Josef Ressel Center for User-friendly Secure Mobile Environments (u'smile)

University of Applied Sciences Upper Austria
FH OÖ Forschungs&Entwicklungs GmbH

Master's Thesis: Mobile Signature Recognition

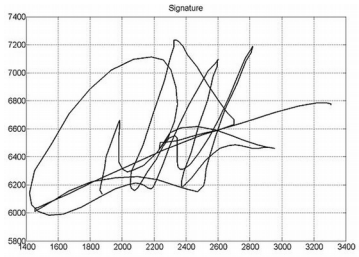
Contact
Rainhard Findling
Machine Learning, Mobile Authentication, Mobile Biometrics

Room: FH3.518
Softwarepark 11
A-4232 Hagenberg/Austria

+43 50804 27188
rainhard.findling@fh-hagenberg.at
www.usmile.at • www.fh-ooe.at

Motivation

Signature recognition [1] is a form of biometric recognition [2] that distinguishes people by their handwritten signatures. Signature recognition can be used to identify users as well as to recognize if signatures are genuine or forged using different feature derivation and matching mechanisms [3-6]. This thesis deals with recognition of digital signatures drawn on screens of mobile devices [7-9], e.g. to authorize mobile banking transactions. We are interested in different aspects, such as a) if there is a significant degradation when the finger is used instead of a capacitive pencil to draw the signature, b) if signatures can be used across different mobile devices without causing degradation, and c) how well forged signatures (=created by someone else) can be detected. This thesis contains significant data analysis and machine learning parts. It is advised to do a thesis related project in the MC520 Applied Machine Learning in Mobile Environments course in the 1st MCM semester. With good performance this thesis can provide the possibility to write a paper for a scientific conference (in combination with MC601 Scientific Working in the 3rd semester).



[wikimedia.org]

Goals

- A literature review should be done, covering existing signature recognition approaches in general as well as specifically for the mobile domain (preprocessing, feature derivation, matching, and results).
- A suitable signature recognition approach should be selected and prototypically implemented to answer the questions of aspect a)-c) above using a publicly available signature database.
- If no public database suits this purpose a mobile signature database should be recorded. The DB should contain multiple samples of signatures from different users and attempts to fake other signatures (both finger and pen, different mobile devices). Creating a small signature recording Android App will be part of this goal.
- The final, fine tuned, and evaluated signature recognition approach should be implemented as Android App.

Research questions

- Which signature recognition approaches are suitable for mobile signature recognition?
- How strong do recognition results change when signatures are drawn with fingers/capacitive pen?
- How strong is recognition performance degraded when using the approach across different mobile devices?
- How well can forged signatures of differently skilled/informed attackers be detected?

Literature

[1] Signature recognition, https://en.wikipedia.org/wiki/Signature_recognition
[2] Biometrics, http://en.wikipedia.org/wiki/Biometrics
[3] Joulia Chapran, 2006. Biometric Writer Identification: Feature Analysis and Classification. In International Journal of Pattern Recognition and Artificial Intelligence, 20(4), p483. Online: http://www.worldscientific.com/doi/abs/10.1142/S0218001406004831
[4] N. Houmani et al., 2012. BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures. In Pattern Recognition, 45(3), 993-1003. Online: http://www.sciencedirect.com/science/article/pii/S0031320311003220
[5] Teodoro Schmidt, Vladimir Riffo, Domingo Mery, 2011. Dynamic Signature Recognition Based on Fisher Discriminant. In Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, Lecture Notes in Computer Science vol 7042, 433-442. Online: http://link.springer.com/chapter/10.1007%2F978-3-642-25085-9_51
[6] Ruben Tolosana, Ruben Vera-Rodriguez, Javier Ortega-Garcia, Julian Fierrez, 2015. Optimal feature selection and inter-operability compensation for on-line biometric signature authentication. International Conference on Biometrics (ICB), 163-168. Online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7139047
[7] Tolosana, R.; Vera-Rodriguez, R.; Fierrez, J.; Morales, A. & Ortega-Garcia, J. Benchmarking desktop and mobile handwriting across COTS devices: The e-BioSign biometric database. PLoS ONE, 2017, 12, 1-17. Online: https://doi.org/10.1371/journal.pone.0176792
[8] Blanco-Gonzalo, R. et al, 2012. Handwritten signature recognition in mobile scenarios: Performance evaluation. IEEE International Carnahan Conference on Security Technology (ICCST), 174-179. Online: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6393554
[9] Ram P. Krish et al., 2013. Dynamic Signature Verification on Smart Phones. In Communications in Computer and Information Science, vol 365, 213-222. Online: http://link.springer.com/chapter/10.1007%2F978-3-642-38061-7_21