Einführung in die technischen Grundlagen der biometrischen Authentisierung

1 Einleitung

Heutzutage steigt der Bedarf an zuverlässigen Personenidentifikationen. Zur Zeit begegnen wir der Problematik der Personenidentifikation z. B. im E-Commerce, bei Zutrittskontrollanlagen, in der Terrorismusbekämpfung usw. Die Identifikation durch den Besitz eines Objektes wie z. B. eines Ausweises dient zwar noch ihrem Zweck, verliert in der heutigen vielfach elektronisch kommunizierenden Welt mit mehr als 6 Milliarden Menschen aber zunehmend an Bedeutung. Aus diesem Grunde gewinnt die Biometrie gerade in der jüngsten Zeit an Bedeutung, da sie die Personenidentifikation mit eindeutigen und teilweise unveränderbaren bzw. über einen langen Zeitraum stabilen Merkmalen eines Menschen verknüpft. Menschen besitzen gewisse, eindeutige Eigenschaften (im Sinne von körperlichen Merkmalen), die sich in der frühesten Phase des menschlichen Lebens in einem Zufallsprozess (randotypisch) ausprägen und für jedes Individuum unterschiedlich sind.

Mit den ständig wachsenden und komplexeren Technologien wird eine genaue und automatisierte Personenidentifikation unerlässlich. Beispielsweise kann man mit dem Identifikationsprozess den Zutritt zu bestimmten Objekten durch bestimmten Rechte regeln. Jeder, der erfolgreich identifiziert und somit akzeptiert wurde, erhält die vorgegebenen Privilegien. Im polizeilichen Umfeld spielt die Identifikation (z. B. *Daktyloskopie*) eine wichtige Rolle. Dies sind nur zwei von vielen Fällen, in denen die „biometrische“ Identifikation zum Einsatz kommt.

Zum allgemeinen Verständnis biometrischer Verfahren seien vorab einige Begriffe erklärt:

Statische Merkmale sind anatomische Merkmale des Körpers, die sich im Laufe des Lebens nicht oder kaum verändern (Fingerabdrücke, Iris, genetische Information, etc.).

Dynamische Merkmale sind Verhaltensmerkmale eines Menschen (Handschrift, Gangart, Stimme, etc.).

Passive Erfassung ist eine Erfassung im „Vorbeigehen“ (z. B. Gesicht durch Kamera).

Aktive Erfassung ist eine Erfassung durch Mitwirkung der Person (z. B. Fingerabdruck).

Identifikation: Feststellung der Identität (Wer ist die Person?). Bei der Identifikation wird das biometrische Merkmal mit *allen* im biometrischen System gespeicherten Referenzmerkmalen verglichen (1:n-Vergleich).

Verifikation: Bestätigung der Identität (Ist die Person die, die sie zu sein vorgibt?). Bei der Verifikation gibt der Anwender dem biometrischen System seine Identität vorab bekannt (z. B. die User-ID über Tastatur oder Karte) und das System muss das biometrische Merkmal dann nur noch mit dem *einen* zur User-ID passenden Referenzmerkmal vergleichen (1:1-Vergleich).

Biometrisches System: Ein System zur biometrischen Erkennung von Personen. Es erfasst die biometrischen Daten einer Person und vergleicht sie mit vorher erfassten Referenzdaten mit dem Ziel, die Identität dieser Person festzustellen (Identifikation) oder die behauptete Identität zu bestätigen oder zu widerlegen, d. h.. sie zu akzeptieren oder zurückzuweisen (Verifikation).

Biometrische Systeme enthalten generell die funktionalen Komponenten Datenaufnahme (ggf. mit Vorverarbeitung), Merkmalextraktion, Referenzbildung und Vergleich (*Matching*). Mit Hilfe eines Sensors wird ein Bild von den biometrischen Merkmalen aufgenommen und weiter vorverarbeitet, woraus dann die biometrischen Merkmale extrahiert werden, die als Template (Merkmalvektor) gespeichert werden. Beim **Enrolment** werden die Bilddaten oder die extrahierten Merkmale als Referenzdaten ggf. zusammen mit weiteren Daten der Person (Name, ID, ...) gespeichert. Bei der Verifikation und Identifikation werden die biometrischen Daten der agierenden Person erneut aufgenommen und mit den Referenzdaten verglichen. Dazu müssen sie ebenfalls die Verarbeitungsschritte Datenaufnahme, Vorverarbeitung und Merkmalextraktion durchlaufen und dem Vergleich zugeführt werden. Das Ergebnis einer Verifikation ist entweder *match*

oder *non-match* und führt zu **Akzeptanz** oder **Rückweisung** der behaupteten Identität. Im Falle der Identifikation liefert das System eine Liste der gespeicherten Einträge, bei denen der Vergleich zu *match* führte.

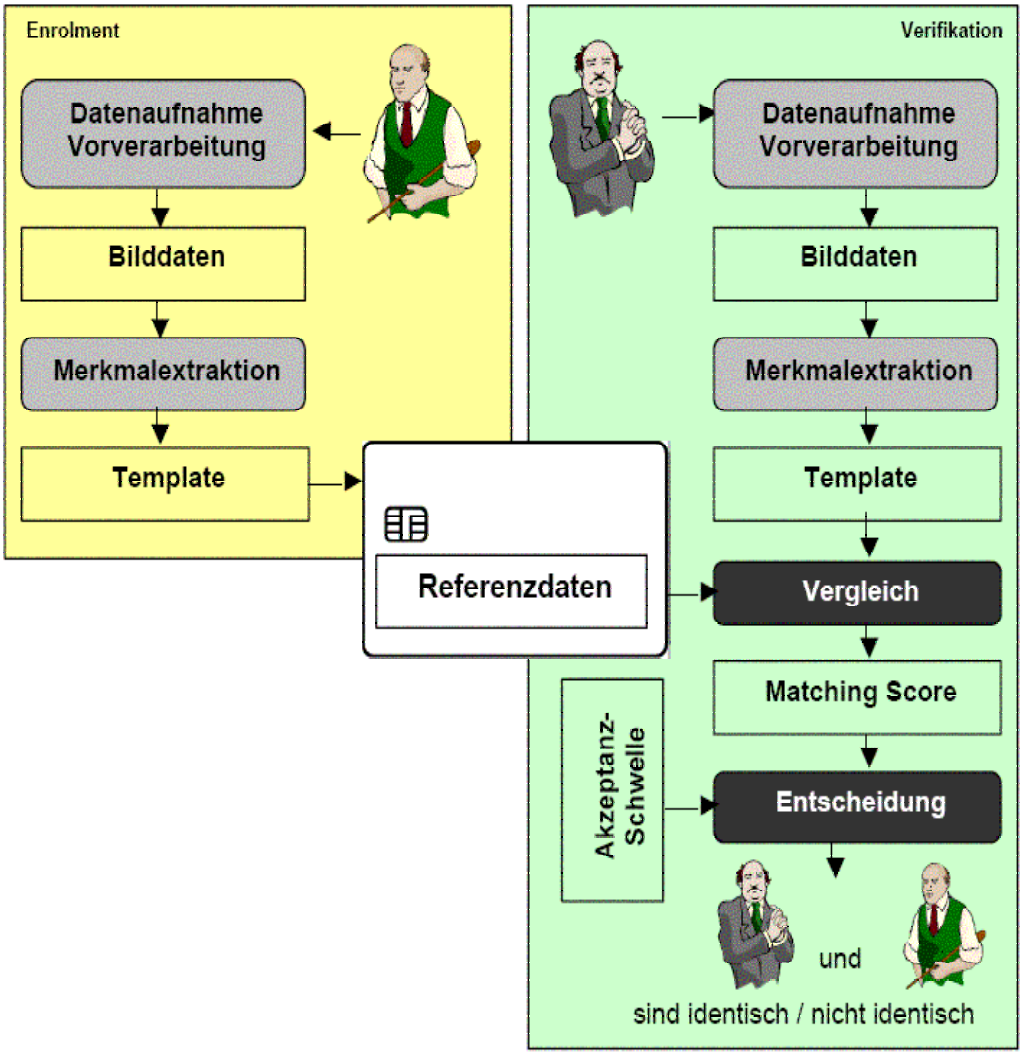

Abbildung 2.1: Komponenten eines biometrisches System zur Verifikation[1]

[1] Quelle: BSI-Studie "BioFinger".

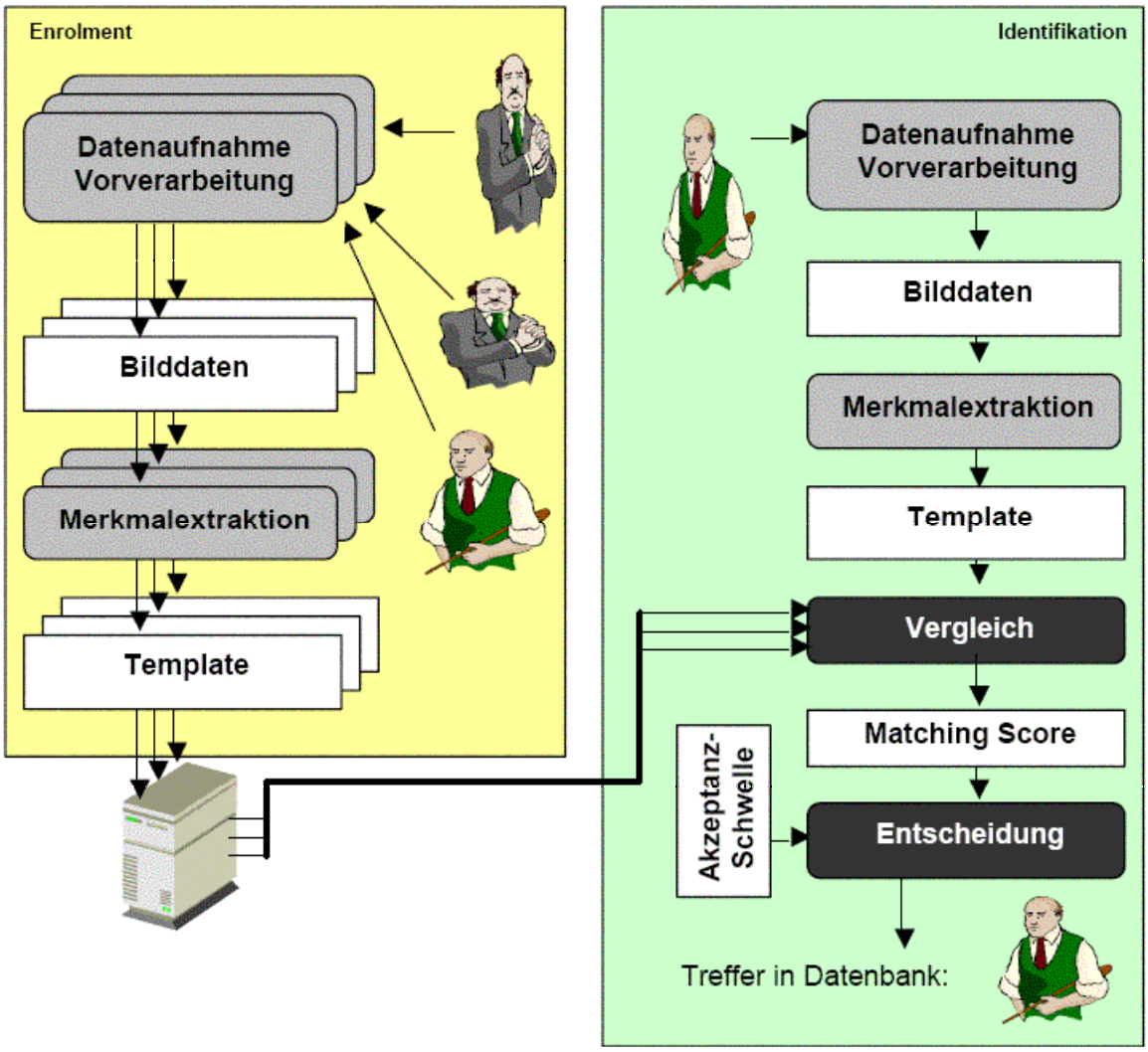

Abbildung 2.2: Komponenten eines biometrisches System zur Identifikation[2]

Affinität: Zwei Aufnahmen eines biometrischen Merkmals werden genau dann als **affin**[3] bezeichnet, wenn sie vom selben Körper(-teil) aufgenommen wurden und so den selben Ursprung haben. Der Abdruck, der mit System A von meinem rechten Daumen gemacht wurde, ist dem Abdruck affin, der von meinem rechten Daumen mit System B gemacht wurde; beide Abrücke sind aber dem von meinem linken Daumen nicht affin.

Genuines sind die Fälle, in denen affine Aufnahmen verglichen werden.

Imposter sind die Fälle, in denen nicht affine Aufnahmen verglichen werden.

Matching Score: Affine Aufnahmen, also Aufnahmen ein und desselben biometrischen Merkmals, die zu verschiedenen Zeitpunkten oder gar mit verschiedenen Sensoren gemacht wurden, sind i.A. in ihrer datentechnischen Darstellung unterschiedlich, so dass ein Bit-zu-Bit-Vergleich niemals Gleichheit feststellen wird. Gleiches trifft für die extrahierten Merkmale zu. In Folge dessen arbeitet der Vergleichsalgorithmus so, daß er eine Kennzahl ermittelt, den *Matching Score*, die das Maß der Übereinstimmung der verglichenen biometrischen Merkmale ausdrückt (z. B. 1 für große und 0 für keine Übereinstimmung). Liegt der
Matching Score oberhalb einer festgelegten **Akzeptanzschwelle**, lautet die Entscheidung des Systems

[2] Quelle: BSI-Studie "BioFinger".

[3] affin : verwandt, d.h. derselben Herkunft

match und das System akzeptiert die Person, andernfalls lautet die Entscheidung *non-match* und die Person wird zurückgewiesen.

2 Grundsätzliche Anforderungen an ein biometrisches System

Jede physiologische oder verhaltensbedingte Eigenschaft kann als *biometrisches Merkmal* zur Personenidentifikation verwendet werden, sofern sie folgende Anforderungen erfüllt:

(a) Universalität: jede Person muss dieses Merkmal besitzen,

(b) Einmaligkeit: keine zwei oder mehr Personen mit gleichem Merkmal dürfen existiren,

(c) Erfassbarkeit: diese Eigenschaft ist quantitativ messbar.

Die in der Praxis überwiegend verwendeten biometrischen Eigenschaften erfüllen allerdings meistens nicht alle oben genannten Anforderungen. Sie sind deshalb teilweise nur bedingt für den Einsatz in praktischen biometrischen Systemen geeignet. Darüber hinaus sind weitere praktische Aspekte zu berücksichtigen:

(a) *Leistungsfähigkeit* des Systems, die quantitative Aussagen über erreichte Identifikationsgenauigkeit, -geschwindigkeit und geforderte Robustheit gegenüber systematischen Faktoren erlaubt,

(b) *Akzeptanz* des Systems im praktischen Einsatz,

(c) *Überwindungssicherheit* des Systems, d. h.. Robustheit gegenüber gezielten Methoden, das System zu überwinden.

(d) *Ökonomische Machbarkeit*, d. h.. die Kosten müssen angemessen sein.

(e) Benutzbarkeit, Verwendbarkeit und Zweckmäßigkeit aus technischer und organisatorischer Sicht

Praktische biometrische Systeme müssen demnach i.d.R.

(a) eine akzeptable Identifikationsgenauigkeit und -geschwindigkeit erbringen,

(b) vernünftige Anforderungen an die biometrischen Eigenschaften erfüllen,

(c) nichtinvasiv sein,

(d) von den Anwendern akzeptiert werden

(e) und ausreichend robust gegenüber Missbrauch sein.

3 Leistungsfähigkeit eines biometrischen Systems

Die Leistungsfähigkeit eines biometrischen Systems zeigt sich dadurch, in welchem Maß Akzeptanz und Rückweisung des Systems der Affinität der verglichenen biometrischen Merkmalen entsprechen. Hierzu ergeben sich vier unterschiedliche Fälle:

		die verglichenen biometrischen Merkmale sind tatsächlich	
		affin *Genuines*	nicht affin *Imposters*
das System ermittelt	Akzeptanz *match*	richtige Akzeptanz *True Acceptance*	falsche Akzeptanz *False Acceptance*
	Rückweisung *non-match*	falsche Rückweisung *False Rejection*	richtige Rückweisung *True Rejection*

False Acceptance Rate (FAR)

Die FAR ist die Wahrscheinlichkeit, dass ein biometrisches System nicht affine Merkmale akzeptiert.

$$FAR = \frac{\text{Anzahl der Vergleiche nicht affiner Merkmale, die einen Match ergeben}}{\text{Gesamtanzahl der Vergleiche nicht affiner Merkmale}}$$

False Rejection Rate (FRR)

Die FRR ist die Wahrscheinlichkeit, dass ein biometrisches System affine Merkmale zurückweist.

$$FRR = \frac{\text{Anzahl der Vergleiche affiner Merkmale, die einen Non-Match ergeben}}{\text{Gesamtanzahl der Vergleiche affiner Merkmale}}$$

Failure To Acquire Rate (FTA) gibt den Anteil der fehlerhaften Aufnahmen im automatischen Modus der Aufnahme des Sensors wieder, also der Aufnahme biometrischer Merkmale, die vom System abgelehnt wurden. Je höher dieser Wert ist, desto schlechter ist der Sensor für die Aufnahme geeignet. In diesem Sinne stellt diese Fehlerrate eine Kennzahl für die Bewertung des Sensors dar.

Failure To Enroll Rate (FTE) gibt den prozentualen Anteil der Benutzer an, die von dem System nicht eingelernt werden konnten. Die FTE-Raten treten oft im Zusammenhang mit Systemen auf, die über die Kontrolle der Qualität z. B. des Fingerabdrucks entscheiden, ob ein Template erzeugt wird oder nicht. D.h. Aufnahmen mit niedriger Qualität werden in das System nicht eingelernt. In diesem Sinne stellt die FTE eine Kennzahl dar, welche die Fähigkeit des Algorithmus bewertet, mit qualitativ schlechten Aufnahmen zurecht zu kommen.

False Match Rate (FMR)

Die FMR gibt den Anteil der beim Merkmalsvergleich fälschlicherweise akzeptierten Personen an. Vorher auf Grund schlechter Qualität (z. B. des Bildes) abgewiesene Versuche (*Failure To Acquire*, FTA) werden im Gegensatz zur FAR nicht berücksichtigt.

False Non-Match Rate (FNMR)

Die FNMR gibt den Anteil der beim Merkmalsvergleich fälschlicherweise nicht akzeptierten Personen an. Vorher auf Grund schlechter Qualität (des Bildes) abgewiesene Versuche (*Failure to Acquire*, FTA) werden im Gegensatz zur FRR nicht berücksichtigt.

Der mathematische Zusammenhang der Fehlerraten ist wie folgt.

$$FAR(T) = (1 - FTA) \times (1 - FTE) \times FMR(T)$$

$$\begin{aligned} FRR(T) &= FTA + (1 - FTA) \times FTE + (1 - FTA) \times (1 - FTE) \times FNMR(T) \\ &= 1 - (1 - FTA) \times (1 - FTE) \times (1 - FNMR(T)) \end{aligned}$$

MR und FNMR sowie FAR und FRR sind keine konstanten Werte, sondern hängen von der Wahl der Akzeptanzschwelle und von den Verteilungsfunktionen für Imposters und Genuines ab, die für jedes System charakteristisch sind.

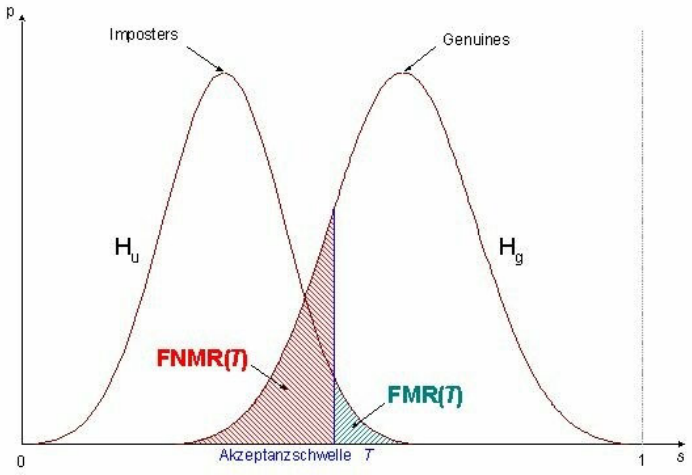

Abbildung: FMR und FNMR sowie FAR und FRR[4].

Die Abbildung skizziert FMR und FNMR. Die Fehlerraten ergeben sich aus den Wahrscheinlichkeitsdichten für den Vergleich unterschiedlicher und gleicher Fingerabdrücke:

$$FMR(T) = \int_{T}^{1} p_u(s \mid H_u)ds \qquad FNMR(T) = \int_{0}^{T} p_g(s \mid H_g)ds$$

[4] Quelle: BSI-Studie "BioFinger".

FMR und FNMR können als Funktionen der Akzeptanzschwelle ausgedrückt werden und ergeben folgendes typisches Bild.

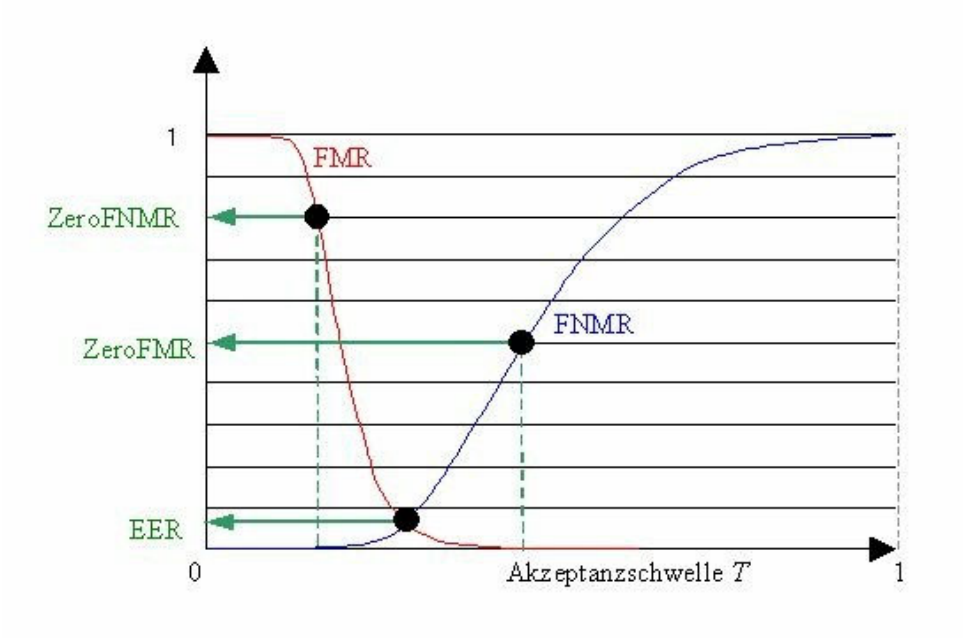

Abbildung: FMR und FNMR[5]

Die **Equal Error Rate (EER)** ist durch die Bedingung FNMR(*T*) = FMR(*T*) definiert.

ZeroFNMR ist die untere Grenze der FMR, für die gilt: FNMR = 0.

ZeroFMR ist die untere Grenze der FNMR, für die gilt: FMR = 0.

Es gibt noch weitere Parameter wie die Verifikations- / Identifikationsgeschwindigkeit, welche die Leistungsfähigkeit der Systeme bewerten. In den Verifikationsprozessen ist wegen des Vergleiches „one-to-one“ die Geschwindigkeit im Wesentlichen durch die benötigte Rechenzeit des Verifikationsalgorithmus limitiert. Es ist gewöhnlich leicht, hier die gestellten Geschwindigkeitsanforderungen zu erfüllen. In dem Identifikationsprozess dagegen insbesondere in Systemen, die Millionen von Einträgen enthalten, limitiert die Zahl der benötigten Vergleiche die Gesamtgeschwindigkeit des Systems.

Weitere Aussagen zur Erkennungsleistung und Sicherheit von marktverfügbaren Fingerabdruck-, Gesichts- und Iriserkennungsverfahren lassen sich dem öffentlichen Abschlussbericht des Projekts BioP II entnehmen, der demnächst auf der BSI-Webseite zum download zur Verfügung stehen wird.

[5] Quelle: BSI-Studie "BioFinger".