

Die 14 Märchen der Biometrie

Eine Reihe von „grundlegenden“ Aussagen zur biometrischen Personen-erkennung ist schon so alltäglich, dass jeder Zweifel an ihnen als Frevel erscheint. Doch oft entspricht genau das Gegenteil den Tatsachen. So manche Behauptung stammt schlichtweg noch aus dem „Kalten Krieg“ der gegnerischen Fraktionen, als es um die Frage ging, welches biometrische Merkmal gewinnt. Einige dieser Mythen und Halbwahrheiten auszuräumen, ist die Absicht dieses Beitrags.

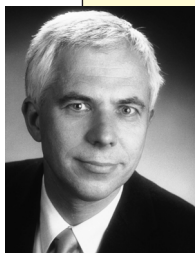
Von Manfred Bromba, München

Märchen Nr. 1:

Je niedriger die Falschakzeptanzrate (FAR), desto größer die Sicherheit

Sicherheit ist in der Regel mit der Fähigkeit verknüpft, fehlerhafte Authentifikationen zu verhindern. Die FAR beschreibt nun zwar sehr gut die Leistungsfähigkeit der Erkennungsalgorithmen – aber leider nicht alle Arten von Falschauthentifikationen. In manchen Anwendungen stellen beispielsweise die nicht in der FAR erfassten Fälschungen biometrischer Merkmale ein viel größeres Risiko dar, so dass eine weitere Verringerung der FAR keinen zusätzlichen Nutzen mehr bringt. Beispiel: Ein Fingerprint-System zeichnet sich normalerweise bei gleicher Falschrückweisungsrate (FRR) durch eine wesentlich kleinere FAR aus als ein Gesichtserkennungssystem. Trotzdem kann das Gesichtserkennungssystem abhängig von der jeweiligen Anwendung mehr Sicherheit bieten als das Fingerprint-System, wenn es besser gegen Fälschungen geschützt ist.

Über unseren Autor:



Dr. Manfred Bromba ist Geschäftsführer der Bromba GmbH und Biometrieberater. Kontakt: www.bromba.com

Märchen Nr. 2:

Biometrische Merkmale sind nicht kopierbar

Jedes biometrische Merkmal lässt sich entweder mechanisch oder nach geeigneter Messung zumindest als Datensatz kopieren. Nicht nur der Chaos Computer Club hat dafür eindrucksvolle Beispiele geliefert und damit so manche Falschaussage aus der Pionierzeit der Biometrie widerlegt.

Märchen Nr. 3:

Biometrische Merkmale sind unfälschbar

Alle bekannten und genutzten biometrischen Merkmale sind mit mehr oder weniger hohem Aufwand fälschbar. Allein die Tatsache, dass für eine bestimmte Merkmalsart noch keine Fälschungsmethode bekannt ist, bedeutet nicht, dass dies nicht möglich ist: Alles ist nur eine Frage der Entdeckung und des Aufwands.

Märchen Nr. 4:

Iris- und Retina-Erkennungssysteme scannen das Auge mit Laserstrahlen

In der Anfangszeit war es ein beliebtes Spiel der Verfechter einer bestimmten Merkmalsart, das jeweilige Konkurrenzsystem durch angstmachende Halbwahrheiten zu verunglimpfen. Sogar heute findet man gelegentlich noch die Behauptung, Iris- oder Retinaverfahren würden mit Laserstrahlen ins Auge leuchten. Mag sein, dass es einmal Realisierungsvorschläge zur (ungefährlichen) Benutzung des Lasers gegeben hat. Fakt ist jedoch, dass dies weder notwendig ist, noch gibt oder gab es Serienprodukte, die Laserstrahlen benutzen. Erstaunlicherweise hält sich dieses Gerücht aber so hartnäckig, dass die Anbieter von Irissystemen nicht mehr

von „Irisscan“, sondern von „Iriserkennung“ sprechen – um nur keine Assoziationen mit dem Laserscanner an der Kasse zu wecken.

Märchen Nr. 5:

Biometrische Merkmale lassen sich nicht aus Templates rekonstruieren

Dieses Argument wird gerne genutzt, um Datenschutzbeauftragte zu beruhigen. Fakt ist: Biometrische Merkmale lassen sich mittels geeigneter mathematischer Methoden aus Templates (den wesentlichen biometrischen Daten) zumindest so weit rekonstruieren, dass es möglich wird, dadurch ein biometrisches Erkennungssystem zu täuschen. Das heißt, das Erkennungssystem kann Originalmerkmal und Rekonstruktion nicht voneinander unterscheiden. Nur die nicht-redundante Information, die während der Template-Erzeugung beseitigt wurde, lässt sich nicht rekonstruieren. Somit ist zumindest sichergestellt, dass sich für die Erkennung unbrauchbare Gesundheitsdaten, falls überhaupt vorhanden, nicht aus dem Template rekonstruieren lassen.

Märchen Nr. 6:

Eine Lebenderkennung löst alle verbliebenen Sicherheitsprobleme

Eine Lebenderkennung wird oft als Maßnahme gegen Fälschungen vorgeschlagen. Leider war es bisher immer so, dass – sobald eine Methode offenbart oder „enttarnt“ wurde – relativ einfache Verfahren zur Umgehung angegeben werden konnten. Immerhin gelingt es mit guten Verfahren, den Aufwand für eine Fälschung deutlich zu erhöhen. Eine perfekte Methode wird es jedoch nie geben.

Märchen Nr. 7:

Das Passwort ist kein biometrisches Merkmal

Es wird gerne eine strikte Einteilung der Authentifikationsverfahren in Besitz, Wissen und Biometrie vorgenommen und das Passwort als Gegenpol zur Biometrie gesehen. Bei genauerer Betrachtung finden sich jedoch fließende Grenzen. Ordnet man beispielsweise, wie vielfach üblich, biometrischen Merkmalen zufällig entstandene (randotypische), vererbte (genotypische) und erlernte (Verhaltens-) Merkmalsanteile zu, so ließe sich das Passwort als Grenzfall eines Merkmals mit fast 100% Verhaltensanteil charakterisieren. Sogar eine biometrische Performanz mit Maßen wie FAR und FRR ließe sich bestimmen, vorausgesetzt, es wird der gesamte Erfassungs-Kanal einschließlich Mensch betrachtet. Manche betrachten das Erlern-

te Passwort sogar als mechanisches Verknüpfungsmuster der Gehirnzellen, für das es nur (noch) keine geeignete Messvorrichtung gibt.

**Märchen Nr. 8:
DNA ist das Beste**

Häufig findet sich die Behauptung, die DNA-Erkennung würde die beste biometrische Leistungsfähigkeit aller bekannten Merkmale in Bezug auf Falschenrollenrate (FER), Falschakzeptanzrate (FAR) und Falschrückweisungsrate (FRR) aufweisen. Jedoch gibt es neben der heute noch recht langwierigen Analyseprozedur zwei Probleme: Erstens erlaubt die DNA mit derzeitigen Verfahren keine Unterscheidung von eineiigen Zwillingen. Dies ist zwar keine Beschränkung für die Kriminalistik – noch beeinflusst es die messbaren Fehlerraten. Aber es kann bestimmte Identifikationsanwendungen etwa am Geldautomaten ausschließen. Zweitens ist zumindest dem Verfasser keine groß angelegte statistische Untersuchung zur Bestimmung von Fehlerraten bekannt, die die Kriterien nach ISO/IEC 19795 erfüllt und somit die oben genannte Behauptung rechtfertigen könnte.

**Märchen Nr. 9:
DNA ist kein biometrisches Merkmal**

Es gibt verschiedene Gründe, warum selbst manche Biometriker DNA (deutsch: DNS) nicht als biometrisches Merkmal akzeptieren. Der bekannteste ist, dass heute noch kein vollautomatisches Erfassungs- und Analyseverfahren verfügbar ist. Des Weiteren beträgt die Analysezeit derzeit

günstigstenfalls noch einige Stunden, während sich andere biometrische Verfahren mit Sekunden begnügen. Fakt ist, dass sich die DNA-Analyse als extrem leistungsfähiges Werkzeug bei der Erkennung und zur Unterscheidung von Personen bewährt hat. Es ist nur noch eine Frage der Zeit und des technischen Fortschritts, bis die vollautomatische Verarbeitung in Echtzeit möglich ist. Es sollte jedoch nicht vom aktuellen Stand der Technik abhängen, ob ein biometrisches Merkmal als solches anerkannt wird oder nicht.

**Märchen Nr. 10
Durch Gesichtserkennung verletzen
Überwachungskameras Bürgerrechte**

Viele glauben, die automatisierte Gesichtserkennung würde zusammen mit Überwachungskameras eine vollständige automatische Verfolgung aller Personen erlauben und damit Orwell'schen Horrorszenarien gerecht werden. Diese Sorge wird noch durch zahlreiche Pilotversuche zur Auffindung gesuchter Krimineller verstärkt. Aus grundsätzlichen Erwägungen heraus kann jedoch Entwarnung gegeben werden. Um eine Verfolgung von Personen zu ermöglichen, muss das Erkennungssystem im Identifikationsmodus arbeiten und hat so mit zwei Problemen zu kämpfen:

1. Bei einer Identifikation steigt die FAR fast linear mit der Zahl der Gesuchten und der Zahl der Untersuchten.
2. Das System hat es nicht nur mit kooperativen, sondern vor allem mit nicht-kooperativen (gleichgültigen) und anti-kooperativen (sich versteckenden) Personen zu tun.

Punkt 2 kann die FRR (Falschrückweisungsrate) für einzelne Personen bis auf 100% hochschnellen lassen. Als Folge bleibt nur der Ausweg, auf Kosten der Falschakzeptanzrate die Erkennungsschwellwerte herabzusetzen.

Beispiel: Gute Gesichtserkennungssysteme lassen sich für kooperative „Nutzer“ auf eine FAR von 0,1% bei einer FRR von 10% einstellen, wenn wir eine Verifikation (1:1-Vergleich) voraussetzen. Für nicht-kooperative Nutzer nehmen wir einmal an, die Verifikations-FAR betrage 1% bei einer FRR von ebenfalls 10%. Wenn das System nun einen einzelnen Gesuchten mit 1.000 von der Kamera erfassten Personen vergleicht, wird es den Gesuchten (wenn er denn vorbeikommt) mit einer Wahrscheinlichkeit von 90% (= 1 - FRR) detektieren. Andererseits wird es von den 1.000 erfassten Personen 10 Personen ($\sim 1.000 \times \text{FAR}$) irrtümlich für den Gesuchten halten! Als manuelle Unterstützung für die Polizei ist dies eine gute Rate. An Stelle von 1.000 Personen müsste die Polizei dann nur noch zehn untersuchen – eine Arbeitserleichterung um den Faktor 100. Für ein automatisches Verfahren wäre diese Fehlerrate allerdings völlig untragbar. Noch viel kritischer wird die Situation, wenn nicht eine einzelne Person, sondern etwa 1.000 gesucht werden. Dann würde in unserem Beispiel fast jeder Erfasste falsch erkannt. Selbst wenn sich die Erkennungsleistung für die Gesichtserkennung noch um einen Faktor 100 verbessern ließe (was wahrscheinlich schon jenseits



des Möglichen liegt), würde sich diese Situation nicht drastisch genug verbessern, um die Verfolgung großer Personenzahlen zu ermöglichen. Trotzdem ist es immer wieder erstaunlich, wie selbst staatliche Stellen immer neue Pilotversuche ansetzen, wohl in der Hoffnung doch noch irgendwo die Naturgesetze aushebeln zu können. Heißt das jetzt, dass Überwachungskameras überflüssig sind? Nein. Einmal lässt sich an bestimmten Orten die Kriminalität durch Abschreckung deutlich senken. Zum Anderen sind die gespeicherten Informationen eine wertvolle Hilfe bei der manuellen Aufklärung von Kriminalfällen – wobei dann aber auch nicht-biometrische Kurzzeitmerkmale wie Kleidung und die übrigen Körpermerkmale (etwa Körpergröße) zur Auswertung zur Verfügung stehen.

Märchen Nr. 11:

Gute Gesichtserkennungssysteme können eineiige Zwillinge unterscheiden

Auf der CeBIT 1999 erzählte ein Aussteller von Gesichtserkennungssoftware, dass er am Messestand einen Zwilling registriert hätte. Dieser Zwilling wäre dann auch problemlos erkannt worden, der andere hingegen wurde ordnungsgemäß abgelehnt. Die naheliegendste Erklärung ist jedoch, dass es sich beim zweiten Erkennungsversuch um eine "Falschrückweisung" gehandelt hat. Warum? Weil die Gesichtserkennung die meisten eineiigen Zwillinge nicht unterscheiden kann. Denn die Gesichtsgometrie ist primär genetisch geprägt – randotypische (zufällige) Anteile sind statistisch gesehen gegenüber der natürlichen Variation (etwa durch Mimik) und den beleuchtungsbedingten Messfehlern vernachlässigbar. Die randotypischen Anteile sind jedoch essentiell, um eineiige Zwillinge auseinander halten zu können. Wichtig ist, wie überall in der Biometrie, die statistische Betrachtungsweise. Es ist also höchstens die Aussage möglich: „In den meisten Fällen ist eine Gesichtserkennung nicht in der Lage, zwei eineiige Zwillinge mit brauchbarer Zuverlässigkeit auseinander zu halten.“

Märchen Nr. 12:

Iris- und Retinaerkennung lassen sich zur Ermittlung von Krankheiten missbrauchen

Viele Menschen glauben, dass das Auge ein Spiegel aller Körperfunktionen sei und damit in der Lage ist, auch Krankheiten aller Körperbereiche zu offenbaren. Leider gibt es für diesen Glauben keine wissenschaftliche Bestätigung. Natürlich gibt es Augenkrankheiten, die eine Iris- oder Retinaerkennung deutlich erschwe-

ren, weil sie die normalerweise unveränderlichen Merkmale verändern oder die Datenerfassung beeinträchtigen. Des Weiteren gibt es Krankheiten wie Bluthochdruck, die sich durch Sekundäreffekte im Auge bemerkbar machen. Diese Effekte sind in der Regel aber nur zur Feststellung geeignet, dass „ein Problem vorliegen könnte“.

Auf der Homepage der Firma e-EyeCare wird gezeigt, was mit einem solchen System heute und demnächst möglich ist. Das System von e-EyeCare analysiert nichtinvasiv den Augenhintergrund und die dort sichtbaren Blutgefäße unter der sinnvollen Annahme, dass sich von Gefäßveränderungen im Auge auf Gefäßveränderungen im Gehirn und eventuell den gesamten Körper schließen lässt. Durch komplexe Bildverarbeitung und manuelle ärztliche Analyse kann man auf diese Weise recht bequem das Risiko (nicht die Existenz) für Gefäßkrankheiten wie den Schlaganfall ermitteln. Für die Auswertung der Iris existiert bis heute kein vergleichbares Verfahren.

Die Rohdaten der Retina liefern also nur begrenzte Erkenntnisse über Krankheiten, und die biometrischen Daten (Templates) lassen sich ganz von Gesundheitsdaten freihalten – und zwar irreversibel. Das liegt daran, dass zum Merkmalsvergleich bei der Retinaerkennung nur die unveränderlichen Verzweigungspunkte von Bedeutung sind, nicht aber der Augenhintergrund oder die Blutgefäßdicke und -beschaffenheit. Im Allgemeinen würden Informationen über akute Krankheiten bei einer Identifikationsanwendung sogar stören, da sie veränderlich sind, während man für die Identifikationsinformation auf möglichst stabile Daten setzt. Deshalb arbeiten bekannte Verfahren der Iriserkennung mit Schwarzweißinformationen. Die Augenfarbe wird nicht ausgewertet, da sie sich bei manchen Menschen im Krankheitsfalle (im Gegensatz zum Regenbogenmuster) ändern kann.

Märchen Nr. 13:

Die Benutzerakzeptanz wird primär durch das biometrische Merkmal bestimmt

In vielen Vergleichen biometrischer Merkmale hat es sich eingebürgert, auch die Benutzerakzeptanz als Bewertungskriterium aufzuführen – oft frei nach dem Motto, „Fingerprint wird von der Polizei zur Identifikation von Verbrechern genutzt, also muss nicht nur die Akzeptanz der Methode unter Verbrechern niedrig sein, sondern auch unter allen anderen Nutzern“. In der Tat sind solche Bewertun-

gen meist reine Spekulation oder (ohne Quellenangabe) irgendwo abgeschrieben. In der Praxis hängt die Benutzerakzeptanz primär vom Vorteil der Anwendung für den Benutzer ab, und da spielen Faktoren wie Benutzungsergonomie und Systemzuverlässigkeit eine weit größere Rolle als der Merkmalstyp. Anwender können ihre vorgefasste Meinung in kürzester Zeit ändern, wenn das biometrische Erkennungssystem diese Bedingungen erfüllt. Um die Benutzerakzeptanz zu messen, ist es allerdings erforderlich, einen praxisnahen Vergleichstest durchzuführen.

Märchen Nr. 14:

Die Leistungsfähigkeit hängt von der Zahl der Freiheitsgrade ab

Die Zahl der Freiheitsgrade beziehungsweise unabhängigen Messparameter eines biometrischen Merkmals wird gerne als Maß für die Leistungsfähigkeit herausgestellt. Je mehr Freiheitsgrade, desto besser sei das biometrische Verfahren. Tatsache ist jedoch, dass die Zahl der Freiheitsgrade völlig ungeeignet ist, um biometrische Merkmale zu vergleichen. Ein einfaches Beispiel soll das verdeutlichen: Die menschliche Körpergröße ist ein biometrisches Merkmal mit dem Freiheitsgrad 1. Nehmen wir an, die Körpergröße wäre konstant und ließe sich unter Verwendung modernster physikalischer Methoden mit einem Fehler von deutlich besser als 1 Nanometer messen, dann würde dieses einfache biometrische Merkmal die mit deutlich mehr Freiheitsgraden operierende Gesichtserkennung in Bezug auf Erkennungsfehler eindeutig in den Schatten stellen. Dass dies in der Praxis nicht der Fall ist, hat wenig mit den fehlenden Freiheitsgraden zu tun, sondern damit, dass der Mensch seine Größe willentlich ändern kann, dass sich die Größe im Tagesverlauf um mehrere Millimeter verringert und dass es schier unmöglich ist, eine reproduzierbare Messvorschrift zu definieren (wie muss der Kopf geneigt sein, mit oder ohne Haare, vor oder nach dem Essen), die die hohen Messgenauigkeitsanforderungen zu erfüllen in der Lage ist.

Somit sollte eigentlich klar sein, dass ein Merkmal mit wenigen Freiheitsgraden bei entsprechender Stabilität und Messbarkeit durchaus besser sein kann als eines mit hoher Zahl an Freiheitsgraden, aber schlechter Genauigkeit. Was letztendlich entscheidet sind die Falschrückweisungs- und Falschakzeptanzraten FRR und FAR, die einzig einen Performanzvergleich erlauben, vorausgesetzt, sie wurden nach ISO/IEC gemessen. ✓