Was ist Biometrie?

Unter Biometrie in Zusammenhang mit einer Personenidentifikation versteht man die Erkennung von Personen anhand von einzigartigen und unverwechselbaren biometrischen Merkmalen. Diese Merkmale sind unmittelbar an den Körper der Person gebunden und müssen nicht erst zusätzlich zugeordnet werden.
Zu den biometrischen Verfahren die mit passiven physiologischen Merkmalen arbeiten und zur Personenidentifikation eingesetzt werden gehören:

Fingerabdruckerkennung
: Ein biometrisches Verfahren über spezielle Sensoren optischer, kapazitiver, thermischer oder direkt-optischer Technologie mit hoher Erkennungsleistung.

Gesichtserkennung
: Aus Bildaufnahmen werden charakteristische Merkmale des Gesichtes in sogenannten Templates gespeichert, die wiederum mit Templates eines gespeicherten aktuellem Originalbildes verglichen werden.

Iriserkennung
: Mit einer Kamera aufgenommene einzigartige komplexe Strukturen des Bindegewebes zwischen Hornhaut und Iris liefern ein einzigartiges Erkennungsmerkmal, ähnlich dem Fingerabdruck.

Venenerkennung
: Basiert auf der Erkennung der Gefäßstruktur einer Ifrarotaufnahme des Handbereiches. (Lebenderkennung durch Temperaturmessung)

Handgeometrie
: Ein günstig zu realisierendes Verfahren mit einigen Schwächen bei der eundeutigen Erkennung.

Von den oben genannten Verfahren hat mit einem Anteil von ca. 40% die Fingerabdruckerkennung den größten Anteil und hat eine der niedrigsten Falschrückweisungs- und Fehlerakzeptanzraten unter den biometrischen Verfahren.

Warum Biometrie?

Biometrische Merkmale sind bezogen auf den Benutzer einzigartig und eindeutig. An ein biometrisches Merkmal muss sich der Benutzer nicht erinnern, er kann es weder vergessen noch verlieren sondern trägt es ständig bei sich. Körperliche Merkmale können nicht wie ein Passwort oder Karte einfach weitergegeben und missbräuchlich verwendet werden.

Deshalb bietet sich die Biometrie als Alternative oder Ergänzung zu herkömmlichen Methoden wie Karte oder PIN/Passwort zum Einsatz in Zeiterfassungs- und Zutrittskontrollsystemen an, weil die körperlichen Merkmale im Gegensatz zu Besitz- oder Wissenselementen unmittelbar personengebunden sind.

Warum Fingerabdruckerkennung?

Von allen biometrischen Verfahren hat in den letzten Jahren weltweit die Erkennung anhand des Fingerabdruckes die weitaus größte Verbreitung erfahren. Deshalb existieren mit der Fingerabdruckerkennung auch die umfangreichsten praktischen Erfahrungen.

In einer 2005 vom BSI durchgeführten umfangreichen Studie zur Leistungsfähigkeit verschiedener biometrischer System erzielten Fingerabdrucksysteme mit optischen

Sensoren die besten Ergebnisse (vor Iriserkennung und Gesichtserkennung). Es wurde bescheinigt, dass die Fingerabdruckerkennung auch für sehr hohe Sicherheitsanforderungen geeignet ist.

Fingerabdrucksysteme weisen bezüglich der Anschaffungskosten gegenüber allen anderen Systemen deutliche Vorteile auf.

Grundlagen der Fingerabdruckerkennung

Die Einzigartigkeit des Fingerabdruckes (Es existieren keine zwei Menschen mit gleichem Fingerabdruck, selbst eineiige Zwillinge mit genetisch identischer DNA weisen unterschiedliche Fingerabdrücke auf) lassen ihn als ideal geeignet erscheinen zur Verwendung in automatisierten Erkennungssystemen.

Grundlagen der Fingerabdruckerkennung

Für die automatisierte Erkennung werden die Fingerabdruck-Feinmerkmale, die so genannten Minuzien verwendet. Diese ergeben sich aus dem Vorhandensein von Verzweigungen und Endungen in der Fingerlinienstruktur. Die Anordnung dieser punktförmig definierten Merkmale ergibt ein ganz spezifisches Bild, das ebenfalls einmalig ist und sich maschinell auswerten lässt. Die Anordnung dieser Minuzien, ihre relative Lage zueinander und ihre Richtung, ist hauptsächlich zufällig und nicht vererbbar.

Der Ablauf der biometrischen Identifizierung ist bei allen biometrischen Systemen unabhängig vom verwendeten Verfahren prinzipiell gleich:

1. Enrolment
   Registrierung des Nutzers im System (Enrolment) durch Erfassung der biometrisch relevanten Eigenschaften dieser Person und Erstellung und Speicherung eines Datensatzes (Template)
2. Matching
   Erfassung der biometrisch relevanten Eigenschaften einer Person, Erstellung eines Datensätzen (Templates) und Vergleich der aktuell präsentierten mit den zuvor abgespeicherten Daten (Matching)

Zur Erfassung einer Person in einem biometrischen System wird beim Enrolment vom Fingerabdruck zunächst ein Bild erzeugt. Mittels eines speziellen Algorithmus, der bei jedem Hersteller unterschiedlich ist, wird dieses in einen Datensatz, das Template, umgewandelt und gespeichert. Es ist nicht möglich aus diesem extrahierten Datensatz auf dem umgekehrten Wege wieder einen Fingerabdruck zu generieren.

Beim Matching wird ein Vergleich zwischen dem gespeicherten Template und dem Datensatz der bei einer erneuten Präsentation gewonnen wurde, durchgeführt. Wird eine

hinreichende Übereinstimmung festgestellt, erkennt das System den Benutzer.

Identifikation und Verifikation

Identifikation und Verifikation - 1:n und 1:1 Vergleiche

Bei der Verwendung biometrischer Systeme zur Authentifizierung von Personen stößt man immer wieder auf die Begriffe Identifikation und Verifikation. Ziel einer biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln *(Identifikation)* oder eine behauptete Identität zu bestätigen bzw. zu widerlegen. *(Verifikation)*

Bei einer **Identifikation** wird ein biometrische Merkmal mit allen im System gespeicherten Referenzmerkmalen verglichen (1:n Vergleich). Gibt es eine Übereinstimmung, ist die Identifikation erfolgreich und die zum betreffenden Referenzmerkmal gehörende User-ID lässt sich weiterverarbeiten.

Bei einer **Verifikation** gibt der Nutzer dem System seine Identität vorab bekannt (z.B. über eine PIN oder Karte), das System muss das biometrische Merkmal dann nur noch mit einem zur User-ID passenden Referenzmerkmal vergleichen. Im Übereinstimmungsfall ist die Verifikation erfolgreich.

Effektivität von biometrischen Systemen

Die Erfassung und Auswertung biometrischer Merkmale ist naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale sowohl im Laufe der Zeit als auch temporär durch äußere Einflüsse ändern und auch die Präsentation gegenüber dem System niemals gleich erfolgt. Die zu unterschiedlichen Zeitpunkten erzeugten digitalen Abbilder des gleichen biometrischen Merkmals können also nicht zu 100% identisch sein. Es erfolgt also beim Matching deshalb keine Überprüfung auf Gleichheit sondern auf hinreichende Ähnlichkeit.

Für die Effektivität und Sicherheit biometrischer Systeme existieren zwei allgemein anerkannte Messgrößen:

Die Falsch-Zurückweisungsrate (FRR)

Die FRR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der berechtigte Personen unberechtigterweise zurückgewiesen werden. Die FRR ist in der Regel ein

Komfortmerkmal, da falsche Abweisungen vor allem lästig sind aber die Sicherheit nicht beeinträchtigen. Der typische Wert für BMZ Nova Systeme liegt bei weniger als 1%.

Die Falschakzeptanzrate (FAR)

Die FAR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der nichtberechtigte Personen als berechtigt akzeptiert werden. Da eine falsche Akzeptanz in der Regel zu Schäden führt, ist die FAR ein sicherheitsrelevantes Maß. Die FAR wird allgemein als wichtigstes Kriterium für die Qualität einer Biometrielösung angesehen. Der typische Wert für BMZ Nova Systeme liegt bei 0,0001%.

Beide Werte können durch Änderung der Toleranzschwellen innerhalb des Systems beeinflusst werden, stehen jedoch immer in direkter Abhängigkeit zueinander: eine Verringerung der FAR führt unmittelbar zu einer Erhöhung der FRR und umgekehrt.

BMZ Zeitsysteme

Borsari + Meier AG
Seefeldstrasse 62
CH-8008 Zürich

Tel. +41 (0)44 383 05 94
Fax +41 (0)44 383 25 64

www.bmz.info
bmznova@bmz.info