

Das EU-Projekt »3D Face«.  
3-D-Gesichtserkennung für die unbeaufsichtigte  
Grenzkontrolle

Christoph Busch, Alexander Nouak

2. Februar 2007

Beitrag zum

10. Deutschen IT-Sicherheitskongress  
des Bundesamtes für Sicherheit in der Informationstechnik

im Themenbereich »2 Identitätsmanagement«

Prof. Dr. Christoph Busch  
Alexander Nouak  
Fraunhofer-Institut für Graphische Datenverarbeitung IGD  
Fraunhoferstraße 5  
64283 Darmstadt  
Telefon: +49 6151 155-147  
Fax: +49 6151 155-499  
E-Mail: christoph.busch@igd.fraunhofer.de  
alexander.nouak@igd.fraunhofer.de

# Das EU-Projekt »3D Face«.

## 3-D-Gesichtserkennung für die unbeaufsichtigte Grenzkontrolle

### Inhaltsverzeichnis

<b>1</b>	<b>Hintergrund</b>	<b>1</b>
<b>2</b>	<b>Gesichtserkennungsverfahren</b>	<b>2</b>
<b>3</b>	<b>Dreidimensionale Gesichtserkennung</b>	<b>3</b>
<b>4</b>	<b>Projektziele</b>	<b>4</b>
<b>5</b>	<b>Ausblick</b>	<b>12</b>

### Zusammenfassung

Seit November 2005 sind biometrische Daten in allen neu ausgestellten deutschen Reisepässen integriert. Die zusätzliche Nutzung von dreidimensionalen Modellen verspricht erhebliche Leistungssteigerungen für die Grenzkontrolle. Durch die Kombination von Informationen zur Geometrie sowie zur Gesichtstextur können 3-D-Gesichtserkennungssysteme Posenvariationen und schwierige Lichtverhältnisse bei der Aufnahme besser verarbeiten.

Um das Potenzial der dreidimensionalen Gesichtserkennung zu ermitteln, startete im April 2006 das durch die Europäische Kommission geförderte Projekt *3D Face*. Der Beitrag beschreibt den Ansatz und die Forschungsziele in diesem Projekt: So sollen nicht nur bessere Erkennungsleistungen erzielt, sondern auch eine neue, fälschungssichere Aufnahmetechnik entwickelt werden. Zudem wird an Verfahren gearbeitet, die gespeicherte Template-Daten in der biometrischen Referenz schützen.

## 1 Hintergrund

Die Verordnung des europäischen Rates aus dem Jahr 2004 über die Standardisierung von Sicherheitsmerkmalen und Biometrie in Pässen für EU-Bürger [Eur04] führten die Verwendung digitaler Gesichts- sowie Fingerbilder in allen künftig ausgegeben EU-Pässen ein. Gleichzeitig werden die von der International Civil Aviation Organization (ICAO) erarbeiteten technischen Spezifikationen mit dem Passstandard 9303 für die Speicherung biometrischer Daten in maschinenlesbaren Reisedokumenten [Int04a], [Int06] in allen Mitgliedsstaaten der europäischen Union umgesetzt, um die Unterstützung der Grenzkontrollen durch biometrische Verfahren zu befördern. Seit November 2005 sind bereits elektronische Gesichtsbilder in allen neu ausgestellten deutschen Reisepässen integriert. Aktuell wird durch die Änderung des Passgesetzes die Integration von Fingerbildern vorbereitet [Deu07].

Gemäß den Empfehlungen der ICAO wird die biometriegestützte Grenzkontrolle primär auf den Verfahren zur 2-D-Gesichtserkennung aufbauen. Die Nachteile dieser Verfahren sind hinlänglich bekannt: Die Leistungsfähigkeit solcher Systeme ist vor allem deshalb nicht zufriedenstellend, weil Unterschiede in der Ausrichtung des Gesichts (*Pose*), Lichtveränderungen und andere Störfaktoren die Bildqualität beeinträchtigen und ggf. im Vergleich zur Referenzaufnahme verschlechtern können. Noch gravierender ist der Umstand, dass 2-D-Gesichtserkennungssysteme bislang über keine robusten Mechanismen zur Lebenderkennung und zur Überwindungssicherheit verfügen. Demzufolge ist ein zuverlässiger Einsatz dieser Technologie in unbeaufsichtigten Umgebungen derzeit nicht zu realisieren.

Das im April 2006 gestartete und durch die Europäische Kommission innerhalb des 6. Forschungsrahmenprogramms geförderte Projekt *3D Face* konzentriert sich auf die Erforschung der Verfahren zur 3-D-Gesichtserkennung, bindet aber die Verfahren der 2-D-Gesichtserkennung und deren Einsatz in sicheren Umgebungen in die Entwicklung mit ein [3D 06]. Dabei werden Ansätze verfolgt, die reichhaltigen Informationen zu nutzen, welche die Geometrie der Gesichtsoberfläche bietet. Es wird mit den Verfahren der 3-D-Gesichtserkennung einerseits eine signifikante Verbesserung der Erkennungsleistung erwartet und andererseits ein Aufnahmesystem erstellt, das resistent gegenüber Fälschungen ist. Dies ist Voraussetzung für möglicherweise nicht überwachte Grenzkontrollen [Int04b].

## 2 Gesichtserkennungsverfahren

Die Gesichtserkennung ist das biometrische Verfahren, das der Mensch selbst am häufigsten zur Erkennung verwendet. Während dabei jedoch intuitiv Kontextinformationen wie Körperform und -größe zusätzlich analysiert werden, stehen diese Parameter einem computergestützten Gerät zunächst nicht zur Verfügung. Die in der biometrischen Gesichtserkennung bislang eingesetzten Systeme verwenden im Normalfall eine Foto- oder Videokamera, um zweidimensionale Frontalbilder zu erfassen. Systeme, die auf diesen Sensoren aufbauen, verarbeiten das 2-D-Bild und müssen zunächst das eigentliche Gesicht im Kamerabild lokalisieren und herausfiltern. Ein Frisurwechsel, aber auch Bärte und Brillen können die Aufgabe für den Gesichtsfindungsalgorithmus erschweren.

Bei der zweidimensionalen Gesichtserkennung ist es unerlässlich, dass das Bildmaterial in sehr guter Bildqualität vorliegt. Wichtige Kriterien sind dabei eine ausreichende Ausfüllung des 2-D-Bildes durch das Gesicht (etwa zu 70%), eine Frontalaufnahme, guter Kontrast, Bildschärfe, gleichmäßige Ausleuchtung, ein neutraler Gesichtsausdruck und keine Verdeckung des Gesichtes bzw. der Landmarken (z. B. Augenwinkel bzw. Mittelpunkte der Augen) durch Haare, Brillen oder Kopfbedeckungen. Werden diese Bildqualitätskriterien nicht erfüllt, muss mit einer schwachen Erkennungsleistung des biometrischen Systems gerechnet werden.

Die Einhaltung all dieser Kriterien sowohl bei der Aufnahme des Referenzbildes (Passausstellung) als auch beim späteren Vergleich (bei der Grenzkontrolle) ist schwer herzustellen: Nur selten wird die Gesichtsausrichtung (*Pose*), der Gesichtsausdruck (*Mimik*) und die Beleuchtungssituation identisch sein.

Ein weiterer Nachteil ist, dass zweidimensionale Gesichtserkennung naturgemäß keine Überwindungssicherheit leisten kann. So lassen sich die Sensoren in aller Regel durch das Vorhalten

eines ausgedruckten Fotos oder auch das Abspielen eines Videos von einer zugangsberechtigten Person durch Zuhilfenahme eines einfachen Laptops täuschen. Selbst die Bildqualität eines Fotohandys war in eigenen Experimenten bereits ausreichend, um ein Produkt-System zu überwinden. Heutige Gesichtserkennungssysteme verfügen nicht über hinreichende Mechanismen, um eine Lebenderkennung zu gewährleisten. In der Konsequenz können diese Systeme nur in überwachten Umgebungen betrieben werden – bis auf weiteres müssen also die Passagen in den biometrischen Grenzkontrollspuren von einem Grenzbeamten beaufsichtigt werden.

### 3 Dreidimensionale Gesichtserkennung

Der für eine vollautomatische Grenzkontrollspur mindestens notwendige Schritt, der gegenwärtig in akademischen und industriellen Forschungslabors untersucht wird, ist der Übergang zur 3-D-Gesichtserkennung, deren Verfahren auf einer dreidimensionalen Vermessung des Gesichts beruht. Bei der Vermessung können die aus der Photogrammetrie seit langem bekannten Stereovision-Systeme oder auch Multi-Kamera-Systeme eingesetzt werden: Bei der Auswertung der Aufnahmen wird – bei bekannten Kamerastandpunkten – aus einem Satz von 2-D-Bildern nach dem Triangulationsprinzip eine Tiefeninformation errechnet [KW97]. Alternativ kann ein aktives Aufnahmesystem eingesetzt werden, das aus einer aktiven Komponente mittels Projektion farbiger Streifen oder strukturierter Muster auf das Gesicht und einem bzw. mehreren Sensoren besteht [SPB04].

Durch die Auswertung der Sensorinformation kann der Abstand zwischen Gesichtsprofil und Sensor erfasst und somit die Tiefeninformation eines Gesichts als dritte Dimension gespeichert werden. Diese Information kann über die ganze Gesichtsfläche ermittelt werden und liefert eine vollständige Gesichtsgeometrie der Person. Zusätzlich wird an jedem Oberflächenpunkt eine Farbinformation bestimmt. Das resultierende dreidimensionale Modell erlaubt eine gegenüber der einfachen Frontalaufnahme bessere Erkennung bei Kopffrotationen oder ungünstigen Kamerawinkeln. Allerdings ist je nach Messtechnik die Qualität des Modells noch zu verbessern, um Messfehler wie etwa Löcher oder Unstetigkeiten der erfassten Oberfläche zu bereinigen.

Bevor ein 3-D-Modell mit einem Referenzmodell verglichen werden kann, müssen Landmarken des Gesichtes (Augenwinkel, Nase etc.) bestimmt werden, so dass eine identische Ausrichtung der Modelle hergestellt werden kann. Dazu kann beispielsweise das *Iterative Closest Point* Verfahren eingesetzt werden [BM92], bei dem eine Ausrichtung durch Optimierung eines globalen Distanzmaßes durchgeführt wird. Erst dann können Ähnlichkeitsmaße bestimmt werden, die nun auf Geometrieinformationen wie lokalen Krümmungsmaßen oder Abstandsmaßen zwischen den geometrischen Oberflächen beruhen. Diese Geometrieinformationen sind vor allem an denjenigen Punkten der Oberfläche von Interesse, die eindeutig als Landmarke lokalisiert wurden. Zusätzlich wird die Farbinformation mittels Texturdeskriptoren ausgewertet. Ein weiterer wichtiger Vorteil der dreidimensionalen Erfassung ist die Invarianz gegenüber Skalierungen. Während bei einer zweidimensionalen Aufnahme der unbekannte Abstand der Person zur Kamera zu unterschiedlich großen Bildern führt, sind die dreidimensional erfassten Modelle immer metrisch korrekt. Dieser Vorteil der 3-D-Gesichtserkennung ist in Abbildung 3 auf Seite 6 zu erkennen. Es wird deutlich, dass bestehende Grundmaße des Kopfes – wie beispielsweise der Augenabstand – erhalten bleiben und nicht durch Umrechnung auf ein standardisiertes Bildformat

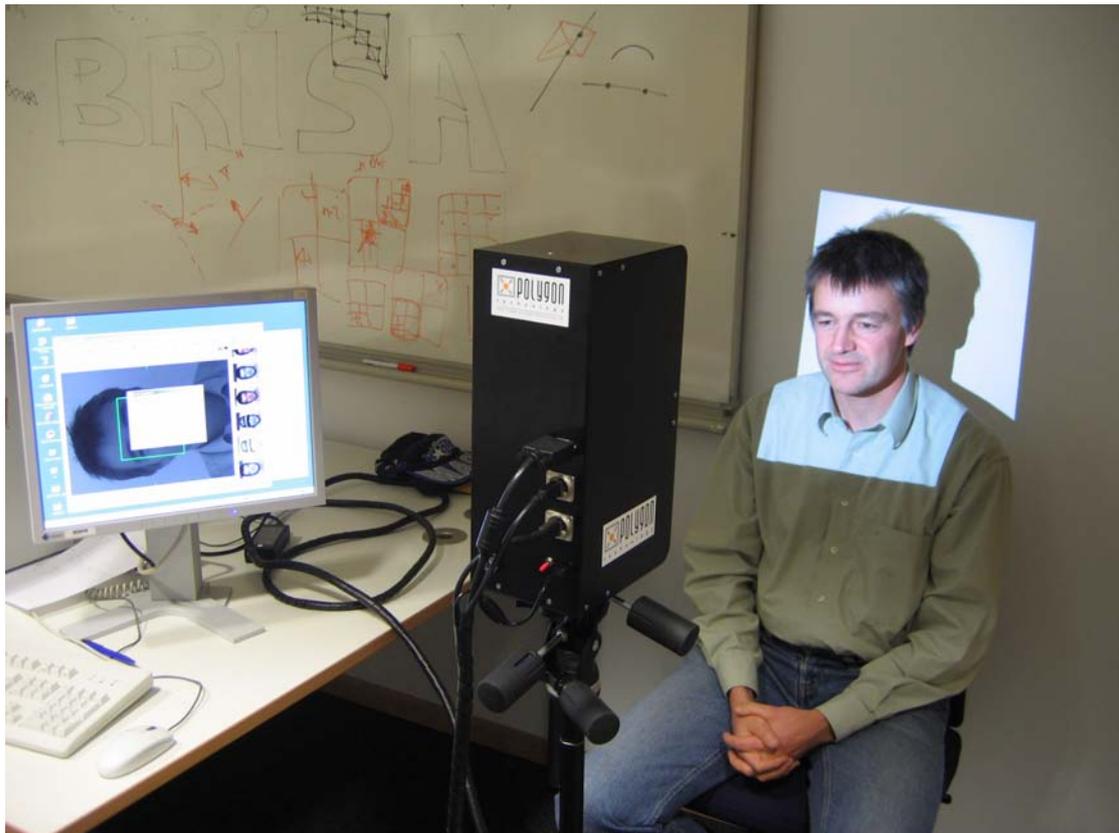


Abbildung 1: Aktives Aufnahmesystem zur dreidimensionalen Vermessung des Gesichtes

(und einheitlichen Augenabstand) verloren gehen. Diese Grundmaße können helfen, den Merkmalsraum zu unterteilen und damit die Wahrscheinlichkeit von Falsch-Akzeptanz-Fehlern (z. B. im Falle ähnlicher Textureigenschaften des Gesichts und ähnlicher Krümmungseigenschaften der Gesichtsgeometrie zwischen zwei Personen) zu reduzieren.

Bei der 3-D-Gesichtserkennung liegen gegenüber dem herkömmlichen zweidimensionalen Verfahren deutlich mehr Informationen vor, was zu einer höheren Trennschärfe für das Klassifikationsverfahren führen soll. Diese Annahme wird gestützt durch die Untersuchungen von Lu und Jain, die auf einer Datenbasis von 100 Subjekten zeigen, dass die Auswertung von 3-D- und 2-D-Informationen die Erkennungsleistung von 84% (2-D) auf 98% (3-D+2-D) steigern konnte [LJ05].

## 4 Projektziele

Das Hauptziel des Projekts *3D Face* ist es, die Leistungsfähigkeit der Verfahren derart zu verbessern, dass eine volloperative Umsetzung auf Flughäfen möglich wird. Erfahrungsgemäß lassen sich bei einem operativen Test der biometrischen Erkennungsleistung geringere Raten erzielen,

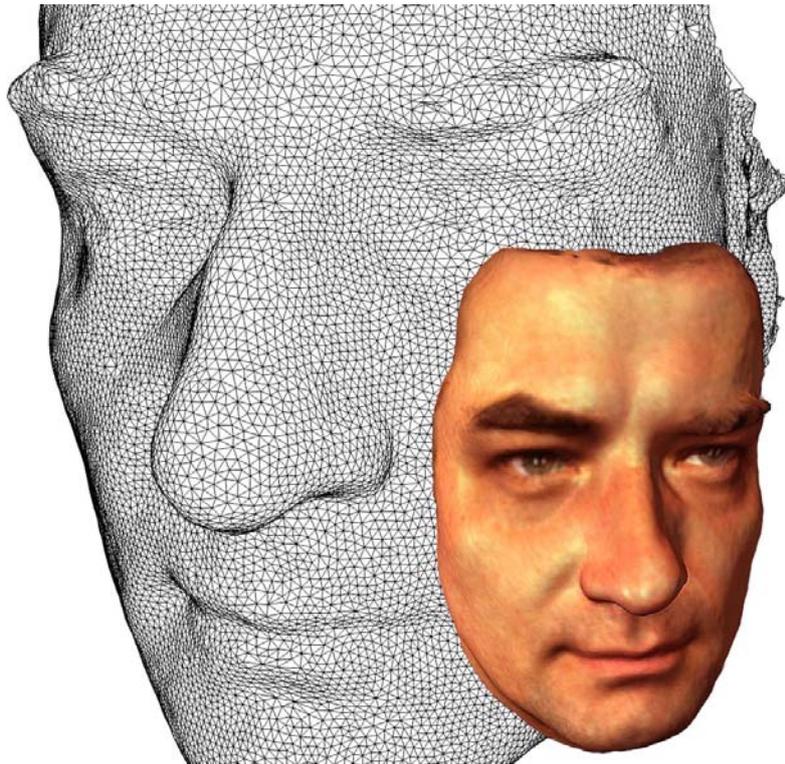


Abbildung 2: 3-D-Modell – Gesichts-Geometrie und Farbinformation

als diese bei Tests im Labor (*Technology-Testing*) beobachtet werden können, da die genannten Einflussfaktoren bei einer Pilotierung nicht equivalent kontrolliert werden können und die Varianz der zu erkennenden Muster (3-D-Modelle) deutlich größer sein wird.

Im Einzelnen verfolgt das Projekt *3D Face* die folgenden Projektziele:

#### 1. Entwicklung eines Prototypen

Ein wesentliches Anliegen bei der Entwicklung des Aufnahmesystems ist es, sowohl 3-D- als auch hochauflösende 2-D-Daten innerhalb desselben Koordinatensystems zu generieren, wobei sowohl kürzeste Aufnahmezeiten als auch minimaler Einfluss der Beleuchtungsverhältnisse angestrebt werden. Der im Projekt entwickelte Prototyp setzt als aktives System strukturiertes Licht ein. Als Komponenten kommen dabei handelsübliche Elemente zum Einsatz. Ein Projektor emittiert auf Luminiszenzdiodenbasis (LED) das Streifenmuster auf das Subjekt. Eine hochauflösende Kamera (1280 x 960 ppi) erfasst eine 2-D-Aufnahme und damit die Textur, während eine Hochgeschwindigkeitskamera mit einer Framerate von 100 fps für die Erfassung der 3-D-Daten zuständig ist. Dadurch wird eine Scandauer von etwa 0,25 Sekunden erreicht. Die generierten Daten werden als Punktwolke oder im Format VRML 2.0 im Originär-Format bereitgestellt, aus denen in einem späteren Schritt ein standardisiertes Austausch-Format abgeleitet werden kann.

#### 2. Aufbau von Testdatenbanken

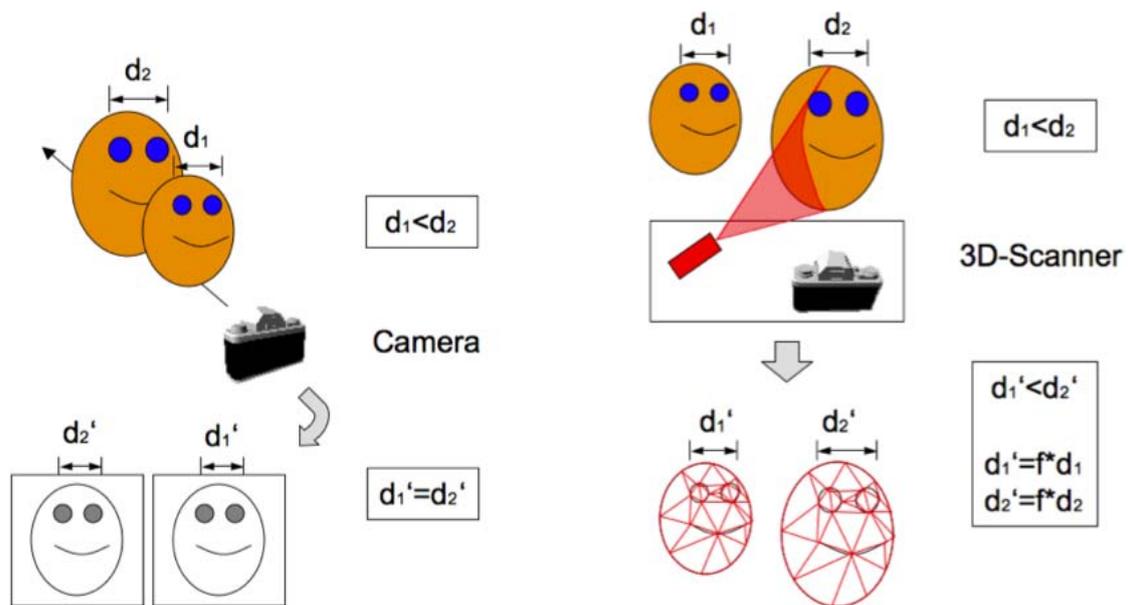


Abbildung 3: Vorteile der 3-D-Gesichtserkennung

Zur Analyse der Erkennungsleistung ist eine umfangreiche Datensammlung erforderlich. Diese wird im Projekt *3D Face* in zwei Phasen erhoben. In der ersten Phase werden an drei verschiedenen Standorten von insgesamt 600 Personen unter Laborbedingungen 2-D- und 3-D-Gesichtsdaten erhoben. Die freiwillig teilnehmenden Personen (techn. *Subjekte*) werden zu unterschiedlichen Terminen und wie die Abbildung 5 auf Seite 8 zeigt bei möglichst großer Variation des Gesichtes bezüglich Haare, Kopfbedeckungen oder Brille erfasst, wobei zusätzlich Metadaten wie Alter, Geschlecht, ethnische Gruppe etc. aufgezeichnet werden. Insgesamt sollen mindestens 11 Scans pro Person für Entwicklung und Analyse zur Verfügung stehen. Um ein hohes Maß an Interoperabilität zu untersuchen, werden die Aufnahmen nicht ausschließlich mit dem im Projekt entwickelten Prototypen erfasst, sondern es werden unterschiedliche Aufnahmeysteme zum Einsatz kommen. Die so erstellte Datenbasis wird zu einem Teil der Algorithmenentwicklung bereitgestellt und steht zum anderen Teil den abschließenden Tests zur Verfügung.

Die zweite Phase der Datensammlung ist eng mit dem Feldversuch am Ende der Projektlaufzeit verknüpft (siehe Abschnitt 7 auf Seite 11). Unter realistischen Bedingungen werden hier die Daten von etwa 2000 Versuchsteilnehmern erfasst und es wird damit gerechnet, dass sich mit dieser Analysebasis aussagekräftige Ergebnisse erzielen lassen, die bestätigen, dass die gesetzten Ziele erreicht wurden.

### 3. Erforschung der Multimodalen Analyse

Da mit dem Aufnahmesystem bei der Datenerfassung mit dem Gesichtstexturbild und der Gesichtsgeometrie zwei abhängige Informationskanäle zur Verfügung stehen, bietet es sich an, diese als zwei biometrische Modalitäten zu betrachten und die Verfahren der



Abbildung 4: Prototyp eines 3-D-Aufnahmesystems in drei verschiedenen Ansichten

Multimodalen Analyse anzuwenden [RJ03]. Traditionell kommen bei der Multimodalen Analyse vorrangig die Konzepte *Feature-Level-Fusion* (Verknüpfung der Merkmalsvektoren), *Score-Level-Fusion* (Verknüpfung der Vergleichsergebnisse) und *Decision-Level-Fusion* (Verknüpfung der Entscheidungen) zum Einsatz. Beim Verfahren der *Feature-Level-Fusion* werden die Informationen aus der Merkmalsanalyse in beiden Informationskanälen zu einem Merkmalsvektor zusammengeführt, der dann mit der Referenz verglichen wird. Bei *Score-Level-Fusion* erfolgt Merkmalsanalyse und Vergleich für jede Modalität getrennt und es werden nachgeschaltet beide (oder mehrere) Score-Werte zusammengeführt. Da die Score-Werte jedoch ggf. in unterschiedliche Bereiche abbilden, sind dabei nicht-triviale Score-Normalisierungen durchzuführen. Das Konzept des *Decision-Level-Fusion* ist insbesondere bei der Verwendung von mehreren Informationskanälen (z. B. Gesichtsbild, Gesichtsgemetrie, hochaufgelöste Hauttextur etc.) von Interesse, wobei man in diesem Fall eine positive Übereinstimmung dann feststellen kann, wenn in allen Kanälen eine positive Entscheidung vorliegt oder ein Mehrheitsentscheid der Komparatoren durchgeführt wird (*The-winner-takes-it-all-principle*).



Abbildung 5: Verschiedene 3-D-Scans eines Testteilnehmers in unterschiedlichen Posen

Bei der multimodalen Fusion gibt es derzeit noch wenig Erfahrung bei der Einbindung von 3-D-Geometriedaten, weshalb diesem Aspekt ein besonderes Augenmerk im *3D Face* Projekt gewidmet wird.

#### 4. Test der Erkennungsleistung

Entsprechend dem im Jahr 2006 fertig gestellten ISO-Teststandard 19795-1 [ISO06] wird im Projekt ein Testplan umgesetzt, der in der ersten Phase Aufschluss über die Leistungsfähigkeit der Einzelkomponenten des System, d. h. Normalisierungsverfahren (Translation und Rotation des Modells vor dem Vergleich), Merkmalsextraktionsverfahren, Fusionsverfahren einerseits und den Laborleistungen des Gesamtsystems andererseits liefern soll. In einer zweiten Phase wird ein integriertes Funktionsmuster im Rahmen einer Pilotierung an zwei europäischen Flughäfen über sechs Monate betrieben und die dabei erhobenen Daten zur weiteren Optimierung der Einzelkomponenten verwendet.

Als Erkennungsleistung wird eine Falsch-Akzeptanz-Rate (FAR) von unter 0,25% sowie eine Falsch-Rückweisungs-Rate (FRR) von unter 2,5% angestrebt. Die angestrebten Fehlerraten werden in der Pilotierung unter Betriebsbedingungen (Operational Testing) überprüft, wie sie auf Flughäfen vorherrschen. Dazu zählen vor allem die schnelle Bearbeitung und ein nebenläufiger Betrieb.

#### 5. Steigerung der Überwindungssicherheit

Sofern in einigen Jahren die ersten Grenzkontrollspuren installiert werden, wird vermutlich ein Grenzbeamter mehrere Kontrollspuren im Auge behalten müssen. So wird es heute schon im SmartGate-Projekt in Australien praktiziert, um damit zu verhindern, dass Fälschungen einer biometrischen Charakteristik präsentiert werden. Sinnvoller wäre es, überwindungssichere Systeme einzusetzen. Die ICAO, die ihren Passstandard kontinuierlich weiterentwickelt [Int06], denkt bereits in diese Richtung. Sie hat im Oktober 2004 in ihrem request for information die Hersteller aufgefordert, die Technologieentwicklungen

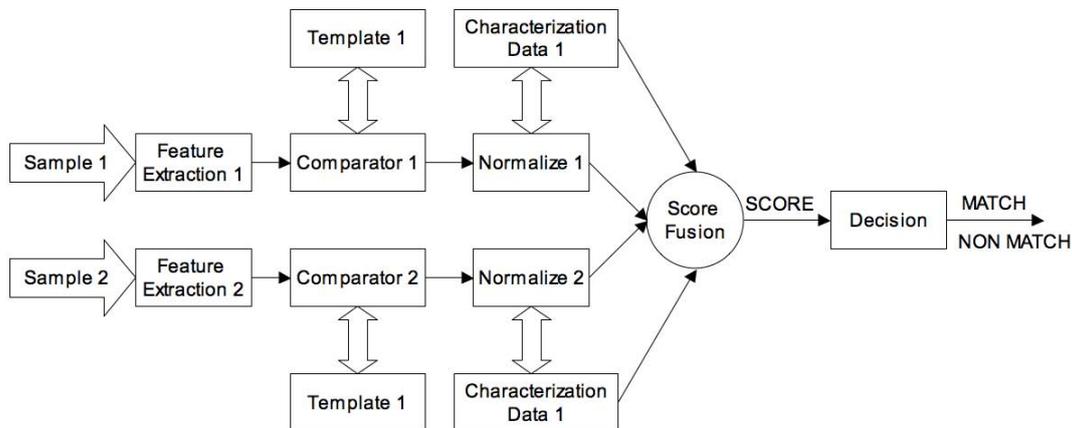


Abbildung 6: Ein Framework zum Score-Level-Fusion (nach [ISO06])

mitzuteilen, die zukünftig eine nicht überwachte Grenzkontrolle ermöglichen: »... *new technologies is now sought ... technologies and processes that are suitable for automated self-identification at international borders that will enable unattended border crossing*« [Int04b].

Unabhängig von der Erkennungsleistung der Verfahren, kann man der 3-D-Gesichtserkennung eine verbesserte Robustheit hinsichtlich der Überwindungsangriffe attestieren, da ein Replikat deutlich schwieriger zu erstellen ist. Schon die Beschaffung der 3-D-Geometrie ist ohne Kooperation der zu replizierenden »Zielperson« mit erheblichem Aufwand verbunden. Die Produktion eines 3-D-PrintOuts ist zwar technisch beispielsweise mit einem Stereo-Lithographieverfahren möglich – ein derart hergestellter künstlicher Kopf könnte jedoch mit einfachen Lebenderkennungsmechanismen automatisch detektiert werden, was die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert.

## 6. Erforschung von Schutzmechanismen für biometrische Templates

Biometrische Daten (Biometrische Samples oder Templates) sind im Sinne der geltenden Datenschutzregelungen personenbezogene Daten und daher einem besonderen Schutz zu unterwerfen. Bei der Analyse der Datensicherheit wird oft der Prozess der Speicherung der Referenzdaten betrachtet: Meist wird die biometrische Wiedererkennung mit einem Token verknüpft, wie dies beim ePass der Falls ist. Wünschenswert wäre es, wenn bei der Wiedererkennung der Vergleich gleich direkt in dieser Karte durchgeführt werden könnte. Bei diesem sogenannten *Comparison on Card*<sup>1</sup> liefert die Karte ein positives oder negatives Ergebnis an die Anwendung zurück, ohne dass die Anwendung Zugriff auf die Referenzdaten erhält. Dies ist vor allem dann ein guter Schutz für die sensitiven biometrischen

<sup>1</sup>In der internationalen Standardisierung wurde der Begriff *Comparison* bewusst ersetzend für den bislang genutzten Begriff *Matching* geprägt, da *Comparison* das Ergebnis des Vergleichs offen lässt – der Begriff *Matching* hingegen suggeriert, dass der Vergleich auf der Karte tatsächlich positiv ausfallen wird.

Samples, wenn die Karte über eine direkte Schnittstelle zum bildgebenden Aufnahmesystem verfügte. Für die Gesichtserkennung ist das jedoch nicht denkbar.

Im zweiten Konzept werden die Referenzdaten der Passinhaber in einer zentralen oder dezentralen Datenbank gespeichert. Dies wird nach dem Entwurf des Passgesetzes für den deutschen Rechtsraum nicht der Fall sein, könnte jedoch in anderen ICAO-Mitgliedsländern so implementiert werden. Mit der Speicherung von Samples in einer Datenbank werden einige potenzielle Probleme assoziiert: Diese reichen vom Identitätsdiebstahl (beim Zugriff auf Bilddaten) und dem damit einhergehenden Wunsch, gespeicherte Referenzdaten »zurückrufen« zu können, über die Gefahr des Cross-Matching (auch bei der informationsreduzierenden Verwendung von Templates als Referenzdaten könnten Datenbank-Administratoren durch Abgleich der Datensätze Querbezüge herstellen) bis hin zur Thematik der Zusatzinformation (die potenziell als medizinische Überschussinformation aus den Bilddaten auslesbar ist). Zur Lösung dieser Probleme wird im *3D Face* Projekt ein Verfahren entwickelt, das als *Template Protection* bezeichnet wird [vdVKS<sup>+</sup>06] und welches das Speichern (im Token oder in einer Datenbank) von Bild- oder Templatedaten in ungeschützter Form entbehrlich macht. Die Vorgehensweise ist angelehnt an die Absicherung von Passwortdaten in einem Unix-System. Bei der Unix-Authentisierung ist es nicht so, dass das von einem Nutzer verwendete Passwort im Klartext im System (oder in einer Datenbank) gespeichert wird. Vielmehr wird bei der Einrichtung eines Nutzeraccounts (*Enrolment*) unter Verwendung einer Einwegfunktion (*Hashfunktion*) ein Hashwert berechnet. Die Funktion hat die Eigenschaft, dass Sie nicht invertierbar ist, d. h. aus dem Hashwert lässt sich das Passwort nicht zurückrechnen. Zudem werden nur solche Einwegfunktionen eingesetzt, die kollisionsfrei sind, d. h. es gibt nicht zwei Eingabestrings (Passwörter), für die sich derselbe Hashwert ergibt. Die Hashwerte für alle Nutzer werden in einer öffentlich zugänglichen Datei gespeichert. Wenn der Nutzer sich erneut authentisieren möchte, wird wiederum vom Input ein Hashwert gebildet, der dann mit dem Hashwert verglichen wird, der in der Tabelle hinterlegt wurde.

Analog dazu kann das Verfahren zum Schutz von Templates ablaufen. Biometrische Samples und damit auch Merkmalsvektoren sind allerdings – im Unterschied zu den Passwort-Datensätzen – mit einem Rauschen belegt. Dies ist durch die Variation der Umwelteinflüsse (z. B. Lichtverhältnisse) aber auch durch die Variation der biometrischen Charakteristik selbst (z. B. Alterung) bedingt. Aus diesem Grunde müssen die im Template gespeicherten Merkmale noch einmal gefiltert werden, um eindeutige Datensätze reproduzieren zu können. Anschaulich kann man diese Filterung als *Quantisierung* des Merkmalsvektors verstehen, bei dem für ein bestimmtes Merkmal verschiedene Wertebereiche jeweils auf einen Mittelwert abgebildet werden. Für die berechneten quantisierten Merkmale wird eine Qualitätsprüfung vorgenommen, um die Robustheit des Verfahrens sicherzustellen. Das bedeutet, dass nur diejenigen stabilen Merkmale weiterverarbeitet werden, die auch wiederholt mit dem gleichen Mittelwert berechnet wurden. Um die Erneuerbarkeit des Vektors herzustellen, werden anschließend aus dem Merkmalsvektor einzelne Komponenten selektiert, wobei die Selektionsfunktion durch ein Geheimnis gesteuert wird. Über den verbleibenden reduzierten Vektor wird der Hashwert berechnet und in der Datenbank abgelegt.

Bei einer biometrischen Verifikation wird das präsentierte Recognition-Sample nur in einem gewissen Maße ähnlich sein zu dem Sample, das beim Enrolment verwendet wurde. Durch den geschilderten Ansatz lassen sich jedoch die gleichen stabilen Komponenten im Merkmalsvektor berechnen und mit dem gleichen Geheimnis kann ermittelt werden, welche Komponenten für die Hashberechnung erforderlich sind. Der sich durch diesen Ansatz ergebende Gewinn für die Datensicherheit der personenbezogenen Daten ist enorm.

## 7. Pilotierung

Die Pilotanwendung wird die biometrische Grenz- und Zugangskontrolle an Flughäfen sein. Dazu wurden in das internationale Konsortium, das sich aus 4 Industrieunternehmen, 2 mittelständischen Unternehmen, 3 Forschungseinrichtungen sowie 2 Universitäten zusammensetzt, weitere Partner eingebunden, die als Anwender die Gruppe der Flughafenbetreiber vertreten. In der zweiten Testphase werden im *Operational Testing*, die Erkennungssysteme an mindestens zwei bedeutenden europäischen Flughäfen für sechs Monate eingesetzt. Dabei sollen von ca. 2000 Teilnehmern biometrische Gesichtsdaten erfasst und ausgewertet werden.

## 8. Standardisierung

Nachdem erst im Jahr 2002 das internationale Standardisierungskomitee SC37 gegründet wurde<sup>2</sup>, das die Biometriestandardisierung betreibt, konnten schon im Sommer 2005 nach einer sehr kurzen Bearbeitungszeit die ersten Standards publiziert werden.

Die Standardisierung im Bereich der Informationstechnologie wird von einem Joint Technical Committee (JTC) zwischen der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) erarbeitet. Ein wichtiger Teil der Tätigkeiten des JTC1 Subcommittees SC37 ist es, Datenaustauschformate zu formulieren, nach denen die Repräsentation einer biometrischen Charakteristik, z. B. eines Gesichtsbilds oder des Bilds eines Fingerabdrucks, in einem spezifizierten Datensatz kodiert werden kann. Dieser Datensatz kann dann als Referenz in einer SmartCard oder in einer Datenbank abgelegt werden. Wenn es sich um ein offenes System handelt, muss diese Referenz interoperabel sein, d. h. ein anderer Hersteller muss das Format des Datensatzes lesen und verstehen können und zudem auf derartigen Daten eine gute Erkennungsleistung herstellen können.

Bei der Spezifikation des ePasses war die Interoperabilität ein sehr hohes Ziel, so dass bei der Definition der Logischen Datenstruktur (LDS) zwei bildbasierte Standards eingeflossen sind: Das ist einerseits der Standard ISO/IEC IS 19794-5 zur Speicherung von Gesichtsbildern [ISO05b], der in derzeit ausgegebenen deutschen Pässen bereits eingesetzt wird und andererseits der Standard ISO/IEC IS 19794-4 zur Speicherung von Fingerbildern [ISO05a], die dann ab Herbst 2007 in den Pässen der Bundesrepublik Deutschland ergänzt werden. Die im Projekt *3D Face* gewonnenen Erkenntnisse sollen durch aktive Beteiligung in bestehende Standards sowie in eine neue internationale Norm für ein 3-D-Gesichtsdatenformat einfließen. Dazu wird der Standard IS 19794-5 gegenwärtig um

---

<sup>2</sup>ISO/IEC JTC 1 on Information Technology Subcommittee 37 on Biometrics (<http://www.jtc1.org>)

Datenfelder zur Speicherung von 3-D-Geometrie-Daten erweitert. Neben dem reinen Tiefenbild (*Range-Image*) sollen auch 3-D-Point-Maps und 3-D-Vertex-Kodierungen zum Einsatz kommen. Das Tiefenbild kodiert in einem Grauwert-Bild die Entfernung von einem gedachten Zylinder zur Gesichtsoberfläche. Die Kodierung von 3-D-Punkten hingegen hat den Vorteil, dass Verdeckungen abgebildet werden können und ggf. forensische Auswertungen möglich werden. Erfreulicherweise konnte international als Projekt-Editor für diesen wichtigen Standard ein Mitglied des deutschen Normenausschuss NI37 gewählt werden.

## 5 Ausblick

Auch wenn biometrische Systeme derzeit noch kaum verbreitet sind, mit dem neuen ePass, der seit Herbst 2005 ausgegeben wird, kommt in den kommenden Jahren jeder Bundesbürger mit Biometrie in Berührung. Während des Einführungszeitraums von 10 Jahren, sollen Schritt für Schritt auch die Grenzkontrollpunkte mit einem biometrischen Verifikationssystem ausgestattet werden.

Mit dem Übergang von zweidimensionalen zu dreidimensionalen Gesichtserkennungssystemen erhofft man sich eine Steigerung der Sicherheit dieser Authentisierungsmethode. Das Projekt *3D Face* hat sich zur Aufgabe gemacht, diesen Übergang zu realisieren und Verfahren zur 3-D-Gesichtserkennung zu erforschen. Auch wenn die Kosten für ein 3-D-Aufnahmesystem derzeit noch um ein vielfaches über den Kosten eines 2-D-Aufnahmesystems liegen, sind die technischen Perspektiven vielversprechend: Die Natur und Komplexität der biometrischen Charakteristik, die in 3-D-Gesichtserkennung gegeben ist, macht einen erfolgreichen Überwindungsangriff im Vergleich zu derzeitigen 2-D-Gesichtserkennungssystemen aber auch im Vergleich zu Fingerabdruckerkennungssystemen unwahrscheinlich. Sofern gleichzeitig, wie erhofft, auch die Erkennungsleistung verbessert werden kann, wird eine vollautomatische und sichere Zugangskontrolle in Zukunft denkbar.

Möglicherweise wird in Zukunft die Strategie der sekundären biometrischen Daten, die neben dem Lichtbild im Chip des ePasses gespeichert werden, überdacht werden. Die Entscheidung für zwei Fingerbilder (beide Zeigefinger), wie sie in der EU-Richtlinie 2004 formuliert wurde, war zum Zeitpunkt der Entscheidung unter anderem dadurch begründet, dass durch die Auswertung einer Zwei-Finger-Präsentation eine gegenüber einem einfachen 2-D-Lichtbild höhere Erkennungsleistung erzielt werden kann. Sofern jedoch die biometrisch gestützten Grenzkontrollen an den EU-Außengrenzen allein auf der Zwei-Finger-Präsentation basieren, würde die Europäische Union quasi zur »biometrischen Insel«: Die Bindung biometrische Charakteristik zum ePass könnte lediglich für EU-Bürger vorgenommen werden, da Bürger anderer Herkunft keine entsprechenden Referenzen in ihren Pässen vorweisen könnten.

Sollten sich die Hoffnungen auf eine Steigerung der Erkennungsleistung von 3-D-Gesichtserkennung erfüllen, wäre durch eine Übernahme des aktualisierten ISO-Standards 19794-5 und einer entsprechenden Aktualisierung von ICAO 9303 eine international standardisierte Grenzkontrolle auf einheitlichen primären biometrischen Daten zu erreichen.

## Literatur

- [3D 06] 3D FACE CONSORTIUM: *3D Face. Integrated Project funded by European Commission*. <http://www.3dface.org>, 2006. Zuletzt besucht: 2.2.2007.
- [BM92] BESL, P.J. N.D. MCKEY: *A method for registration of 3D shapes*. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14, 239–256, 1992.
- [Deu07] DEUTSCHER BUNDESRAT: *Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften*. [http://www.bundesrat.de/nr\\_8694/SharedDocs/Drucksachen/2007/0001-0100/16-07,templateId=raw,property=publicationFile.pdf/16-07.pdf](http://www.bundesrat.de/nr_8694/SharedDocs/Drucksachen/2007/0001-0100/16-07,templateId=raw,property=publicationFile.pdf/16-07.pdf), 2007. Zuletzt besucht: 21.1.2007.
- [Eur04] EUROPARAT: *Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten*. [http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2004/l\\_385/l\\_38520041229de00010006.pdf](http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2004/l_385/l_38520041229de00010006.pdf), 2004. Zuletzt besucht: 15.2.2007.
- [Int04a] INTERNATIONAL CIVIL AVIATION ORGANIZATION TECHNICAL ADVISORY GROUP 15 MACHINE READABLE TRAVEL DOCUMENTS/NEW TECHNOLOGIES WORKING GROUP: *Biometrics Deployment of Machine Readable Travel Documents, Version 2.0*. Technischer Bericht, ICAO, 2004.
- [Int04b] INTERNATIONAL CIVIL AVIATION ORGANIZATION TECHNICAL ADVISORY GROUP 15 MACHINE READABLE TRAVEL DOCUMENTS/NEW TECHNOLOGIES WORKING GROUP: *Request for Information*, 2004.
- [Int06] INTERNATIONAL CIVIL AVIATION ORGANIZATION: *Supplement to Doc9303-part 1-sixth edition*. Technischer Bericht, ICAO, 2006.
- [ISO05a] ISO/IEC TC JTC1 SC37 BIOMETRICS: *ISO/IEC 19794-4:2005. Information Technology – Biometric Data Interchange Formats – Part 4: Finger Image Data*. International Organization for Standardization and International Electrotechnical Committee, 2005.
- [ISO05b] ISO/IEC TC JTC1 SC37 BIOMETRICS: *ISO/IEC 19794-5:2005. Information Technology – Biometric Data Interchange Formats – Part 5: Face Image Data*. International Organization for Standardization and International Electrotechnical Committee, 2005.
- [ISO06] ISO/IEC TC JTC1 SC37 BIOMETRICS: *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization and International Electrotechnical Committee, 2006.

- [KW97] KRAUS, KARL PETER WALDHÄUSL: *Photogrammetrie. Band 1: Grundlagen und Standardverfahren*. Bildungsverlag Eins, Bonn, 1997.
- [LJ05] LU, XIAO GUANG ANIL K. JAIN: *Integrating Range and Texture Information for 3D Face Recognition. Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05)*, 1, 156–163, Breckenridge, CO, 2005.
- [RJ03] ROSS, ARUN ANIL JAIN: *Information Fusion in Biometrics*. Pattern Recognition Letters, 24(13):2115–2125, 2003.
- [SPB04] SALVI, JOAQUIM, JORDI PAGÈS JOAN BATLLE: *Pattern codification strategies in structured light systems*. Pattern Recognition, 37(4):827–849, 2004.
- [vdVKS<sup>+</sup>06] VEEN, MICHIEL VAN DER, TOM KEVENAAR, GEERT-JAN SCHRIJEN, TON H. AKKERMANS FEI ZUO: *Face Biometrics with Renewable Templates*. DELP, EDWARD J. PING WAH WONG (): *Proceedings of SPIE. Security, Steganography, and Watermarking of Multimedia Contents, 6072 Security, Steganography, and Watermarking of Multimedia Contents*. SPIE, 2006.