BIOMETRICS

ABSTRACT

Biometrics is the science and technology of authentication (i.e. establishing the identity of an individual) by measuring the person's physiological or behavioral features. The term is derived from the Greek words "bios" for life and "metron" for degree. In information technology (IT), *biometrics* usually refers to technologies for measuring and analyzing human physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes. Examples of behavioural characteristics which can be measured include signature recognition, gait recognition, speaker recognition and typing recognition. In a typical IT biometric system, a person registers with the system when one or more if his physiological characteristics are obtained, processed by a numerical algorithm, and entered into a database. Ideally, when he logs in, all of his features match 100%; then when someone else tries to log in, she does not fully match, so the system will not allow her to log in. However, current technologies are nowhere close to matching this ideal. Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false nonmatch or reject rate (FRR), and the failure to enroll rate (FTE or FER).

In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter. One of the most common measures of real-world biometric systems is the rate at the setting at which both accept and reject errors are equal: the equal error rate (EER). Claimed error rates sometimes involve idiosyncratic or subjective elements.Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty. Forensic DNA evidence enjoys a particularly high degree of public trust at present (ca. 2004) and substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA. As with many interesting and powerful developments of technology, excessive concern with the biometric may have the effect of eclipsing a more general critical faculty. Biometrics may become associated with severe miscarriages of justice if bedazzlement with the performance of the technology blinds us to the following possibilities, where an individual could:

- plant DNA at the scene of the crime
- associates anothers identity with his biometrics, thereby impersonating without arousing suspicion
- fools a fingerprint detector by using a piece of sticky tape with an authentic fingerprint on it
- fools an iris recognition camera by showing a photo of anothers iris
- interferes with the interface between a biometric device and the host system, so that a "fail" message gets converted to a "pass".

This paper will give you a detailed study about biometrics.

Table of contents:

INTRODUCTION:

Before we go any further let us define exactly what we mean when we talk about biometric technologies. The term 'biometrics' refers strictly speaking to a science involving the statistical analysis of biological characteristics. Here biometrics is used in a context of analysing human characteristics for security purposes. The distinction can be clarified with following definition:

"A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity."

This measurable characteristic, *Biometric*, can be *physical*, such as eye, face, finger image, hand and voice or *behavioural*, like signature and typing rhythm. Biometric system must be able to recognize or verify it quickly and automatically.

It is often said that with biometric products you are able to reach the highest level of security. To help illustrate this point, a much quoted

"Biometrics" are automated methods of recognizing a person based on a physiological or behavioral characteristic.

Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins.

Biometricrecognition:

Biometric recognition can be used in identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match.

A system also can be used in verification mode, where the biometric system authenticates a person's claimed identity from his/her previously enrolled pattern.

Using biometrics for identifying and authenticating human beings offers some unique advantages. Only biometric authentication bases an identification on an intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed.

While all biometric systems have their own advantages and disadvantages, there are some common characteristics needed to make a biometric system usable.

First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike."

Newer methods, even those with a great deal of scientific support, such as DNA-based genetic matching, sometimes do not hold up in court.

Most people find it acceptable to have their pictures taken by video cameras or to speak into a microphone. In the United States, using a fingerprint sensor does not seem to be much of a problem. In some other countries, however, there is strong cultural opposition to touching something that has been touched by many other people.

While cost is always a concern, most implementers today are sophisticated enough to understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration support and an enrollment operator can overtake the initial cost of the hardware. Also of key importance is accuracy. Some terms that are used to describe the accuracy of biometric systems include false-acceptance rate (percentage of impostors accepted), false-rejection rate (percentage of authorized users rejected), and equal-error rate (when the decision threshold is adjusted so that the false- acceptance rate equals the false-rejection rate).

When discussing the accuracy of a biometric system, it is often beneficial to talk about the equal-error rate or at least to consider the false-

acceptance rate and false-rejection rate together. For many systems, the threshold can be adjusted to ensure that virtually no impostors will be accepted. Unfortunately, this often means an unreasonably high number of authorized users will be rejected.

To summarize, a good biometric system is one that is low cost, fast, accurate, and easy to use.

Facial recognition system:

A facial recognition system is a computer driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database.

It is typically used for security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. The London Borough of Newham , in the UK, has a facial recognition system built into their borough-wide CCTV system; *see also Closed-circuit television*.

Popular recognition algorithms include eigenface, fisherface and the Hidden Markov model.

Critics of the technology complain that the LB Newham scheme has, as of 2004 , never recognised a single criminal, despite several criminals in the system's database living in the Borough and the system having been running for several years. An experiment by the local police department in Tampa, Florida, had similarly disappointing results.

Physical anthropology:

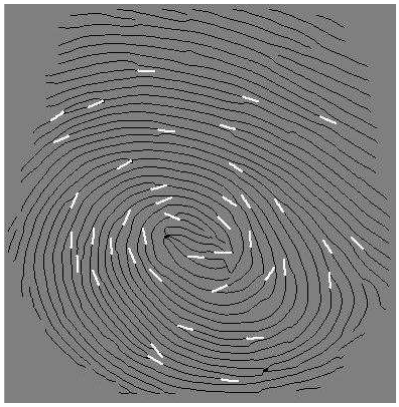
Physical anthropology, sometimes called "biological anthropology," studies the mechanisms of biological evolution, genetic inheritance, human adaptability and variation, primatology, and the fossil record of human evolution. See also: Race.

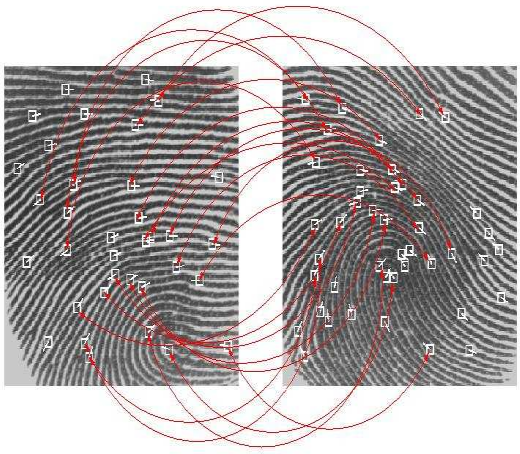
Some of the early branches of physical anthropology, such as early anthropometry, are now rejected as pseudoscience. Metrics such as the cephalic index were used to derive behavioral characteristics.

Fingerprint recognition:

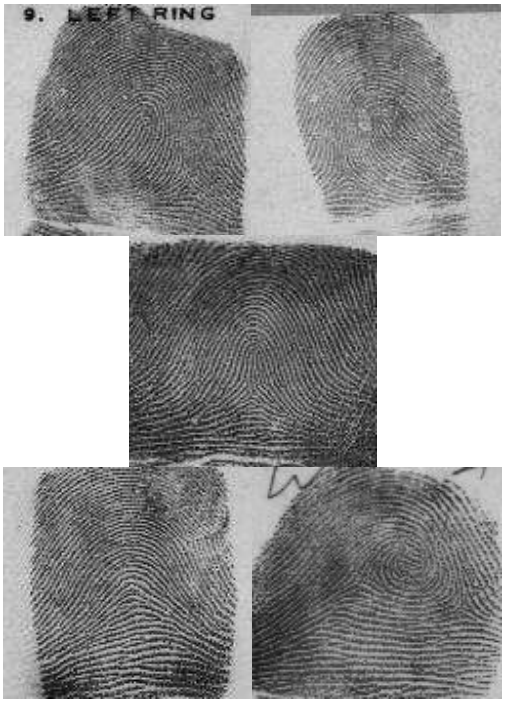
Fingerprint recognition is a biometric security method that integrates with applications and other technologies to provide a way to identify a person by scanning a person's fingerprint to gain access. Fingerprint recognition is a way to provide higher security because a fingerprint

Fingerprint Matching





Fingerprint Classification



biometric system does not use any passwords or pin #'s but only valid fingerprints.

Because there are several fingerprint recognition solutions that are available today, we will only give you a general outline of how fingerprint recognition can work.

The first step is to setup your fingerprint recognition devices and scan all fingerprints that will have access. You will only need to do this once as the fingerprint recognition device stores the fingerprints as templates in a mathematical algorithm form. Depending on your setup, the device may store this in a database or use smart card technology for local storage of these fingerprint templates.

When an individual is wanting access, the individual must put their finger on the fingerprint recognition device or depending on the system, you may only need to put it close to the fingerprint scanning area. The fingerprint recognition device then captures the individual's fingerprint and puts in into a template form using a mathematical algorithm and compares it to its database or storage of fingerprints to determine if it matches any existing fingerprints. If the fingerprint device finds a match then access is granted.

As we noted above, this example may vary from vendor to vendor. If you're looking for more in-depth fingerprint recognition security information, then you should contact a biometric security vendor to request more information.

Fingerprint Matching:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques can be placed into two categories: minute-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation. matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures can not be completely characterized by minutiae. We are trying an alternate representation of fingerprints which will capture more local information and yield a fixed length code for the fingerprint. The matching will then hopefully become a relatively simple task of calculating the Euclidean distance will between the two codes.

We are developing algorithms which are more robust to noise in fingerprint images and deliver increased accuracy in real-time. A commercial fingerprint-based authentication system requires a very low False Reject Rate (FAR) for a given

False Accept Rate (FAR). This is very difficult to achieve with any one technique. We are investigating methods to pool evidence from various matching techniques to increase the overall accuracy of the system. In a real application, the sensor, the acquisition system and the variation in performance of the system over time is very critical. We are also field testing our system on a limited number of users to evaluate the system performance over a period of time.

Fingerprint Classification:

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!). To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

Fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. We have developed an algorithm to classify fingerprints into five classes, namely, *whorl, right loop, left loop, arch, and tented arch*. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a FingerCode which is used for classification. Our classification is based on a two-stage classifier which uses a K-nearest neighbor classifier in the first stage and a set of neural networks in the second stage. The classifier is tested on 4,000 images in the NIST-4 database. For the five-class problem, classification accuracy of 90% is achieved. For the four-class problem (arch and tented arch combined into one class), we are able to achieve a classification accuracy of 94.8%. By incorporating a reject option, the classification accuracy can be increased to 96% for the five-class classification and to 97.8% for the four-class classification when 30.8% of the images are rejected.

Fingerprint Image Enhancement:

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. We have developed a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and furrow structures of input fingerprint images based on the estimated local ridge orientation and frequency. We have evaluated the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification system. Experimental results show that incorporating the enhancement algorithms improves both the goodness index and the verification accuracy.

Applications:

Biometrics is a rapidly evolving technology which has been widely used in forensics such as criminal identification and prison security. Recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication in a large number of civilian applications. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry and key-less ignition. Due to increased security threats, many countries have started using biometrics for border control and national ID cards.

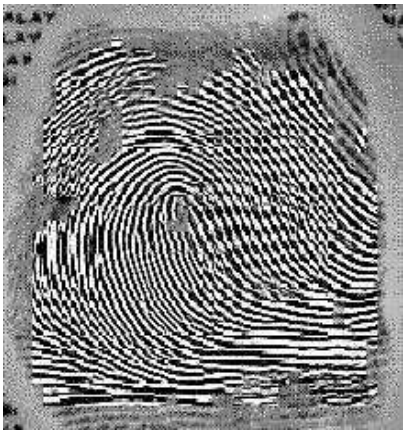
Future biometrics:

A system that analyses the chemical make-up of body odor is currently in development. In these systems sensors are capable of capturing body odor from non-intrusive parts of the body such as the back of the hand. Each unique human smell consists of different amount of volatiles. These are extracted by the system and converted into a biometric template. All testing and fastest

possible analysis of the human DNA takes at least 10 minutes to complete and it needs human assistance. Thus, it cannot be considered as biometric technology in its sense of being fast and automatic. Additionally current DNA capture mechanisms, taking a blood sample or a test swab inside of the mouth, are extremely intrusive compared to other biometric systems. Apart from these problems DNA, as a concept, has a lot of potential.

Ear shape biometrics research is based on law enforcement needs to collect ear markings and shape information from crime scenes. It has some potential in some access control applications in similar use as hand geometry.

Fingerprint Image Enhancement



There are not excessive research activities going on with the subject.

Keystroke dynamics is a strongly behavioural, learnt biometric. As being behavioural, it evolves significantly as the user gets older. One of the many problems include that highly sophisticated measuring software and statistical calculations have to be made real time if the user actions should be constantly verified. Standard keyboard could be used in simplest cases.

Veincheck is a technique where infrared camera is used to extract vein pattern from the back of the hand. The pattern is very unique and the capture method is user friendly and non-intrusive as hand geometry check. Maybe combining them could result very accurate and easy-to-use biometric.

Conclusion:

Authorizing the user with secret PIN and physical token is not enough for applications where the importance of user being really the one certified is emphasized. If biometric technologies are not used we accept the possibility that the token and secrecy of PIN can be compromised. On applications like bank account cards the companies count the money lost because of fraud and value the risk with the bottom line. When new uses like electronic id-cards which are validated with automation emerge the possible harm done to a individual

cannot be paid back to account, it must be prevented.

Biometrics itself is not solution to this problem. It just provides means to treat the possible user candidates uniquely. When doing so biometric system handles the unique data scanned from the user. Secrecy of this information has to be ensured by strong cryptographic methods. The best case could still be that the biometric templates would never leave the scanner device, with or without encryption. The result should only be granting the scanning device, which could be special smart card carried by user itself, to complete the challenge-response sequence needed. In that case your fingerprint may be the password, but theproblematics with management of public and secret fcryptographic keys stays the same. Some biometric technologies itself are ready for mass markets. The off-the-shelf components available are suitable for very small scale, closed systems. Before larger scale deployment the integration to SPKI schemes and standards like X.509 has to be completed .

References:

www.technicalpapers.co.nr