OPINION

Access control system design and implementation using open source personality identification software

Stuard Sem

Sem S. Access Control System Design and Implementation Using Open Source Personality Identification Software. J Biomed Eng: Curr Res. 2022; 4(2):10-11

ABSTRACT

The most important feature of any door locker security system is the ability to verify the identification of everyone entering via that door. Instead of surveillance equipment that need passwords or pin codes, biometric traits such as distinctive characteristics in people's faces and voice signals can be used to authenticate them. These traits are difficult to modify, copy, or steal. To achieve high accuracy, double biometrics, which include facial recognition and speech recognition algorithms, can be used concurrently to increase security. This system is designed to prevent theft in high-security facilities such as the house house, bank, and other locations by detecting strangers and securing door lockers. This system is tested in a Windows environment before being modified to a Unix environment when running on the Raspberry Pi 3 platform using Python. Raspberry Pi electronic board is a single-board computer that runs on battery power and has wireless internet connectivity through USB modem. It also has connections for a camera, microphone, LED, and a 12 volt door lock. When a person steps in front of the door, the Raspberry Pi's camera and microphone are used to validate the individual's facial image and voice signal to decide if they are legitimate or imposters. The system will unlock the door after the individual has been authenticated. Otherwise, it will sound an alert and snap a photo of the impostor, which it will then email to the authorised person.

INTRODUCTION

The recently, there has been a pressing need to improve present items and technologies to make them smarter and easier to use. Especially now that the phrase "smart house" has been widely utilised. Furthermore, as security risks grow, conventional procedures, particularly those relating to the door locker, become increasingly important. To increase the security of any item, it is necessary to address its current flaws and provide additional capabilities. The biggest disadvantage of the present door locker is that anybody may unlock it by stealing or copying the key. Friends and relatives, on the other hand, will not be able to open this door and enter the house unless they have the key (or know the pin code or password). As a result, to address this problem, simply convert traditional door lockers to smart lockers that use biometric modalities. Many biometric modalities exist, including voice, face, fingerprint, retina, and iris. In terms of accuracy, robustness, and usability/user adoption, each modality has its own set of benefits and drawbacks. For example, utilising iris data gives excellent accuracy and robustness, but it has limited usability and user acceptability. In contrast, modalities with better user acceptability, such as face and voice (the modalities of concern in this article), have limited application due to robustness and accuracy issues. Real-world systems incorporating these modalities are necessary.

Uni-biometric systems suffer from limitations such as the lack of uniqueness and universality of the selected biometric characteristic, noisy data, and spoof attacks. Multi-biometric systems use data from many biometric modalities to improve recognition performance and overcome other restrictions that uni-biometric systems encounter Sensor, feature, match score, and decision levels are the four levels of information that makeup fusion. Fusion is achieved at the decision level in this study using the (AND) operator for both face and speech recognition. In the literature, numerous distinct strategies for fusing the face and speech modalities have been described Because the suggested system is based on biometrics and combines face and voice recognition, it will increase security level accuracy and efficiency over a single biometric recognition system. The construction of an access control system based on a fusion modal for multimodal face and speech biometric characteristics is presented in this study. Face features are recovered using the Local Binary Patterns (LBP) technique, while voice characteristics are extracted using Mel Frequency Cepstral Coefficients (MFCC) features. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are used to assess performance (FRR). This paper's rest is divided into the following categories: The suggested system, which includes a Raspberry Pi 3 model b+ and a block diagram comprising the two biometrics, is reviewed in section III, which includes a literature study of earlier works and articles related to this work. Section III explains the appro-

Managing Editor, Journal of Biomedical Engineering: Current Research, Berkshire, UK

Correspondence: Stuard Sem, Managing Editor, Journal of Biomedical Engineering: Current Research, Berkshire, UK. e-mail biomedical@theresearchpub.com

Received:- 15 March, 2022, Manuscript No. pulbecr-22-4928; Editor assigned:- 17 March, 2022, PreQC No. pulbecr-22-4928 (PQ); Reviewed:- 04 April, 2022, QC No. pulbecr-22-4928 (Q); Revised:- 11 April, 2022, Manuscript No. pulbecr-22-4928; Published:- 13 April, 2022; DOI:-10.37532/ pulbecr.22.4(2).10-11

-ach, covering the stages involved in face recognition and speech recognition, as well as the algorithms utilised to implement these biometrics.The suggested system's discussion and results are detailed in Section V. The biometrics fusion of face and voice based on door lockers are implemented using Raspberry Pi 3 in this study. Raspberry Pi is a single-board computer created by the RASPBERRY PI foundation in the United Kingdom to improve computer science education in schools and underdeveloped nations as a result, this Raspberry Pi embedded system will regulate access based on the entered person's face and voice information.