Vortrag zum Thema:

„Bestimmung der Güte eines Biometrischen Systems“

mit Augenmerk auf die

„Grundbegriffe der Biometrie“

Seminar:

„Biometrische Identifikationsverfahren“

im Sommersemester 2004 an der Humboldt-Universität zu Berlin

Leiter:

Matthias Schwan

Vortragender:

Mathias Anders, 172681

Inhaltsverzeichnis

Abbildungsverzeichnis

Abstract

Durch das verstärkte Bedürfnis nach Sicherheit erlebt die Industrie für biometrische Erkennungsgeräte eine Art Boom. Dies erfordert aber auch höhere Anforderungen an die Qualität und Leistung solcher Geräte. Was wiederum erfordert, dass sich wissenschaftlich mit dem Thema auseinandergesetzt werden muss. Sowohl unter den Gesichtspunkten der technischen Machbarkeit als auch – und eigentlich viel mehr – mit Grundsatzfragen, ob solche Technologie menschenwürdig und gesetzlich ist. Damit beschäftigte sich das Seminar „**Biometrische Identifikationsverfahren**“ im Sommersemester 2004.

Aufgabenstellung

Dieser Vortrag soll als Einleitung zur Biometrie dienen. Um biometrische Erkennungsgeräte effektiv nutzen zu können, bedarf es an solidem Verständnis der Grundbegriffe. Das bedeutet, zu allererst warum man Biometrie überhaupt verwenden soll, wie solche Geräte funktionieren und wie gut sie ihre Arbeit erledigen.

Biometrische Geräte variieren stark in ihrer Komplexität, ihren Fähigkeiten, Leistungen und Genauigkeiten, haben andererseits aber auch viele Gemeinsamkeiten.

Template-Generierung, **Matching** oder **Enrollment Process** sind nur einige der verschiedenen Grundbegriffe, die in der Biometrie – oder besser: Biometrik – immer wieder verwendet werden.

Hier werden diese und andere Grundbegriffe genannt und definiert, ihre Zusammenhänge darlegt und somit ein Einblick in die Biometrie – und Biometrik geschaffen.

Weiterhin leitet dieses Papier in die **Bestimmung der Güte eines biometrischen Systems** ein und definiert damit verschiedene Fehlerraten und deren Zusammenhänge.

Was ist Biometrie, was ist Biometrik?

Diese beiden Begriffe treten sehr häufig paarweise auf. Meistens werden sie auch noch synonym verwendet, obwohl sie eigentlich verschieden sind. Was bedeutet nun was?

Biometrie beschäftigt sich mit der Erfassung und „Vermessung“ von Lebewesen und deren Eigenschaften, meistens zu statistischen Zwecken.

Biometrik hingegen ist die automatisierte Messung individueller physiologischer und verhaltenstypischer Merkmale einer Person zum Zwecke der Identifizierung oder Verifizierung der Identität dieser Person.

Das Adjektiv **biometrisch** kann sich sowohl auf **Biometrie** als auch auf **Biometrik** beziehen.

Warum Biometrik?

Die gängigsten traditionellen Formen der Authentisierung, sind die durch Wissen und die durch Besitz. Mit Wissen sind Passwörter oder PINs usw. gemeint, mit Besitz, Dinge wie Schlüssel oder Chipkarten usw.

Leider haben diese Formen ihre Nachteile. Passwörter kann man sich nicht merken oder sie werden abgeschaut oder gar absichtlich weitergegeben. Schlüssel können vergessen, verloren, gestohlen oder aber auch absichtlich weitergegeben werden. Ein biometrisches Merkmal, wie zum Beispiel Fingerabdrücke, hingegen, hat man und dass ein solches vergessen oder weitergegeben wird, ist eher weniger wahrscheinlich. Im Folgenden werden ein paar Vorteile der Biometrik aufgezählt. Was aber auf gar keinen Fall bedeutet, Biometrik löse die älteren Formen ab, sondern ergänzt diese zu höherer Sicherheit. Biometrik ist auch nicht für alle Sicherheitsüberprüfungen die zweckmäßige Lösung.

- **Erhöhung des Sicherheitslevels**
  Betrüger können zum Beispiel mit dem Diebstahl von Schlüsseln oder mit Erraten von Passwörtern in ein Sicherheitssystem eindringen. Passwörter sind häufig so gewählt, dass man sich nicht vergisst, was bedeutet, sie sind einfach. Gute Passwörter enthalten Zahlen und Sonderzeichen. Leider kann man diese sich nur schwer merken, was wiederum bedeutet, dass solche Passwörter aufgeschrieben werden. Im schlimmsten Falle sogar an die Orte, wo sie gebraucht werden, etwa als Schnipsel an den Monitor geklebt. Ein biometrisches Merkmal zu stehlen, stellt sich hier als schwer da – wenn auch nicht unmöglich – aber es muss viel mehr Aufwand betrieben werden.

- **Erhöhung des Nutzerkomforts**
  Heutzutage muss man sich eine ganze Reihe von Passwörtern, PINs und so weiter merken, weiterhin gibt es viele Nutzer, die eine Fülle von Karten und Schlüsseln mit sich umhertragen müssen. Biometrische Merkmale können eher nicht „vergessen“ werden. Auch ist durch die bessere Zuordnung mit einem biometrischem Merkmal gegeben. Dies könnte die Passwortmenge reduzieren – und auch die Anzahl der Schlüssel am Bund und nimmt, zumindest erstmal theoretisch, Last von Nutzer und Administrator.

- **Erhöhung der Zuordbarkeit und Erhöhung von Betrugsaufdeckung**
  Viele Menschen haben derzeit viele Identitäten. Verschiedene Internetadressen, verschiedene Nummern, in Ämtern zum Beispiel, loggt sich mit verschiedenen Accounts in verschiedene Computernetze ein. Die Verwaltung eines biometrischen Merkmals könnte all diese verschiedenen Identitäten unter einer zusammenfassen und dafür sorgen, dass eine Person eindeutig identifiziert wird. Das erhöht auf die Chance, Betrüge aufzudecken, denn mit dem Hinterlegen eines biometrischen Merkmals, ist es schwierig, sich mehrfach für eine Sache einzutragen.

- **Erhöhung der Betrugsabschreckung**
  Allein die Anwesenheit von biometrischen Geräten schreckt schon viele ab, die bei weniger Sicherheit durchaus zu Betrug geneigt hätten. Biometrik wird von vielen als sehr sicher angesehen – von vielen auch als chic, etwa einen Retina-Scanner zu haben.

Definition einiger biometrischer Begriffe

Dieser Teil stellt den Hauptteil – und das Thema dieses Papiers da. Es werden Schlüsselbegriffe der Biometrik genannt, definiert, gegen einander gehalten und ihre Gemeinsamkeiten gezeigt.

- **Automatisiert**
  Physiologische und verhaltenstypische Merkmale werden für gewöhnlich *manuell* überprüft, um die Identität herauszufinden oder zu überprüfen. Das passiert tagtäglich wenn wir unsere Freunde begrüßen oder unser Personalausweis überprüft wird. Biometrik hingegen ist automatisiert. Maschinen werden hier benutzt, um jemanden zu identifizieren oder seine Identität zu überprüfen. Daher dauert ein solcher Vorgang auch nur wenige Sekunden und solche Systeme überprüfen in dieser Zeit tausende Einträge einer Datenbank.

- **Physiologische Merkmale**
  Diese Merkmale werden direkt vom menschlichen Körper abgeleitet. Sie sind allesamt einzigartig bei jedem Menschen. Beispiele sind dafür die Fingerabdrücke, das Gesicht, die Iris, die Geometrie der Hand und die Netzhaut des Auges, auch Retina genannt. Es gibt sicherlich noch viele weitere einzigartige Merkmale, allerdings muss man auch darauf achten, dass es nicht die Würde verletzt, bestimmte Merkmale abzutesten. Für die genannten wurden diverse verschieden qualitative Geräte gebaut.

- **Verhaltenstypische Merkmale**
  Merkmale dieser Art werden nicht direkt sondern indirekt vom menschlichen Körper abgeleitet. Auch diese sind einzigartig, aber wesentlich schwerer zu messen. Beispiele hierfür sind eine Stimmverifikation, das Leisten einer Unterschrift oder die Art, eine Tastatur zu bedienen. Bei der Stimmerkennung geht aber nicht darum, Worte wieder zu erkennen, sondern darum, die Stimme zu einer Person zuzuordnen. Die Unterschrift-Überprüfung und die Überprüfung mit Hilfe der Tastatur sind ähnlich, es geht um Zeitverhalten und Druckausübung.

- **Identität**
  Dieses Wort wird gerne falsch oder ungenau verstanden – insbesondere im Kontext der Biometrik. Hier muss eine klare Linie zwischen einem **Individuum** und einer **Identität** gezogen werden. Ein **Individuum** ist ein einzelnes bestimmtes Lebewesen, trivialerweise eine Person. Aber eine Person kann mehrere **Identitäten** haben. Herr Max Mustermann hat sicherlich eine „eMail-Identität“ *mustermann@hier.de*, eine auf Arbeit *Dr. Max Heinrich Mustermann* und so weiter. Hat jemand alle seine zehn Finger in einem biometrischem System registriert, so kann das Gerät diese als zehn verschiedene Identitäten ansehen, nicht als ein einzelnes Individuum. Diese Idee wird ausgenutzt, um die Sicherheit eines Systems zu erhöhen. So kann es etwa sein, dass eine Person drei Finger nach einander eingeben muss, um Zugang zu erhalten.

- **Verifizieren (einer Identität) und Identifizieren**
  Beide Tätigkeiten sind von großer Bedeutung in der Biometrik oder Biometrie. Ein System, das identifizieren soll, sucht das eingegebene Muster in einer Datenbank ab in dem es alle oder eine bestimmte Menge der Einträge mit dem Suchmuster vergleicht. Das geschieht beispielsweise bei der Polizei, die Fingerabdrücke bei einem Tatort entnimmt und diese mit ihrer „Verdächtigen-Datenbank“ vergleicht. Es beantwortet die Frage „Wer bin ich?“ Da es die Datenbank absucht, muss der Vergleichsalgorithmus genauer sein, als beim Verifizieren, um nicht aus Versehen mit einem falschen Eintrag zu matchen. Man nennt solche Systeme hin und wieder auch 1:N-Systeme (eins-zu-n) Unterschieden werden auch hier zwei Systeme: ein „positives“ und ein „negatives“. Das positive ist so geschaffen, dass es eine Person in der Datenbank findet. Die Idee dahinter ist trivial. Das negative hingegen ist so geschaffen, dass es davon ausgeht, dass die zu überprüfende Person *nicht* in der Datenbank enthalten ist. Die Idee hier, ist abzusichern, dass sich jemand nicht zweimal registrieren lässt. Das wird besonders bei großen öffentlichen Programmen angewendet, wo es viele gibt, die versuchen würden, sich mehrmals unter verschiedenen Namen anzumelden.

  Solch riesige Systeme können mehr als 100'000 Einträge verwalten. Ihre Funktionsweise unterscheidet sich stark von ihren kleineren Geschwistern in punkto Genauigkeit und Antwortzeit so sehr, dass sie eine völlig andere Art Technologie sind. Es sind auch nicht alle biometrischen Konzepte anwendbar: Unterschriftenüberprüfung, Stimmverifikation und Handgeometrieprüfung können nicht so gut differenziert werden, wie es dafür nötig wäre.

  Bei einem System, das eine Identität verifizieren (=authentisieren) soll, gibt die Person sich vorher als jemand aus und das Gerät überprüft das. Hierbei wird das eingegebene Muster nicht in der Datenbank gesucht sondern das mit der Identität verglichen, die angegeben wurde. Es beantwortet als die Frage: „Bin ich der, für den ich mich ausgebe?“ Es kann ein wenig genauer arbeiten und sich für den Vergleich mehr Zeit lassen, da es ja nur einen einzelnen Eintrag überprüfen muss. Solche Systeme werden auch 1:1-Systeme (eins-zu-eins) genannt.

- **Logischer und Physikalischer Zugang**
  Was macht ein biometrisches System, nachdem es identifiziert oder verifiziert hat? Das hängt davon ab wofür es gebaut wurde. Wir interessieren uns hier für die hauptsächliche Aufgabe: Zugang gewähren (oder ablehnen). Wir unterscheiden zwei grob zwei Arten von Zugang: Logischen und Physikalischen.

Physikalischer Zugang bedeutet, Zutritt zu einem bestimmten örtlichen Bereich zu bekommen. Dieser ist überwacht und gesichert und das Zugangssystem ist – im besten Falle – der einzige Eingang in einen solchen Bereich. Beispiele für solche Bereiche wären Banktresore, Serverräume, Kontrollräume. Weiterhin versteht man den Zugang zu Gegenständen als physikalischen Zugang. Als Zukunftsvision soll es auch solche Systeme für das Starten von Autos geben. Sie würden den Schlüssel zwar nicht ersetzen, aber gut ergänzen.

Logischer Zugang bedeutet, Zutritt im übertragenen Sinn zu bekommen. Die Anmeldung an einem PC (einzeln oder am Netz), Zugang zum Bankkonto oder das Inauftraggeben einer Überweisung wären Vorgänge, bei dem man logischen Zugang anfordert.

Für beide Arten des Zuganges arbeiten die Systeme prinzipiell identisch. Die Peripherien unterscheiden sich aber. Der physikalische Zugang benötigt eine Peripherie, die einen Bereich baulich von der Außenwelt trennt. Das biometrische Gerät, das logischen Zugang gewährt, ist eher „nur“ an einen Computer angeschlossen.

Wegen des riesigen Wertes der Informationen, die in kooperierenden Netzwerken hinterliegen, welche häufig auch vom Internet aus erreichbar sind, sieht die Biometrie-Industrie auf lange Sicht eher in Herstellung von Systemen für logischen Zugang ihre Zukunft. Während sich Nutzer bis zu über zwanzig Mal täglich an einem Rechner einloggen, wird physikalischer Zugang wesentlich seltener angefordert.

Zuletzt soll hier noch gesagt werden, dass nicht immer eine klare Grenze zwischen physikalischem und logischem Zugang unterschieden werden kann. Beispiel für beides wäre etwa ein Geldautomat, der einem Zugang zu Geld und Kontodaten ermöglicht.

Biometrisches Matching

- **Enrollment und Template-Generierung**
  Bei diesem Vorgang tritt der Nutzer zum ersten Mal an ein bestimmtes biometrisches System und lässt sich registrieren. Das nennt man **Enrollment**. Aus den Daten, die bei ihm abgelesen werden, wird mit einem streng geheimen Hersteller-Algorithmus ein **Template generiert**. Dieses Template heißt „**Referenztemplate**“ Die meisten Templates sind lediglich wenige Kilobyte groß, es gibt sogar solche, die nur etwa 9 Byte enthalten. Ein Template ist aber nicht die komprimierte Version eines Fingerabdruckes, Iris-Scans und so weiter, sondern eine Aufzählung besonderer oder herausstechender Merkmale (**Merkmalsextraktion**). Dieses Referenztemplate wird dann in einer Datenbank abgelegt.

  Die Qualität des Registriervorgangs ist sehr wichtig, damit ein Template mit gut unterscheidbaren Merkmalen angelegt werden kann. Das ist ein kritischer Faktor für Genauigkeit auf lange Sicht, um Fehlerraten zu senken.

  Beispiel: Bei einem Gesichtsscan bedeutet das, man sollte Hut oder Brille abnehmen, sich richtig hinstellen, die Mine nicht verziehen und so weiter. Auch sind hier Lichtverhältnisse von großer Bedeutung.

- **Matching**
  Ein Nutzer tritt vor das System und es werden, wie beim Enrollment, biometrische Daten eingelesen, aus denen ebenso ein Template generiert wird. Handelt es sich um ein Identifikationsvorgang (1:N), dann wird dieses Template mit allen einer einigen hinterlegten Templates in der Datenbank verglichen. Ist es ein Verifikationsvorgang (1:1), dann wird es lediglich mit dem Eintrag verglichen, der der Person entspricht, die der Nutzer vorgibt zu sein.
  Der Vergleichsalgorithmus ist im Übrigen ebenso geheim, wie der der Template-Generierung. Er errechnet aus dem Vergleich eine Punktzahl, denn die Templates werden sich niemals gleichen, die dann mit einem Schwellwert verglichen wird. Wird dieser Schwellwert überschritten, so ist das ein Matching. Da heißt, die Person wurde entweder gefunden, oder für die befunden, für die sie sich ausgegeben hat. Bei Nicht-Matching, wird der Nutzer häufig noch einmal aufgefordert, die Eingabe wieder zu versuchen.

  Sollten sich die Templates absolut gleichen, gehen viele Systeme von einem Betrug aus und geben ein Nicht-Matching zurück.

Genauigkeit Biometrischer Systeme

Unglücklicherweise gibt es nur wenige Diskussionen, die sich mit der Güte und der Genauigkeit biometrischer Systeme auseinandersetzen. Auch gibt es wenig Verständnis davon, was Güte in echter Umgebung bedeutet, im Gegensatz zu Laborbedingungen. Warum? Die Industrie ist leider sehr darauf bedacht hohe Maßzahlen zu erreichen – insbesondere die der Vergleichalgorithmen, welche aber nur mit generischen Templates überprüft werden. Die Testumgebung beachtet nicht untrainierte und unmotivierte Nutzer.

Beispiel: Stellen Sie sich vor ein Mikrofon und sagen Sie, ohne rot anzulaufen, die Phrase, die Sie rezitieren müssen. Einigen ist es egal und haben eher keine Probleme mit der Präsentation ihres biometrischen Merkmals.

Die Algorithmen sind also meistens leider nur auf ihre *theoretischen* Fähigkeiten getestet worden. Einer der Gründe dafür, sind Kosten. Es ist leicht einzusehen, dass ein ausgiebiger Praxistest eines Systems recht teuer werden kann.

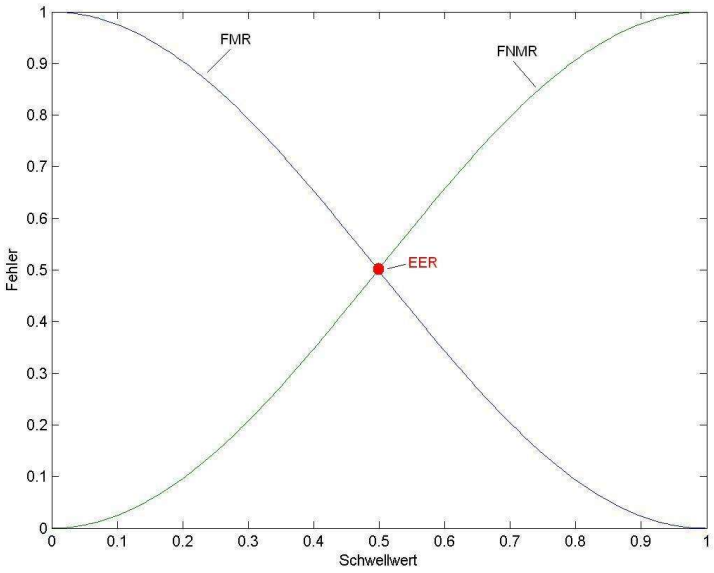
Kommen wir nun zu den Schlüsselbegriffen zur Messung der Güte eines Systems. Es handelt sich um die Fehlerraten: FMR (False Match Rate), FNMR (False Non Match Rate) und FTE (Failure To Enroll) Rate.

- **False Match Rate (FMR)**
  Denkt man über Fehlerraten nach, so fällt einem meistens als erstes die Rate ein, dass jemand Zutritt erhält, der eigentlich nicht berechtigt ist. Das ist die FMR. Der Algorithmus matcht, obwohl er nicht sollte. Das liegt daran, dass die Vergleichspunktzahl hoch genug ist. Man kann der FMR entgegenwirken, indem man den Schwellwert höher legt. Aber das erhöht gleichzeitig die Rate des Fehlers, dass jemand fälschlich abgewiesen wird. Die FMR wird in Prozent angegeben.

- **False Non Match Rate (FNMR)**
  Das ist eben die Rate, mit der der Algorithmus nicht matcht, obwohl er sollte. Das liegt daran, dass beim Vergleichen die Punktzahl nicht hoch genug war um den Schwellwert zu überschreiten. Man kann dem entgegenwirken, indem man den Schwellwert herabsetzt, was aber wiederum die FMR erhöht. Hier sieht man gut den kritischen Zusammenhang zwischen FNMR und FMR. Auch dieser Wert wird in Prozent angegeben.

- **Failure To Enroll (FTE) Rate**
  Bisher wurde Güte vor allem an FMR und FNMR gemessen. Aber durch das Verwenden generischer Templates wurde nicht daran gedacht, dass jemand es nicht schaffen würde, ins System aufgenommen zu werden. Die Gründe dafür sind unter anderem, wenn ein biometrisches Merkmal nicht differenzierbar genug ist. Stellen wir uns hier etwa einen Chemiker vor, dessen Fingerkuppen so verätzt sind, dass sie quasi ungeeignet für fingerabdruckbasierende Systeme sind. Ein Unternehmen, das viel mit Chemie zu tun hat, wird sich wohl kaum dafür entscheiden können, wenn es darum geht, Labore zu sichern. Die FTE Rate ist also ebenso kritisch, wie die FMR und die FMNR. Die FTE wird ebenso in Prozent angegeben.

- **Equal Error Rate (EER)**



Dieser Wert wird aus der FMR und der FMNR abgeleitet. Die beiden Fehler stehen sich, wie schon gesagt, gegenüber. Die Herabsetzung des einen bedeutet die Erhöhung des anderen. Die EER ist gerade der Wert, wo FMR und FNMR sich schneiden, also gleich sind. Die EER wird als genereller Indikator verwendet. Allerdings ist die EER irreführend, wenn es darum geht, die Fähigkeiten eines Systems zu beschreiben. Meistens nimmt man nämlich einen höheren FNMR in Kauf um die eigentliche Aufgabe, unautorisierte Personen abzuweisen, besser ausführen zu können. Überdies sagt diese Rate nichts die FTE aus. Hat ein System nämlich eine kleine EER aber eine FTE von 15%, dann ist wohlweißlich nicht sehr leistungsfähig und in einer echten Umgebung kaum anwendbar.

- **Ability To Verify Rate (ATV)**
  Eine bessere Zahl stellt die ATV da. Sie setzt sie aus der FTE und der FNMR wie folgt zusammen:

$$ATV = (1 - FTE)(1 - FNMR)$$

  Was bedeutet das? Ein hoher ATV-Wert bedeutet, dass sowohl beide eingehende Fehler klein sind. Zusammen mit der FMR kann man eine gute Aussage über die Qualität eines biometrischen Systems aussagen. Ein kleiner ATV bedeutet, dass es wahrscheinlich schwierig zu benutzen ist oder dass es generell viele Nutzer nicht akzeptiert, meistens aber beides.

Quellenangabe

S. Nanavati, M. Thieme, R. Nanavati:
„Biometrics - Identity Verification in a Networked World“,
A Wiley Tech Brief, John Wiley & Sons, Inc, 2002.