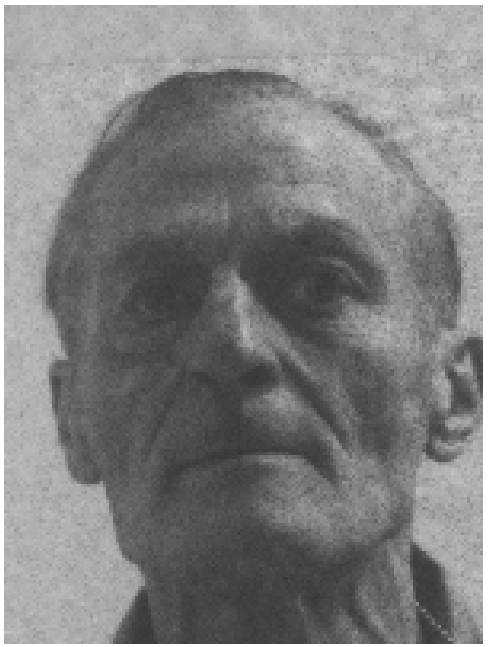
Face Recognition Performance: Man vs. Machine

Andy Adler
Systems and Computer Engineering
Carleton University, Ottawa, Canada

Are these the same person?



Same person? **Yes**

- I have just demonstrated a parallel face recognition computer

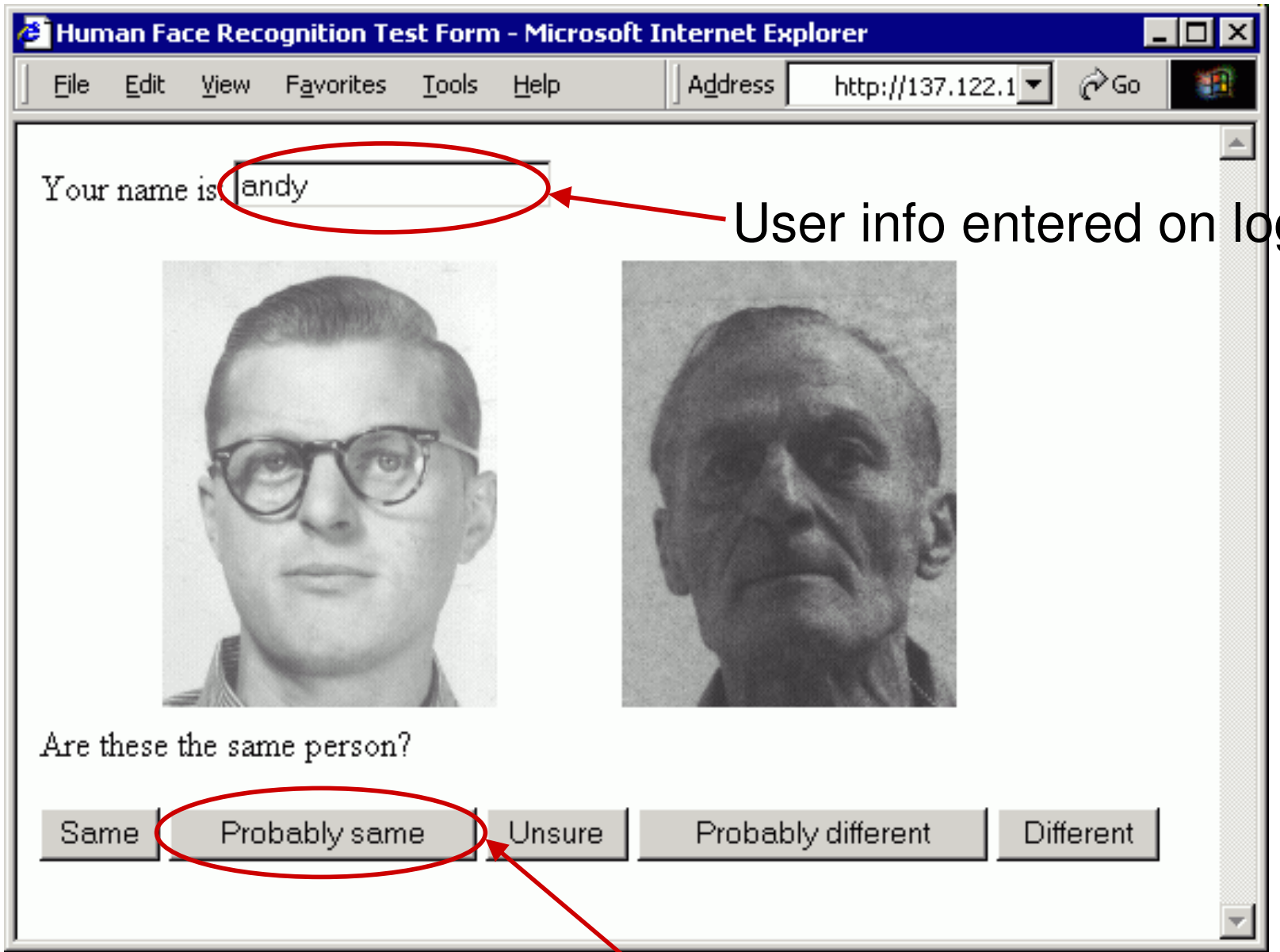
- Of all biometric modalities, automatic face recognition is most often compared to human performance
- Surprisingly little work has been done to quantify these levels of performance

Talk Outline

- Human vs. Machine Face Recognition
- Security issues in Biometrics
- Biometrics Research – current issues

Man vs Machine: Test Design

Participants	Employees of 3M Security Systems Division (then AiT) in Ottawa, Canada
Participation	Voluntary – announcement at company weekly meeting
Participant demographics	16 Male, 5 Female, ages 20-40, predominantly Caucasian
Test format	Web based: subject participated from their office
Instructions	Focus on accurate results



User info entered on login page

Select choice: no time limit

Choice of images

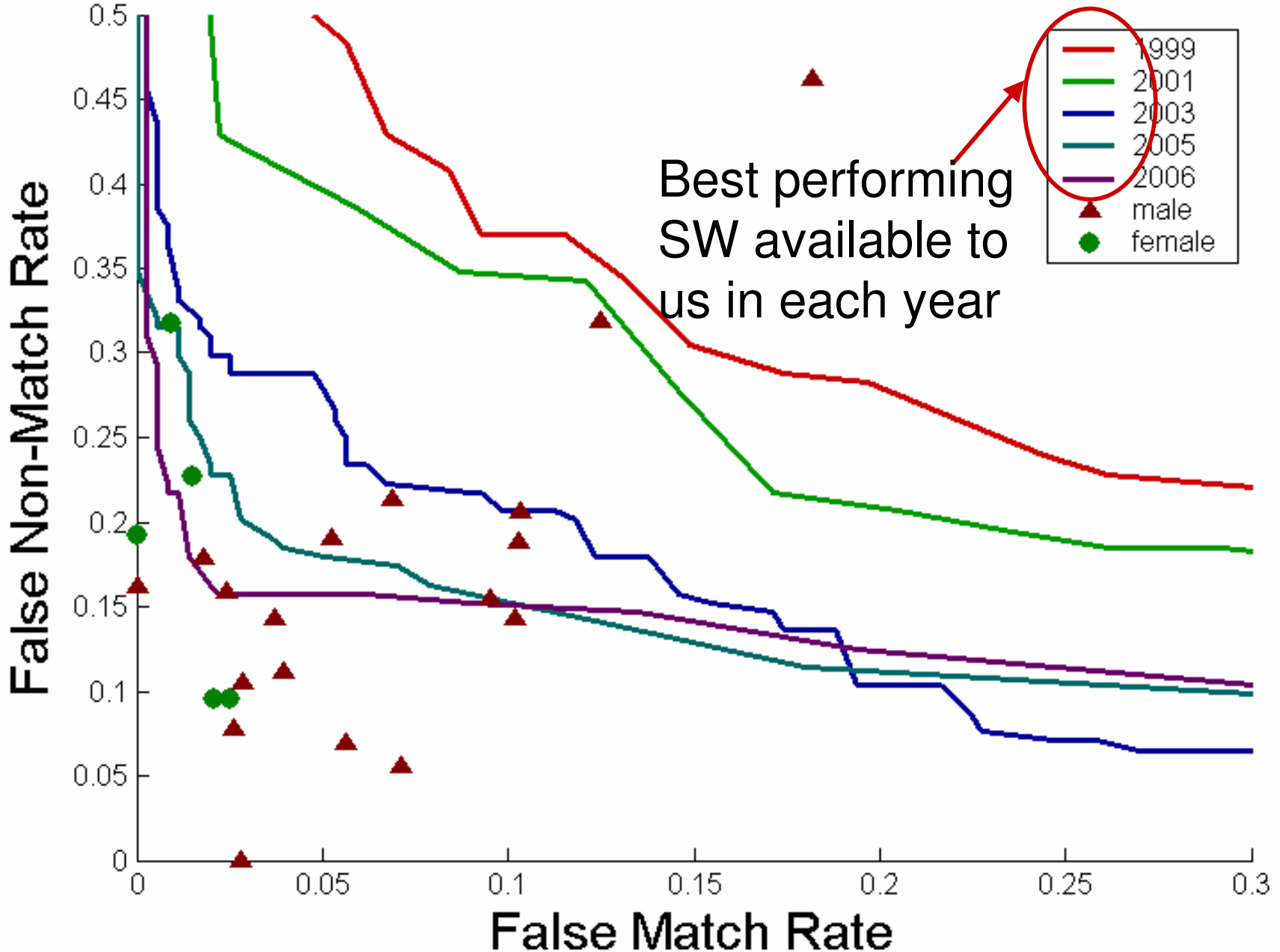
- *Goldilocks* problem:
  Too easy test -> all score 100%
  Too hard test -> all score 0%

- Database used: *NIST Mugshot*
  - Large age changes between captures
  - Population that tends to change appearance

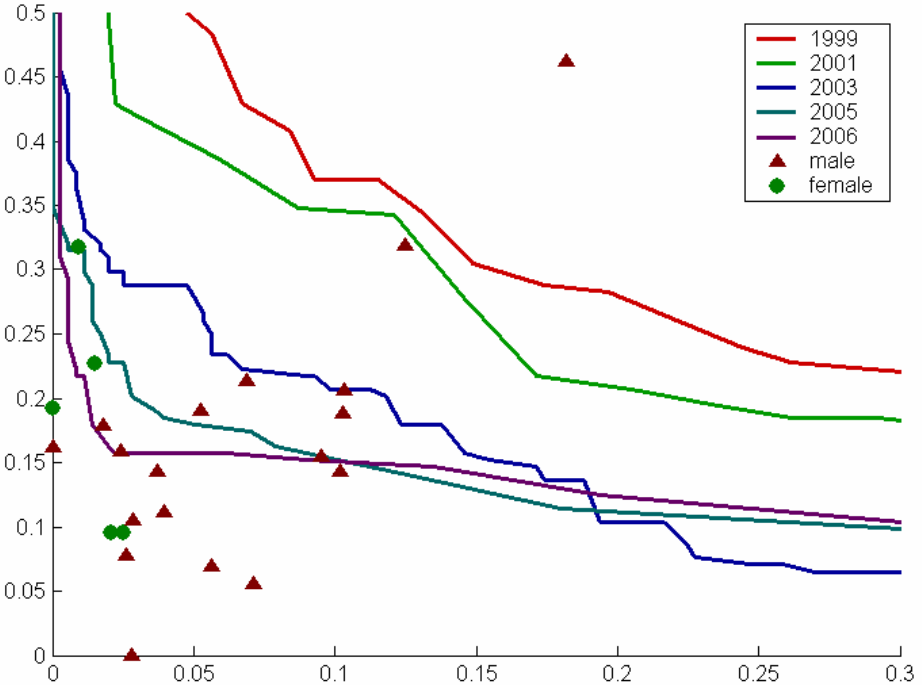
Analysis

- Human results
  - Post-processed to choose optimal “threshold” for them
  - An operating point FMR/FNMR calculated

- Software results
  - Same images presented to FR software (worked with 13 packages and versions)
  - Error tradeoff curve calculated


False Non-Match Rate
False Match Rate
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
0.05
0.1
0.15
0.2
0.25
0.3
1999
2001
2003
2005
2006
male
female
Best performing SW available to us in each year

Results



- Error rates are high
- Significant improvement in SW 1999-2006
- 52% of attentive humans can outperform face recognition software
- No significant difference male/female

Conclusion

- FR software is now equal to untrained human performance, even when humans have the advantages:
  - Unlimited time
  - Motivated
  - Difficult database
  - No gender sorting

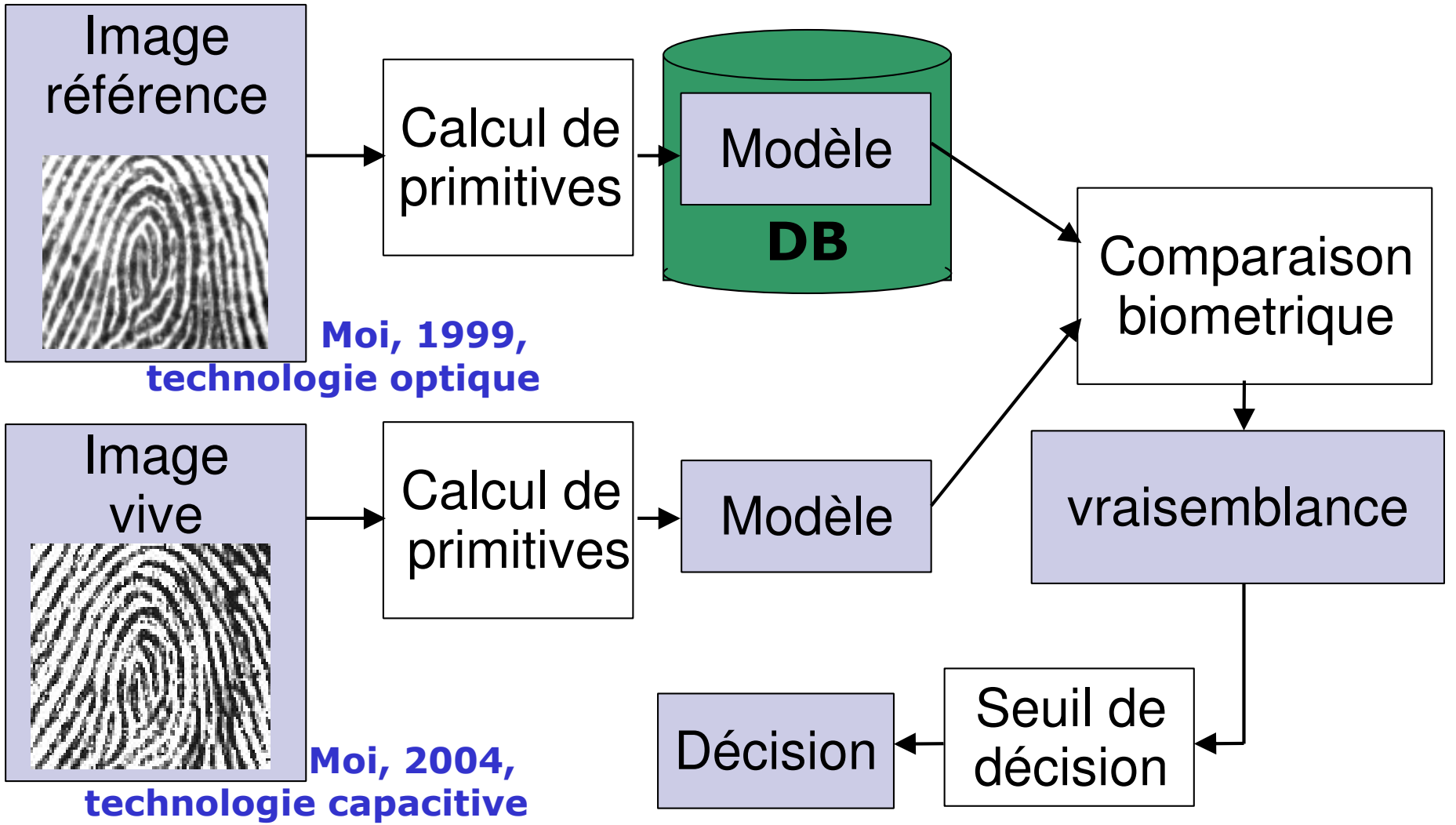
Other work

- Significant body of work in psychological literature about human face rec.
- Much is not of much interest for biometrics
  - Eg. Recognize familiar faces, famous faces
- Recent work in US to look at performance of trained government staff. Classified

Unanswered questions

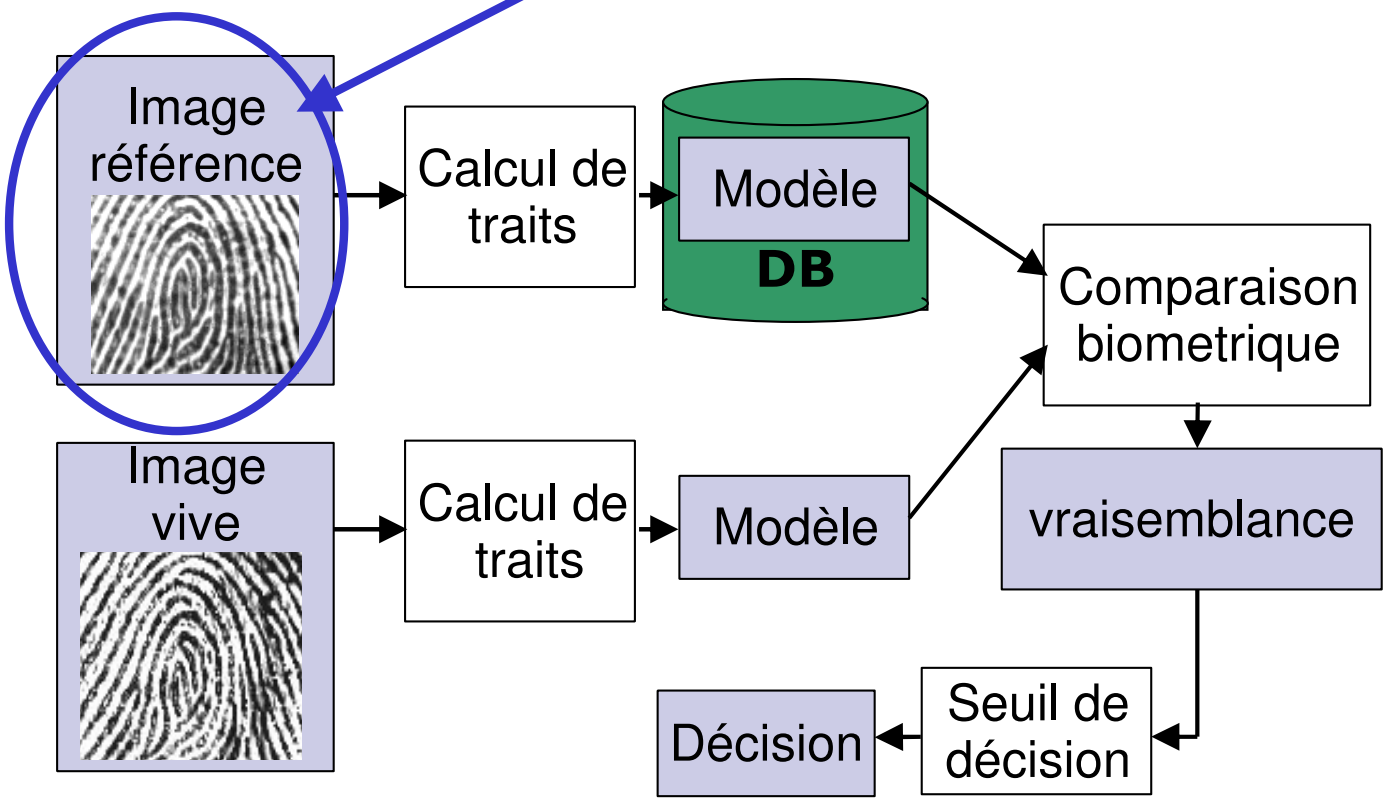
1. What is the effect of motivation, routine and boredom?
2. Do experts outperform untrained recognizers?
3. What distinguishes good recognizers from poor ones?
4. What if a live subject is available / video?
5. Cooperation Human / Machine

Système biométrique



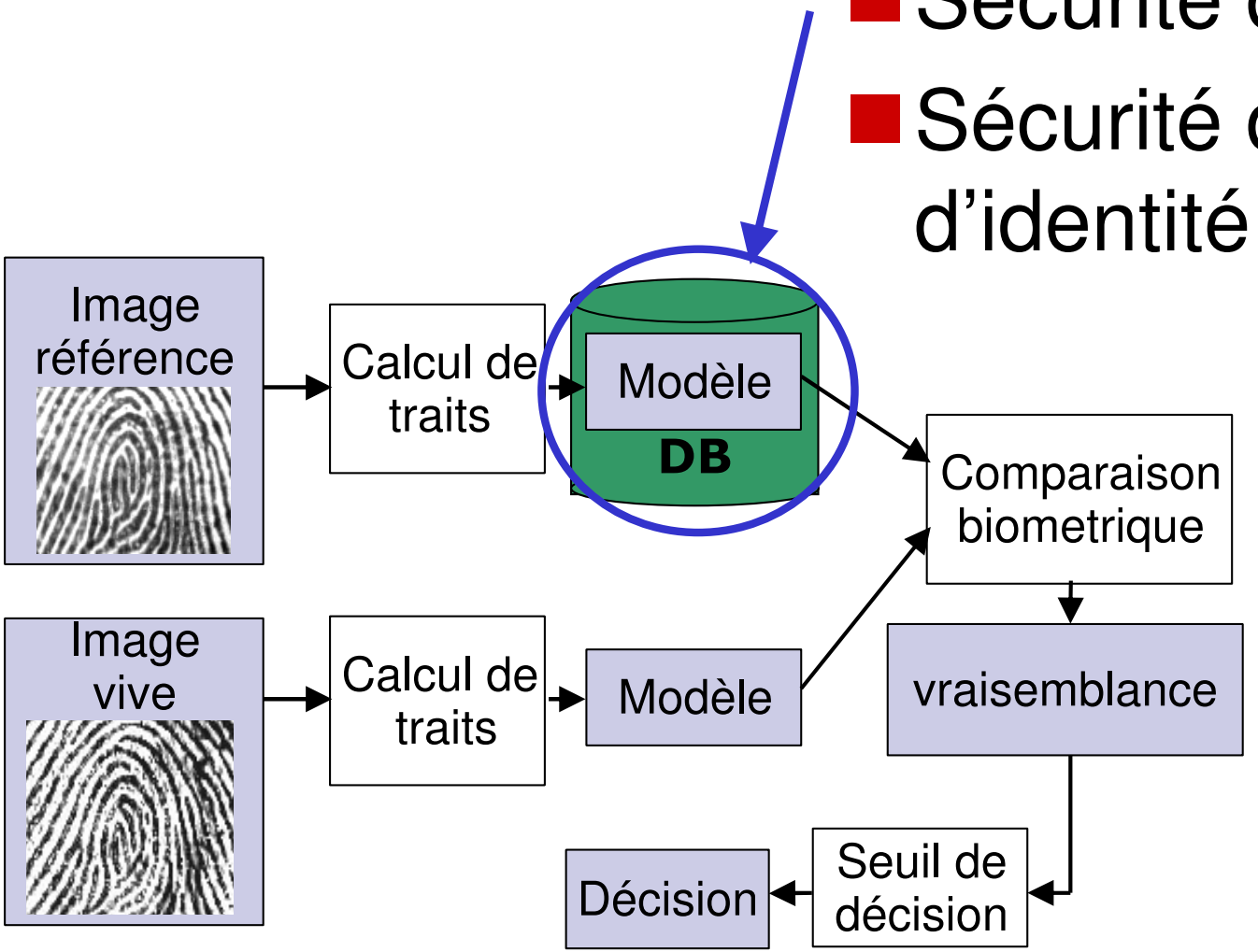
Sources d'erreurs

- Mauvaise qualité
- Tricherie (fraude)



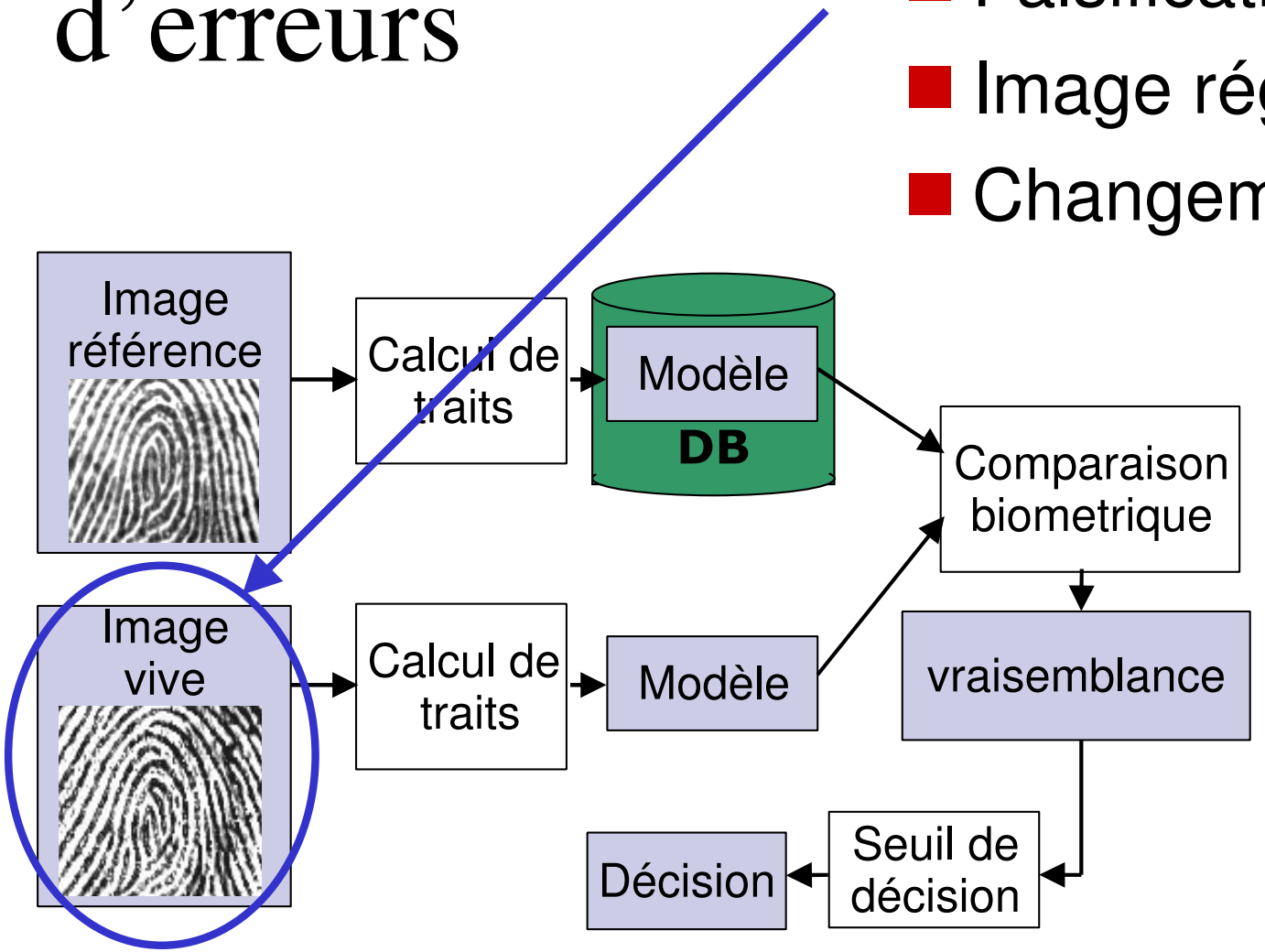
Sources d'erreurs

- Sécurité de la DB
- Sécurité des cartes d'identité

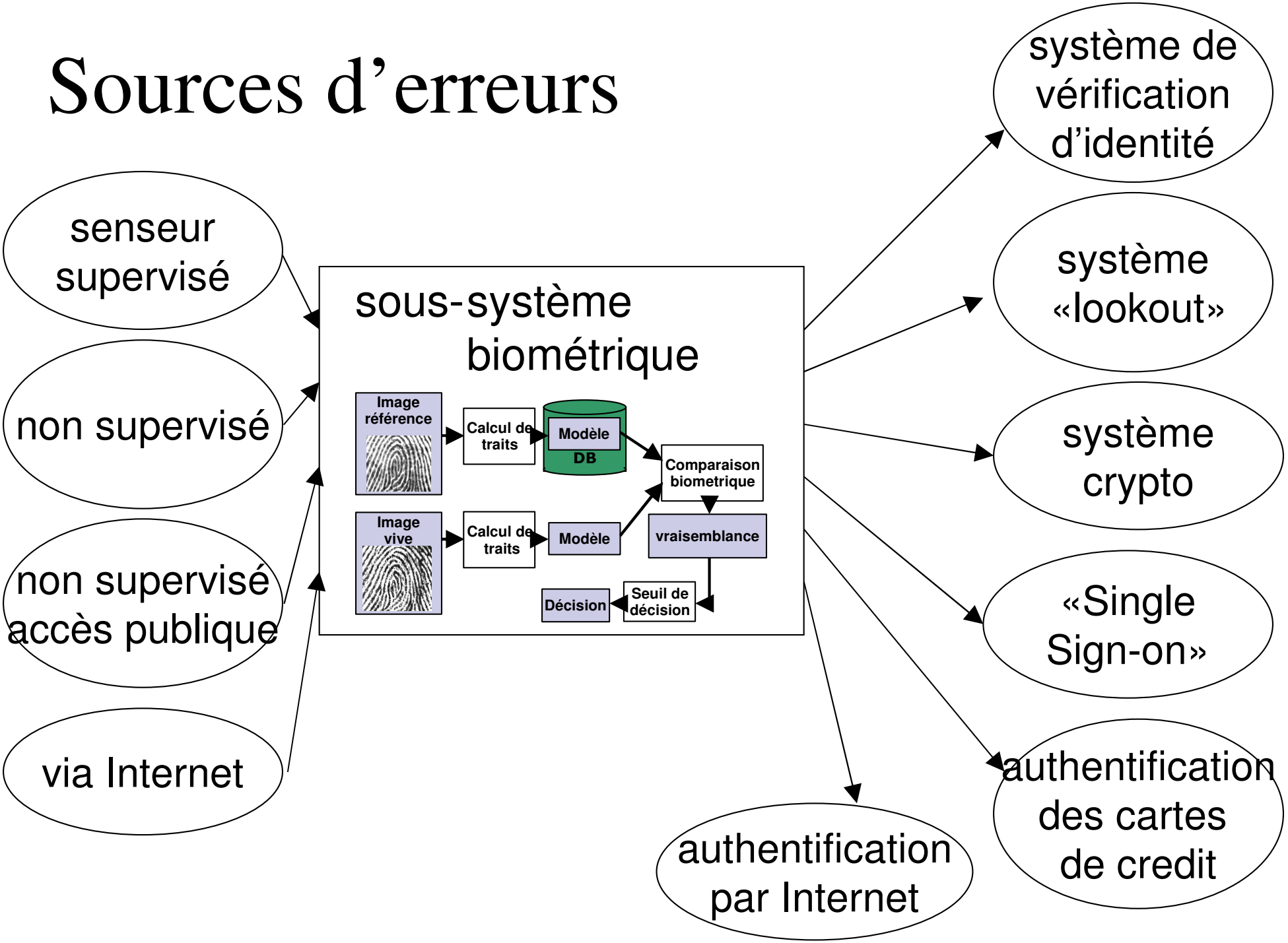


Sources d'erreurs

- Mauvaise image (papier sablée)
- Falsification «Spoof»
- Image régénérée
- Changements avec age



Sources d'erreurs



Exemple: *doigts de ma famille*

Age 4 Age 6 Age 34 Age 35 Age 65

Qui gère l'inscription?

- Scénario #1: ***Gouvernement***
- Exemple: ***Passeport***
- L'empreinte est prise à l'inscription et ajoutée au passeport

Qui gère l'inscription?

- Scénario #2: ***Industrie***
- Exemple: ***Carte de crédit***
- La *signature dynamique* est enregistrée à l'inscription

Qui gère l'inscription?

- Scénario #3: ***Individu***
- Exemple: ***Téléphone cellulaire***
- L'utilisateur s'identifie à son téléphone avec son empreinte

Vulnérable ✗ / *Sécure* ✓	Passe-port	Carte de crédit	Cellu-laire
Vol	✓	✓	✓
Duplication	✓	✓	✓
Vol et modification	½	½	✗
Fraude à l'inscription	½	✗	✗
Falsification «spoof»	½	½	✗
Hameçonnage	✓	✗	✗
Recherche aux poubelles	✓	✗	✓
Données servent ailleurs	½	✗	✓
Soucis vie privée	✗	✗	✓

Biometrics Research: my interests

- Measures of performance
- Face recognition in video data
- Security and privacy
- Cold weather biometrics performance
- Collaboration human / machine