Spenden biometrischer Samples

Für unser Forschungsvorhaben benötigen wir biometrische Daten, um Schwachstellen existierender biometrischer Systeme aufzeigen und beheben zu können. Hiervon sollen gerade zukünftige biometrische Anwendungen auf mobilen Endgeräten profitieren.

Bitte unterstützen Sie uns.

- 8 Aufnahme-Sessions, je 15 Minuten
- 6 Wochen zwischen zwei Sessions
- Spende biometrischer Merkmale
  - Stimm-Daten
  - Pseudonym-Unterschrift
  - Impersonationsversuche auf die Stimm- und Unterschrift-Profilen anderer Probanden

Als kleines Dankeschön für unsere Probanden:

- zur ersten Session: 16 GB USB 3.0 Stick,
- zur Abschluss-Session: Smartphone Akku,
- sowie kleine Dreingaben zu jeder Session.

Unter den Teilnehmern, die an allen Sessions teilnehmen, wird eine Digitalkamera verlost.

Die Ergebnisse des Forschungsprojektes werden eine kooperative Dissertation der Hochschule und der Technischen Universität Darmstadt unterstützen.

⇒ einfach am Web-Survey teilnehmen und anmelden:
https://www.dasec.h-da.de/projects/current-projects/biomobile/survey/

Weitere Informationen und Kontakt

BioMobile Projekt-Info Webseite:
https://www.dasec.h-da.de/projects/current-projects/biomobile/

Andreas Nautsch, M.Sc. (Hochschule Darmstadt)

Wissenschaftlicher Mitarbeiter / Doktorand
E-Mail: andreas.nautsch@h-da.de
https://www.dasec.h-da.de/staff/andreas-nautsch/

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Projektpartner der Hochschule Darmstadt:

- atip GmbH http://www.atip.de/
  Experte für Sprach-Dialog-Systeme
- Bundeskriminalamt KT 54
  Fachbereich für Sprechererkennung, Tonträgerauswertung und Autorenerkennung

Förderträger:
Hessisches Ministerium für Wissenschaft und Kunst,
Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE)

LOEWE
Exzellente Forschung für Hessens Zukunft

Forschungs-Institut:
Center for Advanced Security Research Darmstadt (CASED)

CASED

Gesucht

Proband für Forschungsprojekt: Smartphones & Biometrie

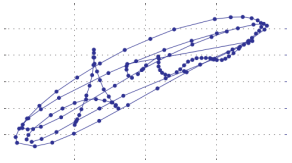
Info-Flyer

da/sec – Biometrics & Internet-Security,
Fachbereich Informatik,
Hochschule Darmstadt

Forschungsprojekt

In dem Forschungsprojekt *BioMobile* [1] werden robuste Algorithmen zur biometrischen Authentifikation mittels Stimme und Unterschrift auf mobilen Endgeräten untersucht. Neben einem großen Facettenreichtum an Sensoren besitzen moderne Smartphones vor allem zweierlei: ein Mikrofon und ein Display.

Neben Stimm-Merkmalen bieten dynamische Unterschriften [2] Sicherheit durch Analysen des Schreibprozesses.



Anwendungsgebiete und Perspektiven:

- Smartphone-Entsperrung mittels Stimm-Profil
- Biometrisches Unterschreiben von PDF-Verträgen
- Vermeidung von Identitäts-Missbrauch in Call-Centern und beim Online Banking
- Usability durch weniger Passwörter merken
  - Stimme & Schrift als Master Passwort
  - Sichere Verbindungen & Kryptographie

Was wir erforschen wollen

Der Hauptfokus von *BioMobile* liegt auf der Erkennung von Menschen anhand ihrer Stimme. Dabei stellen mobile Endgeräte besondere Herausforderungen dar, da nicht jedes Gerät die beste Hardware beinhaltet und sich Umgebungseinflüsse wie Hintergrundgeräusche fortweg ändern wie bspw. andere Sprecher.

Ziel: robustere biometrische Performanz

- Qualitätsabhängige Kalibrierung
- Multi-modale Systeme: Stimme & Unterschrift
- Herausforderung: Verhaltens-Biometrie
  Gleichzeitig Sprechen & Schreiben

Untersuchungsaspekte unserer Forschung:

- Einfluss der Signal-Qualität:
  Smartphone-Aufnahme ⇔ GSM-Netz Übertragung
- Einfluss verschiedener Endgeräte
  - Samsung Galaxy Note 4
  - HTC One M9
  - LG G2 mini
  - Motorola Moto 2nd Gen.
- Robuste Erkennung in verschiedenen Umgebungen
- Sicherheit gegenüber Angriffen
  - bei ähnlichen Sprechern
  - bei Unterschrifts-Fälschungen
  - von Blutsverwandten

Die echte Unterschrift eines Probanden bleibt geschützt: wir nehmen Pseudonym-Unterschriften auf.

Datenschutz-Information

- **Vertrauliche Informationen** werden nicht digitalisiert gespeichert. In einer digitalen Datenbank erscheint dann ein Kommentar zur *nicht Verfügbarkeit*.
- **Anonymisierte** Daten-Speicherung auf **hochschul-internen** Festplatten mit **Zugangskontrolle**.
- Es besteht jederzeit das **Recht**, alle aufgenommenen **eigene Daten einzusehen** und auf Wunsch **löschen zu lassen**.
- Die Daten werden **ausschließlich für Forschungszwecke** verwendet.

Literatur

[1] C. Busch, C. Rathgeb, und A. Nautsch, "Biometrische Sprecher-Erkennung unter unkontrollierbaren Einflussfaktoren im multi-modalen Einsatz auf mobilen Endgeräten (BioMobile)," 2015. [Online]. Verfügbar: https://www.dasec.h-da.de/projects/current-projects/biomobile/

[2] M. Martinez-Diaz, J. Fierrez, und J. Galbally, "The DooDB Graphical Password Database: Data Analysis and Benchmark Results," *IEEE Access*, 2013. [Online]. Verfügbar: http://atvs.ii.uam.es/files/2013_IEEEAccess_DoodlesDB_Marcos_Published.pdf

[3] K. A. Lee, A. Larcher, G. Wang, P. Kenny, N. Brümmer, D. van Leeuwen, H. Aronowitz, M. Kockmann, C. Vaquero, B. Ma, H. Li, T. Stafylakis, J. Alam, A. Swart, und J. Perez, "The RedDots Data Collection for Speaker Recognition," in *ISCA Interspeech*, 2015. [Online]. Verfügbar: http://www.crim.ca/perso/patrick.kenny/kong_interspeech_2015.pdf