iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53375

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Voice Recognition Based Money Transaction Using Stegnography

F. P. Jawalkar[1], A. K. Kamble[2], M. S. Khanolkar[3], M. A. Gangarde[4]
[1, 2, 3, 4]*Department of Electronics and Telecommunication, SavitriBai Phule Pune University*

Abstract: ***Security has been one of the most crucial challenges in today's environment when insecurity is widespread. Voice biometrics is a developing field in security, particularly for the purpose of authentication. Voice biometric speaker recognition utilizes the distinctive qualities of the human voice, including physiological and behavioural traits. These traits have the ability to identify a person and have distinct and relevant vocal features. This method also makes it possible to verify a user regardless of environment or channel changes. With the use of Machine Learning (ML), software can recognize voice and match it during authentication. Voice recognition is a part of speech recognition. A software system can match a customer's identification to their voice using voice recognition, a feature of AI. In this system, first the user has to register using their voice. After registration the user will log into their account. Then the user will select the person to whom the transaction is to be made and enter the amount to be transferred. Then the transaction will be successful. Here we will secure voice in the database at bank server. In this project, the main objectives are to use voice recognition for login, to use audio steganography for security purposes and to build a web application for the mentioned objectives.***
Keywords: Voice Authentication, Feature Extraction, MFCC, Audio Steganography

I. INTRODUCTION

With the rapid growth of mobile internet and smartphones, security shortcomings of mobile software and mobile data communication have shifted the focus to strong authentication. The existing user-id/password system is insufficient for mobile use since it is challenging to enter data on a small form factor device and there is a greater chance that the device may fall into the hands of unauthorized users, even though it works fine for desktops and laptops. Strong voice-based authentication in mobile situations has a lot of potential because of recent advancements in voice biometrics. This is especially relevant to the banking and finance sectors, as financial institutions are searching for solutions to provide flexible and simple authentication to mobile consumers while ensuring security and drastically lowering illegal usage [1]. The voice assistant revolution, led by Amazon's Alexa, Apple's Siri, Google Assistant, and others, has naturally led to voice-based payments [3].

Steganography is an intelligent data hiding technique where the secret data is embedded in a cover media in a way that the media carrying the secret message are undetectable and unnoticed by the intruder or attacker. There are 6 steganography techniques, as follows Text Steganography, Image Steganography

Audio Steganography, Video Steganography, DNA Steganography, and Network Steganography. In our system we are using Audio steganography. Audio steganography is a method of hiding information in an audio signal. When data is incorporated into the signal, it is modified. This modification must be made so that the human ear cannot distinguish it.

II. LITERATURE SURVEY

According to Mondal and Bours, biometrics is a method of providing identification using detectable physical properties [9]. It employs body traits as a tool to encode, scramble, or descramble data. Currently utilized biometric identification techniques include voice recognition, retina and iris scanning, palm prints, handwritten signatures, finger vein analysis, and facial anatomy. Biometrics is a practical answer in the struggle against fraud and theft, especially when it comes to the Internet, because the aforementioned characteristics are particular to each individual. Because biometric features are difficult to lose, hack, or duplicate, this sophisticated application is regarded to be superior to employing passwords or PINs. The idea is that you are your own password, based on these features. People misplace cards, misplace documents that have been countersigned, or write down PINs on pieces of paper so that others can access them. Using a part of yourself, a registered biometric identifier, that can be used to verify your identity is one way to protect data.

Mohammad Al Rousan and Benedetto Intrigila concluded that biometrics are able to achieve fast and easy-to-use authentication with high accuracy and a relatively low cost [2]. In this paper, the authors have tabulated a comparison of various biometric techniques based on various parameters. The voice biometric has a medium distinctiveness and a medium performance. But the issue is with the acceptance. People still think voice biometric is somewhat insecure. Biometrics, particularly voice biometric, in few years, use of money, credit cards, and checks will all be replaced by the use of biometrics. But it is important to be cautious about who can use the collected biometric data and for what purposes.

According to Nilu Singh, Alka Agrawal and R. A. Khan, voice based authentication goes through two different processes one after the other [7]. First is feature extraction and second is the model creation. Feature extraction uses techniques like MFCC and LPC. Different types of model creation include GMM, HMM, pattern matching, vector quantization, decision tree and neural networks. In this research paper, features like speaking rate, speaking style, pitch prosody is considered. These features are associated with linguistic components of voice such as syllables and it is noticeable that changes occur in measurable parameters, for example fundamental frequency F0, energy and duration of speech. This solution has many advantages like convenience, increased security and accuracy whereas the cost of implementation is high.

Sonali Goyal and Neera Batra compared the LPC and the MFCC technique for voice authentication systems. They concluded in their paper that the LPC technique is 89.23% accurate and the MFCC technique is 92.7% accurate [10].

According to Rohit Tanwar, Kulvinder Singh and Sona Malhotra [5], different finance firms as well as industry are relying on voice recognition authentication for their security. With the improvement in research for NLP, speech recognition can be used for disable people who are otherwise not able to authenticate themselves using traditional techniques

Hanlin Liu, Jingju Liu and Xuehu Yan [6] proposed an audio steganography scheme based on the time length of WeChat voice message, which is oriented to social network behavior. After chaotic scrambling and run length encoding, the secret information is encoded into run length, which then is mapped to time length that represents the secret data. The sender sends a voice message with corresponding time length, and the receiver extracts the secret information based on the time length of the voice message.

As per Dr. G. Sundari and Mrs. Alaknanda S. Patil [8], stenography is one of secure methods to transform secret data in wired or wireless communication. Though a variety of embedding methods are available for audio steganography the LSB embedding is the only method with lower computational difficulty but higher security by varying the secret data embedding position. The sturdiness can be again increased by introducing PN sequence generator and secret key.

Enas Wahab Abood et al developed a hybrid approach to protect a plain text message that was encrypted using the Hill encryption method and randomly distributed within an audio file using audio symbol signs to represent message bits [4]. The audio file can only be a *.wav stereo file, and two secret keys are required to decrypt the system and generate hiding spots. The findings of the calculation of PSNR, MSE, and SSIM between the cover before and after embedding reflected the system's imperceptibility criterion. Also, for various text sizes, the time required to secure messages was fairly low, and the encryption process took less time than hiding.

Ali M. Meligy, Mohammed M. Nasef and Fatma T. Eid offered an audio steganography algorithm for embedding text, audio, or images that is based on the Lifting Wavelet Transform (LWT) transform with modification of the Least Significant Bit (LSB) technique and three random keys. These keys are used to increase the robustness of the LSB technique because without them, no one would be able to determine the type of secret message, its length, or its initial position within the LSB. Performance of this algorithm is calculated by comparing the SNR [14].

M. Parthasarathi and T. Shreekala proposed an alternative strategy which focused on minimizing the distortion to the prediction error and the data size overhead [12]. This strategy is based on the prediction error that results from it and the challenge of handling the nonlinear quantization process. The advantage is that they achieve a lower distortion in the quality of audio while the disadvantages are that the data size increases during extracting and embedding. Also there may be a loss in the hidden data.

Based on this study, we compared Recognition Rates (as shown in Table I) for various feature extraction techniques for English language, English numerals and for Devanagari [15]

TABLE I
COMPARISION OF FEATURE EXTRACTION TECHNIQUES

Sr. no.	Technique	Language	Recognition rate
1.	Linear Predictive Analysis (LPC)	English	91.4%
		English Numerals	94%

Sr. no.	Technique	Language	Recognition rate
		Devanagari	82.3%
2.	Mel Frequency Cepstral Coefficient (MFCC)	English	99.9%
		English Numerals	92.93%
		Devanagari	85.3%
3.	Zero Crossing with Peak Amplitude (ZCPA)	English	96.67%
		English Numerals	95.4%
		Devanagari	38.5%

The analysis of different techniques of audio steganography based on some parameters like strengths, weaknesses, embedding technique, hiding rate have been discussed in this paper (Refer Table II). The study showed that the Least Significant Bit technique can be easily broken, while the phase encoding method is better in terms of security and signal manipulation.

TABLE II
COMPARISION OF AUDIO STEGANOGRAPHY TECHNIQUES

Methods	Embedding Techniques	Strengths	Weakness	Hiding Rate
Least Significant Bit	LSB of each sample in the audio is replaced by one bit of hidden information	Simple and easy way of hiding Information with high bit rate.	Easy to extract and to destroy.	16 Kbps
Echo Hiding	Embeds data by introducing echo in the cover signal	Resilient to lossy data compression algorithms.	Low security and capacity.	40-50 Bps
Phase Coding	Modulate the phase of the cover signal.	Robust against signal processing manipulation and data retrieval needs the original signal.	Low Capacity	333 Bps
Parity Coding	Break the signal into separate samples and embeds each bit from secret message in sample region parity bit.	Sender has more of a choice in encoding the secret bit.	Not Robust	320 Bps
Spread Spectrum	Spread the data over all signal frequencies.	Provide better robustness.	Vulnerable to time scale modification.	20 Bps

III. TECHNICAL APPROACH

In this project, we have used Convolution Neural Networks to authenticate users' voices. At first, the user will sign up or register using their voice. That voice will be stored in the database (here local storage for demonstration purpose).

After that the user needs to login using their voice. This time the voice will be matched with the previously stored voice in the database. Its characteristics like pitch, frequency, harmonic structure, intensity will also be compared with the previously stored voice. If the voice matches with their original data, then the user can login successfully into the application.

After successfully logging in, the user will select the person which he wants to pay. User will type the amount which he is going to pay. Then the amount will be transferred to another account.
The technical approach is summarized in Fig.1 given below

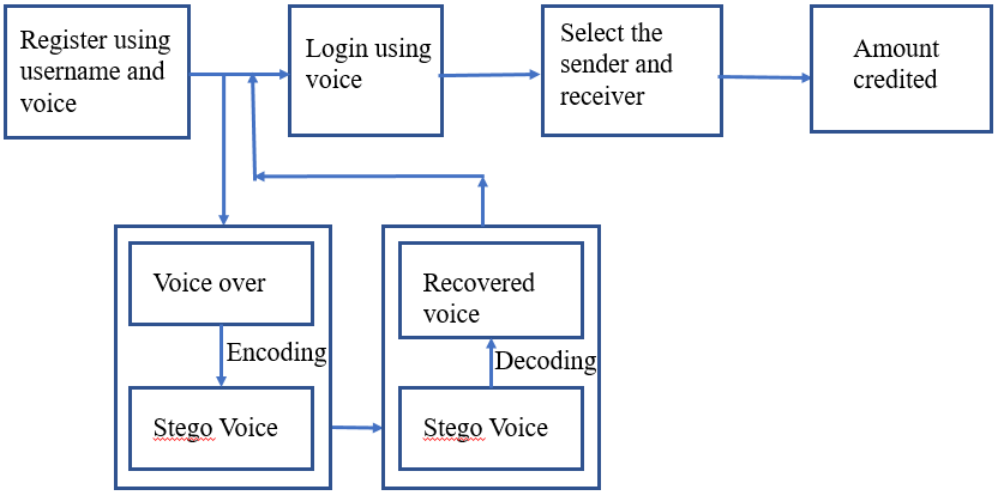


Fig.1. Block Diagram of Technical Approach

IV. CONCLUSION

This report proposes a voice recognition based application to transact money, using steganography for security. For voice authentication, we have used MFCC feature extraction technique which extracts features of a particular voice and GMM model. In voice recognition (voice matching and conversion), the system basically operates in two modes, i.e, training and recognition. In training mode, a new voice is included in the database, whereas in recognition mode, an unknown voice gives input signal, which the system tries to match and recognize. This system can be used both as identification and verification, using feature extraction.
For security, steganography is one of secure methods to transform secret data in wired or wireless communication. Though a variety of embedding methods are available for audio steganography, we have used the Phase Coding audio steganography method. We calculated the hiding rate for one audio and it came to be 2.9244e-05 bps. Also the SNR comes to be -0.0838dB. This is because the audio file is large and the text is small.

V. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our college especially our E&TC department for providing an opportunity to work on the project. We would like to convey our heartfelt gratitude to Dr. M. A. Gangarde for his tremendous support and assistance in the completion of survey paper of our project and constantly encouraging and guiding us throughout the semester without which completing out required project work in short span could not be possible. His initial guidance regarding the study of several research papers related to our project helped us a lot while completing our project.

REFERENCES

[1] Amjad Hassan Khan, M. K., & Aithal, P. S. (2022): "Voice Biometric Systems for User Identification and Authentication – A Literature Review". International Journal of Applied Engineering and Management Letters (IJAEML), 6(1), 198-209. DOI: https://doi.org/10.5281/zenodo.6471040
[2] Mohammad Al Rousan and Benedetto Intrigila (2020): "A Comparative Analysis of Biometrics Types: Literature Review". Journal of Computer Science, 16 (12): 1778.1788 DOI: 10.3844/jcssp.2020.1778.1788
[3] G. Yu. Peshkova, O. V. Zlobina (2020): "Digital transformation of banking with speech technologies". -ISSN: 2357-1330. ICEST. DOI: 10.15405/epsbs.2020.10.03.34
[4] Enas Wahab Abood et al (2020): "Securing Hill encrypted information With Audio steganography: a New Substitution Method", J. Phys.: Conf. Ser. 1591 012021
[5] Rohit Tanwar, Kulvinder Singh, Sona Malhotra (2019): "An Approach to Ensure Security using Voice Authentication System" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878
[6] Hanlin Liu, Jingju Liu, Xuehu Yan (2018): "Social Network Behavior-Oriented Audio Steganography Scheme" Eighth International Conference on Instrumentation and Measurement, Computer, Communication and Control

[7] Nilu Singh, Alka Agrawal, and R. A. Khan.(2018): "Voice Biometric: A Technology for Voice Based Authentication". Article in Advanced Science, Engineering and Medicine. DOI: 10.1166/asem.2018.2219

[8] Mrs. Alaknanda S. Patil, Dr. G. Sundari (2018): "An Embedding of Secret Message in Audio Signal" 3rd International Conference for Convergence in Technology (I2CT)

[9] Mondal, S., & Bours, P. (2017): "A study on continuous authentication using a combination of keystroke and mouse biometrics".

[10] Sonali Goyal and Neera Batra (2017): "Issues and Challenges of Voice Recognition in Pervasive Environment". Indian Journal of Science and Technology, Vol 10(30), DOI: 10.17485/ijst/2017/v10i30/115518.

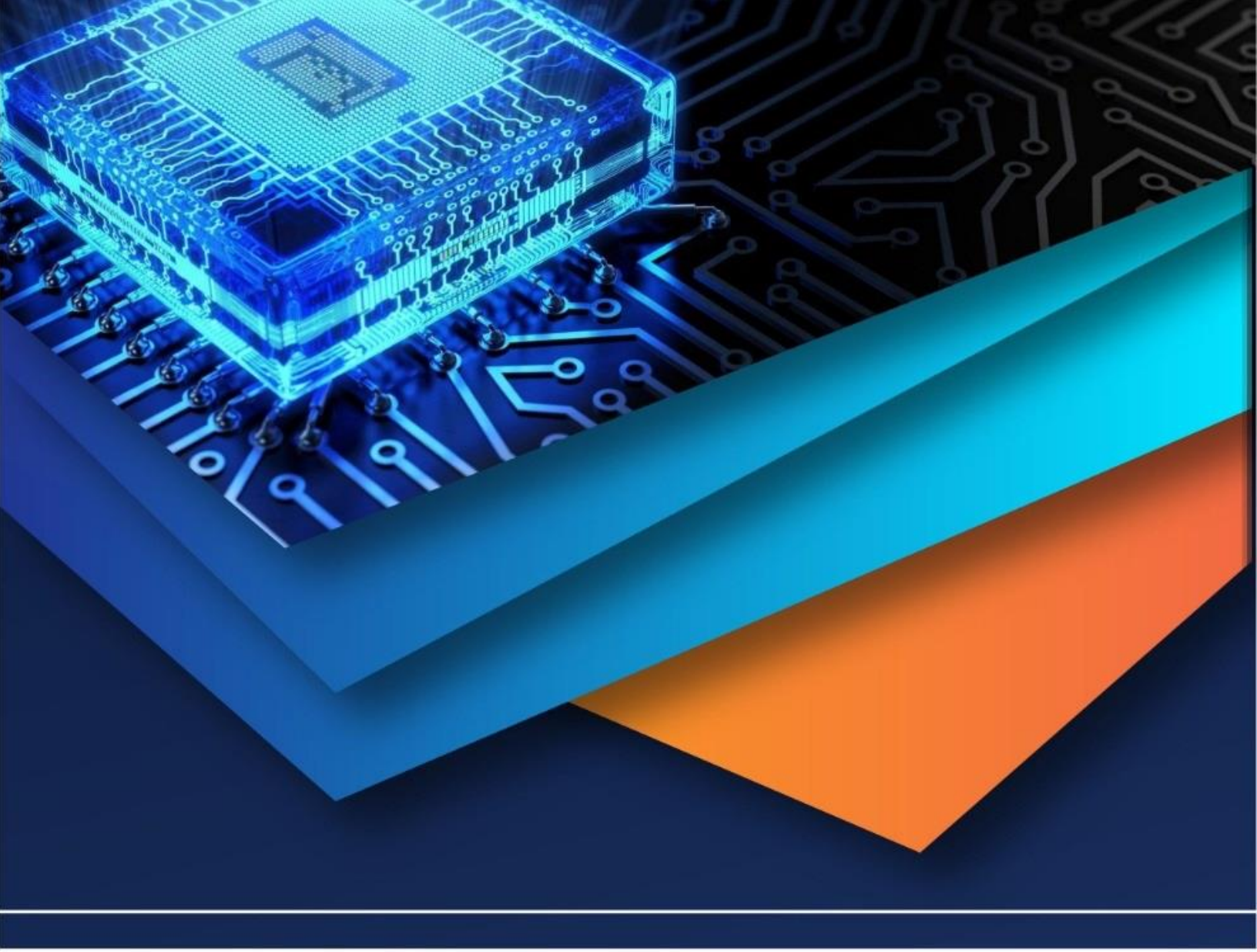
[11] Palwinder Singh (2016): "A Comparative Study of Audio Steganography Techniques" (IRJET)

[12] M. Parthasarathi and T. Shreekala (2017): "Secured Data Hiding in Audio Files Using Audio Steganography Algorithm", International Journal of Pure and Applied Mathematics Volume 116.

[13] Shweta Vinayakarao Jadhav, Prof. A.M Rawate (2016): "A New Audio Steganography with Enhanced Security based on Location Selection Scheme", IJESC.

[14] Ali M. Meligy, Mohammed M. Nasef and Fatma T. Eid (2015): "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys", I.J. Computer Network and Information Security.

[15] Pratik K. Kurzekar, Ratnadeep R. Deshmukh, Vishal B. Waghmare, Pukhraj P. Shrishrimal (2014): "A Comparative Study of Feature Extraction Techniques for Speech Recognition System". International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2319-8753, DOI: 10.15680/IJIRSET.2014.0312034



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY