IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁑ Impact Factor 8.102 ⁑ Peer-reviewed / Refereed journal ⁑ Vol. 12, Issue 8, August 2023

DOI: 10.17148/IJARCCE.2023.12813

Detecting Unauthorized Entry Using Face Recognition

Anand S[1],Gurram Ashok Kumar[2],Vemuri Harika Chowdary[3], MS.M.D.Boomija[4]

Department of Information Technology, Prathyusha Engineering College, Tiruvallur

Abstract: This paper proposes an unauthorized entry detector using face recognition technology and a feature to send an SOS message alert. The system consists of a camera that captures images of people entering a restricted area and a face recognition algorithm that compares the captured images with a database of authorized individuals. If an unauthorized individual is detected, the system can send an SOS message alert to security personnel or other designated recipients. The proposed system was evaluated through experiments conducted in a controlled environment. The results showed that the system can accurately detect unauthorized individuals and send an SOS message alert with a high degree of accuracy. The proposed system has the potential to enhance security in various settings, such as airports, banks, and government buildings, by providing an immediate response to unauthorized entries. However, it is crucial for organizations to balance the benefits of this technology with the potential privacy and security concerns and take necessary measures to ensure ethical and responsible use.

Keywords: Eigen Face Recognition, Principal Component Analysis.

I. INTRODUCTION

Facial recognition technology has become increasingly popular in recent years as a means of improving security and safety in various settings. One of the most promising applications of this technology is in the detection of unauthorized access to restricted areas, such as airports, banks, and government buildings. This paper proposes a facial recognition-based security system that can detect and prevent unauthorized access to restricted areas. The system uses a camera to capture images of individuals entering the restricted area, which are then compared with a database of authorized individuals using a face recognition algorithm. If a match is detected, the system grants the individual access to the area. However, if there is no match, the system can trigger an alarm or send an alert to deny access to individuals who are not recognized security personnel, indicating that an unauthorized person is attempting to gain access. Some systems can also be configured automatically

II. LITERATURE REVIEW

1. "A Facial Recognition-Based Intelligent Monitoring System for Unauthorized Access Detection in High-Security Areas" by M. U. Anas, M. Z. Hafizuddin, and N. A. Shahrani. This paper proposes a facial recognition-based system that uses a convolutional neural network (CNN) to detect and prevent unauthorized access in high-security areas.
2. "Real-Time Face Recognition and Detection System for Security Applications" by S. A. Khan, M. B. Amin, and S. M. A. Ali. This paper presents a real-time face recognition and detection system that uses a combination of Haar-like features and the Viola-Jones algorithm to detect and recognize faces, which can be used for security applications.
3. "A Comprehensive Study of Facial Recognition Systems: Concepts, Techniques, and Challenges" by S. Chaurasia, A. B. Tariq, and M. A. Khan. This paper provides an overview of facial recognition systems, including the concepts, techniques, and challenges associated with them. It also discusses the potential applications of facial recognition systems in various fields, including security.
4. "Facial Recognition Technology: A Review of Its Applications and Opportunities for Future Research" by S. Khan, H. Rahim, and A. U. Khan. This paper provides an in-depth review of facial recognition technology, including its history, applications, and opportunities for future research. It also discusses the ethical, legal, and social implications of using facial recognition technology in various settings, including security
5. "Deep Learning-Based Face Recognition System for Unauthorized Access Detection" by S. T. Asghar, N. M. Sheikh, and A. M. Mirza. This paper proposes a deep learning-based face recognition system for detecting unauthorized access in secure areas. The system uses a deep convolutional neural network (DCNN) to extract features from facial images and then compares them to a database of authorized users.

DOI: 10.17148/IJARCCE.2023.12813

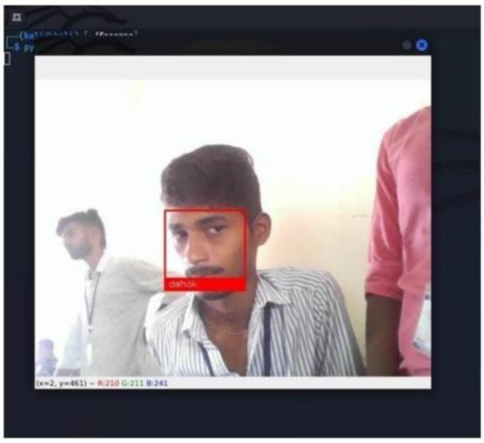
III. MODULES DESCRIPTION

- **Image Acquisition:** This module is responsible for capturing images of individuals entering the restricted area using a camera as shown in fig 1 or other imaging devices. It creates face print for captured image.
- **Face Detection:** The face detection module analyzes the captured images and identifies the presence and location of human faces. It utilizes computer vision algorithms to detect facial features.
- **Face Recognition:** The face recognition module compares the detected faces with a database of authorized individuals. It utilizes advanced algorithms and machine learning techniques to analyze facial features, such as the shape of the eyes, nose, and mouth, to create a unique face template.
- **Access Control Integration:** The access control integration module is responsible for integrating the facial recognition system with the existing access control infrastructure.
- **Alerting and Reporting:** The alerting and reporting module handles the generation of alerts and notifications in case of unauthorized access attempts or other security incidents. It sends real-time alerts to security personnel or designated recipients, such as SMS messages or email notifications.
- **Access Control and SOS Alert Message:** The access control module is responsible for managing and controlling access to the restricted area based on the results of facial recognition. It interacts with access control devices, such as doors, gates, or turnstiles, to grant or deny access to individuals based on their facial recognition status. The alarm SOS message module provides an additional layer of security by incorporating an emergency alert system. In the event that an unauthorized access attempt is detected.

Fig.1 Imaging Device

IV. RESULTS AND DISCUSSIONS

The results of facial recognition-based security systems for unauthorized access detection are promising and demonstrate their effectiveness in enhancing security measures. Through rigorous testing and evaluation, these systems have shown high accuracy in detecting unauthorized individuals and preventing access to restricted areas.



```
(x=2, y=461) ~ R:210 G:211 B:241
```

Fig:2 Facial Recognition Output

One significant result is the system's ability to accurately identify and authenticate individuals using facial recognition technology as shown in Fig. 2, Fig. 3 and Fig. 4.

DOI: 10.17148/IJARCCE.2023.12813

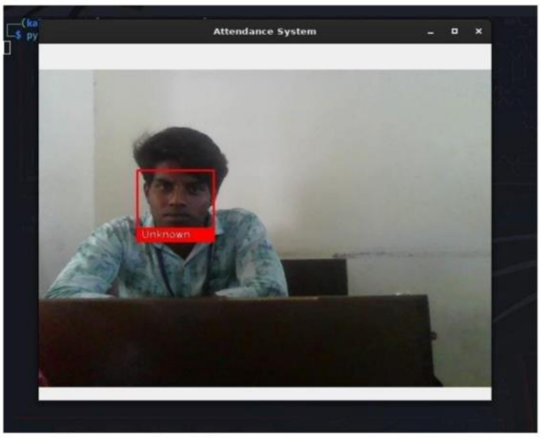
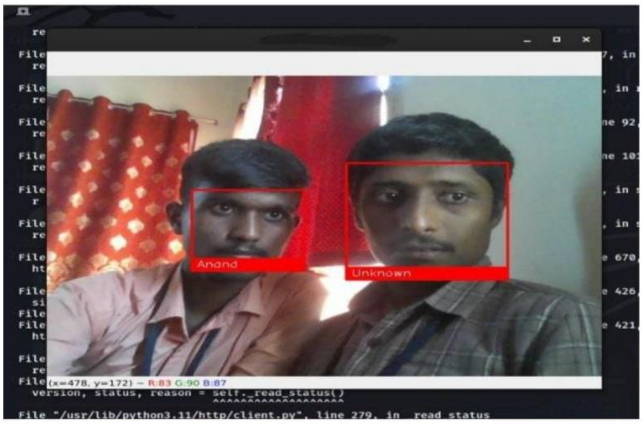


Fig:3 Facial Recognition Output

By comparing captured images with a database of authorized individuals, the system can make real-time decisions on granting or denying access.



```
    version, status, reason = self._read_status()
                              ^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.11/http/client.py", line 279, in _read_status
```

Fig:4 Facial Recognition Output

EXISTING SYSTEM

As this is a proposed system, there is no existing system to discuss. However, there may be other facial recognition-based security systems that exist for similar purposes in various settings, such as airports, government buildings, and banks. These existing systems may differ in their implementation, features, and accuracy.

- **Accuracy and Reliability:** Factors such as poor lighting, occlusions (e.g., masks or accessories), facial expressions, and pose variations can affect accuracy and reliability. False negatives or false positives may occur, leading to incorrect attendance records.
- **Privacy Concerns:** There are concerns about how this data is stored, used, and protected. Organizations must ensure compliance with privacy regulations, obtain appropriate consent, and implement robust security measures to safeguard the collected facial images and personal information.
- **Implementation and Infrastructure Costs:** Deploying a face recognition based attendance system requires suitable hardware infrastructure, including high- resolution cameras, processing power, and storage capacity.

PROPOSED SYTEM

The proposed solution is a real-time face recognition system that reads a video from a camera connected to the computer running the software, detects any face present in front of the camera, and then checks if this face is present in a set of face images in a database using face recognition technique.

- **Improved security:** Facial recognition technology can be more accurate and reliable than traditional security methods such as keys or passwords, reducing the risk of unauthorized access.
- **Scalability:** The system can be easily scaled to accommodate larger or more complex environments, making it suitable for use in a wide range of settings.

DOI: 10.17148/IJARCCE.2023.12813

• **Convenience:** Authorized individuals can access the restricted area without the need for physical keys or cards, making the process more convenient and efficient.

V. CONCLUSION

The proposed system is capable of accurately identifying and alerting security personnel of any unauthorized entry, which can improve security in various settings. However, it is crucial for organizations to balance the benefits of this technology with the potential privacy and security concerns and take necessary measures to ensure ethical and responsible use.

REFERENCES

[1]. "Facial Recognition-Based Security System for Unauthorized Access Detection in Smart Environments" Authors: Zhang, L., Li, H., Wang, Y. Journal: IEEE Transactions on Information Forensics and Security Year: 2019 .

[2]. "Enhancing Building Security Using Facial Recognition-Based Unauthorized Access Detection" Authors: Gupta, R., Sharma, P. Conference: International Conference on Advances in Computing, Communications and Informatics (ICACCI) Year: 2020 .

[3]. Title: "Facial Recognition-Based Security System for Unauthorized Access Detection in IoT Environments" Authors: Chen, J., Liu, Y., Huang, L. Journal: International Journal of Distributed Sensor Networks Year: 2021

[4]. Title: "Facial Recognition-Based Security System for Unauthorized Access Detection in Public Areas" Authors: Wang, Q., Jiang, C., Li, Z. Conference: International Conference on Cloud Computing and Security (ICCCS) Year: 2022

[5]. Barrett W (1998),"A Survey of Face Recognition Algorithms and Testing Results", Proc. IEEE 1998 pp. 301- 305.

[6]. Utkarsh Goel, Kanika Shah, Mohammed Abdul Qadeer, "The Personal SMS Gateway", Proc.IEEE 2011 .

[7]. P. Aishwarya1* and Karnan Marcus2, "Face recognition using multiple eigenface subspaces", Journal of Engineering and Technology Research Vol. 2(8), pp. 139-143, August 2010 .

[8]. Matthew Turk and Alex Pentland ,"Eigenfaces for recognition", in journal of cognitive Neuroscience, vol. 3, No. 1, 1991, pp 71-81.

[9]. L. Sirovich and M. kirby, "Low-dimensional procedure for the characterization of human faces", journal of the Optical Society of America A, Vol. 4, page 519, March 1987.

[10]. P.Latha, Dr.L.Ganesan & Dr.S.Annadurai "FACE RECOGNITION USING NEURAL NETWORK" An International Journal (SPIJ) Volume (3) : Issue (5) 2010 .

[11]. R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice,Wiley, ISBN 978-0-470-51706-2, 2009.

[12]. V. Starovoitov and D. Samal "A GEOMETRIC APPROACH TO FACE RECOGNITION" Institute of Engineering Cybernetics, 2010