesh or radial line pattern upon close inspection. The visible mesh gives the iris its distinctive pattern by including features like rings, striations, furrows, and crypts, among others. The essential point is that since the iris pattern is independent of genetic makeup, it differs amongst twins, including identical twins, and it remains constant throughout life[28].

1. **Odour:**

Each object releases an odour that is unique to its chemical make-up, and this smell can be utilized to identify between different objects. His would be carried out using a variety of chemical sensors, each tuned to a particular class of chemicals.[29]

1. **Behavioural trait as a Biometrics identifier –** these are the traits that are not static and acquired by human during his development.
2. **Voice Biometrics**

The voice recording needs to be digitized for authentication. 'The user has the ability to acquire speech speaking (text independent) or writing (text dependent) a well-known text'. In the last scenario, the text system-generated or fixed. Either the individual words or the complete text can be read out constantly. Additionally, the acquired speech is then improved and given unique elements to create a voice template. Extracted.

1. **Biometrics of gait:**

The peculiar way a person walks is referred to as gait, and it is a complicated spatio-temporal biometric. It can be used to locate a person's location and identify them. Gait is a behavioural biometric that is influenced by a variety of things, including body weight, the type of surface you walk on, your shoes, your clothing, etc.

1. **Biometrics for keystrokes:**

It is thought that every person types on a keyboard in a different way. In terms of identification, his biometric is likewise not particularly distinctive or unique, but it does help to identify a person. Emotional condition, keyboard posture, type of keyboard, etc. all affect keystroke pattern. The benefit of employing keystroke behaviour for recognition is that it may be discreetly examined as the person types the data.



1. **Various Biometric System used in Forensic Investigation.**
2. **Fingerprint Biometric system**

Fingerprints are crucial in criminal investigations as they are unique, natural patterns formed by friction ridges on fingertips. They cannot be altered or forged, and are unique throughout life. They serve as permanent markers of human identity, similar to DNA fingerprinting, making fingerprints valuable evidence in court for identification. Ridges in fingers contain minutiae, which are curved segments raised and valleys between them. Galton first identified these details, which can help to identify unknown individuals and compare fingerprints. Each fingerprint contains over 100 ridge characteristics. For comparing two fingerprints first the patterns are compared and further their classification is done. After classification the ridge characteristics are examined and identified. For matching sufficient number of minutiae in same order of sequence and their relative position in both prints are determined. Fingerprint biometric system works by recognizing the fingerprint details by scanning the pressed fingers against the smooth surfaces. Various optical and scanners are used to capture the details. Fingers’ each ridge and valley and distinct points called minutiae are scanned by the scanners.

AFIS is a type of biometric system that uses digital imaging to capture a fingerprint, which can then be compared to a database of fingerprint records to help determine the identity of an individual. AFIS aids in classifying and retrieving fingerprints by converting the image of a fingerprint into digital ridges that contain data showing ridges at their points of termination (ridge endings) and their branching into two ridges (bifurcations). AFIS is commonly used in law enforcement where sets of prints recovered in the crime scene were compared against the database of known and unknown prints[30]. The heart of AFIS technology is the ability of a computer to scan and digitally encode fingerprints so that they can be subject to high-speed computer processing.

The basic function of every type of scanner is to obtain an image of a person's fingerprint and find a match for it in its [database](https://en.wikipedia.org/wiki/Database). The measure of the fingerprint image quality is in [dots per inch](https://en.wikipedia.org/wiki/Dots_per_inch) (DPI).

1. **DIGITIZATION AND PROCESSING OF FINGERPRINTS**

Demands imposed by the painstaking attention needed to visually match the fingerprints of varied qualities, the tedium of the monotonous nature of the manual work and increasing workloads due to a higher demand on fingerprint recognition services prompted law enforcement agencies to initiate research into acquiring fingerprints through electronic media and to automate fingerprint individualization based on digital representation of fingerprints. As a result of this research, a large number of computer algorithms have been developed during the past three decades to automatically process digital fingerprint images. the following five major steps are required in designing automated fingerprint processing systems: digital fingerprint acquisition, image enhancement, feature (e.g., minutiae) extraction, matching, and indexing/retrieval.

1. **IMAGE ACQUISITION**

The main parameters characterizing a digital fingerprint image are resolution area, number of pixels, geometric accuracy, contrast, and geometric distortion. There are a number of livescan sensing mechanisms (e.g., optical, capacitive, thermal, pressure-based, ultrasound, and so forth) that can be used to detect the ridges and valleys present in the fingertip.

1. **IMAGE ENHANCEMENT**

Fingerprint images originating from different sources may have different noise characteristics and thus may require some enhancement algorithms based on the type of noise. The goal of fingerprint enhancement algorithms is to produce an image that does not contain artificially generated ridge structure that might later result in the detection of false minutiae features while capturing the maximum available ridge structure to allow detection of true minutiae. Adapting the enhancement process to the fingerprint capture method can yield the optimal matching performance over a large collection of fingerprints. Automatic fingerprint image-enhancement algorithms can significantly improve the quality of fingerprint ridges in the fingerprint image and make the image more suitable for further manual or automatic processing. The image enhancement algorithms do not add any external information to the fingerprint image[31][16][17]. The enhancement algorithms use only the information that is already present in the fingerprint image. The enhancement algorithms can suppress various types of noise (e.g., another latent print, background colour) in the fingerprint image and highlight the existing useful features. These image enhancement algorithms can be of two types.

Manual enhancement through a graphical user interface. Through this interface, the forensic expert is able to use various algorithms to choose the region of interest in the fingerprint image, crop the image, invert colour, adjust intensity, flip the image, magnify the image, resize the image window, and apply compression and decompression algorithms. other algorithms may include histogram equalization, image intensity rescaling, image intensity adjustments with high and low thresholds, local or global contrast enhancement, local or global background subtraction, sharpness adjustments (applying high-pass filter), background suppression (low-pass filter), gamma adjustments, brightness and contrast adjustments, and so forth.

Automated Enhancement of Fingerprint acquired images can be done using Enhancement algorithms that are fully automated mode to improve the fingerprint ridge structures in poor-quality fingerprint images. Contextual filtering is used that has a low-pass (smoothing) effect along the fingerprint ridges and a band-pass (differentiating) effect in the direction orthogonal to the ridges to increase the contrast between ridges and valleys. Often, oriented band-pass filters are used for such filtering. One such type of commonly used filters is known as Gabor filters. The local context is provided to such contextual filters in terms of local orientation and local ridge frequency.

1. **FEATURE EXTRACTION**

Local fingerprint ridge singularities, commonly known as minutiae points, have been traditionally used such as the lake, island, spur, crossover, and so forth (with the exception of dots), are simply composites of ridge endings and bifurcations. Automatic fingerprint feature-extraction algorithms were developed to imitate minutiae location performed by forensic experts. Automatic fingerprint minutiae-extraction algorithms only consider ridge endings and bifurcations. Further, most algorithms do not differentiate between ridge endings and bifurcations because they can be indistinguishable as a result of finger pressure differences during acquisition. One common approach followed by the fingerprint feature extraction algorithms is to first use a binarization algorithm to convert the gray-scale-enhanced fingerprint image into binary (black and white) form, where all black pixels correspond to ridges and all white pixels correspond to valleys. Recently, a number of automatic fingerprint feature extraction (and matching) algorithms have emerged that use non-minutiae-based information in the fingerprint images. For example, sweat pores, which are very minute details in fingerprints, smaller than minutiae points, have been successfully extracted by algorithms from high resolution fingerprint images.

1. **MATCHING**

Fingerprint matching can be defined as the exercise of finding the similarity or dissimilarity in any two given fingerprint images. Automatic fingerprint-matching algorithms work on the result of fingerprint feature-extraction algorithms and find the similarity or dissimilarity in any two given sets of minutiae. Automatic fingerprint matching can perform fingerprint comparisons at the rate of tens of thousands of times each second, and the results can be sorted according to the degree of similarity and combined with any other criteria. The alignment algorithm aligns the minutiae and feature extraction algorithm establishes the minutiae in the two sets that are corresponding and those that are noncorresponding, is based on using some tolerances in the minutiae locations and orientation to declare a correspondence. So, finally, a score computation algorithm is used to compute a matching score.

1. **INDEXING AND RETRIEVAL**

The fingerprint matching problem was defined as finding the similarity in any two given fingerprints which should be matched against a large number of fingerprints present in a database. In these applications, a very large amount of fingerprint searching and matching is needed to be performed for a single individualization. Automatic fingerprint indexing algorithms classify fingerprint images into mostly five classes (e.g., left loop, right loop, whorl, arch, and tented arch) based on the many fingerprint features automatically extracted from fingerprint images. Such automatic fingerprint classification algorithms may be used to index all the fingerprints in the database into distinct bins (most implementations include overlapping or pattern referencing), and the submitted samples are then compared to only the database records with the same classification (i.e., in the same bin).

1. **Voice Biometrics**

The term voice biometrics refers to speech processing technology or a technique where voice can be utilised to authenticate a person’s identity overtly and discreetly. The voice identification can be divided into two categories speech processing and biometric security. Voice biometrics perform their tasks by extracting data from the speech stream, just like other speech-processing techniques. Voiceprint is a collection of quantifiable features of a person voice that can be used as a biometric identifier. A mathematical formula is used to express these qualities which are based on the physical arrangement of the mouth and throat of a speaker [32]. The human voice frequently serves as crucial evidence linking a person to criminal act in the era of telephone, radio and tape recorder conversations. The frequency of phone bomb threats, lewd phone calls and tape-recorded abduction ransom messages has increased. The human voice has led law enforcement officials to become interested in the technological solutions that can turn voice into a form that can be used for personal identification [33].

Voice is unique because of the shape of vocal cavities and the way you move your mouth when you speak. To enrol in a voiceprint system, you either say the exact words or phrases that it requires, or you give an extended sample of your speech so that the computer can identify you no matter which words you say.

Based on the idea that heredity, sex, age and other socio-environmental factors have an impact on the vocal cavity dimensions and coupling of the articulators, speech spectrographs are used to identify the voice of the speaker. Therefore, it is quite unlikely that two people could produce voiceprints that are exactly alike. To enrol in a voiceprint system, you either say the exact words or phrases that it requires, or you give an extended sample of your speech so that the computer can identify you no matter which words you say. Voice biometrics is combination of physiological as well as behavioural biometric. There are two different types of voice recognition system text dependent and text independent. In text dependent a voiceprint system, either say the exact words or phrases are required, or an extended sample of your speech can be taken so that the computer can identify the user no matter which words they say.

The sound spectrograph is capable of generating two types of voiceprints, one called as bar voice print and the other called as contour voice print. The voice print obtained in either of the above forms determines what was spoken. It also exhibits time along the horizontal axis; frequency along the vertical axis; and amplitude as a function of density of the pattern of the same vowels spoken by the unknown and the known voices. A visual comparison is made to establish the similarity or dissimilarity in the recorded voices.

The speech identification by spectrographic speech analysis is a complex process. Further, interpretation of the voiceprints depends upon the expertise of the examiner handling the instrument, his experience and skill in recording and interpretation of the spectrograms. .The first step consists of recording the unknown voice on a tape recorder. The next step is to discover the suspected person and obtain his sample voice using the same text as that of the unknown caller. From the two recorded voices, the expert examiner then prepares suitable exemplars from the known and unknown voices. These exemplars are then scanned on the acoustic analysis instrument to obtain voiceprints in the form of graphical patterns [34].

The sound spectrograph is capable of generating two types of voiceprints, one called as bar voice print and the other called as contour voice print. The voice print obtained in either of the above forms determines what was spoken. It also exhibits time along the horizontal axis; frequency along the vertical axis; and amplitude as a function of density of the pattern of the same vowels spoken by the unknown and the known voices. A visual comparison is made to establish the similarity or dissimilarity in the recorded voices. The bar voice prints are exclusively used in the courtroom presentation and the contour voiceprints are used for computer automated classification of speaker’s voice for filing and record. The studies reveal that attempts to disguise the voice by whispering, muffling the voice, or holding the nose, doesn’t alter the basic features in a person’s voiceprint. Voice mimics have also failed to prevent the identification of voice through sound spectrograph.

When people think of voiceprints, they often think of the wave pattern they would see on an [oscilloscope](http://science.howstuffworks.com/environmental/energy/question8.htm). But the data used in a voiceprint is a sound spectrogram, not a wave form. A spectrogram is basically a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds create different shapes within the graph. Spectrograms also use colours or shades of grey to represent the acoustical qualities of sound.

Some companies use voiceprint recognition so that people can gain access to information or give authorization without being physically present. Instead of stepping up to an iris scanner or hand geometry reader, someone can give authorization by making a phone call. Unfortunately, people can bypass some systems, particularly those that work by phone, with a simple recording of an authorized person's password. That's why some systems use several randomly-chosen voice passwords or use general voiceprints instead of prints for specific words. Others use technology that detects the artifacts created in recording and playback. Other systems are more difficult to bypass.

**D) Face biometrics:**

A typical camera can be used to capture a face image. It is the most typical biometric for confirming identity. Holistic or global methods are the two basic methods used to do face recognition feature-based approach.

* **Feature-based approach:**The feature-based strategy depends on the identification of specific facial fiducial points, such as those near the cheekbones, the side of the nose, and the chin, that are less prone to change mouth, makes eye contact, etc. These points' locations are used to calculate the geometrical ties connecting the sites. The areas close to the points can also be locally examined. Then, data is gathered and merged from all local processing at the fiducial locations to produce the general recognition of a face. Since feature point identification comes before analysis, the system is resistant to variations in the image's positions. However, automatic fiducial point detection is inconsistent and sufficient to produce a good accuracy ratio for the face recognition.
* **Holistic approach:**

The holistic technique analyses the complete face image concurrently without localizing the individual locations. There are some differences in this strategy's choice of technology, including a combination of neural networks, statistics, or transformations. The holistic strategy has the advantage that it utilizes the entire face. In general, this produces outcomes in recognition that are more precise. Although, such method requires extensive training data sets because it is sensitive to changes in scale and position[35][36].

* **Hybrid approach:**

A hybrid strategy combines the two strategies mentioned above. Here, the face detection system receives information from both the local and the entire face.

**Face Detection >Feature Extraction >Classification**

**Face recognition techniques:**

* **Eigenface.**

One of the often-employed facial recognition algorithms is called Eigenface. Based on the eigenfaces approach, Karhunen-Loeve uses the Principal PCA, or component analysis, is employed. This approach is successfully used to reduce the dimensionality. In face recognition, Principal Component Analysis is employed

* **Neural networks.**

Neural Networks: Neural networks are utilized in a wide range of applications, including autonomous robot driving, character recognition, object recognition, and pattern recognition issues. Face recognition neural networks' primary goal is the training a system to capture complex classes of faces is feasible. patterns. A neural network will perform at its peak level if: It must have significant training, have several layers, and have rates of nodes, learning, etc

* **Fisher face.**

The most popular and successful method for facial recognition is called Fisher faces. It is dependent on the way of appearance

* **Elastic bunch graphing.**

Face recognition with elastic bunch graph matching works by identifying faces by estimating a collection of features using a bunch graph is a type of data structure. Identical to each landmark are approximated and located using this query image heap diagram. After that, the features are obtained by using the number of "face" instances of the Gabor filter graph"[37][38][39].

**The three steps of facial recognition are detection, analysis, and recognition.**

**Detection**

The technique of identifying a face in a picture is called detection. Face detection and identification from an image including one or more people's faces is made possible by computer vision. Both front and side face profiles with facial data can be detected.

**Analysis**

The facial recognition software then examines the face's image. It maps facial geometry and reads facial expressions. It identifies the facial features that are crucial for separating a face from other items. Typically, the facial recognition system checks for the following:

* The distance between each eye
* separating the chin from the forehead
* the distance between the lips and the nose
* Dimensions of the eye sockets cheekbones'
* appearance of the chin, ears, and lip contours

The face recognition data is then transformed by the system into a face print, which is a series of numbers or points. Similar to a fingerprint, every individual has a distinct face print. A person's face can be digitally reconstructed using the same data that is utilized for facial recognition[40][41].

**Recognition**

By comparing the faces in two or more photographs and determining the chance that two faces match, facial recognition may identify a person. For instance, it can confirm that the face displayed in a selfie taken with a mobile device matches the face in an image of an official ID like a driver's license or passport, as well as confirm that the face displayed in the selfie does not match a face in a collection of faces that have already been photographed.

1. **Hand** **Geometry**

Hand geometry is based on the anatomy of the palm and fingers including the distribution of finger breadth and length, as well as the thickness of palm. These characteristics are highly helpful for identification and verification also known as personal authenticity, even though alone these measures are not very differentiable across individuals. Combining few non-descriptive traits can improve identification outcomes. the human hand has enough anatomical traits to allow for partial personal identification, but it is not thought to be sufficiently distinctive to allow for full personal identification. Hand geometry is time-sensitive and changes in the condition such as any disease, ageing or weight can alter the curve of hand[42]. It is actually based on concept that each person has a unique shape of hand, and that shape will not change significantly in the future. In this the shape size and flow of the ridges on hand are considered and minutiae are extracted as distinctive features. Also, the thickness and area of palm is considered which is divide into thenar (raise portion of palm near thumb), hypothenar and interdigitalis (are below the four fingers) region. Later the geometrical measurements such as length, breath of fingers distance between two fingers are measured. These all characteristic altogether is acquired through scanners which capture a 3-dimensional image of hand. Further, the image is pre-process and features are extracted. Hand geometry is a prime choice for study and development of novel acquisition, pre-processing and verification due to the aforementioned characteristics[26][27][43].

Research conducted in 2003, gave the 30 feature that extracted from the image of hand that are used in biometric system. These are shown explained in given table

|  |  |  |  |
| --- | --- | --- | --- |
|  | Thumb length | 17. | Ring circle radius upper |
|  | Index finger length | 18. | Pinkie circle radius lower |
|  | Middle finger length | 19. | Pinkie circle radius upper |
|  | Ring finger length | 20. | Thumb perimeter |
|  | Pinkie length | 21. | Index finger perimeter |
|  | Thumb width | 22. | Middle finger perimeter |
|  | Index finger width | 23. | Ring finger perimeter |
|  | Middle finger width | 24. | Pinkie perimeter |
|  | Ring finger width | 25. | Thumb area |
|  | Pinkie width | 26. | Index finger area |
|  | Thumb circle radius | 27. | Middle finger area |
|  | Index circle radius lower | 28. | Ring finger area |
|  | Index circle radius upper | 29. | Pinkie area |
|  | Middle circle radius lower | 30. | Largest inscribed circle radius |
|  | Middle circle radius upper |  |  |
|  | Ring circle radius lower |  |  |

1. **ROLE OF BIOMETRICS IN FORENSIC SCIENCE**

By offering distinct and quantifiable physical or behavioural traits that can be used to identify people, biometrics plays a significant role in forensic science. Here are some of the major functions of biometrics in forensic science:

**Identification:** Biometrics, such as DNA, facial recognition, and fingerprints, are used to positively identify people who are involved in criminal activity.

**Authentication**: In a variety of forensic applications, such as gaining access to secure databases, forensic lab restricted areas, and crime scene evidence, biometric data can be used to verify a person's identification.

**Criminal investigations:** To connect suspects to crime scenes, forensic professionals employ biometric data. For instance, fingerprint analysis can link prints discovered at a crime scene to those of known suspects, aiding in the development of a case against them.

**Criminal Databases:** Biometric databases, like AFIS (Automated Fingerprint Identification System) and CODIS (Combined DNA Index System), store and compare biometric data to assist law enforcement agencies in solving crimes by matching evidence to known individuals.

**Support for Witness Testimony:** Eyewitnesses can give descriptions of suspects that can be compared with biometric information to increase the veracity of their testimony.

**Expert Testimony:** Forensic specialists can give expert testimony in court, educating judges and juries about the science behind and validity of biometric evidence.

**Exonerating the Innocent**: By giving verifiable evidence of their absence from a crime scene, biometrics can also be utilized to establish the innocence of people who have been wrongfully convicted of committing crimes.

1. **EMERGING TRENDS IN BIOMETRICS**

New Emerging Biometric Technologies:A) **Finger nail bed**:

Human finger nails possess a high level of individuality, regardless of whether they are shared by identical twins or between individual finger nails. This is utilized as a key for the development of a new biometric verification system utilizing a single nail plate. Nail authentication systems are based on the highly distinctive dermal structure beneath the nail plate, referred to as nail bed. You can't use a full nail plate for authentication because your growing nail plate, but you can use it as a transient biometric. Due to the heterogeneous characteristics of the growing nail plate, the nail bed itself is taken into account. A pentagon structure is created through semantic points mediation, and the texture properties within the structure are masked and utilized as a Region of Interest[44][45].

Nail anatomy research has demonstrated that, as new cells are grown, only the nail plate regenerates, and the distance between the grooves in the nail bed remains relatively constant throughout an individual's life.

The nail is the part of the skin that is attached to the tip of your finger at the end of your finger. The nail unit is made up of a tightly knotted keratinized layer that is nail-plate, nail matrix and nail-bed. Nail bed is the pinkish tissue under the nail plate that is enriched with small blood vessels. The nail bed is made up of two different types of tissues. The deeper dermis that is firmly attached to the base of your finger and the top epidermis that is closest to your nail plate. The dermis has lots of ridges and grooves like channels. The soft bed epidermis slides into the channels and makes tiny rails. This tongue in groove arrangement of two layers is called the arched part of the nail and the valley portion of your nail. It forms a unique structure that is closely parallel and unevenly spaced. You can see the grooved spatial structure of your nail bed on the top nail plate surface. These are longitudinal ridges / striations. These nail striations are very unique for each person and serve as your personal identifier. The uniqueness of nail-based biometrics is entirely dependent on the intrinsic anatomical properties of the nail. The nail surface ridge pattern has some advantages over other biometric characteristics for identification. The hardened nail structure is resistant to decay and environmental changes, except for changes caused by diseases and disorders affecting the nail plate. Diseases such as onychomychoses, psoriasis and beau’s lines can lead to deformation of the nail plate. However, the primary reason for nail plate surface biometrics preference is that nail plate uses intrinsic characteristics of nail bed for identification, which is a concealed structure and therefore crucial identity information is not disclosed.[46][47][48]

**B) Lip movement: -** Lip Authentication is a new way to authenticate people based on visual information taken from their lips while they're speaking. It's perfect for mobile devices since it has unique information. Plus, it's way more lovable than other popular biometric systems like face and fingerprint, and you can capture lip movements with your phone's front-facing camera without needing any special hardware. But research and progress on lip biometrics has been slower than others like face, fingerprint, or even iris. In this biometric we'll take a closer look at a state-of art lip biometric authentication system using a deep Siamese network. We can use a one-time-shot triplet loss test to see how it works in real-world scenarios.

**Multimodal biometrics:**

For improved accuracy and security, multimodal biometrics combines different biometric modalities (such as fingerprint, face, and iris) Deep learning: Using deep neural networks to extract and match features to increase the accuracy

**Real-time authentication:** That continuously analyses user behaviour and biometric data to spot anomalies is called continuous authentication

**Privacy-Preserving Techniques:** That’s safeguard user privacy, such as homomorphic encryption and secure multi-party computation, are referred to as biometrics.

**Mobile Biometrics:** Integrating biometric authentication into smartphones for convenient and secure access.

**Behavioural Biometrics:** Analysing patterns in user behaviour, like typing or mouse movements, for authentication.

1. **Biometric performance measure:**

There are a few important measures that are typically used to assess such systems that are identified below that can be used to examine and compare the performance of biometric technologies.

* **FAR, or False Acceptance Rate:**"Type I error" is another name for the FAR. FAR measures the proportion of imposters who are mistakenly counted as legitimate users. Since nearly all biometric systems strive to provide accurate identity, this number should be as small as feasible for authentication.
* **FRR or False Rejection Rate:**The term "Type II error" also applies to the FRR. FRR measures the proportion of legitimate users who are wrongfully denied. The genuine user will experience as little inconvenience or shame as possible because of: The quantity should be as small as feasible. This error is typically more tolerable because the use can take another shot.
* **EER or Equal Error Rate:**FRR and FAR are connected. Unintentionally, a strict FAR requirement (as low as possible) will raise the FRR. This measurement indicates the point at which the FRR and the FAR are equal. Reduction of the rate EER will boost system performance because it denotes a healthy balance in the sensitivity of the system.
* **CER: Crossover Error Rate:**A benchmark error rate at which FAR and FRR are equivalent in biometric devices and technologies. The biometric equipment is more precise and dependable the lower the CER.[49][50][51]

**MOST ACCURATED MEASURES:**

* FRR and FER are frequently used to evaluate biometric accuracy.
* Both techniques were used to test the system's capacity to grant authorized users only limited access.
* However, depending on how you modify the sensitivity of the mechanism that matches the biometric, these measurements vary greatly.
* You could, for instance, need a tighter alignment of the hand geometry measurements with the user's template (raise the sensitivity). This can increase the false-acceptance rate while also likely lowering its rate of false rejection.
* Plotting FAR and FRR against one another makes more sense because of their interdependence[51].

**Conclusion:**

In today’s technology driven society personal identification is must to even complete day to day routine work like using ATM or email. Person’s name is the first documented personal identification characteristics of known history. This name along with father name or surname is valid till date. For personal identification, but on a local level. Due to the emergency of globalization and advent of technology with which one can manipulate the integrity of any documents. To tackle this biometric system has been employed which is developing day by day with advancements in technology. As discussed in above sections of this chapter biometry is the science of recognition of an individual through exploring the physical and behavioural traits. Physical traits are those which are inborn like, iris, fingerprint, retina, DNA etc. whereas behavioural traits include those traits which are acquired by individual during their life but rather subconsciously. However not a single trait is universal and an ideal biometric system should have instrumentation which recognise combination of different traits to avoid the errors.

Establishment of connections of suspect or victim with a crime scene is essential part of forensic investigation and these advanced biometric systems based on unique, distinctive and quantifiable physical or behavioural traits. Most importantly these biometric system data can be stored easily, which helps in development of databank for future comparison if needed during forensic investigations. Fingerprint biometric system is most frequently used biometric system in forensic science. Although, voice base, gait pattern based, facial features based and palm print passed also of great helping tool for any forensic investigators. Nowadays, with the advent of multimodal biometric system which combine different modalities gives the more accurate identification of an individual. The parameters for working efficiently of any biometrics system FAR, FRR, EER and CER which defines the specificity and sensitivity of any biometric system and it is up to the forensic investigator to choice appropriate biometric system which can be representable to the court of justice. Although countries around the world are developing the data base of their citizens using various biometric identifiers but guaranteeing of safety and judicial use of the data are of utmost importance.

**References**:

1. A.K. Jain, R.P.W. Duin, and J. Mao, Statistical pattern recognition: A review, IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), 2000, 4-37.
2. Tistarelli, M., Grosso, E., & Meuwly, D. (2014). Biometrics in forensic science: challenges, lessons and new technologies. In *Biometric Authentication: First International Workshop, BIOMET 2014, Sofia, Bulgaria, June 23-24, 2014. Revised Selected Papers 1* (pp. 153-164). Springer International Publishing.
3. M. Turk, and A. Pentland, Eigenfaces for recognition, Journal of biometric identification e, 3,1991, 71-86.
4. P.N. Belhumeur, J.Hespanha, and D. Knegman, Eigenfaces vs Fisherfaces: Recognition using Class Specific Linear Projection, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 1997, 711-720
5. Babich, A. (2012). Biometric Authentication. Types of biometric identifiers.
6. Maguire, M. (2009). The birth of biometric security. *Anthropology today*, *25*(2), 9-14.
7. Eng, A., & Wahsheh, L. A. (2013, April). Look into my eyes: A survey of biometric security. In *2013 10th International Conference on Information Technology: New Generations* (pp. 422-427). IEEE.
8. Hawthorne, M., Plotkin, S., & Douglas, B. A. (2021). *Fingerprints: Analysis and Understanding the Science*. CRC Press.
9. Chaudhari, R. D., Pawar, A. A., & Deore, R. S. (2013). The historical development of biometric authentication techniques: A recent overview. *International Journal of Engineering Research & Technology (IJERT)*, *2*(10).
10. Perkowitz, S. (2021). The bias in the machine: Facial recognition technology and racial disparities.
11. Jain, A. K., & Kumar, A. (2012). Biometric recognition: an overview. *Second generation biometrics: The ethical, legal and social context*, 49-79.
12. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4-20.
13. J. Daugman, High confidence visual recognition of persons by a test of statistical independence, IEEE Transactions on Pattern analysis and Machine Intelligence, 15(11), 1993, 1148-1161.
14. Sharma, A. K., Raghuwanshi, A., & Sharma, V. K. (2015). Biometric system-a review. *International Journal of computer science and information technologies*, *6*(5), 4616-4619.
15. Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015, December). Fingerprint biometric based access control and classroom attendance management system. In *2015 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.
16. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (Vol. 2). London: springer.
17. Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). *Biometric systems: Technology, design and performance evaluation*. Springer Science & Business Media.
18. Ali, M. M., & Gaikwad, A. T. (2016). Multimodal biometrics enhancement recognition system based on fusion of fingerprint and palmprint: a review. *Global Journal of Computer Science and Technology*, *16*(2), 13-26.
19. Chaki, J., Dey, N., Shi, F., & Sherratt, R. S. (2019). Pattern mining approaches used in sensor-based biometric recognition: a review. *IEEE Sensors Journal*, *19*(10), 3569-3580.
20. Gayathri, M., Malathy, C., & Prabhakaran, M. (2020). A review on various biometric techniques, its features, methods, security issues and application areas. *Computational Vision and Bio-Inspired Computing: ICCVBIC 2019*, 931-941.
21. Woodard, D. L., & Flynn, P. J. (2005). Finger surface as a biometric identifier. *Computer vision and image understanding*, *100*(3), 357-384.
22. Alqadi, Z., Abuzalata, M., Eltous, Y., &Qaryouti, G. M. (2020). Analysis of fingerprint minutiae to form fingerprint identifier. *JOIV: International Journal on Informatics Visualization*, *4*(1), 10-15.
23. Tarase, G. M. (2013). IDENTIFICATION OF AN INDIVIDUAL THROUGH FINGERPRINTS. *J.Bio.Innov2(2)* , 59-72.
24. Stenman J (2013) Embracing big brother: How facial recognition could help fight crime. CNN.
25. Bača, M., Grd, P., & Fotak, T. (2012). Basic principles and trends in hand geometry and hand shape biometrics. *New Trends and Developments in Biometrics*, 77-99.
26. Zhang D, Kong WK, You J (2003) Online palm-print Identification-Pattern Analysis and Machine Intelligence. IEEE Transactions 25:1041-1050
27. Y. Du, C. Belcher, Z. Zhou, and R. Ives, Feature correlation evaluation approach for iris feature quality measure, Elsevier, Signal Processing, 90, 2010.
28. Aeloor, D., & Patil, N. (2017, January). A survey on odour detection sensors. In *2017 International Conference on Inventive Systems and Control (ICISC)* (pp. 1-5). IEEE.
29. Meadows, I. D. L., & Pouratian, A. J. (1999). *U.S. Patent No. 5,869,822*. Washington, DC: U.S. Patent and Trademark Office.
30. Schuch, P., Schulz, S., & Busch, C. (2018). Survey on the impact of fingerprint image enhancement. *IET Biometrics*, *7*(2), 102-115.
31. Scheffer, N., Ferrer, L., Lawson, A., Lei, Y., & McLaren, M. (2013, November). Recent developments in voice biometrics: Robustness and high accuracy. In *2013 IEEE international conference on technologies for homeland security (HST)* (pp. 447-452). IEEE.
32. Sigona, F. (2018). Voice Biometrics Technologies and Applications for Healthcare: an overview. *JDREAM. Journal of interDisciplinary REsearch Applied to Medicine*, *2*(1), 5-16.
33. Jonakait, R. N. THE NEED FOR REGULATION.
34. J.M. Pandya, D. Rathod and J.J. Jadav, “A Survey of Face Recognition approach”, International Journal of Engineering Research and Applications, Vol. 3, No. 1, January -February2013, pp.632-635.
35. J. S. Bedre and S. Sapkal, “Comparative Study of Face Recognition Techniques: A Review”, Emerging Trends in Computer Science and Information Technology – 2012 Proc.published in International Journal of Computer Applications.
36. A. S. Tolba, A.H. El-Baz and A.A. El-Harby, “Face Recognition: A Literature Review”, International Journal of Signal Processing, Vol. 2, No. 2, 2006.
37. Sushma Jaiswal, Sarita Singh Bhadauria, Rakesh Singh Jadon, “Comparison Between Face Recognition Algorithm-Eigenfaces,Fisherfaces and Elastic Bunch Graph Matching”, Journal of Global Research in Computer Science, Vol. 2, No. 7, Jul2011.
38. Ming-Hsuan Yang, David J. Kriegman and NarendraAhuja, “Detecting Faces in Images: A Survey,” IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, January 2002.
39. M. Kirby and L. Sirovich, “Application of the Karhunen-Loeve procedure for the characterization of human faces”. IEEE Trans. Patt. Anal. Mach. Intell., Vol. 12, 1990.
40. X. Li and S. Areibi, “A Hardware/Software codesign approach for Face Recognition”, Proc. 16th,International Conference onMicroelectronics, Tunisia, 2004
41. Lin-Lin Huang, A. Shimizu, Y. Hagihara and H. Kobatake, Face detection from cluttered images using a polynomial neural network, Elsevier Science 2002
42. NEC automatic palmprint identification system (2003).
43. Adeoye, O. S. (2010). A survey of emerging biometric technologies. *international journal of computer applications*, *9*(10), 1-5.
44. [15]Easwaramoorthy, S., Sophia, F., & Prathik, A. (2016, February). Biometric Authentication using finger nails. In *2016 international conference on emerging trends in engineering, technolo.*
45. [16]Garg, S., Kumar, A., & Hanmandlu, M. (2012, November). Biometric authentication using finger nail surface. In *2012 12th International Conference on Intelligent Systems Design and Applications (ISDA)* (pp. 497-502). IEEE.
46. [17]Al-Sultan, T. G., Abduljabar, A. Q., Alkhaled, W. H., Al-Sawaff, Z. H., & Kandemirli, F. (2023). A new approach to develop biometric fingerprint using human right thumb fingernail. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(1), 98-107.
47. [18]Woodard, D. L., & Flynn, P. J. (2005). Finger surface as a biometric identifier. *Computer Vision and Image Understanding*, *100*(3), 357–384. <https://doi.org/10.1016/j.cviu.2005.06.003.>
48. Delac K, Grgic M (2004) A survey of biometric recognition methods. In: Electronics in Marine. Proceedings Elmar 2004. 46th International Symposium. IEEE.
49. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. Circuits and Systems for Video Technology. IEEE Transactions 14: 4-20.
50. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: Security and privacy concerns. IEEE Security and Privacy 33-42.