



Published on: 29-03-2014

**Ms. C.B. Tatepamulwar**  
School of Computational  
Sciences,  
Swami Ramanand Teerth  
Marathwada University, Nanded  
(M.S.) India.  
fadewarch@gmail.com



QR Code for Mobile users



Conflict of Interest: None Declared

## Comparison of Biometric Trends Based on Different Criteria.

**Ms. C.B. Tatepamulwar<sup>1</sup>, Dr. V. P. Pawar<sup>2</sup>**  
School of Computational Sciences,  
Swami Ramanand Teerth Marathwada University, Nanded (M.S.) India.

### ABSTRACT

This paper gives a brief overview on different physiological and behavioral biometrics. Now days we are quite ensure about security and privacy of our data, that's why we can use biometric techniques for identification and recognition of users for creating safe and secure system. The paper also includes some biometric comparisons based on different criteria's.

**Keywords:** Biometrics, Identification, Biometric techniques, Recognition

### Cite this article as:

Ms. C.B. Tatepamulwar, Dr. V. P. Pawar,  
Comparison of Biometric Trends Based on Different Criteria.  
Asian Journal of Management Sciences.  
02 (03 Special Issue); 2014; 159-165.

**Introduction**

Today we have a big question about identification and recognition of authenticated user for purchasing authenticated data. To overcome this problems biometric trend helps us. Biometric refer to physical and behavioral trait /characteristics of individual. Traditional means of access control include token based identification systems such as driver’s license, password and knowledge based identification systems such as password, personal identification number. The password, pin is used to give the user a unique access to certain sectors but text password does not ensure the maximum security of the system .the password can be stolen ,forgotten and it may be guessed. The solution to this problem is biometric characters which can’t be stolen .forgotten and copied[1,2].

**1.2. Biometric trends:**

Every person has some specific and distinguishable biometric traits. Some Characters are as, Each person should possess the characteristics( Universal), two persons shouldn’t share the characteristics(unique), the characteristics should not change(permanent),easily presentable to a sensor and quantifiable(collectable),accuracy, speed and robust of technology used (performance), also biometric possess acceptability and circumvention.physiological trends include iris,fingerprint,palm print, gait , retina,odour,DNA,ear and behavioral trends include voice,

**1. Techniques:**

**2.1. Ear recognition:**

The ear recognition is a physical biometric which is characterized by the shape of the outer ear, lobes and bone structure. It is new biometric, not widely used yet also an unique technique. Ears are smaller area than any other like face so we get reduced spatial resolution. Another advantage is that ears are not as variable as e.g. faces. Biometric ear shape is of three types which are pictures, earmarks, and thermo gram. Thermo gram is regional map of the surface of the body made by a thermograph. The ear of every person has a unique pattern and structure. By this a person can be identified. This pattern is unique biological trait of each and every human[1].

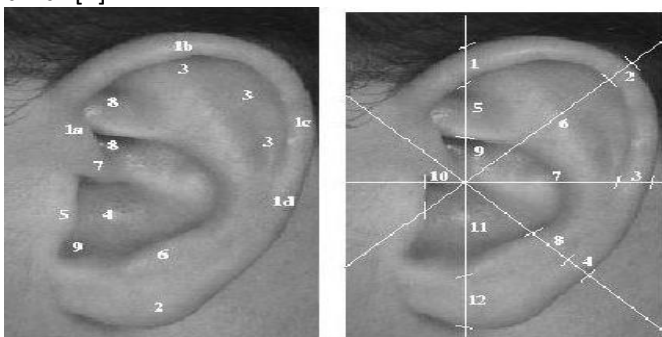


Fig. 1 Image of ear(source: paper 4)

**2.2. Fingerprint recognition:**

Fingerprint is a pattern of ridges and valleys on the surface of the fingerprint. These patterns of ridges are of three types i.e. arch, loop and the cycle.

- i. Loop: the ridges enter from one side of finger, from a curve, and exit on same side.
- ii. Arch: the ridges enter from one side of finger, rise in the center forming an arc, and exit the other side of finger.
- iii. Whorl: ridges form circularly around the central point of finger.

Finger prints of twins are also different. Fingerprint verification process is high reliable, robust, accurate, highly distinctive. Fingerprint is user convenient, mostly used. It is also stable over time. There are some disadvantages in fingerprint capturing. Functional defects are possible if the fingertips are very dirty or worn. Injury to fingertip also cause defect. Dry skin grease and sweat can cause recognition difficulties[3].



Fig. 2. Fingerprint pattern (source: Data set)

**2.3. Gait recognition:**

Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints. Gait is similar to acquiring a facial picture and hence may be an acceptable biometric. Gait based systems use the video – sequence footage of a walking person to measure several different movements of each articulate joint[3,4].



Fig.3. Phases of gait (source: paper Data set)

#### 2.4. Keystroke recognition:

It is hypothesized that each person types on a keyboard in a characteristic way. Keystroke dynamics is a behavioral biometric for some individuals, one may expect to observe large variations in typical typing patterns. Means the rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics[4,5].

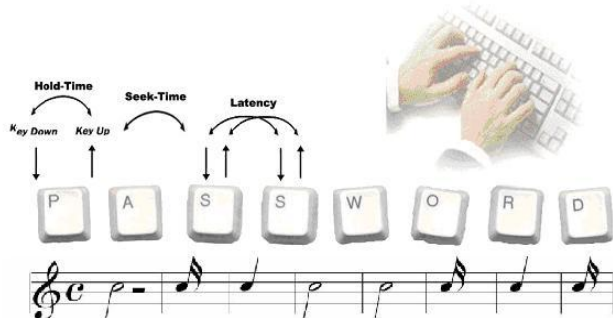


Fig. 4. Keystroke pattern(Source: paper1)

#### 2.5. Speech recognition:

Speech recognition or automatic speech recognition (ASR) system is converts the audio signal to a machine readable format. ASR recognizes the words and these words are worked as input[6].

#### 2.6. Retina recognition:

Retinal scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were introduced by EyeDentify in 1985. The iris recognition cannot be confused. The retina is a thin tissue of the posterior neural cells that formed the eye. Cappilaries of complex structure supplies blood to the retina. Retinal blood vessels in the network are so complex that even identical twins do not share a similar pattern. The retina remains unchanged from birth until death. Retina is not directly visible & so a coherent infrared light source is necessary to illuminate the retina. The infrared light source is immersed more rapidly by blood yacht in the retina than by the surrounding tissue. The analysis of retina blood vessel pattern is for characteristics points within the pattern. The retina scan is more susceptible to some diseases than the iris scan, but such diseases are relatively rare. Due to that retina scan is permanent biometric[6].

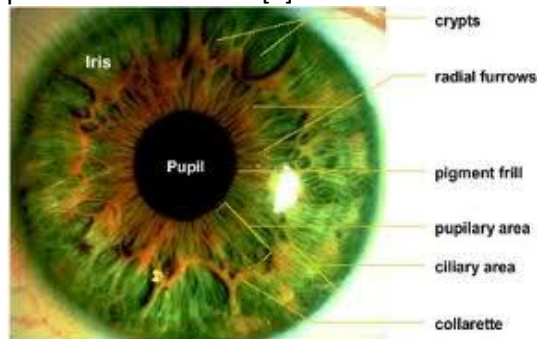


Fig. 5. Retinal scan(source paper 5)

#### 2.7. Palm recognition:

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. Palm print scanner need to capture a large area, they are more expensive than the fingerprint sensor. Human palms also contain additional distinctive features such as principle lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. When using a high resolution palm print scanner, all the features as hand geometry, rides wrinkles, and valley can be combined to build a highly accurate biometric system. It is a 3-dimentional image of hand from which extracted features are compared with the database feature vectors. These features are bulky but identification is done in short time[7].



Fig. 6. Palm print taken by sensor

#### 2.8. Speaker recognition:

The voice is a unique feature of every individual. Using voice recognition it is possible to identify a user from the existing database by utilizing the unique features of the voice including the pitch, time, aplitude, intensity. The voice acoustic properties of speech have been found that an individual use to the individual.the acoustic pattern of both anatomy & reflects the behavioral patterns learned. Voice is compared with a previously created voice print. Compare the characteristics lip motions while person speak. This will help in identification associated with speaker[5,8].

#### 2.9. Signature recognition:

In signature recognition system we calculate the movement of the pen while signing process rather than the static image of the signature. Some aspects like pen pressure, the sound the pen makes help in user's recognition. The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured in terms of pressure, direction, acceleration, length of the stroke, number of strokes and their duration. Various kinds of devices are used to capture signature. Special pens are able to capture movements in all three dimensions. Tablets have two significant disadvantages. First, the resulting digitalized

signature looks different from the usual user signature. Secondly, while signing the user does not see what he or she has already written[8,9].

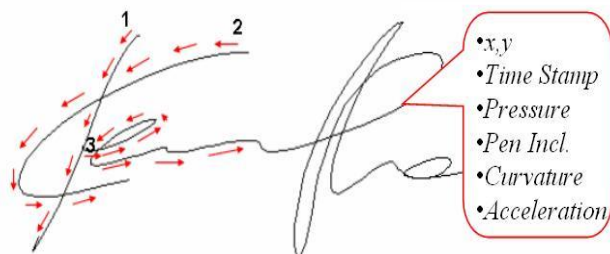


Fig.7. signature taken using tablet(source: paper 6)

### 2.10. DNA recognition:

In DNA the information identify from every cell in the body in a digital form. It is called as ultimate identifier. This method is expensive, comparatively slow, not yet fully automated. This method also has some limitations that it contains information about race, paternity, and medical conditions for certain disease & Theoretical limitation is Identical twins have the same DNA[5,6,8].



Fig.8. DNA structure (source Wikipedia)

### 2.11. Face recognition:

Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order that a facial recognition system works well in practice, it should automatically detect whether a face is present in the acquired image; locate the face if there is one; and recognize the face from a general viewpoint (i.e., from any pose). Uses an image or series of images either from a camera or photograph to recognize a person. In the matching the face from a digital image or a video frame from video source is matches with the existing database. Facial features are used for

comparison. some facial recognition algorithms are used to retrieve landmarks, or features of the face of an image to detect faces. As an example an algorithm can be analyzed relative to the location, size, and the eyes, nose, cheekbones, jaw shape[3,6].

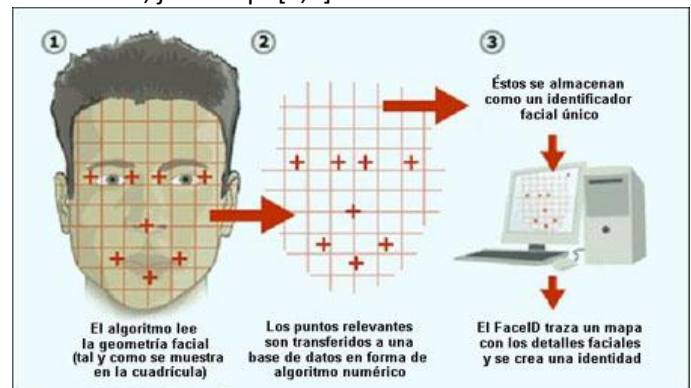


Fig.9. Facial image captured by a camera(source paper 2)

### 2.12. Odor recognition:

Each and every person has different body odor. Some immunity genes produce body odor which are different in different persons, so that every human smell is unique. Odor is captured by sensors that are capable to obtain the odor from nonintrusive parts of the body such as back of hand. Human smell is made of chemicals known as volatiles. They are extracted from the system and converted into a template. This template is used for comparison with stored templates [1,3,9].

#### 2. Biometric verification system

Biometric verification system involves some units for capturing data, for matching or for many purposes to execute latest and stored template, which gives authentication to correct user. The units are as follows,

##### 3.1. Acquisition unit:

For acquisition or consumption of image scanner, many types of camera, sensors are used. The quality of output is totally depends upon quality of input image.

##### 3.2. Image preprocessing:

In this unit by using various preprocessing the image quality is enhanced. The noise and low frequency backgrounds are removed from image.

##### 3.3 Feature extraction:

In this part image features are extracted those can be used to identify the person. Each person has a unique characteristics, attribute that can give his identity such as finger print image of person has the features like whorls, arches, loops, ridges, furrows and minutiae. These are called as feature vectors. We can use many extraction techniques and algorithms for feature extraction.

##### 3.4. Matching:

In the matching unit, the features of captured image are compared with stored template image features. If images are matched then verification is true or completed

successfully. this verification /matching is done one to one or one to many.

In this way we can use two types for verification, image techniques in which both optical and numerical image correlation techniques are used and second are feature techniques in which extracts features and develop representations from the features. If we combine both

techniques then resultant techniques is more accurate, which we can call hybrid technique[8,9].

**4. Biometric Comparison Based on Various Criteria :**

This paper is to provide the comparative study about various biometrics, so after studying a number of research papers and articles, I am giving a number of comparison tables based upon various criteria[9].

BIOMTRIC	UNIQUENESS	UNIVERSALITI	PERMANENCE	CIRCUMVENTION	PERFORMANCE	COLLECATABILITY	DISTINCTIVNESS
SIGNATURE	P	P	p	G	P	G	P
SPEAKER	P	A	P	G	P	A	P
FACE	L	G	A	G	P	G	P
IRIS	G	G	G	P	G	A	G
KEYSTROKE	P	P	P	A	P	A	P
PALMPRINT	A	A	G	M	G	A	A
RETINA	A	G	A	P	G	P	G
GAIT	A	A	P	A	P	G	P
FINGERPRINT	G	A	G	A	G	A	G
EAR	A	A	G	A	A	A	A
DNA	G	G	G	P	G	P	G
ODOR	G	G	G	A	P	P	P

Table 1. Comparison of trends based on various criteria  
P=poor, A=average, G=good. ( Source: Biometric Wikipedia and paper. 9)

Biometric	Trait
Fingerprint	Finger lines, pore structure
Signature (dynamic)	Writing with pressure and speed differentials
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Retina	Eye background (pattern of the vein structure)
Hand geometry	Measurements of fingers and palm
Finger geometry	Finger measurement
Vein structure of back of hand	Vein structure of the back of the hand
Ear form	Dimensions of the visible ear
Voice	Tone or timbre
DNA	DNA code as the carrier of human hereditary features

Table 2. List of various biometric features  
(Source: paper. 9)

Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Easy of Use	high	high	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signature	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	high
Long Term Stability	High	Medium	high	high	Medium	Medium	Medium

Table 3. Characteristics features Biometric Techniques  
(Source: paper. 9)

**Conclusion:**

Biometrics is a rapidly evolving technology that is being widely used in forensics, security; prevent unauthorized access in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. There are numerous forms of biometrics now being built into technology platforms. As biometric technology matures,

there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business. Selection of a particular biometric technology for identifying and authenticating users depends of a number of factors such as security requirements of the application under consideration, the environment in which the users will be authenticated; the frequency of usage, type of access required, cost factors, etc.

#### References:

1. Renu Bhatia, "Biometric and Face Recognition Technique", International Journal of Advanced Research in Computer Science and software Engineering, Vol.3, issue 5, May 2013 pp.93-99.
2. Debnath Bhattacharya and Rahul Ranjan, " Biometric Authentication : A review, International Journal of u-and-e service, science and technology vol. 2 Bo.3 Sept. 2009 pp.13-28.
3. Sourav Ganguly and Subhyyan Roy Moulick, "A Review on Different Biometric Technique", International Journal of Engineering Research and Technique, Vol.1 Issue 5, July-2012 pp.1-7.
4. Anil K Jain and Salil Prabhakar, " An Introduction to Biometric Recognition, IEE Transaction a Circuits and System for Video Technology, vol 14, No.1 Jaunary 2014 PP.4-20.
5. J. Daugman, "Recognizing persons by their Iris patterns," in *Biometrics:Personal Identification in a Networked Society*, K. Jain, R. Bolle, and S. Pankanti, Eds. Norwell, MA: Kluwer, 1999, pp. 103–121.
6. L. O’Gorman, "Seven issues with human authentication technologies,"in *Proc.Workshop Automatic Identification Advanced Technologies (AutoID)*,Tarrytown, NY, Mar. 2002, pp. 185–186.
7. E. d. Os, H. Jongbloed, A. Stijsiger, and L. Boves, "Speaker verification as a user-friendly access for the visually impaired," in *Proc. Eur. Conf.Speech Technology*, Budapest, Hungary, 1999, pp. 1263–1266.
8. A. Eriksson and P. Wretling, "How flexible is the human voice? A case study of mimicry," in *Proc. Eur. Conf. Speech Technology*, Rhodes,1997, pp. 1043–1046.
9. K. P. Tripathi, "A Comparative study of Biometric technologies with reference to Human computer Interface", International Journal of Computer Application, vol. 14 , No. 5 January 2011, pp.10-15.