Biometrics

Anubha Singh

The word "biometrics" is derived from the Greek words 'bios' and 'metric' ; which means life and measurement respectively. This directly translates into "life measurement".

General science has included biometrics as a field of statistical development since the early twentieth century. A very good example is the statistical analysis of data from agricultural field experiments comparing the yields of different varieties of wheat. In this way, science is taking a life measurement of the agriculture to ultimately determine more efficient methods of growth.

Biometrics technologies measure a particular set of a person's vital statistics in order to determine identity.

Biometrics in the high technology sector refers to a particular class of identification technologies. These technologies use an individual's unique biological traits to determine one's identity. The traits that are considered include fingerprints, retina and iris patterns, facial characteristics and many more.

Types of Biometrics

There are basically two types of biometrics:

1. **Behavioral biometric definition** : Behavioral biometrics basically measures the characteristics which are acquired naturally over a time. It is generally used for verification.

Examples of behavioral biometrics include:

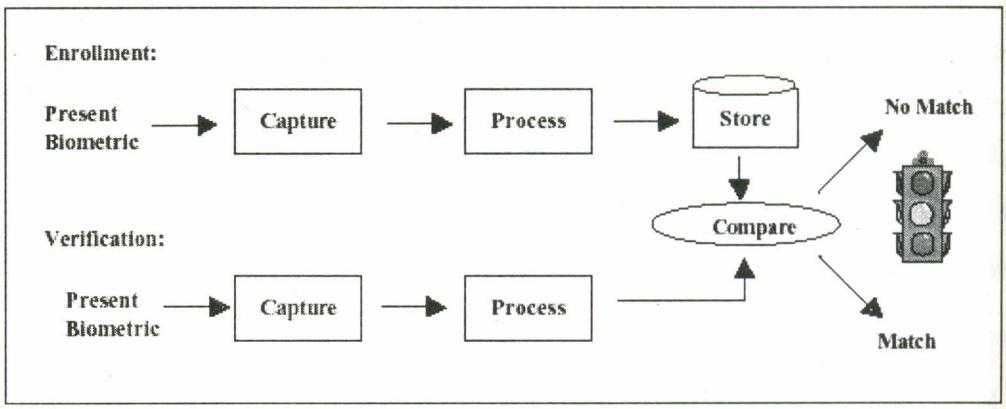
- Speaker Recognition - analyzing vocal behavior
- Signature - analyzing signature dynamics
- Keystroke - measuring the time spacing of typed words

2. **Physical biometric definition** : Physical biometrics measures the inherent physical characteristics on an individual. It can be used for either identification or verification.

Examples of physical biometrics include:

- Bertillonage - measuring body lengths (no longer used)
- Fingerprint - analyzing fingertip patterns
- Facial Recognition - measuring facial characteristics
- Hand Geometry - measuring the shape of the hand
- Iris Scan - analyzing features of colored ring of the eye
- Retinal Scan - analyzing blood vessels in the eye
- Vascular Patterns - analyzing vein patterns
- DNA - analyzing genetic makeup

Working principle: Biometric devices consist of a reader or scanning device software that converts the gathered information into digital form, and a database that stores the biometric data with comparison with existing records.



Biometric History - How did it start?

Biometric history indicates that the science did not originate at a single place. People all over the world were using the basics for mainly identifying individuals from each other. We'll explain about biometric history in brief over the next few paragraphs.

The history of biometrics dates back to a long time. Possibly the most primary known instance of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer *Joao de Barros.*

Barros wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink so as to differentiate the young children from one another. This is one of the most primitive known cases of biometrics in use and is still being used today. In the 1890s, an anthropologist and police desk clerk in Paris, *Alphonse Bertillon*, decided to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study.

Bertillon developed a technique of multiple body measurements which later got named after him - **Bertillonage**. His method was then used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one. After the failure of Bertillonage, the police started using finger printing, which was developed by *Richard Edward Henry* of Scotland Yard, essentially reverting to the same methods used by the Chinese for years. (which still is going strong !)

Biometric history in the recent past (three decades) has seen drastic advancements and the technology has moved from a single method (fingerprinting) to more than ten prudent methods. Companies involved with new methods have grown into the hundreds and continue to improve their methods as the technology available to them also advances. Prices for the hardware required continue to fall making systems more feasible for low and mid-level budgets and thus making this more adaptable in small businesses and even households.

Biometrics Fingerprint : Most used biometrics technology

Lets understand what "fingerprinting" is, before we start on with biometrics fingerprint technology. Fingerprinting basically means to take an image (either using ink or a digital scan) of an individual's fingertips and then store or records its characteristics.

The whorls, arches, and loops are what make up these characteristics of a fingertip. These are recorded along with the patterns of ridges, furrows, and

minutiae. This information may then be processed or stored as an image or an encoded computer algorithm to be compared with other fingerprint recor

For fingerprint Recognition look at:

- Friction ridges.
- Core
- Crossover.
- Delta.
- Island
- Ridge Ending.
- Pore.

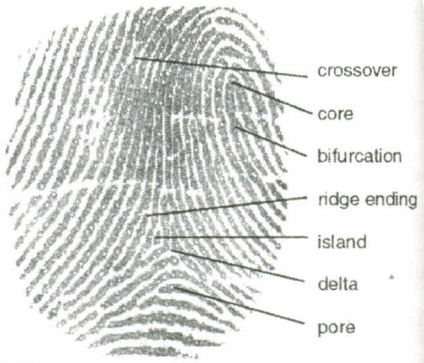
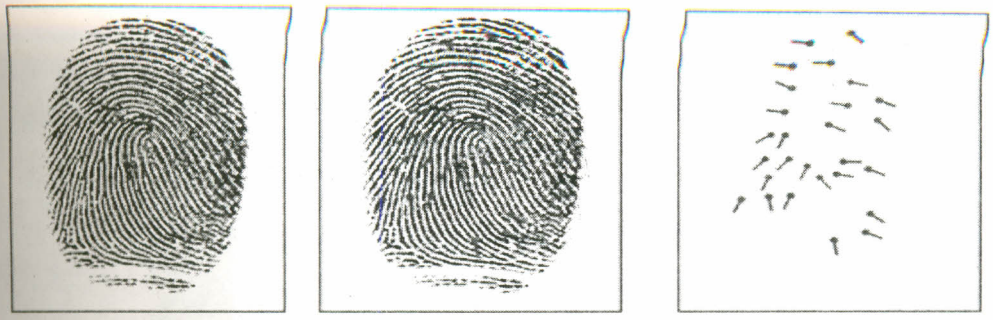


Figure 1

Biometrics Fingerprint Technology - The Process

The user places his finger against a small biometrics fingerprint reader(or biometrics fingerprint scanner) surface (optical or silicon) usually of about 2 inch square size. This biometrics fingerprint reader is attached to a computer and takes the information from the scan and sends it to the database. There it is compared to the information stored within. The user is usually required to leave his finger on the reader for less than 5 seconds during which time the identification or verification takes place. To prevent fake fingers from being used, many biometrics fingerprint systems also measure blood flow, or check for correctly arrayed ridges at the edges of the fingers

Finger Image



Finger Image Finger Image + Minutiae Minutiae

Basics of biometric facial recognition:

Biometric Facial recognition analyzes the characteristics of an individual's face images captured through a digital video camera. It records the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are stored in a database and used as a comparison when a user stands before the camera.

Biometric facial recognition has been widely, touted as a fantastic system for recognizing potential threats (whether terrorists, scam artists, or known criminals) but so far it has been unproven in high-level usage. It is currently used in verification only systems with a good deal of success.

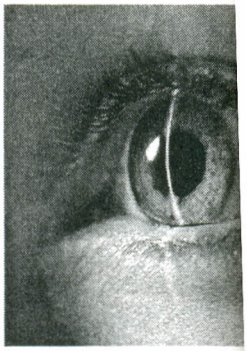
Biometric Facial Recognition - The Process:

User faces the camera, standing about two feet from it. The system will locate the user's face and perform matches against the claimed identity on the facial database. It is possible that the user may need to to move and reattempt the verification based on his facial position. The system usually gives a decision in less than 5 seconds.

To prevent a fake face or mold from faking out the system, many systems now require the user to smile, blink, or otherwise move in a way that is human before verifying.

Biometric Iris Scanning : Using Eyes to Identify

Basics of biometric iris scanning:



Iris scanning analyzes the features that exist in the coloured tissues surrounding the pupil which has more than 200 points that can be used for comparison, including rings, furrows and freckles. The scans use a regular video camera and can be done from further away than a retinal scan. It will work perfectly fine through glasses and in fact has the ability to create an accurate enough measurement that it can be used for identification purposes, and not just verification.

Biometric Iris Scanning - The Process:

The person alligns himself so that he is able to see his own eye's reflection i the iris scanning device. The user may be able to do this from up to 2 feet awa or may need to be as close as a couple of inches depending on the device Verification time is generally less than 5 seconds, though the user will onl need to look into the device for a couple moments.

To prevent a fake eye from being used to fool the iris scanning systems, iris scanners may vary the light shone into the eye and watch for pupil dilation also.

Retinal Biometrics : Using the Eyes to Identify

Basics of Retinal Biometrics:

Retinal biometrics involves the scanning of retina and analysing the layer of blood vessels at the back of the eye. Retinal scanning involves using a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. It does require the user to remove glasses, place their eye close to the device, and focus on a certain

point. Whether the accuracy can outweigh the public discomfort is yet to be seen.

Retinal Biometrics - The Process:

The user looks through a small opening in the retinal biometrics device at a small green light. The user must keep their head still and eye focused on the light for several seconds during which time the device will verify his identity. This process takes about 10 to 15 seconds total.

There is no known way to replicate a retina, and a retina from a dead person would deteriorate too fast to be useful, so no extra precautions have been taken with retinal scans to be sure the user is a living human being.

Voice Recognition Biometrics: Identification based on voice frequencies

Voice recognition biometrics requires the user to speak into a microphone. What he speaks can be his password or an access phrase. Verification time is approximately 5 seconds.

To prevent recorded voice use, most voice recognition devices require the high and low frequencies of the sound to match, which is difficult for many recording instruments to recreate well. Also, some devices generate random number sequences for each verification.

Signature Verification

Principle: The movement of the pen during the signing process rather than the static image of the signature. Many aspects of the signature in motion can be studied, such as pen pressure, the sound the pen makes.

Advantages of Biometrics : Why opt for biometric technology?

Biometrics allows you to replace "what you have" and "what you know" security adages with the all important "who you are" byword, hence contibuting one of the most substial benefits to the security arena.

Advantages of biometrics will help in your quest to curb the "Why Biomterics" question. We have enlisted some of the most sought after advantages of biometrics for you;

Advantages of Biometrics :

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. For e.g.Minimise the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. Prevent unauthorised use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

Disadvantages of BIOMETRICS:

- The finger print of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication.
- It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there there are too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time
- For people affected with diabetes, the eyes get affected resulting in differences.
- Biometrics is an expensive security solution.