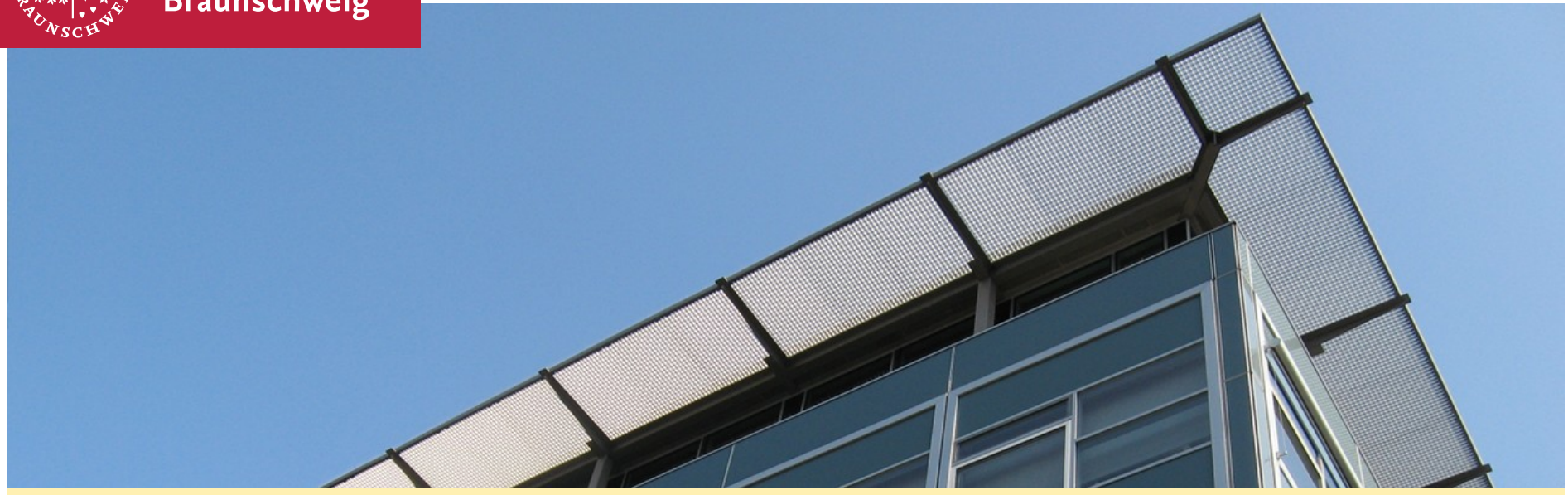
Technische Universität Braunschweig

Institute of Operating Systems and Computer Networks



Secure communication based on noisy input data

Introduction

Stephan Sigg

April 19, 2011

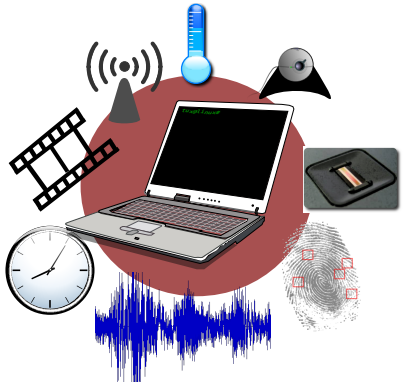
Overview and Structure

- Classification methods
- Feature extraction
  - Features from audio
  - Features from RF
- Fuzzy Commitment
- Fuzzy Extractors
- Authentication with noisy data
- Error correcting codes
- Entropy
- Physically unclonable functions

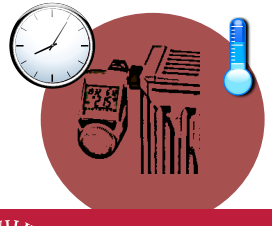
Outline

Sensors and sensor classes

- We are surrounded by a multitude of sensors
  - Sensor readings utilised for
    - Information provisioning
    - Situation classification
    - Authentication
    - Cryptography



Time
RF
Temperature
Light
Audio
Video
Smoke
Fingerprint
...



Sensors and sensor classes



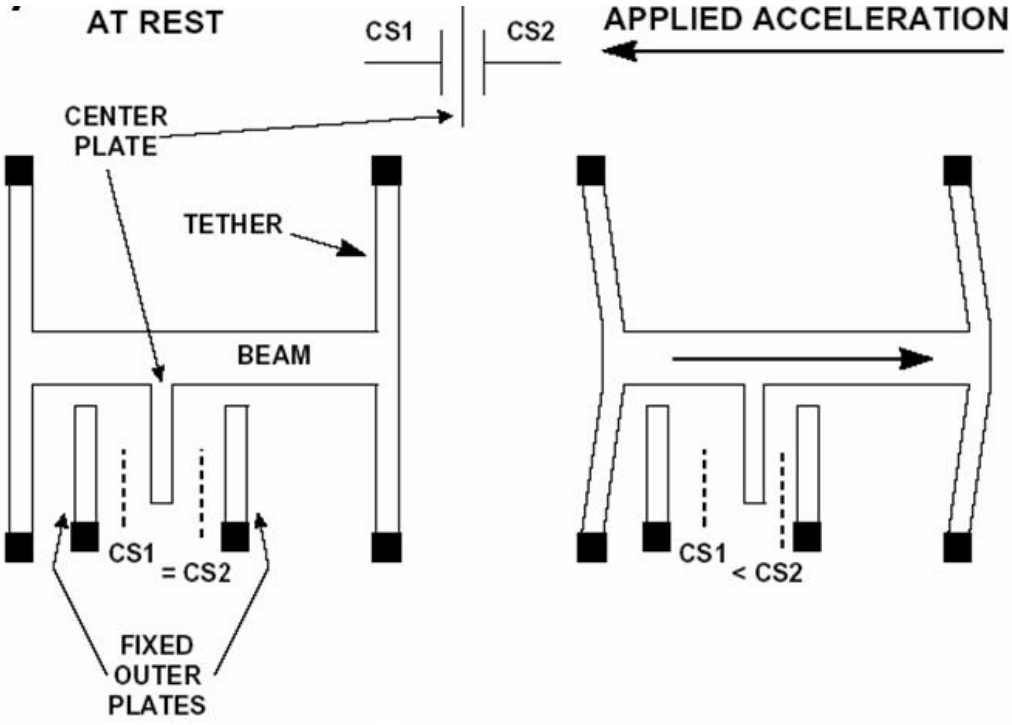






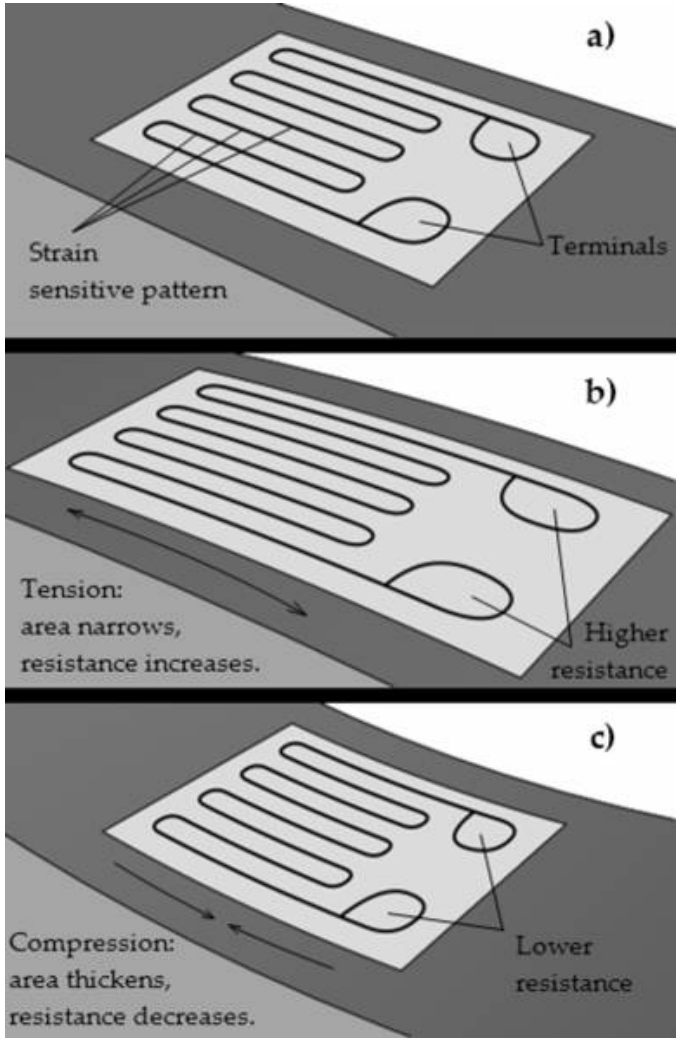

Sensors and sensor classes

- MEMS acceleration sensors
  - E.g. Analogue Devices ADXL
  - Low energy consumption, small, cheap, medium precision
  - MEMS = Micro-mechanical System: Mechanic in Silicon (Silizium)
  - Here: Comparison of capacity CS1 and CS2 leads to acceleration



Sensors and sensor classes

- Pressure sensors
  - Z.B. IEE about 3-10 Euro
  - Very imprecise

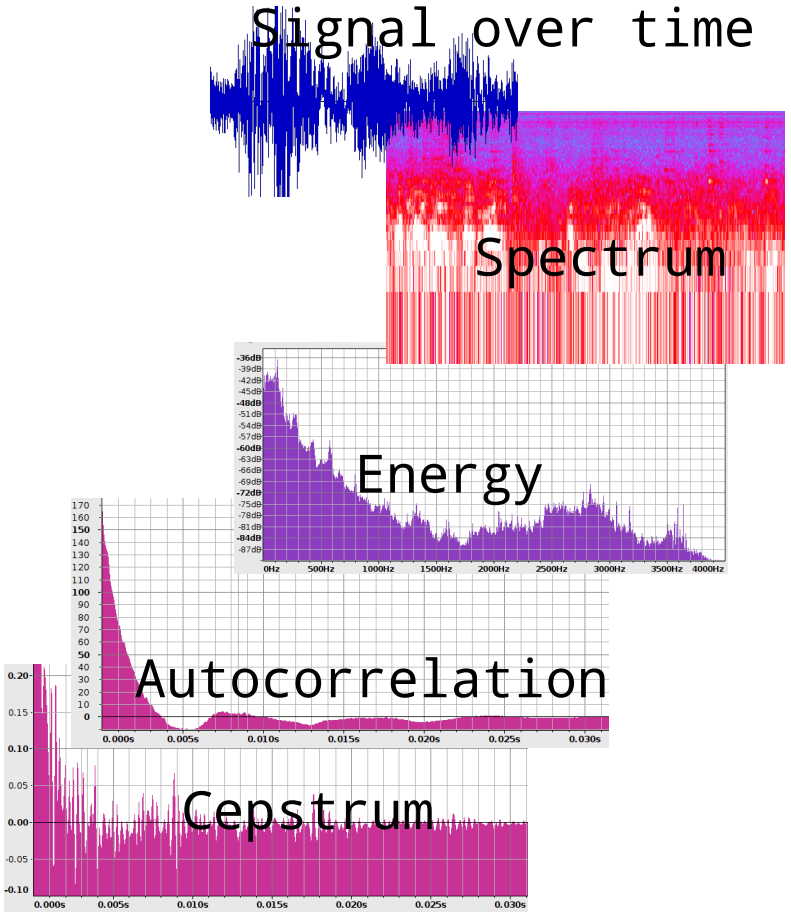


Sensors and sensor classes

- Output of sensors has to be interpreted typically
  - Raw electrical signals
  - Interpretation of signals as electric values
  - Binary or Real valued representation
  - Further identification of features
  - Feature extraction
  - Interpretation of features and classification

Features and feature extraction

- What is a feature and why do we need it?
  - Captured data might be hard to interpret
  - Many aspects can be contained in a single data stream
  - Example: Audio
    - Loudness
    - Energy on frequency bands
    - Zero crossings
    - Direction changes

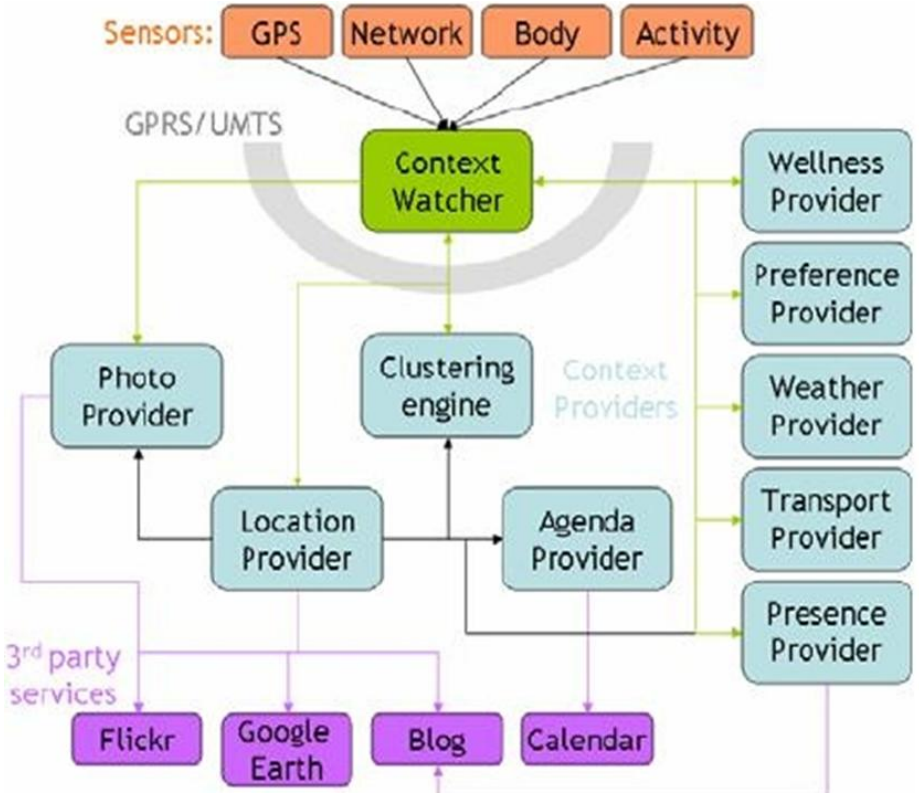


Examples and case studies: Media Cup

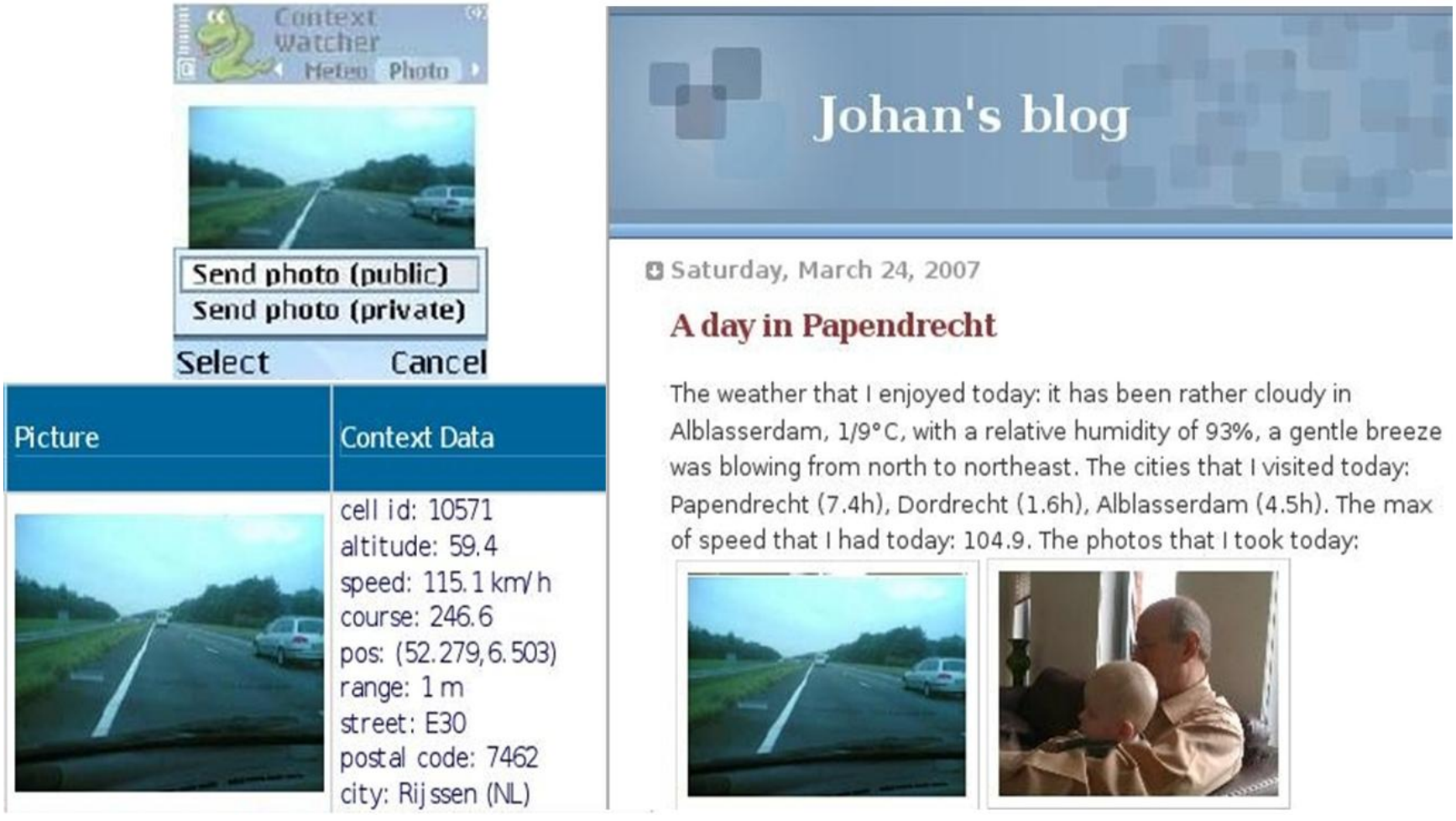
- Media Cup: Context recognition
  - Activity: Trigger sleep mode (save energy)
  - Level of activity
  - Own context: Object movement, person is nervous, specific handling of objects
  - Environmental context: Vibration, earthquake
- Sensor: Ballswitch
  - (nearly) no quiescent current
  - Various types, filled with gas/liquid
  - e.g. Acceleration with fixed value (liquid)
  - Vibration (filled with gas)

Examples and case studies: Context Watcher

- Context Watcher
  - Location
    - GSM cell-ID; GPS
  - Mood
    - user input
  - Activity
    - calender based
  - Bio-data
    - heart and foot sensors
  - Weather
    - location based over internet
  - Photo/picture
    - camera



Examples and case studies: Context Watcher



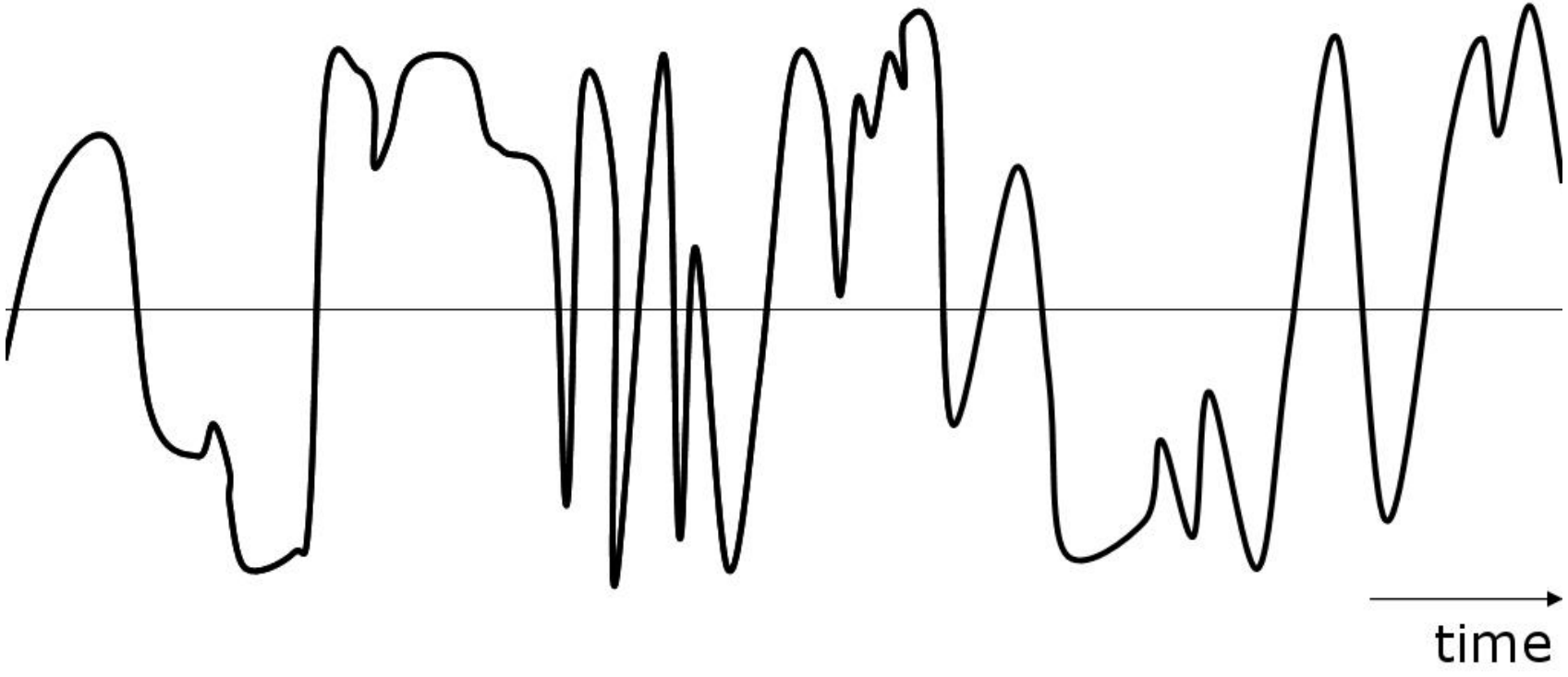
Examples and case studies: TEA

TEA-Audio

- Requirements
  - Restricted memory space
  - Computing power restricted
- Benefit
  - Many sensors $\rightarrow$ Many features
- Example approach
  - Utilise time domain (no transformation)
  - Utilise statistic measures
  - Feature extraction based on small amount of data

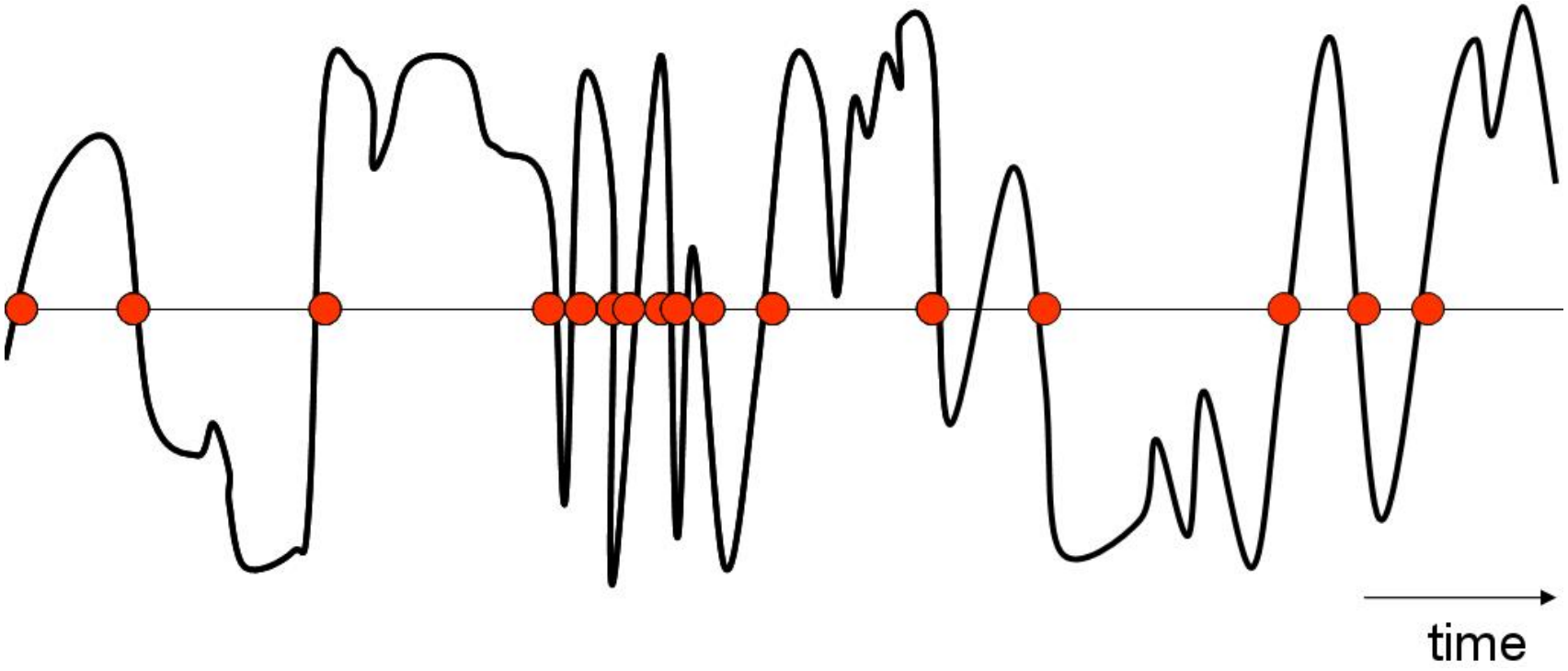
Examples and case studies: TEA

- Audio data in time domain



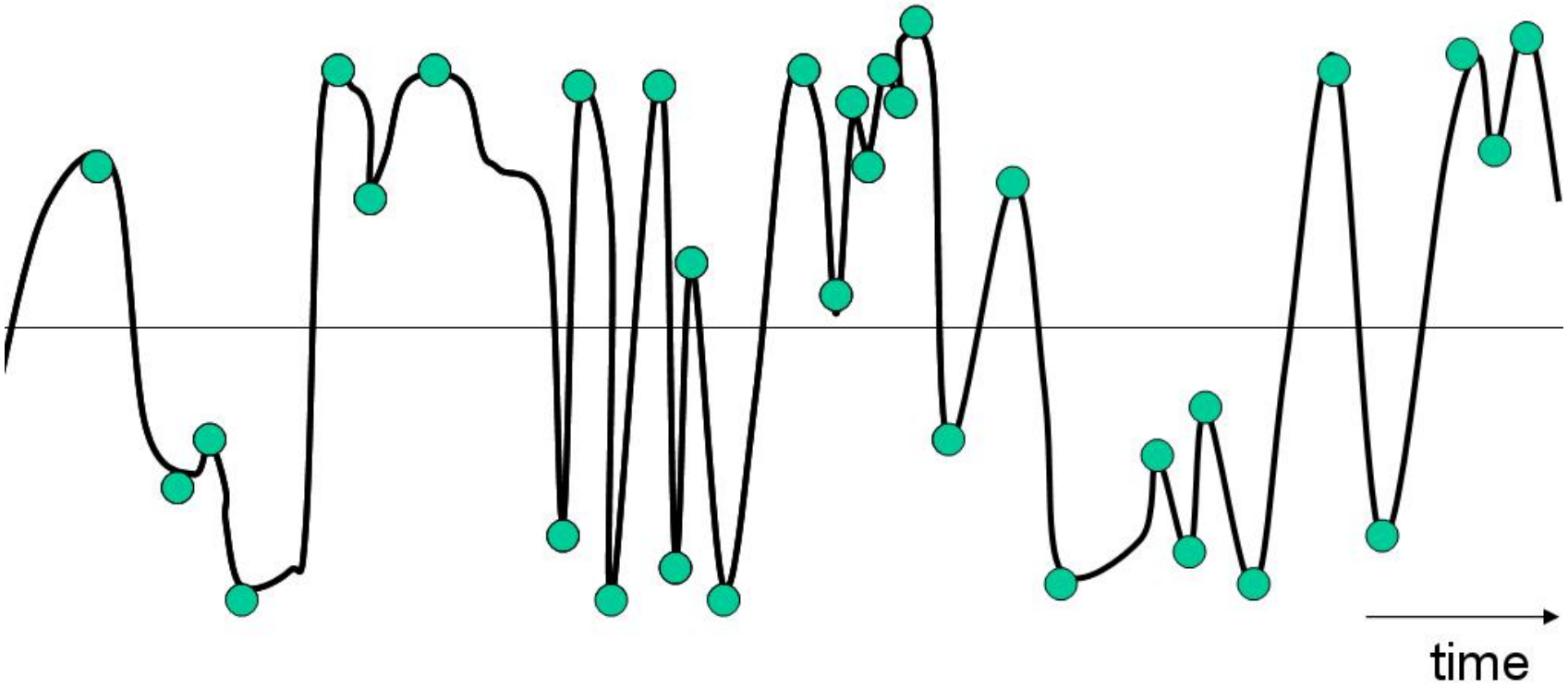
Examples and case studies: TEA

- Count zero crossings
- Distance between zero crossings



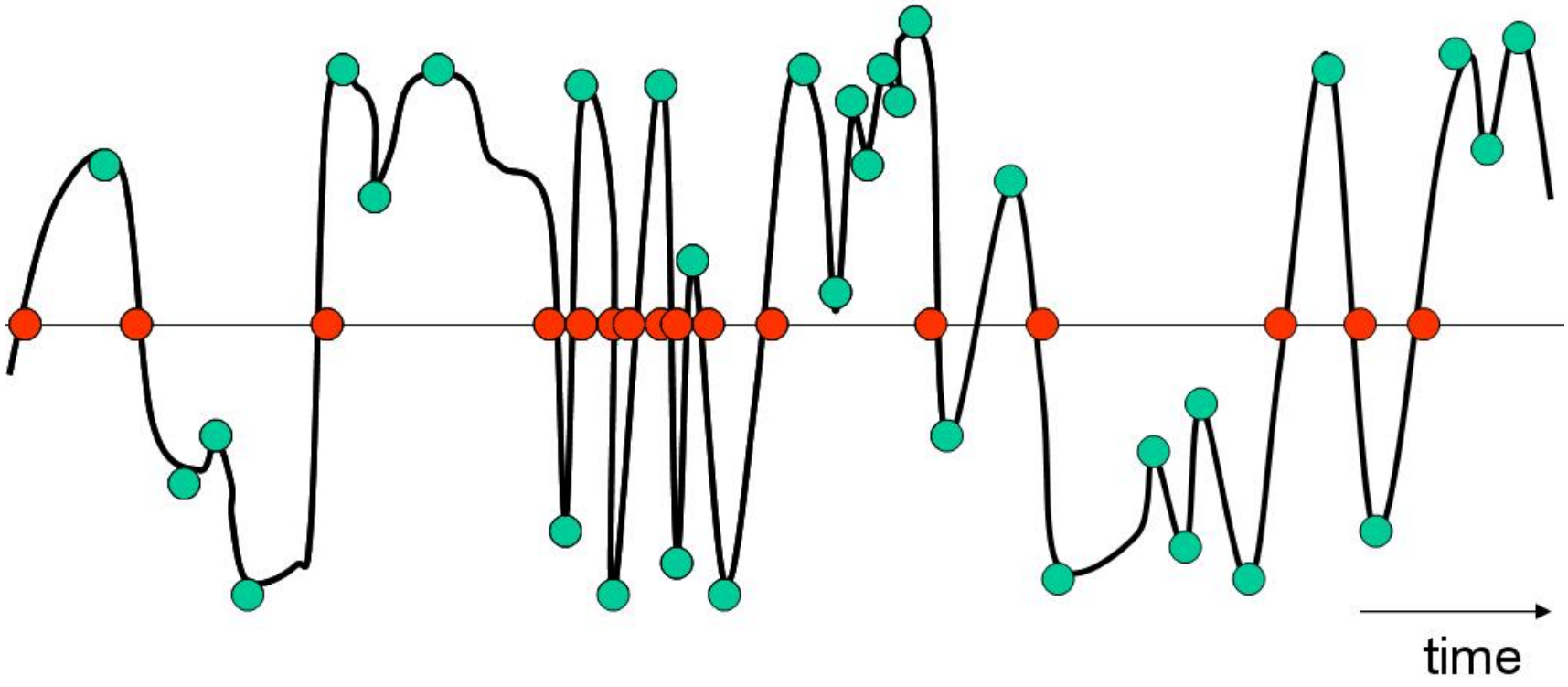
Examples and case studies: TEA

- Count of direction changes



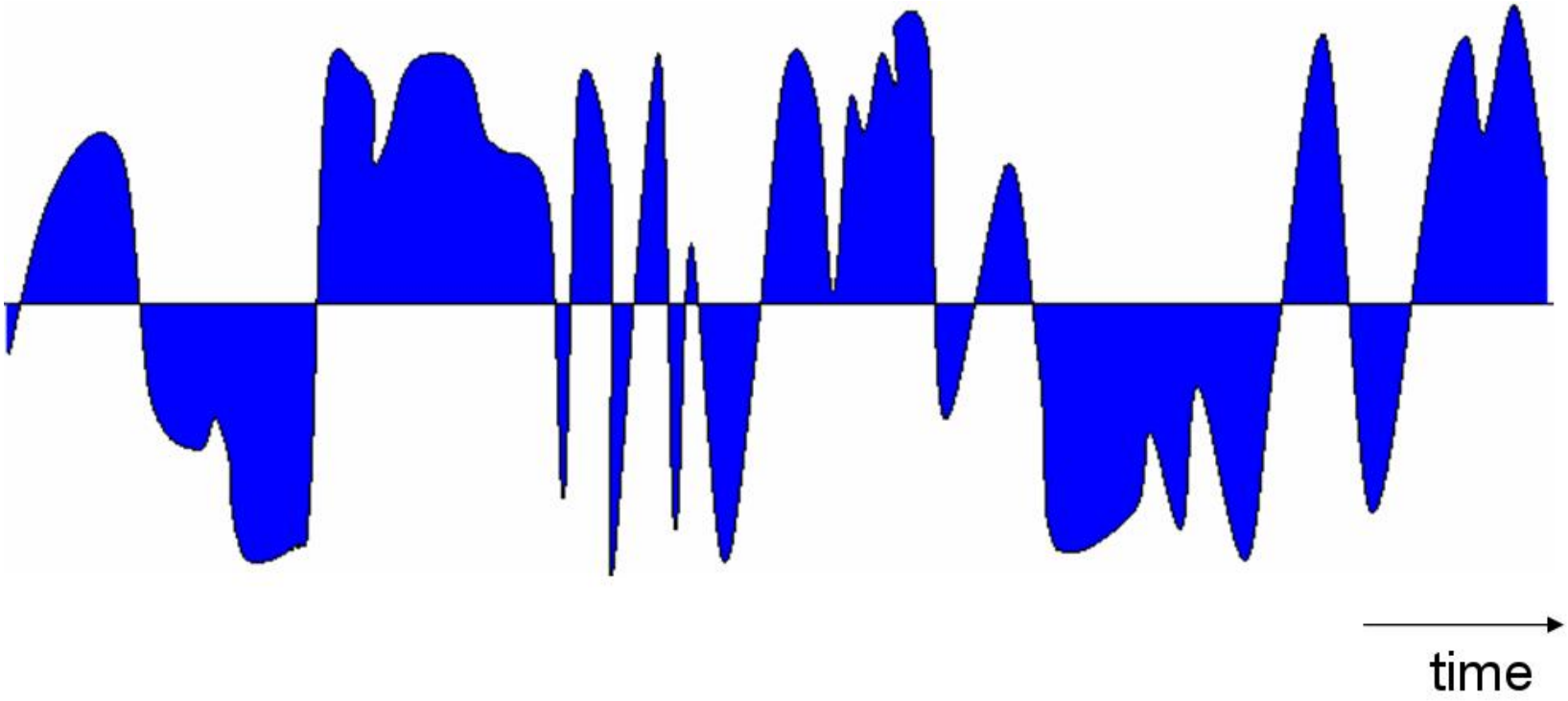
Examples and case studies: TEA

- ratio: $\frac{\text{direction changes}}{\text{zero crossings}}$



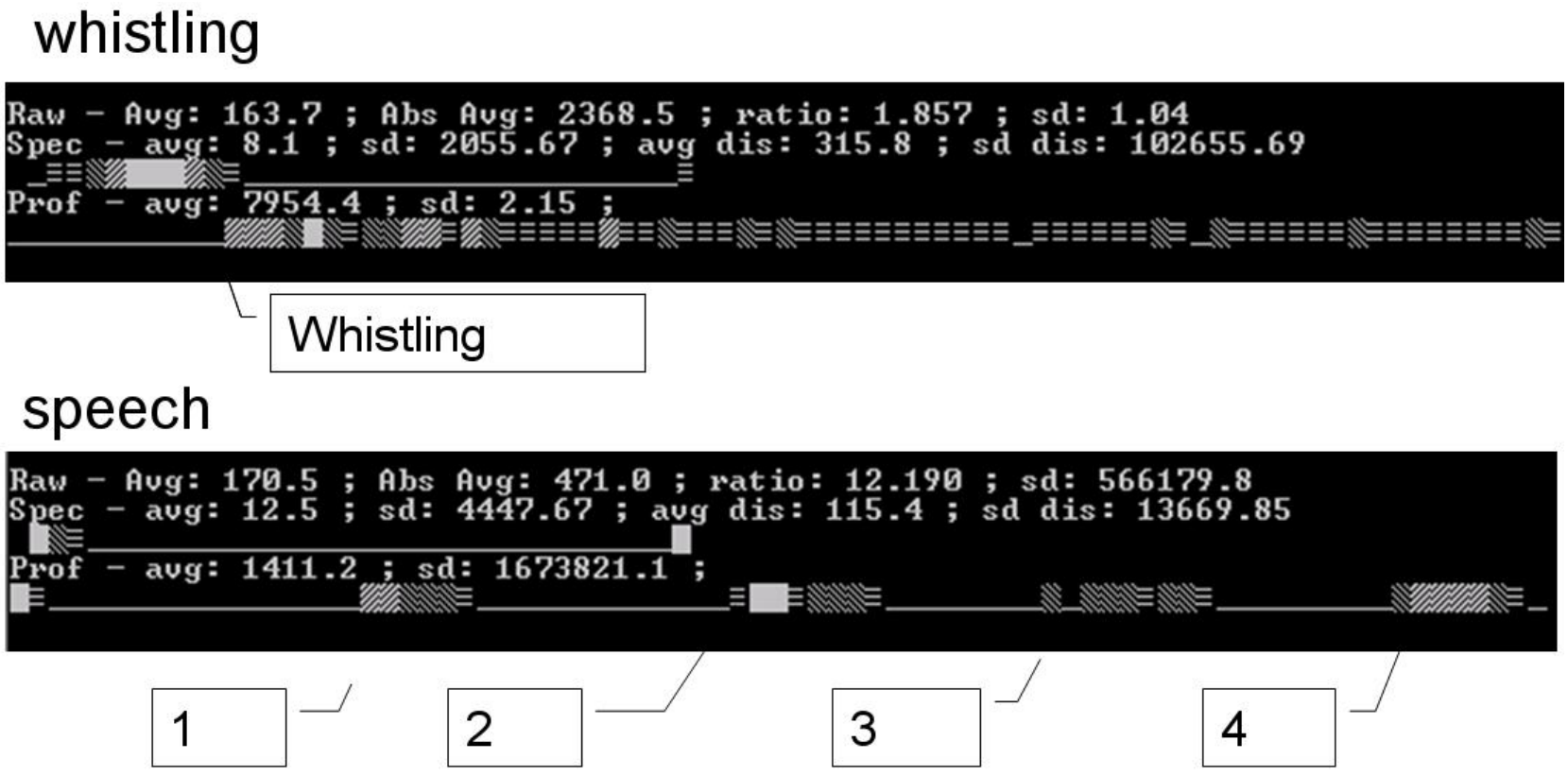
Examples and case studies: TEA

- Integral



Examples and case studies: TEA

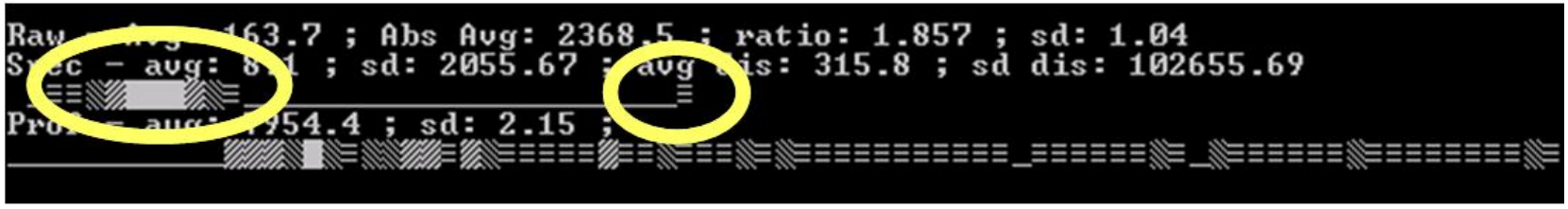
- Several chunks for speech



Examples and case studies: TEA

- Distance between zero crossings: distinct behaviour of oscillation at start and end

whistling

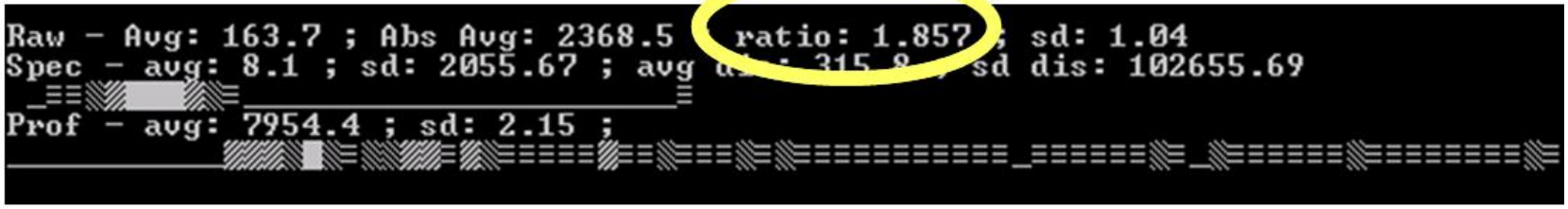


speech

Examples and case studies: TEA

- Distinct ratio: $\frac{\text{zero crossings}}{\text{direction changes}}$

whistling



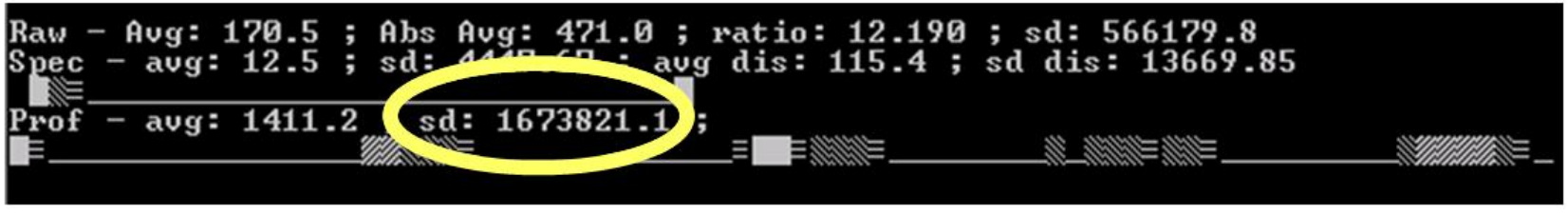
speech

Examples and case studies: TEA

- Significant change in standard deviation of chunks

whistling

speech



Outline

Questions?

Stephan Sigg
sigg@ibr.cs.tu-bs.de

Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- P. Tulys, B. Skoric, T. Kevenaar: Security with Noisy Data – On private biometrics, secure key storage and anti-counterfeiting, Springer, 2007.
- R.O. Duda, P.E. Hart, D.G. Stork: Pattern Classification, Wiley, 2001.