Identification Systems
Lecture 1

Piotr Syga

2021-03-02

Course Outline

Main goal: Learning and confirming one's identity

Selected topics:

- ePassports
- 'tokens' and constrained devices
- biometrics (speaker recognition, fingerprints, signatures, palmprints, face geometry, . . .)
- possibly deepfakes – recognition, using it in verification

Course Goal

- learning details on existing standards in identity confirmation
- introduction to biometric identification – modes, collecting data, enrollment, inaccuracies, data processing, threats
- learning how to construct identification protocols,
- protecting against privacy threats, spoofing and presentation attacks, privacy-by-design

Literature

- Bolle, R.M. et al.: Guide to Biometrics. Springer
- Jain, A.K., Ross, A.A., Nandakumar, K.: Introduction to Biometrics. Springer
- ICAO: Machine Readable Travel Documents
- Finkenzeller, K.: RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication
- Su, J. et al: A Partitioning Approach to RFID Identification
- Bender J., Fischlin, M., Kügler, D.: Security Analysisof the PACE Key-Agreement Protocol
- Szeliski, R.: Computer Vision: Algorithms and Applications, 2nd ed.
- Smith, S.W.: The Scientist and Engineer's Guide to Digital Signal Processing. California Technical Publishing, San Diego, CA, USA
- Gonzalez, R.C., Woods, R.E.: Digital Image Processing. Pearson
- selected papers on biometeric identification

Grading

Group tasks

Report

Presentation

Each part is graded, the final mark is a weighted sum of the parts $M = 0.5G + 0.35R + 0.15P$. Each student in a group receives an individual grade, such that their average does not exceed group's M.

Grading

Group tasks 3–5 members, designing, implementation and verification of a selected identification or authorization scheme (details during exercises)

Report

Presentation

Grading

Group tasks

Report

A document containing the crucial information about the design, its purpose, main goals, advantages and limitations. The description should include, among others, the process of data collection, the enrollment, data processing and protection, identification/authorization, and the evaluation of the method.

Presentation

Grading

Group tasks

Report

Presentation

Short (time constrained) presentation of the project during the last lecture, including the main goals and successes of the project, the main obstacles to overcome. The presentation should include 'live' demonstration of new user registration and identification/authorization of a known user. It may include the identification process of a user nor registered in the database or the antispoofing methods

Basic means of identity confirmation

- what we know
- what we have
- what we are

Problems with accuracy, reproducibility, non-copyability, protection of the mean, measurement.

Identification vs Authorization

There are two main tasks in identity confirmation:

Identification:

Based on a given mean, we compare the input with whole database and determine the correct (or closest) matches. In terms of close-matches, we need to determine a confidence threshold.

Authorization/Verification:

Based on a given mean, we compare the input with claimed identity of a particular subject. Depending on the mean used, it may require a perfect match or fitting in the confidence interval.

Passports – basic info and standards

- a personal identification method that utilizes multiple means
- Machine Readable Travel Document – allows 'splitting the user database'
- biometric data stored off-card
- ICAO Doc 9303 – Machine Readable Travel Documents



Figure: Polish biometric passport

Motivation for biometry

- Security – adding layer of biometric link protects against spoofing and cloning
- Standarization – a shared, precise norms emerged worldwide (US visa waiver, ICAO, EU) influencing popularity and increasing possibilities
- Interoperatibilty – with standards, the same documents may be used for more than passing borders, allowing international multi-purpose ID
- Control efficiency – automated or fully–automatic border control significantly increases throughput

Biometric Passport worldwide

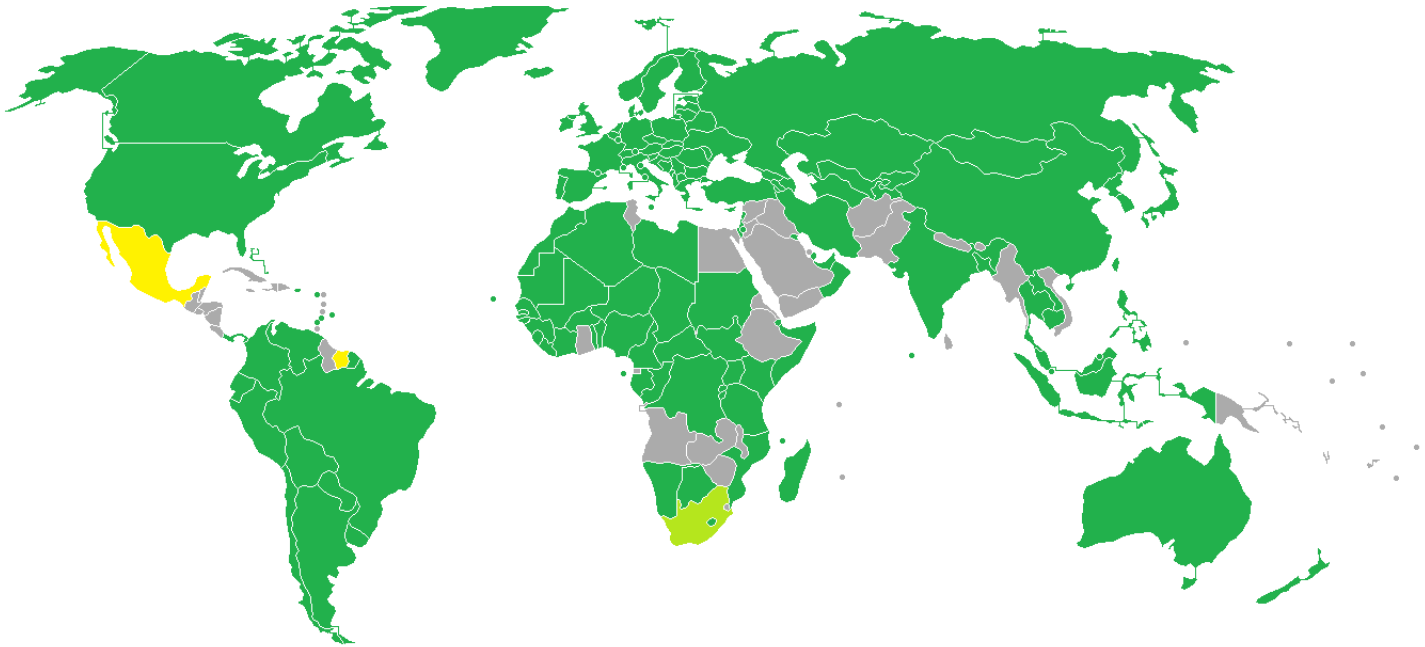


Figure: Biometric passports worldwide in early 2020.

Passport system outline

1. Booklet with the microprocessor
2. Biomteric data (2–4 fingerprints, face geometry) stored electronically
3. MRZ with personal data (with a copy on the chip), machine readable image for face geometry comparison
4. Reader communicating with a chip
5. **Mutual** identification of a chip and the reader
6. Both electronic and visual identification system connected to the control system
7. Spoofing prevention system adjusted to automatic detection
8. Efficient biometric system
9. PKI

Biometric systems

The eBooklet contains biometric samples, so that technical details like used feature weights, storing format etc. may be country dependent. The matching takes place on a unit separate from the database and the booklet.

- Face recognition
  - inprinted image of a frontal face
  - matching color image of a frontal face stored in the chip, compressed using JPEG standard
- Fingerprints
  - only electronic version of the images are stored
  - data containing 2 index fingers (thumbs, middle fingers or ring fingers (in order) are used if failed to aquire)
  - grayscale image with WSQ compression
- Other
  - optional (electronic only modes) may include palmprints and irides grayscale images
  - storing additional data (both additional modes and fingerprints) is discouraged due to privacy issues

European requirements on face images

- Recent photo (the limit varies between 1 and 6 months)
- Uniform, white or gray background
- Frontal shot with natural face expressions and no tilt
- Face should cover 70-85% of the image, matching the standard schema
- Eyes open without flashes or reflections
- Uniform image illumination
- No hair or glasses obscuring the eyes or cheeks
- No head coverage (with exceptions made on medical or religious basis)
- Exact/minimal resolution 600 dpi
- Limited file size (24kB)

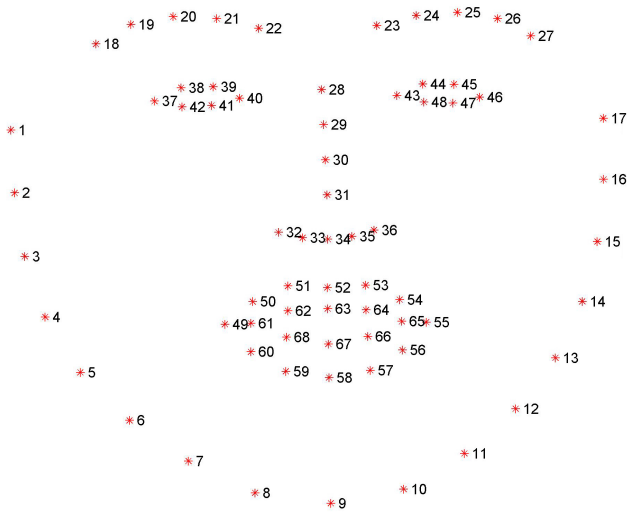
European requirements on face images

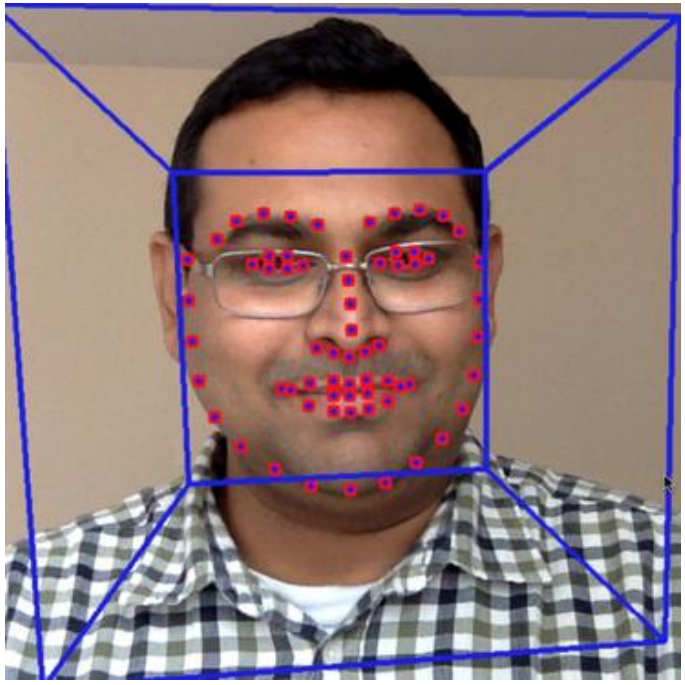


European requirements on face images



European requirements on face images





Booklet structure

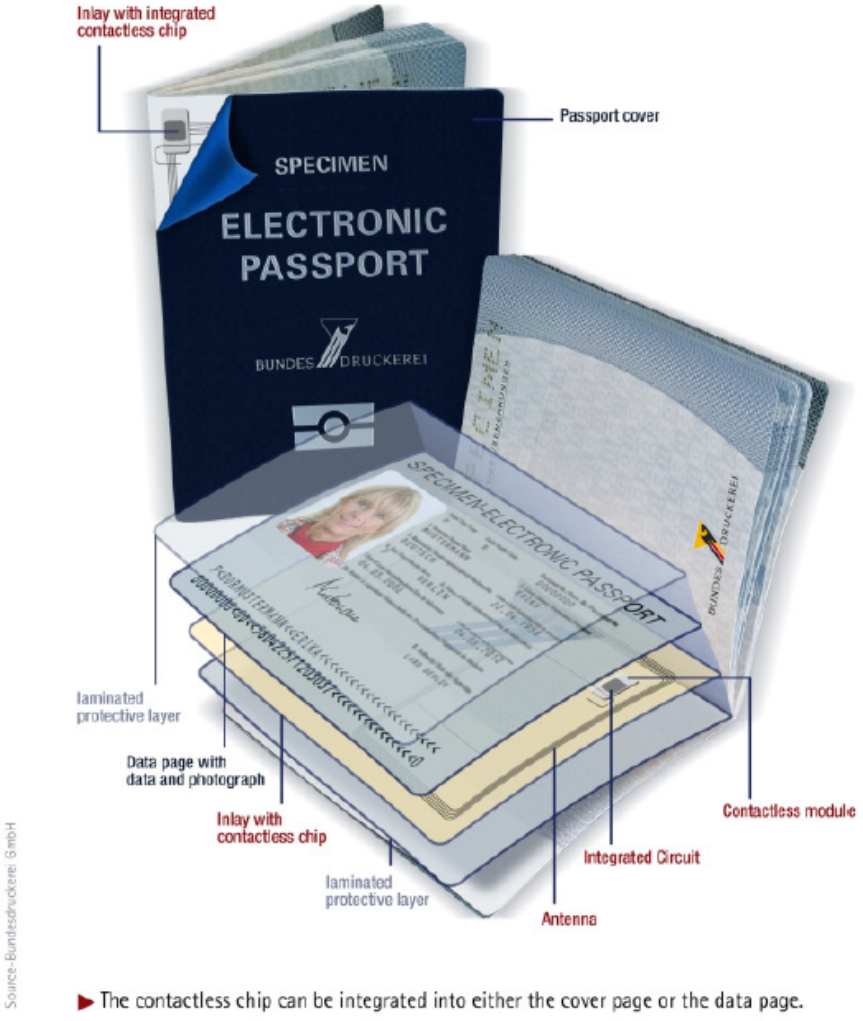


Figure: German passport scheme (Bundesdrukerei)

Booklet structure



Figure: Chip placement (rfidiot.org)

Integrated components

- Contactless Chip compliant with ISO/IEC 14443 powered by EM induction
- Application Protocol Data Units compliant with ISO/IEC 7816-4
- 8 bit microprocessor with EEPROM (min. 32kB) and crypto-co-processor
- card operating system with JavaCard OS frameworks

Structure of the data

- Main unit of division – Data Group
  The standard started with 12 data groups, now contains over 20, with some of them being optional (they may remain empty).
  Examples: DG1 = MRZ, DG2 = photo
- Data Groups are orginezed into Logical Data Structure compliant with ISO/IEC 7816-4
- The hash of the concatenation of all the DG is signed and stored within Document Security Object
- Certificate of the signer for validating the signature is included