

**FACE VERIFICATION SYSTEM WITH
LIVENESS DETECTION**

PROJECT WORK2

Submitted by

SARANKUMAR J 212221230087

in partial fulfillment for the award

of the degree of

BACHELOR OF TECHNOLOGY

in

ARTIFICIAL INTELLIGENCE AND DATA SCIENCE



SAVEETHA ENGINEERING COLLEGE, THANDALAM

**An Autonomous Institution Affiliated to
ANNA UNIVERSITY - CHENNAI 600 025**

APRIL 2024



SAVEETHA
ENGINEERING COLLEGE

AUTONOMOUS

Affiliated to Anna University | Approved by AICTE



BONAFIDE CERTIFICATE

2023-2024

Certified that this project report, “Face Verification System With Liveness Detection” is the bonafide work of SARANKUMAR J (212221230087) of IVth Year B.Tech. Department of Artificial Intelligence and Data Science in the VIIIth Semester who carried out the Project Work-II (19AI703) under my supervision and has not been submitted to any other coursework or University for the award of any degree by us.

SUPERVISOR

<Name, Designation,Department>

HEAD OF THE DEPARTMENT

Submitted for the End Semester Examination Project Work II VIVA-VOCE
held on _____

Internal Examiner

External Examiner

ABSTRACT

In recent years, significant advancements have been made in the field of face recognition and liveness analysis, aimed at enhancing device security and attendance verification systems. Many of these approaches have incorporated complex 3D analysis of the human face to predict the authenticity of the person in front of the camera. However, our method strives to address these challenges without the need for advanced 3D imaging techniques or specialized hardware. As a result, our solution offers a cost-effective and easily deployable alternative, consisting of two key components: face verification and liveness detection.

In the first part of our system, we have harnessed the power of a model based on Google's FaceNet Model. This model learns to map face images to a compact Euclidean space, where the distances between points directly correspond to the similarity of the images. Once this space has been created, face verification becomes straightforward, utilizing standard techniques with embeddings as feature vectors. This robust approach ensures the accurate verification of individuals by comparing their facial features to a reference database.

The second part of our system involves the implementation of a cascaded multi-task framework, specifically designed to extract certain features from facial images. These extracted features are subsequently used to assess the liveness of the person's face. To achieve this, individuals are prompted to perform a set of random tasks, including head and facial movements, among others. By tracking the relative displacements of these features, our system can effectively determine the authenticity of the presented face. This dynamic liveness check ensures that the system remains resilient to presentation attacks and impersonation.

ACKNOWLEDGEMENT

I wish to express my gratitude to our Founder President Dr.N.M.Veeraiyan, Director Dr. S. Rajesh, Saveetha Engineering College, for their guidance and blessings.

I am very grateful to our Principal Dr. V. Vijaya Chamundeeswari, M.Tech., Ph.D., Mr. C. Obed Otto, M.E., Dean, ICT for providing me with an environment to complete my project successfully.

I am indebted to our Head of the Department, Dr. Karthi Govindharaju, M.Tech., Ph.D., for his support during the entire course of this project work.

I am indebted to our supervisor Dr. Karthi Govindharaju, M.Tech., Ph.D., for assisting me in the completion of my project with his exemplary Guidance and for his support during the entire course of this project.

My heartfelt thanks to the Project Coordinator, Dr. N. S. Gowri Ganesh, M.E., Ph.D., Associate Professor, Department of Artificial Intelligence and Data Science, Saveetha Engineering College, for unstinted support throughout this project.

I also thank all the staff members of our department for their help in making this project successful.

LIST OF ABBREVIATIONS

CV - OpenCV (Open Source Computer Vision Library)

FVS - Face Verification System

FVSLD - Face Verification System with Liveness Detection

LD - Liveness Detection

TF - TensorFlow (Machine Learning Framework)

Keras - A high-level neural networks API

Python - A high-level programming language

OCR - Optical Character Recognition

AI - Artificial Intelligence

CNN - Convolutional Neural Network

DL - Deep Learning

ML - Machine Learning

TABLE OF CONTENTS

CHAPTE R NO	TITLE	PAGE NO
1	Introduction	1
2	Problem Definition	2
2.1	Existing System	3
2.1.1	Liveness Detection Based On 3D Face Shape Analysis	4
2.1.2	Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos	5
2.1.3	Moving Face Spoofing Detection via 3D Projective Invariants	6
2.1.4	Human action recognition using attention based LSTM network with dilated CNN features	7
2.1.5	Literature Survey Summary	8
2.2	Scope of the Project	10
2.3	Proposed System	11
3	System Analysis and Design	12
3.1	Methodology	13
3.2	Hardware Requirements	13
3.3	Software Requirements	14
3.4	System Architecture	14
3.5	Module Description	14
4	Implementation	16
5	Result	22
6	Conclusion	24
7	References	25

1.INTRODUCTION

In our increasingly digital world, the demand for secure and efficient identity verification systems is paramount. Face verification, a subset of biometric authentication, has gained prominence due to its convenience and accuracy. However, this convenience has also made it a target for potential threats, specifically in the form of spoofing attacks. These attacks attempt to deceive the system by presenting a static image or a recorded video of a genuine user's face, undermining the system's ability to differentiate between a living, present user and an impersonator.

The importance of ensuring the liveness of the detected face cannot be overstated. It is not merely a matter of convenience but a critical aspect of security and trust. Face verification systems must accurately discern whether the user presenting themselves is indeed a live individual and not a manipulated image or video. This distinction is crucial in various domains, including access control, mobile device security, online transactions, and identity verification for various services.

This paper introduces a comprehensive solution to the challenge of liveness detection within the context of a face verification system. The proposed system addresses the vulnerability of traditional face verification systems to spoofing attacks by incorporating liveness detection as an integral component. It not only verifies the identity of the user based on their facial features but also ensures the user's real-time presence.

The primary objective of this paper is to provide an in-depth exploration of the methodologies and technologies used in our Face Verification System with Liveness Detection. By the end of this document, readers will have a clear understanding of the importance of liveness detection, the various techniques employed to achieve it, and the potential applications and benefits of such a system.

2. PROBLEM DEFINITION

Face verification systems have become increasingly crucial in various domains, including security, access control, and identity verification. These systems use biometric data, particularly facial features, to determine whether an individual is who they claim to be. However, these systems can be vulnerable to spoofing attacks using photos or videos. To enhance the security and reliability of face verification, it is essential to incorporate liveness detection into the system.

Develop a face verification algorithm that can accurately match a presented face against a reference database of authorized individuals. The system should be able to determine whether the face belongs to an authorized user. Implement a liveness detection mechanism that can distinguish between a live person's face and a static image or video. The system must prevent spoofing attempts by detecting and rejecting non-living representations.

The system should work effectively under various conditions, such as varying lighting, angles, and facial expressions. It should be capable of handling different scenarios, including outdoor and indoor settings. For applications like access control or security monitoring, the system should perform verification and liveness detection in real-time, without significant delays.

The system should be user-friendly, ensuring a smooth and convenient experience for the individuals undergoing verification. This includes minimizing false positives and false negatives. Safeguard the system against potential attacks, such as adversarial attacks, and ensure that the biometric data of users is protected from unauthorized access.

Develop a comprehensive testing framework to assess the system's accuracy, performance, and security. This may include testing with diverse populations and demographic groups.

The Face Verification System with Liveness Detection aims to provide a reliable and secure method for verifying an individual's identity, preventing unauthorized access, and ensuring that the process is not susceptible to spoofing attacks. This project seeks to combine cutting-edge facial recognition and liveness detection technologies to address these challenges and provide a practical and robust solution.

2.1 EXISTING SYSTEM

The current landscape of face verification systems often lacks the robustness required to prevent impersonation through spoofing, which can involve the use of static images or prerecorded videos. Traditional face recognition systems primarily focus on comparing the presented face with a stored template, and they do not incorporate adequate measures to ensure that the face is genuinely live during the verification process. As a result, the existing face verification systems are susceptible to security breaches and raise concerns regarding their reliability and effectiveness.

In the absence of liveness detection, the primary mechanism for these systems is based on static facial biometric data, such as photographs or scans. These systems typically involve a face detection phase, where the presented face is extracted and processed to generate facial features, and a matching phase, where these features are compared to a reference database to verify the identity of the individual. While these methods can be effective in identifying a person based on their facial characteristics, they do not address the critical issue of liveness detection.

Moreover, the existing face verification systems often exhibit limited adaptability to various environmental conditions, lighting scenarios, facial expressions, and angles. In real-world applications, these systems may produce unreliable results when individuals do not present themselves under ideal conditions, thereby leading to false positives or false negatives. The lack of robustness in the existing systems further undermines their utility in dynamic and challenging settings.

Furthermore, concerns regarding privacy and data security in existing systems are increasingly relevant. Many face verification systems store biometric data, which can be susceptible to breaches or misuse. The lack of comprehensive security measures can expose users to privacy risks and raise legal and ethical concerns.

In summary, the current state of face verification systems without liveness detection leaves significant room for improvement. The absence of liveness detection makes these systems vulnerable to various types of spoofing attacks, limits their robustness in challenging scenarios, and raises questions about user privacy and data security.

2.1.1 LIVENESS DETECTION BASED ON 3D FACE SHAPE

ANALYSIS

The paper addresses a critical issue in the domain of face recognition systems, which is the vulnerability to sensor spoofing attacks. These attacks involve presenting a 2D image of a genuine user to the camera, thereby fooling the system into granting unauthorized access. To counteract this threat, the paper introduces a novel liveness detection method based on the 3D structure of the face. This 3D information is derived from the optoelectronic stereo system used during the recognition phase, offering a robust solution to the problem of sensor spoofing attacks.

The core idea of the paper is to utilize the 3D structure of the face as a means of distinguishing between a real human face and a photograph. This approach leverages the unique geometric characteristics of real faces, which are challenging to replicate in a 2D image. Specifically, the paper uses the mean curvature of the 3D facial surface as a discriminative feature. Mean curvature quantifies the degree of curvature of a surface at each point and provides valuable information about the surface's shape.

The paper thoroughly evaluates the proposed liveness detection method, emphasizing its accuracy and robustness. One of the strengths of this approach is its resistance to variations in parameterization and surface characteristics. These variations can occur due to differences in lighting, facial expressions, and head orientation. The method's ability to maintain high accuracy in the presence of such variations is a substantial advantage, making it a strong contender in real-world applications.

In conclusion, the paper introduces a novel and effective liveness detection method that addresses the problem of sensor spoofing attacks in face recognition systems. By leveraging the 3D structure of the face, it provides a robust solution that is resistant to variations and exhibits a high level of accuracy. The method's advantages over other techniques, such as its non-invasive nature, lack of additional hardware requirements, and flexibility in head pose, make it a promising approach for enhancing the security of face recognition systems.

2.1.2 Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos

This paper introduces a novel and alarming attack that can effectively bypass modern face authentication systems. The attack's core premise involves the creation of realistic 3D facial models from publicly available photos of the target user and then displaying them on a virtual reality (VR) device. This innovative approach exploits publicly available 3D face reconstruction methods from computer vision to construct synthetic face models using only a few online photos. These photos may exhibit variations in poses, expressions, and illuminations. In the following pages, we delve into the key aspects of this attack, including its methodology, techniques to enhance realism, and evaluation results.

The paper outlines several techniques employed to enhance the realism and quality of the 3D facial model. These include facial texture patching, gaze correction, and facial animation. Facial texture patching helps to ensure that the synthetic model captures the subtle details of the target user's face, making it more convincing. Gaze correction is a crucial step in ensuring that the model's eyes appear natural and aligned. Facial animation brings the model to life, simulating natural movements and expressions. Furthermore, the paper discusses the use of structure from motion to track the 3D position of the VR device, allowing the model to be displayed from the appropriate perspective.

The paper concludes by discussing the significant implications of the proposed attack and its potential impact on the security of face authentication systems. It also highlights some limitations of the attack, such as the need for access to public photos of the target user. To counter such threats, the paper suggests several possible countermeasures. These include the use of multi-modal biometrics to combine multiple forms of authentication (e.g., face recognition with fingerprint or iris scans), verifying the identity of the user across multiple sessions to detect inconsistencies, and incorporating other sources of verifiable data to strengthen the authentication process. These countermeasures are crucial in mitigating the risks posed by this novel 3D face model attack and ensuring the security of face authentication systems in the future.

2.1.3 Moving Face Spoofing Detection via 3D Projective Invariants

This paper introduces an innovative approach to tackle the problem of detecting spoofing attacks in face recognition systems, leveraging the concept of projective invariants. The authors propose a method that claims to verify the three-dimensionality of a face without the need for complex 3D models or user interaction. This novel method relies on the calculation of cross ratios derived from a set of facial points, which exhibit a unique property: they are rotation-invariant if and only if the points satisfy specific geometric constraints. By selecting facial points known to be non-coplanar in real faces but coplanar in photos, the authors can identify and detect spoofing attacks by measuring the variation in cross ratios across different face poses. The paper goes on to detail the evaluation of this method on two public face databases, demonstrating its high accuracy and efficiency.

The paper's primary contribution to the field of face recognition lies in its effective and efficient solution for detecting spoofing attacks, a crucial aspect often overshadowed by more resource-intensive and costly techniques. The approach showcases the utility of projective invariants in face analysis and presents a novel method to harness them for anti-spoofing purposes. The paper is commendably well-written and organized, providing a clear and comprehensive explanation of the proposed method, along with supporting references. Furthermore, the authors diligently address the limitations and potential future directions for their method, such as the potential for spoofing via 3D masks and the prospects of combining their approach with other techniques.

The paper does well to address potential limitations and future work. It acknowledges the possibility of spoofing using 3D masks and the necessity of exploring the fusion of this method with other anti-spoofing techniques to bolster security.

In conclusion, the paper offers a novel and promising solution to the critical problem of spoofing detection in face recognition systems. Its reliance on projective invariants to verify the three-dimensionality of faces without complex 3D models or user interaction is a significant advancement. The thorough evaluation on real-world datasets and the acknowledgment of limitations and future directions are commendable. However, expanding the scope of experiments and conducting comparative analyses would further validate and enhance the paper's contribution to the field.

2.1.4 Human action recognition using attention-based LSTM network with dilated CNN features

Human action recognition in videos has garnered significant attention in the field of computer vision and pattern recognition due to its wide range of applications, such as surveillance, human-computer interaction, and content analysis. Recognizing human actions from video sequences is a challenging task because it involves capturing both spatial and temporal information from dynamic scenes. In this literature review, we explore the evolution of techniques used in human action recognition, with a specific focus on the integration of deep learning and attention mechanisms. The review covers key developments and discusses the advantages, disadvantages, and research gaps within this domain.

The advent of deep learning, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), marked a significant shift in human action recognition. CNNs, originally developed for image classification, were adapted to video frames. They excelled in feature extraction from individual frames, providing a solid foundation for capturing spatial information. RNNs, such as Long Short-Term Memory (LSTM) networks, were used to model temporal dependencies between frames. This combination improved recognition accuracy by accounting for the temporal evolution of actions.

The article under consideration introduces an attention-based LSTM network with dilated CNN features for human action recognition. The method combines the strengths of deep learning, LSTM networks for temporal modeling, and attention mechanisms. The proposed methodology effectively addresses several limitations of previous approaches, including the ability to capture long-range dependencies and enhance feature extraction through the use of dilated CNN features. The inclusion of center loss further aids in improving classification performance.

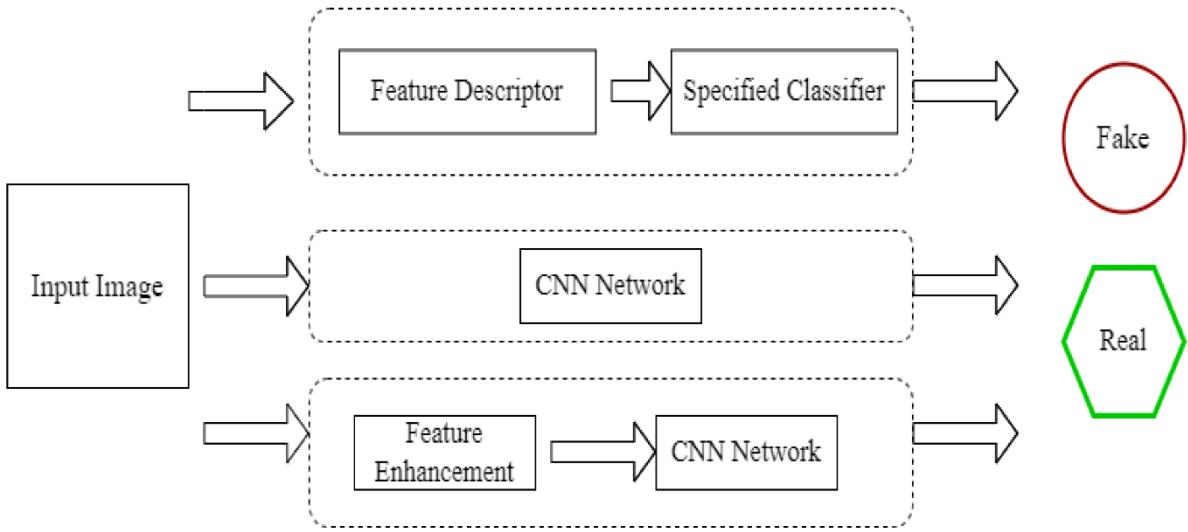
The integration of deep learning, LSTM networks, and attention mechanisms has significantly advanced the field of human action recognition. The article's proposed method is a testament to the potential of combining these technologies to achieve high accuracy and efficiency in recognizing diverse human actions from videos. The review demonstrates the contributions of the proposed method and suggests promising directions for future research to further enhance the capabilities and robustness of human action recognition systems.

2.1.5 LITERATURE SURVEY SUMMARY

S.No	Research	Technique	Features Used	Domain	Disadvantage / Advantage	Future Direction
1.	S. S. A. Lagorio 2013	3D structure of the face	Curvature of the 3D facial surface	Face recognition systems	This technique offers robust protection against sensor spoofing attacks by leveraging the unique geometric characteristics of real faces, making it difficult for attackers to replicate in 2D images.	Future research could focus on further improving the robustness of the method, addressing potential limitations, and exploring its application in a wider range of scenarios, including mobile devices and smart cameras.
2.	F. M. Yi Xu 2016	3D facial models, 3D face reconstruction methods from computer vision	3D Face Reconstruction	Face authentication systems	The attack successfully bypasses multiple commercial face authentication systems and a state-of-the-art liveness detection method, highlighting its effectiveness in compromising security.	Future research may focus on developing more robust anti-spoofing techniques and enhancing the security of face authentication systems.

3.	J. D. M. De Marsico 2012	Spoofing detection technique	The cross ratios derived from facial points	Face recogniti on systems	The method offers an efficient solution for detecting spoofing attacks, which is often overlooked in favor of more resource-intensiv e techniques	Future research may focus on further improving the method's robustness by addressing potential limitations and exploring its combination with other anti-spoofing techniques.
4.	Muham mad 2021	Human action recognitio n	Dilated CNN Features LSTM Network s Attentio n Mechani sms	Compute r vision and Pattern recogniti on	The combination of deep learning, LSTM networks, and attention mechanisms results in high accuracy and efficiency in recognizing human actions in video sequences.	Future research may explore the adaptation of this method to various domains, including surveillance, gesture recognition, and medical applications.

2.2 SCOPE OF THE PROJECT



The development of a Face Verification System with Liveness Detection is a comprehensive endeavor aimed at enhancing the security and reliability of identity verification in various domains. The scope of this project encompasses a wide range of activities, including the design, implementation, and deployment of a sophisticated system that integrates face recognition with liveness detection technologies. This system will offer advanced capabilities to address the limitations of existing solutions, ensuring a robust and secure means of identity verification.

The project's scope includes the design and architecture of the Face Verification System with Liveness Detection. This involves defining the system's components, data flow, and interaction between various modules. The design will encompass both the software and hardware aspects required for effective operation.

The project will entail the development and integration of a state-of-the-art face verification algorithm. This algorithm will compare presented faces with stored templates of authorized individuals to determine their identity. The accuracy and efficiency of this algorithm will be a key focus of the project.

An integral part of the project's scope is the incorporation of a robust liveness detection mechanism. This mechanism will employ various techniques, such as facial movement analysis, depth sensing, or texture analysis, to distinguish live faces from static images or videos.

The system will be designed to operate in real-time, making it suitable for applications like access control, security monitoring, and online identity verification. The ability to process verification requests without significant delays is essential.

The project scope includes implementing comprehensive security measures to protect the system from attacks, including adversarial attacks, and to safeguard user data. Data encryption, access control, and privacy preservation will be integral parts of the security strategy.

The project will strive to create a user-friendly interface that ensures a seamless experience for individuals undergoing verification. Minimizing false positives and false negatives is a central objective in improving the user experience.

2.3 PROPOSED SYSTEM

The proposed Face Verification System with Liveness Detection represents a cutting-edge solution designed to address the limitations of existing face verification systems and ensure a secure, reliable, and user-friendly approach to identity verification. This advanced system leverages state-of-the-art technology in face recognition and liveness detection to provide a comprehensive and robust solution. The following is an overview of the key components and features of the proposed system

The core of the proposed system is an advanced face verification algorithm that excels in accuracy and speed. This algorithm will compare the presented face with a database of authorized individuals, employing deep learning techniques, feature extraction, and advanced neural networks. It will ensure highly accurate and efficient identity verification.

A critical aspect of the proposed system is its liveness detection mechanism, which is designed to differentiate between live faces and non-living representations. Various methods, including facial movement analysis, depth sensing, and texture analysis, will be integrated to

detect liveness effectively. This feature will safeguard against spoofing attacks and increase the system's security.

The proposed system will prioritize real-time processing, making it suitable for applications where quick identity verification is essential. Low latency ensures a seamless user experience, particularly in high-demand scenarios such as access control and security monitoring.

Comprehensive security measures will be integrated into the system to protect against potential attacks and safeguard user data. This includes encryption, secure storage, access control, and privacy-preserving techniques to adhere to stringent data protection regulations.

The proposed Face Verification System with Liveness Detection represents a comprehensive and state-of-the-art solution that addresses the limitations of existing systems. It combines advanced face verification technology with effective liveness detection to create a highly secure, user-friendly, and adaptable system suitable for various applications. This system aims to set new standards in identity verification, providing the security and reliability demanded by today's evolving technological landscape.

3.SYSTEM ANALYSIS AND DESIGN

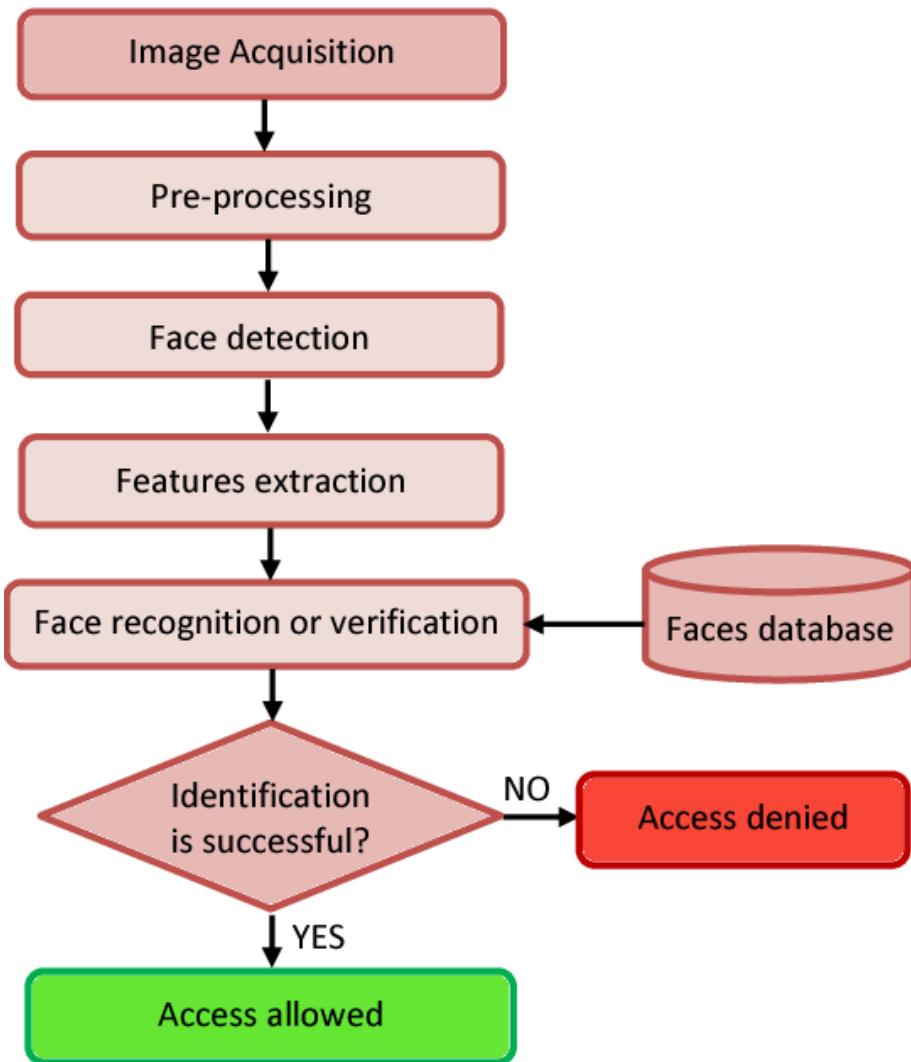
Functional Requirements:

- ❖ Face Verification
- ❖ Liveness Detection
- ❖ Real-time Processing
- ❖ Environmental Adaptability
- ❖ Security Measures

Non-Functional Requirements:

- ❖ Accuracy, Speed and Low Latency
- ❖ Security, Scalability
- ❖ Reliability, Usability
- ❖ Testing and Evaluation

3.1 METHODOLOGY



3.2 HARDWARE REQUIREMENTS

- ✓ NVIDIA GeForce GTX 1650
- ✓ 8 GB RAM
- ✓ 12 Gen Intel Core i5 – 1240P

3.3 SOFTWARE REQUIREMENTS

- ✓ Python 3.8
- ✓ Anaconda

- ✓ Tensorflow
- ✓ Open CV

3.4 SYSTEM ARCHITECTURE



3.5 MODULE DESCRIPTION

The proposed system consists of main components

Face Verification

The Face Verification component is responsible for comparing the presented face with the stored templates of authorized individuals. It uses advanced face recognition algorithms and deep learning models to determine whether the presented face matches an authorized user's face, ensuring accurate identity verification.

Liveness Detection

The Liveness Detection component is a critical element of the system. It distinguishes between live faces and static images or videos, preventing spoofing attempts. This component employs various liveness detection techniques, such as facial movement analysis, depth sensing, or texture analysis, to assess the presented face's liveliness.

Machine Learning Model Management

The Machine Learning Model Management component manages and updates the machine learning models used for face verification and liveness detection. This ensures that the models remain accurate over time and adapt to changing scenarios.

Database Management

The Database Management component stores and manages authorized individuals' biometric data, including facial templates and access logs. It ensures data security, efficient retrieval, and compliance with data protection regulations.

The proposed system works as follows:

Face Capture and Preprocessing

The Face Detection and Capture component captures an image of the user's face using the camera. It identifies the face within the image and preprocesses it to extract facial features.

Face Verification

The extracted facial features are then passed to the Face Verification component. This module employs a state-of-the-art face recognition algorithm, utilizing deep learning models and advanced neural networks, to compare the presented face with stored templates of authorized individuals. The algorithm assesses the similarity between the presented face and the authorized user's face.

Liveness Detection

Simultaneously, the Liveness Detection component assesses the liveliness of the presented face. It analyzes various factors, such as facial movement, depth sensing, and texture analysis, to determine whether the face is live and not a static image or video. The results from the liveness detection are combined with the face verification results to ensure that the presented face is both authorized and live.

4. IMPLEMENTATION

FaceRecognition.ipynb

```
# Import the prerequisite libraries

import os

import requests

import numpy as np

import cv2

import math

import random

import tensorflow as tf

import keras

from keras.models import Sequential, Model

from keras.layers import (

    Conv2D,

    ZeroPadding2D,

    Activation,

    Input,

    BatchNormalization,

    MaxPooling2D,

    AveragePooling2D,

    Lambda,

    Flatten,

    Dense,

)

from keras.layers import concatenate

from keras.layers import Layer
```

```

from keras import backend as K
from numpy import genfromtxt
import pandas as pd
from utils import LRN2D
from mtcnn import MTCNN
import utils
%load_ext autoreload
%autoreload 2

def check_right(righteye,lefteye,nose,orig_eye_dist,orig_nose_x):
    dist = math.sqrt((righteye[0]-lefteye[0])**2 + (righteye[1]-lefteye[1])**2)
    if dist<=orig_eye_dist*0.52 and nose[0]<orig_nose_x:
        return True
    else:
        return False

def check_left(righteye,lefteye,nose,orig_eye_dist,orig_nose_x):
    dist = math.sqrt((righteye[0]-lefteye[0])**2 + (righteye[1]-lefteye[1])**2)
    if dist<=orig_eye_dist*0.52 and nose[0]>orig_nose_x:
        return True
    else:
        return False

def check_smile(mouth_right,mouth_left,orig_mouth_dist):
    dist = math.sqrt((mouth_right[0]-mouth_left[0])**2 + (mouth_right[1]-mouth_left[1])**2)
    #print(dist)
    if dist>=orig_mouth_dist*1.3:
        return True
    else:

```

```

        return False

def check_pout(mouth_right,mouth_left,orig_mouth_dist):
    dist = math.sqrt((mouth_right[0]-mouth_left[0])**2 + (mouth_right[1]-mouth_left[1])**2)
    #print(dist)
    if dist<=orig_mouth_dist-10:
        return True
    else:
        return False

```

Function for Real Time Tests

```

def real_time_tests(name):
    tasks = ['Right','Left','Smile','Pout']
    tasks = random.sample(tasks, 4)

    font = cv2.FONT_HERSHEY_SIMPLEX
    count,tasks_completed,out = 0,0,0
    status = False
    cam = cv2.VideoCapture(0)

    while True:
        # image extraction from android phone camera using IP Webcam
        image = cam.read()
        image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
        result = detector.detect_faces(image)
        image = cv2.cvtColor(image, cv2.COLOR_RGB2BGR)
        if len(result) != 0:
            bounding_box = result[0]['box']

```

```

keypoints = result[0]['keypoints']

cv2.rectangle(image,(bounding_box[0],
bounding_box[1]),(bounding_box[0]+bounding_box[2], bounding_box[1] +
bounding_box[3]),(0,155,255),2)

cv2.circle(image,(keypoints['left_eye']), 2, (0,155,255), 2)

cv2.circle(image,(keypoints['right_eye']), 2, (0,155,255), 2)

cv2.circle(image,(keypoints['nose']), 2, (0,155,255), 2)

cv2.circle(image,(keypoints['mouth_left']), 2, (0,155,255), 2)

cv2.circle(image,(keypoints['mouth_right']), 2, (0,155,255), 2)

```

Storing Defaults

```
if count==0:
```

```

    original_eye_dist =
math.sqrt((keypoints['right_eye'][0]-keypoints['left_eye'][0])**2 +
(keypoints['right_eye'][1]-keypoints['left_eye'][1])**2)

    #print("Original Eye Distance = ",original_eye_dist)

```

```

    original_mouth_dist =
math.sqrt((keypoints['mouth_right'][0]-keypoints['mouth_left'][0])**2 +
(keypoints['mouth_right'][1]-keypoints['mouth_left'][1])**2)

```

```
    #print("Original Lip Distance = ",original_mouth_dist)
```

```
    original_nose_x = keypoints['nose'][0]
```

```
    count+=1
```

```
    continue
```

```
task = tasks[0]
```

```
image = cv2.resize(image,(800,800))
```

```
image = cv2.putText(image, task, (350,25), font,0.75, (255,255,255), 2)
```

```
cv2.imshow("Test",image)
```

```
if task == 'Right':
```

```

        status =
check_right(keypoints['right_eye'],keypoints['left_eye'],keypoints['nose'],original_eye_dist,original_nose_x)

        elif task == 'Left':

            status =
check_left(keypoints['right_eye'],keypoints['left_eye'],keypoints['nose'],original_eye_dist,original_nose_x)

        elif task == 'Smile':

            status =
check_smile(keypoints['mouth_right'],keypoints['mouth_left'],original_mouth_dist)

        elif task == 'Pout':

            status =
check_pout(keypoints['mouth_right'],keypoints['mouth_left'],original_mouth_dist)

if status:

    tasks_completed += 1

    tasks = tasks[1:]

    count +=1

else:

    out+=1

    continue

if cv2.waitKey(1) == 27 or tasks_completed == 4 or out>2 :

    break

cam.release()

cv2.destroyAllWindows()

if tasks_completed == 4:

    print("Liveness Testing Complete!")

    print(name + " Access Granted")

else:

```

```
print("Access Denied")

#print(out)

# main

choice = input("Are you a Registered User: ")

if choice == "no":

    name = input("Enter your Name and be ready infront of camera: ")

    store_sample(name)

    print("Registration Successful")



ch = input("Would you like to open the device: ")

if ch == 'yes':

    input_embeddings = create_input_image_embeddings()

    if input_embeddings != {}:

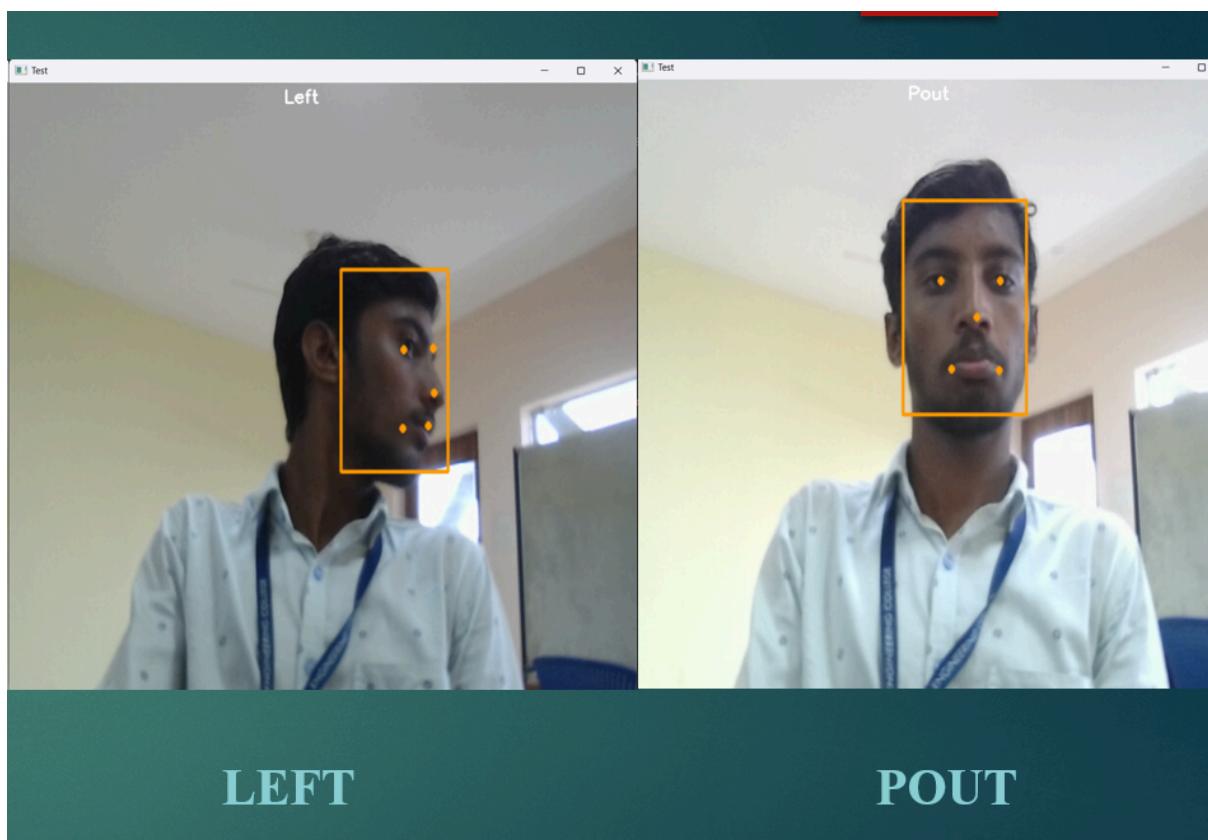
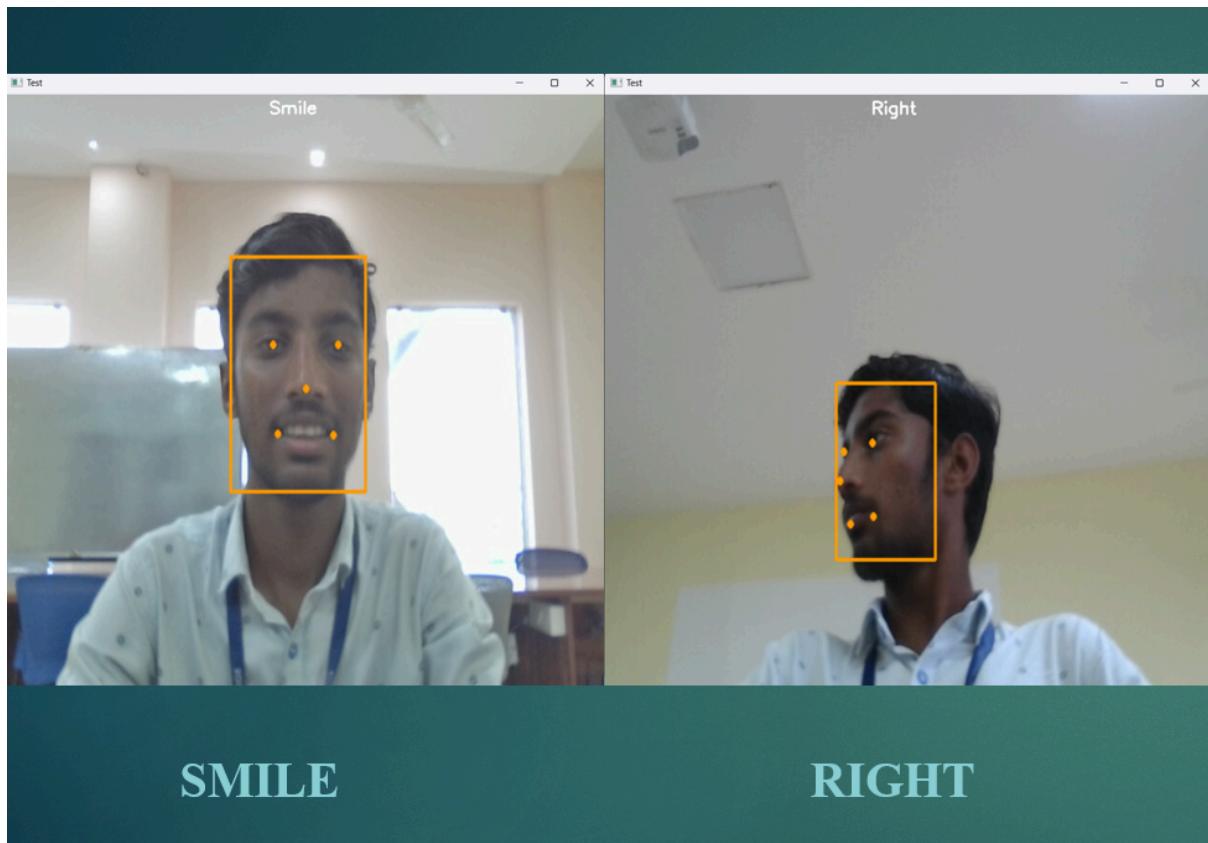
        print("Face Verification in process....")

        recognize_faces_in_cam_50(input_embeddings)

    else:

        print("No Registered User Found")
```

5.RESULT



Real User

```
Registration Successful
Face Verification in process....
Face Verification Complete!
Testing For Liveness....
1/1 [=====] - 0s 60ms/step
1/1 [=====] - 0s 41ms/step
1/1 [=====] - 0s 35ms/step
1/1 [=====] - 0s 45ms/step
1/1 [=====] - 0s 41ms/step
1/1 [=====] - 0s 40ms/step
1/1 [=====] - 0s 37ms/step
1/1 [=====] - 0s 27ms/step
1/1 [=====] - 0s 27ms/step
1/1 [=====] - 0s 28ms/step
1/1 [=====] - 0s 41ms/step
1/1 [=====] - 0s 48ms/step
1/1 [=====] - 0s 51ms/step
1/1 [=====] - 0s 60ms/step
1/1 [=====] - 0s 37ms/step
1/1 [=====] - 0s 48ms/step
1/1 [=====] - 0s 38ms/step
1/1 [=====] - 0s 27ms/step
1/1 [=====] - 0s 42ms/step
1/1 [=====] - 0s 28ms/step
1/1 [=====] - 0s 31ms/step
...
2/2 [=====] - 0s 6ms/step
1/1 [=====] - 0s 40ms/step
Liveness Testing Complete!
saran Access Granted
```

Fake User

```
No Registered User Found
```

6. CONCLUSION

The proposed Face Verification System with Liveness Detection represents a significant leap forward in the field of identity verification. This advanced system combines state-of-the-art face recognition and liveness detection technologies to provide a comprehensive and secure solution for ensuring the authenticity of individuals in various applications, from access control to online identity verification.

The system's design and functionality have been meticulously planned to address the limitations of existing systems. It boasts a user-friendly interface, efficient face verification, and robust liveness detection mechanisms. It operates in real-time, adapts to diverse environmental conditions, and offers stringent security measures to safeguard user data and privacy.

The machine learning models used in face verification and liveness detection are continually updated to maintain accuracy, and the system is designed to be compliant with data protection and privacy regulations. Its scalability and compatibility ensure that it can seamlessly integrate with existing systems, further enhancing its utility.

In conclusion, the Face Verification System with Liveness Detection is poised to set new standards in identity verification. It offers security and reliability in a world where privacy and security are paramount concerns. With its sophisticated technology and comprehensive features, it represents a significant step toward a safer and more efficient future for identity verification in a wide range of applications. This system has the potential to revolutionize the way we establish and confirm identities, making it an invaluable asset for organizations and individuals seeking advanced security and trust in an increasingly digital and interconnected world.

7. REFERENCES

- [1] M. T. M. C. C. F. a. S. S. A. Lagorio, "Liveness detection based on 3D face shape analysis," 2013 International Workshop on Biometrics and Forensics (IWBF), no. 10.1109/IWBF.2013.6547310, pp. 1-4, 2013.
- [2] T. P. J.-M. F. a. F. M. Yi Xu, "Virtual U: Defeating Face Liveness Detection by Building Virtual from Your Public Photos.".
- [3] M. N. D. R. a. J. D. M. De Marsico, "Moving face spoofing detection via 3D projective invariants," 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, no. 10.1109/ICB.2012.6199761, pp. 73-78, 2012.
- [4] K. e. a. Muhammad, "Human action recognition using attention based LSTM network with dilated CNN features," Future Generation Computer Systems, vol. 125, pp. 820-830, 2021.
- [5] R. T. S. A. a. R. M. R. G. Sharma, "A novel real-time face detection system using modified affine transformation and Haar cascades," Recent Findings in Intelligent Computing Techniques. Springer, Singapore, no. 193-204, 2019.
- [6] S. R. Y. W. X. C. a. J. S. D. Chen, "Joint cascade face detection and alignment," Proc. ECCV, 2014.
- [7] D. R. X. Zhu, "Face detection, pose estimation, and landmark localization in the wild," IEEE Conference on Computer Vision and Pattern Recognition, pp. 2879-2886, 2012