International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1455-1459 www.ijaem.net ISSN: 2395-5252

Entry Verification at Vip Meetings Using Ai Techniques

Archana Jadhav[1], Sonakshi Agrawal[2], Devika Nambiar[3], Aishwarya Daud[4], Shubhangi Dhanure[5]

Professor, Department of Information Technology [1]
Student, Department of Information Technology[2,3,4,5]
JSPM's Rajarshi Shahu College of Engineering, Pune, Maharashtra

Submitted: 15-04-2022 Revised: 27-04-2022 Accepted: 30-04-2022

ABSTRACT—This paper proposes a four step authentication process at VIP meetings entrance to allow only authorized personals to enter.This is implemented by using face recognition with liveness detection followed by audio verification and OTP generation. Face recognition is a very powerful method to identify an individual using their facial features which we have implemented using Haar-Cascade algorithm. Our model solves the issue of face spoofing i.e. it do not get tricked by photos of individuals during face detection as it also works on liveliness detection using CNN algorithm. Audio verification further helps to enhance the security by making sure the right code word is said by the user at the verification time. OTP generation and verification is the final step in the security model.

Keywords— face recognition, liveness, Face SpoofingVIP,Haar-Cascade algorithm, audio verification, OTP

I. INTRODUCTION

In today's modern times, VIPs security plays a crucial role as they are often targets of terrorist attacks, extremist organization and religious groups. VIP security is devoted to confirm the safety of important political figures, famous celebrities, business executives and other people who are potentially in peril of private attacks.

Our sole aim to implement this security model is to make sure that no person or object not confirmed to be safe or secure reaches near the protected person and provide full protection. We can achieve this with the help of machine learning and artificial intelligence.

In the present system, there are no such software application system provisions in the country to carry out the VIP meeting security measures, other than basic muscular power and finger prints. Mostly the security is controlled and regulated by the top agencies like SPG, NSG, ITBP, CRPF and CISP. This increases the no. of people present at a location which is a concern not only in terms financial amount the government has to spend on these agencies but also in today's covid world when we want social distancing and least crowds.

II. PROBLEM DEFINITION

Using four step authentication method based on AI techniques which are face recognition, liveness detection, audio verification followed by OTP generation to ensure the security of VIP person at meetings.

III. LITERATURE SURVEY

Face recognition is one of the most extensively utilised biometric techniques. It is a biometric identification approach that uses a person's facial biometric pattern and data to authenticate their identity. Biometric facial recognition, unlike other forms of authentication such as email verification, passwords, fingerprints, or photos, employs unique mathematical and dynamic patterns that make it one of the safest and most effective.

Mohammad Ashraful Hoque [3] developed a system that can detect human faces from live video streaming, which gives a warning for ensuring a significant role in the surveillance security aspects. This paper proposed that the Haar-Cascade Algorithm is one of the most suitable and effective face detection algorithms. The basis of this control system is an Arduino Uno based on the ATMega328p microcontroller with a Pan-Tilt mechanism, and the image processing system is based on the Open Source Computer Vision System (OpenCV). The results of the analysis show that lighting conditions have an impact on system performance. As a result, this technology should be

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1455-1459 www.ijaem.net ISSN: 2395-5252

able to cover the need for daylight rather than darkness.

Bhavana R. Maale [2] introduces a 3-stage face detection system architecture that is based on the Haar Cascade Classifiers is used. According to the research, Haar-based face detection for real-time applications is a common and powerful face detection algorithm. In frontal face detection, the Haar based face detector has high precision. The level of identification depends on the form of images in the database. The bigger the database, the more time for recognition.

A malicious face spoofing can readily fool face recognition. The cheaters who want to trick the face recognition system by using facial images from photographs or videos can acquire unauthorised access. As a result, liveness detection is a crucial study issue for detecting face spoofing.

Abdelrahamn Ashraf Mohamed [4] approach in their paper is a deep learning technique called sequential CNN (convolutional Neural Network), which is divided into two stages: feature extraction and classification. CelebASpoof (2020) is the dataset that was utilised to identify live and non-live faces. The performance of the proposed approach is measured in terms of accuracy. The proposed CNN technique attained a generally acceptable accuracy of 87% for testing and 94.7% for cross validation. Many new techniques are being developed for future work, such as capsule neural networks, which are expected to improve results.

Bofan Lin [4] present a generic solution for face anti-spoofing that uses both rPPG and texture information.First, multi-scale long-term statistical spectral (MS-LTSS) features with variant granularities are designed for representation of rPPG data. Second, for extracting global-local and multi-level deep texture characteristics at the same time, a contextual patch-based convolutional neural network (CP-CNN) is used. Finally, for decision level fusion, a weight summation strategy is used, which allows the method to be generalised to include not just print and replay attacks, but also mask attacks. To demonstrate the superior outcomes of the proposed method compared to state-of-the-art methodologies, comprehensive experiments were conducted on five databases: 3DMAD, HKBU-Mars V1, MSU-MFSD, CASIA-FASD, and OULU-NPU. This combined model improves efficiency and accuracy.

Shivani Shenai [5] introduces audio-visual fusion-based quick biometric authentication. It incorporates a score level fusion of quick facial recognition using Local Binary Patterns, audio feature extraction using MFCCs (as well as delta MFCCs), and voice recognition using GMM with EM to authenticate a random pass. As a result, with a Genuine Acceptance Rate of 100 percent, this approach is more accurate and secure than traditional or unimodal authentication, with a GAR of 93.87% for face and 97.33% for voice, respectively.

Xinman Zhang [7] introduces an Android-based multimodal biometric authentication system incorporating face and speech biometrics is created in this research. To reduce the time and space complexity of this system, an improved LBP coding-based feature extraction method is used. We also provide an enhanced VAD approach for lowering the voice endpoint misjudgment ratio, discarding the invalid voice segment, and increasing algorithm effectiveness in low SNR cases. We describe an adaptive fusion technique to provide multimodal biometric fusion authentication, which solves the disadvantages of unimodal biometric authentication and effectively increases authentication performance, taking into account the hardware performance of Android-based smart terminals.

IV. PROPOSED SYSTEM

Desktop based authentication system

Our Desktop application mainly consists of five modules. Following is the description of the same:

1) Registration:

For any user to register, the user has to enter a new username, then register his face by facing towards the camera. The user then has to provide the code word for audio verification. User is also expected to provide email id for being able to receive OTP for final step. It has two sub modules:

i. Create face data
ii. Train face data

2) Face Recognition:

It is the first step of authentication. The face is detected and verified during the live video capture. We are using Haar cascade algorithm to implement this module.

3) Liveness Detection:

Face spoofing is when an attacker can gain an illegal access as an authorized person with the help of printed images, Videos, and 3D Masks. In this second step, face spoofing is prevented with the help of CNN algorithm.

4) Audio Verification:

This is the third step of authentication. Here the user is expected to speak the same code word he had provided during the registration process. This

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1455-1459 www.ijaem.net ISSN: 2395-5252

module is implemented with the help of speech-to-text library in python.

5) OTP Generation and Verification:
This is the fourth and final step of authentication. The OTP is generated using a predefined library function random() and is send to the user's registered email id. If the user enters the correct OTP he gets verified and gains access to enter the protected area.

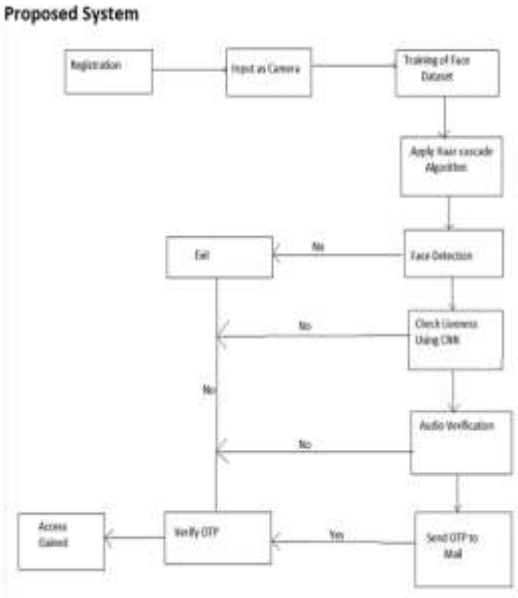

Fig 1. Proposed system

V. LEARNING CURVE OF THE MODEL

The dataset is generated during registration of the user. After successful capturing of face data using integrated camera, it is further trained using machine learning modules. The training dataset and test dataset is generated to determine the learning curve of our proposed model

Figure 2 shows the accuracy of our model by valuating the results of test dataset against training.

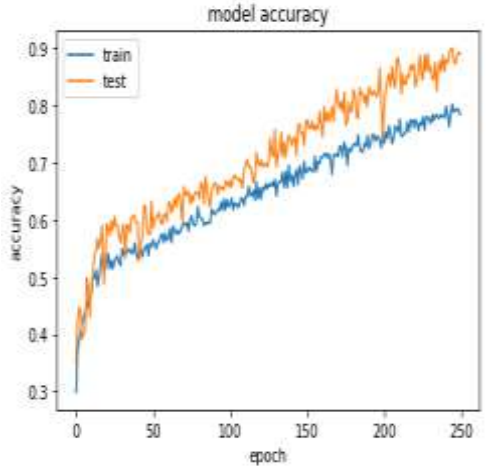

Fig. 2Model accuracy

Figure 3 shows the model loss of our proposed model which turns out to be very low.

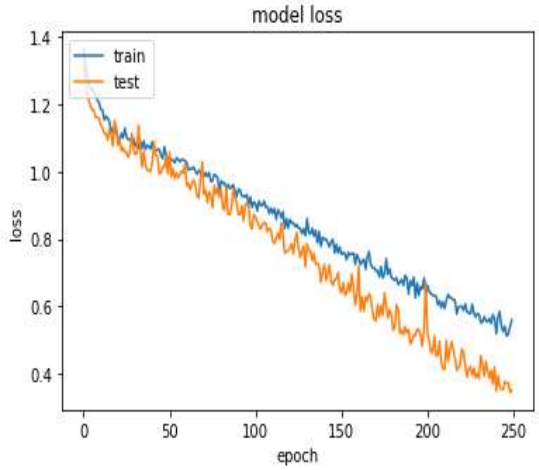

Fig 3 Model loss

By analyzing both the graphs shown in figure 1 and figure 2 we can say that our model has high accuracy and low loss which is one of the ideal case.

VI. METHODOLOGIES

1) HAAR FEATURE-BASED CASCADE CLASSIFIERS

HCC (Haar-Cascade Classifiers) is a part of Viola-Jones face detection technique. Haar feature-based cascade classifier is the most effective method among of all other object detection methods. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. Image of faces arecalled 'Positive Image' and image of without faces arecalled 'Negative Image'· [1] Haar Feature is shown in figure 4.
The value of each feature is calculated by:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1455-1459 www.ijaem.net ISSN: 2395-5252

Features = sum (pixels in the black area) - sum (pixels in the white area)

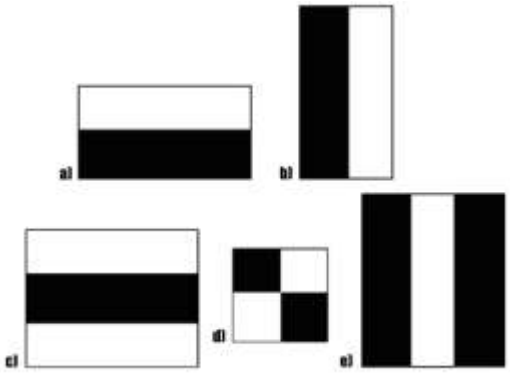

Fig 4 Haar like features. [3]

Figure 5 shows the feature calculation from the sum of the pixels between white and black rectangle. First two pictures of the first row show the two good features First picture seems to focus on the properties of eyes and second picture focus on the properties of nose [1].

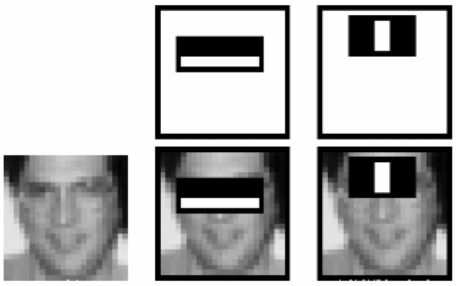

Fig 5Haar-like features (Extended). [3]

2) CNN - CONVOLUTIONAL NEURAL NETWORK

Convolutional neural network is a class of deep learning method. It is attracting interest across a variety of domains and have become dominant in several computer vision tasks. CNN is composed of multiple building blocks, like convolution layers, pooling layers, and fully connected layers. It is designed in such a way that it automatically and adaptively learn spatial hierarchies of features through an algorithm known as back propagation

Our model is developed using sequential CNN. It will be divided into various parts. First is the pre-processing part, responsible for feature extraction. After that augmentation will be done. Then the data will be passed on to the CNN layers to train. After that the model will be able to determine whether the image is spoof or live. The proposed CNN approach achieved a relatively acceptable accuracy for testing which is 87% and for cross validation 94.7%. The system consists of two stages which are the feature extraction stage and the classification stage. [4]

3) SpeechRecognition and pyttsx3:

Python libraries such as SpeechRecognition and pyttsx3 are used to convert audio to text in over 120 languages.

pyttsx3 is a text-to-speech conversion library in Python. Unlike alternative libraries, it works offline and is compatible with both Python 2 and 3. An application invokes the pyttsx3.init() factory function to get a reference to a pyttsx3. [6]

It supports three TTS engines :

- sapi5 – SAPI5 on Windows
- nsss – NSSpeechSynthesizer on Mac OS X
- espeak – eSpeak on every other platform [6]

The most common and best package is SpeechRecognition which helps in the speech verification process.The audio input is given for the process of Speech Recognition.After that a text is produced based on the audio input. We will match the text produced with the code word which was registered for further authentication process.SpeechRecognition library of python is open source and one of the most common and best package for speech recognition process.Audio files provided in SpeechRecognition can be in AfIFF-C, AIFF, WAV format, commonly wav format is widely used.

4) random () and SMTP : For OTP Module

- random():

We are using random() function for OTP generation. random() generate random floating numbers between 0 and 1.

Syntax: random.random()

Parameters: This method does not accept any parameter.

Returns: This method returns a random floating number between 0 and 1.[6]

- Simple Mail Transfer Protocol (SMTP):

It handles sending e-mail and routing e-mail between mail servers.

The smtplib module of python, defines an SMTP client session object which is used to send mail to any machine with an SMTP or ESMTP listener daemon.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 4 Apr 2022, pp: 1455-1459 www.ijaem.net ISSN: 2395-5252

An SMTP object has an instance method which is typically used to do the work of mailing a message called sendmail.

VII. RESULTS AND DISCUSSION

Following are the performance parameters for our proposed model we calculated.

Performance parameter	Accuracy	Precision	Recall	F1 score
Obtained value	93%	0.93	0.97	0.94

Table 1.Obtained values of performance parameters for proposed model

	Precision	**Recall**	**F1 Score**	**Support**
0	0.92	0.75	0.83	16
1	0.92	0.98	0.95	49
Accuracy			0.92	65
Macro avg.	0.92	0.86	0.89	65
Weighted avg,	0.92	0.92	0.92	65

Table 3.Classification report

VIII. CONCLUSION

A four-way cyber security application is built in this study for providing effective security at VIP meetings.. Face recognition is a type of biometric identification that relies on the uniqueness of a person's face for security. Liveness detection will distinguish live persons from spoofing attacks such as photos, videos or masks. Voice authentication could be useful in a variety of situations, including security, protection, education, and call-based and web-based services. This system will also generate OTPs for added security.

REFERENCES

[1]. P. Viola and M. Jones, “Rapid Object Detection using a BoostedCascade of Simple Features”, Accepted Conference on Computer Vision and Pattern Recognition, 2001, pp. 1-9

[2]. Bhavana R. Maale and Dr. Suvarna Nandyal, “Face Detection Using Haar Cascade Classifiers” International Journal of Science and Research (IJSR) Vol. 10, Issue 3, 2021, pp. 1179 – 1182

[3]. Mohammad Ashraful Hoque, Thouhidul Islam, Tanvir Ahmed, Al Amin “Autonomous Face Detection System from Real-time Video Streaming for Ensuring the IntelligenceSecurity System” International conference on advance computing and communication systems, 2020, pp. 261-265.

[4]. Abdelrahamn Ashraf Mohamed, Marwan Mohamed Nagah, Mohamed Gamal Abdelmonem, Mohamed Yasser Ahmed, Mahmoud El-Sahhar, Fatma Helmy Ismail, “Face Liveness Detection Using a sequential CNN Technique”, IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 1483-1488

[5]. Shivani Shenai, Gaurav Patil, Vedant Sawant, Muskan Paryani, Rupali Hande, “Fast Biometric Authentication System Based on Audio-Visual Fusion” 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) ,2021, pp. 1520 – 1526

[6]. https://www.geeksforgeeks.org

[7]. Xinman Zhang1, Dongxu Cheng 1, Pukun Jia2, Yixuan Dai1, And Xuebin Xu3, “An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice” IEEE Access Published 0n 1 June 2020, Vol. 8, 2020, pp. 102757- 102772