Introduction

What is biometrics?

A biometric is any human feature that can be measured and used for automated or semi-automated identification. Common examples are **fingerprints, iris patterns, and facial patterns**; less well-known biometrics include **ear** geometry, body odour (**smell**) and **gait** (the body movement while walking).

In different organizations like financial services, e-commerce, telecommunication, government, traffic, health care the security issues are more and more important. It is important to verify that people are allowed to pass some points or use some resources. The security issues are arisen quickly after some crude abuses. For these reason, organizations are interested in taking **automated identity authentication** systems, which will improve customer satisfaction and operating efficiency.

The authentication systems will also save costs and be more accurate that a human being. (Jain et al., 2000) Basically there are three different methods for verifying identity:

(i) possessions, like cards, badges, keys;

(ii) knowledge, like userid, password, Personal Identification Number

(iii) biometrics like fingerprint, face, ear.

The word "biometrics" is derived from the Greek words 'bios' and 'metric' ; which means life and measurement respectively. This directly translates into "life measurement". These life measurement technologies use an individual's unique biological traits to determine one's identity.

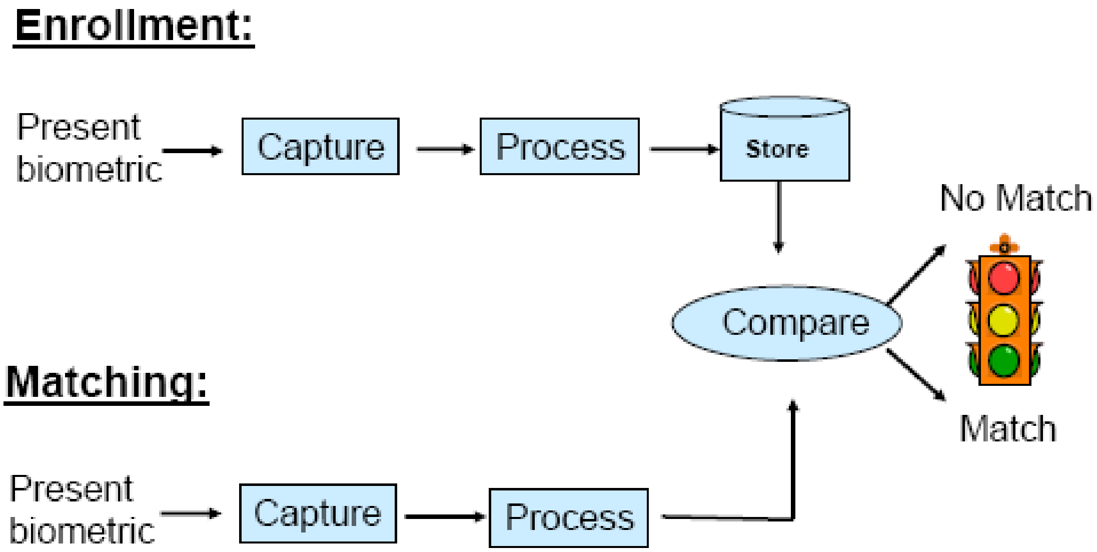


Fig 1 : biometric system

- **ENROLLMENT**

-Adding biometric information to a data file. It can include s screen for duplicates in database.

- **IDENTIFICATION**

-Matching against many records.(1:N)

- **VERIFICATION**

-Matching against a single record.(1:1)

Origin of Biometrics:

Finger printing being used in China in the 14th century. After14th century, In the 1890s, an anthropologist and police desk clerk in Paris, ***Alphonse* *Bertillon*,** decided to fix the problem of identifying convicted criminals. Bertillon developed a technique of multiple body measurements which later got named after him **- Bertillonage**.

TYPES OF BIOMETRICS:

There are basically two types of biometrics:

3.1. PHYSICAL BIOMETRICS.
3.2 .BEHAVIORAL BIOMETRICS.

PHYSICAL BIOMETRICS 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:

1. Bertillonage - measuring body lengths (no longer used)
2. Fingerprint - analyzing fingertip patterns
3. Facial Recognition - measuring facial characteristics
4. Hand Geometry - measuring the shape of the hand
5. Iris Scan - analyzing features of colored ring of the eye
6.Retinal Scan - analyzing blood vessels in the eye
7.DNA - analyzing genetic makeup

BEHAVIORAL BIOMETRICS 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:

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

PHYSICAL BIOMETRICS:

1. BERTILLONAGE BIOMETRIC PROCESS:

This process first developed by **alphonse bertillon** in 1890. He is measured the people based on the following characters. There are include the **height, length, and breadth of the head, the length of different fingers.**

HISTORY:

After 1890 **bertillonage method** was help to identify the criminals. . Bertillon based his system does. The system was a success, identifying hundreds of repeat offenders, and was used world-wide until 1903, when two identical (within the tolerances) measurements were obtained for two different persons at the Fort Leavenworth prison.so, the bertillonage biometric method goes to failure.

EVALUATION RESULTS:

Non-unique measurements allowed for multiple people to have the same results, reducing the usefulness of this method. Also, the time involved to measure a subject was prohibitive for uses other than prison records

2 FINGER PRINT RECOGNITION:

The uniqueness of fingerprints is due to the series of ridges and furrows on the fingers. The pattern of the ridges and furrows is identified using the Henry Classification The three basic classifications for fingerprints are arch, loop, and whorl. Other unique points on the finger called minutiae points occur at ridge bifurcation or end points. The other measurements pattern type, Ridge counts, Distance between ridges, core, pores.

PROCESS:

Fingerprint matching techniques fall into one of two categories: minutae-based and correlation-based. **Minutae-based** matching maps the location of minutiae points on the finger. Minutae-based matching also does not take into account the ridges and furrows of the finger. The **correlation-based** method measures the unique points of the fingerprint relative to a registration point. All fingerprint matching based on minutiae is made difficult by different sized minutiae patterns. Also, the ridge structure cannot be totally defined by the minutiae.

HISTORY:

Finger printing was first used in a fashion in 14th century in china.In the later half of the 19th century, Richard Edward Henry of Scotland yard developed a method of categorizing and identifying marks in fingerprint

USES:

Fingerprint scanning is used in Number of banks and financial organisations and ATM. Entry devices for building door locks and computer network access.

MERITS:

- ❖ It require small storage space for the biometric template and also reducing the size of the database memory.
- ❖ Long time use-proven and high accuracy

- ❖ General ease and speed of use
- ❖ Supports both 1:1 verification applications.
- ❖ Numerous vendor selections.

DEMERITS:

- ➢ It is easy to fool by criminals by mould such as malleate plastic and gummy finger.
- ➢ Small percentage of population have poor prints due to injury, age, disease, or Occupation.
- ➢ It requires physical contact with sensor.

3. FACE RECOGNITION:

BASICS:

In 1960 the **Woodrow W. Bledsoe** to create the very first semi-automated face recognition system. They developed a 21 point check for the machines to identify and calculate the ratios between these facial structures. The 21 points included very intricate features of the face such as thickness of the lips and color of the hair. In the 1980's facial recognition systems were beginning to become available in commercial retail.

PROCESS:

This type of biometrics does not require anyone to physically touch a machine, just stand within a designated space. The picture is then analyzed by "comparing distances between things like the eyes, nose, mouth, and jaw edges" of a person.

USES:

Facial recognition system mainly used for averting terrorist crimes. It is already in use in many law enforcement areas.Softwares have also been developed for computer networks and automated bank tellers that use facial biometrics for user verification purpose.

MERITS:

- ❖ Identify criminals in entrance of airport,ATM,shops.
- ❖ 3D face scans, Identify the identical twins.
- ❖ Terrorist watch,surveillance,prisoner management

DEMERITS:

- ➢ Non instrusiveness, Irritation of light
- ➢ Some times affected by eyeglass.
- ➢ Face expression, position and Facial hairs.
- ➢ Appearance change overtime.
- ➢ Age and sex.

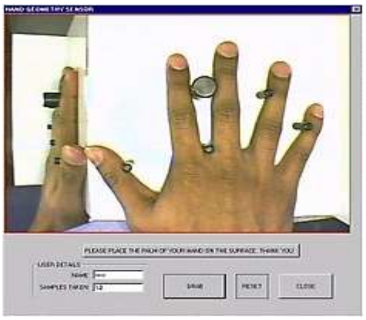
4. HAND RECOGNATION:

BASICS:

Hand scanning involves the measurement and analysis of the shape of one's hand. Various traits of the hand, such as finger length, width and curvature, as well as unique features may be used for identification Another type of biometric scan can be done to identify the dorsal venous network of the hand. This essentially shows the blood vessels on the back of the hand and may be another useful factor for verification.

PROCESS:

Hand geometry scan require that users place their hands onto a surface with 5 pegs. This aligns the hand so that the scanner can get a consistent reading on each scan. The scan is then compared to the database for verification.

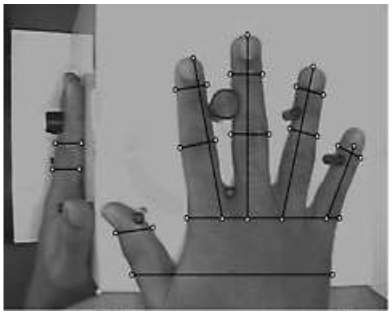


PLEASE PLACE THE PALM OF YOUR HAND ON THE SURFACE. THANK YOU

USER DETAILS

NAME:

SAMPLES TAKEN: 12



HISTORY:

Hand scanning can be termed as a forefather of modern biometrics by virtue of a 20 yr history of live applications.

USES:

Biometric hand scanning systems are employed at over 8,000 locations, including the Colombian legislatures, San Francisco International Airport, day care centers, a sperm bank, welfare agencies, hospitals.

MERITS:

- It is easy to use, fast and high public acceptance.
- It is very low failure to Enroll Rate and proven over many years of use.
- Primary applications are physical access and time/attendance.
- It is work well in outdoor environments.
- It is very small and adaptive template.

DEMERITS:

- It's proprietary hardware cost is high.
- Also, while injuries to hands can cause difficulty in using.
- Use only in 1:1 accuracy.
- Donot detect whether a hand is living or not.

5. RETINA RECOGNATION:

Retinal biometrics measures blood vessels patterns at the back of the eye. And the light source is shone through the pupil to iiuminate the retina.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.

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.

HISTORY:

In1930's research suggested that the patterns of blood vessels on the back of the human eye were unique to each individual. The first retina scan device made for commercial use, in 1984.

USES*:*

Retina scan is used high-end security applications, controlling access to areas or rooms in military installations, power plants, and the high risk security areas.

MERITS:

- ❖ Supports both 1:1 verification and 1:N identification
- ❖ Areas or rooms in military installations, power plants.
- ❖ No two retinas will ever be exactly alike.
- ❖ Even after deceased, the blood vessels cannot be imitated since they decay rapidly
- ❖ Fast, accurate scan. Difficulty in fooling

DEMERITS:

- ➢ Generally considered intrusive; uncomfortable user interface.
- ➢ It requires removal of eyeglasses.
- ➢ It capture can take 10 to 15 seconds and not commercially marketed.
- ➢ Consumer's thinking it is potentially harmful to the eye.

6. 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.Measures up to 266 unique factors. It twill work perfectly fine through glass.

PROCESS:

The person alligns himself so that he is able to see his own eye's reflection in the iris scanning device. The machine takes around ten seconds to shine a “low intensity coherent light source” onto the retina to illuminate the blood vessels. 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.

HISTORY:

This technique was originally proposed in 1936 by **ophthalmologist Frank Burch**. In 1987 Aran Safir Leonard Flom and John Daugman to create algorithm for iris recognition.

USES*:*

It can be used for identification purposes, and not just verification. Law enforcement agencies, Lancaster County Prison in Pennsylvania for prisoner identification , The Charlotte/Douglas International Airport in North Carolina and the Flughafen Frankfort Airport.

MERITS:

- ❖ High accurate,very stable over lifetime.
- ❖ It can works through glasses ans contacts and no physical contact required.
- ❖ It not affected by common eye surgeries.
- ❖ It supports both 1:1 verification and 1:N identification applications.

DEMERITS:

- ➢ More memory for data storing.
- ➢ The cost of material is high.
- ➢ It can be affected by some eye diseases(cataracts)
- ➢ It often confused with more invasive retinal scanning.
- ➢ False positive is extremely low and its relative speed.

7. DNA RECOGNITION:

human having 23 pairs of chromosomes.99.7% of an offspring’s DNA is shared with their parents. The remaining .3% of an individuals DNA is variable coding unique to individual ·

PROCESS:

The basic steps of DNA profiling include:

1.Isolate the DNA (sample can originate from blood, saliva, hair, semen, or tissue)

2. Section the DNA sample into shorter segments containing known variable number tandem repeats (VNTRs) identical repeat sequences of DNA

3. Organize the DNA segments by size

4.Compare the DNA segments from various samples

USES:

It make more cost efficient method of identification. Development of DNA sequencing and sample comparison techniques·It used for network security.

MERITS:

It used for identify the forenstic application.they are

- ❖ Murder
- ❖ Rape
- ❖ Identify blood relation

DEMERITS:

- ➢ It take too much of time.
- ➢ Some people did not belive this technique
- ➢ Take too much of cost

BEHAVIORAL BIOMETRICS:

1 SIGNATURE BIOMETRICS:

Biometric signature recognition systems will measure and analyze the physical activity of signing, such as the stroke order, the pressure applied and the speed. Some systems may also compare visual images of signaturesit deals with how it is work rather than visual. This process is also known as typing rhythm or typing pattern.

PROCESS:

The user signs on a tablet or on paper that is laying over a sensor tablet. The device records the signature and compares it to its database. Verification takes about 5 seconds. as a unique verification tool to ascertain several key elements: message authentication, message/data integrity, and non-repudiation (legal aspect of events).

USES:

It is used to Access to documents, contract / agreement execution, acknowledgement of goods or services received, banking services and credit card transaction.

MERITS:

- ❖ It works in conjunction with familiar signing process.
- ❖ It can be used with devices that have built-in graphics components-PDAs, etc.

DEMERITS:

- ➢ People may not always sign in a consistent manner.
- ➢ It can be affected by behavioral factors(stress, distractions, standing/sitting)
- ➢ Best used in 1:1 contexts.
- ➢ While it is easy to copy the image of a signature.

2. SPEAKER RECOGNITION:

BASIC:

The wave patterns in the voice and the measurement of physiological characteristics, such as the nasal passages and vocal chords, as well as the frequency, cadence and duration of the vocal pattern are all included in considering a voiceprint

PROCESS:

The voiceprint is a biometric voice identifier not a recording or a sound file; so an imposter could not record one's words and replay them into the system and get access granted. User speaks into microphone his password or access phrase. Verification time is approximately 5 seconds.

USES:

Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking).

MERITS:

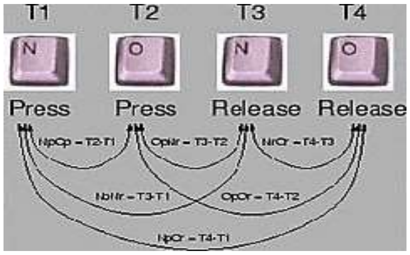
- ❖ Security
- ❖ Accuracy
- ❖ Convenience
- ❖ Shortened Verification/ Speeds
- ❖ Protects Privacy

DEMERITS:

- ➢ Mimic by others.
- ➢ Voice may affected by physical facts.

3 KEYSTROKE IDENTIFICATION:

Keystroke technique factors such as Flight Time (the time it takes to move from one key to another) and Dwell time (the time a person spends on any given key).



PROCESS:

A template is made consisting of the user typing a series of words over several sessions to break up the time. Forced typing over long periods of time can induce fatigue, stress, and other factors, such as simple typing mistakes, which may inhibit the template's accuracy. Once proper calibrated, the template will be easily able to distinguish whether the acceptable user is typing or not by comparing the flight and dwell times to those set on the template.

MERITS:

It is used in the following applications.

- Companies
- Input the signals according to their own rhythmic patterns.

DEMERITS:

- No Time consuming.
- Duplicate by that user than by that of another user.
- Easily identify new acceptable user while in place limits.

COMPARISION OF VARIOUS BIO-METRIC TECHNIQUES:

Comparison of various biometric technologies,(**H**=High, M=Medium, **L**=Low)

Biometrics:	**Universal**	**Unique**	**Permanence**	**Collectability**	**Acceptability**
Face	**H**	**L**	**M**	**H**	**H**
Fingerprint	**M**	**H**	**H**	**M**	**M**
Hand geometry	**M**	**M**	**M**	**H**	**M**
Keystrokes	**L**	**L**	**L**	**M**	**M**
Hand veins	**M**	**M**	**M**	**M**	**M**
Iris	**H**	**H**	**H**	**M**	**L**
Retinal scan	**H**	**H**	**M**	**L**	**L**
Signature	**L**	**L**	**L**	**H**	**H**
Voice	**M**	**L**	**L**	**M**	**H**
Facial thermograph	**H**	**H**	**L**	**H**	**H**
DNA	**H**	**H**	**H**	**L**	**L**

Table 1. The permanence of different biometrics over the time. The best permanence has most 0-symbols and the worst least. (Bromba GmbH, 2003)

DNA	**********
IRIS	******
FINGERPRINT	****
VOICE	***

A biometric system

A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina [1], and the one presented in this thesis, the iris.

Biometric systems work by first **capturing a sample of the feature**, such as recording a digital sound signal for voice recognition, or taking a digital colour image for face recognition. The sample is then **transformed** using some sort of mathematical function into a biometric template. The biometric **template** will provide a normalised, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity. Most biometric systems allow two modes of operation. An **enrolment** mode for adding templates to a database, and an **identification** mode, where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates.

A good biometric is characterised by use of a feature that is; highly unique – so that the chance of any two people having the same characteristic will be minimal, stable – so that the feature does not change over time, and be easily captured – in order to provide convenience to the user, and prevent misrepresentation of the feature.

Iris Recognition

The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. A front-on view of the iris is shown in Figure 1.1. The iris is perforated close to its centre by a circular aperture known as the pupil. The function of the iris is to control the amount of light entering through the pupil, and this is done by the sphincter and the dilator muscles, which adjust the size of the pupil. The average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter [2].

The iris consists of a number of layers, the lowest is the epithelium layer, which contains dense pigmentation cells. The stromal layer lies above the epithelium layer, and contains blood vessels, pigment cells and the two iris muscles. The density of stromal pigmentation determines the colour of the iris. The externally visible surface of the multi-layered iris contains two zones, which often differ in colour [3]. An outer ciliary zone and an inner pupillary zone, and these two zones are divided by the collarette – which appears as a zigzag pattern.

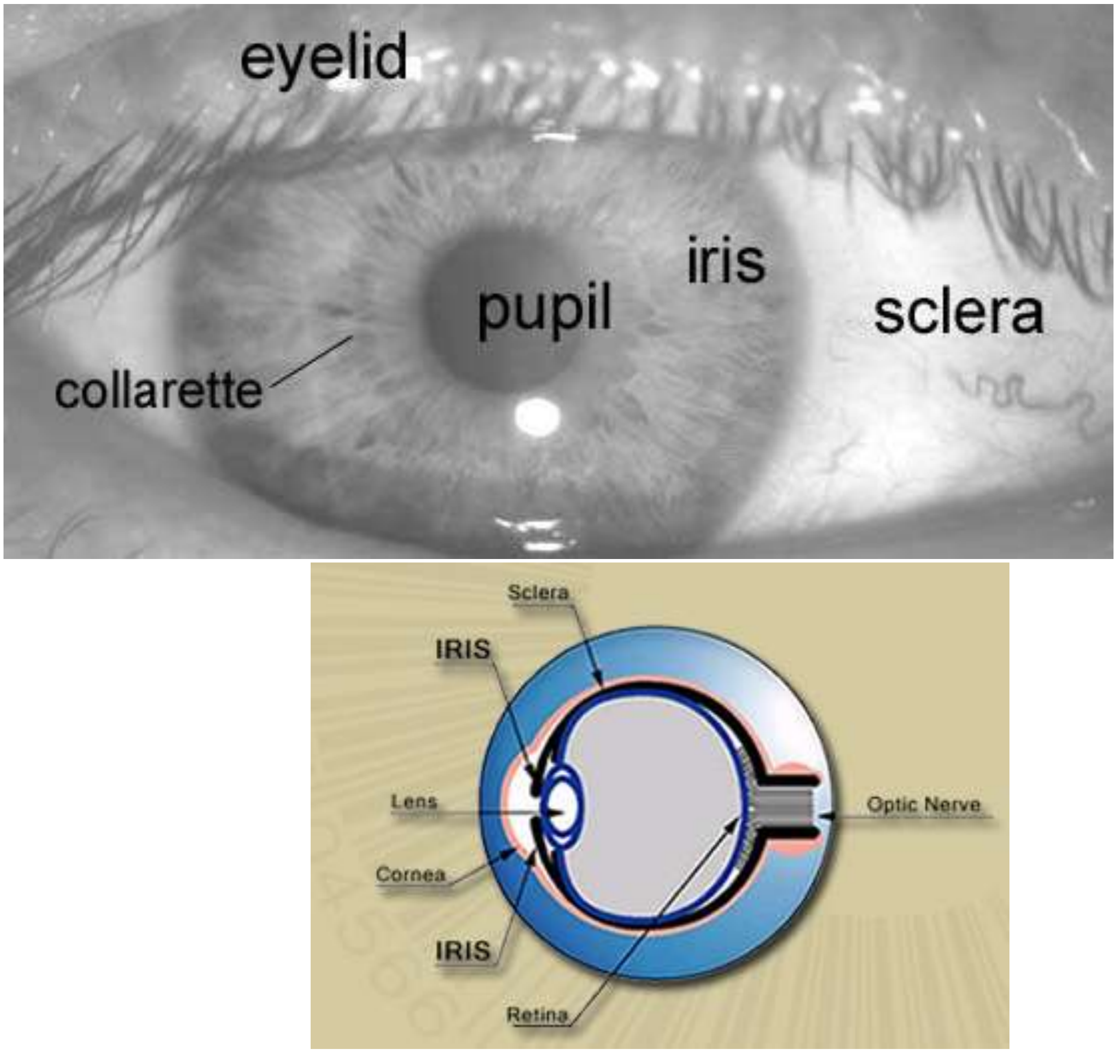


Figure 1.2 – A front-on view of the human eye.

Formation of the iris begins during the third month of embryonic life [3]. The unique pattern on the surface of the iris is formed during the first year of life, and pigmentation of the stroma takes place for the first few years. Formation of the unique patterns of the iris is random and not related to any genetic factors [4]. The only characteristic that is dependent on genetics is the pigmentation of the iris, which determines its colour. Due to the epigenetic nature of iris patterns, the two eyes of an individual contain completely independent iris patterns, and identical twins possess uncorrelated iris patterns. For further details on the anatomy of the human eye consult the book by Wolff [3].

The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitised image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates. When a subject wishes to be identified by an iris recognition system, their eye is first photographed, and then a template created for their iris region. This template is then compared with the other templates stored in a database until either a matching template is found and the subject is identified, or no match is found and the subject remains unidentified.

Although prototype systems had been proposed earlier, it was not until the early nineties that Cambridge researcher, John Daugman, implemented a working automated iris recognition system [1][2]. The Daugman system is patented [5] and the rights are now owned by the company Iridian Technologies. Even though the Daugman system is the most successful and most well known, many other systems have been developed. The most notable include the systems of Wildes et al. [7][4], Boles and Boashash [8], Lim et al. [9], and Noh et al. [10]. The algorithms by Lim et al. are used in the iris recognition system developed by the Evermedia and Senex companies. Also, the Noh et al. algorithm is used in the ‘IRIS2000’ system, sold by IriTech. These are, apart from the Daugman system, the only other known commercial implementations.

The Daugman system has been tested under numerous studies, all reporting a zero failure rate. The Daugman system is claimed to be able to perfectly identify an individual, given millions of possibilities. The prototype system by Wildes et al. also reports flawless performance with 520 iris images [7], and the Lim et al. system attains a recognition rate of 98.4% with a database of around 6,000 eye images.

Compared with other biometric technologies, such as face, speech and finger recognition, iris recognition can easily be considered as the most reliable form of biometric technology [1]. However, there have been no independent trials of the technology, and source code for systems is not available. Also, there is a lack of publicly available datasets for testing and research, and the test results published have usually been produced using carefully imaged irises under favourable conditions.

Fingerprint recognition

A **fingerprint** is an impression of the friction ridges of all part of the finger. A friction ridge is a raised portion of the ***epidermis*** on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal papillae".

To the left is a macro shot of a palm and the base of several fingers; as seen here, debris can gather between the ridges. To the right is the fingerprint created by that friction ridge structure.

It is estimated that 5% of people are not able to deliver a reliable fingerprint, either for temporary reasons (e.g. calloused or dirty fingers) or for permanent reasons (e.g. eczema).

In the tests conducted by the National Physical Laboratory in the UK , the best-performing fingerprint recognition systems, had false rejection rates of approximately 6 in 100 at a false acceptance rate of 1 in 1000 . independent tests in the US (known as FpVTE), showed false rejection rates of 6 in 1000 for a false acceptance rate of 1 in 1000. Results depend on the testing conditions, the quality of enrolled samples and many other factors.

The IAFIS system in the U.S is the largest deployment of biometrics worldwide; it includes 47 million subjects in its criminal master file. In Europe databases of fingerprints are much smaller (for example police in the UK have only 4 million records stored). Even excluding IAFIS, fingerprint recognition held an estimated 48% of the market. The EURODAC database holds 250000 fingerprints of asylum seekers. The use of this database has allowed the identification of some 7% duplicate requests for asylum throughout Europe.

The state of New York has over 900 000 people enrolled in a system which tracks entitlement to social services and benefits and protects against double enrolment.

Galton discovered an 1823 dissertation by Jan Purkynˇe, a Czech physician and anatomist, which noted the presence of friction ridges on human fingertips. Although Purkynˇe did not propose that these ridges be used for identification, he did make the earliest attempt to classify the pattern types, sorting them into nine categories, which today would correspond to the arch, tented arch, two types of loop, four types of whorl, and a twinned loop.

Galton made his crucial contribution to the development of fingerprint classification. He realized that the key to a workable classification system lay in reducing, rather than expanding, the number of pattern types, deciding that all fingerprints could broadly be characterized as one of three basic pattern types: arch, loop, or whorl .

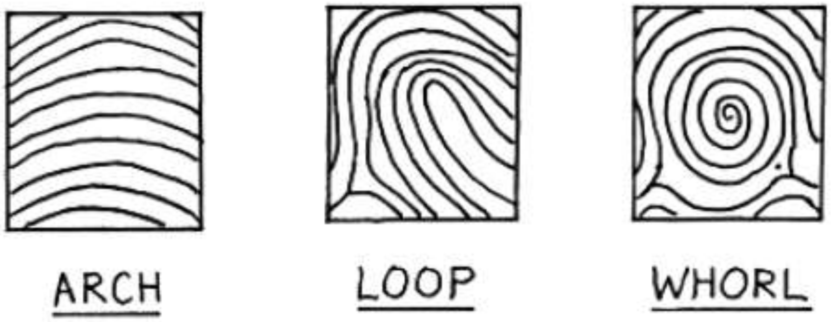


Fig. 1.3. Francis Galton's three basic fingerprint pattern types.

The primary classification could, therefore, range from 1/1 (zero whorls) to 32/32 (10 whorls).With a range between 1/1 and 32/32, there were 322, or 1024, possible primary classifications. The fingerprint cards were stored in a filing cabinet with 32 rows and 32 columns of pigeonholes. A fingerprint card with a primary classification 20/11, therefore, would be found in the 20th pigeonhole on the 11th horizontal row.

The secondary classification went on to characterize the fingers of the right hand (in the numerator) and the left hand (in the denominator). Because whorls had already been described in the primary classification, they were omitted in the secondary classification. The patterns of the fingers were characterized as arches (A), tented arches (T), radial loops (R), or ulnar loops (U).

Further sub-classification was performed by ridge tracing. Whorl patterns originate in two *deltas*, where the transverse ridges divide (like a river delta) to form the whorl.

Loops were sub-classified by ridge counting. The examiner counted the number of ridges between the delta and the core, and these values were appended to the secondary classification. Ridge counts from 1 to 9 in the index finger (1 to 10 in the middle finger) were characterized by I, counts above these threshold by O. The third term of the equation was the actual numerical ridge count of each little finger if it was, as was typical, a loop.
(Whorls in both thumbs, high-ridge-count radial loops in the right index and middle fingers, low-ridge-count ulnar loops in the left index and middle fingers. Nineteenridge-count loop in the right little finger. Eight-ridge-count loop in the left little finger.) [4]

Like Galton, Vucetich simplified his scheme to four basic pattern types: arch, loop with "internal inclination," loop with "external inclination," and whorl. For the thumbs, each of these patterns was designated with a letter: A, I, E, or V.

For the fingers, they were indicated with the numbers 1– 4.Vucetich's *primary classification* was given by the pattern types of the fingers in order, from thumb through little finger, expressed as a fraction with the right hand over the left. For example, the primary classification

$$\frac{V1211}{E1311}$$

indicated a whorl on the right thumb, an external loop on the left thumb, arches on both index fingers, an internal loop on the right middle finger, an external loop on the left middle finger, and arches on the remaining fingers.

The **challenges** of forensic fingerprint identification are quite different from those of 10-print identification. While 10-print identification requires complicated systems of pattern classification in order to hone in on a likely set of potentially matching cards, once the set of candidate matches has been produced, the examiner has a great deal of information available to make the comparison. Ten-print identification involves comparing *inked* impressions of a complete set of (usually) 10 fingers.

An obvious lack of matching ridge characteristics between the finger impressions of any of the 10 fingers of different persons eliminates the possibility that the two sets of prints derive from the same hands. When the task is forensic identification, the situation is quite different.

Latent prints typically do not have the clarity of information of inked prints; are limited in area compared to inked prints, which are *rolled* on the card in order to maximize area; contain background noise, impressions of foreign particles, and other artifacts that somehow must be distinguished from true ridge detail; and suffer from greater pressure distortion than inked prints. [4]

In order to use fingerprint patterns for forensic purposes, three basic steps are necessary:

1. Establish the relative permanence of fingerprint patterns.
2. Establish the variability of fingerprint patterns.
3. Develop a method, process, and confidence measure for attributing a crime-scene impression to a known finger.

The FBI manages a fingerprint identification system and database called **IAFIS**, which currently holds the fingerprints and criminal records of over fifty-one million criminal record subjects, and over 1.5 million civil (non-criminal) fingerprint records. U.S. Visit currently holds a repository of over 50 million persons, primarily in the form of two-finger records. For fingerprints recorded at 1000 ppi spatial resolution, law enforcement (including the FBI) uses JPEG 2000. [4]