



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: <https://doi.org/10.22214/ijraset.2023.56367>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

FaceBreach Alert: Multi-Modal Intrusion Detection emphasizing Face Recognition

Omica Kale¹, Sanika Kshirsagar², Rupali Bathe³
Computer Department, Savitribai Phule Pune University

Abstract: *The face is one of the easiest ways to distinguish the individual identity of each other. Face recognition is a personal identification system that uses personal characteristics of a person to identify the person's identity. Human face recognition procedure basically consists of two phases, namely face detection, where this process takes place very rapidly in humans, except under conditions where the object is located at a short distance away, the next is the introduction, which recognize a face as individuals. Stage is then replicated and developed as a model for facial image recognition (face recognition) is one of the much-studied biometrics technology and developed by experts. There are two kinds of methods that are currently popular in developed face recognition pattern namely, Eigenface method and Fisher face method. Facial image recognition Eigenface method is based on the reduction of face dimensional space using Principal Component Analysis (PCA) for facial features. The main purpose of the use of PCA on face recognition using Eigen faces was formed (face space) by finding the eigenvector corresponding to the largest eigenvalue of the face image. The area of this project face detection system with face recognition is Image processing. The software requirements for this project is MATLAB software.*

Keywords: *Digital Image Processing, Face Detection, Face Recognition, Motion Detection*

I. INTRODUCTION

In sensitive area where generally no one is allowed So first we will detect the motion after the motion detection it automatically revoke the functions for face detection. The identification of human can be done through the face of human. So first we detect face of human after that, does that face has mask or it is naked face. If it is naked face check in our database that does that human is present in database or someone else. Real time security face recognition is part of the field of biometrics. Biometrics is the ability for a computer to recognize a human through a unique physical trait. Face recognition provides the capability for the computer to recognize a human by facial characteristics.

Real time security face recognition is part of the field of biometrics. Biometrics is the ability for a computer to recognize a human through a unique physical trait. Face recognition provides the capability for the computer to recognize a human by facial characteristics. Today, biometrics is one of the fastest growing fields in advanced technology. Predictions indicate a biometrics explosion in the next century, to authenticate identities and avoid and unauthorized access to networks, database and facilities. A facial recognition device is a device that takes an image or a video of a human face and compares it to other image faces in a database.

The structure, shape and proportions of the faces are compared during the face recognition steps. In addition, distance between the eyes, nose, mouth and jaw, upper outlines of the eye sockets, the sides of the mouth, location of the nose and eyes, and the area surrounding the cheek bones are also compared. When using a facial recognition program, several pictures of the person must be taken at different angles and with different facial expressions. At time of verification and identification the subject stands in front of the camera for a few seconds, and then the image is compared to those that have been previously recorded. Facial recognition is widely used because of its benefits.

The advantages of facial recognition are that it is not intrusive, can be done from a faraway distance even without the person being aware that he/she is being scanned. Such thing is needed in banks or government offices for example, and this is what makes facial recognition systems better than other biometric techniques in that they can be used for surveillance purposes like searching for wanted criminals, suspected terrorists, or missing children. Face recognition devices are most beneficial to use for facial authentication than for identification purposes, because it is easy to alter someone's face, and because the person can disguise using a mask. Environment is also a consideration as well as subject motion and focus on the camera. Facial recognition, when used in combination with another biometric method, can improve verification and identification results dramatically.

II. EXISTING SYSTEM

- 1) *Home Security Systems*: Residential security systems often include sensors for doors, windows, and motion detection. These systems can be connected to monitoring services and may include features like video surveillance and remote access control.
- 2) *Commercial and Industrial Security Systems*: Businesses and industries use more advanced systems that combine various technologies, such as access control, CCTV cameras, motion sensors, and alarm systems to protect their properties and assets.
- 3) *Access Control Systems*: Access control systems are commonly used in office buildings, data centers, and research facilities. These systems restrict entry to authorized personnel through key cards, biometrics, or PIN codes.
- 4) *Video Surveillance Systems*: Video surveillance systems use cameras to monitor and record activities in and around a facility. These are often integrated with other security features like facial recognition and object tracking.
- 5) *Smart Home Security Systems*: Smart home systems integrate intruder detection with home automation. They may include features like remote control, integration with smart locks, and alerts sent to mobile devices.
- 6) *Biometric Security Systems*: Biometric systems use fingerprint, iris, facial recognition, and other biometric data to control access and verify identity.
- 7) *Government and Military Security*: High-security installations use complex intrusion detection systems. These often involve layered security, access control, and advanced surveillance.
- 8) *Fire and Intrusion Alarm Systems*: These systems provide alerts for both fire and intrusion. They are used in commercial buildings and homes to ensure safety and security.

III. PROPOSED SYSTEM

The proposed Intruder Detection System is a comprehensive security solution that combines multiple advanced technologies to enhance security and safety. Key features of the system include motion detection, object detection, height detection, and mask detection to accurately identify potential intruders. The system employs a network of sensors, cameras, and processing units to monitor the environment in real-time.

A. Main Features

- 1) *Motion Detection*: Uses motion sensors to identify any movement within the monitored area.
- 2) *Object Detection*: Employs deep learning models for precise identification of objects and individuals.
- 3) *Height Detection*: Utilizes stereo vision and LiDAR technology to estimate the height of detected objects.
- 4) *Mask Detection*: Monitors compliance with health and safety regulations by detecting mask-wearing.
 - a) *User Interface*: A user-friendly interface provides easy system configuration and monitoring.
 - b) *Remote Access*: Allows for remote monitoring and control for real-time response to security incidents.
 - c) *Scalability*: Suitable for small residences to large industrial complexes.
 - d) *Privacy Protection*: Adheres to privacy regulations and respects the rights of individuals.
 - e) *Customization*: Tailored to the specific needs and security requirements of the environment.

IV. ALGORITHMS

To develop an Intruder Detection System with capabilities such as motion detection, object detection, height detection, and mask detection, you can use a variety of algorithms and technologies. Here are some commonly used algorithms and techniques for these specific functionalities:

A. Motion Detection

- 1) Background Subtraction (e.g., Gaussian Mixture Models)
- 2) Optical Flow (e.g., Lucas-Kanade)
- 3) Frame Differencing

B. Object Detection

- 1) You can use deep learning models like:
 - 2) YOLO (You Only Look Once)
 - 3) Faster R-CNN (Region-based Convolutional Neural Networks)
 - 4) SSD (Single Shot MultiBox Detector)
 - 5) Haar Cascade Classifiers (for simpler object detection tasks)

C. Height Detection

- 1) Stereoscopic vision techniques using two cameras to estimate object heights.
- 2) LiDAR (Light Detection and Ranging) for precise 3D height sensing.

D. Mask Detection

Use deep learning models or image processing techniques to detect whether individuals within the monitored area are wearing masks.

E. Image Preprocessing

Techniques for image enhancement, normalization, and resizing to prepare input images for object detection and analysis.

V. LITERATURE SURVEY & EXISTING SYSTEM:

[1]

Title	An Intelligent Motion Detection Using OpenCV
Name of Author	Dr. Yusuf perwej
Year of Publishing	2022
Details	One of the key reasons is that dealing with numerous restrictions such as environmental fluctuations makes the moving object detection process harder. For object detection and counting, OpenCV includes a number of useful techniques.

[2]

Title	Real-Time Face Mask Detection using OpenCV and DeepLearning.
Name of Author	H.S. Upendra
Year of Publishing	2021
Details	In this research study, the Haar-Cascade algorithm, also known as the Viola-Jones algorithm, and OpenCV library classifiers are implemented to find whether someone is wearing a mask or not.

[3]

Title	Highly Accurate and Fine-grained Person Name Recognition
Name of Author	Rui Zhang
Year of Publishing	2021
Details	It proposes a fine-grained annotation scheme based on anthroponymy. To take full advantage of the fine-grained annotations, we propose a Co-guided Neural Network (CogNN) for person name recognition.

[4]

Title	Adaptive moving object detection algorithm based on back ground subtraction and motion estimation.
Name of Author	Shengrong Gong
Year of Publishing	2018
Details	use adaptive Gaussian mixture model (AGMM) to model background and get regions of moving objects by background subtraction.

VI. PROBLEM STATEMENT

The problem is that in some sensitive area where no one is allowed, so detect the motion to identify if someone is entering in there and check if that person is present in dataset or not.

VII. OBJECTIVES

- 1) *Implement Motion Detection:* Develop an accurate and reliable motion detection algorithm that can differentiate between human motion and other types of movement within the surveillance area.
- 2) *Implement Face Detection:* Utilize a robust face detection algorithm that can detect and locate faces within captured video frames, even under varying lighting conditions and different camera angles.
- 3) *Train Facial Recognition Model:* Develop a machine learning model capable of recognizing authorized individuals by comparing detected faces against a prepopulated database of known individuals. The model should be able to handle variations in facial appearance.
- 4) *Integrate Access Control Mechanisms:* Integrate the facial recognition system with access control mechanisms such as electronic door locks or turnstiles. Enable seamless communication between the system and access control devices for granting or denying access based on facial recognition results.
- 5) *Ensure Security and Privacy:* Implement appropriate security measures to protect the facial recognition system and the stored face data. Address privacy concerns by adhering to relevant regulations and implementing privacy safeguards.

VIII. ADVANTAGES

- 1) *Enhanced Security:* It significantly improves security by detecting potential intruders and alerting relevant authorities or personnel, reducing the risk of unauthorized access and security breaches.
- 2) *Real-Time Monitoring:* The system provides continuous real-time monitoring, enabling prompt responses to security threats as they occur.
- 3) *Reduced False Alarms:* By combining multiple detection methods (motion, object, height, and mask detection), the system can reduce false alarms, ensuring that alerts are triggered only when actual intruders are detected.
- 4) *Customization:* The system can be tailored to the specific needs of the environment it's installed in, allowing for a high degree of customization to suit different security requirements.
- 5) *Multi-Layered Detection:* The combination of different detection capabilities offers a multi-layered approach to security, making it more robust against sophisticated intrusion attempts.

IX. DISADVANTAGES

- 1) *Maintenance:* Regular maintenance and calibration are necessary to ensure the system remains accurate and effective, adding ongoing costs and effort.
- 2) *Privacy Concerns:* The use of cameras and sensors for monitoring may raise privacy concerns, and it's essential to address these issues, especially in residential settings.
- 3) *Technical Challenges:* Integrating different detection methods and technologies can be complex and may require technical expertise.

X. APPLICATIONS

- 1) *Residential Security:* Protecting homes and properties from break-ins and unauthorized access, ensuring the safety of residents and their belongings.
- 2) *Commercial and Industrial Security:* Safeguarding offices, warehouses, factories, and industrial facilities from theft, vandalism, and unauthorized intrusions.
- 3) *Retail Stores:* Preventing shoplifting and monitoring customer activity in retail environments.
- 4) *Banking and Finance:* Securing banks and financial institutions against robberies and unauthorized access to sensitive areas.
- 5) *Healthcare Facilities:* Protecting healthcare facilities, patient rooms, and storage areas for medications and medical equipment.
- 6) *Critical Infrastructure:* Ensuring the security of critical infrastructure such as power plants, water treatment facilities, and data centers.
- 7) *Education Institutions:* Enhancing campus security by monitoring entrances and restricting unauthorized access to school or university buildings.
- 8) *Airports and Seaports:* Enhancing security at transportation hubs to prevent unauthorized access to restricted areas.
- 9) *Data Centers:* Protecting data centers against physical intrusions to safeguard critical data and infrastructure.
- 10) *Border Control:* Monitoring and securing border areas to prevent illegal crossings and smuggling.

XI. SYSTEM OVERVIEW

The Intruder Detection System is designed to monitor and secure a specified area, such as a home, office, or facility, by detecting and alerting to potential intrusions.

The system combines various sensors and technologies to achieve its objectives:

- 1) *Motion Detection:* Motion detection is captured with the help of the frame rate change and the video change by taking snapshots continuously and comparing them with the previous ones.
- 2) *Object Detection:* Cameras or other imaging devices capture visual data and employ object detection algorithms, CNN, to identify and locate objects within the frame.
- 3) *Name Detection:* Name is detected with the help of face recognition by using cnn algorithms and training the system with the persons facial data.
- 4) *Mask Detection:* Cameras and deep learning models are used to identify whether individuals within the monitored area are wearing masks, enhancing security in environments with mask-wearing requirements.
- 5) *Decision-Making and Alerting:* The system's decision-making algorithm evaluates the collected data to determine whether an intruder is present. If an intruder is detected, it triggers alerts, which can include sounding alarms, sending notifications to designated users, or activating security measures.
- 6) *User Interface:* The system is typically equipped with a user-friendly interface that allows users to monitor the system's status, configure settings, and access security footage.

XII. BLOCK DIAGRAM

Fig.1 shows the block diagram of the proposed Unauthorized Entry Detection System. Precisely, the proposed system is to detect intruders or authorized persons and alert the security with a buzzer and vibration on positive detection.

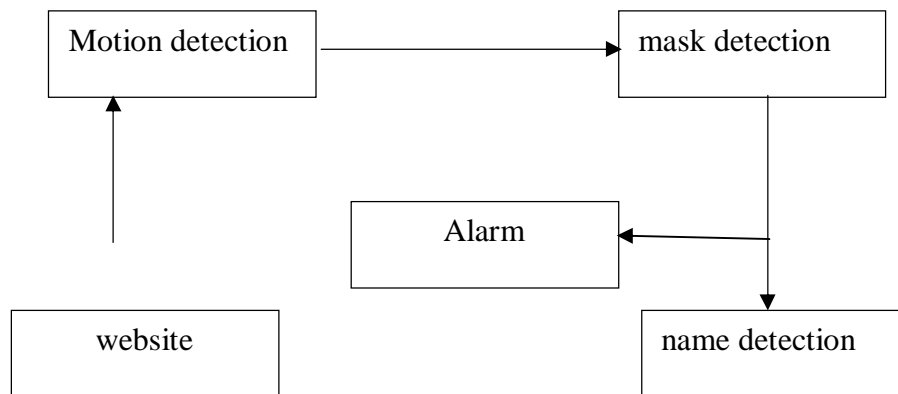


Fig.1: Block Diagram of Proposed System

- 1) *Motion Detection:* To detect if there is any kind of motion in the premises then the system will give an alert.
- 2) *Name Detection:* The aim is to identify if the person entering the room is an authorized person or a unauthorized person by detecting his facial features and giving an output as a name or an alarm.
- 3) *Mask Detection:* If the unknown person is not been recognized or if the entered person is wearing a mask then the system will immediately set an alarm as its not possible for the system to recognize the persons face and process it to check if the person is known or unknown and will predict that the person is a threat to the area of valuables and set a high level alarm
- 4) *Alarm:* If the conditions of the system don't satisfy as of detection of motion, unknown person entry, mask detection then the system will turn on the alarm.

XIII. DATA FLOW DIAGRAM

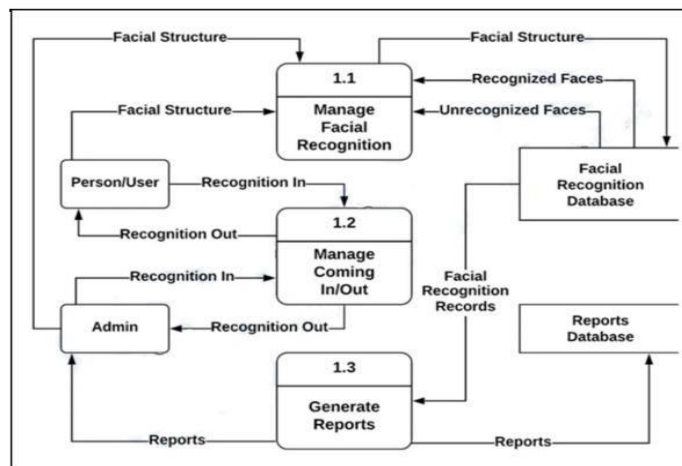


Fig.2: Data Flow Diagram of Proposed System

XIV. ARCHITECTURE DIAGRAM

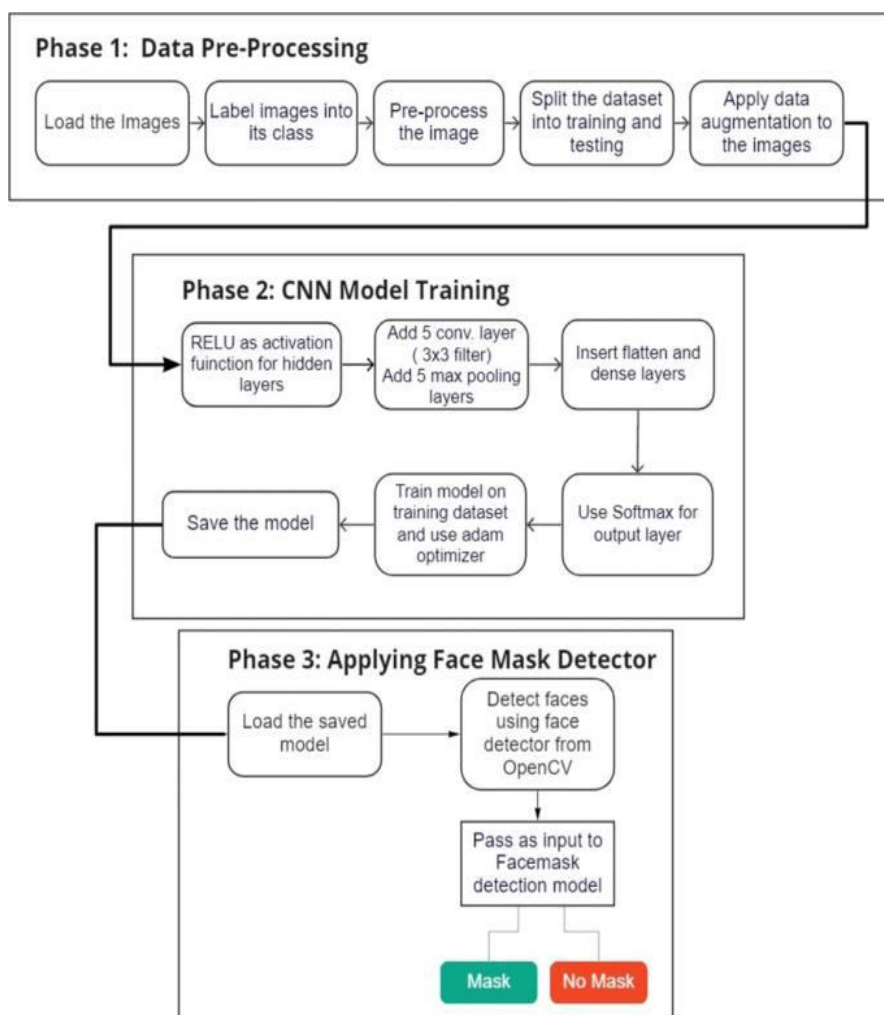


Fig.3: System Architecture Diagram of Proposed System

A. Hardware

1) Webcam



Fig 4: Webcam

2) Specifications

TABLE I
SPECIFICATIONS

Sr. No.	Technical Parameters	Technical Detail
1.	Focus Type	Fixed
2.	Connectivity	USB
3.	Has Tilt	Yes
4.	Sales Package	1 Webcam, User Manual
5.	Focus Range	60 cm
6.	Lens Type	Fixed Lens
7.	Tilt Angle	72.4 Degree
8.	Model Id	CH-0221
9.	Built In Microphone	Yes
10.	Has Night Vision	Yes
11.	Compatible Devices	Laptop, PC
12.	Color	Black
13.	Brand	Flipkart SmartBuy
14.	Flash Memory Type	SD
15.	Colour	Black
16.	MP	2 MP
17.	Product Dimensions	17.2 x 16 x 8 cm; 90 Grams
18.	Optical zoom	2 x
19.	Digital zoom	2 x
20.	Video Capture Resolution	1080p
21.	Plug and Play	No drivers needed, just plug the webcam via the USB port into the computer
22.	Power Source	DC 5V 110mA
23.	Connector Type	USB

B. Software

We are using “PYTHON” coding for our implementation. This language gave high accuracy on face detection. Thus, we have two main functions on that. First one for detecting the eye blinking and the second one is for reading the blinking. This calculation invoked into the complete set of 1 programs. The camera system continuously monitors and sends the video file to the programming. The function which is for getting the data to observe it and the blinking detection function reads the file if it detects then it completely makes reading with that corresponding function and the signals are send to the alerting mechanism.

- 1) *OpenCV*: OpenCV is an open-source software library for computer vision and machine learning. The OpenCV full form is OpenSource Computer Vision Library. It was created to provide a shared infrastructure for applications for computer vision and to speed up the use of machine perception in consumer products. OpenCV, as a BSD-licensed software, makes it simple for companies to use and change the code. There are some predefined packages and libraries that make our life simple and OpenCV is one of them.
- 2) *Computer Vision*: The term Computer Vision (CV) is used and heard very often in artificial intelligence (AI) and deep learning (DL) applications. The term essentially means giving a computer the ability to see the world as we humans do. The entire process involves image acquiring, screening, analyzing, identifying and extracting information. This extensive processing helps computers to understand any visual content and act on it accordingly.

XV. CONCLUSION

The most modern technologies used in the struggle against theft and destruction are video monitoring and surveillance. With the help of technology, it is possible to see and record every square inch and passing second of the area of interest. Face detection and identification techniques are used to achieve the aim. To discover, locate, and extract faces in obtained pictures, knowledge-based face detection techniques are applied. Based on the findings of the study presented, real-time face mask identification using OpenCV and deep learning algorithms is a remarkable solution for straightforward facemask recognition.

REFERENCES

- [1] Belhassen Akrouf and Walid Mahdi, “Yawning detection by the analysis of variational descriptor for monitoring driver drowsiness”, International Image Processing, Applications and Systems (IPAS), 5-7 Nov. 2016.
- [2] Eugene Zilberg, Zheng Ming Xu, David Burton, Murad Karrar and Saroj Lal, “Methodology and initial analysis results for development of non-invasive and hybrid driver drowsiness detection systems”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), 27-30 Aug. 2007.
- [3] Tianyi Hong and Huabiao Qin, “Drivers drowsiness detection in embedded system”, IEEE International Conference on Vehicular Electronics and Safety, 13-15 Dec. 2007.
- [4] Fouzia, R. Roopalakshmi, Jayantkumar A. Rathod, Ashwitha S. Shetty And K. Supriya, “Driver Drowsiness Detection System Based On Visual Features”, 2018 Second International Conference On Inventive Communication And Computational Technologies (ICICCT), 20 – 21 April 2018.
- [5] Yashika Kalyal, Suhas Alur And Shipra Dwivedi, “Safe Driving By Detecting Lane Discipline And Driver Drowsiness”, Ieee International Conference On Advanced Communications, Control And Computing Technologies, 8-10 May 2014.
- [6] C. V Anilkumar, Mansoor Ahmed, R Sahana, R Thejashwini, P. S Anisha, “Design of Drowsiness, Heart Beat Detection System And Alertness Indicator For Driver Safety”, IEEE International Conference On Recent Trends In Electronics, Information & Communication Technology (Rteict), 20-21 May 2016.
- [7] Jang Woon Baek, Byung-Gil Han, Kwang-Ju Kim, Yun-Su Chung And Soo-In Lee, “Real-Time Drowsiness Detection Algorithm For Driver State Monitoring Systems”, Tenth International Conference On Ubiquitous And Future Networks (Icufn), 3-6 July 2018.
- [8] Gao Zhenhai, Le DinhDat, Hu Hongyu, Yu Ziwen and Wu Xinyu, “Driver Drowsiness Detection Based on Time Series Analysis of Steering Wheel Angular Velocity”, 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 14-15 Jan. 2017.
- [9] M. Omidyeganeh, A. Javadtalab, S. Shirmohammadi, “Intelligent Driver Drowsiness Detection Through Fusion Of Yawning And Eye Closure”, IEEE International Conference On Virtual Environments, Human-Computer Interfaces And Measurement Systems Proceedings, 19-21 Sept. 2011.
- [10] Brandy Warwick, Nicholas Symons, Xiao Chen and Kaiqi Xiong, “Detecting Driver Drowsiness Using Wireless Wearables”, 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems, 19-22 Oct. 2015
- [11] Hyung-Tak Choi, Moon-Ki Baek and Kyu-Chul Lee, “Driver Drowsiness Detection based on Multimodal using Fusion of Visual feature and Bio-signal”, 2018 International Conference on Information and Communication Technology Convergence (ICTC), 17-19 Oct. 2018.
- [12] Aldila Riztiane, David Habsara Hareva, Dina Stefani and Samuel Lukas, “Driver Drowsiness Detection Using Visual Information On Android Device”, International Conference on Soft Computing, Intelligent System and Information Technology (ICSIT), 26-29 Sept. 2017.
- [13] Cyun-Yi Lin, Paul Chang, Alan Wang and Chih-Peng Fan, “Machine Learning and Gradient Statistics Based Real-Time Driver Drowsiness Detection”, IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 19-21 May 2018.
- [14] Omar Rigane, Karim Abbes, Chokri Abdelmoula, Mohamed Masmoudi, “A Fuzzy Based Method for Driver Drowsiness Detection”, 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 30 Oct.-3 Nov. 2017.
- [15] Abdullah Salem Baquhaizel, Mohamed El Amine Ouis, Meriem Boumehed, Abdelaziz Ouamri And Mokhtar Keche, “Driver Drowsiness Detection System”, 2013 8th International Workshop On Systems, Signal Processing And Their Applications (Wosspa), 12-15 May



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)