Thema A

Rekapitulation, Erweiterung und Systematisierung technischer Fehler biometrischer Systeme

In dieser Seminareinheit wurde der Aufbau eines biometrischen Systems vorgestellt sowie dessen verschiedene Fehlerarten thematisiert, um diese in verschiedene Kategorien einzuteilen.

Es gibt sechs Anforderungen an biometrische Systeme:

- Universalität
- Einmaligkeit
- Konstanz
- Erfassbarkeit
- Leistungsfähigkeit
- Akzeptanz

In dieser Seminareinheit wurde der Fokus auf die Erfassbarkeit und Leistungsfähigkeit gelegt.

Allgemein gibt es zwei Fehlerarten, äußere Fehler und inhärente Fehler. Äußere Fehler sind Fehler, die beispielsweise bei der Anwendung gemacht werden. Inhärente Fehler hingegen sind Fehler, die schon im System vorhanden sind, beispielsweise im Algorithmus.

Ein biometrisches System unterteilt sich in sieben Subsysteme:

1. Data Capture System: Zuständigkeit für das Rohmaterial (Samples)
2. Transmission Subsystem: Übermittlung von Samples und Features
3. Signal processing Subsystem: Erkennung/ Erfassung von Unterscheidungsmerkmalen
4. Data Storage Subsystem: Speicherung von Templates
5. Matching Subsystem: Berechnung von Ähnlichkeitswerten zwischen Fingerprint und gespeichertem Template
6. Decision Subsystem: Ergebnisausgabe
7. Administration Subsystem: Regelung der Implementierung und Nutzung

Dieses biometrische System ermöglicht das Enrolment sowie die Identifikation und die Verifikation. Der Unterschied zwischen der Identifikation und der Verifikation ist ein entscheidender: Bei der Verifikation ist von vornherein bekannt, um welche Person es sich handelt. Es muss nur entschieden werden, ob der Fingerabdruck dem aus dem gespeicherten Template entspricht. Bei der Identifikation hingegen muss das biometrische System die Templates nach einem Treffer durchsuchen. Somit ist am Anfang nicht bekannt, um welche Person es sich handelt.

Fehlerquellen lassen sich in vier Kategorien unterteilen: Eine Allgemein-Kategorie, Sensor & Enrolment, Fingerabdruckbild & Template und Vergleichsalgorithmen.
Unter „Allgemein“ fallen beispielsweise das Alter und Geschlecht des Benutzers oder, dass kein brauchbarer Fingerabdruck vorhanden ist. Auch menschliches Versagen durch falsche Anweisungen oder die Inkompatibilität von Sensor und Algorithmus fallen in diese Kategorie.
Die Kategorie „Sensor & Enrolment“ umfasst sowohl Störungen bei der Erfassung, schlechte Bildqualität und Umwelteinflüsse als auch falsche Bedienung, z.B. dass der Finger falsch aufgelegt wurde, oder Trockenheit/Feuchtigkeit der Finger.
In der Kategorie „Fingerabdruckbild & Template“ kommt das Alter des Templates zu Tragen, denn nach 10 Jahren verdoppelt sich die Falschrückweisungsrate. Auch die Nachbearbeitung der Bilder für Merkmalsextraktion, der Kontrast sowie eine manipulierte Datenbank mit falschen Templates gehören in diese Kategorie.
Schließlich gibt es in der Kategorie „Vergleichsalgorithmen“ Fehler, die, wie der Name schon verrät, mit dem Algorithmus zu tun haben. Unter anderem fallen darunter ein zu großer oder kleiner Schwellenwert und eine undeutige Berechnung der Konfidenz eines Matching, d.h. es wird weder akzeptiert noch abgewiesen.

Zusätzlich können sich bei einer Person noch zwei Fehler ergeben:
Wird eine Person A als Person A abgewiesen, nennt sich dies False Rejection.
Wird eine Person B als Person A identifiziert, nennt sich dies False Acceptance.