International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2276-2297

A Comprehensive Survey on Various Biometric Systems

T.Sabhanayagam [1], Dr. V. Prasanna Venkatesan[2] and Dr. K. Senthamaraikannan[3]

[1] Research Scholar, Center for Computer and Information Technology Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India.
[1]And Assistant Professor, School of Computing, SRMIST, Chennai
[1]Orcid: 0000-0002-9782-7068

[2] Dr.V.Prasanna Venkatesan, Proof & Head, Dept. of Banking Technology, Pondicherry University, Puducherry, India.

[3] Dr. K.Senthamaraikannan, Prof & Head, Dept. of Statistics, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India.

Abstract

Biometrics gains significant importance in this technical world and it means analysis of biological data. It is defined as the technology of analyzing individual person based on physiological, behavioural or morphological traits such as face, fingerprint, iris, retina, voice, and signature etc,. It is possible to establish one's identity with the help of biometric techniques. Today biometric have been successfully deployed in various fields like forensic science, security, identification and authorization system. For the last three decades, lot of research work has to be carried out for the growth of biometric system based on fingerprint, voice, iris, face, etc, but recently new biometrics has been come up. To provide a comprehensive survey, this paper presents an overview to various biometric systems, their applications, limitations and the different type of biometrics recognition systems.

Keywords: Biometrics, physiological, behavioural, identification, techniques.

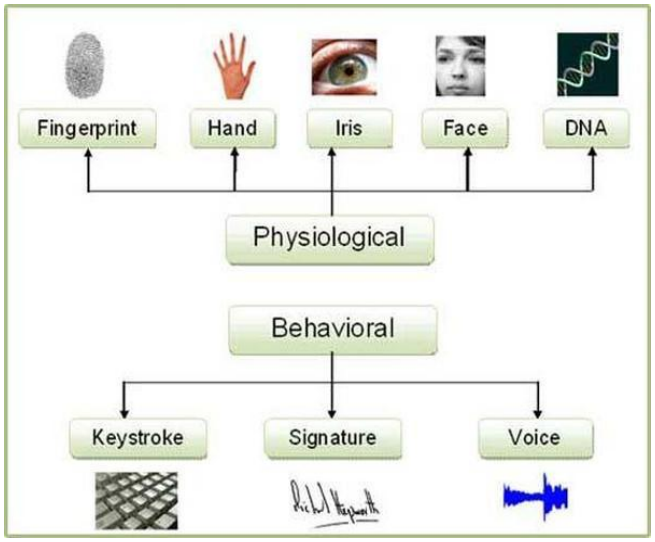

Figure 1: Categories of Biometrics

INTRODUCTION

Biometric is a methodological study of measuring and analyzing biological data for the purpose of authentication or identification. Biometrics refers to certain physiological or behavioral characteristic that is uniquely associated to a person. In fact, biometric technology is ancient Egyptian times technology. The Biometrics can be defined as the study of measuring and analyzing the unique physical or behavioral traits, which is used for the purpose of recognizing a person. The word " ***biometric"*** is originated from the Greek words '**bios**' (life) and '**metric** 'or ***'metrikos'*** *(*measure) , directly translates into "**life measurement"**. Physical characteristics include – Face Fingerprint, DNA, Ear, Iris, Retina and Hand geometry and they are associated with the shape or measurements of the human body. Behavioral characteristics include – Signature, Voice and Gait and they are associated with the behavior or dynamic measurements of an individual [1][2][3] . Each biometric trait has its own merits and demerits. Depend on the application requirement, appropriate biometric trait should be used for a given authentication application. The Figure 1 shows the categories of biometrics.

The emerging technology applications use the physical characteristics to recognize the humans. Nowadays, variety of applications depends on the verification or identification purpose to confirm the individual's identity. Traditional passwords, PINs and ID cards have been used for personal identification [2][3] to secure the systems by restricting the access, but these can be easily breached. The passwords cannot be remembered and ID can be pirated. Whereas the biometrics cannot be stolen, forgotten, borrowed or forged. Also biometric features can be used with additional security [4]. The biometric systems have various benefits by comparing traditional authentication systems. Walls, huge forts and people are used as authentication techniques for ensuring security and privacy. The authentication technique is based on by Knowledge, by Possession and by Property and its goal to protect a system against the unauthorized use. Authenticated users are allowed to access the information to ensure the protection of information and it is required that the individual being recognized should be present at the time of authentication [5].The conventional authentication technique depends on something you have and something you know whereas biometric authentication is something you are. Thus authentication process based on biometrics is the most secure system.

OBJECTIVE AND SCOPE

Biometrics provide better security and more suitable than traditional approaches of human recognition. In few applications, biometrics can supplement or replace the current technology. The aim of this paper is to contribute a comprehensive survey and difference between the existing biometrics techniques and new biometric techniques.

BIOMETRICS – BRIEF HISTORY

The study of human metrics, called Biometrics, has a long history that goes back to prehistoric times. Biometrics is an ancient idea and techniques of recognizing people with their physical or behavioral characteristics have existed for centuries. Facial recognition is an example for one of the ancient and basic biometrics since the faces have been used to distinguish between known and unknown people from the beginning of civilization. Have a look at some of the most essential historical moments in the development of biometrics from the Table 1.

Table 1: Time Line of Biometrics

Time line	Description	Time line	Description
1858	Sir William Herschel, Civil Service of India developed First standardized Hand images System	**1996**	Beginning of Annual speaker recognition evaluations hosted by NIST.
1870	"Bertillonage" or anthropometries developed by Alphonse Bertillon to identify individuals based on body measurements, physical descriptions and photographs.	**1997**	NSA published First commercial, generic biometric interoperability standard.
1892	A classification system for fingerprints using minutiae, developed by Sir Francis Galton to identify individuals and it is still used today**.**	**1998**	CODlS (Combined DNA Index System) to digitally store, search and retrieve DNA forensic database, is launched by FBI.
1894	The use of fingerprints for identification published by The Tragedy of Pudd'nhead Wilson	**1999**	Comparative study of biometrics and machine readable travel documents is launched.
1896	A fingerprint classification system developed by Sir Edward Henry, Inspector General of the Bengal Police. It is used by FBI many years.	**1999**	FBI's IAFIS major components became operational.
1903	Fingerprints for identification of Criminals used by New York State Prison system	**2000**	First Face Recognition Vendor Test (FRVT 2000) is held
1903	Due to inadequate measurements between two individuals, Bertillon System collapsed.	**2000**	First research paper on vascular patterns for recognition is published
1907	Palm System developed by Hungarian used in criminal case	**2000**	Biometrics Degree program established by West Virginia University (WVU) and FBI.
1921	Fingerprint analysis department founded by FBI	**2001**	At the Super Bowl in Tampa, Florida, Face recognition system is used.
1936	Ophthalmologist Frank Burch proposed Iris Pattern for Identification purpose.	**2002**	The International Organization for Standardization (ISO)/IEC standards committee on biometrics is established.
1960	First semi-automated Face recognition created by Woodrow W. Bledsoe	**2002**	Formation of M1 Technical Committee on Biometrics.
1960	A Swedish Professor, Gunnar Fant created First model of acoustic speech production.	**2002**	A paper on IAFIS (Integrated Automated Fingerprint Identification System) and Palm print technology is submitted to Identification Services Committee.
1960	FBI uses the first AFIS system developed by NIST.	**2003**	Formal US Government coordination of biometric activities begins.

1963	Hughes published a research paper on fingerprint automation.	**2003**	A blueprint to integrate biometrics into machine readable travel documents is adopted by the ICAO (International Civil Aviation Organization).
1965	North America Aviation begins first Automated Signature recognition research.	**2003**	European Biometrics Forum established
1969	An automated process of fingerprint recognition is attempted by FBI with NIST	**2004**	The United States Visitor and Immigrant Status Indication Technology (US-VISIT) program becomes operational
1970	Goldstein, Harmon and Lesk made Face Recognition for further automation	**2004**	The Department of Defense (DOD), US government implemented the ABIS (Automated Biometric Identification System) to track and identify national security threats.
1970	Dr. Joseph Perkell modelled first Behavioral components of speech	**2004**	For all federal employees and contractors, mandatory government-wide personal identification card (HSPD-12 , Homeland Security Presidential Directive 12) issued by President Bush
1974	First commercial hand geometry systems become available	**2004**	First state wide automated palm print databases are deployed in the US by Connecticut, Rhode Island and California
1975	First Automated Fingerprint using sensors and minutiae extracting technology developed by NIST in collaboration with FBI.	**2004**	Face Recognition Grand Challenge (FRGC) begins to develop algorithms to improve specific identified areas of interest in face recognition.
1976	Texas Instruments developed First prototype system for speaker recognition and tested by US Air Force and The MITRE corporation.	**2005**	US Patent concept for iris recognition expires. But the patent for Dr. Daugman on the lrisCodes® implementation of iris recognition will expire only in 2011.
1977	Veripen,Inc given patent rights for the acquisition of dynamic signature information.	**2005**	At Biometrics Consortium Conference, the prototype system for Iris on the Move sponsored by the ITIC (Intelligence Technology Innovation Center) is announced.
1980	To promote and study the use of speech processing techniques**,** NIST Speech Group is established.	**2006**	USA and EU issues biometric passports
1985	Ophthalmologists, Dr. Leonard Flom and Dr.Aran Safir, proposed that no two irides are similar.	**2008**	The FBI and Department of Defense started working on biometric databases to include iris, face, palm data and fingerprint records.
1985	David Sidlauskas is awarded patent for Hand identification system.	**2008**	Hungarian NPP deploys Hand Geometry Identification
1986	NIST with ANSI published Exchange of fingerprint minutiae data standard (first version of the existing fingerprint interchange standards)	**2009**	Hungary issues biometric passports
1986	Patent is awarded stating that the iris can be used for identification for Drs. Leonard Flom and Aran Safir	**2009**	Hitachi develops finger vein scanner
1987	Face recognition using Eigenfaces technique developed by Kirby and Sirovich.	**2010**	U.S. national security apparatus utilizes biometrics for terrorist identification
1988	Deployment of First semi-automated facial recognition system.	**2011**	Biometric identification used to identify body of Osama bin Laden using DNA with facial technology.
1991	Turk and Pentland pioneered Face detection for real time face recognition.	**2011**	India deploys mass Iris Recognition System

1992	The National Security Agency within US Government established Biometric Consortium.	**2013**	Apple Inc., designed and released fingerprint feature called Touch ID made available in all the version of iPhones and iPads.
1993	The Defense Advanced Research Products Agency (DARPA) initiated FERET (FacE REcognition Technology) program.	**2014**	Hungarian Stadium displays vein scanner
1994	Dr. John Daugman is patented for his First iris recognition algorithm.	**2016**	Hungary deploy biometric personal ID cards
1994	IAFIS (Integrated Automated Fingerprint Identification System) competition is held.	**2016**	Windows Hello is available. It is more personal way to sign in to Windows 10 devices with just a look (face) or a touch (fingerprint) which is enterprise-grade security without having to type in a password.
1994	Hungarian company is benchmarked for Palm System.	**2017**	**Wearable Biometrics -** Israeli researchers have developed a way to authenticate handwritten signatures with wearable technology like smartwatches and fitness trackers
1994	The INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System) implemented biometrics.	**2017**	S**wiss startup Bio watch, SA** has developed and tested the world's first fully functioning prototype for a wearable device secured by wrist vein patterns that can be used for payments, access control, ticketing, ID management, environment personalization, and more.
1995	Iris prototype becomes available as a commercial product.	**2017**	**Internet of Things (IoT**) - another emerging area of technology that offers great potential for biometrics which covers a vast array of "things" and biometrics could support identity in a number of areas, including in the home, the workplace, and for automobiles.
1996	Hand geometry is implemented at Atlanta Olympic Games.	**2017**	Smart speaker devices like Amazon Echo, using the Alexa voice recognition platform, and Google Home, provide an opportunity to link speech recognition, control, and voice biometrics.
		2017	The Jaguar, Land Rover patenting a biometric system to allow car owners to open the door based on a combination of facial and gait recognition, and other auto manufacturers testing various models where sensors are integrated into door handles, key fobs, touchscreens, and steering wheels.

According to a number of recent research reports, the Biometric Security is on the rise. Many mobile users are being comfortable with fingerprint identification for access as its simple and unique to each person. In 2020, there will be a rising demand for Smartphones, tablets and wearable mobile devices to add in biometrics.

BIOMETRICS SYSTEM - GENERIC

The general biometric system constitutes of four modules viz., Sensor, Feature Extraction, Matcher and Decision Making and comprises of five integrated components as shown in Figure 2(a). The capturing and storage of enrollment (reference) biometric features and the captured new biometric samples with comparison of corresponding enrolled features are the operations performed by a general biometric system. The efficiency of a biometric system depends on the reliability of the sensor used and the features extracted from the sensed signal [6]. The learning phase and the recognition phase are the two phases of biometric system.

(i) Sensor module/ Image acquisition: to capture the individual's raw biometric data in the form of video, audio and an image or some other signal.

(ii) Feature extraction Module: automated process of extracting distinctive biometric features to generate Template and can be done using Machine learning, Computer Vision and Pattern Recognition techniques.

(iii) Database module: a respiratory of registered /enrolled biometric information of users and stores various templates of user.

(iv) Matching module: compares the currently extracted features against the stored templates to generate match

value or match score, which is computed one to find the similarity between two biometric samples.

(v) Decision-making module: gives the decision as accepted or rejected by comparing the matching scores with given threshold value.

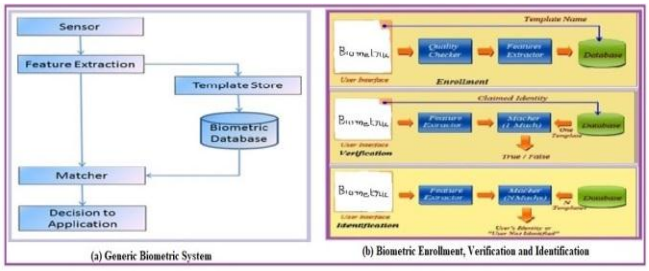

Figure 2: (a) Generic Biometric Systems

(b) Enrollment, Verification and Identification

A biometric system may be either an Identification system or a Verification or Authentication system. Verification refers to one-to-one process. It is also known as authentication, used to compare against the user claiming his/her genuine identity to verify his/her claimed identity. That is used to verify a person's identity. The output is binary, either accept or reject, based on matching procedure. Identification refers to one-to-many process. It is used to compare against each enrolled biometric template from the database to search for the identity of the highest similarity template. That is used to determine a person's identity.

There is a significant different from Verification and Identification. **Identification** is the mechanism of comparing presented biometric of an individual to all the other's biometric pattern already available in the database and it is one to many matches [1: M]. **Verification** is a process of validating an identity of presented biometric of an individual with the comparison of extracted biometric data and the captured biometric data in the system and it is a one to one match [1:1].

Enrollment and Authentication are the two operational modes in the biometric recognition process. The enrollment is the process of extracting and storing unique feature of individual. The authentication process is the matching of extracted features with the stored template in database. The figure 2(b) illustrates the generic process of these steps. The table 3 summarizes the benefits of the biometrics and table 2 lists the advantages and disadvantages of biometrics.

Table 2: Advantages and Disadvantages of Biometrics

Advantages	Disadvantages
Improved Security	Environment and usage can affect measurements
Improved Customer Experience	Systems are not 100% accurate
Can't be forgotten or lost	Require integration and/or additional hardware
Reduced operational costs	Can't be reset once compromised.

Table 3: Benefits of Biometric Technology

Cooperation Not Required	Requires no user cooperation for recognition
Guarantees Physical Location	Ensures the presence of the subject at the time of authentication.
High-Throughput	High throughput even during false identification or some fraud
Unforgettable	Can't be forgettable easily since it uses physical or character
Unlosable	Can't be lost or stolen
Unsharable	Cannot be shared with anyone.
Cost Reduction	Proper implementation can achieve cost reduction.
Compliance	Enhanced access control by authentication because of its user's physical and behavioral characteristics.
Emergency Identification	Very careful and quick identification can be done through biometrics traits enrolled in the biometric system
No Identity Theft	Use of biometric authentication reduces identity theft

Biometric technology is used for variety of applications and can be divided into main three groups- **Commercial, Government and**

Forensic applications. The biometrics is deployed in many areas shown in the following table 4.

Table 4: Applications of Biometrics

Commercial Applications	Access Control (Logical Access and Physical Access)
	Time and Attendance Management
	Financial Services and Banks
Government Applications	Border Control / Airports
	Security and Immigration checks
	Communication Systems
	Healthcare and Social Services
Forensic Applications	Justice / Law Enforcement
	Surveillance

CHARACTERISTICS OF BIOMETRICS SYSTEM

Each biometric has its own demerits and demerits. It is very difficult to make a direct comparison. For that there are some significant factors such as universality, uniqueness

(distinctiveness), permanence, collectability, performance, acceptability and resistance to circumvention [4][7][8] identified by the Researchers which are defined as the essential characteristic requirements of any biometric traits listed in the table. Sometimes these characteristics are known as the **seven pillars of biometrics** [2]. The table 5 gives the insight into these characteristics of various biometric techniques.

Table 5: Characteristics of Biometrics

Universality	Each individual should have the biometric characteristic
Uniqueness	Each person should have the feature but distinct from others.
Permanence	The biometric trait should be constant for certain period of time
Collectability	Ease of data capturing, measuring and processing
Performance	Security, speed, accuracy and robust.
Acceptability	Accepted by the user population without any objection
Circumvention	Ease of use of a substitute i.e.., act of cheating

BIOMETRIC TECHNIQUES

Biometric is powerful, distinguishable, measurable, physical or behavioural trait of an individual used to determine the identity of that individual. Any biometric trait can be easily convertible, subject to fewer changes over the time and should be unique. For example voice is biometric trait which varies from person to person. Similarly, iris never changes throughout one's lifetime. The biometric systems are based on Pattern Recognition Systems [2].Cognitive biometric is recent technology depends on the response from the brain with a particular stimulus and it is a user authentication or identification uses the bio-signals. The different biometrics techniques are discussed here. The merits and demerits associated with each technique are listed in the Table 6 along with their applications and appropriate technique can be selected based on the application requirement.

Table 6: Advantages, Disadvantages and Applications of Biometrics techniques

Modalities	Advantages	Disadvantages	Applications
Fingerprint	• Most contemporary Technology. • Relatively inexpensive • More secure and highly reliable. • Template size is small and so matching is fast • Consumes less memory space. • Most widely used technology • High accuracy • Ability to enroll multiple fingers • Wide range of deployment environments • Not intrusive and do not change naturally	• Cuts, scars or absence of finger can produce obstacle for the recognition process. • Easily deceived through artificial finger made of wax. • Has physical contact with the system. • Requires large amount of computational resources • Worn out or may be altered over time • Exposed to noise and distortion due to dirt and twists • Some people have damaged or eliminated fingerprints	• Authentication of Driver License • Border Control/Visa Issuance. • Access control in organizations. • Law Enforcement Forensics
Face	• Totally non-intrusive i.e., involves no physical contact • Storing of templates in database is easy. • Socially accepted • Reduced statistic complexities for recognizing face image. • Similar to human process of authentication • Convenience and Matured technology • The existing image capturing devices i.e. cameras can be used. • Faster in identification process	• Facial traits change/ vary over time. • In case of Twins distinctiveness is not guaranteed. • Can affect the recognition accuracy – varying expressions • Highly dependent on lighting for correct input • Most people are uncomfortable because of privacy abuse • More suitable for authentication • 2D contains limited information • Unstable to illumination, orientation and facial expressions • Will not work when using a mask or other face-covering veils	• Identity Verification. • Access Control Verification. • Human Computer Interaction. • Criminal Identification. • Surveillance

Retina	• Cannot be forged • Highly reliable since no two people have the same retinal pattern • Rate of error is 1 out of 10,000,000 (virtually 0%) • Highly accurate technology • Provides most security in authentication • Low occurrence of false positives • Very quick Verification.	• Not very user friendly • Diseases such as cataracts, glaucoma, diabetes etc., affect the accuracy of the results. • Medical conditions such as hypertension causes privacy issues • Intrusive to Individuals and Enrolment and scanning are slow. • Limited usage • Expensive technology i.e. high equipment cost • Subject should be very close to the camera	• Security (FBI, CIA, and NASA) • Ophthalmological diagnostics
Iris	• Highly accurate (Iris pattern matches 1 in 10 billion people) • Highly scalable • Accuracy is not affected by wearing of glasses or contact lenses. • No physical contact with the system. • Small template size so Promising processing speed (2 to 5 seconds) • Minimal false acceptance rate • Remains stable throughout the life • Highly protected and has high degree of randomness. • Encoding and decision-making are tractable	• Relatively costlier • The scanner can be deceived by High quality images. • Needs user's cooperation for accurate scanning. • Less convenience in usage since the user must hold still while the scanning is taking place. • Less competition in market • Obscured by eyelashes, lenses, reflections • Illumination should not be visible or bright • Challenging at a larger distance long distance • Vulnerable to inadequate image quality • Diabetes or some other serious disease cause alterations in iris.	• Identification (**Adhaar card** in India) • Access Control (Google uses for their data centers) • National security (land, air and sea ports of entry of UAE).
Hand Geometry	• User friendly and durable. • The result is not affected by skin moisture or texture changes. • It is easy to use and small template size • Non- intrusive • Can operate in challenging and rough environments • Established and reliable technology • Has low failure to enroll (FTE) rate	• Not unique and not accurate. • Only for adults it is efficient. • Not yet developed and results are not accuracy • FAR (false acceptance rate) and FRR (false rejection rate) are relatively high • Wearing of Jewel may cause obstacle while scanning • Fairly Expensive • Injuries to hands may prevent the system from working properly	• Nuclear power plants • Military access control
DNA	• Provides the highest accuracy. • The chance of 2 individuals sharing the same DNA profile is less than one in a hundred billion..	• Acquisition of Sample is long procedure to get desired result. • Though it gives more information, privacy issues are there. • More storage space is needed • The result is affected by the Sampling contamination or degradation of sample. • High Cost and Poor convenience. • The processing time is very long • No real-time matching	• Proving guilt or innocence. • Physical and network security.

		• Intrusive - a physical sample must be taken	
Ear	• Fixed shape and appearance • Most stable and less computational complexity • Faster identification • Reduced processing time	• Error in recognition as the images are not ideal • Unclear recognition due to the effect of hair, hats, and earrings. • Not believed to be very distinctive	• Law Enforcement Forensics • Surveillance.
Body Odour	• Identification is possible by mixture of odors by recognizing the mixture's components.	• Still there are no existing applications. • Artificial noses are not comfortable to do all the job • Senses of quantification are difficulty. • Distinctiveness is reduced by Deodorants and perfumes.	• Law Enforcement Forensics • Surveillance.
Palm Print	• More distinctive features can be captured compared to fingerprints • More suitable in identification systems than fingerprints. • More reliable and permanent in nature • Good recognition with low resolution cameras and scanners	• Scanners are bulkier and expensive • Problem in recognition for low quality images • Variations in illumination and distortions in an uncontrolled environment	• Personal Identification • Medical Diagnosis • Blood relation Identification • Selection of athletes
Lip Motion	• Distinctive and unchangeable attributes for every examined person. • Used by forensics professionals and criminal police training. • Template Size is small and depends on static mouth/face photos. • Interaction of user is not necessary and can be used without the knowledge of user. • Visible and not hidden/overcast by anything. • Can be hybrid - lips-voice or lips-face biometric systems	• Needs more attention for hybrid system • The relevant information may not be acquired from the specific facial attributes. • Variations (smile) may cause difficulty in recognition	• Financial Transaction Authentication • Transactions at ATM machines • Credit Card user passwords • Access Control
Hand Vein	• Contactless and hygienic • Non-invasive • Highly Accurate • Difficult to forge • Non-intrusive • Distinctive and unique	• Unfamiliar • Relatively expensive • Quality of image is affected by numerous factors such as body temperature and heat	• Driver Identification system • Door Security system • Login Authentication • Financial and Bank Services • Physical access control and time attendance • Travel and Transportation • Hospitals, Schools ,Construction sites
Gait	• It is non-invasive. • Easily acquired from distance • Used for finding medical disorders (marking walking pattern changes - Parkinson's disease) • Convenience in usage.	• Lack of complete accuracy • Not a reliable technique • Not invariant with time • Computationally expensive since it requires more computations	• Forensics. • Medical diagnostics • Chiropractic and Osteopathic Utilizations • Comparative biomechanics
	• Signature cannot be imitated. • Low False Acceptance Rate (FAR)	• There will be a possibility of change in the live sample template when there is a change in behavior while signing. • Signatures can be forged by the	• Verification and authorization of documents • Banking Systems (The Chase Manhattan Bank, Chicago,

Signature	• Has wide acceptance in public • Non-invasive in nature • Has reasonable accuracy rate • For huge amount of business transactions, it is good. • Has no privacy rights issues. • Easy to restore the template if it is stolen.	Professionals to deceive the system • User must familiar with the usage of signing tablet. • Same individual can have inconsistent signature • Signature of individual changes over time • Has very limited market	the First bank using Signature System)
Keystroke	• Needs no special hardware or new sensors and low cost • Identification is fast and secured. • A person typing does not have to worry about being watched. • No training is required for enrolling or registering their live samples	• Diseases, gap in days, change of keyboard etc., can change the typing rhythm • Not a mature technology • No discriminating information. • Less convenience in use	• Authentication system. • Multifactor authentication System • Surveillance System.
Voice	• Easy to implement. • No need for some extra new devices • Low cost • Usage is convenient • Low invasiveness	• Susceptible to quality of microphone and noise. • Serious illness or some problems in throat can affect the accuracy. • Can be easily spoofed • High rate of false non match • Significant decrease in performance due to the factors affecting the input system	• Web based Transactions • Interactive Voice Response based banking and health systems. • Audio signatures for digital documents. • Entertainment and emergency services. • Online education systems
Thermo gram	• Non- intrusive • No physical contact is required • Easy Enrollment • Works accurately even in dim light or total darkness • Invariant to Illumination	• More Expensive • Needs Specialized Sensor camera	• Condition Monitoring • Low Slope and Flat Roofing Sequences • Thermal Mapping • Medical and Chemical Imaging • Digital Infrared Thermal Imaging in health care • Neuromuscuo skeletal disorders • Surveillance in Security, Law enforcement and defence

1) **Fingerprint Biometrics**

The fingerprint recognition is the oldest and the most well–known biometric authentication approach. It is digitized, automated version of the ancient ink-and-paper system used for identification by law enforcement agencies. It is based on the recognition of individual's fingerprint, by analyzing its characteristics. Fingerprints are distinguishable and immovable for every individual and their basic properties never change with time. Even the fingerprints of identical twins are distinct. Also, the fingerprints on both the fingers of the same individual are different. A fingerprint is made up of ridges and furrows. The patterns of ridges, furrows and the minutiae points on the finger are used to determine the uniqueness of a fingerprint. The loops, whorls and arches (Figure 3) are the three basis categories of ridge patterns [9][10][11].The pattern comparison of ridges, furrows and minutiae points are involved in the fingerprint biometrics.

The two fundamental principles **immutability** (ridge patterns never change during the life time) **and uniqueness** (distinct ridge patterns on different fingers of the same individual) are used in identification of individual's fingerprint. The finger print biometrics has its own strength and limitations listed in the Table 7. The techniques for fingerprint matching are classified into three types.

i. **Minutiae-based approach:** It is the identification of minutiae points along with their relative position on finger.
ii. **Correlation-based approach:** It is based on abundant gray scale information. It can work with bad quality data.
iii. **Pattern based / Image based matching:** It compares the basic fingerprint patterns between claimant and a stored fingerprint templates.

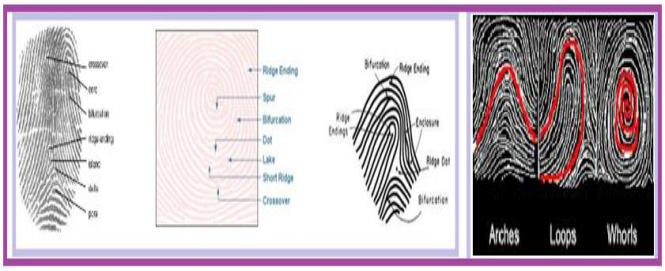

Figure 3: Finger print Impression with its parts and Arches, Loops and Whorls

Table 7: Categories of Minutiae

Categories of Minutiae	Description
ridge ending	Abrupt ending of a ridge
Bifurcation	Division of single ridge into two ridges
lake or enclosure	A single ridge bifurcates and rejoins shortly and continues as a single ridge
short ridge, island or independent ridge	A ridge begins and ends after travelling a short distance.
Dot	An independent ridge having same length and width
Spur	A short ridge with bifurcation extended as long ridge
crossover or bridge	A connecting ridge between two parallel running ridges.

2) Face Recognition

Face recognition is an emerging subject which gets dynamic and constant improvement. Face Recognition has attracted the Researchers in the field of Security, Psychology, Optics, Neural Networks, Machine learning, Image Processing, Computer Vision and Pattern Recognition. It has expanded not by Engineers but also by Neuroscientists and the most important application is Image Analysis and Understanding.

Face recognition is a non-intrusive and popular method. The dimensions, ratio and other physiological attributes of the face form the basis for the Face recognition. Based on the size, location and the shape of the facial traits such as nose, lips, eyes, chin, jaw and their spatial relationships (Figure 4), the humans recognize and distinguish faces.

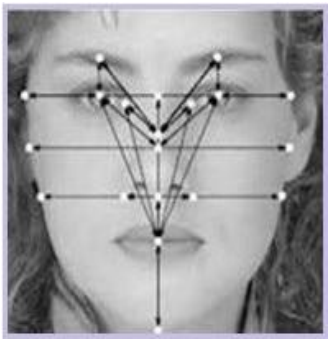

Figure 4: Attributes / Features of the Face Images

Researchers use both specific and general features for facial recognition. Face recognition can be carried out in the following ways [12][13].

i. **Facial metric:** The location and shape of facial attributes are measured. For example, distance between nose to lip or pupil to chin
ii. **Eigen faces:** The overall face image is analyzed i.e., collection of weights describing the canonical faces.
iii. **Skin texture analysis:** This is an emerging technique of face recognition along with other visual details of skin. Finding the location of the unique spots, lines and patterns in a person's skin.

Generally, the face recognition procedure is separated into three steps – **Face Detection, Feature Extraction and Face Recognition.** The face recognition system receives the input as an image or video stream and gives the output as an identification or verification of the subject which occurs in the image or video. The Face Detection and Feature Extraction phases would run concurrently. The figure 5(a) shows the general configuration of the face recognition.

The first step is the face detection to identify and locate a face in an image. The feature extraction is the next step to extract the features of the face, called feature vector and plays important role in the recognition of facial expressions which verifies the uniqueness of the face and discriminating property between two individuals. The third and final step is the face recognition which involves two tasks, namely, **authentication or verification** and **identification**. Authentication or verification involves the process of comparing the face image with the face image template and to true or false for the given identity. Identification is the process of comparing the face image with several other face images in the database to find the identity of the face with several possibilities and gives the most probable identification. The figure 5(b) shows the work flow of these steps on an input image.

There are three basic approaches in face recognition [14]. **Feature-based Approach** uses the local features of the face like eyes, mouth, nose, etc., is used for the segmentation of the face and used as input data for face detection. **Holistic Approach** uses the entire face as an input in face detection and used as the input in face recognition. **Hybrid Approach** uses the combination of feature-based and the holistic approaches. Another popular approach called **Template-based approach,** used to recognize and detect faces by

computing the correlation of an input image to a standard face pattern by using the entire facial features.

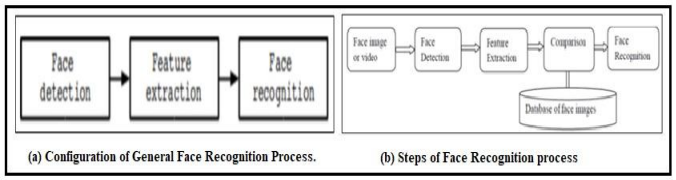

Figure 5: (a) General Face Recognition Process **(b)** Steps of Face Recognition process

3) Retina Biometrics

The Retinal scan biometric is based on the distinctive patterns on a person's retina, which is significantly different from the iris recognition. It is older than the Iris scanning which also uses the part of the eye. There is a unique pattern called the blood vessels at the rear side of the eye, which covers the 65% of the inner surface of the eyeball. The retina is a thin tissue which is made up of neural cells and situated as the innermost layer of the eye.

Even identical twins have distinct patterns of retina and it is stable throughout the life. It is impossible to fake the retina and it decays so quickly after the death and can be accessed only from a living person. The retina templates are typically 40 to 96 bytes. It has an error rate of 1 in 10,000,000 [15]. The Enrollment and scanning of retina are intrusive and slow. Retina biometrics is used in Government, military and banking.

The digitized retinal patterns are captured by mapping a low-intensity ray of visible or infrared light into the retina to illuminate the blood vessels since the retina is not directly visible and on the retina, path of the light is traced. The variations of retinal patterns are transformed into digital code and stored in database. The person undergoing retinal scan has to focus on a specified location for 15 seconds approximately and keep their eyes close to the scanner and remain still. The blood vessels are read by the coupler. The retina scan requires the user cooperation so that it is not acceptable in many applications and even though it has been used in prisons, military bases, nuclear reactors and other highly secured locations and also in medical applications. It is still in a prototype development stage and unavailable commercially. The image acquisition of retina image is difficult and it requires specific hardware and software.

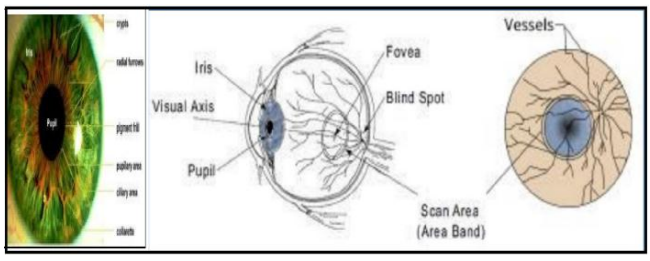

Figure 6: Retina scan biometrics

4) Iris Biometrics

The Iris is the elastic, thin, pigmented, circular connective tissue in the eye which controls the size and the diameter of the pupil and limits the amount of light entering the eye. It is grown-up at the initial stages of a life called morphogenesis. It is constant throughout the life. The iris is distinct for everyone and even the identical twins have the different iris patterns [16]. Also the left and the right irises of the same individual is treated to be different not the same. The iris is protected by the cornea and it is visible from the outside. The color of the iris can be blue, brown or green which becomes the "color of the eye". In some cases the color may be the combination of light brown, green and gold. The iris may be a unification of specific features such as freckles, crypts, filaments, corona, striations pits, rings and furrows [17]. The characteristics of the iris cannot be changed by the eye surgery or the wearing of glasses and contact lenses. The following figure shows sample eye image and the iris in Figure 7.

Figure 7: Iris Biometrics

Iris recognition is one of the best protected approaches for authentication and recognition. The accuracy of Iris recognition is most promising. The false acceptance rate as well as rejection rate is very low. A special gray scale camera is used to take iris pattern at the range of 10- 40 cm from camera. The appropriate methodology is used to determine the iris in the image and if it exists, then a net of curves covering the iris is created and also the iris code is created based on the darkness of the points. It is influenced by two things – firstly, the overall darkness of the image and secondly, the changes in the size of the iris.

The comparison of two iris code can be computed by the hamming distance based on the difference in the number of bits and it is very fast. Also the template matching technique can be used and it uses the statistical calculation to match the stored iris template and the obtained iris template [18][19]. The iris recognition is applied in the following areas: border control, passports and Identity cards and other government purposes, database access, login authentication, aviation security, hospital security, controlling access to restricted buildings, areas, homes and prison security.

5) Hand Geometry Biometrics

In the field of biometrics, the Researchers found that human hand, particularly human palm, has some features that may be used for personal authentication. These features include the density of the palm, width and length of the fingers, etc. and these measurements are not unique. The shape of the hand becomes stable in the later stage of life. Only the features of hand are not sufficient for authentication. However, they are

accurate for identification purposes when the measurements of fingers and hand are combined with various individual features. The shape of the hand may be changed due to illness, age or change in weight and it is time sensitive. The fact is that every individual has different hand shape which will not rapidly change in the future.

Hand Geometry biometrics is an older than palm print, established from early 70's. It is widely accepted technology and follows simple processing techniques. The hand geometry forms a base for research and development of new acquisition, pre-processing and verification techniques. The following figure 8 shows the various measurements of hand geometry.

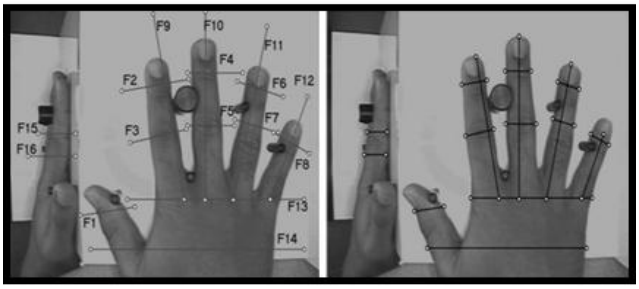

Figure 8: Hand Geometry

Contact Based and Contact Less are the two types of Hand Geometry systems. In Contact Based, hand of claimant is placed and positioned on the surface of a scanner with the help of five pins for proper position of hand for the camera. In Contact Less, the hand image is acquired directly. The optical scanners are of two types. The black and white bit map image of hand's shape is created in the first category with the help of black and white camera and light. The bitmap image consists of only 2D characteristics of hand, which is processed by the computer software. The other category which uses two sensors for the hand shape measurements, for both vertical and horizontal and it uses all the 3D features of the hand. Only the video signal of the hand shape is produced by some of the scanners. The digitalized processing of these image signals is done in the computer to get desired image of the hand [20][21].

An optical camera can also be used to acquire two orthogonal 2D images of the palm and the sides of the hand. Typically the hand geometry collect up to 90 dimensional measurements, which includes height, length and width of the finger, distance between joints and shapes of the knuckle. Hand geometry systems based on geometry of the hand only and not on fingerprints. Even dirty hands can be read by the reader. After reading, the hand template is developed with hand geometric characteristics and it is stored for the comparing the individual hand readings. The user places the hand on the scanner, it usually takes 3D image of the hand – the shape and length of the fingers and wrists are measured. The device compares it with already stored patterns in the database and for the entire procedure this process takes only few seconds. Today, in the offices, factories and other business organization environments, hand scanners are well accepted.

6) DNA Biometrics

The biometrics such as face recognition, fingerprint, iris scanning, retinal scanning, voice dynamics and handwritten recognition become popular and got rapid progress. These techniques have been incorporated into the system and these are based on the similarity of feature-points measurement, which gives inaccuracy results for a universal identification system. **DNA (Deoxyribonucleic acid**) becomes the best identifier. It is a genetic material presents in each living organisms and present in the cell's nucleus. The DNA of each individual human being consists of hereditary traits. It is intrinsically, digital and remains same throughout the each individual's lifetime and even after the individual's death. DNA is genetic code, which is unique to every individual and only identical twins have same DNA.

Approximately, 60 trillion cells are present in the human body. DNA is the blueprint for the human body design. It is a polymer which consists of nucleotide units each having three parts – a base, a sugar and a phosphate. Adenine (A), Guanine (G), Cytosine (C) and Thymine (T) are the four bases which combine to form base pairs and which determines the individual's anatomy and physiology as in figure 8. The backbone structure of the DNA molecule is formed by the portions of the sugar and phosphate to create nucleotide. In the cell, the DNA presents in the form of double-stranded that is double helix formed from two complementary strands spiral around each other i.e., long double helix structure called chromosomes.

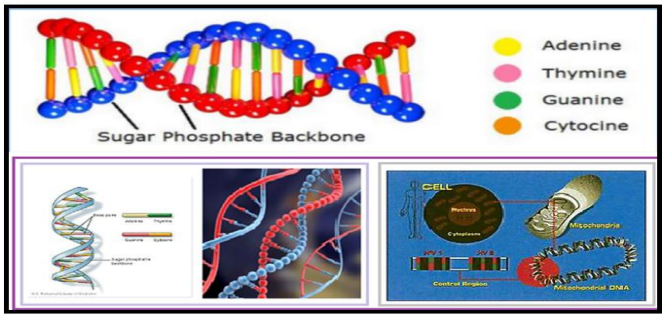

Figure 9: DNA Biometrics

In human cells, DNA is splitted into chromosomes to share the genetic material and humans have 23 pairs of chromosomes in their DNA and their genes,in total of 46 chromosomes. The 99.7% of the DNA of the parent is shared with offspring.The remaining 0.3 % is unique to the individual's DNA, which is variable and contains repetitive coding , which forms the basis for DNA biometrics.

DNA recognition generally is used for identification rather than verification [78]. The mechanism of creating a DNA profile is called DNA sequencing / genetic profiling. The similarity between these DNA profiles is matched with to already captured and stored DNA samples in database. The DNA samples having more details are more precise enough for identifying the individual while comparing. The CODIS System is the most common existing DNA database, used by the Federal Bureau of Investigation. Since the DNA biometrics is in developing stage, it is not used universally [23][24]. The basic steps of DNA profiling are:

1. Isolation/separation of the DNA samples from blood, saliva, hair, semen, or tissue.
2. Separation of the DNA sample into smaller segments/fragments (identically repeated sequences of DNA)
3. Organization of the segments/ fragments of DNA by size
4. Comparison of the segments/ fragments of DNA from different samples.

Currently, DNA Biometrics is used to identify the criminals in Forensic Applications [24]. DNA has information about the race, paternity and medical conditions. It is intrusive since it requires sample from body. Still, analyses of DNA have not been automated sufficiently to become popular biometric technology. The DNA analysis of human is feasible in 10 minutes. Since 1985, the DNA evidence has been used in courts of law to innocence or guilt. It is used in identification of missing or dead people and also for verifying paternity. The DNA Biometrics differs from all other biometrics since

- A concrete/real physical sample is needed or not the image.
- In DNA, only physical samples are matched. Feature extraction or Template storing is needed.

The future of DNA depends on the technological development and advancement in the field of DNA sequencing and sample comparisons. A work is started on creating a new device called Ion-Selective Field-Effect Transistor (ISFET), as portable DNA sequencer by combining existing DNA biosensors, at National University in San Diego. This will make DNA biometric more familiar [22].

7) Ear recognition

The shape of the ear is used to perform identification by the Ear geometry recognition. It is recommended that the characteristics and the shapes of the human ear are generally distinct. To remove hair, an infrared light can be used and ability to recognize at a distance.

In law enforcement applications individuals are determined by the ear with the help of ear markings are found at crime places. It is yet to be seen that how far this technology will be useful in access control applications. An ear shape verifier similar to telephone handset contains lighting unit and camera to acquire the images of the ear also called as Optophone, manufactured by a French company ART Techniques [4][25].

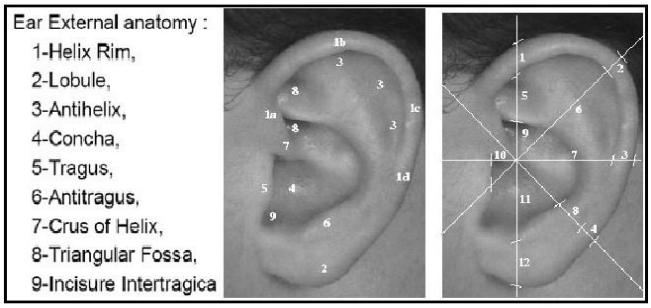

Figure 10: Ear Biometrics

8) Skin Reflection

The skin is made up of different layers with optical properties and distinct morphologies. It consists of two layers – the inner layer, the dermis and the outer layer, the epidermis. Lumidigm established that the absorption spectrum of the skin depends on the individuals. The light properties and electrical properties are the two properties of the skin, which can be used to recognize the person [26]. The lights at different wavelengths are sent into the skin through various LEDs and the scattered lights are read by the photodiodes, analyzed to perform the authentication.

Generally, there are two distinct reflection components when light is reflected from the skin , namely, a specular or interface reflection component, occurs at the surface , in only one direction and a diffuse or body reflection component, formed by the some of the scattered light return to the surface and exit from the skin in different directions. This consists of the information about the individual's skin color and the individual's unique biological "spectral signature". The infrared light is used by the researchers on the skin. This is shown in the Figure.10.

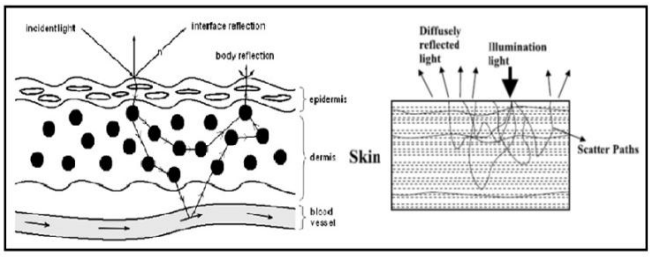

Figure 11: Skin Reflection

9) Lip Biometrics

Lips biometrics is not so familiar to use as biometric features. Human lips recognition biometrics is the most interesting and emerging way of identifying human and usually lip prints are used in forensic science[27][28].The lip features are unique for the individuals and stable over the time[29]. In the speaker recognition the lip movement is used for identification and it is only a subsystem of combination of various biometrics. The lip prints are similar to finger prints and vary from individual to individual [30]. The accuracy can't be obtained if used as alone. The figure 11 shows the shape, prints and movements of lip.

In general, the features of lips can be classified into three different categories: lips texture features, lips shape features and lips motion features. Researchers also found that lip-prints have been used in the determination of sex [31]. The lips biometrics has the following biometrics. The lips biometrics is Passive, Anatomical, Usually visible and Implemented in hybrid.

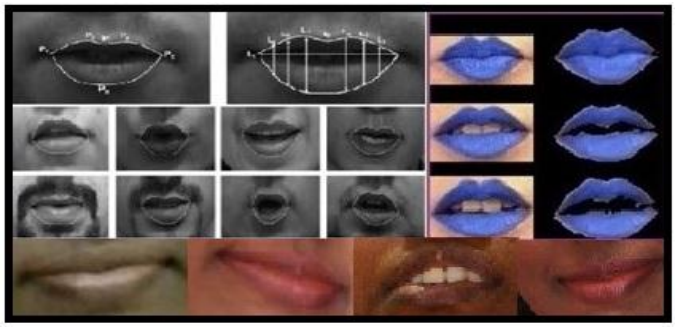

Figure 12: Lip Motion Biometrics

10) Body Odor

A number of researchers have identified that Body odor biometric system is a viable system for identifying a person [32]. The study of odor biometrics is an emerging area which is complex and difficult and it is complexity because of the sensory nature of smell [32]. The human odor released from the different parts of body and exists in the form of exhalation, armpits, urine, stools, farts or feet [32].

Each human smell is unique and it is made up of chemicals called volatiles which could be distinguishable for every individual [33]. It is physical biometrics without any contact to the human body to recognize a person by analyzing olfactory properties of the human body scent [34]. The olfactory means the sense of smell. The sensors which are capable of acquiring the smell are used to get the odor from the back hand or armpit [33], the nonintrusive parts of the body and are converted into a template or unique data string, which are extracted by the system [32]. The body odor consists of significant sensitive personal information. By analyzing the body odor, few diseases or activities happened in the last hours (for example sex) can be possible to diagnose [35]. The functions such as attracting mates, assertion of territorial rights, communication and protection from a predator [36] are served by the body odor. The individual's distinctiveness could be reduced by the usage of deodorants and perfumes.

11) Palm print

The palm region of the hand can be defined as a palm print. The palm consists of the line patterns such as principal lines, wrinkles and ridges. The line of heart, the life line and the head line are known as the principal lines. These line patterns are distinct and unique for every individual and it is a physiological biometric [37]. The palm and fingers are closely related and the pattern is formed by the elevated section of the skin, called ridges. It is called a palm print if acquired from the palm and called fingerprints if acquired from the tip of the finger. The figure 12 shows the palm print.

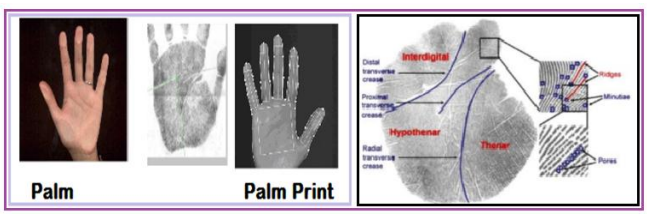

Figure 13: Palm Print Biometrics

In 1858, Sir William Herschel recorded the handprints of Indian civil services employees to match them during their paydays. Palm print scanners are more costly since it is required to acquire bigger portion of the palm. At the time of scanning, the individuals need either touch their hands to a screen or contactless. The authentication procedure of the palm print is very similar to fingerprint i.e., depends on the impressions of friction ridges.

Generally, the ridge patterns like flow of the ridges, features of ridges and the individual ridge's details are studied in a palm print. The matching of the features of the palm print are based on minutiae points, ridge matching and correlation points. To save the template of palm print, the large memory space is required. The following table lists the advantages and disadvantages of the palm print.

The most recent technology, called Palm vein recognition, which uses near-infrared illumination in the palm of an individual's hand to expose the unique vascular patterns. The palm print is unique to individuals and remains unchanged throughout a certain period. Palm print Patterns are applied in Medical disorders – genetic disorders and Downs syndromes and Fortune telling – past and future indication based on the patterns.

12) Hand Vein

The vein recognition system is one of the recent biometric technologies. The main focus of the vein recognition systems is the veins in the user's hands .It is also known as vascular biometrics. The vein recognition systems attract the researchers since it has variety of functions which other biometrics technologies do not have. The level of security is high. The veins are blood vessels that carry blood to the heart. These vein patterns are unique for every individual. Also the vein patterns are unique for the twins and even each individual's left and right hand is distinct. The accuracy of the vein recognition systems is very impressive. The veins are highly stable, robust and developed before birth. The hand vein patterns are shown in the figure 13.

Figure 14: Hand Vein Biometrics

Each finger in the human is directly connected to the brain. The hand Vein patterns are still in the developing stage of research. The system is made by the British Technology Group. Vein check is the instrument with the template of size 50 bytes [1][2][38]. The high resolution cameras using infrared or near infrared light are used to acquire the patterns of the vein. Then the patterns are compressed and digitized. The pattern-matching technique is used to match the patterns. It is not intrusive and even it works for the even if the hand is not clean. The vein biometric system suffers from some

disadvantages like invasive, not affordable to all and it is still being tested and reliability is yet to be proved.

13) Fingernail Bed

One of the emerging technologies is Nail recognition and the study of nail recognition is on progress. The nailbed is one of the essential methods of recognizing fingernail. It is a parallel epidermal located directly below/beneath the fingernail and the travels over the nailbed during growth. It appears on the outer surface of the nail in the form of ridges [39]. This technology is developed by FnBiometrics, which uses a RFID chip. Depending on the individual, the chip is capable of sensing the electrical capacitance of the nail and flesh below itself. The following figure 14 depicts the nailbed.

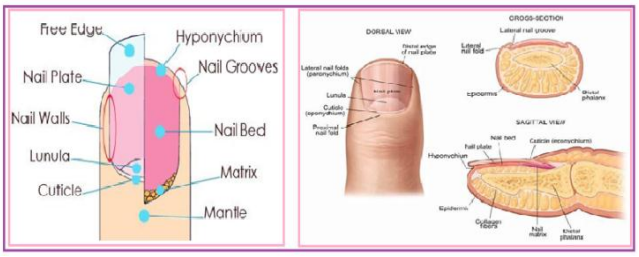

Figure 15: Finger Nail Bed

14) Gait Biometrics

Gait Biometric recognition is an individual‘s walking style. The Gait can be described as the human locomotion causing coordinated and cyclic sequence of movements. It is almost latest technique comparing to the conventional approaches such as fingerprint, face etc. and has 90% accuracy. Commonly, a familiar person is identified by recognizing his/her walking style such as posture of body, swaying and walking distance between the two feet.

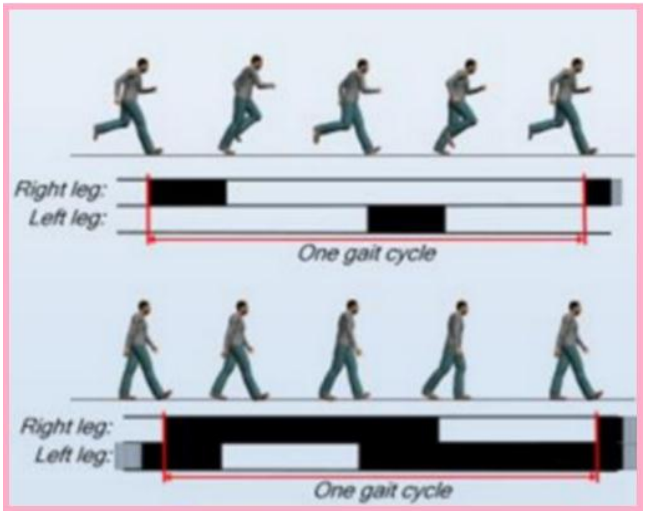

Figure 16: Gait Biometrics

Gait biometrics has several attractive characteristics. Capturing of individual’s gait can be done very easily without their cooperation or even awareness. Some research is going on visually-based systems to analyze the each part of body’s movements using video cameras [40]. The individual’s gait is frequent events with each gait cycle called strides and it has two stages – one foot in the ground (Stance Phase) and the other foot not in the ground (Swing Phase). The shape and dynamics are the two aspects for the gait biometrics. The configuration or different gait phases performed by the shape of the individuals is referred as the shape and the rate of change of one phase to another phase is referred as the Dynamics. Both shape and human motion research has to be synthesized in the research for the growth of gait biometrics. Gait biometrics can be classified into behavioural and physical biometrics. The human walk is the behavioural biometric and anatomy of the feet and body’s weight is physical biometrics. The individual’s gait is unique to some extent only.

With the help of a camera video image is captured and recorded. Then, by using appropriate segmentation and motion detection methods, the walking persons are detected and segmented from the background and then gait features are extracted by creating a mathematical model. The identification can be done by comparing the similarity measures between extracted gait features and the stored features in gait database. Generally, gait features are the challenges to overcome since they are variants due to clothing, footwear, carrying objects, speed, walking surface speed and indoor vs outdoors and so on. The important step in gait recognition is to extract robust and discriminative feature.

15) Signature Dynamics Biometrics

Signature biometrics is a behavioural biometric and uses the pattern of signature to identify the individual. The individual’s way of signing his or her name is the distinct feature of that individual. More emphasis is on the behavioural pattern of how the signature is signed rather than the appearance of the signature. It is operated in two ways – Static and Dynamic signature recognition. The signature biometrics is shown below.

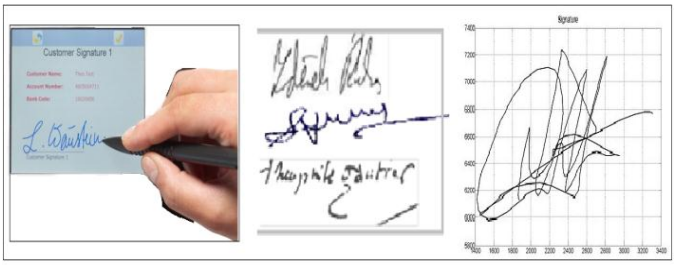

Figure 17: Signature Biometrics

In the static or off-line method, the signature is put in the paper and it can be digitized through camera or an optical scanner. The signature is recognized by the system with the help features of signature such as velocity, speed and pressure. In the dynamic or on-line method, the signature is acquired through digitized tablet in real time i.e., capturing behavioral traits such as speed, pressure, direction of stroke, size of signature and time duration [4].

The behavioural patterns for signature verification includes the pen’s angle, pauses, the time duration, the speed, the pressure and direction of strokes while signing. The graphical appearance of the signature can be easily duplicated but

imitation of the signature with same behavioural traits of the person while signing is very difficult [41].

The size of signature should be small enough as well as big enough to fit on the tablet for acquiring adequate data, quality of the tablet for generating template during enrollment and the verification must be done in the similar environmental backgrounds as that captured during the enrollment time. These are the constraints for Signature Recognition system.

16) Keystroke Biometrics

During World War II, Military Intelligence used a technique called **Fist of the Sender,** uses the rhythm of typing to check whether the Morse code was sent by ally or enemy. The rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics. A keystroke is behavioural biometric technique and it offers sufficient discriminatory information when each individual type on a keyboard in a characteristic way. The person's typing pattern, the rhythm, and the speed of typing on a keyboard are analyzed by this biometric.

The typing dynamics may not be interesting to many of the researchers for identification. But the studies have revealed that the two factors, namely, **dwell time**, the duration of time for which a key is pressed and **flight time**, the elapsed time between releasing a key and pressing the following key or inter-character timing can give 99% accurate identification of the person who is typing [42] .

The time taken to find the right key, the flight time and the dwelling time are differentiating the individual in the way they type on the keyboard. Also there is variation in the speed and rhythm of typing. The keystroke recognition can be classified into two types – Static, one time recognition at the beginning of interaction and Continuous, recognition throughout the course of interaction.

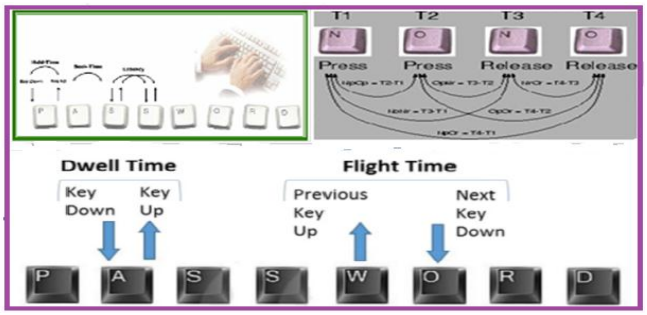

Figure 18: Key Stroke Dynamics

17) Voice Biometrics / Speaker Recognition Biometrics

Today, the voice recognition biometrics is most significant research area. Voice biometrics also known as speaker recognition biometrics. It is shown in the figure 19. They are used for the applications based on telephone. Almost, human voice features are distinct for every individual as well as for twins also and voice could be replicated perfectly. For every individual, unique voice patterns are produced by the combination of physical and behavioural factors. The vocal tract, lips, nasal cavity and shape and size of mouth are the physical characteristics and the pronunciation, emphasis, speed of speech, accents are the behavioural characteristics.

The voice recognition relies on how the person speaks and the focus is on the speech produced by the vocal features not on the pronunciation or the sound. There is no need of any extra special and costlier hardware. The acoustic pattern traits of the speech are used by voice recognition to differentiate the individuals and these patterns consists of both behavioural patterns (speaking style, voice pitch) and physical (shape and size of the throat and mouth) [43][44]. The vocal tract is not affected even by cold and so there will be no adverse impact on the accuracy.

During enrollment time, the individual is asked to repeat the short phrases to prevent the unauthorized access. Audio devices such as microphones, telephones and PC microphones can be used to capture the voice. Using Analog to Digital ADC converter, the generated electrical signal from the microphone is transformed into digital signal and recorded as digitized sample. The appropriate matching algorithm compares the input voice and stored digitized voice for identification.

Speaker dependent and Speaker independent are the two types of voice recognition. Speaker dependent system depends on the knowledge of individual's particular voice traits. The system has to be learned and trained those traits through voice training, in particular accent and tone. Speaker independent voice recognition can able to recognize the speech such as words and phrases from various users with the restriction in the context of the speech. No need to train the system. Text dependent, Text prompted and Text independent are the three styles of spoken input employed by the voice system. It is very hard to design the speaker dependent voice recognition.

The various factors such as ambient noise, variation of speaker as well as in the tone of the same speaker, sensitiveness of phonetic input systems, distance and regular variations are used to analyze the performance of speech recognition system. The voice recognition systems are used in healthcare, government offices, banking, entertainment applications, PIN smart cards, access control, customer authentication and other security purposes.

Due to age factor, the change in voice needs to be addressed by the system. There is a significant difference between Speaker recognition and Speech recognition. The voice or speaker recognition is to recognize the person WHO is speaking and used to identify an individual by tone, accent and voice pitch. The Speech Recognition is to comprehend WHAT spoken and used in menu or map navigation and hand free computing.

Figure 19: Voice Biometrics

18) Thermograms

In general, thermograms are defined as the visible quantity of infrared energy emission, transmission and reflection of an object. Then, it is converted into a temperature and shown as the distributed image of temperature. Also, known as Thermal imaging or Infrared Thermography (IRT). It is developed in mid-1990s. Thermography is similar to facial recognition and facial thermography is used to detect the heat patterns produced by bifurcation of blood vessels, diffused by the skin. These patterns are known as thermography. It is distinct and even it is different for two identical twins. An infrared camera is required to detect these heat patterns, which are unique for every individual. In the infrared distance of the electromagnetic spectrum, these thermographic sensors detect radiation approximately 9,000–14,000 nanometers or 9–14 μm and generates images of that radiation, called thermograms, as shown in the figure 20.

When the rotational- vibrational movements of infrared light are changed, it is absorbed by the molecules. Humans become easily visible in day or night since they are warm-blooded. As a result, an attempt has been made to diagnosis breast cancers and in particular, thermography is useful in military and other surveillance camera usages. It would be impossible to forge the thermal imaging.

In near future, there will be significant change in biometric security, which may be the replacement of Fingerprints and Iris recognition by Thermal imaging. The table lists the strengths and limitations of thermograms.

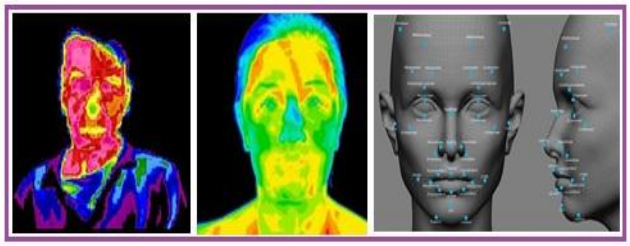

Figure 20: Thermograms

19) Brain Wave Biometrics

The recent emerging research and promising area of biometrics identification of human's brainwave. The brainwave biometrics is also known as cognitive biometrics. Many researchers have found that each individual's brainwave features are unique. These features are potential enough to use as biometric authentication Electroencephalogram (EEG) can be used to measure brainwave activity and security can be enhanced by employing EEG features. Presently, measuring brainwaves is time consuming process. But it can be used in future in the special security areas. The advantages of brainwave biometrics are (i) the difficulty in eavesdropping on personal brain wave data and (ii) the brainwaves can reflect individual mental activities. The individuals are identified on the basis of templates which reflect brain activities as a cognitive process.

The brainwave biometric approach is classified into three methods. Firstly, brainwave based on Alpha (α) waves and Gamma (γ) waves [45][46][47], secondly, motor imagery [48][49][50][51] and lastly, near infrared spectroscopy (NIRS).

20) Latest Biometric Trends

a) Smartphones*:* Smartphones are the most potential space for biometrics applications. It is highly integrated with biometrics for unlocking and locking the phone through fingerprint recognition, voice recognition and face recognition. It eases the operation and also the increase the safety and security of the data**.**

b) Wearables: The current boom is on wearable devices, highly based on biometrics. They measure the biological characteristics of the individual like heart rate, sweat and brain's activity. The information related to the health of the individual can be identified with the help of wearable device.

c) E-Commerce: With the help of E-commerce, people use the online shopping but still there is a threat in online payment. It is being suggested that the use of fingerprints, iris and facial recognition can be used instead of credential which ensures a secure login.

d) Cloud-Based biometrics: A lot of popularity is gained for Cloud computing in the world of corporates since it provides secure, highly convenient and mass storage space for all the valuable data but still security concerns are there. The security can be ensured by deploying biometrics for access control applications, intelligent environments and smart spaces.

COMPARISON OF BIOMETRICS

The comparison of the different biometric methods by considering the various factors. The biometric features of face, voice, fingerprint, iris, hand geometry, retina, keystroke, gait, signature and DNA have the characteristics like Universality, Uniqueness, Permanence, Performance, Collectability or Measurability, Acceptability and Circumference. These characteristics are distinct for each biometric type. These can be measured in High, Medium and Low [17] [52] denoted by H, M, and L, respectively. Any human physiological or behavioural features can serve as a biometric characteristic as long as it satisfies these requirements. Table 8 compares the biometric features based on different factors.

Table 8: Comparison of Various biometric techniques based on biometric traits

Identifier / Criteria	Universality	Uniqueness	Collectability	Permanence	Performance	Acceptability	Circumvention
Fingerprint	Medium	High	Medium	High	High	Medium	Medium
Face	High	Medium	High	Medium	Low	High	High
Iris	High	High	High	High	High	Medium	Low
Hand Geometry	High	Medium	High	Low	Medium	Medium	Medium
Retina	High	High	Medium	High	High	Low	Low
DNA	High	High	Low	High	High	Low	Low
Gait	High	Medium	High	Medium	Low	Medium	Medium
Odor	High	High	Low	High	Low	Medium	Low
Palm print	Medium	High	Medium	High	High	Medium	Medium
Ear	Medium	Medium	Medium	High	Medium	High	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	Low
Signature	Low	Low	High	Low	Medium	High	High
Keystroke	Low	Low	Medium	Low	Low	Medium	Medium
Voice	Medium	Low	Medium	Low	Low	High	High
Thermograms	High	High	High	Low	Medium	High	Low

PERFORMANCE AND EVALUATION OF BIOMETRIC SYSTEMS

The important aspect of biometrics technology is to evaluate their performance. The performance of any biometric authentication techniques can be measured by the various parameters such as False Accept Rate (FAR), False Reject Rate (FRR) and Crossover Rate (CER) or Equal Error Rate (EER) [52][53][54]. A true identity claim wrongly rejected is called False Rejection. Similarly, a false identity claim wrongly accepted is known as False Acceptance. To make limited entry to authorized users FAR and FRR are used.

False Rejection Rate (FRR) measures the probability of rejecting an authorized user incorrectly as an invalid user. It can be calculated using the following method.

$$FRR = \frac{\text{Number of False rejections}}{\text{Number of Identification Attempts}}$$

False Acceptance Rate (FAR) measures the probability of accepting an unauthorized user as a valid user, which computed as follows. A biometric system is highly secured if it has low FAR. The figure 21 illustrates FAR and FRR.

$$FAR = \frac{\text{Number of False Acceptances}}{\text{Number of Identification Attempts}}$$

Failure to Enroll (FTE) and Failure to Capture (FTC) are the other recognition error rates. The **FTE** is the percentage of input is invalid and fails to enroll in the recognition system. The **FTC** is the percentage that the system fails to capture a biometric characteristic when present correctly.

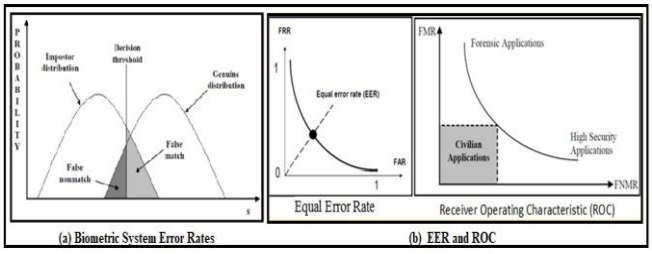

Figure 21: (a). Biometric System Error Rates (b) EER and ROC

If $S \geq T$, compared samples belong to a same person and if $S < T$, samples belong to a different person where S – Similarity score and T – Acceptance threshold. The **imposter distribution** is the distribution of pairs of samples generated from different persons and the **genuine distribution** is the distribution of pairs of samples generated from the same person.

The figure 21(a) shows the point at which FAR is equal to FRR is known as Equal Error Rate (EER) or Crossover Rate (CER) , which indicates the proportion of false acceptances is equal to the proportion of false rejections. The relationship between FAR and FRR can be depicted graphically in figure 21(b), called ROC, a performance measure of a biometric system. With the help of ROC, performance of different biometric system can also be compared using their independent thresholds.

If EER/CER is low, the accuracy of the biometric system is high. The biometric systems are built in acceptance threshold. If the threshold is high, FAR decreases and FRR increases. Always, low FAR and high FRR would ensure that any unauthorized user will not be permitted to access. The tables 9 and 10 show performance of various biometric techniques [52] [53] [54] [55].

Table 9 Performance Evaluation

Identifier / Criteria	Fingerprint	Face	Iris	Hand Geometry	Retina	DNA	Signature	Voice	Keystroke
FAR	2%	1%	0.94%	2%	0.91%	-	-	2%	7%
FRR	2%	10%	0.99%	2%	0.04%	-	-	10%	0.10%
CER	2%	-	0.01%	1%	0.80%	-	-	6%	1.80%
FTE	1%	-	0.50%	-	0.80%	-	-	-	-

Table 10 Performance based on significant factors

Identifier / Criteria	Finger print	Face	Iris	Hand Geometry	Retina	DNA	Signature	Voice	Keystroke
Socially Introduced	1981	2000	1995	1986	1999	1965	1970	1998	2005
Cost	L	M	H	H	H	H	M	L	M
Popularity	H	H	M	L	L	H	H	H	L
Ease of Use	H	H	M	H	L	L	H	H	L
Accuracy	M	L	H	M	H	H	M	L	L
Stability	H	M	M	M	H	H	M	M	L
Speed	H	M	M	H	M	L	H	H	M
Stability	H	M	M	M	H	H	M	M	L
Safety	M	M	H	M	H	H	H	H	L
Error of incidence factors	Dryness, dirt, age	Lighting, age, glasses, hair	glasses, poor lighting	Injury, age	Glasses, contact lens	Equipments	Change in signature	Noise, cold	Device, weather

(L- Low, M- Medium, H-High)

FUTURE OF BIOMETRICS

The problems with traditional biometrics may be overcome with the technology of the future.

1. Expanding the range of identification is the solution for the requirement of user's cooperation with the traditional technologies.
2. The individual technologies' shortcomings can be replaced by Multi-factor authentication.
3. In real time the behavioural biometrics analyze people and force the users to re-identify themselves.

Generally, behavioural biometric methods can be analysed without cooperation from the user, which uses the unique features such as signature identification, keystroke identification and analysis of gait. Video based identification is more feasible solution. Another type of behavioural biometrics is Gesture based identification, which is most feasible with touchscreen devices.

DISCUSSIONS

Biometric authentication becomes highly promising since human physical characteristics are much more difficult to forge. The security code, passwords, hardware keys, smart card, magnetic stripe card, ID cards, physical keys can be lost, stolen, duplicated or left at home. Passwords can be forgotten, shared or observed and people have to remember a multitude of passwords like ATM PIN, mail password etc.

For variety of application biometrics authentication is fast, easy, accuracy, reliable and less expensive. Nowadays, biometrics uses non-invasive methods for identification of individuals. Image acquisition, pre-processing, feature extraction and template storing in the system database are the stages involved in the processing of biometric system. The comparison of the input query image features and stored features are done for authentication during verification.

The noisy sensor data, spoof attacks, interclass similarity and intra-class variations are the limitations. To increase the performance accuracy and to design a biometric system or to propose a new approach to the existing system, one has to understand the basic biometric system, its parameters, limitations, biometric scenario, biometric characters used for an application, types of errors and existing approaches. Any biometric system is not an optimal system. Always there is a need for improving the accuracy and performance of the biometric system.

CONCLUSIONS

Basically, Biometric is developed on methods of pattern recognition .Biometrics is an evolving technology which is being widely applied in the areas like forensic, security, ATM, smart cards, PC and networks. Biometrics is more secured when compared to conventional methods of authorization. This paper presents a literature survey on the various techniques involved in identification and the emphasizes is given on biometric recognition system. The biometric recognition systems are the automatic recognition system to overcome the drawbacks of traditional systems. But, biometric-based systems also have some limitations and can be overcome with the evolution of biometric technology.

In various applications, the biometric recognition system have been proved to be accurate and very effectively. Acquisition of biometric features can be processed easily in the presence of a person. In the future, multimodal biometric system will alleviate a few of the problems in unimodal system and certain that biometric based recognition will have great influence on our day to day life. Today biometric plays significant role in many application areas such as military, forensic, access control etc. In this paper, various biometric techniques are defined and compared. The biometrics is becoming a developed technology in the field of security though there are some problems with biometrics systems.

Recent advancement in biometric technology have resulted in increased accuracy and reduced cost. Today biometric solutions have proved that authentication becomes fast and user-friendly. Many areas will benefit from biometrics. Currently, there is a gap between the feasible biometrics projects and biometric experts. To remove this knowledge gap, biometric discussion groups may be organized and make the biometric knowledge seekers to participate in it. Only minimal user knowledge and effort would be required for the end user. In the future biometric devices will surely become more involved in many civil areas. The current research trends have shown the prospect of using Brain waves and ECG as biometric identification. The current research indicates that the identification of human is more effective and far more challenging. Various journal and international conferences research papers have been studied and summarize the progress in the direction of cost-effective and an innovative manner.

In real time and in near future, the identification of users with very high degree of confidence is required for the automated systems. Smart mobile devices has already spread wide the biometric, which increases the significant acceptance. For the brightest future and development, continuous and multiple modality automated authentication methods are determined.

REFERENCES

[1] Anil K. Jain, Karthik Nandakumar and Arun Ross, "50 years of biometric research, Accomplishments, Challenges and Opportunities", Pattern Recognition Letters, 2016, vol.79, pp.80-105.

[2] Jain K. Anil, Ross Arun and Prabhakar Salil, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 2004, vol.14, no.1, pp. 4-20.

[3] A. K. Jain, A. Ross and S. Pankanti, "Biometrics, A Tool for Information Security", IEEE Transactions on Information Forensics And Security, 2006, vol.1, no.2, pp. 125 – 144.

[4] S.Prabhakar, S.Pankanti and A.K.Jain, "Biometric

Recognition, Security and Privacy Concerns", IEEE Security & Privacy, 2003, pp. 33-42.

[5] J.L.Wayman, "Fundamentals of Biometric Authentication Technologies", International Journal of Image and Graphics, World Scientific Publication, 2001, vol.1, no.1, pp. 93-113.

[6] J.L.Wayman, A.K.Jain, D.Maltoni, D.Maio and et al, "Biometric Systems, Technology, Design and Performance Evaluation", New York, Springer Verlag, 2005.

[7] Alfred, C. Weaver, "Biometric Authentication", IEEE Computer Society, 2006, vol.39, no.2, pp. 96-97.

[8] Kresimir Delac, Mislav Gregic, "A Survey of Biometric Recognition Methods", 46th International Symposium Electronic in Marine, ELMAR-2004, Zadar, Croatia, June 2004.

[9] D.Maltoni, D.Maio, A.K.Jain and S.Prabhakar, "Handbook of fingerprint recognition", Springer, New York, 2003.

[10] R.Cappelli, D.Maio, D.Maltoni, J.L.Wayman and A.K.Jain, "Performance evaluation of fingerprint verification systems", IEEE Transactions on Pattern Recognition and Machine Intelligence, 2006, 28, no.1, pp. 3–18.

[11] A.K. Jain, L.Hong and R. Bolle, "On-line fingerprint verification", IEEE Transactions on Pattern Recognition and Machine Intelligence, 1996, vol.19, no.4, pp. 302–314..

[12] Sourav Ganguly and Subhyyan Roy Moulick, "A Review on Different Biometric Technique", International Journal of Engineering Research and Technique, 2012, vol.1,no.5, pp.1-7, July-2012.

[13] S.Z. Li, A.K.Jain and et al, "Handbook of Face Recognition", New York, Springer Verlag, 2004.

[14] Rama Chellapa, Charles, L.Wilson and Saad Sirohey, "Human and machine recognition of faces, a survey", Proc. IEEE, May 1995,vol.83, no.5, pp. 705-740.

[15] C.Marin˜o, Æ M. G Penedo, Æ.M.Penas, Æ M. J.Carreira and F.Gonzalez, "Personal authentication using digital retinal images", Journal of Pattern Analysis and Application, Springer, May 2006, vol.9, no.1, pp. 21– 33.

[16] John Daugman, "How Iris Recognition Works", IEEE Transactions on Circuits and Systems for Video Technology, January 2004, vol.14, no.1.

[17] Himanshu Srivastava, "Personal Identification Using Iris Recognition System, A Review", International Journal of Engineering and Applications (IJERA), 2013, vol.3, pp.449- 453.

[18] R.Sanjay, Ganorkar, A.Ashok and Ghatol, "Iris Recognition, an Emerging Biometric Technology", In Proc. of 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp. 91 – 96,

[19] K.W.Bowyer, K.Hollingsworth and P.J.Flynn, "Image understanding for iris biometrics, a survey" Computer Vision and Image Understanding, May 2008,vol.110, no.2, pp. 281-307.

[20] R.Sanchez-Reillo, C.Sanchez-Avilla and A.Gonzalez-Macros, "Biometrics Identification Through Hand Geometry Measurements", IEEE Transactions on Pattern Analysis and Machine Intelligence, Oct. 2000,vol.22, no.18, pp. 1168-1171.

[21] E.Kukula and 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.

[22] "Biometrics News Portal-DNA Biometrics", http,//www.biometricnewsportal.com/dna_biometrics.asp, 04/03/2008.

[23] "Genetics Home Resource Website - What is DNA", United States National Library of Medicine. National Institute of Health, http,//ghr.nlm.nih.gov/handbook/basics/dna, 2008.

[24] "Inderscience Publishers - Handheld DNA Detector",ScienceDaily, http,//www.sciencedaily.com/releases/2008/03/080310173246.htm, 2008

[25] Shrutika Deokar and Sudeep Talele, "Literature Survey of Biometric Recognition Systems", International Journal of Technology and Science, May 2014, vol.1, no.2.

[26] Shradha Tiwari , J.N. Chourasia and Vijay S.Chourasia, "A Review of Advancement in Biometric Systems", International Journal of Innovative Research in Advanced Engineering, January 2015, vol.2, no.1.

[27] J.Ball, "The current status of lip prints and their use for identification", Journal of Forensic Odonto-stomatology, 2002, vol.20, no.2, pp. 43–46.

[28] T.R.Saraswathi, G.Mishra and K. Ranganathan, "Study of lip prints". Journal of Forensic Dental Science, 2009,vol.1, pp.28-31.

[29] E.Gomez, C.M Travieso, J.C.Briceno and M.A. Ferrer, "Biometric Identification System by Lip Shape", In, Proc. of Carnahan Conference on Security Technology,2002, pp. 39–42, 2002.

[30] H.E.Cetingul, Y.Yemez, E. Erzin and A.M.Tekalp, "Discriminative Analysis of Lip Motion Features for Speaker Identification and Speech-Reading", IEEE Trans. Image Processing, 2006, vol.15, no.10, pp.2879–2891.

[31] V.Sonal, C.D.Nayak and S.S.Pagare, "Study of Lip-

Prints as Aid for Sex Determination", Medico-Legal Update,2005, vol.5,no.3.

[32] Magda Brattoli, Gianluigi de Gennaro, Valentina de Pinto, Annamaria Demarinis Loiotile, Sara Lovascio and Michele Penza., "Odour Detection Methods, Olfactometry and Chemical Sensors", Sensors, 2011, vol.11, pp.5290-5322.

[33] "Z. Korotkaya -Biometric Person Authentication, Odor", pp.1- 6, http,//www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf as visited on 10/08/2008.

[34] Olufemi Sunday Adeoye., "A Survey of Emerging Biometric Technologies", International Journal of Computer Applications, 2010, vol.9,no.10, pp. 1-5.

[35] Duan Xufang, Block Eric, Li Zhen, Connelly Timothy, Zhang Jian, Huang Zhimin, Su Xubo, Pan Yi and et al., "Crucial role of copper in detection of metal-coordinating odorants", Proc. Natl. Acad. Sci. U.S.A,2012.

[36] Chatchawal Wongchoosuk, Mario Lutz, and Teerakit Kerdcharoen., "Detection and Classification of Human Body Odor Using an Electronic Nose", Sensor, 2009, vol.9, pp.7234-7249.

[37] A. Kumar, , D.C.Wong, H.C.Shen and A.K.Jain, "Personal Verification using Palm print and Hand Geometry Biometric", In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, June 2003, pp. 668 - 678.

[38] Ramen V. Ramen and V.Yampoolskiy, "Biometrics , a survey and classification", Biometrics, 2008, vol.11, no.1.

[39] R.Kavitha Jaba Malar and V.Joseph Raj, "Geometric Finger Nail Matching using Fuzzy Measures", International Journal of Innovative Technology and Exploring Engineering (.IJITEE), September 2014, vol.4, no.4.

[40] D.Cunado, M.S.Nixon and J.N. Carter, "Automatic extraction and description of human gait models for recognition purposes", Computer Vision and Image Understanding, 2003, vol.90, pp.1–41.

[41] Samir K.Bandopadhaya., Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly and Poulumi Das., "Statistical Approach for Offline Handwritten Signature Verification",Journal of Computer Science, Science Publication, May 2008, vol.4, no.3, pp. 181 – 185.

[42] F.Monrose and A. Rubin, "Authentication via keystroke dynamics", In Proc. of 4th ACM Conference on Computer and Communications Security, Switzerland, April 1997, pp. 48–56.

[43] A.Eriksson and P.Wretling, "How flexible is the human voice? A case study of mimicry", In Proc. Of European Conference on Speech Technology, Rhodes, Greece, September 1997, pp. 1043–1046.

[44] S.Furui,"Recent Advances in Speaker Recognition", In Proc. of First International Conference on Audio and Video based Biometric Person Authentication, UK, March 1997, pp. 859-872.

[45] I.Biel, O.Pettersson, , L.Philipson and P.Wide, "ECG Analysis, A New Approach in Human Identification", IEEE Transactions on Instrumentation and Measurement, June 2001, vol.50, no.3, pp. 808 – 812.

[46] Yongjin Wang, Foteini Agrafioti, Dimitrios Hatzinakos and Konstantinos N. Plataniotis, "Analysis of Human Electrocardiogram for Biometric Recognition", EURASIP Journal on Advances in Signal Processing, January 2008,2008.

[47] C.Miyamoto, S. Baba, and I.Nakanishi, "Biometric person authentication using new spectral features of electroencephalogram (EEG)", Proc. Int. Symp. Intelligent Signal Processing and Communications Systems (ISPACS), 2009, pp. 1-4.

[48] Koji Tsuru and Gert Pfurtscheller., "Brainwave Biometrics, A New Feature Extraction Approach with the Cepstral Analysis Method", Trans Jpn Soc Med Biol Eng, 2012, vol.50**,**no.1, pp.62-167.

[49] R.Palaniappan and D.P. Mandic,"Biometrics from brain electrical activity, A machine learning approach", IEEE Transactions on Pattern Analysis and Machine Intelligence ,20017,vol.29**,** pp**.**738-742.

[50] A.Riera, A.Soria-Frisch, M.Caparrini, C.Grau and G.Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis", EURASIP J. Adv. Signal Process,2008, pp. 1-8..

[51] J.Hu, "New biometric approach based on motor imagery EEG signals", Proc. Int. Conf. Future BioMedical Information Engineering FBIE 2009, 2009, pp. 94-97.

[52] P.Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface International Journal of Computer Applications, 2011, vol.14, no.5.

[53] Simon Llu and Mark Silverman., "A Practical Guide to Biometric Security Technology", IT Pro, 2001.

[54] Himanshu Srivastva, "A Comparison Based Study on Biometrics for Human Recognition", IOSR Journal of Computer Engineering (IOSR-JCE), 2013, vol.15, pp. 22-29.

[55] Gursimarpreet Kaur and Chander Kant Varma., "Comparative Analysis of Biometric Modalities", International Journal of Advanced Research in Computer Science and Software Engineering, 2014,vol.4,no.5.