Identifikation durch Handgeometrie

Alexander Gruler, Dietmar Stoll
Seminar

Biometrische Systeme – Der Körper als Passwort
Abteilung Neuroinformatik
Universität Ulm
WS 2001/02

1. Einleitung - Vorteile und Anwendung

Im Vergleich zu anderen Verfahren ist die Erkennung mittels Handgeometrie vor allem billig, sehr schnell, sie hat eine hohe Akzeptanzrate (im Vergleich z.B. zum Iris-Scan) und es existieren noch keine öffentlichen Datenbanken wie bei Fingerabdrücken. Der Speicherplatzaufwand pro Benutzer ist, je nach Verfahren, mit 25 – 50 Byte ebenfalls sehr gering und die Sicherheit des Verfahrens nahm in den letzten Jahren deutlich zu. In den USA wird die Handgeometrie-Erkennung beispielsweise in Flughäfen wie San Francisco für den Zugang zu Sicherheitsbereichen und in über 90% aller Kernkraftwerke eingesetzt. Zudem wird die Handerkennung auch in Betrieben zur Arbeitszeiterfassung und in Universitäten zu Zugangskontrolle von Sporthallen und Mensa eingesetzt.

2. 'Enrollment': Erzeugen eines User-Templates

Der Benutzer meldet sich beim System einmalig mit mehreren (i.d.R. 3 – 5) Hand-Scans an (engl.: Enrollment), aus denen dann ein individuelles Template für den späteren Identifikations- und Verifikationsprozess erzeugt wird.
Die Hand des Benutzers wird mit einer CCD-Kamera im Lesegerät von oben und seitlich aufgenommen. Aus diesen Bildern werden die Konturen der Hand erzeugt und daraus verschiedene Merkmale extrahiert: Die Fingerspitzen und Punkte zwischen den Fingern (Interfinger-Points) werden ermittelt. Aus deren Länge wird die Maßeinheit berechnet, die die Position weiterer Fingerbreitenmesspunkte bestimmt. Außerdem werden noch die Handbreite, Abstände und Winkel zwischen verschiedenen Interfinger-Points, Fingerkrümmung und Höhe der Handfläche und Finger gemessen. Aus diesen Maßen wird ein Merkmalsvektor, das Template, ermittelt.
Beim erstmaligen Einsatz und bei der Erforschung eines solchen Systems möchte man zunächst herausfinden, welche Merkmale besonders für das Template geeignet sind, und nur diese werden dann tatsächlich auch im Merkmalsvektor (Feature-Vektor) gespeichert. Da sich die einzelnen Merkmale des Vektors möglichst stark unterscheiden sollen, berechnet man für jedes Merkmal des Templates das Maß der „Diskriminierung", die Feature-Discrimination-Ratio. Die Interclass-Variability sagt aus, wie groß die Varianz des gleichen Merkmals (z.B. Handbreite) zwischen allen Benutzern des Systems ist, die Intraclass-Variability ist ein Maß dafür, wie stark das Merkmal bei mehreren Messungen beim gleichen Benutzer variiert. Die Feature-Discrimination-Ratio eines Merkmals j ist als $F_j = \frac{Interclass - Variab.}{Intraclass - Variab.}$ definiert, sie wird besonders groß, wenn sich das Merkmal von anderen Benutzern sehr stark, bei Messungen des gleichen Benutzers aber nur sehr wenig unterscheidet. Für die Intraclass-Variability nimmt man meist die Messungen, die man vom Benutzer bei der Anmeldung bekam. Bei dem Projekt der Universidad de Madrid wurden 25 Merkmale von ursprünglich

31 gemessenen für den Feature-Vektor ausgewählt, von kommerziellen Firmen wie z.B. RecogSys Inc. war erwartungsgemäß nichts zu erfahren.

3. 'Comparison Process' : Identifikation und Verifikation

Für den Vergleich zwischen Template und dem zu identifizierenden oder verifizierenden Vektor sind die bekanntesten Methoden: Euklidischer Abstand, Hamming-Distanz, Radial-Basis-Function-Neural-Networks und Gaussian-Mixture-Model-Neural-Networks.
Der Euklidische Abstand ist durch

$$d = \sqrt{\sum_{i=1}^{\dim} (x_i - t_i)^2}$$

gegeben, wobei dim die Dimension (=die Anzahl der Merkmale) des Merkmalsvektors, *x* den gemessenen Sample-Vektor und *t* den Template-Vektor, mit dem verglichen werden soll, bezeichnen. In diesem Verfahren werden also die Abweichungen von allen Merkmalen jeweils gleichstark berücksichtigt, jede Dimension wird als gleich wichtig betrachtet.

Bei der Hamming-Distanz

$$d(x_i, t_i^m) = \#\left\{ i \in \{1,...,\dim\}, \left| x_i - t_i^m \right| > t_i^v \right\}$$

wird die Anzahl der Abweichungen der einzelnen Merkmale berechnet. x_i bezeichnet die i-te Komponente des gemessenen Vektors, t_i^m ist der Mittelwert (aus den bei der Anmeldung des Benutzers gemessenen Werten) des Templatevektors, t_i^v die Standardabweichung davon. Daraus folgt, dass die Hamming-Distanz größer wird, je mehr Merkmale des zu untersuchenden Vektors vom Template-Vektor um mehr als die Standardabweichung des Merkmals des Template-Vektors abweicht.

RBF-Netzwerke bestehen aus zwei Schichten, in der ersten Schicht berechnet jedes Neuron j den transformierten Abstand zu seinem Gewichstvektor, durch die sog. radiale Basisfunktion

$$d = \exp\left(-\frac{\left\| x - c_j \right\|^2}{2\sigma^2} \right),$$

in der zweiten Schicht wird eine lineare Transformation vorgenommen. Um RBF-Netzwerke für die Verifikation zu verwenden, erstellt man für jeden Benutzer ein eigenes RBF-Netzwerk und sollte dieses mit den Daten aller anderen Benutzer trainieren. Dies ist meist aus Datenschutzgründen nicht zulässig, weshalb die RBF's für die Verifikation selten eingesetzt werden. Für die Klassifikation benutzt man nur ein RBF, das mit den Template-Vektoren aller Benutzer trainiert wird.

Die GMM-Technik ist eine Mischung aus neuronalen Netzen und einem statistischen Ansatz. Man modelliert die Wahrscheinlichkeit, dass der gemessene Vektor zu einem Benutzer u gehört, durch die Summe von M (mehrdimensionalen) Normalverteilungen. Diese ist durch

$$P(x/u) = \sum_{i=1}^{M} \frac{c_i}{(2\pi)^{L/2} \left| \sum_i \right|^{1/2}} \exp\left(-\frac{1}{2} (x - m_i)^T \sum_i^{-1} (x - m_i) \right)$$

gegeben. L ist die Dimension des Merkmalsvektors und x bezeichnet den zu verifizierenden Vektor. Für jeden Benutzer werden M Gauß-Modelle erstellt, die durch die Gewichte c_i und den Mittelwertsvektoren m_i der Modelle gekennzeichnet sind. K_i ist die Kovarianz-Matrix des i-ten Modells. Die Gewichte c_i muss man nun geeignet trainieren.

4. Experimentelle Ergebnisse

In den Versuchen des Projektes der Universidad de Madrid schnitt das GMM – Verfahren am besten ab.

Richtige Klassifizierung		Euklid	Hamming	GMM	RBF
Anzahl	3	86%	75%	88%	90%
enrollment vectors	4	85%	82%	93%	91%
(25 features)	5	86%	87%	96%	91%

Je kleiner die Dimension des Merkmalvektors, desto kleiner wird im Allgemeinen auch die Erkennungsrate, dies wird besonders bei auf neuronalen Netzen basierten Erkennungsverfahren deutlich. Euklid und Hamming haben grundsätzlich eine niedrigere Erkennungsrate.

Richtige Klassifizierung		Euklid	Hamming	GMM	RBF
Feature-Vektor	25	86%	87%	96%	91%
Dimension	21	84%	86%	97%	95%
	15	86%	88%	96%	89%
	9	77%	75%	91%	82%

5. Exkurs: FAR und FRR bei der Verifikation

Mit False Accept Rate FAR (oder False Match Rate) bezeichnet man bei der Verifikation die Wahrscheinlichkeit, dass ein Unberechtigter vom System akzeptiert wird, die False Reject Rate FRR (oder False Non-Match Rate) gibt die Wahrscheinlichkeit an, dass ein Berechtigter vom System abgewiesen wird.
Bei nahezu jedem biometrischen Erkennungsverfahren kann man eine Schwelle (den sog. Threshold) einstellen, ab der eine Person abgelehnt, bzw. akzeptiert wird. Beispielsweise wird im GMM-Verfahren der Handgeometrie immer eine Wahrscheinlichkeit berechnet, mit der der zu verifizierende Benutzer auch tatsächlich zu der von ihm angegeben Klasse gehört. Hier wäre der Threshold also eine Mindestwahrscheinlichkeit, die für eine erfolgreiche Verifikation gegeben sein muss. Analog nimmt man beim Euklid- und Hamming-Verfahren den berechneten Abstand als Schwelle. Je höher der Threshold, desto genauer muss der gemessene Vektor mit dem Template übereinstimmen.
Die FAR, aufgetragen gegen den Threshold ist i.A. eine monoton fallende Funktion, d.h. je strenger die Grenze gesetzt wird, desto weniger Betrüger werden akzeptiert, gleichzeitig werden aber auch einige Berechtigte zurückgewiesen. Den Punkt, bei dem die Wahrscheinlichkeiten von FRR und FAR gleich sind, nennt man Equal Error Rate (ERR). In der Praxis wird man den Treshold bei Sicherheitsrelevanten Anwenungen höher einstellen und in Kauf nehmen, dass mehr berechtigte Benutzer abgewiesen werden, während man in der Kriminialistik den Threshold (z.B. bei Gesichtserkennung) niedriger einstellt und Verdächtige dann mit konventionellen Methoden näher untersucht.

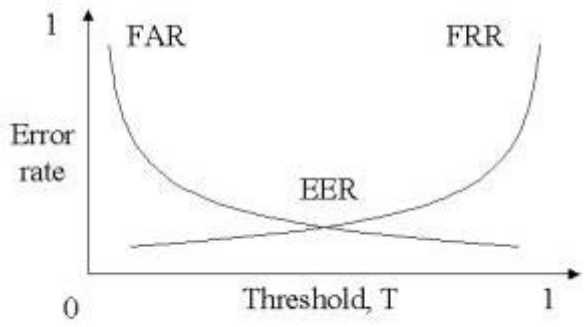

Abb.: FAR und FRR in Abhängigkeit des Thresholds

6. Zusammenfassung

Handgeometrische Systeme können durch ihre relativ günstigen Anschaffungskosten gut für mittlere Sicherheitsbereiche wie z.B. Arbeitszeitüberwachungssysteme, Zutrittskontrollen in Universitäten und Bibliotheken eingesetzt werden. Die Erkennungsraten sind im Vergleich zum Experiment der Universität Madrid mittlerweile deutlich angestiegen, die False Acceptance Rate (FAR) liegt bei heutigen Systemen zwischen 0.0001% und 0.1% und die False Reject Rate (FRR) zwischen 0.0007% und 1.0%.

Literaturverzeichnis:

1. Biometric Identification through Hand Geometry Measurements, Raul Sanchez-Reillo, Carmen Sanchez-Avila, Ana Gonzalez-Marcos, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 10, October 2000
2. http://www.handreader.com/, Recognition Systems Inc.
3. On the Error-Reject Trade-Off in Biometric Verification Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, July 1997
4. Biometric Decision Landscapes, John Daugman, Technical Report TR482, University of Cambridge, Computer Laboratory, 1999
5. Biometrics Work Group, Best Practices in Testing and Reporting Performance of Biometric Devices, Version 1.0, 12 January 2000