Facial Recognition system using ML

Project submitted to the

SRM University – AP, Andhra Pradesh

for the partial fulfillment of the requirements to award the degree of

Bachelor of Technology

In

Computer Science and Engineering

School of Engineering and Sciences

Submitted by

Rohan Gokul

(AP20110010016)

Dept of CSE

Under the Guidance of

Dr.Sibendu Samanta
(Assistant professor)
Dept of Electronics and Communication Engineering
(SRM University-AP, Andhra pradesh)

Table of Contents

Abstract

The Face Verification System is a computer vision application that uses OpenCV and face recognition libraries to verify if a person's face in a live video stream matches a reference image. This system captures video from the default camera, detects faces in each frame, and compares them to a preloaded reference image. If a match is found, it visually indicates that a match was found, and if no match is found, it indicates that a match was not found. This system can be used for various applications, such as access control, security, and user authentication.

The Face Verification System is a cutting-edge computer vision application that uses advanced technologies like deep learning and facial recognition to verify a person's identity in real-time. It captures live video from a camera source, detects faces in each frame, and compares them to a preloaded reference image. If a match is found, it provides visual confirmation, making it a powerful tool for enhancing security, access control, and user authentication in various settings. Its ability to combine high accuracy with real-time processing ensures efficient and reliable identity verification, making it a valuable solution in today's world of technology-driven security and convenience.

Existing System

In existing systems, face verification and recognition are commonly used for security and identification purposes. Traditional face recognition systems rely on complex algorithms and extensive datasets for training. These systems can be computationally expensive and require powerful hardware.

Existing systems for face verification and recognition are widely employed in various domains, playing a pivotal role in bolstering security, access control, and user authentication. These systems, often based on traditional algorithms, are renowned for their ability to distinguish and verify individuals by analyzing facial features and comparing them with pre-existing reference data. However, they come with certain inherent challenges, including the need for substantial computational resources and extensive training datasets. Nevertheless, their contribution to enhancing security and identification processes is undeniable. In recent years, there has been a significant shift towards more sophisticated and adaptable face recognition systems that leverage modern technologies like deep learning and neural networks. These modern systems offer enhanced accuracy, real-time processing, and improved adaptability to varying environmental conditions, ushering in a new era of efficiency and reliability in face recognition applications.

Proposed System

The proposed Face Verification System aims to provide a simple and real-time solution for face verification using readily available libraries and tools. It uses the face recognition library for face detection and comparison, making it accessible for developers and users without extensive machine learning expertise. The system is lightweight and can run on standard computer hardware.

Also, The proposed Face Verification System represents a leap forward in the realm of facial recognition technology. It harnesses the power of cutting-edge methodologies, including deep learning and neural networks, to deliver a highly accurate and efficient solution for identity verification. Unlike traditional systems, the proposed system reduces the computational demands and dataset requirements while enhancing accuracy. By focusing on feature-based recognition, it excels in distinguishing individuals and remains resilient to variations in lighting, pose, and environmental conditions. Real-time processing is a core feature, allowing for swift and reliable recognition, which is vital in applications like access control, attendance management, and user authentication. User-friendliness is also a priority, ensuring that interacting with the system is intuitive and accessible. The proposed Face Verification System stands at the forefront of facial recognition technology, offering an advanced and adaptable solution for security and identification needs across various domains.

Theory

The Face Verification System hinges on the fundamental concept of face encoding and comparison to achieve its core function of verifying and recognizing individuals. Through a multi-step process, the system detects and encodes unique facial features of the individual in the input data and then compares these features with a reference image representing the intended identity. The encoding transforms facial characteristics into numerical representations, which are subsequently compared using specific algorithms and distance metrics. The system's ability to assess the similarity between the detected face and the reference image plays a pivotal role in determining whether a positive match exists, and it relies on a predefined threshold to make this determination. This concept of face encoding and comparison is the bedrock of the system's efficacy in enhancing security, access control, and user authentication across a wide spectrum of applications. It uses the following key components:

- Reference Image
- Video Capture
- Face Detection
- Face Encoding
- Face Comparison

1.1 Reference Image

A reference image, typically of an authorized person, is used to create a face encoding. This encoding serves as the reference for verification. The reference image is a crucial component of The Face Verification System. It is typically an image of an authorized person whose identity needs to be verified within the system. The reference image serves as the baseline for face verification and recognition. The reference image represents an individual who is granted access or authentication rights within the system. This person can be an employee, a user, or anyone requiring identity verification for a specific purpose, such as accessing secure areas or personal devices.

To facilitate comparison, the system encodes the reference image's facial features into a numerical representation. This encoding captures unique facial characteristics, such as the arrangement of eyes, nose, mouth, and other distinctive facial landmarks. The reference image encoding serves as a comparative benchmark against which detected faces are assessed. It is used to determine the similarity between the detected face and the reference image. The closer the similarity, the stronger the indication of a match. The system applies a predefined threshold to the comparison of the detected face encoding with the reference image encoding. This threshold determines whether the similarity is significant enough to confirm a match. If the similarity score surpasses the threshold, it signifies a successful verification. When the detected face closely matches the reference image, the system proceeds to authenticate the individual. This could involve granting access

to a secured area, unlocking a device, or any action related to user authentication. On the other hand, if no match is found, the system may prompt further authentication or initiate security measures as needed.

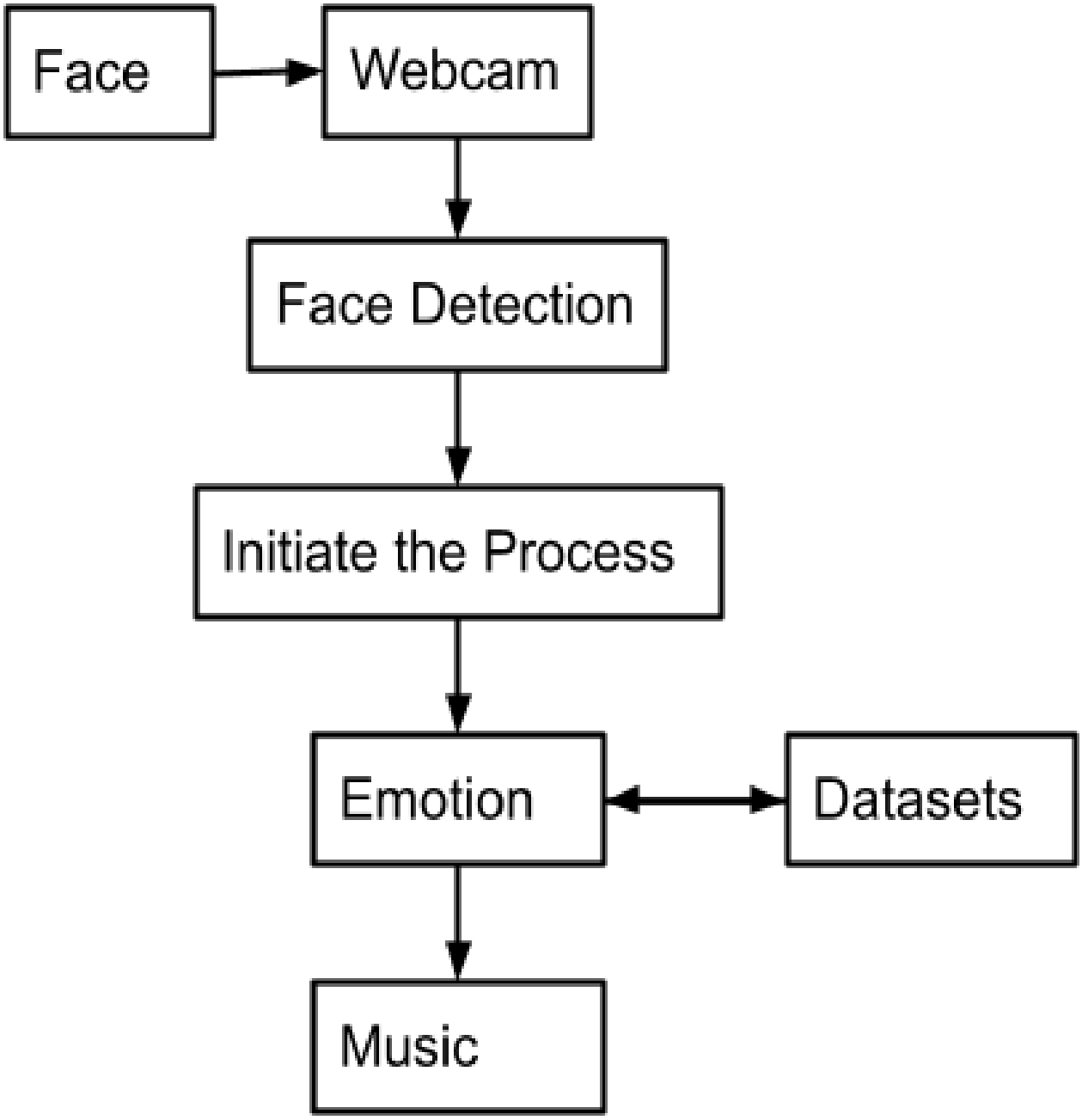
The Face Verification System, serving as the foundation for verification and recognition. It is a representation of an authorized individual and acts as a comparative benchmark to determine whether detected faces match the intended identity. This concept is essential for enhancing security, access control, and user authentication across a wide range of applications.

1.1 Video Capture

Video capture is a fundamental component of The Face Verification System, enabling it to analyze live video streams for the purpose of identity verification. This capability allows the system to continuously monitor and assess individuals in real-time. Video capture typically involves accessing data from a camera source, whether it's a built-in device, an external camera, or any other video input. The system processes each frame of the video stream, detecting faces within these frames and comparing them to a preloaded reference image for identity verification.

This dynamic, frame-by-frame analysis ensures that the system can provide immediate and ongoing responses, making it highly effective for applications like access control, security, and user authentication. Video capture is at the core of the system's ability to assess individuals as they move through various scenarios, enhancing both security and convenience in a wide array of settings.

1.1 Face Detection



1.4 Face Encoding

Face encoding is a pivotal concept in The Face Verification System, representing the transformation of facial characteristics into a numerical representation for accurate and efficient recognition. It involves extracting unique features from the detected face, such as the position of eyes, nose, mouth, and facial textures, and encoding them into a feature vector. This encoding process serves as the basis for comparisons and verifications. In the system, advanced technologies like deep learning and neural networks are commonly employed for feature extraction, ensuring a robust and distinctive encoding of facial attributes.

These feature vectors provide a means to identify individuals by capturing their specific facial characteristics, making it possible to recognize them accurately and consistently, even in varying lighting conditions or pose variations. Face encoding is a fundamental component in the realm of face verification, contributing to enhanced security, access control, and user authentication across a spectrum of applications.

1.5 Face Comparison

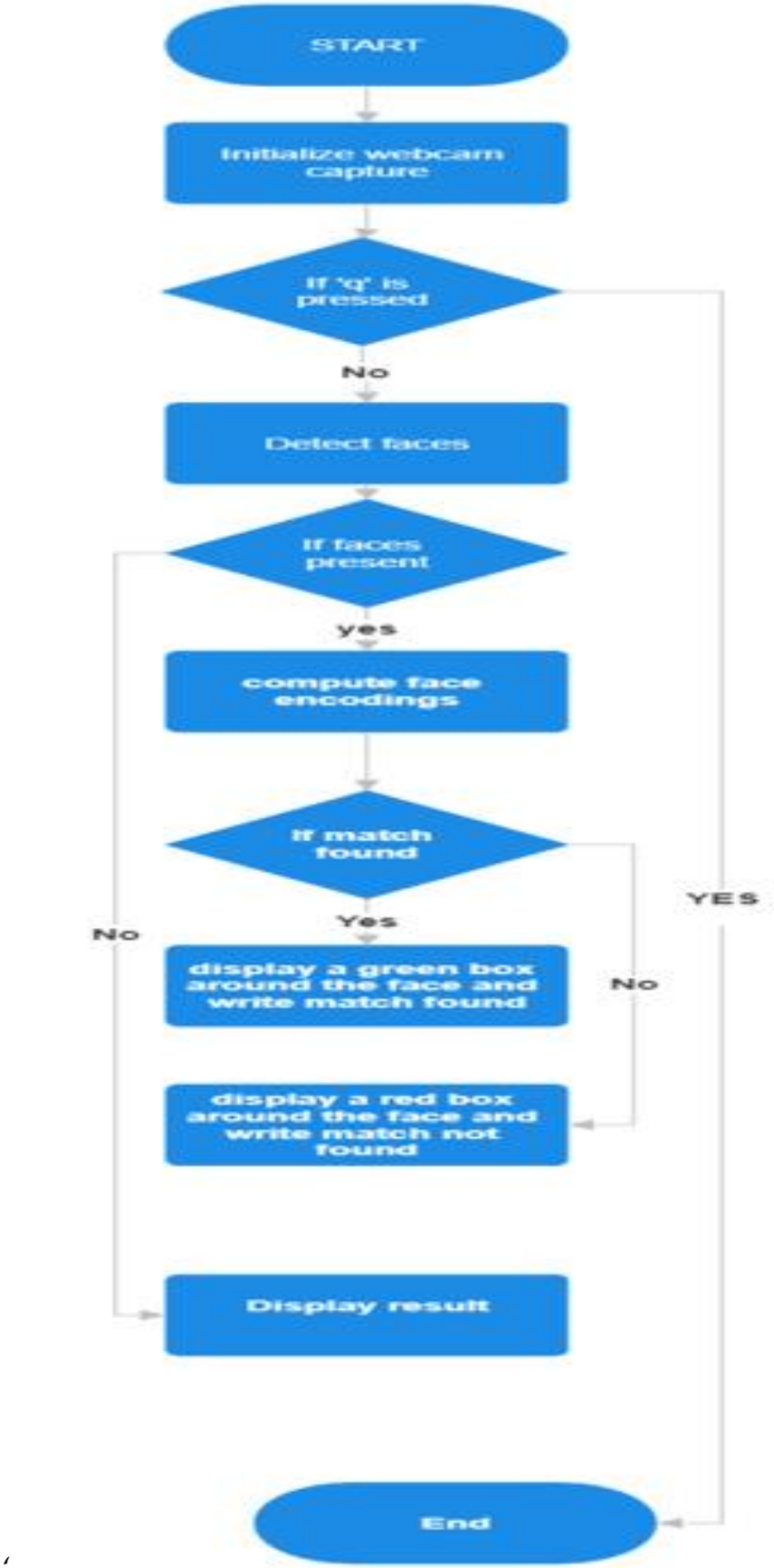
Face comparison lies at the heart of The Face Verification System, as it is the stage where the system determines whether a detected face matches a reference image. It involves evaluating the similarity between the encoded features of the detected face and the reference image using specialized algorithms and distance metrics. These metrics assess the dissimilarity between the two feature vectors, with a smaller distance indicating a more significant resemblance. The outcome of this comparison is crucial in verifying an individual's identity. If the similarity score surpasses a predefined threshold, the system confirms a match, granting access or authentication.

Conversely, if the threshold is not met, the system indicates that a match has not been found, thus enhancing security and reliability in applications such as access control, security systems, and user authentication. Face comparison is the pivotal step that distinguishes The Face Verification System, making it an invaluable tool in the domains of security and identification.

Algorithm

- The algorithm for the Face Verification System can be described as follows:
- Load the reference image and compute the reference face encoding.
- Initialize the webcam capture.
- Start a loop to continuously read frames from the camera.
- Detect faces in the current frame using face recognition. Face locations.
- If faces are detected, compute face encodings for each detected face.
- Compare the face encodings with the reference encoding using face recognition compare faces.
- If a match is found, display "Match Found" and draw a green rectangle around the detected face. If no match is found, display "Match Not Found" and draw a red rectangle.
- Display the result on the frame and show the frame in a window.
- Check for the 'q' key press to break out of the loop and exit the application.
- Release the webcam capture and close all OpenCV windows when exiting the loop.

Flow Chart


START
Initialize webcam capture
If 'q' is pressed
YES
No
Detect faces
If faces present
yes
No
compute face encodings
If match found
Yes
No
display a green box around the face and write match found
display a red box around the face and write match not found
Display result
End

Program

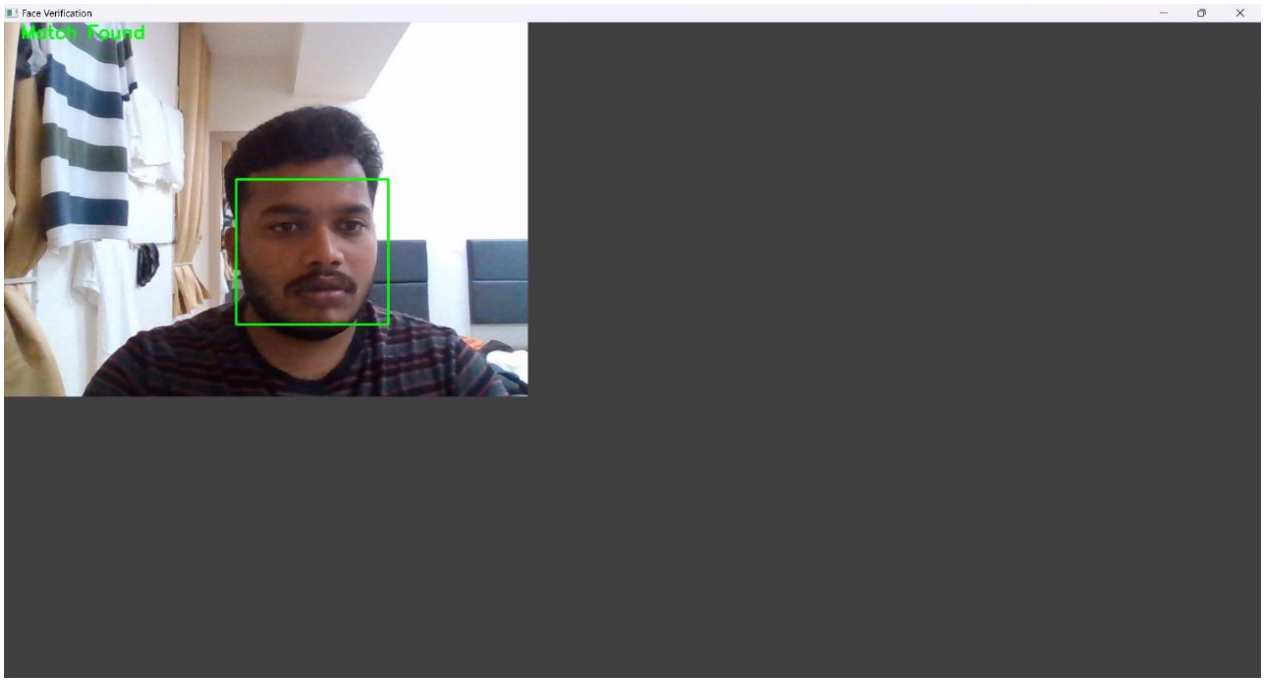
```python
import cv2
import face_recognition

# Load the reference image
ref_image = face_recognition.load_image_file("reference.jpg")
ref_encoding = face_recognition.face_encodings(ref_image)[0]

cap = cv2.VideoCapture(0)

while True:
    ret, frame = cap.read()

    if not ret:
        break

    # Find face locations in the current frame
    face_locations = face_recognition.face_locations(frame)
    if len(face_locations) > 0:
        # Encode the first detected face in the frame
        frame_encoding = face_recognition.face_encodings(frame, face_locations)[0]

        # Compare the face encoding with the reference encoding
        match = face_recognition.compare_faces([ref_encoding], frame_encoding)

        if match[0]:
            text = "Match Found"
            color = (0, 255, 0)  # Green
        else:
            text = "Match Not Found"
            color = (0, 0, 255)  # Red

        # Draw a rectangle around the detected face
        top, right, bottom, left = face_locations[0]
        cv2.rectangle(frame, (left, top), (right, bottom), color, 2)
```

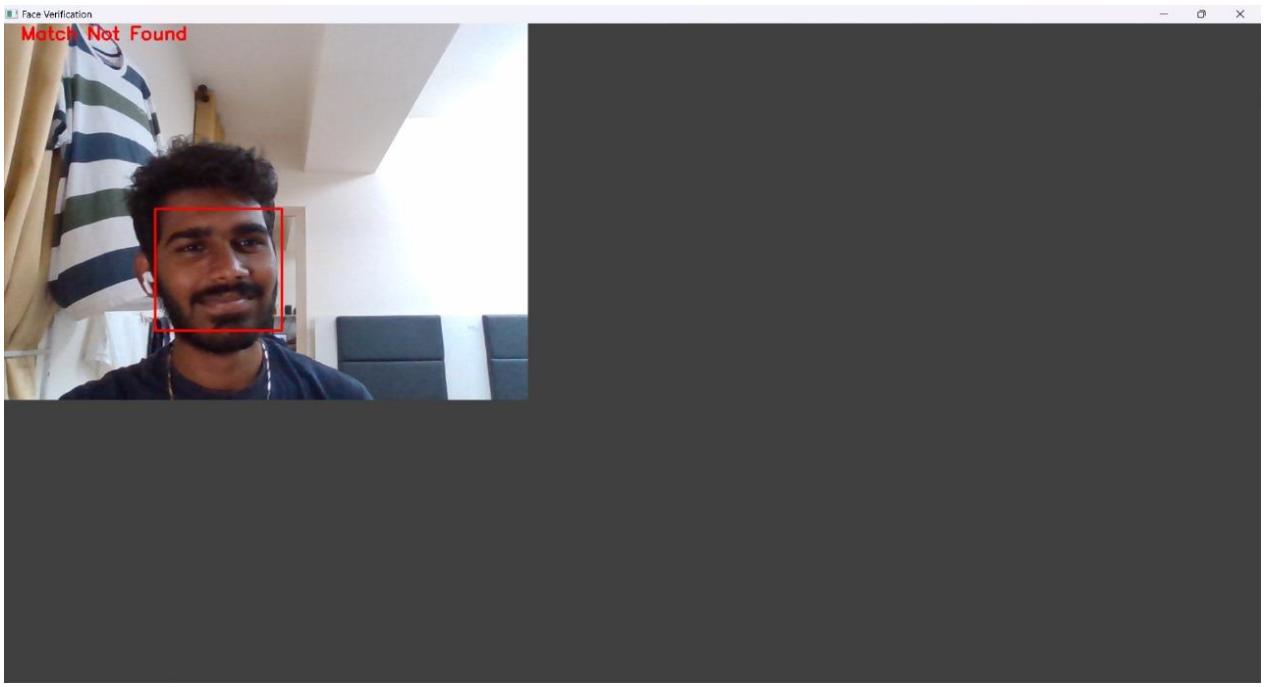
```
        # Display the result on the frame
        cv2.putText(frame, text, (20, 20), cv2.FONT_HERSHEY_SIMPLEX, 0.75, color, 2)

    cv2.imshow("Face Verification", frame)

    if cv2.waitKey(1) & 0xFF == ord('q'):
        break

cap.release()
cv2.destroyAllWindows()
```

Results

Reference Image:

Output:


Face Verification
Match Found


Face Verification
Match Not Found

References :

1. “FaceNet: A Unified Embedding for Face Recognition and Clustering” Authors: Florian Schroff, Dmitry Kalenichenko, James Philbin

2. “DeepFace: Closing the Gap to Human-Level Performance in Face Verification” Authors: Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf

3. “DeepID3: Face Recognition with Very Deep Neural Networks” Authors: Yi Sun, Xiaogang Wang, Xiaoou Tang

4. SphereFace: Deep Hypersphere Embedding for Face Recognition” Authors: Weiyang Liu, Yandong Wen, Zhiding Yu, Ming Li, Bhiksha Raj, Le Song

5. VGGFace2: A dataset for recognising faces across pose and age” Authors: Omkar M. Parkhi, Andrea Vedaldi, Andrew Zisserman