Aalto University
School of Electrical Engineering

ambient intelligence

Mobile Match-on-Card Authentication Using Offline-Simplified Models with Gait and Face Biometrics

Rainhard Dieter Findling[1], Michael Hölzl[2], René Mayrhofer[2]

IEEE Transactions on Mobile Computing. DOI: 10.1109/TMC.2018.2812883

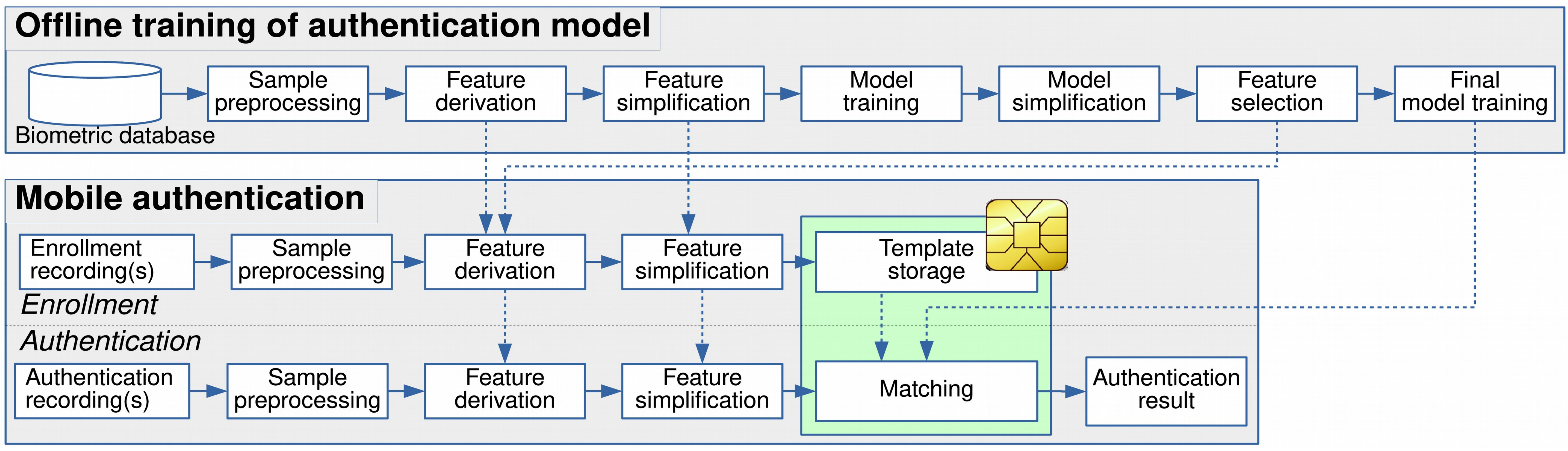
[1]Ambient Intelligence Group, Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland
[2]Department of Networks and Security, JKU Johannes Kepler University Linz, Austria
rainhard.findling@aalto.fi

Problem statement

Biometrics used in authentication with mobile devices need to be protected to reduce the risk of their unauthorized disclosure. Smart cards (SCs) can act as storage and perform match-on-card (MOC) authentication with biometrics to achieve this. However, SCs are limited in computational power, transmission bandwidth and amount of storage. Enabling MOC-based authentication universally applicable to arbitrary biometrics, which does not cause significant reduction in authentication accuracy, would thereby facilitate the transfer of a broader range of biometrics used with mobile authentication to utilizing SCs.

Method

We simplify the biometric sample feature space and the authentication model parameter space (classification via linear combinations) with arbitrary biometrics to enable MOC authentication. We thereby transmit, store, and process reduced amounts of data to and on SCs. To generate authentication models that do not need retraining to enroll new users we perform offline training with a database of the corresponding biometrics. We demonstrate the application on acceleration based mobile gait authentication and face authentication, and investigate the effects of using 16 and 32 bit SCs over non-simplified features and models.



Offline training of authentication model

Biometric database → Sample preprocessing → Feature derivation → Feature simplification → Model training → Model simplification → Feature selection → Final model training

Mobile authentication

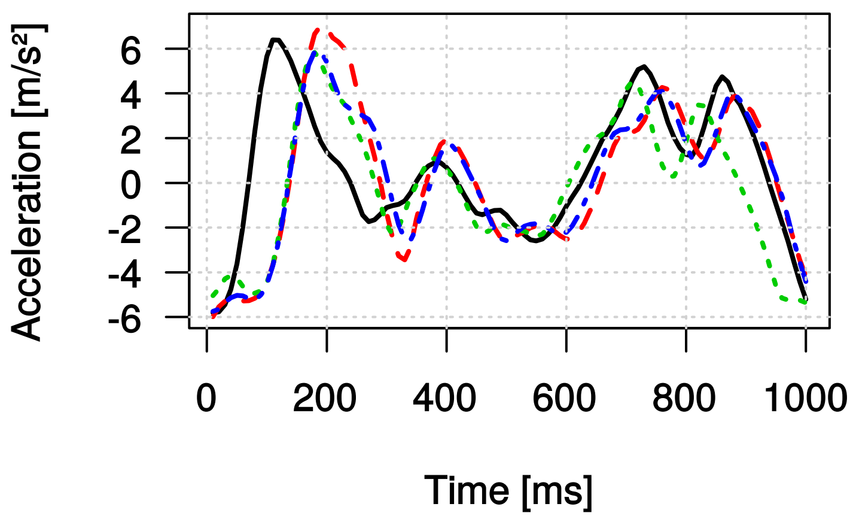
Enrollment

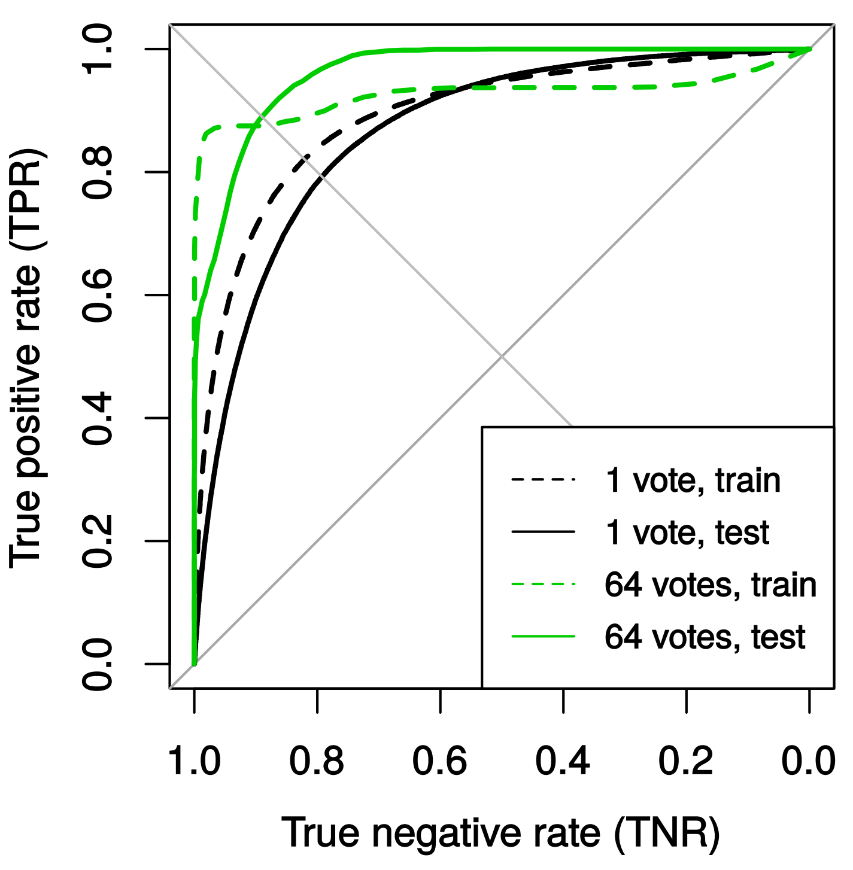
Enrollment recording(s) → Sample preprocessing → Feature derivation → Feature simplification → Template storage

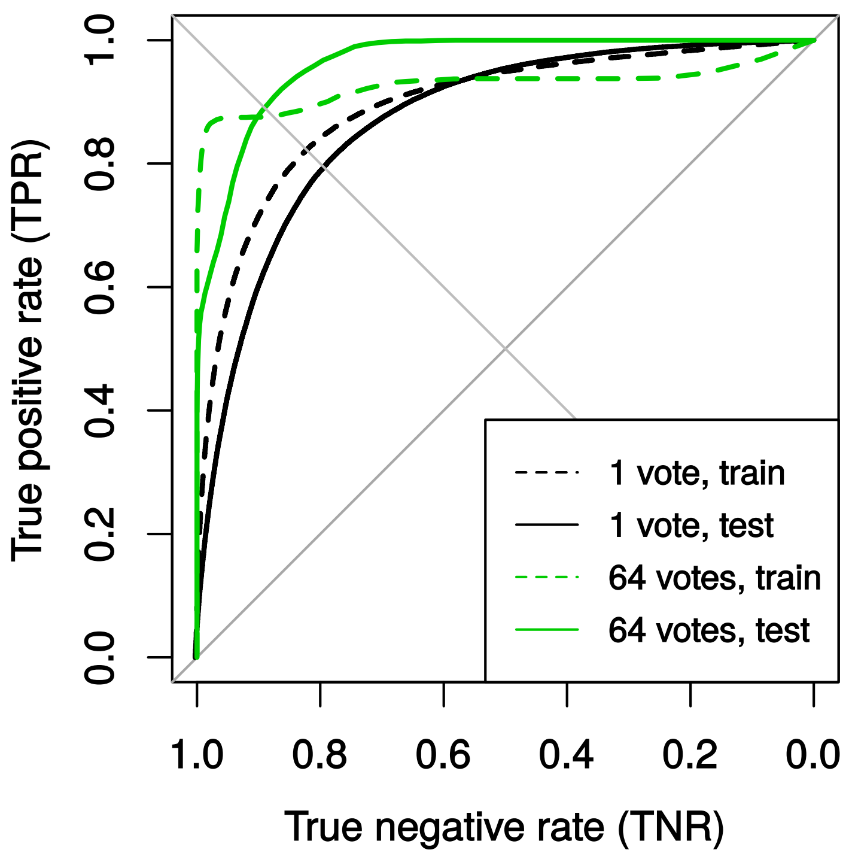
Authentication

Authentication recording(s) → Sample preprocessing → Feature derivation → Feature simplification → Matching → Authentication result

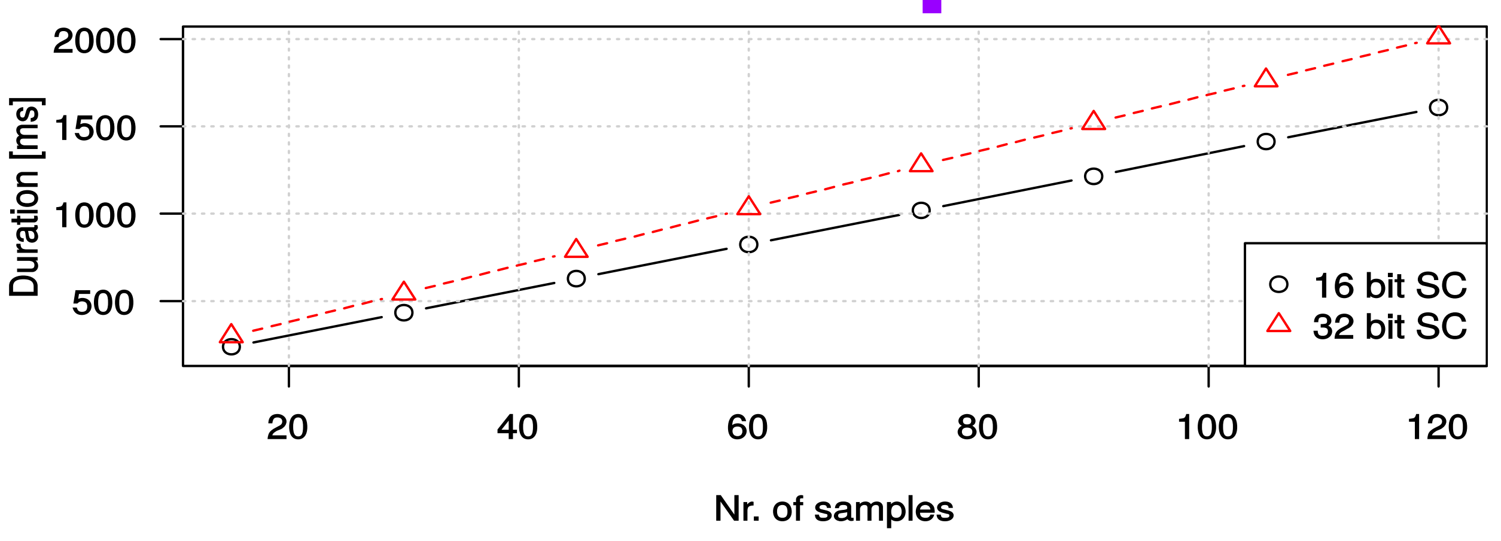
Gait authentication

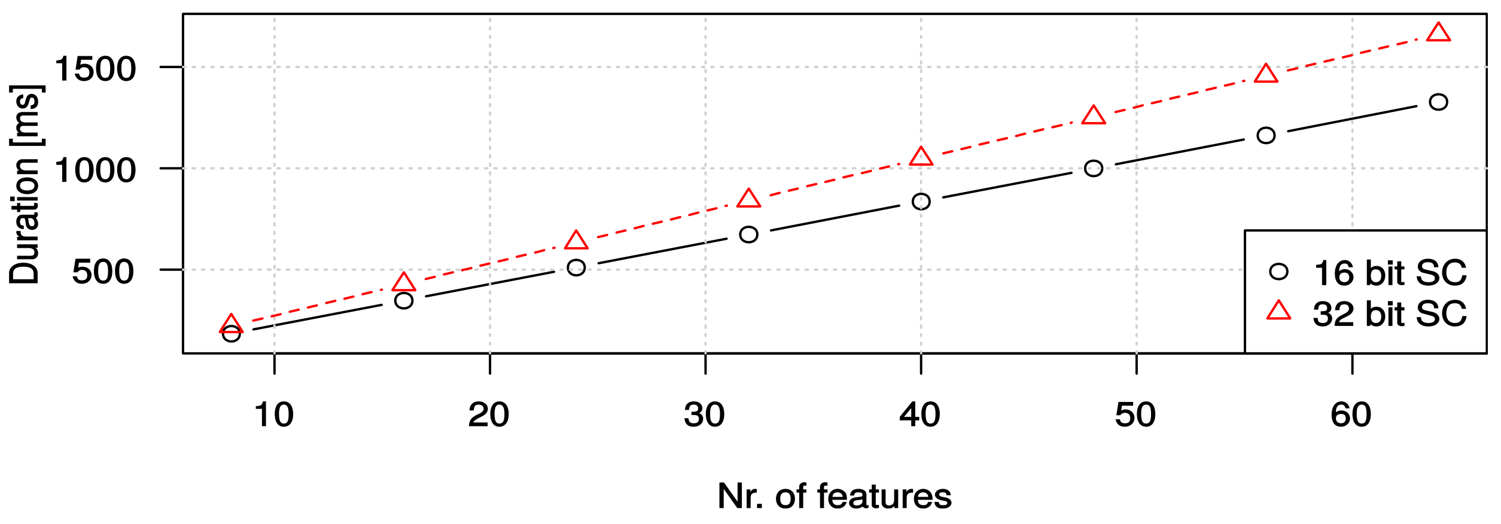






Transmission speed





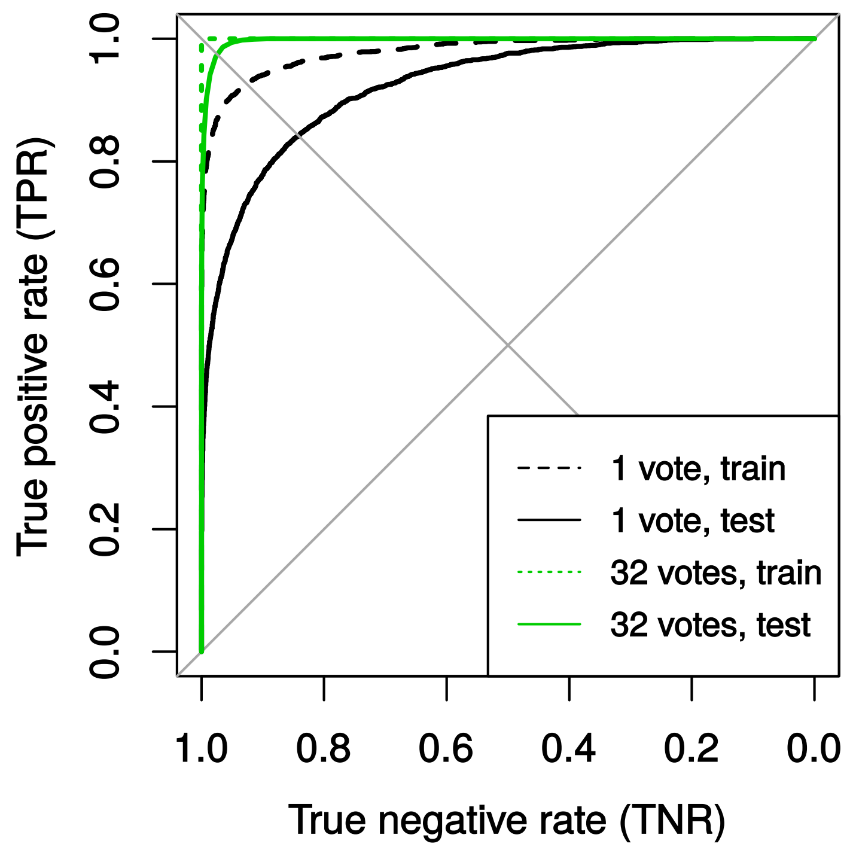
Simplification exc. (features)

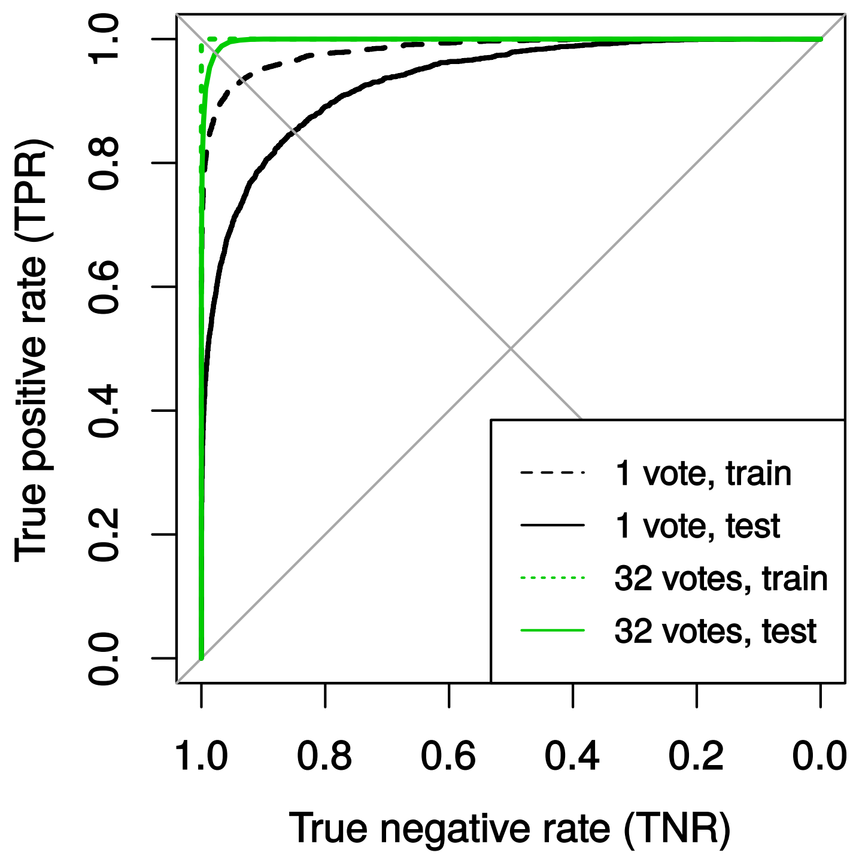
$$\vec{f_r} = \text{round}\left(\frac{\vec{f_o} - mean(\vec{f_o})}{2 \cdot SD(\vec{f_o})}\right) \cdot (2^{\frac{B}{2}-1} - 1) + (2^{\frac{B}{2}-1} - 1)$$

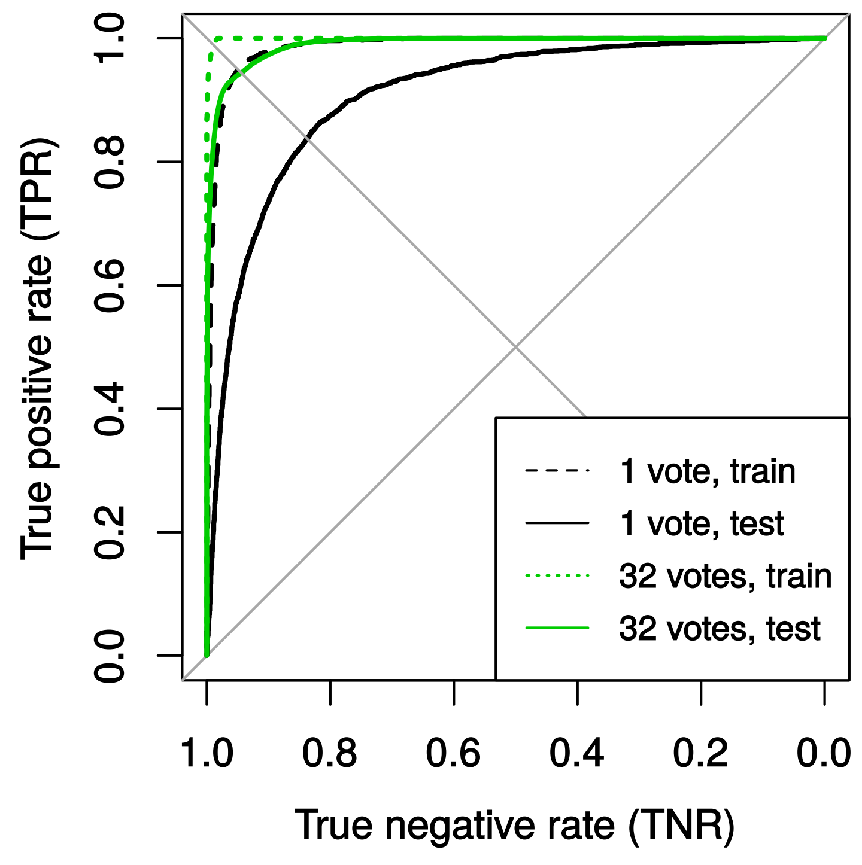
$$\vec{f_t} = \begin{cases} 0 & \text{for } \vec{f_r} < 0 \\ 2^{\frac{B}{2}} - 1 & \text{for } \vec{f_r} > 2^{\frac{B}{2}} - 1 \\ \vec{f_r} & \text{else} \end{cases}$$

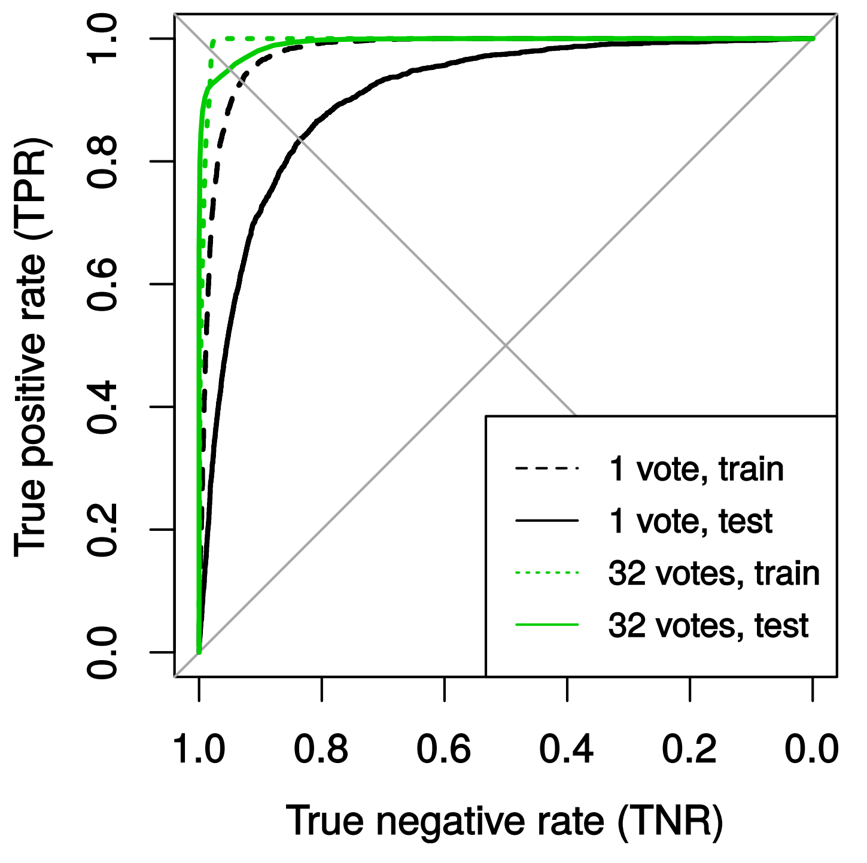
Evaluation Type	Results
Transmission speed 1 sample, 75 features	32ms (16bit SC) 17ms (32bit SC)
Gait authentication ~2 sec on SC	16 bit SC: 11.4% EER 32 bit SC: 11.4% EER Real valued: 11.5% EER
Face authentication Yale-B DB ~1 sec on SC	16 bit SC: 2.4% EER 32 bit SC: 3% EER Real valued: 2.5% EER
Face authentication Panshot Face Unlock DB ~1 sec on SC	16 bit SC: 5.4% EER 32 bit SC: 5.3% EER Real valued: 5.3% EER

Face authentication









Conclusions

- Biometric authentication with SCs in mobile devices seems feasible in a simplified model and feature space. There seem to be no significant drawbacks in using a 16 or 32 bit instead of a real valued space. This indicates features and models can be represented sufficiently with the corresponding, reduced amount of information
- Gait authentication: about 2 sec on SCs, 11.4% EER, with total of 64 comparisons
- Face authentication: about 1 sec on SCs, 2.4-5.4% EER, with total of 32 comparisons