SOFTWARE IMPLEMENTATION OF A FACE RECOGNITION SYSTEM FOR INTRUSION DETECTION AND REPORTING

[1]E. A. Anthony, [2]H. A. Sulaimon & [3]L. P. Damuut
[1] Department of Computer Science, Kaduna State University
Kaduna State, Nigeria.
[2] Department of Computer Science, Federal College of Education, Zaria
Kaduna State, Nigeria.
[3] Department of Computer Science, Plateau State University,
Plateau State, Nigeria.
E-mail: abrakson021@gmail.com **Phone:** + 2348036420271.

Abstract
In light of the increasing crime rate in every part of the world, an enhanced surveillance system has become an inevitable need. The need for Security systems have rapidly grown to high-risk areas like banks, homes, companies, governmental institutions to mention just a few. A good security system should be 24-hour monitoring, ease of use, difficulty to hack, reliability, heat and motion sensors, ability to control doors, and gates. Present day security devices are not sufficient to handle the atrocity perpetuating by the intruders and there is a need to develop an efficient system for it. Introduction of object detection and facial recognition has increased the effectiveness of surveillance by many folds. In this paper, a moving object detection and facial recognition system was developed to detect the intruders and call the owner of the properties through phone call until a response is received. Based on the series of test carried out on the system, there is a direct proportionality between the number of capture and the face percentage accuracy and the percentage accuracy of the system is 5:20%. For every 5 captures, it will be 20% accurate. This means if captured 20 times, 100% accuracy would be realized. This is what actually happened at the training stage of the system development, which will reduce the number of false face recognition.

Keywords: Security Systems, Motion Detection, Object Detection, Face Recognition, Intruders

Introduction

The need for Security systems have rapidly grown to high-risk areas like banks, homes, companies, governmental institutions etc. A good security system should be 24-hour monitoring, ease of use, difficulty to hack, reliability, heat and motion sensors, ability to control doors, and gates. An automated home security system, equipped with state-of-the-art technological devices like digital TVs, digital cameras in a car, has become one of our basic needs. Most homes are now or camcorders, smart refrigerators, washing machines, and other valuable items. It is also common knowledge that these are the favorite items of burglars who finds in them a quick way of making a living.

Recent advances in the Face Recognition (FR) technologies may give an impression that the problem of face matching is essentially solved, e.g. via deep learning models using thousands of samples per face for training and validation on the available benchmark data-sets. Human vision system seems to handle face localization and matching problem differently from the modern FR systems, since humans detect faces instantly even in most cluttered environments, and often require a single view of a face to reliably distinguish it from all others. This prompted us to take a biologically inspired look at building a cognitive architecture that uses artificial neural nets at the face detection stage and adapts a *Single Image Per Person (SIPP)* approach for face image matching.

Sergio and Rojas (2015) stated that Facial recognition is a computer application composes for complex algorithms that use mathematical and metrical techniques, these get the image in raster mode space (digital format) and then process and compare pixel by pixel using different methods for obtaining faster and reliable results.

This paper explores the scientific background as to why face detection recognition has become a trusted form of authentication and alert the presence of an intruder through simulated phone call repeatedly until a response from the owner of the house is received.

2.0 Related Work

Saleh *et al.* (2019) proposed a Smart Intruder Alert System Based on Microprocessor and Motion Detection. Motion detection is attained with a new approach which incorporates PIR sensors with

ARM cortexA53 microprocessor. The sensor is used more effectively with GSM modem through efficient communication between them with the help of both coding and required customization. SMS and calls are initiated from GSM based on the data obtained from sensor.
Nikhil *et al*. (2018) proposed the profoundly pervasive strategy for utilizing CCTV for security has its own offer of traps. Utilizing Face acknowledgment, they propose a framework by utilizing raspberry pi and a camera which identifies faces and remembers them. On the off chance that the countenances are in the database, then they will put them into a log document. If not in the given database the Proprietor will be alarm by utilizing a SMS sent utilizing a GSM module and an email sent by means of web.

Nagaraj *et al*. **(**2015) developed a full-fledged mechanism known as the Intruder Recognition System used to detect, capture and send the facial part of the intruder to the authorized owner for taking action against the intrusion. Passive infrared (PIR) sensors are used to sense the presence of any person in the vicinity of the concerned area. The PIR signals generated are sent to the ARDUINO UNO which is interfaced with the computer. The webcam is used for capturing the image. The fuzzy logic and Local Binary Pattern (LBP) are used to extract face features.
In Nima, *et al.* (2017) approach, a new method for face detection was proposed based on Eigen face as feature extraction and Bat algorithm as classification. This method used for finding people faces as vector in images. The obtained results show that proposed method has high accuracy and speed in comparison to other methods.

Nishu (2014) recent research in computer vision has increasingly focused on building systems for observing humans and understanding their look, activities, and behaviour providing advanced interfaces for interacting with humans, and creating sensible models of humans for various purposes. The research detects moving objects from a static background scene based on frame difference.

The motion detection module is responsible to determine the level of activity while the face detection module differentiates between authorized people and intruders. Several experiments were conducted with live stream video from a camera and the results obtained are very reliable (Sameerchand *et al*., 2013).

Mahalakshmi *et al*. (2013) proposed an architecture for the setting up of a visual surveillance system using CCTV cameras. They also provided considerable technical details about the equipment required and how to install and to use them. Unfortunately, the system has not yet been tested and therefore results are yet to be provided.

Sameerchand *et al.*, (2013) developed a unified intruder alert system by integrating motion detection with face recognition. The motion detection module is responsible to determine the level of activity while the face detection module differentiates between authorized people and intruders. Several experiments were conducted with live stream video from a camera and the results obtained are very reliable. The system effectively distinguishes between the property owners and other people and alarms are raised when the motion level exceeds a threshold value. The capture image is sent to the owner's mailbox when such an alarm is raised which he can view from his mobile device, anywhere and anytime.
Tuscano *et al.*, (2013) implemented a simple but effective surveillance system (Smart Web Cam Motion Detection Surveillance System) which upon detection of motion sounds an alarm, start video recording, sends an email and send an MMS to the mobile phone of the security officer in charge of the building. However, the system does not perform face recognition to eliminate false alerts and motion levels are not categorized.

3.0 Methodology

The intrusion detection algorithm depicts the flow of the system. The monitoring and motion detection stage implies identifying the change in position of object and placing a target on it. It is also seen as the process whereby a system (in this case a surveillance system) has the capability to detect and capture an event in the camera's field of view and upon the event, take required actions.

The face detection is triggered with motion, after which the face recognition stage tries to match the captured face with the already stored faces in the database. If the face is recognized, the event data are stored, otherwise the system alerts the presence of an intruder through a real-time phone call from a computer system. The last stage ensures the phone call is repeated for a number of times until a response from the owner is received.

Intrusion Detection Algorithm

Inputs: motion detection, face detection

*Outputs: Events Data saved (*time*date*face), Real-time Call*

1. Input: Monitoring/Motion Detection = Object detected
2. While (Trigger Face Detection/Recognition Algorithm)
3. if (Face Not Detected)
4. Return "Monitoring/Motion Detection"
5. Else if (Face Detected)
6. Return "Capture Detected face"
7. End if
8. End while
if (Face Recognized)
*Return "Events Data saved *time*date*face)*
9. Else if (Face Not Recognized)
10. Return "Real-time Call (count 0)"
11. While (call count <3)
12. if (call responded)
13. Break loop
14. Else if (call not responded to)
15. Return "replace a call (count +1)
16. End if
17. End while

4.0 Result and Discussion

This section gives an overview of how the Intrusion Detection System (IDS) software components interacts, how a system that will detect the presence of an intruder using motion detection was implemented and how intruders can be traced using face recognition technology and notifies the owner of the house or property via a phone call.

4.1 Features of IDS: The distinct features of IDS include Add Person, Edit Person, White or Black List option, Activate IDS, Minimize IDS, Default Camera, Call Alerts, Train IDS and Exit options as shown in figure 1.

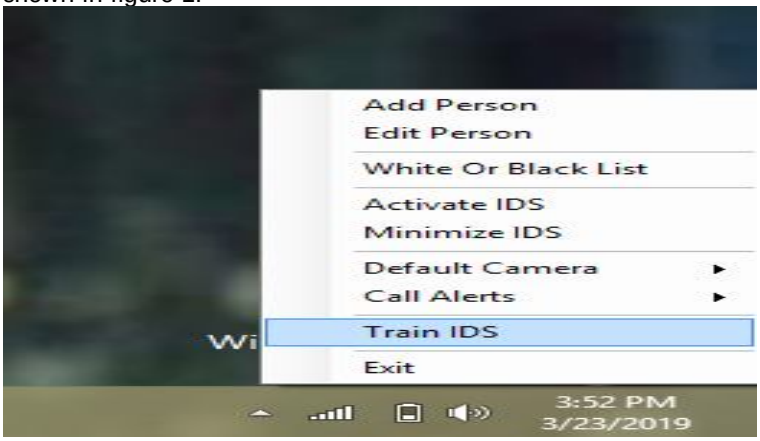

Figure 1: IDS features

Add Person: this option allow a captured face to be saved to the database as part of the recognized faces.

Figure 2: IDS Add Person features

Edit Person: this option allows an already captured face attributes or details to be changed.

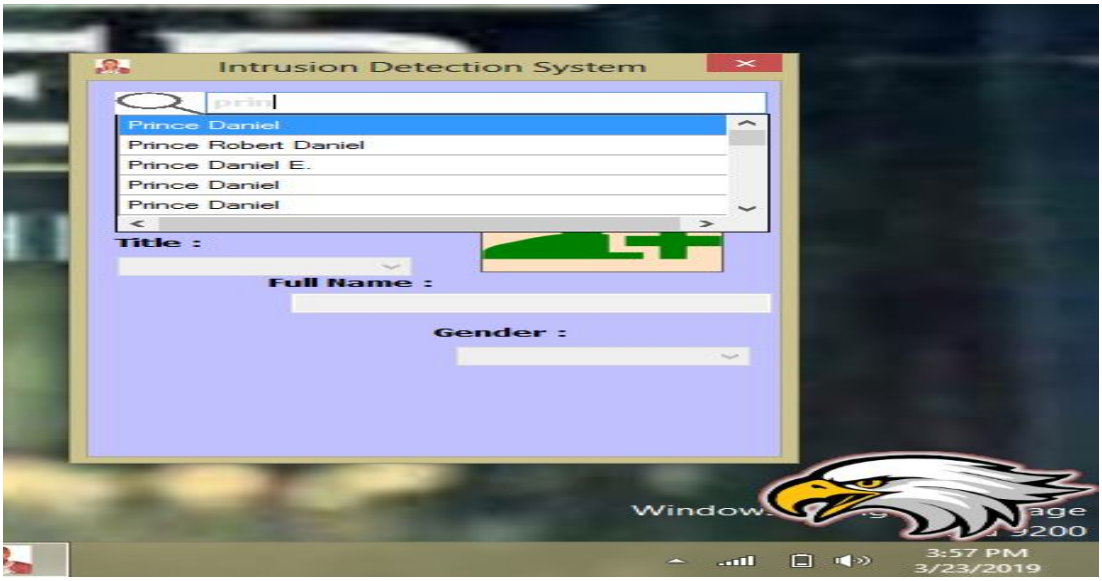

Figure 3: IDS Edit Person feature

White or Black List: this option allows you to move faces from the black list to the white list and vice versa, as shown in figure 4.

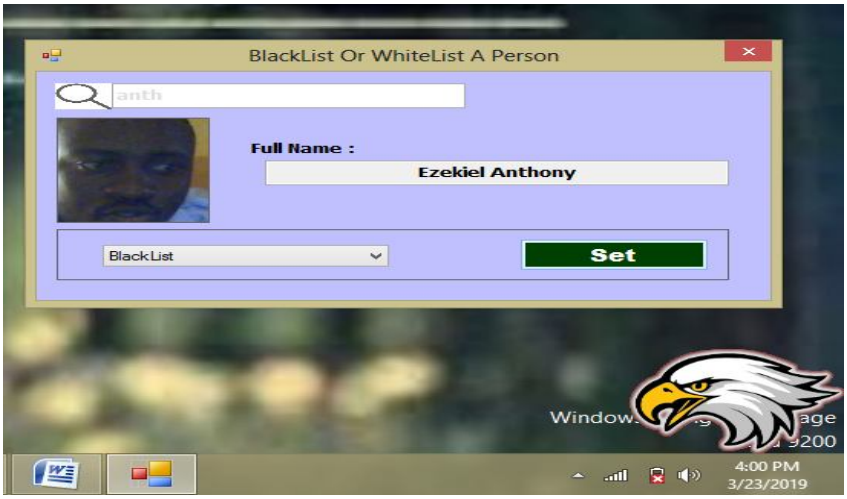

Figure 4: IDS White or Black List feature

iv. Activate IDS: this feature set the recognition process running, comparing the captured face with that in the database, to take appropriate actions, automatically and continuously.

***v. Minimize IDS*:** this feature hides the application currently on screen. IDS Icon remains at the bottom right corner of the screen, but seats at the system tray when minimized.

vi. Default Camera: the system makes provision for different camera options to be used at a specific time. Use this option to set and select the camera to use.

vii. Call Alerts: this feature is responsible for forwarding a call if an unauthorized person is recognized by the system.

viii. Train IDS: this feature is used to train IDS. Training IDS refers to the capturing of faces into IDS database distinctively for the task of facial recognition.

ix. Exit options: this exit command is used to close IDS, in other words stopping it from running.

4.2 IDS Face recognition

Face recognition can easily be done if individual faces are saved in the database. The system at this point can be trained to identify a face at different angles and posture, thereby giving the system adequate information about a person's face. Figure 5 shows IDS training mode interface.

Training mode in IDS is one of the features available for capturing and storing faces along with their names, gender and even titles. These faces can either be on the white or black list. Faces on the white list are trustworthy and those on the black list aren't.

Figure 5: IDS Training Interface

Figure 6 shows IDS capturing faces to save into the database with provision for title, full name, gender with an automatically continues training for this individual, capturing different angles of the face for a more accurate recognition.

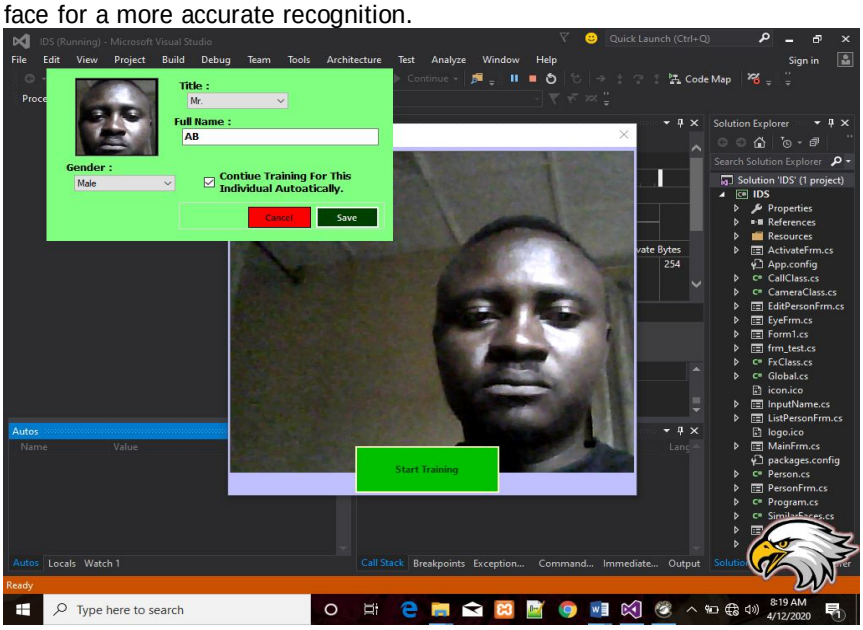

Figure 6: IDS Capturing Interface

4.2.1 Face Validation This phase shows the Activation of IDS, as it set the recognition process running, comparing the captured face with that in the database, to take appropriate actions, automatically and continuously as shown in figure 7. If image is recognized, data consisting of person and time is saved, otherwise a phone call alert is placed to report the presence of an intruder.

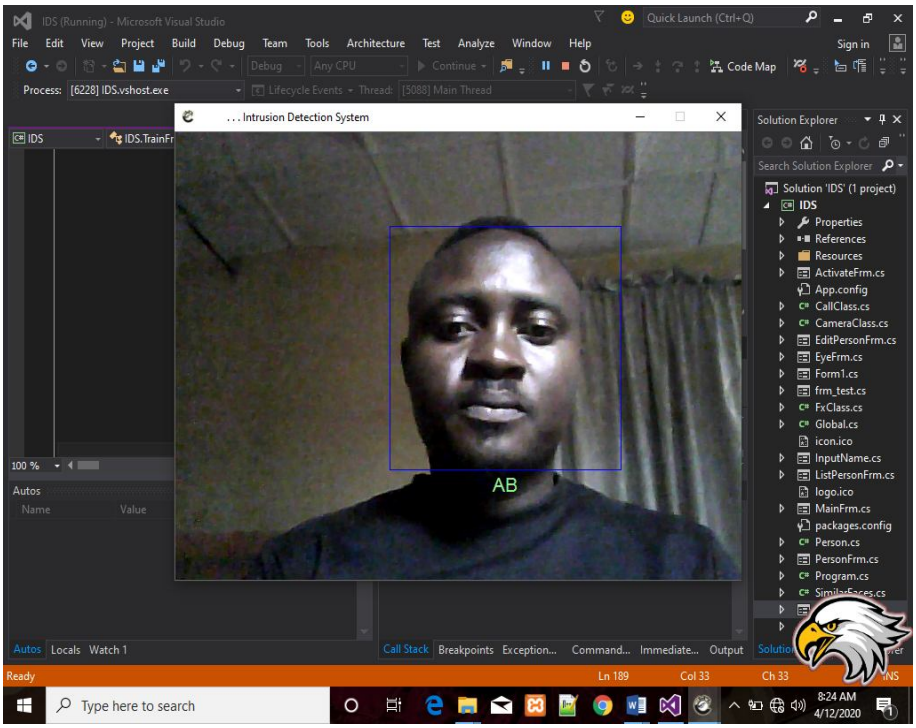

Figure 7: IDS face validation

4.3 Facial Percentage Accuracy Test

Based on the series of test carried out on the system, there is a direct proportionality between the number of capture and the face percentage accuracy and the percentage accuracy of the system is 5:20%. For every 5 captures it will be 20% accurate as shown in table 1 and graphically represented in Figure 8. That means, if there are 25 captures, then there would be 100% accuracy. This is what actually happen when training IDS, which help in reducing false face recognition by the system.

Table 1: Facial Percentage Accuracy Test-Table.

Number of Capture	Percent Accuracy (%)
01	04
02	08
03	12
04	16
05	20
06	24
07	28
08	32
09	36
10	40
11	44
12	48
13	52
14	56
15	60

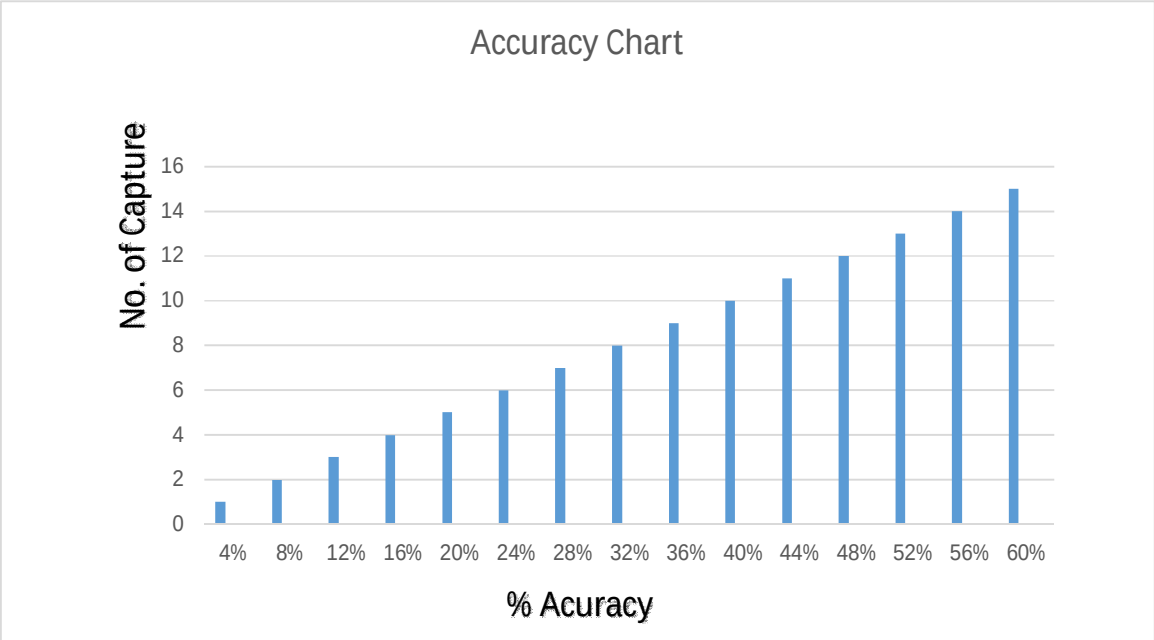

Figure 8: Facial Percentage Accuracy Test Chart

4.4 Measure of System Effectiveness by the Respone Time Interval

From the test carried out in the system, as illustrated below in Figure 9, the following inference are made:

1. The system takes about 850ms to start.
2. When IDS is active, it takes about 2ms to detect a face.
3. If the detected face is not recognized, it takes about 0.5ms to analyze, capture and store the intruder's facial image before further recognition. At exactly 3ms, it forwards a call alert.

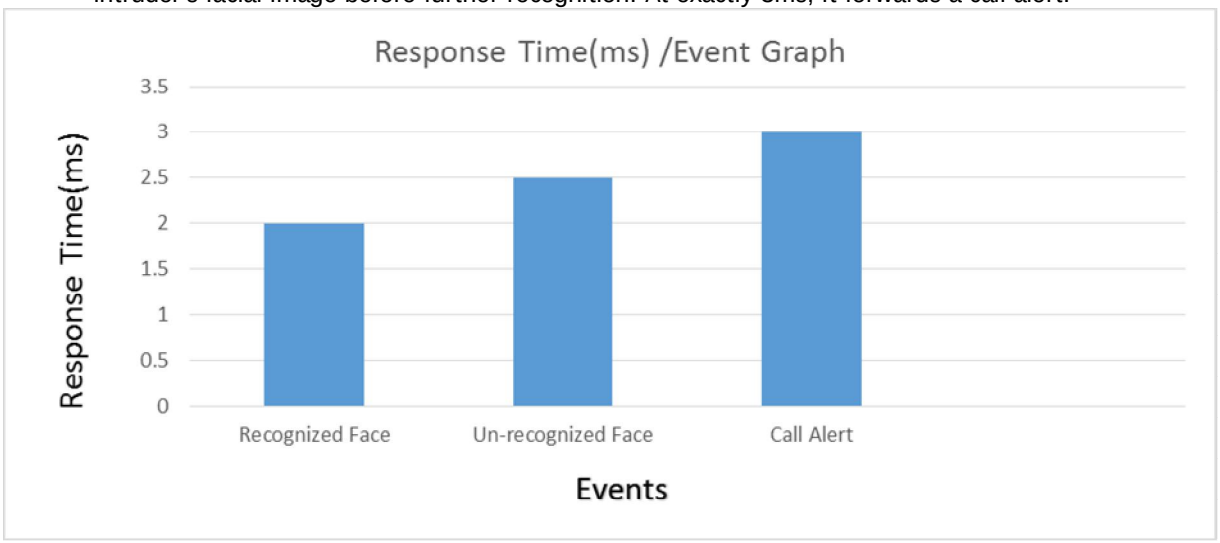

Figure 9: Response Time graph (microseconds) / Event Graph

Conclusion / Further Works

In conclusion, a Face Recognition System for Intrusion Detection and Reporting has been devised and achieved. Moving objects were detected and Face detection recognition system to validate faces and eventually alert the presence of an intruder through simulated phone call. Even though this system could capture multi-faces, the system can only place a real-time call to one recognized face at a time, a further improvement could be done to identify multiple faces and alert the presence of the entire intruders on a call. IDS could also be made to work with multiple cameras at a time. Also, having several layers of calls will improve the degree of the security of properties; I suggest that multiple numbers should be called simultaneously to enhance the degree of any response.

REFERENCES

Mahalakshmi R., Manjula M., Saranya S., Vaishnavi P., Shalini J., Arasa K. R. (2013). Intrusion Detection by Facial Recognition using CCTV Cameras with Video Management System, *International Journal of Advanced Electrical and Electronics Engineering*. 2(2), pp. 59-62

Nagaraj U., Shreesha M., & Abdullah P. (2015) Intruder Recognition System.1 Shree Dharmasthala Manjunatheshwara Institute of Technology 2 Manipal Institute of Technology 3 P.A.College of Engineering.

Nikhil, K., Bharat, K., Vigneshwari, S., & Gowrii, S. (2018) Surveillance Camera with Facial Detection and Recognition using machine learning. *International Journal of Pure and Applied Mathematics*, School of Computing, Sathyabama Institute of Science & Technology, Chennai (Vol 118).

Nima A., Rama H. P., Seyed M. J., & Bashir B. N. (2017) *A New System for Face Detection based on Eigen Face and Bat Algorithm.* Bulletin de la Société Royale des Sciences de Liège, 1 (86) 461 – 473461

Nishu S. (2014) Motion Detection Based on Frame Difference Method. *International Research Publications House.* Department of Computer Science Punjabi University, Patiala, Punjab. (1559-1565)

Saleh A. K., Ishtiaq A., Abu S., Sazzad A. (2019) A Smart Intruder Alert System Based on Microprocessor and Motion Detection. Department of Electrical and Electronic Engineering American International University-Bangladesh Dhaka-1229, Dhaka, Bangladesh.

Sameerchand, P., Faugoo, I., & Nandrakant B. (2013) A Unified Intrusion Alert System using Motion Detection and Face Recognition. *International Conference on Machine Learning and Computer Science Kuala Lumpur (Malaysia)*

Sergio, A.G., & Rojas, A.G. (2015). Multiple face detection and recognition in real time. Retrieved from *http://www.codeproject.com/Article/239849/multiple-face-detection-and-reconition-in-real-time.*

Tuscano C., Lopes B., Machado S. (2013). Smart Web Cam Motion Detection Surveillance System. *International Journal of Modern Engineering Research,* 3(2), pp. 1169-1171.