Biometrische Identifikationssysteme

Beurteilung der Einsatzmöglichkeiten und der Vor- und Nachteile aus Sicht des Anwenders
Klarstellung zu hygienischen und/oder gesundheitlichen Bedenken

Biometrische Erkennungsmethoden haben einen enormen Aufschwung erlebt. Dazu beigetragen hat der zunehmende Einsatz bei der Zugangskontrolle, z.B. zu Programmen, Netzwerken oder zum Entsperren von mobilen Endgeräten. Stark ansteigend ist auch die Nachfrage bei der Zutrittssteuerung, nicht nur als Hochsicherheits-Lösung, vielmehr auch aus ergonomischen und Komfort-Gründen. Damit sollen die Schwachstellen anderer Identifikationsmethoden, wie vergessener oder ausgespähter PIN und verlorener, gestohlener bzw. beschädigter Ausweis eliminiert oder ergänzt werden.
Vorurteile gegen die Biometrie beruhen oft auf ungenügenden Informationen und überholten Vorbehalten. Denn die Biometrie hat sich in den letzten Jahren, mit zunehmender Akzeptanz, stets weiterentwickelt.
Diese Zusammenfassung stellt deshalb die Grundlagen der Biometrie dar, die Verfahren, die wichtigsten objektiven Messwerte sowie Fakten, die es gestatten, hygienische oder gesundheitliche Bedenken ausräumen zu können. Sie bietet eine allgemeine Beurteilung der Einsatzmöglichkeiten und der Vor- und Nachteile.

1. Personenerkennung bei der Zutrittssteuerung

Die automatisierte Personenerkennung basiert ganz allgemein und insbesondere bei der Zutrittssteuerung auf drei möglichen Konzepten: Der Prüfung des Wissens der Person (PIN-Code), des Besitzes der Person (Ausweis, Smartphone) und der Eigenschaften der Person (Biometrie). Biometrische Erkennungsverfahren sind das einzig verbindliche Mittel, um nicht nur einen Ausweis, sondern direkt den Besitzer zu erkennen sowie den falschen Benutzer abzuweisen. So beschreibt auch die für die Zutrittsteuerung gültige Norm DIN EN 60839-11 Anforderungen an Biometrie beim Einsatz an Sicherheitsgrad 4 Türen als zusätzliches Merkmal für die Personenerkennung. Der Markt befindet sich jedoch auf Anbieter- und Anwenderseite in einem gravierenden technischen und psychologischen Umschwung. Vorbehalte sind weitgehend entkräftet, Kosten nachhaltig gesunken. Ein weiterer Kostenrückgang ist zu erwarten.

2. Was ist Biometrie und wie funktioniert sie?

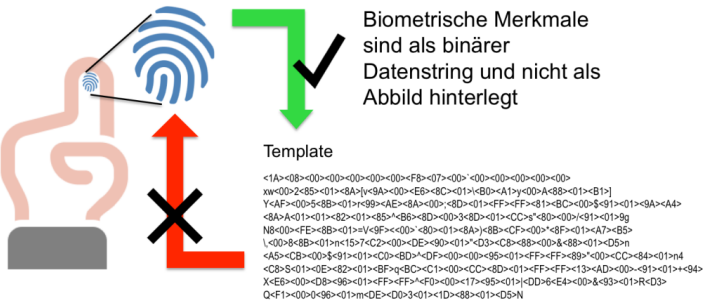
Biometrische Erkennungsverfahren, häufig kurz als Biometrie bezeichnet, sind Verfahren, die eine Person anhand physiologischer Charakteristika (z. B. Fingerabdruck, Gesicht, Muster der Iris, Handvene) oder Verhaltensweisen (z. B. Stimme, Bewegung, Unterschrift) automatisiert erkennen. Dazu wird der Teilbereich des menschlichen Körpers „vermessen“, der für das angewandte biometrische Verfahren benötigt wird. Bei der erstmaligen Benutzung, dem sogenannten Enrollment, werden die Kennwerte des Nutzers gespeichert - vergleichbar mit der Ausstellung eines Ausweises. Dieser Datensatz, das „Template“, enthält nur die für den Erkennungsalgorithmus benötigten Informationen, die aus den ursprünglich erfassten Rohdaten ermittelt wurden. Bei der weiteren Benutzung werden die aktuell aufgenommenen Messwerte mit diesem gespeicherten Datensatz verglichen, wie bei einer Passkontrolle.

Der gespeicherte Datensatz ist also meist keine Bild- oder Tondatei. Er enthält keine „Rohdaten“ wie ein Passbild, ein kriminalistischer Fingerabdruck oder eine Sprachaufnahme, sondern nur die daraus extrahierten Merkmale, z. B. eine mathematische Beschreibung der Endungen und Verzweigungen der Fingerabdrucklinien beim Fingerprint oder des Iris-Musters bei der Iris-Erkennung.

Die komprimierten biometrischen Daten werden entweder im Gerät selbst oder auf dem Ausweismedium des Benutzers vorgehalten. Im letzteren Fall werden nach Präsentation des Ausweises diese Daten vom biometrischen Leser eingelesen und mit den erkannten, physiologischen Merkmalen verglichen. Die Entkopplung der Daten vom Gerät und der Vorhaltung auf dem Ausweismedium bieten den Vorteil, dass lokal im biometrischen Leser keine personenbezogenen Daten vorgehalten werden müssen.

3. Welche zusätzlichen Informationen stecken hinter biometrischen Rohdaten?

Aus den Rohdaten lassen sich einige Rückschlüsse ziehen, insbesondere aus einem Bild des Gesichts, z. B. auf das Geschlecht, das ungefähre Alter oder die Hautfarbe einer Person. Aber auch aus dem Bild des Augenhintergrundes, der Retina, sind grundsätzlich Rückschlüsse auf Krankheiten wie Diabetes oder Bluthochdruck möglich. Welche Rückschlüsse noch möglich sind, ob sie automatisiert gezogen werden können und ob auch Templates diese „Zusatzinformationen" enthalten könnten, ist noch nicht hinreichend erforscht. Deshalb enthält das Template nur die für den Erkennungsalgorithmus benötigten Informationen, die aus den ursprünglich erfassten Rohdaten ermittelt wurden. Nach heutigem Wissensstand lässt sich aus diesen komprimierten Daten kein biometrisches Merkmal (z.B. Fingerabdruck) rekonstruieren. Solche Sekundär-Kriterien sind evtl. theoretisch denkbar, aber zweifellos nicht primäres Ziel beim Einsatz in der Zutrittssteuerung. Im Zweifelsfall ist die Nutzung der Sekundär-Kriterien im Rahmen einer Betriebsvereinbarung auszuschließen.



Eine Rekonstruktion der biometrischen Merkmale aus den Templates ist bei heutigen Verfahren nicht möglich!

4. Einzigartigkeit, Konstanz, Verbreitung

In der biometrischen Identifikation oder Verifikation werden einzigartige Merkmale einer Person über statische (physiologische) oder dynamische (verhaltensbedingte) Verfahren erfasst. Bei den statischen Verfahren sind heute Fingerabdruck, Venenerkennung, Iris und Gesicht zur Grundlage der Bemessung geworden, bei den dynamischen Verfahren (die kaum oder selten bei Zutritt zum Einsatz kommen) werden z.B. Unterschrift und Sprachmuster oder das Sprachfrequenzspektrum herangezogen. Die Erfassung erfolgt über entsprechende Sensoren.

Biologische Eigenschaften, die als biometrische Merkmale heranzuziehen sind, müssen die Attribute Einzigartigkeit, Konstanz, Verbreitung sowie schnelle und sichere Erfassbarkeit aufweisen. Die Einzigartigkeit ist bei einer hinreichend großen Varianz des Merkmals bei einzelnen Individuen gewährleistet. Die Konstanz legt eine möglichst geringe Änderung des Merkmals beim einzelnen Individuum im Laufe der Zeit zugrunde. Die Verbreitung schließt vorhandene und messbare oder abnehmbare Merkmale bei möglichst allen Nutzern ein. Für eine biometrische Erkennung müssen die drei genannten Attribute erfüllt sein. Natürlich soll sie auch schnell, sicher und mit vertretbarem Aufwand zu richtigen Ergebnissen führen. Von besonderer Bedeutung ist die Akzeptanz bei allen Anwendern.

5. Welche Arten biometrischer Erkennungsverfahren gibt es?

Aufgrund der Vielzahl verschiedener Arten biometrischer Merkmale sind unterschiedliche, teilweise sehr aufwändige Verfahren zur zuverlässigen Erkennung nötig. Häufig sind sie speicher- und rechenintensiv. Viele Verfahren hatten zunächst mit Akzeptanzproblemen zu kämpfen, da sie aus psychologischen (gedankliche Nähe zur Kriminalistik beim Fingerabdruck), hygienischen (Handgeometrie) oder gesundheitlichen Gründen (Retina/Iriserkennung) abgelehnt wurden. Ein Großteil dieser Bedenken konnte durch Untersuchungsergebnisse entkräftet werden.

Heute sind besonders die Erkennung des Fingerabdrucks, der Venen und des Gesichts beliebt. Zunehmende Akzeptanz ist seit einigen Jahren für die Fingerprinterkennung zu beobachten, die durch den Einsatz auch im neuen deutschen Reisepass und im neuen Personalausweis (s. BHE-Papier „Der neue Personalausweis als Ausweis für Zutrittsregelung") starken Auftrieb erhalten hat.

5.1 Fingerabdruck

Der Fingerprint war bisher das bekannteste und weitverbreitetste Identifikationsverfahren. Zur Personenerkennung genügt bei der 2D-Technik ein einfaches Auflegen des Fingers auf dem Sensor. Aus hygienischen Gründen, insbesondere zu Pandemie-Zeiten hat die Akzeptanz dieses Verfahrens erheblich abgenommen. Seit einigen Jahren werden aber auch Systeme angeboten, bei denen ein oder mehrere Finger per Kamera dreidimensional und berührungslos erfasst werden.

2D-Verfahren

Bei den meisten biometrischen Fingerabdruck-Verfahren extrahiert der Fingerabdruck-Algorithmus die Minutien aus dem durch den Sensor gewonnenen Bild. Die Minutien, die Kennpunkte des Fingerabdrucks, bestehen aus Endungen und Verzweigungen der Papillarlinien. Bedingt durch die heute verfügbare Speicherkapazität von RFID-Karten und der Möglichkeit, die Daten des Referenzmusters auf rund 256 Bytes zu komprimieren, kann das Template auch auf RFID-Ausweise abgespeichert werden. Der Fingerprint macht momentan rund 50 Prozent biometrischer Anwendungen aus. Dieser hohe Anteil rührt vor allem daher, dass dieses Verfahren schon seit Jahrzehnten vor allem in der Kriminalistik zum Einsatz kommt und - bedingt durch den geringen Platzbedarf des Sensors - auch in kleinen Eingabegeräten, wie Tastaturen und Smartphones integriert werden kann.

Im laufenden Betrieb kommt es immer wieder vor, dass bei bestimmten Personen der Fingerabdruck nicht erkannt wird. Die Gründe dafür sind vielfältig: Eine zu trockene Haut, Nässe bzw. Kälte sowie eine falsche Fingerpositionierung und Verschmutzungen an Haut oder Sensor. Schwach ausgeprägte Minutien beeinträchtigen die Leseergebnisse. Nicht nur in den Pandemie-Zeiten wird die kontaktbehaftete Nutzung unter Hygiene-Aspekten kritisch gesehen. Abhilfe zur besseren Akzeptanz schafft hier die regelmäßige Reinigung des Sensors mit einem feuchten (nicht nassen), nicht kratzenden Tuch. Geeignet sind Wattestäbchen, Mikrofaser- und Brillentücher.

3D-Verfahren für kontaktlose Fingerabdruckerfassung

Bei kontaktlosen Fingerabdrucksystemen ist zwischen folgenden Geräten zu unterscheiden:

- **Geräte die eine Fingerkuppe für das Template erfassen**

Kameras zeichnen ein Abbild der Fingerkuppe von Nagelansatz zu Nagelansatz auf. Hier wird der Fingerabdruck ohne Kontakt zum Sensor erfasst. Bei dieser 3D-Abbildung werden mehr charakteristische Punkte zur Personenerkennung erfasst als bei einem 2D Fingerabdruck.

Dies hat allerdings Auswirkung auf den Speicherbedarf für die biometrischen Merkmale, die nicht auf allen Chipkartentypen für eine Verifikation gespeichert werden können. Soweit nur ein Template gespeichert werden soll, ist der Einsatz von MIFARE DESFire Karten empfehlenswert.

- **Geräte die Abdrücke von mehreren Fingern für das Template aufnehmen**

Häufig werden kontaktlose Fingerprintsysteme angeboten, die Abdrücke von mehreren Fingern für das Template berücksichtigen, was die Genauigkeit erhöht und Fehler reduziert. Hierbei muss man lediglich seine Hand kontaktlos über einen Sensor streichen oder einer Kamera präsentieren.

Dabei werden 4 Finger in weniger als 1 Sek. gescannt und verifiziert. Ideal für Anwendungen mit einem hohen Durchsatz, weil die Identifizierung (lt. Hersteller) in weniger als einer Sekunde erfolgt.

5.2 Venenerkennung

Das menschliche Venenmuster im Handbereich ist komplex, weist viele Gefäße auf und ist für jedes Individuum einzigartig. Zu seiner Erkennung sendet eine Lichtquelle im Scanner Licht im nahen Infrarotbereich aus, wodurch der Verlauf der Venen durch die Lichtabsorption des Hämoglobins im Blut sichtbar wird. Eine in den Scanner integrierte Kamera nimmt das Venenmuster auf, das System extrahiert das bei jedem Menschen eindeutige Muster. Venen, die nicht direkt unter der Haut liegen und schwächer angezeigt werden, werden durch Algorithmen hochgerechnet.

Aus dem Verlauf der Venen und ihren Verzweigungen wird ein Template für die spätere Wiedererkennung erstellt. Dieses Referenzmuster wird beim Einlernen in eine Datenbank oder zur Verifikation auf einem RFID-Datenträger (Karte oder Transponder) abgespeichert.

Die Venenmustererkennung ist bei jedem Menschen anwendbar, da die Gefäßpositionen zeitlebens unverändert bleiben, und sie hat den Vorteil, dass sich die erforderlichen Informationen nicht wie Fingerabdrücke von jedem Gegenstand abnehmen und so potenziell fälschen lassen.
Kleinere Verletzungen der Finger oder Verschmutzungen der Hände bei Mitarbeitern stellen bei der Venenerkennung im Gegensatz etwa zur Erkennung per Fingerabdruck kein Hindernis dar. Da die Abtastung über Nah-Infrarot berührungslos erfolgt, ist die Verwendung im öffentlichen Bereich auch unter hygienischen Gesichtspunkten gut möglich.

Bei der Erkennung der Venenmuster sind folgende biometrische Systeme zu unterscheiden:

5.2.1 Finger-Venenerkennung

Zur Erkennung wird ein Finger in oder auf einen Sensor gehalten, der das Venenmuster des Fingers auswertet. Die Venen in einem Finger sind allerdings sehr kälteempfindlich, d.h. die Kapillar-Venen können sich bei Kälte komplett zusammenziehen und somit nicht mehr erkannt werden.

5.2.2 Handrücken-Venenerkennung

Der Handrücken wird an einen Sensor gehalten. Dabei können Pigmentflecken oder Haare zu Störungen des Erkennungsvorgangs führen. Dieses Verfahren ist allerdings nicht berührungslos, da der Handrücken und die Handinnenfläche das Erfassungssystem berühren.

5.2.3 Handflächen-Venenerkennung

Die Kamera des Handvenen-Sensors erstellt ein Bild des Venenmusters, das in einem zweiten Schritt in ein rund 0,8 kB großes Template umgewandelt wird. Die FAR (Falsch-Akzeptanz-Rate) liegt nach Anbieterangaben bei 0,00008%. Die Handflächen-Venenerkennung ist unempfindlich gegenüber Hautverunreinigungen, Hautfarbe, Haaren, Muttermalen oder oberflächlichen Verletzungen. Das Handvenenmuster verändert sich weder bei Wärme noch bei Kälte. Ein wichtiger Pluspunkt dieses biometrischen Verfahrens ist die Tatsache, dass die Erkennung völlig berührungslos erfolgt.

5.3 Iris- und Augenbereich-Erkennung

Die Iris, auch Regenbogenhaut genannt, ist die durch Pigmente gefärbte Blende des Auges. Sie reguliert den Lichteinfall in das Auge (Adaptation). In der Iris bilden sich kurz vor der Geburt typische individuelle Muster. Sie sind nach heutigem Wissensstand nicht genetisch bedingt, behalten aber ihre Ausprägung lebenslang. Diese Muster, nicht aber die Farbe, werden zur Erkennung herangezogen. Das Verfahren scheint eine strenge Grenze zwischen Akzeptanz und Rückweisung zu besitzen. Für die Ausleuchtung des Auges gilt das gleiche wie bei der Retinaerkennung, jedoch ist die Beleuchtungsstärke nochmals erheblich niedriger. Zur Zeit liegt der Anteil der Iris-Erkennung, bezogen auf alle biometrischen Verfahren, bei rund 8 Prozent. Da die Iris ein kleiner, sehr schwer zu erfassender Bereich ist und die Kameratechnik oft für die Erkennung – auch in größeren Entfernungen - nicht ausreichend ist (z.B. bei Smartphones) werden die Merkmale der gesamten Augenpartie erfasst. Durch Fortschritte bei modernen Merkmalsextraktions- und Abgleichalgorithmen sind mit der sogenannten periokulären Identifikation noch bessere Resultate möglich.

5.4 Augenhintergrund-Erkennung (Retina-Scan)

Für die Augenhintergrunderkennung (Retina- bzw. Netzhaut-Erkennung) gab es mehrere Systeme am Markt. Im Hinblick auf die relativ geringe Akzeptanz scheint die psychologische Hemmschwelle der Nutzer noch nicht ausgeräumt zu sein. Sie befürchten oftmals, dass zur Ausleuchtung des Auges ein Laserstrahl verwendet wird und verbinden das meist mit einer potenziellen Verletzungsgefahr für ihr Augenlicht. Nach Herstellerangaben trifft dies jedoch definitiv nicht zu. Die Augenhintergrund-Erkennung hat in der EU kaum Bedeutung, auch weil das Marktangebot an Systemen sehr klein ist.

5.5 Sprachmuster- und Sprechererkennung

Bei der Sprachmustererkennung gibt es widersprüchliche Aussagen über die praktischen Erfahrungen. Bei einigen Systemen wirken sich die Umgebungsgeräusche störend aus. Nötige Wiederholungen des Erkennungswortes stören wiederum den Benutzer. Bei umfassenden Neuentwicklungen ist die Spracherkennung im Verbund mit anderen biometrischen Erkennungsverfahren kombiniert. Diese Form der Biometrie ist vor allem beim Online-Banking und beim Online-Shopping weit verbreitet, bei der Zutrittssteuerung aber weniger gebräuchlich.

5.6 Gesichtserkennung (Face ID)

Die Gesichtserkennung nimmt im Alltag eine immer größere Rolle ein: z.B. für Einlasskontrollen am Flughafen oder zum Login beim PC oder Smartphone, statt PIN oder Passwort. Bei diesem Verfahren wird mittels 2D-, Infrarot- und/oder 3D-Kamera automatisch ein Gesichtsbild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen. Zwischen Benutzer und Gerät ist kein Kontakt nötig – ein nicht zu unterschätzender Vorzug.

Innerhalb der Gesichtserkennung ist zwischen der Muster- und der Geometrieerkennung zu unterscheiden. Im Falle des Geometrie-Verfahrens bilden beispielsweise die Abstände von Augen, Nase und Mund die Basis des Vergleichs. Zudem dienen mehrere unterschiedliche Algorithmen zur Gewinnung der individuellen Merkmale und zur Berechnung der Templates. Unterschieden wird zwischen 2D- und 3D-Erkennungsverfahren. Neue Verfahren erlauben eine 3-dimensionale Erkennung des Gesichts, die mehr Toleranz bei der Aufnahme und höhere Erkennungssicherheit bieten. Mittlerweile ist diese Technologie so weit entwickelt worden, dass sogar bei Dunkelheit, starker Sonneneinstrahlung oder bei reflektierendem Sonnenlicht eine Gesichtserkennung erfolgen kann. Mit einer Identifikationszeit von unter einer Sekunde kann ein hoher Personen-Durchsatz erreicht werden. Mittlerweile tolerieren solche Systeme auch Veränderungen des Gesichts z.B. durch Brille, Bart, Mütze oder Mundnasenschutz.

Aus Sicht des Datenschutzes wird diese Technologie aber auch ihrer Nutzer besonders kritisch gesehen. Ein sehr großes Problem ist hierbei der mögliche Identitätsmissbrauch durch das Erlangen der entsprechenden biometrischen Daten (Gesichtsbilder). Beispielsweise gibt es berechtigte Sorgen vor einem flächendeckenden Netz aus Überwachungskameras, die Personen identifizieren können und viele Datenbanken, z.B. in sozialen Netzen, sind mit Passbildern gefüllt, die eine schnelle Personenzuordnung ermöglichen. In keinem Fall dürfen die Risiken der Gesichtserkennung unterschätzt werden.

5.7 Kombination mehrerer biometrischer ID-Verfahren

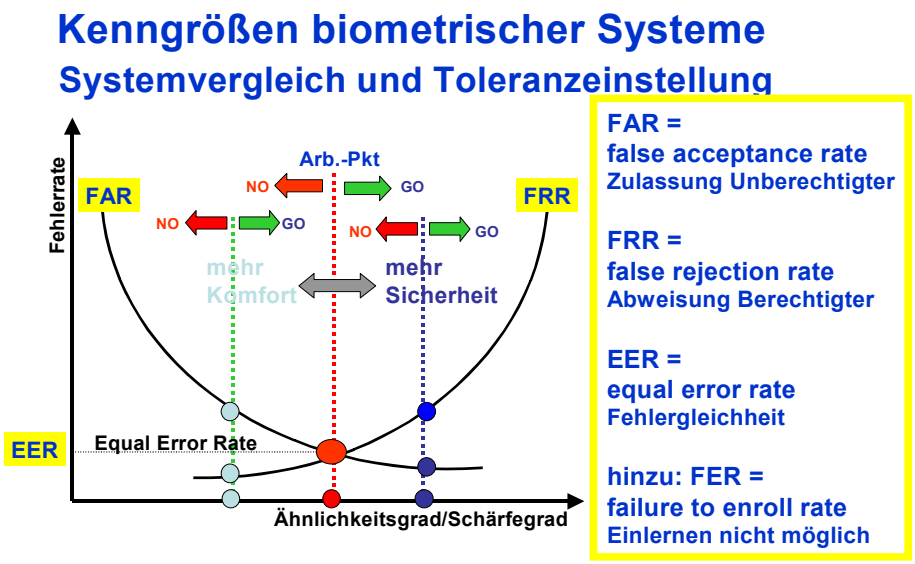
Einige biometrische Merkmale können sich durch Krankheit, Unfall, Alkoholgenuss, Stress, Müdigkeit oder Umwelteinflüsse verändern oder können sogar ganz ausfallen (z. B. Stimme). Deshalb haben alle biometrischen Systeme, die nur ein persönliches Merkmal erfassen und auswerten, ggf. Probleme mit der Erkennungsgenauigkeit. Zur Erhöhung der Sicherheit können mehrere biometrische Merkmale, wie Gesicht, Sprache und Lippenbewegung, kombiniert überprüft werden. Das System kann auch so programmiert werden, dass bei Ausfall einer Erkennungsart (z. B. durch Umwelteinflüsse wie starke Geräusche oder Licht) nur zwei erkannte Merkmale ausreichen. Wobei dann immer noch die Erkennungssicherheit höher sein kann als bei der Auswertung nur eines biometrischen Merkmals.

6. Objektive Messkriterien: FAR und FRR

Bei den biometrischen Verfahren wird die Sicherheit nach drei Kriterien beurteilt:

- nach der Rate der Zulassung Unberechtigter (FAR – false acceptance ratio)
- nach der Rate der Abweisung Berechtigter (FRR – false rejection ratio)
- nach der Rate der nicht einlernbaren Personen (FER – failure to enroll)

Im Fall des Kriteriums „Abweisung Berechtigter“ ist der Komfort bei der Benutzung des Systems beeinträchtigt, es entsteht jedoch kein Sicherheitsrisiko.
Beim Kriterium „Zulassung Unberechtigter“ wird durchaus die Sicherheit beeinflusst. In Hochsicherheitsbereichen ist deshalb die FAR zu Ungunsten der FRR so niedrig wie möglich eingestellt. In anderen Anwendungen, bei denen es primär auf eine hohe Durchlassrate oder schnellen Eintritt ankommt, ist die FRR möglichst niedrig gehalten. Dabei wird gerne notgedrungen eine etwas erhöhte FAR in Kauf genommen.



Die Genauigkeit dieser Abtastung ist entscheidend abhängig von der Wiederholgenauigkeit der Positionierung bei der Messwerterfassung. Bei biometrischen Verfahren soll die FAR möglichst kleiner/gleich 0.01% und FRR kleiner/gleich 1%, also besonders niedrig sein. Auch die neue ZK-Norm IEC 60839-11-1 nennt für FAR Werte zwischen 1% und 0,1% für die 4 Sicherheitsgrade der Zutrittssysteme.
Die FER gibt an, mit welchem Prozentsatz nicht einlernbarer Personen man bei diesem biometrischen Erkennungssystem rechnen muss. Liegt die Rate relativ hoch, ist nicht nur eine geeignete Fallback-Massnahme vorzusehen, man muss vielmehr im späteren Echtzeitbetrieb auch mit einer erhöhten FRR rechnen.

7. Nah am Ideal

Systemgebunden oder durch die vom Entwickler gewählten Algorithmen und Bewertungskoeffizienten ist bei einem spezifischen Biometriesystem der Wert EER (equal error rate - Gleichheit der Fehlerraten) definiert. Dieser Wert entspricht dem Schnittpunkt der beiden Kurven FAR und FRR. Je niedriger der Wert EER ist, umso besser unterscheidet das System zwischen Berechtigten und Nichtberechtigten. Mit der Einstellung des Arbeitspunktes, der entweder als Schärfegrad oder Toleranz des Systems (d.h. eine umgekehrte Darstellung von FAR und FRR) systemweit und meist zusätzlich auch noch individuell eingestellt werden kann, wird das System auf höhere Sicherheit oder auf höheren Komfort eingestellt. Das nur theoretisch erreichbare Idealsystem hätte einen EER = 0 und damit auch FAR = FRR = 0.

8. Fakten zu hygienischen oder gesundheitlichen Bedenken

Biometrische Systeme werden manchmal als unhygienisch eingeschätzt. Für die hauptsächlich eingesetzten Systeme gilt aus technisch-hygienischer Sicht:

8.1 Fingerabdruck und Handgeometrie

Bei beiden Verfahren berühren alle Teilnehmer einen Gegenstand. Zur Fingerabdruckerkennung wird ein Kunststoff- oder Glasträger mit dem Finger berührt. Seit einiger Zeit wird ein System angeboten, bei dem der Finger per Kamera dreidimensional und berührungslos erfasst wird. Bei der Handgeometrie ist die Hand auf eine Platte mit Führungsstiften zu legen. Diese Platte wird vom Hersteller neuerdings aseptisch produziert. Bei beiden Verfahren findet ein Kontakt mit i. d. R. einem einzigen Finger bzw. einer Handfläche statt, der weniger intensiv ist als die Berührung eines Türgriffs, Türknaufs oder einer Türstange und der im Allgemeinen als zumutbar empfunden wird.

8.2 Venenerkennung

Dieses Verfahren arbeitet optisch und ohne Berührung des Sensors, da die Hand in einigem Abstand vor den IR-Sensor gehalten wird.

8.3 Augenhintergrund- und Iris-Erkennung

Beide Verfahren arbeiten optisch und berührungsfrei.

8.4 Sprachmuster- und Sprechererkennung

Auch diese Verfahren arbeiten berührungsfrei, da ein Mikrofon/Schallaufnehmer besprochen wird.

8.5 Gesichtserkennung

Bei der Gesichtserkennung wird eine Kamera verwendet – ein berührungsfreies Verfahren.

9. Ist Biometrie gefährlich, z. B. wenn in meine Augen geleuchtet wird?

Bis auf die kaum eingesetzten Retina-Erkennungssysteme, bei denen der Augenhintergrund mit einer Lampe geringer Intensität beleuchtet wird, werden bei biometrischen Systemen mit Kameras höchstens allgemeine Beleuchtungsquellen wie Lampen oder LEDs eingesetzt, die die Iris oder das Gesicht erhellen.
Theoretisch kann es - wie bei jedem Gerät - zu Fehlfunktionen kommen; eine spezifische Gefahr gibt es nicht. Laser werden nach heutigem Wissensstand nicht zur Ausleuchtung biometrischer Merkmale eingesetzt. Die auf einigen Geräten genannte Einstufung in eine „Laserklasse" wird für alle Geräte mit optischer Ausleuchtung gefordert.

10. Ist Biometrie schnell genug für Zutrittssteuerung?

Bei biometrischen Systemen spielt die Erkennungszeit eine entscheidende Rolle. Da sie meist höher ist als die Buchungszeit, die mit einem herkömmlichen Ausweis erreicht wird, ist generell der verringerte Durchsatz pro Zutrittspunkt zu beachten. In jedem Fall darf die Erkennungszeit die Geduld der Buchenden nicht überstrapazieren, denn die Akzeptanz eines Systems ist wesentlich von der Benutzeranzahl und seinem Bedienungskomfort sowie von der zentralen (Datenbank) oder dezentralen Speicherung (auf Ausweis) des Templates abhängig. Moderne biometrische Systeme bieten Erkennungszeiten von unter einer Sekunde bis zu wenigen Sekunden.

11. Wachsende Zahl von Anwendungen

Biometrische Technologien werden immer häufiger eingesetzt, neben der Zutrittsteuerung zu Hochsicherheitsbereichen zunehmend auch zum Entsperren von mobilen Geräten, wie Smartphones und Tablets. Neben der Sicherheit spielt außerdem der Komfortaspekt eine große Rolle, denn Passwörter oder Ausweise können abhanden kommen. Die Biometrie ist dann anderen Identifikationsverfahren überlegen, wenn die Daten der Benutzer auf dem Gerät (Zutrittsleser, Smartphone, etc.) gespeichert werden und nicht über Netzwerke übertragen oder auf zentralen Servern gesammelt werden – zwei häufige Kritikpunkte an der biometrischen Authentifizierung.

Biometrie stellt je nach Einsatzbereich eine sinnvolle Ergänzung zu den auf Wissen und Besitz basierenden Verfahren dar. Die sichere Identifikation über ausschließlich biometrische Verfahren ist beim heutigen Stand der Technik auch mit größeren Teilnehmerzahlen möglich, beispielsweise mittels 3D-Gesichts-, Handvenen- und der Fingerprint-Erkennung. Abhängig von der Teilnehmerzahl und den Sicherheitsanforderungen werden biometrische Erkennungsverfahren zur Verifikation oder Identifikation genutzt. Die Vorselektion innerhalb der Verifikation erfolgt dabei über PIN-Code oder die Überprüfung einer Ausweiskarte durch ein Zutrittsterminal. Mit den zu erwartenden technischen Verbesserungen und vor allen Dingen den nachfolgenden Kostensenkungen sind biometrische Lösungen künftig auch für Anwendungen in alltäglichen Sicherungsbereichen möglich.

12. Zwei wiederkehrende Begriffe: Identifikation versus Verifikation

Die Identifikation prüft in einem so genannten „one-to-many-Vergleich" die Identität der betreffenden Person. Damit beantwortet sie die sicherheitsrelevante Frage „Wer bin ich?". Ein zusätzlicher Ausweis oder eine PIN sind nicht erforderlich.

Bei der Verifikation (Authentifikation) bestätigt das System über einen one-to-one-Vergleich die Identität des Nutzers. Die Frage: „Bin ich tatsächlich der Besitzer dieser Identität?" lässt sich auf diese Weise beantworten. Die zu prüfende Identität ist auf einem Ausweis oder durch eine PIN abgebildet, dessen Zugehörigkeit zu dem Ausweisinhaber ermittelt wird. Die in Europa bisher fast nur in Hochsicherheitsanlagen installierten biometrischen Erkennungsverfahren werden vor allem zur Verifikation eingesetzt. Selbst bei der in Nordamerika verbreiteten Sprechererkennung am Telefon in Homebanking-Anwendungen findet eine Verifikation statt, da die Vorselektion über die Nennung der Kontonummer erfolgt.

Nach heutigem Stand der Technik ist es sinnvoll, die biometrische Erkennung zur Verifikation und nicht ausschließlich

als Identifikation zu nutzen. Innerhalb der Zutrittssteuerung lässt sich so nicht nur die Unterscheidung der Berechtigten untereinander, sondern auch die sichere Abweisung der riesigen Zahl der Nichtberechtigten sicherstellen. Zu beachten ist, dass es bei der Identifikation ab einer Teilnehmergröße von ca. 500 Personen aufgrund der Anzahl der Vergleiche zu verlängerten Reaktionszeiten kommen kann. Die Identifikation ist somit zeitintensiver und birgt zudem eine Fehler-Multiplikation in sich, da die Fehlerraten pro Vergleich angegeben sind.

13. Ist der Einsatz von Biometrie in Betrieben zustimmungspflichtig?

Zustimmungspflichtig sind Anlagen und Verfahren, die es erlauben, automatisch bzw. maschinell Rückschlüsse auf die Leistung oder auf das Verhalten der Arbeitnehmer zu ziehen. Biometrie als solche lässt sicher keine Rückschlüsse zu, aber sie wird zur Erkennung der Teilnehmer z. B. einer Zutrittsanlage eingesetzt. Daher ist ihr Einsatz ebenfalls zustimmungspflichtig. Hierzu ist bei einer bereits vorhandenen Zutrittsanlage ein Zusatz zum Zustimmungsvertrag der ZK zu erstellen, in der die Erweiterung auf biometrische Erkennungsverfahren vereinbart wird. Diese Zustimmung wird mit der Arbeitnehmervertretung und nicht mit jedem einzelnen Arbeitnehmer herbeigeführt.

Die Datenschutz-Grundverordnung nennt „biometrische Daten“ ausdrücklich und definiert sie als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“. Will ein Unternehmen also biometrische Verfahren für die Zugangs- oder Zutrittssteuerung einsetzen, muss es zuerst die datenschutzrechtlichen Voraussetzungen klären, wie sie Art. 9 DS-GVO aufführt. Außerdem sollte die Erforderlichkeit nachgewiesen werden und ein Datenschutzbeauftragter (der auch ein externer Dienstleister sein kann) ab 20 Mitarbeiter bestellt werden. Die Erforderlichkeit der Verarbeitung biometrischer Daten ergibt sich immer dann, wenn alternative Systeme (z.B.: mit Ausweis und PIN) nicht die erforderliche Sicherheit hinsichtlich der Verhinderung eines unbefugten Zutritts erzielen! Beispielsweise wäre dies die Zutrittssteuerung zu einem Rechenzentrum (siehe Foto) mit besonders sensiblen (personenbezogenen) Daten.

14. Was hat der Anwender, der Benutzer von Biometrie?

Eine gut und zügig funktionierende biometrische Zutrittssteuerung wird als sicherer und bedienungsfreundlicher als andere Identifikationsverfahren empfunden. Hauptargument ist, dass auf den Mitarbeiterausweis, je nach der angewandten Sicherheits-Philosophie, ggf. verzichtet werden kann. Somit benötigt der Mitarbeiter während seiner Tätigkeit im Betrieb keinen Ausweis - ein Vorteil nicht nur bei tätigkeitsbedingtem Kleiderwechsel. Biometrische Verfahren erkennen ja den Mitarbeiter persönlich - und nicht nur seinen Ausweis. Bei hohen Sicherheitsanforderungen ist es allerdings sinnvoll das Verfahren zur Verifikation (PIN/Ausweis plus biometrische Identifikation) und nicht ausschließlich als Identifikation zu nutzen. Biometrie erhöht die Sicherheit, da Manipulation z. B. durch die unerlaubte Weitergabe eines Firmenausweises an eine nicht berechtigte Person oder die unrechtmäßige Benutzung durch den Finder einer verloren gegangenen Karte entfällt.

15. Fazit

Die Diskussionen um das Für und Wider beim Einsatz biometrischer Erkennungsverfahren werden leidenschaftlich und teils auch kontrovers geführt. Eine Klassifizierung erfolgt nur selten oder gar nicht. Man muss aber die Einsatzfälle und Umgebungsbedingungen genau beachten, da sie für die Verfahren, die Merkmalsdarstellung und auch für Datensicherheit und Datenschutz erhebliche Unterschiede mit sich bringen. Biometrie hat angesichts der bisher gewonnenen Erkenntnisse eine nachhaltige Zukunft. Biometrie erhöht nicht nur deutlich die Sicherheit in einem Betrieb und des Einzelnen, sondern bietet dem Nutzer auch eine Erhöhung des Komforts im Vergleich zu wissens- und besitzbasierenden Identifikationssystemen. Für die objektive Aufklärung und Information über solche Systeme können Hersteller und Anwender nie genug tun.

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, info@bhe.de, www.bhe.de