BIOMETRICS –AN EMERGING TOOL FOR PERSONAL IDENTIFICATION IN FORENSIC

Abstract

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

Keywords: Biometric System, Identification in Forensic, Physiological Biometrics.

Authors

Megha Yadav
Research Scholar
Department of Forensic Science
Guru Ghasidas Vishwavidyalaya
Bilaspur, Chhattisgarh, India.
meghaforensics@gmail.com

Shantnu Singh Rathore
Research Scholar
Department of Forensic Science
Guru Ghasidas Vishwavidyalaya
Bilaspur, Chhattisgarh, India.
rathore4n6@gmail.com

Lt. Col. Kautuk Shrivastav
MBA, Student
GNIM, Guru Govind Singh Indraprastha University
Delhi, India.
kautukshrivastavonweb@gmail.com

Dr. Chanchal Kumar
Assistant Professor
Department of Forensic Science
Guru Ghasidas Vishwavidyalaya
Bilaspur, Chhattisgarh, India.
chanchalbios@gmail.com

Blessi N. Uikey
Assistant Professor
Department of Forensic Science
Guru Ghasidas Vishwavidyalaya
Bilaspur, Chhattisgarh, India.
blessiuikey@gmail.com

I. INTRODUCTION

A biometric system is a technology that uses unique physical or behavioural characteristics for the identification or authorization of a person's identity [1]. Biometrics is a combination of technology and scientific authentication methods which is mainly based on the 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 defined 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 biometric technology is to establish the individual's identity. Associating an identity with an individual is known as personal identification which plays a substantial role in the field of forensic science. Accurate identification of an individual helps in establishing an identity and these unique traits acquired at the crime scene can be helpful after comparing with a set from the data stored in the Biometric system. This Biometric system is useful in the real-time identification of an individual with a database of a complete set of information and hence provides a forensic scientist with a conclusion with a proper result of comparison [2].

The Biometric system automatically recognises individuals using the biometric tool by taking the inputs through scanning devices and then supplying acquired data to the biometric detectors. Subsequently, the biometric system matches the input from the database using algorithms and provides the result. Authentication techniques are used to verify a person's claimed identity; in this case, only the stored biometric attributes that match the claimed identity are compared [3]. Fingerprints, iris scans, face recognition, voice recognition, fragrance, gait patterns, lip prints, hand geometry, nail, and knuckle scans are examples of these qualities. Biometric systems are widely used to obtain control and security such as unlocking smartphones 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, so the biometric data collected must be carefully protected to prevent unauthorized access or misuse.

II. 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 (unfa miliar) individuals ever since the dawn of civilisation. As with the increase in population and ease in migration, the difficulty to recognise arises. The earliest traces of biometrics date back to the Babylonian Empire where fingerprint and thumb impression were recorded for business transactions on clay tablets around 500 BC. But the first occurrence of a biometric identity system was found to be documented in the 1800s in Egypt, while constructing the pyramids, clay slabs with fingerprints of nearly 30000 years old have been found in Tutankhamun's tomb in Egypt. The administrator started to keep records of workers by recording their physical and behavioural traits. Later the use of thumbprint was used as an official seal on documents by Chinese emperors since 240 BC [5]. Joao de Barros the explorer reported that Chinese merchants used to take the palm print and footprints of children on paper using ink to distinguish the children. During the eighteenth century, many anatomical works appeared among which E.J. Purkinje's contribution of 1823 was an

important landmark in the field of fingerprints. He published a treatise on the diversity of ridge patterns and gave a system of classification of fingerprints. In 1858, W.J. Hershel started using fingerprints for official use for the first time on a large scale. Alphonse Bertillon, a French anthropologist described a system for differentiating and classifying criminals through specific body measurements. The first system which focuses on meticulous measurements of different body parts. According to Bertillon some elements of the body remain constant or unchanging throughout life such as the size of the skull or the 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 the individuality and permanence of fingerprints [7]. The fingerprint classification system given by Edward Richard Henry; Inspector General was adopted as a means of identification in place of the anthropometric system in March 1897. In 1901 fingerprints for criminal identification was officially introduces in England. The use of Henry's system with modification was started in 1902 by the FBI and law enforcement agencies throughout the U.S. Beginning in 1903, the New York state jail system commonly utilised fingerprints for criminal identification across the nation. [8]. The Leavenworth Federal Penitentiary in Kanas and the Police Department of St. Louis (Missouri) 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. Later many other law enforcement agencies started using Fingerprints as a form of personal identification during the course of the following 25 years. Frank Burch an Ophthalmologist presented the knowledge of using the iris distinctive patterns 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]. Woody Bledsoe pioneered the subject of automated reasoning by developing a method of facial recognition using machine learning. He presented the notion of feature extraction methodology, which was the first step toward leveraging distinguishing biological qualities for individual verification [10]. Due to substantial advances in computer processing, automated biometric systems have just lately become practicable. However, many of today's automated technologies have their origins in notions that extend back hundreds or even thousands of years. Trauring's study on fingerprint matching in 1963 was the first scholarly work on automated biometric recognition [11].

III. 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

- Using PINS and passwords (something the user knows, a combination of words, numbers or symbols)
- Using Cards (Something the user has, special card, Keys, Identity cards)
- Using anatomical/Behavioural traits (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 a 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, various elements need to be taken into consideration, 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 a lot of criteria, which include Universality, permanence, acceptability, collectability, performance, and circumvention. Etc. (13).

The Following Seven Characteristics are of Importance for Ideal Biometrics.

1. **Universality:** The characteristics or traits that each person will have. Every individual accessing the application must have a trait which can be used as an 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 and 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 circumstances; it should not show variability with changes in condition.

4. **Measurability:** how easily the trait can be measured efficiently without the requirement of very big scanning devices as well as easy to record and measure.

5. **Performance:** How well the biometric system functions. The characteristics explain the speed and accuracy of a Biometric in the process of recognition and authentication.

6. **Acceptability:** How easily it is for a user to accept the biometric system.

7. **Circumvention:** this refers to how the trait can be artificially imitated to fool the system i.e., how easily the system can be fooled. This explains how it can detect the altered artificial trait given to the system [14].

IV. WORKING OF A BIOMETRIC SYSTEM

The Biometric is A Computerized-Based Recognition System which is divided into Two Phases.

- **Enrolment:** During the phase of enrolment the biometric trait of the user is acquired and recorded in the central database. The process of enrolment is a one-time process, in this phase of enrolment; the measurements of the biometric trait are 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.

- **Recognition**: this is the second stage of the biometric system, which is to be the challenging phase. In this, the identity of a person claiming to be is determined. The physiological or behavioural biometric attribute is then re-acquired from the subject

and compared to the information stored in the system. This stage must be precise and rapid [15].

The Working of A Biometric System Can Be Divided into Four Components.

- **Sensor:** This is the first component of the biometric system which acts as an interface between the computer system and the 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 microphones or platens to record voice, digital pads in case of Signature biometrics. The efficiency of the acquisition process in the 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 the 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].

- **Feature Extraction:** In this segment, the raw biometrics data acquired through sensors is pre-processed before the unique features 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. Following that, the essential biometric data is extracted from the background noise using a method known as segmentation [18][19]. Finally, the segmented (extraneous ridges or smudges removed) biometric data is processed through a quality enhancement algorithm to increase the trait's quality and reduce noise. In this feature extraction process, a compressed but communicative digital image of the acquired biometric trait is created known as a *template*. This template will contain only prominent features that are discriminatory in nature which are essential for recognition (detecting minutiae points in a fingerprint is the key feature extraction step in a fingerprint biometric system [20].

- **Data Base:** The biometric system database acts 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 the database along with the personal identity of the individual such as name of the person, Personal identification number PIN, address, gender etc. The biometric data is then stored separately in a centralise or decentralised database based on the biometric system. The biometric data is broken into small fragments and the encrypted data is stored.

- **Matcher:** In this segment of the identification process, the questioned feature is compared against the store template from the database. [21]

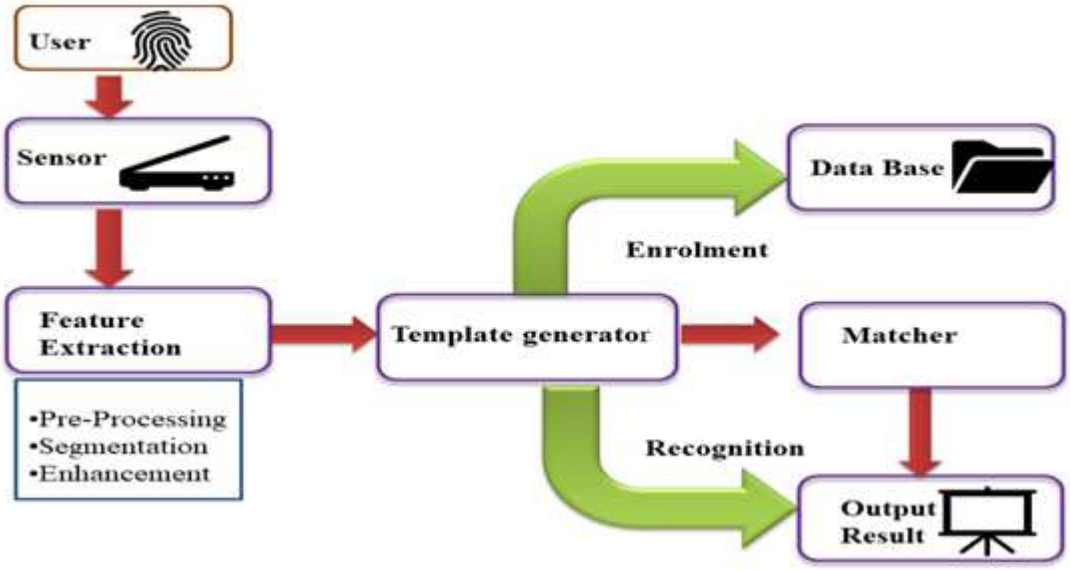

Figure 1: Illustration of working of Biometric System

V. TYPES OF BIOMETRICS

1. **Physiological Biometrics:** The analysis of the physical characteristics feature of a person that is notably identified through five senses. These physiological characters are static in nature. These include Fingerprints, Face biometrics, Iris biometrics, odour, DNA, etc.

Physiological Traits as Biometric Markers

- **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. the raised portion is defined as furrows and the space between two ridges is defined as valleys. These corrugated lines flow from one side of the finger to the other in ridges that resemble lines. These ridges have no flow ongoing and create a pattern. The flow pattern results in a categorization pattern like arches, whorls and loops whereas the ridge flow discontinuity creates feature spots known as minutiae [22, 23, 24].

- **Face Biometrics:** A typical camera can be used to capture a face image. This is the most common or easily accepted biometric for confirming identity. Holistic or global approach and feature-based approach are the two basic methods used for facial recognition

The feature-based method is based on the identification of specific credible 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 images 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.

- **Hand Geometry:** The basic premise underlying utilising the hand as a biometric feature is hand physiology and geometrical measurement of the palm and fingers. A camera or scanner is used to capture the picture or biometric data. By maintaining the user's hand on a chosen platform, the top and side views are taken or scanned. Both the top and side perspectives are caught in a single shot. Various hand characteristics are detected from the picture, such as first detecting the fingers and their breadth, then determining the length and thickness of the fingers. In addition, the curvatures of the hand and fingers, as well as their relative geometry, are determined. [26]. Aligning the user's 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].

- **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].

- **Odour:** Each living component releases an odour that is unique to its own chemical makeup, 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]

2. **Behavioural Trait as a Biometrics Identifier:** these are the traits that are not static and acquired by humans during his development.

- **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 is 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.

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

- **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.

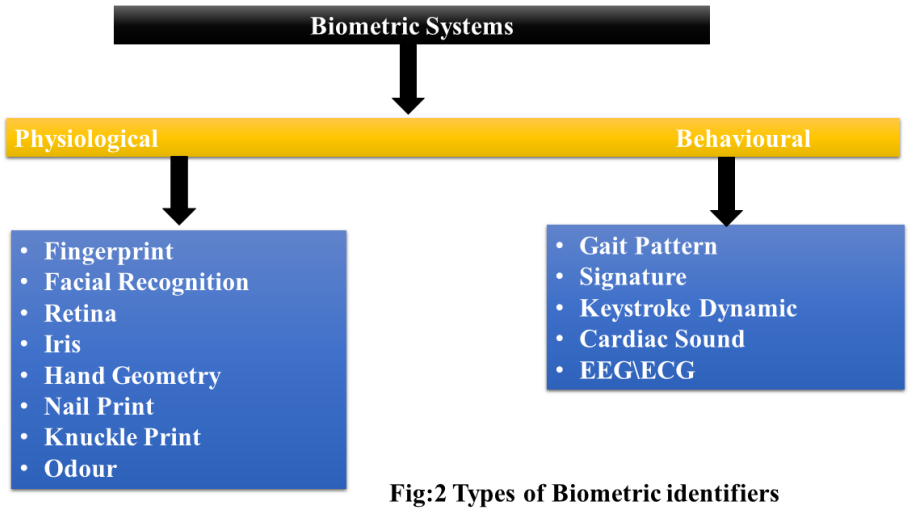

Fig:2 Types of Biometric identifiers

Figure 2: Type of Biometric Identifiers

VI. VARIOUS BIOMETRIC SYSTEMS USED IN FORENSIC INVESTIGATION

1. **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 the same order of sequence and their relative position in both prints are determined. The 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 an abbreviation for automatic fingerprint identification system, which is a computer-based approach that works by taking digital pictures using a scanner and then matching the collected data to fingerprints recorded in a database. The identification is based on finding the minutiae and comparing them in obtained and stored fingerprints. The AFIS greatly helps in fingerprint classification and retrieval by converting scanned or digital formats including ridges with differentiating properties. The bifurcation, or

branching of two ridges, and the ridge ending, or point of termination of the ridge, are the primarily targeted details for comparison. This AFIS system is commonly used by security agencies for criminal identification by matching sets of fingerprints retrieved from crime scenes to the print information kept in the database. [30]. The fundamental purpose of AFIS technology is to enable computers to digitally encrypt and scan fingerprints so that they can be processed quickly. Through AFIS, developed latent fingerprints may also be analyzed. The scanner's fundamental job is to capture an image of a user's fingerprint and look up a match in its database. Dots per inch (DPI) is a unit used to express the quality of a fingerprint image.

- **Digitization and Processing of Fingerprints:** Demands imposed by the painstaking attention required to visually match fingerprints of varying qualities, the tedium of monotonous manual work, and increasing workloads due to increased demand for fingerprint recognition services prompted investigators to initiate an investigation into procuring fingerprints through electronic media and automating fingerprint identification associated with digital representation of fingerprints. As a result of this study, during the last three decades, a huge number of computer algorithms for autonomously processing digital fingerprint photos have been developed. The following five key processes are necessary in the creation of automated fingerprint processing systems: Digital fingerprint capture, picture augmentation, feature extraction (e.g., minutiae), matching, and indexing/retrieval.

- **Image Acquisition:** The resolution area, pixel count, geometric correctness, contrast, and geometric distortion are the key features of digital fingerprint pictures. A range of livescan sensing methods, including optical, capacitive, thermal, pressure-based, ultrasonic, and others, can detect the ridges and valleys in the fingertip

- **Image Enhancement:** After the step of Image acquisition i.e., after taking the digital fingerprint image from scanners we cannot use the same image as it is for further processing. The captured images contain some noise characteristics in the form of dark extra ridges or smudged regions. Because of this image enhancement algorithms are required whose function is to remove noise from the acquired image. The enhanced image contains the bright, clear and contrasting ridge patterns; it also removes the artificially generated ridges. This eliminates the possibility of inaccurate minutiae detection during the feature extraction stage, leaving only actual minutiae and ridge characteristics accessible. This picture-enhancing phase provides for the most accurate matching in the database's collection of millions of fingerprints. The level of details of the fingerprint ridges in the fingerprint picture can be considerably improved by automated fingerprint image enhancement methods, which also improve the image's suitability for additional human or automated processing. The image enhancement methods do not enrich the fingerprint picture with any external data. [16,17,31]. Only data that is already available in the fingerprint picture is used by the improvement techniques. The enhancement algorithms can minimize various forms of noise in the fingerprint picture and bring attention solely to important value elements. These image enhancement techniques may be classified into two classes. The first method is manual enhancement through a graphical interface in which forensic specialists improve image quality by employing different needed algorithms. This method operates on the collected image's region of interest. This image may also

be cropped to acquire the appropriate area, the intensity of the image adjusted, the contrast of the image with the backdrop enhanced, the image enlarged or zoomed, and the image size resized, compressed, or decompressed. Intensity adjustments, brightness and contrast adjustments, histogram equalisation, image intensity rescaling, image intensity adjustments with high and low thresholds, local or global contrast enhancement, local or global background subtraction, sharpness adjustments (using a high-pass filter), and so on are examples of enhancement algorithms. The fingerprint ridge pattern in poor fingerprint pictures may be automatically improved by using enhancement algorithms that function entirely automatically. Contextual filtering is used to increase the contrast between ridges and valleys. It has a low pass (smoothing) effect along the fingerprint ridges and a band-pass (differentiating) effect in the direction orthogonal to the ridges. For this form of filtering, oriented bandpass filters are commonly used. Gabor filters are one type of often-used filter. Local context is obtained via such contextual filters in the form of local direction and local frequency.

- **Feature Extraction:** Fingerprint ridges comprise minute distinguishing features termed Minutiae or Galton's details, which are used to match fingerprints. Bifurcation, short hills, lakes, islands, spurs, crossroads, and many more details are typically utilized. The algorithms in feature extraction extract and find these details. Only bifurcation and ridge ending are mostly examined for matching purposes in the minutiae extraction of fingerprints. Some algorithms will be unable to distinguish between bifurcation and ridge-ending.

  Local fingerprint ridge singularities, also known as minutiae spots, such as the lake, island, spur, crossing, and so on (except for dots), are merely composites of ridge ends and bifurcations. To replicate the minutiae placement done by forensic analysts, automatic fingerprint feature extraction techniques were formed. Only ridge ends and bifurcations are considered by automatic fingerprint minutiae extraction techniques. Furthermore, most algorithms may not detect between ridge ends and bifurcations since they might be indistinguishable due to changes in finger pressure during acquisition. A binarization technique is used to convert the grayscale-enhanced fingerprint picture into binary (black and white) form, where all black pixels correspond to ridges and all white pixels belong to troughs. This is one of the most used fingerprint feature extraction algorithms. Numerous automated fingerprint feature extraction (and matching) approaches that use data from fingerprint images other than minutiae have emerged. Algorithms, for example, have been proficient in recovering sweat pores—extremely minute fingerprint patterns smaller than minutiae points—from high-resolution fingerprint photographs.

- **Matching:** Fingerprint matching is the process of finding similarities and differences between two sets of fingerprint pictures. The fingerprint-matching algorithm's role is to analyse the extracted feature from the feature extraction step and identify the common minutiae elements in the ridges with their placements and directions. The outcomes of fingerprint feature extraction methods are used by automatic fingerprint-matching algorithms to assess whether two sets of minutiae are similar or distinct. Automatic feature matching can examine fingerprints millions of times per second and filter the results based on the degree of

similarity. The alignment algorithm's role is to align all the minutiae, and the feature extraction algorithm's function is to identify the unique spots that are minutiae in the two comparing fingerprint sets. After the comparison, the similarity score is calculated using a computational process to evaluate the matching percentage.

- **Indexing and Retrieval:** In AFIS, matching is constrained not just by comparing two sets of fingerprint data, but sometimes unfamiliar fingerprints are matched with the enormous number of fingerprints saved in the database. A vast number of databases are analysed for this purpose, as well as a significant number of fingerprint searches and matching across the database. For identification and individualization, the fingerprint indexing method initially categorises the print at level I- pattern-based categorization, which is divided into five types: whorl, arch, tented arch, left-handed loop, and right-handed loop. Based on the retrieved characteristics, categorization is conducted, and fingerprints are indexed in the database. After indexing, the matching fingerprint is obtained by comparing it to the same print.

2. **Voice Biometrics:** The phrase voice biometrics refers to speech processing technology or a system that uses voice to validate a person's identification in an overt and discrete manner. Speech processing and biometric security are two subcategories of voice identification. Voice biometrics perform their tasks by extracting data from the speech stream, just like other speech-processing techniques. Voiceprint is a set of measurable characteristics of a person's voice that may be used as a biometric identification. These features, which are based on the physical layout of a speaker's lips and throat, are expressed mathematically [32]. In the age of telephone, radio, and tape recorder conversations, the human voice frequently acts as essential evidence tying a person to criminal conduct. The number of phone bomb threats, obscene phone calls, and kidnapping ransom messages on tape has skyrocketed. Human speech has piqued the curiosity of law enforcement officials in technical solutions that can convert voice into a form that may be utilised for personal identification [33]. The form of our vocal chambers, as well as the way our lips moves as we talk, both contribute to the uniqueness of our voice. To employ voice as a biometric attribute in a voiceprint system, the user should either say the exact words or phrases requested, or offer a substantial sample of speech so the computer can recognise the claimed identity independent of the words spoken. Speech spectrographs are used to identify the speaker's voice based on the premise that genetics, sex, age, and other socio-environmental variables have an influence on the vocal cavity sizes and coupling of the articulators. As a result, it is highly rare that two people will yield similar voice prints. Voice biometrics is a hybrid of physiological and behavioural biometrics. Voice recognition systems are classified into two types: text dependent and text-independent. In a text-dependent voiceprint system, either utter the precise words or phrases necessary or take an extensive sample of your speech so that the computer can identify the user regardless of the words they say. The sound spectrograph may generate two types of voiceprints, one termed a bar voice print and the other a contour voice print. What was spoken is determined by the voice print produced in one of the three methods. It also shows time as a horizontal axis, frequency as a vertical axis, and amplitude as a function of the density of the sequence of the identical vowels pronounced by the unknown and identified voices. A visual comparison is done to

investigate whether the recorded sounds are similar or distinct. The contour voiceprints are utilised for computer automatic classification of the speaker's voice for filing and recording, but the bar voiceprints are only used in courtroom presentations. Attempts to hide the voice by whispering, muffling the voice, or gripping the nose, according to the study, do not change the essential elements of a person's voiceprint. Voice replicas have also failed to prevent voice recognition using a sound spectrograph. Speech identification via spectrographic speech analysis is a difficult technique. Furthermore, the interpretation of the voiceprints is dependent on the knowledge of the examiner operating the device, as well as his experience and talent in recording and interpreting spectrograms. The first step is to use a tape recorder to record the mysterious voice. The next step is to track down the suspect and record his voice using the same text as the anonymous caller. The expert examiner then prepares relevant exemplars from the known and unknown voices based on the two recorded voices. These exemplars are then scanned using an audio analysis device to provide voice prints in the form of graphical patterns [34]. When most people think about voiceprints, they see a wave pattern on an oscilloscope. However, the data utilised in a voiceprint is a sound spectrogram rather than a wave shape. A spectrogram is essentially a graph that shows the frequency of a sound on the vertical axis and time on the horizontal axis. Different speech sounds produce various forms on the graph. Colours or shades of grey are also used in spectrograms to depict the acoustical properties of sound. Some companies hire voiceprint recognition to allow customers to find access to the information or grant consent without physically being present. Instead of approaching an iris scanner or hand geometry reader, anybody can offer authorization over the phone. Unfortunately, certain systems, including those that operate over the phone, may very well be circumvented by simply recording an official person's password. As a result, some systems employ several randomly generated voice passwords or broad voiceprints rather than prints for individual phrases. Others employ technology that identifies artefacts produced during recording and playback. Other techniques are more complex to circumvent.

3. **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, make 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 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 a 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

4. Face Recognition Techniques

- **Eigen Face:** 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 train 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.

- **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 the palm. These characteristics are highly helpful for identification and verification also known as personal authenticity, even though these measures are not very differentiable across individuals. Combining a 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 conditions such as any disease, ageing or weight can alter the curve of the hand [42]. It is actually based on the 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 the palm is considered which is divided into the thenar (raised portion of the palm near the thumb), hypothenar and interdigitalis (below the four fingers) region. Later the geometrical measurements such as length, breath of fingers distance between two fingers are measured. These all characteristics altogether is acquired through scanners which capture a 3-dimensional image of the hand. Further, the image is pre-processed and features are extracted. Hand geometry is a prime choice for the 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 features extracted from the image of hand that are used in biometric systems. These are explained in given table

1.	Thumb length	17.	Ring circle radius upper
2.	Index finger length	18.	Pinkie circle radius lower
3.	Middle finger length	19.	Pinkie circle radius upper
4.	Ring finger length	20.	Thumb perimeter
5.	Pinkie length	21.	Index finger perimeter
6.	Thumb width	22.	Middle finger perimeter
7.	Index finger width	23.	Ring finger perimeter
8.	Middle finger width	24.	Pinkie perimeter

9.	Ring finger width	25.	Thumb area
10.	Pinkie width	26.	Index finger area
11.	Thumb circle radius	27.	Middle finger area
12.	Index circle radius lower	28.	Ring finger area
13.	Index circle radius upper	29.	Pinkie area
14.	Middle circle radius lower	30.	Largest inscribed circle radius
15.	Middle circle radius upper		
16.	Ring circle radius lower		

VII. 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.

VIII. EMERGING TRENDS IN BIOMETRICS

New Emerging Biometric Technologies

1. **Fingernail Bed:** Human fingernails possess a high level of individuality, regardless of whether they are shared by identical twins or between individual fingernails. 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 the nail bed. You can't use a full nail plate for authentication because of 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 a nail plate, nail matrix and nail bed. The 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 is firmly attached to the base of your finger and the top epidermis 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 onychomycosis, 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. [46-48].

2. **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. However, 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-the-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 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.

IX. 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.

1. **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.

2. **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: The quantity should be as small as feasible. This error is typically more tolerable because the user can take another shot.

3. **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.

4. **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. [49-51]

Most Accurate 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].

X. CONCLUSION

In today's technology-driven society, personal identification is a must to even complete day-to-day routine work like using an ATM or email. A person's name is the first documented personal identification characteristic of known history. This name along with the father's name or surname is valid till date. For personal identification, but on a local level. Due to the emergence of globalization and the advent of technology, one can manipulate the integrity of any document. To tackle this biometric system has been employed which is developing day by day with advancements in technology. As discussed in the 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 the 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 recognises a combination of different traits to avoid errors.

The establishment of connections of suspect or victim with a crime scene is an essential part of forensic investigation and these advanced biometric systems are based on unique, distinctive and quantifiable physical or behavioural traits. Most importantly these biometric system data can be stored easily, which helps in the development of a databank for future comparison if needed during forensic investigations. The fingerprint biometric system is the most frequently used biometric system in forensic science. However, voice base, gait pattern, facial features and palm print are also great helping tools for any forensic investigators. Nowadays, with the advent of multimodal biometric systems 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 define the specificity and sensitivity of any biometric system and it is up to the forensic investigator to choose an appropriate biometric system which can be representable to the court of justice. Although countries around the world are developing the database of their citizens using various biometric identifiers 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] Easwaramoorthy, S., Sophia, F., & Prathik, A. (2016, February). Biometric Authentication using finger nails. In *2016 international conference on emerging trends in engineering, technolo.*
[45] 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] 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] 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.

