The Historical Development Of Biometric Authentication Techniques: A Recent Overview

Rahul D Chaudhari
S.S.V.P.S. Science College, Dhule
North Maharashtra University, Jalgaon

Ashok A Pawar
S.S.V.P.S. Science College, Dhule
North Maharashtra University, Jalgaon

Rakesh S Deore
S.S.V.P.S Science College, Dhule
North Maharashtra University, Jalgaon

***Abstract*— Over the last few decades, a new area of Human Computer Interaction has been established whose products are likely to create a large business in the near future. It has been called 'Biometrics'. Biometrics is seen by many as a solution to a lot of the user identification and security problems. This paper presents an overview of the biometrics authentication technology, its utilization and introduces the resent issues underlying the biometrics.**

***Index Terms*—Biometrics, Identification, Verification, Evaluation.**

I. INTRODUCTION

Authentication is a most important component in human computer interaction. Reliable authorization and authentication are becoming essential for many application such as boarding an aircraft (in travel documents & visa), financial transaction into the banks, industry employee, healthcare provider and government organization. Authorization is almost always conferred in a single individual or in a small group of individuals identity verification becomes a challenging task when it has to be automated with high accuracy and hence with low probability of break – in and reliable non- repudiation. The user should not be able to know how transaction carried out and should be unsuitable as little as possible. Which only makes the task more difficult [1]. Biometric is one such strong authentication technology.

Identifying people is a crucially significant of society and culture, since for many activities ensuring the identity and authenticity of people is a prerequisite. Biometric authentication has grown in popularity as a way to provide secure personal identification and verification which control access to valuable information, to economic assert and to parts of the national infrastructure. In this paper, we present information on Biometric Authentication techniques and application. We hope that this work will provide a good knowledge about Biometric system to which the beginner researcher to do work in this area.

II. BIOMETRICS

"Biometrics are automated method of recognizing a person based on a physiological or behavioral characteristic". Some time biometrics is the science of identifying or verifying the identity of a person based on physiological and behavioral characteristics. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [2].

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by Hand, Face, Ear, Eye, Finger Print, DNA,. Behavioral biometrics is related to the behavior of a person, including but not limited to: typing rhythm(Keystroke), Signature and voice. Some researchers have coined the term behavioral biometrics to describe the latter class of biometrics.[3,4,5] The selection of a particular biometric for use in a specific application involves a weighting of several factors that are as follows.

1	Universality	Each and every person should have the characteristic such as fingers, iris, face, DNA which can be used for identification.
2	Distinctiveness	Every person should be sufficiently different in terms of the characteristic with other person.
3	Permanence	These characteristic should not largely change throughout human being life.
4	Collectability	Human characteristic can be measured and collected for quick identification.
5	Performance	The degree of accuracy and speed of identification must be quite high before the system can be operational.
6	Acceptability	Which indicates the extent to which people are willing to accept the use of a particular biometric characteristic in their daily lives.
7	Circumvention	In order to provide added security, a system needs to be harder to circumvent identity management systems.

Table: Seven Pillars Of Biometrics System

Depending on the application context, a biometric system may operate on two modes either in *verification* mode or *identification* mode :

A. *Verification mode:-*

In the verification mode, the system validates a person's identity by comparing the captured biometric data with his own biometric templates stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN Personal Identification Number, a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not [6].

B. *Identification mode:-*

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity without the subject having to claim an identity or if the subject is not enrolled in the system database then it is fails. Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience. While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics [6].

III. THE ORIGIN OF BIOMETRICS

The term "biometrics" is derived from the Greek words bio (life) and metric or metry (to measure). Interestingly, the term "biometrics" was not used to describe these technologies until the 1980s. The first reference found for the term *"biometrics"* was in a 1981 article in *The New York Times* [7, 8].

In the centuries after several types of non-automated biometrics methods used by human being but "automated" biometric technologies are invented with the development of computers [7]. The first known reference to non-automated biometrics was in prehistoric picture writing of a hand with ridge patterns that was discovered in Nova Scotia[8]. Finger-print recognition represents the oldest method of bio- metric identification, with its history going back as far as at least 6000 B.C [7].

The first recorded use of fingerprints was by the ancient Assyrians, Babylonians, Japanese, and Chinese for the signing of legal documents. In ancient Babylon, fingerprints were used on clay tablets for business transactions. A form of fingerprinting was used in China, as reported by explorer Joao de Barros. He wrote that Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the children from each other. The first modern study of finger-prints was done by Johannes Evan-gelista Purkinje, a Czech physiologist and professor of anatomy at the University of Breslau. In 1823, he proposed a system of fingerprint classification. The English began using palm and fingerprints in India in July 1858, when Sir William Herschel pressed handprints on the backs of con-tracts. Herschel moved from palm-prints to prints of the right index and middle fingers [7].

In the 1890s, an anthropologist and police desk clerk in Paris, France, named Alphonse Bertillon sought to fix the problem of identifying repeat offenders who often gave aliases each time they were arrested. Bertillon realized that certain elements of the body remained stable and unchanging, such as the size of the skull or the length of the fingers. He developed a method of multiple body measurements that was named after him and called **Bertillonage**. His system was used by police around the world but quickly faded when it was discovered that some people shared the same measurements in certain parts of their bodies [7].

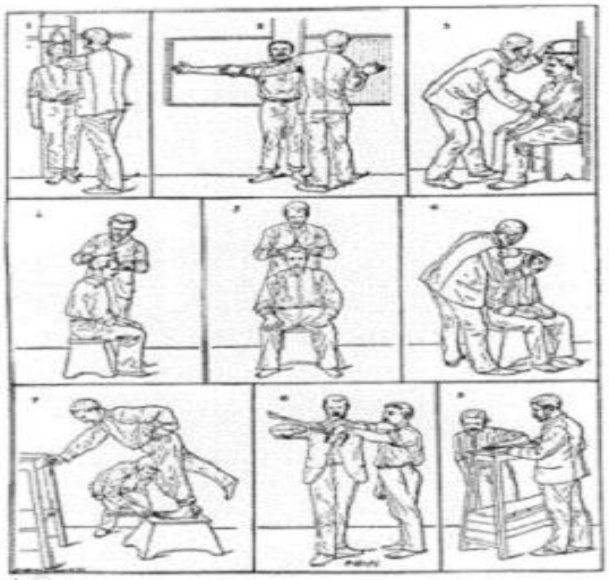


Fig:- Chart demonstrating "Bertillonage" measurements

In the late 19th century, Sir Francis Galton wrote a detailed study of fingerprints in which he presented a new classification system using prints of all 10 fingers. According to Galton's calculations, the odds of two individual fingerprints being the same were 1 in 64 billion. Galton identified the characteristics by which fingerprints can be identified (minutia), which are same ones still in use today. This classification of minutia is often referred to as Galton's Details [7].

Also, during the 1890s, the police in Bengal, India, under the British police officer Sir Edward Richard Henry, began using fingerprints to identify criminals. As assistant commissioner of metropolitan police, Henry established the first British fingerprint files in London in 1901. The Henry Classification System to be use today in all English speaking countries [7].

In 1903, the New York State Prison System began the first systematic use of fingerprints in the United States for criminals. In 1904, the use of fingerprints began in Leavenworth Federal Penitentiary in Kansas and at the St. Louis [Missouri] Police Department. In 1905, the U.S. Army began using fingerprints. Two years later, the U.S. Navy began using fingerprints and was joining the following year by the Marine Corps. During the next 25 years, increasing numbers of law enforcement agencies joined in the use of fingerprints as a means of personal identification [7].

In 1936 concept of using the iris pattern for identification to recognize, an individual is proposed by ophthalmologist Frank Burch [9].

Some of the earliest work on machine recognition of faces can be traced back to the 1960s at a company called Panoramic Research in Palo Alto, California. This research, later referred to as artificial intelligence, was conducted by

Woody Bledsoe, a pioneer in the field of automated reasoning. The technique he developed was called "man-machine facial recognition" and used a process known as feature extraction [7].

In 1965 North American aviation developed the first signature recognition system.

1974 was a breakthrough year for automated biometrics as the University of Georgia began using hand geometry in its dormitory food service areas. Both the Stanford Research Institute in the United States and the National Physical Laboratory in the United Kingdom had begun working on signature recognition systems [7].

In 1985, one of the first retinal scanning systems was deployed for securing access to a Defense Department facility at the Naval Postgraduate School [7].

In the mid-1980s, the State of California began collecting fingerprints as a requirement for all driver license applications [7].

The first biometric industry organization, the International Biometrics Association (IBA), was founded in 1986–1987[7].

Iris recognition technology was developed in the 1980s by Dr. John Daugman at the University of Cambridge. Other new technologies produced during this time included facial thermography and the first commercially available facial recognition systems [7].

In 1998, the International Biometric Industry Association (IBIA) was founded in Washington, DC, as a non-profit industry trade association to advance the collective international interests of the biometric industry. The National Biometric Security Project (NBSP) was founded in 2001 to respond to the events of September 11, 2001, and the need for accelerated development and deployment of biometrics technologies [7].

After the start of 20th century, the lot of biometric techniques used by a human being in there daily life.

IV. HOW BIOMETRICS WORKS

At their most basic level, biometric technologies are pattern recognition systems that use either image acquisition devices, such as scanners or cameras in the case of fingerprint or iris recognition technologies, or sound or movement acquisition devices, such as microphones or platens in the case of voice recognition or signature recognition technologies, to collect the biometric patterns or characteristics [10].

The process of a biometric system can be divided into two independent phases. The learning phase (Enrolment phase) and authentication (verification).

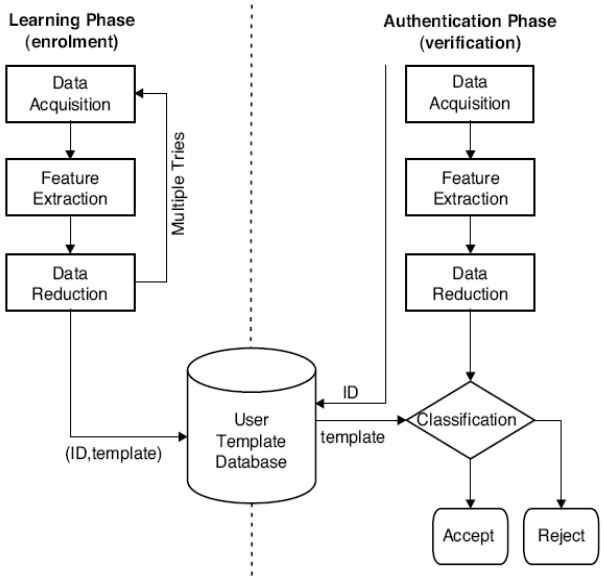


Fig :- Architecture Of Biometric System[11]

The enrolment phase is responsible for training system to identify a given person. The efficiency, accuracy and usability of a biometric system depend directly on the enrolment process During the enrolment phase, a biometric system collecting the biometric sample through one or more acquisition cycles. A feature extractor processes this representation, to generate a more compact and expressive representation called a template. For a facial image, these features may include the size and relative positions of the eye, nose, and mouth extracted from the facial image. The template for each user is then stored in a biometric database. The database can be a central or distributed database, such as the one in which each user's template is stored on a smart card and issued to the user [11].

The challenging phase can be in the form of authentication (verifying a claim "I am Peter ") or identification thus determining the identity of a person from a database of known persons. In an authentication system, when the captured characteristic and the stored template of the claimed identity are the same, the system concludes that the claimed identity is correct. In an identification system, when the captured characteristic and one of the stored templates match within a predetermined threshold, the system identifies the person with the matching template [11].

In the authentication (verification) phase, a single gait sequence is taken, pre-processed and entered in the feature extraction block. This single set of features is compared to the template previously stored, obtaining a ratio of likeliness to verify the user's claimed identity [11].

V. BIOMETRIC TECHNIQUES AND METHODS

Human biometric characteristics can be divided into two different categories: Physiological and Behavioural.

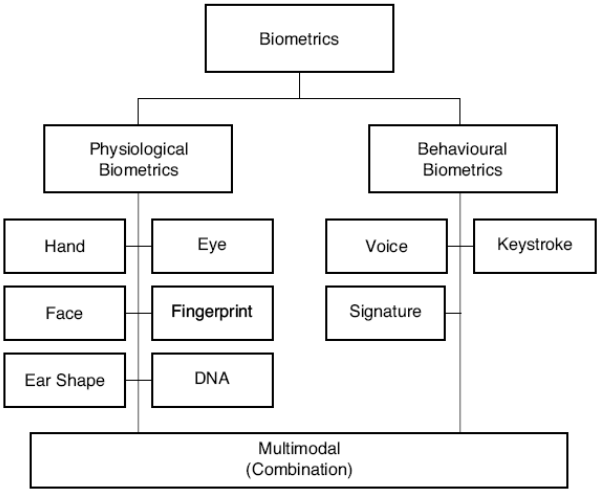


Fig : Biometric Methods

The physiological characteristics are relatively stable, such as face, fingerprint, hand silhouette, iris pattern, blood vessel pattern of the retina, or DNA fingerprint. Those biometric traits are essentially fixed and do not change over time. On the other hand, behavioural characteristics are more prone to change depending on factors such as aging, injuries, or even mood. There are so many techniques based on seven factors are provided in above table. Those are as follows:

A. Hand Geometry Technology

Hand geometry systems have the longest implementation history of all biometric modalities. David Sidlauskas developed and patented the hand geometry concept in 1985, and the first commercial hand geometry recognition systems became available the next year. The 1996 Olympic Games implemented hand geometry systems to control and protect physical access to the Olympic Village [12].

It is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after a certain age. These techniques include the estimation of length, width, thickness and surface area of the hand [13,14].

Hand geometry recognition systems measure the physical dimensions of a hand (or finger) from a 3D image. The measurements collected include the shape, width and length of the fingers and knuckles, and the thickness of the hand (or finger). The user places his/ her hand on the sensor, which includes guidance poles to ensure the correct positioning of the user's hand and fingers. The sensor uses a camera to take images of both the top and the side of the hand. The sensor does not record any surface details, such as finger or palm prints, scars, or skin colour and the resulting image is black and white [15,16,17,18].

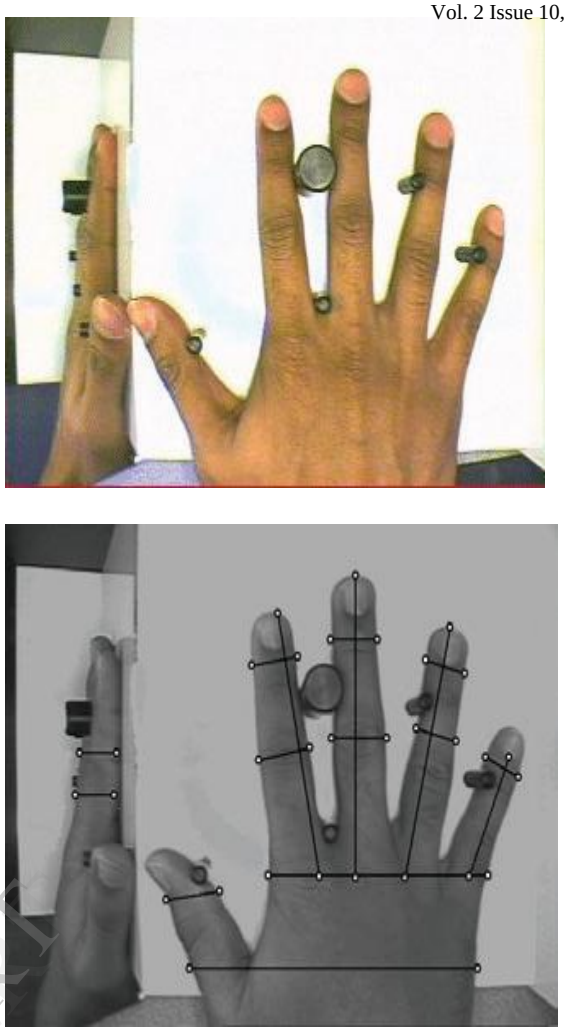
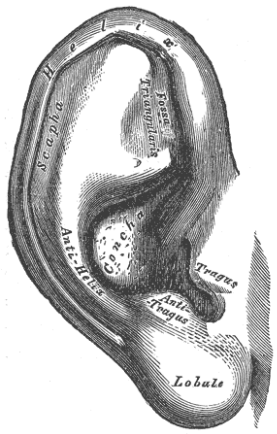


Figure 4: Collecting a hand geometry sample.[19]

The enrollment process of a hand geometry system typically requires the capture of three sequential images of the hand, which are evaluated and measured to create a template of the user's characteristics. Upon the submission of a claim, the system recalls the template associated with that identity; the claimant places his/her hand on the plate; and the system captures an image and creates a verification template to compare to the template developed upon enrollment. A similarity score is produced and, based on the threshold of the system, the claim is either accepted or rejected [12].

B. Ear

This form of biometric recognition is based on analyses of the shape of the outer ear, the ear lobes and bone structure, and both 2D and 3D methodologies are used. A sensor (*e.g.* a camera) collects a side profile image of the user's head, from which the system automatically locates the ear and isolates it from the surrounding hair, regions of the face, and the user's clothes. The algorithm uses a combination of colour and depth analysis to first localise the ear pit, then generates an outline of the visible ear region. The algorithm has to account for differences in skin tone (caused by lighting variation), as well as differences in ear size, ear shape, hair occlusion, and the presence of earrings [18].



C. Face

Facial recognition research has been ongoing since the 1960`s and multiple approaches have been devised [12]. Biometric facial recognition is an automated or semi-automated process, which records and compares the spatial geometric distinguishing features of the face [20]. This can include the location and shape of facial attributes – including the eyes, eyebrows, nose, lips, chin – and their spatial relationships, analysis of the entire facial images, and even the analysis of skin texture [18].

Using digital cameras facial recognition technology capture facial images and, like their biometric technology counterparts, generate templates for comparing a live face to a stored enrollment template.

There are four primary method used by facial recognition for generating facial based biometric templates and identification.

1. "Spectral Decomposition Methods" (Eigenfaces and local Feature Analaysis)
2. Elastic bunch graph matching,
3. Support Vector Machines
4. Local Correlation ("texture") Methods.

1. Eigenface

It is deriving from the well known mathematical technique of Principal Component Analysis based on "eigen vectors", is a technology with some patents held by MIT. It uses two dimensional, global grayscale images to "decompose" a facial image. That is, a facial image is represented by some combination of factory-set, global (full face) eigenfaces, added up like overlaid transparencies. These eigenfaces resemble "ghost" faces. Any face image can be approximated by some combination of the ghost-like eigenfaces. The particular weightings of the factory-standard eigenfaces required to represent the sample is stored as the template. Matching is then attempted by comparing the weightings required to represent a sample face to those stored as the template. If they are similar, the images may have come from the same source. Because the basis transparencies are "global" (looking like an entire face), any change in a sample facial image changes the required weightings for all of the eigenface components [7].

2. Local Feature Analysis

It is based on the same principle as eigenfaces, but each basic factory-set transparency does not look at all like a "ghost" image. Rather, most of the basis transparencies are 0 (zero) valued, having non-zero values over only a small local portion of the face image. Consequently, it is more flexible in accommodating changes in facial appearance and/or expressions. The LFA method uses dozens of features from various areas of the face. This method is not a global representation of the face [7].

3. Elastic Bunch Graph Matching (EBGM)

It was developed by Professor Christoph vonder Malsburg at the University of Southern California. In this method, a bendable grid is placed on the face image and Gabor filters of various size, orientation, and frequency are placed on each vertex of the grid. The values of the image under the various filters form a "jet" (a series of numbers) on each vertex of the grid. These jets are stored as the reference. When a sample face is compared to the reference, moderate bending of the grid is allowed to create sample jets of best fit to the reference[7].

4. Support Vector Machines

It has been successfully used by vendors, as well. The many thousand individual pixels of a face image are multiplied by a "kernel" to actually increase the number of numerical values representing the face. The kernel is chosen to provide maximum separation of the various faces in the new, higher dimensional space [7].

5. Local Correlation ("texture") Method Analysis

It is also called "texture mapping," looks for small regions of similarity between the pixels of the sample image and pixels of the template, saved as an entire image. If enough of these regions can be found and if they are in the same basic areas of both images, the images are deemed to have come from the same source [7].

D. Iris Recognition

The original concept of using the iris for recognition purposes was suggested in the 1930s, however, it was not until the early 1990s that an algorithm for automated iris recognition was developed [18].

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris (Figure 1). The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle (Figure 2) [9].

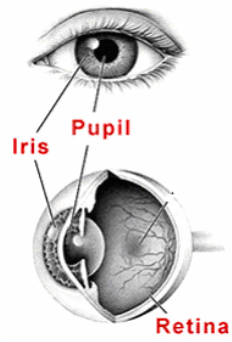


Figure 1: Iris Diagram

Figure 2: Iris Structure

The user looks at the sensor, in this case a camera, and the detailed structure of his/her iris is illuminated using near infrared light. The algorithm involved then produces a mathematical representation of the complex iris structure. The image is also modified to reduce noise and other irrelevant information caused by eyelashes and eyelids occluding (masking) the iris and to account for resolution issues due to the level of illumination. This modification process can result in the loss of actual iris pattern information, but it is not considered to adversely affect the matching process. Finally, the remaining pixels relating to the iris are converted to bit pattern representations (templates or IrisCodes) of the iris, which are often up to 2048 bits in size. During the recognition process a live iris image is converted to a template and is compared with the enrolled template *via* a bit-to-bit comparison, which measures the correlation between the irises [18].

E. Fingerprint Recognition

The idea that no two individuals have the same fingerprints and that fingerprints patterns do not change significantly throughout life became accepted during the 19th century. This gave rise to the practice of using fingerprints for the identification of individual.

The skin on the surface of a fingertip consists of raised folds of skin, known as ridges, and these ridges are separated by valleys. The pattern of ridges and valleys on a fingertip represents a fingerprint, which is what is used in biometric recognition. The three major fingerprint features used for pattern recognition are **arches, loops and whorls**, one of which is found on a given fingerprint. Two other major features may also be used for recognition, i.e. the core and delta. The core is the centre point of a particular fingerprint pattern and the delta is a point from which three patterns deviate. The core and the delta can be used as landmarks to orient two fingerprints for matching; however, it should be noted that these features are not found on all fingerprints [18].

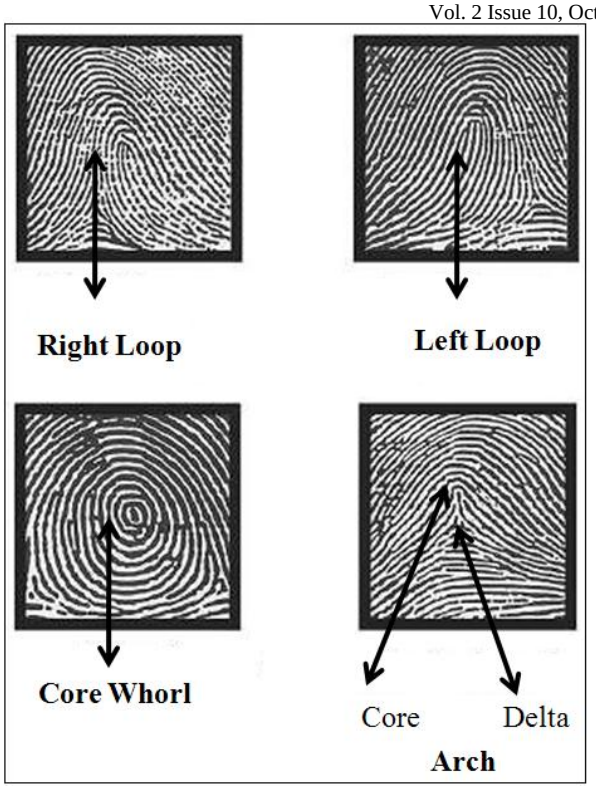


Figure : Fingerprint patterns: Arch, Loop and Whorl.

The minor features used in fingerprint recognition are known as minutiae – hence, the process is known as minutiae matching. Minutiae are discontinuities that disrupt the flow of fingerprint ridges and there are two main types, *i.e.* endings and bifurcations. An ending is where a ridge stops and a bifurcation is where a ridge splits in two [18].

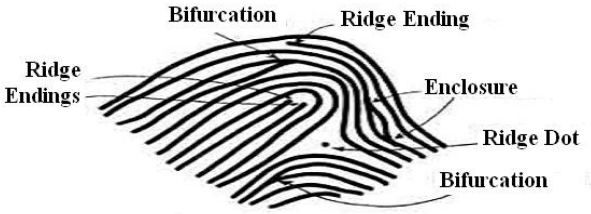


Figure : Minutiae

The basic steps of fingerprint recognition are generally the same for both pattern and minutiae matching. A high quality image is initially collected using one of three different sensor types, namely optical, silicon (capacitance) or ultrasound. With an optical sensor the user places their finger on the sensor surface (platen) and a laser light illuminates the fingerprint. This light is reflected by the ridges of the fingerprint and is converted to a digital signal [18].

Fingerprint-based systems can also be further categorized into four broad groups:

1. Minutiae-based matching (analyzing the local structure),
2. Direct Correlation Techniques,
3. Optical Comparison,
4. Spectral Ridge-Pattern Matching (analyzing the ridge or global structure) of the fingerprint.

Most fingerprint technology vendors' algorithms analyze minutiae points. The current international standard for minutiae extraction recognizes two general characteristics as comprising minutia points: ridge endings (the end of a ridge) and bifurcations (Y-shaped split of one ridge into two ridges).

The process of feature extraction is a crucial step in fingerprint recognition since all subsequent operations are dependent on the quality of the image. While the actual feature extraction algorithm used is proprietary to the system vendor, the general process involves reducing the "noise" of the image and enhancing the ridge definition to allow more precise detection of the minutiae (or pattern features). The algorithm filters out distortions and false minutiae caused by dirt, scars, sweat, etc., but this may also result in deletion of actual minutiae. The resulting template contains between 10 and 100 minutiae, whereas the original image would have contained between 50 and 200 minutiae. Approximately 80 per cent of vendors utilise minutiae matching in some format, with the remainder using pattern matching. In pattern matching, the enrolled template represents a series of ridges from the original fingerprint, and during verification (or identification) this is compared with a submitted template corresponding to the same area of the fingerprint. The use of multiple ridges reduces the dependency on individual minutiae points, which can be affected by wear and tear, during the matching process. However, as a result, pattern matching templates tend to be larger than minutiae templates, 900–1200 bytes compared with 250–700 [18].

F. DNA (Deoxyribonucleic Acid)

Each and every individual human being is identifiable by genetic variation found in his/her DNA. DNA (DeoxyriboNucleic Acid) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have the identical DNA pattern. DNA is currently used mostly in forensics applications for identifying people. In the case of forensics, the first stage in DNA analysis involves the collection of a DNA sample (a collection of cells), such as blood or hair, for example, from a crime scene. The DNA is then isolated from this sample and the targeted loci are first amplified, then the DNA is cut and sorted so that the different sections are arranged by size, i.e. related to the number of repeating units. The final DNA profile when transcribed is a digital representation of the requisite areas of variability with the number of repeat units at each locus indicated [18].

With forensic DNA identification, two DNA profiles, for example, one taken from the scene of a crime and a reference profile generated from a criminal suspect are compared. If both DNA profiles are different, the individual suspect is unlikely to be the source of the sample from the crime scene. If the DNA profiles match, then the question arises whether or not the DNA sample collected from crime scene is actually from the suspect or from someone else with the same DNA profile. The significance of the match is dependent on the number of loci that are compared, for example, the probability of two profiles from two different people matching exactly over ten or more loci is considered to be one in one billion (except in the case of identical twins). The result is related directly to the frequency of a particular allele in the population; therefore, if multiple alleles between two DNA profiles match, this increases the likelihood that they came from the same individual. Despite this, a number of factors can increase the likelihood of a false match occurring. For example, if the original sample contained only a small amount of DNA; if only a small number of loci are compared; if the DNA profile from the crime scene is incomplete or degraded in some way; or if either DNA profile was contaminated. Therefore, it should be noted that DNA profiling is not foolproof [18].

G. Dynamic Signature

The way in which an individual signs his/her name is considered to be characteristic of that person and as such could provide a feasible mode of biometric recognition. Dynamic signature recognition is an automated method of examining an individual's signature [18].

Signature verification consists primarily of a specialized pen (or stylus) and writing tablet, which are connected to a computer for processing and verification. To begin the data acquisition phase of enrollment, the individual must sign his/her name multiple times on the writing tablet [7].

After the data is acquired, the signature verification system extracts writer's behavioral characteristics, including how long it took the person to sign his/her name; the pressure applied; the speed in signing the signature; the overall size of the signature; and the quantity and various directions of the strokes in the signature, and uses this information in future comparison of the live signature to the enrollment template for the verification of enrollment claims [7].

Fig: Scan image of signature

H. Voice or Speaker Recognition

Speaker, or voice, recognition is a biometric modality that uses an individual's voice for recognition purposes. The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual [21].

Voice is often classified as a combination of a behavioural and a physiological biometric because certain features of an individual's voice are based on the shape and size of their vocal tracts, mouth, nasal cavities, lips, etc. From a biometrics perspective there are basically two different types of voice/speaker recognition system, i.e. text dependent and text independent systems. In a text dependent system the user speaks a particular, predetermined, pass phrase, for example, a sequence of numbers. When enrolling in such a system, the user may be required to repeat the pass phrase a number of times, to enable the algorithm to take account of any intra-class variation. Consequently, the enrolment process lasts longer, but this is thought to result in increased accuracy[18].

In a text independent system the user's voice is recognised regardless of what he/she is saying. Such systems are said to offer greater security against abuse than text dependent systems, but they are more difficult to design. In general, sound waves from the individual's voice recording are calculated as feature vectors, which are then modelled as a voiceprint (template) for that individual (see Figure 8). During the recognition process, the sequences of feature vectors from the sample and enrolled voiceprints are compared using pattern analysis, i.e. the system does not

compare the voice itself. If these patterns are sufficiently similar, a match is given [18].

I. Keystroke Dynamics

Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the Biometric Systems 32 typist. These systems should be cheap to install as all that is needed is a software package [21].

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometrics is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity authentication. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe a large variations from typical typing patterns. The keystrokes of a person using a system could be monitored unobtrusively as that person is keying in other information [22]. Keystroke dynamic features are based on time durations between the keystrokes. Some variants of identity authentication use features based on inter-key delays as well as dwell times - how long a person holds down a key. Typical matching approaches use a neural network architecture to associate identity with the keystroke dynamics features. Some commercial systems are already appearing in the market [23].

VI. CONCLUSION

Biometrics refers to an automatic method of recognizing a person based on a physiological or behavioral characteristic. This paper discussed the various types of biometrics authentication techniques. A number of civilian and commercial applications of biometrics based identification are emerging today i.e Colleges, Government offices and companies etc. Biometric techniques provide a strong user authentication with it`s different application areas but even if the accuracy of the biometric techniques is not perfect yet, for children. There is no any techniques available for children which takes it`s physiological or behavioral characteristic property. There is need to improve one of biometrics authentication technique for children to get his physiological and behavioral characteristics.

ACKNOWLEDGMENT

We would like to thank the Department of Computer Science , S.S.V.P.S.Dr.P.R.Ghogre Science College, Dhule.

REFERENCES

[1] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, "Guide to Biometrics", Spinger Professional Computing.
[2] John Vacca, "Biometic Technologies and Verification System", Elsevier
[3] Jain A, Hong L, & Pankanti, S, "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110, 2000.
[4] Jain Anil K, Ross Arun, "Introduction to Biometrics". In Jain A K, Flynn P, Ross A , "Handbook of Biometrics". Springer. pp. 1–22. ISBN 978-0-387-71040-2.
[5] "Biometrics for Secure Authentication" (PDF). Retrieved 2012-07-29.
[6] L. O'Gorman, "Seven Issues With Human Authentication Technologies", Proc. Of Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 185-186, Tarrytown, New York, March 2002.
[7] Biometric Technology Application Manual Volume One: Biometric Basics Compiled And Published by: National Biometric Security Project 2008.
[8] James L. Wayman in Biometrics-Now and Then: The Development of Biometrics Over the Last 40 Years. New York Times article: "Technology; Recognizing the Real You" Pollack. September 24, 1981.
[9] NSTC Subcommittee, "Iris Recognition", Aug. 2006, http://www.biometricscatalog.org/NSTCSubcommittee.
[10] Biometric Technology Application Manual Volume One: Biometric Basics Compiled And Published by: National Biometric Security Project 2008.
[11] Philippe C. Cattin, "Biometric Authentication System Using Human Gait" Swiss Federal Institute of Technology Zurich, 2002
[12] NSTC Subcommittee on Biometrics , 2006.
[13] E. Kukula, S. Elliott, "Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance", In Proc. of 35th Annual International Carnahan Conference on Security Technology, UK, Oct. 2001, pp. 83 – 88.
[14] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric", In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, Jun. 2003, pp. 668 - 678.
[15] Zunkel (1999) op. cit.
[16] Jain et al. (2004) op. cit.
[17] OECD, Working Party on Information Security and Privacy (2004) op. cit.
[18] Irish Council for Bioethics , Dublin ISBN 978-0-9563391-0-2 ,2009
[19] This image is taken from Ross A, Jain A and Pankanti S. A Hand Geometry-Based Verification System. Available online at: http://biometrics.cse.msu.edu/hand_proto.html, accessed 12 August 2008.
[20] Woodward et al. (2001) Op.Cit
[21] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, Minkyu Choi, "Biometrics Authentication : A Review", International Journal of u & e – Service Science & Technolo
[22] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
[23] Anil Jain, Ruud Bolle, Sharath Pankanti, "BIOMETRICS Personal Identification In Networked Society", Kluwer Academic Publishers, 2002

Rahul D Chaudhari is a lecturer in the Department Of Computer Science at S.S.V.P.S.Dr.P.R.Ghogrey Science College, Dhule which is affiliated to North Maharashtra University, Jalgaon. He received his M.Sc Computer Science from North Maharashtra University, Jalgaon. His research interests include Human Computer Interface, Brain Computer Interface, & Biometric Authentication.

Ashok A Pawar is a lecturer in the Department Of Computer Science at S.S.V.P.S.Dr.P.R.Ghogrey Science College, Dhule which is affiliated to North Maharashtra University, Jalgaon. He received his M.Sc Computer Science from North Maharashtra University, Jalgaon. His research interests include Speech Recognition, Pattern Recognition & Biometric Authentication.

Rakesh S Deore is a Head Of Department Of Computer Science at S.S.V.P.S.Dr.P.R.Ghogrey Science College, Dhule which is affiliated to North Maharashtra University, Jalgaon. He submitted his Ph.D thesis in Dr. Babasaheb Ambedkar Marthwada University, Aurangabad. He is also qualified NET & SET examination in the subject of Computer Science. His research interests include Human Computer Interface, Brain Computer Interface, Pattern Recognition & Image Processing.