HUMBOLDT-UNIVERSITÄT ZU BERLIN

Institut für Informatik

Sommersemester 2005

Seminar Biometrie im Kontext

Vergleich biometrischer Verfahren

Andreas Dittrich

Diese Seite ist mit Absicht leer gelassen worden.

Inhaltsverzeichnis

Diese Seite ist mit Absicht leer gelassen worden.

Biometrische Systeme spielen in der heutigen politischen Diskussion über grundlegende Probleme der Identitätssicherung eine immer wichtiger werdende Rolle. Die Bewertung reicht von der reinen Verteufelung bis zur Allzweckwaffe, beide Einschätzungen sind als zu undifferenziert abzulehnen. Dennoch gibt es de facto noch keinen Standard für ein allgemeines Vorgehen beim Vergleich der Systeme; man lebt von Herstellerinformationen oder politischen Willenserklärungen. In diesem Bericht werden deswegen die gebräuchlichsten biometrischen Verfahren hinsichtlich ihrer benutzten Merkmale kategorisiert und deren grundsätzliche Eigenschaften erläutert. Abschließend wird die Praxistauglichkeit der Verfahren beim jetzigen Stand der Technik erörtert.

Einteilung der Merkmale

Aktive Merkmale

Als die Menge aller aktiven Merkmale werden alle diejenigen Merkmale bezeichnet, welche verhaltensabhängig sind und eine aktive Mitarbeit des zu vermessenden Objekts erfordern. Die populärsten Vertreter sind sicher die Hand- und Unterschriftenerkennung. Hier werden sowohl der Schriftzug mit Druck- und Geschwindigkeitsverlauf, als auch die Syntax des Geschriebenen überprüft, so sind auch rein optische Überprüfungen möglich. Ebenfalls verbreitet ist die Stimmerkennung, also die Erkennung des Klangbildes oder der Aussprache des menschlichen Sprachorgans. Diese beiden Methoden sind in der Praxis zu unterscheiden, da letztere auch eine semantische Analyse des Gesprochenen beinhaltet. Im weiteren Kreis der nutzbaren Merkmale finden sich weiterhin das Tippverhalten auf einer Computer-Tastatur, also die Kombination der Anschlagsgeschwindigkeit und der Stärke des Tastendrucks. Auch Gesichtsmimik von Personen ist messtechnisch erfassbar und überprüfbar. Naturgemäß weisen aktive Merkmale eine große Varianz auf: Verhaltensabhängige Charakteristiken ändern sich signifikant im Laufe eines Lebens, besonders deutlich wird dies zum Beispiel bei der Handschrift.

Passive Merkmale

Die Menge der passiven Merkmale umfasst alle messtechnisch erfassbaren physiologischen Eigenschaften des menschlichen Körpers und seiner Teilobjekte. Prominentester Vertreter dieser Klasse ist der Fingerabdruck, welcher seit Ende des vorletzten Jahrhunderts mit Erfolg in der Kriminalistik angewandt wird. Hier werden das Fingerlinienbild und die Porenstruktur der Fingerkuppen vermessen. Im Hochsicherheitsbereich immer öfter verwendet wird die Iriserkennung, also die Erfassung und der Vergleich der Regenbogenhaut um die Pupille herum. Weniger gebräuchlich sind Überprüfungen der Hand- und/oder Fingergeometrie, was sowohl die Finger- und Handballenmasse beinhalten kann, als auch die Venenstruktur auf dem Handrücken. Selten im Einsatz befinden sich Verfahren, welche die Blutgefäße auf der Retina im Augeninneren untersuchen.

Immer populärer wird es, die Kodierung der DNA als Träger der menschlichen Erbanlagen zum biometrischen Vergleich zu benutzen.

Entstehung der Merkmale

Entscheidend für die Eignung eines Merkmals ist oft der Ursprung der Ausprägung. Die verschiedenen Entstehungsarten sind im Folgenden aufgelistet.

Genotypische Merkmale sind im Erbgut enthaltene Eigenschaften der untersuchten Körperteile. Sie können sowohl vererbt sein, als auch durch zufällige Mutationen des Erbmaterials entstehen. Randotypische Merkmale bilden sich durch den Einfluss zufälliger Prozesse während des Wachstums des Embryos im Mutterleib. Konditionierte Merkmale schließlich sind erlernte Verhaltensweisen, welche sich durch Training über einen bestimmten Zeitraum herausgebildet haben.

Keines der bisher genannten Merkmale ist zu allen Teilen einer der drei Ursprungsformen zuzuordnen. Den Einfluss der verschiedenen Arten stellt die folgende Tabelle dar:

	konditioniert	randotypisch	genotypisch
DNA	o	o	**ooo**
Gesicht	o	o	**ooo**
Retina	o	**ooo**	o
Iris	o	**ooo**	o
Handgeometrie	o	o	**ooo**
Fingerabdruck	o	**ooo**	o
Stimme (Klang)	oo	o	**ooo**
Tastenanschlag	**ooo**	o	o
Schrift	**ooo**	o	oo

Tabelle 1: Entstehungsarten biometrischer Merkmale[1]

Die Entstehungsarten haben unterschiedliche Einflüsse auf die Verwertbarkeit des Merkmals. Rein genotypisch entwickelte Eigenschaften weisen zum Beispiel nicht die erforderliche Zufälligkeit auf und können nicht nur bei eineiigen Zwillingen, sondern auch in der näheren Verwandtschaft messtechnisch identisch sein. Ebenso kritisch zu betrachten sind rein beziehungsweise stark konditionierte Merkmale, welche unter den meisten Umständen auch von anderen erlernt werden können. Als Beispiel seien hier die verschiedensten Handschriftenfälschungen der letzten Jahrhunderte genannt. Außerdem sind konditionierte Merkmale stark abhängig von äußeren und inneren Einflüssen während des Messvorgangs. Zufällige – randotypische – Anteile in der Entstehungsform sind somit unverzichtbar für die Anwendung eines Merkmals in Bereichen der Identifikation und Verifikation, nur sie garantieren die hinreichende Einzigartigkeit. Die randotypische Entstehung eines Merkmals lässt sich etwa durch seine fehlende Korrespondenz zur Körper-

[1] Tabellenwerte nach Bromba, Dr. Manfred: Bioidentifikation – Fragen und Antworten; http://www.bromba.com/faq/biofaqd.htm#entstehen [Stand 10.7.2005]

symmetrie erkennen: Das Irismuster ist bei beiden Augen unterschiedlich, ebenso die Fingerlinienbilder.

Merkmalseigenschaften

Um überhaupt als biometrisches Merkmal angewandt werden zu können, müssen verschiedene, grundsätzliche Eigenschaften erfüllt sein. Diese umfassen die Universalität, Einzigartigkeit, Beständigkeit und Erfassbarkeit. Das Merkmal muss also bei jedem Menschen vorhanden sein, es muss sich ausreichend von allen anderen unterscheiden, im Laufe des Lebens darf es sich nicht oder nur minimal verändern und schließlich muss es messtechnisch erfassbar sein. Vorab sei erwähnt, dass beim heutigen Stand der Technik keines der aktuell genutzten Merkmale alle diese Kriterien vollständig erfüllt, sei es durch prinzipielle Unzulänglichkeiten oder Probleme in der praktischen Umsetzung. Vom Idealfall ausgehend, wird im Folgenden hauptsächlich auf die Nachteile der verschiedenen Methoden bezüglich dieser vier Basiseigenschaften eingegangen werden.

Universalität

Grundsätzlich gilt: Jedes einzelne biometrische Merkmal ist bei bis zu fünf Prozent der Bevölkerung nicht erfassbar und wenige Merkmale sind schon von Geburt an vorhanden. So prägt sich die Geometrie der Gesichtszüge erst verhältnismäßig spät aus und auch die Handgeometrie ist erst im Erwachsenenalter vollständig ausgeprägt. Andererseits gibt es Merkmale, bei denen der soziografische Hintergrund des zu vermessenden Individuums eine große Rolle spielt. Das Tippverhalten auf einer Rechnertastatur lässt sich sinnvoll nur bei geübten Schreibern verwenden.

Einzigartigkeit

Die Empfindlichkeit der benutzten Messinstrumente schafft prinzipielle Probleme bezüglich der Einzigartigkeit eines Merkmals. Auch wenn wir davon ausgehen können, das jedes Charakteristikum in der Realität einzigartig ist: Eine absolute

Genauigkeit beim Messvorgang und eine beliebig hohe Auflösung des Messergebnisses ist nicht möglich. Somit ist de facto kein Merkmal messtechnisch einzigartig. Die dadurch entstehende Problematik lässt sich mathematisch in folgender Fragestellung darstellen: Wie viele Personen *n* sind nötig, damit bei einer bestimmten Anzahl technisch unterscheidbarer Daten *m* das Auftreten zweier Personen mit gleichem Merkmal wahrscheinlich ist, also die Wahrscheinlich größer als 0,5 ist? Folgende Formel berechnet die Funktion:

$$n = \frac{1 + \sqrt{1 + (8 \ln 2) m}}{2}$$ [2]

Mit heutiger Technik sind etwa 300 Millionen unterschiedliche DNA-Abdrücke messbar. Daraus ergibt sich, dass nur etwa 20000 Personen nötig sind, damit das Auftreten zweier identischer Merkmale wahrscheinlich ist. Die Charakteristik der genannten Formel verbessert dieses Verhältnis bei 300 Milliarden unterschiedlichen Abdrücken nur geringfügig, man braucht nur etwa 200000 Personen um das gleiche Verhältnis zu erhalten. Anders ausgedrückt: Um wahrscheinlich kein doppeltes Merkmal unter der gesamten Menschheit mit einer angenommenen Bevölkerung von sechs Milliarden Menschen zu erhalten, müssten etwa 26 Trillionen Kennzeichen unterschieden werden können. Dies scheint auf den ersten Blick weit hergeholt, bei Massenanwendung, wie der Auslieferung biometrischer Pässe stellt sich jedoch genau dieses Problem.

Dennoch lässt sich das eben genannte Problem in speziellen Fällen relativieren. Zum Beispiel wird in Bereichen der Strafverfolgung meist eine bestimmte Merkmalsausprägung gesucht, die Formel hierfür lautet entsprechend:

$$n = \frac{m}{2}$$

Ergänzend zum Beispiel der DNA seien noch Klone und eineiige Zwillinge erwähnt, welche am Anfang ihres Lebens das gleiche Ausgangs-Erbmaterial besitzen; die Vererbung ist eine prinzipielle Schwachstelle. Manche Merkmale sind

---

[2] nach Dr. Claudia Eckert: IT-Sicherheit. Konzepte – Verfahren – Protokolle. Oldenbourg Verlag München Wien, 2005, Seite 183f.

zudem schwer oder nur mit hohen Toleranzen aufzunehmen, was gleichzeitig die theoretische Einzigartigkeit vermindert. Beispiele hierfür sind die Gesichtserkennung, welche hohe Toleranzen verarbeiten muss oder etwa die Vermessung der Handgeometrie, hier ist das Merkmal schlichtweg nicht vielfältig genug. Positiv seien die Iris oder die Blutgefäße auf der Retina erwähnt, welche eine extrem hohe Vielfalt aufweisen und sich somit besonders für Anwendungen im Hochsicherheitsbereich eignen.

Beständigkeit

Um den langfristigen Einsatz eines biometrischen Kennzeichens zu sichern, sollte es eine minimale zeitliche Varianz seiner Eigenschaften aufweisen. Diese Varianzen können verschiedenste Ursachen haben: Das menschliche Wachstum und auch die natürlich Alterung verändern die meisten Merkmale mit der Zeit. Abnutzung, Verschmutzung und Verletzungen sind ebenfalls große Fehlerquellen. Diese Einflüsse können sowohl die Messbarkeitseigenschaften verschlechtern, aber auch zu temporären oder permanenten Ausfällen führen.

Temporär beschränkte Ausfälle wären zum Beispiel eine neue Brille, welche die Gesichtserkennung fehlschlagen lässt oder eine Erkältung, welche die Stimme so stark verfremdet, dass sie nicht mehr korrekt zugewiesen werden kann. Ein Gipsarm wird durch die eingeschränkte Bewegungsfähigkeit des Armes auch die Handschrift verändern. Hautkrankheiten können Fingerlinienmuster verändern, aber auch ganz alltägliche Vorkommnisse, wie abgeschliffene oder verklebte Fingerkuppen bei Menschen, die viel mit den Händen arbeiten, führen zu erhöhten Fehlerquoten bzw. zum Fehlschlagen des Messvorgangs. Die Einnahme verschiedener atropinhaltiger Medikamente irritiert bei der Messung der Iris die Lebenderkennung.

Permanente Ausfälle entstehen zum Beispiel durch Unfälle und das damit verbundene Verlieren eines Merkmals. Aber auch Krankheiten können zu dauerhaftem Fehlen eines Charakteristikums führen: Augenlinsen- oder Netzhauttrübungen verhindern die Erkennung der Blutgefäße auf der Retina, Diabetes verändert die Regenbogenhaut um die Pupille stark und erschwert oder verhindert die Iriserkennung.

Zusammenfassend lässt sich sagen, dass besonders konditionierte Merkmale einer hohen zeitlichen Varianz unterliegen, namentlich Gesicht, Stimme, Tippverhalten oder das individuelle Schriftbild. Durchschnittlich variant sind die stärker exponierten und mit der Umwelt interagierenden Teile des Körpers, wie Finger, Hände, aber auch der Geruch. Am Körper geschützte Teile und deren Merkmale weisen naturgemäß die höchste Beständigkeit auf, hierzu gehören die Iris, die Retina und die DNA.

Erfassbarkeit

Abschließend ist eine Grundvoraussetzung für den Einsatz in biometrischen Systemen, dass das Merkmal messtechnisch erfassbar ist, also mit technischen Methoden beim derzeitigen Stand der Technik aufzunehmen, zu verarbeiten und zu erkennen ist. Dieses Kriterium erfüllen alle genannten und kommerziell verfügbaren Verfahren.

Kriterien für den Einsatz

Die Erfassung biometrischer Daten erfolgt auf viele Arten, sie kann optisch über Kameras und CCDs erfolgen, wie im Fall der Iris oder der Retina aber auch der Gesichtserkennung. Chemosensorische Erfassungen finden im Fall der DNA oder des Geruchsmusters statt. Akustische Sensoren zeichnen Stimmdaten auf. Es sind aber auch multisensorische Systeme zum Beispiel bei der Fingerbilderkennung im Einsatz. Damit diese technischen Vorrichtungen im Alltag einsetzbar sind, müssen sie bestimmten Kriterien für den praktischen Einsatz genügen, welche unabhängig vom vermessenen Merkmal oder der verwendeten Methodik gelten. Die Ergebnisse sind jedoch nicht übertragbar, sondern jeweils nur für den entsprechenden Anwendungszweck gültig

Die Kriterien umfassen alle Phasen des Messvorgangs. Zum einen muss die Methode den Anforderungen entsprechend technisch umsetzbar sein: Dies beinhaltet sowohl die Schnelligkeit der Berechnung eines Ergebnisses als auch die Kompatibilität zu ähnlichen Systemen auf Datenebene. Eng hiermit verbunden ist die ökonomische Machbarkeit, das Einhalten der Spezifikationen sollte mit vertretbaren

Kosten für die Betreiber verbunden sein. Das System muss Ansprüchen bezüglich Robustheit, Empfindlichkeit und Resistenz gegenüber äußeren Einflüssen genügen. Hier geht es sowohl um fehlerfreie und selten nötige Wartung, aber auch um die dauerhafte Genauigkeit und nicht zuletzt die Überwindungssicherheit des Gesamtsystems. Abschließend darf die Nutzerfreundlichkeit nicht vergessen werden. Es muss für die Menschen, die es zu benutzen gedenken, einfach und gleichzeitig zuverlässig funktionieren und hygienisch einwandfrei auch im Dauerbetrieb bleiben.

Zu unterscheiden ist noch die professionelle erkennungsdienstliche Erfassung im Einzelfall gegenüber der automatisierten Massenauswertung. Selbstverständlich sind hier unterschiedliche Maßstäbe zur Bewertung anzusetzen. Die professionelle Fingerabdrucksüberprüfung der Strafverfolgungsbehörden arbeitet beispielsweise mit etwa 250 bis1000 mal größeren Templates als normale Verbrauchergeräte.

Technische Umsetzbarkeit

Die technische Umsetzbarkeit umfasst die Teilaufgaben der Erfassung, Verarbeitung und des Vergleichs innerhalb eines biometrischen Systems. Die größten Probleme entstehen hier im Bereich der Erfassung, welche den größten Varianzen unterliegt. So gibt es grundsätzliche Probleme einiger Sensoren bei unterschiedlichen Lichtverhältnissen oder Temperaturveränderungen. Dies beeinflusst zum Beispiel die Gesichtserkennung im Freien. Für diese sind der Betrachtungswinkel und Detailreichtum wichtig, Variationen in der Mimik erhöhen je nach Methode die Varianz. Der Aufwand, welcher hier betrieben werden muss, um eine einheitliche Messumgebung zu wahren ist recht hoch. Diese Probleme haben in ähnlichem Maße Vorrichtungen für die Handgeometrieerkennung, welche zusätzlich noch eine aufwendige 3D-Optik für Volumenaufnahmen besitzen müssen, somit also nicht mobil sind, was in bestimmten Anwendungen ein Ausschlusskriterium sein kann.

Besonders gut umsetzbar sind die Verfahren der Iris- und Retinaerkennung, welche eine herausragende Genauigkeit bei dem Verifikationswerten besitzen. Im Falle der Retina ist dies jedoch mit aufwendiger Spezialtechnik verbunden.

Robustheit, Empfindlichkeit, Resistenz

Ein grundsätzliches Problem biometrischer Erkennungsmethoden besteht in den gegensätzllichen Zielrichtungen eines rauschtoleranten Systems und eines Systems mit einer sicheren Erkennung des Musters im untersuchten Signal. Störende Faktoren gibt es allerorten: Die Fingerabdruckerkennung arbeitet hauptsächlich mit kapazitiven Sensoren, welche jedoch wesentlich empfindlicher auf Temperaturschwankungen reagieren als die wesentlich seltener eingesetzten optischen Sensoren. Außerdem besitzen sie meist eine recht kleine Fläche, dort sollte also immer die gleiche Stelle des Fingers aufgelegt werden, um Fehlabweisungen zu vermeiden. Eine große Schwachstelle stellen latente Abdrücke des Hautfetts dar, welche im Nachhinein noch erkannt werden können und so fehlerhaft Zugriff gewähren oder verweigern. Eine Lösung bieten hier Ultraschallsensoren, welche den akustischen Widerstand der Haut messen und gegen Fettspuren unempfindlich sind. Insgesamt ist die Fingerabdruckerkennung nicht zur Identifikation eines großen Personenkreises geeignet, dafür sind die genannten Probleme, zuzüglich der Varianzen im praktischen Einsatz, wie Verschmutzung und Abnutzung zu groß. Besser geeignet scheinen hier Messungen am Auge, welches besser geschützt im Körper liegt. Die Retina-Untersuchung lässt sich zum Beispiel menschenmöglich nicht überwinden, man erkauft sich mit dieser Methode jedoch eine hohe fehlerhafte Rückweisungsrate und es existieren Probleme bei der Erkennung für Menschen mit Kontaktlinsen oder Hornhautverkrümmung.

Um sicherheitskritischen Anforderungen zu genügen, sollten die verschiedenen Verfahren in der Lage sein, eine Lebenderkennung durchzuführen. Dies ist längst nicht bei allen zurzeit auf dem Markt erhältlichen Systemen der Fall. Die meisten ausgelieferten kapazitiven Fingerabdruckscanner sind zum Beispiel nicht dazu in der Lage. Es existieren noch keinerlei fundierte Erkenntnisse, ob eine Lebenderkennung kapazitiv überhaupt möglich ist. Möglich ist es innerhalb eines Hybridsystems, welches gleichzeitig den Pulsschlag oder Blutfluss überprüft. Die Irismethoden besitzen allesamt eine Lebenderkennung, die allerdings bei Menschen versagt, welche aufgrund von Medikation temporär erweiterte Pupillen haben, und deren Augenmuskeln nicht wie erwartet auf die Lichtreflexe reagieren. Bei der

Gesichtserkennung existiert bisher nur eine rudimentäre Lebenderkennung mittels Bewegungsmessung.

Ein weiteres Problem ist der so genannte *Look-alike-fraud*, also Betrug durch Individuen mit für das Messsystem ähnlichen Merkmalseigenschaften; dieser lässt sich in Gesichtserkennungssystem kaum wirksam unterbinden, da hier durch starkes Rauschen sehr tolerante Systeme notwendig sind.

Ökonomische Machbarkeit

Es gibt kein derzeit diskutiertes biometrisches Verfahren, welches grundsätzlich ökonomisch nicht machbar wäre. Hier regeln Markt und Marketing den Erfolg der jeweiligen Methode. Was heute noch eine teure Nischenlösung darstellt, kann morgen schon den Durchbruch schaffen und durch Massenproduktion und Verfahrensverbesserung wirtschaftlich werden. Leider verhindern verschlossene Hersteller oft eine genaue Beurteilung der Gesamtkosten einer Anschaffung oder machen Versprechungen bezüglich der Spezifikationen, die sie dann im Nachhinein nicht einhalten können. Eine abschließende Bewertung an dieser Stelle wäre unseriös, auf jeden Fall aber ist der Fingerabdruckscan aufgrund seiner Verbreitung relativ günstig zu implementieren, während der Irisscan noch vergleichsweise teuer ist. Methoden zur Stimmerkennung sind durch den bevölkerungsweiten Anschluss ans Telefon eventuell – je nach Methode – schon gegeben.

Nutzerfreundlichkeit und Akzeptanz

Entscheidend für den verbreiteten Einsatz der Verfahren ist letztlich die Akzeptanz der Benutzer. Hierfür muss grundsätzlichen Bedenken Rechnung getragen werden.

Wo immer physischer Kontakt für die Überprüfung des Merkmals nötig ist, herrschen hygienische Bedenken seitens der Nutzer. Auch wenn diese Befürchtungen stark selektiv sind – so nehmen wir oft benutzte Türklinken in die Hand, ekeln uns aber vor dem zuvor benutzten Fingerabdruckscanner – muss diesen Bedenken Rechnung getragen werden. Besonders bei der massenhaften Abfertigung sind hygienische Bedenken durchaus berechtigt. Die verschiedenen Verfahren sind un-

terschiedlich gefährdet, bei einem Handgeometriescanner ist das Risiko einer Krankheitsübertragung aufgrund der großen Fläche vergleichsweise höher als bei einem Fingerabdruckscanner.

Ein biometrisches System sollte bequem zu bedienen sein, um seine Akzeptanz zu steigern. Während sich ein Fingerabdruck ohne weitere Probleme nehmen lässt, müssen zur Verifikation der Handgeometrie die Finger relativ lange in unbequemer Lage gehalten werden. Bei der Retina ist eine anstrengende Untersuchung in zwei Zentimetern Abstand durchzuführen. Etwas weiter weg kann der Benutzer bei der Irisuntersuchung stehen, etwa 15 bis 30 Zentimeter bei einem passiven System, welches die Augen nicht selbstständig findet, und bis zu einem Meter bei aktiven Systemen, welche allerdings auch erheblich teurer sind. Die weit verbreitete Angst vor Laserstrahlen ist allerdings völlig unbegründet: Es wird gar kein Laser benutzt. Einen interessanten Aspekt bieten hier fast alle aktiven Merkmale: Da sie meist nicht *per se* überprüft werden, sondern spezifische Ausprägungen – die Unterschrift bei der Handschrift, eine Wortfolge bei der Stimme – ist durch die Semantik eine gewisse Anonymität gewährleistet. Außerdem besteht die Möglichkeit einer nachträglichen Änderung der Referenzdaten, eine Koppelung an eine Willenserklärung wird so möglich.

Soziale Aspekte spielen bei der Meinungsbildung zur Biometrie keineswegs eine untergeordnete Rolle. Im Gegenteil: Die eigentlich einfach und unkompliziert abzuwickelnde Fingerabdruckerkennung wird oft in kafkaeske Verbindung mit den Behörden der Strafverfolgung und einer erkennungsdienstlichen Behandlung gebracht. Unterbewusst fühlt sich der Untersuchte verdächtig, die Methode suggeriert aufgrund ihrer Herkunft ein Schuldgefühl. Es bleibt abzuwarten, ob eine weite Verbreitung biometrischer Methoden diese Angst zerstreut oder, im Gegenteil, ihr sogar Vorschub leistet. Besonders aus der Ferne überprüfbare Merkmale schüren Misstrauen und Befürchtungen, dass hier Überwachungen stattfinden. Hierzu gehören das Gesicht, der Gang, der Geruch und auch die menschliche Stimme. Ebenso ist der RFID-Chip in den neuen EU-Pässen bis auf seinen digitalen Schutzmechanismus berührungslos auslesbar. Die Konditionierung der Bevölkerung spielt allerdings auch hier eine starke Rolle. So gehört die Überwachung des Alltags mit Videokameras in Großbritannien zur Normalität und auch an deut-

schen Arbeitsplätzen wird man schon heute permanent durch Kameras gefilmt, eine Überwachung wäre technisch also durchaus jetzt schon möglich.

Abschließende Betrachtung

Je nach Anwendungsgebiet gibt es meist mehrere Methoden, welche den Anforderungen an ein biometrisches System genügen. Im Hochsicherheitsbereich empfehlen sich überwindungssichere System wie Iris- oder Retinascan, für die schnelle und kostengünstige Abwicklung großer Mengen an Individuen eher der etablierte Fingerabdruckscan. Eine technische Betrachtung kann allerdings immer nur eine Momentaufnahme sein und Verfahren, welche heute zu teuer oder technisch nicht machbar sind, sind vielleicht in fünf bis zehn Jahren ausgereift. Die abschließende Tabelle soll somit nur einen kurzen Überblick nach heutigem Stand der Technik geben:

	Komfort	Genauigkeit	Verfügbarkeit	Kosten
DNA	o	ooooooo	**ooooooooo**	ooooooooo
Gesicht	**ooooooooo**	oooo	ooooooo	ooooo
Retina	oooooo	oooooooo	ooooo	ooooooo
Iris	oooooooo	**ooooooooo**	oooooooo	oooooooo
Handgeometrie	oooooo	ooooo	oooooo	ooooo
Fingerabdruck	ooooooo	ooooooo	oooo	ooo
Stimme (Klang)	oooo	oo	ooo	oo
Tastenanschlag	oooo	o	oo	**o**
Schrift	ooo	oooo	ooooo	oooo

Tabelle 1: Eignung biometrischer Merkmale nach heutigem Stand der Technik[3]

[3] Tabellenwerte nach Dr. Manfred Bromba: Bioidentifikation – Fragen und Antworten; http://www.bromba.com/faq/biofaqd.htm#Besten [Stand 10.7.2005]

Um die Akzeptanz zu fördern, muss die Gesellschaft über großflächig eingesetzte Systeme hinreichend aufgeklärt werden. Leider wird dafür in der heutigen politischen Landschaft kaum Sorge getragen. Dabei gibt es durchaus datenschutzrechtlich bedenkliche Merkmale. Hier hilft ein Rückblick auf ihre Entstehung: Natürlich enthält die DNA ungleich mehr Informationen als zu Verifikation eines Individuums nötig sind. Und auch im Gesicht steht wesentlich mehr geschrieben, namentlich die ethnische Zugehörigkeit, körperliche Defekte oder auch Krankheiten. Solange hier nicht auf allen Seiten – der Industrie, der Politik und anderer, Biometrie einsetzender Stellen – öffentlich gemacht wird, welcher Art die erhobenen Daten sind und wie sie weiterverarbeitet und gespeichert werden, solange diese Transparenz nicht herrscht, wird es schwer, den Nutzern die zusätzlichen finanziellen und persönlichkeitsrechtlichen Kosten zu erklären.

Quellen

Petermann, Thomas und Sauter, Arnold: Biometrische Identifikationssysteme. Sachstandsbericht. Büro für Technikfolgenabschätzung beim Deutschen Bundestag. Berlin, 02/2002

Leitold, Herbert und Posch, Reinhard: Leitfaden Biometrie. Überblick und Stand der Technik, Zentrum für sichere Informations-technologie Austria, A-SIT. Wien, 26/01/2004

Teletrust Deutschland e.V.: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog. Erfurt, 10/07/2002

Leitold, Herbert: Biometrische Verfahren. Stand der Technik und Normen. Zentrum für sichere Informations-technologie Austria, A-SIT. Wien, 13/05/2004

Daum, Henning: Activities in Biometrics, Fraunhofer IGD. Darmstadt, 01/2003

BSI: BioFinger. Evaluierung biometrischer Systeme Fingerabdrucktechnologien. Berlin, 08/2004

BSI: BioFace II. Vergleichende Untersuchung von Gesichtserkennungssystem. Berlin, 06/2003

Eckert, Claudia: IT-Sicherheit. Konzepte – Verfahren – Protokolle. Oldenbourg Verlag München Wien, 2005

Quellen im Netz

Chaos Computer Club Berlin: Biometrie. Internet:
https://berlin.ccc.de/index.php/Biometrie [Stand 31.8.2005]

Chaos Computer Club: Biometrische Merkmale in Ausweisen erhöhen Sicherheit nicht. Internet: http://www.ccc.de/biometrie/ [Stand 31.8.2005]

IBG. Independent Biometrics Expertise. Internet:
http://www.biometricgroup.com/ [Stand 31.8.2005]

aufenthaltstitel.de: Biometrie - Sachstand und Ausblick. Internet:
http://www.aufenthaltstitel.de/biometrie/index.html [Stand 31.8.2005]

Bromba, Manfred: Bioidentifikation – Fragen und Antworten. Internet:
http://www.bromba.com/faq/biofaqd.htm [Stand 31.8.2005]

Neumann, Karsten: Tätigkeitsbericht. Biometrie in Ausweisen. Internet:
http://www.lfd.m-v.de/taetberi/tb6/6_219.html [Stand 31.8.2005]

BSI: Biometrische Verfahren. Internet:
http://www.bsi.de/fachthem/biometrie/verfahren/index.htm [Stand 31.8.2005]

Stop84.de: Biometrie. Internet:
http://stop1984.com/index.php?text=themen.txt\#Biometrie [Stand 31.8.2005]