Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022)
IEEE Xplore Part Number: CFP22P17-ART; ISBN: 978-1-6654-0118-0

ANTI-THEFT MONITORING FOR A SMART HOME

NAGAMANI T[1], BENIGA W H[2], DHANISH K S[3], SHERINE BENITTA A[4]

[1]Asst Professor-II, Department of computer science and Engineering, Bannari Amman Institute of Technology Sathyamangalam-638401, Erode Dt., Tamilnadu, India.
[1]nagamanit@bitsathy.ac.in

[2,3]Student, Department of Computer Science and Engineering, [4]Student, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam-638401, Erode Dt., Tamilnadu, India.
[2]beniga.cs19@bitsathy.ac.in,
[3]dhanish.cs19@bitsathy.ac.in,
[4]sherinebenitta.it19@bitsathy.ac.in

2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) | 978-1-6654-0118-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSSIT53264.2022.9716311

Abstract – The proposed methodology aims to provide a sudden notification regarding the ongoing theft to the house owner. Home security is very essential nowadays as the chances of intrusion is getting increased day by day. The existing system theft monitoring has many drawbacks like it will only intimate about the theft only after it occurs and also it can't differentiate human from non-human things. WSN (Wireless Sensors Networks) collaborated along with the IoT are providing solutions for the smart home technologies. This paper proposes anti-theft system for a smart home which easily locates the intruder even when they are hides fully their body with clothes, sheets and any heavy materials. This system also provides an advanced way to identifies an intruder even in the dark with the help of CCTV camera without any sort of night vision capability. The most important thing is to develop a less expensive and beneficial system for the person to detect any sort of unauthorised activities and send notification instantly to the member of the house. This project assures to implement security to the home with a wide recording film data handling. However, all those above proposed methods can be put together and thus provides threats to security. Thus, here is our elaborate version of "ANTI-THEFT MONITORING FOR A SMART HOME".

Keywords- smart anti-theft system; smart home; intrusion detector; IoT; WSN; fully hidden humans.

I. INTRODUCTION

In this modern world, security and surveillance are the most significant issues. Recently, the acts of burglary and hijackism have highlighted the requisite for effective supervision and on the spot notification regarding the occurring thefts to the members of the house. Video recorders and CCTV cameras are the solutions provided in the market for surveillance which can detect misbehaving happenings of a strangers in a place which cannot differentiate human and non-human. Recently, the statistics of theft has raised enormously because of not having awareness and less availability of gadgets. Face detection and the intruder recognition becomes too hard if a burglar closes the face partially or entirely using few stuffs. This proposal can be put in to the home monitoring system in a smart way using IoT. A combined network of sensors, hardware and cameras to search unwanted happenings on the house are used to develop a smart home. The proposed system works on two divisions, an interfaced software and hardware. An advanced node of sensing is installed and joined to a node of central sensing that recognizes the data send to the storage server at the hardware interface division. The software modules are classified into several levels which consists of logging, retrieving and storing of data. The role of this software is to identify and report unauthorized activity of human with the help of wide data handling techniques to household members. The initial section depicts an introductory session about legacy structure, its major issues and about the society impact. The second section portrays the existing system. The third section explains the proposed system. The fourth section talks about the hardware used for the proposal. The fifth section gives the experimental setup of the system. The sixth section describes the working of the proposal. The seventh section describes the methodologies used and the final section concludes the proposed system.

II. RELATED WORK

Legacy systems can't provide real-time theft notification neither detect partially or fully covered faces to the house owner. Detecting intrusions at night with the use of CCTV camera and not with the scotopic vision capable system is too challenging for the old system. The drawback with this type of setup is that it requires 24/7 hr presence of a house member or manual surveillance video, which will not be possible. [1] In addition to this, it is a tedious task to see all recorded clippings after the theft occurs. It would be like that the server of storage have huge number of family members films that won't help in detecting trespassers.

In the recent technology world, the action towards theft in most of the places has happened due to lack of security and surveillance. But in the recent few evolutions of technology towards the creation of anti- theft monitoring systems has given a good approach to the market. CCTV camera which has been placed in all the areas of the house has been monitored24/7,if any unauthorized approach towards belongings in the house can automatically detect the face of the improved who is approaching and can have scanned copies of his facial expressions even if he tries to hide his face. As said in the publication of Zhiwei Zhang, Dong Yi, Zhen lei and Stan Z Li, the face detection is the most important part in the subject of multispectral face biometrics, but it is been rarely known and the most important part in detecting is to detect their face emotions and expressions it has two geometry feature, an appearance based measuring geometric feature is the distance that is between two different components of the face, as soon as the belongings are being touched it send distance message to the household members. The system is defined using sensors, cameras and customized hardware. It prevents theft from being happened. It can even sense the intruders face in a dark area.

III. PROPOSED WORK

These days, intruders aware about the technologies and they carry many smart gadgets like smart anti-lock systems, gas cutters etc with them during the burglary. So, it will be straight to disconnect surveillance camera for them that has the connection indirectly to the DVR and DB server locating at the residence. So, the current system has to be modulated and hence we need to develop an advanced approach that can't only provide unwanted activities, it should also stop the occurring theft by intimating the owner as soon as possible. Every legacy structure will work on the detection of object, detecting the movement of the objects and tracing the object. These sort of systems susceptible to pseudo alarms or messages that would ends in posting fake urgency intimations to the house members, which would end in delivering false urgency messages to the owner of the house, getaway of burglar next to the occurring thefts and unessential confusions to the family members. A proper monitoring of trespassers, recognizing them and security to the home are the solutions to solve these issues.

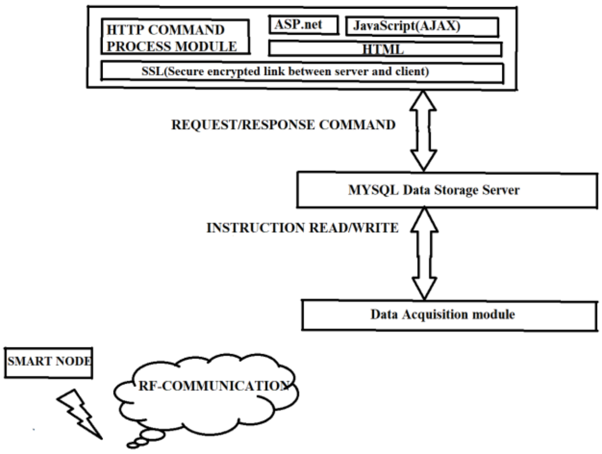


Fig 1. anti-theft system for a smart home

The entire assembly of the units sensing are proceeds. Monitoring the smart home and framework controlling are put on two distinctive levels, such as equipment and programming. All sensor arrangements are in equipment programming. Body Sensors Setup (BSS), Ambient Sensors Setup (ASS), Crisis Sensors Setup (CSS) and Other Sensors Setup (OSS) are four subdivisions of equipment framework. An impact sensor is enabled with BSS. Observing the inhabitants in various states provided by BSS remote. This integrates physical checking gadgets which records all behaviours of the inmates without interfering in their routine. ASS has three units. They are motion, temperature and pressure sensing unit. Many manual push buttons like fright button for urgency cases, house fire enables safety system and alarm is in the CSS. OSS provides checking utility and the control of electrical devices of home via the electronic sensing unit. In addition to it, OSS integrates contact sensing unit. The information accumulation, mining and storage to database server are the main role of OSS. At last, information from the server are grouped and griped by ML and Information Mining Models for sending needful for website and output. Overall setup of sensing unit in wireless mode is presented in the succeeding categories.

3.1. USED HARDWARE

Raspberry-Pi: Raspberry-pi is a credit card size computer board consists of CPU with 64/32-bit quad-core ARM cortex-A53 and 1.2GH and internal storage of 1GB. It also has RAM, I/O, CPU/GPU, USB hub, Ethernet, 2x USB, HDMI port, 3.5mm audio jack and a memory card slot. Here, desktop is connected using HDMI cable to VGA converter cable. Keyboard and mouse are connected to the USB connection. In this proposal, open type CV software is used to detect the face. This type of pi model is very accurate for this research as it has all the requirements needed.

3.2. EXPERIMENTAL SETUP

CP-PLUS analog camera model 850 tvl, Bluetooth enabled hardware and a wi-fi, 1 GB RAM, memory card with 256 GB and a smart phone is used. In each room camera is provided for safeguarding the home from intruders who are equipped with advanced gadgets. These days, burglars know about connection of surveillance camera to a pc and can be able to disconnect to stop functioning. Raspberry pi fixed here have wi-fi and Bluetooth connection, permits keeping this device anywhere where wi-fi is available. The proposed system can function during the power failure, if the pc is connected with the hotspot connection. Additionally, the specialised hardware is wrapped with a layer of plastic to shield from water getting inside the electrical wires.

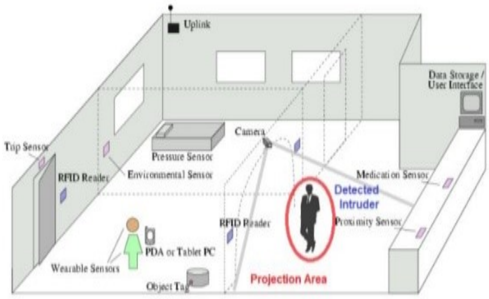


Fig 2. Predicted zone of the anti-theft system for a smart home

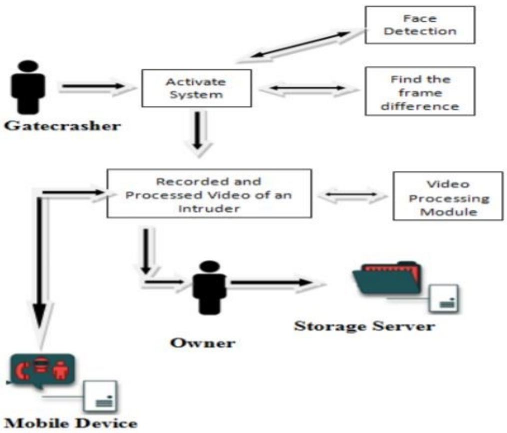


Fig 3. Flowchart of the system

As given in Fig 2, when the intruder comes into the surface of the monitored area, the proposed system works. Face detection module locates the motion of the burglar as seen in the Fig 3. The face detection module has a role to identify human and non-human things. If at all any human activity is detected, camera will be activating at a speed of 15 fps. [2] The captured initial frame will be forwarded to the house members via mobile applications. Rest of the frames at 45 fps for up to 40 fps will be captures and store as mp4 format by the video processing module. The captured 40 seconds video is compressed to about 10 s in fast forward format. Reason for compressing the video is to make that video enabled in case of any slow internet cases. Thus, the video will be forwarded to the owner of the house which makes them to take instant decision.

3.3. WORKING

A. Function module .

It captures the intruder's presence in the surveillance area as in Fig 3 at a rate of 15 fps. After the intruder is detected, this module sends frames to the detection module for detecting the intruder.

B. Detection module

Whenever in the surveillance area, the intruder comes, detection module locates the presence and find whether it is a human or not. This module has four classes.

1) Face and eye detection module:

It captures the face and distinguish human from non-human things. This will locate the brightest portion of the face usen pixel processor module, if the burglar covered their face partially. This module further sends images to the pixel processor module.

2) Pixel processor module:

If the intruder covered their face partially, this module detects the brightest part of face like eyes, cheeks or head. It also detects the gesture using the motion detector module. This prevents the probabilities of pseudo alerts.

3) Motion detector module:

Suppose if an intruder is a human, this module detects the movement and captures the first frame at the rate of 15 fps and snaps the following to a rate of 45 fps. The main reason to increase the rate of frames from 15 fps to 45 fps is for making the family members to enable the video in slow network situations. Then, this video will be sent to the comparative module to get rid of the chance of the false alerts.

4) *Comparative module:*

This module distinguish human from non-human things using Haar Cascade Algorithm and shares notification to the household members to intensify the probability of false alarms.

C. Storage module:

It saves all photographs of the captured intruders. Any sort of unauthorized activities in the surveillance zone of the house is located by this anti-theft monitoring system in three classes such as initial, secondary and final phase.

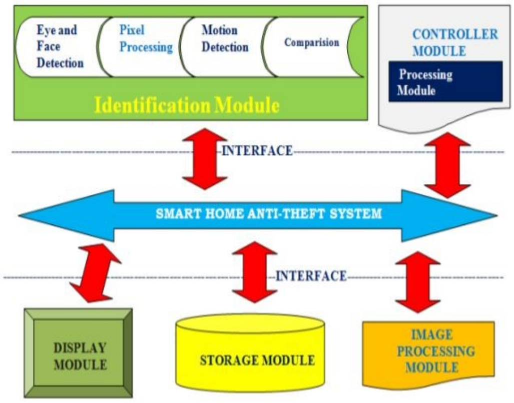


Fig 4. Block diagram for the anti-theft system for communication

3.4. METHODOLOGY

According to the survey, it is found that no feasible remedies are available which identifies the intruders covered their faces and send messages instantly to the members of the house to end the ongoing theft. [3] It is found that the cause behind not introducing these sorts of methodologies is because of the complexity, accuracy, efficiency and the time duration to develop such systems. In order to solve the challenges mentioned above, we have proposed a methodology which sends notification suddenly about the ongoing theft to the house owner.

It was divided in three divisions.

(A) Initial Phase

(B) Secondary Phase

(C) Final Phase

A. Initial Phase

Face and eye detector module is coded using Haar cascade algorithm which detects edges, lines and center-surround features. Haar Cascade Classifiers are given in Fig 5. As in Fig 5 and Fig 6, rectangle features are captured and computed.

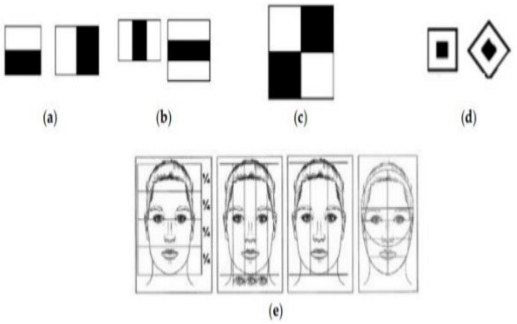


Fig 5. Classifiers based on Haar cascade (a) features of edge (b) features of line (c) features of rectangle (d) centre-surrounding feature (e) classifier of faces

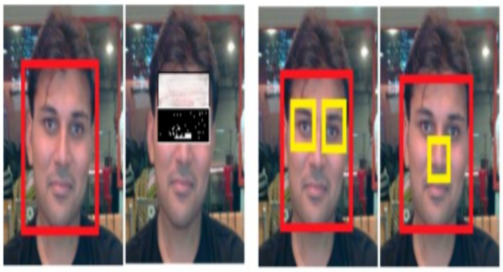


Fig 6. Samples of Image classifiers

The reason for the usage of Haar cascade classifiers is to detect numerous faces consists of overlapping face patterns by separating strong classifiers and weak classifiers as in Fig 7 and Fig 8a. Feature value is the difference of sum of pixels in white and black rectangles. This algorithm elaborates weak classifier by thresholding recorded digits. An advanced Cascade Classifiers directs strong classifier to reach very low false recognition rates. From Fig 7, positive result from first classifiers activates the analysis of second classifier which then activates the third and so on. Suppose through this entire step, any negative result is found, then it would end in ending up the sub window. [4] In this case, many classifiers are developed with the modulated Haar cascade to minimise false negatives.

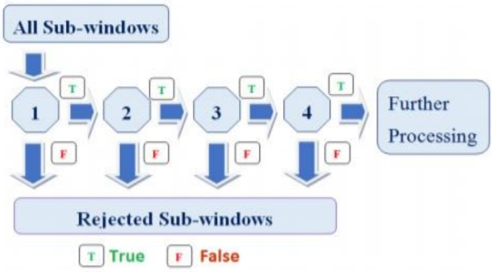


Fig 7. Diagrammatic view of Cascade Classifiers

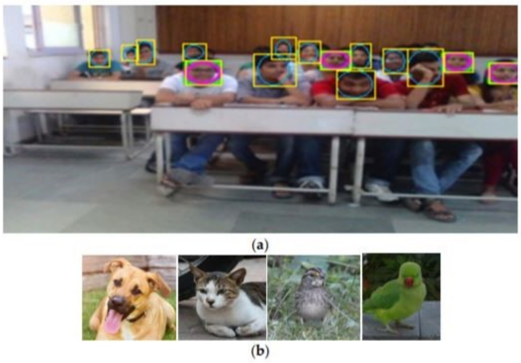


Fig 8. (a) Examples for Crowd Cascade Image Classifiers (b) samples of non-human objects

Compared with the current existing methods, this method is 15 times faster than any other works. According to location of the face framework depicts by Rowley et al, multi classifier based real time face detection system is the fastest algorithm in finding faces as compared to the current methodologies. This proposal can capture crowded faces in one frame as in Fig 8a. Fig 8b shows samples of non-human objects which is not captured by the system.

B. Secondary phase

After the completion of initial face detection, a secondary phase was outlined to get rid of false positives that snaps hidden half faces according to the brightest portions. For each and every constructive sample, a dynamic threshold of range of 0.5 to 0.7 is put to locate the brightest part of the intruders. After performing various research, it is identified that the system does not need different dynamic threshold values for day and night intrusions. To detect retinal and bright facial features, an intelligent Gabor filters are used. This Gabor filter is a strong tool for heterogenous features of image extraction and can be capable of extracting common features from the diverse image. It also has similar behaviours as of human visual system.

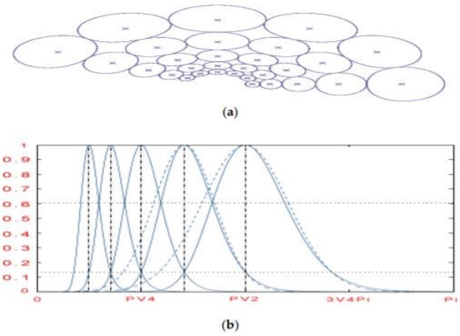


Fig 9. (a) Gabor filters (b) level curves

C. Final phase

Once the secondary phase is ended, if this system is not capable of capturing trespasser's facial features, then the system will move to final phase. Suppose, if the intruder detected is human, it will trace the movement of the human and intimate the presence of an intruder in the house to the house owner by sending shortened video at the speed of 45 frames per second. Moreover, according to the variations of the face, this system can be able for capturing the intruder. The brightest part of the face is captured by a dynamic threshold even they are closed their face with some type of materials. It can also identify the intruders in nighttime or in poor light cases which requires normal analog camera which makes the system more economical. Captured videos, reference images are acquired from captured sequence to detect the intruder's movement.

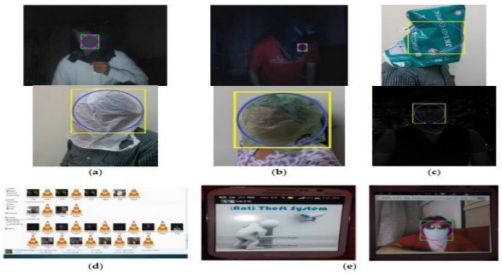


Fig 10. Classifier samples covered their faces with materials (a) dark plastic (b) dark plastic in movement (c) dark night capture (d) samples of stored video with compressed and timestamp (e) mobile app which receives notification of the theft

Fig 10 depicts different image classifiers where the intruder covered their faces fully in different cases. This is very clear from the Fig 10 sample; it is inessential to look straight to the camera capturing for the burglar.

IV. RESULTS

According to the Fig 12a, many research were done using numerous samples in which the intruder covered their faces with some sort of materials. The Fig 11 shows the analysis of face detection for over many variated samples. [5] The faces are detected with the accuracy of 78%.

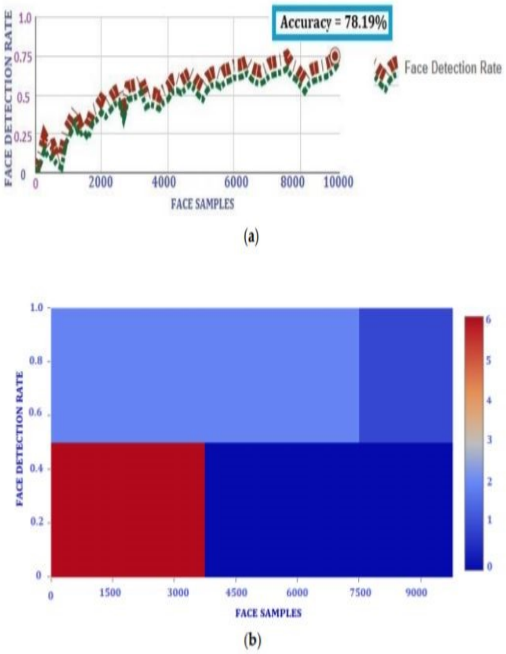


Fig 11. (a) rate of detected face analysis of 10,000 samples who covered their full face (b) map representation of samples covered their faces fully

The analysis of male and female used in experiments were depicted in Fig 12. This system works in detecting male, female, animal faces even when it is covered with objects. The data are collected and stored.

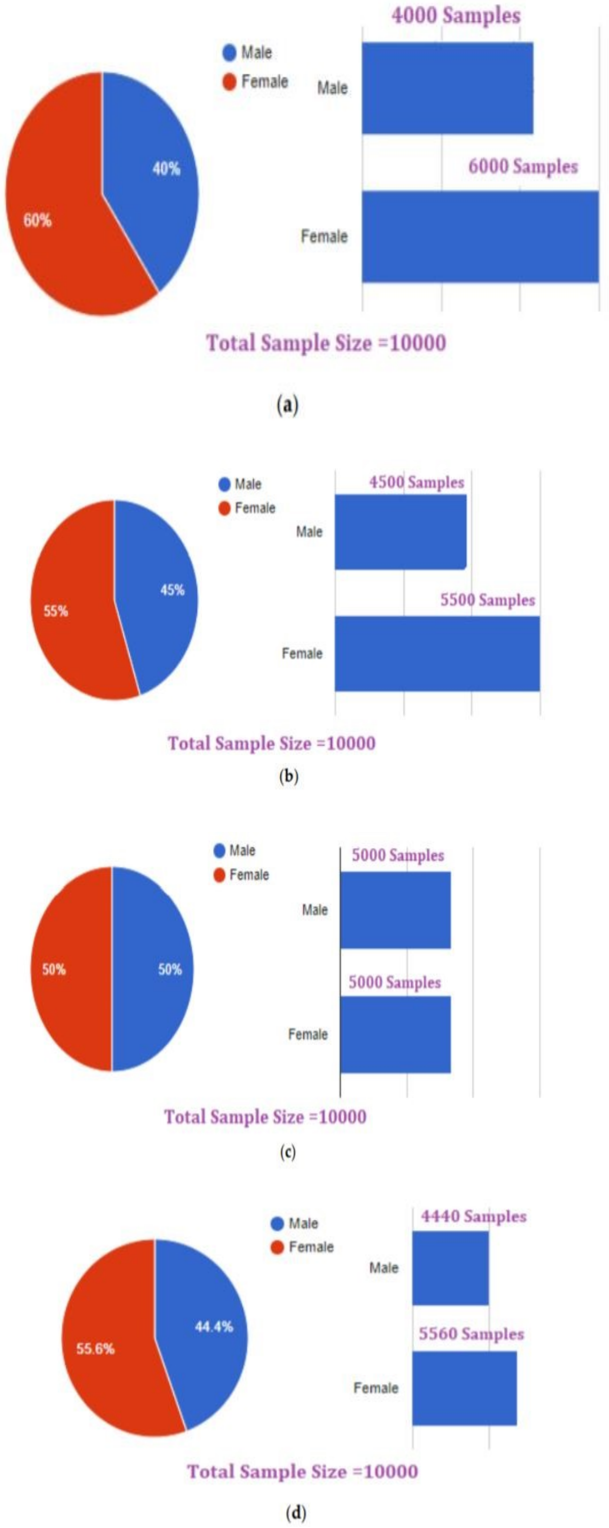


Fig 12. Ratio of male-female faces (a) not unclear (b) covered faces partially (c) full covered face (d) dark captured face

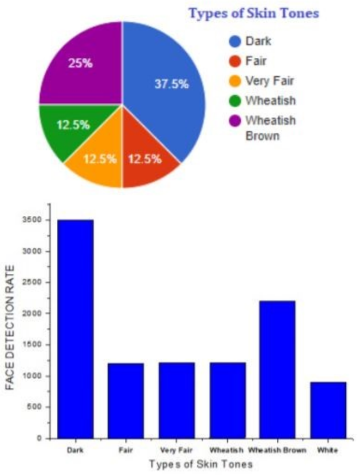
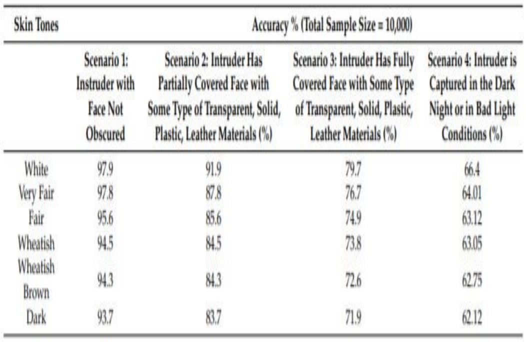


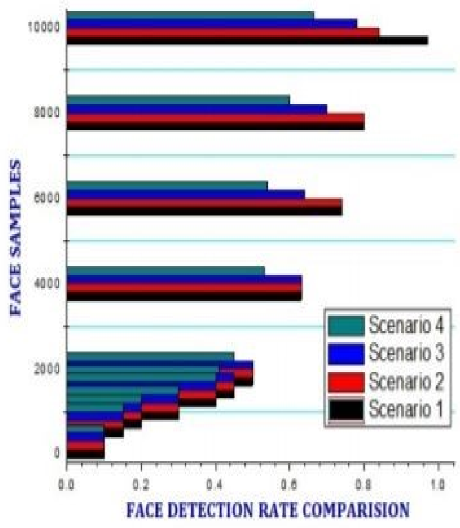
Fig 13. Analysis of skin tones samples



Skin Tones	Accuracy % (Total Sample Size = 10,000)			
	Scenario 1: Instruder with Face Not Obscured	Scenario 2: Intruder Has Partially Covered Face with Some Type of Transparent, Solid, Plastic, Leather Materials (%)	Scenario 3: Intruder Has Fully Covered Face with Some Type of Transparent, Solid, Plastic, Leather Materials (%)	Scenario 4: Intruder is Captured in the Dark Night or in Bad Light Conditions (%)
White	97.9	91.9	79.7	66.4
Very Fair	97.8	87.8	76.7	64.01
Fair	95.6	85.6	74.9	63.12
Wheatish	94.5	84.5	73.8	63.05
Wheatish Brown	94.3	84.3	72.6	62.75
Dark	93.7	83.7	71.9	62.12

Fig 14. Accurate variations of skin tone analysed samples in numerous cases

Fig 14 shows the accurate variations of skin tones collected in various samples. This helps in finding the person who involved in unauthorized activities.



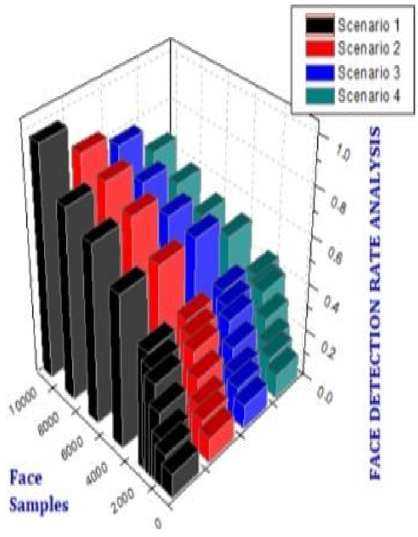


Fig 15. Rate of the detection of the faces with 2000 samples in number of times

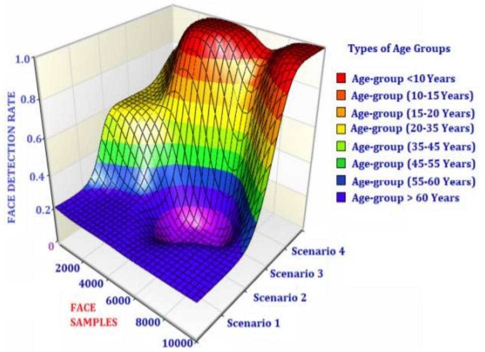


Fig 16. Detection of various age groups for face detection analysis

Fig 15 depicts about the rate of the detection of faces of various samples in n number of times. It also scans the age group of the people.

All together the data are collected and stored in the form of graph, chart and segregated to find out the theft. Using this system, we can keep our home secured and protected.

V. CONCLUSION

Based on our research, the project on anti-theft monitoring for a smart home has brought many innovative ideas to keep our home safe and secure. This project paves a way for wireless sensation and theft detection happening and it also removes the need of DVR for capturing as well as usage of huge amount of storing the memory. The alarm system which is being used has a capability to differentiate human and non-human things. These processes give instant messages based on real time application and the way of potential theft to happen. There are many ways to find the intruder detection as face not observed, face fully covered, face partially covered, capture by an analog camera. If he/she comes to know about the presence of security purposes he/she tries to cover their faces that also is predicted by the percentage level of detection. If the intruder uses the DOS to disable wi-fi interconnection in the area of theft, then the proposed system won't have capability to send notifications to the respective members of the house due to lack of internet connection. So, in the new upcoming projects researchers will be trying to replace the defect. Till this the project's development, however, sounds good. Hope that new upcoming projects will be launching soon.

REFERENCES

[1] Samir Rana, Ritu Mewari, Lata Nautiyal, International Journal of Engineering and Technology, 7 (4.12) (2018) 42-46

[2] Ranjith H D, Anusha B, Arfha Fathima, Fathima Muhammed Iqbal, Hafeeza Jinan, RTESIT - 2019, Vol.7, ISSUE-08

[3] Mohd Azlan Abu, Siti Fatimah Nordin, Mohd Zubir Suboh, Mohd Syazwan Md Yid, Aizat Faiz Ramli, ISSN 0973-4562, Vol.13, Number 2 (2018) pp.1253-1260

[4] Khanna Samrat Vivekanand Omprakash, International Journal of Advanced Engineering Technology, E-ISSN 0976-3945

[5] Arun Hampapur, Brown L, Jonathan Connell, Pankanti S, Proc. 2003, Joint Conference of the Fourth International Conference, Vol.2

[6] Madhura, S. “IoT Based Monitoring and Control System using Sensors”. Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 2 (2021): 111-120

[7] Bagde, Sejal, Pratiksha Ambade, Manasvi Batho, Piyush Duragkar, Prathmest Dahikar, and Avinash Ikhar. “Internet of Things (IOT) Based Smart Switch. “Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 2 (2021): 149-162

[8] Sachin Kumar, Prayag Tiwari, Mikhail Zymbler, Journal of Big data 6, Article number: 111 (2019)

[9] Timothy Malche, Priti Maheshwary, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)

[10] Anindya Nag, Md Eshrat E Alahi, Nasrin Afsarimanesh, Sumedha Prabhu, Sensors in the Age of the Internet of Things: Technologies and applications(pp.171-199)

[11] Akram Khan, Abdullah Al-Zahrani, Safwan Al-Harbi, Soliman Al-Nashri, Iqbal A. Khan, 2018 15th Learning and Technology Conference(L&T)

[12] Jyotsna P. Gabhane, Shradha Thakare, Monika Craig, International Research Journal of Engineering and Technology (IRJET), Vol. 4, Issue-05 (2017)