

Biometrische Identifikationssysteme
Seminar SS 2004
Matthias Schwan

Dynamische und Statische Unterschrift
Nora Popp
Yvonne Gläser

Inhaltsverzeichnis

1. Einleitung
- 1.1 Das Biometrische System
2. Die Unterschrift
- 2.1. Biometrische Bedeutung der Unterschrift
- 2.2. Ansätze der Unterschriftenverifikation
3. Offline-Verifikation
- 3.1. Aufbereitung der Daten
- 3.2. Segmentierung der Daten
- 3.3. Vergleich der Daten
- 3.4. Praxisbeispiel
4. Online-Verifikation
- 4.1. Ablaufschema einer Online – Erkennung
- 4.2. Datenerfassung
- 4.3. Merkmalsextraktion
- 4.4. Vergleich der Daten
5. Die Bedeutung des Schwellwertes
6. Strichreferenzen
7. Einschätzung
8. Literaturverzeichnis

1. Einleitung

Die Biometrie bezeichnet vor allem in den naturwissenschaftlichen Zweigen wie Biologie oder auch Medizin, auf die Erfassung und Vermessung von Lebewesen und ihren Eigenschaften. Im Mittelpunkt dieser Ausarbeitung steht der Begriff Biometrik als die automatisierte Messung eines individuell-physiologischen oder verhaltenstypischen Merkmals einer Person zum Zweck der biometrischen Identifikation bzw. Authentifizierung und somit zu einer Unterscheidung von anderen Personen.

Zu den physiologischen Merkmalen (passive) zählen das Gesicht, die Iris, das Fingerbild oder auch die Hände, zu den verhaltenstypischen Merkmalen (aktive) die Stimme und, das Thema dieser Ausarbeitung, die Unterschrift.

Für all diese Merkmale sind folgende Eigenschaften, um sie in einem biometrischen Identifikationssystem zu nutzen, wichtig: Universalität, Einzigartigkeit, Beständigkeit und Erfassbarkeit.

1.1. Das biometrische System

Die Grundlage eines jeden biometrischen Systems, unabhängig vom genutzten Merkmal oder der angewandten Technik, ist das Enrolment. Es handelt sich hierbei um das erstmalige Erfassen oder auch Vermessen des biometrischen Merkmals des späteren Nutzers. Zum Prozess des Enrolments gehört auch die Umwandlung der gewonnenen Daten in einen Referenzdatensatz und die anschließende Speicherung des so gewonnenen Templates.

In den ,dann folgenden, biometrischen Überprüfungen werden die neuen Messdaten mit dem gewonnenen Template verglichen. Hierbei sollte ein hohes Maß an Übereinstimmung vorhanden sein.

Eine biometrische Überprüfung kann durch eine Identifikation oder Verifikation stattfinden. Bei einer Identifikation findet ein 1:n Vergleich statt, dessen Ziel es ist festzustellen um welche Person es sich handelt. Die Verifikation erfolgt durch einen 1:1 Vergleich, hier wird geklärt, ob es sich bei der Person, die erkannt werden will, auch um diejenige handelt, für die sie sich ausgibt.

Im Folgenden möchten wir noch kurz auf einige Kenngrößen eingehen die zur Bestimmung der Leistungsfähigkeit eines biometrischen Systems von Bedeutung sind. Zu nennen sei zu

Beginn die sogenannte Toleranzschwelle, sie ist ein Wert für den Grad der Übereinstimmung von Referenz – und Messdaten. Ab diesem Wert oder dieser Schwelle wird eine Identifikation sowie Verifikation als erfolgreich betrachtet.

Es ist in diesem Zusammenhang darauf zu verweisen, dass somit auch Nutzer fälschlicherweise zurückgewiesen werden oder fälschlicherweise akzeptiert werden können.

Die Rate falscher Ablehnung (FRR = False Rejection Rate) sowie die Rate falscher Akzeptanz (FAR = False Acceptance Rate) müssen empirisch ermittelt werden. Diese beiden Raten stehen derart in Zusammenhang, dass ein Absenken der einen einen Ansteigen der anderen mit sich zieht oder umgekehrt.

Beide Raten werden direkt durch die Wahl der bereits erwähnten Toleranzschwelle beeinflusst. Wir sprechen bei einer Gleichheit der FAR und FRR von der EER, der Equal Error Rate. Zum Schluss möchten wir noch auf die False Enrolment Rate (FER) hinweisen, die Rate fehlerhafter Registrierungsversuche bzw. Enrolmentversuche.

2. Die Unterschrift

Die Bedeutung unserer Unterschrift besteht schon seit Jahrhunderten unter anderem in ihrer gesellschaftlichen Akzeptanz als weltweites Authentifizierungsmerkmal. Sie ist den meisten kulturellen Traditionen ein rechtsgültiges Symbol des Einverständnisses zum Inhalt eines Dokuments. Seit jeher werden Kaufverträge, Testamente oder auch Friedensverträge durch Unterschriften bestätigt.

Die Entwicklung unserer Handschrift und somit auch unserer Unterschrift vollzieht sich in der Auseinandersetzung mit der in der Schule gelehrtten Ausgangsschrift.

Sie wird durch den jeweiligen Zeitstil geprägt und aufgrund verschiedener Schreibvorlagen und Lerntechniken treten Variationen auf.

Unser persönlicher Schreibstil ist durch ein personenspezifisches Schreibtraining zu einer sensorischen Fertigkeit aufgebaut worden. Für das Schreiben werden Arm-, Handgelenk-, und Fingerbewegungen überlagert. Diese Überlagerungen müssen in einer festen zeitlichen Abfolge und exakt aufeinander abgestimmt sein. Interessant ist, dass wir, trotz des hohen Maßes an Koordination und Exaktheit, als geübte Schreiber nahezu unbewusst schreiben.

2.1. Biometrische Bedeutung der Unterschrift

Die Unterschrift ist das einzige aktive biometrische Merkmal welches nicht zufällig abgegeben wird, sie kann nicht verloren gehen, gestohlen werden und im Normalfall nicht vergessen werden. Eine Unterschrift zu erzwingen ist sicher möglich, ob aber die unter Stress abgegebene Unterschrift eine Identifikation oder Verifikation ermöglicht, kann angezweifelt werden. Sie zählt leider zu den am wenigsten akkuraten biometrischen Merkmalen, da sie sehr abhängig vom Nutzerverhalten ist. Jenes kann durch Stress oder auch Krankheit stark beeinflusst werden, aber auch generell verändert sich unsere Handschrift im Laufe des Lebens.

Eine Konstanz im Hinblick auf zum Beispiel völlige Deckungsgleichheit bei wortgleichen Schriftzügen ist nicht gegeben.

Abb. 1



Abb. 1 Variation der 20 Unterschriften von 4 Personen

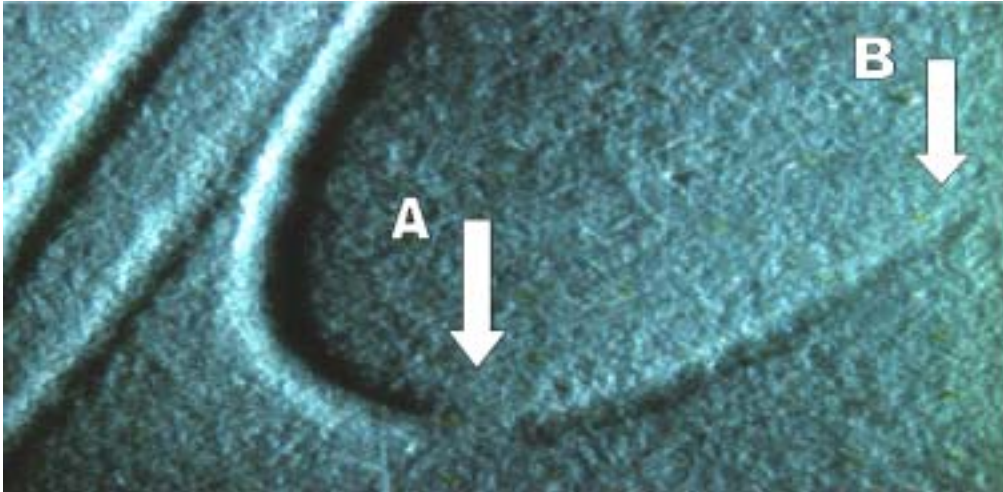
Jede Schrift weist auch unter gleichbleibenden Bedingungen eine mehr oder minder große natürliche Schwankung auf .

2.2 Ansätze zur Unterschriftsverifikation

Schon seit langem wird in forensischen Schriftgutachten mit dem statischen Abbild der Handschrift gearbeitet. Zugleich werden auch die dynamischen Merkmale der Handschrift

wie zum Beispiel Strichbeschaffenheit, Druckgebung, Bewegungsrichtung aber auch Kugelschreiberpasten mit Hilfe eines Stereomikroskops (Abb. 2) untersucht.

Abb. 2 Aufnahme eines Stereomikroskops



Zu erwähnen seien vielleicht noch die Graphologen, die anhand der statischen Unterschrift Rückschlüsse auf die Persönlichkeit des Schreibers ziehen.

Innerhalb der Unterschrift-Erkennung unterscheiden wir nun zwischen der statischen Unterschrift und der dynamischen Unterschrift.

Die statische Unterschrift, auch Offline - Signatur genannt, bezieht sich auf das sichtbare schriftliche Abbild. Eine dynamische Unterschrift wird auch als Online – Signatur genannt und schließt die Betrachtung dynamischer Merkmale wie Druck oder auch die Stiftausrichtung mit ein.

3.Offline-Verifikation

Eine Offline – Verifikation vollzieht sich folgendermaßen, zumeist liegt eine Unterschrift auf einem Blatt Papier vor. Das wird dann, mit zum Beispiel einem Scanner in den Computer eingelesen und liegt dort als Bild eines binären, grauwertigen Feldes vor.

3.1. Aufbereitung der Daten

Die Aufbereitung der vorliegenden Daten wird mit Hilfe folgender Algorithmen vollzogen. Zu Beginn wird die Schrift durch Binarisierungsverfahren vom Hintergrund separiert. Eine mögliches Binarisierungsverfahren ist die Verwendung von Intensitätsschwellen. Man geht davon aus, dass die Schrift gegenüber dem Hintergrund dunkel ist. Es wird dann per Schwellwertverfahren ein Pixel als Vordergrundpixel klassifiziert, sofern seine Intensität kleiner als der Schwellwert ist, ansonsten wird der Pixel dem Hintergrund zugeordnet. Oftmals findet dann eine Skelettierung des Bildes statt, so dass die Strichbreite auf ein Pixel ausgedünnt wird, der Vorgang wird auch als Thinning bezeichnet. Desweiteren werden etwaige Störpixel durch das sogenannte Smoothing ausgeschlossen. Als eine weit vorbereitete Methode sei hier das Glätten durch eine Gaußfunktion genannt. Außerdem werden noch Normalisierungsschritte (Normalization) durchgeführt, um die schreiber – und situationsbedingte Variabilität zu kompensieren. Dabei wird üblicherweise die Schrift horizontal ausgerichtet und Schriftgröße sowie Schriftneigung korrigiert.

Im praktischen System werden aber nicht alle Algorithmen zusammen benötigt beziehungsweise angewandt.

3.2. Segmentierung der Daten

Es gibt Systeme die nach einer Vorverarbeitung der Daten noch eine Segmentierung der Daten vornehmen, da sie nicht mit isolierten Wörtern (Wortmodellen) arbeiten können. Mit der Segmentierung ist die Unterteilung des Signals in Einheiten, die Buchstaben, Wörtern oder Strichen entsprechen gemeint. Sie dienen später als Grundlage für die Klassifikation.

3.3. Vergleich der Daten

Der Vergleich der Daten vollzieht sich nun entweder mit Hilfe statistischer Methoden oder durch neuronale Netzwerke. Zu den statistischen Methoden zählen die linearen Klassifikatoren, nächster Nachbar Klassifikator sowie k-nächster Nachbar Klassifikator, ebenso kommt hier der Treshold-Klassifikator zum Einsatz.

Bei den neuronalen Netzwerken spielen back propagation network, fuzzy ARTMAP sowie multi-layer perception neural network eine Rolle.

Eine Vielzahl von Systemen basiert darauf, dass mehrere Klassifikatoren die Unterschrift unabhängig voneinander verifizieren. Eine Akzeptanz oder Nichtakzeptanz ist dann eine Mehrheitsentscheidung der Klassifikatoren. Eine andere Möglichkeit ist die Festsetzung des Akzeptanzgrades durch die Klassifikatoren und dann eine Entscheidung mit Hilfe von Fuzzy-Theoremen.

3.4. Praxisbeispiel

Als ein Beispiel aus der Praxis sei kurz das Produkt SignCheck der Firma SoftPro vorgestellt. Bei diesem Produkt arbeiten Komponenten der Netzwerktechnologie und Fuzzy Logik zusammen.

Das Modul SignCheck kalkuliert, extrahiert und gewichtet 60 verschiedene primäre und 500 sekundäre statische Merkmale und fasst diese in Parametervektoren zusammen.

Zu den charakteristischen Merkmalen zählen beispielsweise Bogenformen, Aufstriche, Hüllkurven, Abzweigungen sowie Schleifen.

Abb. 3

Merkmalsvergleich zweier Unterschriften - Beispiele



Abb. 4

Einzelmerkmale - Beispiele



Nach der Berechnung der Vektoren wird ein Ähnlichkeitsgrad zwischen der Unterschrift und den Referenzunterschriften ermittelt. Wenn ein gewünschtes Minimum an Ähnlichkeit nicht erreicht wird, ist es möglich den Vorgang zu einer visuellen Überprüfung weiterzuleiten.

4. Online-Erkennung

Die Online – Erkennung bezieht sich nicht nur auf das schriftliche Abbild sondern bindet in die Betrachtung auch die dynamischen Merkmale einer Unterschrift mit ein.

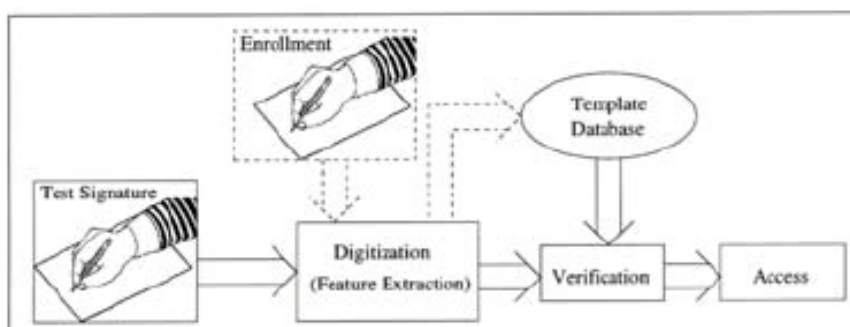
Zu den typischen Merkmalen gehören die Schreibgeschwindigkeit, der Schreibdruck, der Stiftwinkel, aber auch die Dauer des Schreibens. Diese dynamischen Merkmale sind von Person zu Person verschieden. Sie spiegeln individuelle Schreibverhaltensmuster wider und sind deshalb nur sehr schwer zu immitieren.

Die Art und Zahl der verwendeten Merkmale variiert je nach Hersteller von 5 bis weit über 40 Merkmalen. Sie werden mit Hilfe von speziellen Pads oder Stiften in Echtzeit, während des Schreibvorgangs, erfasst und digitalisiert..

4.1. Ablaufschema einer Online-Erkennung

Das Prinzip der Online – Erkennung entspricht dem vieler anderer biometrischer Systeme.

Abb. 5



Zu Beginn werden die Referenzdaten erfasst (Enrollment). Da die Unterschrift eines Nutzers nie völlig gleich ausfallen kann, muss ein Kennfeld aus mehreren Unterschriften (Template) erstellt werden, in welchem die später zu erkennende Unterschrift liegen muss.

Diese Daten werden in einer Datenbank hinterlegt und mit einer persönlichen ID versehen.

Das System benutzt die ID-Information um die Referenzdaten zu extrahieren und diese mit den Werten der neueingegebenen Unterschrift zu vergleichen.

Wenn sich ein Nutzer verifizieren will, werden die Referenzdaten mit den extrahierten Daten der neu geleisteten Unterschrift, durch Berechnung der Ähnlichkeit, verglichen. Anhand eines vordefinierten Schwellwertes (Treshold) wird die Unterschrift akzeptiert oder nicht.

Nachdem eine Unterschrift als echt erkannt wurde, kann ein Teil der alten Daten durch den entsprechenden Teil an neu aufgezeichneten Daten ersetzt werden. Somit können die Referenzdaten dem Veränderungsprozess einer individuellen Unterschrift angepasst werden.

4.2. Datenerfassung

Um die dynamischen Merkmale eine Unterschrift zu erfassen, sind spezielle Pads oder Stifte notwendig. In diesen Geräten befinden sich Drucksensoren, die den Verlauf der Unterschrift aufzeichnen. Aus den so so gewonnenen Daten können die einzelnen Parameter, wie Geschwindigkeit und Druck, extrahiert und weiterverarbeitet werden.

Ein Beispiel für die Unterschriftserkennung via Schreibpad ist das „Hesy Signature Pad“.

Abb.6



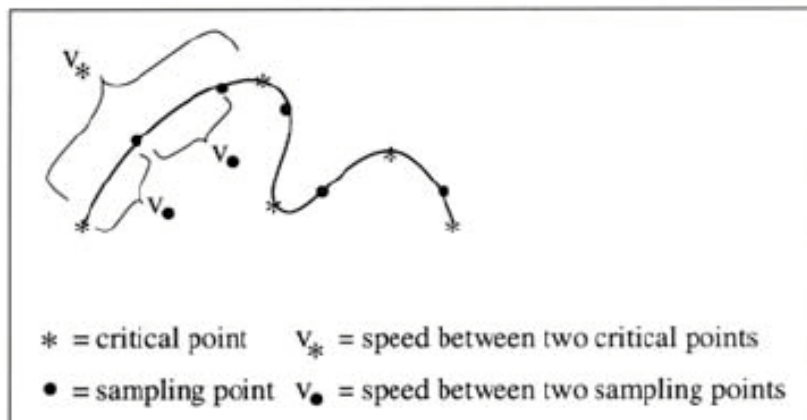
4.3. Merkmalsextraktion

Die Merkmale einer online-Signatur können in zwei Klassen unterteilt werden: die statischen und die dynamischen Merkmale. Sie werden als Parameter und Funktionen betrachtet.

Die Parameter werden normalerweise durch Merkmalsvektoren repräsentiert. Sie werden über den gesamten Schreibprozess ermittelt, wie z.B. die durchschnittliche Schreibgeschwindigkeit, die maximale Schreibgeschwindigkeit, das Maß der Krümmung, das Verhältnis von langen und kurzen Strichen, die Länge der einzelnen Segmente, etc.

Abbildung 7 zeigt, wie die Schreibgeschwindigkeit an lokalen Punkten mit relativer bzw. absoluter Geschwindigkeit erfasst wird.

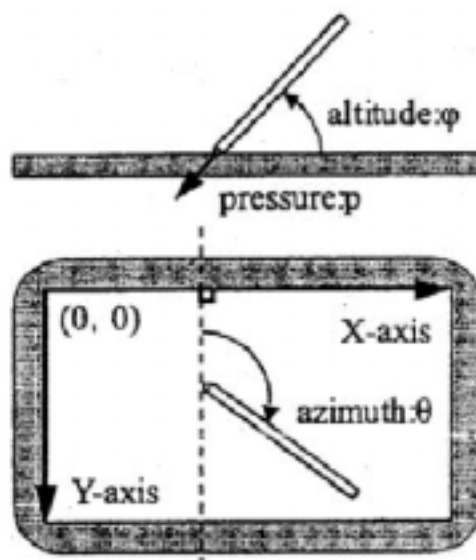
Abb. 7



Die dynamischen Merkmale stellen die Unterschrift als Funktion der Zeit dar und beziehen sich auf jeden Moment des Schreibvorgangs. Diese Merkmale können als eine Menge von Zeitfunktionen repräsentiert werden, wie z.B. die Stiftposition $x(t), y(t)$, die Geschwindigkeit $v(t)$, die Beschleunigung $a(t)$, der Druck $p(t)$, etc.

In manchen Methoden wird auch die Stiftneigung und das Auf- und Absetzen des Stiftes betrachtet.

Abb. 8



4.4. Vergleich der Daten

Wenn sich ein Nutzer verifizieren will, muss das System die benötigten Parameter der Unterschrift extrahieren und in geeigneter Form (Merkmalsvektoren, Zeitfunktionen) verarbeiten. Danach wird ein Ähnlichkeitsmaß berechnet und mit einem vordefinierten Schwellwert verglichen, um zu entscheiden, ob die abgegebene Unterschrift akzeptiert oder zurückgewiesen wird. Wenn die neue Unterschrift eine hinreichend große Ähnlichkeit zu einer der Referenzunterschriften aufweist, wird das System akzeptieren. Hat sie jedoch zu keiner der Referenzunterschriften eine hinreichend große Ähnlichkeit, wird sie vom System nicht akzeptiert.

Vergleichsmethoden

Gewichteter Abstand

Diese Methode wird hauptsächlich in Systemen benutzt, die mit Parametern arbeiten. Die neu abgegebene Unterschrift und die Referenzdaten werden als Merkmalsvektoren dargestellt. Die Ähnlichkeit wird aus dem gewichteten Abstand zwischen diesen Vektoren ermittelt. Die Gewichte werden mit Hilfe einer Trainingsmenge von Unterschriften der jeweiligen Person errechnet.

Statistische Methoden

Diese Methoden arbeiten mit Parameterwerten und die bedingte Wahrscheinlichkeit einer Referenzunterschrift bei gegebener neuer Unterschrift [$P(R|U)$, Bayes-Theorem] wird als die Ähnlichkeit zwischen Input und Referenz betrachtet. Die Wahrscheinlichkeitsmodelle werden vorher mit Hilfe von Trainingsdaten gelernt.

Weitere wichtige Methoden arbeiten mit *Neuronalen Netzen*, *Dynamic Time Warping* und *Hidden-Markov-Modellen*.

5. Die Bedeutung des Schwellwertes

Die Frage nach einem geeigneten Schwellwertes hängt stark vom Einsatzbereich des Erkennungssystems ab, da durch ihn die Akzeptanzrate beeinflusst wird. In den meisten Systemen wird ein globaler, für alle Nutzer gleicher, Wert verwendet. Es ist jedoch auch möglich den Schwellwert individuell anzupassen.

Wird die Schwelle zu tief angesetzt, nimmt die FAR zu und die FRR dagegen ab. Deshalb wird meist ein Schwellwert verwendet, bei dem FAR und FRR gleich sind. Die totale Fehlerrate wird so am niedrigsten gehalten.

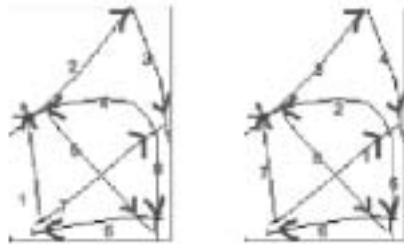
Bei Handschrift - bzw. Unterschriftsystemen oder -verfahren wird meistens mit einer Templategröße von 400-1.500 Bytes gearbeitet, die Verifikationszeit beträgt 5 – 15 Sekunden, eine Registrierungszeit ca. 30 Sekunden. Die False Acceptance Rate beträgt von 0,5 bis zu 20 %, die False Rejection Rate beträgt 2,8 bis 25 %.

6. Strichreferenzen

Eine andere Möglichkeit zur schriftlichen Verifikation bezieht sich nicht mehr auf den kompletten Unterschriftzug, sondern auf die Auswertung von Strichinformationen. Hierbei ist die Strichneigung das wichtigste Charakteristikum, welche an kurzen Teilstrichen aus Start- und Endkoordinaten bestimmt wird. Auch bei diesem Verfahren handelt es sich um dynamische Schrifterkennung. Zu jeder Strichrichtung wird die mittlere Stiftneigung und der mittlere Schreibdruck in der Referenzdatenbank gespeichert. Je nach Genauigkeit wird zwischen 8, 10,12 oder mehr Strichrichtungen unterschieden, von denen auch in diesem Fall mehrere Referenzen abgegeben werden müssen. Zum Vergleich der Schriftähnlichkeit wird jeweils der Winkel zwischen Referenzdaten und den aquirierten Daten einer jeden Richtung bestimmt.

Durch diese Methode ist es möglich, auch andere Worte und sogar kleine Bilder zur Verifikation zu verwenden. Der Nutzer kann sein „Passwort“ beliebig oft wechseln und nur die Strichrichtungen müssen im Schriftzug erkennbar sein.

Abb. 9 Das Haus vom Nikolaus

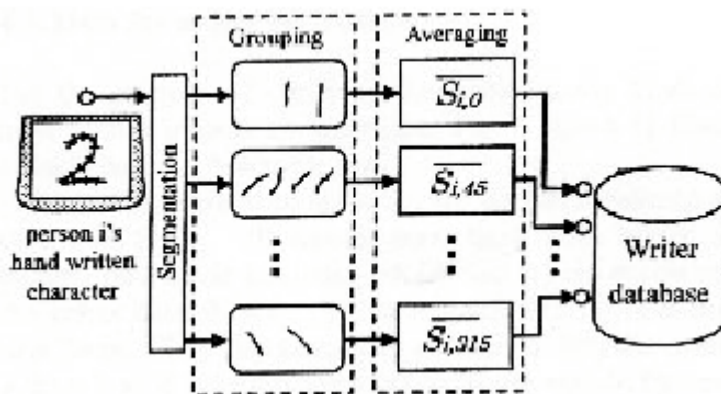


Erstellen von Strichreferenzen

Der Schreibvorgang wird wieder anhand des Stiftdrucks erkannt

Ein Schriftzug wird in einzelne Teilbereiche (vorher festgelegte Zeitintervalle) untergliedert und diese Segmente werden nach Strichen mit ähnlichen Richtungen gruppiert. Die Richtung eines Segments kann durch die x-y-Position des Start- und Endpunktes bestimmt werden. Strichinformation einer Richtung (Stiftneigung) werden gemittelt.

Abb. 10



7. Einschätzung

Welche Stärken und Schwächen hat das System der biometrische Unterschrifterkennung?

Als erstes sei der Vorteil der hohen Nutzerakzeptanz genannt. Mit der Unterschrift bekunden wir unseren freien Willen, wir geben sie nur wenn wir möchten und es ist uns möglich damit Abläufe zu steuern. Der Aspekt der menschlichen Aktion integriert zugleich auch den wichtigen Punkt der Lebenderkennung. Als positiv betrachtet wird die Möglichkeit, solche Systeme an konventionelle Systeme anzuschließen.

Einen Nachteil ergeben die natürlichen Schwankungen der Unterschrift. Sie erschweren eine eindeutige Verifikation. Desweiteren bleibt die Möglichkeit, eine fremde Unterschrift zu trainieren und zu fälschen. Dies wird jedoch bei der dynamischen Unterschriftenerkennung weitgehend ausgeschlossen, da ein potentielle Fälscher kein Feedback über die dynamischen Merkmale einer Unterschrift erhält, und sie somit auch nicht nachahmen kann.

In der Praxis findet die Unterschriftenerkennung zumeist bei Kreditinstituten Anwendung (Unterschriftüberprüfung bei Transaktionen), aber auch eine Kombination von klassischer Unterschrift und digitaler Signatur wird angeboten .

8. Literaturverzeichnis

- T. Petermann, A. Sauter, "Biometrische Identifikationssysteme - Sachstandsbericht", Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Arbeitsbericht Nr.76, Februar 2002.
- G. Lassmann (edt.), "Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren", TeleTrust Deutschland e.V., AG6 Biometrische Identifikationsverfahren, Version 2.0, Juli 2002.
- D.D. Zhang, "Automated Biometrics - Technologies and Systems", Kluwer Academic Publishers, 2000.
- S. Nanavati, M. Thieme, R. Nanavati, "Biometrics - Identity Verification in a Networked World", A Wiley Tech Brief, John Wiley & Sons, Inc, 2002.
- Josef Scharinger, "Online Signatur Verifikation", Paper, Seminar SS2004, Universität Linz
- Michael Speckner, "Unterschriftenerkennung", Paper, Hauptseminar WS 2003/2004, Universität Ulm
- Prof. Dr. Heinz-Michael Winkels, „IT-Sicherheit“, Paper, Februar 2003, Fachhochschule Ulm
- Norman Richnow, Sascha Schimke, Andreas Peuler, „Vorstellung und Vergleich zweier Verfahren zur On-line Handschrift Verifikation“, Paper
- <http://www.softpro.de/>
- <http://www.hesy.de/>
- <http://www.cs.uni-magdeburg.de/~sschimke/mus/>