Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)

doi:10.3233/ATDE221260

Covid-19 Contactless Remedies for Students in Educational Institutes

Yashu Swami[a]
[a] *Department of ECE, Aditya Engineering College (A), Surampalem, India*

Abstract. As we all know fingerprint recognition is one of the secure and accurate Biometric Technologies. If think about it in deep even with the Biometric system the virus can be spread during these situations. To overcome this, we need to come up with a secure and contactless way of authentication. So, let's update to some contactless remedies like Iris authentication which are unique for every individual and they don't need to have any physical contact. So, we can use this Iris detection for a secure and contactless authentication system. The main aim of this research is to provide contactless remedies for students in Educational institutes like Smart Locking system, Attendance management system, and Library Transaction by using their Iris authentication and Face Recognition. Coming to the outline of the attendance management system, we will first collect the data from the Kaggle repository. Next, we split the data into training and testing, then we will train the data using transfer learning techniques and test the model by using test data. Finally, we integrated the trained model with the flask. If the Iris matches then the attendance of a particular person will be posted. If not matched then we train the model by adding new person's data. For the construction of modern electronic security systems, real-time face recognition is crucial. Face detection, feature extraction, and face recognition are the three procedures involved. After recognizing the face, it will check whether the person's face matches the collected database. If it matches it will show the person's name, the number of books he took, and what those books are for Library transactions and in the same way the locker will be open if the person's data is matched. The proposed methods are secure and unique contactless ways of authentication for every individual. So, we can use these detection and authentication systems for secure and contactless applications. It can be successfully used for students in Educational institutes like Smart Locking system, Attendance management system, and Library Transaction by using their Iris authentication and Face Recognition. The Covid-19 infection in society will undoubtedly decline if the proposed argument is implemented.

Keywords. Covid-19, Iris Authentication, Face Recognition, Transfer Learning, Neural Networks, Attendance management system, Smart Locking system, Kaggle repository

1. Introduction

We all know how the Covid-19 has changed our lives. Because of this situation everyone should follow contactless remedies.so in this pandemic situation there a great need of contactless technologies. So, in this research you can see some contactless technologies like smart locking system, library transaction and attendance management system. And attendance management system is implemented by Iris detection and remaining smart locking system and library transaction using face detection. From this we can decrease the contact between people and minimize the increase of Covid-19 cases. The main problem statement of this research is to decrease the contact between people especially students in educational institute. The Delhi government issued a letter to senior secretaries, secretaries, autonomous organizations, and municipal corporations on March 5th, 2020, announcing the suspension of biometric attendance in its offices in order to stop the spread of the coronavirus. But on February 17th, 2020, Maharishi Valmiki Hospital in India's capital city announced that it was suspending biometric attendance as a "precautionary measure" after a number of its staff members complained to the authorities that using the biometric system causes "psychological unease" due to the coronavirus scare. The Hon'ble Prime Minister Shri Narendra Modi Ji declared a similar action on behalf of the Government of India, suspending biometric attendance in all of its offices. The National Green Tribunal, the Sports Authority of India, Goa, Maharashtra, Punjab, and many more state governments quickly turned off their biometric attendance systems. One of the many instructions given to 180 to 200 IT directors of organizations during a meeting with the Hyderabad Police Commissioner was to "Turn off Biometric attendance".

2. Literature Survey

The idea of utilizing the iris pattern for identification first surfaced in 1936. Frank Burch, an ophthalmologist, presented the idea of identifying people based on their iris patterns. Iris Recognition Using Low-Resolution Iris Image for Attendance Monitoring was carried out by Teh Mei Hsiung et al. [1]. The design of an iris recognition system is disclosed in this study based on the many factors. The optimal method to use will be chosen by comparing Daugman's Integro Differential Operator and Hough Transform, two current Iris segmentation approaches. Hough Transform has more accuracy between the two (100 percent). In 2014, Kalpana Jaswal Et al. [2] used the methodology of Iris pattern is first segmented (Daugman's Integro Differential Operator), Following a quick normalization of its constituent parts and picture enhancement, filtering is carried out utilizing wavelet decomposition and Fourier transformation. The methodology proposes using the MATLAB toolbox, allows easy image acquisition and processing.

Amena Khatun et al. [3] used MATLAB (software) in 2015 to follow the technique of picture collecting, processing, Iris localizing, modifying, matching, and sending email to the pre-defined E-mail address without human interaction. Following image processing and radius calculation (image capture), the proposed system stores the results in databases that will be utilized to compare with subsequent users' images for authentication. The system indicates that the value is matched with the recorded value and records this person's attendance if the next image matches the one that was previously saved. Face detection is a computer technique that uses artificial intelligence to recognise and extract human faces from digital photographs. This sort of technology allows for real-time monitoring and tracking of persons when combined with biometric security systems. Face detection often functions as the initial step and has a substantial influence on how subsequent activities inside the app will perform in apps that involve facial tracking, analysis, and identification. Using Eigenface and ANN for face recognition, Amritha Purushothaman et al. [4] developed a door entry system in 2018. Using the Raspberry Pi and ZigBee to construct Wireless Sensor Networks (WSN) for communication between the Raspberry Pi and other modules, Principal Component Analysis (PCA) is utilized for face recognition. The owner is notified through SMS or email when the system recognizes the visitors. Through a website or mobile device, the owner may manage access. This study offers the ideas of efficient Adicoost classifier, integral picture, and cascade classifiers, which reduce computations and produce an effective and quick detection system. Fisher faces, Eigenfaces, and Local Binary Pattern are the three most popular detection techniques (LBP). While Fisher Faces is based on Linear Discriminant Analysis (LDA), which seeks to identify features that can discriminate between two or more classes, Eigenfaces is based on PCA, where the major focus is on analyzing the dataset and finding patterns in it. LBP is an effective method that assigns binary values to each pixel by evaluating its surroundings. The article came to the conclusion that LBP is the best among the three in terms of recognition accuracy, operation time, and recognition accuracy for various distances from the camera based on the experimental findings. Kanza Gulzar [5] et al. suggested a mechanism to guarantee vehicle security. The device, which is based on Arduino, photographs the individual who is attempting to start the car. PCA is the face recognition algorithm. Only if the driver's face matches a picture stored in the database will the car start. If not, the intruder's photograph will be taken and kept for later examination.

An Intelligent Security Lock prototype that functions as a smart electronic/digital door locking system was created by Varad Pandit et al. [6]. We talk about the software system, including the app, and the lock device design. The paper offers a Bluetooth-enabled mobile app lock control solution. The lock uses cutting-edge technology to satisfy all security needs. Face recognition in the app offers secure authentication. All lock/unlock operations are recorded, along with the date and time. Additionally, it offers real-time camera monitoring and notifications for intrusion detection via the app. Therefore, the lock is a special fusion of the many security aspects listed above, offering a perfect solution to the security issue.

3. Methodology

3.1. Face Recognition

The main controlling device proposed for face recognition methodology is Raspberry Pi 3 B+. It acts as a mini computer. The input devices of the system is Web camera and a power supply is given to the Raspberry Pi. The output device of the system is DC motor and LCD module. Figure 1represents the block diagram for Face recognition.

- Web camera: Camera module is Pi camera interfacing to the Raspberry Pi module. The Resolution of the camera that we have used is 5megapixel. It has 6 LEDs which provides better lighting. When we run the code in the terminal of Raspberry Pi the video stream will start with the help of webcam.
- The power supply to the Raspberry Pi is given with the help of adapter. Here we use 5V and 2A supply.
- DC motor: If the face of a person is matched with the database, then the motor driver activates the DC motor so that we can consider that the lock of the door is opened.
- LCD module: The LCD module is used to display the result of the program. It displays the person's name that matched the face and door open. In library transaction it displays the number of books taken and name of the books.

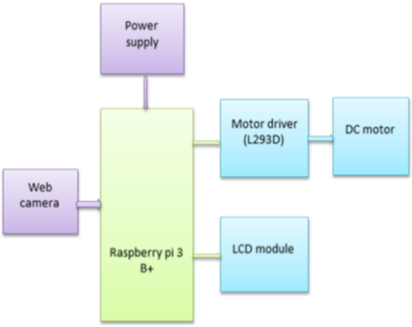

Figure 1. Block diagram for Face recognition

3.2. Iris Recognition

A biometric technique known as iris recognition uses distinctive patterns in the area of the eyeball that surrounds the pupil to identify individuals. Iris is a perfect biometric verification method since each one is distinctive to a certain person. Some of Iris acknowledgment confirmation's applications, such as the time participation framework and others, have recently been suggested due to the technology's rapid advancement. Iris recognition is popular as a method of identification because it is a very reliable biometric, highly resistant to false matches, and it can be used quickly to search through large databases, which is especially useful in fields like law enforcement and border control. Iris recognition is a powerful and incredibly reliable technique for correctly identifying people. In this we have developed an Iris based attendance system using deep learning algorithm and integrated with flask. Figure 3 represents the block diagram for Iris Authentication.

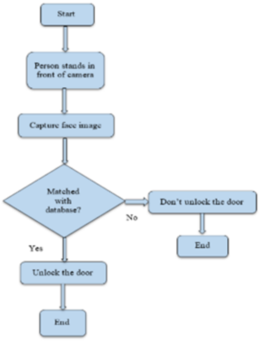

Figure 2. Flowchart of Image capturing and database comparison.

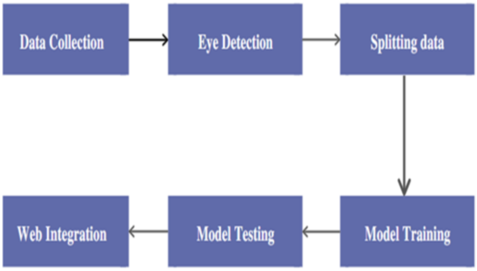

Figure 3. Block Diagram for Iris Authentication

The first block is data Collection; here we have collected the data from Kaggle repository which is an open-source dataset provider. The data consists of 15-person Iris data in which each person consists of 10 Iris images. The data that we have collected also consists of thumbnails and each image of an eye is not in a certain format. So, we have processed the data into a certain format so that every image is in the same size, color and the thumbnails are removed. Next, we have performed eye detection using eye cascade in OpenCV to verify whether the eye is present or not in every image of data that we have collected. The gathered data is then divided into training and testing data. Splitting the data into two sets is a typical method in machine learning. The training set and the testing set are these two sets. The training set is used to train the model, as the name implies, while the testing set is used to evaluate the model's accuracy. A software uses the training data as an initial batch of data to learn how to employ technologies like neural networks and create complex outputs. Splitting your dataset is essential for an unbiased evaluation of prediction performance. The test set is needed for an unbiased evaluation of the final model. We have split the data as training and testing in the ratio of 7:3.

4. Results and Discussion

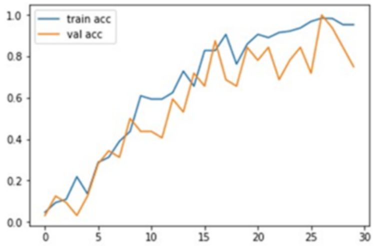

Figure 4(a). Training accuracy vs. Validation accuracy with 30 Epochs.

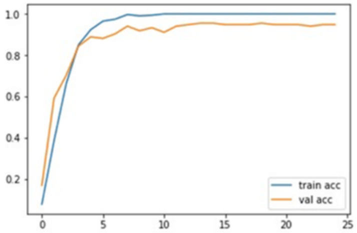

Figure 4(b). Training accuracy vs. Validation accuracy with 25 Epochs.

The plotted graphs in Figure 4(a) and 4(b) states the training accuracy and validation accuracy by taking number of epochs and accuracy as parameters. Accuracy is the amount of correct classifications or the total amount of classifications. The training accuracy is defined as the accuracy of a model on examples it was constructed on. The testing accuracy is the accuracy of a model on examples it has not seen. In ideal case, training accuracy must be higher than validation accuracy.

The plotted graphs in Figure 5(a) and 5(b) gives the training loss and validation loss by taking number of epochs and loss function as parameters. Training loss is the error on the training set of data. Validation loss is the error after running the validation set of data through training loss is the average of the losses over each batch of training data. When the epochs increase both validation and training error drops. If the training loss is much lower than validation loss then the network might be over fitting, to reduce it the network size has to be the trained network. In ideal case, training loss is much higher than the testing loss because decreased.

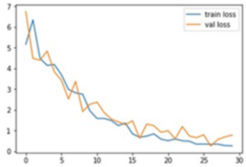

Figure 5(a). Training Loss vs. Validation Loss with 30 Epochs.

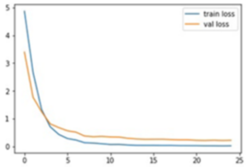

Figure 5(b). Training Loss vs. Validation Loss with 25 Epochs.

The LCD displays the output of the video stream and tries to capture the person's face through face matching as shown in Figure. 6(a). If the face of the person matches then it displays as "PERSONX MATCH DOOR OPEN" on the LCD shown in Figure 6(b). So, this will result to open the door of the locker automatically. As an indication the DC motor will be rotate for 2 sec. If the face of the person doesn't match then it displays as "UNKNOWN PERSON". So, this will result to unlock the door and DC motor will not rotate.

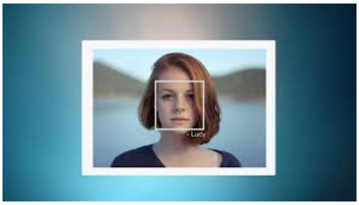

Figure 6(a). Face Matching

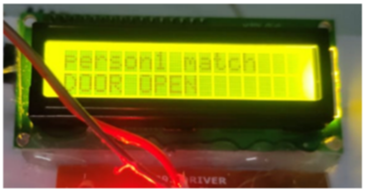

Figure 6(b). LCD display output for smart locking.

Similarly, we can use the same logic for other student transactions and works also like library transactions, assignment collection, paper submission etc. Hence, we can overcome the fingerprint recognition threat as we know through Biometric system, the virus can easily spread. The proposed methods are secure and unique contactless ways of authentication for every individual. So, we can use these detection and authentication systems for secure and contactless applications. It can be successfully used for students in Educational institutes like Smart Locking system, Attendance management system and Library Transaction by using their Iris authentication and Face Recognition. The Covid-19 infection in society will undoubtedly decline if the proposed argument is put into practise.

References

[1] Teh Wei Hsiung and Shahrizat Shaik Mohamed, "Performance of Iris Recognition using Low-Resolution Iris Image for Attendance Monitoring", School of Science, Information & Engineering, KDU College, 2011.

[2] Kalpana Jaswal, Sanchita Kadambari, Praveen Kumar, Seema Rawat, "Methodology for Iris Recognition for Application in Biometric Systems", Amity University, Noida, October 2014.

[3] Amena Khatun, A. K. M. Fazlul Haque, Sabbir Ahmed, Mohammad Mahfujur Rahman, "Design and Implementation of Iris Recognition Based Attendance Management System", Daffodil International University, 21-23 May 2015.

[4] Amritha Purushothaman, Suja Palaniswamy, "Pose and Illumination Face Recognition for Automation of Door Lock System", Amrita School of Engineering, ICICCT 2018.

[5] Gulzar, Kanza, Jun Sang, and Omar Tariq, "A cost effective method for automobile security based on detection and recognition of human face", 2nd International Conference on Image, Vision and Computing (ICIVC), IEEE, 2017.

[6] Varad Pandit, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga, Prof.Sachin Bojewar, "Intelligent Security Lock", Vidyalankar Institute of Technology, International Conference on Trends in Electronics and Informatics ICEI 2017.