WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Face Voice Key: (Face authentication and voice recognition)

P. Swati[1] ,Ojaswi Shinde[2],Jay Kumar[3],Megha Yadav[4],Saurabh Shukla[5]

[1]Assistant Professor ,Department of Computer Science And Engineering , Bhilai Institute of Technology Raipur (C.G.),India
[2345] Department of Computer Science And Engineering , Bhilai Institute of Technology Raipur (C.G.),India

ABSTRACT:

FaceVoice Key Voice authentication and facial recognition are two critical rudiments of a biometric security system. This enhances the slyness and ease of the verification of identity. This design looks into the possible combination of these generalities with a strongmulti-factor authentication system. The voice authentication element examines the audio features just like voice, tone, and speech. To insure safe and dependable authentication, meanwhile, the facial recognition module employs advanced image processing and machine knowledge algorithms to descry facial features and authenticate stoners at a high position of delicacy. It also reduces pitfalls associated with risks like counterfeiting or counterfeiting. either, it improves vacuity for stoners. This design is inclusive of developing and training a deep knowledge model. Using point birth ways and assessing system performance on a variety of data sets. This design demonstrates the eventuality of biometric integration in shaping the future of authentication technology. Facial authentication and voice recognition are biometric technologies used to authenticate or identify individualities predicated on their unique physical and behavioral characteristics.

Facial authentication analyzes facial features analogous as the distance between the eyes, chin shape, and other distinctive marks. also take a print and compare it with the stored template. Generally used for unleashing smartphones. access control and surveillance Because itsnon- protrusive and fast operation, in fact if there are lights, angles, the mask may be told by obstructions or To speech recognition reviews and recognizes or monitors individual speech sounds. similar as high and low pitch situations Pitch and cadence are used greatly in operations similar as virtual assistants. Secure banking system and call center authentication. While fluently used and effective But sensitive to girding noise. Sound reduplication and changes due to Complaint Both technologies have their special graces and faults. They can be used concertedly for increased security inmulti-factor authentication systems..

Introduction:

Voice Authentication Systems Voice authentication systems can also be called voice biometrics, which is a technology designed to corroborate identity using specific characteristics of a person's voice. It works by assaying various aspects of a person's speech, voice, tone, and style.
A system of vindicating a person's identity using unique audio features, analogous as a point. This system gives each person a unique voice that can be analyzed and used to corroborate their identity. This technology is considerably used in security systems. customer service and access control

Voice authentication systems have come a transformative technology for user security and authentication. Taking advantage of the unique characteristics of a person's voice These systems give a accessible and effective system of authentication that goes beyond traditional styles analogous as watchwords and Legs, and their prolusion has come an increasingly popular option. It explores the introductory principles of voice authentication. and its benefits and the adding significance of adding security in particular bias. financial deals and access to sensitive information

Facial Recognition Facial recognition technology analyzes the unique features of a person's face to corroborate their identity. This requires a series of measures.
Facial Recognition and Voice Authentication Revolutionizing Security

Facial recognition and voice authentication are two advanced biometric technologies that are changing the terrain of particular and marketable security. Both systems calculate on unique physical and behavioral characteristics to identify and authenticate individualities. To ensure accurate and safe access to various systems, outfit, and installations. The integration of these technologies into modern operations reflects the growing demand for farther robust and user-friendly authentication styles.

Facial recognition involves assaying and mapping facial features to identify people. These systems use complex algorithms to measure parameters analogous as distance between the eyes, chin shape, facial shape, etc. Cameras equipped with artificial intelligence(AI) can capture images and compare these features with stored data. This makes facial recognition effective andnon- protrusive. Mobile styles, at fields, are ubiquitous in banking and public verification systems. This makes it accessible and safe, still, there are challenges analogous as variations in lighting, currency and age, as well as insulation enterprises. continuous technological and ethical considerations are demanded.

Voice authentication, on the other hand, Take advantage of the unique parcels of a person's voice, analogous as pitch. pitch and cadence; anatomize speech patterns and sound characteristics and produce a point- suchlike sound for comparison in after use of the voice authentication system. This system has been used in call centers. intelligent adjunct and financial services To authenticate stoners without using watchwords or physical commemoratives.

Literature Review

1. **" Face –voice based mutlimodel biometric authentication via FaceNet and GMM " by Bayan Alharbhi, Hanan S Alshanbari (2023)**
   - Multimodal Integration: The system combines FaceNet for face recognition and Gaussian Mixture Models (GMM) for voice recognition, utilizing score-level fusion to improve authentication accuracy and reduce error rates.
   - High Security: It is designed for applications requiring robust security, such as banking and mobile device access, offering increased resistance to spoofing and other biometric vulnerabilities.
   - Performance: The approach achieves a low equal error rate (EER), demonstrating superior reliability compared to single-modality systems by leveraging the strengths of both facial and voice biometrics.
2. **"Deep Speaker Embeddings for Text-Independent Speaker Verification" by Snyder et al. (2018)**
   - Introduced *x-vectors*, a deep-learning-based embedding for speaker verification.
   - Highlighted the execution of x-vectors in both text-dependent and text-independent assignments.
   - Strength: Scalability for large-scale datasets.
3. **"Voice Privacy Challenges and Solutions" by Tomi Kinnunen et al. (2020)**
   - Discussed vulnerabilities of speaker verification systems to spoofing attacks and adversarial examples.
   - Proposed privacy-preserving methods, such as feature anonymization.
4. **"Robust End-to-End Text-Independent Speaker Verification Using CNNs" by Zhang et al. (2021)**
   - Utilized convolutional neural networks (CNNs) for handling noisy and variable environments.
   - Explored attention mechanisms to improve robustness in speaker embeddings..
5. **"Multimodal Speaker Recognition with Voice and Speech Patterns" by Qian et al. (2022)**
   - Proposed a multimodal approach combining voice and speaking style for enhanced accuracy.
   - Tackled challenges in cross-language speaker verification.
6. **"Adversarial Attacks on Face Recognition Models" by Sharif et al. (2018)**
   - Investigated vulnerabilities of face recognition systems to adversarial examples.
   - Proposed countermeasures, including robust training strategies.
7. **"Lightweight Face Recognition with MobileFaceNet" by Howard et al. (2020)**
   - Developed MobileFaceNet, a compact model optimized for mobile devices.
   - Balances accuracy and computational efficiency, catering to edge applications

Implications for FaceVoice Key

FaceVoice Key: Voice authentication and face recognition have far-reaching implications in technology, security, and ethics. Voice authentication has improved security in risky industries such as banking and healthcare, providing easy access in a hands-free manner. The collection of voice data raises privacy concerns, thus necessitating strong encryption and strict adherence to regulations to avoid misuse. Face recognition, like all biometric technologies, has changed security, becoming a widespread technology in policing, border control, and surveillance. However, these applications bring up some ethical issues, such as mass surveillance and potential misuse in an authoritarian context. In addition, the technology is subject to challenges related to bias and fairness: the unbalanced nature of the datasets could lead to inaccuracies or discriminatory outcomes.

Existing Work :

Existing Work Significant developments have been made within the domain of voice authentication, based on the applicability of machine learning approaches and probabilistic models. Important approaches include x-vectors proposed by Snyder et al.To create robust speaker embeddings with the aid of using profound neural structures at the mission of text-impartial speaker acknowledgment, and Gaussian Blend Models for speaker confirmation, a nook stone for modeling probabilistic distribution on the features of voice.

Deep learning innovations such as FaceNet and ArcFace have transformed face authentication. FaceNet uses deep convolutional neural networks with a triplet loss function to produce precise embeddings, allowing for good facial recognition and clustering. The ArcFace model further improves the separability of features with an advanced loss function and achieves state-of-the-art performance on benchmark datasets.

Such models, like MobileFaceNet, are lightweight and, therefore, suitable for mobile and embedded devices, with an optimal balance of computational cost and accuracy for applications requiring efficiency. The multimodal biometric systems combining voice and face authentication have been increasingly used because of the high reliability and security offered by them. These systems are reducing error rates and resisting spoofing attacks by using the strength of both modalities. This trend is going to overcome the weaknesses in single-modality systems especially in the high-security applications, such as banking, access to mobile devices, and border control. Multimodal approaches constitute an important step forward toward building strong, user-friendly authentication solutions.

Proposed Methodology :

The proposed method for integrating face verification and voice recognition is a multi-step approach to ensure safety, accuracy, and efficiency. First, the problem definition step focuses on identifying the objectives of Systems such as creating requirements such as secure access controls. or user identity information Facial recognition and voice samples are collected from various users. The dataset should include different facial expressions, lighting conditions, and angles for facial data. Different accents, tones, and pitches for the audio data. Pre-process these datasets and normalize facial images for example scaling and color correction and clean up audio files for example noise reduction and format conversion.

Next feature extraction is applied which transform raw data into meaningful presentation in both formats. for face verification Facial features like landmarks and embeddings, such as Cepstral Mel frequencies, are extracted using deep learning techniques like convolutional neural networks (CNN) or pre-trained models like FaceNet or VGGFace. Deep, such as WaveNet or Speech2Text speech recognition frameworks Features like coefficient (MFCC), spectrogram, or embedding are extracted. And these features are as input for classification or matching algorithms.

After the properties get separated. This starts the process of classification and decision making. Various machine learning models such as SVM, random forests, or deep neural networks can be used to classify or validate the inputs. There are multiple fusion techniques that help unite the face and the neck.

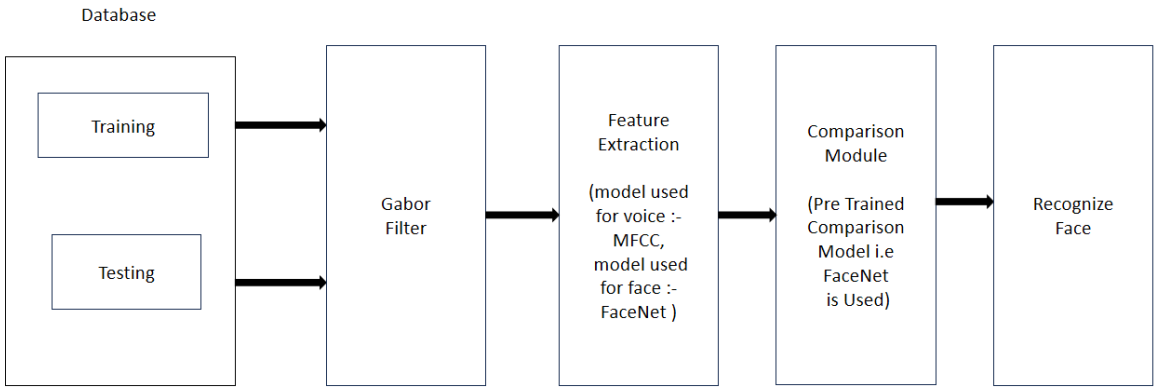

Fig:- Flow Chart

Implementation :

```
[ ]: import tensorflow as tf
import numpy as np
import os
import glob
import pickle
import cv2
import time
from numpy import genfromtxt

from keras import backend as K
from keras.models import load_model
K.set_image_data_format('channels_first')
np.set_printoptions(threshold=np.inf)


import pyaudio
from IPython.display import Audio, display, clear_output
import wave
from scipy.io.wavfile import read
from sklearn.mixture import GaussianMixture
import warnings
warnings.filterwarnings("ignore")

from sklearn import preprocessing
import python_speech_features as mfcc
```

Fig:- Importing Libraries

Audio processing

```
#Calculate and returns the delta of given feature vector matrix
def calculate_delta(array):
    rows,cols = array.shape
    deltas = np.zeros((rows,20))
    N = 2
    for i in range(rows):
        index = []
        j = 1
        while j <= N:
            if i-j < 0:
                first = 0
            else:
                first = i-j
            if i+j > rows -1:
                second = rows -1
            else:
                second = i+j
            index.append((second,first))
            j+=1
        deltas[i] = ( array[index[0][0]]-array[index[0][1]] + (2 * (array[index[1][0]]-array[index[1][1]])) ) / 10
    return deltas

#convert audio to mfcc features
def extract_features(audio,rate):
    mfcc_feat = mfcc.mfcc(audio,rate, 0.025, 0.01,20,appendEnergy = True, nfft=1103)
    mfcc_feat = preprocessing.scale(mfcc_feat)
    delta = calculate_delta(mfcc_feat)

    #combining both mfcc features and delta
    combined = np.hstack((mfcc_feat,delta))
    return combined
```

Fig:-Audio Processing

Delete User

```
[15]: # deletes a registered user from database
def delete_user():
    name = input("Enter name of the user:")

    with open("C:/Users/shukl/Voice-Authentication-and-Face-Recognition-master/face_database/embeddings.pickle", "rb") as database:
        db = pickle.load(database)
        user = db.pop(name, None)

        if user is not None:
            print('User ' + name + ' deleted successfully')
            # save the database
            with open("C:/Users/shukl/Voice-Authentication-and-Face-Recognition-master/face_database/embeddings.pickle", 'wb') as database:
                    pickle.dump(db, database, protocol=pickle.HIGHEST_PROTOCOL)

            # remove the speaker wav files and gmm model
            [os.remove(path) for path in glob.glob('./voice_database/' + name + '/*')]
            os.removedirs('./voice_database/' + name)
            os.remove('./gmm_models/' + name + '.gmm')

        else:
            print('No such user !!')

delete_user()
```

```
Enter name of the user: saurabh
No such user !!
```

Fig:- Deleting a user

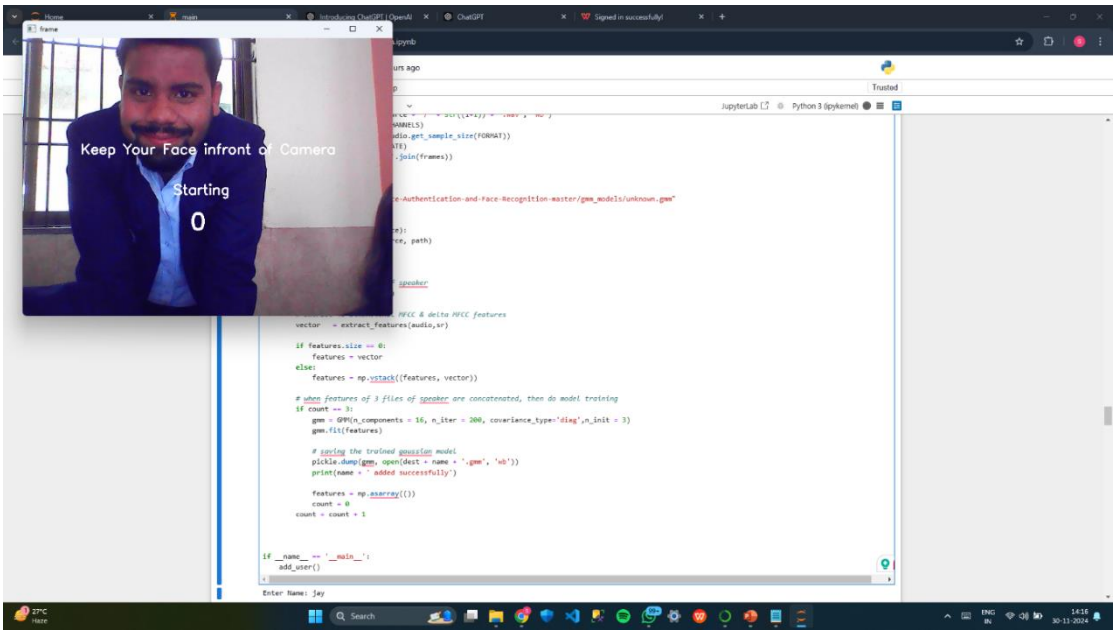

Fig:- Adding a New User

Conclusion :

Facial affirmation and voice affirmation biometrics provide strong security methodologies for a wide amplify of applications: updating consolation and end-user experience. These are curiously physiological behavioral properties-based systems.

This makes the procedure more secure and harder to copy compared to ordinary plans, like passwords or PINs. Go up against verification Facial affirmation is a non-contact and frictionless way of confirmation. The exactness and faithful quality are advanced with the progress in AI and significant learning. In show disdain toward of the truth that it is outstandingly supportive and germane for various applications, tallying opening flexible phones Secure installment and get to control Assurance, spoofing, through shroud or photographs, and normal impediments, such as horrendous lighting, and related issues, it is character codes. Voice affirmation grants the utilize without hands and offers a common interface for both affirmation and command execution.

They are of much advantage especially to physically weakened individuals or those experiencing strongly touch interaction. On the other hand, they might stand up to impedances from commotion in the environment, enunciation, and conceivable mirroring or bewildering of sounds. Interoperability and future trends Multi-factor biometric security, given by arranges facial affirmation and voice affirmation, decreases the vulnerabilities related with each. More solid calculation combinations measures to expect adulterating, and data encryption will address current controls and move forward these systems…

REFERENCES:

1. 1.“ Go up against –voice based mutlimodel biometric affirmation through FaceNet and GMM “ by Bayan Alharbhi, Hanan S Alshanbari (2023)
2. 2."Voice Security Challenges and Courses of action" by Tomi Kinnunen et al. (2020)
3. 3."Robust End-to-End Text-Independent Speaker Affirmation Utilizing CNNs" by Zhang et al. (2021)
4. 4."Multimodal Speaker Affirmation with Voice and Talk Plans" by Qian et al. (2022)
5. 5."FaceNet: A Bound together Embedding for Stand up to Affirmation and Clustering" by Schroff et al. (2015)
6. 6."Adversarial Attacks on Stand up to Affirmation Models" by Sharif et al. (2018)
7. 7.Large-Scale Learning of Generalizable Stand up to Representations" by Deng et al. (2019) 8."Lightweight Go up against Affirmation with MobileFaceNet" by Howard et al. (2020)