# Home Automation: Instant Theft Detection Reporting To Owner Using IoT

[1]Dr Nara.Sreekanth, [2]Karishma, [3]Jyothsna
[1]Associate Professor, [2]UG Student, [3]UG Student
BVRIT HYDERABAD college of engineering for women

**Abstract - For over 10 years, Surveillance cameras have been the prime alternative to guarantee security at spots of interest. The principle downside of this framework is that it just stores video captured and neglects to caution the concerned personnel in real-time about the ongoing crime. In this proposed system, theft can be distinguished and informed to the client progressively. This project is related to image processing and IOT applications. The system uses pi camera and PIR sensors connected to Raspberry pi to detect the intrusion in real time. On recognizing an interruption, the concerned individual (unfortunate casualty) is told about the robbery by means of sending email and SMS. The victim also receives an image of the intruder and has access to either accept or decline the request email or SMS.**

**Keywords - IoT, Raspberry Pi, CCTV, theft detection.**

## 1. Introduction

The concept of home automation has been around since the late 1970s. Because of the advancement of technology and services, people's expectations of what a home should do or how the services should be provided and accessed at home has changed a lot during the course of time, and so has the idea of home automation systems If we look at different home automation systems over time, they have always tried to give effective, helpful, and safe ways for home occupants to get to their homes. Irrespective of the change in user expectations, advancement of technology, or with the change of time, the role of a home automation system has remained the same.

The most fundamental meaning of any security framework is found in its name. It is a methods or strategy by which something is verified through an arrangement of inter-networking segments and gadgets. In this case, we're discussing home security frameworks, which are systems of coordinated electronic gadgets cooperating with a central control panel to ensure against criminals and other potential home intruders. Our work basically centers around the security part of home computerization

We initially examine how the idea of security has changed in current home computerization frameworks, at that point center around different difficulties in the field from a security perspective.

For over 10 years, Surveillance cameras have been the prime alternative to guarantee security at spots of interest. The principle downside of this framework is it just stores streaming video and neglects to caution the concerned personnel in real-time about the ongoing crime. In this proposed system, theft can be distinguished and informed to the client progressively. This project is related to image processing and IOT applications. The system uses pi camera connected to Raspberry pi to detect the intrusion in real time. On recognizing an interruption, the concerned individual (casualty) is told about the robbery by means of sending email and SMS. The owner of the house receives an image of the intruder and has access to either accept or decline the requested email or SMS.

## 2. Related Work

The project carried out is a part of Image processing and IOT[11].

### 2.1 Existing System

In the Pre-Existing system, the crime investigation is done by continuously visualizing the footage recorded by the CCTV cameras. Which is lethargic task to accomplish.

#### 2.1.1. Disadvantages of Existing System

#### 2.1.1.1. PRIVACY IS AN ISSUE:

A couple of occurrences in the past reveal, where surveillance cameras have worked up debates, particularly in expert setups. There have been situations where workers have questioned being under consistent reconnaissance without their authorization and referring to the 'invasion of privacy' as the reason. A few have also resorted to taking legal action against their employers in relation to this.

Commentators of surveillance camera frameworks have disapproved of them being put in workplaces and contended that doing as such suggests that the business has either officially expected or is persuaded that his representatives are looking for trouble and will accomplish something incorrectly, which is the reason their exercises should be recorded.

### 2.1.1.2 IT CAN BE A COSTLY AFFAIR:

While sham cameras may not be costly, the genuine one's costs hundreds, even a great many dollars relying upon the highlights and the quantity of cameras and checking frameworks you purchase. Getting them deployed and their routine upkeep implies included expenses. If you're thinking of installing them yourself, lay that your idea to rest, unless you have good knowledge of wiring systems or you may end up damaging the cameras.

### 2.1.1.3 THEY CAN BE VULNERABLE:

When we, as users of security cameras, try to keep ourselves updated on the latest in security systems, we should not forget that intruders and criminals are doing the same too. A clever trespasser will probably know all about them and may have figured out a way to go undetected.

Further, educated hoodlums may have comprehended the innovation and worked out approaches to debilitate/separate them from their capacity source. Additionally, if he recognizes your installed cameras as phony/fakers, they can be totally pointless in any wrongdoing avoidance.

In the worst cases, hackers can play havoc with your security camera system by using the Internet and use them to spy on you instead. This makes security cameras vulnerable to damage and/or misuse.

### 2.1.1.4. CAN'T STOP THEFT:

Cameras empower clients to record film for later survey, and to help seize hoodlums, and get equity from the law. They can't, in any case, stop a wrongdoing when it is in advancement. They don't caution neighbors or the police like an alert framework would. This means that you will incur losses even as you run to the court, make insurance claims and reorder stolen inventory, which may no longer make you feel absolutely protected and even reason you to lose confidence in them.

### 2.2 Proposed System

But here in the PROPOSED SYSTEM. We don't have the continuous video.

**1)** Firstly, the faces of the family members are scanned and stored in the database.
**2)** When the new member's tries to enter the house then the camera captures the image of the new individual and sends the message and image to the authenticated phone number or e-mail id.
**3)** A necessary action is taken by family members.

## 3. Experimental Setup

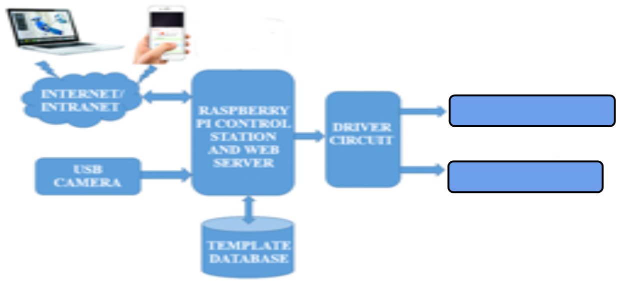


**Figure 3.1 :** Architecture of HOME AUTOMATION INSTANT THEFT DETECTION REPORTING TO OWNER USING IoT

In the Figure 3.1, Initially the images of the family members are captured using one camera and stored into the datasets. This dataset consists of different folders for different family members.

After that process when any person tries to enter into the house, then the camera captures the image of the that person and compares it with the existing datasets. Then there are two possibilities of action taking place. They are:

- Faces match (Authorized Person)
- Faces does not match (Unauthorized Person)

**Authorized Person:**

The person is called Authorized if the new face matches with existing face in datasets, confirms he is an authorized person, then the doors open automatically.

**Unauthorized Person:**

A person is called unauthorized if the new face does not match with the existing datasets. Once the system detects, an unauthorized person then alarm ring cautioning the neighbors. Simultaneously the captured image of unauthorized person is sent to the authorized person via registered authorized email id.

### 3.1 Requirement Specifications

For doing this project, the hardware and software specifications are as given below:

### 3.1.1 HARDWARE SPECIFICATIONS:

Ø Raspberry Pi
Ø DC Motor
Ø 8GB RAM
Ø Camera
Ø USB Cable
Ø Buzzer(Alarm)

### 3.1.2. SOFTWARE SPECIFICATIONS :

Ø Raspbian OS
Ø Python
Ø OpenCV

### 3.2 Workflow

### 3.2.1 Datasets Creation.

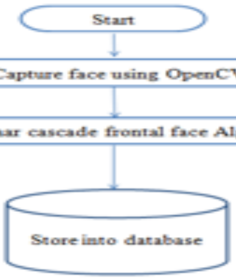

Start
Capture face using OpenCV
Use haar cascade frontal face Algorithm
Store into database

**Figure 3.2.1 Datasets Creation.**

Figure 3.2.1: A step by step elaboration of the dataset creation is show in this figure.
First, we must create datasets for the identification of authorized users. For the identification of faces we use Haar Cascade algorithm.

### 3.2.2 For Detection

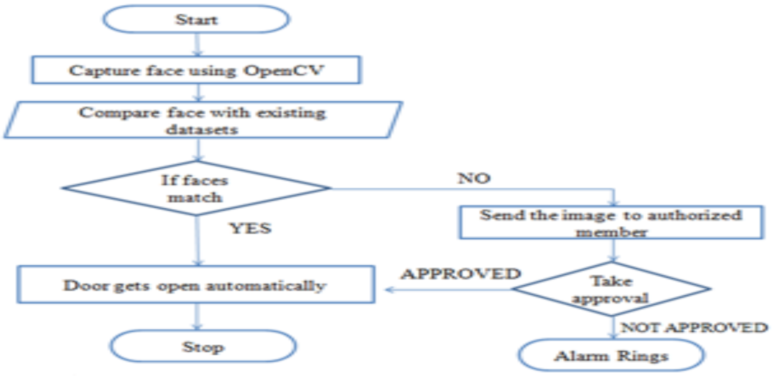

Start
Capture face using OpenCV
Compare face with existing datasets
If faces match
NO
YES
Send the image to authorized member
Door gets open automatically
APPROVED
Take approval
NOT APPROVED
Stop
Alarm Rings

**Figure 3.2.1 For Detection**

### 3.3.1 Haar Cascade Algorithm

Object Detection using Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones in their paper, "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001[10]. It is an AI based methodology where a coursework is prepared from a ton of positive and negative pictures. It is then used to detect objects in other images.

Here we will work with face detection. At first, the calculation needs a great deal of positive (pictures of appearances) and negative (pictures without countenances) to prepare the classifier. Then we need to extract features from it. For this, Haar highlights appeared beneath the picture that are utilized. They are just like our convolution kernel. Each element is a solitary esteem gotten by subtracting the aggregate of pixels under white square shape from the entirety of pixels under dark square shape.

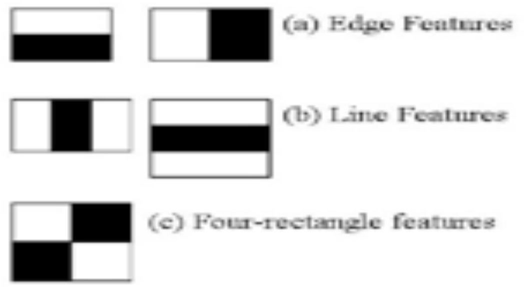


Figure 3.2.1.1 Haar Cascade

### 3.4.1. The Source Code for Creating Datasets:

```
#creating database
import cv2, sys, numpy, os
import urllib
import cv2
import numpy as np
import imutils
#url="http://192.168.1.2:8080/shot.jpg"
haar_file = 'haarcascade_frontalface_default.xml'
datasets = 'datasets'  #All the faces data will be present this folder
sub_data = 'jyothsna'        #These are sub datasets of this folder, for my faces I've used my name
path = os.path.join(datasets, sub_data)
if not os.path.isdir(path):
 os.mkdir(path)
(width, height) = (130, 100)            # defining the size of images
 face_cascade = cv2.CascadeClassifier(haar_file)
# The program loops until it has 30 images of the face.
cam = cv2.VideoCapture(0)
 count = 1
while count < 31:
 #imgPath=urllib.urlopen(url)
   #imgNp=np.array(bytearray(imgPath.read()),dtype=np.uint8)
 #img=cv2.imdecode(imgNp,-1)
 ret,img = cam.read()
 img = imutils.resize(img, width=400)
 gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
 faces = face_cascade.detectMultiScale(gray, 1.3, 4)
 for (x,y,w,h) in faces:
       cv2.rectangle(img,(x,y),(x+w,y+h),(255,0,0),2)
           face = gray[y:y + h, x:x + w]
           face_resize = cv2.resize(face, (width, height))
           cv2.imwrite('%s/%s.png' % (path,count), face_resize)
 count += 1
 print count
 cv2.imshow('OpenCV', img)
 key = cv2.waitKey(10)
 if key == 27:
           break
cv2.destroyAllWindows()
```

### 3.4.2 The Source code for Detection

```
    import cv2
    import time
    import urllib
    import imutils
    import subprocess
    import numpy as np
    import cv2, sys, numpy, os
    import RPi.GPIO as GPIO
    #url="http://192.168.1.2:8080/shot.jpg"
    url= cv2.VideoCapture(0)
     motor = 21
```

```
   buzzer =20
    GPIO.setwarnings(False)
   GPIO.setmode(GPIO.BCM)
   GPIO.setup(motor,GPIO.OUT)
   GPIO.setup(buzzer,GPIO.OUT)
   GPIO.setup(26, GPIO.IN, pull_up_down = GPIO.PUD_UP)
   size = 4
   haar_file = 'haarcascade_frontalface_default.xml'
   datasets = 'datasets'
   print('Training...')
   (images, labels, names, id) = ([], [], {}, 0)
   for (subdirs, dirs, files) in os.walk(datasets):
          for subdir in dirs:
          names[id] = subdir
          subjectpath = os.path.join(datasets, subdir)
          for filename in os.listdir(subjectpath):
          path = subjectpath + '/' + filename
          label = id
          images.append(cv2.imread(path, 0))
            labels.append(int(label))
          id += 1
   (width, height) = (130, 100)
   (images, labels) = [numpy.array(lis) for lis in [images, labels]]
   #model = cv2.face.createFisherFaceRecognizer()
   model = cv2.createFisherFaceRecognizer()
  model.train(images, labels)
  face_cascade = cv2.CascadeClassifier(haar_file)
   webcam = cv2.VideoCapture(0)
   value=False
    try:
          while True:
              if(GPIO.input(26)==0):
                    value=True
          wait_time = 10
          auth = 0
          while value:
                    print("capture")
                    ret,im=url.read()
                    im = imutils.resize(im, width=200)
                 cv2.imwrite('/var/www/html/pan.jpg', im)
                 gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
                    faces = face_cascade.detectMultiScale(gray, 1.3, 5)
                    for (x,y,w,h) in faces:
                 cv2.rectangle(im,(x,y),(x+w,y+h),(255,255,0),2)
                  face = gray[y:y + h, x:x + w]
                    face_resize = cv2.resize(face, (width, height))
                    #Try to recognize the face
                    prediction = model.predict(face_resize)
                    cv2.rectangle(im, (x, y), (x + w, y + h), (0, 255, 0), 3
                    if prediction[1]<500:
                        cv2.putText(im,'%s - %.0f' % (names[prediction[0]],prediction[1]),(x-10, y-10),
cv2.FONT_HERSHEY_PLAIN,1,(255, 0, 0))
                    print( names[prediction[0]]);
                    auth = 1
                    wait_time = 0
                    value=False
                    break
                    elif(wait_time < 1):33
                    auth =2
                    value =False
                    else:
                    wait_time-=1
                    cv2.putText(im,'scanning',(x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
                 cv2.imshow('OpenCV', im)
                 cv2.imwrite('/var/www/html/capture.jpg', im);
                    cv2.imwrite('capture.jpg', im)
                    key = cv2.waitKey(10) & 0xFF
                    if key == 27:
                    break
                    if(auth == 2):
                    cv2.imwrite('capture.jpg', im)
                 cv2.imwrite('/var/www/html/capture.jpg', im);
                    print("unauthorized user")
                    GPIO.output(buzzer,True)
                    subprocess.Popen("sudo python mail.py",shell=True).communicate()
                    time.sleep(1)
                    GPIO.output(buzzer,False
                    elif(auth == 1):
                    print("authorized user");
                 GPIO.output(motor,True)
                 #subprocess.Popen("sudo python mail.py",shell=True).communicate()
                    time.sleep(5)
                    GPIO.output(motor,False)
   except:
          KeyboardInterrupt()
          cv2.destroyAllWindows()
```

### 3.4.2 The Source code for Sending E-Mail

```
    import time
    import os
    import glob
    import smtplib
    import base64
    from email.mime.image import MIMEImage
    from email.mime.multipart import MIMEMultipart
    import sys
    gmail_user = "karishma.reshma98@gmail.com"
    gmail_pwd = "nencheppa"
    FROM = 'karishma.reshma98@@gmail.com'
    TO = ['15wh1a0564@bvrithyderabad.edu.in'] #must be a list
    time.sleep(1)
    msg = MIMEMultipart()
    time.sleep(1)
    msg['Subject'] ="Unauthorized person"
    time.sleep(1)
    fp = open("capture.jpg", 'rb')
    time.sleep(1)
    img = MIMEImage(fp.read())
    time.sleep(1)
    fp.close()
    time.sleep(1)
    msg.attach(img)
    time.sleep(1)
    try:
            server = smtplib.SMTP("smtp.gmail.com", 587) #or port 465 doesn't seem to work!
            print "smtp.gmail"
            server.ehlo()
            print "ehlo"
            server.starttls()
            print "starttls"
            server.login(gmail_user, gmail_pwd)
            print "reading mail & password"
            server.sendmail(FROM, TO, msg.as_string())
            print "from"
            server.close()
            print 'successfully sent the mail'
    except:
            print "failed to send mail"
```

## 4. Results Output Screen

### 4.1 Output Screen for the 3.4.1 source code.

Figure 4.1.1 Output Screen for Creating Datasets.

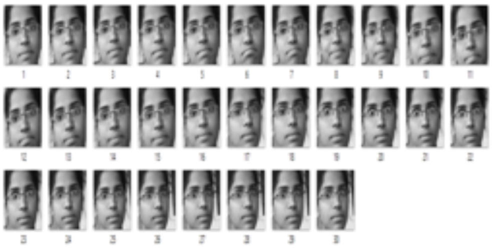


Figure 4.1.2 Series of Images stored in Datasets folder

### 4.2 Output Screen for the 3.4.2 source code.

Figure 4.2.1 Capturing the new person ( Authorized )

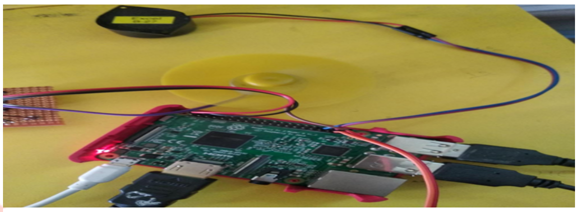
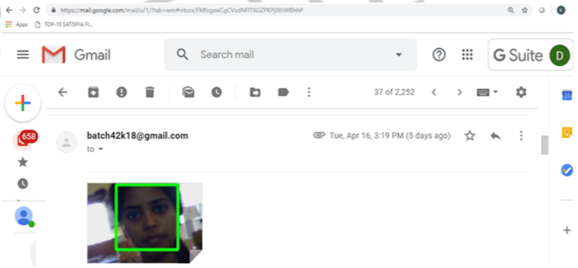


Figure 4.2.2 Raspberry Pi circuit connection with the buzzer, a camera, a DC Motor turn on for the authorized user

Figure 4.2.1 Capturing the new person (Un-Authorized )

### 4.3 Output Screen for the 3.4.3 source code.



batch42k18@gmail.com
to
Tue, Apr 16, 3:19 PM (5 days ago)

Figure 4.3.1 Raspberry Pi circuit connection capturing the new person face and sending unauthorized person face through e-mail to the owner's registered e-mail id.

## 5. Conclusion and Future Enhancement

Security has become a major concern these days especially with the burgeoning rate of thefts and crimes. Studies show that homes without security systems are more likely to be targeted by burglars than those with professionally monitored systems. Security frameworks are frequently the primary line of safeguard against break-ins. In the normal CCTV cameras, the continuous video is recorded. But, in this application the camera detects and respond only to the new member. There by reducing the time, to detect the chance of theft and immediate action can be initiated by the concern.

In the future this technique can be further implemented in local area protection and for any stores. It can also use in online assessment where it is used to check whether the registered person is writing that exam or not. For better results in the classification of faces, we can integrate well advance approaches as mentioned in [ 9, 10] where only six features of a face are considered.

## 6. References

[1.] Akash V. Bhatkulel, Ulhas B. Shinde, Shrinivas R. Zanwar, "Internaltional Journal of Innovative Research in Computer and Communication engineering [IJIRCC]", Home Based Security Control System using Raspberry Pi and GSM, vol. 4, no. 9, pp. 16259-16264, September 2016

[2.] See, S. Lee, "An integrated vision-based architecture for home security system", vol. 53, no. 2, pp. 489-498, May 2007.

[3.] http://article.sapub.org/10.5923.j.ac.20170702.06.html

[4.] B. Choudhury, T. S. Choudhary, A. Pranmanik, W. Arif, J. Mehedi, &quot;Design and implementation of an SMS based home security system&quot;, IEEE International Conference on Electrical Computer and Communication Technologies [ICECCT], pp. 1-7, 2015

[5.] Zhaoqing Peng, Takumi Kato, Hideyuki Takahashi, Tetsuo Kinoshita, &quot;Intelligent Home Security System Using Agent-based IoT Devices&quot;, IEEE 4th Global Conference on Consumer Electronics [GCCE], pp. 313-314, 2015

[6.] Anwar Shaik, D. Kishore, &quot;IOT based Smat Home Security System with Alert and Door Access Control using Smart Phone&quot;, International Journal of Engineering Research &amp; Technology, vol. 5, no. 12, pp. 584-509, December 2016

[7.] A.R. Al-Ali, M. Al-Rousan, &quot;Java-based home automation system&quot;, IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 498-504, May 2004

[8.] Nara. Sreekanth, Munaga HM Krishna Prasad, " International Journal of Management, Technology And Engineering[IJMTE]", Left And Right Horizontal Elliptical Texture Matrix(Lrhetm) For Age Classification", Vol. IX, Issue I, January 2019, pp. 134- 147, ISSN NO: 2249-7455

[9.] Nara. Sreekanth, Munaga HM Krishna Prasad, " Universal Review", Age Classification Based On Gradient Cross-Diagonal Elliptical TEXTON Matrix(GCDETxM)", Vol. VIII, Issue I, January 2019, pp. 36- 49, ISSN NO: 2277-2723

[10.] https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf

[11.] https://circuitdigest.com/microcontroller-projects/raspberry-pi-iot-intruder-alert-system

[12.] D. A. Chowdhry, A. Hussain, M. Z.U. Rehman, F. Ahmad, A. Ahmad, M. Pervaiz, &quot;Smart security system for sensitive area using face recognition&quot;, IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET), pp. 11-14, May 30 June 1 2013.

### Authors Profile

**Ms. D.Karishma** is an under graduate student with Reg No: 15WH1A0564 is pursuing her B.Tech degree in Computer Science and Engineering from JNT University, studying at BVRIT HYDERABAD college of Engineering for Women, Hyderabad, Telengana., India. She is currently in final year second semester. Her area of interest includes Digital Image Processing, Internet of Things. She attended few related workshops and pre-conference, which helped in doing this project.

**Ms. R. Jyothsna** is an under graduate student with Reg.No: 15WH1A0565 is pursuing her B.Tech degree in Computer Science and Engineering from JNT University, studying at BVRIT HYDERABAD college of Engineering for Women, Hyderabad, Telengana., India. She is currently in final year second semester. Her area of interest includes Digital Image Processing, Internet of Things. She attended few related workshops and pre-conference, which helped in doing this project.

**Dr. Nara Sreekanth** received his B.E. degree in Electronics and Communication Engineering from Gulbarga University, studied at Rural Engineering College in Bhalki, Karnataka., India in 1997. He received his M.Tech. degree in Computer Science from JNT University, studied at School of Information Technology in Masab Tank, Hyderabad, India in 2002. He received his Ph.D in Computer Science and Engineering form Sri Satya Sai University of Technology & Medical Sciences the premier university, in Sehore, Madhya Pradesh., India in 2018. He has served PIRMEC, HITSCOE and VGNT; as Assistant Professor and Associate Professor and taught various courses for UG and PG students, during in his 15 years of teaching experience. He is currently working as Associate Professor, Dept of C.S.E, BVRIT Hyderabad college of Engineering for women, Bachupally, Telengana, India. His area of research interests includes Digital Image Processing, Internet of Things, Cloud Computing and Data Mining. He is a Professional Member of ACM and also, he is a Life Member for IEAE and IAENG. He has published more than 1 research publications in various National, Inter National conferences, proceedings and Journals.