Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Biometrics

Tradtionally means of automatic identification:

- possession-based (credit card, smart card)
- knowledge-based (password, PIN)
- biometric-based (fingerprint, iris scan)

Possession and knowledge based authentication mechanisms are replaceable, but can be lost, stolen, forgotten, or guessed by imposters. Annually, it is estimated there is over $1 billion in fraudulent credit card transcations and $3 billion in fraudulent ATM withdrawals. These traditional approaches are unable to differentiate between an authorized person and an imposter since they check against something known or in possession by the person being authenticated.

What is biometrics?

Biometrics is the science which deals with the automated recognition of individuals based on their biological and behavioral characteristics. It uses **biometry**, the mathematical and statistical aspects of biology, to recognize a person by determining the authenticity of a specific biological and/or behavioral characteristic possessed by that person.

The scientific literature on quantitative measurement of humans for the purpose of identification dates back to the 1870s and the measurement system of Alphonse Bertillon. Bertillon used a system of body measurements such as skull diameter, arm length, foot length, etc to identify prisoners in the United States until the 1920s. In the 1880s, Henry Faulds, William Herchel, and Sir Francis Galton proposed

quantitative identification through fingerprint and facial measurements. Biometrics was introduced into forensic identification by Edmond Locard in the 1920s.

Authentication vs Identification

Verification is the process of recognizing a person by comparing the captured biometric characteristic with a biometric template stored in the system. It performs a one-to-one match and checks if the person is who they claim they are.
Identification is the process of recognizing a person by searching a template database for a match. It performs one-to-many matches to assign an identity to the person.

Uses of Biometrics

Biometric systems are used for physical access control in places like airports and other travel infrastructure. It can also be used for logical access in places like banks to regulate access to money. It is also commonly used to ensure uniqueness of individuals, such as for enrollment in a benefits program.

The development of digital signal processing techniques in the 1960s led to work in automatic human identification. Speaker and fingerprint recognition systems were among the first to be explored. The potential application of this technology for high-security access control was recognized, leading to increased government usage. Retinal and signature verification systems came in the 1980s, followed by facial recognition and iris recognition systems in the 1990s.

Misconceptions

Hollywood typically portrays facial recognition as instantaneous, tied to a database of all criminals, and working 100% of the time. In reality, facial recognition algorithms are vastly affected by lighting, angle, face size, and image quality. They require a high end computer for processing and are still being evaluated as a tool for law enforcement. Match confidence varies depending on the application and data sharing between law enforcement organizations is difficult.

Types of Biometrics

Biometric systems measure various physiological or behavioral characteristics such as fingerprints, voice pattern, iris/retinal pattern, hand shape, face shape, handwriting, keystroke usage, and finger shape. This is only a partial list as new features such

as gait, ear shape, head resonance, optical skin reflectance, and vein structure are being developed all the time. Because of the broad range of characteristics, imaging requirements for biometric technologies vary greatly. Examples:

- voice - one dimensional signal
- hand writing - several simulataneous one dimensional signals
- fingerprint - two dimensional image
- hand geometry - multiple two dimensional measures
- face and iris scan - time series of two dimensional images or a three dimensional image

Ideally, biometric characteristics for identification have five qualities.

- **Robust** - unchanging on an individual over time.
- **Distinctive** - showing great variation over the population.
- **Available** - the entire population should ideally have this measure.
- **Accessible** - easy to image using electronic sensors.
- **Acceptable** - people do not object to having this measurement taken.

Quantitative measures of these five qualities have been developed.

- Robusness is measured by the false negative rate (Type I error), the probability that a submitted sample will not match the enrollment image.
- Distinctiveness is measured by the false positive rate (Type II error), the probability that a submitted sample matches the enrollment image of another user.
- Availablility is measured by the rate of enrollment failure, the probability that a user will not be able to supply a readable measure to the system upon enrollment.
- Accessibility is quantified by the throughput rate of the system, the number of systems that can be processed in some unit time.
- Acceptability is measured by polling the device users.

Biometric Systems

Biometric systems generally perform one of two tasks:

- Positive identification - the submitted samples are from an individual known to the system.
- Negative identification - the submitted samples are from an individual not known to the system.

They can also have other types of classifications:

- **Overt vs Covert** - if the user is aware that a biometric identifier is being measured, then the use is overt. Most access control systems are overt. Generally only some forensic applications are covert.
- **Habituated vs Non-habituated** - users presenting the biometric trait on a daily basis can be considered habituated after a short period of time. Users who have not presented the trait recented are considered non-habituated.
- **Attended vs Non-attended** - whether or not the use of the biometric device will be observed and guided by system management during operation.
- **Open vs Closed** - an open system uses public data collection, compression, and format standards while a closed system operates on proprietary formats.

For open systems, compression and transmission protocols have to be standardized so that every user of the data can reconstruct the original signal. Current standards for data transmission include wavelet scalar quantization for fingerprint data, JPEG images for facial images, and code excited linear prediction for voice data.

Feature Extraction

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features.

- **Template** - stored features that samples are matched against
- **Model** - the construction of a complex mathematical expression capable of generating features characteristic of a particular user.
- **Enrollment** - placing a template or model into the database for the very first time.

Pattern matching processes compare the sample to multiple templates or models from the database one at a time, sending on a quantitative "distance" measure for each comparision. In place of a "distance" metric, some system use "similarity" measures, such as maximum likelihood values.

Biometrics and Privacy

Biometric measures can be used in place of a name, social security number, or other form of identification to secure anonymouse transactions. The real fear is that biometric measures will link people to personal data or allow movements to be tracked. After all, credit card and phone record data can be used in court to establish a person's activities and movements. Phone books are public databases linking people to their phone number. These databases have a one to one mapping that allow for names to be determined from phone numbers. Unlike phone books, biometric databases cannot be reversed to determine names from measures because biometric measures, although distinctive, are not necessarily unique.

Five US states have electronic fingerprint records of social service recipients. Six states maintain electronic fingerprints of all licensed drivers, and nearly all states maintain copies of driver's licenses and social service recipient photos. FBI and state governments maintain fingerprint databases on convicted felons and sex offenders, and the federal government maintains hand geometry records on those who have voluntarily requested border crossing cards.

In general, biometric measures contain no personal information and are more difficult to forge or steal. They can be taken without a person's knowledge, but cannot be linked to an identity without a pre-existing invertible database. Since they are not always secret and publicly observable, they cannot be revoked or changed if compromised.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech