ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse36862019.pdf
https://doi.org/10.30534/ijatcse/2019/36862019

Engineering and Deploying a Cheap Recognition Security System on a Raspberry Pi Platform for a rural Settlement

Victor Osamor[1], Onyeka Emebo[2], Barka Fori[3], Moses Adewale[4]
1Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria, vcosamor@gmail.com
[2]Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria, onye.emebo@covenantuniversity.edu.ng
[3]Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria, barkafori@gmail.com
[4]Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria, moses.adewale@stu.cu.edu.ng

ABSTRACT

Security is one of the most fundamental challenges of mankind, providing affordable devices for apprehending criminals. Using smart technology is on the rise and the ability to have full surveillance records of both authorised and unauthorized entrance to designated facility or important resource in a timely manner is highly desirable in modern society of today. This paper proposes the use of Histogram of Oriented Gradients (HOG) to train a model capable of recognising authorised personnel on a raspberry pi device for the purpose of security and ease of access to vital infrastructure. HOG was the preferred choice because it is not computationally intensive as compared to Convolutional Neural Networks (CNN) and most other relatively comparable computational algorithms. The HOG network detect faces and sends a report to Firebase Database and an image is also sent to Google Cloud Storage (GCS) a package on the Google Cloud Platform (GCP). Both data from Firebase and GCS are sent to a companion android application where the user can view who entered specific locations, at specific time with accompanying pictorial evidence. The recognition system was deployed on a raspberry pi device that's feeds in visual data via an inexpensive camera. Collectively, the proposed system is a relatively cheap smart technology security system with inherent ability to accomplish real-time surveillance tasks using widely penetrated android phone technology while maintaining low computational overheads.

Key words: Face Recognition, Histogram of Oriented Gradients (HOG), Raspberry Pi, Security

1. INTRODUCTION

Home security might seem like an ancient problem, but there has been a continuous source of worry for tenants and home owners with alarming numbers of homes being broken into with yearly, The Federal Bureau of Investigation (FBI) estimates that a home burglary occurs every 13 seconds in the United States. They also believe that 3 of 4 houses in the United States will be broken into by 2038 [1]. A major challenge of burglary and car theft is that only 13% of these crimes are cleared by the police out of those reported and the major issue faced by police is the lack of physical evidence to tie a suspect to a crime. The FBI also reported that 51% of houses have repeated attacks within a month of the first attack and when the criminals don't return to the same house, they target another house within that neighbourhood. Most houses were breached through the front door in 34% of cases, 23% happened through the ground floor windows, 22% of criminals came in through the back door, 9% through the garage, 4% through an unlocked entrance and 2% enter through somewhere on the ground floor [2], with most of these crimes occurring between 6am to 6pm which falls within most working hours as depicted in figure 1.

The rapid growth of computing and telecommunication devices has led to the production of new sensory devices with wireless network capabilities, these devices can operate with low energy, autonomous and at any location and they form the fundamental structure of IoT, IoT devices have sensors, actuators and computing nodes as their major components which makes them able to read in data from the environment, process the data with the computing node and act upon the data with their actuators. The most notable feature of IoT is artificial intelligence, sensors, connectivity, active engagement and small implementation use [3], [4]. IoT devices is estimated to grow to about 27 billion by 2021 [5]. With these advancements we also have chances at providing evidence to law enforcement authorities that could help prevent these crimes or convict the suspects.

This research is carried out using a Raspberry Pi model B+ as an edge computing device with pi-camera serving as the input mechanism that feeds in visual data to the raspberry pi device which performs facial detection and recognition respectively and reports the information gathered to an android companion application via a google real time firebase when there is

internet connectivity or storing the data on a local storage when the device is offline. This solution is affordable and employs the use of smart computing algorithms and technologies to solve a problem that has plagued many.

Smart computing is becoming a trend with huge companies like Google, Microsoft and Facebook all champion a move by open sourcing their Machine Learning (ML) frameworks to the public to help guide individuals into building smart applications and smart devices like Android things. Open source machine learning tools has led to an explosion of use cases in different domains ranging security [6], sports, financial predictions [7], healthcare [8] and agriculture [9]. Machine Learning is being embedded deep into our daily lives and decision making.

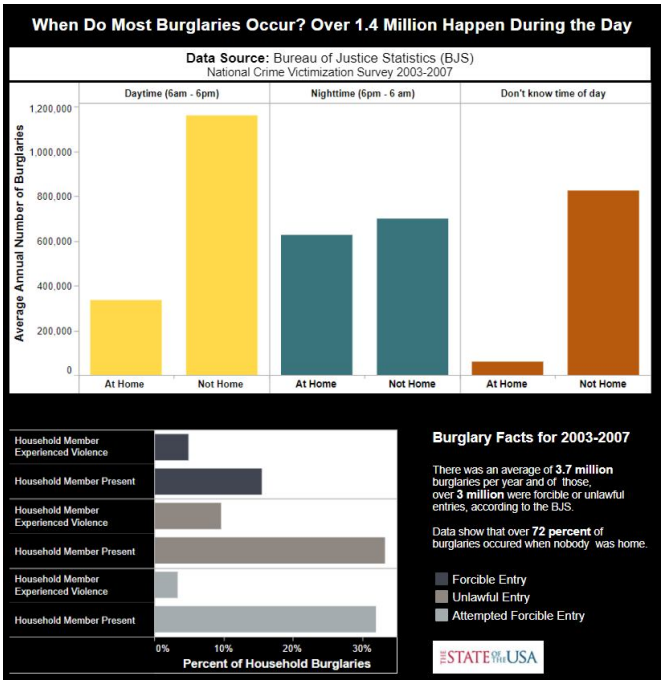

Figure 1: Burglary occurrence timeline

2. RELATED WORK

Intelligent Edge (IE) or Edge Intelligence is computing that uses edge devices alongside machine learning and networking infrastructure. This form of computing has grown over the years due to increase in accessibility of ML tools and devices like Raspberry Pi, Arduino and IoT devices [10].

Machine Learning on edge devices like smart phones, Raspberry Pi, smart watches etc. performing computing on edge nodes like routers and switches is intelligent edge aim of bringing computation to nodes rather than servers on the cloud [10], [11]. Within security domain it means we can have edge devices that listen and watch-out for misbehaviour and provide reports and evidence of crimes committed or providing security against thieves.

Human faces are very diverse in how they look and how a computer receives that as input data for recognition systems. Application of these systems within certain domains is also a key factor to consider [12]. Two major approaches suggest either to represent data of facial appearance as face data or geometry derived from the face. The two systems have been compared by Brunelli and Poggio but an ensemble of both is what is most common these days, leveraging on both appearance and geometrical data [13].

Xu, Liu and Li [14] built a system that was able to detect known and unknown faces at very low resolution, this works by extracting feature vectors from face images and fed into an already trained classifier and from there-on predicts the class of the face if it was known or unknown. Our system however has a dataset of known faces used to train a model for classification and live-feed faces are extracted, classified, uploaded to google cloud store and the android app and in a situation where it fails a local copy is saved for the further use.

Arduino boards and GSM have been used by Kaur et al. on Android to send SMS when certain events occur in the home to notify the home owner, however this does not provide pictorial evidence for use by law enforcement agencies and does not provide a backup for deleted SMS messages. It uses an Infrared sensor to tell if their changes in a room and sends an SMS to the phone of the owner who can turn on an alarm via a Piezo buzzer [15].

Jun et al. developed a system that used infrared sensors, Bluetooth and Zigbee technology to monitor the status of a room and notify the user via SMS or MMS to specialized phones [16], these specialized phones aren't openly available, they also didn't provide backup for deleted data and no model trained on registered faces to prevent a false alarm.

Saranu et al. developed a system for burglar detection using a raspberry pi, PIR sensor, web camera, temperature sensor, mobile dongle, mobile phone and a sub motor. The system is initiated by the PIR sensor used to detect entry into the house, this event switches on the camera to monitor the activities in the room. The raspberry pi conveys the video to the to the owner via the mobile dongle, this leaves the owner to decide whether the activity observes is abnormal or not, if it is the owner initiates an event to release chloroform into the room causing the burglar to go unconscious. The system provides the live usage of monitoring and controlling the activities inside the house when the owner is not present but the system is not autonomous [17]. Naresh et al. proposed the Bluetooth based automation and security system using ARM7, the paper proposed the interfacing of the home electrical parameters to the GPIO (General Purpose Input Output) ports of the microcontroller in an embedded system board and their status is passed to the ARM7 with Bluetooth device and only authorized persons can access home appliances [18].

Chowdhury et al. presented the "access control of doors and home security by the raspberry pi through the internet", the system takes a shot of a person with the camera and sends it via twitter feeds when it detects the presence of a person. The system allows the authorized person to be able to send back a message to the person at the door. The system keeps records of the visitors for retrieval in case of an emergency situation [19]. Bai et al. sued many ultrasonic sensors for the detection of intruders, when a person passes through the field of sense of the sensor, the system turns on the video camera to capture activities in the room, the decision to turn on the camera is done using majority voting mechanism of the ultrasonic sensors [20]. Chandra et.al presented a system that uses an ADC sensor and a PIR sensor attached to a raspberry pi, when an intruder enters into a house the system the intruder's image and sends it to the authorized mail through the internet and SMTP (Simple Mail Transfer Protocol) [3].

Aydin et al. developed a system using raspberry pi as the main controller and PIR sensor to sense movements, when the system detects movement, it activates the camera to capture the image and detect the face and sends it to a smart phone utilizing telegram API [21]. However, the system only detects faces but no info about the face is provided. Huang et al. presented a low power consumption remote home security alarm system developed by applying WSN (Wireless Sensor Network) and GSM technology, the system is able to detect theft and other events such as gas leakage and fire incidence, upon detection of any event, the system sends alarm messages remotely to the users, mobile phone [22].

Bangali and Shaligram suggested two methods for home security system, the first involves the use of a web camera, whenever motion is detected in front of the camera, the system produces a security alert and sends a mail to the owner of the apartment, the second method involves the use of GSM GPS module [23]. Kumari et al. developed "PiCam", a system developed for the deaf based on a raspberry pi which includes a camera, vibrator, wireless GSM and Bluetooth. Images are captured and notification sent to the user's wearable device when the door bell is pressed [24], this is to help know if the person at the door is an intruder or not, additionally a SMS is sent to the owner. Images are stored with date and time to a server for future referencing.

3. METHODOLOGY

A Raspberry Pi Model B+ was used as the computing edge device which housed 32 gigabyte of storage, 1 gigabyte of RAM with a 20,000 milliamps of backup power via a power-bank, due to the hardware limitations of the Raspberry Pi running, building a convolutional neural network model will be impractical hence the choice to use a Histogram of Oriented Gradients (HOG) based model [25].

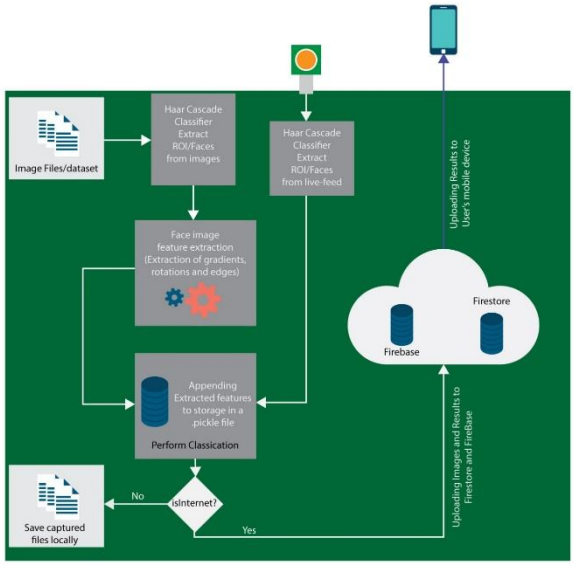

Figure 2: Framework of proposed system

3.1 Data Acquisition

The Histogram of Oriented Gradients uses a feature-based descriptor for detecting objects in computer vision (CV) and image processing. It characterizes local objects and shapes based on distribution of local intensity of the direction of edges and gradients in a fast and simple manner [14]. This is all done without prior knowledge of edge and gradient positions. HOGs tend to be quite sturdy to different light setting as the histogram produces a translational invariance. All this data is summarized into a HOG feature which summarizes the distribution of computations in the boundaries of the image which helps on recognition of deformable and textured objects [26].

The Raspberry Pi reads in data via a pi-cam, this is small in expensive camera module housing a 5-megapixel camera, the images are then fed to a frontal face Haar Cascade classifier, this helps in extracting the region of interest for facial recognition which is the face within the frame of the image. The goal of the Haar Cascade classifier is to help us achieve figure 3a and 3b which holds mostly facial data that is critical to achieving facial recognition [25].

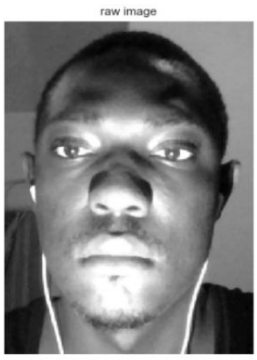

Figure 3a: Image of face cropped out from full frame with mostly relevant information.

Figure 3b: HOG of image in Figure 3a

Haar Cascade is classifier that is used to detect a particular image from source, it is often trained on a server using thousands of images that aren't the object we are training for, called negative images and an image of what we are training for, in this case we are using haar_frontalface_cascade.xml file developed by OpenCV [27], [28]. This helps us detect faces within image frames as our region of interest (ROI).

3.2 Building the Model

During the training phase the face the ROI is fed as parameter to the facial recognition facial_encoding function from dlib library and each encoding obtain on each face image and appended to an encoding list of each face to be registered. This generated list is written to a pickle file, a process called pickling which serializes the list of encoding to a file as a character stream and pickling is done in way that it regenerates the list from a file without losing any data or structural integrity of the list. This encoded file is what is loaded into memory during facial recognition.

After training and successfully generated a pickle file the model is ready to be using, at this stage frames of images are gotten from a live camera feed and this frame are also stripped of irrelevant data leaving only the faces which is used to make inference against registered faces. If a face found and not recognized it is marked as unknown and the time, date and image URL is uploaded to firebase real-time database and an image is uploaded to google cloud storage as shown in Figure 5 and 6. Once this data is uploaded it is immediately reflected in a companion android application.

Figure 4: Image of face data tree of recognized faces with link to captured image.

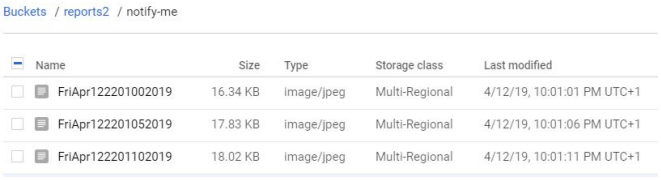

Figure 5: Image of face google cloud storage bucket with captured images.

Firebase database was used in this case because of its immediate update of data changes which is critical in a security application, as any time wasted is time the criminals can use to cover their tracks. In a situation where there is no network the image is saved locally for later viewing of the user.

Figure 6: Captured Image from the picam

3.2 Deployment

A raspberry pi model B+ is the device used for testing the project, it has a camera as shown in Figure 9, 32 gigabytes of storage, 1 gigabyte of RAM, and powered by a 20,000 milliamps power-bank.

The facial recognition model was trained on the raspberry pi device hence influencing the choice of picking Histogram of Oriented Gradients over Convolutional Neural Networks and the devices being small and light makes it easier to conceal, carry and embedded into picture frames home appliances and furniture as long as the device is properly cooled.

The model was able to predict and provide accurate information when test and the results of the output on the companion application is shown in Figure 8.

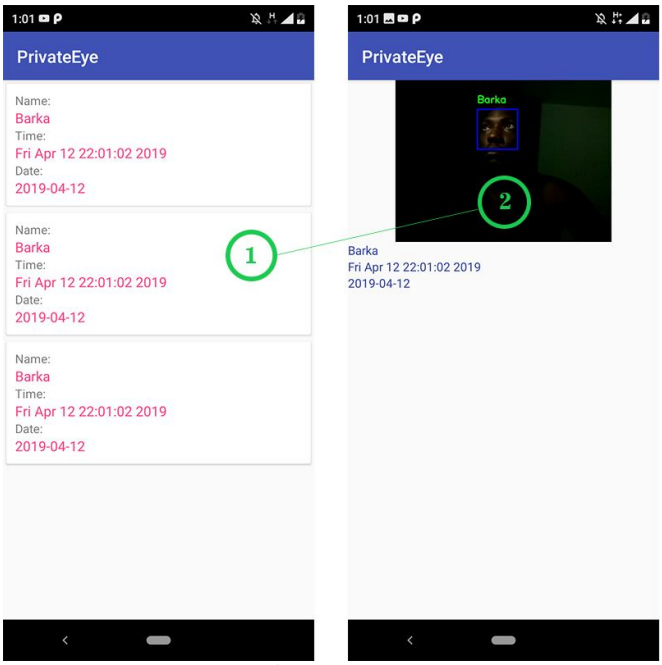

Figure 7: Screenshot of android application showing uploaded results

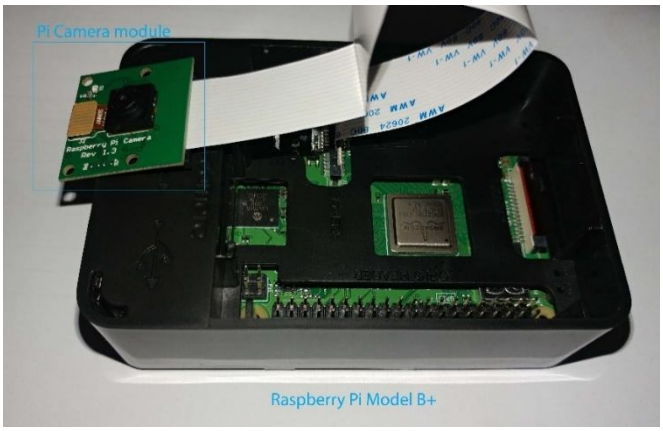

Figure 8: Raspberry pi model b+ with camera module.

4. CONCLUSION

This research was geared at developing an affordable, smart and reliable face recognition security device and system with cloud backend for automated capturing and storing of relevant security related data, equipped with visual detail analysis. The developed system is cheaper than conventional systems, and furthermore, the implementation is internet-driven [29], [30], report is real-time with cheaper device which is able to recognize faces of registered and unregistered users and report to an android application via google cloud platform that will provide evidence of trespassing or intrusion. Usually, as it is with several prediction works [31], there is likelihood of false negative and false positive that may affect the speed, specificity and accuracy of recognition, hence an open problem is recommended for this system to improve performance. This could be archived with further improvement in the use of image compression techniques to compress the images before uploading the images a GCP bucket for storage. This will lead to faster response rate between cloud and mobile device and in turn increasing the response rate of image processing and recognition.

ACKNOWLEDGEMENT

We would like to acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation, and Discovery (CUCRID).

REFERENCES

1. S. Lohmeyer, **New Statistical Approach to Burglary, Related Violence**, 2010. [Online]. Available: http://www.stateoftheusa.org/content/new-approach-to-burglary.php.
2. FBI-UCB, **FBI Burglary report 2017**, 2018. [Online]. Available: https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/burglary.
3. M. L. R. Chandra and B. V. Kumar, **IoT enabled home with smart security**, *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 1193–1197, 2017. https://doi.org/10.1109/ICECDS.2017.8389630
4. J. Daramola, V. Osamor, and O. Oluwagbemi, **A grid-based framework for pervasive healthcare using wireless sensor networks: A case for developing nations**, *Asian Journal of Information Technology*, vol. 7, no. 6, pp. 260–267, 2008.
5. U. Andra, **Network Security in the Age of Hyperconnectivity: Pervasive, Proactive, and Persistent Protection is Essential to Thwart Cyberattacks**, 2017. [Online]. Available: https://blogs.cisco.com/sp/network-security-in-the-age-of-hyperconnectivity-pervasive-proactive-and-persistent-protection-is-essential-to-thwart-cyberattacks.
6. I. Sadgali, N. sael, and F. Benabbou, **Performance of machine learning techniques in the detection of financial frauds**, *Procedia computer science*, vol. 148, pp. 45–54, Jan. 2019. https://doi.org/10.1016/j.procs.2019.01.007
7. B. M. Henrique, V. A. Sobreiro, and H. Kimura, **Literature review: Machine learning techniques applied to financial market prediction**, *Expert Systems with Applications*, vol. 124, pp. 226–251, Jun. 2019. https://doi.org/10.1016/j.eswa.2019.01.012
8. A. Oguntimilehin, G. A. Babalola, and K. A. Olatunji, **A Clinical Diagnostic Model Based on Supervised Learning**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3, pp. 949–953, 2019. https://doi.org/10.30534/ijatcse/2019/94832019
9. S. More and J. Singla, **Machine Learning Techniques with IoT in Agriculture**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3, pp. 742–747, 2019. https://doi.org/10.30534/ijatcse/2019/63832019
10. X. Li and Z. Lin, **Face Recognition Based on HOG and Fast PCA Algorithm**, in *The Fourth Euro-China Conference on Intelligent Data Analysis and*

Applications, Advances in Intelligent Systems and Computing, 2018, vol. 682, pp. 10–22.
11. N. J. Mulder et al., **Development of bioinformatics infrastructure for genomics research**, *Glob. Heart*, vol. 12, no. 2, pp. 91–98, 2017.
12. V. C. Osamor, E. F. Adebiyi, J. O. Oyelade, and S. Doumbia, **Reducing the Time Requirement of k-Means Algorithm**, *PLoS One*, vol. 7, no. 12, 2012. https://doi.org/10.1371/journal.pone.0049946
13. R. Brunelli and T. Poggio, **Face Recognition: Features versus templates**, *IEEE transactions on pattern analysis and machine intelligence*, vol. 15, no. 10, pp. 1042–1052, 1993. https://doi.org/10.1109/34.254061
14. X. Xu, W. Liu, and L. Li, **Low resolution face recognition in surveillance systems**, *Journal of Computer and Communications*, vol. 02, no. 02, pp. 70–77, 2014.
15. S. Kaur, R. Singh, N. Khairwal, and P. Jain, **Home Automation and Security System**, *Advanced Computational Intelligence*, vol. 3, no. 3, pp. 17–23, 2016. https://doi.org/10.5121/acii.2016.3303
16. J. Hou, C. Wu, Z. Yuan, J. Tan, Q. Wang, and Y. Zhou, **Research of intelligent home security surveillance system based on zigbee**, In 2008 *International Symposium on Intelligent Information Technology Application Workshops*, pp. 554-557.
17. P. N. Saranu, **Theft Detection System using PIR Sensor**, in 2018 *4th International Conference on Electrical Energy Systems (ICEES)*, no. 4, pp. 656–660.
18. D. Naresh, B. Chakradhar, and S. Krishnaveni, **Bluetooth based home automation and Security System Using ARM9**, *International Journal of Engineering Trends and Technology (IJETT).*, vol. 4, no. 9, pp. 4052–4058, 2013.
19. M. N. Chowdhury, M. S. Nooman, and S. Sarker, **Access control of door and home Security by Raspberry Pi through internet**, *International Journal of Scientific & Engineering Research*, vol. 4, no. 1, pp. 550–558, 2013.
20. Y.W. Bai, L.S. Shen, and Z.H. Li, **Design and implementation of an embedded home surveillance system by use of multiple ultrasonic sensors**, *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 119–124, 2010. https://doi.org/10.1109/TCE.2010.5439134
21. I. Aydin and N. A. Othman, **A new IoT combined face detection of people by using computer vision for security application**, in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 0–5.
22. H. Huang, S. Xiao, X. Meng, and Y. Xiong, **A Remote Home Security System Based on Wireless Sensor Network and GSM Technology**, in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, pp. 535-538.
23. J. Bangali, A. Shaligram, and S. M. Service, **Design and mplementation of Security Systems for Smart Home based on GSM technology**, *International Journal of Smart Home*, vol. 7, no. 6, pp. 201–208, 2013. https://doi.org/10.14257/ijsh.2013.7.6.19
24. P. Kumari, **PiCam: IoT based wireless alert system for deaf and hard of hearing**, in *2015 International Conference on Advanced Computing and Communications (ADCOM)*, 2016, pp. 39–44.
25. A. Rastogi, **Teat detection algorithm: YOLO vs. Haar-cascade**, *Journal of Mechanical Science and Technology*, no.4, January, 2019. https://doi.org/10.1007/s12206-019-0339-5
26. R. Padilla, C. C. Filho, and M. Costa, **Evaluation of haar cascade classifiers designed for face detection**, *World Academy of Science, Engineering and Technology*, vol. 64, pp. 323–326, 2012.
27. N. Rekha and M. Z. Kurian, **Face detection in real time based on HOG**, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 3, no. 4, pp. 1345–1352, 2014.
28. S. R. Khan, A. Al Mansur, A. Kabir, S. Jaman, and N. Chowdhury, **Design and Implementation of low cost Home Security System using GSM network** *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, pp. 3–8, 2012.
29. A. A, Azeta., S. Misra, V. I. Azeta, V. C. Osamor, **Determining suitability of speech-enabled examination result management system**. **Wireless Networks**, vol. 25, no. 6, pp 3657–3664, 2019. https://doi.org/10.1007/s11276-019-01960-5
30. V. C. Osamor, A. A. Azeta, O. O. Ajulo, **Tuberculosis-Diagnostic Expert System: An architecture for translating patient's information from the web for use in tuberculosis diagnosis**. *Health Informatics Journal*, vol. 20, no. 4, pp. 275-287, 2014. https://doi.org/10.1177/1460458213493197
31. V. C. Osamor and J. Tiuryn, **Analysis of replacing DNase-seq data with histone marks in computational dimer prediction**, *BMC Neuroscience 16(Suppl 1)*, 2015 https://doi.org/10.1186/1471-2202-16-S1-P261