Face Recognition Alert System

N Sudha Laxmaiah, G. Neha Latha, J. Meghana sri

[1]Assistant professor, Department of CSE, Bhoj Reddy Engineering College for Women, India

[2,3]B.Tech Students, Department of CSE, Bhoj Reddy Engineering College for Women, India

ABSTRACT

The Face Recognition Alert System is an advanced security solution that leverages cutting-edge machine learning and computer vision techniques to identify individuals based on their facial features. Designed to enhance security and streamline access control, the system automates the recognition process, dynamically granting or restricting access based on facial match outcomes. Unauthorized access attempts trigger multi-layered responses, including real-time email and SMS alerts with visual evidence, as well as audible notifications for immediate attention. By integrating widely used libraries like OpenCV and Twilio API, this system ensures scalability, usability, and robust functionality. It overcomes the limitations of traditional security methods by providing real-time detection, minimizing human error, and enhancing response times, making it ideal for applications demanding high security and operational efficiency.

1-INTRODUCTION

Face recognition technology has emerged as a powerful tool in modern-day security and authentication systems. This system leverages advanced machine learning algorithms and computer vision techniques to identify or verify an individual's identity based on their facial features. The application of face recognition spans a wide array of domains, from personal security to public safety, owing to its ability to provide contactless and efficient solutions for identity verification. The following implementation demonstrates the use of face recognition technology to detect, recognize, and respond to the presence of authorized and unauthorized individuals.

One of the highlights of this system is its capability to respond dynamically based on the recognition outcome. When an individual whose facial features match the stored encodings is detected, the system triggers specific actions such as granting access or displaying a welcome message. Conversely, if an unrecognized face is detected, the system records the image of the individual and initiates alert mechanisms. This includes sending an email with the unauthorized individual's photo as an attachment, sending a real-time SMS notification to alert the relevant stakeholders, and playing an audible alert to signify the breach. These multi-layered responses ensure that the system effectively handles unauthorized access while maintaining robust security.

The implementation also emphasizes usability and practicality. By utilizing widely available libraries such as opencv, face_recognition, and smtplib, the system is designed to be both scalable and user-friendly. The email alert system ensures prompt communication in case of a security breach, attaching visual evidence of the unauthorized individual to provide a clear context. The integration of the Twilio API enables the system to send SMS notifications, ensuring that alerts reach the intended recipient immediately. The use of sound playback as an auditory alert adds an extra layer of real-time notification, making the system suitable for various environments where immediate attention is required.

Overall, the face recognition system described in this implementation serves as a comprehensive solution for monitoring and responding to the presence of individuals in a given area. Its ability to handle real-time detection, recognition, and alert generation makes it an ideal tool for applications that demand high security and efficiency. The code not only highlights the technical intricacies of face recognition but also demonstrates the integration of multiple functionalities to create a robust, practical, and reliable system for identity verification and monitoring.

2.REQUIREMENT ANALYSIS

Functional Requirements:

Face Detection: This module is responsible for finding a human face in the captured image or video frame. It uses modules to identify facial features like eyes, nose, and mouth within the image

➢ **Face Recognition:** This module takes the detected face from the first stage and compares it to a stored database of authorized faces. It uses advanced features to match the unique characteristics of the face against the stored templates.

➢ **Verification:** If there is a match with a sufficient confidence level, the system grants access.If

Software Architecture

there is no match, the system will send an email and SMS to the Authorised person.

Non-Functional Requirements:

➢ **Performance**: The system should allow access within 2 seconds of recognizing an authorized face.

➢ **Reliability**: The face recognition alert system should have an uptime of at least 99.9%, ensuring it is operational and accessible almost all the time

➢ **Security**: The system should maintain logs of all access attempts, including successful and failed authentication attempts, for audit and security purposes.

3-DESIGN

Architecture

Project architecture represents number of components we are using as a part of our project and the flow of request processing i.e., what components in procession the request and in which order. An architecture description is a formal description and representation of a system organized in a way that supports reasoning about the structure of the system. Architecture is of 2 types. They are

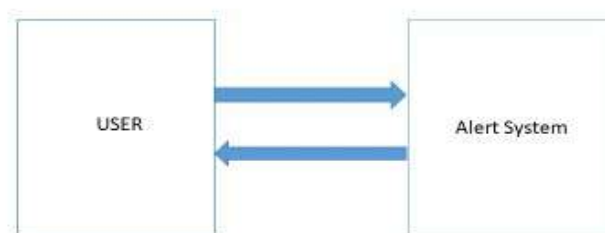1. Software architecture
2. Technical architecture

Fig 1 Software Architecture

The architecture of the system describes its major components, their relationships, and how they interact with each other. Software architecture and

design includes several contributory factors such as business strategy, quality attributes, human dynamics, design and IT environment. Software

Architecture typically refers to the bigger structures of a software system, and it deals with how multiple software processes cooperate to carry out their tasks.

Software design refers to the smaller structures and it deals with the internal design of a single software process.
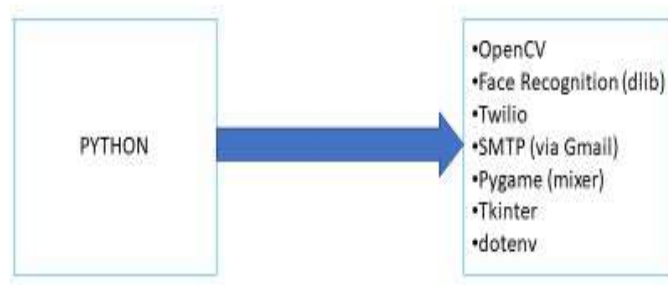
Technical Architecture

Fig 3.2 Technical Architecture

The technical architecture defines the technologies that are used to implement and support a business intelligence solution that fulfils the information and

.

data architecture requirements. These technologies cover the entire BI life cycle of design, development, maintenance, performing tuning, and user support
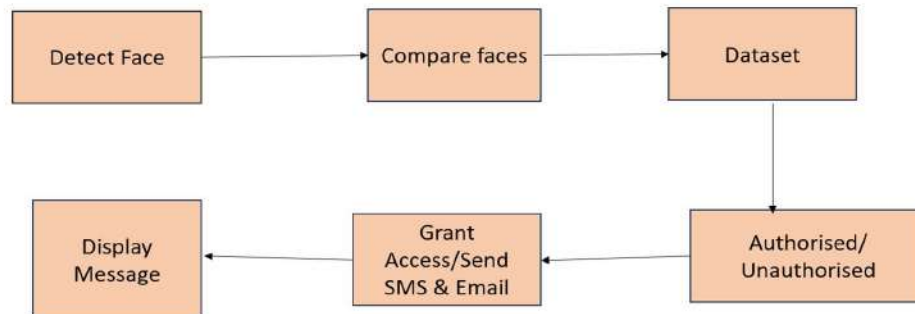
System Architecture

Fig 3.3 System Architecture

The system architecture for Facial Recognition Alert System. It begins with the "Detect Face" module, where a face is captured through a camera or sensor. The detected face is then processed by the "Compare Faces" module, where it is compared with faces stored in the "Dataset." The dataset contains the

facial features of authorized individuals. Based on the comparison results, the system determines whether the detected individual is "Authorized" or "Unauthorized."

If the individual is authorized, the system proceeds to the "Grant Access/Send SMS & Email" module,

granting access and sending notification alerts (such as SMS or email) to the concerned parties for tracking purposes. If the individual is unauthorized, the system prevents access and can optionally send alerts for security purposes. The "Display Message" module informs the user of the decision, showing whether access is granted or denied. This architecture ensures a streamlined and secure facial recognition process for access management.

4-IMPLEMENTATION

Python

Python is a high-level, general-purpose programming language known for its simplicity, readability, and versatility. Designed with a focus on developer productivity, it supports multiple programming paradigms, including procedural, object-oriented, and functional programming. Python's extensive standard library and numerous third-party packages make it ideal for diverse applications such as web development, data science, machine learning, automation, and more.

Face Recognition

This technology extracts facial encodings, which are numerical representations of unique facial features. By comparing these encodings with a pre-saved database of known faces, the program identifies individuals. It uses efficient algorithms to locate faces in live video feeds, match them against known data, and flag unknown persons for further action.

OpenCV (Computer Vision)

OpenCV is utilized for video processing, image handling, and drawing operations. It captures real-time video frames from the webcam, processes them for face detection, and highlights detected faces by drawing rectangles around them. The library is also responsible for resizing frames, converting them to RGB format for compatibility with

face_recognition, and saving images of unauthorized persons for alert purposes.

5-TESTING

Dimensions of Testing

There are many different dimensions to consider:

- Layers of the application (database)
- Scale of testing (unit, module, integration, scenario)
- Type of testing (functional, performance, security, etc.)
- Methodology (exploratory, scripted manual, automated)

Unit Testing

During this first round of testing, the program is submitted to assessments that focus on specific units or components of the software to determine whether each one is fully functional. The main aim of this endeavor is to determine whether the application functions as designed. In this phase, a unit can refer to a function, individual program or even a procedure, and White box testing method is usually used to get the job done. One of the biggest benefits of this testing phase is that it can be run every time a piece of code is changed, allowing issues to be resolved as quickly as possible.

Integration Testing

Integration testing allows individuals the opportunity to combine all of the units within a program and test them as a group. This testing level is designed to find interface defects between the modules/functions. This is particularly beneficial because it determines how efficiently the units are running together. Keep in mind that no matter how efficiently each unit is running, if they properly integrated, it will affect the functionality of the software program.

System Testing

System testing is the first level in which the complete application is tested as a whole. The goal at this level is to evaluate whether the system has complied with all of the outlined requirements and to see that it meets Quality Standards. System testing is undertaken by independent testers who haven't played a role in developing the program. This testing is performed in an environment that closely mirrors production. System Testing is very important because it verifies that the application meets the technical, functional, and business requirements that were set by the customer.

Acceptance Testing

The final level, Acceptance testing (or User Acceptance Testing), is conducted to determine whether the system is ready for release. During the Software development life cycle, requirements changes can sometimes be misinterpreted in a fashion that does not meet the intended needs of the users.
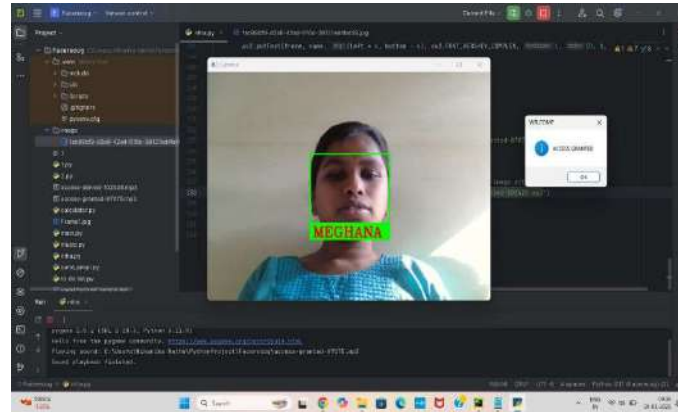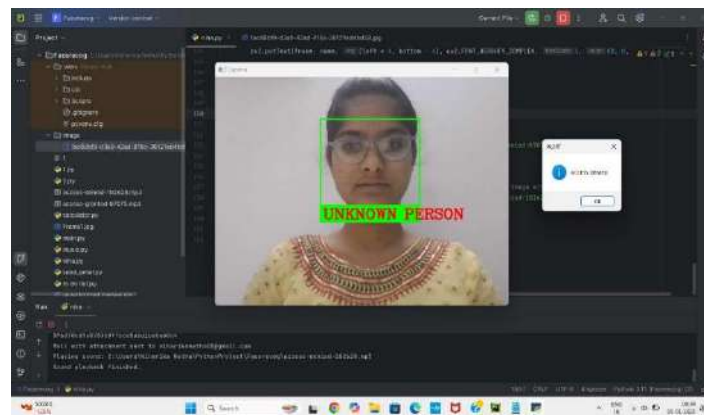
6.SCREENSHOTS
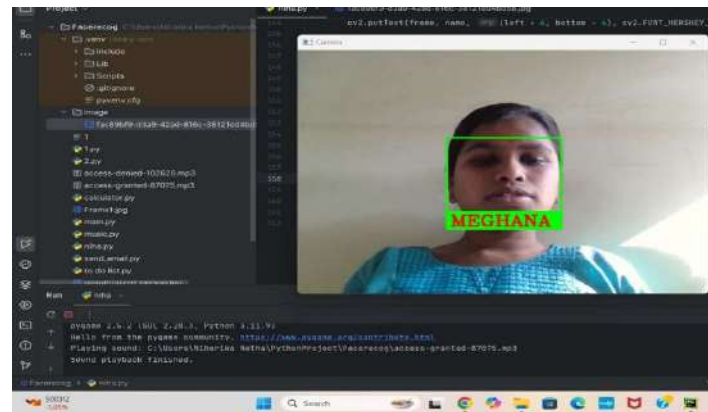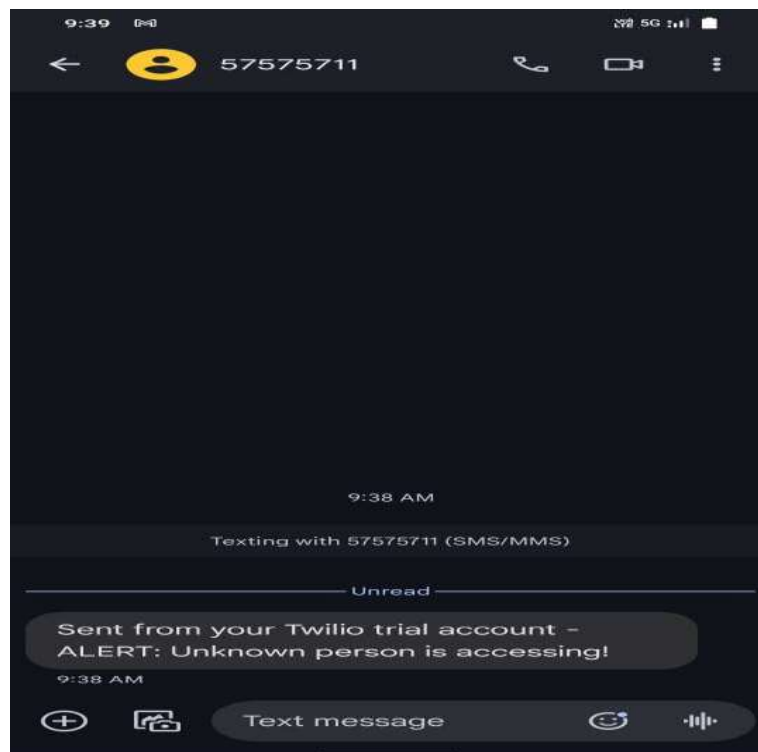

Screenshot 6.1 Input for Authorised User
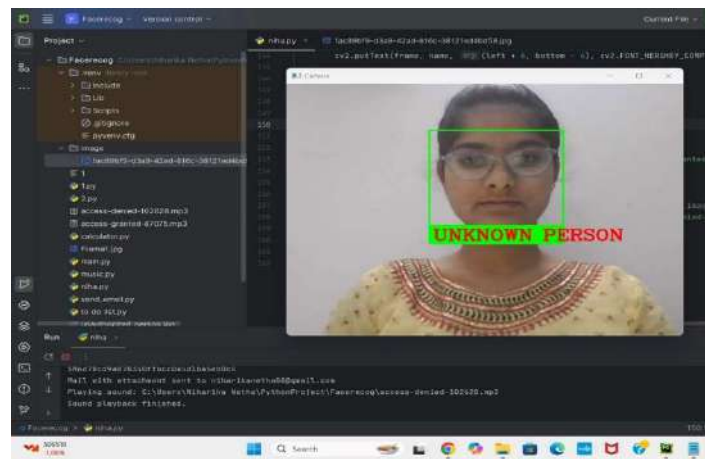
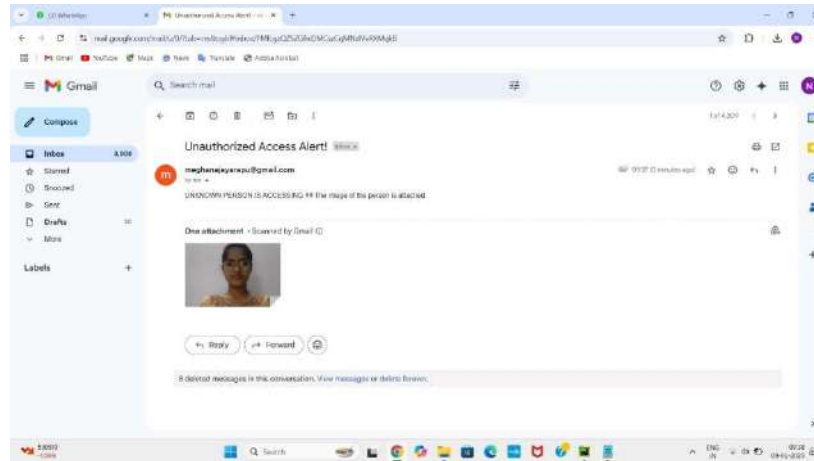Screenshot 6.2 Input for Unauthorised User

Screenshot 6.3 Figure showing output for authorized user

Screenshot 6.4 Figure showing output for unauthorized user

Screenshot 6.5 Figure showing Alert Message Via SMS

Screenshot 6.6 Figure showing Alert Message Via EMAIL with Image Attachment

7.   Conclusion and Future Scope

Conclusion

The implementation of a face recognition alert system marks a significant advancement in security and user convenience, leveraging cutting-edge facial recognition technology to ensure a highly secure and efficient experience. By accurately identifying and verifying individuals in real time, the system enhances safety by restricting unauthorized access and promptly alerting users in case of security breaches. Its integration with features like real-time notifications, audio alerts, and automated actions further elevates its utility, offering a seamless blend of security and technological sophistication. This innovation not only mitigates potential risks but also redefines the way security is managed in modern applications.

Future Scope

The future scope of a face recognition alert system is vast and promising, driven by advancements in artificial intelligence, machine learning, and sensor technology. Key areas for growth include enhanced accuracy and speed in facial recognition under varying conditions, such as low light or crowded environments, through the integration of advanced neural networks. The system could evolve to include emotion recognition and behavioral analysis, providing deeper insights into potential threats or unusual activity. Its application can be extended to industries like smart homes, banking, healthcare, and public safety, offering personalized experiences and heightened security. Additionally, future developments may focus on decentralization and edge computing to ensure privacy and reduce reliance on cloud-based systems. Integration with IoT devices and blockchain technology can further secure data and improve interoperability. As the technology matures, it holds the potential to become a cornerstone of next-generation security and automation solutions.

8.References

[1]   F. Javed Mehedi Shamrat, A. Majumder, P. R. Antu, S. K. Bannon, I. Nowrin and R. Ranjan, "Human face recognition in vedios" in Pervasive Computing and Social Networking, Springer, pp. 143-157, 2022.

[2]   D. Salama AbdELminaam, A. M. Almansori, M. Taha and E. Badr, "A deep facial recognition system using computational intelligent algorithms", Pios one, vol. 15, no.12pp.e0242269,2022.

[3]   D. Rathore, G. K. Das and A. Saxena, "Concept of face recognition: a review", International Journal For Technological Research In Engineering, 2021.