International Journal for Modern Trends in Science and Technology, 9(04): 156-162, 2023
Copyright © 2023 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0904025
Available online at: http://www.ijmtst.com/vol9issue04.html

Enhancement of Security System Using Arduino and Facial Points

Dr. Balamuralikrishna Thati, Chandra Sekhar Pedasingu, Jayanth Kumar Tummalaxharla, Alekhya Varre, Charmika Sanikommu, Naga Sindhu Sunkara

Dept of CSE, Dhanekula Institute of Engineering and Technology, Vijayawada

To Cite this Article
Dr. Balamuralikrishna Thati, Chandra Sekhar Pedasingu, Jayanth Kumar Tummalaxharla, Alekhya Varre, Charmika Sanikommu and Naga Sindhu Sunkara. Enhancement of Security System Using Arduino and Facial Points. International Journal for Modern Trends in Science and Technology 2023, 9(04), pp. 156-162. https://doi.org/10.46501/IJMTST0904025

Article Info
Received: 05 March 2023; Accepted: 28 March 2023; Published: 03 April 2023.

ABSTRACT

A smart home security system is a type of system that allows you to monitor and control who can enter your home. It's also very easy to use, and it's relatively affordable. Unfortunately, the main issue with a traditional security system is that it can easily be broken and can be makes it penetrable to through the Techniques and methods of the Hacking. This often leads to the robbery since the security system will require the expensive installation and have to good chunk of money to get high Accurate Results. In order to solve this issue, we have developed a smart home security system that uses both the Internet of Things and Machine Learning. The system works by connecting a web camera to a laptop and then using a neural network Algorithm to recognize faces. The system will determine whether the Detected person's image is with one of the members of the home by analyzing facial recognition of pre trained data which consists of 128 encodings for each face in the Analyzed images Because Module utilized Deals with the each and every point in the Human faces. Face Detection and Recognition will be done one after another first come face comes the Face detections and Later the Face Recognition. It will then lock the door if it doesn't match the one shown on the screen and with all the encodings of the trained data too. This type of security system is ideal for homes since it can perform multi-face recognition. If the owner wants to allow guests, the system will send a security key to the individual through a telegram with the Telegram bot. After all the Research this project had surpassed the Accuracy of the Raspberry pi as its Accuracy will too low because of its 1.5 mp tiny cam and the modifications also will be intricate but this design is facile so its best and simple which comes at very low cost and gives almost high Accurate results than any of the Face Detections Devices and the Algorithms.

KEY WORDS: Face Detection, Face Recognition, Telegram Bot, Laptop, Camera, pre trained data, 128 Encodings, Facial Points , Raspberry pi, Analyzed images. Module.

1.INTRODUCTION:

A home security system is a vital part of any household's plan to protect its valuables and keep its occupants safe from potential criminals. In the U.S., there are around 7,020 home burglaries every day. According to statistical data , over 85% of all burglaries are committed in residential areas. Also, over 48% of robberies are carried out with guns. Identity theft is on the rise in the Russia, Canada, and the United Kingdom [1], and it is predicted that over 5 out of 6 homes in the country will be broken in the next two decades. . A home security system that uses the Internet of Things and facial recognition can help prevent these crimes. The IoT will allow a system to detect motion and trigger it using sensors such as Pir and Ultrasonic[2]. This technology can also be used to determine the position of a person in front of the camera. For instance, if the distance between the camera and the person is less than 230 cm, the face detection [module can perform well. A face recognition system that uses the LBP algorithm has an accuracy of 70% when it is tested using real-time images [3]. A camera will be able to recognize the face of a person while they are in front of it, and it will compare the faces with those in the home member database that's stored in the Raspberry Pi. The CNN algorithm that's used in our design is very accurate and is very low-cost. Conventional home security system uses radio signal between windows and video surveillance to control the panel. This method can be easily cracked using various advanced technologies, such as data interception and software programming]. Another drawback of this system is that it can prevent the signal from getting through to the control panel by jamming it. This is done by sending radio noise to prevent the signal from getting through to the sensors. At present, we have introduced an Arduino-based security system that can prevent this issue.

2. AURDINO BASED SECURITY SYSTEM:

This project is about developing a security system that uses an Arduino board and a laptop. The main idea of this system is to use the micro controller to control the lock and unlock operations. The laptop is connected to the board through a sequence communication. In order to implement this system [4], we need to write a part that will allow the computer to communicate with the Arduino.

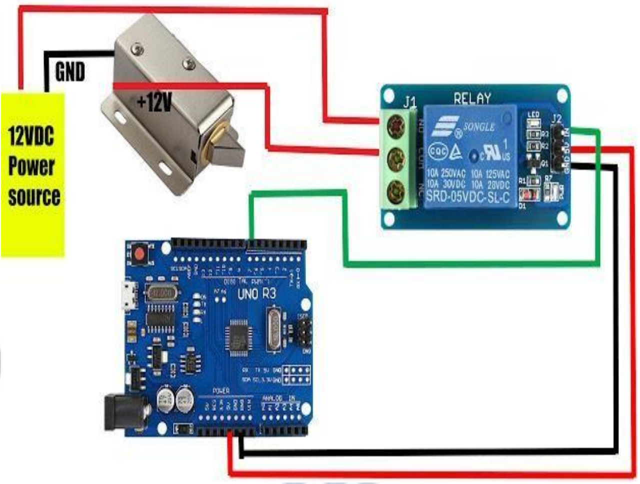


Figure 1: Established connection between the Hardware Components

As you can see Clearly the Figure 1 shows the Exact Wired Link Between the Physical Components which are used in this Design. The CNN algorithm is used in the Face recognition software. It is a very accurate and unique algorithm that is used to recognize the faces in real time. It is additionally trained with many human faces [5][6]. This makes it different from other algorithms such as the Histogram of gradients, the local binary pattern, and the Haar Cascade [7]. All of these are not very accurate and produce less accuracy than the CNN algorithm based on the Comparison between machine Learning Algorithms. The concept of the security system that uses the facial points and Arduino is to enhance the efficiency of the system by using Machine Learning and IOT [8][9]. The person who can enter the premises can be distinguished by the facial recognition that uses the HOG, ANN, or YOL algorithms. The Arduino can be used to control the door's lock and unlock system. The stored data can be accessed through the photos in the training data set. The Pictorial view can also be accessed through the software application. The goal of this project is to create a low-cost and effective security system that uses facial recognition and a camera to detect the face of a person entering the premises. The system will be using a Solenoid Lock, which is the only device that can communicate with the electromagnetic signals [10]. The training data will be stored in the software application, which will allow the owner to access the system. If he wants to allow any guests to enter the premises, he will send a message through the app. The Machine Learning Algorithm Plays the Key role.

3. LITERATURE SURVEY

This is a home security monitoring system that uses the Raspberry Pi. It features various features such as temperature monitoring and motion sensors.

Home Security Monitoring system with IOT Based Raspberry pi

Published By: I Gusti Made Ngurah Desnanjaya, LPPM STIKI Grant, LPIK

The Above Project had been developed using the Raspberry pi but they have concentrated more on the other Activities than the Face Recognition

The Raspberry pi Algorithm had been used to recognize the faces of the Human but the Clarity and the Accuracy is low. They haven't used any machine Learning Algorithms as the Raspberry have the Inbuilt Algorithm for the Face Recognition

In the Affordable Cost they have Extracted the Designs and it shown a way to connect to telegram without using the GSM Module as shown in Figure 2. This Article Focuses on the other Aspects than the Face recognition but it raised an idea to develop the best security System at Medium Cost.

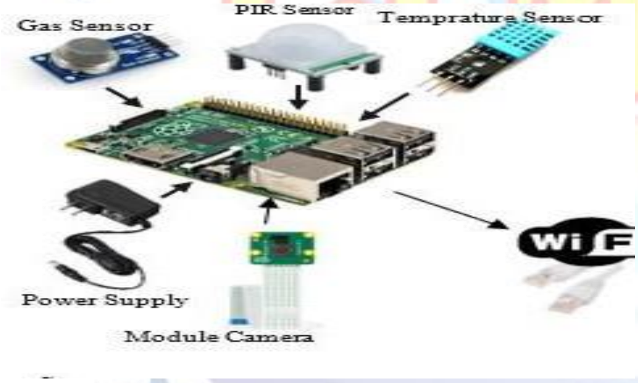


Figure 2: components Structure of Raspberry pi

Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms.

Published by: Aimin Yang, Chunying Zhang, Yongjie Chen, Yunxi Zhuansun, and Huixiang Liu. This Security system mainly Focuses on the Video Surveillance by using the machine Learning Algorithms for the Privacy and Security

The Physical Components all are implemented perfectly the thesis for this project is give Below The rise of the Internet of Things (IoT) has led to the development of smart home systems that are secure and can be accessed by users. These systems are able to collect and use data from multiple sensors in the home. The data collected by these systems can then be used to provide a remote control for the home. The security of a home is guaranteed with this IoT architecture. The software and hardware components of this system are designed according to its architecture. The image recognition and speech recognition modules are mainly utilized. In order to improve the system's accuracy, an algorithm is proposed that will match stereo.

This security System is Cost Effective

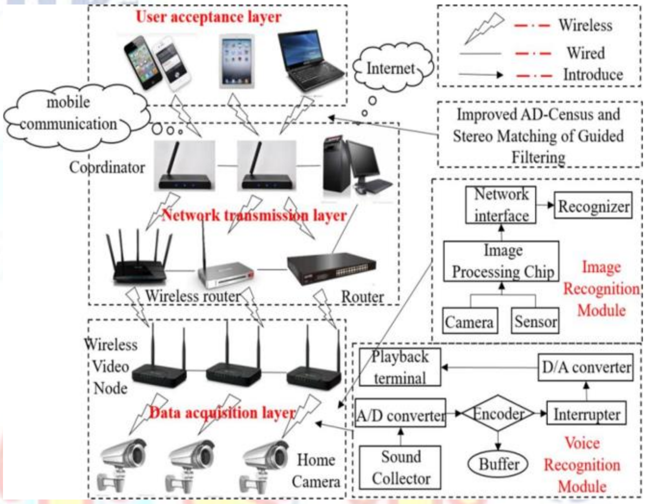


Figure 3: Advanced level monitoring System

The Most Advanced Video Surveillance the above Figure 3 explains all of the procedure and working of the Video surveillance With this we understood that the Machine Learning Algorithms can be used for the Real time Video Surveillance But there are so many modules are used in this which makes the physical or network structure too difficult to Understand but the Working and the Performance of the project is definitely best and the sensors are also used to change the mechanics of the module so that there should not be any malfunctions in the Working of this type of model using Stereo

4. METHODOLOGY

Today, everything in the digitizing world is equipped with the latest technology, but the current system is not able to provide us with the necessary security to perform our work efficiently. One of the main issues that we face is the lack of a reliable and secure connection between the camera and the Raspberry Pi. This will be solved by implementing various algorithms and sensors. In order to improve the current security system, we will use an inexpensive and easy-to-use microcontroller known as Arduino as the main controller. This will allow us to implement various sensors and algorithms that will help us monitor and control our work. In order to implement a door locking mechanism, we will use a solenoid lock, which is controlled by Arduino and a connected PC with a face recognition algorithm. Android and web applications will allow remote access to the system. The CNN Algorithm plays the main role in the Detection of the Faces so the CNN Algorithm gives more Accuracy than any other Algorithm.

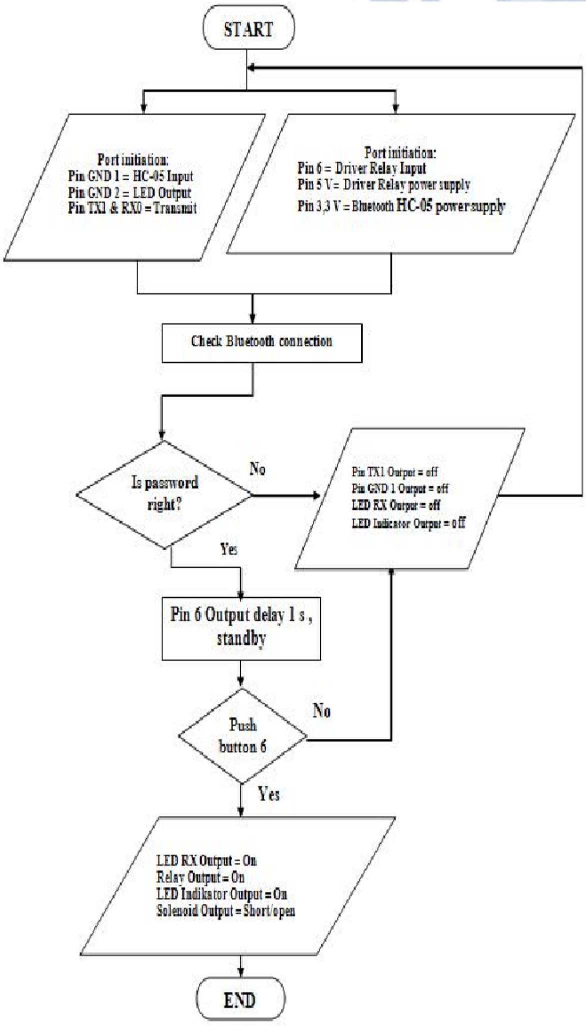


Figure 4: Work flow of Solenoid Lock

Now Laptop will be connected to the Arduino Board and the message 1 and 0 is transmitted from the Laptop the Arduino Board and it Transmits the Message to the Relay Switch and Again the Relay Switch sends the input of 0 or 1 to the Solenoid lock .The Solenoid Lock work Procedure is given in the Figure 4 if the input 1 then lock will be Opened or Else it remains locked .but the input 1 will be given based on the security key or the Face recognition .If the Face is matched with pre Trained data set then the output 1 will be generated or the security key is correct also means then also output 1 will be produced.

5. ALGORITHM

The Proposed algorithm for the Face recognition is the Conventional neural Networks. The CNN Algorithm can be imported from the Face Recognition module, this module can consist of the different Algorithms but our system imports the CNN algorithm. The CNN algorithm is very different Algorithm and best effective algorithm in order to recognize the human Faces.

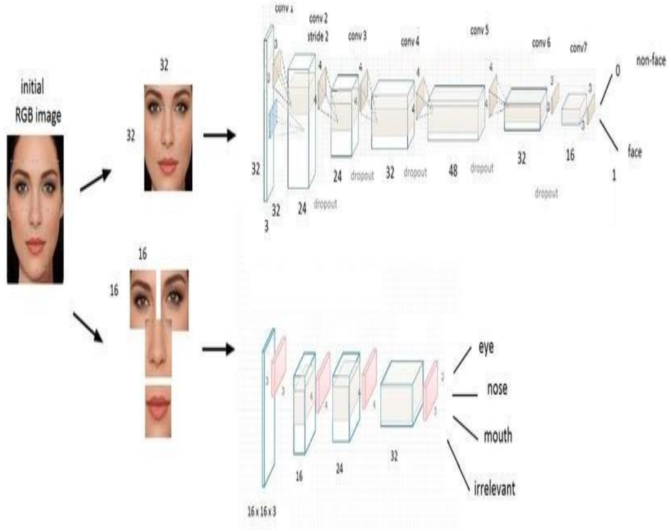
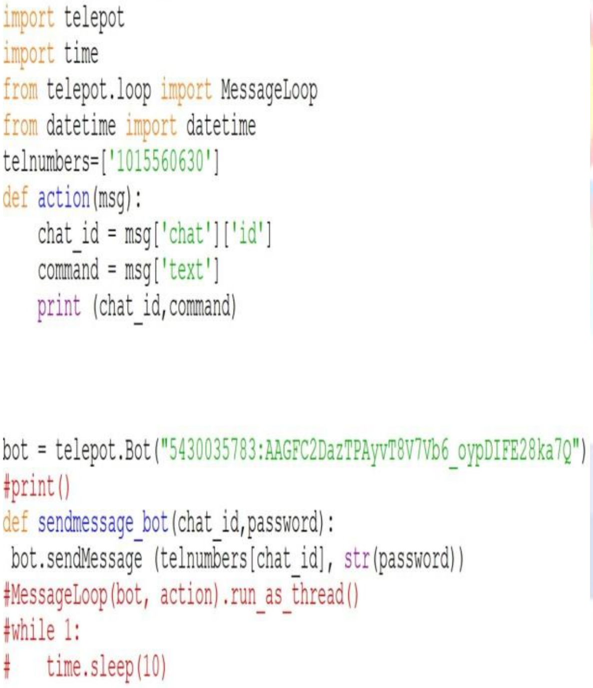


Figure 5: CNN Algorithm Internal splitting of Image

The CNN model is a framework that can improve the accuracy of facial image classification. It is based on the LeNet-5 framework, but it has various differences in its structure. For instance, the input data, network size, and full connection layer are different. The model is composed of two sets of pooling and convolutional layers. The two layers are arranged in the same way as the sketches. The input layer has only one feature map, which is utilized to put the facial image into the CNN framework. The first convolutional layer is C1. It has six feature maps and a randomly generated kernel. The first pooling layer, S1, has six feature maps. Its output is calculated by taking into account the previous layer's output. The elements in the feature map are connected to the corresponding kernel in C1's feature map. These will not overlap with the receptive fields of the other elements. The two pooling and convolutional layers, known as S2 and C2, are respectively equipped with 12 feature maps and follow the same calculation steps as their predecessors. A single-layered perceptron is also connected between the S2 and the output layers. The output layer's output is a 40-dimensional representation of a face recognition algorithm as you can see clearly in the above Figure 2 the Splitting of the images of human Face and it's time to implement this in the Real Time Scenario which is used for multi-label classification. We store the 128-bit encodings of the required faces and compare them with the live face to identify an individual or an open door using a relay connected to an Arduino.

6. CODING PROGRAMS

The Below Coding program in the Image 1 is used to connect the Telegram bot to owner Account it sends the Security Key Randomly generated between the 0000 and 9999 and if any unknown person face is detected means it sends the message wrongs person tried the remaining part of the code function is written in the main program to call the Function and sends the messages Automatically without any External Help.



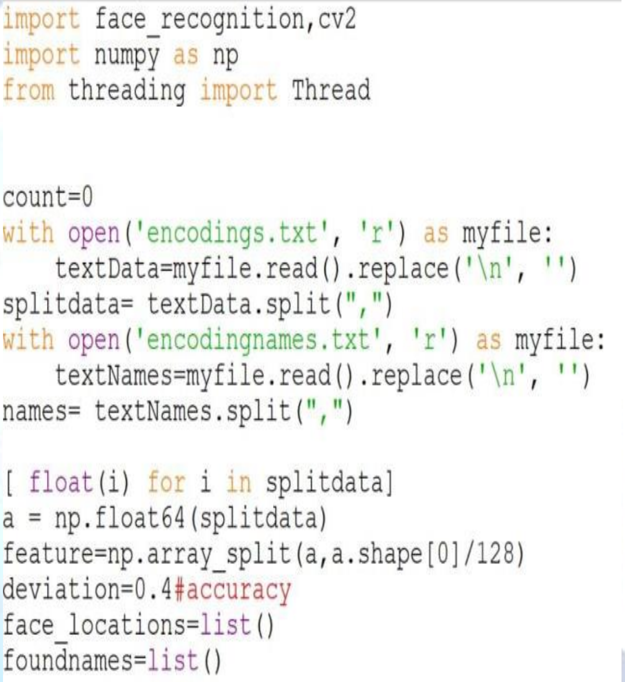
```
import telepot
import time
from telepot.loop import MessageLoop
from datetime import datetime
telnumbers=['1015560630']
def action(msg):
    chat_id = msg['chat']['id']
    command = msg['text']
    print (chat_id,command)



bot = telepot.Bot("5430035783:AAGFC2DazTPAyvT8V7Vb6_oypDIFE28ka7Q")
#print()
def sendmessage_bot(chat_id,password):
 bot.sendMessage (telnumbers[chat_id], str(password))
#MessageLoop(bot, action).run_as_thread()
#while 1:
#    time.sleep(10)
```

Image 1: Telegram API Link

Now the code of face recognition and use of the CNN Algorithm is Shown below in Image 2 it's the code from the Snippet tool. The Original Code has more lines of the code than the Code which is shown below this is the Sample code which will be used in the Testing Phase. There is one point to be noted that the Accuracy of the Entire Project will depend upon the deviation mentioned in the below Image 2 Deviation and the Accuracy are Inversely proportional to Each Other .The More the Deviation the Less the Accuracy the Less the value of the Deviation the More the Accuracy .We had Given one Standard Value which is giving the Accuracy of More than 90% if we further decrease the deviation then the Accuracy will go beyond the 94% but the Problem is it takes more Computational time than the Average Picture Processing Time and as there are Encoded data also stored in the Pre Trained Data it's Better to have Less Trained data in the Encodings

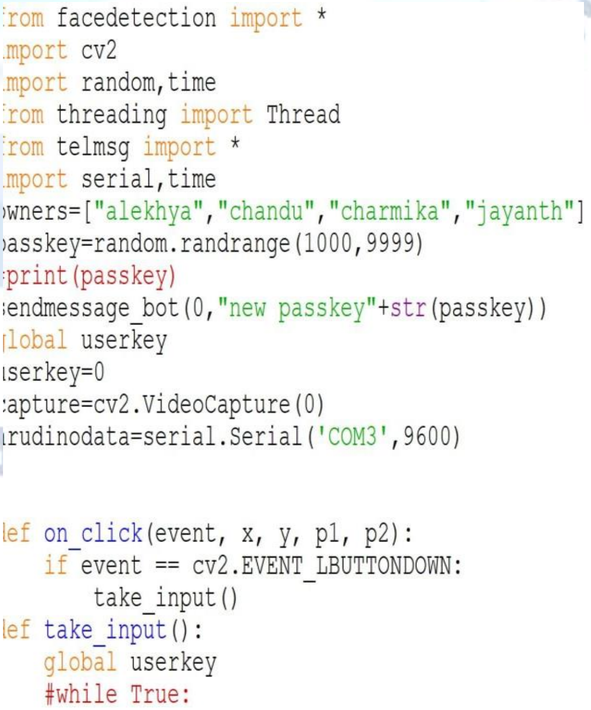


```
import face_recognition,cv2
import numpy as np
from threading import Thread


count=0
with open('encodings.txt', 'r') as myfile:
    textData=myfile.read().replace('\n', '')
splitdata= textData.split(",")
with open('encodingnames.txt', 'r') as myfile:
    textNames=myfile.read().replace('\n', '')
names= textNames.split(",")

[ float(i) for i in splitdata]
a = np.float64(splitdata)
feature=np.array_split(a,a.shape[0]/128)
deviation=0.4#accuracy
face_locations=list()
foundnames=list()
```

Image 2: Comparison of pre-Trained data



```
rom facedetection import *
mport cv2
mport random,time
rom threading import Thread
rom telmsg import *
mport serial,time
wners=["alekhya","chandu","charmika","jayanth"]
asskey=random.randrange(1000,9999)
print(passkey)
endmessage_bot(0,"new passkey"+str(passkey))
lobal userkey
serkey=0
apture=cv2.VideoCapture(0)
rudinodata=serial.Serial('COM3',9600)


lef on_click(event, x, y, p1, p2):
    if event == cv2.EVENT_LBUTTONDOWN:
        take_input()
lef take_input():
    global userkey
    #while True:
```

Image 3: Imports the Module Face Recognition

The testing phase of our system has completed. All that's Left is importing the Module of Face Recognition as described in the Image 3. We have 4 images that are stored in the pre- trained data of the encodings. If the face is detected, the message "wrong person tried" will be sent to the owners. The unknown user then has to provide the correct security code in order to enter the house or the lock will remain locked. But the Hardware links and Wired Connections should be Perfect as given in the Pictorial View of the Figure 1. A CNN algorithm was used to analyze 10 individuals all of them were recognized. With the help of this algorithm, the accuracy of the results was increased to 90% even more.

7. RESULTS

These are the estimates of the various face recognition algorithms that are used in the field. Although the exact results may vary depending on the implementation, the complexity of the network, the size of the image given in the Figure 5, and the hardware architecture are some of the factors that can affect the accuracy of the results. Pre-trained models can also help reduce the time spent in the computation of the face recognition.

ALGORITHM	ACCURACY
Conventional Neural Networks	98%
You only look once	94%-96%
Artificial Neural Networks	85%-95%
Local Binary pattern	80%-90%
Histogram of Gradients	85%-95%
Support vector machines	80%-90%
Haar Cascade	80%-90%

Table 1: Highest Accuracy percentage of Algorithms

In our project we have used the CNN Algorithm to improve Accuracy of the Face recognition and it depends upon the Hardware Architecture and several conditions also need to beverified. As you have seen the Approximate Values of the Accuracy mentioned in the percentage given in the Table 1. The Below result Is based on our Hardware components.

The CNN had got the Accuracy of more than 90% which is very much High when compared to the Other Face Recognition Machine Learning Algorithms and more than the Raspberry pi. The Above Recorded results noted in the Table 2 are based upon our hardware Architecture and pre-Trained data of the Encodings.

ALGORITHM	REQUIREMENTS	PERFORMANCE	ACCURACY
Conventional Neural networks	Low	Medium-High	High (More than 90%)
You only look once	High	Low	Medium-High
Artificial Neural Networks	Medium	Medium	Medium -High
Local Binary pattern	Low	Low-Medium	Low-Medium
Histogram of Gradients	Low-Medium	Medium	Medium-High
Support vector machines	Medium	Medium-high	Medium-High
Haar Cascade	Low	Medium	Medium-High

Table 2: Recorded Data Based on project Design

8. CONCLUSION

The goal of this paper is to improve the accuracy of the face reorganization algorithm by implementing an improved version using the Arduino. This method can be done by implementing various algorithms such as ANN, HOG, YOLO, and LPB. We will additionally get the different types of accuracy rate by selecting the appropriate algorithm. The Arduino and the Laptop are connected to each other using the relay switch and the Solenoid lock. The main advantage of this method is that it eliminates the need for the Raspberry Pi. The laptop processor will allow us to get the more accurate results than the normal camera. We will also store the owner data in the pre-trained data encodings so that we can easily add images to the repository. The user can easily allow any guest to join the Telegram channel if they have a valid security key. The key is sent to the chat ID of the app with the help of the Telegram Bot. The program that we will be using is a Python Application that will be developed by us. It will be able to connect to the API of the Telegram app. The CNN algorithm will be able to produce more accurate and efficient results than the other machine learning algorithms. This is an advanced security system of the Arduino that will allow us to perform more accurate and efficient face recognition.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Badan Pusat Statistik, “Criminal Statistics 2018 Stat. Krim. 2018, 2018. [Online]. Available:https://www.bps.go.id/publication/2018/12/26/89c06f465f944f3be39006a1/statistik-kriminal-2018.html.

[2] Hassan, H.; Bakar, R.A.; Mokhtar,A.T.F. ” “Face recognition based on auto-switching magnetic door lock system using microcontroller” IEEE-International Conference on System Engineering and Technology (ICSET), 2012

[3] R K Kodali, V Jain, S Bose and L Boppana 2016 IoT based smart security and home automation system (Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA) no October 2017 pp 1286–1289

[4] R. Kumar Shukla and A. Kumar Tiwari, "Comparison of Analytics of Machine Learning Based Approaches for Face Detection and Recognition".

[5] M Suman Menon, Anju George, N Aswathy and Jaimy James, "Custom Face Recognition Using YOLO", 2021 3rd international Conference on Signal Processing and Communication (ICPSC),

[6] S. Ørnager and H. Lund, "Images in Social Media: Categorization and Organization of Images and Their Collections"

[7] Yatidharan Choudhary, Apeksha Aggarwal, Ajay Agarwal, "Detecting Drivers' Drowsiness using Haar Cascade Classifier", 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)

[8] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things: A vision architectural element and future directions".

[9] Razan AL MOGBIL, Muneerah AL ASQAH and Salim EL KHEDIRI, "Iot: Security challenges and issues of smart homes/cities", In 2020 International Conference on Computing and Information Technology (ICCIT-1441),

[10] M. Pugh, J. Brewer, and J. Kvam, “Sensor fusion for intrusion detection under false alarm constraints,” in 2015 IEEE Sensors Applications Symposium (SAS), (2015).