Multimodal Biometric Systems

Under the Guidance of :

Dr. Joyeeta Singha

Prepared By :

19ucc023 – Mohit Akhouri

19uec023 – Hitesh Goyal

19uec113 – Agraj Garg

19ucc043 – Aditya Pandey

What are Biometric Systems ?

- Biometric Systems use personal characteristics of a person to authenticate or identify a person.

- Some of the Biometric characteristics that can be used are as follows :

  - Face
  - Fingerprint
  - Hand Geometry
  - Palm Print
  - Iris
  - Voice
  - Signature
  - Keystroke dynamics

Aim and Objective

- The Aim of the project is to design a multimodal biometric system which could be used for verification and recognition purposes.
- Our objective is to design such a multimodal biometric system which provides better results in terms of reliability, security and accuracy compared to the unimodal biometric systems.
- Unimodal Biometric systems perform person recognition based on a single source of biometric information.
- Unimodal systems are often affected by some problems which are discussed in the upcoming slides.

Why Multimodal Biometrics ?

- **Noisy Sensor Data** – Noise can be present in the biometric data which is acquired due to defective or improperly maintained sensors.
- **Non-Universality** – A Biometric trait is said to be universal if every individual in the target population is able to present biometric trait for recognition. NIST reported 2% people cannot enroll using finger print.

- **Lack of Individuality** – Features extracted from biometric characteristics of different individuals can be quite similar. A small proportion of population can have nearly identical facial appearance due to genetic factors.

Why Multimodal Biometrics contd….

- **Lack of invariant representation** – The biometric data acquired from user during verification may not be identical to data used for generating user's template during enrollment.

- **Spoofing** – Unimodal Biometrics is vulnerable to spoofing where the biometric data can be imitated or forged.

Applications

- There are many applications of biometric systems which are :
  - **Access Control** – Biometric systems can be used for access control in physical spaces such as offices, govt. buildings, airports and residential complexes.
  - **Time and Attendance** – Biometric systems can be used for time and attendance management in workplaces, schools and other organizations.
  - **Financial Services** – Biometric systems are used in the financial sector for secure authentication and fraud prevention.
  - **Forensics** – Biometric data such as fingerprint, DNA and facial features can be used in forensic investigations.
  - **Border Security** – Biometric systems are deployed at border checkpoints to enhance security and facilitate immigration process.

Literature Survey

- **"Multimodal Biometric System Based on Fingerprint, Iris and Face Recognition" By Smith et al.**
  - Proposes a multimodal biometric system that combines fingerprint, iris and face recognition modalities.
  - The paper focused on developing efficient feature extraction techniques for each modality and explore fusion strategies to integrate information efficiently.
  - The authors conducted experiments using a large dataset and achieved superior recognition accuracy compared to unimodal biometric systems.
  - The multimodal biometric system designed has enhanced security and robustness against spoofing attacks.

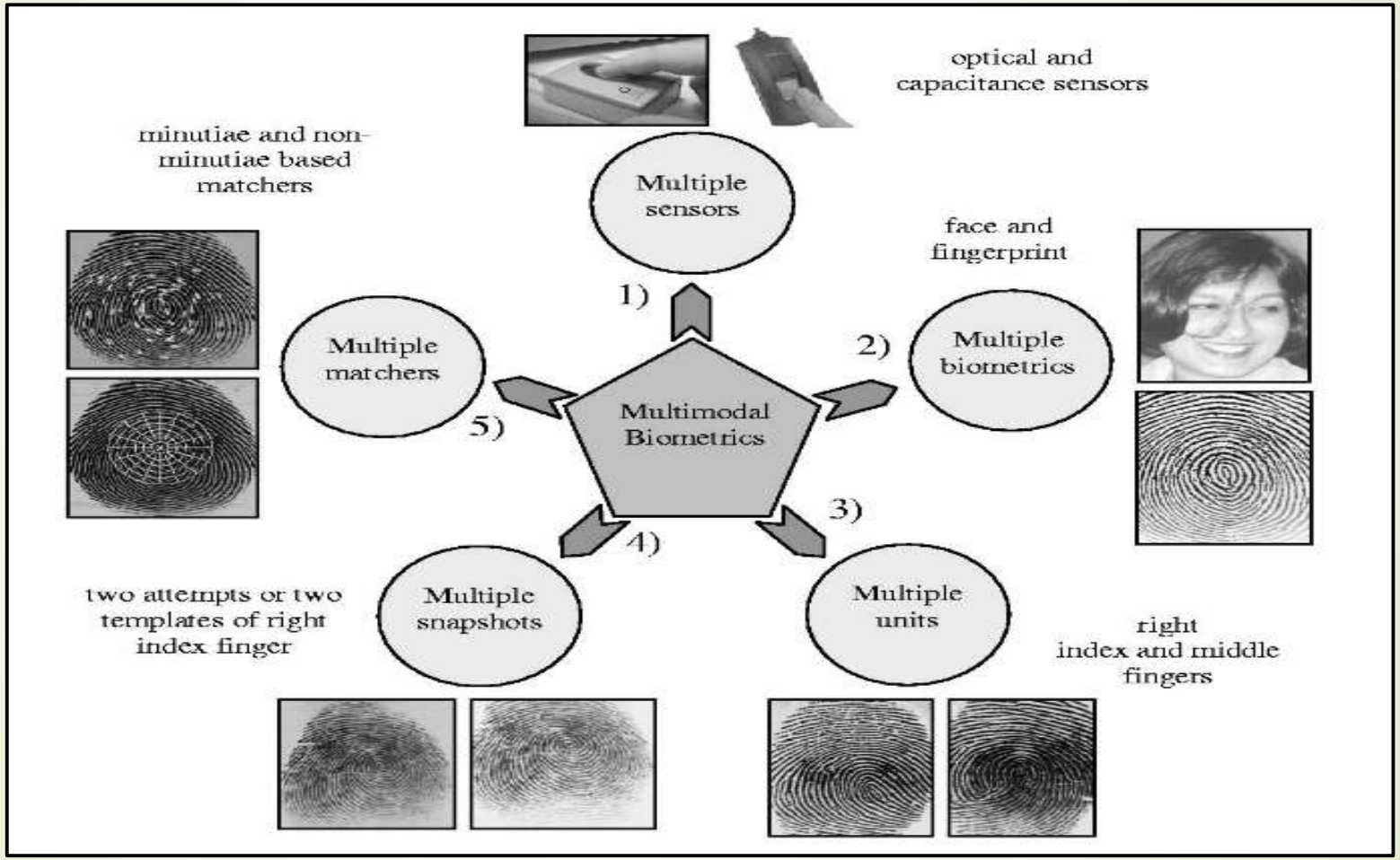
Literature Survey contd....

- "**A Novel Approach for Multimodal Biometric Fusion using Deep Learning" By Lee et al.**
  - This paper presents a novel approach for multimodal biometric fusion using deep learning techniques.
  - It presents a deep neural network architecture which combines features extracted from fingerprint, iris and face modalities.
  - Deep Learning improved the accuracy and reliability of multimodal biometric systems.
  - These systems can be used where accurate identification is crucial.

Literature Survey contd....

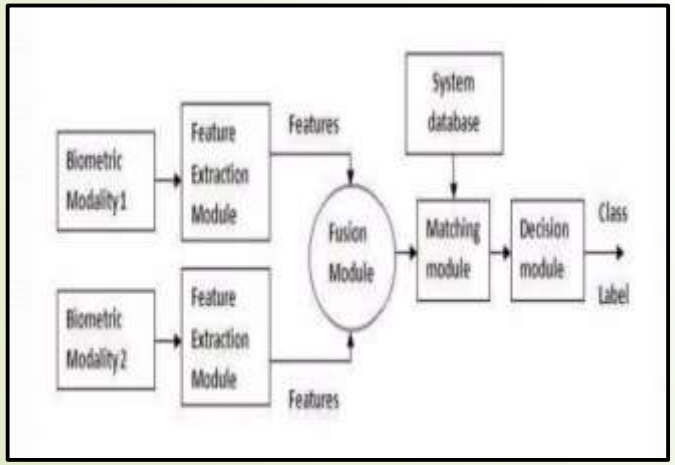
- **"Secure Multimodal Biometric System based on Fingerprint and Palmprint Fusion" By Chen et al.**
  - This research paper focused on development of secure multimodal biometric system using fingerprint and palmprint fusion.
  - The proposed system combines features extracted from fingerprint and palmprint modalities using a fusion algorithm based on score-level and feature-level fusion techniques.
  - The proposed system demonstrates enhanced accuracy and resilience against spoofing attacks compared to unimodal systems.
  - These systems can be used in access control and identity verification.

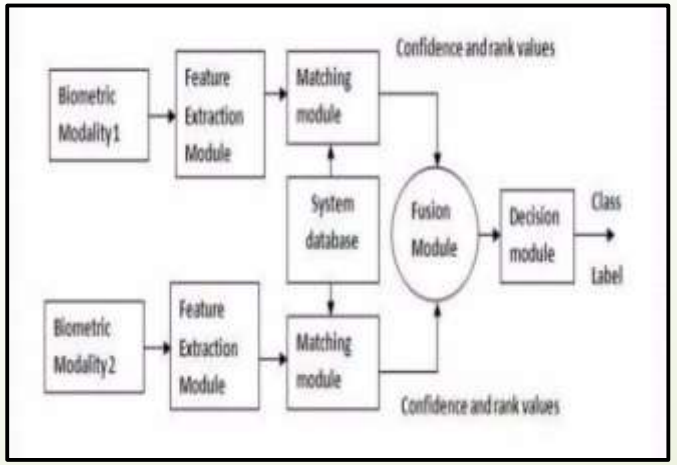
Scenarios in Multimodal Biometric Systems

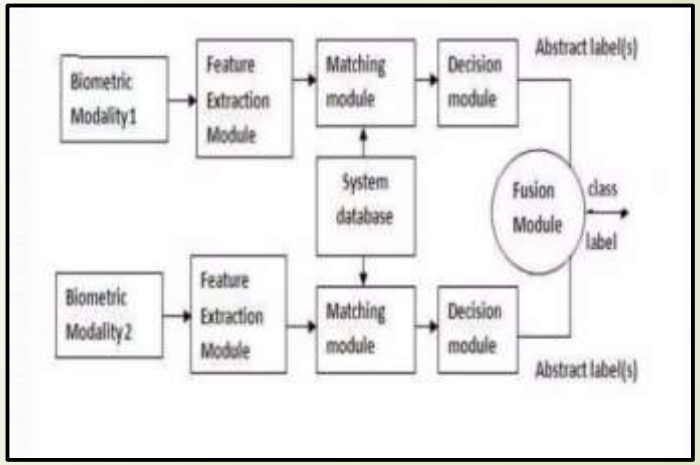


Fusion in Multimodal Biometric Systems

- **Feature Level Fusion** – Combining feature vectors. When features of different modalities are compatible with each other, then more accuracy.
- **Matching Score Level Fusion** – Individual matching score of different feature vectors is found and fused to make classification.
- **Decision Level Fusion** – Each biometric modality makes it own recognition decision based on its feature vector.





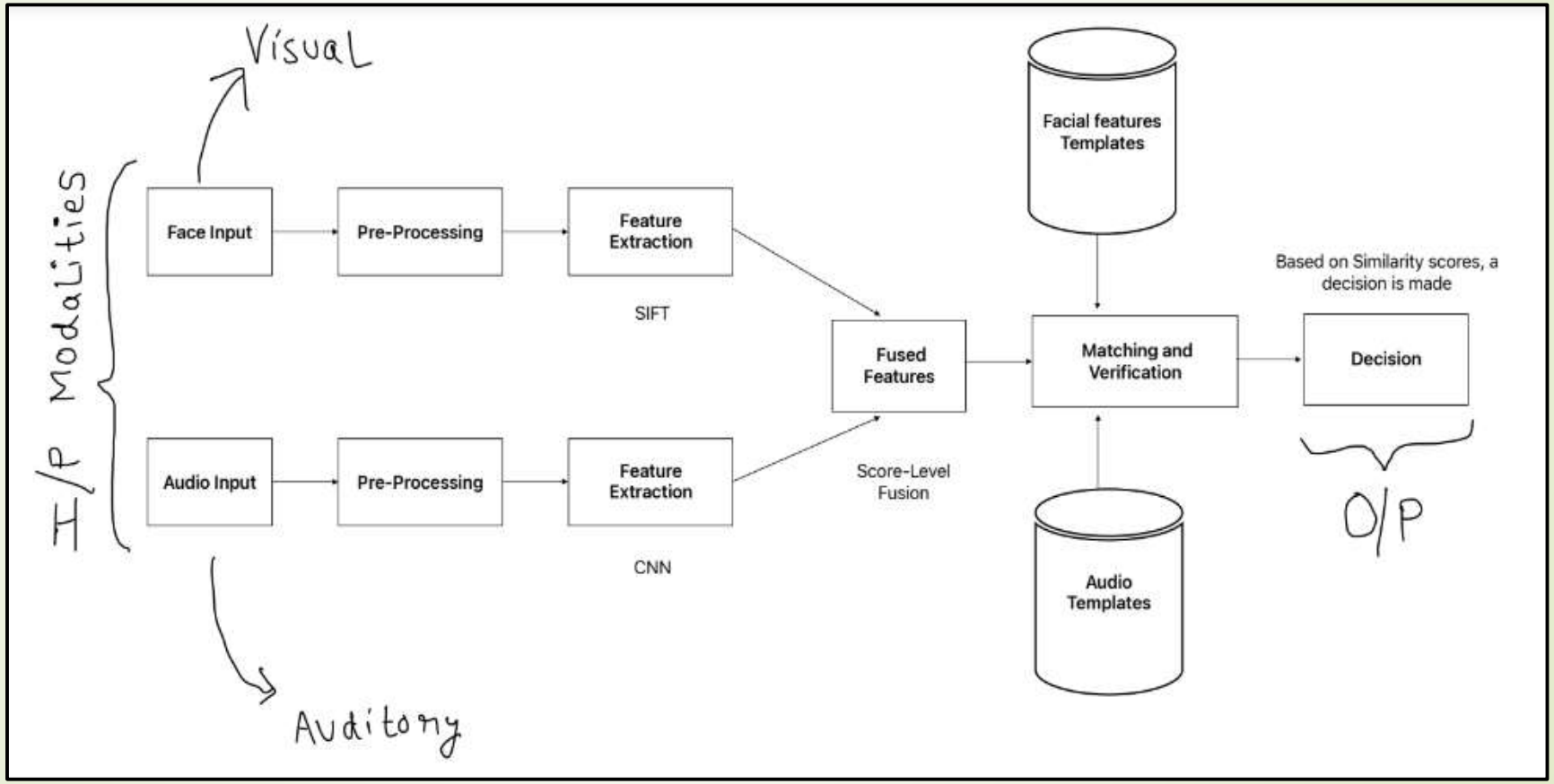


Proposed System

- We can make a multimodal biometric system using these two modalities :
  - Facial Features (Visual Modality)
  - Audio (Auditory Modality)

- The system will capture facial and voice biometric data from individuals. This can be done using a camera or webcam to capture facial images and a microphone to record voice samples.
- The captured data will be pre-processed to enhance quality.
- Feature extraction will be done from the pre-processed data.
- The extracted features will be combined using a fusion algorithm.
- Finally, the fused features will be compared with the enrolled templates in database and based on similarity scores, a decision will be made.

Workflow of the system designed



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
```

```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
```

Code Snippets contd....

```
# 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
```

Code Snippets contd....

```
# 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)
```

```
    # 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.")
```

Results and Findings

- The Multimodal biometric system designed offered several advantages compared to the unimodal counterparts which are :
  - **Improved Accuracy** – By utilizing both facial and voice modalities, system can benefit from the complementary information provided by each modality thereby reducing false acceptance and false rejection rates.
  - **Enhanced Robustness** – Face Recognition may be susceptible to illumination variation while voice recognition may be affected by background noise. By integrating both modalities, more reliable authentication is there.
  - **Improved User Experience** – Users can authenticate themselves using face and voice simultaneously.
  - **Increased Resistance to Spoof Attacks** – Attempting to spoof both voice and face may be difficult for attackers.

Conclusion and Future Work

- In conclusion, multimodal biometric systems enhances accuracy and reliability compared to their unimodal counterparts.
- However, there are still some challenges which need to be addressed which are :
  - **Performance Improvement** – We can develop more advanced fusion algorithms that reduce false acceptance and false rejection rates and are more accurate.
  - **Usability and User Experience** – Efforts can be made to address user concerns and improve the usability of multimodal biometric systems.
  - **Scalability and Efficiency** – We can conduct research to develop scalable and efficient multimodal biometric systems to handle large user populations.
  - **Ethical and Privacy Considerations** – Future work in multimodal biometrics should emphasize on ethical considerations and privacy protection.

References

- S. Ribaric, Kristina Kis, “A biometric verification system based on the fusion of palmprint and facial features”, October 2005
- A. Khattab, “Multi-modal Biometric System”, October 23, 2016
- Priyanka S. Patil, A. Abhyankar, “Multimodal Biometric Identification System Based on Iris & Fingerprint”, 2013
- Rajendra Prasad Nayak, “Seminar on Multimodal Biometric Systems”, NIT Rourkela
- Blaise Craig, “Multimodal Biometric Security”, 2017
- https://www.innovatrics.com/glossary/biometric-system/

THANK YOU