Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

CrossRef DOI of original article: 10.34257/GJCSTGVOL20IS6PG29

Smart Lock using Image Recognition

Afnanul Hassan[1], Zaria Fahamida[2], Proloy Sen[3] and Dr. Syed Akhter Hossain[4]

[1] Daffodil International University

Received: 6 December 2019 Accepted: 1 January 2020 Published: 15 January 2020

Abstract

In the 21st century, for a digital lifestyle in a smart city, security is one of the core ingredients to ensure digital continuity. The existing smart security technologies use a smartphone, card, and fingerprint that need additional devices to carry or can spread out infectious diseases. Now it is high time to think about an additional device free and more timeconsuming technique. So, an intelligent system is proposed in this paper to secure our doors with face authentication. The human face is a unique and easy identifying feature of a human. The registered user?s image is saved in the device as a dataset to train the lock. The system recognizes the registered faces very fast and controls the hardware part to be unlocked. The system is capable of detecting and recognizing human faces from a real-time video. It is usable in the door lock, car lock, hutch, and many more security purposes.

Index terms— face detection, image recognition, open CV, smart lock, raspberry Pi.

1 Introduction

ay after day, we are moving towards modernity. But the percentage of home robbed and things stolen is 70.5% [1] of the total crime in the last ten years, and it is escalating, which is a barrier to our smart lifestyle. The existing smart technologies of door security needs memorizing a password or carrying additional devices like mobile phone, cards. Being stolen or lost the additional devices or forgetting the password can hamper the existing smart security systems. Changing the hand of the additional device or getting the password leaked can allow any stranger to pass through the lock. Besides that, the fingerprint system can spread out infectious diseases. Many authors proposed various kinds of digital door locks, password-based locks, etc. [2]. But the solution proposed in this paper is to recognize the valid user's face to unlock the lock because faces are one of the most important visual stimuli [3]. Also, it is a unique feature of every man. From a real-time video, the image of a human face is detected and recognized using the LBPH (Local Binary Pattern Histogram) algorithm. LBPH algorithm has become a standard and mostly used image recognition and detecting technique. Compared with other algorithms LBPH algorithm cannot only recognize the frontal face but also recognize the side face. This algorithm is widely used for image recognition. So, the face authentication technique for security purposes can be a timely and more intelligent idea.

The paper is organized as follows. Section II summarizes the previous works done by many authors. Section III describes the complete architecture of the proposed system with details of the used algorithm. Section IV contains the conclusion.

2 II.

3 Related Works

Onoyan A.O. et al. [4] has developed a biometric-based door lock system by using ATMEGA 328 Arduino microcontroller, fingerprint scanner R305. When the fingerprint be matched with the registered fingerprints, a signal is sent to incite the door lock process, and the door stays open for 5 seconds. Adarsh V Patil et al. [5] has manifested an android based smart door locking system. Arduino Uno, android, smartphones have been

used to complete this lock security system. A pre-determined password concept is used. Anuradha R.S et al. [6] has proposed an optimized locking and unlocking a process by using a wireless system. The proposed idea had been implemented by using Arduino Uno, DC motor, Wi-Fi. This system aimed to allow a user to lock and unlock a door within the Wi-Fi range from inside or outside a house. Agbo David O et al. [7] has implemented a door locking system using an android app and the Bluetooth module. The app could be connected with the Bluetooth module HC-05 to show the current activity about the door is open or close. If the password is correct, the door will be opened. Otherwise, it will be kept closed. Janaki Venukumar et al. [8] stated that security is the most vital issue nowadays for us when we are out of our households. The proposed project shows a keyless system for operating lock using a pre-defined password. To get entered the must memorize the password. Lia Kamelia et al. [9] proposed that present days are the era of living in smart technology. So, the term "smart home" gives broad thinking to us of living in new technologies. To make the smart home just using the device of our pocket, the mobile phone where Bluetooth will be enough to communicate with devices. Arvasu Chikara et al. [10] proposed a solution for the bank system to secure our money because a bank deserves an extra level of security. The solution is a combination of fingerprint authentication and face authentication. The image and fingerprint data of the authentic persons are saved by the bank authority in the database. The authentic person must match both face and fingerprint to have access to the money of the bank.

The idea of a smart home lock with automated technologies is practiced throughout this decade. But most of them are developed to work with an android device. Some use Bluetooth and some Wi-Fi. Both of these need an additional device to use the lock. Fingerprint and pre-defined password systems reduced the necessity of extra device but needed user interaction. Moreover, the fingerprint authentication system can spread infectious diseases. Besides all of these systems, our proposed system will work without an additional device and user interaction. The system will just see the user and be unlocked after authentication.

4 III.

5 System Architecture

The proposed system has an aim to protect premises and belongings smartly and without the necessity of an additional device. It just recognizes the authorized user's faces to unlock the lock. This process can make life easier. In the proposed system, the lock needs to detect and recognize the human face. So, the proposed lock consists of Raspberry Pi 3 which is a lowcost mini-computer in credit card size., which comes with Bluetooth 4.1 and a camera. As shown in Fig. 1 the whole process has two main parts, such as (a) Registration Process and (b) Unlocking process. At the registration process, the 1st user starts from inputting information like name, and then the lock detects and saves 20 images of the user's face to train. On the other hand, any new user must be verified by inputting any previous user's information like name. After training, the lock will be ready to be unlocked, and at the unlocking process, the lock keeps capturing video. If any registered user's face is recognized, it will stay open for 7 seconds and then becomes ready to be locked again. The complete system architecture can be described in 5 main steps.

6 a) Receiving User Data via Bluetooth

At the very beginning, the lock needs registered users with face's images to know who is the authentic person. The user can use a mobile application that provides an entirely user-friendly interface to input user data. This is the one and the only use of any additional device. The lock, which is made with Raspberry Pi 3, receives the user information via Bluetooth 4.1 from the mobile application. The 1st user can be registered without hassle. But in the case of multiple users, other users must input any previous user's information to be registered.

7 b) Face Detection and Dataset Creation

While the data of new users be received, the lock itself starts capturing real-time video to detect any face. From the video, if any human face is found, the system saves the image's ROI (Region of Interest). Thus 20 faces will be saved along with the name of the new user.

While detecting face, the system converts each frame of video into grayscale to make the task easier. Using the Numpy library, the grayscale image can be converted into an n-dimensional array.

In this case, the OpenCV (Open Source Computer Vision) python library works with the Haarcascade classifier to classify human frontal face, and except ROI (Region of Interest) other numbers of the n-dimensional array will be changed into "0". Thus, the ROI of the face will be classified, and only the face is captured and saved in the lock's dataset. The dataset is created uniquely for an individual lock. So, authentic faces for a deferent lock is different.

8 c) Training Dataset

The Face detection procedure cannot be completed without training the system according to the dataset. The dataset is combined with the user's name, ID, and image of the user. The name and ID are received from the Android app, and the camera itself will capture the pictures of faces after detection. Combining all of these a

file with .yml extension is created to work. When the file is created, the camera becomes ready to recognize the authentic face. The training procedure is done by following the LBPH algorithm.

The LBPH Face Recognizer is a mostly used face detection algorithm [11]. It works with the Numpy array, which is an n-dimensional Array created from the grayscale image of the input image. Now the algorithm is going to be discussed.

The n-dimensional array mainly contains the density of white in every pixel from the range of 0 to 255. As shown in the following Fig. **??** value of every pixel be compared with neighboring pixels in radius 'r'. Here for the pixel threshold, 90 is compared with the neighboring pixel in radius, r = 1. Lower and equal values than the threshold values are changed into '0' otherwise changed into '1'. The binary digits from neighboring pixels can make an 8-bit binary value. Here the 8-bit value is 10001101, which is 141 in decimal. So, the new threshold value is set 141. Thus, the process continues for every pixel.

9 Fig. 2: Applying LBP operation

The LBP Operation can be applied on a large scale just by increasing the value of r. Fig. 3 is visualizing the LBP operation on a large scale if it is used with different values of r. The final histogram signifies the key image topographies of the image. The LBPH algorithm works the same for each face, and everything keeps saved in a .yml file

10 d) Recognizing Face to Unlock the Lock

This step is the most significant because the algorithm is now trained. Each histogram formed mainly signifies each image in the registered users' dataset. Henceforward, the system takes input images from the camera. For the input image of a new person, the same steps are taken to create a histogram that signifies the input image. Now the final histogram (hist2) is compared with the trained images' histogram (hist1). A difference, D is calculated for all images of n number in the dataset according to the following Eq. (**??**) [12].

The minimum value of D defines the matching with the input image and the specific image. If any matching happens, the person recognizes as an authentic person. If the person is authentic, the lock unlocks. Otherwise, it remains the same without being opened.

11 e) Unlocking the Lock

Whenever the lock recognizes any face from the database, the lock outputs a "1" that provides current to a servo motor. The servo motor rotates a disk, and the disc helps to unlock the lock. The mechanism of working is shown in Fig. 5. Where the servo motor can turn the wheel, and the wheel works to lock and unlock the device.

12 Expected result and Discussion

The proposed idea can register new faces and then identify those to open the lock. the dataset is created with registered users' frontal faces to train the machine. The system takes 20 faces of each user. The faces are saved with the user name and unique ID. Fig. 6 shows the dataset creates for an individual user. After training the proposed system waits for the registered faces and if found it opens within a moment otherwise remains closed. The effectiveness or accuracy of the system is calculated using Eq. (2) [13].

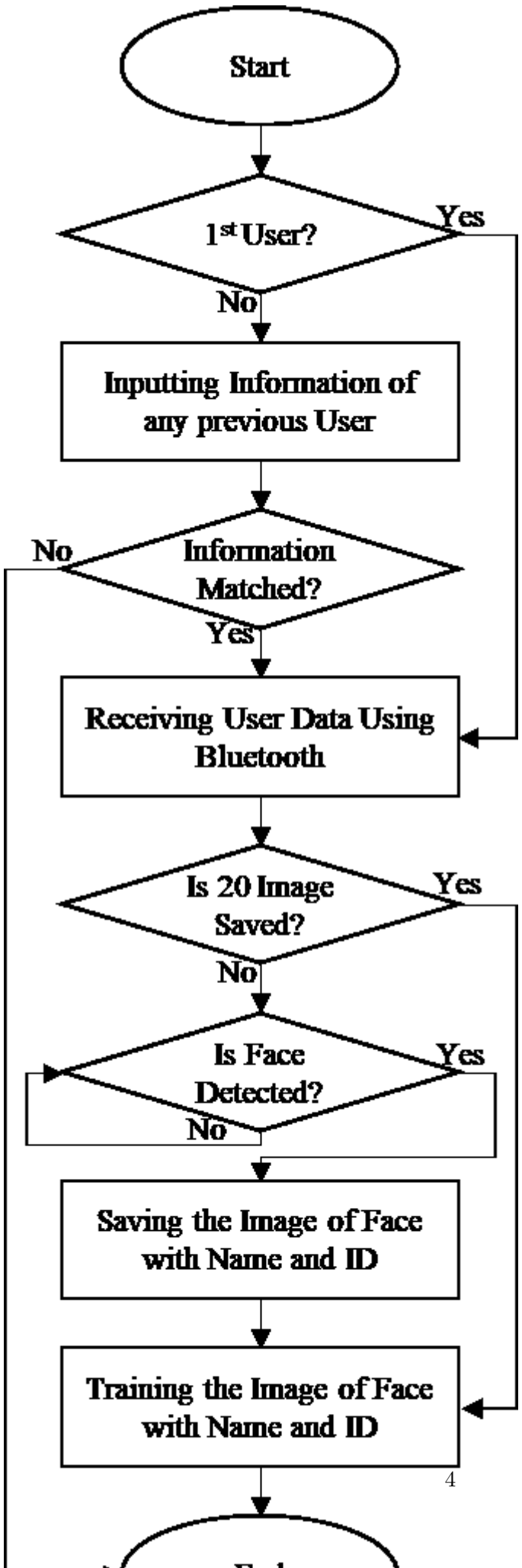
The accuracy is measured by counting the number of correct predictions and the total number of predictions. For this proposed idea the accuracy is calculated 76%. A quality camera and enough light give a more accurate performance. The process is so fast that it takes about no time to be unlocked if any registered face is found.

V.

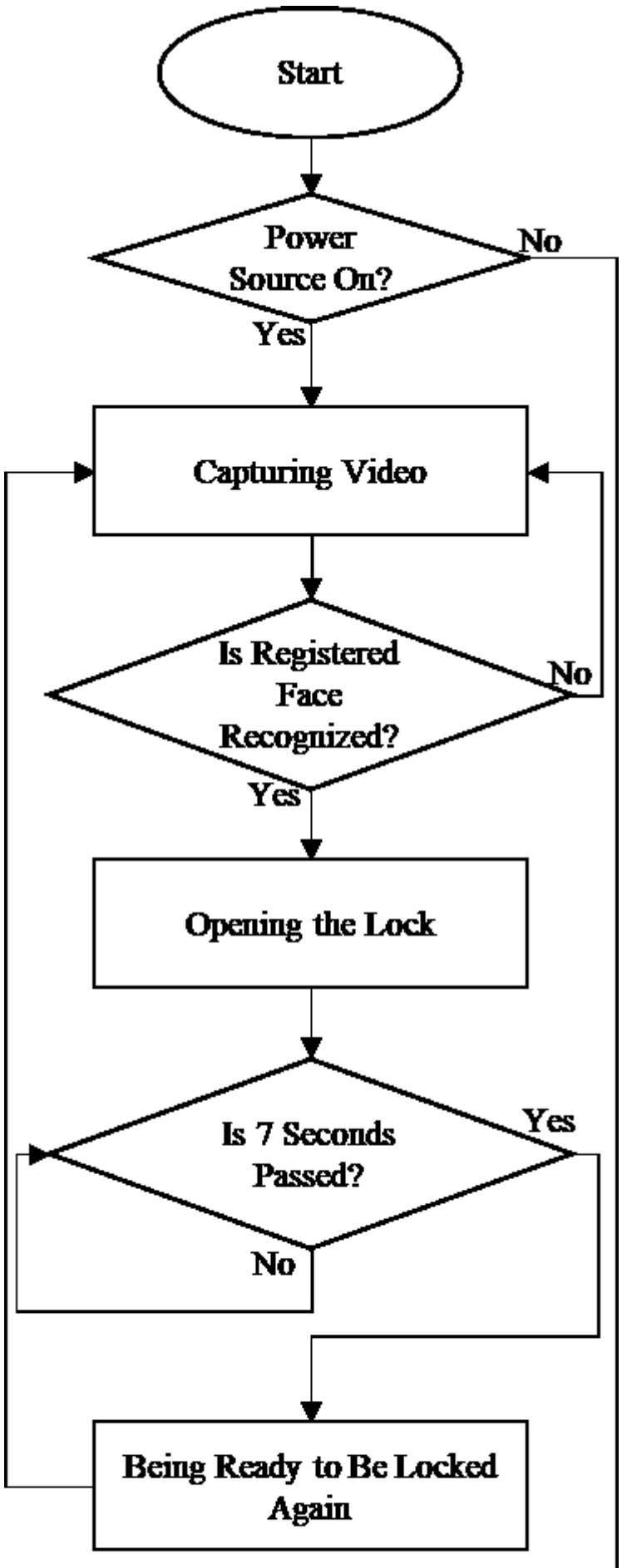
13 Conclusion

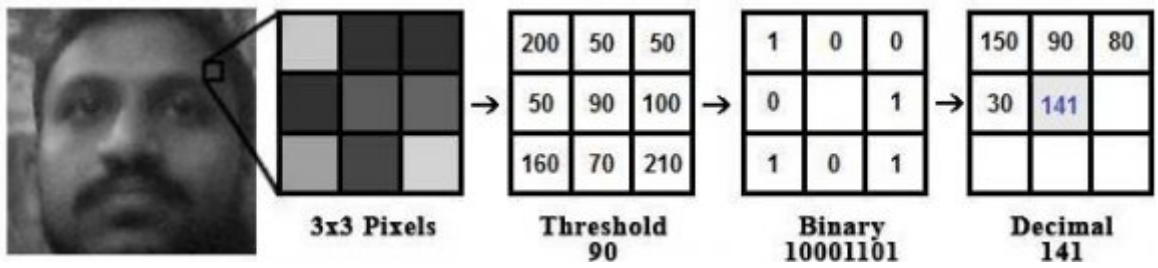
The proposed idea of using image recognition in a lock can make lives smarter. The system uses the

OpenCV computer vision library to recognize the authentic registered user by image processing. Working with every pixel of an image makes the system more accurate. According to the registered users' dataset it can recognize faces accurately. In low light, it may take a few more seconds to recognize. But enough light gives a perfect service. The experimental result shows that the system can detect and recognize one or more than one face from a real-time video. At least one authentic face is enough to open the lock. The system can be widely used in any security purposes like a door, car, hutch, etc. [1]



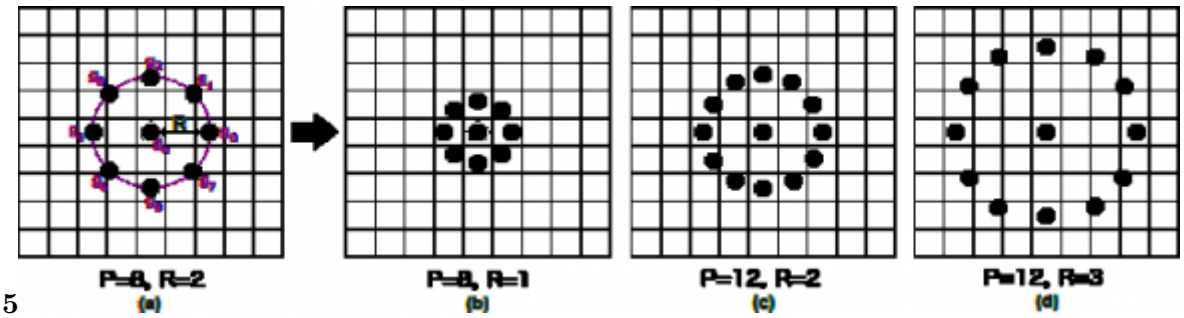
10.34257/GJCSTGVOL20IS6PG29


Start
Power Source On?
No
Yes
Capturing Video
Is Registered Face Recognized?
No
Yes
Opening the Lock
Is 7 Seconds Passed?
Yes
No
Being Ready to Be Locked Again



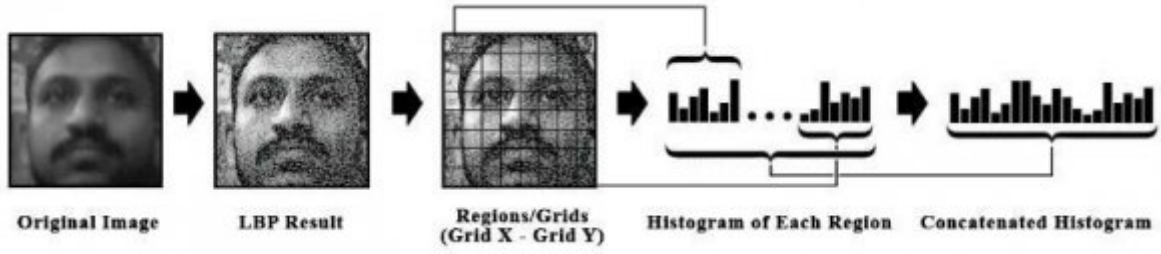
4

Figure 3: Fig. 4 :



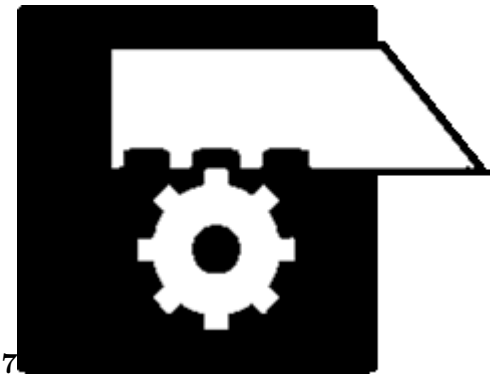
5

Figure 4: Fig. 5 :



6

Figure 5: Fig. 6 :



7

Figure 6: Fig. 7 :

Figure 7:

[Leopold and Rhodes ()] 'A Comparative view of face perception'. D A Leopold , G Rhodes . *J. Comp. Psychol* 2010. 124 (3) p. .

[Patil et al.] *Android Based Smart Door Locking System*, A Patil , Ch Patgar , S Prakash , S A Kumar , J .

[Venukumar ()] 'Arduino Based Door Access Control'. J Venukumar . *Int. J. Res. Advent Technol* 2016. 4 (8) .

[Kamelia et al. ()] *Door-Automation System Using Bluetooth-Based Android for Mobile Phone*, L Kamelia , A Noorhassan , M Sanjaya , E Mulyana . 2014. 9.

[Ahmed et al. (2018)] 'LBPH based improved face recognition at low resolution'. A Ahmed , J Guo , F Ali , F Deeba , A Ahmed . *Int. Conf. Artif. Intell. Big Data, ICAIBD* 2018. 2018. May. 2018. p. .

[Nehete et al. ()] *Literature Survey on Door Lock Security Systems*, P R Nehete , J P Chaudhari , S R Pachpande , K P Rane . 2016.

[Local Gabor Binary Pattern Histogram Sequence (LGBPHS): A novel non-statistical model for face representation Proc. IEEE I 'Local Gabor Binary Pattern Histogram Sequence (LGBPHS): A novel non-statistical model for face representation'. *Proc. IEEE Int. Conf. Comput. Vis*, (IEEE Int. Conf. Comput. Vis) 2005. I p. .

[Odu et al. ()] 'Low-Cost Removable (Plug-In) Electronic Password-Based Door Lock'. A David Odu , M Chinaza Alice , O J Odinya . *Am. J. Eng. Res* 2017. (6) p. .

[A. R. S. 1, B. R. 2, K. K. 3, K. S. 4, S. Venkatasubramanian, and B. E. Student ()] 'Optimized Door Locking and Unlocking Using IoT for Physically Challenged People'. *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO* A. R. S. #1, B. R. #2, K. K. #3, K. S. #4, S. Venkatasubramanian, and B. E. Student (ed.) 2007. 3297.

[Onyan and Enalume ()] *Property Security Using a Biometric Based Door Lock System*, A O Onyan , K O Enalume . 2018.

[Chikara et al. ()] *Smart Bank Locker Using Fingerprint Scanning and Image Processing*, A Chikara , P Choudekar , D Asija . 2020. p. .

[The Complete method of calculating accuracy is described in «https://developers.google.com/ machine-learning/crash-course/cla *The Complete method of calculating accuracy is described in «https://developers.google.com/ machine-learning/crash-course/classification/accur acy» accessed on 29-05-2020 at 6*, p. 20.

[The crime rate in Bangladesh is broadly] *The crime rate in Bangladesh is broadly*, `<<https://www.numbeo.com/crime/country_result.jsp` (country=Ban gladesh» accessed on 29-05-2020 at 6:20 p.m)

[Zhang et al. ()] W Zhang , S Shan , W Gao , X Chen , H Zhang ; W , S Shan , W Gao , X Chen , H Zhang . *Local Gabor Binary Pattern Histogram Sequence (LGBPHS): A novel non-statistical model Zhang*, 2005.