Biometrienicht nur in der Strafverfolgung

Einsatzmöglichkeiten von Sprachbiometrielösungen

Biometrie ein alter Hut?

Schon vor über 100 Jahren diente der Fingerabdruck bei Scotland Yard zur Überführung eines Einbrechers. Basierend auf den Forschungen des deutschen Anthropologen Hermann Welker, der 1856 die Unveränderlichkeit der Haut- bzw. Papillarleisten des Fingers erforschte, gelang dem Briten Sir Francis Galton erstmals die kriminalistische Nutzung dieses biometrischen Merkmals: Er entdeckte, dass Fingerabdrücke bei jedem Menschen verschieden sowie während des ganzen Lebens konstant sind und sich somit als Identifizierungsmittel eignen.

Kerstin-Alexandra Zeller
Freie Journalistin

Daraufhin entwickelte man ein Klassifikationssystem für Fingerabdrücke und legte fünf Grundmuster fest. Die Biometrie hatte sich also das erste Mal im Rahmen der Strafverfolgung bewährt und eine Täterüberführung überhaupt erst ermöglicht.
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. 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. Der Begriff der Identifikation bzw. der Identifizierung geht gerade im Bereich der Erkennungsverfahren oftmals mit dem Terminus der Verifikation einher, unterscheidet sich jedoch deutlich. Während Identifikation bzw. Identifizierung das eindeutige Erkennen eines Individuums aus einer Gruppe von Personen beschreibt, versteht man unter Verifikation eine Überprüfung der vorgegebenen Identität mit hinterlegten Basisdaten.

Gereon Tillenburg
Geschäftsführer der
TWINSOFT GmbH & Co. KG

Doch erst mit den heutigen technischen Möglichkeiten lassen sich auch komplexe biometrische Charakteristika in akzeptablem Maß automatisch für forensische Zwecks nutzen und auswerten. Dabei spielen Geschwindigkeit, Datenmenge und Skalierbarkeit der Erfassungssysteme eine erhebliche Rolle. Denn bei biometrischen Verfahren läuft die Erkennung automatisch und in Echtzeit.

Was sind biometrische Charakteristika?

Diese nahezu unveränderlichen körperlichen Merkmale 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. 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
- Ohr

• Stimme
• Unterschrift
• Tippverhalten
• Lippenbewegung
• Gangstil
• Körpergeruch
• DNA

Eine Person kann also durch Messung und Vergleich ihrer spezifischen biometrischen Merkmale von anderen Personen unterschieden werden. Man spricht von 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.

Stimmt die Stimme?

Für Identifikationsverfahren im kriminaltechnischen Sinn sind 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 Handgeometrie, Stimmmerkmale oder die Retina. Gerade für polizeiliche Ermittlungsarbeiten eignet sich neben dem klassischen Fingerabdruck die Stimme zur Identifizierung, Einengung und Überführung von möglichen Tätern. Denn die Stimme lässt sich auch auf eine weite Entfernung hin, sogar via Telefon und Sprechanlage analysieren und identifizieren. Und selbst eine leichte Heiserkeit oder eine verstellte Stimme sind bei dem heutigen Stand der Technik kein Problem. Der Versuch zeigt, dass sogar bei Verwendung einer Fremdsprache eine Zuordnung möglich ist. Kollegen des Landeskriminalamtes konnten sich quasi selbst „überführen„: Die Software „TWINSOFT Identifier„ hat die Testperson selbst mit verstellter Stimme einwandfrei und unter Nutzung einer Fremdsprache mit hoher Wahrscheinlichkeit dem Referenzmuster der Testdaten zugeordnet. Die Identifikation per Stimme bietet damit eine enorme Zeitersparnis, denn ein Kreis von Verdächtigen kann alleine mit Stimmproben auf ein Minimum eingegrenzt werden. Wertvolle Zeit, die unter Umständen Leben retten kann.


Stimmerkennung ist eine kosten- und zeiteffiziente Technologie, die für die Zukunft interessante zusätzliche Optionen eröffnet (Foto: Hofem)

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, wie zum Beispiel der Fingerabdruck bei AFIS, dem Automatisierten Fingerabdruckidentifizierungssystem oder bei EURODAC (European Daktyloscopy). Dieser Registrierungsprozess (Enrolment) dient zum Erfassen der relevanten Merkmale. Die erfassten Daten 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 Merkmalvergleicher 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. 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.

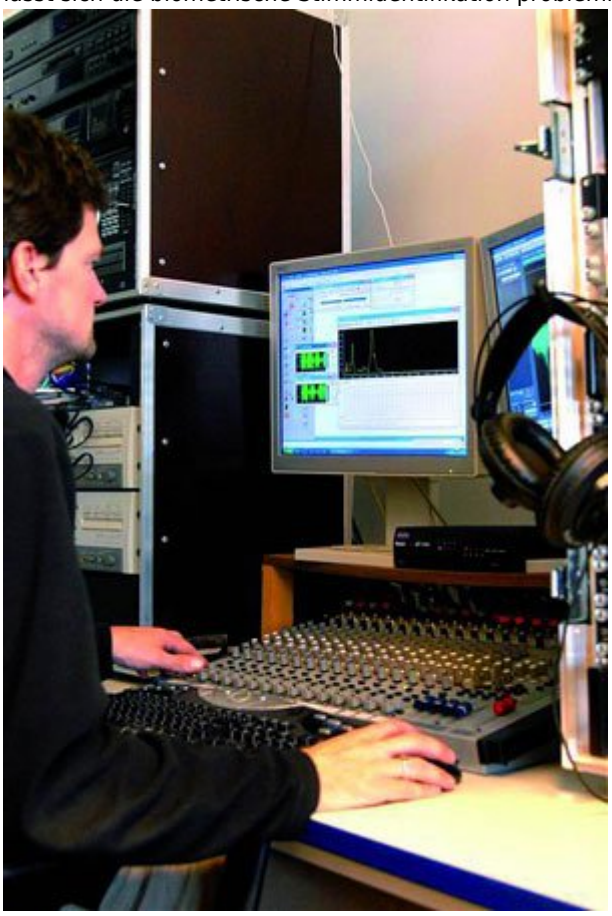
Wie funktioniert das bei der Stimme?

Bei Stimmerkennungsverfahren 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. Da aber die Ermittlungsarbeiten zumeist in einem eingegrenzten Zeitraum stattfinden, relativieren sich diese Einflussfaktoren auf ein Minimum. Um eine Stimme identifizieren zu können, muss zunächst auch hier ein Vergleichswert vorliegen. Es werden also Basisdaten als Referenzmuster ermittelt. Die erfassten Stimmmuster, die beispielsweise durch Mitschnitte von Telefongesprächen aufgezeichnet werden können, werden gebündelt, und als verschlüsselter Datensatz in einer Datenbank hinterlegt. Sie enthalten nun die extrahierten Merkmale des Originals in Form eines Stimmvektors (Hashwert).
Mithilfe eines Tiefpassfilters werden Störgeräusche entfernt und die Lautstärke normalisiert. Dann wird bei Test- und Referenzmuster die Stille am Anfang und am Ende entfernt, um eine Vergleichbarkeit zu gewährleisten (Merkmalsextraktion). Wie bei allen biometrischen Verfahren werden nach diesen Schritten die Merkmalsvektoren extrahiert, um dann eine Identifikation aufgrund des Vergleichs von Test- und Referenzmuster zuzulassen.

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 oder chirurgische oder kosmetische Eingriffe. 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. Deshalb sind die gewonnenen biometrischen Merkmale nie gleich und es kann nur mit Ähnlichkeitswerten gearbeitet werden. Die Analyse liefert also eine Rankingtabelle der hinterlegten Stimmmuster. Diese kann dann vom jeweiligen Ermittlerteam dem vorgegebenen Ranking entsprechend abgearbeitet werden – willkürliches Fischen im Verdächtigentümpel entfällt.
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.

Sprachbiometrie praxistauglich?

Das man mit AFIS schon seit 1993 eine Biometrielösung – nämlich den Fingerabdruck – nutzt, ist den meisten Kollegen eine Selbstverständlichkeit. Wie jedoch soll das bei der Stimme funktionieren? Im Prinzip mit genau den gleichen Mitteln, quasi mit einer angelegten Stimmdatenbank. Mithilfe des vom „TWINSOFT Identifier„ erstellten Rankings kann bei Ermittlungsarbeiten die Zahl der Verdächtigen deutlich eingeschränkt und vor allem objektiv priorisiert werden. Die Einsatzmöglichkeiten sind vielfältig: Terrorprävention, Täterermittlung, Erpressung, usw. Auf jeden Fall stellt die Stimmerkennung eine kosten- und zeiteffiziente Technologie dar. Gerade bei Ermittlungsarbeiten im Rahmen der Terrorprävention wäre die eindeutige Identifikation per Stimmerkennung ein hervorragendes Fahndungsmittel. Vorab erhaltene Botschaften per Video, Drohanrufe oder Mitschnitte per Internet liefern den nötigen Referenzdatensatz. Werden nun Verdächtige ins Visier genommen, kann mittels Stimmabgleich festgestellt werden, ob es sich um die gesuchte Person handelt. Hier ließe sich eine ganze „Terror-Datenbank„ – wie bei Fingerabdrücken schon vorhanden – anlegen und entsprechend abgleichen.
Auch für den Einsatz am Flughafen eignet sich die Stimm-analyse zur Identifikation einer Person. Gibt der Fingerabdruck kein einwandfreies Ergebnis, bietet die Stimme ein zusätzliches biometrisches und somit eindeutiges Merkmal. Täuschungen rein optischer Systeme durch „Gummifinger„ oder Abfotografieren bei 2D-Gesichtserkennungssystemen werden damit ausgeschlossen. Auch bei Großveranstaltungen mit hohem Sicherheitsstatus (G8-Gipfel, Staatsbesuche, usw.) lassen sich per Stimmanalyse mögliche Verdächtige entweder gleich durch eine Kontrolle im Eingangsbereich oder aber durch gezielte Auswahl eines bestimmten Personenkreises mit geringem Personal- und Technikeinsatz überprüfen. Selbst bei verdeckten Ermittlungen lässt sich die biometrische Stimmidentifikation problemlos einsetzen. Die Praxistauglichkeit wurde bereits unter Beweis gestellt.



Ein Kreis von Verdächtigen kann alleine mit Stimmproben auf ein Minimum eingegrenzt werden (Foto: Hofem)

Selbst im Rahmen der internen Verwaltung liefern Sprachbiometriesysteme gute Dienste – denn auch hier erleichtern sie den Passwortreset oder regeln sicher Zugriffsrechte auf sensible Daten. 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„ ersetzt.Denkbare Zukunftsmusik: Lebenderkennung in Entführungsfällen. Mithilfe hinterlegter Sprachmuster könnte leicht überprüft werden, ob ein Entführungsopfer noch am Leben ist. Per Telefon könnte sich das Opfer verifizieren. Eine Aufzeichnung der Stimme seitens der Entführer ist nutzlos, da die Verwendung von Sprachkonserven durch eine Zufallsabfrage von Ziffern oder Wörtern verhindert wird. Definierte Antwortzeiten auf diese Zufallsabfragen machen eine Suche nach der richtigen Sprachkonserve nahezu unmöglich. Vielleicht eine gute Zukunftsinvestition für gefährdete Personen.