Biometrics - IT00207/IT28X07

Lecture 2: Hand Geometry and Fingerprint Recognition

Dr. DT van der Haar

Academy of Computer Science and Software Engineering
University of Johannesburg

1 Hand Geometry
- History
- Technology
- Acquire Biometric
- Uses
- Robustness and Accuracy
- Vulnerabilities

2 Fingerprint Recognition
- History
- What is a fingerprint?
- Minutia
- Fingerprint points of interest
- Authentication
- Identification
- Minutia
- Levels of Minutia

- Sources of difference
- First Age of Automation
- Second Age of Automation
- Template extraction and size
- Measuring performance
- Vulnerabilities
- Data Sets

3 Algorithms
- Preprocessing
- Gabor Filters
- Feature extraction
- Matching

4 Homework

Hand Geometry

History

- Egypt
- Asian
- Second most widely used biometric

Technology

Measure:

- Length
- Width
- Thickness
- Surface area of hand
- Four fingers

Acquire Biometric

In order to acquire the biometric you require:

- A light source
- Camera (can be CCD)
- Single mirror (for side profile)
- Flat surface with with pegs
- 90 Measurements

Represent a 9 byte template
A 3d shape of a hand requires a 32 000 pixel CCD.

Uses

It can be used in the following applications

- Access control (especially in nuclear plants)
- Time and Attendance (to avoid buddy punching)
- Metering resource use (such as printing, cafeterias and tour groups)
- Border control

Robustness and Accuracy

Only 2 vendors (including Disney) have run tests and as a result there is a limited amount of information that can be used to compare against other biometric attributes.

Vulnerabilities

The limitations and vulnerabilities include:

- It is expensive
- Requires adequate lighting
- Alignment issues
- etc.

Fingerprint Recognition

History

- Artwork
- Healing
- Law enforcement
- Alignment issues
- Drug abuse

What is a fingerprint?

An impression left by friction ridges of a human finger that can be made up of:

- Perspiration
- Organic solids (amino acids)
- Inorganic solids (salts, etc.)

Matching:

- Henry system (Arch, loop and tented arch)
- Minutia

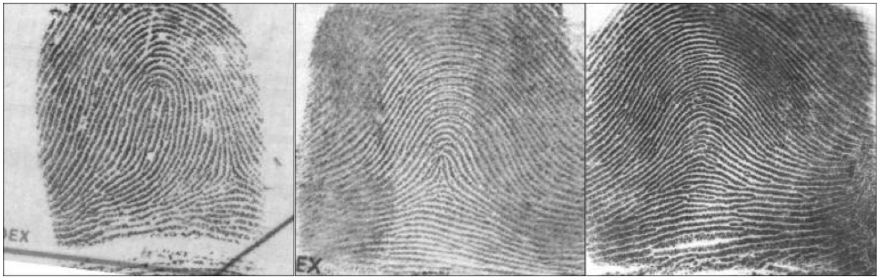

Figure: Examples of fingerprints

Fingerprint points of interest

- **Loop**: The loop is the most common type of fingerprint pattern and accounts for about 65% of all prints.
- **Arch**: The Arch pattern is a more open curve than the Loop. There are two types of arch patterns the Plain Arch and the Tented Arch.
- **Whorl**: Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

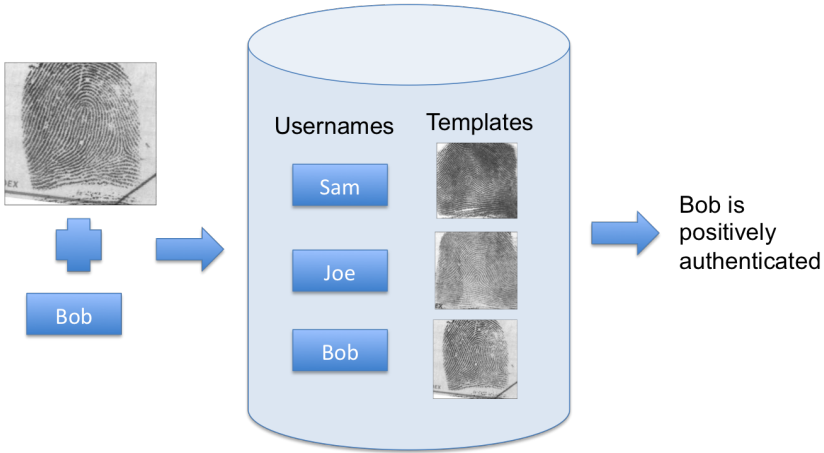

Figure: 1-to-1 Authentication System

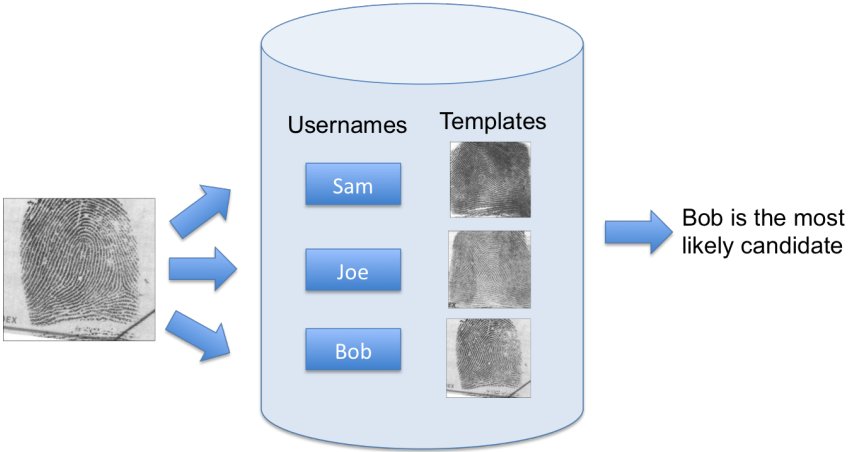

Figure: 1-to-many Identification System

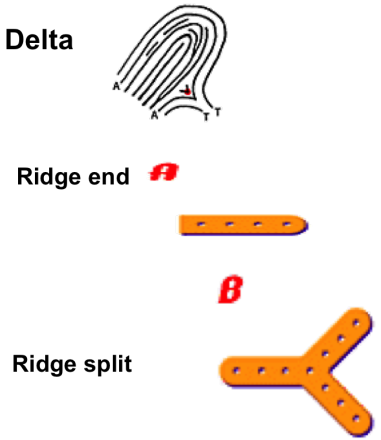

Figure: Examples of Minutia 1

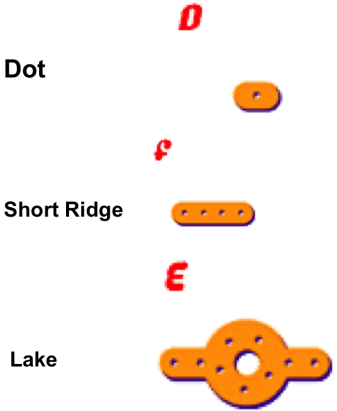

Figure: Examples of Minutia 2

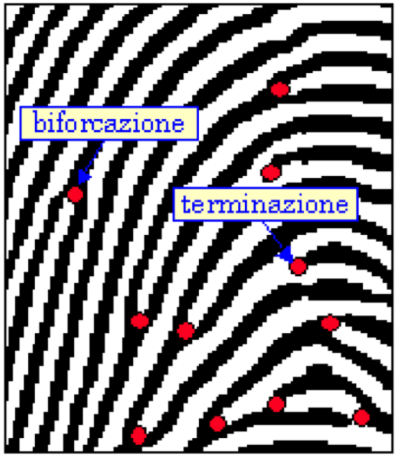

Figure: Bifurcations

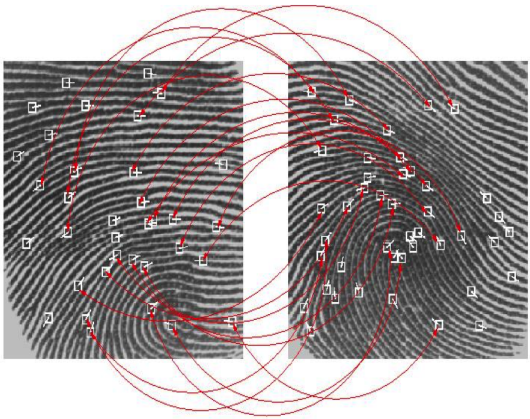

Figure: Minutia matching

Levels of Minutia

- Level 1: Holistic view, ridge count and orientation
- Level 2: According to minutia and on the Cartesian axis
- Level 3: Ridge edge shape and pores
- *Level 4: fingerprint molecular identification (FMID)*

Sources of difference

- Position on scanner
- Orientation
- Pressure
- Missing minutiae
- Humdity
- Dirt
- Damaged finger

Fingerprints have been through:

- The first age of automation (clear with FBI standards with size, type of ink, text fields and 14 spaces)
- and the second age of automation (fingerprint scanners)

- Palm print to identify anybody on latent impressions left by any part
- Uses live scan technology with inkless collection to reduce time, clean up and add consistency.

There are two types of models:

- Single row scanners
- Two dimensional array

The types of single finger flat scanners include:

- Optical (CCD and LED)
- Thermal (solid state device)
- Capacitive (solid state)
- Ultrasonic (transducer type)

1. Acquire image
2. Process image to thin images
3. Find minutiae
4. Derive template (1000 byte)
5. Calculate match score
6. Apply threshold

Measuring performance

In the past performance was measured according to accuracy, reliability and selectivity. Now replaced with FTER, FAR, FRR, FTAR and FMR

Vulnerabilities

Fingerprint recognition vulnerabilities include:

- Masking the finger (to avoid a match)
- Spoofing the device
- Micro occlusions
- etc.

Data Sets

Examples of Data Sets that contain fingerprints include:

- NIST sets
- CASIA
- MCYT
- LivDet (for liveness)
- ATVS (for fake fingerprints)

Algorithms

Preprocessing

Separate false ridges, join broken ridges and maintaining ridges.
The algorithms you can use are:

- Fingerprint image enhancement (contextual, low or band pass, Gabor filters and Fourier transform analysis).
- Ridge orientation estimation (piece-wise or continuous approach)
- Ridge orientation modelling (zero-pole model)
- Singular point detection (pattern, partition and project based)

Preprocessing II

Preprocessing III

(a) (b) (c) (d)

Gabor Filters

A linear filter used for edge detection using a Gaussian kernel function modulated by a sinusoidal plane wave for a respective frequency and orientation. In the discrete domain these are defined as:

$$G_c[i,j] = Be - \frac{(i^2+j^2)}{2\sigma^2} cos(2\pi f(i\ cos\theta + j\ sin\theta) \quad (1)$$

$$G_c[i,j] = Ce - \frac{(i^2+j^2)}{2\sigma^2} cos(2\pi f(i\ cos\theta + j\ sin\theta) \quad (2)$$

Where B and C are normalizing factors, f frequency being looked for in the texture and θ the orientation.

Gabor Filters II

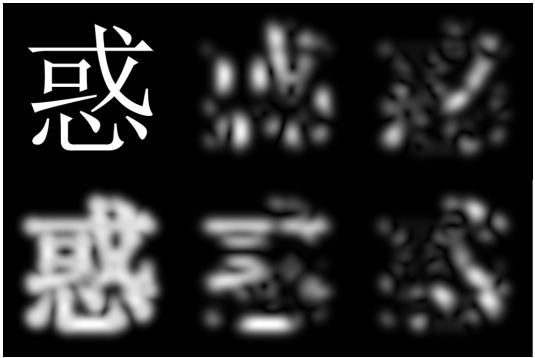

Figure: Gabor filter applied to Chinese character with four orientations to the right and the original and superposition on the left

Feature extraction

Where various features are found that are a succinct representation of the high dimensional space
The features you can use are:

- Ridges, valleys (tessellation pattern)
- Minutia (coordinates, angle and type)
- Pores, crease and ridge fragments

Matching

Where the features are matched against each other.
The matching approaches you can use include:

- Distance measure
- Hough transform
- RANSAC
- Support Vector Machine (SVM)

Homework

Reading for next week

1. Viola, Paul, and Michael J. Jones. "Robust real-time face detection." International journal of computer vision 57, no. 2 (2004): 137-154.
2. Turk, Matthew A., and Alex P. Pentland. "Face recognition using eigenfaces." In Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on, pp. 586-591. IEEE, 1991.