The focus of this thesis is the inconspicuous authentication multimodal biometric recognition via face, fingerprint and signature characteristics of X. Such an authentication method enables to recognize one based on the facial features, finger patterns and the way (s)he signs. There are two main advantages of this approach. First, finger and face can be captured via easily available sensors, which are already adapted through day to day life activities. Hence, there are no additional hardware costs for deploying this method. Second, a user does actively come across to enroll him as these traits are well known and widely acceptable.

These two factors assure the high usability of face, fingerprint and signature based biometric authentication, which does not require extra interaction time. In addition, the computational power of embedded hardware is steadily increasing, resulting in a wide variety of different applications. Some of these applications, like customer services, require the user to authenticate him.

Different authentication methods exist. The most common one is the knowledge-based authentication, where the user has to enter a secret, e.g. a PIN or password. Token-based authentication methods require the user to present some kind of physical object like a smartcard or a regular door key. This thesis focuses on biometric authentication. Biometric methods authenticate the user based on his physiological or behavioral characteristics. The main advantage of these methods is that the secret necessary for authentication is directly linked to the subject; hence, it cannot be forgotten or passed to somebody else easily.
The main procedure when using a biometric system is as follows. During enrolment, the subject presents his biometric characteristic to the sensor and the biometric reference is computed and stored for later comparison. During authentication, the biometric characteristic is captured again and the extracted biometric probe is compared to the reference. Based on the similarity or dissimilarity of the two data, the subject is authenticated or rejected. Various systems using different biometric modalities exist; the most common are face and fingerprint authentication.

In this thesis a behavioral biometric modality is evaluated, namely signature, which is the way a subject is signing in combination with face and fingerprint. The data are captured via fingerprint sensors, face cameras and signature pad available in the laboratory. The following figure 1.1 shows a typical workflow of the thesis.

![Figure 1.1 Typical flow of the work presented](image)

Previous research on face-fingerprint, face-signature, face-fingerprint-speech based biometric recognition indicated that these biometric modalities have promising features. Nevertheless, the so far conducted research had several drawbacks.

- The evaluation databases were collected using dedicated sensors; hence it was unclear if the sensors vary with different environments are of suitable precision.
The main focus was on extracting features and using template-based classification algorithms. Other approaches, like machine learning algorithms, have not been considered although they showed promising results for different biometric modalities.

The testing databases do mainly contain only standard databases and often the data are collected with controlled environment.

Solving these drawbacks is the motivation to the research described in this thesis. This is reflected by the research questions presented in the following section.

1.1. Research Questions

The main research question motivating the work in this thesis is

“Can multimodal biometric authentication using face, fingerprint and signature recognition improve the performance at different fusion levels i.e. at score and decision fusion?”

The before-mentioned drawbacks of previous research have to be overcome to answer this question.

The research is divided into the following more specific questions:

1. Are basic image processing algorithms in combination to high performance algorithms more suitable than the formerly proposed biometric recognition methods?

2. What are suitable features extraction techniques to describe multimodal biometrics?

3. Does the multimodal biometric system using face, fingerprint and signature are suitable to real-time environment with improved accuracy?

3. Do we propose a hybrid score and decision level fusion system for better performance?

4. Does the biometric performance decrease due to change in type of sensors and environment at the time of enrollment?

5. How is the biometric performance when reference and probe are obtained from data collected with environments and sensors?

6. How is the biometric performance of the proposed methods in a scenario test?
7. Are current systems capable of performing the necessary feature extraction and classification steps with an acceptable computational complexity for modified biometric data?

1.2. Structure of the Thesis

This thesis considers the aspects to be solved in order to deploy a face fingerprint and signature based multimodal biometric recognition as an authentication method. To introduce the reader to the area of authentication on multimodal biometrics and to face, fingerprint and signature recognition, the state of the art for these topics is presented. The design of an application for authentication is presented.

The focus of the thesis is the verification of relevant features and composition of suitable face, fingerprint and signature recognition methods. Different databases focusing on different goals are applied in the evaluation.

To get comparable results, several methods are evaluated in a similar manner on each database.

The following sections give a short overview over the remaining part of the thesis.

Chapter 2 Authentication for Digital Era

For authentication on digital machines, two different approaches are relevant. The most popular is PIN authentication, which is a knowledge-based authentication method. Biometric authentication is an alternative approach with the advantage that the user does not have to remember the secret key because it is extracted from the required biometric characteristic. Various methods for both approaches, knowledge-based and biometrics are presented in this chapter. In addition, the results of a survey concerning multimodal authentication are presented.

Chapter 3 Proposed Models for Multimodal Biometrics Authentication

This chapter presents the design of a multimodal biometric authentication system using face, fingerprint and signature modalities. The system offers the possibility to integrate and test several authentication methods, like face recognition or signature authentication. Referring to this system, the components of a general biometric system for individual biometrics viz. face authentication system, fingerprint authentication system and signature authentication system are explained. The three different systems and two multimodal systems are proposed and described.
Chapter 4 Experiments and Results

The performance evaluation had the goal to perform a scenario test on a close to realistic data set. This means that subject data taken for the study is not only from controlled environment and standardized database but also from real-time Flickr portal image database like AFLW face database, CMU facial expressions etc. This chapter presents the results for PCA, DCT-PCA, DWT-PCA, SWT-PCA algorithm, and the developed multimodal biometric technique at score level and decision levels of fusion. The thorough evaluation presents amongst others the best amount of training data, and classification results for each subject.

Chapter 5 Conclusion and Future Work

Based on the results described in the previous chapters, final conclusions are made in this chapter. The research questions and respective answers are summarized. In addition, proposals for future work are made.