

Introduction to Biometrics¹

Gerik Alexander v.Graevenitz

von Graevenitz - Biometrics, Bonn, Germany

May, 14th 2004

Introduction to Biometrics

Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics. There are many types of biometric technologies on the market: face-recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice and signature.

The method of biometric identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: The person to be identified is required to be physically present at the point-of-identification or the identification based on biometric techniques obviates the need to remember a password or carry a token or a smartcard.

With the rapid increase in use of PINs and passwords occurring as a result of the information technology revolution, it is necessary to restrict access to sensitive/personal data. By replacing PINs and passwords, biometric techniques are more convenient in relation to the user and can potentially prevent unauthorised access to or fraudulent use of ATMs, Time &

¹ published under the title "Biometrics in Access Control" in A&S International, Volume 50, Taipei, 2003, pp. 102-104

Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports, driver's licenses and insurance cards may be forgotten, stolen, or lost.

Various types of biometric systems are being used for real-time identification; the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilise iris and retinal scan, speech, face, and hand geometry.

Identification versus Verification

Sometimes Identification and Verification are used as similar terms, but they have two different meanings. Identification means determining a person by presenting his biometric feature. For this purpose a database of templates is searched and matched against the biometric sample until the best fitting (most similar) template is found. This method also known as "1:N" or "one-to-many-comparison". In comparison to identification, verification means testing if the user is really the person he/she claims to be. The presented biometric feature is compared against the previously stored biometric reference data either on a smartcard or in a database. In contrast to the identification method only one biometric comparison is being performed.

False Rejection Rate / False Acceptance Rate

In contrast to methods based on knowledge or possession like PINs/passwords or tokens, biometric systems work with probabilities, because biometric features are invariably caused by noise in the measurement – therefore

biometric systems are not exact methods. A second point is that for example, fingerprint systems can suffer from accuracy problems created by limitations of sensors and algorithms.

These limitations result in two problems called False Acceptances and False Rejections. The False Acceptance Rate (FAR) is the success probability for an unauthorised user or a user that does not exist within a biometric system to be falsely recognised as the legally registered user. A low tolerance threshold for the biometric data to be matched leads to a lower FAR value, but to higher values of the False Rejection Rate (FRR). In contrast, the False Rejection Rate (FRR) rate is the probability of the legally registered user to be falsely rejected by the biometric system when presenting his biometric feature. High tolerance limits for the biometric data to match lead to a very low FRR value, but to higher values for the False Acceptance Rate (FAR). Both values FAR and FRR are negatively correlated. However, these measures can vary significantly depending on how one adjusts the sensitivity of the mechanism that matches the biometric.

If the tolerance thresholds for the biometric data to be matched for a successful verification are chosen, so that the values for a false acceptance rate and false rejection rate are equal, this common value is called the equal error rate (EER). The equal error rate is also known as the crossover error rate (CER). The lower the equal error rate is, the higher the accuracy of the biometric system.

For applications where convenience and general user acceptance are more important than security (i.e. hotel room access, automatic teller machine authentication), administrators have to settle for a high FAR in order to ensure that authorised individuals are always granted access. The disadvantage of a low FRR is a greater likelihood of granting access to unauthorised individuals.

Types of Biometric Methods

In general a biometric system is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

Face: Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs extra peripheral features that are not included in basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

Fingerprint: Fingerprint recognition represents the oldest method of biometric identification, its history is going back as far as at least 6000 BC. The use of fingerprints as a personal code has a long tradition and was already used by the Assyrians, the Babylonians, the Chinese and the Japanese. Since 1897, dactyloscopy (synonym for non-computer-based fingerprint identification) has been used for criminal identification. A fingerprint consists of ridges (lines across fingerprints) and valleys (spaces between ridges). The pattern of the ridges and valleys is unique for each individual. There are two major methods of fingerprint matching: Minutiae matching and global pattern matching. The first approach analyses ridge bifurcations and endings, the second method represents a more macroscopic approach, considering the flow of ridges in terms of, for example, arches, loops and whorls. The equal-error-rate is low, therefore fingerprint recognition is very accurate. The prices of such systems

compared to other biometric systems are quite low and also the user acceptance is very high.

Hand geometry: This involves analyzing and measuring the shape of the hand and the lengths of the fingers. It might be suitable where there are more users or where users access the system infrequently. Accuracy can be very high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations use hand geometry readers in various scenarios, including time and attendance recording.

Retina: A retina-based biometric system involves analyzing the layer of capillary vessels located at the back of the eye. This technique involves using a low intensity ray light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. In general the user has to take off his or her glasses. The equal-error-rate is quite low.

Iris: An iris-based biometric involves analyzing features found in the colored ring that surrounds the pupil. This uses a fairly conventional camera element and requires no close contact between the user and the reader. Users with glasses with a high dioptré have to take off his/her glasses. Iris recognition systems have got a very low equal-error-rate and are very secure. The price of an iris-recognition system is very high.

Signature: Signature verification analyses the way the user signs his name. Signing features such as velocity, speed, and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification. Signature verification is generally

used for verification and not for identification, because of the high equal-error-rate.

Vein: Vein verification is a physical biometric technology that is under development. It analyses the pattern of veins, the traces and the shapes in the back of the hand and in the wrist using a red ray of light. The hardware system is very complicated and expensive.

Voice: Voice authentication captures the characteristics such as cadence, frequency, pitch and tone of an individual's voice. Voice verification works with a microphone or with a regular telephone handset, although performance increases with higher quality capture devices. The hardware costs are very low, because today nearly every PC includes a microphone or it can be easily connected one. However voice recognition has got its problems with persons who are husky or mimic another voice. Additionally the likelihood of recognition decreases with poor-quality microphones and if there is background noise. Voice verification will be a complementary technique for e.g. finger-scan technology as many people see finger scanning as a higher authentication form. In general voice authentication has got a high EER, therefore it is in general not used for identification.