International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SECURITY SYSTEM BASED ON VOICE AUTHENTICATION

Rohit Waykole[1]

[1]*Department of Electronics and Telecommunication,*
MIT College of Engineering, Pune, India.

ABSTRACT

Biometrics is a physical characteristic unique to each individual &more popular to identify people and authenticate them for access to secure areas and systems. This paper presents the security systems based on the voice biometrics. It describes the methods and algorithms used in the existing systems. The paper contains the architecture of the system, its functionality and method used to verify the speaker also the performance optimization methods of the implementation.Accuracy and the speed are two of the biggest factors taken into consideration while implementing the algorithms, so this paper summarizes the current efforts to overcome these problems and provide better accuracy and speed.

Keyword:access control,biometrics, security, speech recognition, voice authentication, etc.

I. INTRODUCTION

Biometrics has an extremely helpful application in security;it can be used to validate a person's identity and control access to a restricted area or electronic framework, in view of the start that sure of these physical qualities can be utilized to remarkably recognize people. All security frameworks that utilization client based approval oblige clients to be precisely distinguished to guarantee that the right get to benefits are conceded. Biometrics as an confirmation instrument is intense in light of the fact that not at all like different strategies as of now used to confirm individuals, for example, passwords or get to control identifications, it can't be effectively taken away, lost, falsified, or overlooked. There are several categories of biometrics: fingerprints, hand geometry, retina, iris, face, handwriting, and voice

It is conceivable to verify a user through three diverse methodologies: something that he knows, similar to a secret key i.e. password or a PIN, something that he has, similar to a key, or something that he is, biometric characteristics. The biometric frameworks are more basic on the grounds that since the client does not need to recollect the watchword or to fear losing it, "yet they are not secret. You leave your fingerprints on all that you touch, and your iris examples can be watched anyplace you look." [1].

The improvement of the biometric frameworks is firmly coupled to the IT advancements, and this is the motivation behind why today they are extremely utilized. There are countless strategies: unique mark, iris, signature, walk, hand geometry, voice, retinal example, and so forth. It is conceivable to recognize these qualities into principle fields: -

- **Physiological:** unique mark, iris, hand, confront;
- **Behavioral:** voice, signature, walk.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

As per their disparate quality they can be utilized as a part of various situations. In this paper, we will examine the biometric authentication using voice, specifying first of all how it works, the problems connected to its usage (like legal and privacy issues) and ultimately, the attack risks that such a system may suffer.

II.LITERATURE SURVEY

In literature, the problem and the previous techniques of voice authentication are described.

HairolNizam Mohd. Shah et.al.[2] introducedthe voice recognition algorithm is produced by utilizing MFCC technique to separate the element of the voice flag. The reference voice is being put away in preparing stage and contrast and the voice in testing stage to coordinate the both outcomes. The framework is effectively perceive the validate client's voice and rejected all the others impostor's voice. The yield result is separated into two classes which are acknowledged and dismisses. In the event that acknowledged, the Arduino will actuate the magnet door to unlock. On the off chance that the yield is rejected, the Arduino will remain the magnet entryway as bolt and the bell will caution for 1 second.

Scheffer et.al.[3] proposedan extra preferred standpoint of biometric speaker recognition frameworks is their capacity of performing remote verification by utilization of telephones on the other hand versatile applications, without the need of utilizing specific gear, barring the amplifier of the telephone. Voice biometrics are thought to be an exceptionally convenient and natural method for identity recognition.

Weiwu Jiang et.al.[4]proposed the different acoustic features, speaker displaying systems, session-changeability lessening strategies, and VAD plans have been utilized for individual systems. This procedure has prompted to a huge execution pick up when the subsystems were melded. In particular, the combination framework lessens the EER by 42% and min DCF by 56% when contrasted and the best individual subsystems. It was additionally found that the recently proposed FSH subsystem is integral to JFA and performs altogether superior to anything JFA when its projection frameworks were prepared by the sort of discourse that matches the evaluation conditions.

D. P. Munteanu.et.al.[5] introduced a programmed speech verification system was proposed in view of a nonstop discourse recognizer. In the preparing stage, are prepared two recognizers: one speaker dependent for the customer model and one speaker-free for the world model. Both recognizers have a similar structure what's more, number of parameters. In the check organize, for the input state, they are playing out a constrained arrangement Viterbi system. A standardized acoustic score is acquired and contrasted and an edge for acknowledgment choice. The trial comes about uncover that the strategy proposed here can acquire mistake rates under 1%.

A. Larcher, J. F.et.al.[6] introduced the new method is designed for embedded applications. It takes favorable circumstances of a GMM/UBM content autonomous approach and the HMM/Viterbi speech recognition control. Execution of our approach is proportional to the GMM/UBM gauge framework when not considering the phonetic substance (case of EER in KNOWN condition, GMM: 4.49, EBD4.56) though the proposed approach beats the GMM/UBM when impostors don't have the foggiest idea about the customer expression (EER in UNKNOWN condition, GMM: 0.87, EBD: 0.56).

H. S. Mohammadi and R. Saeidi, et.al.[7]proposed a novel GMM structure called sorted GMM is presented which is profited from a fast scoring capacity while its memory prerequisite is quite recently hardly higher than

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

customary GMM. Additionally, the preparation and streamlining plans of GMMs for the proposed strategy are portrayed. The utilization of the proposed strategy in speaker confirmation system is laid out. The execution of a speaker confirmation framework in light of the new strategy was contrasted and other GMM based speaker confirmation frameworks tentatively. The after effects of tests demonstrate that the streamlined sorted GMM presents an attractive execution and it outflanks the as of now known SBM-SGMM which itself gives an adequate execution for quick scoring GMMs while its computational cost is not as much as that of the SBM-SGMM.

III. PROPOSED SYSTEM

There are three different types of methods for the voice verification operation: text-dependent speaker verification, text-prompted speaker verification and text-independent speaker verification.

The method used in this paper is text-dependent speaker verification in which the detected identity is always confirmed by the use of already decided pass-phrase. This is highly convenient method with large practical potential.

1. Speech Processing in Embedded System

Speech has specific set of requirements and ergonomics. The most important requirement is to retain the short and constant voice over the different environments.

It is necessary that physical parameter must fulfill the minimum requirements i.e. the bandwidth of the signal must be between 300Hz – 3.7 KHz.

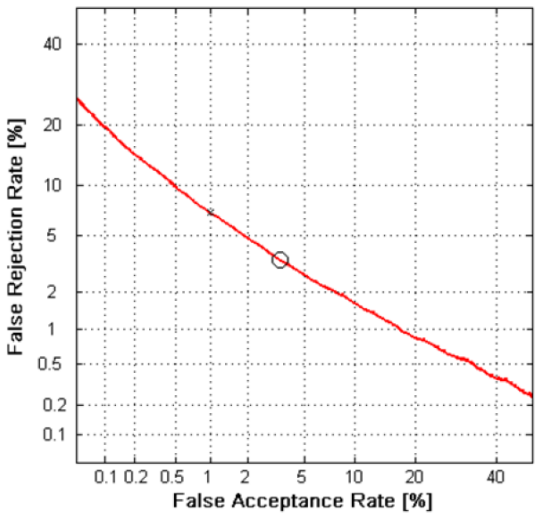

Fig: DET curve acquired for the speaker verification system

2. Architecture of the System

The architecture of the system follows the EN 50133-1:1996 standard [9]. The system architecture of the proposed method is shown in below. It accepts the two inputs, one for the identification of the user and second for the authentication purpose.In this prototype, a RFID tag is used for the identification and the speech recognition is used for the authentication the user.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

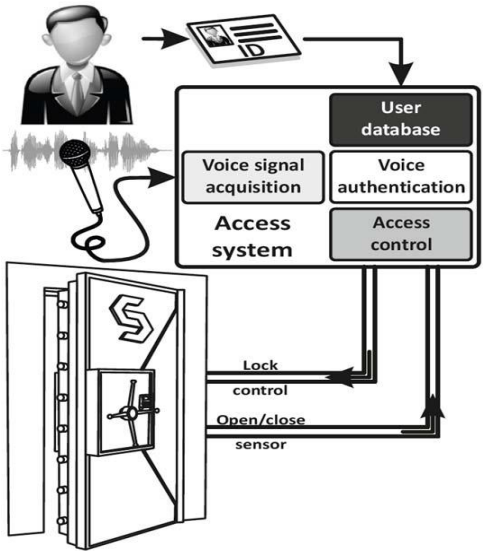

Fig: System Architecture

3. Voice acquisition and processing

Initially we have to store the pre-determined pass-phrase in the system memory. Then for identification procedure, the user has to scan his RFID tag at the RFID reader. After the successful identification, user will be asked to utter the password i.e. his personal pass-phrase which is already store din database. The system will compare both and will send the further signal to grant access or not.

The parameterization is done in real-time by use of audio buffer. Once the buffer is full, the contents are subjected to the MFCC parameterization. In order to avoid the loss of data, time limit is followed for processing particular no. of elements.

The resulting MFCC matrix is used for the further processing. A final result of voice signal parameterization can be seen in fig.

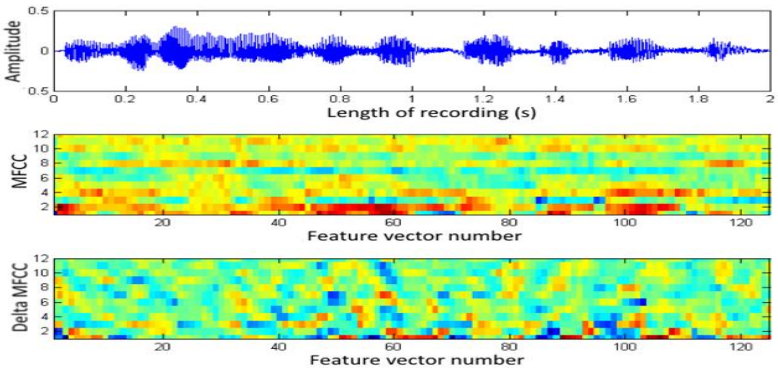

Fig: A recording of pass phrase with its MFCC and delta MFCC parameters

The system contains a few modules, the undertaking of which is to be up to standard. The most vital piece of the whole framework is the Access Control Module, which forms all of the information got by the framework. Alternate modules guarantee the outside correspondence, information enrollment and legitimate capacity of the User Database. It additionally takes into account productive handling of computerized signs on account of an inherent skimming point co-processor. The execution of the committed openly accessible continuous working

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

framework controls the work of the considerable number of peripherals, and additionally preparing the obtained biometric information, and permitting the correspondence with an outer gadget in a local area network.

IV. CONCLUSION

The described project of voice authentication for security system is an attempt to obtain the better results whileprocessing the voice signal regardless of the surrounding environment for the accurate recognition of the user.It gives better results as compared to the existing system.The accuracy of the system is about 75%. Sometimes due to the high disturbance in the background, the system does not identify the user. The accuracy of the system can be increased by modifying the algorithm, so there is scope to improvement to the system which can be considered as future work.

REFERENCES

Journal Papers:

[1] Jakub Gałka et al, "Voice Authentication Embedded Solution for Secured Access Control"In*IEEE Transactions on Consumer Electronics, Vol. 60*, No. 4, November 2014

[2]Hairol Nizam Mohd. Shah*,Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, Chow Kok Lin and Zalina Kamis "Biometric Voice Recognition in Security System "Indian Journal of Science and Technology, Vol 7(2), 104–112, February 2014

[3]Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition*, Columbus, USA, pp. 1891–1898, Jun. 2014.

[4]N. Scheffer, L. Ferrer, M. Graciarena, S. Kajarekar, E. Shriberg, andA. Stolcke, "The SRI NIST 2010 speaker recognition evaluation system," *in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Pros.*,Prague, Czech Republic, pp. 5292–5295, May 2011.

[5] Weiwu Jiang , Man-Wai Mak , Wei Rao and Helen Meng The Hkcupu System For The Nist 2010 Speaker Recognition Evaluation 1978-1-4577-0539-7/112011 IEEE 5288 ICASSP 2011 pp. 5288-5291

[6]D.-P. Munteanu and S.-A. Toma, "Automatic speaker verification experiments using HMM," in *Proc. IEEE 8th InternationalConference on Communications*, Bucharest, Romania, pp. 107–110, Jun. 2010.

[7]A. Larcher, J.-F. Bonastre, and J. S. Mason, "Short utterance-basedvideo aided speaker recognition," in *Proc. IEEE 10thWorkshopon Multimedia Signal Processing*, Cairns, Australia, pp. 897–901, Oct. 2008.

[8]H. S. Mohammadi and R. Saeidi, "Efficient implementation of GMM based speaker verification using sorted Gaussian mixture model," *in Proc. European Signal Processing Conf. EUSIPCO*, Florence, Italy, Sep. 2006

9] "European Standard EN 50133-1: Alarm systems Access control systems for use in security applications. Part 1: System requirements," EN 50133-1:1996/AC: 1998/A1:2002, Technical Body CLC/TC 79, European Committee for Electro technical Standardization, 2002.