Biometrics Systems and Building Blocks

Guodong Guo

8/24/2017
Human recognition

- Humans typically use **body characteristics** such as **face**, **voice**, and **gait** along with other **contextual** information (e.g., location and clothing) to recognize one another.

- The ability to **identify** individuals uniquely and to **associate** personal **attributes** (e.g., name, nationality, etc.) with an individual has been crucial to the fabric of **human society**.
Personal identity

• The set of attributes associated with a person constitutes their personal identity

• Identity management applications
  – regulating international border crossings
  – restricting physical access to important facilities like nuclear plants or airports
  – controlling logical access to shared resources and information
  – performing remote financial transactions
  – distributing social welfare benefits
Identity theft problem

- The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have led to the risk of identity theft.
- Rising magnitude of identity theft and heightened concerns about national security have reinforced the need for reliable identity management systems.
Person Recognition

• Fundamental task in identity management
  – establish the *association* between an *individual* and his *personal identity*

• *Person recognition*
  – The process of *determining a person’s identity* or *verify the identity claim* of an individual
Three basic methods for person recognition

• what he/her knows
  – Knowledge-based

• what he/her possesses extrinsically
  – Token-based

• who he/her is intrinsically
  – Biometric recognition
Knowledge-based

- It is based on the fact that the individual has exclusive knowledge of some secret information, e.g.,
  - Password
  - personal identification number
  - cryptographic key
Token-based

• It assumes that the person has exclusive possession of an extrinsic token, e.g.,
  – identification card
  – driver’s license
  – passport
  – physical key
  – personal device such as a mobile phone
Biometric recognition

- **Biometric recognition** can be defined as the science of establishing the identity of an individual based on the **physical** and/or **behavioral characteristics** of the person either in a fully **automated** or a **semi-automated** manner.

- Examples?
Drawbacks of knowledge-based and token-based person recognition

• Passwords or ID cards can be easily forgotten/lost, guessed/stolen, or shared

• Moreover, they cannot provide vital identity management functions, e.g.,
  – non-repudiation and detecting multiple enrollments by the same person under different identities
Examples

• Individuals can easily deny (repudiate) using a service by claiming that their password had been stolen or guessed.

• Individuals can also conceal their true identity by presenting forged or duplicate identification documents.

• Traditional mechanisms like passwords and tokens do not provide strong evidence for post-event person recognition, e.g.,
  – suspect identification at a crime scene
Advantages of Biometric recognition

- It offers a *natural* and *more reliable* solution to the problem of person recognition
- Biometric identifiers are *inherent* to an individual, it is more *difficult* to *manipulate*, *share*, or *forget* these traits
- Biometric traits constitute a strong and *reasonably permanent* link between a person and his identity
- It can *prevent* users from making *false repudiation claims*, although the individual might deny it, e.g., claim multiple benefits in welfare disbursement.
- Biometric recognition can *replace* or *complement* existing knowledge-based and token-based mechanisms.
Any person who presents his biometric identifier to a biometric system for the purpose of being recognized can be called a user of the system.
Biometric Systems

• A **biometric system** measures one or more **physical** or **behavioral** characteristics of an individual to **determine** or **verify** his/her identity

• **characteristics** include fingerprint, palmprint, face, iris, retina, ear, voice, signature, gait, hand vein, odor, or the DNA information

• These characteristics are referred to by **different terms**, such as **traits**, **indicators**, **identifiers**, or **modalities**
Two main phases (1)

• **Enrollment phase:**
  – During the *enrollment* phase, the biometric data is acquired from the individual and stored in a database along with the person’s identity.

• Typically, *salient* and *distinctive features* are extracted from the biometric data.

• Only the *extracted feature set* gets stored, while the raw biometric data is discarded.
Two main phases (2)

• **Recognition phase:**
  – During the *recognition* phase, the biometric data is *re-acquired* from the individual and *compared* against the stored data to determine the user identity
Four basic building blocks

• A biometrics system is usually built with
  – sensor
  – feature extractor
  – database
  – matcher
Sensor module

• Measure or record the raw biometric data of the user;
• Integrated into a user interface (human-machine interface) in a biometric system
• A suitable or good user interface
  – facilitate rapid user habituation
  – enable the acquisition of good quality biometric samples from the user
Image quality depends on the sensor

- Factors like *resolution*, *frame rate*, and *sensitivity* of the camera play an important role in determining the image quality
Sensor design

• Need to consider factors like
  – cost, size, and durability of the sensor
  – the demographic characteristics of the target population, e.g.,
    • age and gender, and other cultural issues (e.g., some users may be averse to touching a sensor surface)
Feature extraction module

- **Pre-processing** may be needed before features are extracted.

- **The three commonly used pre-processing steps**
  - quality assessment (determine the suitability for further processing),
  - segmentation (separate the required biometric data from the background noise), and
  - enhancement (improve data quality and reduce the noise).
Quality Assessment

• If the raw data is not of sufficient quality, there are two options:
  – re-acquire the data from the user, or
  – trigger an exception (failure alarm) alerting the system administrator to activate suitable alternate procedures
    • typically involving some form of manual intervention by the system operator
Segmentation

• The goal is to separate the required biometric data from the background noise.

• Some examples:
  – Detecting a face in a cluttered image is a good example of segmentation
  – Iris localization from eye images is another example of segmentation
Signal quality enhancement

• It is to **improve** the biometric data quality and further **reduce** the noise

• Example:
  
  – For image data, enhancement algorithms like **smoothing** or **histogram equalization** may be applied to minimize the noise introduced by the camera or illumination variations.

  – (See Figure 1.5, page 8 in text), it shows a face image obtained after segmentation and quality enhancement based on histogram equalization.
Feature extraction

• It refers to the process of generating a compact but expressive digital representation of the underlying biometric trait, called a template.

• Template: The template contains only the salient discriminatory information that is essential for recognizing the person.

• Example:
  – The position and orientation of minutia points
Template in two phases

• During enrollment, the template gets stored in the database.

• At the time of recognition, the template is retrieved from the database, and matched against the feature set extracted from the new biometric sample acquired from the user.
gallery and probe images

• In many image-based biometric systems, the raw biometric images may also be stored in the database along with the templates during enrollment.
• Such images are often known as gallery images, reference images, stored images, or enrollment images.
• The images acquired during recognition are known as probe images, query images, or input images.
Multiple templates

• The template of a user can be extracted from a single biometric sample, or generated by processing multiple samples acquired during enrollment

• Purpose
  – Some systems store multiple templates in order to account for the large variations that may be observed in the biometric data of a user

• Example
  – Face recognition systems may store multiple templates of an individual, with each template corresponding to a different facial pose with respect to the camera
Database module

• The biometric system database acts as the repository of biometric information

• A key decision is to use a centralized or decentralized database
  – Storing all the templates in a central database may have a higher security, because the data can be secured through physical isolation and by having strict access control mechanisms.
Matching module

• A biometric matcher is to compare the query features against the stored templates to generate match scores.

• Match score
  – The match score is a measure of the similarity between the template and the query
  – A larger match score indicates greater similarity between the template and the query
  – If a matcher measures the dissimilarity between the two feature sets, the score is referred to as a distance score
Match Score (cons.)

• A smaller distance score indicates greater similarity

• Example
  – In a fingerprint-based biometric system, the number of matching minutiae between the input and the template feature sets can be considered as the degree of similarity (match score)
From match scores to decision making

• The matcher module also encapsulates a decision making module, in which the match scores are used to
  – either validate a claimed identity (verification) or
  – provide a ranking of the enrolled identities in order to identify an individual (identification).

• Up to this point, we have introduced the four basic building blocks of a biometric system