Audio Spoof Detection Integrated with a Home Automation System Using IoT

Dr.Mohanapriya M.E , Ph.D
Associate Professor,Coimbatore Institute Of technology
Yokesh RS
Nalin Suriya
Gourav Gopal
Vishal Karthik

Introduction:

Development of VCD's, have boosted the realization of smart homes, voice-controlled authentication systems etc.,.These VCDs are vulnerable to different spoofing attacks. Audio Authentication is becoming very essential part of our lives. Audio Authentication spoofing is becoming an issue. High-quality audio recorders enable bypassing this audio authentication system by just recording the human voice and reusing them for accessing the same system. Thus, there exists a need to develop a voice anti-spoofing framework capable of detecting multiple audio spoofing attacks.

Literature Survey:

In paper Fusion of Belts and GMM-UBM Systems for Audio Spoofing Detection (2019), Bidirectional Long Short Term Memory (BiLSTM) networks with constant Q cepstral coefficients (CQCC) are used to classify real audio from fake audio in anti-spoofing systems.By fusing the BiLSTM and GMM-UBM systems, a fusion mechanism is used to increase the variability of the systems' decision-making processes and their accuracy.Over the baseline systems, these proposed systems significantly improved performance.

In this paper , IoT based speech recognition system(2022) speech recognition based IoT system is carried out.For IoT system Raspberry pi board is used and for wifi communication ESP-32 module is used. For speech recognition Support vector machine model is used for training the speech recognition model.

Proposed System:

An Iot system which acts as an home automation system is proposed which uses a Bidirectional LSTM model to classify the audio samples and GMM model to identify the specific voice of the speaker. If the given audio input is found to be an spoofed audio or an invalid user , then the system denies the access to the system. Features fed into both the bidirectional LSTM model as well as GMM model are generated using MFCC methodologies.

The proposed system performs binary classification of audio data which are mapped to two classes

a) Authentic/Bonafide
b) Spoofed

And identifies the speaker voice using the GMM model and performs the necessary action in the Home automation system.

Dataset Used.

1. Audio Spoof Detection Model

The Dataset used in the model is Automatic Speaker Verification(ASV) 2019.

ASV Spoof dataset contains two types of Audio files

- Physical Access - Bonafide utterances are made in a real, physical space in which spoofing attacks are captured and then replayed within the same physical space using replay devices of varying quality.
- Logical Access - Bonafide and spoofed utterances generated using text-to-speech (TTS) and voice conversion (VC) algorithms are communicated across telephony and VoIP networks with various coding and transmission effects

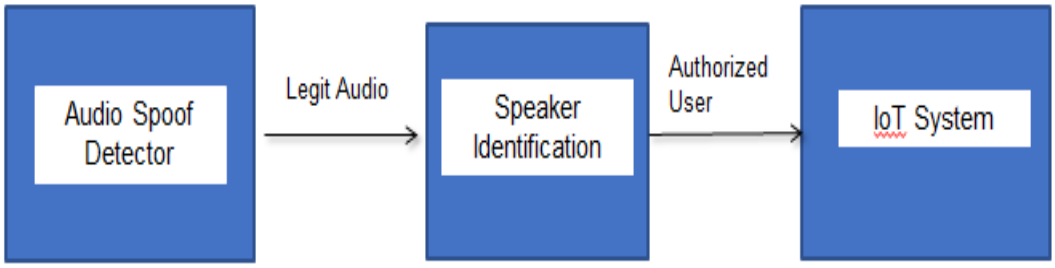
The dataset includes genuine and spoofed speech from 20 speakers (8 male, 12 female).Each spoofed utterance is generated according to one of 2 voice conversion and 3 speech synthesis algorithms.

The voice conversion systems include those based on (i) neural-network-based and (ii)transfer-function-based methods.

The speech synthesis systems were implemented with (i) waveform concatenation, (ii) neural-network-based parametric speech synthesis using source-filter vocoders and (iii) neural-network-based parametric speech synthesis using Wavenet.

2. Speaker Identification Model

The model receives 5 audio samples from the user for training and creates an GMM model for that specific speaker. When an audio file is given as input it compares the scores of all the GMM model and finds the model that produces the highest score value. The speaker is then identified with the label for whom the it is made.

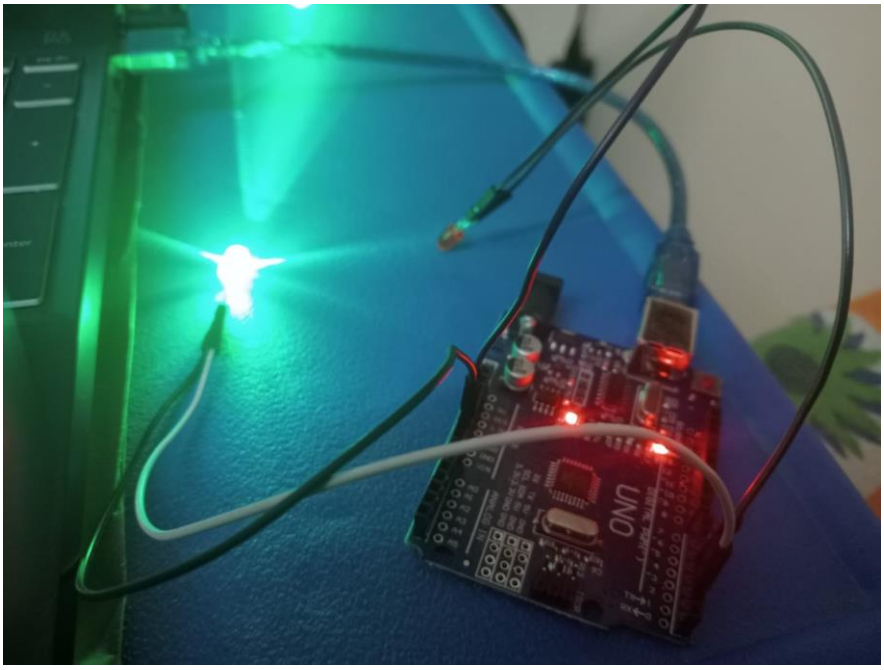


Result:

```
 1.Register for New User
 2.Give Command:
 3.Exit Application
2
----------------------record device list---------------------
Input Device id  0  -  Microsoft Sound Mapper - Input
Input Device id  1  -  Microphone Array (Realtek(R) Au
Input Device id  2  -  Stereo Mix (Realtek(R) Audio)
-------------------------------------------------------------
1
recording via index 1
recording started
recording stopped
```

```
1/1 [==============================] - 0s 428ms/step
0
Access Granted!
```

```
498
20
[-22.5388012  -21.48969341]
    detected as -  Yokesh.gmm
COM3 - Standard Serial over Bluetooth link (COM3)
COM6 - USB-SERIAL CH340 (COM6)
COM4 - Standard Serial over Bluetooth link (COM4)
Select Port: COM6
COM6
Arduino Command: (ON/OFF):ON
Arduino Command: (ON/OFF):OFF
Arduino Command: (ON/OFF):L
Arduino Command: (ON/OFF):ON
Arduino Command: (ON/OFF):OFF
Arduino Command: (ON/OFF):
```



Conclusion:

The Home automation system developed in this project is a reliable and efficient solution for safeguarding against audio spoofing attacks. The integration of an audio spoof detector and speaker identification system ensures that only authorized users can access the automated devices in the home. The accuracy obtained for the audio spoof detection model is 85%, which is a significant improvement over existing methods.

The proposed speaker identification system, which utilizes MFCC feature extraction and GMM model, has been tested against both known and unknown users. The system performed as expected, effectively identifying the known user while denying access to the unknown

users. This ensures that only authorized users can control the home automation system, thereby increasing security.

The use of Arduino UNO board, LED lights, servo motor, connecting wires, and breadboard for IoT integration provides a cost-effective and reliable solution for home automation. The integration of IoT devices with the audio spoof detector and speaker identification system ensures that users can control their home environment with ease and convenience.

The System demonstrates the effectiveness of integrating an audio spoof detector and speaker identification system with IoT devices for home automation. The proposed system provides reliable protection against audio spoofing attacks while ensuring that only authorized users can access the automated devices in the home. The accuracy obtained for the proposed system is promising and shows great potential for future research in this field.