Seminar 12:
Biometric authentication

PV181 Information security and cryptography

Agáta Kružíková, kruzikova@mail.muni.cz

Katarína Galanská, xgalansk@fi.muni.cz

Overview

This week

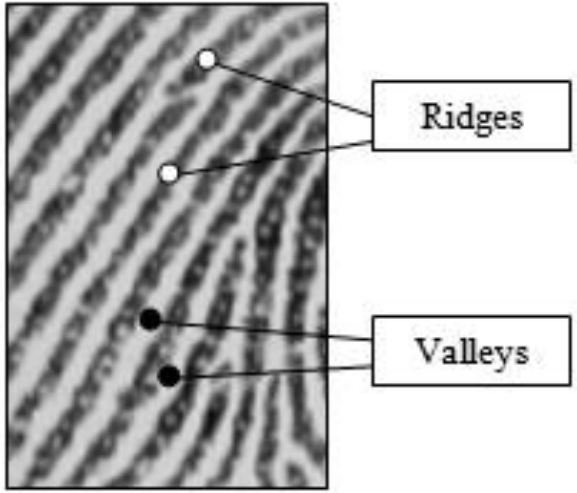
- Intro
- Practical part I: Fake fingerprints creation
- Biometrics and fingerprint theory
- Practical part II: Testing and processing fake fingerprints

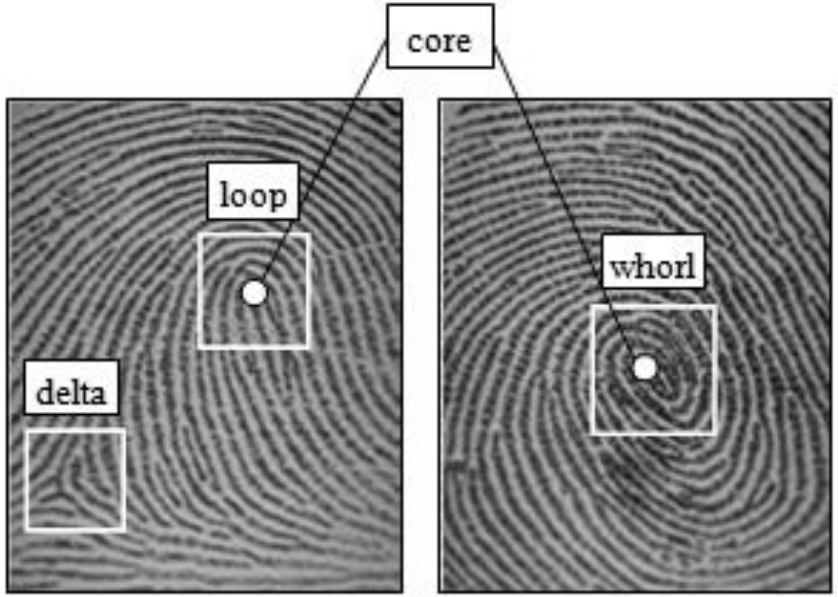
Biometric authentication

1. “Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).”
   (See: Handbook of Applied Cryptography)

2. Authentication based on:
   - something I know (e.g., password)
   - something I have (e.g., access card)
   - **something I am (e.g., fingerprint)**
   - something where I am (e.g., location)

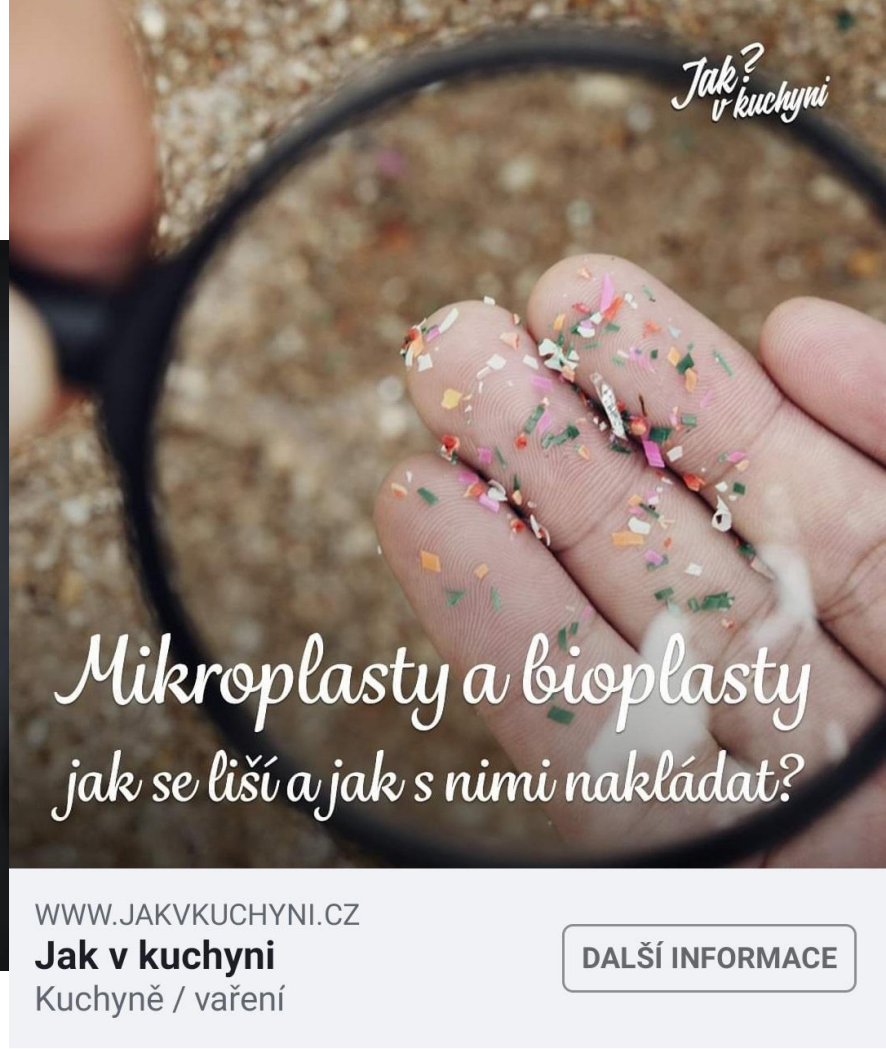
Fingerprint characteristics





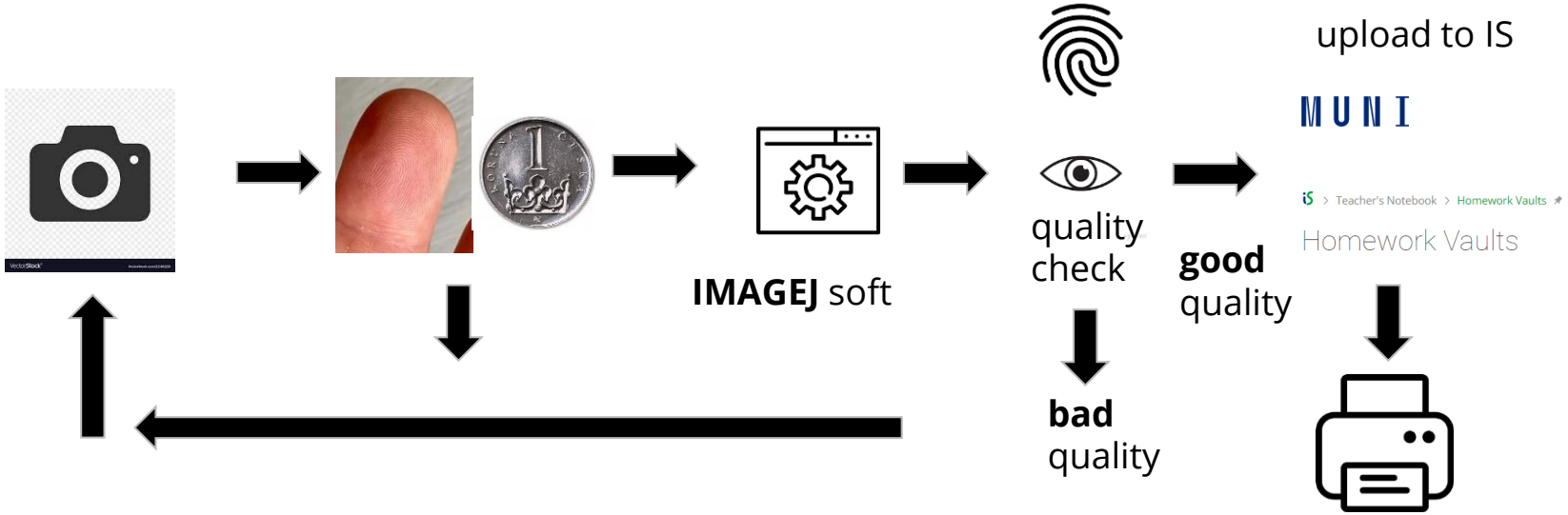
Practical part I

Motivation



Source: https://www.pexels.com/photo/close-up-of-human-hand-327533/

Process diagram and software (part 1)



(Pre)Step I: Take a photo of your finger

- Choose one finger
- Put a coin (ideally 1 Kč) next to the finger for scale (there should be space between coin and finger)

- A light source (e.g., a window) should be on one side
- Sharp, good quality (500+ pixels in height)
- Try multiple times to achieve the best result

(Mid)step: Check if you have correct photo

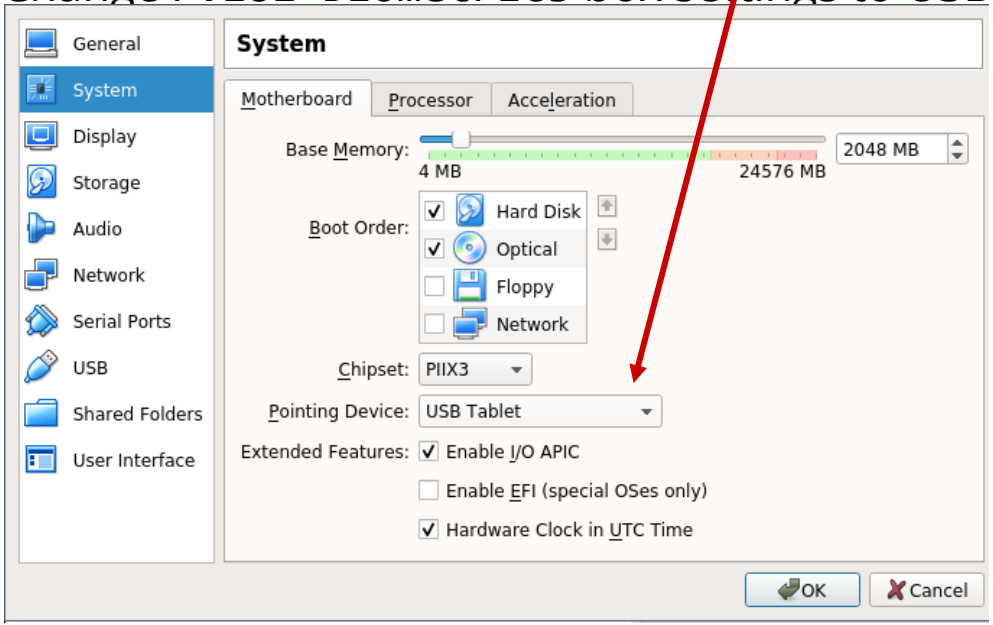
- Coin distance matters!
- It should be at the same level as the fingertip

PreStep: Setting up Virtual Machine

- Software which you need for today's seminar are preinstalled in Ubuntu VM
- Run Oracle VM VirtualBox 6.1
- **File** → **Import Appliance** `PV181 Biometrics.ova`
- Add extension **File** → **Preferences** → **Extensions** → **Add a new package** `Oracle_VM_VirtualBox_Extension_Pack-6.1.32.vbox-extpack`
- You can find all files in IS

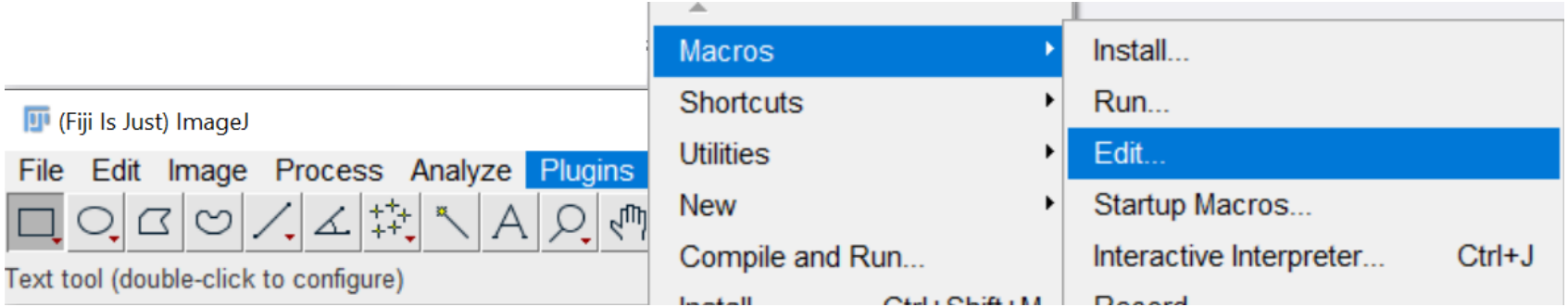
[Debug] Virtual Machine

- In case you **don't see a mouse pointer** in the box
  - Change `PV181 Biometrics` box settings to USB Tablet

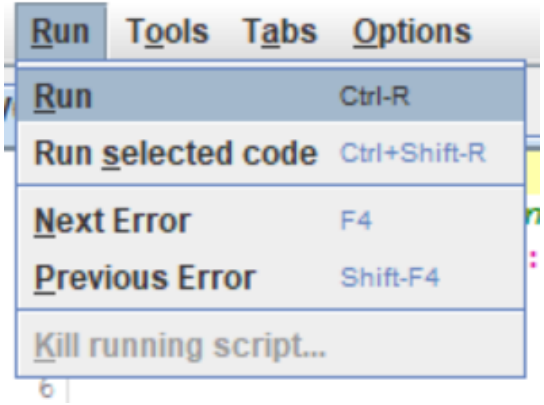


Step II: Process the photo

- Launch **ImageJ** (win-key and write ImageJ, click on the icon, not at the link!)
- Open the script: `/home/pv080/FingerprintProcessing/PV181script.ijm`
- Using **Plugins** → **Macros** → **Edit**



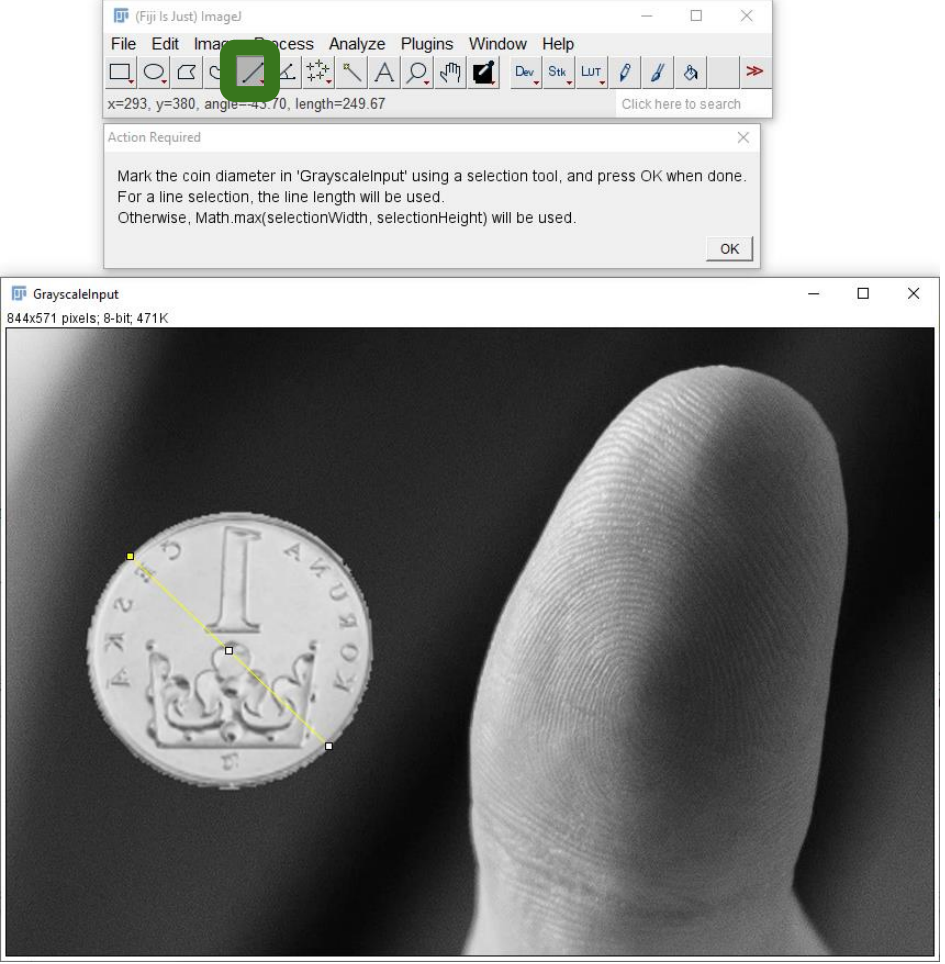
Step II: Process the photo



- In newly opened window → **Run** → **Run**
- Select your photo
- **Open**
- Mark a coin and a finger manually (see next slide)

Step II: Process the photo

- Mark coin diameter (select **Straight**)
- Mark only fingertips (it is better to cut a piece of finger than include the background) (select **Polygon selection**)
  - Nails mark as a part of background (do not include them into selection)
- **Firstly mark it and then press OK**


(Fiji Is Just) ImageJ
File Edit Image Process Analyze Plugins Window Help
x=293, y=380, angle=-43.70, length=249.67
Click here to search
Action Required
Mark the coin diameter in 'GrayscaleInput' using a selection tool, and press OK when done.
For a line selection, the line length will be used.
Otherwise, Math.max(selectionWidth, selectionHeight) will be used.
OK
GrayscaleInput
844x571 pixels; 8-bit; 471K


Mark the finger selection in 'GrayscaleInput' using a selection tool, and press OK when done.
OK
(Fiji Is Just) ImageJ
File Edit Image Process Analyze Plugins Window Help
Click here to search
GrayscaleInput
844x571 pixels; 8-bit; 471K

Step II: Example of a correct output log

Log

File Edit Font

```
Opening /home/pv080/FingerprintProcessing/Example.tif
Coin marked manually.
Coin marked manually with radius = 126.5484 pixels, image DPI = 321.433
Finger selection marked manually.
Finger width: 178.0512, finger scale = 0.3561
Median filtered
Background subtracted
MedianWithoutRidges CED filtered
Starting Gabor filtering (Python script)...
Gabor filtering done
```

Step II: Process the photo

- Final files named **ForPrintWithoutGabor.tif** and **ForPrintGabor.tif** will be created and saved in the same directory as your photo file
- Use both files for the next steps
- You can repeat the process multiple times, but before running the script in ImageJ again, **rename the previous ones** (otherwise files will be **overwritten**!)
  - E.g., rename output files **ForPrintWithoutGabor.tif** and **ForPrintGabor.tif** to **ForPrintWithoutGaborX.tif** and **ForPrintGaborX.tif** where X=1, 2…
- Files will be saved next to your original files

Step IV: Print (done by tutors)

- Upload the best results (two files) “**ForPrintWithoutGabor.tif**” and “**ForPrintGabor.tif**” into IS Homework Vault → we’ll print it for you onto plastic foil (and then instantly delete it)
- Homework Vault:

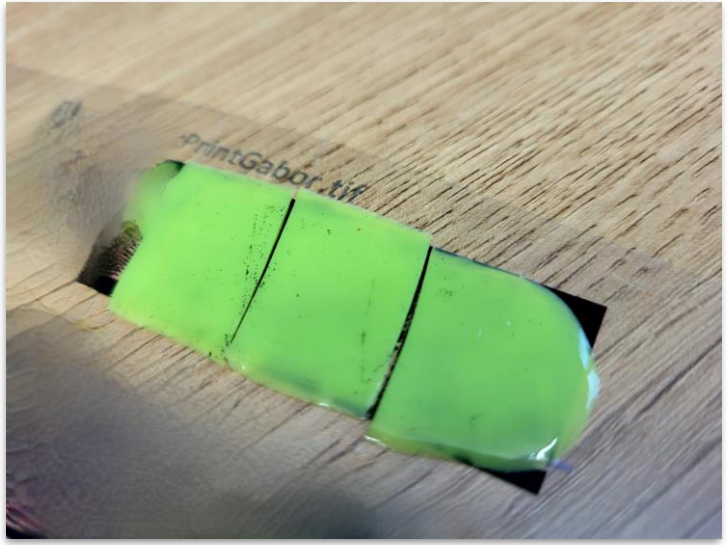
  https://is.muni.cz/auth/el/fi/podzim2022/PV181/ode/133910660

Midstep: Scanning (When waiting)

- Scan your genuine fingerprint which you are trying to fake (ask teachers for fingerprint reader)
- In terminal, type:
  Live finger: `StartFingerScanner -u Live`
  - Mark `invert`
  - Click `Scan`
  - Scan the same fake finger multiple times
  - Save 10 **good** scans (while scanning click on **Stop** and then **Save**)

Step V: Covering in silicone

- The silicone will form a copy of your finger (at all 5 samples)
- Avoid pushing the silicone into the form
- Ask tutors for silicone
- You have **90 seconds** to work with the material!

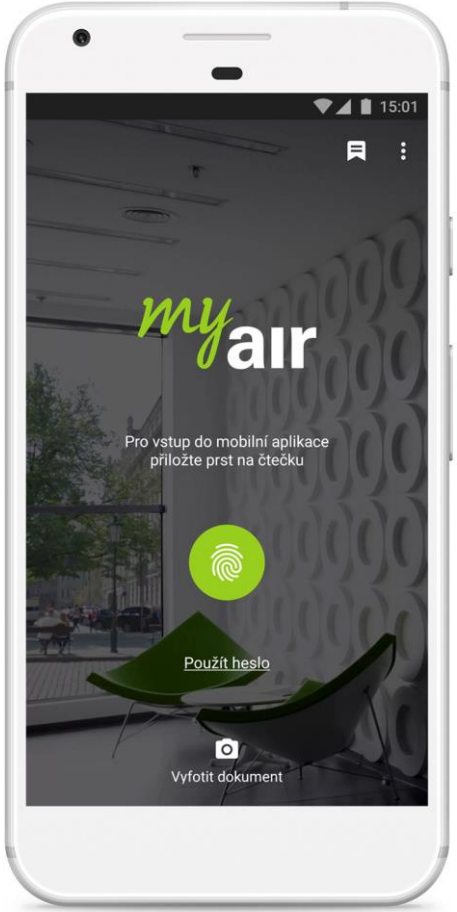


Biometrics

“What uses of biometrics have you seen in your life?”

Biometrics now (optimistic)

- Smartphones
  - Fingerprints, face
- Passports
  - Fingerprints, face
- Contract signing
  - Signature
- Nuclear power plants :-)
  - Dukovany use hand geometry



Biometrics (pessimistic)

- Fingerprint reader end-user licence agreement: “The biometric (fingerprint reader) feature in this device **is NOT a security feature and is intended to be used for convenience only**. It Should not be used to access corporate networks or protect sensitive data, such as financial information.”
- Used in 2005
- Other problems
  - Unencrypted transfer, liveness detection, ...

Biometrics soon (maybe)?

- MasterCard Identity Check Mobile
  - Prove holder's identity by fingerprint/selfie
  - Blinking/nodding as liveness testing
  - Being introduced in 12 EU countries
  - Supported by Alibaba e-shop
  - **"Selfies to kill off passwords 'in five years' says MasterCard in 2015.**

Source: http://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/

Recap: What are the basic criteria for biometrics?

- **Uniqueness** (sufficiently different across population)
- **Universality** (everybody has it)
- **Permanence** (invariant in the period of time)
- **Collectability** (possible to measure and digitize it)
- **Performance** (recognition accuracy should be good)
- **Acceptability** (individuals should be OK to present it)
- **Circumvention** (hard to fake)

(See: Handbook of biometrics)

Recap: What are the basic criteria for biometrics?

- Compare these criteria for fingerprint vs. face recognition:
- **Uniqueness** (sufficiently different across population)
- **Universality** (everybody has it)
- **Permanence** (invariant in the period of time)
- **Acceptability** (individuals should be OK to present it)

Authentication types and error rates

Verification

- One to one.
- Determines if person is who he claims to be.

Identification

- One to many.
- Search entire database.
- Determine identity of person.

Authentication types and error rates

Verification

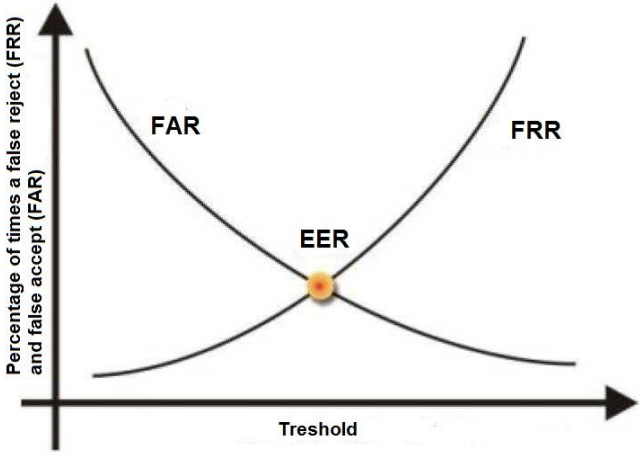
- One to one.
- Determines if person is who he claims to be.

Identification

- One to many.
- Search entire database.
- Determine identity of person.

What could go wrong?

- Never 100% match (error rates)
  - **FAR** (false acceptance rate)
    - **Security issue**
  - **FRR** (false rejection rate)
    - **Usability issue**
  - **EER** (equal error rate)



Commercial vs. forensic use

Commercial

- Low precision
- Enrollment can be repeated
- Only extracted characteristics saved
- Fast and automatic

Forensic

- High precision
- Enrollment just once
- Full biometric data saved
- Slower, expert interventions may be necessary

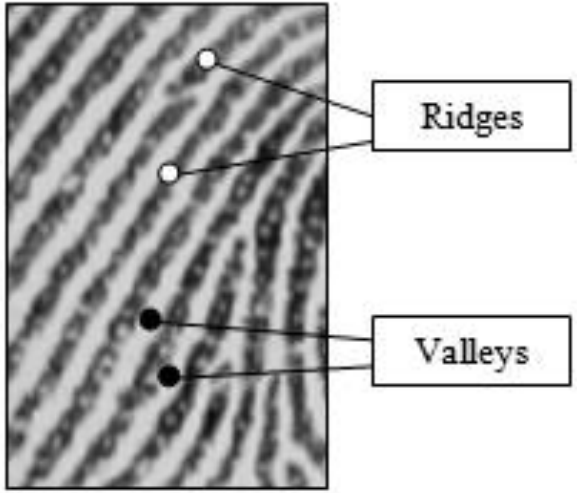
Biometrics – basic problem?

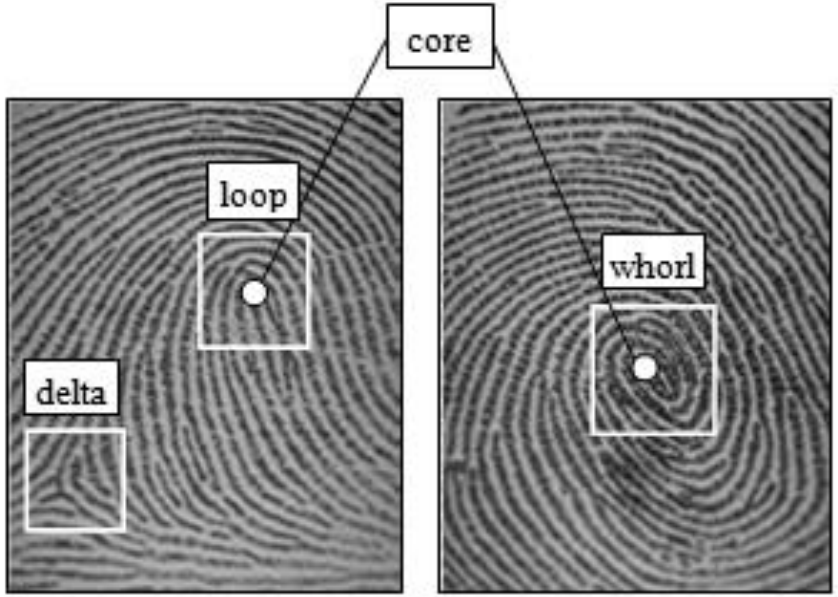
Biometrics are not secret!

And cannot be changed…

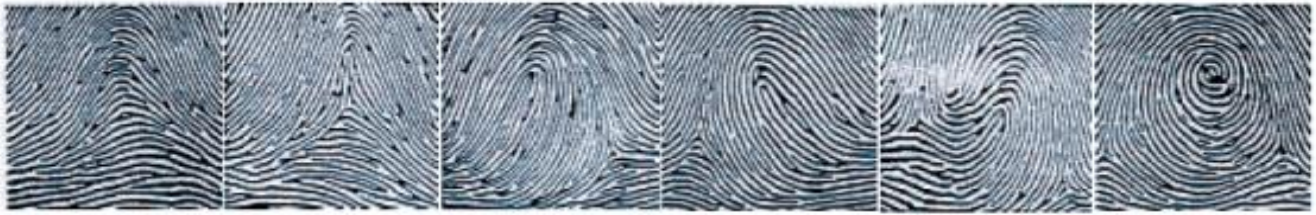
Fingerprints

Fingerprint characteristics



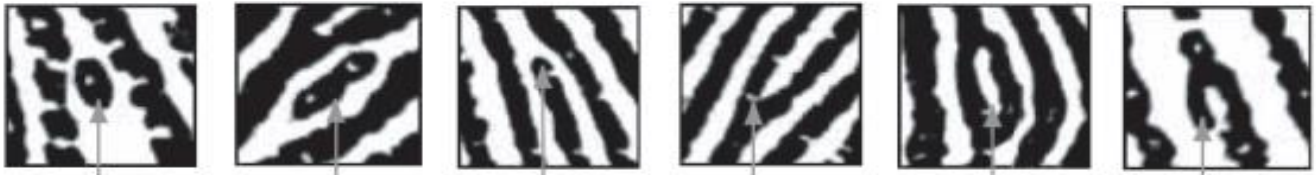


LEVEL 1 FEATURES



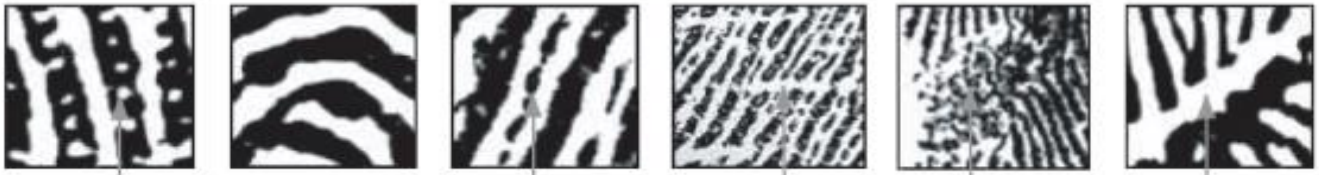
ARCH | TENTED ARCH | LEFT LOOP | RIGHT LOOP | DOUBLE LOOP | WHORL

LEVEL 2 FEATURES



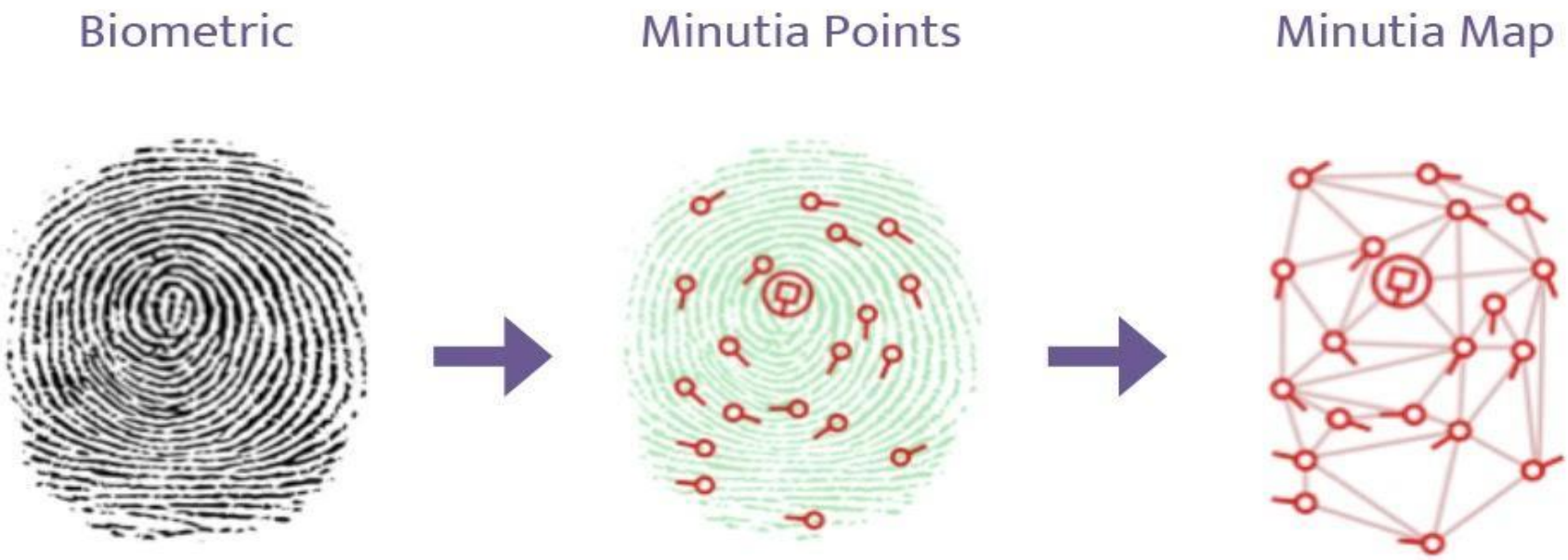
LINE-UNIT | LINE-FRAGMENT | ENDING | BIFURCATION | EYE | HOOK

LEVEL 3 FEATURES

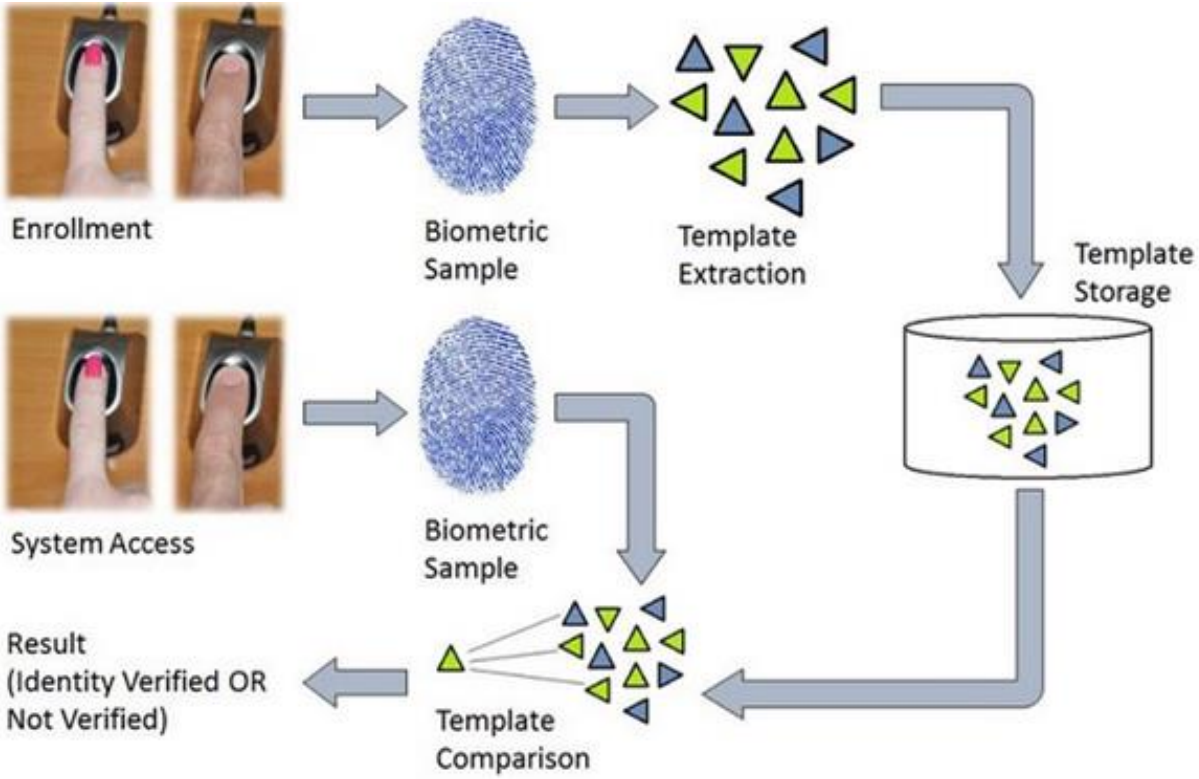


PORES | LINE SHAPE | INCIPIENT RIDGES | CREASES | WARTS | SCARS

Fingerprint minutiae



Fingerprint authentication



Fingerprint readers: Optical and Capacitive

- **Optical**
  - Basically 2D picture
  - Oldest technology
- **Capacitive**
  - Arrays of tiny capacitor circuits → ridges change stored charge (touch), but valleys do not (air)
  - Material matters!
- **Ultrasonic**
  - Signal return time
  - Oftenly in-display sensors

Fingerprint readers: Optical and Capacitive

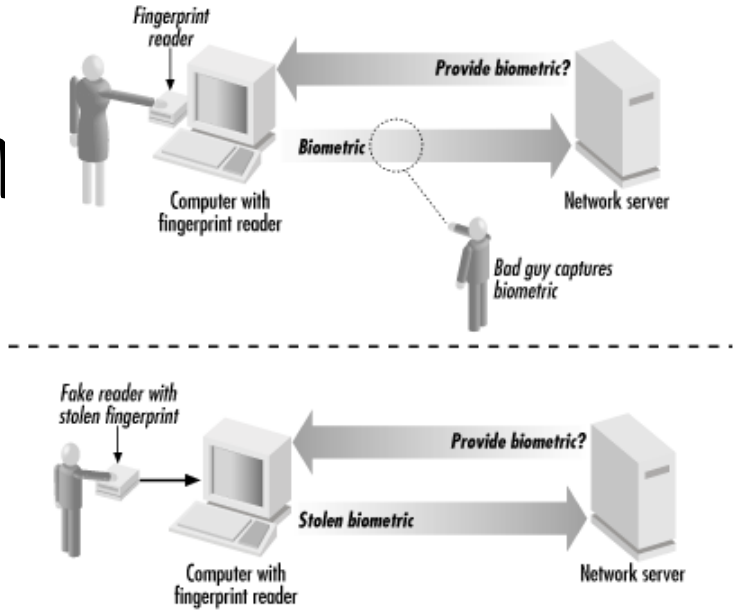
- **Optical**
  - Basically 2D picture
  - Oldest technology
- **Capacitive**
  - Arrays of tiny capacitor circuits → ridges change stored charge (touch), but valleys do not (air)
  - Material matters!
- **Ultrasonic**
  - Signal return time
  - Oftenly in-display sensors

- Are smartphone readers different from external readers?
  - https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

How can we detect that a sample is from a live person?

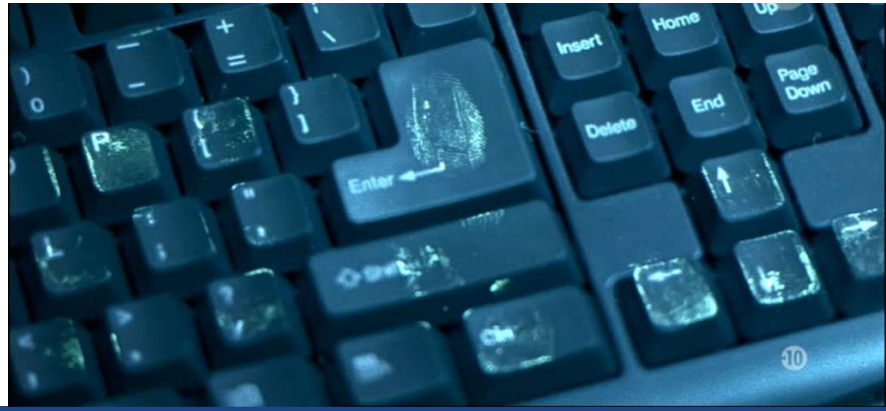
- **Testing the finger reaction to sensor stimuli**
- **Measurement of:**
  - Temperature
  - Skinfinge resistance
  - Pulse/blood flow
  - (See: Handbook of biometrics)

Attacks and liveness detection



Source: https://www.oreilly.com/library/view/web-security-privacy/0596000456/ch06s02.html

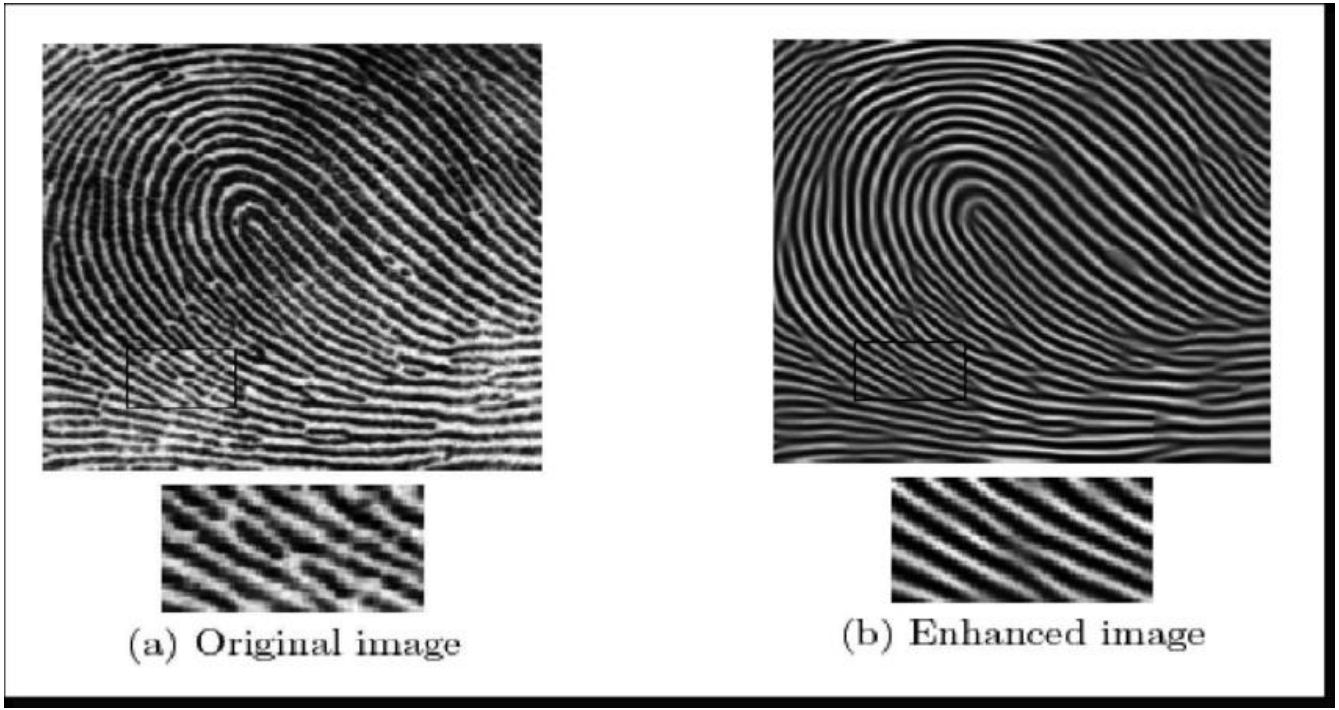
Source: https://medium.com/@alex.kilpatrick/biometric-spoofing-9b613e4c5e3a



Practical part: What was happening on the background

- Why is the result a 1-bit black/white image with clear ridges?
  - Foil needs to have ridges when printed! (that's why B/W)
  - Your tutor already processed the scan from the reader into B/W image for you
- The files already contain scale information for printing (if you took the photo correctly)
- What does Gabor filter enhancement do? Check saved files

Practical part: Gabor filtering



Sallal, Kawthar & Rahma, Abdul Monem. (2006). Cryptographic Keys Generation Using Biometric Technologies.

Fingerprint processing

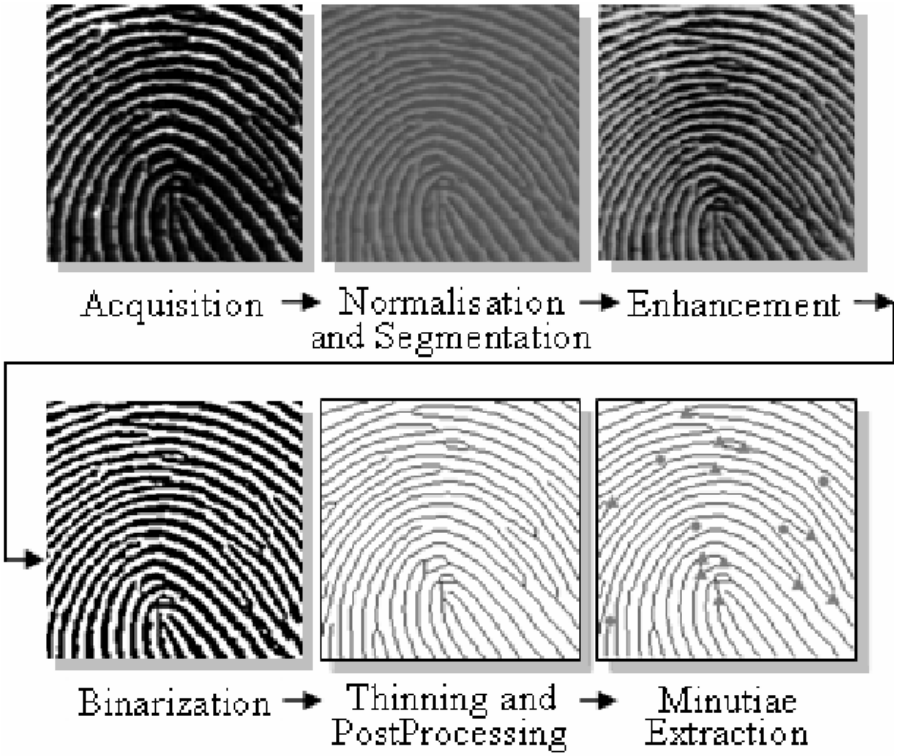


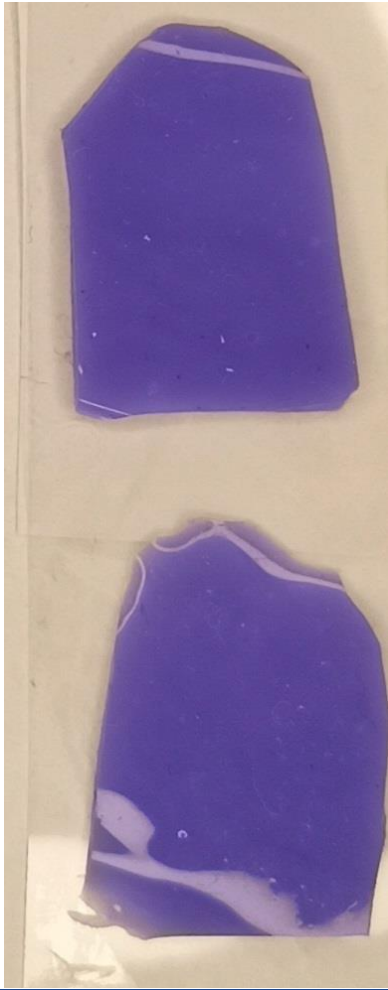
Fig. 1. Minutiae extraction process.

Milici, G., Raia, G., Vitabile, S., & Sorbello, F. (2005). Fingerprint Image Enhancement Using Directional Morphological Filter. *EUROCON 2005 - The International Conference on "Computer as a Tool", 2*, 967-970.

Practical part II

Step VI: Cut out the fake

- Peel the silicone off the foil when dry (after cca 15 minutes)
  - Printing ink should not peel off
  - If applicable, remove the ink from the silicone
- Cut out the silicone around the fake fingerprint (you will get finger shaped form as shown on the right)



Step VII: Using a falsificate

- Try to verify the fingerprint on the reader
  - Read the finger and fake
  - Do visual comparison
  - Do automatized comparison (see next slide)

Midstep: Scanning

- Scan your genuine fingerprint which you are trying to fake (ask teachers for fingerprint reader)
- In terminal, type:
  Live finger (if not done yet): `StartFingerScanner -u Live`
  Fake finger: `StartFingerScanner -f -u WithoutGabor`
  `StartFingerScanner -f -u`
  - Mark `invert`
  - Click `Scan`
  - Scan the same fake finger multiple times
  - Save 10 **good** scans (while scanning click on **Stop** and then

Step VIII: Scan postprocessing

Use the NIST Biometric Image Software (NBIS):

- Work in terminal (`Ctrl + Alt + t` or search for `term`)
- Postprocess all scans:
  - Run the script in the terminal: python gabor.py
- Create minutia map and compare fingerprints
  - Run the script in the terminal: `python nbis.py`
- Check result file `summary.txt`

Step VIII: Scan postprocessing (background)

- NIST Fingerprint Image Quality (NFIQ)
  - The output ranges from **1** (best quality) to **5** (worst quality)
- Create minutia map (MINTCT)
  - Minutia detection system
  - Create a minutia map in the .xyt
  - Check the number of identified minutiae in the new .min file.
- Compare the fake and the real fingerprint scans (BOZORTH3):
  - Compute the match score
  - A score above 40 means a true match (in this software)

Step VIII: Smartphone hacking

- Do it in this order!
- Prerequisite 1: Smartphone with fingerprint reader
- Prerequisite 2: Genuine fingerprint registration
- Counterfeit login (before counterfeit registration)
- Counterfeit registration
- Counterfeit login (after counterfeit registration)

Step IX: Submit your results (voluntary)

- Help us to improve the seminar for the next semester
- Submit results from smartphone hacking into the questionnaire: https://survey.fi.muni.cz/index.php/934171?lang=en
- Rename `summary.txt` with unique identification of your choice
- Upload renamed summary.txt file into IS File Vault: `https://is.muni.cz/auth/of/1433/PV181/podzim2022/`

Homework: Faking other biometrics

- Write a short report (2+ pages) summarizing current
- Usage and current faking techniques for a biometric
- System of your choice (but not fingerprint).
  - Deadline: 14. 12. 2022 8:00
  - Up to 10 points awarded (see the scoring rubric)
  - Submit a single PDF file to IS MUNI
  - File automatically prefixed by you name and UČO
  - **Cite all your references properly! (blogs, news, ...)**
  - **Be concise using mostly your own words**