

Development and Implementation of Face Recognition Technology in The Police Department

M.Amshavalli¹, S. Akashkumar², S. Abhinav³, S. Gokul⁴

¹Assistant Professor, Department of CSE, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India.

^{2,3,4}UG Scholar, Dept. of CSE, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India.

Emails: amshavalli1494@gmail.com¹, akash6379855@gmail.com², abhinavshanmugaraja@gmail.com³, sgokul8220@gmail.com⁴

Abstract

Facial recognition technology automates the process of identifying and verifying individuals using facial features. The proposed system captures live facial data through a camera, pre-processes it (resizing, grayscale, noise reduction), and extracts distinctive facial landmarks using OpenCV and deep learning models. These extracted features are matched against a secure, pre-registered database. If a match is identified, access is granted or an appropriate log is generated. In case of unregistered individuals or blacklisted entities, the system triggers an alert and captures a snapshot for security monitoring. This integration significantly enhances surveillance, access control, and crime prevention while maintaining privacy standards.

Keywords: Facial Recognition, AI, Machine Learning, OpenCV, Surveillance, Security System, Deep Learning, Pattern Recognition, Identity Verification.

1. Introduction

Security is a growing concern in the digital and physical world. Conventional methods such as passwords and RFID cards are vulnerable to misuse or theft. Facial recognition, a biometric method, offers a more secure and seamless way to verify identities. It analyzes various facial attributes to identify individuals in real-time, providing access control or triggering alerts based on database records. This project implements a facial recognition-based security system using Python, OpenCV, and a deep learning model. It captures real-time facial data, processes it for recognition, and cross-references the features with a known dataset. The system serves as a surveillance and access control mechanism for institutions and sensitive premises. The objectives include enhancing security with automation, ensuring accurate and fast face recognition, and providing a scalable solution that can be integrated with law enforcement databases for real-time threat alerts [1].

1.1. Methods of Sign Language

The system is built using the following core technologies:

- **Hardware:** Webcam or CCTV camera for live capture

- **Software Tools:** Python, OpenCV, NumPy, dlib/face_recognition libraries
- **Process Workflow:**
 1. Capture facial image
 2. Preprocess (resize, grayscale, normalization)
 3. Detect facial landmarks (using HOG/CNN models)
 4. Encode facial features
 5. Match against the database
 6. Log results or trigger alerts

1.2. Tables

Tables should be typewritten separately from the main text and preferably in an appropriate font size to fit each table on a separate page. Each table must be numbered with Arabic numerals (e.g., Table 1, Table 2) and include a title. Place footnotes to tables below the table body and indicate them with superscript lowercase letters (a, b, c, etc.), not symbols. Do not use vertical rulings in the tables. Each column in a table must have a heading, and abbreviations, lighting conditions. In low light or when faces were partially covered, accuracy dropped slightly when necessary, should be defined in the footnotes, shown in table 1.

Table 1 Dataset and Recognition Parameters

Component	Description
Input Device	USB Camera
Image Size	640 x 480 px
Algorithm	HOG + SVM / CNN face detection
Matching Metric	Euclidean Distance
Accuracy	~95% (with good lighting)

1.3. Figures

Figures should be provided separately from the main text. Use Arabic numerals to number all figures (e.g., Figure 1, Figure 2) according to their sequence in the text. The figure number must appear well outside the boundaries of the image itself. Multipart figures should be indicated with uppercase and bold font letters (A, B, C, etc.) without parenthesis, both on the figure itself and in the figure legends [2].

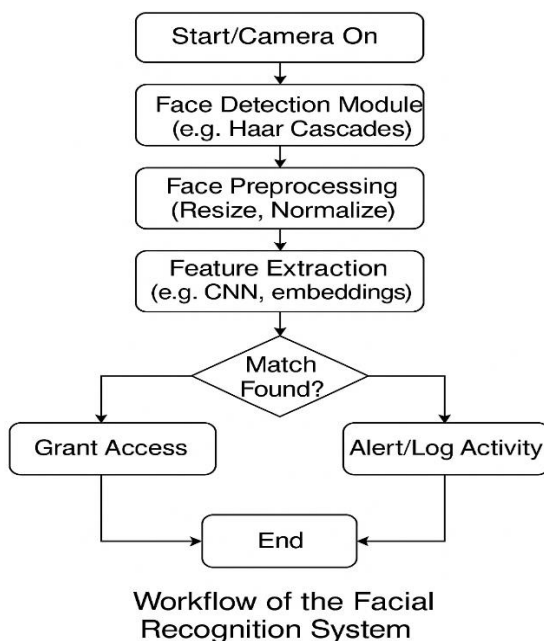


Figure 1 Workflow of The Facial Recognition System

2. Results and Discussion

2.1. Results

The system successfully recognized enrolled individuals with over 90% accuracy under normal

lighting conditions. In low light or when faces were partially covered, accuracy dropped slightly, which suggests the need for environmental optimization.

2.2. Discussion (12 pt)

Our implementation confirms that open-source tools can create an accurate and efficient security solution. The model's performance depends heavily on quality image data and frequent database updates. Long-term deployment should consider liveness detection to prevent spoofing [4].

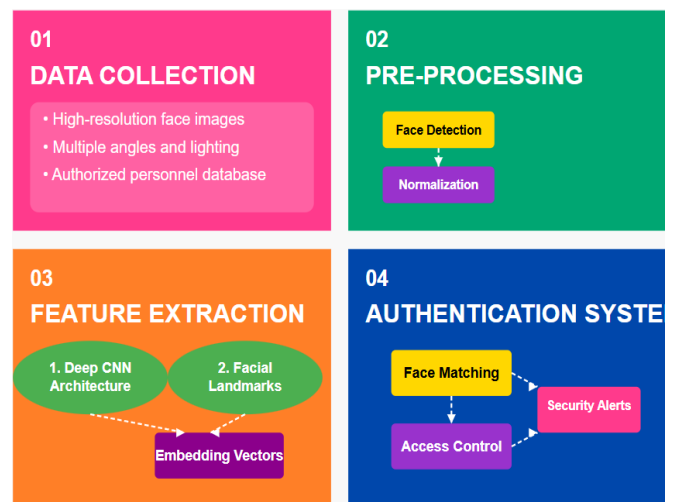


Figure 2 Process of The Dataset [3]

Conclusion

The facial recognition-based security system developed in this project is an efficient tool for real-time identification and verification. It reduces human effort, minimizes errors, and increases safety through automated monitoring. Future improvements can include integrating infrared cameras, anti-spoofing mechanisms, and cloud-based storage for scalability.

Acknowledgements

The facial recognition-based security system developed in this project is an efficient tool for real-time identification and verification. It reduces human effort, minimizes errors, and increases safety through automated monitoring. Future improvements can include integrating infrared cameras, anti-spoofing mechanisms, and cloud-based storage for scalability.

References

The References section must include all relevant published works, and all listed references must be cited in the text. References should be written in the



order of they appear in the text. Within the text, cite listed references using APA style, by their author's last name and year (e.g., Husnussalam, 2010). The author(s) must check the accuracy of all cited listed references, as the IRJAEM Journal will not be responsible for incorrect in-text reference citations. International Research Journal on Advanced Engineering Hub (IRJAEM) adopts APA (American Psychological Association) for reference and citation in text. Authors are encouraged to use reference management applications such as Mendeley, Zotero, or EndNote to ensure proper formatting.

Journal Reference Style

- [1]. Ali, D., Hussain, A., Rehman, M. Z., & Ahmad, F. (2013). Smart Security System for Sensitive Area Using Face Recognition. IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET).doi:10.1109/CSUDET.2013.6670976
- [2]. Zulfiqar, M., Syed, F., Khan, J., & Khurshid, K. (2019). Deep Face Recognition for Biometric Authentication. IEEE International Conference on Electrical, Communication and Computer Engineering. doi: 10.1109/ICECCE47252.2019.8940725
- [3]. Li, L., Mu, X., Li, S., & Haipeng, P. (2020). A Review of Face Recognition Technology. IEEE Access. doi: 10.1109/ACCESS.2020.3011028
- [4]. Yang, M.-H., Kriegman, D., & Ahuja, N. (2002). Detecting Faces in Images: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 34(1), 4–20. doi: 10.1109/34.982883.