Multimodal Biometric Systems

Project report submitted in partial fulfillment
of the requirements for the degree of

Bachelor of Technology
in
Electronics and Communication Engineering

by

Mohit Akhouri - 19ucc023
Hitesh Goyal - 19uec023
Agraj Garg - 19uec113
Aditya Pandey - 19ucc043

Under Guidance of
Dr. Joyeeta Singha

Department of Electronics and Communication Engineering
The LNM Institute of Information Technology, Jaipur

May 2023

Acknowledgments

We would like to express our sincere and heartfelt gratitude to our mentor and supervisor, **Dr. Joyeeta Singha** for giving us this opportunity to work on this project under his guidance and whose expertise in this field, inspiring ideas and his understanding, patience and mentorship gave us a sense of direction and was very instrumental to complete the project in an effective and sagacious way.

This project helped us in enriching our knowledge about the different concepts and techniques used in the project and how to use them in correct way. The project helped us in expanding the spectrum of our knowledge further more. We would also like to thank our family and friends who helped in keeping ourselves motivated throughout this journey.

Abstract

The project revolves around the idea of developing a **Multimodal Biometric System** for verification and recognition purposes. We discussed about the role of biometrics in today's world and why we need to shift our attention from unimodal biometric systems to multimodal biometric systems. Multimodal biometric systems have gained significant attention in recent years as an innovative approach enhancing reliability and accuracy. These systems use multiple biometric modalities such as facial features, iris scans, voice, fingerprints and much more to create a comprehensive and robust biometric system.

The project focused on different types of input modes in multimodal biometric systems and types of fusion which we can achieve in these types of systems. The fusion of multiple biometric traits leads to increased accuracy and reliability compared to uni-modal systems. By combining the strengths of different modalities, multimodal biometric systems can overcome the limitations of unimodal biometric systems, such as sensitivity to environmental factors or vulnerabilities to spoof attacks.

We also studied three research papers related to the design of multimodal biometric systems and gained a comprehensive understanding of how these systems work. We can combine modalities such as fingerprints, iris scans and facial features and can achieve a much more better result compared to unimodal counterparts. **Deep Learning** may also be utilized in these systems which combines features from multiple modalities and accordingly take the decision. We can develop much advanced fusion techniques to combine information from multiple input modalities.

We designed a system using two modalities which were - voice data and facial features. The results obtained from these systems were compared with unimodal counterparts and found to be much better. Multimodal biometric systems have both pros and cons and we need to take care of the fact when to design these systems for maximum benefit. Some challenges are also there in designing these systems which could be a part of future research work.

Contents

Chapter 1

Unimodal Biometric Systems

1.1 About Biometric Systems

Biometric Systems use personal characteristics to authenticate or identify a person. The system designed would collect biometric characteristics which are unique to every person. As biometrics is on the rise, biometric systems are being integrated in the most common areas of everyday life. The most efficient one is called **Automated Biometric Identification System**.[1]

There are different types of biometric systems which are in use today :

- **Fingerprint Recognition** : This is one of the most widely used biometric traits. Fingerprint recognition systems analyze the unique patterns and ridges on an individual's fingertips to establish identity. They are commonly employed in law enforcement, access control systems, and mobile devices.
- **Facial Recognition** : Facial recognition systems capture and analyze facial features, such as the shape of the face, eyes, nose, and mouth, to identify individuals. These systems have gained popularity in surveillance, airport security, and mobile device unlocking.
- **Iris scans** : Iris recognition systems use the intricate patterns in the colored part of the eye to identify individuals. The complex and stable nature of iris patterns makes this biometric trait highly reliable. Iris recognition is often utilized in high-security environments and border control.
- **Voice Recognition** : Voice recognition systems analyze the unique vocal characteristics, including pitch, tone, and pronunciation, to authenticate individuals. They are commonly used in phone banking, voice assistants, and forensic investigations.

- **Palmprint Recognition** : Palmprint recognition systems capture and analyze the distinctive patterns on an individual's palm. Palmprints are useful in scenarios where fingerprints may be difficult to obtain or analyze accurately, such as in healthcare or physical access control.

- **Keystroke Dynamics** : Keystroke dynamics is a form of behavioral biometrics that focuses on analyzing the unique typing patterns and rhythms of individuals. Keystroke dynamics systems monitor and analyze various aspects of an individual's typing behavior, such as the duration of key presses, the time intervals between keystrokes, and the overall typing speed. These behavioral patterns are considered unique to each individual and can be used to establish their identity.

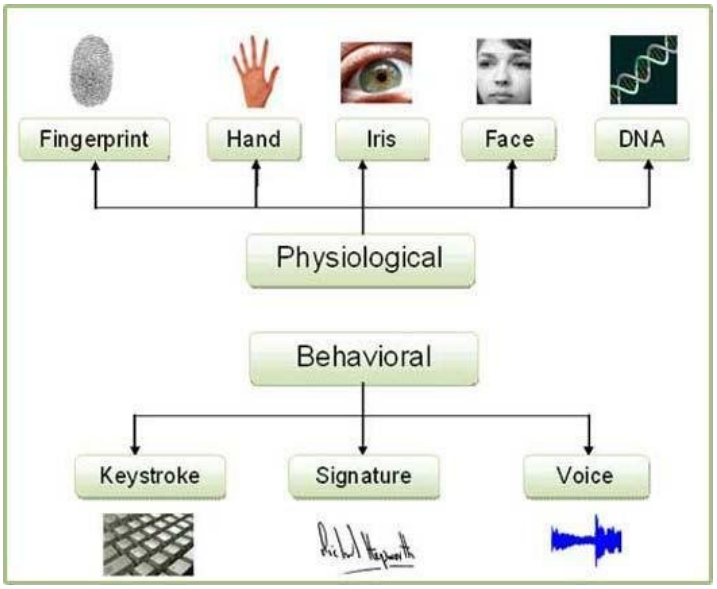

FIGURE 1.1: Types of Biometric Systems

1.2 History of Biometrics

In the second century B.C., the **Chinese emperor Ts'In** She was already authenticating specific seals with a fingerprint. Fingerprints were first used in a commercial setting in 1858 by **William James Herschel**, a British administrator in India. Having been put in charge of building roads in Bengal, he had his subcontractors sign contracts with their fingers. That was an early form of biometric authentication and a sure way of finding them quickly if they defaulted. At the end of the 19th century, **Bertillon**, a French police officer, took the first steps in scientific policing. He used physical measurements of specific anatomical characteristics to identify reoffending criminals, which often proved successful. [2]

1.3 Applications of Biometric Systems

Biometric systems find applications in almost every sphere of life which are summarized in the points below [2] :

- **Justice and Law enforcement** : Biometric technology and law enforcement have a very long history, and many very important innovations in identity management have emerged from this beneficial relationship. Fingerprint, face, and voice recognitions play a unique role in improving public safety and keeping track of the people we are looking for.
- **Border control and airport** : Biometric systems are being used at the border points. They help to automate the proess of border corssing. Reliable and automated passenger screening initiatives and automated SAS enhances international passenger travel experience.
- **Healthcare Sector** : Biometric proved as a enhanced model in the healthcare sector. Medical records are accurate and can be accessed quickly through the use of biometric systems.
- **Financial Transactions** : Biometrics are increasingly being integrated into financial services for secure and convenient transactions. For example, some banks are implementing fingerprint or facial recognition in mobile banking apps for user authentication during login or for authorizing transactions.
- **Smart Homes and IoT** : Biometrics are integrated into smart home systems for personalized and secure access. Facial recognition or fingerprint scanning can be used to unlock doors, activate personalized settings, and control IoT devices within a smart home environment.
- **Identity Verification** : Biometric systems are employed for identity verification purposes, particularly in industries such as banking, border control, and law enforcement. By comparing an individual's biometric data with stored records, these systems can authenticate a person's identity with a high level of accuracy.

1.4 Working of a Unimodal Biometric System

The Architecture of a unimodal biometric system consists of different parts which are depicted in the figure below.

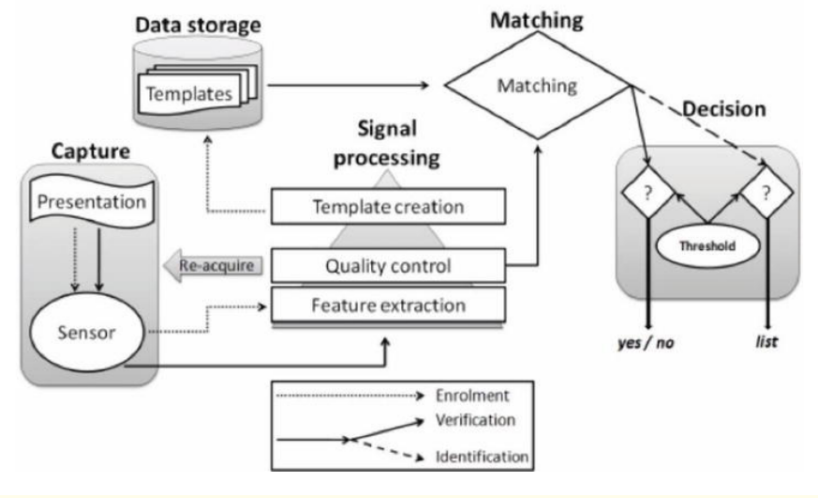

FIGURE 1.2: Architecture of a Biometric System

The description of various components in the architecture of a biometric system are discussed as following :

- **The capture module** that represents the entry point of the biometric system and consists in acquiring the biometric data in order to extract a digital representation. This representation is used later in the following phases.
- **The module of signal processing** makes it possible to optimize the processing time and the digital representation acquired in the enrollment phase in order to optimize the processing time of the verification phase and the identification.
- **The storage module** that contains the biometric templates of the system enrollees.
- **The matching module** that compares the data extracted by the extraction module with the data of the registered models and determines the degree of similarity between the two biometric data.
- **The decision module** that determines whether the similarity index returns through the matching module is sufficient to make a decision about the identity of an individual. [2]

1.5 Problems faced by Unimodal Biometric Systems

Unimodal biometric systems, which rely on a single biometric modality for identification and authentication, can face several challenges. Here are some common problems associated with unimodal biometric systems [3] :

1. **Accuracy and Reliability** : Unimodal systems can be affected by accuracy and reliability issues specific to the chosen biometric trait. Factors like variations in biometric features, environmental conditions, or sensor limitations can lead to false positives (incorrectly accepting an unauthorized person) or false negatives (failing to recognize an authorized person).

2. **Noisy Sensor Data** : Noise may be present in the acuired biometric data due to improperly maintained or faulty sensors. The noise may affect the reliability and accuracy of biometric systems.

FIGURE 1.3: Noisy Sensor Data for fingerprint and iris scans

3. **Non-Universality** : Certain biometric traits may not be universally present in every individual or may not be suitable for all users. For example, individuals with certain medical conditions or disabilities may have difficulty providing usable fingerprints or iris scans, limiting the effectiveness of unimodal systems.

FIGURE 1.4: Non-Universality of fingerprint scans

4. **User Acceptance and User Experience** : Unimodal systems may not always provide a seamless or user-friendly experience. Users may find certain biometric traits inconvenient or uncomfortable to use, leading to a lower level of user acceptance and potential resistance to adoption.

5. **Vulnerability to Spoofing Attacks** : Unimodal systems are often susceptible to spoofing attacks, where an unauthorized individual tries to deceive the system by presenting fake or replicated biometric traits. Techniques such as presenting artificial fingerprints, high-resolution photographs, or voice recordings can trick the system into granting access to unauthorized individuals.

Chapter 2

Multimodal Biometric Systems

2.1 Introduction

Multimodal Biometric Systems refer to systems that combine multiple biometric modalities or traits to enhance identification and authentication processes. Instead of relying on a single biometric trait, such as fingerprints or facial recognition, multimodal systems leverage a combination of different biometric characteristics for more robust and accurate identification.

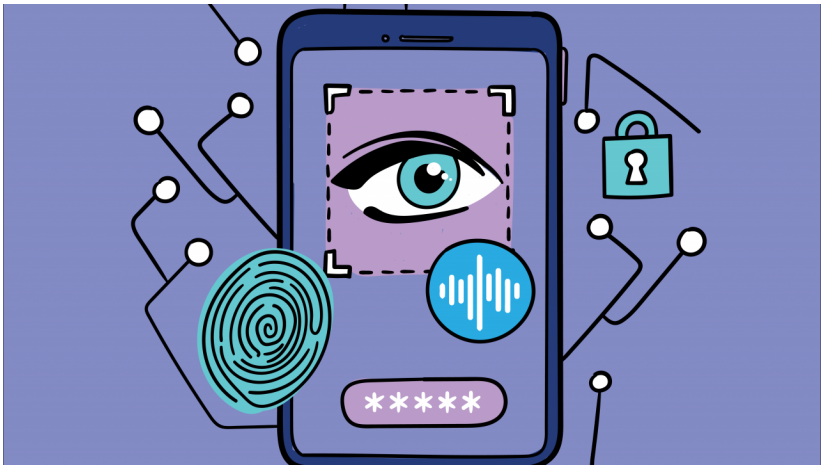

FIGURE 2.1: Multimodal Biometric Systems

By utilizing multiple biometric modalities, multimodal systems can compensate for the limitations or vulnerabilities present in individual traits. They enhance the system's robustness against spoofing attacks, provide better accuracy in identification, and offer increased flexibility and user acceptance by accommodating various user preferences and requirements.

It is important to note that the selection of specific biometric modalities for a multimodal system depends on factors such as the application, level of security required, user population, and infrastructure considerations.

2.2 Scenarios in Multimodal Biometric Systems

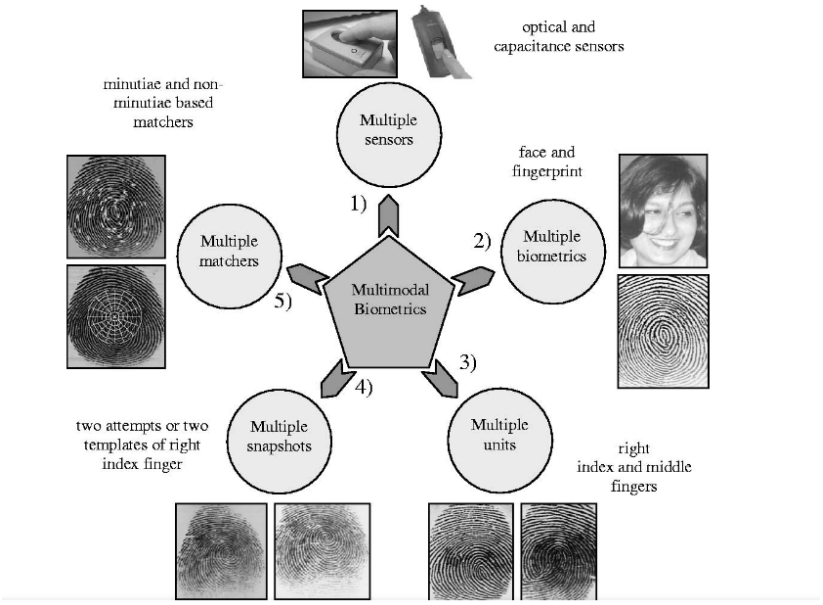

FIGURE 2.2: Scenarios of a Multimodal Biometric System

Multimodal biometric systems can be designed to operate in one out of the five following scenarios which are discussed as below [4]:

- **Multiple sensors** : The information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.
- **Multiple biometrics** : Multiple biometric characteristics such as fingerprint and face are combined. These systems will necessarily contain more than one sensor with each sensor sensing a different biometric characteristic. In a verification system, the multiple biometrics are typically used to improve system accuracy, while in an identification system the matching speed can also be improved with a proper combination scheme.
- **Multiple units of the same biometric** : Fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.
- **Multiple snapshots of the same biometric** : More than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.
- **Multiple representations and matching algorithms for the same biometric** : This involves combining different approaches to feature extraction and matching of the biometric characteristic. Verification system can use the combination scheme to make recognition decision while identification system may use combination scheme for indexing.

2.3 Modes of Operation of Multimodal Biometric Systems

A Multimodal Biometric System can operate in any one the following three modes [3] :

- **Serial Mode** : In serial mode, the output of one biometric trait is used to narrow down the possible identities before the next biometric trait is put into use.

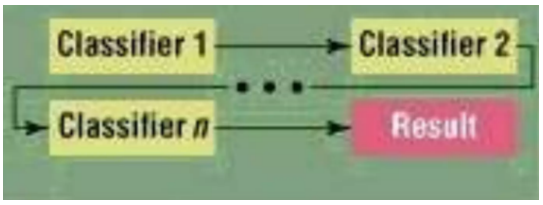

FIGURE 2.3: Serial Mode

- **Parallel Mode** : Information obtained from multiple biometric modalities are used simultaneously to peform identification and recognition.

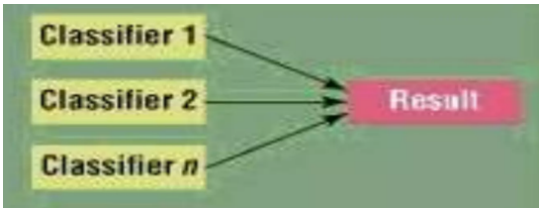

FIGURE 2.4: Parallel Mode

- **Hierarchical Mode** : In this mode, Individual classifiers are arranged in a tree-like structure.

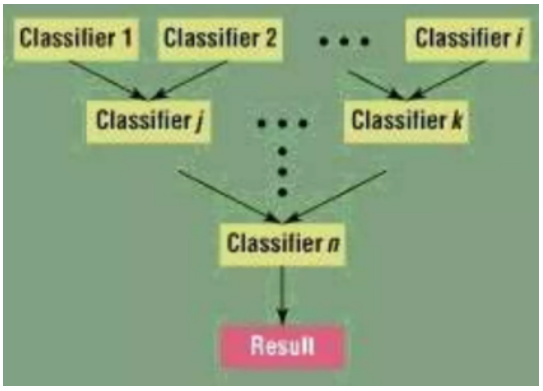

FIGURE 2.5: Hierarchical Mode

2.4 Types of Fusion in Multimodal Biometric Systems

Multimodal Biometric systems integrate information provied by multiple input biometric modalities. The biometric information can be consolidated at various levels. The different types of fusion techniques are discussed as below [3] :

- **Fusion at the feature extraction level** : In this type of fusion, **feature vectors** are being combined. Fusion at feature level provides better recognition results. The only catch here is that, if features of different modalities are compatible with each other then fusion at feature level achieves more accuracy,

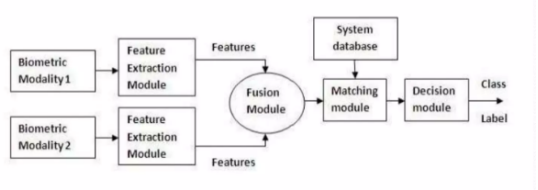

FIGURE 2.6: Feature Level Fusion

- **Matching Score Level Fusion** : Each biometric matcher provides a similarity score which indicates the proximity of the input feature vector with the template feature vector. These scores can be combined for verification. **Weighted averaging** can be used to combine the matching scores reported by multiple matchers.

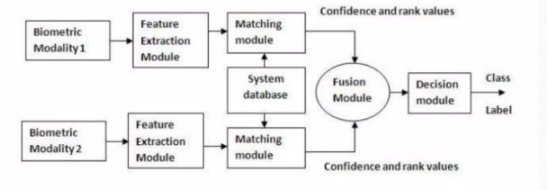

FIGURE 2.7: Matching Score Level Fusion

- **Decision Level Fusion** : Each biometric system makes its own recognition decision based on its own feature vector. **Majority vote scheme** used to make final decision.

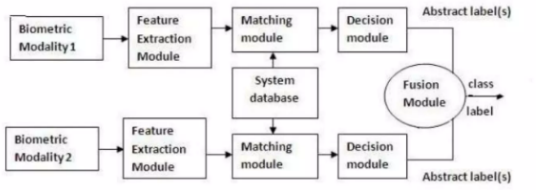

FIGURE 2.8: Decision Level Fusion

Chapter 3

Literature Review

3.1 Research Paper 1

The research paper "**Multimodal Biometric System Based on Fingerprint, Iris, and Face Recognition**" by **Smith et al.** shed light on the following points [5] :

- The authors propose a **comprehensive multimodal biometric system** that combines the modalities of fingerprint, iris, and face recognition.
- The study focuses on developing efficient and accurate feature extraction techniques for each modality.
- The authors explore **fusion strategies** to effectively integrate the extracted features.
- Extensive experiments are conducted using a large dataset to evaluate the performance of the proposed system.
- The results demonstrate **superior recognition accuracy** compared to single-modal systems.
- The multimodal system exhibits **enhanced security** and **robustness** against spoofing attacks, making it suitable for applications where high levels of accuracy and reliability are essential.

3.2 Research Paper 2

The research paper"**A Novel Approach for Multimodal Biometric Fusion Using Deep Learning**" by **Lee et al.** shed light on the following points [6] :

- This research paper presents a novel approach for multimodal biometric fusion using **deep learning** techniques.
- The study aims to leverage the capabilities of deep neural networks to enhance the performance of multimodal biometric systems.
- The authors propose a **specialized neural network architecture** that combines the features extracted from multiple biometric modalities, such as fingerprints, iris patterns, and facial features.
- The fusion model employs a **hierarchical framework** that captures both local and global features, enabling **improved discriminative capabilities**.
- The research includes extensive experiments conducted on benchmark datasets to evaluate the performance of the proposed approach.
- The results demonstrate **significant performance gains** compared to traditional fusion techniques.
- The utilization of deep learning in multimodal biometric fusion shows promise for achieving higher accuracy and more reliable identification results.

3.3 Research Paper 3

The research paper "**Secure Multimodal Biometric System based on Fingerprint and Palmprint Fusion**" by **Chen et al.** shed light on the following points [7] :

- This research paper focuses on the development of a secure multimodal biometric system based on the fusion of **fingerprint** and **palmprint** modalities.
- The study addresses the challenge of **ensuring robustness and security** in biometric systems.
- The authors propose a fusion algorithm that combines the features extracted from fingerprint and palmprint biometrics at both the **score** and **feature levels**.
- The fusion process enhances the system's accuracy and resilience against various **spoofing attacks**.
- Experimental evaluations are conducted using **benchmark datasets** to assess the performance of the proposed system.
- The results demonstrate improved accuracy compared to single-modal systems.
- The proposed secure multimodal biometric system has potential applications in access control and identity verification, offering **enhanced security** and **reliability** in real-world scenarios.

Chapter 4

Proposed System

4.1 Description of the System

The Multimodal biometric system employs two modalities which are as follows :

- Facial Features - **Visual Modality**
- Voice - **Auditory Modality**

4.2 Workflow Diagram of the System

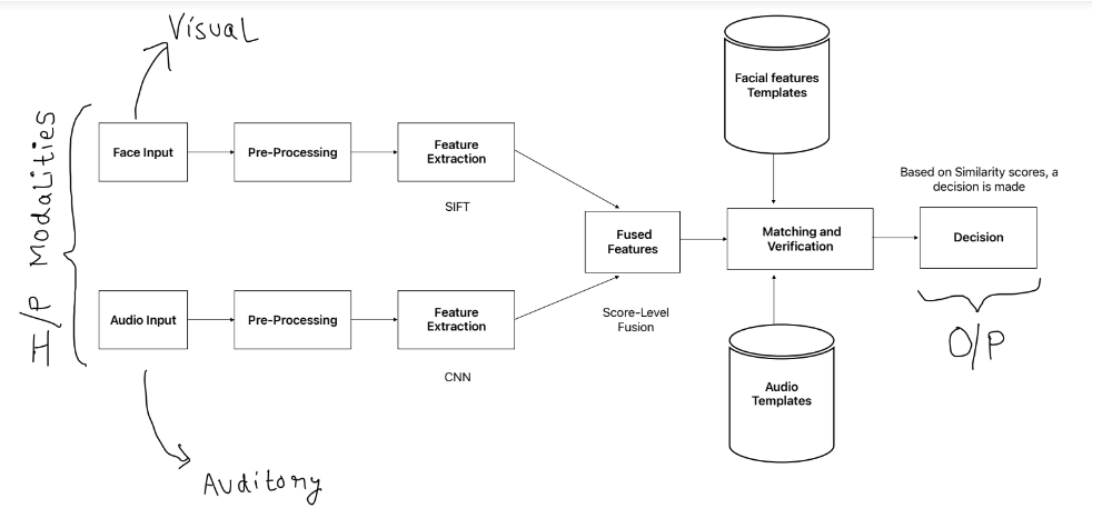

FIGURE 4.1: Block Diagram of the System

4.3 High Level Overview of the system

The **high-level overview** of the system will be as follows :

1. **Data Acquisition** : The system will require devices to capture both facial and voice biometric data from individuals. For facial data, a camera or a webcam can be used, while a microphone will be used to capture voice data.
2. **Preprocessing** : The captured data will be preprocessed to enhance its quality and extract relevant features.
    - Preprocess the **facial data** :
        - Perform face detection to locate faces in the images or video frames.
        - Perform face alignment to normalize the facial features.
        - Apply normalization techniques to improve image quality, such as contrast adjustment or noise reduction.
    - Preprocess the **audio data** :
        - Apply noise reduction techniques to remove background noise.
        - Perform voice activity detection to identify speech segments.
        - Extract voice features, such as MFCC, from the speech segments.
3. **Feature Extraction** : In this step, representative features will be extracted from the preprocessed data. The algorithms for feature extraction from facial and voice data will be as follows -
    - Feature Extraction from **Preprocessed facial data** :
        - Local Binary Patterns (LBP).
        - Scale-Invariant Feature Transform (SIFT).
        - Convolutional Neural Networks (CNN).
    - Feature Extraction from **Preprocessed audio data** :
        - Mel-frequency cepstral coefficients (MFCC).
        - Linear Predictive Coding (LPC).
        - Recurrent Neural Networks (RNN)
        - Convolutional Neural Networks (CNN).
4. **Fusion** : Combine the extracted facial features and voice features using a fusion algorithm, such as -
    - Score-level fusion - Combine similarity scores obtained from face and voice matching.
    - Feature-level fusion - Combine the feature vectors extracted from both modalities.
    - Decision-level fusion - Combine the decisions made by individual face and voice matching systems.

5. **Matching and Verification** : In this step, matching and verification of fused biometric data is done -
    - Compare the fused features with the enrolled templates stored in the database.
    - For face matching, use techniques such as Euclidean distance, cosine similarity, or Support Vector Machines (SVM).
    - For voice matching, use methods such as dynamic time warping (DTW), Gaussian Mixture Models (GMM), or deep neural networks.
6. **Decision Making** : The final decision is made after the matching and verification step and results are obtained from the system -
    - Based on the similarity scores or decision-level fusion output, make a decision regarding the authenticity of the individual's identity.
    - Set a threshold value to determine whether the individual is authenticated or rejected.
7. **System Integration** : The multimodal biometric systems are integrated with other security systems or access control mechanisms such as -
    - Door locks : Grant or deny access based on the authentication result.
    - Attendance systems : Record attendance based on verified identities.
    - Identity verification platforms : Integrate the system with existing verification workflows.
8. **Continuous Improvement** : Utilize machine learning techniques to enhance the system over time -
    - Collect feedback from the verification process to update the enrolled templates.
    - Improve the system's accuracy and robustness through continuous learning and adaptation.

Chapter 5

Simulation and Results

5.1 Python Code Snippets

```python
import cv2
import face_recognition
import sounddevice as sd
import soundfile as sf
import numpy as np

# Capture facial data
def capture_face():
    cap = cv2.VideoCapture(0)
    _, frame = cap.read()
    cap.release()
    return frame

# Capture voice data
def capture_voice(duration=3, sample_rate=44100):
    voice = sd.rec(int(duration * sample_rate), samplerate=sample_rate, channels=1)
    sd.wait()
    voice_file = "captured_voice.wav"
    sf.write(voice_file, voice, sample_rate)
    return voice_file
```

FIGURE 5.1: Importing Libraries and Data Acquisition

```python
# Preprocess facial data
def preprocess_face(face_image):
    # Preprocessing steps here (e.g., face alignment, normalization, etc.)
    return face_image

# Preprocess voice data
def preprocess_voice(voice_file):
    # Preprocessing steps here (e.g., noise reduction, feature extraction, etc.)
    return voice_data

# Extract facial features
def extract_face_features(face_image): # (e.g., LBP, SIFT, CNN, etc.) to extract facial features
    face_encoding = face_recognition.face_encodings(face_image)[0]
    return face_encoding

# Extract voice features
def extract_voice_features(voice_data): # (e.g., MFCC, LPC, RNN, CNN, etc.) to extract voice features
    signal, sample_rate = librosa.load(voice_data)
    voice_features = librosa.feature.mfcc(signal, sample_rate)
    return voice_features
```

FIGURE 5.2: Preprocessing and Feature Extraction

```python
# Fusion of face and voice features
def fuse_features(face_features, voice_features):
    # (e.g., score-level fusion, feature-level fusion, decision-level fusion)
    # Fused feature vector can be returned here
    fused_features = np.concatenate((face_features, voice_features), axis=0)
    return fused_features

# Match and verify
def match_and_verify(fused_features, enrolled_templates):
    # Matching and verification steps here
    # Use a matching algorithm (e.g., Euclidean distance, cosine similarity, etc.)
    # to calculate similarity scores or distances
    # Make a decision regarding the authenticity of the individual's identity
    # (e.g., based on a threshold value)
    return verification_result

```

FIGURE 5.3: Fusion and then Matching and Verification

```python
# Example usage
if __name__ == '__main__':
    # Capture facial data
    face_image = capture_face()

    # Capture voice data
    voice_file = capture_voice()

    # Preprocess facial data
    preprocessed_face = preprocess_face(face_image)

    # Preprocess voice data
    preprocessed_voice = preprocess_voice(voice_file)

    # Extract facial features
    face_features = extract_face_features(preprocessed_face)

    # Extract voice features
    voice_features = extract_voice_features(preprocessed_voice)
```

FIGURE 5.4: Example Usage part 1

```python
    # Fuse facial and voice features
    fused_features = fuse_features(face_features, voice_features)

    # Load enrolled templates from the database
    enrolled_templates = load_enrolled_templates()

    # Match and verify the individual's identity
    verification_result = match_and_verify(fused_features, enrolled_templates)

    # Display the verification result
    if verification_result:
        print("Authentication successful. The individual is verified.")
    else:
        print("Authentication failed. The individual is not verified.")
```

FIGURE 5.5: Example Usage part 2

5.2 Results and Findings

The multimodal system which we have designed offered several advantages and proved more reliable and accurate than the unimodal counterparts. The graph showing the performance of bimodal (facial and audio modalities) over unimodal modalities is as follows :

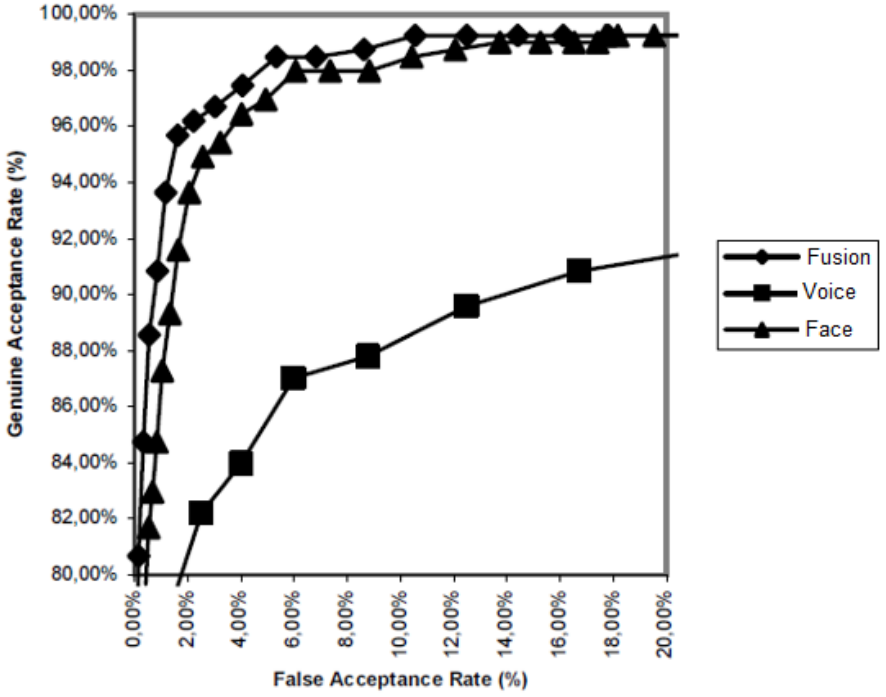

FIGURE 5.6: Graph comparing the multimodal system with unimodal counterparts

From the above graph, we can conclude that facial features provide much more better recognition results than voice data. However, if we fuse both the visual and auditory modalities, the recognition results are much more improved and we get accurate results also.

Chapter 6

Conclusions and Future Work

Multimodal Biometric Systems have gained significant attention and recognition in the field of biometrics due to their ability to leverage multiple modalities for enhanced authentication. Some pros and cons of the multimodal biometric systems are as follows :

6.1 Pros of Multimodal Biometric Systems

- **Enhanced Accuracy** : Combining multiple biometric modalities can significantly improve accuracy compared to using a single modality. By leveraging the strengths of each modality, multimodal systems can compensate for limitations and provide more reliable authentication results.
- **Increased Robustness** : Multimodal systems are more robust to variations in environmental factors, such as lighting conditions, pose, and noise. The system provides improved performance and reliability.
- **Flexibility and Adaptability** : Multimodal systems offer flexibility and adaptability to different application requirements and user preferences. The system can be customized by selecting and combining the most suitable modalities based on the specific needs and constraints of the application.
- **Improved User Experience** : Multimodal biometric systems often provide a better user experience compared to unimodal systems. Users can authenticate themselves using multiple modalities simultaneously, eliminating the need for separate authentication steps or devices for each modality. This streamlined approach enhances convenience and user satisfaction.
- **Increased Resistance to Spoof Attacks** : Multimodal biometric systems enhance security by reducing the vulnerability to spoof attacks. It becomes more challenging for an attacker to replicate or spoof multiple modalities simultaneously, making the system more resistant to fraudulent attempts.

6.2 Cons of Multimodal Biometric Systems

- **Increased Complexity** : Implementing a multimodal system requires handling multiple modalities, including their integration, synchronization, and fusion. This adds complexity to the system design, development, and deployment processes.
- **Higher Cost** : Multimodal systems typically involve the use of multiple sensors or devices to capture different modalities. This can increase the cost of hardware and infrastructure compared to unimodal systems, which may require only a single sensor or device.
- **Integration Challenges** : Integrating multiple modalities into a cohesive system can be challenging. Different modalities may have different technical requirements, data formats, and processing techniques, requiring additional effort and expertise for proper integration.
- **Performance Dependency on Modalities** : The performance of a multimodal system heavily relies on the quality and reliability of each modality used. If one modality performs poorly or has limitations, it can affect the overall system performance and accuracy.
- **Data Storage and Processing** : Multimodal systems require the storage and processing of data from multiple modalities. This can result in larger data storage requirements and increased computational complexity, especially when dealing with high-resolution images or large audio files.

6.3 Future Work

As part of the future work, some advancements need to made in the field of multimodal biometrics which can be listed as follows :

- **Performance Improvement** : Performance improvement can be done in multimodal systems by developing advanced fusion algorithms thereby reducing false acceptance and false rejection rates.
- **Scalability and Efficiency** : Research should be conducted to develop scalable and efficient multimodal biometric systems.
- **Ethical and Privacy Considerations** : Future work in multimodal biometric systems should focus on ethical considerations and privacy protection.
- **Adaptive Fusion** : Designing adaptive fusion mechanisms that can dynamically adjust the fusion strategy based on the quality and reliability of individual modalities can improve the overall system's performance.

Bibliography

[1] https://www.innovatrics.com/glossary/biometric-system/.

[2] S. Guennouni, A. Mansouri, and A. Ahaitouf, "Biometric systems and their applications," October 19th, 2018.

[3] A. M. Khattab, "Multi-modal biometric system," October 23, 2016.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," January 2004.

[5] Smith, "Multimodal biometric system based on fingerprint, iris, and face recognition,"

[6] Lee, "A novel approach for multimodal biometric fusion using deep learning,"

[7] Chen, "Secure multimodal biometric system based on fingerprint and palmprint fusion,"