CAPTEURS D’EMPREINTES DIGITALES, DÉTECTION DU VIVANT ET SÉCURITÉ

JEAN-FRANÇOIS MAINGUET
MIDI MINATEC : AGENDA

• Qu’est-ce que la biométrie? Comment ça marche?
• Les applications de la biométrie: où la trouve-t-on?
• Les capteurs d’empreintes digitales: comment ça marche?
• Quelle est la précision?
• Peut-on tromper un capteur d’empreinte digitale?
INTRODUCTION TO BIOMETRICS

WHAT IS “BIOMETRICS”?  

- The automated recognition of individuals based on their biological and behavioral characteristics
INTRODUCTION TO BIOMETRICS

CONCEPTUAL DIAGRAM OF A GENERAL BIOMETRIC SYSTEM

Capture (sensor) → Features extraction → Template creation → Template → Associated data → Compare

Enroll

Yes / No

User interface
Policy management
Portal

Compare

Threshold

Yes / No

Feature extraction

Template creation

Associated data

Template

Name, key, bank account…

User interface
Policy management
Portal

Yes / No

Feature extraction

Template creation

Associated data

Template

Name, key, bank account…

User interface
Policy management
Portal

Yes / No

Feature extraction

Template creation

Associated data

Template

Name, key, bank account…
BIOMETRIC MODALITIES

- fingerprint
- palmprint
- pores
- face
- iris
- gait
- fingerprint
- palmprint
- pores
- DNA
- keystroke dynamics
- hand
- finger
- geometry
- signature
- voice
- signature
dynamics
- mouse
dynamics
- tapping
- pulse
- fingernail
- odor
- head resonance
- knuckle creases
- finger wrinkles
- bioelectric field
- Skin impedance
- Hand pressure profile
- Bone sound transmission
- Eye movement tracking
- Dynamic Grip Recognition
- Corneal surface topography
- 3D Finger surface
- EEG, Frontal Sinus
- Nose, Butt
- Skull sound
- skin spectrum
- ear shape
- ear canal
- skin
- spectrum
- dental
- lips
- sweat
- head resonance
- skin
- spectrum
- fingerprint
- palmprint
- pores
- DNA
- keystroke dynamics
- hand
- finger geometry
- signature
- voice
- signature
dynamics
- mouse
dynamics
- tapping
- pulse
- fingernail
- odor
- head resonance
- knuckle creases
- finger wrinkles
- bioelectric field
- Skin impedance
- Hand pressure profile
- Bone sound transmission
- Eye movement tracking
- Dynamic Grip Recognition
- Corneal surface topography
- 3D Finger surface
- EEG, Frontal Sinus
- Nose, Butt
- Skull sound
MODALITIES

Rejected Biometric Technologies

catscan sign-ins

haradse voice i.d.

tongue prints

FEELINGS
The good: it works!

- Many successful applications to date
  - Commercial
  - Government
  - Civil
THE GOOD: IT WORKS!
THE FIRST REVOLUTION

NOTEBOOK COMPUTERS

- The chart shows the trend of new notebook designs from 1998 to 2010, with a significant increase in the years 2005 and 2006.
- The text highlights the first revolution in notebook computers, emphasizing the importance of their widespread adoption.

(Additional context and details based on the images and chart)
THE GOOD : IT WORKS!
THE SECOND REVOLUTION

New fingerprint enabled phone models
(PDA + cell phones = smartphones)

July 2012:
Apple buys Authentec
THE GOOD : IT WORKS!
APPLICATIONS

USB flash disks 2002
Watch 2001
Hard Drive 2002
Safe 2002
Padlock 2005
Time attendance

THE GOOD : IT WORKS!
APPLICATIONS
THE GOOD: IT WORKS!
APPLICATIONS ACCESS CONTROL

Door lock 2004
Turnstile

Marijuana vending machine 2008

Car, truck 1999

Driving school
THE GOOD : IT WORKS!
APPLICATIONS ACCESS CONTROL

Washing machine 2005

Lighter 2016

Coffee 2010
THE GOOD : IT WORKS!
APPLICATIONS

GOVERNMENTAL APPLICATIONS

India is enrolling the full population (fingerprint, iris, face): 1 billion in 2016

One Billion People in Developing Countries Have Taken Part in Biometric Identification Programs: The Use of Biometrics Technology for Development, LMICS, 2012.

- **Latin America & Caribbean**: 34 surveyed cases, covering 280 million people (est)
- **Africa**: 75 surveyed cases, covering 286 million people (est)
- **Asia**: 41 surveyed cases, covering 648 million people (est)

Prevalence of developmental biometrics:
- National: at least one country-wide application (e.g., national ID, elections)
- Subnational: at least one state or ministry-level application (e.g., civil-service payroll, pensions)
- Project: at least one project-level application (e.g., health and demographic survey)
E-PASSPORTS

• Needs for more secured travel documents
• Contactless smart card chip inside the passport containing a copy of the written data
• Requested by USA, standards from the ICAO
THE GOOD : IT WORKS!

- Focus on some modalities
  - Hand (oldest automated biometric modality)
  - Face
  - Iris
  - Fingerprint
FINGERPRINT BASICS
WHAT IS A FINGERPRINT?

- Skin on finger consists of friction ridges with pores (sweat glands)

- Ridge discontinuities are minutiae points
FINGERPRINT BASICS
TYPE OF CAPTURE

• Static: the user just touches the sensing area
• Sweep: the user sweeps their finger across the sensing area
  ▪ Advantage for silicon sensors: less area = less expensive
FINGERPRINT BASICS
TYPES OF FINGERPRINT SENSORS

- **Optical**
  - Reflection FTIR
  - Direct image
    - Structured light
    - Pinhole
  - Transmission
  - OCT

- **Electro-Optical**
  - Piezo-led
  - Emissive polymer

- **Capacitance**
  - Passive
  - Active (RF field)

- **Pressure**
  - Piezo
  - Conductive membrane
  - Tactile (MEMS)

- **Thermal**
  - Passive
  - Active

- **Combination**
  - (whenever possible)
    - Silicon, TFT (glass)
    - Static, swipe
    - Contact, contactless
FINGERPRINT BASICS

CAPACITANCE SENSOR, PASSIVE

- Fingerprint valleys and ridges vary thickness of air dielectric layer, which modulates effective capacitance

CAPACITANCE SENSOR, ACTIVE = RF FIELD

- RF signal sent into the skin and read at pixel level
- Signal crosses the coating via a capacitor
THE BAD: IT DOESN'T ALWAYS WORK…

ACCURACY

Accuracy

Threshold?

Security:
- Cryptography
- Aliveness detection
THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY

SCORING & THRESHOLD

- Is this the same person? Give a note!

Threshold

Accepted

Rejected
THE BAD: IT DOESN’T ALWAYS WORK… ACCURACY

- Accepted false: FAR
- Accepted genuine: FRR
- Rejected genuine: FRR

Score vs. Probability

FAR / FRR

Threshold

Genuine

Impostors
FINGERPRINT ACCURACY
Many different algorithms exist to compare fingerprints

Two common types:

- Minutiae-Based
  - Minutiae locations and directions compared
  - Minutiae are generally mandatory for governmental applications (linked to standards)

- Pattern-Based
  - General shape of the ridges compared
THE BAD: IT DOESN'T ALWAYS WORK…
ACCURACY: DIFFICULT FINGERS
SENSOR SIZE

Same accuracy?
• **The more data, the better**
  - Next Biometrics has ordered the “Madrid report” which shows that size does matter.
    - 3 market leading sensors, 600 people, 180,000 prints and more than 100 million comparisons
  - Apple is the opposite, and do not show any test results.
SPOOFING
THE BAD: IT DOESN'T ALWAYS WORK... SECURITY

“The 6th day”
THE SIXTH DAY
THE SIXTH DAY
THE SIXTH DAY
THE BAD: IT DOESN'T ALWAYS WORK...
SECURITY

BOND . . . JAMES BOND . . .
THE BAD: IT DOESN'T ALWAYS WORK...
SECURITY

Diamonds are Forever (circa 1971)
BIOMETRICS
SECURITY THREATS: SPOOFING

solution:
Aliveness Detection
add specific
sensor(s) + algorithm

Enroll

Simulated or artificial
biometric specimen

Template creation

Features extraction

Associated data

Template

Compare

User interface
Policy management
Portal

Yes / No

Alive / Fake

Threshold

Name, key,
bank account…

Threshold

Aliveness detection
sensor(s)
BIOMETRICS
SECURITY THREATS

Solution: Cryptography

Capture (sensor)

Features extraction

Template creation

Name, key, bank account...

Template substitution, theft, insertion

Compare

Unauthorized user enrolled

Alive / Fake

Modify threshold

Enroll

Verify

Intercept / Insert

Modify threshold

Threshold

User interface

Policy management Portal

Backup system, exception handling procedure

Bypass biometric system

Hardware / Software / Firmware / Network: tamper, modify, bypass, back doors, design flaws, etc.

Modify threshold

Unauthorized user enrolled

Aliveness detection sensor(s)

Template

Enroll

Verify

Intercept / Insert

Compare

Alive / Fake

Modify threshold

Threshold

User interface

Policy management Portal

Backup system, exception handling procedure

Bypass biometric system

Hardware / Software / Firmware / Network: tamper, modify, bypass, back doors, design flaws, etc.

Modify threshold

Unauthorized user enrolled
THE BAD: IT DOESN’T ALWAYS WORK… SECURITY

ALIVENESS DETECTION LEVELS

• Aliveness: hard to detect
  ▪ What is a dead finger?
    A surgeon is able to mend a cut finger (if kept in ice)!
  ▪ Whole hands have already be transplanted from a deceased donor: also the fingerprints!

• Definition of levels:
  ▪ Zero effort: a latent print left on the sensor
  ▪ Fake/copies:
    • Fingerprint image
    • Fake made of gelatin, latex…
    • Thin layer of material glued to a real finger
  ▪ Original finger:
    • Cut out
    • Belonging to a dead person
- CUT FINGER?
Biometric information is often public.
- Think about face recognition!
- You cannot rely on the biometric data secrecy!

Donor cooperation helps but is not mandatory.
- DNA: just pick up organic residues
- Face: a simple photo
- Iris: a good high resolution photo
- Fingerprint: latent prints
- Voice: a recorder
- Hand: a mold
- Vein: no visible trace

Having the original sensor device helps.
- You get a genuine electronic copy!
- And so, you can create a fake to spoof this sensor…
• How difficult is it to make a fake finger?
  ▪ With cooperation
    • Making a mold is quite easy, and you can find information over the Internet.
    • Most articles dealing with this suppose cooperation.
  ▪ From a latent print
    • Having the right latent print is not so obvious. (It is difficult to know which finger it is!)
    • Identifying the latent print is very often difficult, even for a forensic professional.
    • From a good picture, making a mold is not too hard; like a rubber stamp or a printed board.
FAKE FINGERPRINTS

- Many different materials have been tried
  - Gelatin
  - Silicone
  - Rubber
  - Wood glue
  - Hot glue
  - Soft plastic
  - Latex
  - Alginate
  - Clay
  - Glycerin
  - …

- We consider that making a latex copy is difficult, but far from being impossible.
THE BAD: IT DOESN’T ALWAYS WORK… SECURITY

IPHONE 5 & 6

- Touch ID: no aliveness detection
- Authentec said their sensor is working with a live finger…. But never said that fakes are also working!
• First real known case

- Malaysia end of March 2005, where a team of carjackers on the prowl in Subang Jaya chopped off part of the left index finger when they realized that the S-Class Mercedes Benz had a security feature which would immobilize the car without his fingerprint.
SPOOFING

- **Graft**
  - George attempted to enter the U.S. illegally on September 24, 2005 through the Nogales, Ariz. Port of Entry during which time U.S. Customs and Border Protection officers noted that his fingerprints had been surgically replaced with skin from his feet.
  - George stated that this procedure had been done to “clean” his identity by a doctor in Phoenix.
THE BAD: IT DOESN’T ALWAYS WORK… SECURITY

SOME ALIVENESS DETECTION SYSTEMS

- Skin impedance (Guardware)
- Skin distorsion (Maltoni)
- Perspiration (Schuckers)
- Pulse oximetry
- Red eye
- Eye blink
- pupillary light reflex / hittus

- Skin spectrum (Lumidigm)
- 3M Biosentry ultimate (1996) pulse detection + EKG

- Fourier analysis

- Natural iris
- Fake iris printed on a contact lent
- 2D Fourier spectrum of natural lent
- 2D Fourier spectrum of fake lent printed on a contact lense
THE BAD: IT DOESN’T ALWAYS WORK…
SECURITY

ALIVENESS DETECTION

• What Liveness Testing IS:
  ▪ A means to minimize the effectiveness of artificial or simulated biometric specimens and thus improve the security posture of the biometric system.

• What Liveness Testing IS NOT:
  ▪ A guarantee that the biometric specimen belongs to the authentic live human being.

• “If man can make it, man can break it!”

Your fingerprint!
QUESTIONS?

“This new Apple iPhone is great. It takes high quality pictures and recognizes my fingerprint. It's just like when I get arrested.”
MERCI POUR VOTRE ATTENTION