Biometrics & Privacy

Stefan Katzenbeisser
Security Engineering Group
Technische Universität Darmstadt

skatzenbeisser@acm.org
http://www.seceng.informatik.tu-darmstadt.de

Biometrics

Goal: Identification of people through “intrinsic” features of a person

Advantages:

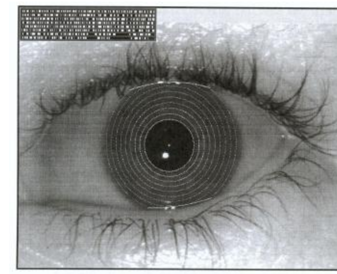
- Feature cannot be lost or stolen
- Easy to use, no password necessary
- Uniqueness
- Forgery resistance (?)

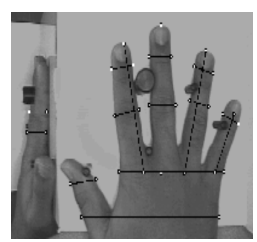
Disadvantages:

- Privacy problems
- Low level of acceptance
- May be measured without consent of user
- No revocation mechanism

Requirements

- **Universality**: Every person has the feature
- **Uniqueness**: Feature is unique for a person
- **Permanence**: Feature does not change over time
- Feature can be **measured** with sensors
- **Performance**: Fast and accurate measurements
- **Acceptance** of user
- **Security** against forgeries





Enrollment

- Registering a user is called **enrollment**

- During the process, the biometrics are measured and ...
- ... a „template“ is stored

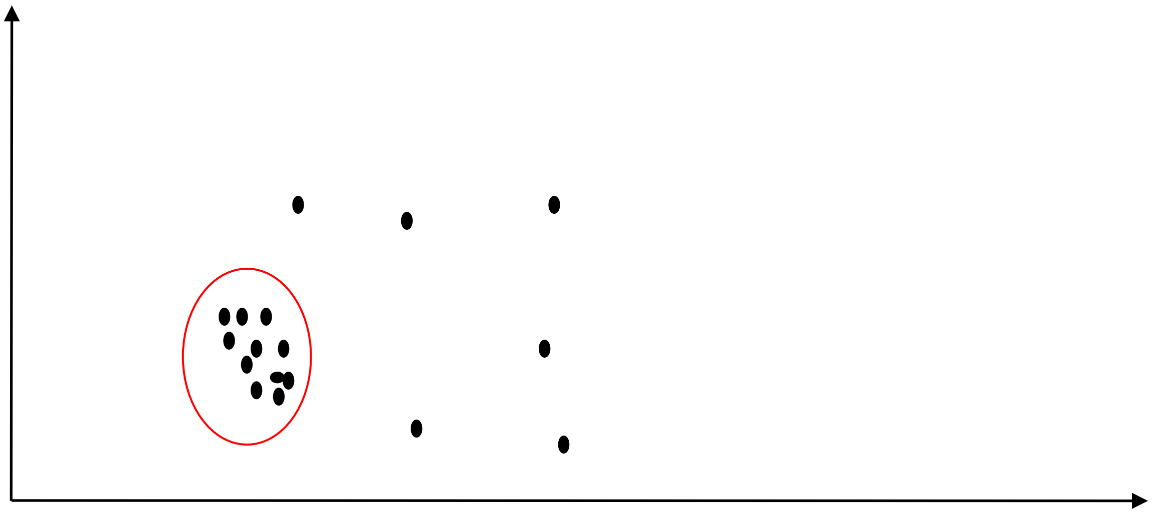
- Subsequent measurements are matched against templates only

- Can be combined with preprocessing to identify “robust” features

- Examples:
  - Fingerprints: minutiae extraction
  - Face recognition: computation of eigenfaces
  - DNA: extraction of Short Tandem Repeats

Verification

- Matching a „template“ against a new measurement
- Must be robust against noise in measurements
- Essentially a classification problem
  ➔ well-studied in statistics
- Classification will **never** be perfect due to inherent statistical variation



Parameters of a Biometric System (1)

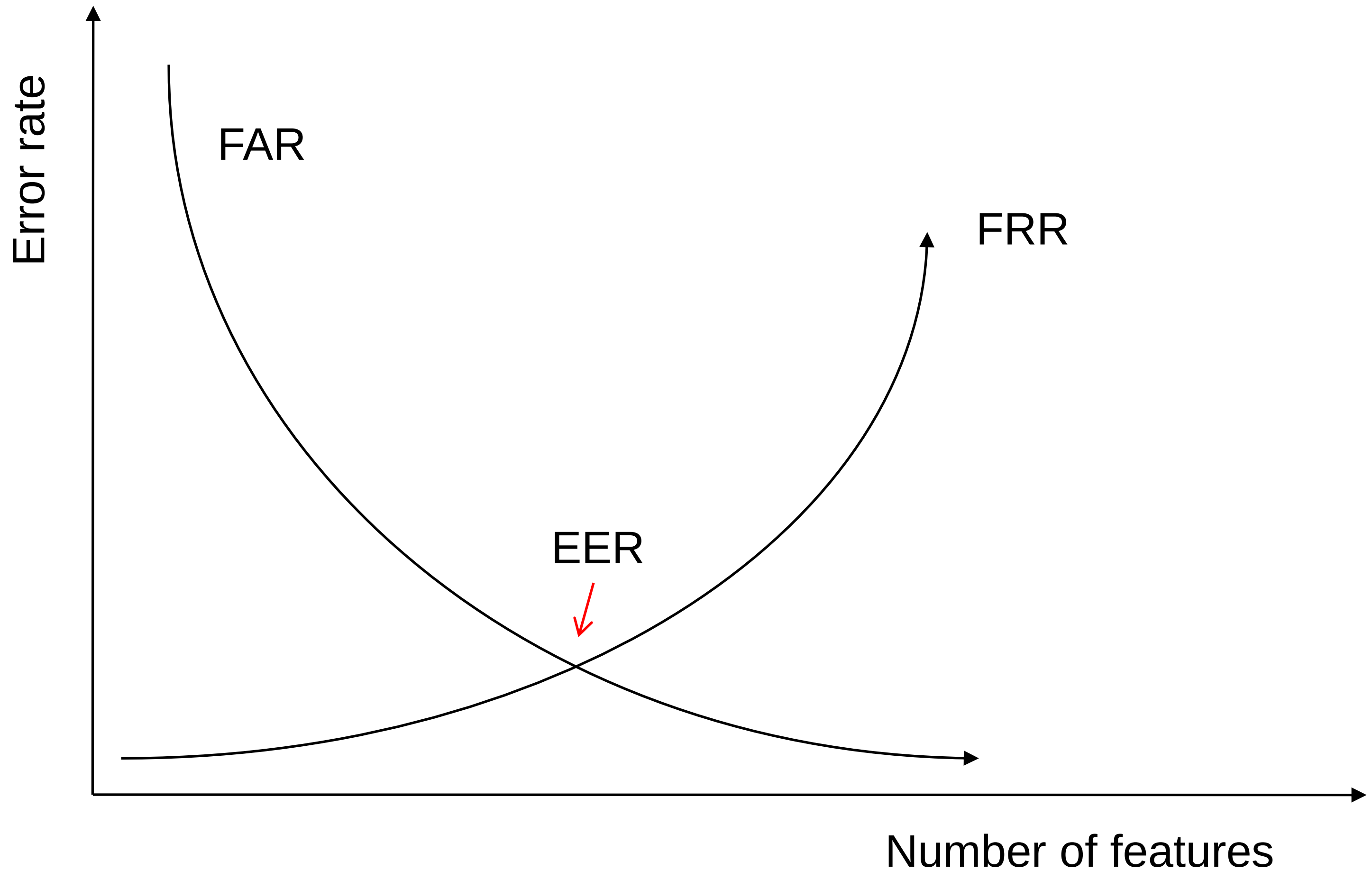
- **False positives:** Unauthorized person will wrongly be identified
  ➔ May yield a security problem
  False Acceptance Rate (FAR)

- **False negatives:** Authorized person will not be identified
  ➔ May yield problems regarding acceptance & usability
  False Rejection Rate (FRR)

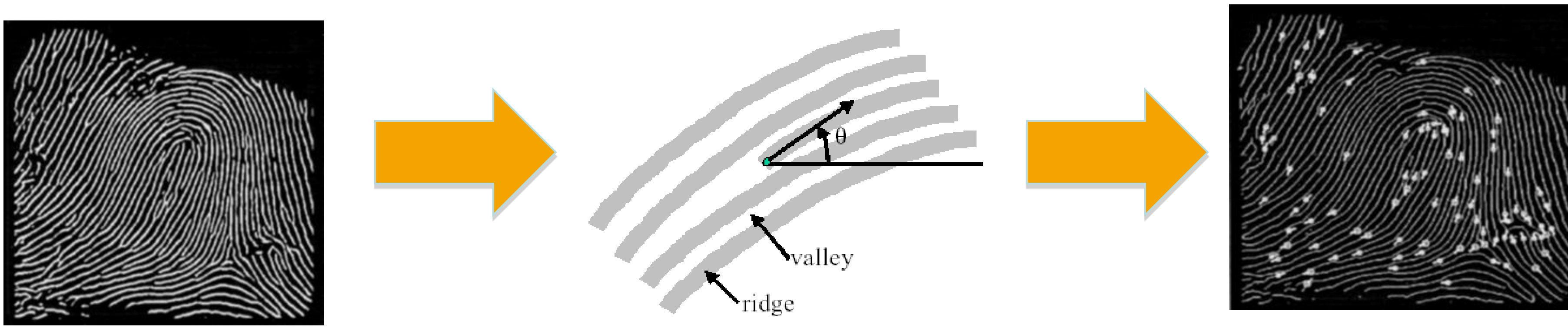
- Biometrics is based on statistical tests; FAR and FRR cannot simultaneously be made zero!
- FAR and FRR can be influenced by adding features
- Equal Error Rate (EER)

- Mostly „dubious“ numbers based on vendor data

Parameters of a Biometric System (2)

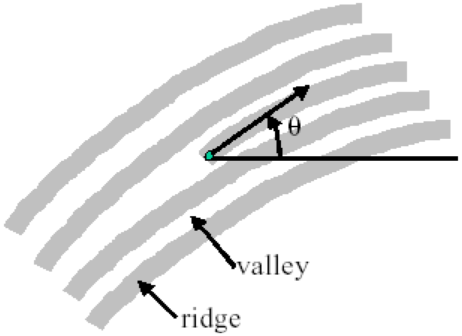


Fingerprints (1)



- Most algorithms based on **minutiae**: special points of the fingerprint
- Pattern of minutiae seems to be unique for each person
- Minutiae represented by position and angle
- Comparison of minutiae only
- Problems: Spatial synchronization, missing minutiae due to noise, ...

Fingerprints (2)

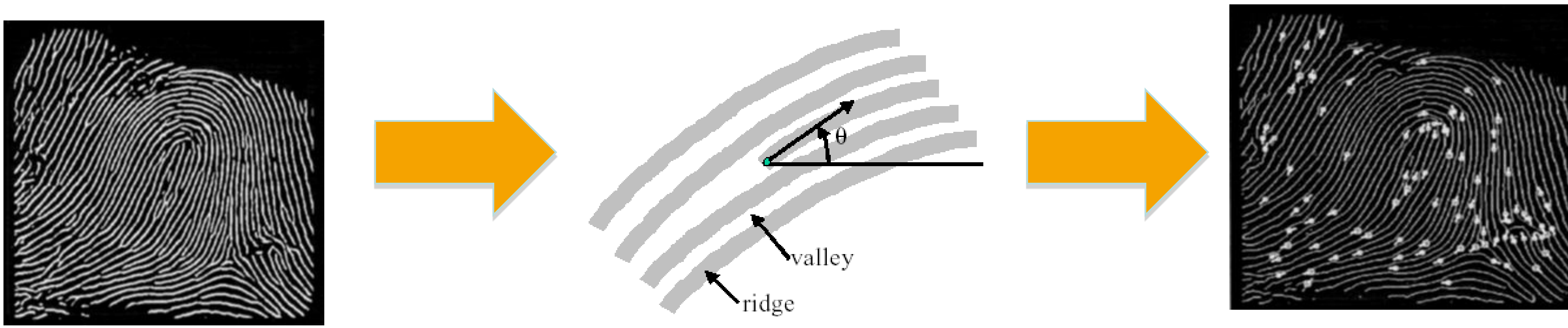


- Represent a fingerprint as a sequence of minutiae $((x_1, y_1, \theta_1), (x_2, y_2, \theta_2) ..... , (x_n, y_n, \theta_n))$
- Measure distance between minutiae

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

$$\Delta\theta = \begin{cases} |\theta_i - \theta_j|, & \text{if } |\theta_i - \theta_j| \leq 180° \\ 360° - |\theta_i - \theta_j|, & \text{if } |\theta_i - \theta_j| > 180° \end{cases}$$

Fingerprints (3)



- Select tolerance levels **dTol** and **θTol**
- Two minutiae match if **d ≤ dTol** and **Δθ ≤ θTol**
- Two fingerprints match, if at least k minutiae match
- Number k determins accuracy of test

Face Recognition (1)

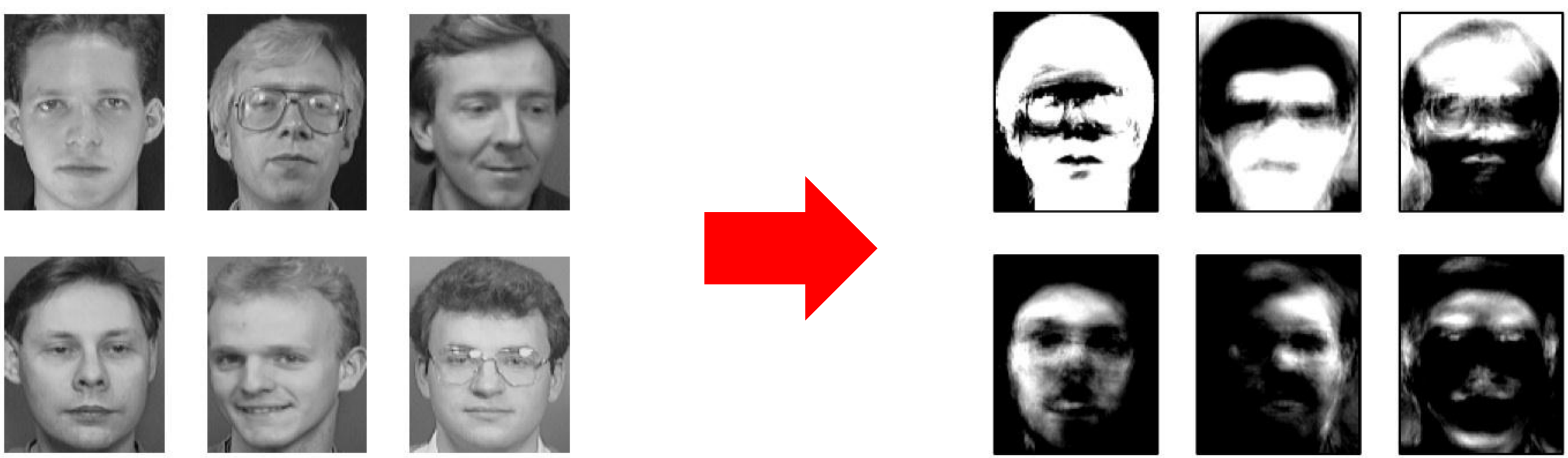
- Several algorithms known to recognize faces on images
- One of the most known algorithms relies on “eigenfaces”

- Face image is represented as vector in high-dimensional space (coordinates of vector correspond to gray-scale values of pixels)

- Use of Principal Component Analysis (PCA)
  - to determine low-dimensional subspace
  - vector of high-dimensional space should be represented as linear combination of low-dimensional vectors with “small information loss”
  - transforms a large number of correlated values into a smaller number of uncorrelated variables (principal components)

Face Recognition (2)
Enrollment

- Given some training images (e.g. images of the enrollment phase),
- PCA is used to determine principal components (eigenfaces), forming the „face space“
- All enrolled images are projected into the face space to obtain a biometric template
- Face space representation represents „approximation“ of faces



Face Recognition (3)
Recognition

TECHNISCHE UNIVERSITÄT DARMSTADT

- Every face image is thus represented as a small vector in face space
- Upon recognition, the new face image is projected into the face space to obtain the facial template
- The facial template is compared to templates stored in the database
- The face template from the database with minimal Euclidean distance is chosen, or a mismatch is reported if this distance is larger than a threshold
- Problems to be solved: light conditions, registration of images, quality of photos, ...

Privacy?

- Use of biometrics raises privacy problems!
- This is particularly true for „intrusive“ biometrics:
  - Patters of veins (medical data!)
  - DNA (may code health-relevant data)
- Is biometric data a secret?
- Attacks:
  - Fabricate artificial fingerprint to deceive sensor (liveness test required!)
  - Attacks against person (cut off finger?)
- Privacy-Enhancing Technologies for biometric data