

# FaceBreach Alert: Multi-Modal Intrusion Detection Emphasizing Face Recognition

Omica Kale<sup>1</sup>, Sanika Kshirsagar<sup>2</sup>, Prof. Rupali Bathe<sup>3</sup>

Students, Department of Computer Engineering<sup>1,2</sup>

Professor, Department of Computer Engineering<sup>3</sup>

Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

**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. PROPOSED METHODOLOGY

- Agile Development: Break down the project into smaller tasks and prioritize them. This allows for iterative development, quick problem resolution, and regular feedback.
- User-Centered Design: Involve end-users in the development process through usability testing and feedback sessions to ensure the system meets their needs.
- Rapid Prototyping: Develop prototypes to validate key functionalities and identify and resolve problems early on.
- Performance Optimization: Continuously optimize critical components, such as face detection algorithms, to enhance efficiency.
- Continuous Integration and Testing: Implement automated testing and regular integration to detect and fix issues early.
- Collaborative Problem-Solving: Foster collaboration within the team to collectively solve problems and share knowledge.
- Documentation and Knowledge Management: Maintain detailed documentation and establish a knowledge management system for quick access to resources and solutions.

### 2.1 Architecture

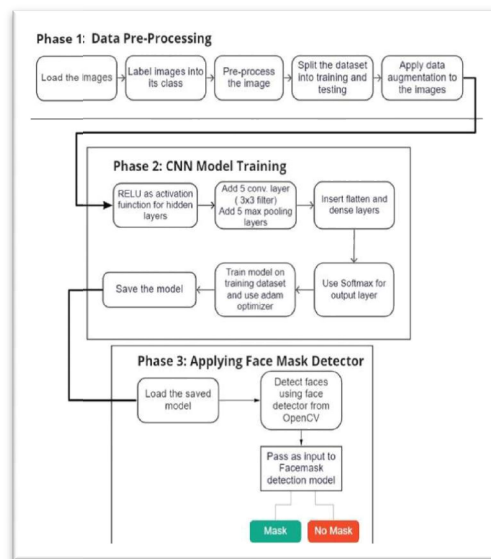


Fig. 1 System Architecture Design

### 2.2 Advantages of Proposed System

- 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.
- Real-Time Monitoring: The system provides continuous real-time monitoring, enabling prompt responses to security threats as they occur.

- **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.
- **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.
- **Multi-Layered Detection:** The combination of different detection capabilities offers a multi-layered approach to security, making it more robust against sophisticated intrusion attempts.

Fig.2 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.

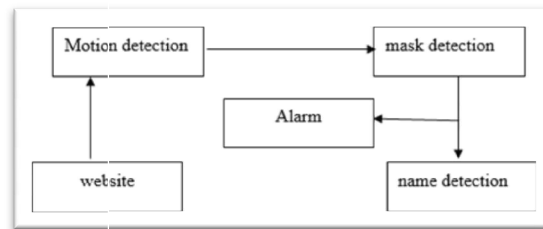


Fig. 2 Block Diagram

**Motion detection:**

To detect if there is any kind of motion in the premises then the system will give an alert.

**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.

**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 it's 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

**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.

### III. SYSTEM DESIGN

#### Introduction

**System Architecture:** The system architecture defines the overall structure of the smartsecurity surveillance system. It outlines the components, their interactions, and the flowof data and information within the system. It may include modules for motion detection,face detection, face recognition, alarm triggering, database management, and integration with IoT devices or security systems.

**Motion Detection Module:** This module focuses on detecting motion within the video frames or camera feed. It may employ algorithms like background subtraction, optical flow, or frame difference to identify moving objects.

**Face Detection Module:** The face detection module is responsible for identifying humanfaces within the video frames. It may utilize algorithms such as Haar cascades, CNNs,or HOG to detect and localize faces accurately.

**Face Recognition Module:** This module performs face recognition against a database ofknown individuals. It extracts facial features from the detected faces and compares them with the stored face data to determine if a match exists. Algorithms like Eigenfaces, Fisher faces, LBP, or deep learning-based approaches may be used for face recognition.

**Alarm Triggering Module:** When a covered face is detected or an unrecognized face isidentified, the alarm triggering module activates the appropriate alarm mechanism. It may involve playing audio alerts, displaying visual indicators, or sending notifications to security personnel

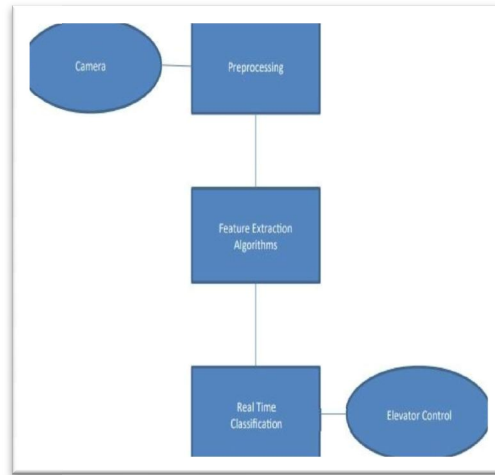


Fig. 3 Level 0 Data Flow Diagram

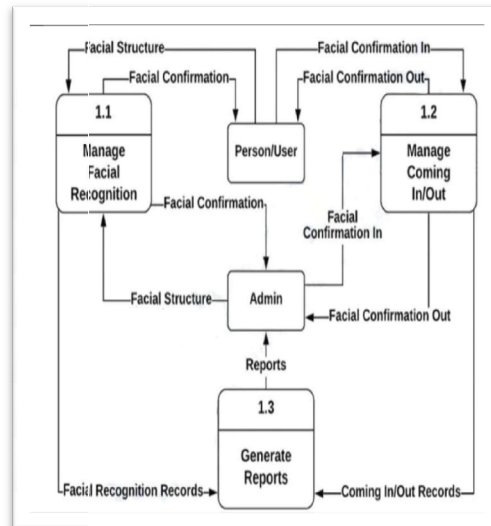
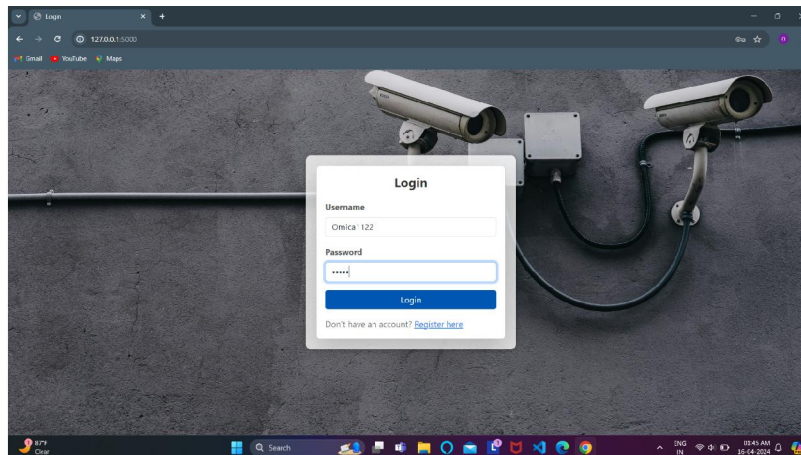
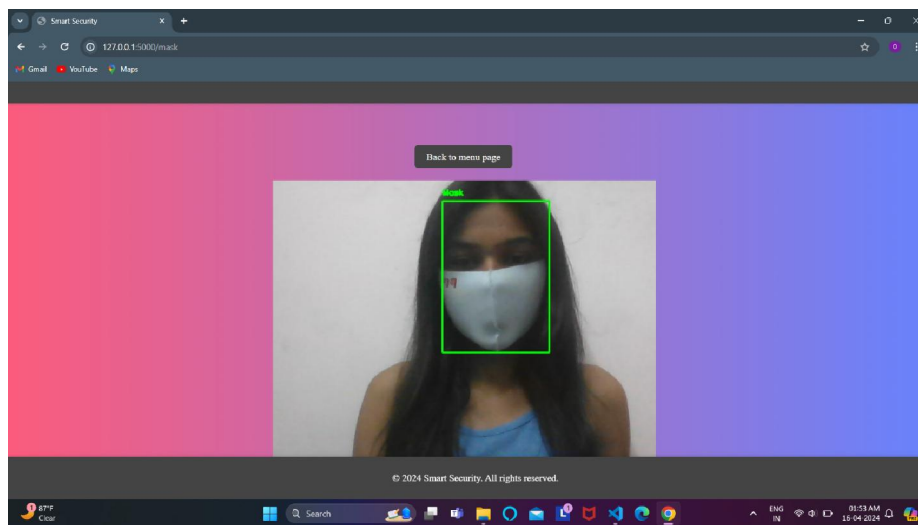
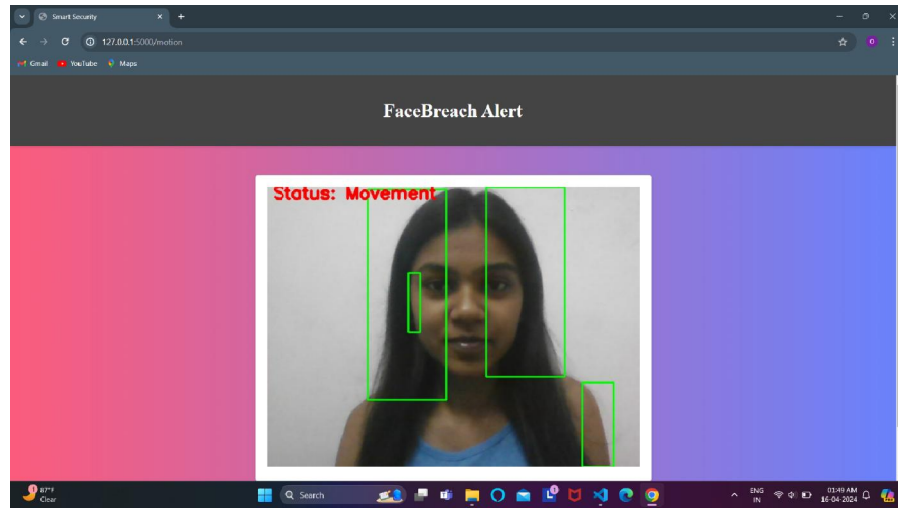
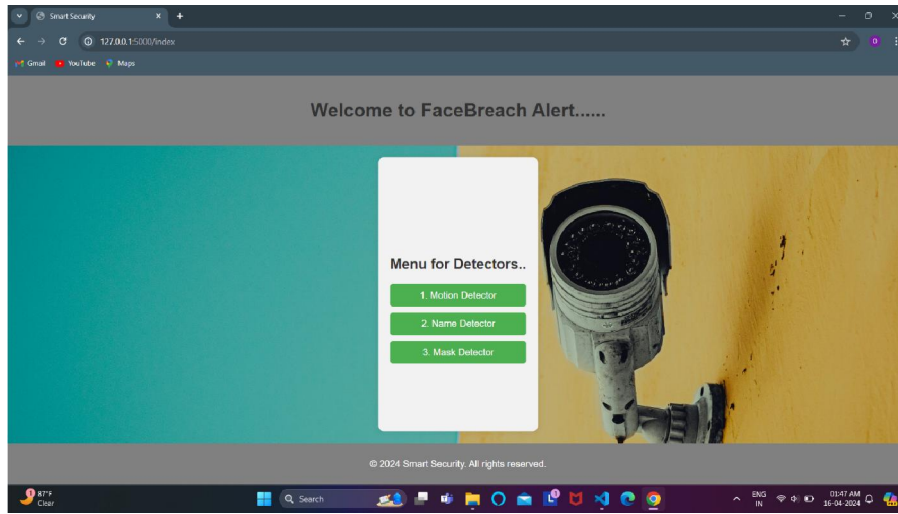


Fig. 4 Level 1 Data Flow Diagram

### V. RESULTS





#### V. CONCLUSION

We can use this application to recognize a person. Face detection improves surveillance efforts and helps track down criminals and terrorists. Personal security is also enhanced since there is nothing for hackers to steal or change such as passwords easy to integrate. Smart surveillance system significantly contributes to situation awareness. Such systems transform video surveillance from data acquisition tool to information and intelligence acquisition systems. Real-time video analysis provides smart surveillance systems with the ability to react in real time. Our system senses the intrusion and sends notifications to authorized persons so that action can be taken in response to the intrusion. This web app can be live hosted on a server, a user interface can be made more user-friendly and more professional-looking, can add more useful features for making it commercially viable.

#### REFERENCES

- [1] Real-Time Face Mask Detection using OpenCV and DeepLearning, Department of ECE, KoneruLakshmaiah Education Foundation, Andhra Pradesh, India.
- [2] An Intelligent Motion Detection Using OpenCV. International Journal of Scientific Research in Science, Engineering and Technology Print ISSN: 2395-1990
- [3] Y. You, S. Gong, C. Liu, "Adaptive moving object detection algorithm based on back ground subtraction and motion estimation", Int. J. Advancements in Computing Technology, vol. 5, no. 6, pp. 357-363, 2013 Conference, WWW2019,2019.
- [4] M. Murshed, A. Ramirez, O. Chae, "Statistical Background Modeling: An Edge Segment Based Moving Object Detection Approach", Proc. of IEEE International Conf. on Advanced Video and Signal Based Surveillance, pp. 300-305, 2010
- [5] Geethapriya. S, N. Duraimurugan, S.P. Chokkalingam, "Real-Time Object Detection with Yolo", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249– 8958, Volume-8, Issue-3S, February 2019.
- [6] Marengoni and Stringhini. High Level Computer Vision using OpenCV. 2011. Universidade Presbiteriana Mackenzie.
- [7] Design a face recognition system, The 15th International Conference on Machine Design and Production June 19 – 22, 2012, Pamukkale, Denizli, Turkey.