



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 – 503 19 63 – 0
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 – 873 5514
Fax: ++43 316 – 873 5520

LEITFADEN BIOMETRIE – ÜBERBLICK UND STAND DER TECHNIK (AKTUALISIERTE VERSION, JÄNNER 2004)

Dipl.-Ing. Herbert Leitold – A-SIT • eMail: Herbert.Leitold@a-sit.at
Prof. Dr. Reinhard Posch – CIO Austria • eMail: Reinhard.Posch@cio.gv.at

Überblick: Der Einsatz von Biometrie als Ergänzung oder Ersatz herkömmlicher Methoden der Informationssicherheit ist zunehmend in öffentlicher Diskussion. Dabei betrachtete Aspekte sind vielschichtig, sie umfassen Elemente des Datenschutzes, vermeintliche oder tatsächliche Verbesserung von Sicherheitsmaßnahmen, bis hin zu gesteigertem Komfort des Benutzers. Die Diskussion ist nicht zuletzt auch deshalb kontrovers, weil der Stand der Technik teils überschätzt, dementsprechend mögliche Anwendungsgebiete der Biometrie oft falsch interpretiert und bewertet werden.

In diesem Beitrag wird vom Stand der Technik ausgehend Biometrie diskutiert, um eine Basis einer Strategie des Biometrieinsatzes in Österreich zu bilden. Es wird auf allgemein verständliche Darstellung Wert gelegt, weshalb technische Terminologie weitgehend vermieden wird. Es wird erst ein Überblick über Biometrie gegeben. Es werden Verfahren charakterisiert und kurz diskutiert. Leistungscharakteristika biometrischer Verfahren werden vorgestellt. Darauf aufbauend skizziert der Bericht die Anwendungsgebiete der Biometrie, wobei automatisierte Anwendungen in Informationssystemen von primärem Interesse sind. Entsprechend des Stands der Technik werden Kernaussagen für eine Strategie des Biometrieinsatzes in Österreich entwickelt.

Es handelt sich bei diesem Bericht um eine Aktualisierung des Leitfadens Biometrie vom Februar 2002, in den unter anderem jüngst veröffentlichte Ergebnisse von Studien (NIST report, BSI BioFace) eingearbeitet sind.

Inhalte

Inhalte	1
Glossar	2
Einleitung	3
Überblick Biometrie	3
Biometrische Merkmale	4
Verifikation vs. Identifikation	5
Leistungscharakteristika	5
Vorteile und Nachteile	8
Komfort	8
Vielfalt des Merkmals, Skalierbarkeit	8
Aufnahme und Verwahrung der Templates und Referenzdaten	9
Weitergabe des Merkmals	10
Unbewusste Abgabe des Merkmals	10
Lebenderkennung	10
Häufige Verfahren	11
Gesichtserkennung	11
Iris-Scan	11
Fingerabdruck	12
Anwendungsfälle	12
Ersatz von Wissen	13
Multifaktor-Authentifikation	13
Sicherung von Identifikationsdokumenten	13
Bereiche hohen Sicherheitsbedarfs	14
Kritische Zusammenfassung	14
Strategiesummary	15

Glossar

Im Folgenden werden zum besseren Verständnis einige Begriffe im Zusammenhang mit Biometrie, die im Verlauf des Dokuments mehrfach verwendet wurden, zusammengefasst.

Biometrische Daten:	Physiologische oder verhaltenstypische Merkmale einer Person, die über genetische Prozesse (z.B. DNA, Aussehen), Zufallsprozesse (z.B. Fingerabdruck, Iris) oder konditioniert (z.B. Sprache, Schriftzug) entstehen.
FAR,FRR, FER/FTE	Qualitätsmerkmale biometrischer Systeme: FAR False Accept Rate – Eine falsche Person wird fälschlicherweise akzeptiert (vgl. Look-Alike Fraud) FRR False Rejection Rate – Die richtige Person wird fälschlicherweise zurückgewiesen. FTE Failure to Enroll – Die Referenzdaten können nicht aufgenommen werden, da die Qualität zu gering ist (z.B. schlecht ausgeprägte Papillarlinien der Finger).
Look-Alike Fraud	Vor allem bei Personaldokumenten die Täuschung über Weitergabe des Dokuments an ähnlich aussehende Personen.
Identifikation (1:n)	Über das Merkmal wird die Person aus einer Menge identifiziert – 1:n Vergleich. Dies bedarf Datenbanken der Merkmale (bzw. Templates) mit der Bindung der Merkmale an die Person.
Referenzdaten:	Aus der Ersterfassung als Abbild (Rohdaten) oder als Template gespeicherte biometrische Daten, wie ein Abbild des Fingerabdrucks oder ein Videobild der Regenbogenhaut.
Rohdaten	Bild des biometrischen Merkmals, etwa ein Foto des Gesichts oder das Bild eines eingelesenen Fingerabdrucks.
Template	Strukturierte Reduzierung der Rohdaten, in der Charakteristika der Rohdaten extrahiert werden, etwa Minutien des Fingerabdrucks oder Lage charakteristischer Punkte des Gesichts.
Verifikation (1:1)	Vergleich mit lokal gespeicherten Verifikationsdaten (z.B. auf Chipkarte) – 1:1 Vergleich zwischen Verifikationsdaten und Referenzdaten.
Verifikationsdaten:	Die zum Vergleich mit den gespeicherten Referenzdaten abgegebenen Merkmale.

Einleitung

Die Verwendung biometrischer Merkmale zur Identifikation der natürlichen Person ist seit langem etabliert. Beispiele aus der erkennungsdienstlichen Praxis sind die Daktyloskopie¹ oder in jüngster Vergangenheit der DNS-Vergleich. Es sind aber nicht zuletzt auch die Photographie in Ausweisdokumenten, der Handschriftvergleich, das Erkennen einer Stimme oder die Analyse der spezifischen Ausdrucksweise zur Bestimmung der Autorschaft eines Schriftstücks oder Kunstwerks Anwendung mehr oder weniger eindeutiger Merkmale der natürlichen Person. Diese Beispiele zeigen bereits die Vielschichtigkeit biometrischer Verfahren, wie sie auch unterschiedliche Qualitäten hinsichtlich des Grades der Erkennung der Person oder der Resistenz gegenüber bewusster Überwindung und Fälschung vermuten lassen.

Die aus dem erkennungsdienstlichen Bereich bekannte Eindeutigkeit gewisser biometrischer Merkmale² zusammen mit steigenden Anforderungen an die Sicherheit in der Informations- und Kommunikationstechnologie (IKT) haben verschiedene Anwendungen der Biometrie entstehen lassen, die auch die breite Öffentlichkeit betreffen, was vor allem die öffentliche Diskussion zu Biometrie anregt. Prominente Beispiele dazu sind die Erweiterung von Ausweisdokumenten um elektronisch gespeicherte biometrische Merkmale³, Personenkontrollen in Flughäfen⁴, die Zugangskontrolle zu Gebäuden, aber auch Systeme zur Komfortsteigerung wie das Ersetzen von Benutzernamen/Passwort für das Computer-Login.

In diesem Beitrag wird die Biometrie in der Informationstechnologie diskutiert und bewertet. Dabei beschränkt sich der Beitrag auf jene Bereiche, in denen Biometrie zur Authentifikation oder Identifikation in computerunterstützten Anwendungen eingesetzt wird. Derartige computerunterstützte Anwendungen aus dem erkennungsdienstlichen Bereich werden nur für qualitativen Vergleich herangezogen (etwa AFIS⁵ Systeme oder DNS-Chips⁶).

Der Beitrag gibt zuerst einen Überblick über Biometrie und deren Leistungscharakteristika. Generelle Vorteile und Nachteile der Anwendung biometrischer Verfahren werden diskutiert. Die wichtigsten Verfahren werden kurz vorgestellt, um damit typische Anwendungsfälle zu diskutieren. In einer kritischen Zusammenfassung werden Kernaussagen entwickelt, die grundsätzliche Überlegungen zu einer Biometrie-Strategie darstellen.

Überblick Biometrie

In diesem Abschnitt wird ein kurzer allgemeiner Überblick über biometrische Merkmale und Verfahren gegeben. Es wird dabei in Anlehnung an die in diesem Umfeld üblicherweise verwendete Terminologie eine Unterteilung in „Verifikation“ und „Identifikation“ getroffen. Die wesentlichsten Leistungsmerkmale, nach denen biometrische Verfahren bewertet werden, werden erläutert.

¹ Fingerabdruckverfahren

² etwa Fingerabdrücke

³ vgl. USA: enhanced border security and visa entry reform act H.R. 3525;
vgl. Deutschland: Terrorismusbekämpfungsgesetz

⁴ vgl. Iris-Scanner für Vielflieger in Amsterdam/Schiphol oder Projekt EyeTicket in London Heathrow zur Beschleunigung des Einreiseprozesses

⁵ Automatisches Fingerabdruck Identifikations-System

⁶ Probenträger, die DNS-Proben zur weiteren Analyse aufbereiten

Biometrische Merkmale

Biometrische Verfahren beruhen darauf, dass aus einem Merkmal der natürlichen Person ein Datenmuster abgeleitet wird, das gegen ein Referenzmuster verglichen wird. Dabei lassen sich die Merkmale grundsätzlich in drei Kategorien „konditioniert“, „vererbt“ und „zufällig“ einteilen, aus denen sich in gewissen Grenzen bereits Eigenschaften des Merkmals hinsichtlich der technischen Anwendung ableiten lassen:

- Konditionierte Merkmale: Im Verlauf des Lebens angeeignete Merkmale sind beispielsweise die Handschrift, Rhythmus und Dynamik von Tastaturanschlägen oder Schrift, teils das Aussehen bzw. die Körperform⁷. Es ergibt sich als eine wesentliche Eigenschaft, dass das Merkmal in dem Maße, als es durch eine Person konditioniert ist, durch eine andere erlernbar ist und somit ein Angreifer in der Verkörperung der darzustellenden Person nicht auf die Präsentation eines Duplikates des Merkmals, etwa über Prothesen, angewiesen ist.
- Vererbte Merkmale: Genetisch bedingte Merkmale sind neben der DNS selbst etwa das Gesicht und Körperdimensionen (soweit nicht konditioniert) oder die Handgeometrie. Es ergeben sich entsprechend stark ausgeprägte Ähnlichkeiten innerhalb der Verwandtschaftsverhältnisse oder durch humangenetische Ähnlichkeiten in Regionen. Diese Ähnlichkeiten können die Qualität des Merkmals in Anwendungen einschränken, in denen „Look-Alike Fraud“ als problematisch anzusehen ist, etwa im Bereich der Reisedokumente.
- Zufällige Merkmale: Dies sind Merkmale, die sich in der Entwicklung eines Menschen zufällig ausbilden, etwa Venenmuster wie die der Retina, die Rissbildung der Regenbogenhaut (Iris) oder die Minutien der Fingerabdrücke. Diese Merkmale weisen, insofern entsprechende Vielfalt der Merkmale gegeben ist, hohe Unterscheidbarkeit von Individuen auf. Eine Nachahmung des Merkmals durch Angreifer ist nicht durch Erlernen oder gezielte Suche in einem Personenkreis mit potentiell ähnlichen Merkmalen möglich, sondern bedarf im Allgemeinen der Erstellung eines Replikates, etwa einer Prothese.

Allgemein führen zufällige oder ererbte Merkmale meist zu statischen Verfahren in dem Sinn, als der Anwender zum Zeitpunkt der Erfassung neben der Präsentation des Merkmals keine dynamische Handlung ausführen muss. Um die Präsentation eines Replikats des Merkmals zu verhindern, ist eine weitere Aktivität notwendig, wie etwa eine Lebenderkennung. Konditionierte Merkmale sind oft dynamisch, etwa Schriftodynamik oder Lippenbewegung, jedoch mit oben erwähntem Problem der Erlernbarkeit behaftet.

Ohne den Anspruch auf Vollständigkeit zu erheben, wird folgend eine Liste gegeben, die im Zuge biometrischer Verfahren verwendete Merkmale angibt:

- Fingerabdruck
- Gesichtsform
- Handgeometrie
- Handschriftodynamik
- Ohrenform
- Retina
- Rhythmus der Tastaturanschläge
- Sprachbild
- Unterschrift
- Venenmuster

⁷ neben vererbten Merkmalen auch konditionierte, wie sportliche Figur oder Übergewicht

Aus obiger Liste werden im Abschnitt „Häufige Verfahren“ jene charakterisiert, die entsprechend oft Anwendung finden und somit in Ausführungen zu einer Biometrie-Strategie zu erwähnen sind.

Verifikation vs. Identifikation

Biometrische Merkmale können grundsätzlich in Verfahren mit zwei Zielsetzungen „Verifikation“ und „Identifikation“ unterschieden werden, je nachdem ob ein vom Anwender präsentiertes Merkmal gegen ein Referenzmerkmal dieser Person verifiziert wird, (d.h. 1:1 Vergleich) oder ob diese Person über den Vergleich mit den Referenzmerkmalen eines bekannten Personenkreises identifiziert wird (d.h. 1:n Vergleich):

- Verifikation: Dies wird im Zuge der Authentifizierung, also des Nachweises einer behaupteten Identität, durchgeführt. Der Anwender hinterlegt Referenzdaten entweder in einer Komponente unter seiner Kontrolle (z.B. einer Chipkarte) oder unter einem Identifikator (der „behaupteten Identität“), sodass die Verifikation des Merkmals gegen die dem Identifikator zugeordneten Referenzdaten erfolgt. Beispiele für Verifikation sind der Ersatz einer PIN durch ein biometrisches Merkmal oder der Vergleich des Passphotos mit einem Videobild.
- Identifikation: Das Merkmal einer vorerst noch unbestimmten Person wird gegen eine Menge von Referenzdaten bekannter Personen verglichen, um die Person zu identifizieren. Ein Beispiel ist die Zugangskontrolle zu Gebäuden, bei der die Zugangsberechtigten den bekannten Personenkreis bilden. Der Prozess der Identifikation über biometrische Daten kann der Person bewusst sein, wie meist in der Zugangskontrolle, kann der Person auch nicht bewusst sein, etwa im Zuge der Fahndung.

Aus der Verwahrung der Referenzdaten lassen sich bereits grundsätzliche Unterschiede hinsichtlich des Datenschutzes identifizieren: In Identifikationssystemen ist eine zentrale Verwahrung von Referenzdaten erforderlich, etwa in einer Datenbank. In Verifikationssystemen können die Referenzdaten unter Kontrolle des Benutzers stehen, etwa in einer Chipkarte.

Leistungscharakteristika

Biometrische Verfahren sind nie exakt, es wird die Person immer nur mit einer gewissen Wahrscheinlichkeit bestimmt. Dies liegt einerseits daran, dass die Auflösung der erfassten Merkmale begrenzt ist⁸. Zum anderen liegt eine gewisse Unschärfe in den Merkmalen selbst, die in wiederholten Erfassungen nicht identisch abgebildet werden⁹.

Zur Leistungsbeschreibung biometrischer Systeme werden vornehmlich drei charakterisierende Werte herangezogen, die Fehlakzeptanzrate, die Fehlrückweisungsrate und die Fehlerfassungsrate:

⁸ die Beschränkung in der Erfassung kann sowohl durch die Sensoren technisch bedingt sein, aber auch durch geringe Vielfalt des biometrischen Merkmals etwa bei der Handgeometrie

⁹ kurzfristige Effekte können etwa Verschmutzungen, Verletzungen oder unterschiedliche Blickwinkel des Sensors sein, langfristige Effekte ergeben sich durch Wachstum und Alterung

- Fehlakzeptanzrate (FAR, False Acceptance Rate): Gibt die Häufigkeit an, mit der das System eine nicht berechnigte Person annimmt. Die FAR ist vor allem für das Maß der Authentifikations-Sicherheit verantwortlich.
- Fehlrückweisungsrate (FRR, False Rejection Rate): Gibt die Häufigkeit an, mit der autorisierte Personen vom System zurückgewiesen werden, eine berechnigte Person den Vorgang also wiederholen muss. Die FRR bestimmt vor allem die Praxistauglichkeit hinsichtlich des Komforts für den Benutzer, bzw. der Kosten für alternative Pfade, um die Person im Falle einer Rückweisung zu identifizieren.
- Fehlerfassungsrate (FER oder FTE, Failure to Enroll Rate): In biometrischen Systemen können von jenen Personen keine Referenzdaten erfasst werden, bei denen die physischen Merkmale nicht hinreichend ausgeprägt sind¹⁰. Die FER/FTR begrenzt den Kreis jener Personen, für die biometrische Verfahren nicht anwendbar sind.

Zur Veranschaulichung werden in Folge einige charakteristische Werte hinsichtlich obgenannter Kriterien zitiert¹¹. Der unter einigen vergleichbaren Studien hier exemplarisch ausgewählte Test wurde mit 200 Versuchspersonen durchgeführt und ergab für die FER, also die Rate an durch das System nicht erfassbaren Personen:

Tabelle 1: Fehlerfassungsrate aus [Biometric Product Testing Report]¹¹

System	FER in %
Gesichtserkennung	0.0 %
Fingerabdruck – Chip als Sensor	1.0 %
Fingerabdruck – Optischer Sensor	2.0 %
Handgeometrie	0.0 %
Iris	0.5 %
Venenmuster	0.0 %
Spracherkennung	0.0 %

Die Fehlakzeptanzrate FAR und die Fehlrückweisungsrate FRR sind voneinander abhängig. Es werden in folgender Tabelle typische Werte für FAR bei 3 % und 10 % FRR gegeben:

Tabelle 2: Fehlakzeptanz- und Fehlrückweisungsrate [Biometric Product Testing Report]¹¹

System	FAR bei 3% FRR	FAR bei 10% FRR
Gesichtserkennung	0.5 %	0,09 %
Fingerabdruck – Chip als Sensor	25 %	0,025 %
Fingerabdruck – Optischer Sensor	20 %	7 %
Handgeometrie	0,15 %	0,05 %
Iris	0,0001% (bei FRR=2 %)	
Venenmuster	30 %	6 %
Spracherkennung	1 %	0,015 %

¹⁰ etwa durch Gebrechen oder Abnutzungseffekte, wie schwach ausgeprägte Papillarlinien
¹¹ es werden hier die öffentlich verfügbaren Resultate eines Tests der britischen Communications-Electronics Security Group (CESG) „Biometric Product Testing – Final Report“ Issue 1.0, März 2001, CESG contract X92A/4009309, herangezogen.

Die Abhängigkeit zwischen FAR und FRR ergibt sich daraus, dass die Fehlakzeptanzrate FAR und die Fehlrückweisungsrate FRR gegenläufige Anforderungen darstellen: Stellt man die Toleranzen eines Systems beispielsweise zur Erhöhung der Qualität der Authentifikation eng, um damit also die FAR zu reduzieren, wird die Fehlrückweisungsrate steigen.

Zu beachten ist, dass die in Tabelle 2 verwendete Größenordnung der Fehlerraten FRR bereits als wenig praxistauglich zu bewerten ist. Eine Rückweisung des legitimen Anwenders in einem von zehn Versuchen (d.h. 10 % FRR) ist im Allgemeinen nicht, die Rückweisung in 3 % der Fälle ja nach Anwendung kaum zumutbar.

Studien jüngerer Datums geben einen aktuelleren Stand der Technik und haben durch Tests in größeren Gruppen größere statistische Aussagekraft. Es spricht etwa der ein Report des NIST¹² bei einer Testbestand von 6000 Fingerabdrücken und Aufnahme eines Fingers von einer Verifikationsleistung von 90 % bei 1 % FAR, bei der Gesichtserkennung unter 3000 Probanden von ebenfalls 90 % Verifikationsleistung bei 1 % FAR. In letzterem Fall der Gesichtserkennung wurden diese Werte jedoch nur unter Optimalbedingungen erzielt, bei Aufnahmen im Freien sank die Erkennungsleistung des besten Systems auf 43 %.

Zu ähnlich ernüchternden Ergebnissen für die Gesichtserkennung kam die aktuellere Studie BioFace¹³ des BSI, in der von Fehlrückweisungsrate von 64 % und schlechter, bzw. von Erkennungsleistungen in der Größenordnung von 50 % gesprochen wird.

Um obige Werte in Relation zu Sicherheitsanforderungen einer Anwendung zu stellen, lassen sich technologieneutral zulässige Werte der Fehlerraten in Sicherheitsstufen klassifizieren. Eine Studie zusammenfassend¹⁴ gibt die folgende Tabelle 3 eine derartige Einteilung in die Zuverlässigkeit der Erfassung:

Tabelle 3: Klassifizierung der Zuverlässigkeit der Erfassung [Zertifizierung biometrischer Systems]¹²

Zuverlässigkeit der Erfassung	FAR in %	FRR in %
Schwach	5 % und mehr	7 % und mehr
Mittel	1 % bis 5 %	3 % bis 7 %
Stark	0.3 % bis 1 %	1 % bis 3 %
Sehr stark	0.3 % und weniger	1 % und weniger

Als ähnliche Klassifizierung der Anforderungen an Systeme der Informationssicherheit, können die Gemeinsamen Kriterien¹⁵ (Common Criteria) als international abgestimmter Standard herangezogen werden. Dieser Standard für die Evaluierung und Zertifizierung von Produkten legt für die Funktionsstärke (Strength of Function SOF) für die Verifikation folgende Höchstwerte für die Fehlakzeptanzrate FAR biometrischer Produkte fest¹⁶:

¹² National Institute of Standards and Technology (NIST), „Summary of NIST standard for biometric accuracy, tamper resistance, and interoperability“, November 13, 2002.

¹³ Bundesamt für Sicherheit in der Informationstechnologie (BSI) „BioFace – Vergleichende Untersuchung von Gesichtserkennungssystemen“, öffentlicher Abschlußbericht, Juni 2003.

¹⁴ zitiert aus BSI „Zertifizierung biometrischer Systeme“ Vortrag von Axel Munde zu den Studien BioS und BioKrit bei BSI Symposium Darmstadt, 23.5.2002.

¹⁵ Common Criteria, auch ISO/IEC 15408.

¹⁶ Common Criteria, Common Methodology for Information Technology Security Evaluation, Biometric Evaluation Methodology Supplement, Version 1.0, August 2002.

Tabelle 4: Maximale Fehlakzeptanzraten aus [Biometric Evaluation Methodology]¹⁴

Funktionsstärke	FAR in %
SOF Niedrig	1 %
SOF Mittel	0.01 %
SOF Hoch	0.0001 %

Zu derzeitigem Stand der Technik ist davon auszugehen, dass mit biometrischen Systemen eine Funktionsstärke „SOF Hoch“ nicht erreichbar ist und somit Schutz gegen Angreifer mit hohem Angriffspotential nicht gegeben ist. Nach diesen Überlegungen sind derzeit biometrische Systeme gegen mittleres Angriffspotential (SOF Mittel) oder gegen zufälliges Brechen bzw. Brechen durch Laien (SOF Niedrig) einsetzbar.

Vorteile und Nachteile

In diesem Abschnitt werden grundsätzliche Vorteile und Nachteile biometrischer Verfahren zusammengefasst, um in einem Entscheidungsprozess des Einsatzes von Biometrie Anhaltspunkte zu geben.

Komfort

Für den Benutzer stellt sich mit biometrischen Systemen im Vergleich zu Passwörtern oder PINs der Komfort als einen wesentlichen Vorteil dar – biometrische Merkmale können nicht vergessen werden, sofern sie als konditioniertes Merkmal nicht die Eigenschaft einer Passphrase entwickeln¹⁷. Es können sich für den Betreiber eines Systems gleichzeitig Kosteneinsparungen dann ergeben, wenn sich der in manchen Fällen aus Passwort-Problemen resultierende Help-Desk Aufwand reduziert.

Es ist hier jedoch zu beachten, dass signifikante Fehlrückweisungsrate FRR einen alternativen Authentifizierungsmechanismus als Fall-Back Variante erfordern können¹⁸, der dann etwa wieder über PIN oder Passwort laufen kann. In diesem Fall relativiert sich sowohl der Komfort für den Benutzer, als auch die Kostenreduktion, da PIN oder Passwort des alternativen Mechanismus entsprechend weniger verwendet werden, deshalb potentiell eher vergessen werden.

Vielfalt des Merkmals, Skalierbarkeit

Ein Problem biometrischer Verfahren, insbesondere solcher der Identifikation, ist, dass die Verfahren gut skalieren müssen, wenn sie für große Personengruppen verwendet werden sollen, etwa im nationalen Maßstab. Dies erfordert einerseits biometrische Merkmale, die in entsprechend großer Vielfalt auftreten, um die Personen eindeutig zu identifizieren, sowie Sensoren, die diese Merkmale in ausreichender Auflösung erfassen. Mit Verweis auf Tabelle 4 ist zu beachten, dass deren Werte sich auf die Verifikation (den 1:1 Vergleich) beziehen. Für die Identifikation (1:n Vergleich) muss für steigende Zahl der Benutzer die Qualität der

¹⁷ Beispiele biometrischer Merkmale mit Passphrasen-Eigenschaft sind der Schriftzug oder die Spracherkennung.

¹⁸ vgl. Tabelle 2, wo in der Studie akzeptable Fehlakzeptanzraten teilweise nur mit nicht praxistauglichen Fehlrückweisungsrate von 10 % erreicht wurden.

Systeme entsprechend steigen, um eine äquivalente Funktionsstärke zu erreichen. Die Aussage, dass die Funktionsstärke „SOF Hoch“ mit derzeitigem Stand der Technik nicht erreichbar ist, gilt also umso mehr für die Identifikation¹⁹.

Zu jenen aktuellen Studien, die sich auf größere Grundmengen beziehen, zählen der NIST Report²⁰, FRVT²¹ und BioFace²². Der NIST Report weist für die besten getesteten Systeme bei einer Datenbasis von 10.000 Probanden eine Identifikationsleistung für den Fingerabdruck (ein Finger) von 90 % aus, 77 % bei der Gesichtserkennung bei guten Bedingungen. Für eine Datenmenge von 100.000 Testpersonen sinkt die ermittelte Identifikationsleistung nach diesem Report für das Fingerabdruckverfahren beispielsweise auf 86 %.

Weitere Feldversuche zu biometrischen Systemen sind oft auf einen relativ geringen Personenkreis beschränkt. Der Studie, auf die sich die Tabelle 1 und Tabelle 2 beziehen, liegt etwa ein Versuch mit 200 Teilnehmern zu Grunde. Es sind derartige Studien in vielen Fällen auch insofern nicht demographisch repräsentativ, als sie oftmals unter Laborbedingungen ausgeführt werden und in der Teilnahme von einem hohen Prozentsatz an Mitarbeitern der die Studie durchführenden Organisation gekennzeichnet sind, sich dann auch überproportional auf eine Bevölkerungsschicht beziehen²³.

Ein noch nicht hinreichend gelöstes Problem ist jenes der langfristig anwendbaren Standards, die einen zukunftssicheren Einsatz von Biometrie erlauben. Merkmale werden teils in proprietären Formaten gespeichert, respektive ist die Speicherung der Referenzdaten nicht hinreichend für die weitere Verwendung bei technologischen Fortschritten ausgerichtet, etwa bei höher auflösenden Sensoren. Dies ist beispielsweise bei Ausweisdokumenten mit einer Lebensdauer von 10 Jahren zu berücksichtigen, um resistent gegenüber unterschiedlichen Generation an Systemen zu sein.

Aufnahme und Verwahrung der Templates und Referenzdaten

Ein wesentliches Problem biometrischer Systeme ist die sichere Verwahrung der Referenzdaten. Da das physische Merkmal der Person nicht wie eine PIN oder ein Passwort austauschbar ist, ist eine missbräuchliche Verwendung dieser Daten zu verhindern. Wiederum können konditionierte Merkmale eine Passphrase abbilden, die in gewissem Maße austauschbar ist²⁴.

Es gilt das Erfordernis der sicheren Verwahrung von erfassten Merkmalen sowohl für Verifikationssysteme, um die Referenzdaten eines Systems nicht als Basis der Überwindung eines anderen Systems verwenden zu können, als auch für die Identifikation. Bei letzteren ergeben sich durch die Notwendigkeit der zentralen Speicherung der Daten Bedenken

¹⁹ Anm.: Erkennungsdienstliche Systeme, etwa AFIS Systeme, sind hier nicht betrachtet. Diese zeichnen sich etwa im Vergleich zu handelsüblichen Sensoren durch eine deutlich bessere Erfassungsqualität der Merkmale und Referenzdaten aus

²⁰ National Institute of Standards and Technology (NIST), „Summary of NIST standard for biometric accuracy, tamper resistance, and interoperability“, November 13, 2002.

²¹ z.B. Facial Recognition Vendor Test FRVT des US Department of Defense DoD, Defense Advanced Research Project Agency DARPA und National Institute of Justice - im Jahr 2000 mit ca. 13.000 Bildern als Versuchsbasis und 2002 mit ca. 121.000 Bildern durchgeführt

²² Bundesamt für Sicherheit in der Informationstechnologie (BSI) „BioFace – Vergleichende Untersuchung von Gesichtserkennungssystemen“, öffentlicher Abschlußbericht, Juni 2003.

²³ etwa sind Abnützungen wie wenig ausgeprägte Papillarlinien, die zu hohen Fehlraten FER und FRR bei Fingerabdruck-Systemen führen, bei manueller Tätigkeit der Personen häufiger

²⁴ etwa bei Erkennung des Schriftzugs oder Spracherkennung

aus Sicht des Datenschutzes. In Verifikationssystemen ist dies dann in geringerem Maße gegeben, wenn die Referenzdaten unter Kontrolle des Benutzers gehalten werden, etwa in einer Chipkarte. In beiden Systemen kann jedoch die Erfassung des Merkmals ein für Angreifer verwendbares Template ergeben.

Weitergabe des Merkmals

Ein Vorteil biometrischer Systeme ist, dass das physische Merkmal einer Person nicht auf eine andere Person übertragbar ist²⁵. Die entsprechende Qualität des Systems vorausgesetzt, ist damit in automatisierten Systemen in stärkerem Maße davon auszugehen, dass die Person selbst sich gegenüber dem System authentifiziert, als etwa bei PIN- oder Passwort-Systemen. Dies schließt jedoch die bewusste oder unbewusste Weitergabe eines Abbilds des Merkmals (des Templates) nicht aus²⁶, über die eine Überwindung des Systems möglich sein kann.

Unbewusste Abgabe des Merkmals

Biometrische Merkmale werden oft unbewusst abgegeben, etwa für die Gesichtserkennung erforderliche Daten über Überwachungskameras, Fingerabdrücke werden an Objekten des Alltagsgebrauchs hinterlassen oder Sprachmuster sind über Aufnahmen zu gewinnen. Es sind also Abbilder biometrischer Merkmale nicht als geheime Daten anzusehen.

Die unbewusste Abgabe kann insbesondere auch bei Verifikations-Systemen gelten, bei der der unmittelbare Bezug zu unbewusst abgegebenen Merkmalen der Person oft nicht offensichtlich ist. Beispielsweise ist bei Verlust oder Diebstahl eines Chipkarten-Ausweises mit elektronisch gespeichertem Fingerabdruck davon auszugehen, dass sich auch die Fingerabdrücke des Besitzers am Plastikträger der Chipkarte befinden, die durch einen Angreifer abnehmbar sind.

Lebenderkennung

Statische biometrische Systeme, die einzig auf einem Abbild des physischen Merkmals beruhen und keine dynamische Aktion des Benutzers erfordern, sind im Allgemeinen über ein entsprechend gut erfasstes Abbild des Merkmals oder über ein Replikat (eine Prothese) überwindbar. So sind die Überwindung von Fingerabdrucksensoren über Silikon- oder Gelatinefinger in der Literatur gut dokumentiert²⁷.

Es bedarf der so genannten Lebenderkennung, also des Nachweises, dass eine natürliche Person das physische Merkmal am Sensor abgibt. Dies ist teils organisatorisch lösbar, etwa im Zuge der Grenzkontrolle durch die üblicherweise bei der Passkontrolle gegebene Anwesenheit eines Beamten. Technisch ist das Problem Lebenderkennung oft noch nicht hinreichend gelöst, es hängt hier auch vom biometrischen Verfahren ab, inwieweit eine technische Lösung mittelfristig überhaupt mit entsprechender Überwindungssicherheit erreichbar sein wird.

²⁵ sofern das Merkmal nicht konditioniert ist

²⁶ vgl. Lebenderkennung bzw. Unbewusste Abgabe des Merkmals

²⁷ T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, „Impact of Artificial Gummy Fingers on Fingerprint Systems“, Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

Häufige Verfahren

In diesem Abschnitt wird auf die drei häufigsten biometrischen Verfahren „Gesichtserkennung“, „Iris-Scan“ und „Fingerabdruck“ etwas näher eingegangen. Es werden Stärken und Schwächen nach dem derzeitigen Stand der Technik diskutiert.

Gesichtserkennung

Die Gesichtserkennung beruht auf der Erfassung markanter Punkte des menschlichen Gesichtes über Videoaufnahmen. Es werden die Systeme sowohl zur Identifikation eingesetzt – etwa in Flughäfen zur Lokalisation von Passagieren oder im Zuge der Fahndung über Überwachungskameras – als auch zur Verifikation, um etwa in der Grenzkontrolle eine Person mit dem Photo des vorgelegten Reisedokumentes zu vergleichen, um Look-Alike Fraud zu vermindern.

Die Vorteile der Gesichtserkennung liegen in der kontaktlosen Erfassung der Merkmale, die auch über größere Distanzen erfolgen kann. Problematisch ist die relativ geringe Vielfalt des Merkmals, das zudem auch vererbte Charakteristika aufweist. Studien zeigen auch unzureichende Resistenz gegen Look-Alike Fraud²⁸: Ähnlich wie die Fehlerraten FAR und FRR gegenläufige Anforderungen darstellen, neigen Systeme, die auf gute Verifikation der mit dem Ausweisdokument bezogenen Person ausgelegt sind, dazu, Look-Alikes nicht wahrzunehmen.

Die technische Lebenderkennung beschränkt sich bei der Gesichtserkennung etwa auf die Bewegung der Person. Die Verwendung von Photos oder Masken oder andere bewusste Veränderungen am Aussehen zur Umgehung von Identifikationssystemen sind dabei oft nicht erkennbar. Die Erhöhung der Vielfalt der Merkmale durch Übergang von zweidimensionaler Erfassung auf dreidimensionale Templates ist erst vereinzelt und prototypisch umgesetzt, sodass hier entsprechend aussagekräftige Studien und Ergebnisse fehlen.

Iris-Scan

Iris-Scan beruht auf der Analyse eines Bildes der Regenbogenhaut. Vornehmlich werden monochrome Videoaufnahmen herangezogen, seltener wird auch Farbinformation ausgewertet.

Die Vorteile liegen vor allem in der sehr hohen Vielfalt des Merkmals und in sehr geringen Fehlakzeptanzraten bei gleichzeitig relativ guten Fehlrückweisungsraten²⁹. Damit eignet sich Iris-Scan sowohl für die Verifikation, als auch die Identifikation. Es ist beispielsweise mit dem am Flughafen Amsterdam/Schiphol bestehenden System für Vielflieger eine Installation für einen breiten Anwenderkreis gegeben, konkrete Evaluierungsergebnisse sind jedoch nicht bekannt.

Die Lebenderkennung kann über den Pupillenreflex z.B. bei Beleuchtung mit Infrarotquellen während der Aufnahme erfolgen. Die Erkennung handelsüblicher kosmetischer Kontaktlinsen ist möglich, da diese periodische Strukturen enthalten.

²⁸ z.B. in TNO TPD „Biometrics in travel documents: Suitability of face recognition for look-alike detection“, Proceedings of European Conference for Issuing Authorities of Travelling Documents, Den Haag, Juni 2002

²⁹ vgl. Tabelle 2

Systematische Untersuchungen zu spezifisch für die Überwindung von Iris-Scan Systemen produzierten kosmetischen Kontaktlinsen sind jedoch nicht bekannt. Es ist nicht auszuschließen, dass derartige Angriffe über spezielle Kontaktlinsen eine Überwindung des Systems ermöglichen.

Nachteile sind die etwas komplizierte Erfassung, da der Abstand zwischen Auge und Kamera in relativ geringen Toleranzen zu halten ist, um ein gutes Bild zu erhalten. Weiters können medizinische Gründe wie temporär erweiterte Pupillen zu Fehlrückweisungen führen³⁰.

Fingerabdruck

Die Erfassung des Fingerabdrucks zählt zu den bekanntesten biometrischen Systemen. Hier sind jedoch computerunterstützte Verarbeitung in automatisierten Anwendungen von den erkennungsdienstlichen Anwendungen insofern abzugrenzen, als in letzteren die Erfassung in sehr hoher Qualität mit zumeist Abrollen aller Finger und der Erfassung des Fingerabdruckblattes durch Daktyloskopen erfolgt, gegebenenfalls eine automatische Analyse der Minutien daktyloskopisch kontrolliert bzw. nachbearbeitet wird. Die computerunterstützte Verarbeitung in Automatischen Fingerabdruck Identifikations-Systemen (AFIS) bezieht sich auf den Vergleich einer Tatortspur mit der aus der hochqualitativen Erfassung resultierenden Datenbank.

In Gegensatz zu AFIS Systemen sind Fingerabdrucksensoren in automatisierten Anwendungen durch weitaus geringere Auflösung gekennzeichnet und erreichen derzeit noch nicht die Qualität der Identifikation wie sie aus der erkennungsdienstlichen Praxis bekannt ist. Die derzeit mit kostengünstigen Sensoren erreichbaren Fehlerraten erlaubten Verifikationssysteme relativ guter Qualität. Identifikationssysteme, die auf einen großen Personenkreis abbilden, sind mit dem Stand der Technik als noch nicht möglich zu bewerten.

Ansätze zur Lebenderkennung über Temperaturmessung oder Sensoren zur Erkennung des Pulsschlags oder Blutflusses existieren, fundierte Analysen zu deren Resistenz gegen bewusste Überwindung sind jedoch nicht bekannt.

Als in der Praxis problematisch ist anzusehen, dass durch die auf Kontakt basierenden Sensoren Fehlrückweisungen durch Verschmutzung des Sensors auftreten können, wie auch Verletzungen oder Verschmutzungen an Händen und Fingern häufiger sind, als etwa an den Augen, sodass im breiten Einsatz mit Problemen mit Fehlrückweisungen zu rechnen ist.

Anwendungsfälle

Dieser Abschnitt beschreibt typische Anwendungsfälle der Biometrie, wie sie häufig diskutiert werden. Es wird dabei nicht auf einzelne Verfahren eingegangen, sondern die Umsetzbarkeit am Stand der Technik diskutiert. Dabei bezieht sich der Abschnitt auf die in den vorangegangenen Abschnitten gegebenen Aussagen.

³⁰ etwa durch Augentropfen

Ersatz von Wissen

Unter dem Komfort-Gedanken wird Biometrie oft als Ersatz von Wissen diskutiert, um etwa der Vielzahl von durch Benutzer zu haltenden PINs zu begegnen und das Vergessen selbiger zu verhindern. Vor dem Hintergrund der derzeit erreichbaren Funktionsstärke³¹ erscheint dies in Anwendungen geringen Sicherheitsbedarfs möglich. Ein Beispiel wäre das Aktivieren von Mobiltelefonen, wo eine Alternative bei Fehlrückweisungen über Personal Unlocking Keys (PUK) bekannt und etabliert ist.

Für Anwendungen mittleren bis hohen Sicherheitsbedarfs, etwa die Auslösung sicherer elektronischer Signaturen nach dem Signaturgesetz, ist der Stand der Technik als dazu noch nicht ausreichend ausgereift zu bewerten³². Es ist hier auch zu beachten, dass Wissen aktiv und bewusst abgegeben wird, etwa durch die Eingabe einer PIN. Biometrische Merkmale sind physische Eigenschaften der Person, die auch in bewusstlosem Zustand abnehmbar sind, die Person hier also trotz Lebenderkennung passiv sein kann.

Multifaktor-Authentifikation

Authentifikation lässt sich in drei Methoden klassifizieren, wie folgt:

- Besitz: Etwa ein der Person zugeordneter Token, wie eine Chipkarte
- Wissen: Die Kenntnis einer Information, wie einer PIN
- Eigenschaft: Etwa ein biometrisches Merkmal

Durch Kombination dieser Methoden, beispielsweise Besitz einer Smartcard und Kenntnis der PIN, wird die Qualität der Authentifikation verstärkt. Mit der Einbeziehung biometrischer Merkmale, also beispielsweise Besitz, Wissen und Eigenschaft zusammen, wird der Grad an Sicherheit erhöht. In gleichem Maße kann man mit Einbeziehung biometrischer Merkmale die Komplexität der anderen Elemente verringern, ohne einen Verlust des Sicherheitsniveaus zu erleiden. So kann etwa die Länge eines Passwortes verringert werden, um die Merkmalsbarkeit zu erhöhen. Dies erlaubt eine Steigerung des Komforts für den Benutzer auch in Anwendungen mittleren und hohen Sicherheitsbedarfs und stellt einen der vielversprechendsten Anwendungsgebiete der Biometrie dar.

Sicherung von Identifikationsdokumenten

Die Erweiterung von Identifikationsdokumenten um elektronisch gespeicherte biometrische Merkmale als zusätzliche Sicherheitsmerkmale ist nicht zuletzt durch den US enhanced border security and visa entry reform act H.R. 3525 oder das deutsche Terrorismusbekämpfungsgesetz in öffentlicher Diskussion. Es sind hier international abgestimmte Vorgehensweisen Voraussetzung. Derartige Abstimmungen finden etwa für Reisdokumente im Rahmen der ICAO³³ statt.

³¹ vgl. Abschnitt „Leistungscharakteristika“

³² z.B. legt auch die deutsche Signaturverordnung fest, dass biometrische Merkmale zusätzlich zu Besitz und Wissen verwendet werden können.

³³ International Civil Aviation Organization

Bereiche hohen Sicherheitsbedarfs

Für Bereiche hohen Sicherheitsbedarfs sind biometrische Verfahren als Ersatz anderer Methoden (Besitz und Wissen) mit derzeitigem Stand der Technik als nicht geeignet einzustufen. Es kann hier Biometrie nur als Ergänzung dienen, um den Komfort bei gleich bleibendem Sicherheitsniveau zu erhöhen. Insbesondere fehlen fundierte Erfahrungen hinsichtlich der Überwindungssicherheit gegenüber Angriffen mit hohem Angriffspotential.

Kritische Zusammenfassung

Biometrische Verfahren sind zunehmend in öffentlicher Diskussion. In diesem Dokument wurde ein Leitfaden entwickelt, der sich am Stand der Technik ausrichtet und der als eine Basis einer grundsätzlichen österreichischen Strategie zur Biometrie dienen soll. Aus den in diesem Dokument skizzierten Überlegungen werden in Folge Kernaussagen gegeben, die das Umfeld Biometrie kritisch zusammenfassen:

- **Erfassen und Halten biometrischer Daten zur Identifikation stellen ein Risiko dar, das auch die Wahrung des Datenschutzes gefährdet**
- **Automatisierte biometrische Systeme erreichen nicht die aus erkenntungsdienstlichen Anwendungen bekannte Qualität**
- **Lebenderkennung stellt eines der ungelösten Probleme dar, um biometrische Systeme gegenüber gezielten Angriffen überwindungssicher zu gestalten**
- **Begrenzte Feldversuche lassen nicht auf Skalierbarkeit auf große Personenmengen schließen, etwa im nationalen Maßstab**
- **Der Stand der Technik lässt ein Ersetzen herkömmlicher Sicherheitsmaßnahmen durch Biometrie nur in Anwendungen geringen Sicherheitsbedarfs zu**
- **Biometrie kann eine Erhöhung des Komforts unter Wahrung des Sicherheitsniveaus bieten, wenn sie herkömmliche Methoden sinnvoll ergänzt**

Strategiesummary

Aus den gegebenen Erläuterungen lassen sich die folgenden Aussagen einer Strategie des Biometrieinsatzes zusammenfassen.

- Eine hohe Funktionsstärke (SOF high) ist derzeit und in absehbarer Zukunft nicht erreichbar, daher ist vorerst nur limitierter Einsatz der Biometrie möglich
- Ein Standard für biometrische Merkmale, die eine dauerhafte (etwa 10-jährige) Sicherheit gewährleisten, ist nicht vorhanden, daher können zentrale Datenbanken nicht sinnvoll eingesetzt werden
- Die Identifikationsanwendung außerhalb der erkennungsdienstlichen Aufgaben ist noch nicht technologisch rechtfertigbar
- Anwendungen können im Bereich der Verifikation und der Komfortsteigerung einen wesentlichen Beitrag leisten. Verifikationsanwendungen mit biometrischen Daten unter Kontrolle des Inhabers und mit amtlicher Bestätigung (Signatur) zur breiten Anwendung sind derzeit möglich und können eingesetzt werden. Dies gilt auch für Anwendungen mit Identifikationszuordnung in beschränkten Gruppen (im Normalfall etwa bis zu 100 Personen)
- Anwendungen müssen zur Zeit in kontrollierter Umgebung ablaufen. Der Machtgeber für das Identifikationsobjekt (z.B. Computer, Daten, etc.) muss die Möglichkeit der Kontrolle des Verifikationsprozesses haben.
- Derzeit praktikable Anwendungen für Biometrie sind z.B.
 - Personendokumente mit biometrischen Daten auf dem Dokument, die durch die Behörde bestätigt (signiert) sind
 - Zuordnung von Chipkarten zu Personen (dies ist vom Willensakt der Auslösung einer Funktion zu trennen, da Wachzustand und Bewusstsein zur Zeit in biometrischen Systemen nicht mit vertretbarem Aufwand technisch kontrollierbar sind)
 - Zutrittskontrolle zu Anlagen und Räumen vor allem über Sekundärmechanismen (z.B. biometrisches Merkmal und Karte als Träger der Referenzdaten) oder in beschränkten Populationen.