



ITWissen

Das große Online-Lexikon
für Informationstechnologie

Glossar

Biometrie

- **Authentifizierung**
- **Authentizität**
- **Autorisierung**
- **Bio-API**
- **Biometrie**
- **Credential**
- **Directional Codes**
- **E-Pass**
- **EER, equal error rate**
- **Elektronischer Personalausweis**
- **EPIC, electronic privacy information center**
- **FAR, false acceptance rate**
- **Fingerabdruckerkennung**
- **FingerTip**
- **FRR, false rejection rate**
- **Gangerkennung**
- **Gesichtserkennung**
- **Handerkennung**
- **Handschrifterkennung**
- **Handvenenerkennung**
- **Identifikation**
- **Iriserkennung**
- **Minutien**
- **Retinaerkennung**
- **Spracherkennung**
- **Stimmerkennung**
- **Tastendruckerkennung**
- **Unterschriftserkennung**
- **Verifikation**
- **VLTA, vector line type analysis**

Authentifizierung *authentication*

Unter der Authentifizierung versteht man die Aufgaben- und Benutzer-abhängige Zugangs- und/oder Zugriffsberechtigung. Die Authentifizierung hat den Zweck Systemfunktionen vor Missbrauch zu schützen. In der Kommunikation stellt die Authentifizierung sicher, dass der Kommunikationspartner auch derjenige ist, für den er sich ausgibt.

Bei der Authentifizierung wird zwischen einseitiger und gegenseitiger Authentifizierung unterschieden. In der Praxis ist meistens die einseitige Authentifizierung üblich, wobei beispielsweise beim Login der Benutzer sein Passwort eingibt und damit nachweist, dass er wirklich der angegebene Benutzer ist. Als Sicherheitsdienst für die einseitige *Identifikation* dient der Empfängernachweis durch den die Benutzer-Identität und damit auch der Benutzungsberechtigung gegenüber dem System nachgewiesen werden. Dazu dienen hauptsächlich Passwörter, Passwortverfahren, persönliche ID-Nummern, kryptografische Techniken sowie Magnet- oder Chip-Ausweiskarten. Eine strenge Authentifizierung kann mit der Vergabe von Einmalpasswörtern (OTP) und OTP-Token erfolgen.

Darüber hinaus gibt es Authentifizierungssysteme die mit *biometrischen* Daten arbeiten und Mehrfaktorensysteme, die auf so genannte USB-Token setzen.

Sicherer als die einseitige Authentifizierung ist die gegenseitige, bei der alle Kommunikationspartner ihre Identität beweisen müssen, bevor untereinander vertrauliche Daten ausgetauscht werden. So sollte beispielsweise bei Geldautomaten dieser vor Eingabe der PIN-Nummer beweisen, dass es sich bei dem POS-Terminal um ein echtes Geldterminal handelt und nicht um eine Attrappe.

Authentizität *authenticity*

Authentizität ist die Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Mitteilung. Nach heutiger Rechtsauffassung ist die Authentizität nur dann sichergestellt, wenn die Mitteilung, beispielsweise das Schriftstück, mit Original-Unterschrift versehen ist und zwar von

autorisierten Personen, die die schriftliche Willenserklärung abgeben dürfen. In einigen Fällen schreibt das Gesetz zur Bestimmung der Authentizität notarielle Beglaubigung, Beurteilung oder Beurkundung vor.

Bezogen auf die Informationstechnik geht es bei der Authentizität um die Verbindlichkeit von Daten, Dokumenten, Informationen oder Nachrichten, die einer bestimmten Dateneneinrichtung oder einem Sender sicher zugeordnet werden können. Durch die Authentizität muss sichergestellt werden, dass die Herkunft solcher Information zweifelsfrei nachgewiesen werden kann. Eine Möglichkeit für den Nachweis ist die digitale Signatur (DSig).

Autorisierung *authorization*

Die Autorisierung ist eine Berechtigung, eine explizite Zulassung, die sich auf einen Benutzer bezieht. Sie definiert, wer was in einem Netz was tun oder welche System-Ressourcen nutzen darf. Bei der Autorisierung werden dem Nutzer Rechte zugewiesen. Sie berechtigen den Benutzer eine bestimmte Aktion auszuüben. Um einen wirksamen Schutz zu erreichen, sollten bei der Rechtevergabe der Nutzer nur für die Ressourcen autorisiert werden, die er unbedingt benötigt.

Eine Autorisierung setzt eine Prüfung der ausführenden Person oder Kommunikationseinrichtung voraus. Erst nach der Ermächtigung kann die gewünschte Aktion oder Transaktion ausgeführt werden. So wird beispielsweise eine Transaktion mittels einer Kreditkarte zuerst durch den Kreditkartenherausgeber autorisiert, nach dem die Kartendaten überprüft wurden.

Bio-API *biometric API*

Mit dem Bio-API hat die gleichnamige Vereinigung die Funktionen und Schnittstellen für *biometrische* Verfahren festgelegt. Die Spezifikationen umfassen die Funktion, die für die biometrische *Identifikation* erforderlich sind, ebenso die Schnittstellen-Spezifikationen und die Verwaltung biometrischer Daten.

Biometrie

Die Bio-API hat das Ziel die proprietären Verfahren der verschiedenen Hersteller zusammenzuführen. Sie umfasst die Basis-Funktionen für Bio-Datenbanken, die Schnittstellen für die Hardware und die Managementfunktionen. Als Datenformat für die Bio-API ist das Biometric Identification Record (*BIR*) definiert. Die Bio-API unterstützt alle gängigen Computer-Plattformen.

<http://www.bioapi.org>

Biometrie *biometrics*

Die Biometrie oder Biometrik ist die Lehre von der Messung von lebenden Körpern. Basierend auf der Biometrie haben sich in der Kommunikations- und Informationstechnik spezielle

Biometrische Merkmale	Sensoren	Schwachpunkte
Fingerabdruck	Sensor-Chip optische Scanner	Verschmutzte oder verletzte Finger
Handgeometrie	Optische Scanner	Erkrankungen
Stimmerkennung	Mikrofon	Hintergrundgeräusche Krankheitsbed. Stimmveränd.
Gesichtserkennung	Kamera	Bekleidungs- und witterungs-abhängig
Iris-Erkennung	Spezialkamera	Erkrankung oder Verletzung
Retina-Erkennung	Infrarotlaser	des Auges
Unterschrift	Signatur-Tablett	Psychische und krankheits-bedingte
Tastaturdynamik	Tastatur	Veränderungen
Bewegungsablauf	Kamera	

Biometrische Erkennungsmerkmale und deren Sicherheit

Sicherheitsverfahren entwickelt, die die Erkennung von biometrischen Daten zum Ziele haben. Die biometrischen Daten von Menschen tangieren alle körpereigenen, physiologischen Merkmale und die Verhaltensstrukturen. Zu den physiologischen

Biometrie



Terminal für Karten und Gesichtserkennung,
Foto: Bundesdruckerei

Fingergeometrie, Stimmmerkmale, Gesichtsabmessungen, Iris und Retina.

In biometrischen Systemen werden die körpereigenen Merkmale automatisch erfasst und für die sicherheitsrelevanten Aufgaben wie die Zugriffsberechtigung und die *Authentifizierung*, analysiert. Die biometrischen Identifikationsverfahren setzen auf der Messung von physischen Merkmalen auf, im Besonderen auf dem Fingerabdruck, der *Iriserkennung* und *Retinaerkennung* oder Gesichtserkennung. Die Daten können beispielsweise auf einer Smartcard gespeichert werden. Entsprechende Systeme heißen *Fingerprint*- oder Fingerabdruck-Scanner, Gesichtsbildabtastung oder Iriserkennung.

Da biometrische Daten weder verändert noch an andere Personen weitergegeben werden

Merkmale gehören die Iris und Retina, der *Fingerabdruck*, die Venenmuster und die *Gesichtserkennung*, die Handgeometrie und die Ohrform, der Geruch und das Blutbild. Neben den erwähnten körpereigenen statischen Merkmalen gibt es auch Bewegungs- und Verhaltensmerkmale. Zu diesen dynamischen Merkmalen zählen die *Unterschriftsdynamik*, das *Tippverhalten*, die *Stimmerkennung*, Lippenbewegung und der menschliche Gang. Interessant für die Sicherheitskonzepte sind aber nur die Daten, die einen Menschen eindeutig und zweifelsfrei kennzeichnen und die weder simuliert noch verändert werden können. Dazu gehören u.a. der Fingerabdruck, die Hand- und

können, ist damit eine extrem hohe Fälschungssicherheit gegeben.

Die *Identifikation* mit biometrischen Verfahren basiert auf Wahrscheinlichkeiten. Diese werden durch die drei Parameter Falsch-Akzeptanzrate (*FAR*), *Falsch-Zurückweisungsrate* (*FRR*) und Equal Error Rate (*EER*) bestimmt.

Credential *credential*

Credentials sind Ausweispapiere, Berechtigungsnachweise, Zeugnisse oder Legitimationen in Form von Daten, die einem System die Identität eines anderen Systems oder eines Benutzers bestätigen sollen. Allgemein kann ein Credential eine Geburtsurkunde sein, ein Pass, Führerschein oder *Personalausweis*. Ebenso die unverwechselbaren Charakteristiken der *Biometrie*, wie der *Fingerabdruck*, die Iris oder die Netzhaut.

In der Informationstechnik gehören neben den biometrischen Merkmalen Passwörter, Schlüssel oder Ergebnisse kryptografischer Verfahren dazu oder auch physikalische Komponenten für die Zugriffsberechtigung wie Chipkarten oder Schlüssel.

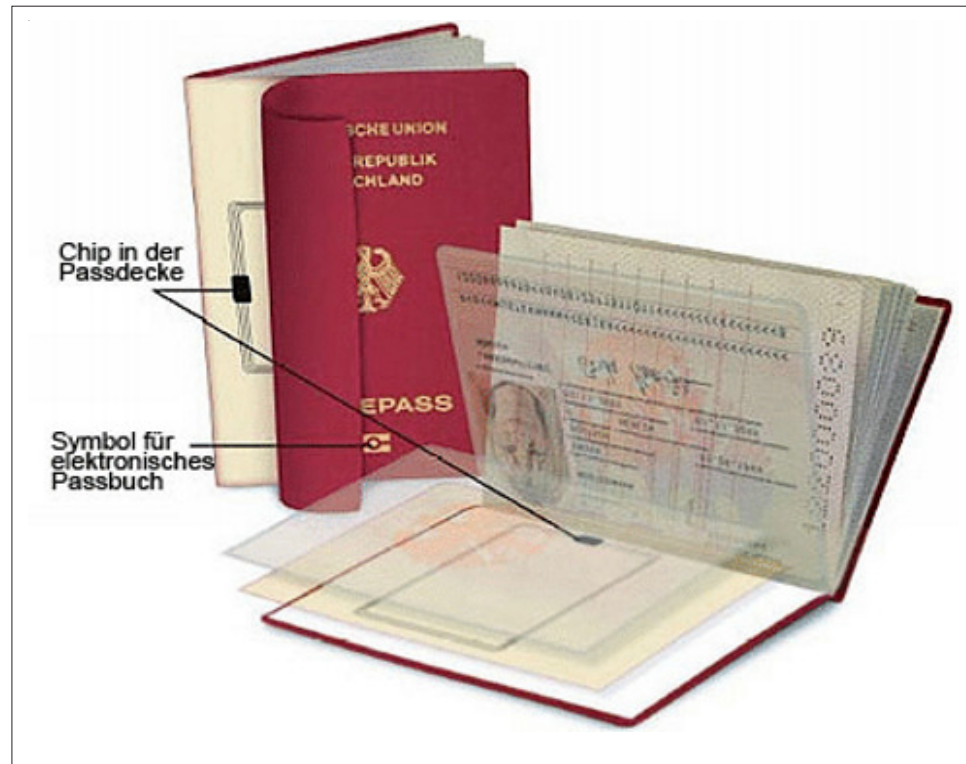
Directional Codes *directional codes*

Directional Codes ist eines von mehreren Verfahren zur *Fingerabdruckerkennung*. Bei diesem Verfahren wird die Richtung der Papillarlinien erfasst und daraus werden Rückschlüsse auf die Grauwertveränderung des Fingerabdruck-Bildes gezogen. Man bezeichnet diese Art der Darstellung auch als Richtungsbild. Die Darstellung dient auch zur Erfassung der Minutien.

E-Pass *ePass, electronic passport*

Seit Oktober 2005 wird in Deutschland der elektronische Reisepass (ePass) anstelle des herkömmlichen Reisepasses ausgegeben. Das Erscheinungsbild entspricht dem des bisherigen maschinenlesbaren Passes, bis auf ein äußeres Symbol, das ihn als elektronischen Pass kenntlich macht.

Der wesentliche Unterschied besteht in einer dünnen Folie mit RFID-Tag und Antenne, die in



Aufbau des elektronischen Passes, E-Pass, mit RFID-Tag.
Foto: Bundespressestelle

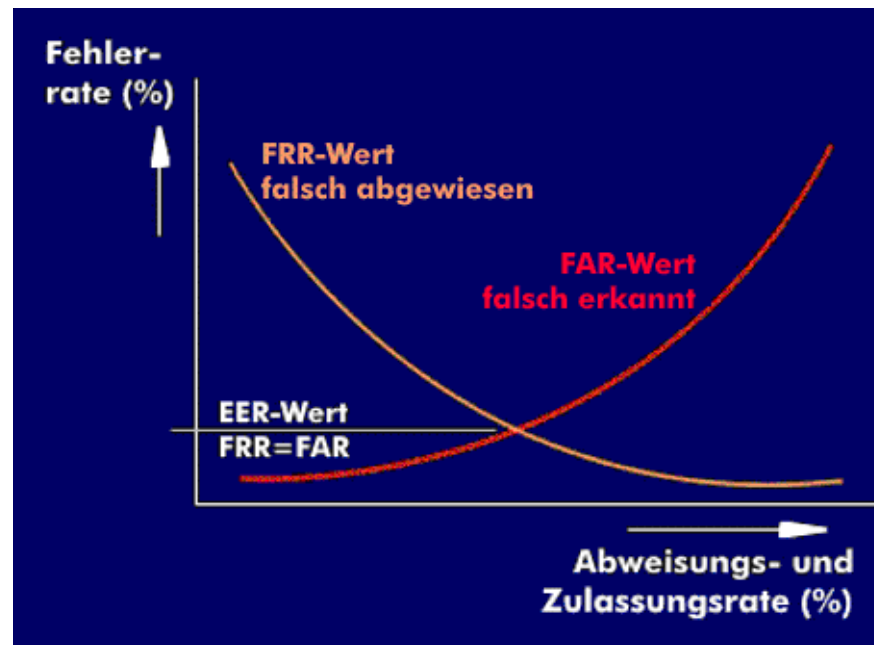
MRZ-Zeile den Namen, das Geschlecht und das Geburtsdatum, darüber hinaus gehören zu den weiteren Datengruppen das Gesichtsbild mit den *biometrischen* Daten und den Fingerabdrücken.

Die personenbezogenen Daten sind durch eine digitale Signatur mit zwei Schlüsseln verschlüsselt. Damit die Daten nicht unbeabsichtigt ausgelesen werden können, hat der E-Pass einen zweistufigen Zugriffsschutz, bei dem das Lesegerät über die maschinenlesbaren

den Passumschlag eingearbeitet ist. Der RFID-Chip ist ein Mikroprozessor mit kryptographischem Coprozessor und einem Speicher von 72 KB. Die auf dem Chip gespeicherten Daten sind in ihrer Struktur von der Luftfahrtbehörde ICAO, einer Unterorganisation der Uno, standardisiert. Die ICAO hat 16 Datengruppen festgelegt, von denen die ersten drei für den deutschen ePass benutzt werden. Die erste Datengruppe ist auch im maschinenlesbaren Pass enthalten und umfasst als

Daten (MRZ) einen geheimen Zugriffsschlüssel errechnet, der zur *Authentifizierung* gegenüber dem RFID-Tag dient. Auch die Funkübertragung zwischen Lesegerät und RFID-Tag ist Dreifach-DES (3DES) verschlüsselt.

EER, equal error rate



Zusammenhang zwischen FRR, FAR und EER

erfolgte richtige Authentisierung und die fehlerhafte Authentisierung gegenübergestellt werden. Sind beide Werte gleich groß, spricht man von der Equal Error Rate (EER).

Die Equal Error Rate (EER) ist ein Maß für die Unsicherheit bei der *biometrischen* Erkennung. Der Wert wird bestimmt durch die Gleichheit der richtigen und fehlerhaften Erkennungen. Er ist dann gegeben, wenn die Falsch-Akzeptanzrate (FAR) und die *Falsch-Zurückweisungsrate* (FRR) gleich sind.

Equal Error Rate wird für die Bewertung von biometrischen Daten für die richtige *Authentifizierung* benutzt, wobei die innerhalb der vorgegebenen Toleranzgrenzen

Elektronischer Personalausweis

In dem vorläufigen Gesetzentwurf für den elektronischen Personalausweis sind die Richtlinien für die Einführung und die Technik festgelegt.

Biometrie

bürgerlichen Freiheiten, dem Schutz der Privatsphäre und konstitutioneller Werten. Unter diese Zielsetzung fallen auch Internet-Aktivitäten und damit die Computersicherheit, die Einschränkung durch Hacker, der Schutz von Minderjährigen gegen jugendgefährdende, gewaltverherrlichende, sexistische, pornografische, terroristische oder militante Inhalte, das Abhören von Gesprächen und Datenleitungen und die Sicherstellung der Informationsfreiheit.
<http://www.epic.org>

FAR, false acceptance rate

Falsch-Akzeptanzrate

Die falsche Akzeptanzrate (FAR) ist eine Fehlerangabe für *biometrische* Verfahren. Dieser Wert ist bei biometrischen Systemen von Interesse, da diese häufig die biometrischen Daten fehlerhaft interpretieren und dadurch Personen ohne Zugriffsberechtigung eine solche gewähren. Beim FAR-Wert handelt sich darum, dass die biometrischen Daten einer Person erkannt wurden, obwohl die biometrischen Daten einer anderen Person erfasst wurden. Somit wurde eine Person fälschlicherweise als die Person erkannt, deren Daten als Referenzdaten vorliegen.

Biometrisches Verfahren	FAR-Werte in %	FRR-Werte in %	Missbrauch
Fingerabdruck	0,001 ... 2	0,1 ... 5	hoch
Iriserkennung	0,0001 ... 1	0,1 ... 2	gering
Gesichtserkennung	0,5 ... 2	1 ... 3	sehr gering
Handgeometrie	1 ... 5	1 ... 5	sehr gering

FAR- und FRR-Werte für verschiedene biometrische Verfahren

Der FAR-Wert gibt die Wahrscheinlichkeit an, mit der eine unberechtigte Person als berechtigt erkannt wird. Sie errechnet sich aus dem Verhältnis der Anzahl an falschen Erkennungen (*NFA*) zu der Anzahl der Versuche durch nicht berechtigte Personen

(*NIA*), angegeben in Prozent. Die falsche Akzeptanzrate ist sehr stark abhängig von den eingegebenen Toleranzgrenzen. Je kleiner diese Grenzen sind, desto höher ist die falsche Akzeptanzrate. Je geringer die Falsch-Akzeptanzrate ist, desto wahrscheinlicher ist die fehlerfreie *Identifikation*.

Aus der False Acceptance Rate (FAR) und der *False Rejection Rate* (FRR) wird für die Bewertung der Wahrscheinlichkeit die Equal Error Rate (*EER*) gebildet.

Fingerabdruckerkennung *fingerprint identification*



Fingerprintterminal, Foto: Kaba GmbH

Die Fingerabdruckerkennung, die Daktyloskopie, ist ein biometrisches Sicherungsverfahren, über das der authentifizierte Zugang zu Geräten und Netzen gesichert wird. Da die Papillarlinien des Fingerabdrucks bei jedem Menschen unverwechselbar und nicht veränderbar sind, stützen sich mehrere Verfahren auf diese charakteristischen Merkmale. Die Einzigartigkeit wird mit eins zu einer Millionen angegeben.

Verfahrensmäßig werden bei der Erkennung von Fingerabdrücken charakteristische Merkmale extrahiert. Mehrere dieser spezifischen Merkmale, die sich in Bögen, Wirbeln und Schleifen zeigen, werden von Fingerabdruck-Scannern erfasst und

Biometrisches Verfahren	FAR-Werte in %	FRR-Werte in %	Missbrauch
Fingerabdruck	0,001 ... 2	0,1 ... 5	hoch
Iriserkennung	0,0001 ... 1	0,1 ... 2	gering
Gesichtserkennung	0,5 ... 2	1 ... 3	sehr gering
Handgeometrie	1 ... 5	1 ... 5	sehr gering

FAR- und FRR-Werte für verschiedene biometrische Verfahren

Hautlinien des Fingerabdrucks an bestimmten Punkten analysiert und bei *Minutien* die Endungen und Verzweigungen der Papillarlinien.

Die Fingerabdruckerkennung ist ein biometrisches Verfahren mit einer relativ geringen Fehlerrate. Bei diesem Verfahren sind die Anforderungen an die Falsch-Akzeptanzrate (*FAR*) und die *Falsch-Zurückweisungsrate* (*FRR*) sehr hoch. Die Falsch-Akzeptanzrate liegt zwischen 0,001 % und 2 %, das bedeutet, dass von 1.000 aufgenommenen Fingerabdrücken weniger als ein gültiger Fingerabdruck abgelehnt wird.

FingerTip ist die von Siemens geschützte Bezeichnung für einen *Fingerabdruck*-Scanner zur *Identifikation* des *Fingerprints*. Beim FingerTip handelt es sich um eine Siemens-Entwicklung basierend auf einem kapazitiven Verfahren, bei dem ein Hochleistungs-Sensor in einem engen Raster die Kapazitätsverteilung der aufliegenden Fingerkuppe misst.

Bei Auflegen eines Fingers entsteht dabei das Ladungsbild der Papillarlinien durch

ausgewertet.

Man unterscheidet drei verschiedene

Erkennungsverfahren, die in den Fingerabdruck-Scannern umgesetzt werden:

Beim Directional Codes wird die Richtung der Papillarlinien erfasst, bei der Vector Line Type Analysis (*VLTA*) werden die feinen

FingerTip

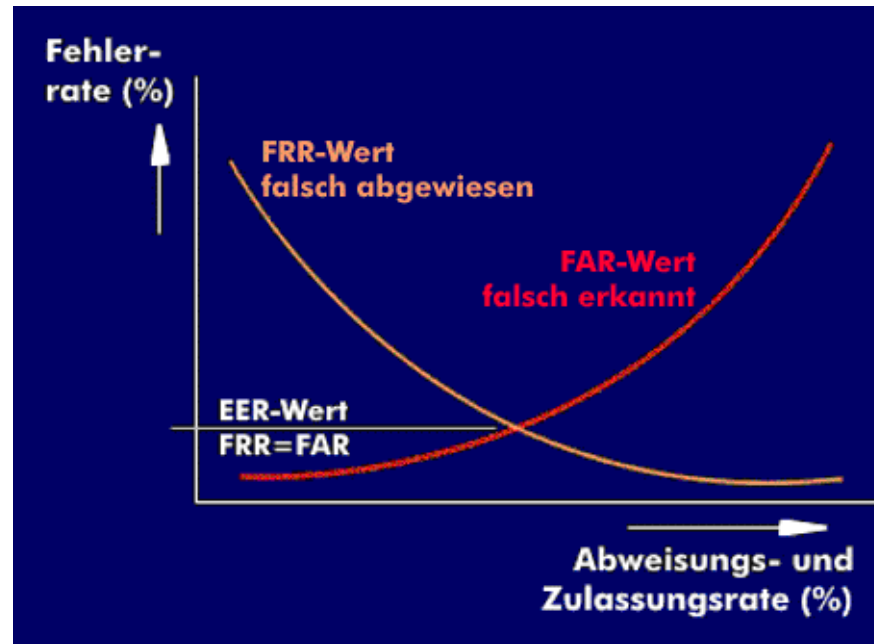
unterschiedliche Rückkoppelungskapazitäten mit den einzelnen Sensorelementen. Aus dieser Struktur berechnet ein Prozessor mittels biometrischem Verfahren die charakteristischen Merkmale des Fingerabdrucks.

Der Hochleistungs-Sensor arbeitet mit einer Auflösung von über 500 dpi, also etwa 20 Bildpunkte pro mm, einer Bildgröße von 220 x 280 Pixel und einer Informationstiefe von 8 Bit pro Pixel.

Der kapazitiv arbeitende Fingerchip kann problemlos in Tastaturen, Notebooks oder Handys untergebracht werden. Im praktischen Einsatz wird ein Fingerprint für die Zugriffsberechtigung gespeichert und mit dem aktuellen, für die Zugangsanforderung eingegebenen Messergebnis verglichen. Bei positiver Identifikation werden die entsprechenden Aktionen eingeleitet: Zugang bereitgestellt, Tresor geöffnet, ein Computer oder Personal Computer (PC) über die FingerTip-Maus oder das -Keyboard aktiviert usw.

FRR, false rejection rate Falsch-Zurückweisungs- rate

Die False Rejection Rate (FRR) ist ein Wert der die Zugangsverweigerung zu einem System beschreibt, obwohl eine Zugriffsberechtigung vorliegt. Dieser Wert ist bei *biometrischen* Systemen von Interesse, da diese häufig die biometrischen Daten fehlerhaft interpretieren. Es handelt sich darum, dass die biometrischen Daten einer Person, deren Daten als Referenzdaten vorliegen, nicht erkannt werden, obwohl es sich um die richtige Person handelt. Der FRR-Wert errechnet sich aus dem Verhältnis von der Anzahl an falschen Zurückweisungen (*NFR*) zu der Anzahl an berechtigten Versuchen (*NEA*), angegeben in Prozent. Ein hoher FRR-Wert sagt aus, dass die biometrische Identifizierung gut ist. Im Gegensatz dazu steht die *False Acceptance Rate* (FAR), die bei hoher Identifizierung einen niedrigen Wert hat. Die False Rejection Rate (FRR) ist ein Wert der die Zugangsverweigerung zu einem System beschreibt, obwohl eine Zugriffsberechtigung vorliegt. Dieser Wert ist bei *biometrischen*



Zusammenhang zwischen FRR, FAR und EER

Identifizierung gut ist. Im Gegensatz dazu steht die *False Acceptance Rate* (FAR), die bei hoher Identifizierung einen niedrigen Wert hat.

In der Art und Weise wie sich Personen bewegen und wie sie gehen gibt es unverwechselbare charakteristische Merkmale, die zur *biometrischen* Identifizierung eingesetzt werden. Der menschliche Gang weist individuelle Bewegungsmuster auf, die sich gut für die maschinelle *Identifikation* eignet. Um nicht komplette Videosequenzen mit den Referenzgangsequenzen vergleichen zu müssen, geht man in dazu über lediglich die Silhouette der Personen und dessen Gangzyklus miteinander zu vergleichen. Dabei spielt der Schrittzyklus bei der

Systemen von Interesse, da diese häufig die biometrischen Daten fehlerhaft interpretieren. Es handelt sich darum, dass die biometrischen Daten einer Person, deren Daten als Referenzdaten vorliegen, nicht erkannt werden, obwohl es sich um die richtige Person handelt. Der FRR-Wert errechnet sich aus dem Verhältnis von der Anzahl an falschen Zurückweisungen (*NFR*) zu der Anzahl an berechtigten Versuchen (*NEA*), angegeben in Prozent. Ein hoher FRR-Wert sagt aus, dass die biometrische

Gangerkennung
gait detection

Auswertung keine Rolle.

Die Gangerkennung gehört zu den dynamischen biometrischen Verfahren, die im öffentlichen Bereich eingesetzt wird. Da im städtischen Bereich viele Straßen, Plätze, Zugänge und andere neuralgische Punkte mittels Videoüberwachung kontrolliert werden, kann man mittels Gangerkennung aus den vielen aufgenommenen Personen diejenigen mit bestimmten Gangmerkmalen ausfiltern.

Gesichtserkennung *computational face recognition*

Die Gesichtserkennung ist ein Verfahren der *Biometrie* für die *Authentifizierung* von Personen. Bei diesem Verfahren wird ein Referenzbild der Person erfasst und mit bestimmten charakteristischen Merkmalen versehen gespeichert.

Zu diesen charakteristischen Kennzeichen gehören diverse Bezugspunkte und -linien, wie beispielsweise der Augenabstand, der Abstand und die Winkelung zwischen Nase und Augen, die oberen Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes usw. Bei der Authentifizierung wird von der betreffenden Person ein Digitalfoto erstellt, das der Rechner mit den spezifischen Charakteristiken des Referenzbildes vergleicht und darauf hin seine Entscheidung fällt.

Beim Abgleich des aufgenommenen Bildes mit dem Referenzbild wird ein Gitternetz über die Aufnahme gelegt um die markanten Punkte zu lokalisieren und ihren Abstand, die Lage und die Position miteinander zu vergleichen.

Die Gesichtserkennung hat eine moderate Erkennungswahrscheinlichkeit, ihre Falsch-Akzeptanzrate (*FAR*) liegt zwischen 0,5 und 2 %.

Handerkennung *hand recognition*

Die Handerkennung ist eines der ältesten *biometrischen* Authentifizierungsverfahren. Sie hat gegenüber der *Fingerabdruckerkennung* den Vorteil, dass sie auch bei verschmutzten oder

verletzten Händen eine relativ hohe Sicherheit bietet.

Die Handerkennung basiert auf dreidimensionalen Handmodellen. Bei der Erfassung der Handfläche wird die Handform und die Fingerform ausgemessen, deren Dicke, Breite und Länge. Das Scannen der Handform erfordert eine dreidimensionale Abtastung, was die Handerkennungs-Scanner recht voluminös macht.

Neben der Handformbewertung gibt es auch die *Handvenenerkennung*.

Handschrifterkennung

HCR, handprint character recognition

Unter Handschrifterkennung sind alle Verfahren zu verstehen, die handgeschriebene Buchstaben, Ziffern, Wörter oder Sätze automatisch erkennen und in eine für den Computer zu verarbeitende Datei umformen. Die HCR-Technik (Handprint Character Recognition) ist eine intelligente Zeichenerkennung (ICR) und aus der optischen Zeichenerkennung (OCR) hervorgegangen.

Schrifterkennungsverfahren analysieren individuelle Handschriften, also solche, die sich nicht nach Erkennungsvorgaben richten. Da Handschriften durch viele individuelle und nationale Charakteristiken geprägt sind und der menschlichen Psyche unterliegen, analysieren die Erkennungsverfahren einzelne Zeichen, aber auch den Schriftverlauf und die Schreibgeschwindigkeit. Die Bewegungs- und Zeichencharakteristika werden gespeichert und in einem internen Wörterbuch verglichen. Mit dieser Texterkennung werden Erkennungsgrade von weit über 90 % erreicht.

Handvenenerkennung

hand vein detection

Die Handvenenerkennung ist eines von vielen *biometrischen* Authentifizierungsverfahren. Basis der Handvenenerkennung ist das Muster des Arterien- und Venenverlaufs in der Hand eines Menschen. Dieses Muster wird mittels Infrarotaufnahme, manchmal in Kombination mit einer Temperaturmessung, erfasst. Venen, die schwächer angezeigt werden, werden durch

Algorithmen hochgerechnet.

Die Handvenenerkennung ist eines der zuverlässigsten biometrischen Verfahren mit einer niedrigen Falsch-Akzeptanzrate.

Identifikation *identification*

Die Identifikation ist die Überprüfung einer Person oder eines Objektes in Bezug auf vorgelegte, eindeutig kennzeichnende Merkmale, die Identität. Diese Identität kann anhand von eindeutigen Merkmalen, die denen eines Ausweises entsprechen, überprüft werden. Oder auch mittels Passwörtern und gespeicherten Referenzpasswörtern.

Für die Identifizierung gibt es verschiedene Medien und Verfahren; u.a. Chipkarten, Magnetkarten, Smartkarten und *biometrische* Verfahren. Darüber hinaus werden in der Warenwirtschaft Strichcodes, 2D-Codes und RFID für die eindeutige Warenkennzeichnung eingesetzt.

Bei der biometrischen Identifikation werden individuelle, körperspezifische Merkmale wie der *Fingerabdruck*, das Gesichtsfeld oder die Iris für die Identifikation genutzt.

Iriserkennung *iris scanning*

Die Iriserkennung ist eines von mehreren Verfahren, das mit *biometrischen* Daten für die *Authentifizierung* arbeitet. Bei diesem Verfahren, das sehr fälschungssicher ist und sich darüber hinaus durch eine niedrige Falscherkennungsrate auszeichnet, wird die Iris mit einem ungefährlichen Laser abgetastet. Das abgetastete Bild wird zur Authentifizierung mit dem eingespeicherten Referenzbild verglichen.

Die Iris, die Regenbogenhaut, hat ebenso wie die Netzhaut, die Retina, hinreichend viele unverwechselbare Merkmale, die zur eindeutigen Identifizierung genutzt werden können. Die Einzigartigkeit wird mit 1:6 Millionen angegeben.

Die Iriserkennung hat eine relativ hohe Erkennungswahrscheinlichkeit, ihre Falsch-

Biometrie

Minutien
minutiae

Biometrisches Verfahren	FAR-Werte in %	FRR-Werte in %	Missbrauch
Fingerabdruck	0,001 ... 2	0,1 ... 5	hoch
Iriserkennung	0,0001 ... 1	0,1 ... 2	gering
Gesichtserkennung	0,5 ... 2	1 ... 3	sehr gering
Handgeometrie	1 ... 5	1 ... 5	sehr gering

FAR- und FRR-Werte für verschiedene biometrische Verfahren

Papillarlinien eines Fingerabdrucks bezeichnet. Diese charakteristischen Punkte der Hautrillen



Kennzeichnung der Minutien in einem Fingerabdruck, Foto: GMD Darmstadt

Retinaerkennung
retina detection

Akzeptanzrate (*FAR*) liegt zwischen 0,0001 % bis maximal 1%, das bedeutet, dass von 1.000 überprüften Iriden höchstens eine Person abgelehnt wird, da deren Iris nicht erkannt wird.

Als Minutien werden Endungen und Verzweigungen der

sind für jeden Menschen und Finger einmalig und nicht veränderbar und werden deswegen für die *Authentifizierung* mittels *Fingerabdruckererkennung* benutzt.

Die Extrahierung der Minutien erfolgt durch spezielle Algorithmen aus dem vom Fingerabdruck-Scanner gelieferten Fingerabdruck-Bild.

Für die Authentifizierung wird eine vordefinierte Anzahl von Minutien mit vorhandenen Referenzdaten verglichen.

Die Retina ist die Netzhaut des Auges. Sie wird ebenso wie die Iris für *biometrische* Authentifizierungsverfahren ausgewertet. Die Retina, die das in das Licht in

Nervenimpulse umwandelt, hat eine unverwechselbare Struktur, die sich für die biometrische Erkennung eignet. Die Invarianz ist äußerst hoch und die Unverwechselbarkeit liegt bei über 1:1 Million. Ebenso wie bei der *Iriskennung* werden die Strukturen der Blutbahnen beim Scannen von Infrarotlicht abgetastet.

Die Falsch-Akzeptanzrate der Retinaerkennung ist relativ gering und die Fälschungssicherheit hoch. Allerdings ist die Akzeptanz der Retinaerkennung wesentlich geringer als die der Iriskennung.

Spracherkennung *voice recognition*

Spracherkennung ist ein Verfahren der Sprachanalyse, bei dem ein computerbasiertes System mit automatischer Spracherkennung (ASR) die eingegebenen Sprachinformationen analysiert, und zwar in Bezug auf die gesprochenen Wörter, auf deren Bedeutung und hinsichtlich der charakteristischen Merkmale des Sprechers.

Die unterschiedlichen Ansätze sind anwendungsspezifisch zu sehen, so für die Spracheingabe bei der Texterfassung, für die Maschinen- und Automatensteuerung und für sicherheitsrelevante Funktionen mit *biometrischen* Daten. Es gibt spezielle Spracherkennungssysteme, die aus einem kontinuierlichen Sprachfluss Schlüsselwörter ausfiltern und erkennen, die durch vielfache Spracheingabe von unterschiedlichen Sprechern neue Wörter lernen und dadurch unabhängig werden von der charakteristischen Sprechweise eines einzelnen Sprechers.

Eingesetzt werden Spracherkennungssysteme in der Texterfassung, der Sprachverarbeitung, in der Automotive-Technik, in Spielen, Einwahlgeräten, Callcentern, Sprachboxen u.v.a.

Stimmerkennung *voice verification*

Die Stimme einer Person ist ein einzigartiges Merkmal, das sich von allen anderen Stimmen unterscheidet. Daher nutzt man das *biometrische* Verfahren der Stimmerkennung zur

Authentifizierung von Personen.

Technisch betrachtet wird ein biometrischer Stimmabdruck von der entsprechenden Person als Referenz erfasst und gespeichert und bei der Verifizierung mit einem bestimmten Wort verglichen, das der zu Verifizierende sprechen muss. Die Stimmmerkmale von Personen unterscheiden sich bis auf die kleinste Lauteinheit, das Phonem, was sich im Frequenzspektrum der Stimme ausdrückt. Die Stimmeingabe wird daher mittels einer Zeit-Frequenz-Transformation in ein Frequenzspektrum umgewandelt, das aus mehreren hundert Kilobits bestehen kann und damit hinreichende Informationen für eine Stimmerkennung bietet.

Stimmmerkmale liegen in ihrer Einzigartigkeit lediglich bei 1:10.000. Die Sicherheit bei der Stimmerkennung kann allerdings durch die Zahl der gespeicherten und abgefragten Wörter gesteigert werden. Stimmerkennungssysteme werden vorwiegend beim Telebanking eingesetzt.

Tastendruckererkennung *keystroke detection*

Das Tippverhalten gehört zu den dynamischen *biometrischen* Merkmalen, anhand dessen Personen identifiziert werden können. Der Rhythmus, mit dem bestimmte Wörter oder Buchstabenkombinationen eingegeben werden und die Zeitspannen zwischen den Buchstaben gehören zu den charakteristischen Merkmalen, die für die biometrische Erkennung genutzt werden.

Aus dem Tippverhalten können Rückschlüsse auf die Tastatureingaben gezogen und mit entsprechenden Keystroke-Programmen können ganze Eingaben rekonstruiert werden. Solche Lauschprogramme können zum Ausspähen von Texten Passwörter oder Pin-Nummern genutzt werden, ohne dass sie vom Benutzer bemerkt werden.

Unterschriftserkennung *signature detection*

Unterschriften gehören zu den dynamischen *biometrischen* Merkmalen. Die Art, wie Personen unterschreiben, wie die Druckverteilung abläuft, mit welcher Beschleunigung und Geschwindigkeit der gesamte Schriftzug und einzelne Passage oder Buchstaben geschrieben werden, die Steilheit der Buchstaben und die Länge der Unterbrechungen innerhalb der Unterschrift sind charakteristische Merkmale, die nicht von anderen Personen nachgemacht werden können. Während die Akzeptanz von Systemen zur *Schrifterkennung* sehr hoch ist, ist deren Invarianz nicht gut und die Einzigartigkeit ist mit etwa 1:10.000 auch relativ gering. Für die Aufnahme der Unterschrift oder auch für die Schrifterkennung werden Grafiktablets oder Touchscreens verwendet. Da dabei ausschließlich die statischen Merkmale der Unterschrift erfasst werden, werden für die dynamischen Merkmale spezielle Druckstifte mit eingebauten Sensoren verwendet.

Verifikation *verification*

Bei der Verifikation handelt es sich um die Überprüfung von Daten, Prozessen, Modellen oder Personen und um die Bestätigung deren Richtigkeit. Verifikation setzt die Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt werden, voraus.

Im Falle von Personen kann die Verifikation für die *Identifikation* der Personen genutzt werden; bei Datensätzen und Datenträgern kann die Fehlerfreiheit verifiziert werden. Die Bestätigung einer Identifikation kann u.a. unter Ausnutzung der *Biometrie* erfolgen, die mit den gespeicherten biometrischen Referenzdaten verglichen werden. Bei der Verifizierung müssen die Verifikations- und Referenzdaten innerhalb einer festgelegten Toleranzgrenze liegen.

Bei der Verifikation eines Datenträgers werden die gespeicherten Daten nach dem Schreibvorgang mit den im residenten Speicher befindlichen Daten verglichen. Dieser Vorgang stellt sicher, dass die aufgezeichneten Daten fehlerfrei sind.

VLTA, vector line type analysis

Vector Line Type Analysis (VLTA) ist ein Verfahren zur *Fingerabdruckerkennung*. Bei diesem Verfahren werden in dem gesamten Fingerabdruck-Bild bestimmte Punkte für das Extrahieren der charakteristischen Merkmale herangezogen. Diese für die Klassifizierung relevanten Punkte werden nach der Analyse der Rillen-Typen bestimmt.

Herausgeber

Klaus Lipinski
Datacom-Buchverlag GmbH
84378 Dietersburg

ISBN: 978-3-89238-190-7

Biometrie

E-Book, Copyright 2010

Trotz sorgfältiger Recherche wird für die angegebenen Informationen keine Haftung übernommen.



Dieses Werk ist unter einem Creative Commons Namensnennung-Keine kommerzielle Nutzung-Keine Bearbeitung 3.0 Deutschland Lizenzvertrag lizenziert.

Erlaubt ist die nichtkommerzielle Verbreitung und Vervielfältigung ohne das Werk zu verändern und unter Nennung des Herausgebers. Sie dürfen dieses E-Book auf Ihrer Website einbinden, wenn ein Backlink auf www.itwissen.info gesetzt ist.

Layout & Gestaltung: Sebastian Schreiber
Titel: © Sean Gladwell - Fotolia.com
Produktion: www.media-schmid.de
Weitere Informationen unter www.itwissen.info