# A Comparative Study of Biometric Technologies with Reference to Human Interface

K P Tripathi
Lecturer (MCA Programme)
Bharati Vidyapeeth Deemed University
Institute of Management, Kolhapur, India

## ABSTRACT
Traditionally the use of biometric devices has improved our ability to provide authenticated access to physical installations. Biometrics is the use of a person's unique physiological, behavioral, and morphological characteristic to provide positive personal identification. Biometric systems that are currently available today examine fingerprints, handprints, iris and retina patterns, and face. Systems that are close to biometrics but are not classified as such are behavioral systems such as voice, signature and keystroke systems. They test patterns of behavior not parts of the body. Over the next few years, the use of biometrics will continue to grow and become much more commonplace.

Today the core technologies have evolved and the cost of the equipment is going down dramatically due to the integration and increasing processing power. Certain applications of biometric identification technology are now cost-effective, reliable and highly accurate. As a result, there is no technological or financial barrier for stepping from the pilot projects to widespread deployment. This paper is an attempt to highlights the biometric technologies in concern with human interface.

## Keywords
Biometrics, Biometric Identification, Biometric Testing, Biometric Applications

## 1. INTRODUCTION
Biometrics refers to the automatic identification of a person based on his or her physiological or behavioral characteristics. This identification method is preferred over traditional methods involving passwords and personal identification numbers (PINs) for several reasons, including the person to be identified is required to be physically present at the point of identification and/or identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, restricting access to sensitive/personal data is necessary. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of the following:

1. ATMs
2. Cellular phones
3. Smart cards
4. Desktop PCs
5. Workstations
6. Computer networks

PINs and passwords may be forgotten and token-based identification methods such as passports and driver's licenses may be forged, stolen, or lost. Thus, biometric systems of identification are enjoying a new interest. Various types of biometric systems are being used for real-time identification.

The most popular are based on face recognition and fingerprint matching; however, other biometric systems use iris and retinal scans, speech, facial feature comparisons and facial thermograms, and hand geometry. [2] [10]

## 2. BIOMETRIC TECHNOLOGY
Biometric technologies are defined as, "automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic". The term 'automated methods' refers to three basic methods in concern with biometric devices:

1. A mechanism to scan and capture a digital or analog image of a living personal characteristic;
2. Compression, processing and comparison of the image to a database of stored images; and
3. Interface with applications systems.[1]

### 2.1 Advantages of Biometrics:
1. Biometric traits cannot be lost or forgotten (while passwords can).
2. Biometric traits are difficult to copy, share and distribute (passwords can be announced in crackers' websites).
3. They require the person being authenticated to be present at the time and point of authentication. [1]

### 2.2 Biometric Features
1. Uniqueness: an identical trait won't appear in two people.
2. Universality: occur in as many people as possible.
3. Performance: don't change over time.
4. Measurability: measurable with simple technical instruments.
5. User friendliness: are easy and comfortable to measure. [1]

### 2.3 Identification vs. Verification
Sometimes verification and identification are interpreted as similar terms but they have two distinct meanings. Identification occurs when an individual's characteristic is being selected from a group of stored images. Identification is the way the human brain performs most day-to-day identifications. For example, if a person encounters a familiar individual, the brain processes the information by comparing what the person is seeing to what is stored in memory.

Biometric devices that implement identification techniques can be quite time consuming. Often anywhere from 5 to 15 seconds or more are required in identifying the appropriate individual. In many cases, verification is used to authenticate a user's identity. A biometric device that uses verification requires that the individual make a claim of identity by presenting a code. The matching formula or algorithm then needs only to compare the live and enrolled images of the user's characteristic. [1]

## 2.4 Physiological vs. Behavioral

When referring to a biometric technology, it is important to distinguish between physiological and behavioral human characteristic.

A physiological characteristic is relatively a stable human physical characteristic, such as a fingerprint, iris pattern, or blood vessel pattern on the back of the eye. This type of measurement is unchanging and unalterable without significant duress.
Alternatively, a behavioral characteristic is a reflection of an individual's psychological makeup, although physical traits, such as size and gender, have a major influence. Some of the examples of behavioral traits used to identify individuals include: Keystroke dynamics, and speech identification and/or verification. [1]

Today, we have the technology and processing power to employ advanced, cost-effective, and much more accurate biometric identification systems. There are two different ways to resolve a person's identity: verification and identification. Verification (am I whom I claim to be?) involves confirming or denying a person's claimed identity. In identification, one has to establish a person's identity (who am I?). Each approach has its own complexities and could probably be solved best by a specific biometric system, including the following: [2]

### 2.4.1 Physical Biometrics:

1. Fingerprint: Analyzing fingertip patterns
2. Facial recognition/face location: Measuring facial characteristics
3. Hand geometry: Measuring the shape of the hand
4. Iris scan: Analyzing features of colored ring of the eye
5. Retinal scan: Analyzing blood vessels in the eye
6. Vascular patterns: Analyzing vein patterns
7. DNA: Analyzing genetic makeup
8. Biometric data watermarking (which is really a method rather than a physical attribute) is used to store/hide biometric information. [5]

### 2.4.2 Behavioral Biometrics:

1. Speaker/voice recognition: Analyzing vocal behavior
2. Signature/handwriting: Analyzing signature dynamics
3. Keystroke/patterning: Measuring the time spacing of typed words.

Fingerprint recognition is one of the oldest biometric technologies, and its application in criminal identification, using eyesight, has been in use for more than 100 years. Today, computer software and hardware can perform the identification significantly more accurately and rapidly. Fingerprint technology is among the most developed biometric technologies, and its price is cost-effective enough to make its way into public use. [6]
Facial recognition is among the newer technologies for commercial applications. Two-dimensional face recognition systems impose a high misidentification rate; however, newer three-dimensional facial recognition is showing significant improvements and much better accuracy. [10]

Iris scanning is among the most accurate of all biometric technologies with very little overlap between acceptance and rejection curves. This system type is expensive and is recommended for very high security requirements. Signature recognition is becoming increasingly popular, and the dynamic recognition of relative pen speeds and pressures has significantly improved the accuracy of this system. This technology is also cost-effective for smaller budgets. [5]

## 2.5 Common Biometric Features used for Authentication

**Table 1: List of Biometric Features**

| 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 |

# 3. HOW DOES BIOMETRICS WORK?

Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system. [6]

**1. Enrollment:** The process by which a user's biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system is called *enrollment*. Subsequent verification and identification attempts are conducted against the template(s) generated during enrollment.

**2. Presentation:** *Presentation* is a process by which user provides biometric data to an acquisition device-the hardware used to collect biometric data. Depending on the biometric system, presentation may require looking in the direction of a camera, placing a finger on a platen, or reciting pass phrase.

**3. Biometric data:** The biometric data users provide in an unprocessed image or recording of a characteristic. The unprocessed data is also referred to as *raw biometric data* or as a *biometric sample*. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrollment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus Biometric systems do not store biometric data-systems use data for template creation. Enrollment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier, and then

provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction.

**4. Feature extraction:** The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template as called *feature extraction.* Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features. For example, voice-scan technologies generally filter certain frequencies and patterns, and finger-scan technologies often thin ridges present in a fingerprint image to the width of a single pixel. Since quality of feature extraction directly affects a system's ability to generate templates, it is extremely important to the performance of a biometric system.

**Table 2: Characteristic Features of Biometric Technologies**

| 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 |

**Figure 1: General Biometric System**

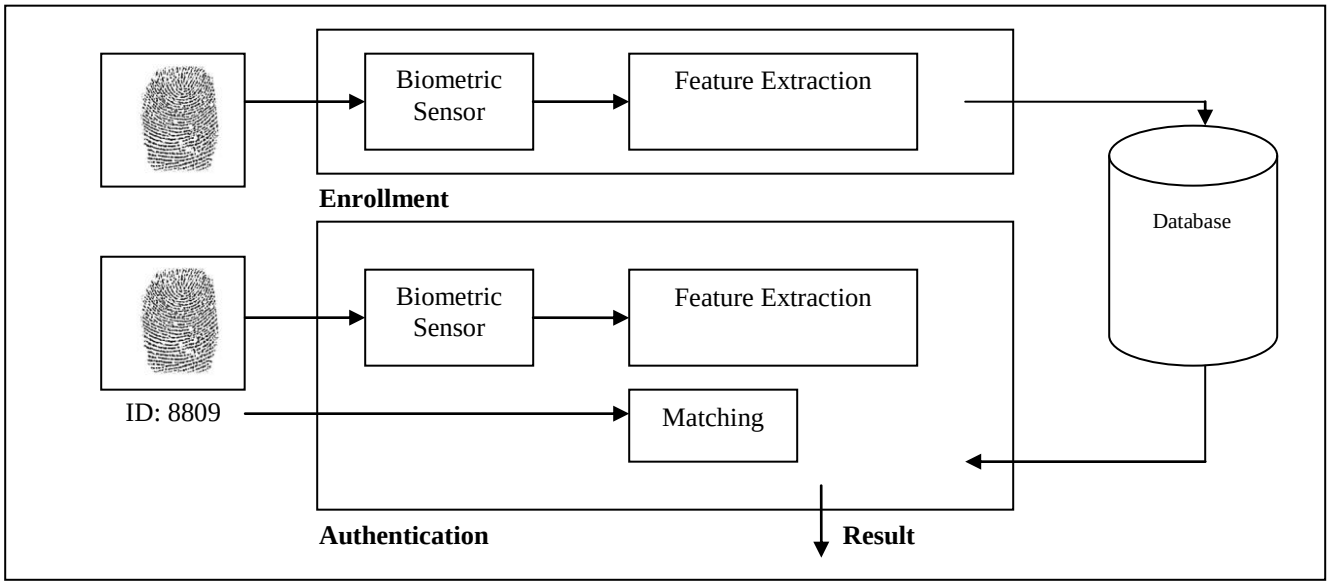


**Table 3: Comparison between Biometric Techniques**

| Biometrics | Universality | Uniqueness | Performance | Collectability | Performance | Acceptability | Circumvention |
|---|---|---|---|---|---|---|---|
| **Retina** | H | H | M | L | H | L | H |
| **Face** | H | L | M | H | L | H | L |
| **Finger print** | M | H | H | M | H | M | H |
| **Hand geometry** | M | M | M | H | M | M | M |
| **DNA** | H | H | H | L | H | L | L |

**H-High, M-Medium, L-Low**

# 4. BIOMETRIC TECHNOLOGIES

## 4.1 Fingerprint Identification

Fingerprint identification is the method of identification using the impressions made by the minute ridge formations or patterns found on the fingertips. No two persons have exactly the same arrangement of ridge patterns (even identical twins), and the patterns of any one individual remain unchanged throughout life.

## 4.2 Hand Geometry

When measuring hand geometry biometrics, three-dimensional image of the hand is taken and the shape and length of fingers and knuckles are measured. Hand geometry has been in use for many years in various applications, predominantly for access control. The technology does not achieve the highest levels of accuracy but it is convenient and fast use. On the capture process a user places a hand on the reader, aligning fingers with specially positioned guides. Cameras, positioned on above and on the side of hand capture images from which measurements are taken at selected points.

## 4.3 Face Recognition

Face recognition technologies analyze the unique shape, pattern and positioning of facial features. The face is natural biometric because it is a key component in the way we humans remember and recognize each other. Face recognition is very complex technology and largely software based. Artificial intelligence is used to simulate human interpretation of faces. The problem with human face is that people do change over time; wrinkles, beard, glasses and position of the head can affect the performance considerably. To increase the accuracy and adapt to these changes some kind of machine learning has to be implemented. There are essentially two methods of capture: using video or thermal imaging. Video is more common as standard video cameras can be used. The precise position and angle of the head and surrounding lightning conditions may affect the system's performance.

## 4.4 Finger Geometry

Finger geometry biometric is very closely related to hand geometry. The use of just one or two fingers means more robustness, smaller devices and even higher throughput. Two variations of capture processes are used, first being similar to hand geometry presented above. The second technique requires the user to insert a finger into a tunnel so that three-dimensional measurements of the finger can be made.

## 4.5 Palm Scanning

Palm biometrics is close to finger scanning and in particular AFIS technology. Ridges, valleys and other minutiae data are found on the palm as with finger images. Main interest in palm biometrics industry is law enforcement as latent images - "palmprints" - found from the crime scenes is equally useful as latent fingerprints. Certain vendors are also looking at the access control market and hope to follow the footsteps of finger scanning. [1]

## 4.6 Signature

Signature is one of the most accepted methods of asserting ones identity. As we normally use it the signature is scrutinized as a static trace of pen on the paper. In digitized form the static geometry of signature is not enough to ensure the uniqueness of its author.

Signature biometrics often referred to dynamic signature verification (DSV) and look at the way we sign our names. The dynamic nature differentiates it from the study of static signatures on paper. Within DSV a number of characteristics can be extracted from the physical signing process. Examples of these behavioral characteristics are the angle of the pen is held, the time taken to sign, velocity and acceleration of the tip of the pen, number of times the pen is lifted from the paper. Despite the fact that the way we sign is mostly learnt during the years it is very hard to forge and replicate.

Signature data can be captured via a special sensitive tablet or pen, or both. On some simpler cases equipment found rather cheap from normal computer stores can be used. A variation on these techniques has been developed and is known as acoustic emission. This measures the sound that a pen makes against paper. Because of the behavioral nature of signature, more than one signature enroll is needed so that the system can build a profile of the signing characteristic.

## 4.7 Voice Scanning

Voice biometrics examines particularly the sound of the voice. Therefore it has to be distinguished as a technology from the also very much researched field of speech recognition. On the following these few closely related but different terms are explained. Speech recognition can be defined as a system that recognizes words and phrases that are spoken. Voice identification has been derived from the basic principles of speech recognition. [1]

# 5. BIOMETRIC TESTING

User acceptance is an important issue to consider when selecting a biometric system for employees to use on a regular basis. The following is a general user acceptance list in descending order, from the most accepted to the least accepted:

1. Iris scan
2. Keystroke/patterning
3. Signature/handwriting
4. Speaker/voice recognition
5. Facial recognition/face location
6. Fingerprint
7. Hand geometry
8. Retinal scan

The identifying power of a particular biometric encompasses has two terms:

1. False Rejection Rate (FRR), or a Type I Error
2. False Acceptance Rate (FAR) or a Type II Error, and
3. Crossover Error Rate (CER).

For example, if the false acceptance rate threshold is increased to make it more difficult for impostors to gain access, it also will become harder for authorized people to gain access. As FAR goes down, FRR rises.

On the other hand, if the false acceptance threshold is lowered as to make it very easy for authorized users to gain access, then it will be more likely that an imposter will slip through. Hence, as FRR goes down, FAR rises. The CER is a percentage rating of Type I versus Type II errors. A lower CER rate means better accuracy. [4][7]

## 6. PERFORMANCE

The following are used as performance metrics for biometric systems:

1. **False accept rate or false match rate (FAR or FMR)**: The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

2. **False reject rate or false non-match rate (FRR or FNMR)**: The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

3. **Receiver operating characteristic or relative operating characteristic (ROC)**: The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the *Detection error trade-off (DET),* which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

4. **Equal error rate or crossover error rate (EER or CER)**: The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

5. **Failure to enroll rate (FTE or FER)**: The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

6. **Failure to capture rate (FTC)**: Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

7. **Template capacity**: The maximum number of sets of data which can be stored in the system.

## 7. BIOMETRIC APPLICATIONS

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. In automobiles, biometrics can replace keys with keyless entry devices.

1. **Government** - Passports, national identification (ID) cards, voter cards, driver's licenses, social services, and so on.

2. **Transportation** - Airport security, boarding passes, and commercial driver's licenses.

3. **Healthcare** - Medical insurance cards, patient/employee identity cards.

4. **Financial** - Bankcards, ATM cards, credit cards, and debit cards.

5. **Security** - Access control and identity verifications, including time and attendance.

6. **Public justice and safety** - Prison IDs, county probation offices' use for identification of parolees, county courthouses' use for ID systems.

7. **Education** - Student/teacher identity verification and access control. Biometrics is now being implemented in large-scale ID systems around the globe. Many new passport and national ID card systems use some type of biometric encoded in a bar code or smart chip.

8. **Driver's licenses** - Technologies being recommended by American Association of Motor Vehicle Administrators (AAMVA), the organization that oversees DMV standards, include biometrics and two-dimensional bar codes. Georgia, North Carolina, Kentucky, and others already utilize biometrics on their respective state driver's licenses.
9. **Access control** - one of the most traditional of applications for biometrics, accessing buildings, offices, cars, and even homes are applications for biometric implementations.

10. **Time and attendance** - a growing number of work places are implementing biometric technologies to allow employees to "punch the clock". This prevents employees from "buddy punching" and ensures that employee productivity actually matches up with recorded times.

11. **Law enforcement** - while this is a substantial section of the market for fingerprint scanners, the hardware is often different than commercially targeted hardware, geared for collection of a large number of one individual. There are also a few tests being done now in prisons where biometrics are used to identify and track prisoners at high security facilities. [2][3][4]

## 8. DISADVANTAGES

A biometric authentication system seems to be an excellent solution to authentication problems; however biometric authentication has some weaknesses:

1. **Education required:** While an increasing number of available technologies are "plug and play", they still require some user education. Users need to know how to position their finger, face, and eye. To be clearly read.

Additionally, implementers will need training on proper installation and maintenance of biometric systems.

2. **Expensive:** While there are several models of fingerprint, voice, and signature verification available in the $100 range, a majority of technologies are still closer to the $500 mark. Unless biometrics can get below the cost of password administration costs, business will get below the cost of password administration costs, business will not chose to implement.

3. **Affected by environment and disease:** It is not the case that your fingerprints, face, or voice remain constant from day to day, small fluctuations (cold or moist hands for fingerprint scanners, different ambient lighting for face recognition, and background noise for voice authentication) can block the devices. Setting the sensitivity lower makes the product more forgiving but increases the odds of a false positive a faker logging on as someone else. Higher sensitivity means greater security, but it also means that an authorized user may be erroneously rejected.

4. **Harmful:** The method of obtaining a retinal scan is personally invasive – a laser light (or other coherent light source) must be directed through the cornea of the eye and uses an infrared light source to highlight the biometric pattern. This can harm an individual's eye. [2]

## 9. CONCLUSION

Biometric authentication refers to automated methods of identifying or verifying the identity of a living person in real time based on a physical characteristic or personal trait. The phrase, "living person in real time" is used to distinguish biometric authentication from forensics, which does not involve real-time identification of a living individual.

Biometrics is, essentially, based on the development of pattern recognition systems. Today, electronic or optical sensors such as cameras and scanning devices are used to capture images, recordings or measurements of a person's 'unique' characteristics. This digital data is then encoded and can be stored and searched on demand, via a computer. Such biometric search is not only very rapid, it is also a process that is accepted globally in establishing forensic evidence in a law court. Consequently, there are numerous forms of biometrics now being built into technology platforms.

## 10. REFERENCES

[1] Arpita Gopal, Chandrani Singh, e-World : Emerging Trends in Information Technology, Excel Publication, New Delhi (2009).
[2] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer
[3] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of Fingerprint Recognition, Springer
[4] John Chirillo, Scott Blaul, Implementing Biometric Security, Wiley Red Books
[5] John Woodward, Nicholas M. Orlans, Peter T. Higgins, Biometrics, Tata McGraw Hill
[6] Lakhmi C. Jain, Intelligent Biometric Techniques in Fingerprint and Face recognition
[7] Nalini K. Ratha, Andrew Senior and Ruud M. Bolle,"Automated Biometrics". IBM Thomas J. Watson Research Center, PP 1-10
[8] Paul Reid, Biometrics for Network Security, Prentice Hall of India.
[9] Roger Clarke, "Biometrics And Privacy"
[10] Rula Abu Samaa'n,"Biometrics Authentication Systems", April 2003, PP 1-2.
[11] Vicki Koerper, "Biometrics: A Brief Introduction", March 10,1998

## 11. AUTHORS BIOGRAPHY

**K P Tripathi** received his M.C.A., degree from Shivaji University, Kolhapur in June 2006 and M.B.A. degree from YCMOU, Nashik in Feb. 2010. He is working as Lecturer in M.C.A. Department, Bharati Vidyapeeth Deemed University Institute of Management, Kolhapur, India. He has presented 5 papers in National Conference and 4 papers in International Conference and 4 in International Journals. His areas of interest include Information Technology, Computer Organization & Architecture, and Mobile Communication.