Human Authentication using Face, Voice and Fingerprint Biometrics

Dr. Dinesh Kumar D S[1], Dr. Rajesh L[2], Prof. Ayaz Pasha S[3]
[1]Associate Professor, Telecommunication Engineering, K S Institute of Technology, Karnataka, India [2]Associate Professor, Electronics & Communication Engineering, East point college of Engineering & Technology, Karnataka, India
[3]Assistant Professor, Electronics & Communication Engineering, East point college of Engineering & Technology, Karnataka, India

***Abstract*— Multimodal biometric approaches are growing in importance for personal verification and identification, since they provide better recognition results and hence improve security compared to biometrics based on a single modality. In this project, we present a multimodal biometric system that is based on the fusion of face, voice and fingerprint biometrics. For face recognition, we employ Haar Cascade Algorithm, while minutiae extraction is used for fingerprint recognition and we will be having a stored code word for the voice authentication, if any of these two authentication becomes true, the system consider the person as authorized person. Fusion at matching score level is then applied to enhance recognition performance. In particular, we employ the product rule in our investigation. The final identification is then performed using a nearest neighbour classifier which is fast and effective. Experimental results confirm that our approach achieves excellent recognition performance, and that the fusion approach outperforms biometric identification based on single modalities.**

***Keywords*— Fingerprint, Authentication, Multimodal Biometrics, Register, PIN, LBP.**

I. INTRODUCTION

In recent years, identity authentication has become increasingly important. People are required to be verified or identified as a valid claimed individual to be able to access ATMs, airports, labs, buildings, files, etc. Traditionally, authentication knowledge-based (e.g. password or personal identification number (PIN)) and token-based (e.g. ID card or key) methods are commonly used. However, these traditional methods are of high risk for many critical security applications, since a password may be forgotten or hacked, or an ID card may be lost or stolen.
Biometrics enable an identity-based method which can provide sufficient security for these applications. Biometric recognition refers to the automatic identification of an individual based on physiological and/or behavioral characteristics. Currently, biometric systems make use of fingerprints, voiceprints, face characteristics, facial thermo grams, iris features, retina images, hand geometry, palm prints, signature, etc. Biometrics cannot be forgotten, borrowed, stolen and forging is practically impossible. Authentication systems operate either in identification mode or verification mode. In identification mode, a potentially very large database is searched and the individual corresponding to the top match score returned.

For verification, the match must be sufficiently high when the test input is matched to the claimed identity. Despite recent advances, biometric systems still have problems in many real world applications. Some biometrics may be non-universal (e.g. about 2-4% of the population do not have adequate quality fingerprints for authentication but this percentage differs according to databases), while some modalities are fragile or weak (e.g. a voiceprint in a noisy environment or a face image under illumination and pose variations). An approach to overcome these problems is to perform authentication using several biometrics to provide a more robust system. This is known as multimodal biometrics, which combine multiple sources of information to establish identity. Multimodal biometric systems can integrate information at various levels. Most often, multimodal biometric fusion is performed at matching- score level. This can be achieved through a variety of methods, e.g. simple sum, weighted sum, min / max rules, etc. Fingerprints and faces are widely used in biometrics research studies as well as in commercial applications, due to the easy data acquisition and relatively low costs. Many researchers have used these biometrics, with some considering the quality score of the fingerprint when fusing results.

II. LITERATURE REVIEW

With respect to the paper [1] Biometrics manages the computerized acknowledgment of people dependent on natural and social attributes. The example acknowledgment framework perceives an individual by deciding the credibility of a particular conduct normal for person. The primary rule of biometric framework is recognizable proof and check. A biometric confirmation framework use fingerprints, face, hand geometry, iris, and voice, mark, and keystroke elements of a person to recognize an individual or to check a guaranteed character. Biometrics authentication is a form of identification and access control process which identify individuals in packs that are under reconnaissance. Biometric security system increase in the overall security and individuals no longer have to deal with lost ID Cards or forgotten passwords. It helps much organization to see everyone is at a certain time when something might have happened that needs reviewed. The current issues in biometric system with individuals and many organization facing are personal privacy, expensive, data's may be stolen.

According to the paper [2] This paper presents a reliable and secure authentication system. It deals with voice, face & fingerprint recognition algorithms to achieve better performance. This means that this system will optimize the security performance. A 3 tier architecture is proposed and implemented with the help of biometric modalities. The security is provided by the combination of voice, face & fingerprint authentication

by achieving 3 tier architecture. The performance of different biometric modalities is found to be quite secure.

According to the paper [3] A perennial need for safety in the community depends on country, city, and district. In some instances, feeling safe is required on a 24/7 basis. A popular and cost-effective solution based on the Raspberry Pi has the promise of being both user-friendly and cost effective. It pairs the Raspberry Pi to a camera module for face recognition. It learns to detect those with granted access to the specified area under protection. Such stored faces are the subject of system training. If during operation the system recognizes the face in the dataset, then the camera shows the matching name with a confidence level possibly granting access, but alternatively it takes a photo of the subject and sends it as an email notifications warning. The proposed system can implement face recognition even from poor quality images performing well over both known and unknown datasets. Face recognition leverages techniques from the OpenCV library and is written in the Python language.

According to the paper [4] Voice authentication is very perspective technology. It doesn't need any special biometrical devices, like finger scanner or face detector. It can be use in any place and in any channels. Our algorithm can help to recognize person by special digital voice portrait. It can be use in direct stream and in real time. It can also use in On-Board telecommunication components.

III. METHODOLOGY

A. Proposed Model

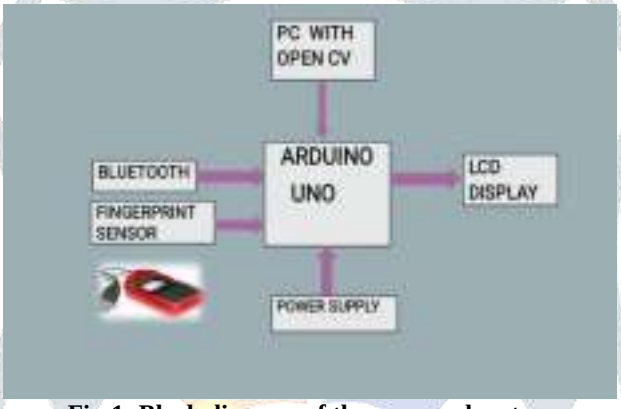


Fig-1: Block diagram of the proposed system

In this Section for Face recognition we have used Haar Cascaded Algorithm this Authentication stores in the computer Vision. Voice recognition we have used a device called Bluetooth, this module is connected to Arduino uno board. Fingerprint sensor will be connected to Arduino uno board. Through sensor will be connected to laptop and another end is connected to Arduino uno board. Power supply will be given. In 3 layer authentication, if we get 2 condition satisfy it leads to be valid output. Resulted output can be seen in LCD display.

B. Flowchart of Proposed Model

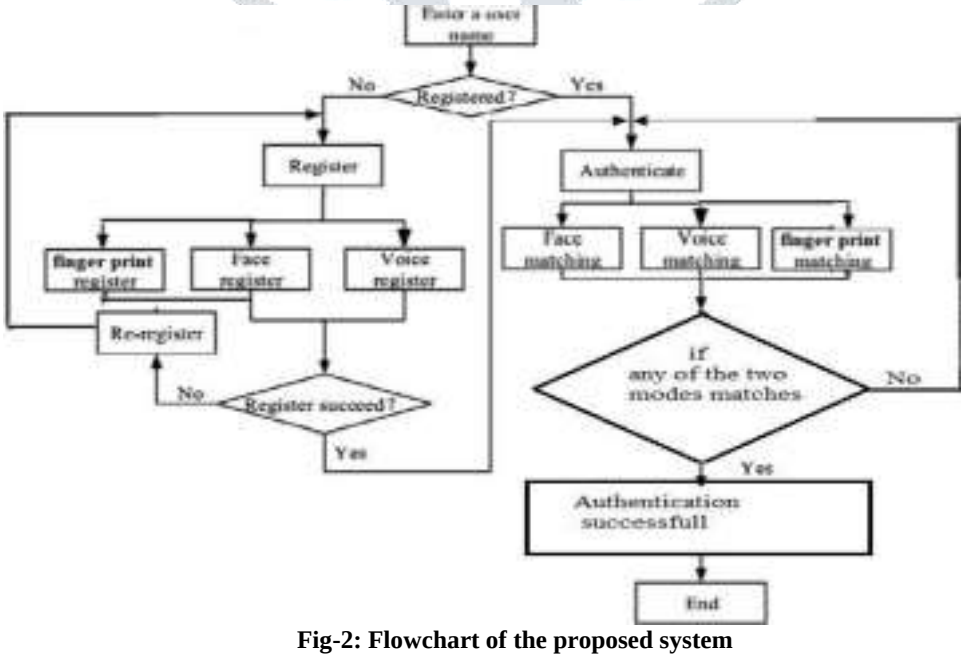


Fig-2: Flowchart of the proposed system

In this section we present our proposed algorithm that combines fingerprint and FACE technology for authentication. The proposed algorithm first scans the fingerprint, process and save its image Database. It then scans the FACE of the user, process and save its image pattern in the Database. When the user tries to access the system for authorization, the user will have to put the biometric 1 (Fingerprint). The fingerprint will be scanned, processed to obtain its pattern. The obtained pattern will be matched with the one saved in the smart home server using hamming distance. If the patterns match each other, the system will let the user enter the second Authorization stage, which is authorization with FRT.

The user will stand in front of the camera whereby his FACE will be scanned and processed to obtain its unique patterns. The patterns will be compared with the ones in Database, whereby if the patterns match, then the user will be Authorized. We also proposed a voice authentication system which detects the particular key word. The key word through voice will be stored in a system and the system checks for the same key word given by the user through voice. If the voice key word matches with the stored key word , the system consider him as a known person. In these three authentication methods the system will consider maximum of two. However, if two of the authentication mechanism fails the user will be Unauthorized.

IV. HARDWARE REQUIREMENTS

1) Arduino

Fig-3: Arduino UNO Board

Arduino Uno is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to DC adapter or battery to get started. The Uno board is the first in a series of USB Arduino boards.

2) Fingerprint module

Fig-4: Fingerprint Sensor

This is a finger print sensor module with TTL UART interface. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The way an optical scanner works is by shining a bright light over your fingerprint and taking a digital photo. The light-sensitive microchip makes the digital image by looking at the ridges and valleys of the fingerprint, turning them into 1's and 0's, and creates the user's own personal code.

3) Power Supply

FIG-5: Power Supply

There are many types of power supply. Most are designed to convert high voltage AC mains electricity to a suitable DC voltage supply for electronic circuits and other devices. A power supply can by broken down into a series of blocks, each of which performs a particular function. DC voltages are required to operate various electronic equipment. These voltages are 5V, 9V or 12Vwhich cannot be obtained directly. Thus, the input to the circuit is applied from the RPS.

4) LCD Configuration

Fig-6: LCD Configuration

The Liquid-crystal display (LCD) 44780 standard requires 3 control lines as well as either 4 or 8 I/O lines for the data bus. The user may select whether the LCD is to operate with a 4-bit data bus or an 8-bit data bus. If a 4-bit data bus is used the LCD will require a total of 7 data lines (3 control lines plus the 4 lines for the data bus). If an 8-bit data bus is used the LCD will require a total of 11 data lines (3 control lines plus the 8 lines for the data bus).

5) Bluetooth Module

Fig-7: Bluetooth module

HC-05Specification: Bluetooth protocol: Bluetooth Specification v2. Frequency:2.4GHz ISM band. Modulation: GFSK(Gaussian Frequency Shift Keying) Emission power: ≤4dBm, Class 2. Sensitivity: ≤-84dBm at 0.1% BER. Speed: Asynchronous: 2.1Mbps(Max) / 160 kbps, Synchronous:1Mbps/1Mbps. Security: Authentication and encryption.

V. INTERFACING OF COMPONENTS

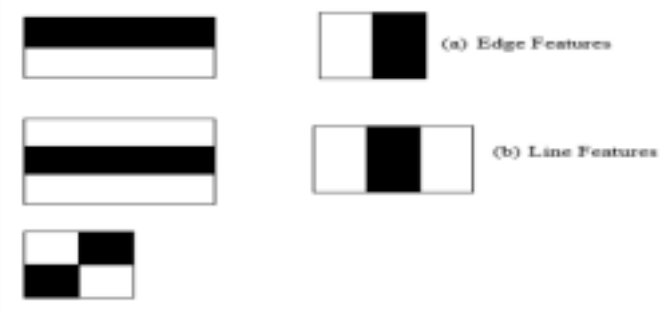
A. Face Recognition

1) Open CV: OpenCV abbreviated as open source computer vision is a library with functions that mainly aim real-time computer vision. With OpenCV one can perform face detection using pre-trained deep learning face detection model which is shipped with the library OpenCV is written in C++ and its primary interface is in C++, but it still retains a less comprehensive though extensive older C interface.

2) Algorithm: The Haar cascade algorithm is the machine learning object detection algorithm used to identify objects in an image or video based on the concept of features.

3) Haar Feature Selection: Haar like Features are the digital image features used in object recognition. Haar feature selection is a cascade

classifier. Initially the algorithm needs to train with lots of positive (images of face) and negative (images without face) images to train the classifier. Then the feature is extracted from it. For this, haar features shown in below fig(8) are used.



(c) Four-rectangle

FIG-8: Three different Haar features

Fig-9: Face detection

The user will stand in front of the camera whereby his/her FACE will be scanned and processed to obtain its unique patterns the fig shown in above(9). It then scans the FACE of the user, process and save its image pattern in the Database. The patterns will be compared with the ones in Database, whereby if the patterns match, then the user will be Authorized. The proposed algorithm first scans the fingerprint, process and save its image Database.

Fig-10: 100 samples of detected face

If the positive region is detected then it considers that the object is found and passes it on to the next stage. If the negative region is detected then the sliding window considers the next smaller region of the image. After the classifier passes the region to the next stage fig shown in above(10). The detector reports an object found at the current window location when the final stage classifies the region as positive.

B. Fingerprint recognition

This is the type of biometric security that uses the human fingerprint and compares its patterns for identifying a person. using fingerprint-capturing device a user's fingerprint image is captured and saved in the database. In authentication process, the user places his hand on the fingerprint-capturing device whereby it captures his image and compares with the one in the database the fig shown in below(11). If matches then access is granted.

Fig-11: Enrolling of Fingerprint

Fingerprint recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints. It is the most used biometric solution for authentication on computerized systems.

C. Voice or Speech Recognition

Voice or speech recognition is the ability of a machine or program to receive and interpret dictation or to understand and carry out spoken commands fig shown in below(12). In our opinion, and in the opinion of many experts, voice biometrics, for the time being, should be used in addition to other more proven authentication methods. For example, combining voice and facial identification is already an avenue being explored by many players.

Fig-12: Pairing of Bluetooth and Voicebot

voice interaction is a part of all our uses and biometrics in the authentication sense because it is the most inherent subject in the technology.

Fig-13: Voice recognition

Speech recognition software works by breaking down the audio of a speech recording into individual sounds, analyzing each sound, using algorithms to find the most probable word fit in that language, and transcribing those sounds into text fig shown in above(13) Voice interaction.

VI. Results

Fig-14: Experiment Setup

The proposed algorithm first scans the fingerprint process and save its image Database. It then scans the FACE of the user, process and save its image pattern in the Database.When the user tries to access the system for authorization,the user will have to put the biometric 1 (Fingerprint).The fingerprint will be scanned, processed to obtain its pattern.The obtained pattern will be matched with the one saved in thesmart home server using hamming distance. If the pattern smatch each other, the system will let the user enter the second Authorization stage, which is authorization with FRT. The user will stand in front of the camera whereby his FACE will be scanned and processed to obtain its unique patterns. The patterns will be compared with the ones in Database Fig(14), whereby if the patterns match, then the user will be Authorized.

We also proposed a voice authentication system which detects the particular key word. The key word through voice will be stored in a system and the system checks for the same key word given by the user through voice. If the voice key word matches with the stored key word , the system consider him as a known person.

A. Fingerprint Biometric Authentication

The type of biometric security that uses the human fingerprint and compares its patterns for identifying a person. using fingerprint capturing device a user's fingerprint image is captured and saved in the database. In authentication process, the user places his hand on the fingerprint capturing device whereby it captures his image and compares with the one in the database. Fingerprint matches the person is authorized person fig shown below(15).

Fig-15: Fingerprint Recognition

B. Voice Biometric Authentication

Voice recognition software works by breaking down the audio of a Voice recording into individual sounds, analyzing each sound, using algorithms to find the most probable word fit in that language, and transcribing those sounds into text shown in the fig(18) below. We also proposed a voice authentication system which detects the particular key word. The key word through voice will be stored in a system and the system checks for the same key word given by the user through voice. If the voice key word matches with the stored key word , the system consider him as a known person shown in the fig (19) below.

Fig-16: Phonemes (transcribing Speech to text process)

Fig-17: Voice Recognition

C. Face Biometric Authentication

A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces and employed to authenticate users through ID verification services, works by pinpointing and measuring facial features shown in fig(16) from a given image.

Fig-18: Face Recognition

The user will stand in front of the camera whereby his FACE will be scanned and processed to obtain its unique patterns. The patterns will be compared with the ones in Database, whereby the pattern is matched, the user has been Authorized shown in the fig(17).

Fig-19: The User Authentication Process

✓ Face Detection Accuracy Computed as:

$$\textbf{accuracy} = \frac{\text{\textbf{\textit{\textbf{\textit{\textbf{\textit

VIII. ACKNOWLEDGEMENT

First of all, we would like to thank Head of Mechanical Engineering Department, to give us the opportunity to work on this project. We wish to express our sincere gratitude to our guide for his kind guidance and valuable suggestions without which this proposed work would not have been taken up. We sincerely acknowledge the encouragement, timely help and guidance given to us by our beloved guide to carry out this proposed work within the stipulated time successfully.

REFERENCES

[1] M. Sivaram, Mohamed Uvaze Ahamed A, D. Yuvaraj, G. Megala, V. Porkodi, Manivel Kandasamy,"Biometric Security and Performance Metrics: FAR, FER, CER, FRR", 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE).

[2] Manabhanjan Pradhan, Chittaranjan Pradhan, Bhabani Shankar Prasad Mishra, Aditya K, "Authentication Using 3 Tier Biometric Modalities", 2018 International Conference on Communication and Signal Processing (ICCSP).

[3] Ibrahim Mohammad Sayem, Mohammad Sanaullah Chowdhury,"Integrating Face Recognition Security System with the Internet of Things" 2018 International Conference on Machine Learning and Data Engineering (iCMLDE).

[4] S.V.Melnik, N. I. Smirnov, "Voice Authentication System for Cloud Network" 2019 Systems of Signals Generating and Processing in the Field of on Board Communications.

[5] Abu Taher Noman, Samzad Hossain, Shariful Islam, Mohammad Emdadul Islam, Nawsher Ahmed, M A Mahmud Chowdhury, "Design and Implementation of Microcontroller Based Anti-Theft Vehicle Security System using GPS, GSM and RFID" 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT)**.**

[6] S. Niket Borade, Ratnadeep R , Deshmukh, and Sivakumar Ramu "Face Recognition using Fusion of PCA and LDA" Borda Count Approach‖, 24th Mediterranean Conference on Control and Automation, IEEE, 2016, Athens, Greece, pp. 1164-1167.

[7] R.Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, "IoT Based Smart Security and Home Automation System", International Conference on Computing, Communication and Automation, IEEE, Noida, India, 2016, PP 1286- 1289.

[8] S. Gunputh, Anshu Prakash Murdan, Vishwamitra Oree, "Design and Implementation of a Low-Cost Arduino-Based Smart Home System" International Conference on Communication Software and Networks, DOI: 10.1109/ICCSN.2017.8230356, IEEE, Guangzhou, China, 2017, pp.1491-1495.

[9] Mohammad javad Ghorbani, Mahdi Alizadeh, Alireza Esfahani Omran, Morteza Modarresi Asem, "An Investigative Review of Human Authentication Based on Fingerprint" 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).

[10] B. M. Mohammad El-Basioni, Sherine M. Abd El-kader, and Mahmoud Abdelmonim Fakhreldin, "Smart Home Design using Wireless Sensor Network and Biometric Technologies‖" International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 3, March 2013, pp. 413-42.