

# Bitte den Finger zeigen!

Begegnen sich gegenseitig bekannte Menschen, so erkennen sie sich anhand bestimmter Merkmale, wie Körpergröße, Gesicht, Sprache, Gangart usw. Grundsätzlich können Sensoren diese – und auch noch weitere Besonderheiten – ebenfalls erfassen. Dies ist das Umfeld der Biometrie, was aus dem Griechischen mit «Lebens-Messung» übersetzt werden kann. Die Signale der Sensoren werden mit vorher aufgenommenen Referenzdaten computergestützt verglichen und die Person kann so mit grosser Sicherheit erkannt oder ausgeschlossen werden. Die wichtigsten Verfahren erfassen das Gesicht, das Fingerbild und die Iris. Aber auch die Unterschrift ist eine wichtige Kenngrösse. In der Medizin und der Kriminalistik wird häufig auf die DNA-Analyse zurückgegriffen, deren Merkmale eindeutig personenbezogen sind.

Hans R. Ris

«Vertrauen ist gut, Kontrolle ist besser», heisst es nicht nur im Militärjargon. Dieses Motto gilt unbestritten bei der Identifizierung einer sicherheitsrelevanten Person, wenn sie sich im Umfeld einer kritischen Umgebung aufhält. Das Ziel einer biometrischen Erkennung ist immer, berechnete Personen von unberechneten zu trennen. Dies geschieht durch

- **Identifikation:** die Identität einer Person wird ermittelt bzw. bestätigt, oder durch
- **Verifikation:** die betreffende Person wird ausgeschlossen

Dabei geht es um die Feststellung der Echtheit (Authentizität) mit der behaupteten oder mit der tatsächlichen Identität der betreffenden Person. Im informationstechnischen Umfeld ist dies ein herausragendes Ziel der Sicherheitstechnik. Grundsätzlich gibt es drei Möglichkeiten der Authentisierung einer Person, durch

- **Geheimes, persönliches Wissen** eines künstlichen Codes, einer Geheimzahl oder eines Passwortes. Dieses kann die betreffende Person vergessen; aber es kann durch Unbefugte auch geknackt werden.
- **Persönlicher Besitz** wie zum Beispiel einer Zutrittskarte, Kreditkarte, eines Schlüssels usw., das der betreffenden Person temporär zugeordnet wird. Dieser Besitz kann verloren gehen oder gestohlen werden und Unbefugte können sich allenfalls Zutritt verschaffen.
- **Persönlichkeitsmerkmale** wie körperliche Eigenschaften oder Verhaltensweisen,



1 Obschon die Biometrie weit fortgeschritten ist, ist die rasche automatische Identifikation einer beliebigen Anzahl Personen (noch) nicht möglich. Gerade auf Flughäfen ist man aus Sicherheitsgründen wie auch aus Gründen der Effizienz daran interessiert, das Abfertigen der Passagiere möglichst zu automatisieren.

die in der Regel dauerhaft an eine Person gebunden sind. Eine Trennung von der Person oder das Verlieren bzw. das Übertragen auf eine andere Person ist grundsätzlich nicht möglich.

Die individuellen Persönlichkeitsmerkmale sind das Umfeld der Biometrie. Darunter versteht man die Technik der Erkennung einer Person anhand persönlicher Charakteristika. Der Ausdruck Biometrie stammt aus dem griechischen und kann mit «Lebens-Messung» übersetzt werden. Meist werden computerunterstützte Erfassungs- und Auswertungssysteme eingesetzt, welche mathematische und statistische Methoden zu Hilfe nehmen. Man spricht daher auch von Biometrik.

Erfolgt die Zuordnung der biometrischen Merkmale zu einer Person korrekt, kann sichergestellt werden, dass es

sich bei dem betreffenden Individuum tatsächlich um die angenommene bzw. behauptete Identität handelt. Gegenüber einer Authentisierung auf der Basis von persönlichem Wissen (Geheimzahl) oder persönlichem Besitz (Schlüssel) ergeben sich erhebliche Vorteile. Biometrische Merkmale basieren immer auf drei Anteilen:

- **Genotypisch**, sind genetisch bedingt und damit häufig vererbbar (zum Beispiel die Hautfarbe)
- **Randotypisch**, sie entstehen zufällig während der embryonalen Phase und bleiben ein Leben lang erhalten (zum Beispiel Fingerabdruck)
- **Konditioniert**, verhaltensgesteuert lernbar und können teilweise anerzogen werden (zum Beispiel Sprache oder Unterschrift).

Zudem lassen sich biometrische Verfahren unterscheiden in

- *Physiologische Merkmale*, die meist passive Besonderheiten einbeziehen, wie zum Beispiel Gesicht, Iris, Finger oder Hand.
- *Verhaltensbezogene Merkmale*, die auf einem aktiven, personencharakteristischen Tun basieren, wie zum Beispiel der Unterschrift, der Stimme oder dem Anschlagrhythmus einer Tastatur. Diese Verfahren unterliegen immer einer natürlichen Schwankung.

### Ablauf einer biometrischen Erkennung

Die biometrische Erkennung basiert bei allen Systemen auf dem gleichen Grundprinzip (Bild 2):

- *Enrollment*: die Erfassung der biometrisch relevanten Eigenschaften einer Person als Referenzdatensatz mit Hilfe von Sensoren wie Kameras, Mikrofon, Tastatur, Druckpads, Geruchssensoren, Fingerabdrucksensoren usw.
- *Templates*: Erstellung der Datensätze der erfassten Person.
- *Matching*: Vergleich der aktuell präsentierten mit den zuvor abgespeicherten Daten des Referenzdatensatz-

zes. Bei Übereinstimmung meldet das Gerät die Erkennung des Nutzers.

Erfassung, Auswertung und Vergleich sind mit gewissen Messfehlern behaftet. Denn die verwendeten Merkmale können sich im Laufe der Zeit ändern. Zudem wird das Merkmal bei der Erfassung und dem Vergleich dem System niemals in der genau gleichen Art und Weise angeboten. So ändert sich die Position des Fingers zum Beispiel auf einem Fingerabdrucksensor oder der Blickwinkel bei der Gesichtskontrolle bei jeder Nutzung leicht. Zwei digitale Abbildungen biometrischer Merkmale sind daher nie identisch. Es ist demzufolge kein exakter Abgleich der Daten möglich.

Die biometrischen Daten werden deshalb nicht auf «Gleichheit» sondern auf eine gewisse «Ähnlichkeit» hin untersucht. Ein gewisser Toleranzbereich ist deswegen zwingend. Damit ist es auch bei einem ausgeklügelten biometrischen Verfahren nur mit einer gewissen Wahrscheinlichkeit möglich, zu bestimmen, ob eine bestimmte Person als «Berechtigter» erkannt wird.

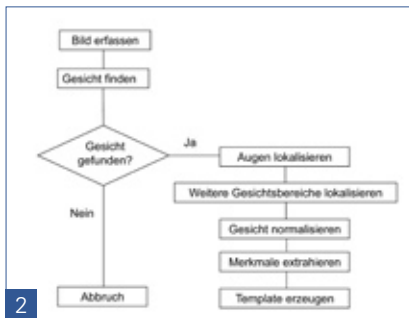
### Fingerbilderkennung

Das Fingerbild (Bild 3) jedes Menschen ist individuell – dies gilt auch für eineiige Zwillinge, die so auch eindeutig unterschieden werden können. Die einzelnen Merkmale bezeichnet man als Minuzien (lat. Kleinigkeiten). Man unterscheidet:

- *Breite der Papillarlinien*
- *Verlauf der Linien*
  - Schleifen, Wirbel, Spiralen, Ellipsen
  - Knotenpunkte, Gabelungen, Linienenden, Inseln

Da diese Minuzien im Verlauf des Lebens konstant bleiben, können sie für einen Vergleich herangezogen werden. Fingerabdrücke erhält man mittels eines Farbadrucks mit Farbe (Tinte) oder mittels eines Sensors, welcher die Papillarlinien auf einem Medium (Glas, Papier, Sensoroberfläche) erfasst. Beim Vergleich wird untersucht, ob zwei Fingerabdrücke identisch sind und damit zum gleichen Urheber (Finger) gehören. Für die Fingerabdrucktastung unterscheidet man die beiden Methoden

- *Off-line*: Farbadruck auf Papier durch Abrollen des mit Farbe (Tinte) benetzten Fingers. Anschliessend kann dieser Abdruck durch einen Scanner oder eine Kamera digital gespeichert werden. Die Methode ist umständlich und zum Beispiel für ein automatisiertes Zutrittssystem nicht geeignet.
- *On-line*: Lebendabdruck eines Fingers (Bild 4 und 5) mit Hilfe eines Sensors. Dazu gehören
  - optische Sensoren
  - E-Feldsensoren
  - polymere TFT-Sensoren
  - thermische Sensoren
  - kapazitive Sensoren
  - kontaktlose 3D-Sensoren
  - Ultraschallsensoren



2



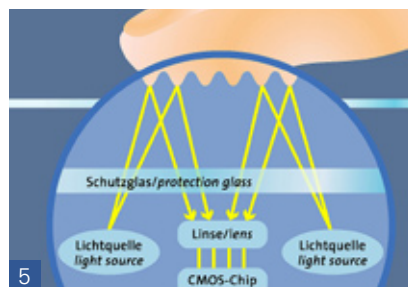
3

(Quelle: Hans R. Frits)



4

(Quelle: www.biometrix.at)



5

(Quelle: www.rst-biometrics.com)



6

(Quelle: Siemens)

2 Ablauf einer biometrischen Erkennung anhand der Gesichtserfassung und Erzeugung eines Templates.

3 Die Fingerlinien (Papillarlinien) verlaufen beim Menschen individuell und sind daher ein wichtiges Identitätsmerkmal.

4 Fingerprint-Terminal für die Zeiterfassung und Zutrittskontrolle.

5 Prinzip des optischen Sensors.

6 Computermouse mit kapazitivem Fingerprint-Sensor. Es kommen Linkshänder und Rechtshänder gut damit zurecht. Nach dem Starten wird ein Finger auf den Sensor gelegt, und schon ist eingeloggt. Platzierung des Fingers und die spezielle Software beschleunigen den biometrischen Scan auf weniger als eine Sekunde.

7 Prinzip des kapazitiven Sensors.

8 Mikroskopaufnahme eines kapazitiven Fingerbildsensors in 60-facher Vergrößerung.

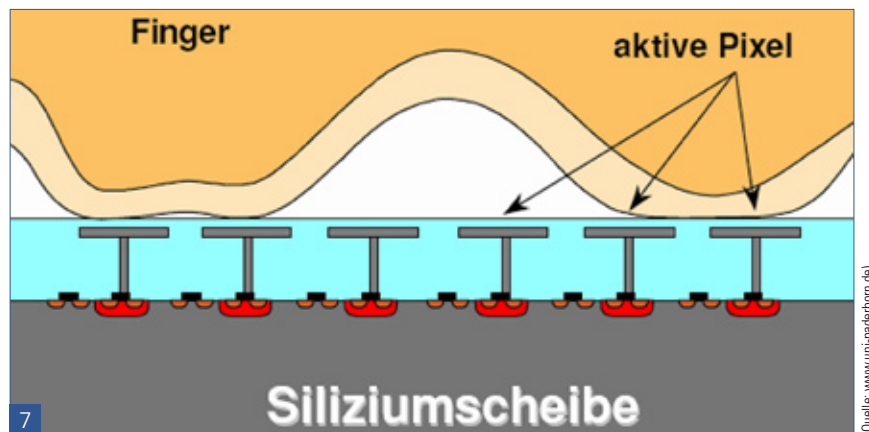
9 Handvenenleser. Mit Hilfe von Infrarotstrahlen werden die Handvenen sichtbar gemacht und biometrisch erfasst.

### Optische Sensoren

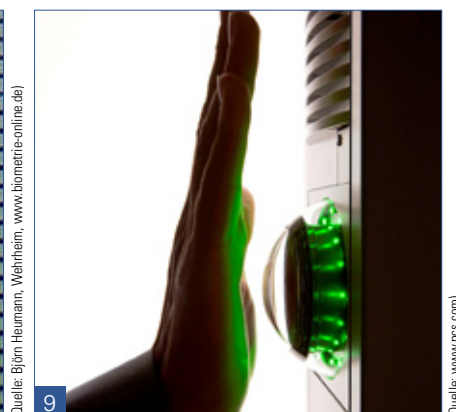
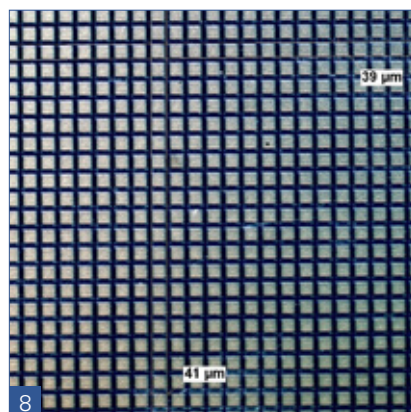
Optische Fingerbildsensoren basieren auf den unterschiedlichen Reflexionseigenschaften der Fingerkuppe, wenn sie mit Licht bestrahlt wird. Die Papillarlinien bilden «Höhenzüge» und «Täler», an denen das Licht ungleich reflektiert wird. Die Erhöhungen reflektieren mehr als die Vertiefungen. Diese Helligkeitsunterschiede kann eine CMOS-Kamera detektieren. Durch die Wahl einer geeigneten Lichtfarbe ist ein kontrastreiches Oberflächenbild und damit eine gute Erkennungsleistung des Systems möglich. Bild 7 zeigt das Prinzip eines kontaktfreien optischen Sensors.

Es gibt aber auch optisch transmissive Sensoren mit einer Lichtleiterplatte. Hier wird der aufliegende Finger von einer geeigneten Lichtquelle durchleuchtet, die wiederum direkt mit einem Kamerachip verbunden ist. Die Lichtleiterplatte sorgt dafür, dass der Finger nicht den Kamerachip berührt, das Licht aber trotzdem ohne Schärfeverlust und ohne sonstige Optik den Kamerachip erreicht.

Optisch kontaktlose Sensoren erfassen den Fingerabdruck über eine geeignete Optik direkt von einem Kamerachip ohne Berührung der Fingeroberfläche.



(Quelle: www.uni-paderborn.de)



### Kapazitive Sensoren

Auf einem fingerkuppengrossen Array (Bild 7 und 8) werden zum Beispiel  $224 \times 288 = 64512$  einzelne Kondensatorplättchen implementiert. Jedes Plättchen wirkt als Pixel. Deren Abstand ergibt dann die Pixel-Auflösungen, bis 512 dpi (Dots per Inch). Die Fingerkuppe bildet die zweite Platte. Bei der Berührung entstehen so Kapazitätsdifferenzen, die entsprechend dem Fingerlinienmuster ausgewertet werden können. Trifft ein Pixel auf eine Rille, also Luft, ist die Kapazität wesentlich niedriger als bei einer aufliegenden Fingerlinie. In diesem Fall ist das Dielektrikum Wasser, das sich durch eine sehr hohe Dielektrizitätskonstante auszeichnet.

Eine weitere Methode basiert auf einer Elektrolumineszenzfolie, mit einer durchsichtigen Rückseitelektrode. Auf der Vorderseite wirkt der Finger als Gegenelektrode. Dort, wo die Fingerlinien aufliegen, ist die elektrische Feldstärke und damit das Leuchten am grössten. Somit entsteht auf der Rückseite ein leuchtendes Abbild der Fingerlinien, das ähnlich wie beim optischen Sensor von einem Bildsensorchip erfasst werden kann.

### Thermische Sensoren

Bei der thermischen Methode erfasst eine spezielle Matrix von Einzelsensoren das Wärmeabbild des Fingers. Bedingt durch

die raue Oberflächenstruktur des Fingers erzeugt der Wärmesensor aus den unterschiedlichen Temperaturgradienten ein dreidimensionales Bild des Fingerabdrucks. Sie haben etwa die gleiche Auflösung wie die kapazitiven und optischen Pendants.

### Ultraschallsensoren

Die Ultraschallsensoren zählen derzeit zu den sichersten, aber auch zu den teuersten Geräten, um Fingerabdrücke zu erfassen. Denn die erzeugten Schallwellen lassen sich weder durch Schmutz oder Verletzungen noch durch Schweiß beeinträchtigen. Mehrere unterschiedlich positionierte Sensoren schicken Schallwellen in Richtung der abzutastenden Fingeroberfläche. Die gleichen Sensoren empfangen die reflektierten Schallwellen und erzeugen durch die unterschiedlichen Laufzeiten der Signale ein dreidimensionales Bild der Fingeroberfläche. Die Auflösung ist vergleichbar mit den kapazitiven und optischen Pendants.

### Handvenenerkennung

Das menschliche Handflächenvenenmuster ist äusserst komplex und befindet sich vor Missbrauch und Manipulationen bestens geschützt innerhalb des Körpers. Die Position der Venen bleibt zeitlebens unverändert und ist bei jedem Menschen unterschiedlich. Hautverun-

reinigungen oder oberflächliche Verletzungen haben keinen Einfluss.

Die Handvenenerkennung beruht auf der Absorption von Infrarotstrahlen (Bild 9) im Blut. Der Sensor sendet Infrarotstrahlung in Richtung der Handflächen aus. Das sauerstoffreduzierte Blut in den Venen absorbiert die Infrarotstrahlung. Die Kamera des Sensors erstellt ein Bild des Venenmusters und wandelt das Bild in ein Template um. Manipulationen sind so gut wie ausgeschlossen.

### Gesichtserkennung

Gesichter können Babys bereits in den ersten Lebensmonaten unterscheiden. Die automatisierte technische Gesichtserkennung ist aber neueren Datums. Sie wurde erst mit der sich dynamisch entwickelten Computer- und Softwareindustrie möglich. Die Technik ist noch nicht so ausgereift, dass aus einer grösseren Personengruppe die Gesichter rasch zugeordnet werden können. Bei der biometrischen Gesichtserkennung wird über eine Kamera das Gesicht einer Person mit einem oder mehreren vorher gespeicherten Gesichtsbildern verglichen.

Es gibt unterschiedliche Erfassungs- und Erkennungssysteme auf der Basis der optischen Mustererkennung bzw. deren Kombinationen. Erfasst wird meist mit der 2D-Methode mit klassischen Kameras. Grundsätzlich wird ein gewisses cha-

rakteristisches Schlüsselement gesucht. Verwendet werden vor allem solche Merkmale, die sich auf Grund der Mimik nicht ständig ändern. So zum Beispiel die oberen Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes. Die erfassten grafischen Merkmale werden mathematisiert und in einem Referenzbild abgelegt.

Mittels einer grafischen Analyse werden markante Stellen (Knoten) des Gesichts (Augen, Nasenspitze, Kinn, Haaransatz usw.) aufgesucht und über Verbindungslinien zu einem Gitternetz verbunden. Anschliessend wird das erfasste Gesicht mit Hilfe dieses Gitternetzes in frontale «Normalposition» gedreht und als Referenzmodell gespeichert.

Verglichen werden die erfassten Merkmale mit den abgespeicherten Referenzmerkmalen mit Methoden der klassischen Bildverarbeitungs- und Bildanalyseverfahren. So werden etwa die Augen mit Hilfe des über das Gesicht gelegten Gitternetzes lokalisiert. Die Augen sind im Gegensatz zur Haut extrem dunkle Punkt im oberen Bereich des Gesichts. Anschliessend werden weitere Gesichtsbereiche nach Merkmalen abgesucht und mit dem Referenzbild verglichen.

Eine neuere, noch nicht ausgereifte Methode ist das 3D-Verfahren (Bild 10). Dabei werden Streifenmuster auf das Gesicht projiziert und diese unter verschiedenen Kamerapositionen aufgenommen. Daraus kann ein dreidimensionales (3D) Muster generiert werden.

### Iriserkennung

Die Iris (Regenbogenhaut) – sie wirkt wie beim Fotoapparat als Blende und reguliert den Lichteinfall – ist bei jedem Menschen verschieden und ändert sich im Laufe des Lebens nur wenig (Bild 11). Sie eignet sich daher bestens als Er-

kennungsmerkmal. Zwischen ihr und der Hornhaut liegen komplexe band- und kammartige Bindegewebestrukturen, die individuell unterschiedlich sind, selbst bei eineiigen Zwillingen.

Die Iris bestimmt auch die Augenfarbe. Praktisch alle Babys haben nach der Geburt blaue Augen. In unterschiedlichem Ausmass wird in den ersten Monaten bei vielen Menschen durch den Farbstoff Melanin (gelblich-braune Pigmente) die Augenfarbe in Richtung «grau-grün-braun» gefärbt. Die Augenfarbe ist auch vererbbar. Blaue Augen sind eigentlich farblos, sie haben praktisch keine Pigmente und spiegeln vor allem den Blauanteil des Lichtes zurück.

Bei hellen Augen können die Strukturen mit einer normalen Kamera aufgenommen werden. Bei dunklen Augen beleuchtet man das Auge zusätzlich mit unsichtbarem Licht im nahen Infrarotbereich. Damit werden die Strukturen besser sichtbar. Aus den aufgenommenen Bildern (Bild 12) wird mit spezieller Software ein digitaler Datensatz gebildet, das Template.

### Spracherkennung

Derzeit konzentrieren sich Biometrieexperten auf die Sprechererkennung. Aus ihrer Sicht ist diese bei Telefonanwendungen die ideale Biometrie. Wenn sowieso eine automatische Spracherkennung installiert ist, fallen keine Zusatzkosten für den biometrischen Sensor an und kein zusätzlicher Aufwand für den Benutzer.

Probleme gibt es aber noch mit lauten Hintergrundgeräuschen. Diese sind nach Meinung der Fachleute in den Griff zu bekommen. Dabei werden sowohl Mikrofon-Arrays als auch adaptive Filterverfahren zur Störunterdrückung untersucht. Zudem kann man einen Sprecher dann sicher identifizieren, wenn man weiss, was

### Biometrie seit 3500 Jahren

Biometrische Methoden werden seit gut 3500 Jahren verwendet. Bereits in Assyrien – im heutigen Irak – haben die Töpfer ihre Waren durch ihren Fingerabdruck personalisiert. Und in der chinesischen Tang-Dynastie wurden vor 1400 Jahren Verträge ebenfalls mit einem Fingerabdruck authentifiziert. 1892 stellte der Engländer Sir Francis Galton fest, dass der Fingerabdruck (Daktyloskopie) ein festes Persönlichkeitsmerkmal ist, das sich im Laufe des Lebens nicht ändert. Und damit war der Weg für die Anwendung des Fingerabdruckverfahrens gebahnt.

er spricht. Damit hat die Sprechererkennung viel mit der automatischen Spracherkennung gemeinsam, bei der es ja darum geht, etwa Namen aus dem Telefonbuch des Handys zu erkennen.

Zwei Ansätze werden verfolgt: Entweder wählt der Nutzer eine ausreichend lange Äusserung für die Authentifizierung. Die Sprache spielt dabei keine Rolle, der Satz muss auch nicht geheim bleiben – bloss merken sollte man sich ihn. Oder das System fordert den Benutzer auf, Wörter oder Zufallszahlen nachzusprechen, was die Erkennung sicherer macht. Aus dem akustischen Signal werden wieder charakteristische Merkmale ermittelt.

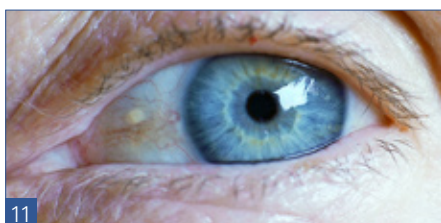
### Unterschrifterkennung

Für Verträge ist die Unterschrift die ideale Biometrie. Ob sie echt oder gefälscht war, liess sich bisher nur an ihrem Erscheinungsbild beurteilen – für gute Fälscher keine grosse Hürde. Biometrische Verfahren messen aber auch dynamische Faktoren wie Geschwindigkeit, Beschleunigung, Druck oder Auf- und Absetzpunkte des Stifts. Als Sensoren dienen für Stifteingabe geeignete Grafiktablets,



10

(Quelle: Siemens)



11

(Quelle: Hans H. Ris)

Biometrische Anwendungen		
Biometrische Technik	Heutige	Künftig
Fingerabdruck	Fingertip-Sensor, Computermaus, Zutrittskontrolle, Ausweis, Pass, Behörden	Für Massenmärkte gut geeignet: Einkäufe via Internet, elektronische Geldbörse, Autoschlüssel, integriert in Ausweise, Bezahlen im Supermarkt
Gesichtserkennung	Zutrittskontrolle Flughäfen, Gesichtsvergleich für Polizeidaten	Zugangskontrollen, Sicherheitsbereiche, Fahndung
Sprechererkennung	Zugang zu Bankdienstleistungen	Biometrie für Massenmärkte und Komfortanwendungen: Mobiltelefone, Call-Center, Bankzugang, Einkäufe übers Telefon
Iris-Scan	Kauf von Flugtickets, Identitäts-Check bei Reisenden, Grenzsicherung	Anwendungen, die sehr hohe Sicherheit erfordern
Unterschriften-erkennung	Unterschriftenprüfung bei Finanzdienstleistungen	Verträge, Zahlen per Kreditkarte
Handkontur-Scan	Sicherheit an Flughäfen, in Banken, in Gefängnissen	Authentifizierung an Multimedia-Kiosken
Multiple Biometrien (z. B. Gesicht und Stimme plus Fingerabdruck)	Ausweise	Smartcard als Ausweis (Führerschein, Versicherung, Pass) und für Online-Zugang zu Behörden

Biometrische Anwendungen.

Biometrisches Merkmal	Beschreibung	Sensor
Handgeometrie	Abmessungen der Finger und des Handballens	Kamera
Fingergeometrie	Fingerabmessungen	Kamera
Venenstruktur der Hand	Venenstruktur der Finger, der Handrückenfläche oder der Innenhand	Kamera (infrarot)
Fingerprint	Fingerlinienbild, Porenstruktur	kapazitiv, optisch, thermisch, akustisch, drucksensitiv
Gesichtsgeometrie	Abstände der gesichtbestimmenden Merkmale (Augen, Nase, Mund)	Kamera
Ohrform	Abmessungen der sichtbaren Ohrteile	Kamera
Retina	Augenhintergrund (Muster der Adernstruktur)	Kamera
Iris	Irismuster	Kamera
Stimme	Klangfarbe	Mikrofon
DNA = DNS	Codierung der DNA = DNS als Träger der menschlichen Erbanlagen	Chemisches Labor
Geruch	Chemische Zusammensetzung des menschlichen Geruchs	Chemosensoren
Unterschrift dynamisch	Schriftzug mit Druck- und Geschwindigkeitsverlauf	Tablett
Tastensanschlag	Rhythmus des Tastensanschlags auf einer Tastatur	Tablett
Passwort	Zeichensatz	Tastatur

Biometrische Merkmale und verwendete Sensoren.

Displays oder künftig auch Spezialstifte mit Kontaktsensoren.

Entscheidend ist aber nicht nur der Sensor, genauso wichtig ist, welcher Algorithmus für die Erkennung verwendet wird. Gute Ergebnisse ergibt ein zusammenhängender Schriftzug, der ohne Absetzen des Stifts zustande kommt. Die Merkmale der Verbindungszüge, wie Richtung der Schriftlinien und Geschwindigkeitskomponenten, ergeben ein Muster, das mit den Referenzmustern der Originalunterschrift verglichen wird. Diese können geschützt auf einer Chipkarte gespeichert sein.

### Sicherheit der Biometrie

Zu einem biometrischen System gehören drei Elemente: ein Sensor, die Erkennungssoftware und die sichere Integration in einer Anwendung. Prinzipiell werden zwei Arten der Kontrolle unterschieden, die Verifikation und die Identifikation. Ein Verifikationssystem untersucht die behauptete Identität des Benutzers, vergleicht also die aktuellen Messdaten mit den Referenzdaten (die der Benutzer z.B. auf einer Chipkarte mit sich führt).

Beim Identifikationssystem werden die biometrischen Daten mit den (meist zentral gespeicherten) Referenzen aller zuvor registrierten Benutzer verglichen und der beste Treffer ermittelt. Allgemein gilt, je sicherer ein System sein soll, desto höher ist die Wahrscheinlichkeit, dass ein berechtigter Nutzer zurückgewiesen wird. Man spricht hier von der «Falsch-Rückweisungs-Rate» (FRR). Umgekehrt,

je fehlertoleranter ein System gestaltet ist, umso häufiger können auch nichtberechtigte Benutzer eindringen. Das heisst, die «Falsch-Akzeptanz-Rate» (FAR) wird höher. Solche Fehlerraten lassen sich nicht theoretisch berechnen, sondern müssen durch Evaluierungen im Rahmen von Szenarien ermittelt werden. FAR und FRR sind Kenngrößen für die Leistungsfähigkeit eines biometrischen Systems.

Vielfach sind bei den Leuten auch latente Ängste bezüglich der durch biometrische Verfahren notwendigen Datenbanken vorhanden. Um diese abzubauen können zum Beispiel Schweizer Bürger/-innen ihren digital lesbaren Pass in speziellen Lesestationen selber einlesen und so erkennen, welche Angaben erfasst sind. ■

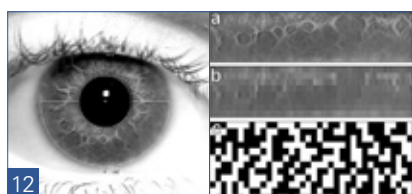
10 Keine moderne Kunst, sondern Gesichtserkennung mit dem 3D-Verfahren. Über projizierte Farbstreifen lassen sich die «Höhenlinien» des Gesichts – und damit seine dreidimensionale Form – ermitteln.

11 Das menschliche Auge ist ein individuelles Organ. Selbst eineiige Zwillinge lassen sich eindeutig unterscheiden.

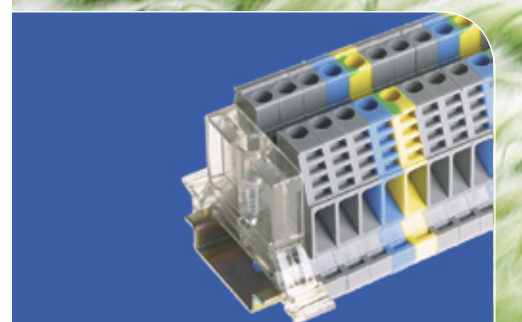
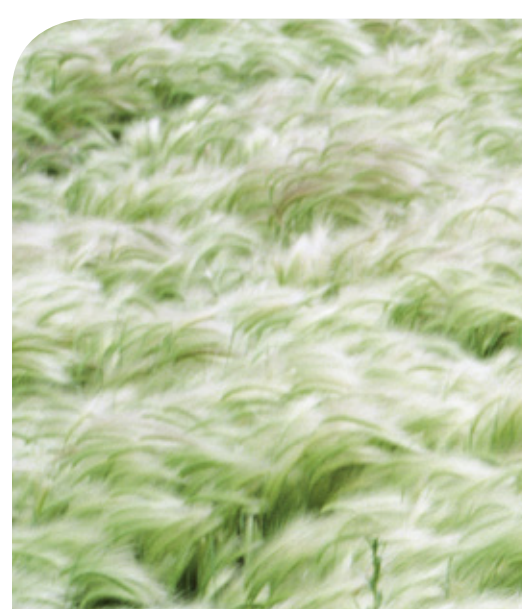
12 Links Aufnahme einer Iris bei einer Wellenlänge von 850 nm (nahes Infrarot). Man erkennt die komplexen Strukturen in der Iris. Die feinen weissen Linien wurden von einem Auswerteprogramm erzeugt und deuten die Region an, die für die Erzeugung eines Templates verwendet wurde. Die innere schwarze Pupille wird nicht verwendet. Der weisse Fleck auf der Pupille wird durch die beleuchtende Infrarot-Diode erzeugt. (Quelle: BSI)

12 Rechts Veranschaulichung der Grundschriffe zur Erzeugung eines Templates aus Bild oben

- Das Bild der Iris, transformiert in einen Streifen. Man erkennt die Strukturen aus dem Originalbild wieder.
- Das Resultat einer mathematischen Mittelung dieses Bildes.
- Das Template, wobei ein weisses Feld «1» und ein schwarzes Feld «0» bedeutet. Felder, die in b. heller (dunkler) als der Durchschnitt sind, werden zu einem weissem (schwarzen) Feld.



(Quelle: BSI)



Auf Woertz-Klemmen können Sie sich in jeder Situation verlassen! Seit Jahrzehnten erledigen Millionen unserer Klemmen einen einwandfreien Job. Sie sorgen für optimale Kontaktqualität und dadurch für eine minimale Verlustleistung.

**Frischer Wind für die Welt der Verbindungstechnik.**

Mehr Informationen unter:  
[www.woertz.ch](http://www.woertz.ch) oder  
 Tel. +41 (0)61 466 33 44

# Kontakt gesucht!

