

Artificial Intelligence Based Person Identification Virtual Assistant

P.Praddeep, P.Balaji, S.Bhanumathi

ABSTRACT---In future all the electronic gadgets are operated by using virtual assistant which is anything but difficult to get to its needs in security. Project aims to provide security for virtual Assistant (VA) through facial recognition. The framework enables just approved users to access voice commands. By this we can get protection and security for virtual assistant (VA). Users can ask their help addresses like time, date and climate and find solution to the inquiries. This virtual assistant causes us to send email through voice commands and it also takes notes from voice commands with security. It gives access to the unapproved user to enlist with the required consent from the administrator. It is can exchange the pictures and documents just by using voice commands. It will take photographs using camera when we use the fitting voice commands. Various users in a family can get access to the virtual Assistant by facial recognition module.

Index Terms: Virtual Assistant, Facial Recognition and Security.

I. INTRODUCTION

In Today's advanced crisp market for artificial intelligence could be a key unlocking the users of tomorrow. Man-made brain power is as of now all around the user. Many depend on it every day as per Gartner about 38% of consumers have utilized virtual assistant benefits on their smart devices as of late numerous enterprises receiving AI to convey the logical conversational consistent and customized home administrations now is the ideal time to be natural and proactive about how users will encounter it and cross over any barrier between the innovation and how it helps users are devouring it then AI gets advanced with power huge information and investigation it can offer a one of a kind and separate client experience.

Users like to associate with the machines using voice commands which are conceivable through the virtual assistant, gadgets for example, smartphones, smart TV's and car navigation systems and so forth. The virtual assistants are the astute operators that can enable users to complete [13].

Undertaking more successfully and advantageously by means of spoken collaborations among user and the virtual assistant. The virtual assistants can support a wide scope for all users in business enterprises, education, government, medicinal services and diversion. The main organizations planned their own virtual assistants, for example, Microsoft's Cortana, Apple's Siri, Amazon's Alexa Samsung S Voice, and Google

Text to speech, manufactured talking face and dialog management [4,14].

The virtual assistant is improved by giving Facial Recognition framework. The facial recognition framework for virtual assistant using AI strategies to detect and recognize faces. They are two kinds of users like approved clients and unapproved users [2]. The user stands before the camera which takes different pictures of the user. The captured pictures experience the face detection process [12]. In this procedure it identifies faces in the pictures and enables access to the virtual assistant for the approved users.

II. RELATED WORK

The author in [1] presented about the attacks to voice assistance, that can be followed in a several availabilities which are given in several operating systems attackers can principally control these apparatuses to perform unapproved commands. The assailants could release the delicate data like user's area visit web pages which contain malware to gain unapproved access to certain gadget this prompts spillage of touch data.

Voice assistance can be utilized without getting any permission from the user. Voice assistance attacks are generally static attacks, attackers broadly utilize recorded sound documents which are played by applications or by static medium this may cause sending mails and same voice calls

Even send post via web-based networking media aggressors can utilize voice help for long range interpersonal communication applications to post destructive things from user account.

At times the voice recognition may fail by getting great example of victim's voice and utilize prepared voice engine to copy his voice. The usage of a voice order framework as an Intelligent Personal Assistant (IPA) can play out various errands or administrations for a person. In this framework one can make inquiries to the framework, conjure its AI generally get it from Wikipedia [2].

The authors in the [4] proposed that insightful projects with natural language processing that are as of now accessible, with various classifications of support, and look at the helpfulness of one explicit bit of programming as a Virtual Personal Assistant. Which are analyzed by fundamental regular language handling and the capacity to work without the requirement for other sort of human info (or programming) may as of now be reasonable in the menial helpers however at some point it might fail because of prepared voice engine to mirror his voice.

Revised Manuscript Received on August 19, 2019.

P.PRADDEEP, Penumarthi Pradeep, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, T.N, India (E-mail: pradep.proton@gmail.com.)

P.BALAJI, Pallapothu Balaji, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, T.N, India (E-mail: pallapothu96@gmail.com.)

S.BHANUMATHI, School of Computing, Sathyabama Institute Of Science and Technology, Chennai, T.N, India (E-mail: banujun8@gmail.com)

III. EXISTINGSYSTEM

Virtual assistance can do anything without an individual for help. VA can do administrative assistance like sending email and taking notes. VA can access the information from online website and gives information to the users. This information can be extracted in Jason and converted into text format this text format again converted into speech. This system will interact with the user and fetched information from online cloud according to the question asked from the user. voice activated digital devices like amazon echo and personal Alexa assistant may also raise personal concerns like amazon is considering giving transcripts Alexa's audio recordings to the third-party. When they hear key word Alexa, they start recording the voice which is not necessary. This recording was stored in the developer's database. As artificial intelligence is based on data and data is based on the recordings of the users.

IV. PROPOSEDSYSTEM

The Facial Recognition to the virtual assistant gives greater security to the system by the Haar Cascade algorithm. The face is recognized by the camera and it is handled through OpenCV in which it detects the faces and articles placed put before the camera and the picture taken is contrasted with the pictures in the in the system by Haar Cascade Algorithm. After recognizing the face it permits to interact with the virtual system.

The virtual assistant hangs tight for our voice commands. Here to the virtual assistant the input is given in speech format through Bluetooth connected device then the system converts the speech in to the text format and understands the input and undergoes processing and gives the appropriate output in the text format later it is converted to speech format as output by the use of Speak (speech synthesizer) and the output is in the audio format.

FACERECOGNITION:

Create a database in which all the training images are stored and all the images are captured by the camera are stored in database. The face recognition is finished by using two algorithms to be specific Haar Cascade Algorithm and Fisher Face Algorithm. In the Haar Cascade algorithm is based on Cascade classifiers which consists of haar features. The cascade classifiers are the concatenation of a set of weak classifiers used to create a strong classifier. These classifiers identify the human face dependent on the most significant highlights like eyes, eyebrows and lips. Haar features are detected based on the concrete computation, in which we allocate a pixel intensity to every single pixel related to grayscale values inside the scope of 0 to 255 where 0 speaks to the white shading and 255 speaks to the dark shading.

0.2	0.3	0.7	0.7
0.1	0.1	0.8	0.6

0.1	0.3	0.6	0.8
0.1	0.2	0.7	0.5

Fig 4.1: original values detected on an image.

0	0	1	1
0	0	1	1
0	0	1	1
0	0	1	1

Fig 4.2: Ideal Haar features and Pixel intensities 0 for white and 1 for black.

Architecture

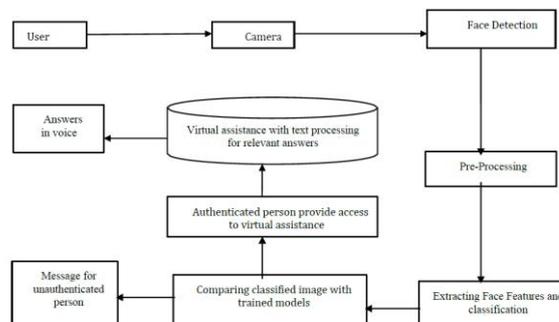


Fig 4.3 Person Identification Virtual Assistant

In the fig 5.3 camera captures the photo of the user and then it trains the models for the images stored in the database with respective to the features of the person. In the detection section it detects the face based on the haar xml file which has some pre-defined features of face. After detecting the face, it will start extracting the features of the face. By considering the features the images are classified accordingly. These classified images are compared with the trained models. If it matches the user can access the virtual assistance.

4.1.2 RECONIZING THE DETECTED FSCE:

In Fisherface Algorithm the pictures which are available in c number of classes with n samples for every individual dataset and it is given as the example set of K's the place K ranges from 1 to c and every individual sample of T has the scope of 1 ton.



$$K = \{K_1, K_2, \dots, K_c\} [11]$$

$$K_i = \{k_1, k_2, \dots, k_n\} [11]$$

To acquire the global mean of the considerable number of pictures and all the class this characterized by μ and μ_i is the mean of pictures within each class. To acquire the change and ascertain the variance matrix which helps us to give the scatter inside the class. For each class discover the contrast between the picture and the mean esteem which is related to class where the picture adjusted.

$$S_w = \sum_{C_j=1}^c \sum_{n_j=1}^n (x_{ij} - \mu_j)(x_{ij} - \mu_j)^T [11]$$

Where x_{ij} is the i th test of class j , μ_j is the mean of class j , and n_j the quantity of tests in class j . S_w is the scatter within the class. The scattering between the classes is determined utilizing

$$S_b = \sum_{C_j=1}^c (\mu_j - \mu)(\mu_j - \mu)^T [11]$$

Where S_b is the scatter between the classes. We now need to discover those premise vectors V where S_w is limited and S_b is augmented, where V is a network whose sections v_i are the premise vectors characterizing the subspace. These are given by,

$$|V^T S_b V| / |V^T S_w V| [11]$$

The answer for this issue is given by the summed up eigen value decay.

$$S_b V = S_w V \Lambda, [11]$$

V. IMPLEMENTATION

Necessary packages

- Bluetooth
- Time
- Httpplib
- urllib2
- json
- subprocess
- cv2
- Sys
- numpy
- os
- subprocess

Create Datasets

The accompanying advances will make the datasets this is finished utilizing haar cascade frontal face default xml file trained features of faces.

1. Make an informational index envelope with the end goal that every one of the countenances to be perceived results in these present circumstances organizer.
2. Instate the Height and width of the face that is taken while catching the picture.
3. Import the haar record utilizing openCV open source application which has some pre-characterized capacities.
4. OpenCv helps us to utilize webcam with the assistance of VideoCapture function. On the off chance that 0 is passed as the content in this capacity it will utilize webcam of the P

C else 1 is passed which initiates different cameras which are associated with the gadget.

5. To take n quantity of pictures loop the functions read from webcam and cvt.color which changes over shading to high contrast of course use loop command inside the loop for each h and every coordinate of face.
6. Inside this nested loop actualize fractions of the OpenCV rectangle shape in which picture caught by the camera, arranges and shading range is given as arguments.
7. To detect the face use function face_cascade.detectMultiScale with gray and cascade values are given as arguments and use resize and image write function for resizing the image.

Face Detection

For Face detection we use Haar Cascade algorithm which involves in the following steps:

1. In the Haar Cascade algorithm is based on Cascade classifiers which consists of Haar features which are in Haar file helps for the detection of the face.
2. The cascade classifiers are the combination of a set of weak classifiers used to create a strong classifier.
3. This combination forms a triangle shape which consists of black and white identification lines on the

Face is recognized using the fisher face algorithm:

This involves in two parts. They are Creating Fisher Recognizer and to use Fisher Recognizer on the camera stream.

Part 1: This involves in training the images in which are stored in the datasets. Create two lists which consist of images and their corresponding names. Loop the image and their id for each and every subdirectory in the dataset. Then create a numpy array common for both the lists. OpenCv help to train models for images with respective their id using train function.

Part 2: In this the Fisher Recognizer helps to recognize the face on camera stream. First it will detect the face in front of the camera using haar file. The detected face is converted into black and white image. Use gray and resize functions for modification of the captured image.

The trained model gives the prediction value for the captured image the minimum limit of the prediction value is five hundred. If the prediction value is less than five hundred then the person is authenticated else the person is unauthenticated.

Get Access to Voice Commands

If the person is authenticated then he or she will get access to voice commands.



Fig 5.1: Flow of Face Recognition Virtual Assistance.

This voice commands are revived via Bluetooth connection through a socket bind with port 1. The socket connection is automatically connected to the virtual assistant if we add the device in the Bluetooth module of the virtual assistant. The received data through attachment was examined through conditions given and offer response to the regarded individual.

For the appropriate responses that ought to be replayed is finished by bringing in Wikipedia and wolfram alpha. Wikipedia will give the responses for the general questions and wolfram alpha will give responds to for the intelligent inquiries. Utilizing voice commands, the virtual assistant can write notes and send email through the SMTP server. It likewise gives answers for climate, date, time and takes photographs of the people.

Flow Chart for face Recognition Virtual Assistance

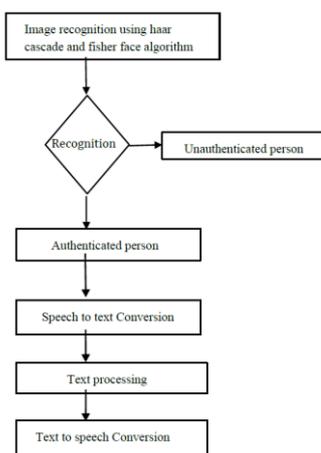


Fig 5.2 Flow of Face Recognition Virtual Assistance.

In the flow chart of fig.5.1 the recognition part takes place first which leaves two possibilities of a person getting authenticated and unauthenticated. If the person is unauthenticated it stops the process and get back to its initial position where as in case of authenticated person it follows the procedure flow. The speech given by the person is converted into the text format which would be getting processed in the next step. Then finally the processed text is

followed with the response given by the module to the speech form. This is how the face recognition virtual assistant takes place.

VI. RESULTS

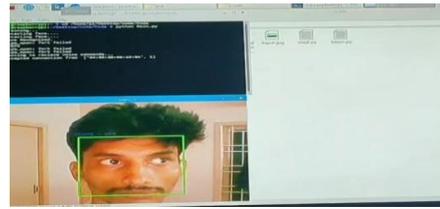


Fig 6.1 Face Input for Authentication The Virtual Assistance.

In the fig 5.3 camera captures the photo of the user and then it trains the models for the images stored in the database with respective to the features of the person. In the detection section it detects the face based on the haarxml file which has some pre-defined features of face. After detecting the face, it will start extracting the features of the face. By considering the features the images are classified accordingly. These classified images are compared with the trained models. If it matches the user can access the virtual assistance.

The input is taken in the form of picture as shown in the figure 6.1. This input is processed with the trained models. There are usually three scenarios when it is processed with trained models namely:

1. Authenticated person.
2. Unauthenticated person.
3. There is no face in front of the camera' comment for the third case of not having input face at the camera vision.

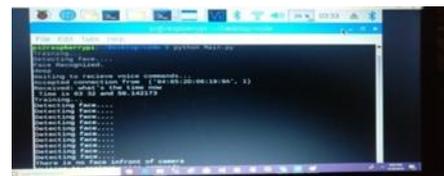


Fig 6.2: Output for the detected Face and Replay for Questions.

In case of an authenticated person it would have the access to the virtual assistant through which we give the input in the form of methodology used in fig.5.1. It as well as give the response to the questions asked by the person.

In case of an unauthenticated person it leaves a message and goes back to its recognition part of its loop in any kind of scenario.

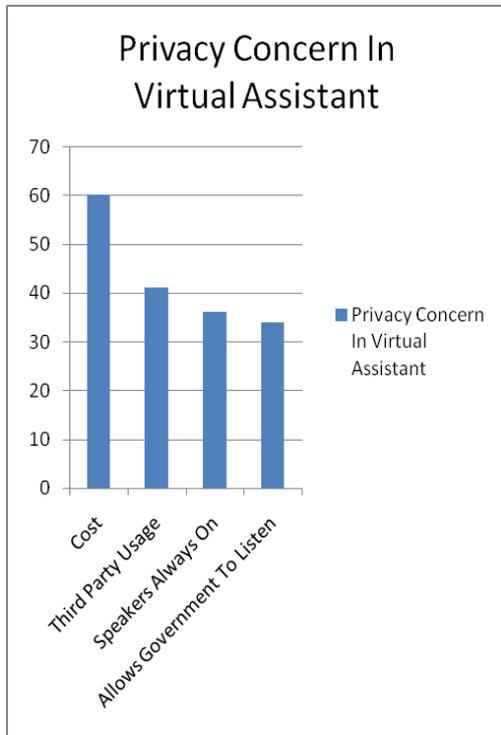


Fig 6.3 Privacy and Security Issues Faced By Virtual Assistants.

The bar chart in fig 6.2 represents the privacy and security issues faced by the virtual assistants. In the year 2017 forty one percentage of the virtual assistance was used by third party. The virtual assistance is always active results in recording sensitive information. Some of these security purpose government will listen to our private conversation all this problems can be resolved using face recognition. This may solve by voice recognition but the attackers uses recorded mimic voice and get access for the virtual assistance. This show the need of security in the virtual assistant.

Table 6.1 Represents Several Voice Assistants and their features and How it differs from Proposed Model

Voice Assistant	Voice Response	Security	Face Recognition	Online Dependency
Siri	YES	NO	NO	YES
Alexa	YES	NO	NO	YES
Cortana	YES	NO	NO	NO
Google	YES	NO	NO	YES
Proposed Assistant	YES	YES	YES	YES

In the table 6.1 represents the several voice assistants including proposed assistant accessibilities in the various fields. All the assistant’s response to the audio input which is known as voice response, The Google Assistant and Siri can be activated when the screen is locked whereas other assistants lack this feature. Proposed Assistant has Facial recognition that enables more security. Proposed system can send mail in more secured way than the other voice assistants.

VII. CONCLUSION

This paper will help to demonstrate that virtual assistant is attacked by third party and gives a solution to the problem. In this the virtual assistant is improvised with Facial Recognition.

The facial recognition system for virtual assistant using Machine learning strategies to detect and recognize faces. After recognizing the face, the users can access the virtual assistant. If the person is third party then it will say unauthenticated person. The unauthenticated person can get access to virtual assistance with administrator permission. This Assistance can send email and take notes of some personal information only for the authorized person it also says some general information like time, date and weather.

REFERENCES:

1. Efthimios and Constantino in 2017, “Monkey says, Monkey Does-Security and Privacy on Voice Assistants”, IEEE journal, ISSN: 2169-3536.
2. Peter Imrie and Peter M. Bednar, 2013, “Virtual Personal Assistant” in Research gate with ISBN: 978-88-6685-007-6 4.
3. Emad S. Othman in November 2017, “Voice Controlled Personal Assistant Using Raspberry Pi”, International Journal of Scientific & Engineering Research Volume 8, Issue 11, 1611, ISSN 2229-5518.
4. Anurag Mishra, Pooja Makula, Akshay Kumar, Krit Karan and V. K. Mittal, May 28-30, 2015, “A Voice-Controlled Personal Assistant Robot”, IEEE journal, Page: 8, INSPEC accession number 15291099.
5. Tatiana Ekeinhor-Komi, Jean-Léon Bouraoui, Romain Laroche, Fabrice Lefèvre, 09 February 2017, “Towards a virtual personal assistant based on a user-defined portfolio of multi-domain vocal applications”, IEEE Xplore, INSPEC 16657478.
6. O. Portillo-Rodriguez, C.A. Avizzano, A. Chavez-Aguilar, M. Raspolli, S. Marcheschi and M. Bergamasco, “Haptic Desktop: The Virtual Assistant Designer”, IEEE/ASME International Conference on Mechatronics and Embedded Systems and Applications.
7. Bisma Shakeel, Tabasum and Mir Shahnawaz Ahmad in July-2017, “Siri – Apple’s Personal Assistant: A Review”, International Journal of Computer Science and Mobile Computing vol.6 Issue.7, ISSN 2320-08.
8. Sanchez, Carlos, Muñoz de la Peña, David, Gomez-Esternand Fabio, “Virtual assistant for individualized practical training on controller design”, ScienceDirect, IFAC 48 29 2015 205210.
9. Prajyot Mane, Shubham Sonone, Nachiket Gaikwad and Jyoti Ramteke, “Smart Personal Assistant using Machine Learning”, International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS-2017.
10. Hyung-Ji Lee, Wan-Su Lee, and Jae-No Chung, 2001 published their paper “Face Recognition Using Fisherface Algorithm And Elastic GRAPH Matching”, IEEE with ISBN 0-7803-6725-1.
11. Sushma Jaiswal, Sarita Singh Bhadauria and Rakesh Singh Jadon, July 2011, “Comparison Between Face Recognition Algorithm-Eigenfaces, Fisherfaces And Elastic Bunch Graph Matching”, Volume 2, No. 7, Journal of Global Research in Computer Science, ISSN-2229-371X.
12. Dr. R. Subhashini, E. Nagarajan and Niveditha. P.R, "Detection Of An Incognitos Intruder in Industries and Semantic Mapping Of Emotions", International Journal Of Applied Engineering Research, ISSN-0973-4562, VOLUME 9, Number 20(2014) pp.6727-6734.



13. R.Subhashini and V. JawaharSenthil Kumar, "Shallow NLP Techniques for Noun Phrase Extraction", Presented in the International Conference on Trendz in Information Sciences & Computing (TISC - 2010) in association with Cognizant Technology Solutions and IEEE from 17th to 19th of December, 2010, Sathyabama University, Chennai.
14. Saranya, E., Sam, B.B., Sethuraman, R. "Speech to text user assistive agent system for impaired person" 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2017.

AUTHORS PROFILE



PenumarathiPradeep, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pradeep.proton@gmail.com.



PallapothuBalaji, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pallapothu96@gmail.com.

S.Bhanumathi, School of Computing, Sathyabama Institute of Science and Technology, Chennai, banujun8@gmail.com