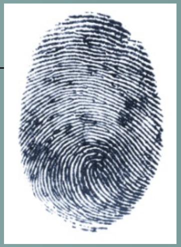
Understanding Biometrics

5. Measuring Biometrics

Dr. Terence Sim



Types of Errors

- False Reject Rate (FRR)
  - The probability of rejecting the true user.
  - Some books use False Non-Match Rate
  - Prob. of detection = 1 – FRR

- False Accept Rate (FAR)
  - The probability of accepting an imposter.
  - Some books use False Match Rate

- Failure to Enroll Rate (FTE)
  - The probability of not being able to enroll a user.

Errors

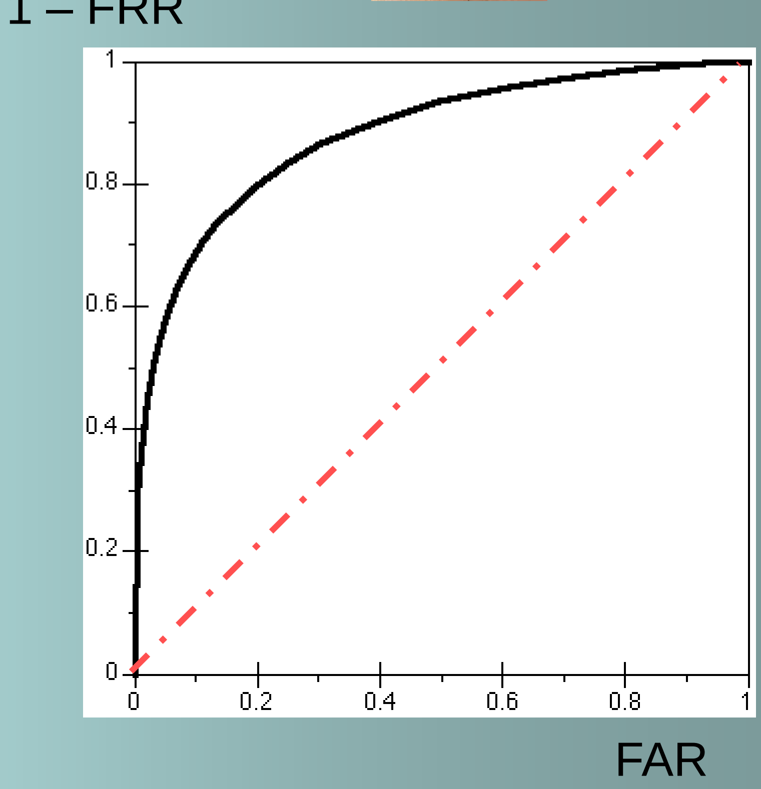
- FAR, FRR are for verification. For identification, it is usual to define Misclassification Rate
  - The probability of incorrectly identifying a user.
  - Thus accuracy = 1 – misclassification rate
- Open-world identification:
  - The user to be identified may not have enrolled in the database.
- Closed-world identification:
  - The user to be identified is known to the system.

Errors

- Ideally, both FAR and FRR are zero.
  - In reality, one error can only be reduced at the expense of the other.
  - This trade-off can be represented in a Receiver-Operator Characteristic Curve (ROC)

ROC curve

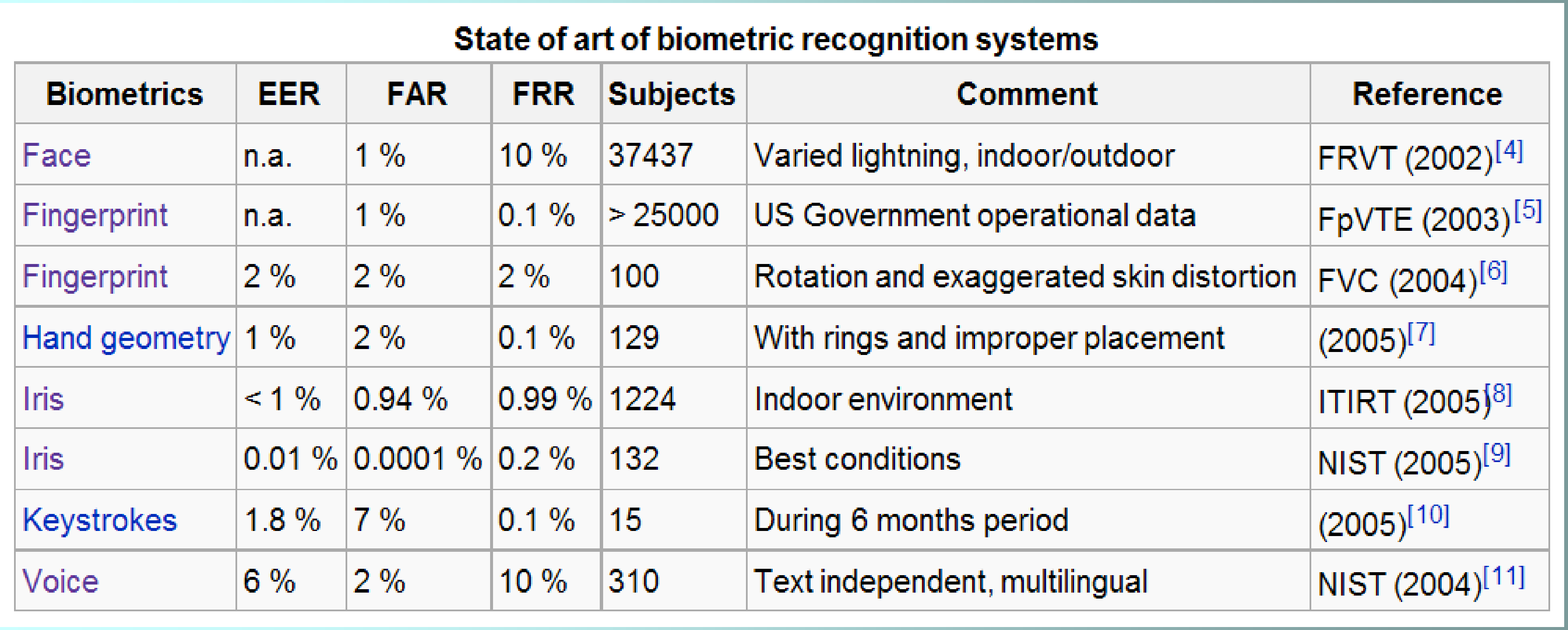
- Plot of prob. of detection (1 – FRR) vs. FAR
- Always above 45 line
- Shows different combinations of (FRR, FAR) at which system can operate.
- Ideal ROC is inverted L
- Power of system = area under ROC curve.



Errors

- A verification system can usually operate at different combinations of (FRR,FAR), by varying the decision threshold.
  - Thus one should always report FRR @ a particular FAR, and never the lowest errors for both.
- Another measure is the Equal Error Rate (EER)
  - This is the error at which FRR = FAR.
- FRR and FAR have different costs.
  - e.g. In an access control application, FRR means user inconvenience, but FAR means security breach.
  - Thus, for particular application, it is usual to set one type of error according to requirements, and let system decide the other.

State-of-the-art errors



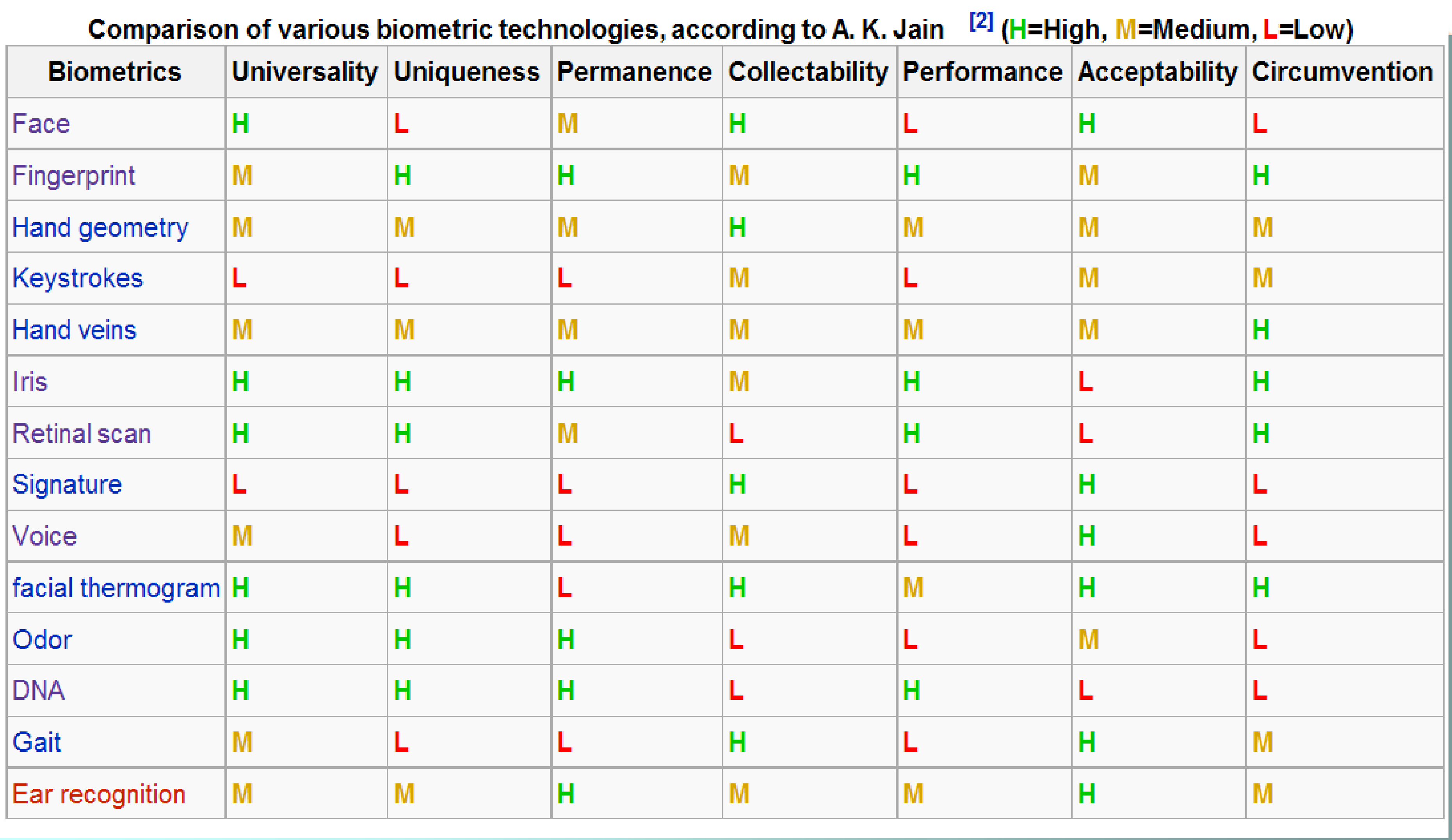
State of art of biometric recognition systems

Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
Face	n.a.	1 %	10 %	37437	Varied lightning, indoor/outdoor	FRVT (2002)[4]
Fingerprint	n.a.	1 %	0.1 %	> 25000	US Government operational data	FpVTE (2003)[5]
Fingerprint	2 %	2 %	2 %	100	Rotation and exaggerated skin distortion	FVC (2004)[6]
Hand geometry	1 %	2 %	0.1 %	129	With rings and improper placement	(2005)[7]
Iris	< 1 %	0.94 %	0.99 %	1224	Indoor environment	ITIRT (2005)[8]
Iris	0.01 %	0.0001 %	0.2 %	132	Best conditions	NIST (2005)[9]
Keystrokes	1.8 %	7 %	0.1 %	15	During 6 months period	(2005)[10]
Voice	6 %	2 %	10 %	310	Text independent, multilingual	NIST (2004)[11]

http://en.wikipedia.org/wiki/Biometric

Jain, A. K. (28-30 April 2004), "Biometric recognition: how do I know who you are?", Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th: 3 - 5

How to measure?



Comparison of various biometric technologies, according to A. K. Jain [2] (H=High, M=Medium, L=Low)

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
facial thermogram	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear recognition	M	M	H	M	M	H	M

7 Criteria

- Universality
  - How common is the biometric across the entire human population?
  - Want something that every human has, not something strange (e.g. width of two noses)
- Uniqueness (a.k.a. Individuality)
  - Is the pattern unique to only one person?
  - How well does the biometric discriminate one person from another?
- Permanence
  - Does the biometric change with age/time?

7 Criteria

- Collectability
  - How easy is it to acquire the biometric sample?
  - Cost of sensors, ease of use, etc.
- Performance
  - Accuracy, speed, robustness of the system
- Acceptability
  - How well do users accept the system?
  - Depends on familiarity, convenience, perception.
- Circumvention
  - How easy is it to fool the system?

7 Criteria

- Universality, Uniqueness, Permanence
  - These are intrinsic properties of the biometric.

- Collectability, Performance
  - These depend on technology, and so will change over time.

- Acceptability, Circumvention
  - These have to do with user perception, deviousness.

Measuring biometrics

- It is clear from table that no biometrics scores *H* across all 7 criteria.

- Thus there is no such thing as “the best biometric”.
  - Only what is appropriate for a particular application.