Emerging trends in Biometric Authentication

Christophe Rosenberger
GREYC Laboratory – France
ENSICAEN – University of Caen - CNRS

SHPCS’09
PLAN

- Authentication
- Trends in biometric authentication
- Achievements
- Conclusion & perspectives
**Definition: Authentication**

Process whose objective is to guarantee the identity of a user or a service given a set level of confidence.

**User Authentication**

**Definition: Authentication factors**

An authentication factor is an authenticator element:

- what we know (password),
- what we own (smartcard),
- What we are or how we behave (biometrics).
Biometric modalities:

- **Biological analysis:**
  Odour, blood, DNA...

- **Behavioural analysis:**
  Keystroke dynamics, voice, gait, signature dynamics...

- **Morphological analysis:**
  Fingerprint, iris, palmprint, finger veins, face, ear...
Properties:
A biometric information must respect the following properties:

- **Universality**: All individuals can be characterized by this information;
- **Uniqueness**: The biometric information must be as dissimilar as possible for two different individuals;
- **Permanency**: It must subsist during all individual’s life;
- **Collectability**: The biometric information must be easily computed;
- **Acceptability**: Users must be ready to give this information.
Authentication

Enrolment

Individual’s checkin in the biometric system

- Unique login
- Biometric reference
- Biometric data
- Sensor

Association

System

Storage
Authentication

Verification

Comparison between the capture and the reference

Reference

Comparison System

Result

login + biometric data

Sensor
Authentication

Low threshold: no problem for genuine users but impostors might be authenticated.

High threshold: no impostor but genuine will be disturbed.

Threshold

Repartition

Decision criterion

Similarity

True rejected

Wrong accepted

SHPCS’09
Authentication

Performance evaluation

FAR : False Acceptation Rate
FRR : False Rejection Rate
EER : Equal Error Rate
ROC curve: FAR vs FRR
PLAN

- Authentication
- Trends in biometric authentication
- Achievements
- Conclusion & perspectives
Biometric technology could be more deployed for logical and physical access control applications.

**Needs:**

- High performance biometric systems;
- Embedded device
  - Low memory
  - Quick verification
  - Correctness
Trends in Biometric Authentication

- Definition of unconstrained biometric systems;
  One capture enrolment systems
  Easiness of use

- Evaluation of biometric systems;
  Performance, acceptability, security

- Definition of privacy preserving systems...
  No storage of the biometric reference
**PLAN**

- Authentication
- Trends in biometric authentication
- Achievements
- Conclusion & perspectives
Facial Authentication

- **Enrolment**: 
  - only one image
  - unconstrained acquisition (face detection)
  - extraction of local face characteristics
Achievements

Verification:

- Image capture
- Preprocessing
- Face detection
- Keypoints detection
- Biometric template

Graph matching
Graph representation

Results

- **Faces94 benchmark:**
  - 152 individuals,
  - 20 images per individual.
  - EER = 0.14%

- **AR benchmark:**
  - 120 individuals: 65 men, 55 women,
  - 26 images per individual.
  - EER = 9%
Palm veins authentication

Enrolment with a single image
**EER = 0%** on a benchmark composed of 24 individuals

Keystroke dynamics authentication

Use of release, press and inter keys times during the typing of a password.
5 captures for the enrolment
EER = 6% on a database of 100 individuals

Achievements

4 captures of the same password
Achievements

Evaluation of biometric systems

Analysis the perception of users

Biohashing

Storage of a biocode computed given a random number and a biometric template

PLAN

- Authentication
- Trends in biometric authentication
- Achievements
- Conclusion & perspectives
Biometrics

- **Benefit:**
  Close relationship between the client and its authenticator

- **drawbacks:**
  - performance (EER>0%)
  - acceptability of users

- **Perspectives:**
  - increase the computing performance
  - improve algorithms (performance, robustness…)
  - respect the privacy of users
Questions

christophe.rosenberger@ensicaen.fr
http://www.ecole.ensicaen.fr/~rosenber/

SHPCS’09