IoT Based Multimodal Biometric

Pooja N Kulkarni[1], Rajendra M[2]

[1]Pooja N Kulkarni :Student, Dept of Computer Science and Engineering Atria Institute of Technology, Bengaluru, Karnataka, India

[2]Rajendra M:Professor, Dept of Computer Science and Engineering, Atria Institute of Technology, Bengaluru, Karnataka, India.

Abstract - Biometric authentication may be a promising approach to securing the web of Things (IoT). Although existing research shows that using multiple biometrics for authentication helps increase recognition accuracy, the bulk of biometric approaches for IoT today still depend on one modality. We propose a multimodal biometric approach for IoT supported face and voice modalities that's designed to scale to the limited resources of an IoT device. Our work builds on the muse of Gofman et al. in implementing face and voice feature level fusion on mobile devices. We used discriminant correlation analysis (DCA) to fuse characteristics from face and voice and used the K-nearest neighbors (KNN) algorithm to classify the characteristics. The approach was implemented on the Raspberry Pi IoT device and was evaluated on a dataset of face images and voice files acquired using a Samsung Galaxy S5 device in real-world conditions such as dark rooms and noisy settings. The results show that fusion increased recognition accuracy by 52.45% compared to using face alone and 81.62% compared to using voice alone. It took an average of 1.34 seconds to enroll a user and 0.91 seconds to perform the authentication. To further optimize speed and reduce power consumption, we proposed classification on a field-programmable gate array (FPGA) chip that may be easily integrated into an IoT device. Experimental results showed that the proposed FPGA-accelerated KNN could achieve 150x faster execution time and 12x lower exhausting compared to a CPU.

Key Words: — Multimodal Biometric, IoT devices, KNN, DCA

1.INTRODUCTION

Human beings are gifted with some eccentric and irreconcilable characteristics. This feature among us is applied intelligently to confirm security while consuming less manpower. biometric identification is taken into account to be the identity verification of a private using either a biological feature which possesses physiological characteristic sort of a fingerprint or a behavioral characteristic sort of a signature . As human fingerprint is stable over . Internet has already proliferated the entire world and also has the luxurious of being an even architecture, so by adopting these internet technologies and lengthening it in appliance control inside homes we will suddenly get the complete advantage of everything that has been developed over 30 years within the field of internet. the web of Things (IoT) could be a system of interrelated beings that are given unique identifiers and therefore the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. thanks to the amount of internet and IoT, the prices become cheap and affordable with time and thus it's wiser to style things supported IoT than the other propriety design.

The biometrics employed in a biometric system can either be physiological or behavioral as mentioned within the paper. The paper glances at the various kinds of biometric traits that are commonly considered as biometric measure. The paper further glances at the assorted factors that are considered in determining whether a biometric is practically viable for a biometric system.

The paper further discusses a couple of biometric system- its working method, the various operations performed and therefore the various components which constitute the biometric system. The paper then glimpses at the various errors that a biometric system can produce during authentication. The paper furthermore discusses about the 2 kinds of biometric systems: Unimodal Biometric System and Multimodal Biometric System. There are several drawbacks encountered in employing a Unimodal Biometric System.

2.BACKGROUND WORK

2.1 Types of Biometric Traits :

According to NIST (U.S. Dept of Commerce), Biometric is "a measurable physical characteristic or personal behavioral trait accustomed recognize the identity, or verify the claimed identity, of an applicant". A biometric system can authenticate a private by considering any of the varied possible biometric traits. The various biometrics of a private that may be measured are diverse. Biometric traits are broadly classified into two categories [1]: 1) Physiological Biometrics and 2) Behavioral Biometrics. The physiological biometrics include biometric traits which are anatomical like fingerprints, hand geometry, face, iris, ear pattern, palm vein, palm print and such. Whereas behavioral biometric analyses the behavioral traits of a private like keystroke dynamics, voice, hand signatory and gait. the kinds of biometrics are depicted within the following flowchart (Fig1).

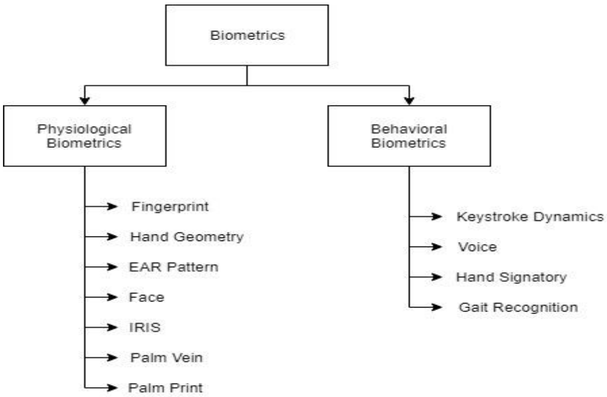


Figure 1: Types of Biometrics

2.2. Biometric Factors

For a biometric measurement to qualify as a biometric and even be practical to adopt during a biometric system, the biometric measurement has to satisfy seven factors: Universality, Uniqueness, Permanence, Collectability, Performance, Acceptance and Circumvention.

Universality: Universality of a biometric feature requires the characteristic to be available in majority of the population. For instance, biometric system using fingerprints are often rendered futile if a private may be a person with disability of arm. just in case of a biometric system obtaining iris image, the biometric are often ineffective if a private is blind.

Uniqueness: Uniqueness determines how a biometric feature is distinct for various individuals. as an example, fingerprints are distinct for every individual then are palmprints.

Permanence: Permanence of a biometric measure requires it to be consistent without considerable changes within the feature over time. as an example, the ridges of a fingerprint might fade or may not be clear because of maturity.

Collectability: Collectability of a biometric measure is that the ease with which it are often gathered so as to authenticate the individual in a while. as an example, fingerprints are comparatively easier to amass, than say palmprints (arthritis may cause inconvenience to the individual), which is why they're used widely.

Performance: Performance may be a set of metrics which determines how effectively a system employing a biometric measure accomplishes the authentication of a private. It involves measuring the speed and accuracy of the system, the resources needed to attain the intended speed and accuracy, likewise because the factors which affect the speed and accuracy of the system.

Acceptability: Acceptability refers to the degree with which a private readily gives the biometric measure. The degree of convenience to the individual has relevancy to the accept.

3.BIOMETRIC SYSTEM

The Biometric System is “An automated system capable of: 1) taking a biometric sample from an end user;

2)extracting biometric data from that sample;

3) checking the extracted biometric data with data contained in one or more references;

4) decide how well they match; and

5) identify whether or not an identification or verification of identity has been achieved” as defined by the NIST. Thus, a biometric system typically acquires the biometric traits of a private and attempts to spot or verify the identity claimed by the individual by processing and comparing the measured traits.

A biometric system operates as a verification or as an identification application supported the necessity. Verification involves confirming whether the claimed identity is that the genuine identity. The system achieves this by comparing the input biometric data with one biometric template of the claimed individual already existing within the database. Whereas, identification involves attempting to find a possible match of the input biometric data and an existing biometric data so as to work out the identity of the unknown individual. Hence, verification could be a one-to-one (1:1) search, while the biometric system achieves identification by performing a one-to-many (1: N) search. Validation assists in positive recognition whereas identification plays a critical role in negative recognition.

Both the operations require the biometric system to initially acquire and store the biometrics of the individual, known as the enrollment process. The enrollment process entails obtaining the biometric data usually through sensors in the style of a digital representation, performing a top quality check on the biometric data so as to make sure the acquired data is suitable for further processing, extracting a feature set from the info, and at last storing the extracted biometric template (feature set) within the system database.

3.1.Requirements

The various components comprising a biometric system [4] are as follows:

1) Sensor: The sensor obtains the biometric data of the user. The sensor can obtain the information through various methods like optical sensors, electro-optical sensors, thermal detectors etc.

2) Feature Extraction: This phase obtains a group of distinct and principal features from the gathered biometric data after processing it. as an example, the feature extraction phase extracts the position and alignment of minutiae on a fingerprint image for a fingerprint biometric system.

3) Matching Score Component: This component compares the features obtained from input for authentication to the features obtained during enrollment of the user and generates an identical score. For the fingerprint biometric, the minutiae points of both the input and enrollment images are compared to come up with an identical score. supported the matching score generated, the biometric system decides whether the individual is an authenticate user or an illegitimate user.

4) System Database: The biometric system uses the system database to store the feature templates gathered during enrollment of authentic users. The enrollment process comprises of obtaining the biometric data of the individual, followed by feature extraction from the obtained data which produces an efficient depiction of the biometric referred to as a template, and eventually storage of the template within the System Database.

Implementation of a biometric for authentication in an exceedingly biometric system is diligently selected taking into consideration the wants and practicality of the biometric within the relevant situation

3.2.Kinds of Biometric System

A biometric system are often unimodal or multimodal based on the quantity of biometric features that are measured for authenticating a personal.

Unimodal Biometric System: Unimodal systems utilize one biometric measure for authentication. The accuracy and efficiency of a unimodal biometric system has improved drastically over time with advances in sensor equipment and technology.

Multimodal Biometric System:

The drawbacks during a unimodal biometric system are often overcome by implementing a multimodal biometric system. A multimodal biometric system captures and combines two or more (multi) modalities of a biometric for authentication purpose.

HOG, LBP, and MFCC Features

HOG features are among the foremost commonly used features in face recognition. they're derived by partitioning a picture into square cells, computing the histogram of gradient orientations in each cell, then normalizing the result employing a block-wise pattern. the method yields a dimensionless real number quantity that's the identifying feature.

LBPs are another popular feature for face recognition and perform robustly in texture classification. The LBP algorithm splits the image into cells. for every pixel in each cell, neighborhoods are created. a district consists of a center pixel and its neighboring pixels. for every neighborhood, the center pixel's intensity is compared to every of it its neighboring pixels' intensities. If a neighbor's intensity is less than the middle pixel's, a 1 is written for that neighbor; otherwise, a 0 is written. this mix of 1s and 0s are then formed into a binary number that's converted to a base 10 number. A histogram of the frequency of every decimal number within each cell is then calculated to make a feature vector.

MFCC features are widely employed in voice recognition. Each MFCC comprises vectors of coefficients that identify key components of an audio signal. The feature vectors are computed by partitioning the signal and calculating filter bank coefficients with the employment of a Fourier transform . A discrete cosine transform [18] is then applied so as to decorrelate the filter banks.

4.IMPLIMENTATION

4.1 Software Implementation: We implemented our approach on a Raspberry Pi 3 Model B with a quad-core 64-bit ARM Cortex A53 1.2 GHz processor and 1 GB of RAM. the complete system was implemented in Python. Modules utilized included: Numpy for matrix computations; Scikit-learn for data preprocessing, principal component analysis (PCA), and KNN implementation; OpenCV for image preprocessing and extraction of HOG features; Scikit-image to extract LBP features; and LibROSA for voice preprocessing and calculation of MFCC features. The DCA algorithm was implemented from scratch using Numpy.

We used a Raspberry Camera Module V2 containing a Sony IMX219 8-megapixel sensor and a USB 2.0 microphone . Figure 2 shows the graphical interface. The interface was implemented using PyQt . Similar to the approach of Gofman et al., we recorded a video of the person's face while they spoke a phrase. From the video we then extracted face image frames and also the recorded voice. This allowed us to capture both biometrics simultaneously.

4.2 Hardware Implementation: In our hardware implementation approach, feature extraction and fusion came about on the CPU while KNN classification took place on the FPGA. the primary step in implementing our KNN classifier on the FPGA device was connecting the CPU, where the feature extraction and fusion came about, to the FPGA, where the sets of features were classified. To achieve this, we used the OpenCL resource framework

Consequently, the KNN algorithm implemented on the FPGA can access the fused sets of features stored in local memory. Although the worldwide memory can even be used, it'd result in slower time interval than the local memory.

Implementation on the FPGA*:* so as to implement the proposed architecture, we employed an Intel I7-3770K CPU with a 3.5GHz operation frequency. The OS on the computer was Windows 7 with a 64-bit OS. We used an Intel DE5 FPGA board that was connected to the CPU through PCIe lanes. The transceivers were capable of achieving a transfer speed of 12.5Gbps, which allowed the DE5 board to be fully compliant with version 3.0 of the PCI express standard. To store the computation matrix, we used two independent banks of DDR3 SO-DIMM RAM to construct global memory. in contrast, the local memory was constructed by on-chip RAM blocks, which are simple and might easily be given access to. Private memory was constructed by flip-flops within data flow that would run at the accelerator's frequency. The execution times and power consumption of classification on the FPGA was compared thereupon of its CPU counterpart. In the future, we conceive to connect the FPGA on to the Raspberry Pi.We used a hierarchical platform-based design for implementing the KNN classifier. the most purpose was to modularize various functions in hardware and software.

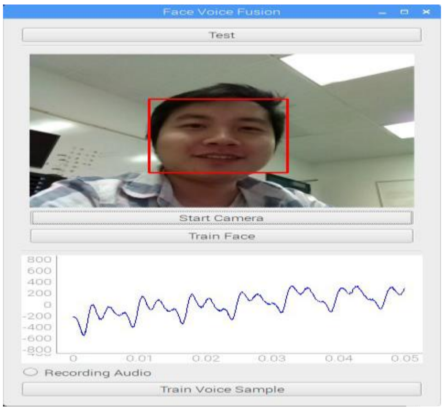


Fig 2.User Interface For Raspberry pi

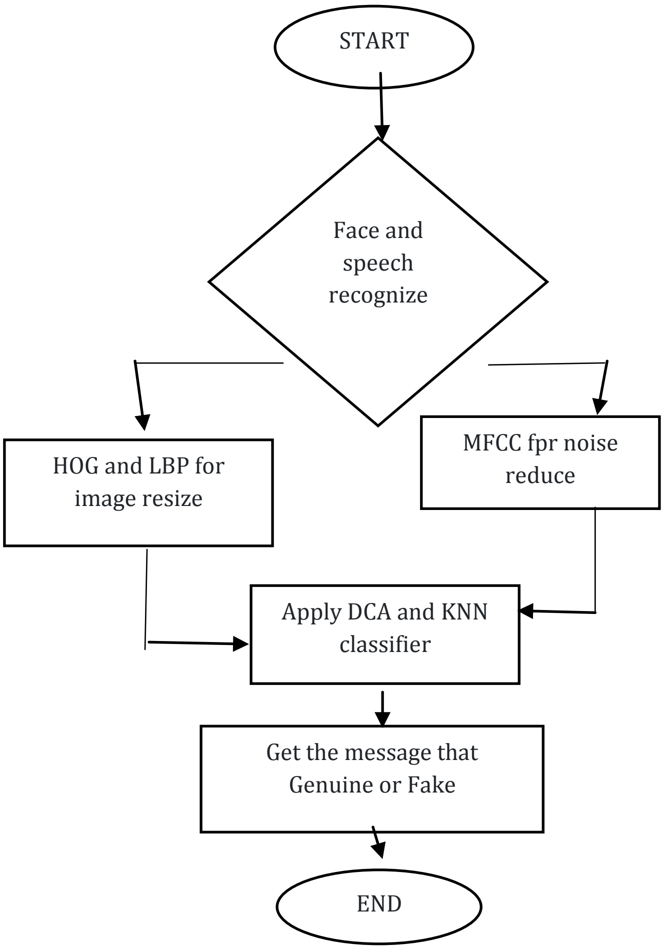
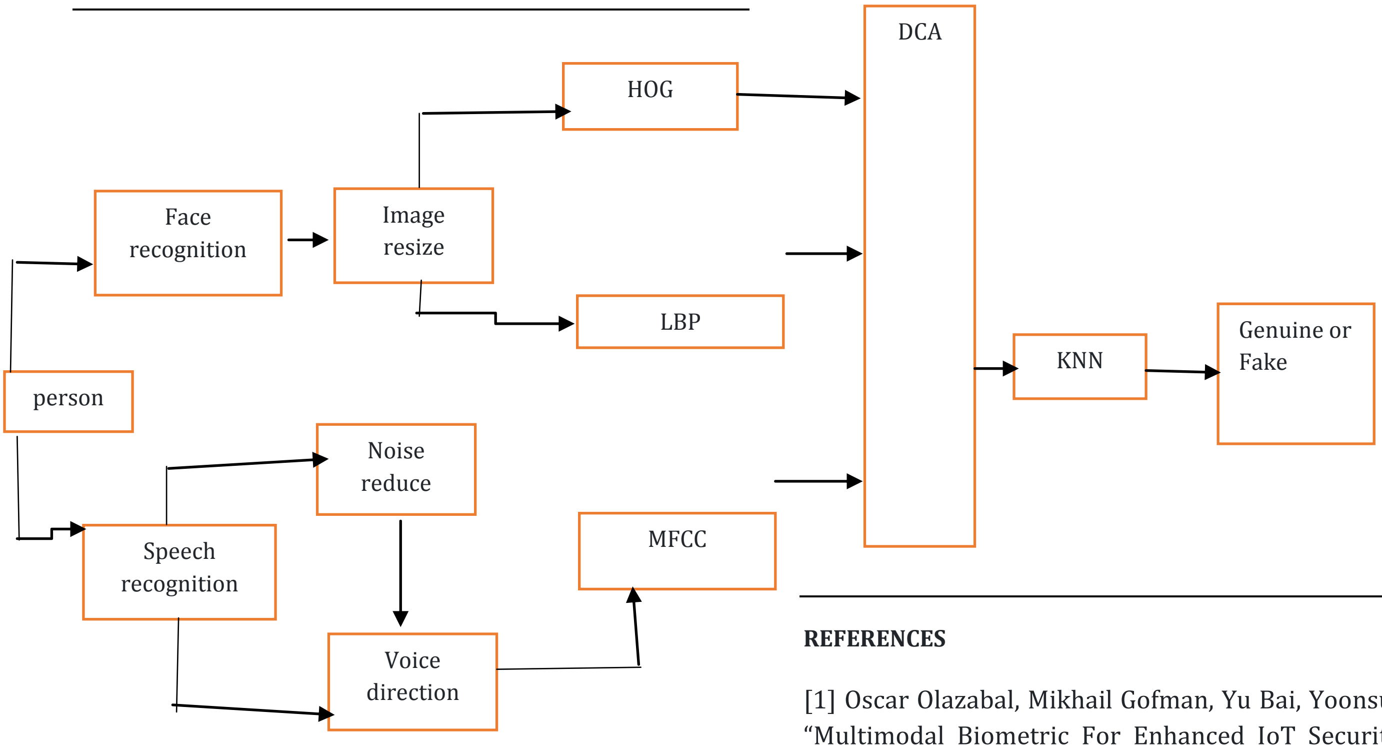

START
Face and speech recognize
HOG and LBP for image resize
MFCC fpr noise reduce
Apply DCA and KNN classifier
Get the message that Genuine or Fake
END

Fig 3. Flowchart for Multimodal Biometric

Fig 4 System Design for Feature Level Approach



5.CONCLUSION

Because of the efficient criterion, system was ready to be designed using low cost. because the new wave IoT is coming in there are many IoT enabled devices for home automation/industry automation and these devices may also be controlled remotely using identity verification over internet. New access control policies like shift based, person based, group based etc. with corresponding criteria's is setup in Web server if any change in access control is desired.Unimodal biometric system presents some difficulties during authentication as discussed within the paper. Hence, it's advisable to implement a multimodal biometric system for authentication. Although a multimodal system increases the efficiency in authorizing a private (as multiple modalities of biometric are compared) and identifying and individual (by indexing using the multiple biometrics to narrow down the search results), Multimodal systems cause inconvenience and vexation to the users if prompted for multiple inputs. Additionally, one common complication is that of user and the value factor and time required in implementing a Multimodal system also increases because of the multiple sensors required to capture and record the multiple biometrics. However, these problems could be overcome with progressive advances in cognitive recognition as a biometric authentication approach.

REFERENCES

[1] Oscar Olazabal, Mikhail Gofman, Yu Bai, Yoonsuk Choi, "Multimodal Biometric For Enhanced IoT Security",IEEE vol.32,page.886-893,2019.

[2] Divil Jain , Dr. P.S. Ramkumar, Dr. K.V.S.S.S.S Sairam,"IoT based Biometric Access Control System",IEEE, vol.5,May 2016.

[3] Medikonda Asha Kiran , Padmatti Yogeshwari , Kosuru Viswa Bhavani, Thudumu Ramya,"Biometric Authentication: A Holistic Review",IEEE 2018.

[4] BOOK: Handbook of Biometrics, by Anil K. Jain et al.Springer, 2007.

[5] Mohammad H. Mahoor , Steven Cadavid, and Mohamed Abdel-Mottaleb, "Multi-modal Ear and Face Modeling and Recognition",Proc. IEEE 16th International Conference on Image Processing, 2009,pp. 4137-4140.

[6] Mohamed Soltane, Noureddine Doghmane, Noureddine Guersi, "Faceand Speech Based Multi-Modal Biometric Authentication",International Journal of Advanced Science and Technology, 2010,Vol. 21(8), pp. 41-46.

[7] Muhammad Imran Razzak1, Rubiyah Yusof and MarzukiKhalid,"Multimodal face and finger veins biometric authentication",Scientific Research and Essays, 2010, Vol. 5(17), pp. 2529.