

## Was ist Biometrie?

Biometrie ist die Lehre von der Anwendung mathematisch-statistischer Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile. Der Begriff Biometrie kommt aus dem Griechischen und setzt sich aus den Worten *bios* (Leben) und *metron* (Maß) zusammen. Mit Hilfe der Biometrie werden physische oder verhaltenstypische Merkmale erfasst und ausgewertet.

### Anwendung

Die Biometrie ermöglicht es, Zufälligkeiten der Natur mathematisch abzubilden. Sie dient daher in unterschiedlichen Wissenschaftszweigen der Planung und Auswertung von Experimenten und Erhebungen. Bei Identifikationssystemen zur Erkennung von Personen dominieren im Moment Überwachungs- und Zugangskontrollsysteme.

### Biometrische Verfahren zur Identifikation und Verifikation

Biometrische Verfahren zur Erkennung von Personen wurden und werden entwickelt, um nur Befugten den Zutritt zu bestimmten Gebäuden, Räumlichkeiten oder Geldautomaten sowie speziellen Bereichen der Informationstechnologie zu gewähren. Des Weiteren wird Biometrie eingesetzt, um die Kontrolle von Personen an Grenzübergängen oder Flughäfen zu verbessern. Sie findet auch bei der Dokumentenausstellung und bei elektronischen Wegfahrsperrern für Autos Anwendung. Darüber hinaus ist ihr Einsatz bei der Abgabe von Willenserklärungen aufgrund automatischer Unterschriftenprüfung im elektronischen Rechtsverkehr möglich. Eine Aufnahme biometrischer Merkmale in Pässe und Personalausweise kann sowohl zur Erhöhung der Sicherheit als auch zur Verhinderung von Dokumentenfälschungen beitragen.

Grundlage biometrischer Verfahren zum computergestützten Erkennen von Menschen bilden biologische Merkmale, wie Fingerabdruck, Handgeometrie, Gesicht, Auge (Iris und Netzhaut) und sogar Körpergeruch. Möglich sind auch verhaltensspezifische Merkmale, wie die Stimme, der Gang, die Unterschrift oder der Rhythmus der Tastaturbetätigung. Um diese Merkmale auszuwerten, werden die Daten zunächst erfasst und mit Hilfe mathematisch-statistischer Methoden so abstrahiert, dass von den wesentlichen Merkmalen Referenzmuster in Dateien abgespeichert werden können. Als Messgeräte dienen Sensoren oder Scanner, wie zum Beispiel Fingerabdruckleser, Iris-Scanner, Gesichts-, Sprecher- oder Schrifterkennungsgeräte.

Systeme zur Identifizierung dienen dem Identitätsnachweis der Person. Durch einen Vergleich mit den gespeicherten Referenzdaten vieler Individuen (1:n-Vergleich = "one-to-many") wird die Identität einer Person ermittelt. Systeme zur Verifizierung stellen fest, ob die von einer Person behauptete Identität tatsächlich zutrifft. Dazu werden die Eingangsdaten mit den für die bestimmte Person gespeicherten Referenzdaten verglichen (1:1-Vergleich = "one-to-one").

## Beurteilung biometrischer Verfahren

Voraussetzung für einen sinnvollen Einsatz biometrischer Verfahren zur Identifikation von Personen ist das Erfassen geeigneter Charakteristika zur unverwechselbaren Unterscheidung einzelner Menschen. Biometrische Merkmale sind von Unbefugten schwer zu fälschen oder zu kopieren, da sie an biologische Besonderheiten einer Person gebunden sind. Bei korrekter Zuordnung zu Referenzdaten erlauben sie eine Überprüfung, ob es sich um die betreffende Person handelt.

Da die Ergebnisse biometrischer Verfahren aus Wahrscheinlichkeitsberechnungen abgeleitet werden, ist eine hundertprozentige Sicherheit nicht gegeben. ekey® Produkte sind zu 99,9999 Prozent sicher. Das entspricht einem extrem guten Codeschloss, allerdings mit dem Unterschied, dass ein potentieller Einbrecher nur zehn Möglichkeiten zum Probieren zur Verfügung hat – nämlich seine zehn Finger.

**Fingerabdruck-Verfahren** gelten als kostengünstig und sehr sicher. Doch



auch innerhalb dieser Gruppe gibt es unterschiedlich sichere Methoden. Bei der *optischen Methode* wird ein Bild vom Fingerabdruck generiert. Sicherer ist die *Messung des Fingerhautwiderstandes* (kapazitive Methode). Die derzeit sicherste ist die *thermische Methode*, die von ekey® ausschließlich angewendet wird. Dabei werden die Temperatur-Unterschiede zwischen den Tälern und Hügeln des Fingerabdrucks gemessen. Aus den

Messungen wird ein Abdruck errechnet, und hieraus wiederum ein Minuzientemplate erzeugt. Bei einem solchen Template handelt es sich um einen binären Code, der anhand der Verhältnisse der Minuzien zueinander erstellt und mit dem Referenztemplate in der Datenbank verglichen wird. Minuzien sind bestimmte Merkmale des Fingerabdrucks. Es gibt sieben verschiedene Merkmalsarten. Der Finger hat durchschnittlich 30 Minuzien.

Auch die Fingerabdrücke eineiiger Zwillinge sind unterschiedlich, mögen sie sich vom Gesicht her auch noch so ähnlich sehen. Der Fingerabdruck entsteht ab der 10. Schwangerschaftswoche im Mutterleib und wird von äußeren (Mutter-inneren) Faktoren beeinflusst.

Die verwendeten Sensorarten haben einen unterschiedlich hohen Sicherheitswert. Beim *Flächensensor* wird der Finger auf den Sensor gelegt und dort gelesen. Hier kommt es bisweilen vor, dass ein latenter Fingerabdruck zurückbleibt, mit dem in einigen Fällen bereits der Scanner überlistet werden kann. Weitaus sicherer sind demgegenüber *Zeilensensoren*, bei denen der Finger über den Scanner gezogen wird. Hier kann kein latenter Fingerabdruck zurückbleiben. Zeilensensoren haben zudem den Vorteil, dass sie durch die Benutzung immer gereinigt werden und somit nicht an Leistungsfähigkeit verlieren.

**Handgeometrieverfahren** gehören zu den ältesten biometrischen Verfahren.

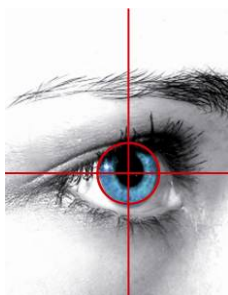


Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Für die biometrische Vermessung werden bis zu 90 Werte für Dicke, Länge, Breite und Fläche der Hand beziehungsweise der Finger gemessen.

Die Hand wird mit Hilfe von Sensoren auf einer ebenen Fläche passend ausgerichtet, so dass alle Finger weit genug gespreizt sind. Sobald alle Sensoren berührt werden, wird ein Bild (im Lesegerät, gespiegelt von einer Kamera), von oben und seitlich aufgenommen. Aus diesen Bildern werden die Konturen der Hand erzeugt. Um das Ganze möglichst genau zu machen, werden die Aufnahmen in Schwarz/Weiß umkonvertiert. Hieraus extrahiert der Rechner dann verschiedene Merkmale wie zum Beispiel die Fingerspitzen und Punkte zwischen den Fingern. Aus deren Länge wird die Maßeinheit berechnet, welche die Position weiterer Fingerbreitenmesspunkte bestimmt. Werte wie die Handbreite, Abstände und Winkel zwischen verschiedenen Interfinger-Points, Fingerkrümmung und Höhe der Handfläche und Finger werden auch noch gemessen.

Der Speicherplatzaufwand für einen Benutzer liegt je nach Verfahren zwischen 20 bis 50 Byte. Da aufgrund der Dickenmessung dreidimensionale Aufnahmen benötigt werden, sind komplizierte Optiken erforderlich. Die Sensortechnik und ihr Gesamtsystem werden daher meist recht voluminös, so dass die Technik bislang überwiegend bei der räumlichen Zugangskontrolle oder zur Zeiterfassung eingesetzt wurde. Handgeometrieverfahren haben den Nachteil, dass sie nur bei Erwachsenen beständig sind, da das Wachstum von Kinderhänden diese deutlich verändert. Zudem sind die Verfahren sehr kostenintensiv, da Großgeräte benötigt werden.

Die **Iriserkennung** ist eine Methode der Biometrie, die der Authentifizierung



von Personen dient. Dabei werden mit Spezialkameras Bilder der Iris (Regenbogenhaut des Auges) aufgenommen und mit algorithmischen Verfahren die charakteristischen Merkmale der Iris extrahiert, in numerische Werte umgewandelt und für die Wiedererkennung gespeichert. Zu den bekanntesten Templateformen zählt der Iriscode. Er beruht auf den Algorithmen des Mathematikers John Daugman.

Selbst genetisch identische Zwillinge oder das rechte und linke Auge einer einzelnen Person haben so unterschiedliche Codes wie zwei völlig verschiedene Menschen. Einmal ausgewachsen, verändern sich die Muster nicht mehr. Verfahren zur Iriserkennung werden als sehr sicher bewertet. Es ist ein zuverlässiges Identifikationsverfahren. Auch in riesigen Datenbanken mit Millionen von Personendatensätzen kann das Verfahren genutzt werden.

Um ein Iriserkennungs-System zu installieren ist eine digitale Kamera, ein Computer und die dazugehörige Software notwendig. Das Verfahren ist deshalb noch sehr kostenintensiv. Häufig wird das Verfahren von Nutzern wegen des Scanvorgangs am Auge, nicht ohne weiteres akzeptiert.

Die Methode bringt vor allem rechtliche Probleme mit sich, da sie auch passiv erfolgen kann, ohne das der Nutzer mitbekommt, dass er gescannt wird. Zudem könnten über die Iris unter Umständen Krankheitsbilder diagnostiziert werden.

**Gesichtserkennungsverfahren** werden vor allem in der Überwachung von



Plätzen, Flughäfen oder Stadien eingesetzt. Allgemein ist diese Technologie für den Einsatz an öffentlichen Plätzen mit hohem Menschenaufkommen prädestiniert. Anstatt Personen zwanghaft dazu zu bekommen, ihre Hand oder Augen auf ein Lesegerät oder vor einem Scanner zu positionieren, nehmen Kameras, unauffällig Gesichtsbilder von Personen auf, die einen bestimmten Bereich betreten, ohne das diese das überhaupt be-

merken.

Einfache Gesichtserkennungsverfahren zählen auf eine geometrische Vermessung besonderer Merkmale (wie Augen, Nase und Mund). Hierbei wird deren Position, Abstand und Lage zueinander bestimmt. Modernere Verfahren setzen jedoch meist auf komplexe Berechnungen. Es wird zwischen der Lokalisierung und der Identifikation des Gesichts unterscheiden. Bei der Gesichtslokalisierung wird geprüft, ob und wo ein Gesicht zu sehen ist und bei der Zuordnung, wer zu sehen ist.

Neben der 2D biometrischen Gesichtserkennung, die auch mit einer handelsüblichen Kamera möglich ist, gibt es auch einen neuen Weg. Dieser basiert auf der dreidimensionalen Erfassung (z.B. mittels Streifenprojektion) des Gesichts. Durch die zusätzlichen Informationen soll eine höhere Trennschärfe, bessere Posen-Unabhängigkeit und Überwindungssicherheit erzielt werden.

Die Gesichtserkennungsverfahren sind jedoch unbeständig bei Alterung der eingelesebenen Person und empfindlich gegenüber Licht- und Temperaturveränderungen. Die Möglichkeit der passiven Überwachung und die fast ebenso hohen Kosten wie bei der Iriserkennung sind weitere Nachteile dieses Verfahrens.

Durch **multiple Biometrie**, lässt sich die größtmögliche Sicherheit erreichen. Hierbei werden entweder mehrere unterschiedliche biologische Merkmale oder zwei biometrischen Merkmale der selben Art (zum Beispiel Zwei-Finger-Authentifizierung) überprüft.

## Biometrie und Datenschutz

Voraussetzung zum erfolgreichen Einsatz biometrischer Verfahren ist der Schutz der Referenzdaten. Bei ekey biometric systems wird darauf besonderes Augenmerk gelegt. Dr. Leopold Gallner, Geschäftsführer von ekey biometric systems, erläutert: „Bei den ekey-Lösungen ziehen wir Minuzien, also eine Reihe von biometrischen Auffälligkeiten des Fingerabdrucks, zur Überprüfung heran. Dabei werden die Besonderheiten auf einer Matrix dargestellt und dann in einen binären Code umgewandelt. Es ist unmöglich von dem binären Code den Fingerabdruck zu errechnen.“

### Vom Fingerabdruck zum binären Code



Ausgangsmaterial:  
Fingerbild 80.000 Byte



Ergebnis: verschlüsseltes  
Template 500 Byte

```

9b a4 68 3c eb 63 c9 09 ff 60 02 dc f5 72 23 37
00 91 21 27 dc 8c a8 2d f8 08 25 6a e7 21 01 18
56 60 0b 36 b4 b2 24 38 5a 28 6b 3b d4 d4 4d 6a
f0 75 05 44 b6 7a 39 88 88 72 3b 33 eb f4 cb 24
fa e6 a5 0a e4 67 8c 94 56 77 21 04 30 b2 25 3c
54 ac ab 27 d1 b1 c1 8a e0 7c 89 20 d7 7e 05 8f
d0 d3 24 70 53 58 aa 22 e7 ba ad 2b e0 77 0d b8
f7 70 2d b0 28 33 2b 2e 7e 84 2a 23 e4 a4 2d cc
e1 75 f7 68 b0 60 23 5f bc b4 25 21 e7 3c ad 2d
fc e1 51 ec f7 78 2b f8 b0 7a 21 58 0c 74 38 2f
f6 8c 2d 24 f2 72 fd 0c f6 63 8d 0d 37 7d 27 3e
8a 77 2f 5d 50 fa ac 4b 82 07 e9 24 52 36 3e a0
92 48 7e a0 fb d6 5c 0c bc 07 11 7f 82 66 8f 4c
c6 24 5c 7f 92 26 30 8e 82 43 0d 6d 93 25 1f 35
52 05 6a 1a a0 16 4a 0d d4 d6 5c 6c c0 34 1f 7b
f0 52 8c ae b1 34 1b 1c a0 14 77 0d 51 f7 4f 6d
d4 63 19 74 a1 59 8d af 72 04 39 1c 82 2d 79 64
de d2 b1 af 71 53 33 30 ed 40 6e 62 be 5a 8d b0
8d e8 48 44 cc 32 61 62 df d3 51 50 5f e4 03 1b
cb 36 62 64 df d3 ae 5f 5f f8 1f 6e 55 ca 90 02
57 07 41 b0 90 24 88 ac 7e 23 00 8a 83 18 5f 33
ff 1a 75 89 d3 e7 0f 8a 82 07 4d 3b f1 1c 49 89
c2 f7 0a 8a 82 06 6b 23 f6 1e 4d 89 b2 f7 0b 8e
a0 06 6b 28 d5 35 4e 0a 52 44 7f 1b d6 33 6d 6e
8a 6f 8c 2c a1 34 0d 1c a6 2b 57 09 e2 d5 1f 7c
a1 43 1f 1a 36 60 8d 5d a1 23 1b 4c 14
    
```

Um den Missbrauch von biometrischen Daten in Unternehmen zu verhindern hat ekey biometric systems in seine vernetzte Lösung, ekey net, eine zusätzliche Sicherheitsfunktion eingebaut, erklärt Gallner: „Wir haben lange selbst in einem großen Konzern gearbeitet. Daher wissen wir wie heikel Sicherheitsthemen für die Mitarbeiter sind. Deshalb kann bei aktivierter Betriebsratsfunktion der Administrator die Datenhistorie eines registrierten Benutzers nur dann ausforschen, wenn der Betriebsrat gleichzeitig anwesend ist.“

### **Fazit ekey-Produkte und Datensicherheit:**

- Der Verarbeitungsprozess funktioniert nur in einer Richtung und ist nicht vom Datensatz (Template) zum Fingerabdruck umkehrbar. Jede Transaktion erfordert somit als Ausgangsinformation den Fingerabdruck und nicht einen Code.
- Es wird kein Fingerbild, sondern bestimmte Merkmale (Minuzien) gespeichert. Aus diesen prägnanten Punkten allein könnte man auch keinen Fingerabdruck zeichnen.
- Aus dem gespeicherten Code kann deshalb kein Fingerabdruck rekonstruiert werden. Vergleichbar ist dies mit dem Barcode auf einer Verpackung im Supermarkt, aus dem auch nicht auf das Aussehen der Verpackung oder den Zustand des darin befindlichen Produkts geschlossen werden kann.
- Mit dem gespeicherten Code allein kann kein Individuum gefunden werden.
- Der Template-Datensatz ist proprietär verschlüsselt und der Schlüssel ist nur ekey biometric systems bekannt.
- Der Datensatz ist lokal gespeichert und nicht auslesbar.
- Der verwendete Algorithmus ist nicht kompatibel mit anderen Systemen.
- Bei den ekey-Systemen handelt es sich um aktive Systeme. Der Benutzer gibt freiwillig und bewusst seinen Fingerabdruck ab.
- Der Datensatz kann jederzeit gelöscht werden.

Damit wird bei ekey-Lösungen verhindert, dass die erfassten personenbezogenen Daten anderweitig und zum Nachteil einer Person genutzt werden. ekey-Fingerscan-Lösungen sind somit datenschutzrechtlich keinesfalls bedenklicher, als heute Schlüssel, Karten, Codes oder andere herkömmliche Verfahren, zu werten.