Federal Office
for Information Security

Fingerprint Image Quality
NFIQ2.0

Markus Nuppeney
Inspection Infrastructures and Architectures
Federal Office for Information Security (BSI)

Outline

Federal Office for Information Security

- Fingerprint applications and challenges
- Problem statement and requirements
- NFIQ2.0 framework and development
- Identifying candidate features
- NIFQ2.0 Light
- Summary and outlook

Official fingerprint applications

Federal Office for Information Security

- Official documents with fingerprints
  - European ePassports
  - European Residence Permits
  - Identity Cards (partially)
- European Visa Information System (VIS)
  - Tenprints from all Schengen (short-time) Visa applicants
    - Data stored for 5 years
  - Biometric verification at Schengen border checks has started
- Criminal AFIS
- Future programs might also use fingerprints
  - EU Smart Borders Package (Entry-Exit-System, RTP)

Challenges for operators

Federal Office for Information Security

- Technical aspects
  - Heterogenous environments
  - Different hardware and software vendors and versions
  - Interoperability issues
- System design
  - At enrolment stage, typically the biometric verification or identification system vendor is unknown
  - Large scale identification scenarios (AFIS) have high quality requirements
    - 100 million records or more!

Challenges in fingerprint biometrics deployment

Federal Office for Information Security

- Timing considerations
  - Timing constraints are the biggest driver in the design of an enrolment and verification process
  - In many cases, quality correlates directly with time
    - Not only technical, but also organizational (e.g. regarding user guidance)
  - Time is money!
    - Officers are expensive
    - Space is expensive
- Which quality is required by the system?
  - How much time (on average) do I need to reach the desired level?
  - Not: How do I achieve maximal quality?

Standardization - then

Federal Office for Information Security

- Based on ISO/IEC IS 29794-1:2009 "Information technology – Biometrics sample quality Part 1: Framework"
- Definitions
  - quality: "the degree to which a biometric sample fulfils specified requirements for a targeted application"
  - quality score: "a quantitative expression of quality"
  - utility: "the observed performance of a biometric sample or set of samples in one or more biometric systems"
- Quality score from 0 to 100

description		size	valid values	notes
Number of Quality Blocks		1 byte	[0,255]	This field is followed by the number of 5-byte Quality Blocks reflected by its value A value of zero (0) means that no attempt was made to assign a quality score. In this case, no Quality Blocks are present.
Quality Block	Quality Score	1 byte	[0,100] 255	0: lowest 100: highest 255: failed attempt to assign a quality score
	Quality Algorithm Vendor ID	2 bytes	[1,65535]	Quality Algorithm Vendor ID shall be registered with IBIA as a CBEFF biometric organization. Refer to CBEFF vendor ID registry procedures in ISO/IEC 19785-2.
	Quality Algorithm ID	2 bytes	[1,65535]	Quality Algorithm ID may be optionally registered with IBIA as a CBEFF Product Code. Refer to CBEFF product registry

Standardization - now

Federal Office for Information Security

- Based on ISO/IEC 29794-1:201X "Information technology - Biometrics sample quality Part 1: Framework"
- Definitions
  - Same as before, but allows for a vector of quality components
  - **Goal: Actionable quality**
- Each element of quality vector has a score from 0 to 100.

Table 2 – Data fields

		Description	Size	Valid values	Notes
		Number of Quality Blocks (N)	1 byte	0 to 255	This field is followed by the number of 5-byte Quality Blocks reflected by its value.
Quality Block 1	Byte 1	Quality Indicator	1 byte	0 to 100 250 255	0 to 100: the encode value is the overall quality score of the representation. It should express the predicted recognition performance of a representation with higher values indicating better quality. 250 (FA_{Hex}): a vector of quality metrics is encoded in bytes 6-N. 255 (FF_{Hex}), an attempt to calculate a quality score has failed
	Bytes 2-3	Quality Algorithm Vendor ID	2 bytes	1 to 65535	Quality Algorithm Vendor ID shall be registered with IBIA as a CBEFF biometric organization. Refer to CBEFF vendor ID registry procedures in ISO/IEC 19785-2.
	Bytes 4,5	Quality Algorithm ID	2 bytes	1 to 65535	Quality Algorithm ID may be optionally registered with IBIA as a CBEFF Product Code. Refer to CBEFF product registry procedures in ISO/IEC 19785-2.
Bytes 6 – 5 x (Number of quality blocks) exist only if quality indicator (Byte 1) is 250 (FA_{Hex}).					
Quality Blocks 2-N	6	Overall quality score	1 byte	0 to 100	A quality score should express the predicted comparison performance of a representation. A quality score shall be encoded in one byte as an unsigned integer. Allowed values are 0 to 100 with higher values indicating better quality
	7	Number of quality vector elements	1 byte	Defined in each Part of this Standard	If the number of quality vector elements mod 5 is not equal to three then padding bytes should be added such that the length of the block is a multiple of five. This will ensure backward compatibility with the implementations conformant with ISO/IEC 29794-1:2009 and ISO/IEC 19794-x:2011. For example, if the number of quality vector elements is 14, 4 padding bytes shall be added so that the length of the image quality record is 25 = 4(padding) + 14(number of quality vector elements) + 7(as shown in rows 1-7).
	8	Quality metrics			As defined in modality specific parts of this International Standard.

Motivation

Federal Office for Information Security

- There‘s no common understanding of a term like *fingerprint of sufficient quality*
  - Sufficient for which application?
  - Quality requirements differ a lot for different applications (e.g. between one-to-one and one-to-many)
  - Quality is not sufficiently well-defined in the standard
- There‘s no common language to establish an interoperable definition of *fingerprint of sufficient quality* for a specific application scenario
  - When developing an application scenario, define a common understanding of the required image quality – at the very beginning!
  - A baseline tool (as common language) is needed for doing this

Joint effort towards NFIQ2.0

Federal Office for Information Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

Federal Office for Information Security

Bundeskriminalamt

Fraunhofer IGD

CASED

secunet

Homeland Security Science and Technology

NFIQ history / milestones

Federal Office for Information Security

- 2004: Release of NFIQ-1 by NIST
  - Open source, accepted by the community
  - Only five different values as output (1 – 5)
- March 2010: 1st workshop at IBPC 2010
  - Wish list on NFIQ2.0
    - Open source, generalization, interoperability
  - NFIQ2.0 should follow a similar technical approach – but better, bigger, faster, etc.
- March 2012: 2nd workshop at IBPC 2012
  - Presentation of concepts and first components
- Sept. 2013: Biometric Consortium Conference (BCC 2013)
  - Presentation of the 1st NFIQ2.0 prototype

NFIQ2.0 design considerations

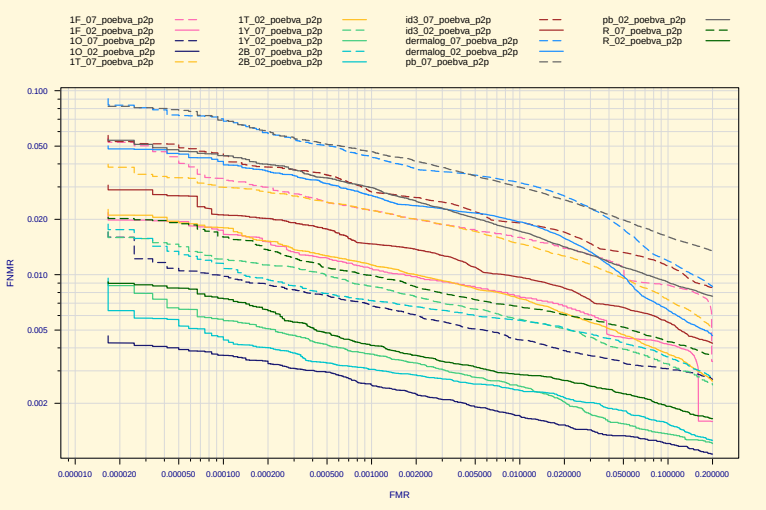
Federal Office for Information Security

- Modular approach for NFIQ2.0 development is desired
  - to be flexible regarding the implementation
  - to have a common basis of functionality needed for NFIQ2.0 development which might then be extended by exchange of certain modules
  - because project team is distributed and located all over the world
  - because only certain project partners have access to certain fingerprint databases
  - because work can be shared and re-used by others
  - to simplify the development process

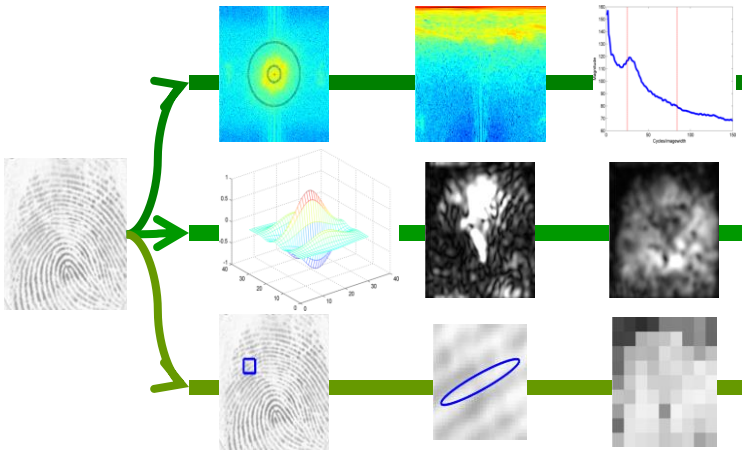
NFIQ2.0 development process

Federal Office for Information Security

- **(1) Public call for participation** (9 comparison score providers)



- **(2) Feature implementation + evaluations** (100+ features)

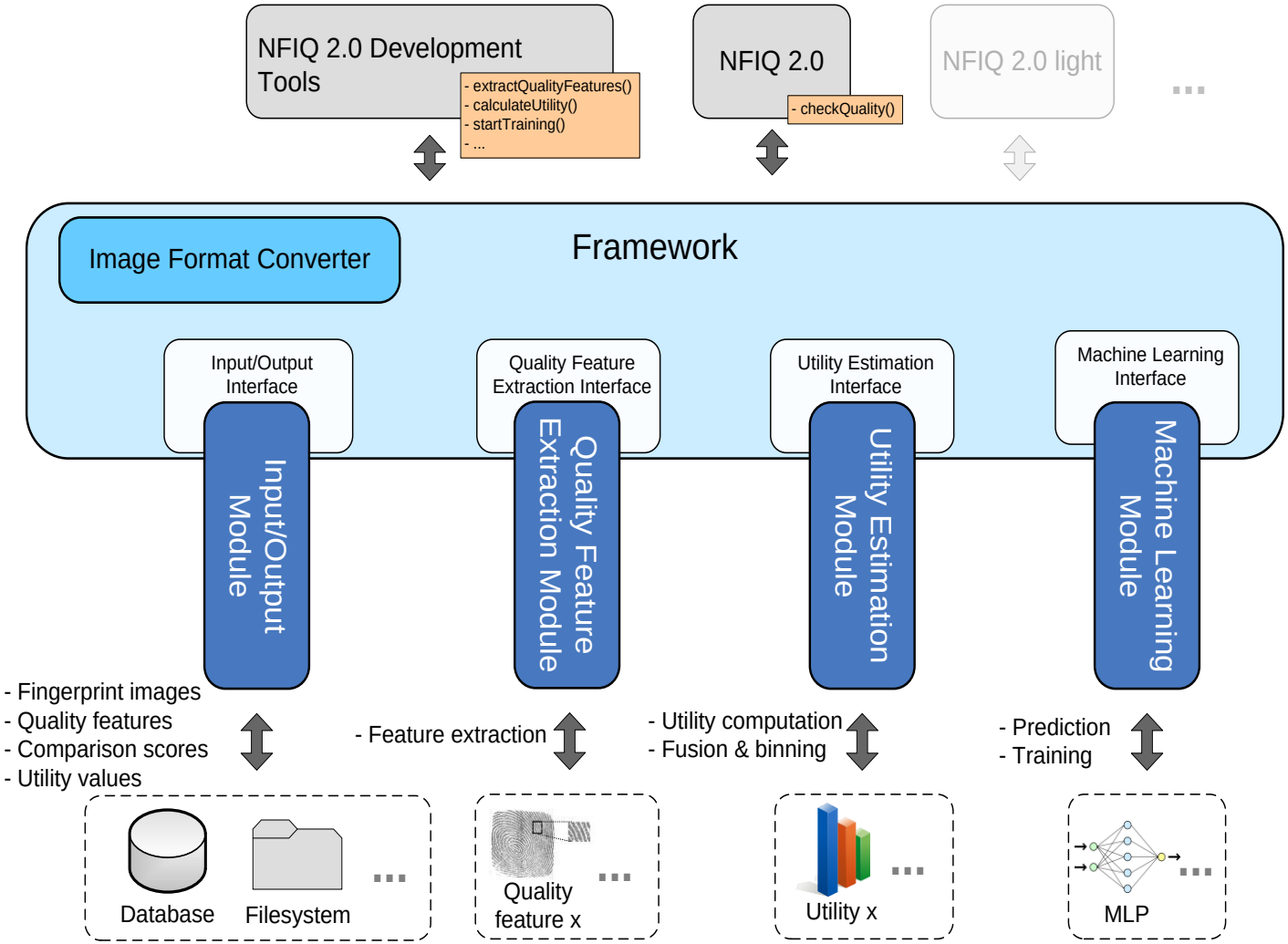


- **(3) Training + Test set construction**

- **(4) Machine learning**

NFIQ2.0 framework

Federal Office for Information Security



NFIQ2.0 features

Federal Office for Information Security

- **Image/signal processing**
  - Local clarity score
  - Ridge valley uniformity
  - Orientation certainty level
  - Orientation flow
  - Frequency domain analysis
  - Radial power spectrum
  - Gabor filters (several variants)
- **Minutiae based**
  - FingerjetFx
    - Open source implementation from digitalPersona
    - Digitalpersona.com/fingerjetfx
  - Total count of minutia
  - Count of minutia in region of interest
    - Various selection of ROI

Requirements

- Must be based on publicly available algorithms
- Standardized interface (inputs and outputs)

Machine learning

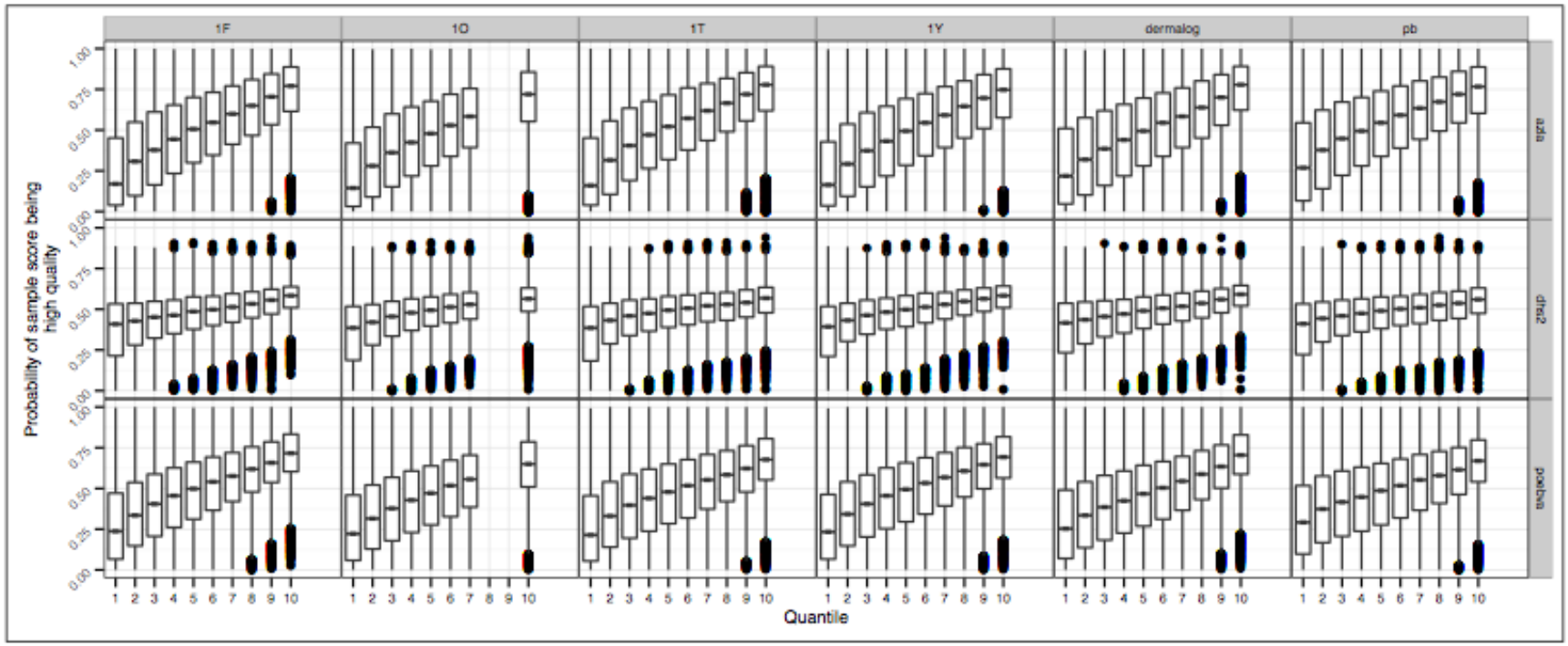
Federal Office for Information Security

- **Two class prediction**
  - High vs. low performers
    - **Class 1:** High performers are images that result in high genuine scores
      - > $CDF^{-1}(0.95)$
    - **Class 0:** Low performers are images that result in false reject
      - Threshold at FMR=0.0001
    - Quality score is the probability that a given image belongs to class 1.
  - Map quality score to recognition rate
- **Random Forest**
  - Ensemble classifier using stochastic process
    - Use vote to determine class memberships
    - Provides class probability in predictions
    - Analysis of features importance and their ranking
  - Training
    - About 5000 samples in each of the low and high performers classes
    - 1000 trees in forest

NFIQ2.0 prototype

Federal Office for Information Security

- Test result :: Boxplot of the output of random forest per quantized comparison score bin for test set



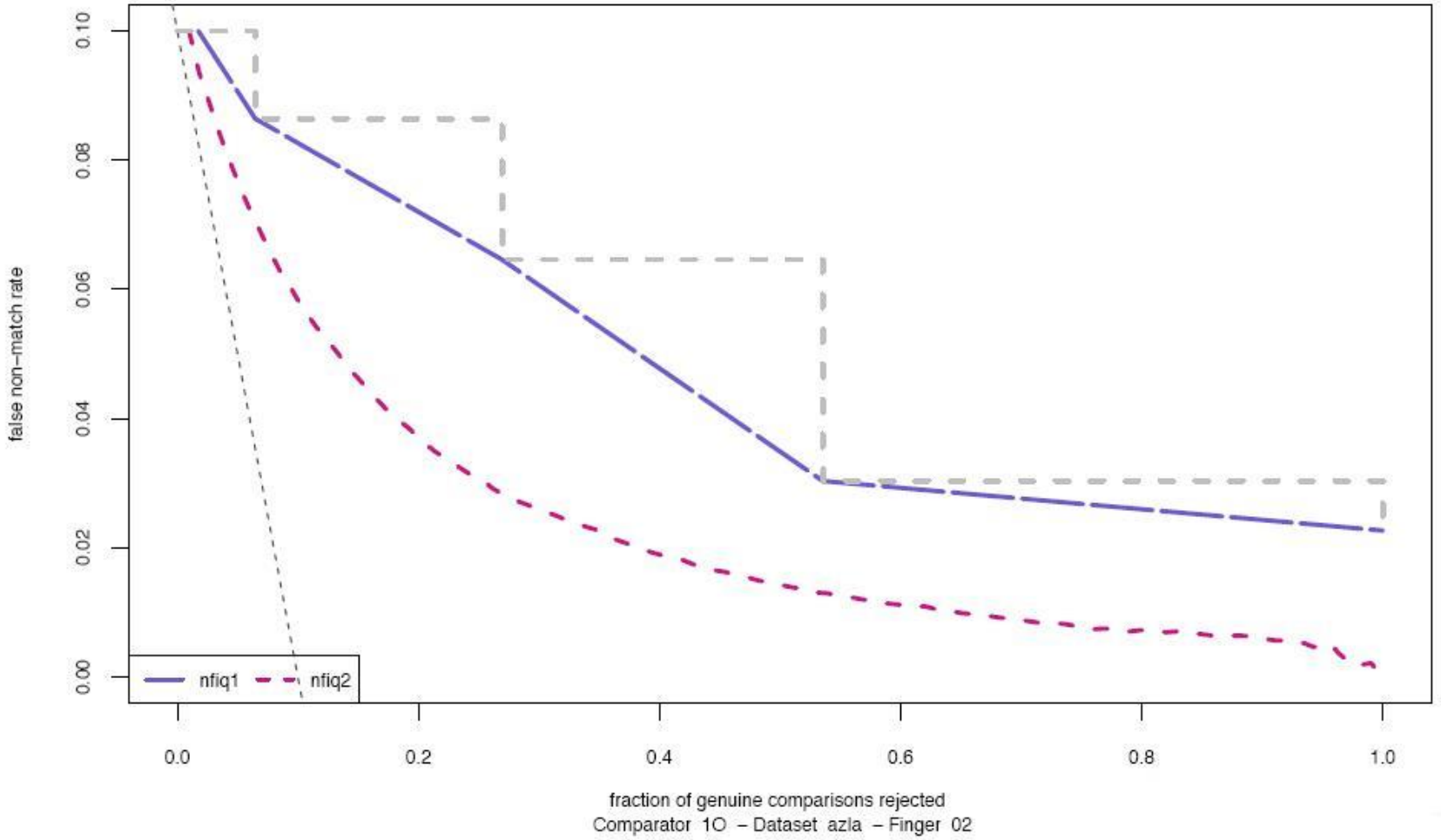
NFIQ2.0 prototype features

Federal Office for Information Security

- Preliminary feature list
  - Size of fingerprint
  - Ridge valley uniformity
  - Orientation certainty
  - Orientation flow maps
  - Gabor features
  - Minutiae count and quality
  - Simple contrast features
  - Radial power spectrum

NFIQ2.0 prototype performance

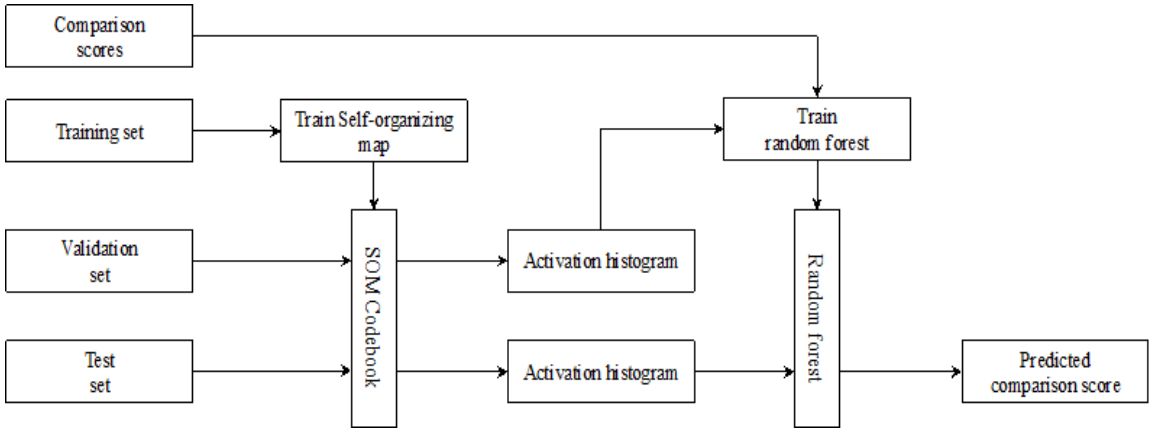
E. Tabassi: „Development of NFIQ 2.0 “,
Biometric Consortium Conference, (2013)



NFIQ2.0 Light

Federal Office for Information Security

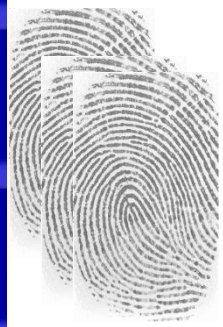
- Motivation
  - Computation complexity of feature extraction is high
  - Therefore, feature computation not feasible in mobile devices/sensors
- Suggested solution
  - Pre-compute a lookup table to speed up the computation
- Two stage process
  - Clustering using Self-Organizing Map
  - Prediction using Random Forest



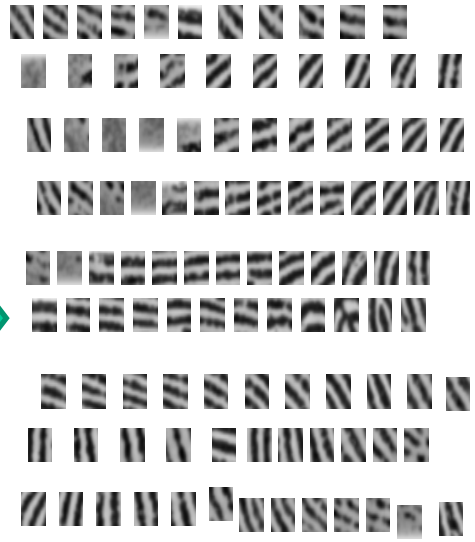
Self Organizing Maps (SOM) for NFIQ2.0 Light

Federal Office for Information Security

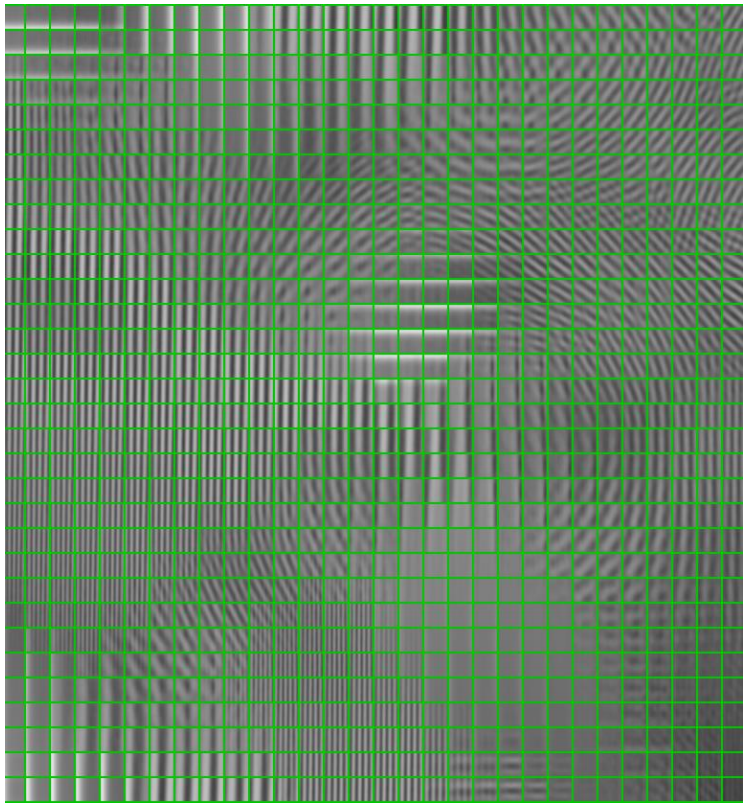
M. Olsen, E. Tabassi, A. Makarov, C. Busch: „Self-Organizing Maps for Fingerprint Image Quality Assessment“, in Proceedings of the 26th Conference on Computer Vision and Pattern Recognition (CVPR 2013), June 23-28, Portland, Oregon, (2013)



Images divided into blocks



SOM code book



NFIQ2.0 Light process flow

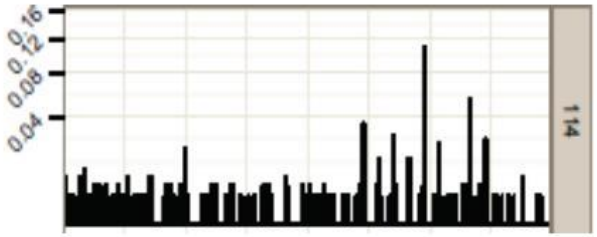
E. Tabassi: „Development of NFIQ 2.0 “,
Biometric Consortium Conference, (2013)

Federal Office
for Information Security

Divide fingerprint image into blocks and look up nearest cluster to get a label

A	A	A	A	A
A	B	C	D	A
A	E	C	D	A
A	E	C	C	A

Finger image is transformed into cluster histogram



Random Forest

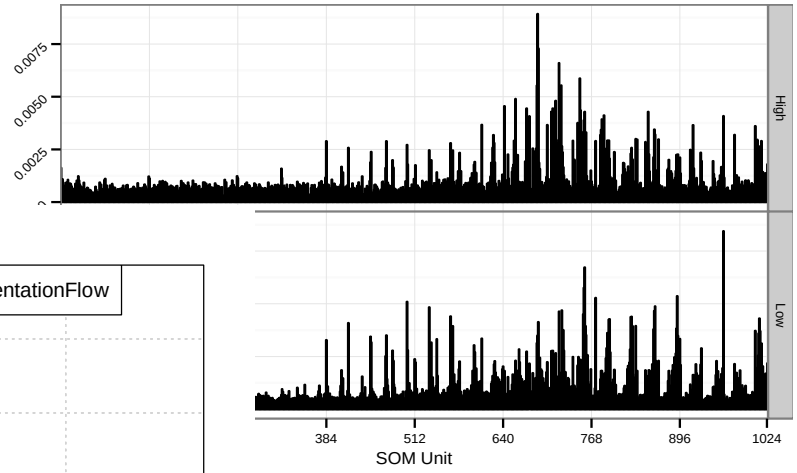
Quality Score

NFIQ2.0 Light prototype performance

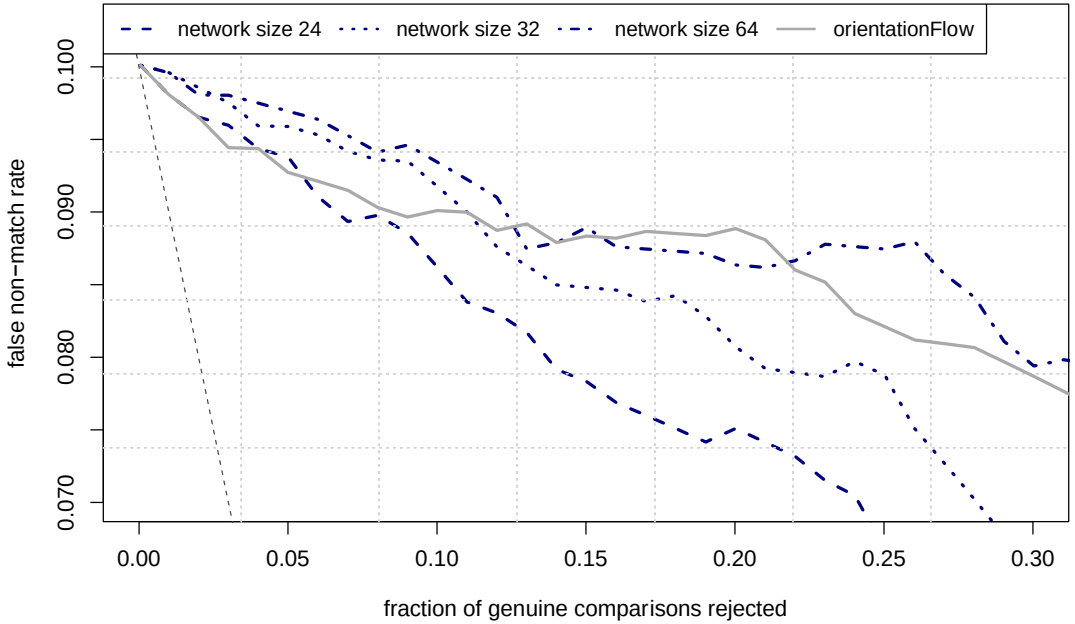
M. Olsen, E. Tabassi, A. Makarov, C. Busch: „Self-Organizing Maps for Fingerprint Image Quality Assessment“, in Proceedings of the 26th Conference on Computer Vision and Pattern Recognition (CVPR 2013), June 23-28, Portland, Oregon, (2013)

Federal Office for Information Security

Features

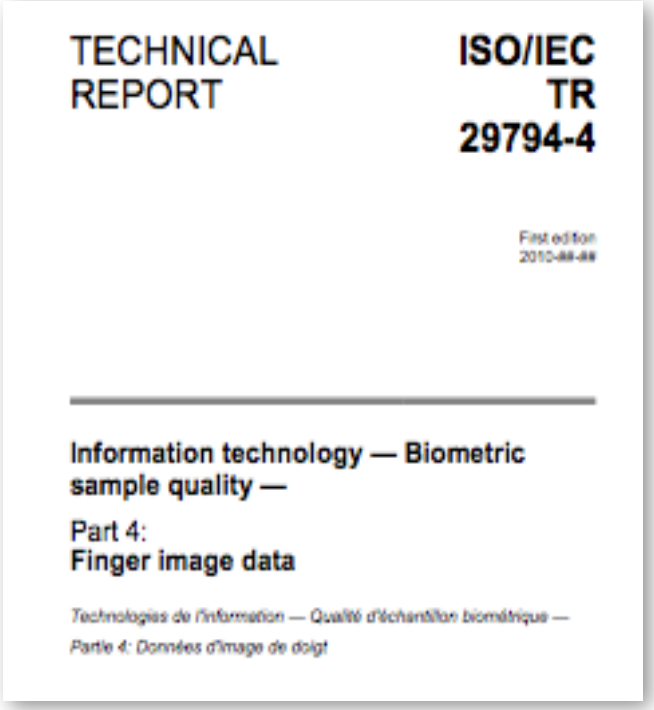


Performance



Dissemination as International Standard

- Results from development will be included in ISO/IEC 29794-4:201x "Information technology – Biometrics sample quality Part 4: Finger image data"
- Quality feature classes
  - Global features
  - Local features (blockwise)
- Expected return of research investment
  - Revision of ISO/IEC 29794-4:201x
    - Currently at 2nd working draft
  - Upgrade from Technical Report (TR) to an International Standard (IS)
- NFIQ2.0 complementing the standard as reference implementation


TECHNICAL REPORT

ISO/IEC TR 29794-4

First edition

Information technology — Biometric sample quality —

Part 4:
Finger image data

Technologies de l'information — Qualité d'échantillon biométrique —
Partie 4: Données d'image de doigt

State of play and expectations for the future

Federal Office for Information Security

- NFIQ2.0 prototype has been presented at the Biometric Consortium Conference (BCC) in September 2013
- Validation of the prototype is currently ongoing
  - Feature selection and validation on large databases
- NFIQ2.0 is expected to be used
  - as baseline tool for defining “fingerprint of sufficient quality”
  - by all major fingerprint-based biometrics systems
  - as calibration base for vendor QA tools
    - Vendor QA tools will not disappear, but – at least – for large scale applications must be comparable (statistically, not on a by-image-basis) to NFIQ2.0
- NFIQ2.0 Light is expected to be implemented in embedded systems and mobile devices (e.g. auto-capture loop of fingerprint sensors)

Thank you!

Federal Office for Information Security

- Federal Office for Information Security (BSI)
- Markus Nuppeney
  - Markus.nuppeney@bsi.bund.de
  - http://www.bsi.bund.de
- NFIQ2.0: http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm