

Enhancing Security With Speech Recognition: A Voice- Based Access Control System

02FE21BEC076: ROHIT SHEKDAR

02FE21BEC071: RECHAL GADVI

02FE21BEC082: SAKSHI SADARE

02FE21BEC079: SAIRAJ PATIL

Under the Guidance of : Prof. NEELAM SOMMANAVAR

CHAPTER 1

Contents

1	Problem Statement	3
2	Abstract	3
3	Introduction	3
4	Literature Survey	4
5	Block Diagram	6
6	References	6

1 Problem Statement

Build a Basic Voice Recognition system that can recognize and differentiate between a few words and phrases.

2 Abstract

This project provides a Python-based Voice Recognition System with a Tkinter graphical user interface. The system uses the Speech Recognition library for audio processing to discriminate between specified words and phrases. The user-friendly Tkinter interface allows for seamless interaction, making it suitable for users with a variety of technical backgrounds. Real-time audio processing, dynamic GUI feedback, and an extendable vocabulary are among the key features. This project provides a flexible basis for incorporating voice commands into a variety of applications, with an emphasis on simplicity and customization.

3 Introduction

Nowadays, a lot of residential area and the companies are using all kinds of security system to make sure their property is secured such as using password and User ID/Pin for protection. Unfortunately, all these security system is not secured at all because the pin code can be hacked, the ID card can be stolen and duplicated. Based on the reasons, a whole new technology of security system must bring out to increase back the confidential of the civilian about the security system¹. A biometric technology is the one which use the user features parameter as the password. The feature parameters of everyone is unique, even the users are twins. Therefore, the voice recognition system is safe for the administrator user. Voice is the most natural way to communicate for humans. In this thesis, the issue of voice recognition is studied and a voice recognition system is developed for certain word being spoken¹. Voice biometric technology for authentication user is more convenient and accurate. This is because the biometrics characteristic if an individual are unique and belongs to the personal until the user dead. It is convenient for the user because nothing to be carried or remembered and would not scare the ID card being stolen or password being hacked. From a technological perspective it is possible to distinguish between two broad types of ASR: Direct Voice Input (DVI) and Large Vocabulary Continuous Speech Recognition (LVCSR). These systems will analyze users' specific voice and use it to fine tune the recognition of that user's speech, resulting in more accurate transcription. For humans, speaking is the most natural form of communication. This thesis examines the problem of voice recognition and develops a voice recognition system for spoken words¹. Voice biometric technology is more accurate and convenient for user authentication. This is due to the fact that each person's biometric characteristics are distinct and remain their own until death. The user will find it convenient as there is nothing to carry or remember, and there is no risk of the ID card being stolen or the password being compromised. The two primary modules of the voice recognition system are feature extraction and feature matching. While feature matching entails the process of identifying the unknown user by comparing extracted features from admin voice input with those from a set of known users, feature extraction is the process of extracting a small amount of data from the voice signal that can later be used to represent each user.

- The password-based and ID/PIN-based security solutions in use today are susceptible to theft and hacking.
- Biometric systems were developed in response to the demand for a more secure technology.
- Passwords in biometric technology, particularly voice recognition, are made up of distinct personal characteristics.
- Since each person has a unique voice, speech recognition is thought to be safe for user identification.
- Voice biometrics reduce the possibility of password hacking and ID card theft while providing accuracy and ease.
- Biometric traits are unique for the duration of an individual's life.
- Direct Voice Input (DVI) and Large Vocabulary Continuous Speech Recognition (LVCSR) are two categories for voice recognition technologies.
- The study and creation of a voice recognition system for spoken words is the main goal of the thesis.
- The two primary modules of the system are feature matching and feature extraction.
- A tiny quantity of data is extracted from the spoken signal during feature extraction in order to represent the user.
- To ensure accurate identification, feature matching compares the traits retrieved from admin voice input with those of recognized users.

4 Literature Survey

Biometric Voice Recognition in Security System

Objectives	Design a voice recognition system using MATLAB for administrator authentication, focusing on MFCC and single-word recognition. Simulate the process to output recognition status.
Method Used	Utilize voice recording, silence detection, Hamming window smoothing, FFT for frequency domain transition, and MFCC for feature extraction. Implement dynamic methods (DTW, GMM), and VQ for mapping vectors. Simulate the entire system in MATLAB.
Limitations	Impact on accuracy due to speech energy variations, susceptibility to background noise, medium-level security, and potential vulnerabilities. Recognizes potential false recognitions or rejections, indicating room for improvements.

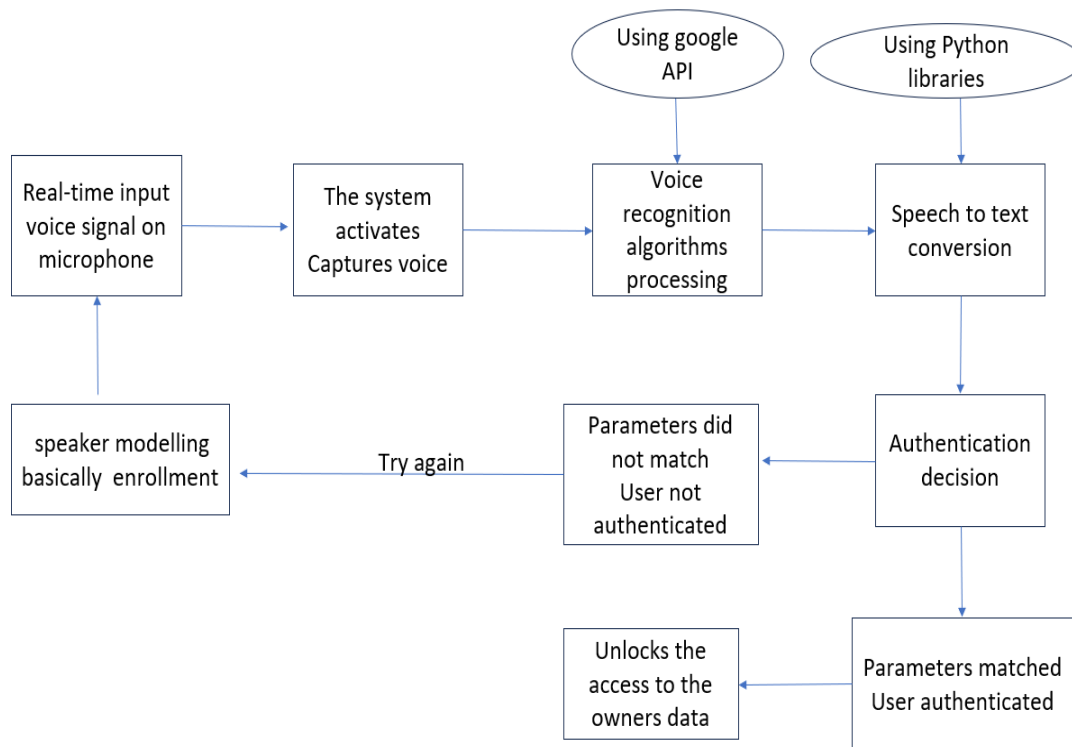
Table 1: Research Objectives, Methods, and Limitations

Implementation of Automated Door Unlocking and Security System

Objectives	By implementing a multimodal biometric security system for cars, the paper aims to enhance security by combining fingerprint and voice recognition. The system verifies the identity of users and allows access only to authorized individuals, sending alerts for potential intruders.
Method Used	The system employs fingerprint recognition using a module (R303) for enrollment and matching. Additionally, voice recognition is implemented using the EasyVR module, translating spoken words into a specific response.
Limitations	The limitations of the system include the potential for false rejections or acceptances during fingerprint and voice recognition. Factors such as noise, variations in voice tones, and environmental conditions may impact the accuracy of the system. In case of failure to authenticate, a buzzer is activated, and an alert message is sent to the car owner.

Table 2: Objectives, Methods, and Limitations of the Multimodal Biometric Car Security System

5 Block Diagram



6 References

- [1] Shah, H.N.M., Ab Rashid, M.Z., Abdollah, M.F., Kamarudin, M.N., Lin, C.K. and Kamis, Z., 2014. Biometric voice recognition in security system. Indian journal of Science and Technology, 7(2), p.104.
- [2] Madhusudhan, M., 2015. Implementation of automated door unlocking and security system. International Journal of Computer Applications, 975, p.8887.