Identification Error Rates and Biometrics System Design

Guodong Guo

9/5/2013

Identification system error rates

- False positive identification rate and False negative identification rate
- False positive identification rate: The expected proportion of identification transactions by users not enrolled in the system, where an identity is returned, is known as the *false positive identification rate* (FPIR)
  - This is analogous to the false match case in biometric verification
  - The FPIR depends both on the size of the enrollment database (N) and the threshold (η).

False negative identification rate

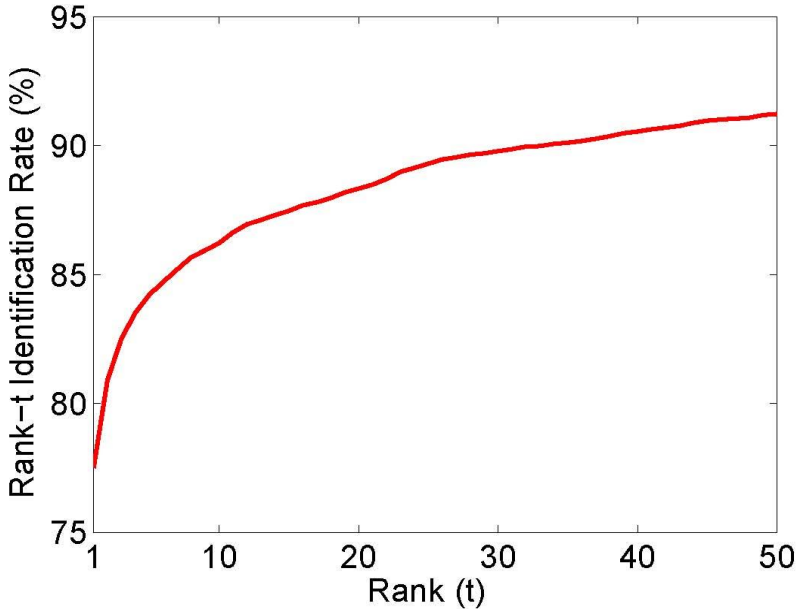
- False negative identification rate: The expected proportion of identification transactions by users enrolled in the system in which the user's correct identity is not returned is called the *false negative identification rate* (FNIR)
- FNIR depends on the size of the enrollment database (*N*), the threshold (η) used for the match scores, and the number of identities *t* returned by the identification system

True positive identification rate

- True positive identification rate (TPIR): The expected proportion of identification transactions by users enrolled in the system, where the user's correct identity is among the *t* identities returned by the system.
  - FNIR = 1– TPIR
- If the biometric system outputs the identities of the top *t* matches, the corresponding TPIR is also known as the rank-*t* identification rate, which we refer to as R_t
- In particular, the value of TPIR for *t* = 1 is called the *rank-one accuracy*

CMC curve

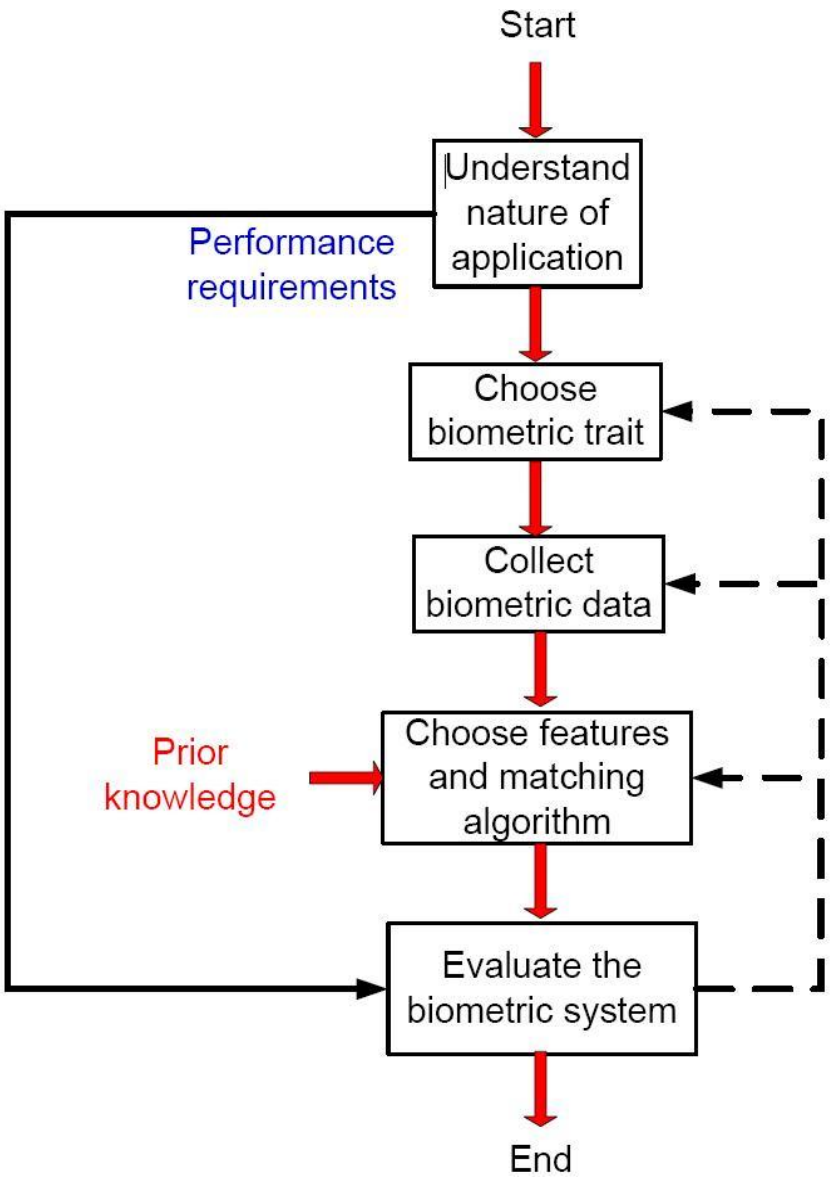
- The rank-*t* identification rate for different values of *t* can be summarized using the Cumulative Match Characteristic (CMC) curve, which plots R_t against *t* for $t = 1,2, \cdots, N$, where *N* is the number of enrolled users.



Some relations

- FNIR = FNMR
  - The probability that the input is falsely declared as a non-match against the user's template is the same as in verification mode
- $FPIR = 1 - (1 - FMR)^N$
  - A false positive identification occurs when the input falsely matches one or more templates in the database. FPIR is then computed as one minus the probability that no false match is made with any of the database templates
  - If the FMR is very small ($<< (1/N)$), FPIR can be approximated as $FPIR \approx N \times FMR$

Design Cycle of Biometric Systems



Nature of the application

- In some applications, biometrics may be used to supplement ID cards and passwords, thereby imparting an additional level of security. Such an arrangement is often called a *multi-factor authentication* scheme
- Depending on the application, we may need to choose between the verification and identification functionalities
  - This choice need not be always mutually exclusive
  - Example: In the large-scale national ID systems, one may need to perform *negative identification* during enrollment to prevent the possibility of the same user acquiring multiple identities

Other factors to consider

- **1. Cooperative** versus **non-cooperative users**: Cooperation refers to the behavior of the user when interacting with the system, e.g.,
- In a verification system, it is in the best interest of a genuine user to cooperate with the system and be accepted as a valid user (e.g., banking);
- In a negative recognition system, a user may not cooperate with the system (e.g., may purposely apply excessive pressure when placing his finger on the sensor) to avoid being recognized
  - A terrorist attempting to conceal his identity from an airport screening application will be non-cooperative

(cons.)

- 2. **Overt** versus **covert deployment**: If the user is aware that he is being subjected to biometric recognition, the application is categorized as *overt*. If the user is unaware, the application is called *covert*.
- Facial recognition can be easily used in a covert application (e.g., surveillance), while fingerprint recognition cannot be used in this mode (except for criminal identification based on latent fingerprints).
- Most commercial uses of biometrics are overt in nature.

(cons.)

- 3. **Habituated users** versus **non-habituated**: If the enrolled users interact with the biometric system quite frequently, they tend to get habituated in providing their biometric data
  - For example, a computer network login application typically has habituated users (after an initial "habituation" period) due to their use of the system on a regular basis
  - A driver's license application typically has non-habituated users since a driver's license is renewed only once in a period of several years.
- This is an important consideration when designing a biometric system because the familiarity of users with the system can affect recognition accuracy since a habituated user is likely to provide good quality biometric data.

(cons.)

- 4. **Attended** versus **unattended operation**: Attended versus unattended classification refers to whether the process of biometric data acquisition in an application is *observed, guided,* or *supervised by a human* (e.g., a security officer)
- An application may have an attended enrollment operation but unattended recognition operation
  - e.g., a banking application may have a supervised enrollment when an ATM card is issued to a user, but the subsequent uses of the biometric system for the ATM transaction are not attended.

(cons.)

- 5. **Controlled** versus **uncontrolled operation**: In a controlled environment, ambient environmental conditions such as temperature, pressure, moisture, lighting conditions, etc. can be moderated during the operation of a biometric system
  - Typically, indoor applications such as computer network login operate in a controlled environment, whereas outdoor applications such as keyless car entry or parking lot surveillance operate in an uncontrolled environment

(cons.)

- 6. **Open** versus **closed system**: If a person's biometric template can be used across multiple applications, the biometric system can be considered as *open*.
- For example, a user may use a fingerprint-based recognition system for entering secure facilities, computer network login, electronic banking, and bank ATMs.
- When all these applications use separate templates (databases) for each application, the system is considered *closed*.
- A closed system may be based on a proprietary template whereas an open system will need standard data formats and data compression methods to exchange and compare information between different systems

Summary of the nature of applications

- All the above factors profoundly influence the design of a biometric system.
- Most of the commercial applications of biometrics, such as access to secure facilities, have the following attributes:
  - verification, cooperative, overt, habituated, attended enrollment and non-attended authentication, and closed

Choice of biometric trait

- A number of biometric traits are being used in various applications.
- Each biometric trait has its pros and cons.
- The choice of a biometric trait for a particular application depends on a variety of issues besides its recognition performance.
- There are Seven factors to consider

Seven factors

- 1. **Universality**
  - Every individual accessing the application should possess the trait
  - This factor determines the failure to enroll (FTE) rate of the biometric system.
- 2. **Uniqueness**
  - The given trait should be sufficiently different across individuals comprising the user population.
  - Otherwise, the false match rate (FAR or FPIR) of the biometric system would be unacceptably high

Seven factors (cons.)

- 3. **Permanence**
  - The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm.
  - A trait that changes significantly over time is not a useful biometric because it will lead to a high false non-match rate (FRR or FNIR).
- 4. **Measurability**
  - It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual.
  - Furthermore, the acquired raw data should be amenable to processing in order to extract discriminative feature sets.
  - This factor significantly impacts the frequency of FTE and FTA failures and the recognition accuracy.

Seven factors (cons.)

- 5. **Performance**
  - Apart from the recognition accuracy (FMR, FNMR, FTE, and FTA), the computational resources required to achieve that accuracy and the throughput (number of transactions that can be processed per unit time) of the biometric system should also meet the constraints imposed by the application.
- 6. **Acceptability**
  - Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.

Seven factors (cons.)

- 7. **Circumvention**
  - This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.
  - It also refers to the process of obfuscation, where a user deliberately alters his biometric trait to evade recognition

Summary of Biometric Traits

- No single biometric is expected to effectively meet all the requirements (e.g., accuracy, practicality, cost) imposed by all applications
  - e.g., forensics, access control, government benefits programs, etc.
- No biometric is *ideal,* but a number of them are *admissible*
- The relevance of a specific biometric to an application is established depending upon the nature and requirements of the application, and the properties of the biometric characteristic

Data collection

- data is required both for designing the feature extraction and matcher modules as well as for the evaluation of the designed biometric system
- care must also be taken to ensure that the database is neither too challenging (collected under the most adverse conditions) nor too easy (collected under the most favorable conditions)
- Ideally, a database should include samples that are representative of the population and must preferably exhibit realistic intra-class variations
  - e.g., collecting data over multiple sessions, spread over a period of time, and in different environmental conditions

Choice of features and matching algorithm

- Most of the research and development in the field of biometrics has been focused on this issue
- Needs some prior knowledge about the biometric trait under consideration
  - e.g., prior knowledge about the “uniqueness” of minutia points facilitated the development of minutiae-based fingerprint recognition systems
- Another important factor is the *interoperability* between biometric systems
  - e.g., the performance of face recognition algorithms is severely affected when the images used for comparison are captured using different camera types

Evaluation

- Evaluation of a complete biometric system is a complex and challenging task
- Questions to address for evaluation:
- What are the error rates of the biometric system in a given application?
  - (matching or technical performance)
- What is the reliability, availability, and maintainability of the system?
  - (engineering performance)
- What are the vulnerabilities of the biometric system?
  - What level of security does the biometric system provide to the application in which it is embedded?
  - (security of the biometric system)
- What is the user acceptability of the system?
  - How does the system address human factor issues like habituation and privacy concerns?
  - (user concerns)
- What is the cost and throughput of the biometric system and what tangible benefits can be derived from its deployment?
  - (return on investment)