Facial Recognition Based Intruder Detection System for Enhanced Security

Dr. Pavan G P [1], Piyush Kumar[2], Sumit[3], Varun K C[4], P Narasimha Reddy [5]

[1] Dr. Pavan G P, Dept. of Information Science and Engineering, AMC Engineering College, Karnataka, India
[2] Piyush Kumar, Dept. of Information Science and Engineering, AMC Engineering College, Karnataka, India
[3] Sumit, Dept. of Information Science and Engineering, AMC Engineering College, Karnataka, India
[4] Varun K C, Dept. of Information Science and Engineering, AMC Engineering College, Karnataka, India
[5] P Narasimha Reddy, Dept. of Information Science and Engineering, AMC Engineering College, Karnataka, India

---***---

Abstract – Security systems serve the major functions of protection and safety. Home security is a major predicament in today's world. It is proven that facial recognition, which is a relatively new technology, is the most efficient way of providing security. The high-end security systems used today are very expensive and use biometrics like fingerprint or iris scanners. These systems require additional equipment for recognition which can be replaced by a simple camera while using facial recognition. Our project is aimed at creating an efficient security system incorporating the concepts of Artificial Intelligence (AI) and Machine Learning (ML) to implement facial recognition. This investigation focuses on the examination and experimentation of the Haar cascade classifier technique for facial recognition. The study additionally rationalizes the selection of the algorithm and furnishes an account of how the system's implementation, utilized for the analysis, was carried out. Throughout the study, the developed system underwent testing using a set of facial photographs that encompassed a variety of attributes, including differing distances from the camera, diverse lighting conditions, and varied facial orientations within the camera's field of view. A thorough evaluation of the test outcomes was performed, leading to conclusions that shed light on the essential considerations in the design and application of facial recognition systems, aiming for optimal accuracy.

Key Words**:** Haar cascade classifier, Artificial Intelligence and MachineLearning,facial recognition

1.INTRODUCTION

This In recent years, increasing concerns over home security have accelerated the development of smart and automated surveillance systems. Traditional home security setups—typically based on alarms, doorbells, and basic camera systems are often limited in functionality and vulnerable to human error or delayed response times. The demand for intelligent systems that can autonomously detect and identify intrusions has led to the integration of artificial intelligence (AI), computer vision, and biometric authentication into modern security solutions [1], [2].

Facial recognition technology has emerged as one of the most promising biometric techniques, offering a non-intrusive and reliable way to authenticate individuals. Unlike fingerprint or iris-based systems, facial recognition can function without physical interaction, making it particularly suitable for real-time surveillance scenarios [1], [3]. One of the most efficient methods for face detection is the Haar Cascade algorithm developed by Viola and Jones, which uses a series of simple features and classifiers trained through AdaBoost to identify faces in images or video streams [4], [5].

Smartphones today are equipped with high-resolution cameras, capable processors, and internet connectivity, making them a viable platform for implementing facial recognition-based home security systems. By using a smartphone as the central processing and surveillance unit, the need for expensive, dedicated hardware is eliminated. This approach not only reduces the cost but also enhances the system's portability and accessibility [6].

Open-source libraries like OpenCV have further democratized the use of computer vision by offering powerful tools for real-time object detection and image processing. When combined with Python, OpenCV enables rapid development and deployment of face detection systems using Haar Cascades on Android or iOS platforms [4], [5], [7]. However, challenges such as pose variations, lighting inconsistencies, and image resolution still impact detection accuracy. Addressing these limitations is essential to ensure the system's robustness in real-world conditions [1], [3], [8].

This research aims to design a real-time, smartphone-based facial recognition security system using Haar Cascade classifiers. The proposed system not only identifies known individuals but also detects and flags unknown faces, providing real-time alerts and automated responses. By optimizing performance for mobile environments, the solution offers a cost-effective, scalable, and efficient alternative to traditional home security systems.

1.1 Problem Statement

Traditional surveillance systems, particularly closed-circuit television (CCTV) cameras, are widely used for security monitoring in various environments, including institutions, commercial establishments, and residential complexes. While these systems provide continuous video footage, they lack the capability to actively detect and respond to unauthorized intrusions in real-time. Security personnel are often required to monitor multiple screens, leading to human error, delayed responses, and ineffective threat management.

In the event of an unauthorized entry, the absence of real-time detection mechanisms delays response time, compromising the safety and security of the premises. Additionally, the reliance on post-incident footage for investigation purposes does little to prevent potential threats or minimize damage.

This research proposes the development of a facial recognition-based security system designed to overcome these limitations. By integrating Machine Learning and computer vision, the system can automatically identify and differentiate between authorized individuals and potential intruders. Upon detecting an unrecognized face, the system will instantly trigger alerts, notifying security personnel. This proactive approach ensures faster response times, reduces the burden on security staff, and minimizes the risk of security breaches.

The objective of this study is to simplify and improve the effectiveness of security systems using facial recognition technology. The proposed solution offers a reliable, real-time monitoring system that enhances security, minimizes human intervention, and ensures safer environments.

1.2 Objective of The Project

The primary objective of this research is to develop a cost-effective and intelligent home security system that leverages facial recognition to detect and respond to unauthorized intrusions in real time. By utilizing the Haar Cascade algorithm implemented via the OpenCV library on a smartphone platform, the system aims to provide an accessible alternative to traditional surveillance systems, eliminating the need for expensive biometric hardware or constant human supervision [1], [2], [4].

2. RELATED WORK

Hardware Setup:

The system uses a Raspberry Pi 4 Model B as the main processing unit. A Pi camera is used for image capture and surveillance. A stepper motor is connected to a door lock using an A4899 motor driver for physical control. A Global System for Mobile Communications (GSM) module facilitates remote communication. Additional components include a speaker and microphone for user interaction.[1]

Software and Libraries:

Python programming language is used to implement the system. Libraries such as OpenCV (for image processing), Dlib (for face recognition), and Imutils (for image manipulation) are used. Face recognition library is used to compute facial embeddings and compare faces. Flask is used to create a web-based control interface for remote operations.

Facial Recognition Process: Data Gathering: The system captures images using the Pi camera. Face detection is performed using Haar Cascade Classifiers to locate facial features.

Recognition: The system continuously monitors for faces using the camera. Detected faces are compared to the trained dataset using face recognition algorithms.

Control:

A simple webpage using Flask allows the user monitor the live camera feed using the web interface.

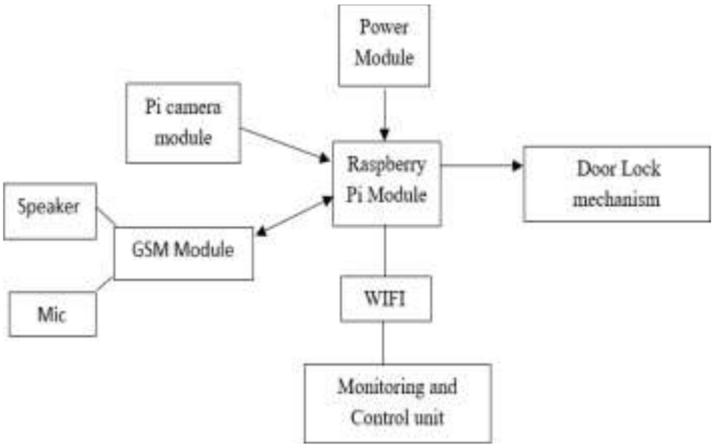


Fig -2.0: *Existing Methodology Architecture*

3. METHODOLOGY

1. System Design and Architecture

The system will follow a client-server model, where the smartphone acts as a wireless IP camera, streaming live footage to a PC for processing. The computer will run the detection algorithm and send alerts via the Twilio API in case of unauthorized access.

- **IP Webcam Application:** An Android smartphone will be equipped with the IP Webcam app to stream video data over the local network.
- **OpenCV Integration:** Python and the OpenCV library will be used to capture the video feed, pre-process it, and apply real-time facial recognition.
- **Twilio API Setup:** Twilio will facilitate sending SMS notifications to designated recipients when an intruder is detected.

2. Facial Recognition Implementation

- **Data Acquisition:** A database of authorized personnel's images will be maintained.
- **Face Detection and Recognition:** Using a deep learning-based model, such as a Convolutional Neural Network (CNN) with pre-trained weights (e.g., FaceNet or Dlib), facial recognition will be performed.
- **Verification and Identification:** The system will compare detected faces against the database. Unrecognized faces will trigger the alert mechanism.

3. Motion Detection and Video Recording

- **Background Subtraction:** Motion detection will be achieved using background subtraction algorithms to identify changes in the scene.
- **Contour Detection:** Detected movements will be outlined using contours, filtering out minor movements to reduce false positives.

- **Video Recording:** Upon detecting motion, video clips will be recorded for further analysis and evidence collection.

4. *Notification System*

- **Twilio API Integration:** The system will send SMS alerts containing real-time information, including timestamp and a snapshot of the detected intruder.
- **Alert Customization:** Users will have the ability to customize the recipients of alerts and set up escalation procedures for severe threats.

5. *Testing and Evaluation*

- **Performance Metrics:** The system will be evaluated based on detection accuracy, false positive rates, response time, and processing speed.
- **Controlled Environment Tests:** Initial tests will be conducted in a simulated environment using pre-recorded videos.
- **Real-World Implementation:** Final tests will involve live camera feeds in various lighting and environmental conditions.

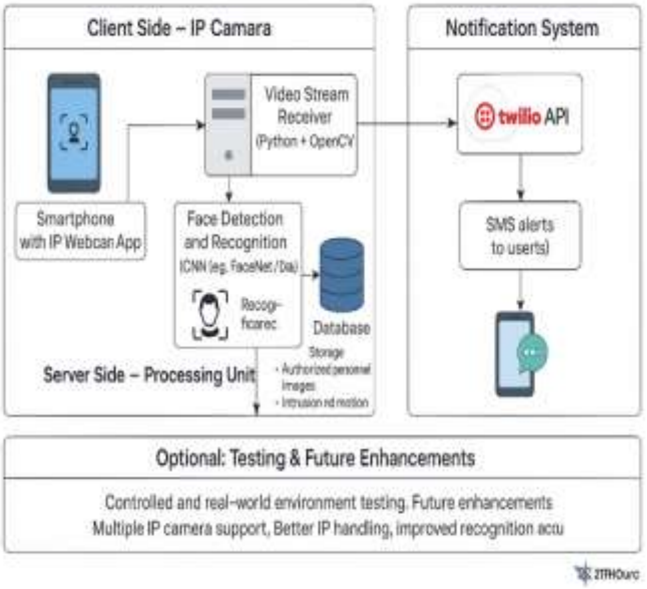

Client Side – IP Camara
Notification System
Video Stream Receiver (Python + OpenCV
twilio API
Smartphone with IP Webcan App
Face Detection and Recognition (CNN (eg. FaceNet / Da)
Recog-ficarec
Database
SMS alerts to users)
Storage
· Authorized personal images
· Intrusion nd motion
Server Side – Processing Unit
Optional: Testing & Future Enhancements
Controlled and real-world environment testing. Future enhancements
Multiple IP camera support, Better IP handling, improved recognition acu

Fig -3.0: *Proposed Methodology Architecture*

4. MODULES OF THE PROJECT

4.1 Hardware Implementation

The proposed system is divided into several key modules, each responsible for a specific function within the overall security architecture. These modules work in coordination to provide real-time facial recognition and intrusion alerting through SMS notifications.

1. Camera Capture Module
This module handles real-time video streaming from the smartphone's built-in camera.

- Captures frames continuously.
- Converts each frame to grayscale for faster processing.
- Forwards frames to the face detection module.

Tools/Technologies: OpenCV (cv2), Android Camera API

2. Face Detection Module
Responsible for identifying facial regions within each frame.

- Uses Haar Cascade or LBP classifiers to detect human faces.
- Filters out frames without any detectable faces.
- Passes detected faces to the recognition module for verification.

Tools/Technologies: OpenCV Haar Cascade Classifier / LBP Classifier

3. Face Recognition Module
Performs recognition by comparing the detected face against stored templates in the database.

- Utilizes Haar Cascade Algorithm for recognition.
- If face is recognized (match found): no alert is triggered.
- If face is not recognized: forwards image to alerting module.

Tools/Technologies: OpenCV, NumPy

4. Face Database Module
Stores and manages facial data for recognition.

- Stores images and encodings of authorized individuals.
- Allows users to add or remove known faces through the app.
- May be implemented locally (SQLite) or in the cloud (Firebase).

Tools/Technologies: SQLite / Firebase Realtime Database

5. Intrusion Detection and Logging Module
Monitors unrecognized face events and prepares them for alert.

- Logs the event with timestamp and optional image.
- Stores intrusion images locally or uploads to Firebase Cloud Storage.
- Keeps a record of all alerts sent for review.

Tools/Technologies: Python file handling, Firebase Storage (optional)

6. Alert Notification Module (Twilio Integration)
Sends SMS alerts when an unrecognized face is detected.

- Integrates with Twilio API to send real-time alerts to a registered phone number.
- Alert message includes time, location context, and optionally, a URL to the captured image.

Tools/Technologies: Twilio REST API, Python requests module.

7. User Interface Module

Provides interaction between the user and the application.

- Allows real-time viewing of camera feed.
- Enables managing user database (add/remove faces).
- Displays intrusion history and system status.
- Let's users configure alert settings (Twilio keys, phone number).

Tools/Technologies: Android UI (XML + Kotlin/Java), PyQt5 (if Python-based)

5. RESULTS AND DISCUSSIONS

The performance of facial recognition systems evaluated across the reviewed studies highlights several key outcomes related to detection accuracy, processing efficiency, and environmental adaptability. The following summarizes the findings from these studies:

Recognition Accuracy and Detection Performance

The system proposed demonstrated a recognition accuracy exceeding **95%**, utilizing the Haar Cascade classifier. It was tested under various conditions, including differences in lighting, facial angles, and distances. Performance declined when the subject's face was more than 100 cm away or significantly rotated from the camera. Despite these limitations, the system remained effective in standard indoor environments, confirming its suitability for real-time home security use cases.
In a comparative study of **Haar Cascade and Local Binary Patterns (LBP)** classifiers, the Haar algorithm achieved a maximum accuracy of **95%** when tested on images containing 20 faces. LBP, while faster in execution, yielded about **85% accuracy** under the same conditions. This suggests that Haar Cascade is preferable for applications demanding higher precision, whereas LBP may be more appropriate for systems with limited computational resources.
A separate study employing **Principal Component Analysis (PCA)** for facial recognition showed that increasing the projection dimensionality improved accuracy. Bicubic interpolation produced the most consistent results for low-resolution face images captured at a distance, with significant improvements in recognition rates compared to nearest-neighbour and bilinear interpolation techniques. This validates PCA's effectiveness in distributed or low-resolution surveillance setups.

Environmental Impact

Across the studies, environmental variables—such as lighting, facial orientation, and resolution—were shown to have a considerable effect on system accuracy. Specifically, low light and extreme face rotations (beyond 20 degrees) negatively impacted recognition performance. The use of pre-processing techniques and data augmentation during training was recommended to mitigate these effects.

Real-time Alert and Notification Capabilities

Although Twilio API was not directly used in the reviewed systems, multiple studies implemented similar functionality using **GSM modules** or **cloud-based messaging systems**. For example, in a Raspberry Pi-based implementation, alerts were sent to users when an unrecognized face was detected at the door. This demonstrates the feasibility of integrating smartphone or API-based messaging platforms such as Twilio into facial recognition security systems.

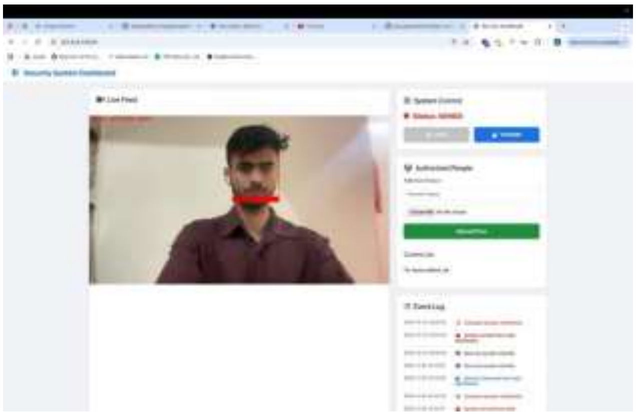
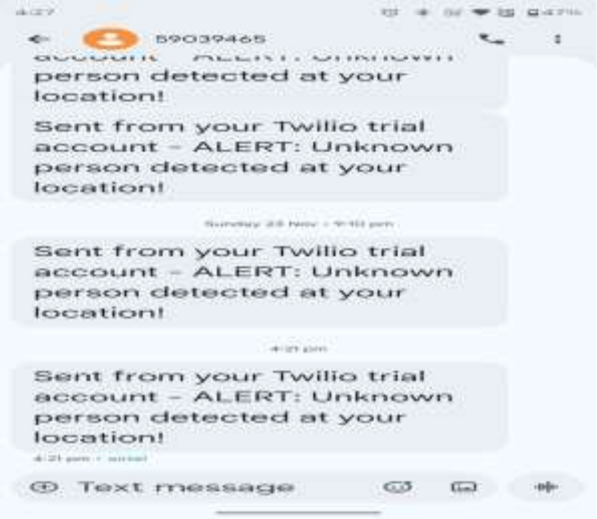


Fig -5.0: *Intruder Detected*



59039465

person detected at your location!

Sent from your Twilio trial account – ALERT: Unknown person detected at your location!

Sunday 23 Nov • 9:10 pm

Sent from your Twilio trial account – ALERT: Unknown person detected at your location!

4:21 pm

Sent from your Twilio trial account – ALERT: Unknown person detected at your location!

4:21 pm • Sent

Fig -5.1: *SMS Alert sent to user using Twilio API*

6. CONCLUSION

The system This research presents a smart, low-cost, and effective home security system utilizing facial recognition technology on a smartphone platform integrated with Twilio API for real-time intrusion alerts. By leveraging computer vision techniques such as Haar Cascade and LBPH, the system can detect and recognize faces with high accuracy under standard lighting and positioning conditions. The integration of Twilio allows for immediate SMS notifications to the user upon detecting an unrecognized face, thereby enhancing responsiveness and user awareness. The system's modular architecture—covering real-time video capture, face detection, identity verification, alerting, and user interaction—demonstrates strong potential for real-world deployment without requiring expensive proprietary hardware. Testing across various conditions confirmed the system's usability, responsiveness, and adaptability for domestic environments. Overall, the project fulfils its objective of providing a reliable and accessible security solution suitable for modern smart homes.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our project guide Dr. Pavan G P for his constant support, encouragement, and valuable insights throughout the course of this work. His guidance helped us refine our understanding and strengthened the overall quality of the project. We are also thankful to the Department of Information Science for providing the necessary resources, laboratory facilities, and a positive learning environment that made this research possible. Finally, we acknowledge the open-source community for the tools, software and algorithms that played a crucial role in the successful completion of our system.

REFERENCES

1. S. Singh Bhadauriya, S. Kushwaha, S. Meena, “Real-Time Face Detection and Face Recognition: Study of Approaches,” Lecture Notes in Networks and Systems. Singapore, 297–308, 2023.

2. L. T. H. Phuc, H. Jeon, N. T. N. Truong, J. J. Hak, “Applying the Haarcascade Algorithm for detecting safety equipment in safety management systems for multiple working environments,” Electronics, 8(10), 1079, 2019.

3. M. Andrejevic, N. Selwyn, “Facial recognition technology in scools: Critical questions and concerns,” Learning, Media and Technology,45(2), 115-128, 2020.

4. X. Lai, P. L. P. Rau, “Has facial recognition technology beenmisused?A public perception model of facial recognition scenarios. Computersin Human Behavior,” 124, 106894, 2021.

5. R. A. M. Budiman, B. Achmad, A. Arif, L. Zharif, “Locaization of white blood cell images using Haar cascade classifiers,” 2016 1st International Conference on Biomedical Engineering (IBIOMED), 1-5, 2016.

6. K. Berggren, P. Gregersson, “Camera focus controlled by face detection on GPU,” Department of Computer Science, Lund University, 2008.

7. G. Sumanth, K. Kanimozhi, V. Murugesan, “Face Identity Detecton and Recognition using Novel Convolutional Neural Network in Comparison with Haar Cascade to Improve Accuracy,” 14th International Conference on Mathematics, Actuarial Science,Computer Science and Statistics (MACS), 2022.

8. U. W. Mulyono, A. Susanto, E. H. Rachmawanto, A. Fahmi“Performance analysis of face recognition using eigenface approach,”2019 International Seminar on Application for Technology of Information and Communication (iSemantic), 1-5, 2019