Fusion of Multibiometrics and Liveness Information for Automated Border Control

Dr Peter Wild

p.wild@reading.ac.uk

Presentation based on

P. Wild, P. Radu, L. Chen, J. Ferryman.
Towards Anomaly Detection for Increased Security in Multibiometric Systems: Spoofing-resistant 1-Median Fusion Eliminating Outliers. (IJCB'14).

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein.

Computational Vision Group @ University of Reading

Team

- Prof J Ferryman
- 7 Postdocs
- 4 PhD Students

Topics

- Iris Biometrics
- Multimodal Biometrics
- Counter-Spoofing
- 2D+3D Face Recognition
- Detection&Tracking
- Behaviour Recognition

Funding

- FastPass, EU FP7
- IPATCH, EU FP7
- P5, EU FP7
- EDEN, EU FP7
- ARENA, EU FP7
- EFFISEC, EU FP7

Further info please visit: cvg.reading.ac.uk

FastPass

Aim	• Harmonised, modular reference system for ABC • User-centric approach
Details	• EU FP7 Security • Jan 2013 – Dec 2016 • 27 Partners, led by AIT
Challenges	• Fast & secure ID check • Fingerprint as important modality (SBP)
Why?	• Address „Spoofing“ for ABC • Increased Usability • Harmonised Usage
Further Info	• Please visit: www.fastpass-project.eu

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Fingerprint Recognition

38.1%

Unique, reliable recognition

Most widely used biometric trait

Cheaper than other biometric sensors (e.g. iris)

Easy to integrate with other systems

Used at border control

Range of sensors: Optical, Solid state, Multispectral imaging, 3D

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Fingerprint Spoofing

Spoofing

- Direct attack at sensor-level
- Replication of original fingerprint
- Data to bypass the sensor

Materials

- Fingerprint images
- PlayDoh
- Gelatin
- Silicon
- Cadaver fingers, etc.

Competitions

- LivDet: Fingerprint Liveness Detection
- Since 2009, every 2 years
- Multiple sensors: optical & swipe
- Various materials

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Towards Anomaly Detection in Multibiometric Fusion

Problem

- Standard fusion sensitive to spoofing

Question

- How to make **them more robust?**

Intuition

- **Detect and eliminate anomalies**
- Modeling human surveillance operators

Solution

- Novel **spoofing-resistant fusion** method
- Improved security, while retaining accuracy

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein.

Related Work

Akhtar et al., BTAS'12

- Score-level fusion can be fooled by a single biometric

Rodrigues et al., BTAS'10

- Likelihood ratio (LLR) and fuzzy logic combining recognition scores and quality

Marasco et al., MCS'11

- Combining liveness detection with match scores modality-wise

Marasco et al., BTAS'12

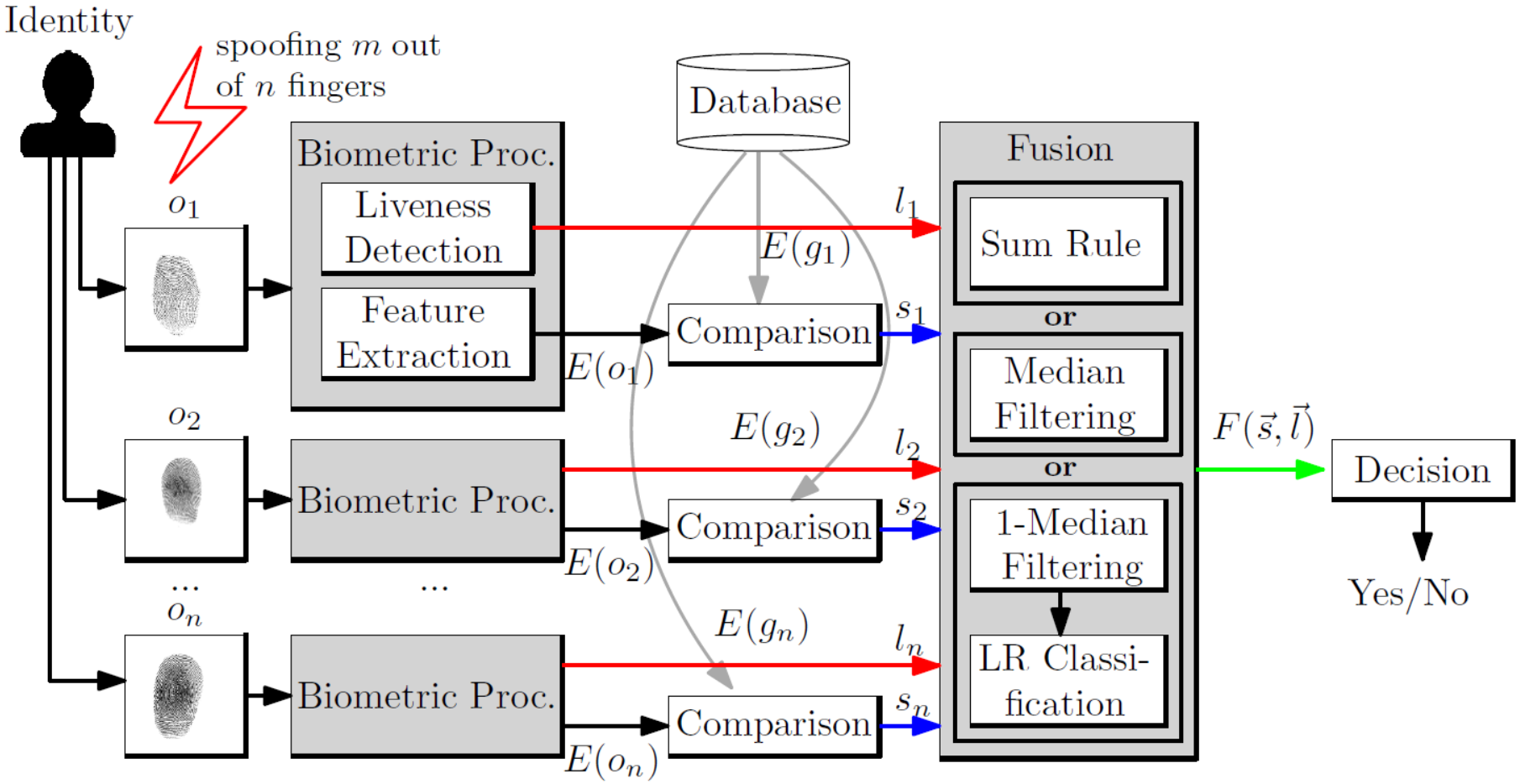
- Bayesian Belief Network for combining match scores and liveness

Rattani et al., WIFS'13

- Learning-based fusion method
- Quality, liveness and match scores are influenced by the sensor

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Counter-spoofing Framework



The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Median Filtering

- Fixed score rules:

$$F_{sum}(\vec{s}) := \frac{1}{n}\sum_{i=1}^{n} s_i; \quad F_{median}(\vec{s}) := \underset{i=1}{\overset{n}{med}}\, s_i$$

- Median Filter:

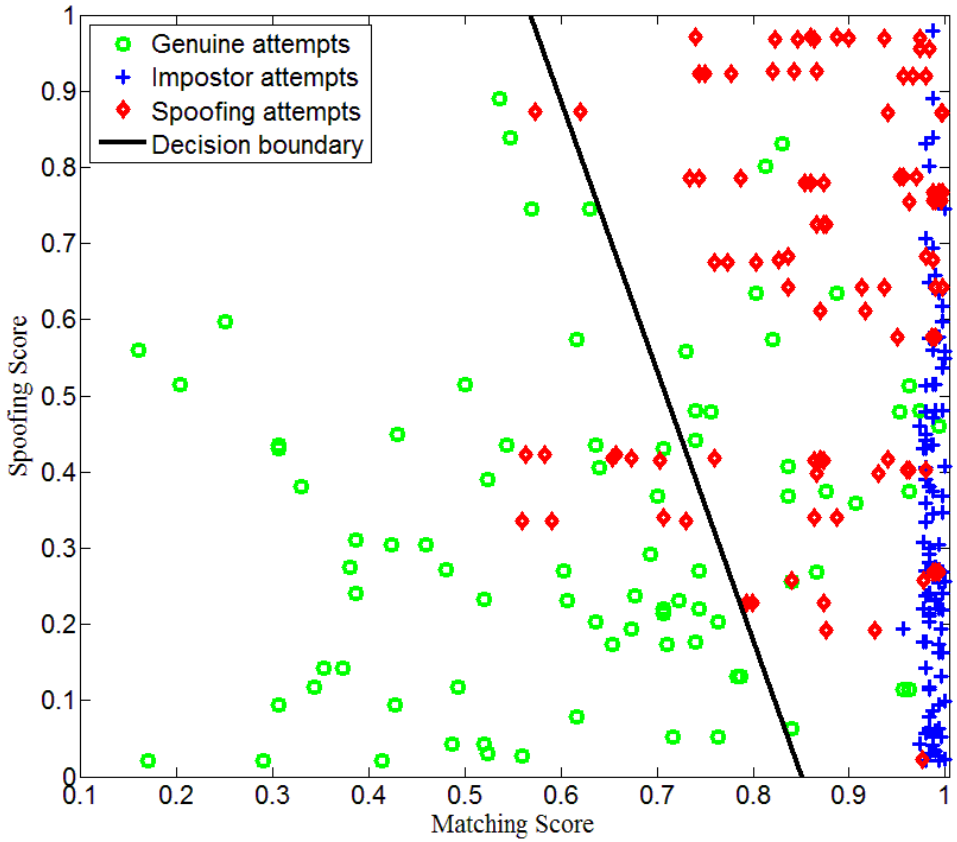
$$F_{mf}(\vec{s}) := \frac{1}{\sum_{i=1}^{n} M(\vec{s}, s_i)} \sum_{i=1}^{n} M(\vec{s}, s_i) s_i$$

$$M(\vec{s}, s_i) := \begin{cases} 1, & if \left| s_i - \underset{j=1}{\overset{n}{med}}\, s_j \right| < \phi; \\ 0, & else. \end{cases}$$

- Median Filtering:

$$F^2_{mf}(\vec{s}, \vec{l}) := \frac{1}{\sum_{i=1}^{n} M\left(\begin{bmatrix}\vec{s}\\ \vec{l}\end{bmatrix}, \begin{bmatrix}s_i\\ l_i\end{bmatrix}\right)} \sum_{i=1}^{n} M\left(\begin{bmatrix}\vec{s}\\ \vec{l}\end{bmatrix}, \begin{bmatrix}s_i\\ l_i\end{bmatrix}\right)$$

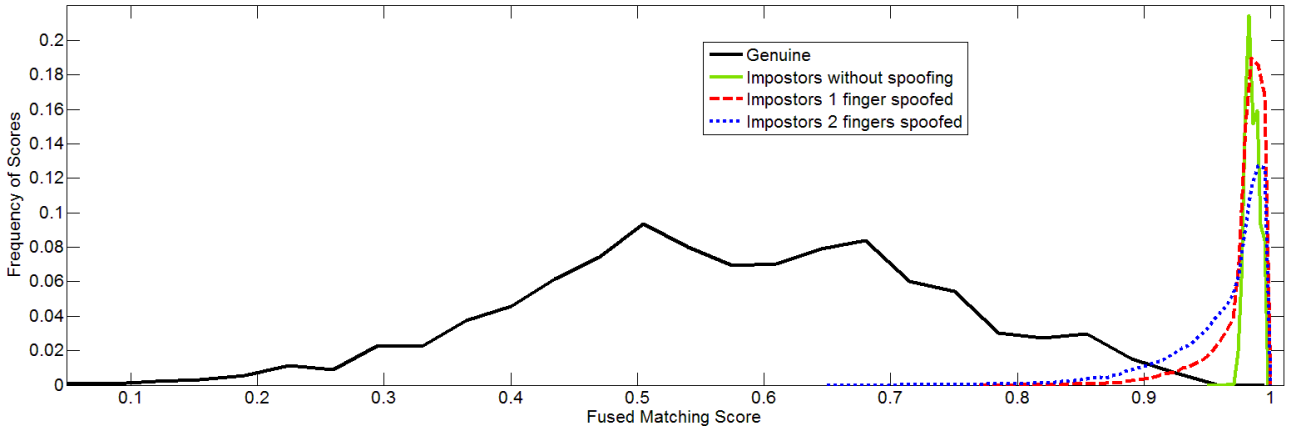
$$M\left(\begin{bmatrix}\vec{s}\\ \vec{l}\end{bmatrix}, \begin{bmatrix}s_i\\ l_i\end{bmatrix}\right) := \begin{cases} 1, & if \left\| \begin{bmatrix}s_i\\ l_i\end{bmatrix} - \underset{j=1}{\overset{n}{med}} \begin{bmatrix}s_j\\ l_j\end{bmatrix} \right\| \\ 0, & else. \end{cases}$$



$$F_{mf}(\vec{s}, \vec{l}) := dist(F^2_{mf}(\vec{s}, \vec{l}), \Psi).$$

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Experiments



Test Database:

- Liv'Det 2013 CrossMatch (2500 live, 2000 spoof images), multibiometric setup
- Right hand images for testing, left hand images for training

Tested Spoofing Attack:

- Impostor has access to m = 0, 1,…n out of n presentable fingerprints (m-spoof)

System:

- Features: NIST *mindtct* (feature extraction) + *bozorth* (comparison)
- Spoofing: regularized LR - 27.65% ferrlive and 24.2% ferrfake

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Results I

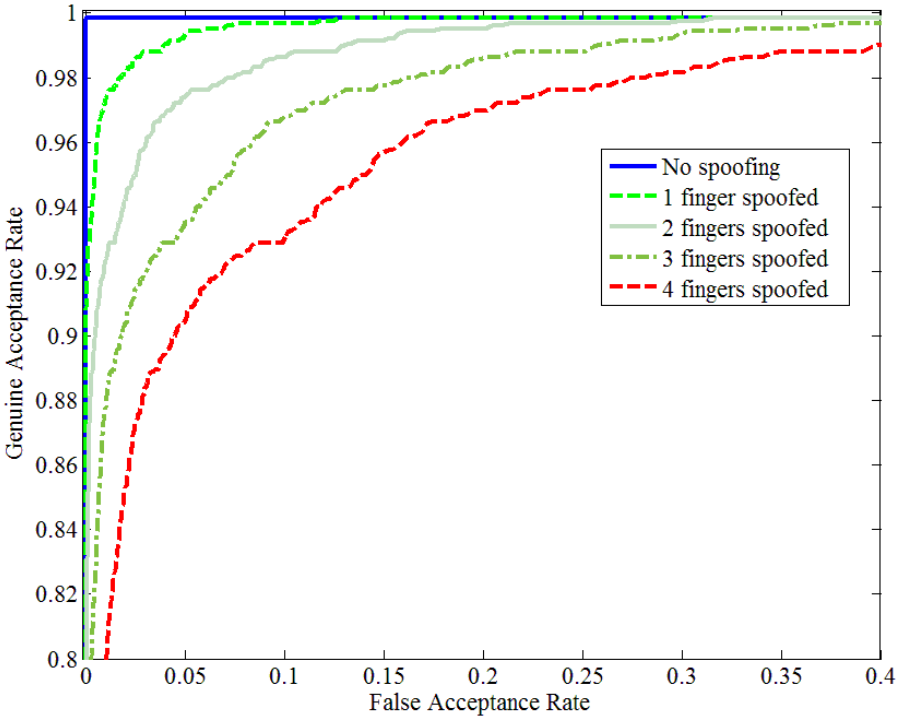
Method	(S)EER					d-Prime				
	0-spoof	1-spoof	2-spoof	3-spoof	4-spoof	0-spoof	1-spoof	2-spoof	3-spoof	4-spoof
Sum rule	0.14	1.91	3.42	5.83	7.52	2.48	2.40	2.27	2.10	1.94
Median rule	1.56	1.23	2.75	5.05	7.5	2.43	2.41	2.27	2.07	1.87
Median filter	1.24	1.29	2.89	5.60	7.76	2.55	2.52	2.34	2.12	1.93
1-Median filter + LR	1.69	1.78	1.78	1.78	1.78	2.89	2.89	2.89	2.89	2.89

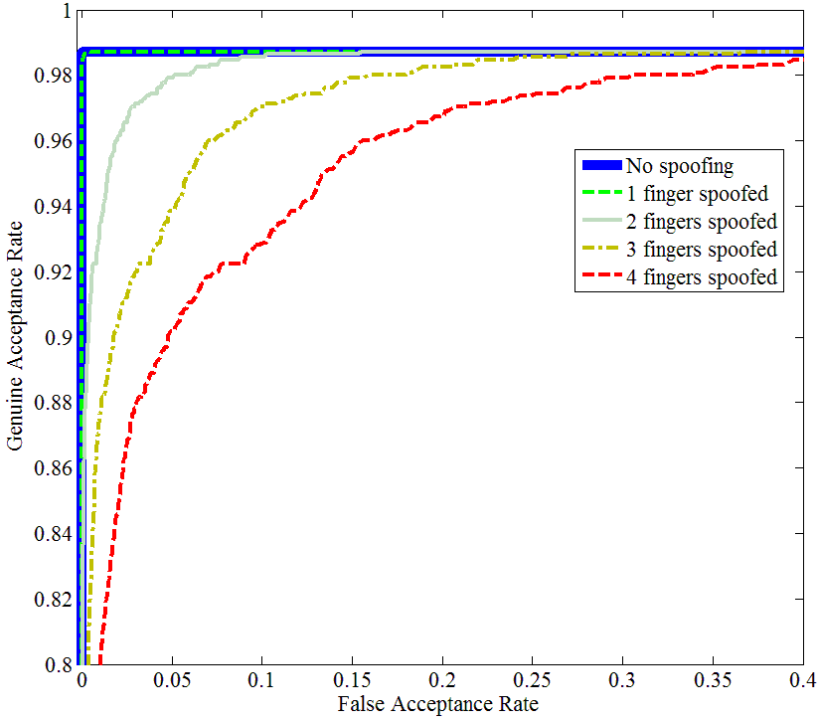
- *How does a spoofing of m out of n fingers impact on fusion?*
  - Even a single spoofed finger severely shifts impostor score distribution.
  - Standard sum rule: every additional finger increases EER by an absolute value of 1.8-2.4%.
  - Even 4-finger spoofing does not necessarily imply success (EER in this case is 7.52% vs. 0.14% 0-spoof).

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Results II

- *How to avoid negative accuracy impact of scores from fake fingerprints?*
  - Median rule is more robust in spoofing (1.23% EER for 1-spoofs);
  - However, for the 0-spoof case, median rule rejects useful information.

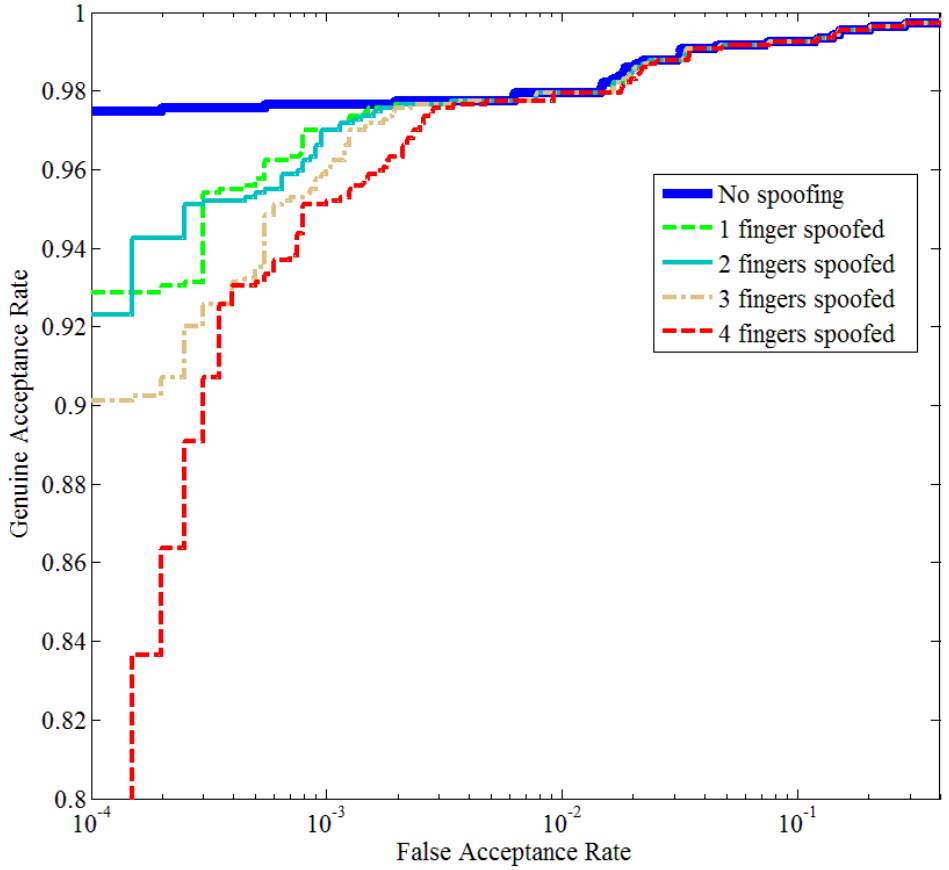




The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Results III

- *How to integrate spoofing countermeasures in fusion rules?*
  - Idea: median has a breakdown point of 0.5 and is able to suppress a number of outliers
  - 1-median filtering (scores+liveness) is much more robust versus 3-spoof and 4-spoof attacks.
  - For (S)FARs greater than 10□ corresponding GARs differ minimally, with stable EERs in 1.69-1.78% (d-Prime 2.89)



The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Summary

Result 1	• Fingerprint Livdet 2013: If 1 or 2 out of 4 samples are spoofed**, median filtering outperforms sum rule**, while not using any ancillary information
Result 2	• It is possible to define fusion rules (median filtering) integrating liveness scores such that **EERs remain stable over all spoofing attempts**.
Remaining Problem	• Median filtering comes at the cost of slightly **reduced 0-spoof performance**
Further Tasks	• **Normalisation** (problematic in multimodal configuration)

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein. All document contained therein cannot be copied, reproduced or modified in the whole or in the part for any purpose without written permission from the FastPass Coordinator with acceptance of the Project Consortium.

Future Work and Remaining Challenges

Multimodal
- Increase difficulty to **spoof multiple traits**
- Decisions in the **absence of certain features**
- Extend to **multispectral** sensors 2D+3D

Quality
- Incorporation of **quality in decision process**
- Types of materials (material-**independence)**
- Increase the **difficulty of replication process**

Optimisation
- **Optimised selection** of filter parameters
- Adaptive fusion schemes
- Normalisation issues

Evaluation
- ABC-specific dataset with realistic attacks
- FastPass Trial Start: Q1 2015 @ VIA
- Extension to multimodal biometrics

The work has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the author's view and the European Union is not liable for any use that may be made of the information contained therein.

Thank you for your attention!

Any Questions?