en
cs de
sk es

TECH
pedia

BENUTZERIDENTIFIKATION

RENATA RYBÁROVÁ, JURAJ KAČUR,
ONDREJ LÁBAJ, GREGOR ROZINAJ

Titel der Arbeit: Benutzeridentifikation

Author: Renata Rybárová, Juraj Kačur, Ondrej Lábaj, Gregor Rozinaj

Übersetzt (von): Radoslav Vargic

Veröffentlicht (von): České vysoké učení technické v Praze

Fakulta elektrotechnická

Kontaktadresse: Technicka 2, Prague 6, Czech Republic

Tel.: +420 224352084

Drucken: (nur elektronisch)

Anzahl der Seiten: 43

Ausgabe: 1. Ausgabe, 2017

ISBN 978-80-01-06238-8

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG

	Definition(en)
	Interessantheit (Interessantes)
	Bemerkung
	Beispiel
	Zusammenfassung
	Vorteile
	Nachteile

ZUSAMMENFASSUNG

Benutzer-Identifikation, Autorisierung und Authentifizierung sollen gewährleisten, dass das System nur von Benutzern mit ausreichenden Berechtigungen verwendet wird. Die Sprechererkennung neigt Grund Identifizierung der möglichen Benutzer in der Systeminstallation Gebiet bereitzustellen. Dies wäre geeignet für Identifikationsaufgaben, wie die Verwendung des persönlichen Profils. Die Gesichtserkennung ist ein Ansatz, der darauf zielt, zuverlässigere Benutzeridentifikation an Hand von Gesichtsmerkmalen durchzuführen. Im Vergleich zur Sprechererkennung können mit der Gesichtserkennung mehr Eigenschaften parametrisiert werden, als mit einer Stimme. Eine Erweiterung der Gesichtserkennung, ist die Einbeziehung von Merkmalen aus einer 3D-Gesichtserkennung, die eine noch exaktere Identifizierung einer Person erlaubt. Diese Methode kann für die Authentifizierung anspruchsvoller Anwendungen (z. B. die Anmeldung zum Bankkonto) verwendet werden.

ZIELE

Das Hauptziel des Moduls ist eine Einführung in die Grundlagen der Benutzeridentifikation, Authentifizierung und Autorisierung. Der Student wird mit den Grundprinzipien der Benutzeridentifikation und der Benutzerautorisierung auf der Basis von Sprechererkennung, 2D-, und 3D-Techniken vertraut gemacht.

LITERATUR

[1] Abate, Andrea F.; Nappi, Michele; Riccio, Daniel; Sabatino, Gabriele. 2D and 3D face recognition: A survey In: Pattern Recognition Letters, Volume 28, Issue 14, 15 October 2007, Pages 1885–1906. available at www.sciencedirect.com.

[2] T. Kinnunen, H. Li, An overview of text-independent speaker recognition: from features to supervectors, Speech communication, Vol. 52, pp. 12-40, Elsevier, 2010

[3] Probst, Michael; Schumann, Sebastian; Rozinaj, Gregor; Minarik, Ivan; Rybárová, Renata; Oravec, Miloš. EVALUATION: Final Multimodal Interface for User/Group-Aware Personalisation, Deliverable 5.5.1, available at http://www.hbb-next.eu/index.php/documents, December 2013.

[4] Bán, Jozef; Féder, Matej; Oravec, Miloš; Pavlovičová, Jarmila. Face Recognition of Images Corrupted by Transmission Errors. In: Redžúr 2012: proceedings; 6th International Workshop on Multimedia and Signal Processing. April 11, 2012, Vienna, Austria. Bratislava: Nakladateľstvo STU, 2012. pp. 15-18, ISBN 978-80-227-3686-2

[5] Rozinaj, Gregor; Minarik, Ivan; Rybárová, Renata; Pavlovičová, Jarmila; Mármol, Félix Gómez; Tormo, Ginés Dólera, Gülbahar, Mark; Schumann, Sebastian. DESIGN AND PROTOCOL: Final User ID, Profile, Application Reputation Framework, Deliverable 3.4.1, available at http://www.hbb-next.eu/index.php/documents, December 2013.

[6] Schneier, Bruce. Sensible Authentication, ACM Queue 1, Volume 1 Issue 10, February 2004. Pages 74.

[7] McCue, A. Is Your Cat a Target for Password-Stealing Hackers?, Silicon.com, 11 August 2004.

[8] Haskett, J.A., Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms In Communications of the ACM 27, 1984.

[9] Madigan, A. Picture Memory - Memory and Cognition: Essays in Honour of Allan Paivio Erlbaum, 1983.

[10] Cranor, L.F.; Garfinkel, S. Security and Usability, O'Reilly, August 2005. ISBN 0-596-00827-9.

[11] Vacca, J.R. Computer and Information Security Handbook, Morgan Kaufmann, 2009. ISBN 978-0-12-374354-1.

[12] Gattiker, U. E. The Information Security Dictionary, KLUWER ACADEMICPUBLISHERS, 2004. ISBN 1-4020-7927-3.

Inhaltsverzeichnis

1 Benutzeridentifikation

Die Benutzeridentifikation gewährleistet, dass ein System oder die Anwendung nur Befehle ausführt, die für einen Benutzer zugelassen sind. Die am weitesten verbreitete Authentifizierungsmethode ist die Verwendung von Passwörtern. Mit der Entwicklung der Informationstechnologien und dem Einsatz von Sicherheitsschutz-Algorithmen begann neben der Authentifizierung durch Passworte, auch die Auswertung biometrischen Faktoren.

Die Verwendung biometrischer Daten beseitigt die möglichen Risiken der weniger fortschrittlichen Technologien, die darauf basieren, was eine Person hat oder weiß, und nicht wer die Person wirklich ist [1]. Es ist eine sehr attraktive und beliebte Technik, denn sie kann in jede beliebige Anwendung oder Sicherheits- und Zugriffssteuerung integriert werden.

Die Sprecheridentifikation neigt Grund Identifizierung der möglichen Benutzer in der Systeminstallation Gebiet bereitzustellen. Die Gesichtserkennung Ansatz zielt darauf, zuverlässigere Benutzeridentifikation basierend auf den Gesichtern liefern, die weit mehr Eigenschaften, die im Vergleich zur Sprachidentifikation Ansatz parametrisiert werden können. Zusätzlich wird die 3D-Gesichtserkennung weiter die Möglichkeiten der Merkmalsextraktion erweitert, um bestimmte Personen genauer zu identifizieren und so für höchste Authentifizierung (und Zulassung) für die anspruchsvollsten Anwendungen (z.B. Bankkonto Anmeldung, etc.) verwendet werden kann. Aus Sicherheitsgründen kann die Authentifizierung durch 3D-Gesichtserkennung ergänzt werden, beispielsweise durch Augenbewegungsverfolgung oder Iriserkennung. Dieser Ansatz kann eine Multi-Faktor-Authentifizierung (Login zzgl. Token) simulieren, die für eine sichere Authentifizierung notwendig ist.

Allerdings haben biometrische Merkmale auch Nachteile. Die Iriserkennung ist extrem genau, aber teuer zu implementieren und die Akzeptanz durch Benutzer ist fraglich. Fingerabdrücke sind zuverlässig und werden vom Benutzer eher akzeptiert. Die Gesichtserkennung bietet einen guten Kompromiss zwischen Zuverlässigkeit und gesellschaftliche Akzeptanz [1].

2 Sprecheridentifikation

2.1 Sprecheridentifikation Übersicht

Die Sprecheridentifikation ist als Teil eines umfassenderen Konzepts der Sprechererkennung bekannt. Es umfasst zwei wichtige und ähnliche, aber immer noch verschiedene Aufgaben, nämlich die Sprecheridentifizierung und der Sprecherverifikation. Mit der ersten Aufgabe wird automatisch entschieden, wem aus einer Gruppe von Benutzern die Sprachprobe gehört, wobei zum Vergleich eine Datenbank verwendet wird, die in einer Lernphase mit den Sprachproben gefüllt wurde.

Optional wird niemand erkannt, wenn das Vertrauen der endgültigen Entscheidung zu niedrig ist. Diese Aufgabe wird oft als Problem einer geschlossen Gruppe bezeichnet, da es einen festen Satz von Benutzern gibt, die erkannt werden kann.

Auf der anderen Seite, wertet der Verifizierungsprozess aus, ob das getestete Individuum derjenige ist, der er oder sie vorgibt zu sein.

Da es sehr viele Anwender gibt (evtl. sieben Milliarden weltweit), ist es unmöglich, eine Kennlinie oder ein Modell für alle Personen zu entwickeln und bezeichnet diesen Umstand als das Open Group Problem. In dieser Situation ist das allgemeine Modell eines Sprechers von großer Bedeutung, um eine angemessene Annahme / Ablehnung von Schwellenwerten festzulegen.

Die Sprechererkennung ist aus mehreren Gründen problematisch. Dies ist seit über 40 Jahren Gegenstand wissenschaftlicher Untersuchungen zahlreicher Forschungsteams. Da gibt es neue und zugängliche Technologien, man kann zunehmend Anwendung in vielen Bereichen finden; einige seien hier erwähnt:

- Kriminaltechnik
- natürliche und nicht-invasive Methode für den sicheren Zugriff und den Schutz von Daten und Diensten
- automatische Indizierung von in Datenbanken gespeicherten Sprach- und Audio-Aufnahmen
- Anwendungen für die Spiele-Industrie
- Hilfen für behinderte Menschen

Aufgrund des breiten Spektrums von Problemen, die angegangen werden müssen, gibt es viele geeignete Lösungen und Techniken der Sprecheridentifikation. Diese können in drei Hauptgruppen geteilt werden:

- **Sprachmerkmale** - Aufgabe der Sprechererkennung oder Sprecheridentifikation

- **Merkmalnormalisierung / Ausgleich** - die Variabilität der Sitzung soll unterdrückt werden

- **Klassifizierung und Entscheidungs-Algorithmus** - Entscheidung, basierend auf Eigenschaften und Modellen, die die größte Übereinstimmung mit der unbekannten Probe repräsentieren.

Die Aufgabe der Sprecheridentifikation ist in zwei große Gruppen unterteilt, dies sind die vom Text abhängigen bzw. die vom Text unabhängigen Probleme. In der ersten Gruppe setzt der Identifikationsprozess keinen bestimmten Text voraus, während in der zweiten Gruppe die Systeme einen nachgesprochen Text erfordern. Dabei erreicht das Text abhängige System offensichtlich höhere Genauigkeiten.

2.2 Eigenschaften von Sprachsignalen

Echte Sprachsignale werden durch Menschen erzeugt, genauer gesagt durch ihren Stimmapparat und das Gehirn, die für jede Person einzigartig sind. Beide hinterlassen ihre Spuren in dem akustischen Signal, und daher kann die Sprache als biometrisches Signal betrachtet werden.

Das Hauptziel der Sprachsignale ist es, die enthaltene lexikalische Information zu vermitteln. Mit Ausnahme des lexikalischen Teiles, der durch die Abfolge der verschiedenen Positionen der Stimmorgane gegeben ist, repräsentiert die biometrische Information über einen Redner hauptsächlich die unterschiedlichen Formen, Größen, Gewichte und Zähigkeit der Stimmorgane sowie die aktuelle Stimmung einer Person (Intonation, Sprachtempo, Stress usw.) und ihren sozialen Hintergrund (Dialekt, Wortschatz, etc.).

Allerdings sind diese verschiedenen Informationen in einem Sprachsignal durch eine schwierige Transformation kodiert, die als irreversibel und nicht bekannt zu betrachten ist. So ist es ein großes Problem, nur die Informationen, die für eine bestimmte Aufgabe (lexikalische, Identifikation, Stimmung, Gesundheitszustand, ...) benötigt werden, zu extrahieren. Jedes Sprachsignal zeigt große Variabilität für einzelne Personen abhängig von ihrer aktuellen Stimmung, Gesundheit und körperlichem Zustand oder anderen Bedingungen. Die akustische Form eines Sprachsignals kann durch Unterschiede in den Aufzeichnungsgeräten, Raumakustik und Hintergrundrauschen beeinflusst werden.

Die Modifikationen von Sprache, die nicht auf den Einfluss eines Lautsprechers (Geräte, Raum, etc.) beruhen, werden Session Variabilität genannt. Dieser Aspekt führt zu großen Problemen und muss in Situationen behandelt werden, wo die Ausgangsbedingungen nicht mit den aktuellen Bedingungen korrespondieren.

2.3 Merkmalextraktion

Aufgrund der zuvor erwähnten variablen Spracheigenschaften und vieler ungünstiger Bedingungen wurden nach und nach zahlreiche Extraktionstechniken erfunden. Grundsätzlich muss ein gutes Sprachmerkmal:

- unterscheidbar sein
- robust gegen verschiedene Hintergrundgeräusche
- unempfindlich gegenüber Änderungen der Aufnahmegeräte und der Einsatzorte
- Sprecher-Variabilität unterdrücken
- leicht zu berechnen und zu verarbeiten sein

Da es sehr viele verschiedene Sprecher-spezifischen Funktionen gibt, die unterschiedliche physikalische Bedeutungen haben, unterscheiden wir drei Arten von Funktionen (aus der Sicht des Redners):

- Akustische
- Prosodische
- Höheres Level

Auf der akustischen Ebene werden kurzerzeitige Merkmale gesammelt, die mit den physikalischen Eigenschaft des Stimmapparates zu tun haben. Diese Methoden repräsentieren im Wesentlichen modifizierte spektrale (Umschlag) Formen, die aus Intervallen von 10 ms bis 30 ms extrahiert werden. Desweiteren, benutzen sie verschiedene psychoakustische Prinzipien des menschlichen Hörsystems um ihre Robustheit zu erhöhen. Derzeit sind es häufig die Mel Frequenz Cepstralkoeffizienten (MFCC), *Perceptual Linear Prediction* (**PLP**) oder Cepstral Linearprädiktionskoeffizienten (CLPC) Funktionen. MFCC und PLP versuchen, modifizierte spektrale Einhüllenden nach einigen psychoakustischen Prinzipien wie kritische Bänder, die menschliche Wahrnehmung von Frequenzen, Kurve gleicher Lautstärke, Umwandlung von Intensitäten nach Lautstärke, zu erfassen. Da sie in der Lage sind, die Spektraleinhüllkurven zu extrahieren, erhalten und betonen sie die Lage, Breiten und Formen der Formantenfrequenzen, die entscheidend für die Wahrnehmung der Unterschiede zwischen den Tönen sind. Damit sind sie für die Spracherkennungssysteme sehr wichtig. Sie spielen auch noch eine bedeutende Rolle für das Sprecher-Erkennungsproblem. Damit kann erklärt werden, dass sie in der Lage sind, die geringen Unterschiede in Positionen und Formen der Formantenfrequenzen zu erfassen, die von Person zu Person variieren. Entsprechende Funktionen sind in bestimmten Telefonen bereits vorhanden. CLPC Funktionen basieren auf der Modellierung des Spracherzeugungsmechanismus anstatt des Hör- und Wahrnehmungsprozesses. Um auch dynamische akustische Eigenschaften zeitlich zu erfassen, können Differenz- und Beschleunigungs-Koeffizienten abgeleitet werden. Weil sie längere Zeitintervalle abdecken, können sie die Unterschiede in Koartikulation detektieren, die spezifisch für einen bestimmten Sprecher sind.

Die prosodische Ebene konzentriert sich vor allem auf die Art des Sprechens, die Stimmung eines Redners, bestimmte Sprechgewohnheiten, körperliche und gesundheitliche Bedingungen usw. Offensichtlich ist diese Information lokalisiert und kann nur in größeren Zeitabständen, die mehrere Sekunden dauern, von Sprache extrahiert werden. Die beliebtesten Merkmale dieser Ebene sind: Rhythmus, Sprachdynamik, Tempo, Modulation der Grundfrequenz, Art der Pausen beim Sprechen, etc. Jedoch sind diese Merkmale schwieriger zu messen und zu bewerten als die auf der akustischen Ebene. Es gibt aber mehrere Methoden für Extraktion und Bewertung über dem richtigen Zeitintervall. Die häufigsten Ansätze sind die Autokorrelationsfunktion, *Average Magnitude Difference Function* (**AMDF**), inverse Filterung für die Grundfrequenz-Erfassung, Energie für die Sprachdynamik und so weiter. Allerdings gibt es viele Modifikationen sowohl für Autokorrelation als auch AMDF.

2.4 Klassifizierung / Entscheidungsalgorithmus

Nach der Merkmalsextraktion und einer möglichen Normalisierung / Kompensationsphase (wird im nächsten Abschnitt dargestellt) muss eine Klassifizierung durchgeführt werden, um zu entscheiden, welcher Benutzer (Funktionen oder Modelle) dem Unbekannten am nächsten kommt. Dennoch ist es möglich, alle abzulehnen, wenn die Koinzidenz / das Vertrauen zu niedrig ist. Es gibt mehrere erfolgreiche Klassifizierungs-Techniken, die sich folgendermaßen unterscheiden: in ihrer Komplexität, in ihrer Art wie sie arbeiten und was sie von den verarbeiteten Daten übernehmen. Diese Methoden sind in verschiedene Hauptkategorien mit ihren jeweiligen Vor- und Nachteile eingeteilt:

- **Nicht-parametrische Methoden** - erlegen den Daten keine Beschränkung auf; sie benutzen kein Modell, um den Raum zu beschreiben. Ihr Hauptvertreter ist die K-Nächster-Nachbar-Methode (KNN). KNN findet k nächsten Vektoren zum Unbekannten und verwendet dann einige Kriterien um über das Ergebnis zu entscheiden.

- **Parameter basierende Methoden**- übernehmen gewisse Strukturen des Merkmalsraums und modellieren ihn mit einigen Parametern. Die erfolgreichste und am häufigsten verwendete ist die Mischung von Gaußverteilungen. Dieses Modell wird als *Gaussian Mixture Model* (**GMM**) bezeichnet. Bei fehlenden Daten und unter Verwendung geeigneter Modelle, die mit dem Raum übereinstimmen, sind diese Verfahren besser als nicht-parametrische Methoden.

- **Diskriminative Methoden** - versuchen den Merkmalsraum, zu modellieren / teilen, so dass der Klassifizierungsfehler so klein wie möglich ist. Es ist sehr einfach, dies mit den Trainingssätzen der Datenbank zu machen, aber es ist schwieriger, es mit ungesehenen Daten zu machen (nur schätzen). In einer solchen Situation ist eine gute Generalisierungsfähigkeit erforderlich (niedrige Fehlerquote). Die wichtigsten Vertreter dieser Gruppe sind neuronale Netze (NN) und *Support Vector Machines* (**SVM**). Sowohl NN als auch SVM können unter bestimmten Bedingungen ausgezeichnete Ergebnisse liefern.

- **Generative Verfahren** - zielen darauf ab, den Raum so nahe wie möglich zu beschreiben, und versuchen nicht, einzelne Benutzer zu unterscheiden. Wenn die Modelle perfekt mit den Daten übereinstimmen (in der Realität tun sie es nicht) ist es möglich, einen optimalen Klassifikator zu konstruieren, der mit geringsten Kosten arbeitet und als Bayes-Klassifikator bezeichnet wird. Auch hier ist das erfolgreichste Modell der oben genannte GMM.

Es ist also vorteilhaft, allgemeine Modelle eines universellen Sprechers zu verwenden, die auf Trainingsproben zahlreicher Sprecher basieren.

2.5 Umweltkompensation

Um die Variabilität einer Sitzung zu verringern, die durch unterschiedliche Trainings- und Testbedingungen (Hintergrundgeräusche, verschiedene akustische Parameter der Aufnahmegeräte und der Zimmer) verursacht werden, wurden mehrere Konzepte entwickelt. Die einfachste Methoden gleichen die Leistung jedes Frequenzbandes aus. Man kann, feste Filtertechniken benutzen, die ein allgemeines Sprachsignal betonen, wie das Verstärken des Sprachmodulationsspektrums oder relative Spektralanalyse (RASTA) Filter. Anspruchsvollere Methoden versuchen optimale Transformationen zu finden, welche die Aufnahme-Funktionen auf die Funktionen in der Bereitstellungsumgebung (das so genannte Feature-Mapping-Verfahren) transformiert. Es kann auch versucht werden, ganze Modelle von Lautsprechern so zu transformieren, dass sie dem Modell der Arbeitsumgebung entsprechen (es heißt Sprechermodell-Synthese). Allerdings basieren diese Methoden auf höherer Mathematik, und ändern ihr Verhalten passend zu den ankommenden Daten. Ändert sich das Arbeitsumfeld, so ändert sich auch die optimale Zuordnung.

Eine andere, weniger anspruchsvolle, aber manchmal nützliche Lösung ist es, vorab aufgezeichnete Sprachproben (Eigenschaften oder Modelle) unter verschiedenen Bedingungen zur Verfügung zu haben und vor der Anwendung die richtige auszuwählen. Dann nutzen Sie für eine bestimmte Aufnahme die Umgebung, die am besten passt. Es ist offensichtlich, dass die besten Ergebnisse beobachtet werden, wenn es eine Übereinstimmung zwischen Trainings- und Testumgebung gibt.

Einen detaillierten Überblick über das Thema der Sprechererkennung sehen Sie z. B. [2].

3 Gesichtserkennung

Gesichter gehören zu den attraktivsten biometrischen Merkmalen und die Gesichtserkennung zur Identifikation von Personen wird zunehmend in einer Vielzahl von Anwendungen eingesetzt. Die Entwicklung von Erkennungsalgorithmen und -Methoden ermöglicht die Nutzung von Identifikations- und Verifikations-Systemen im gewerblichen Bereich. Allerdings erreichen diese Systeme noch nicht vergleichbare Erkennungsraten unter unkontrollierten und ungezwungenen Bedingungen. Gesichtserkennung unter diesen Bedingungen ist noch eine Herausforderung, trotz der jüngsten Fortschritte in der Gesichtserkennungstechniken.

Biometrische Systeme zur Personenidentifikation, die von mehreren Anbietern entwickelt wurden, erreichen eine sehr gute Gesichtserkennungsgenauigkeit. Die meisten dieser Anwendungen erfordern [3]:

- Erkennungssysteme, die mehrere Flächen von einem Video-Frame oder einem Bild erkennen können,
- hohe Erkennungsrate
- Beleuchtungsinvarianz
- Stabilität unter wechselnden Gesichtsausdrücken und Posen
- Erkennung in Echtzeit usw.

Es gibt mehrere Faktoren, die die Leistung und Genauigkeit der Systemen für die Gesichtserkennung beeinflussen können [1]:

- **Beleuchtungs-Schwankungen** entstehen aufgrund der Hautreflexionseigenschaften und der internen Kamerasteuerung. Einige 2D-Verfahren liefern nur unter kleinen Beleuchtungs-Schwankungen gute Ergebnisse bei der Gesichtserkennung.
- **Stellungs-Änderungen (Posen)** beeinflussen den Authentifizierungsprozess, weil sie Verformungen erzeugen. Das System sollte das Problem dadurch lösen, das verschiedene Blickwinkel berücksichtigt, wenn sich das Objekt positioniert (z.B. beim Einsatz von Überwachungskameras). Auf der anderen Seite sind die Algorithmen relativ robust gegenüber dem Gesichtsausdruck (ausgenommen einige extreme Ausdrücke wie ein Schrei).
- **Die Zeitverzögerung** ist auch ein wichtiger Faktor, wenn sich das Gesicht mit der Zeit in einer nichtlinearen Weise über lange Zeiträume (Alters-Variationen) ändert. Im Allgemeinen ist dieses Problem schwieriger zu lösen, verglichen mit den anderen.

3.1 Gesichtserkennungsmethoden

Gesichtserkennungssysteme werden in zwei Kategorien eingeteilt: Verifizierung und Identifizierung.

Die Gesichts-Überprüfung erfolgt in Form einer 1:1-Übereinstimmung. In diesem Prozess wird ein Gesicht einer Person, dessen Identität überprüft werden soll, mit einem Bild als Vorlage verglichen.

Im Gegensatz dazu, ist die Gesichtserkennung ein 1:N Problem. Das Gesicht wird mit allen Bildern einer Gesicht-Datenbank verglichen, um die Identität der Person festzustellen.

Wenn unklar ist, ob sich das getestete Gesicht in der Systemdatenbank befindet, wird wie folgt verfahren. Das Bild des Gesichts wird auch mit allen Bildern in der Datenbank verglichen, wobei für jedes eine Wahrscheinlichkeit berechnet wird. Alle diese Wahrscheinlichkeiten werden nach numerischen Werten geordnet: der höchste Wert steht am Anfang. Falls die Wahrscheinlichkeit den Vorgabewert übersteigt, benachrichtigt uns das System über das Ergebnis [1].

Die ausgewählten Standard-2D-Methoden der Gesichtserkennung:

- Lineare / nichtlineare Methoden der Bildprojektion
    - *Principal Component Analysis (PCA)* - die Methode, basierend auf PCA nennt sich Erkennung des Eigengesichts. Die Hauptidee der PCA ist es, einen Datenraum in eine lineare Kombination aus einer kleinen Sammlung von Basen, die paarweise orthogonal sind und die Richtungen der maximalen Varianz in dem Trainingssatz haben, zu trennen [4].
    - *Kernel PCA (KPCA)* - ist eine Methode der nichtlinearen Merkmalsextraktion. Die KPCA führt zu einer besseren Klassifizierung als die herkömmliche PCA. Die KPCA wird vielfach bei Gesichtserkennung unter variierender Beleuchtung eingesetzt. [4].
    - *Lineare Diskriminanzanalyse (LDA)* - ist in vielen Fällen besser geeignet als die PCA. Die LDA versucht Unterschiede zwischen Klassen zu maximieren, und Unterschiede innerhalb von Klassen zu minimieren. [1].
    - *Discriminant Common Vectors (DCV)* - die Hauptidee des DCV besteht in der Sammlung der Ähnlichkeiten zwischen Elementen der gleichen Klasse. Unterschiede werden dabei ignoriert.[1].
- Neuronale Netze sind nichtlineare Mustererkennungsverfahren. Der Vorteil des neuronalen Klassifikators über den linearen (z.B. PCA, LDA) ist, dass er bei Nachbarschaftsklassen Fehlklassifikationen verringern kann.
- Die Grundidee besteht darin, ein Netz mit einem Neuron für jedes Bildpixel zu konstruieren. Wegen der daraus folgenden hohen Dimension können neuronale Netze nicht direkt mit den Eingangsbildern trainiert werden. Stattdessen wird

eine Dimensionalitätsreduktions-Technik eingesetzt, bevor das eigentliche Training erfolgt [1].

- Fractal und *iterierte Funktionssysteme (IFS)* - IFS Theorie wurde vor allem im Bereich der Bildcodierung entwickelt und in letzter Zeit auch zur Bildindexierung eingesetzt. Der fractale Code eines Bildes ist invariant gegenüber vieler globaler Transformationen wie Drehungen, Kontrast, Skalierung etc. Das IFS Fraktal eines Gesichtsbildes kann zum Trainieren der neuronalen Netzwerke dienen. Hier wird er als Klassifikator verwendet [1].

3.2 Merkmalsextraktion

Einige Gesichtserkennungsalgorithmen basieren auf Merkmalen, die aus einem Bild des Gesichtes der Person extrahiert wurden. Es handelt sich um Gesichtsmerkmale. Zum Beispiel kann ein Algorithmus die relative Position, Größe und / oder Form von Augen, Nase, Mund, Wangenknochen und Wangen analysieren. Diese Merkmale werden dann während der Suche in einer Gruppe von Bildern für die Vergleichs-Funktionen verwendet. Andere Algorithmen normalisieren die Gesichtsbilder und komprimieren die Gesichtsdaten die für die Gesichtserkennung von Bedeutung sind. Ein getestetes Bild wird dann mit den Daten verglichen.

Vor der Merkmalsextraktion sollten alle Bilder vorverarbeitet und normalisiert werden.

Ein Teil der Vorverarbeitung ist die Dimensionsreduktion aller Eingabebilder auf eine definierte Größe. Der Einsatz eines Kontrast beschränkten adaptiven Histogrammausgleichs (*contrast limited adaptive histogram equalization* -- **CLAHE**) – kann verwendet werden. Die normalisierten Bilder können maskiert werden, um den Hintergrund auszublenden und nur den Gesichtsbereich zu behalten.

Das Hauptziel des Normierungsverfahrens besteht darin, die unkontrollierten Variationen, die während des Akquisitionsprozesses auftreten zu minimieren und die beobachteten Unterschiede bei den Gesichtsmerkmalen zu erhalten.

Auch eine Änderung der Körperhaltung kann zu Variationen in den Bildern führen.

Die Merkmalsextraktion umfasst die Verringerung der Menge von Ressourcen, die für die Beschreibung einer großen Datenmenge erforderlich sind. Während der Gesichtserkennung wird die Analyse einer großen Datenmenge durchgeführt. Die Analyse mit einer großen Anzahl von Variablen erfordert im Allgemeinen eine große Menge an Speicher und Rechenleistung. Die Merkmalsextraktion führt zu einer Reduzierung der benötigten Variablen und Daten.

Für die Extraktion von Gesichtsmerkmalen werden am häufigsten die Kantennachweisverfahren eingesetzt. Sehr gute Ergebnisse werden auch mit *Local Binary Patterns* (**LBP**) erreicht.

Kantenerkennung Bezeichnet eine Reihe von mathematischen Methoden, deren Hauptziel es ist, die Punkte in einem digitalen Bild zu erkennen, bei dem sich die Helligkeit stark ändert. Diese Spezielle Kantenoperatoren sollen die Übergänge zwischen den Bildpunkten erkennen und diese Reihen von gekrümmten Liniensegmenten als Kanten markieren.

Die am häufigsten verwendeten Funktionen für die Kantenerkennung sind Sobel-Operator (auch Sobel-Filter genannt), Prewitt-Operator oder Gabor-Filter.

Die Extraktion von Gesichtsmerkmalen aus vorverarbeiteten Bildern kann über LBP-Histogramme durchgeführt werden. LBP-Histogramme sind eine der besten Merkmale zum Erkennen von Gesichtern auch in Fällen, wo nur eine begrenzte Anzahl von Proben zur Verfügung steht und können leicht in Echtzeit [5] (Abb. 2.1) berechnet werden.

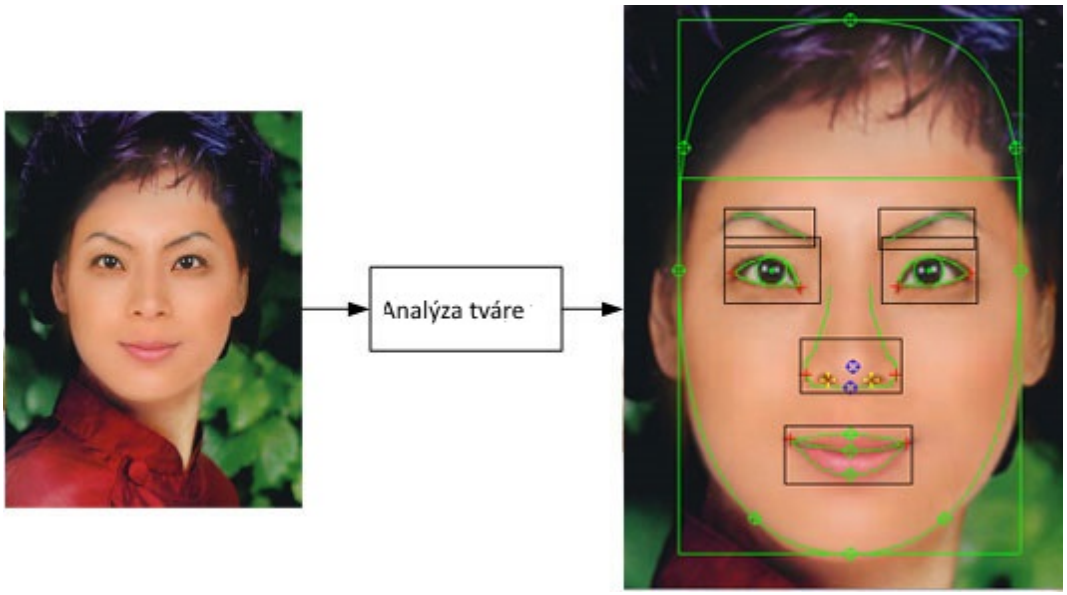

Abb. 2.1 – Beispielergebnis zur Merkmalsextraktion

3.3 Gesichtsklassifizierung

Ein Gesichtserkennungssystem arbeitet in der Regel in zwei Hauptphasen. Die erste Phase ist ein Trainingsprozess und die zweite ist die Klassifizierung von Benutzern. Moderne Gesichtserkennungsverfahren arbeiten ordnungsgemäß, wenn bis zu 10 Bilder einer Person in der Trainingsphase verfügbar sind. Es wurden zahlreiche Techniken zur Gesichtserkennung von nur einem einzigen Bild pro Person entwickelt. Der Trainingsprozess sollte vollständig automatisiert werden und die Benutzer müssen in der Lage sein, ihn zu kontrollieren. Der Trainingsprozess verwendet Clustering-Algorithmen.

Der Hauptzweck aller Clusteralgorithmen ist es, die Cluster oder Klassen im Eingabedatensatz zu identifizieren. Es gibt viele Clusteralgorithmen. Diese Algorithmen können in zwei Gruppen eingeteilt werden: Partitionierungs- und hierarchische Algorithmen [5].

Als Beispiel für einen Clustering-Algorithmus kann K-Mittel genannt werden. Ein anderer Algorithmus, der zur Clusterbildung verwendet wird, ist der **SOM** (*self-organizing map)*, der zu den neuronalen Netzwerk-Techniken oder **DBSCAN** (*density-based spatial clustering of applications with noise*) Methoden gehört.

Zur Klassifizierung von Gesichtsmerkmalen stellen wir zwei Verfahren vor, die abhängig von der Anzahl von Trainingsbildern und der Anzahl von Identitäten verwendet werden können:

- *Support Vector Machine* (**SVM**) - wird verwendet, wenn nur eine relativ geringe Anzahl von Identitäten in dem System angenommen wird. Hauptnachteil dieser Methode ist die zeitaufwendige Ausbildung des Modells, wenn eine große Anzahl von Proben verwendet wird.

- *K-Nächster-Nachbar* (**KNN**) Abstands-Übereinstimmung (mit dem Einsatz des Chi-Quadrat Abstandes) - dieser Algorithmus kann leicht parallelisiert und in verteilten Systemen verwendet werden. Das Training wird einfach durch Einsetzen der Features in die Datenbank [5] durchgeführt.

3.4 Gesichts-Lokalisierung und -Erkennung

Biometrische Gesichtserkennungssysteme finden sich in unterschiedlichen Anwendungen. Derzeit ist ein intelligentes TV-Gerät mit Gesichtserkennungssystem ein typisches Beispiel für eine solche Anwendung. In Smart-TV wird die Gesichtserkennung für die Zuschauer-Authentifizierung verwendet. Auf dieser Basis können personalisierte Dienste oder verschiedene Empfehlungen zur Verfügung gestellt werden. Gesichtserkennungssysteme sollten in Echtzeit arbeiten und in der Lage sein, eine oder mehrere Identitäten zu erkennen. Die meisten dieser Systeme umfassen auch eine grafische Benutzerschnittstelle für den automatischen Trainingsprozess (Abb. 2.1).

Normalerweise erfordert die 2D-Gesichtserkennung die Verarbeitung der Eingabe von einer Kamera. Der Prozess der Gesichtserkennung besteht aus Teilprozessen wie:

- **Bildaufnahme** - liest ein Bild von der Kamera ein, konvertiert es in das System-Format und gibt es an den System-Prozess weiter
- **Gesichts-Lokalisierung** - lokalisiert die Gesichter im Bild und assoziiert die gefundenen Koordinaten mit dem Bild. Abhängig von der verwendeten Kamera wird der entsprechende Lokalisierungsalgorithmus implementiert
- **Trainingsprozess** - Clustering-Algorithmen werden verwendet, z. B. K-means
- **Vorverarbeitung** lokalisierter Flächen einschließlich Histogrammausgleich
- **Normalisierung** – z. B. Größenänderung
- **Merkmalsextraktion** - extrahiert Merkmale aus vorverarbeiteten Gesichtern, LBP kann verwendet werden
- **Gesichtsklassifizierung** – Verwendung von Methoden wie SVN oder KNN
- **Gesichtserkennung** - in der Regel werden nur frontale Gesichter als Bild ausgewertet, weil die überwiegende Mehrheit der Gesichtserkennungsmethoden nur mit diesem Format zuverlässig arbeiten. Sobald das Gesicht erkannt ist, kann es verfolgt werden, was Rechenressourcen spart, auch wenn sich die Haltung der Person ändert [3]. Die Informationen über den erkannten Benutzer werden als Ausgabe gesendet.

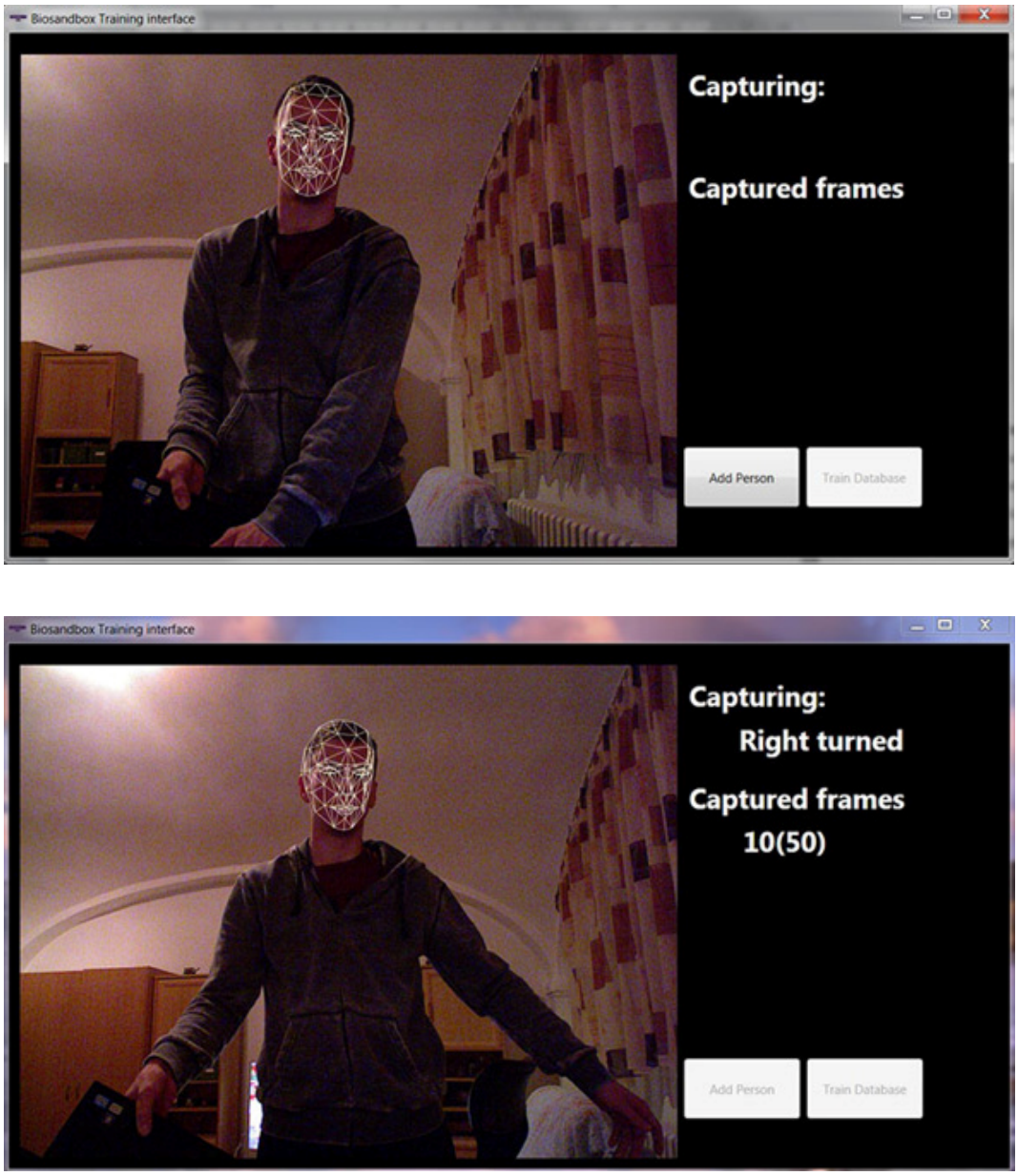

Abb. 2.2 – Beispiel für das Training eines Gesichtserkennungssystem

3.5 Iris-Erkennung

Iris ist eines der beliebtesten biometrischen Merkmale. Die Kombination von berührungslosem Abtasten, Langzeitstabilität und eine hohe Erkennungsgenauigkeit ermöglichen den Einsatz bei der Kontrolle als auch für den Einsatz in Sicherheitsanwendungen.

Es wurde gezeigt, dass die Iris-Erkennungsgenauigkeit von der Qualität des aufgenommenen Irisbildes und der Bildvorverarbeitung abhängt. Um den negativen Einfluss der Beleuchtung zu reduzieren, wird der Einsatz einer Infrarotkamera mit NIR (nahes Infrarot) empfohlen (Abb. 2.3). Die Verwendung von NIR-Licht ermöglicht das hinzufügen einer Nebenlichtquelle, ohne die Bilderkennung zu beeinflussen.

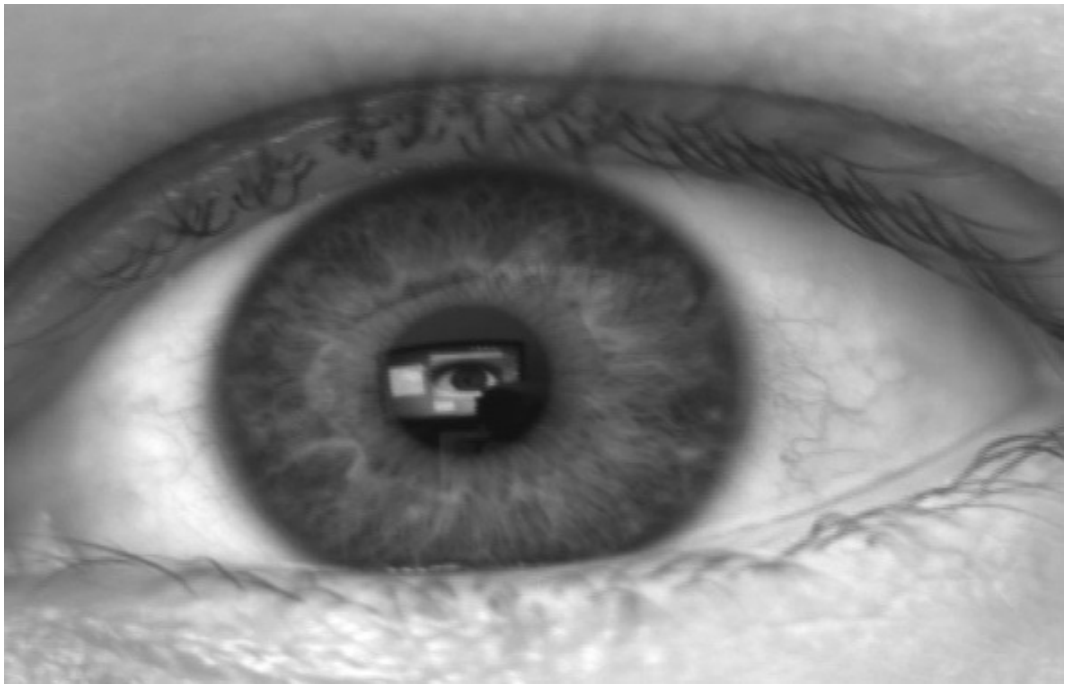

Abb. 2.3 – Ein Beispielsbild mit einer Guppy F-038 B NIR-Kamera aufgenommen

Die Iris basierte Identifikation besteht aus Iris-Lokalisierung, Merkmalsextraktion und Klassifikation. Eines der erfolgreichsten Systeme archiviert in kontrollierten Umgebungen mit hundertprozentiger Genauigkeit. Aber die Lokalisierung und Normalisierung für die Anwendungen muss für den praktischen Einsatz verbessert werden. Dieses System verwendet einen Gabor-Filter bei dem die Merkmalsextraktion, wobei die gefilterten Signale auf zwei Ebenen quantisiert werden. Durch dieses Verfahren bleiben die Zeichenfolgen von Binärziffern (Merkmale) erhalten. Die Erkennung wird durch die Abstimmung der folgenden Proben unter Verwendung des KNN-Verfahrens und einer Hamming-Distanz durchgeführt.

4 3D-Gesichtserkennung

Die Gesichtserkennung auf der Basis einer 2D-Gesichtserkennung ist ein häufiger und natürlicher Ansatz. 3D-Gesichtserkennungs-Ergebnisse ergeben in der Regel eine höhere Sicherheit als die 2D-Gesichtserkennung.

Auf der 3D-Gesichts-Erkennung basierende Techniken sollten mehrere Eigenschaften wie Robustheit gegenüber Beleuchtungsschwankungen sowie Position, Drehung und Skalierung des ursprünglichen Modells in einem absoluten Bezugssystem besitzen [1].

4.1 3D-Gesichtserkennungsverfahren

Im Vergleich zur 2D-Gesichtserkennung profitiert die 3D-Gesichtserkennung von der größeren Anzahl der Gesichtsmerkmale. Beiden Ansätze benötigen die Vorverarbeitung wie Größen-Normalisierung, Rotation in eine neutrale Position usw. Die zusätzliche dritte Dimension liefert reichhaltige Informationen, die 2D-Bilder nicht liefern können. Die wichtigsten Vorteile auf 2D-Gesichtsanalyse sind:

- kein Einfluss durch Beleuchtungveränderungen oder die Verwendung von Kosmetika
- unempfindlich gegenüber Unterschieden im Aussehen
- einfachere Handhabung bei Haltungvariationen
- Projektive Art von 2D-Bildern
- Vereinfacht Gesichtsmerkmalserfassung, Lagebestimmung und Körperhaltungskompensation

Ausgewählte 3D-Gesichtserkennungs-Verfahren:

- Oberflächenbasierten 3D-Gesichtserkennung - Dieser Ansatz basiert auf der klassischen 3D-Objekterkennungstechniken (Abb. 3.1). Es gibt verschiedene Arten von Erkennungsverfahren auf der Basis von:
  - Verwendung von lokalen Krümmung Features, die rotationsinvariant sind (z.B. Kurve des Gesichtsprofils)
  - Verwendung von Punkt-zu-Punkt-Übereinstimmung (Polygon aus mehreren signifikanten Gesichtspunkten)

Abb. 3.1 – Oberflächenbasierte 3D-Erkennung

- Aussehenbasierte 3D-Gesichtserkennung - Bei dieser Methode beschäftigt man sich mit „eigenfaces“ und „fisherfaces“. Eine genaue Ausrichtung der Probe und der Bilder in der Datenbank ist erforderlich. Gesichtsmerkmale wie Augen, Mund, usw. werden ermittelt und für die Erkennung verwendet. Das Verfahren ist einfach zu implementieren und ist nicht zeitintensiv (Abb. 3.2).

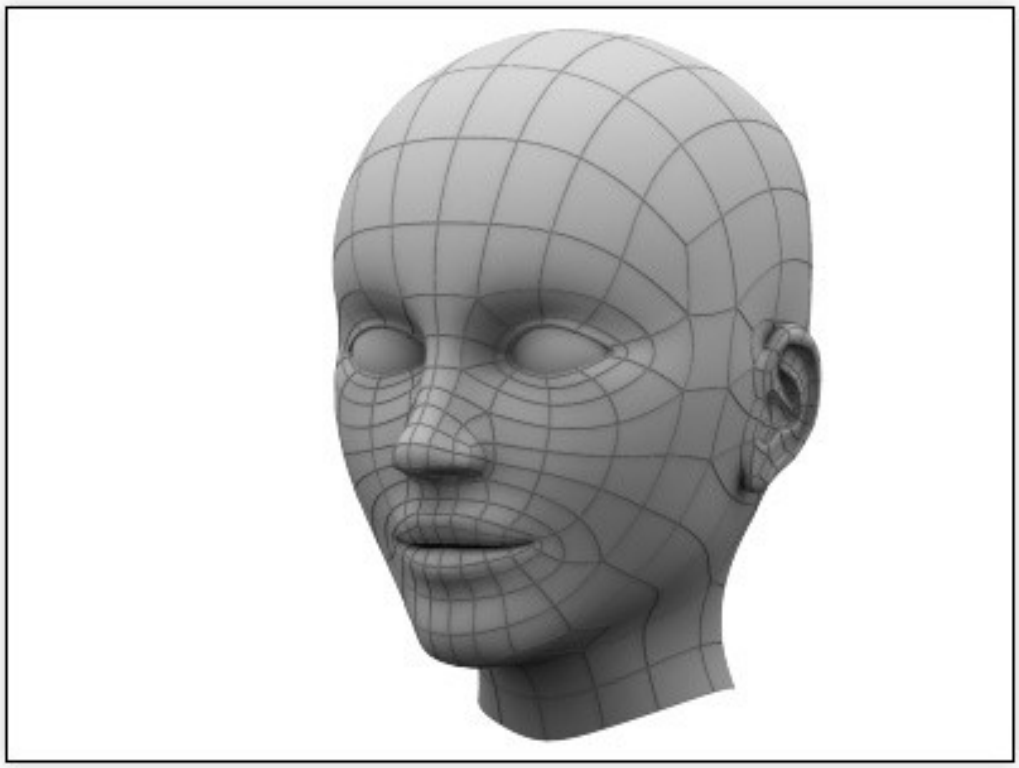

Abb. 3.2 – Aussehenbasierte 3D-Erkennung

- Modellbasierte 3D-Gesichtserkennung - Diese Methode basiert auf der Analyse von Syntheseverfahren, in der das 3D verwandelbare und kommentierte Gesichtsmodell erzeugt wird und die dann mit Modellen in der Datenbank verglichen wird. Das Verfahren eignet sich nicht für Echtzeitanwendungen (Abb. 3.3).

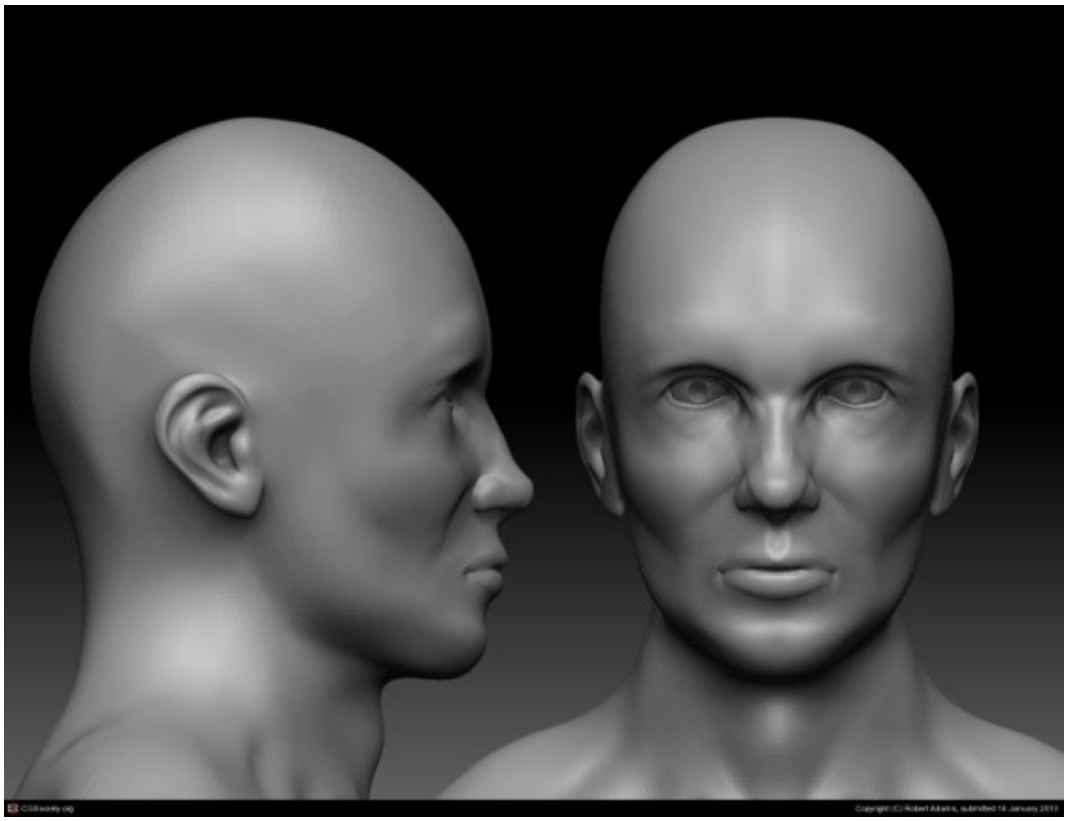

Abb. 3.3 – Modellbasierte 3D-Erkennung

4.2 Vorverarbeitung und Datenerfassung

Am Anfang des gesamten Prozesses wird die 3D-Gesichtsoberfläche erfasst. Das Beispiel der Erstellung von 3D-Gesicht ist in Abb. 3.4 - Abb. 3.6 dargestellt. Es gibt verschiedene Möglichkeiten, wie man dieses Ziel erreichen kann, beispielsweise durch den Einsatz von Stereokameras, Tiefenkameras, Laser, optische oder Laserscanner usw.

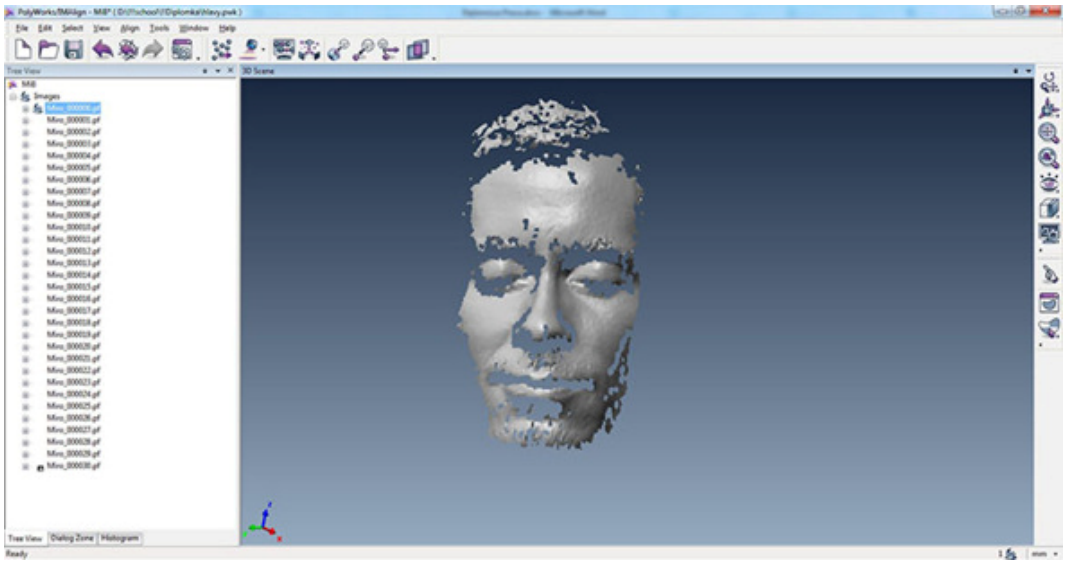

Abb. 3.4 – Ein Scan

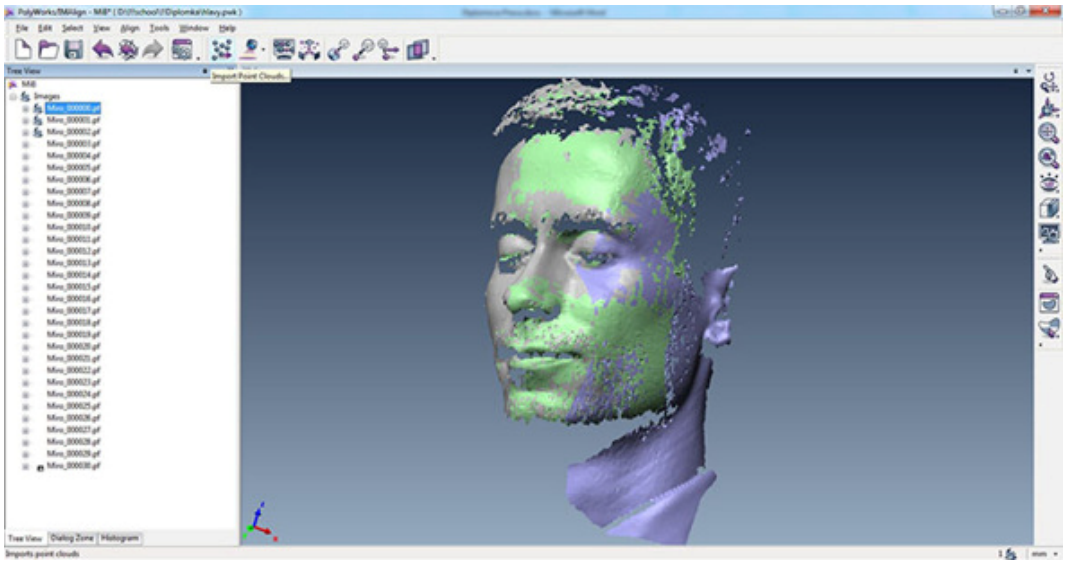

Abb. 3.5 – Mehrere gescannte Bilder erstellen ein Gesicht

Abb. 3.6 – Finales 3D-Modell des Gesichts

Aus dem aufgenommenen Bild wird nur das Gesicht benötigt, weshalb das Entfernen der äußeren Bildteile notwendig ist. Das Gesicht wird mit 4 Punkten am Kopf markiert. Die Seitenkanten werden aus Punkten, am linken und rechten gebildet. Der höchste Punkt bildet den oberen Rand und der tiefste Punkt bestimmt den unteren Rand. Das Entfernen basiert auf diesen vier Punkten.

Die erfassten Daten werden anschließend unter Verwendung von Merkmalsextraktionsalgorithmen vorbereitet.

Der Zweck der Merkmalsextraktion ist es, Information aus den Bildern zu extrahieren, die für die Unterscheidung der Gesichter von verschiedenen Personen relevant und in Bezug auf die photometrischen und geometrischen Variationen der Bilder stabil sind.

Als Merkmale können unterschiedliche Gesichtspunkte (Kopf oben, Stirn, Augen, Kinn, Nase, Kinn, Mund, etc.) und die Abstände zwischen diesen ausgewählten Punkten im 3D-euklidischen Raum (Abb. 3.7) verwendet werden.

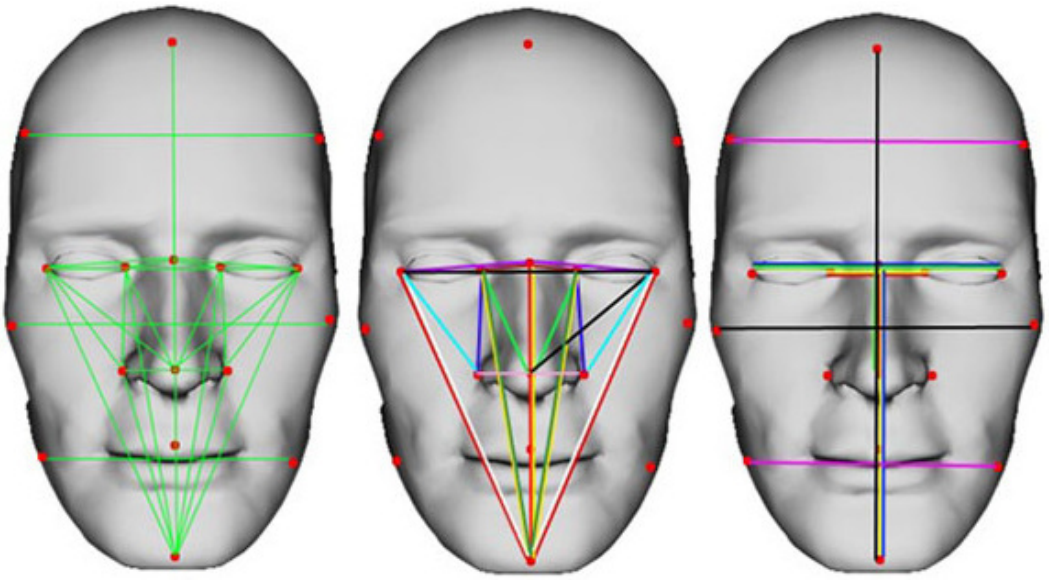

Abb. 3.7 – Beispiel für Gesichtsmerkmale

4.3 3D-Gesichtserkennungsanwendungen

3D-Gesichtserkennung kann auch in vielen Anwendungen verwendet werden wie z.B. für einen sicheren Zugang zu Systemen oder für die Personenerkennung am Smart TV, wenn beim Online-Shopping Kinder nicht zugelassen sind, etc.

Die Aufgabe der 3D-Gesichtserkennungs erfordert, wie die 2D-Gesichtserkennung einen Zugang mit einer Kamera. Für die 3D-Gesichtserkennung muss die 3D-Gesichtsfläche erfasst werden. Der Prozess der Gesichtserkennung besteht aus Teilprozessen wie:

- 3D-Gesichtsoberflächenerfassung - Es gibt verschiedene Wege, wie diese Aufgabe umgesetzt werden kann, beispielsweise durch Stereokameras, Laser oder Tiefenkamera (z.B. der Kinect) usw.
- Vorverarbeitung - die erfassten Daten werden anschließend Vorverarbeitet
- Merkmalsextraktion - der Zweck der Merkmalsextraktion ist es, die kompakten Informationen aus den Bildern zu extrahieren, die zur Unterscheidung zwischen den Gesichtsbildern von verschiedenen Personen und in Bezug auf die photometrischen und geometrischen Variationen der Bilder stabil und relevant sind
- Messung der Entfernung - der letzte Schritt der 3D-Gesichtserkennung ist die Messung des Abstands zwischen dem 3D-Gesicht der Testbenutzer und den 3D-Gesichtern in der Datenbank. Es gibt verschiedene Techniken, um den Abstand zu messen. Die einfachste Methode ist eine lokale und globale Distanz zweier Gesichter zu messen. Hierzu ist es nötig, die Gesichtspunkte wie Augen, Nase, Mund, Kinn, Ohren, etc. richtig und sehr genau zu bestimmen und ihre vorgegebenen Abstände mit etablierten Metriken zu messen. Die anspruchsvolleren Methoden sind KNN-Techniken, einschließlich SVM usw.

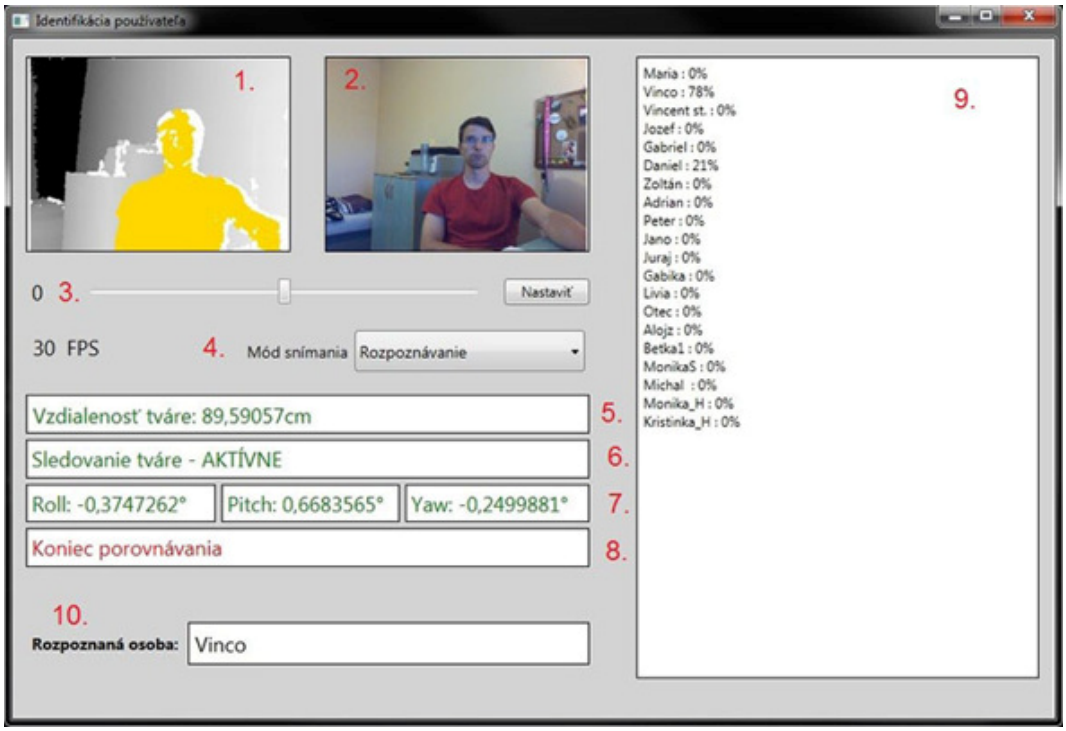

Abb. 3.8 – Beispiel der GUI für die 3D-Gesichtserkennung

5 Authentifizierung

Der autorisierte Zugang zu Systemen verlangt die Überprüfung der Identität. Es gibt im Wesentlichen drei notwendige Schritte, die Identifikation, die Authentifizierung und die Autorisierung [6].

Identifizierung – der Benutzer wird durch Token oder Identifikations-String identifiziert (Telefonnummer oder E-Mail-Adresse)

Authentifizierung - nach der Identifizierung muss ein String oder Token angenommen werden, der und Benutzer muss seine Identität nachweisen.

Autorisierung - Zulassen oder Verweigern des Zugriffs auf den angeforderten Inhalt oder auf eine Reihe von Aktionen abhängig von den erteilten Zugangsrechten.

Das System kann Benutzer authentifizieren, basierend auf der Annahme, die Benutzer wissen etwas (Memometrie), erkennen etwas (Kognometrie), besitzen etwas oder haben etwas was charakteristisch für jede Person (Biometrie) ist. In allen drei Formen teilen das System und der Benutzer ein Geheimnis (das heißt einen Authentifizierungsschlüssel).

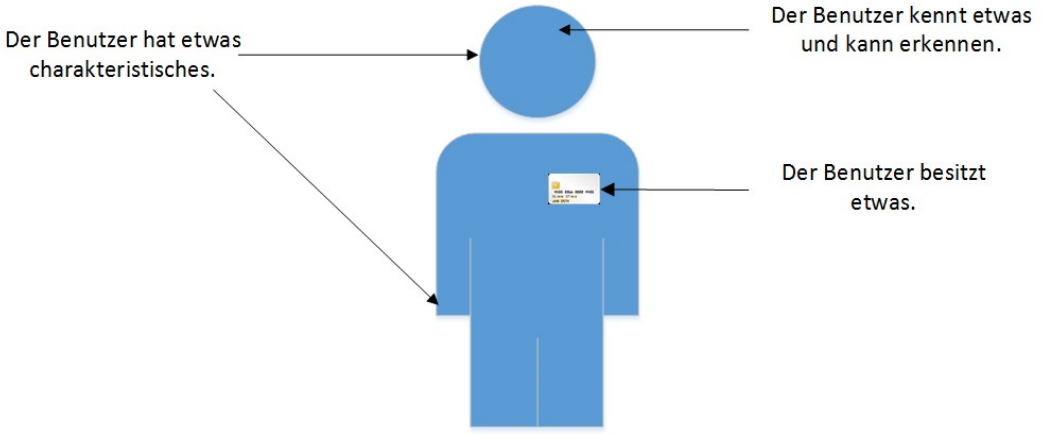

Abb. 4.1 – Benutzerauthentifizierungsoptionen

5.1 Typen von Authentifizierungsmechanismen

Basierend auf aufgeführten Authentifizierungstypen können die folgenden Gruppen von Authentifizierungsmechanismen unterschieden werden.

Biometrie

Biometrie ist der Vergleich von anatomischen, physiologischen und Verhaltensmerkmalen einer Person. Biometrische Authentifizierungsmechanismen fallen in zwei Hauptkategorien:

- **Behavioral Biometrie** - basierend auf den Bewegungen, z.B. die Handhabung des Computer-Maus, Latenz, die Dynamik von Tastenanschlägen oder die Signatur der Dynamik eines Benutzers.
- **Physiologische Eigenschaften** - basierend auf Fingerabdruck, Stimme, Pupille, Merkmalsausprägungen von Gesicht, Hand- oder Fingergeometrie oder sogar die Form des Ohres des Benutzers.

Es ist schwierig, biometrische Technologien miteinander zu vergleichen. Jede hat andere Werte der Genauigkeit, Zuverlässigkeit und Benutzerfreundlichkeit. Die einfachste biometrische Methode ist die Gesichtserkennung. Methoden, die spezifische Position des Körpers für den Sensor (Iris-Erkennung) erfordern und daher weniger komfortabel sind, können aber genauere Ergebnisse erzielen.

Memometrics

Diese Art von Authentifizierungsmechanismus basiert auf der Generierung von Zufallssequenzen von Buchstaben oder Zahlen Passwort genannt, wenn es ein numerischer Wert ist dann nennt man sie PIN, wenn sie mehr als ein Wort enthält bezeichnet man es als Passphrase. Kennwörter können auch eine semantischer Form haben.

Kennwort Typen:

- Zufallskennwort - die beliebteste Art der Authentifizierung mit einem hohen Maß an Sicherheit [7].
- semantischer Kennwort- basiert auf einem deduktiven Prozess, dabei wird der Benutzer aufgefordert mehrere Fragen zu beantworten, um eine genaue Antwort zu erhalten (Abb. 4.2) [8].

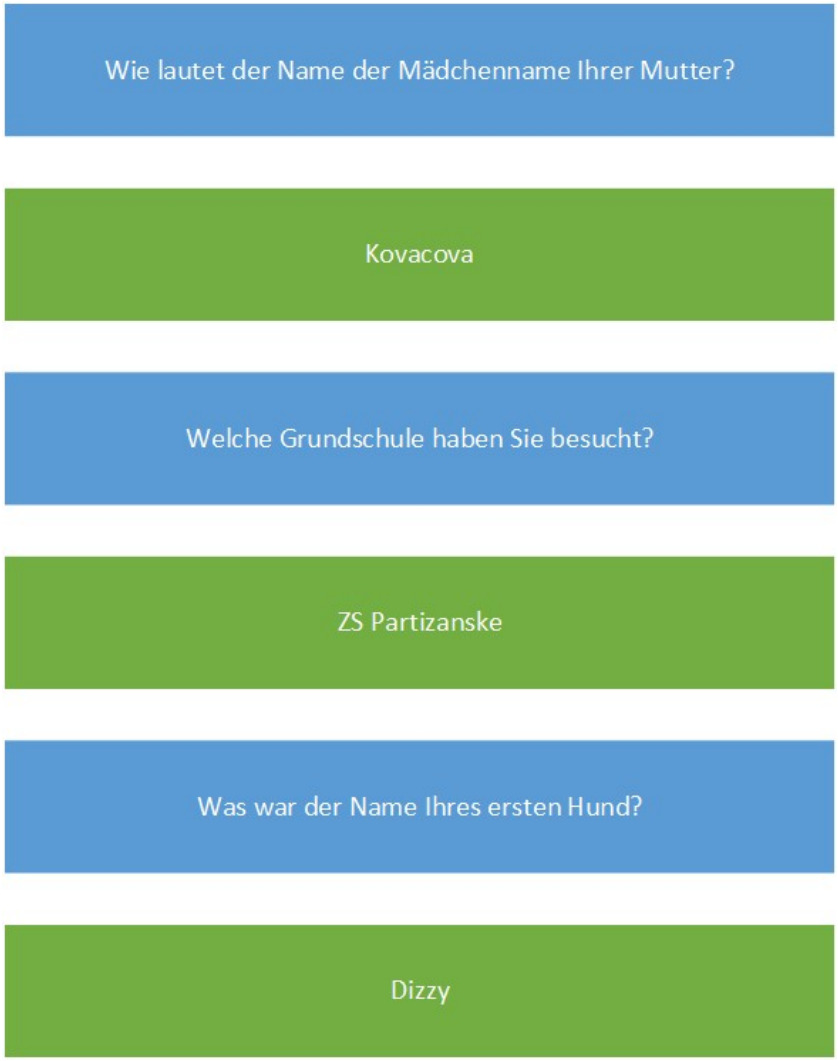

Abb. 4.2 - Grundprinzip des semantischen Kennwortes

Cognometrics

Die Idee der grafischen Authentifizierung basiert auf dem visuellen Gedächtnis des Benutzers. Wissenschaftliche Studien weisen darauf hin, dass der Mensch riesige und nahezu unbegrenzte Möglichkeiten hat, sich Bilder merken [9].

Grafische Schlüsselwörter gewinnen an Popularität vor allem für Handys oder Tablets, z.B. für die Freischaltung. Es gibt zwei Hauptprinzipien:

- Grafische Schlüsselwörter basierend auf Wiedererkennung - der Benutzer wählt das Zielbild zwischen der Menge der störenden Elemente in der Szene aus. Dieser Ansatz basiert auf das visuelle Gedächtnis. Ziel ist es, das zuvor gesehene Objekt zwischen den Mengen der anderen zu erkennen.
- Grafische Schlüsselwörter basierend auf der Position - mit diesem Prinzip muss ein Benutzer Muster zeichnen, in der Regel in einem Gitter und das erfordert ein visuell-räumliches Gedächtnis und präzise Bewegungen.

Eigentum

Die Authentifizierung kann auf etwas basieren, das der Benutzer besitzt. Dieses Objekt ist ein Token. Ein gutes Beispiel ist das Token SecurID von RSA Security in Abb. 4.3 [15].

Abb. 4.3 – Token Beispiel: SecurID - RSA Security

Token erstellt einen Zahlencode durch eine Verschlüsselungsfunktion, die den Sperrenschlüssel und Geheimschlüssel kombiniert und zeigt ihn auf dem LCD an. Um die Authentifizierung durchzuführen, gibt der Benutzer den Zahlencode vom LCD als SecurID Token ein. Der Authentifizierungsserver kennt auch, den Geheimschlüssel, die Uhrzeit und das Datum der im Token des Benutzers gespeichert ist. Mit diesem Wissen führt der Authentifizierungs-Server die gleichen kryptographischen Funktionen aus. Für eine erfolgreiche Authentifizierung muss der erzeugte Wert mit dem Wert, der vom Anwender eingegeben wurde, übereinstimmen.

Eine andere Art von Authentifizierungstoken erfolgt über die USB (Universal Serial Bus) -Schnittstelle.

Tokens werden als *Software (SW)* oder *Hardware (HW)* zur Verfügung gestellt.

Der Hauptnachteil der HW-Token ist, dass Benutzer ihn immer bei sich tragen muss.

Die SW-Token werden auf dem Benutzer-PC oder Laptop gespeichert. In diesem Fall kann der Benutzer auf das System nur von dem PC zugreifen, auf dem der Token gespeichert ist.

5.2 Menschliche Faktoren im Authentifizierungsprozess

Mehrere Authentifizierungsszenarien verwenden Public-Key-Verschlüsselungsverfahren (Public Key-Kryptographie). Ein Benutzer kann zum Beispiel eine Chipkarte besitzen, die den entsprechenden öffentlichen Schlüssel und einen privaten Schlüssel beinhaltet. Während der Benutzerauthentifizierung, sendet das System eine zufällige Herausforderung. Der Benutzer unterschreibt die Herausforderung mit seinem privaten Schlüssel und sendet das Ergebnis. System verifiziert die Signatur mit einem öffentlichen Schlüssel. Auf diese Weise kann das System den Benutzer authentifizieren, ob er den richtigen privaten Schlüssel hält ohne die Notwendigkeit, den Schlüssel zu akzeptieren. Statt einer Speicherung des öffentlichen Schlüssel in einer Datei auf dem Remote-System, kann eine Smartcard eine Herausforderung und ein unterzeichnetes Zertifikat des öffentlichen Schlüssels erzeugen, das von einem Dritten unterzeichnet wird. Dies ist als Public Key Infrastructure (PKI) benannt und basiert auf den ITU-T-Spezifikationen.

Abb. 4.4 zeigt die in dem Authentifizierungsprozess beteiligten Stellen. Bei jedem Schritt dieses Verfahrens kann ein potentieller Angreifer Zugriff auf den Authentifizierungsschlüssel erhalten.

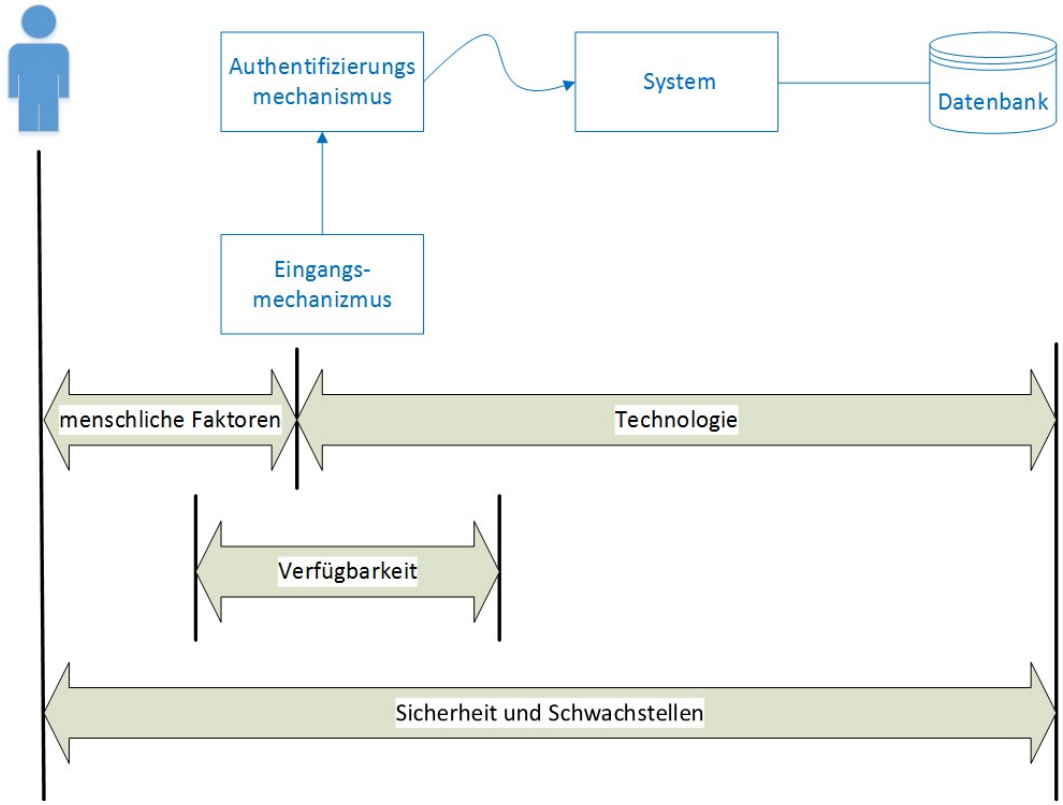

Abb. 4.4 – Entitäten in dem Authentifizierungsprozess beteiligt

Der empfindlichste Bereich ist das Eingabegerät und der Benutzer. Wenn die Authentifizierung auf Wissen (Passwörter, PIN, etc.) basiert, muss sich der Benutzer den Geheimschlüssel einprägen. Das Passwort merken, ist für viele Menschen schwierig, sie teilen oft und bewusst ihr Passwort mit jemandem oder notieren es auf Papier.

Sicherheit kann nicht mit Hardware allein gelöst werden, da die Benutzer ein Teil des Authentifizierungsprozesses sind [10].

6 Autorisierung

Autorisierung bedeutet, basierend auf den Zugriffsrechten, die Verifikation der Person am Eingang (beim Netzbetreiber oder Dienst),. Darüber hinaus definiert sie für den identifizierten und authentifizierten Benutzer, welche Informationen zugänglich bzw. welche Aktionen erlaubt sind.

6.1 Berechtigungsmodell

Berechtigungsmodelle (Abb. 5.1) werden verwendet, um die Zugriffsregeln für das System (oder ein Objekt) und seine Dienste zu definieren und zu steuern. Grundlegende Berechtigungsmodelle sind [11]:

- *Frei verfügbare Zugriffssteuerung (DAC)* - erlaubt dem System (oder ein Objekt) Eigentümer zu definieren, wer Zugriff auf das System hat
- *Verbindliche Zugriffssteuerung (MAC)* – Benutzerzugang ist über Klassifikationen definiert.
- *Rollenbasierte Zugriffssteuerung (RBAC)* - am häufigsten verwendet. Benutzer sind in Gruppen mit definierten Rollen aufgeteilt. Entsprechend der Rolle des Benutzer kann er auf das System zugreifen.
- *Aufgabenbasierte Zugriffssteuerung (TBAC)* - in diesem Modell wird ein Zähler für die Anzahl der Zugriff des Benutzers auf das System definiert. Wenn dieser Wert erreicht ist, wird der nächste Zugriff abgelehnt.
- *Attributbasierte Zugriffssteuerung (ABAC)* - zur Kontrolle werden Benutzerzugriffattribute verwendet.

Alle genannten Modelle können kombiniert werden.

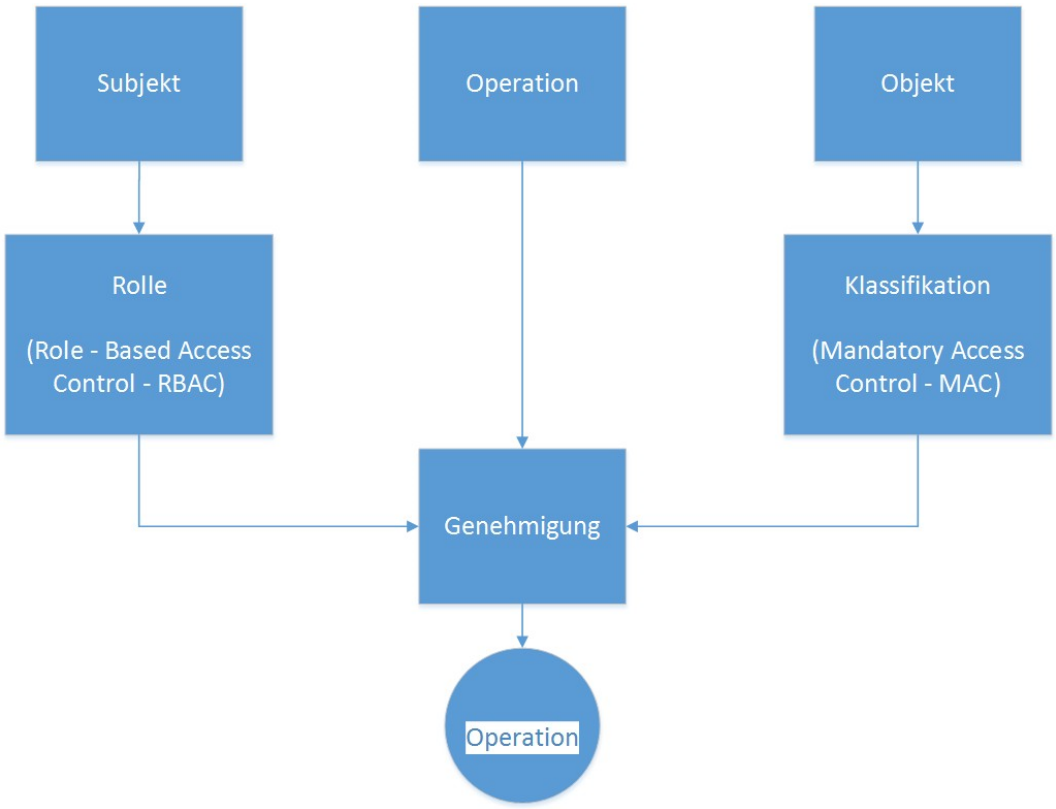

Abb. 5.1 – Berechtigungsmodell

6.2 Zugriffsmanagementregeln

Einer der am häufigsten verwendeten Techniken der Zugriffssteuerung (Abb. 5.2) ist die Zugangsmatrix. Zeilen der Matrix repräsentieren Benutzeroptionen und Spalten repräsentieren Benutzerobjekte. Diese Technik wird häufig als *Access Control List* (**ACL**) [12] bezeichnet.

Inhaltsabhängige Zugriffskontrolle ist eine weitere Technik, bei der ein Benutzer mehr Informationen oder detailliertere Datenobjekte als ein anderer Benutzer erhalten kann. Diese Entscheidung kann von Faktoren wie Alter, verwendetes Terminal, Zugangspunkt, der Zugangs IP-Adresse des Benutzers und der Zeit abhängig sein.

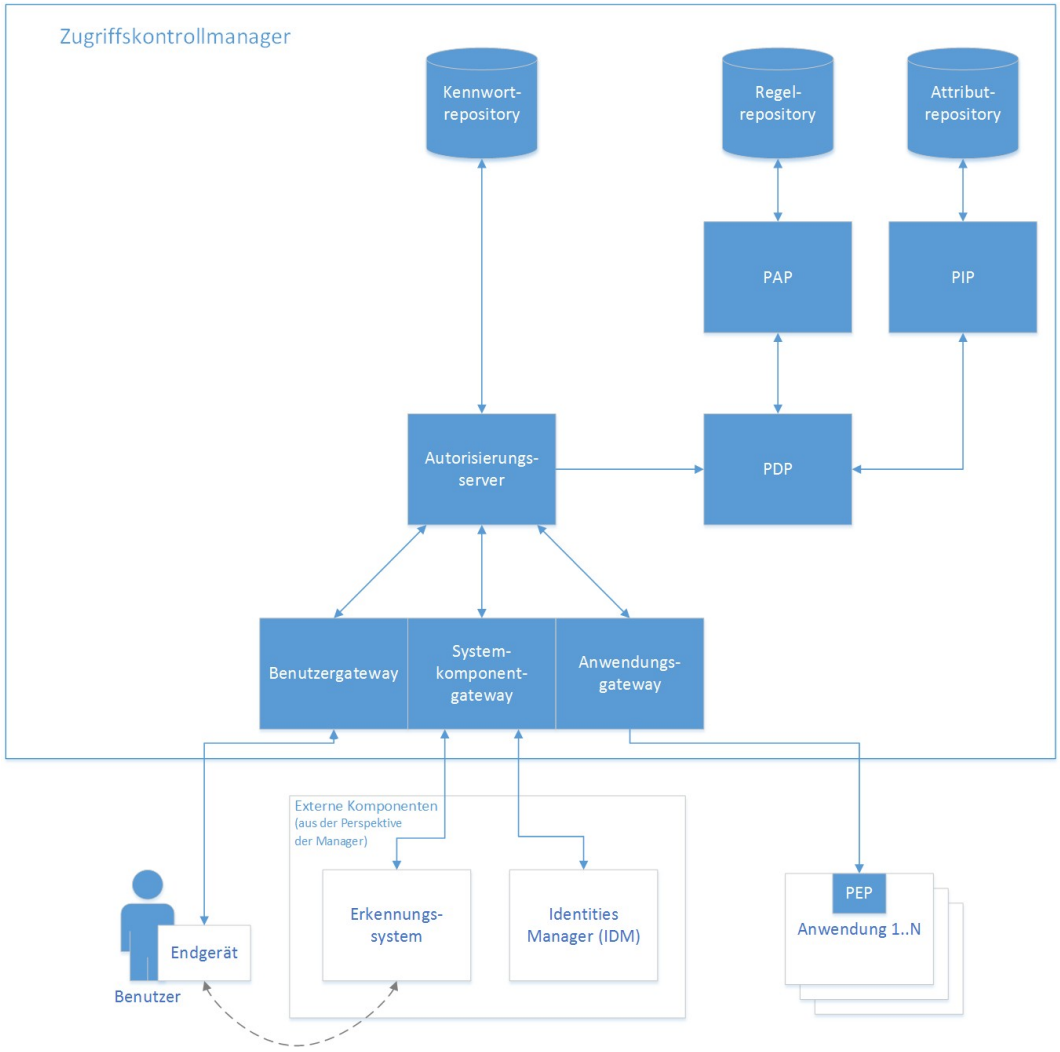

Abb. 5.2 –Zugriffskontrollmanager

6.3 Zugriffsrechte

Der Entscheidungsprozess, wenn eine Anforderung für den Zugriff auf ein bestimmtes System kommt, kann von Zugriffsrechten in einer Autorisierungsdatei abhängig sein. Die Zugriffesregeln basieren auf den Modellen, die in Abschnitt 5.1 Autorisierungsmodell beschrieben wurden.

Beispiel

In einem System wird das RBAC-Modell verwendet und drei Rollen definiert:

- Administrator
- Eigentümer der Gruppe
- Benutzer der Gruppe

Administratoren weisen einem Besitzer oder Benutzer die Zugriffsrechte auf Anwendungen im System zu. Der Gruppenbesitzer kann auch Zugriffsrechte für jeden Benutzer auf spezielle Applikationen in dem System vergeben. Wenn der Administrator dem Gruppenbesitzer die Rechte gegeben hat, die in einer bestimmten Anwendung erlaubt, die Inhalte zu ändern und zu löschen, können Gruppenbesitzer diese Rechte einem Benutzer zuweisen. In diesem Fall kann der Benutzer auch Inhalte erstellen d.h. er kann auch als Eigentümer der Daten auftreten. Beispiel für solche Anwendungen sind Dienste für geteilte multimediale Inhalte.