

5. Verwendung biometrischer Daten

Als Biometrie (aus dem Griechischen: bios=Leben, metron=Maß bzw. metrein=messen) wird die automatisierte Erkennung oder Verifikation der Identität von lebenden Personen anhand von physischen Charakteristiken oder typischen Verhaltensmustern bezeichnet. Biometrische Daten erlangten vor allem nach den Terroranschlägen vom 11. September 2001 besondere Aktualität; aufgrund der mit biometrischen Daten verbundenen Personenbestimmbarkeit besitzen derartige Daten auch datenschutzrechtliche Relevanz. Nachfolgend wird eine technisch/rechtliche Einführung zur Verwendung von biometrischen Daten gegeben.

5.1. Technische Grundlagen biometrischer Daten

Verfahren, die auf physischen Charakteristiken beruhen, verwenden in der Regel statische Merkmale wie die Struktur von Gesicht, Iris, Fingerabdruck oder Hand. Diese sind zum einen genetisch festgelegt (und damit teilweise auch vererbbar), zum anderen entstehen sie während der Embryonalentwicklung auf der Basis von Zufallsprozessen. Verhaltensbezogene Merkmale erfordern dagegen die aktive, dynamische Ausführung einer Aktion wie dem Schreiben der Unterschrift oder dem Sprechen eines Textes. Verhaltensbezogene Merkmale analysieren die personencharakteristischen Anteile menschlicher Handlungen. Diese beruhen auf einem jahrelangen, individuellen Trainingsprozess unter Einfluss von Erziehung und Umweltbedingungen, jedoch auch hier auf Grundlage der physiologischen Voraussetzungen. So basiert der Klang der Stimme sowohl auf den erlernten Sprach- und Sprechgewohnheiten als auch auf der Physiologie des Mund- und Rachenraumes.

Biometrische Merkmale sind im Allgemeinen öffentlich, d.h. im Prinzip kann sie sich jeder beschaffen. Die Sicherheit eines biometrischen Systems kann daher nicht auf der Geheimhaltung der verwendeten Merkmale basieren.

Biometrische Merkmale werden bereits seit langem u.a. von Staat oder Arbeitgebern zur Personenidentifikation verwendet, z.B. in Form von (Pass-) Bildern oder Fingerabdrücken. Ende der sechziger Jahre entstanden die ersten automatisierten Erkennungssysteme, die Verfahren der heutigen biometrischen Systeme.

Anforderungen an biometrische Daten:

Damit sich ein Körpermerkmal bzw. eine Verhaltensweise zur biometrischen Erkennung eignet, muss es folgende Mindestvoraussetzungen erfüllen:

- Universalität: Das Merkmal sollte bei jeder Person vorhanden sein.
- Einzigartigkeit: Das Merkmal unterscheidet sich von Person zu Person.
- Permanenz: Die Ausprägung des Merkmals ist zeitinvariant.
- Erfassbarkeit: Das Merkmal lässt sich quantitativ erheben.

Keine der aufgrund dieser Kriterien in Frage kommenden Merkmale erfüllen alle diese Voraussetzungen in optimaler Weise. Außerdem spielen bei der Auswahl eines geeigneten biometrischen Verfahrens auch noch Aspekte wie die Benutzerfreundlichkeit und Akzeptanz, die Überlistungsresistenz oder das Kosten-Nutzen-Verhältnis eine Rolle. Für jede Applikation muss/sollte daher aufs Neue entschieden werden, welche Biometrie zum Einsatz kommen soll, oder ob möglicherweise sogar eine Kombination mehrerer Verfahren (multiple Biometrien) sinnvoll ist.

Durchgesetzt haben sich zum heutigen Zeitpunkt Systeme zur Fingerabdruckerkennung, Gesichtserkennung, Iriserkennung, Stimmenerkennung, Handgeometrieerkennung oder Unterschriftenerkennung.

Methoden der Authentifizierung:

Traditionelle Methoden, die Authentizität, d.h. die Übereinstimmung einer behaupteten mit der tatsächlichen Identität zu gewährleisten, beruhen entweder auf einem nur dem Benutzer bekannten Wissen (z.B. Passwort, PIN) oder dem Besitz eines persönlichen Schlüssels oder Tokens (z.B. Private Key, Ausweis, Chipkarte). Diese Methoden sind lediglich personenbezogen, d.h. es kann nur geprüft werden, ob Passwort / PIN bzw. Chipkarte gültig sind, nicht jedoch, ob der Inhaber des Legitimationsmittels auch der tatsächlich Berechtigte ist.

Biometrische Merkmale dagegen sind dauerhaft *personengebunden* und bieten somit die Möglichkeit der Überprüfung des zu verifizierenden Merkmals *zusammen* mit dessen zulässigen Besitz. Eine (unfreiwillige oder auch beabsichtigte) Trennung von der Person kann prinzipiell nicht stattfinden.

Bei der biometrischen Personenerkennung lassen sich zwei grundsätzliche Problemstellungen unterscheiden:

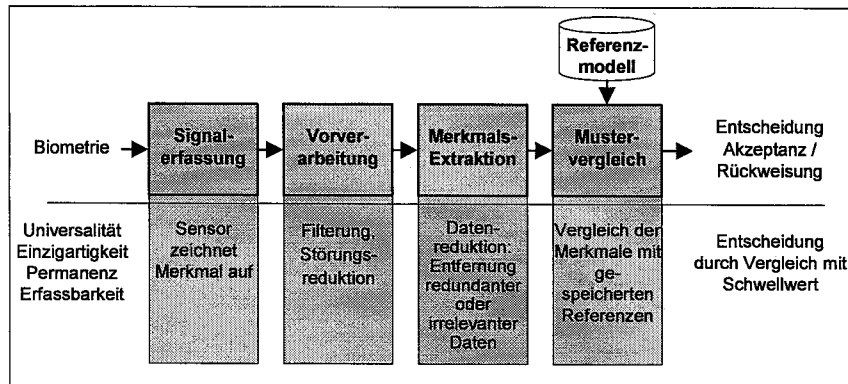
- Verifikation: Bei der Verifikation gibt der Benutzer eine behauptete Identität vor (z.B. indem er einen Namen eingibt oder eine persönliche SmartCard einschiebt). Das

System hat nun zu entscheiden, ob die behauptete Identität zutrifft oder nicht (Ja / Nein - Entscheidung).

- Identifikation: Bei der Identifikation ist die Identität des Benutzers unbekannt und soll vom System festgestellt werden: Dazu müssen die aktuellen biometrischen Daten mit den im Vorfeld erfassten Daten aller in Frage kommenden Personen verglichen werden. Der Benutzer wird als diejenige Person identifiziert, deren Daten am besten mit seinen aktuellen Daten übereinstimmen (1 aus N - Entscheidung).

Ablauf biometrischer Authentifikation:

Prinzipiell ist eine biometrische Authentifikation eine Mustererkennungsaufgabe. Der Aufbau und die Funktionsweise ist bei allen biometrischen Systemen gleich und entspricht dem anderer Mustererkennungssysteme: Die von einem entsprechenden Sensor (Kamera, Mikrofon, Fingerdrucksensor etc.) aufgezeichneten Signale werden zunächst vorverarbeitet, d.h. von Störungen befreit und in der Qualität verbessert. Anschließend werden z.B. durch geeignete Filterung und Transformation Merkmale extrahiert, die es erlauben, verschiedene Personen möglichst gut voneinander zu diskriminieren (hohe Inter-Klassen-Variabilität, geringe Intra-Klassen-Variabilität). Dabei findet eine Datenreduktion statt, d.h. redundante oder irrelevante Daten werden möglichst eliminiert. Die so extrahierten Merkmale werden mit Daten eines Referenzmodells (Referenztemplates) der jeweiligen Person verglichen um auf Basis eines festzulegenden Schwellwertes über Akzeptanz oder Rückweisung dieses Nutzers zu entscheiden.



Um eine neue Person im System zu registrieren, muss für diese ein neues Referenzmodell

angelegt werden (sog. Enrollment). Dies geschieht normalerweise durch Abspeicherung der extrahierten Merkmale zusammen mit der korrespondierenden Personen-Identität.

Wenn aber die Interoperabilität mit den (in der Regel proprietären) Algorithmen verschiedener Hersteller zu gewährleisten ist (wie z.B. bei elektronischen Reisepässen), dann wird während des Enrollments kein eigentliches Referenzmodell erzeugt, sondern es werden direkt die Rohdaten des Sensors abgespeichert (also z.B. ein Bild des Fingerabdruckes). Das zum Mustervergleich benötigte Referenztemplate wird in diesem Fall erst während der Erkennung auf Basis des jeweiligen Algorithmus errechnet. Die Speicherung der Enrollment-Daten kann entweder zentral (in einer Datenbank) oder eine dezentral (z.B. auf einer persönlichen SmartCard) erfolgen.

Die Rohdaten des Sensors können Anteile enthalten, die nicht für die biometrische Authentifikation notwendig sind, jedoch anderweitige Rückschlüsse über eine Person erlauben (sog. überschießende Informationen). Aufgrund der Datenreduktion und Merkmalsextraktion werden diese überschießenden Informationen immer weiter reduziert, sodass aus dem Referenzmodell praktisch keine Rückschlüsse auf die zugehörige Person mehr möglich sind.

Kenngößen und Fehlerquoten:

Bedingt durch eine geringe Variabilität der biometrischen Merkmale selbst, Variationen bei ihrer Präsentation sowie Unzulänglichkeiten in der Verarbeitungskette wird es nie zu einer 100% Übereinstimmung zwischen Referenzmodell und den aktuellen Merkmalen kommen. Eine Entscheidung über Ablehnung oder Akzeptanz eines Nutzers ist daher mit einer gewissen Unsicherheit behaftet, welche sich in den beiden wichtigsten statistischen Kenngrößen biometrischer Systeme widerspiegelt – der Falschakzeptanzrate (FAR) und der Falschrückweisungsrate (FRR). Die Falschrückweisungsrate drückt den Anteil fälschlich zurückgewiesener Berechtigter aus, während die Falschakzeptanzrate den Anteil fälschlich zugelassener Unberechtigter darstellt. Das Verringern einer der beiden Fehlerraten durch Variation des Entscheidungsschwellwertes bewirkt grundsätzlich eine Erhöhung der jeweils anderen Fehlerrate.

5.2. Rechtliche Aspekte biometrischer Daten

Biometrische Daten ermöglichen die Verifikation/Identifikation von Personen. Damit stellen biometrische Daten sog. „personenbezogene Daten“ iSd Datenschutzgesetzes 2000 (DSG)