

Begrifflichkeiten im Bereich der Biometrie



Aus dem Griechischen kommend setzt sich Biometrie aus den Worten Bios = Leben und Metron = Maß zusammen. Geprägt wurde der Begriff in der Mathematik, insbesondere im Bereich der Statistik und der Medizin. Bereits 1841 verwendete Christoph Bernoulli den

Begriff „Biometrie“ für die Messung und statistische Auswertung der menschlichen Lebensdauer. Biometrie wird in diesem Bereich auch als Synonym für Biostatistik verwendet. Die Biostatistik behandelt die Anwendung statistischer Methoden zur Auswertung von Messungen aller Lebewesen. Es betrifft alle Bereiche der Lebenswissenschaften, in denen mit empirischen Untersuchungen Erkenntnisse über medizinische, biologische, psychologische oder ökologische Zusammenhänge gewonnen werden. Zudem wird Biometrie auch in der automatisierten Krankheitsdiagnose angewandt. Die Statistik, Mathematik und die Informatik bilden die Grundlage für Biometrie.

In der Technik und Informatik spricht man ebenfalls von Biometrie. Hierbei wird jedoch häufig die auf biometrischen Merkmalen basierende Identifikation in Form von Erkennungsverfahren verstanden. Alphonse Bertillon entwickelte bereits 1879 ein System (Bertillonage) zur Identitätsfeststellung, das auf 11 Körperlängenmaße basierte (Anthropometrie).

Zu unterscheiden sind demnach zunächst folgende Begriffe:

Biometrie: die biologische Statistik, Zählung und Messung von Lebewesen.

Biometrik: das automatisierte Messen von spezifischen Merkmalen eines Lebewesens.

Biometrische Identifikation: die Unterscheidung von Lebewesen aufgrund ihrer spezifischen biometrischen Merkmale.

Zu klären ist des Weiteren der Begriff der Identifikation bzw. der Identifizierung, der gerade im Bereich der Erkennungsverfahren oftmals mit dem Terminus der Verifikation einhergeht.

Identifikation / Identifizierung: das eindeutige Erkennen eines Individuums aus einer Gruppe von Personen.

Verifikation: Überprüfung der vorgegebenen Identität mit hinterlegten Basisdaten.

Biometrische Merkmale

Bereits die Assyrer in Vorderasien nutzten 2 Jahrtausend v. Chr. den Fingerabdruck zur Authentifizierung von Handelsdokumenten und auch den Chinesen war diese Technik bereits 600 n. Chr. bekannt. Selbst Leonardo da Vinci erkannte schon früh einzigartige anatomische Unterscheidungsmerkmale. Der deutsche Anthropologe Hermann Welker erforschte 1856 die Unveränderlichkeit der Haut- bzw.

Papillarleisten des Fingers. Sir Francis Galton entdeckte, dass Fingerabdrücke bei jedem Menschen verschieden sowie während des ganzen Lebens konstant sind und sich somit ebenfalls als Identifizierungsmittel eignen. Bei Scotland Yard entwickelte man daraufhin ein Klassifikationssystem für Fingerabdrücke und legte fünf Grundmuster fest. Damit gelang 1902 die erste Überführung eines Einbrechers anhand seines Fingerabdrucks.

Doch erst mit den heutigen technischen Möglichkeiten lassen sich auch komplexe biometrische Charakteristika in akzeptablem Maß automatisch nutzen und auswerten. Dabei spielen Geschwindigkeit, Datenmenge und Skalierbarkeit der Erfassungssysteme eine erhebliche Rolle. Im Gegensatz zur Forensik erfolgt bei biometrischen Verfahren die Erkennung automatisch und in Echtzeit.

Bei den biometrischen Erkennungsverfahren werden individuelle biometrische Verhaltens- und Körpercharakteristika abgeglichen:

Messbarkeit: Es müssen technische Möglichkeiten gegeben sein, um die Messgrößen mit dafür geeigneten Sensoren zu erfassen.

Universalität: Das zu erfassende Merkmal ist bei nahezu jeder Person vorhanden.

Einmaligkeit: Das zu erfassende Charakteristikum ist für möglichst alle Personen different.

Permanenz: Der Messwert ist zeitlich invariant.

Doch was sind biometrische Charakteristika? Diese werden bereits in der embryonalen Phase gebildet und sind, wie zum Beispiel die Körpergröße und die

Gesichtsgeometrie, genetisch bedingt zum Teil vererbbar. Neben den genetisch bedingten Anteilen ist eine Reihe von Zufallsfaktoren beteiligt, die sich auf das Erscheinungsbild des Menschen auswirken – diese Merkmalsentstehung nennt man randotypisch. Das Venenmuster der Retina im Auge oder die Merkmale des Fingerabdrucks. Zusätzlich gibt es noch Merkmale, die verhaltensgesteuert oder anerzogen sind. Diese können sich im Laufe des Lebens demnach auch ändern. Die Handschrift, der Gang sowie Dynamik und Rhythmus des Tastaturanschlags.

Dazu zählen:

Körpergröße (Anthropometrie)

Iris (Regenbogenhaut)

Retina (Augenhintergrund)

Fingerabdruck (Linienbild)

Gesichtsgeometrie

Handgefäß- und Venenstruktur

Handgeometrie

Handlinienstruktur

Nagelbettmuster

Stimme

Unterschrift

Tippverhalten

Lippenbewegung

Gangstil

Körpergeruch

DNA

Eine Person kann also durch Messung und Vergleich ihre spezifischen biometrischen Merkmale von anderen Personen unterschieden werden. Man unterscheidet in aktive und passive Merkmale, verhaltens-/physiologiebasierend und dynamisch oder statisch. Zur automatisierten biometrischen Identifikation sind diejenigen Merkmale am besten geeignet, die Voraussetzungen der Messbarkeit, Universalität, Einmaligkeit und Permanenz erfüllen.

Um nun eine technische Umsetzbarkeit zu gewährleisten, muss das Verfahren bei einer möglichst großen Personengruppe anwendbar sein und von diesen akzeptiert werden. Zudem müssen die Realisierungskosten im Verhältnis zur Zielanwendung stehen. Für Sicherheitskonzepte sind aber nur die Merkmale interessant, die einen Menschen hinreichend eindeutig und zweifelsfrei kennzeichnen und die weder simuliert noch verändert werden können. Dazu gehören u.a. der Fingerabdruck, die Hand- und Fingergeometrie, Stimmmerkmale, Gesichtsabmessungen, Iris und Retina.

Funktionsweise von biometrischen Systemen

Je nach verwendetem biometrischem Merkmal stehen unterschiedliche Erkennungssysteme zur Verfügung. Basis eines jeden Systems ist jedoch der „Einlernprozess“, bei dem zunächst Basisdaten als Referenzmuster ermittelt werden müssen. Dieser Registrierungsprozess (Enrolment) dient zum Erfassen der relevanten Merkmale. Diese werden in einem weiteren Schritt bearbeitet, gebündelt, und als verschlüsselter Datensatz hinterlegt. Die Templates enthalten nun die extrahierten Merkmale des Originals, bei der Spracherkennung zum Beispiel in Form eines Stimmvektors (Hashwert). Ein Hashwert lässt im Gegensatz zum Sample keine direkten Rückschlüsse auf die zugehörige Person zu noch kann eine Stimme daraus rekonstruiert werden. Ein Template bezeichnet vielmehr ein mathematisches Modell unterschiedlicher Algorithmen wogegen ein Sample z.B. die aufgezeichnete Stimme an sich oder ein Bild eines Fingerabdrucks darstellt.

Der Authentifizierungsprozess setzt sich aus Sensorermittlung, Merkmalsextraktion und Merkmalsvergleich zusammen (Videokamera, bildgebende Verfahren, Mikrofon, usw.). Der Sensor liefert umfangreiche biometrische Daten, die im Rahmen der Merkmalsextraktion gefiltert werden. Hierbei werden alle nicht geforderten Merkmalseigenschaften mit Hilfe von Algorithmen entfernt. Das Ergebnis ist das biometrische Merkmal. Der Merkmalvergleich errechnet den Vergleichswert (Score) zwischen dem in der Einlernphase gespeicherten biometrischen Template und dem gelieferten Datensatz. Dieser Vergleich liefert einen Prozentwert zurück, der die jeweilige Übereinstimmung widerspiegelt. Der eingestellte Schwellwert entscheidet über die erfolgreiche Erkennung. Wird ein hoher Schwellenwert definiert, muss der ermittelte Datensatz näher am Vergleichswert liegen. Ist der Schwellenwert niedrig gewählt, können etwaige Abweichungen größer sein. Bei einer Identifikation bildet das System so lange Teilmengen aus der Gesamtmenge der Templates, bis ein einziger oder gar kein Treffer (Match) übrig bleibt. Bei einer Verifizierung ist das Ergebnis des Vergleichs entweder ein Treffer oder kein Treffer, was zu Akzeptanz oder Rückweisung der Person führt.

Wie zuverlässig ein System arbeitet, wird anhand zweier Kriterien beurteilt:

Falschakzeptanz (FAR): der Zulassungsrate Unberechtigter. Die FAR gilt als Sicherheitsmerkmal. Je kleiner ihr Wert ist, desto sicherer ist das System.

Falschrückweisungsrate (FRR): die Abweisungsrate berechtigter Personen. Die FRR gilt als Komfortmerkmal. Je kleiner ihr Wert ist, desto komfortabler ist das System.

Die Falschakzeptanz steigt bei der Identifizierung in der Regel stark an, da hier ein Merkmal mit vielen anderen Merkmalen aus der Datenbank verglichen wird. Die Wahrscheinlichkeit steigt also, dass einer nicht-berechtigten Person fälschlicherweise eine Berechtigung zugewiesen wird. Um eine Aussage über die Zuverlässigkeit des Systems machen zu können, müssen beide Werte in Relation zueinander gesetzt werden. Sind beide Werte gleich groß, spricht man von der Equal Error Rate (EER).

Eine Herausforderung der biometrischen Erkennungssysteme liegt darin, dass nicht eine Gleichheit der Merkmale, sondern nur eine hinreichende Ähnlichkeit berechnet wird. Denn die Merkmale werden jedes Mal neu erfasst, welches immer zu Abweichungen führt. Es werden andere Sensoren verwendet oder Hintergrundgeräusche, Beleuchtung, Verletzungen ändern und verzerren das biometrische Merkmal. Hinzu kommen natürliche, wachstums- oder altersbedingte Veränderungen des Körpers. Da also die gewonnenen biometrischen Merkmale nie gleich sind, wird mit prozentualen Ähnlichkeitswerten gearbeitet. Selbst beim Enrolment kann es zu Messfehlern kommen, z.B. durch einen defekten oder ungenau kalibrierten Sensor oder durch eine nicht sachgemäße Bedienung oder Störgeräusche. Die so entstehenden Ungenauigkeiten muss das biometrische System ausgleichen. Dies kann durch Anpassung des Schwellwertes, Optimierung des Template-Algorithmus und anderer Faktoren erfolgen.

Je schärfer ein System jedoch konfiguriert wird desto höher ist die Falschrückweisungsrate, das Optimum richtet sich nach dem Einsatzbereich. Nicht zu vernachlässigen ist auch der Umstand, dass eine zu hohe

Falschrückweisungsrate auch einen psychologischen Faktor einschließt: Die Akzeptanz beim Nutzer sinkt, wenn er fälschlicherweise permanent vom System abgelehnt wird.

Es gibt prinzipiell so viele verschiedene biometrische Vermessungsmöglichkeiten zur Identifikation und Authentifizierung, wie es Möglichkeiten gibt, Menschen eindeutig voneinander zu unterscheiden oder zu erkennen. Zusätzlich sind auch Kombinationen der einzelnen Merkmale innerhalb eines Verfahrens möglich. Es gilt, das passende Verfahren für den jeweiligen Einsatzzweck zu bestimmen. Hauptaugenmerk soll in diesem Fall aber auf die Stimme gelegt werden.

Die Stimme

Bei der Spracherkennung geht es um den Inhalt des Gesprochenen, wogegen sich die Stimmenerkennung mit dem sprechenden Individuum befasst. Die Stimmenerkennung stellt kein visuelles Verfahren dar, sondern versucht, die Stimme akustisch zu vermessen. Das Sprachsignal als solches stellt eine Überlagerung von Wellen verschiedener Frequenzen dar. Dabei spielen die artikulatorische Phonetik (Aufbau und Funktion des Sprechapparats, Produktion von Sprache) und die akustische Phonetik (physikalische Struktur des Sprachschalls) eine Rolle. Die Stimmenerkennung kommt dem natürlichen Sprechgebrauch des Menschen entgegen und macht sie zu einem einfach zu bedienenden Mittel - sogar aus weiter Entfernung, z.B. per Mobiltelefon. Die Stimme ist z.T. genetisch bedingt, weist jedoch auch erlernte Merkmale auf. Bei Stimmenerkennungsverfahren werden ca. 3.000 Merkmale extrahiert. Physiologische Unterschiede können die Stimme verändern, u.a. die Länge der Stimmbänder, die Größe des Kehlkopfes oder letztlich das Volumen des Resonanzkörpers. Betonung und Artikulation können zu einer Verzerrung im Sinne der Stimmenerkennung beitragen. Eine Veränderung der Stimme durch Krankheit ist nicht ausgeschlossen und trübt ebenfalls den Eindruck einer verlässlichen Methode.

Grundlage dieser Technik bilden die Spracherkennungssysteme der 1970er Jahre. Spracherkennung und Stimmenerkennung unterscheiden sich in den jeweiligen Einsatzgebieten. Die zugrunde liegenden Algorithmen zur Aufbereitung basieren meist auf ähnlichen Methoden. Die weitere Extrahierung der relevanten Merkmale funktioniert jedoch verschieden. Als Eingabe dient ein Mikrofon, wobei mithilfe eines Tiefpassfilters o.ä. Störgeräusche entfernt werden müssen. Da Menschen oft eine unterschiedlich laute Aussprache haben und die Entfernung zum Mikrofon nicht immer identisch ist, sollte zunächst noch die Lautstärke normalisiert werden. Daraufhin wird bei Test und Referenzmuster die Stille am Anfang und am Ende entfernt, um eine Vergleichbarkeit zu gewährleisten. Wie bei allen biometrischen

Verfahren werden nach diesen Schritten die Merkmalsvektoren extrahiert, um dann eine Identifikation oder Verifikation zuzulassen.

Die erfassten Sprachsignale werden in kleine Stücke zerteilt und Stück für Stück analysiert. Ein einfaches Signal, z.B. eine Sinuskurve, besteht nur aus zwei Komponenten: der Amplitude (der Spannungsausschlag auf der Y-Achse) und der Frequenz (dem Reziproken der Periodendauer von Peak zu Peak). Jean Baptiste Joseph Fourier fand im 18. Jahrhundert heraus, dass sich jedes beliebige Signal durch die Summe aus unter Umständen unendlich vielen einzelnen Sinus- und Kosinuskurven darstellen lässt. Vereinfachen lässt sich das Verfahren, wenn man sich die Kurven im "Frequenzbereich" ansieht. Hier stellt sich die Sinuskurve lediglich als ein kurzer Ausschlag der Höhe A bei der Frequenz $f_0 = 1/T_0$ dar. Diese Übertragung des Signals aus dem Zeitbereich in den Frequenzbereich (auch Spektralbereich genannt) bezeichnet man als "Fourier-Transformation". Die Fourier-Transformation des Zeitsignals nennt man "Spektrum". Digital realisiert man das mit der so genannten "Fast-Fourier-Transformation", kurz FFT. Grundsätzlich gibt es zwei verschiedene Methoden der Analyse eines Sprachlauts: Entweder wird das Signal im Zeitbereich untersucht; dabei betrachtet man den Amplitudenverlauf über der Zeit, oder man analysiert das Signal im Frequenzbereich. Es gibt auch Mischformen - zum Beispiel die in der Stimmanalyse besonders relevanten Cepstral-Analyse, bei der Zeit- und Frequenzanalysen miteinander kombiniert werden. Hierdurch sind harmonische Anteile im Signal deutlich zu erkennen und Hall und Echo werden gefiltert.

Die Stimmenerkennung wird größtenteils als positiv empfunden und gestaltet sich als sehr einfach; man könnte sie auch in absoluter Dunkelheit und über weite Entfernungen hinweg durchführen. Probleme treten häufiger durch Störgeräusche auf. Altersbedingte Veränderungen der Stimme fangen die Anwendungen durch Nachkalibrierung des Templates ab. Trotz der breiten Akzeptanz, derer sich die Stimmenerkennung erfreut, wäre eine Täuschung durch vorherige Aufnahme von Phrasen unter Umständen zu bewerkstelligen, sodass oft zusätzlich ein geheimer Frage-Antwort Katalog oder eine Ziffernabfrage in Zufallsreihenfolge hinzugezogen

wird. Dadurch müsste der Betrüger die passenden Antwortkonserven bereits kennen, was sich bei entsprechender Diskretion als recht schwierig erweisen kann. Zudem sind die Antwortzeiten entsprechend limitiert, die passende Konserve in der kürze der Zeit bereitzustellen stellt eine extreme Herausforderung dar. In Verbindung mit einer solchen Methode „ist das System nahezu unüberwindlich“.

Anwendungsmöglichkeiten

Es ist sicherlich wesentlich benutzerfreundlicher, sich mithilfe seiner persönlichen biometrischen Merkmale zu identifizieren und authentifizieren, als mithilfe komplizierter Passwörter, PIN, TAN oder Dokumenten und ID-Cards, die man immer griffbereit haben muss. Die biometrischen Verfahren sind längst serienreif und praxistauglich. Analysten erwarten eine Nachfragesteigerung entsprechender Lösungen von rund 15 bis 20 Prozent. Auch Verbraucher verlangen eine erhöhte Sicherheit und eine hohe Benutzerfreundlichkeit und Servicequalität.

Biometriesysteme unterstützen bereits heute Unternehmen, Behörden und öffentlichen Einrichtungen, Personen sicher und schnell zu identifizieren. Gerade der Bereich der Stimmerkennung lässt aufgrund seiner flexiblen und mobilen Einsetzbarkeit (per Festnetz, Voice over IP, Mobiltelefon) ein breites Einsatzspektrum zu.

So hat jeder fünfte Anrufer bei einem Helpdesk seine Zugangsdaten vergessen. Für den kompletten Vorgang des Rests rechnet man rund 30 Minuten. Mit einer Voice-Lösung lässt sich der gleiche Vorgang in knapp drei Minuten lösen. Zudem erhöht sich der Sicherheitsaspekt deutlich, denn das Prinzip „Haben und Wissen“ wird mithilfe des biometrischen Merkmals „Stimme“ umgangen.

Auch der Einsatzbereich im kriminalistischen Bereich stößt auf großes Interesse. Von der Identifikation von Straftätern durch das biometrische Stimmerkennmerkmal bis hin zu Kontrollfunktionen wie einem verfügten „Hausarrest“. Auch zur Verhinderung von Sozialmissbrauch wäre eine Verifikation mittels Stimmerkennung vorstellbar. Weitere staatliche Einsatzmöglichkeiten wären auch bei der Identifikation zur Wahlberechtigung möglich.

Denkbar sind auch alle Anwendungen, die auf eine Zugangs- bzw. Zugriffssicherung basieren, wie der Dokumentenschutz, Telefon- und Homebanking, Freischaltungsvorgänge, Auskünfte über sensible Daten und alle Bereiche der Gebäudesicherheit.

Ein weiterer Einsatzbereich stellt auch die Möglichkeit der Personalisierung dar. Individuelle Dienste, Konfiguration technischer Geräte, personenbezogene Einstellungen und sogar die Nutzung für individualisierte Marketingaktionen sind denkbar.

Datenschutz und Sicherheit

Ein biometrisches Merkmal lässt sich nicht, wie etwa ein Passwort, auswechseln. Deshalb spielen die Sicherheit und der Datenschutz in diesem Bereich eine erhebliche Rolle. Es existieren bereits Verfahren zur automatisierten Kopierererkennung. Im Fall der Spracherkennung spielen Methoden zur Lebenderkennung keine Rolle wie bei Fingerabdruck oder Handlinienstruktur. Die Verwendung von Sprachkonserven wird durch eine Zufallsabfrage von Ziffern oder Wörtern verhindert. Definierte Antwortzeiten auf diese Zufallsabfragen machen eine Suche nach der richtigen Sprachkonserve nahezu unmöglich. Einem Mitschnitt bei der Datenübertragung wird mit Techniken wie ein verschlüsseltes VPN (Virtual Private Network) entgegengewirkt.

Da die als Templates gespeicherten Vergleichswerte nur die extrahierten Merkmale enthalten des Originals in Form eines Stimmvektors enthalten, lassen sich daraus auch keine Rekonstruktionen der Originalstimme erstellen und missbräuchlich verwenden. Biometrische Zugriffssysteme tragen demnach dem Verlangen von Unternehmen und Privatpersonen gerade in Telefon- und Internetanwendungen Rechnung. Dem Ausspionieren von Zugriffsdaten wie Passwort und Sicherheitsabfragen (Geburtsdatum, Mädchenname der Mutter, Haustier), das mit Hilfe von Trojanern oder im Rahmen von Social Networks immer mehr Verbreitung findet, wird mit Biometrie-Anwendungen entgegengewirkt.

Natürlich unterliegen auch biometrische Authentifikationssysteme den datenschutzrechtlichen Bestimmungen zu personenbezogenen Daten, da sich die verwendeten biometrische Merkmale meist im Laufe des Lebens nicht mehr verändern. Sie unterliegen demnach dem Selbstbestimmungsrecht und der Entfaltungsfreiheit.

- Die Verwendung personenbezogener Daten ist nur mit Einwilligung oder einer Rechtsverordnung zulässig. Eine Einwilligung ist selbstverständlich widerruflich.

- Personenbezogene Daten müssen verschlüsselt oder allein im Nutzerbereich abgespeichert werden, wo selbst der Betreiber sie nicht im Klartext lesen kann.
- Personenbezogene Daten dürfen nur zweckgebunden zu den vorab definierten Bestimmungen verwendet werden.
- Personenbezogene Daten dürfen nur in dem Umfang erhoben und verarbeitet werden, in dem es zur Erreichung des Verwendungszwecks erforderlich ist.
- Die betroffene Person hat das Recht zu wissen, welche Daten und zu welchem Zweck erhoben werden und was mit diesen Daten geschieht. Sie haben das Recht zur Berichtigung, Sperrung und Löschung.
- Personenbezogene Daten dürfen nicht bei Dritten erhoben werden, Ausnahmen bedürfen der gesetzlichen Regelung.
- Die verantwortlichen Stellen haben die technischen und organisatorischen Maßnahmen nach dem Bundesdatenschutzgesetz zu treffen.

Literatur

Michael Behrens, Richard Roth „Grundlagen und Perspektiven der biometrischen Identifikation“

Bundesamt für Sicherheit in der Informationstechnik „Grundsätzliche Funktionsweise biometrischer Verfahren“

Andreas Gutsche, Marina Trierscheid „Grundlagen der Biometrie“

Fraunhofer Institut „Biometrie-Benchmark“

Teletrust Deutschland e.V. „Datenschutz in der Biometrie“

Oliver Weiss „Now you ´re talking! “

Markus Wolschon „Praxistaugliche Biometrie und RFID“