International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Debit Card Transaction using Face Recognition for Authentication in ATM Machine

Dr. Dayanand Jamkhandikar[1], Simra Maheen[2], Sara Fatima[3], Sohila Fatima[4], Sneha Reddy[5]

[1,2,3,4]*Guru Nanak Dev Engineering College, Karnataka, India*

Abstract – *Debit cards are used for making the transactions at various places including ATM. These transactions use only 4-digit PIN number for identification. In this paper, we propose a system that replaces the vulnerability of an existing system which carries debit card transaction using PIN along with face recognition. All the authorized user faces are recorded and stored in a database. Whenever the user enters in ATM for Debit card transaction the system will ask for the PIN if it is correct then it captures the photograph of the user which is matched with the database. If mach is found the system allows the user to continue with the transactions else the user will be declined to make the transaction even if PIN is correct. The proposed system integrates with the face detection and face recognition technology using OpenCV algorithms.*

Key Words: **ATM Transactions, Machine Learning, OpenCV, LBPH, Facial Recognition, Haar - Cascade Classifier.**

1. INTRODUCTION

Nowadays, debit cards are used worldwide. Debit cards are fast becoming the most common payment method of big purchasers. Debit cards and the pin codes of the debit card can be stolen or lost. The proposed solution provides a secure method for debit card authentication using suitable algorithm. We have implemented ideas for "Debit card authentication" based on facial recognition. The proposed solution provides a method for credit card transaction system which will integrate with the face detection and face recognition technology using Haar Cascade algorithms.

1.2 Objectives

- The overall objective is to proceed a debit card transaction in ATM machines only the face of a user is recognized.
- To detect faces real time.
- To recognize the detected face by the use of suitable algorithm.
- If the face matches, then proceed it for transaction.

1.2 Scope of the Project

We are setting up a design a system comprising of two modules. The first module (face detector), which is basically a camera application that captures the face of the user and store it in a file using computer vision face detection algorithms and face extraction techniques. The second module is a desktop application that does face recognition of the captured images in the file and then proceed it for transaction.

1.3 Existing System

Debit card is entered into ATM machine, you just need to swipe the card and enter 4-digit PIN number then select the type of Transaction like to make withdrawals, view your balance or transfer money etc. Debit card fraud is becoming the biggest risk in debit card transactions. Debit cards and the pin codes of the debit card can be stolen or lost. This may commonly occur when users give their credit card numbers to unfamiliar individuals or when cards are lost.

1.4 Proposed System

Proposed system is designed with following objectives:
1. First step is to capture the face of the debit card user.
2. Store the captured image in database.
3. Facial Recognition techniques used.

- The first step is to find a good database of faces with multiple images for each individual.
- The next step is to detect faces in the database images and use them to train the face recognizer.
- The third step is to test the face recognizer to recognize faces it was trained for.

4. Query the captured face of a person by detecting the features of a face that is store in database.
5. If face matches, then processed for transaction.

2. LITERATURE SURVEY

Different Algorithms and techniques have been designed to implement the facial recognition as a key element for authentication of card holder. These cards were not normal office cards or any other card than the credit card. Many institutions use e-ID cards as access control authorization, it means that one just needs to possess card in order to get access to resources e.g. room or elevator. In such a scenario it is sufficient to steal or duplicate a card of legitimate user in order to get all its credentials. It is also possible to borrow such an e-ID card from third parties in an unlimited way.

Based on these arguments we propose a new solution preventing from using electronic cards by unauthorized persons as well as limiting the usage of stolen cards. Simultaneously the whole system should be as transparent as possible for users and not force them to change their habits in major way. We aim to provide such a solution that fulfils the following criteria: it is based on electronic card technology, almost transparent for users, does not require any special additional actions, increases system security, and eliminates undesired behaviors e.g. borrowing cards. In face recognition, there are also various techniques. Some of them are: -Linear Binary Pattern -Eigen faces -Fisher faces.

3. DESIGN

3.1 Architecture

The overall system architecture is shown as a use case diagram in fig 1. It shows the detection and recognition process. Subject A and B are positioned in front of the webcam. The detector will then load the cascade classifier for detecting the Haar-like features. After detecting the faces the detector will forward the coordinates of the detected faces to the recognizer. Then the recognizer tries to recognize the subject. If the recognition process was successful and display the name over the previously drawn rectangle.

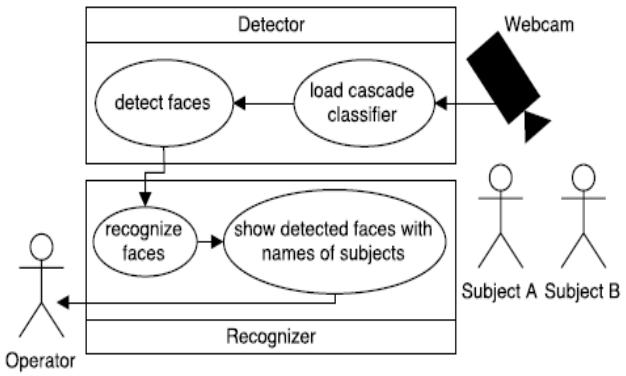


Fig 3.1 Use Case Diagram

3.2 Face Detection

Face detection is a computer technology being used in a variety of applications that identifies human faces in digital images. Face detection also refers to the psychological process by which humans locate and attend to faces in a visual scene.

Haar - Cascade Classifier

Haar like features are rectangular patterns in data. A cascade is a series of "Haar-like features" that are combined to form a classifier. A Haar wavelet is a mathematical function that produces square wave output. Haar like features, which is a trained cascade Due to its efficiency, Haar-like rectangle features have become a popular choice as image features in the context off detection. We compare our rectangular features with Haar like features Haar-like features are attributes extracted from images used in pattern recognition.

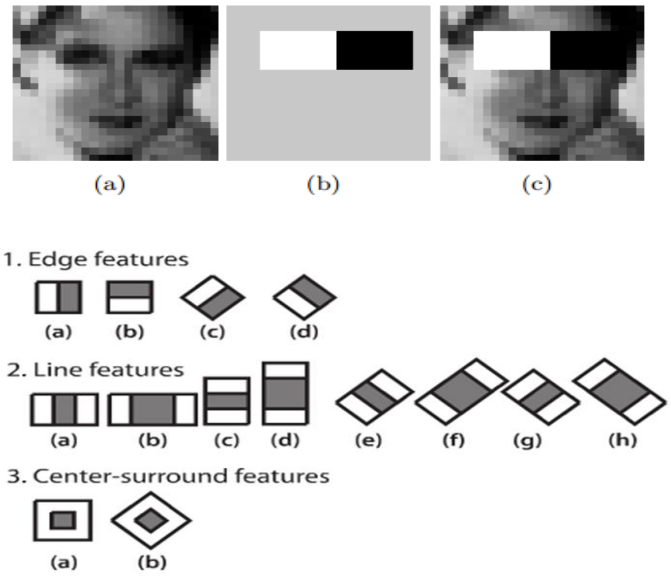


Fig 3.2 Haar like Features

3.3 Face Recognition Process

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database.

3.3.1 Creating Database

1. Read videos frame by frame.
2. Process each frame to recognize faces so we will need face recognizer.
3. Crop and save each recognized face as an image under the appropriate file path.

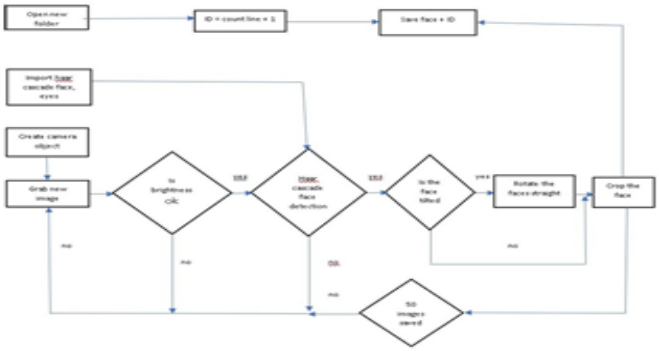


Fig 3.3 The Flowchart for the image collection

3.3.2 Training the Classifiers

Fig 3.4 Flowchart of the training application

learning is a collection of faces of people or subjects that your system is built to recognize. These training sets store face label pairs i.e. face images with their names. The face images are obtained from multiple snaps of people who the system has to recognize such that each person's set of snaps covers all possible facial expressions, posture and light conditions that may be possible at recognition time. A faces database can be implemented as a folder in Windows or as a table Database Management System (DBMS) like MS Access.

3.3.3 Local Binary Pattern

LBP is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. It has further been determined that when LBP is combined with histograms of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets. Using the LBP combined with histograms we can represent the face images with a simple data vector.

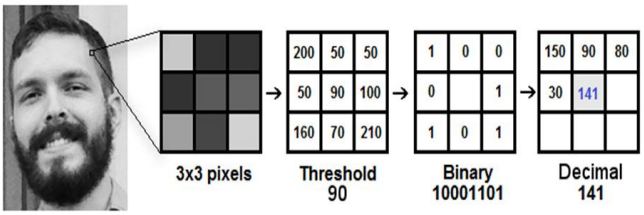


Fig 3.5 Local binary pattern histogram generating 8-bit number

The advantage of this technique is even if the luminosity of the image is changed as in fig 3.10, the result is the same as before. Histograms are used in larger cells to and the frequency of occurrences of values making process faster. By analyzing the results in the cell, edges can be detected as the values change. By computing the values of all cells and concatenating the histograms, feature vectors can be obtained. Images can be classified by processing with an ID attached. Input images are classified using the same process and compared with the dataset and distance is obtained. By setting up a threshold, it can be identified if it is a known or unknown face. Eigenface and Fisherface compute the dominant features of the whole training set while LBPH analyze them individually.

3.3.4 The Face Recognition

Face detector is used to detect faces in the image, cropped and transferred to be recognized.

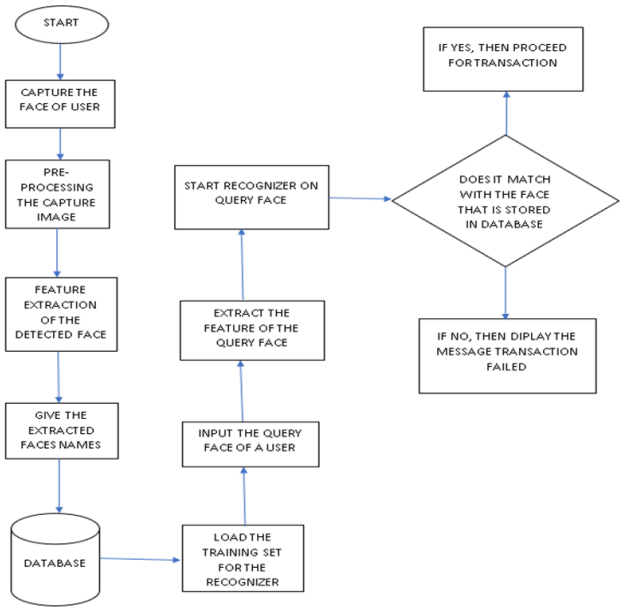


Fig 3.6 Sequence of events

3.4 Display the Transaction Message

Once the face recognition process is completed count will automatically increase by one. It asks for user id to calculate the count. If the face matches and the system will ask for the pin for more security. If the pin matches, it will proceed for transaction and displays the message that the transaction is completed. Suppose the pin entered is wrong then the system will display the message transaction declined due to wrong password.

3.5 Overall Flow Diagram of System

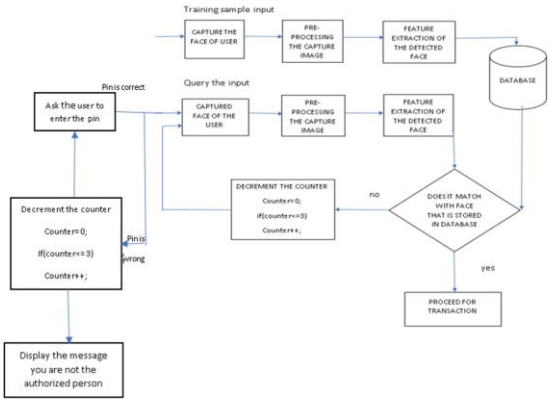


Fig 3.7 The final architecture of the proposed system

4. EXPERIMENTAL SETUP

4.1 Tools

The following tools are used in the implementation of the proposed system.

4.1.1 Opencv

The OpenCV algorithms could be performed, a software had to be developed which implements the face detection and recognition algorithm. Implementing the recognition algorithm requires to also implement OpenCV's face trainer.

4.1.2 python 3.6

Python is a popular programming language available for most modern computer operating systems. Python IDLE is an environment for writing, editing, debugging and running Python programs. It is included when you install the standard set of Python tools.

4.2 Modules Implementation

1. Creating database
2. Recording faces
3. Face Recognition
4. Video or image tester
5. Display transaction message

5. EXPREMENTAL RESULTS

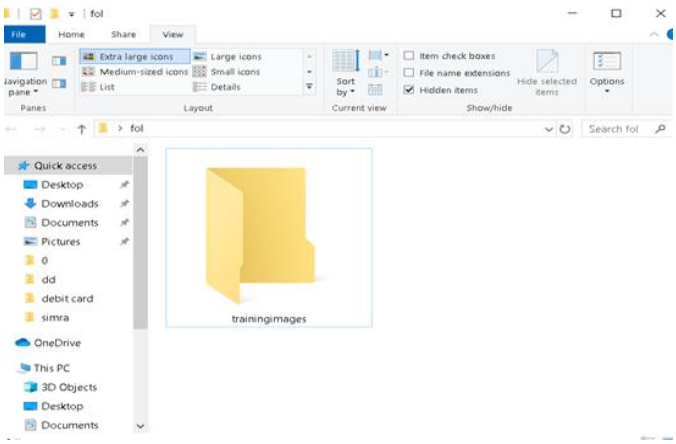
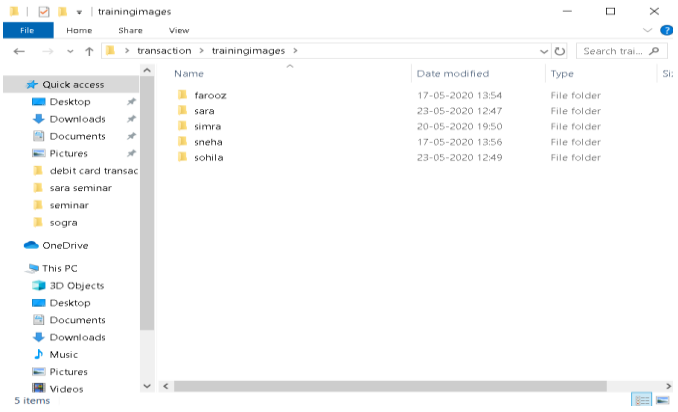


Fig 5.1 snapshot of training images folder

The images which is captured is store in a training images folder The Image is then cropped after capturing few sample faces of one person the live video frame and assign a ID to each image in it and it will save those samples in a folder labelled with 0,1,2...so no inside training images folder.



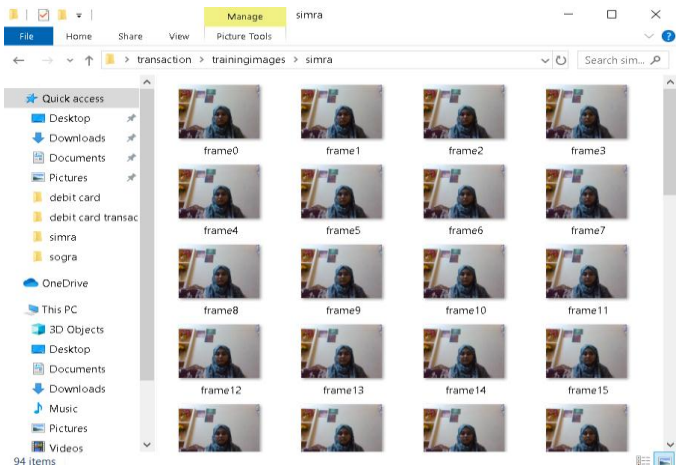


Fig 5.2 snapshot of the entire user's image folder

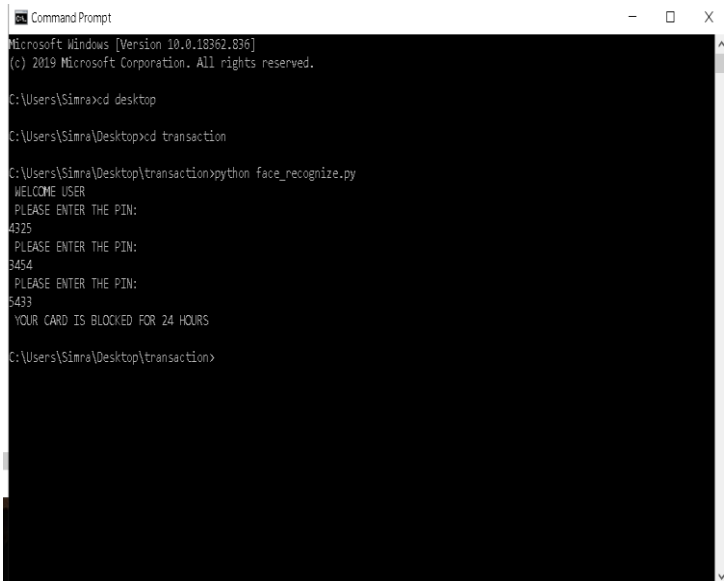


Fig 5.3 snapshot of a command the PIN enter by the user is wrong

Fig 5.4 snapshot of a command the PIN enter by the user is correct

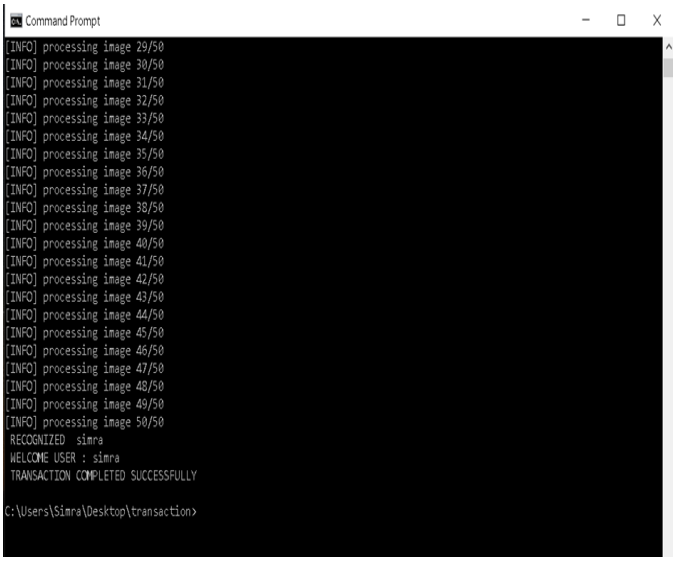


Fig 5.5 snapshot of a command displaying transaction message successful after face recognition

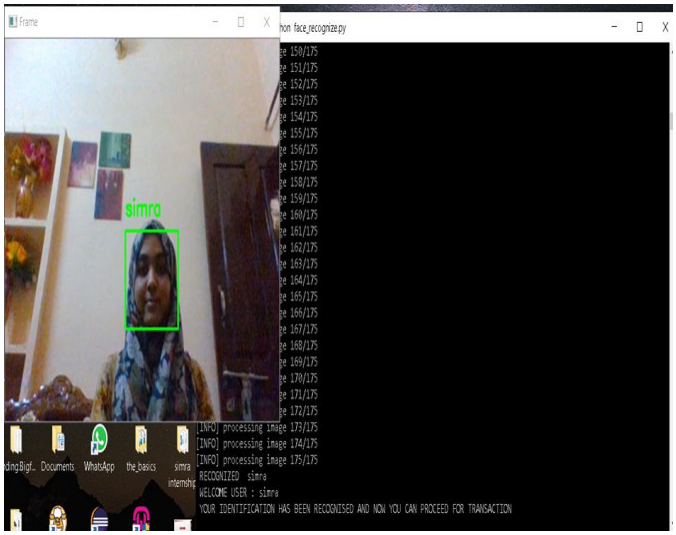


Fig 5.6 snapshot 1 of a command displaying your identification message successful after face recognition (true case)

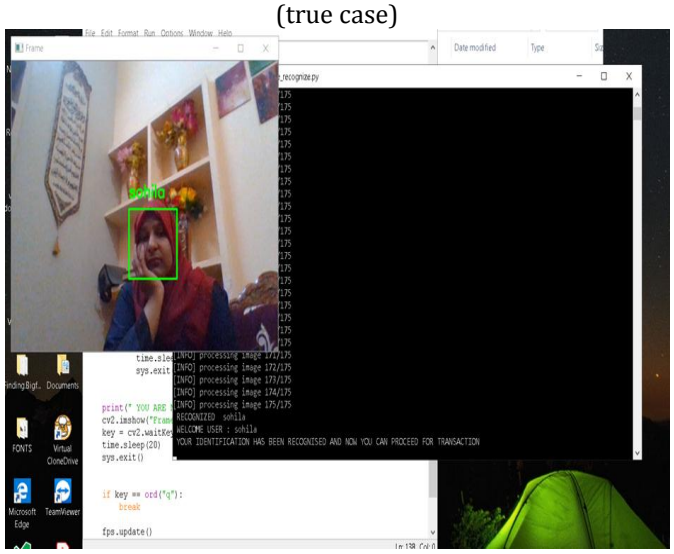


Fig 5.7 snapshot 2 of a command displaying your identification message successful after face recognition (true case)

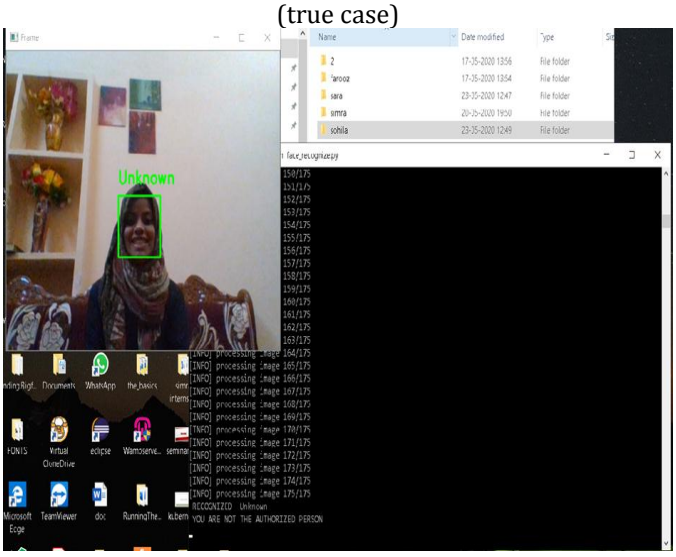


Fig 5.8 snapshot of a command displaying you are not the authorized person after face recognition (false case)

6. CONCLUSION AND FUTURE SCOPE

Purpose of Our proposed project on debit card authentication using face recognition is reducing debit card frauds that may occur in ATM payment process. The proposed system employs Haar wavelet transform to capture the features of the face. The experimental results show that the performance is satisfactory. The proposed system can further improve by employing deep convolution network for better results. All current face recognition algorithms fail under the vastly varying external conditions. Hence a framework invariant to external conditions will be certainly useful.

REFERENCES

[1] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 6, June 2016

[2] Shang-Hung Lin, 'An Introduction to Face Recognition Technology', Informing Science Special Issue on Multimedia Informing Technologies – Part 2, Vol.3, No.1, (2000).

[3] Dr.Pramod Kumar, Mrs. Monika Agarwal, Miss. Stuti Nagar, 'A Survey on Face Recognition System - A Challenge',International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, (2013).

[4] P. Mohanaiah, P. Sathyanarayana, L. GuruKumar, 'Image Texture Feature Extraction Using GLCM Approach', International Journal of Scientific and Research Publications, Volume 3, Issue 5, (2013)

[5] AlaaEleyan, Hasan Demirel, 'Co-occurrence matrix and its statistical features as a new approach for face recognition', Turk J ElecEng& Comp Sci, Vol.19, No.1, (2011).

[6] 'Securing ATM by Facial Recognition Authentication" P. Muniasamy1 , S. Joney Babayal2 1,2Assistant Professor in Computer Science, Ayya Nadar Janaki Ammal College, Sivakasi

[7] Paul Viola and Michael J. Jones. Robust real-time face detection. International Journal of Computer Vision, 57(2):137–154, 2004.

[8] Ahonen, Timo, Abdenour Hadid, and Matti Pietikainen. "Face description with local binary patterns: Application to face recognition." IEEE transactions on pattern analysis and machine intelligence 28.12 (2006): 2037–2041.

[9] Face recognition with OpenCV, Python, and deep learning by Adrian Rosebrock on June 18, 2018.