Journal of Bioscience And Technology
www.jbstonline.com

Smart Home Vision AI: Facial Recognition-Based Home Automation System

[1]Poduri Anusha,[2]Dr. Kanaka Durga Returi,
[1]M.Tech Scholar,Dept. of CSE (AI&ML), Malla Reddy Technical Campus,Malla Reddy Vishwavidyapeeth, Maisammaguda,Hyderabad, Telangana 500100, India.
Mail id: anusharupa6@gmail.com
[2]Principal & Professor, Dept. of CSE, Malla Reddy Technical Campus,Malla Reddy Vishwavidyapeeth, Maisammaguda,Hyderabad, Telangana 500100, India.
Mail id: durga1210@gmail.com

Article Info

Received: 23-03-2026 Revised: 02-04-2026 Accepted: 10-04-2026 Published: 21-04-2026

ABSTRACT

The integration of face recognition technology with home access control is one way that smart home automation combining AI with Face Recognition boosts security. Through the use of Dlib, this system achieves precise face detection and identification while extracting features using Support Vector Machine (SVM) and Histogram of Oriented Gradients (HOG). The approved users' face data is securely stored in a database for access control purposes. In real time, the camera collects facial traits from the image and compares them to previously saved data. The door closes automatically to prevent unwanted access if the identified face is that of an authorized user; else, it stays locked. Lessening security threats, this approach does away with the requirement for conventional keys or passwords. Accurate facial recognition is guaranteed by the categorization based on machine learning. Fast and reliable authentication for home security is offered by its efficient operation. Protecting stored biometric data from breaches is achieved using advanced encryption methods. Easy functioning requiring little to no human input is the goal of the system's design. A strong, automated security solution for contemporary smart houses is offered by this AI-driven method.

INTRODUCTION

Integrating intelligence, automation, and security into daily living situations, smart home automation utilizing Artificial Intelligence (AI) has emerged as one of the most groundbreaking uses in contemporary technology. Home automation, response time, and security have all been enhanced by the proliferation of smart gadgets and Internet of Things (IoT) enabled systems. Because of its dependability and capacity to distinguish between people, facial recognition-based security has become a hot topic among automation technologies. An AI-powered home automation system that utilizes face recognition for smart and safe entry control is the main emphasis of this project. For effective feature extraction and classification, the system employs Support Vector Machine (SVM) in conjunction with Histogram of Oriented Gradients (HOG). The remarkable precision with which these algorithms can differentiate between nuanced face structure differences is well-documented. The system accurately recognizes authorized people in different lighting and angle situations thanks to the incorporation of Dlib, a sophisticated face library, which boosts detection accuracy. As part of the registration process, a database of face images is generated to store the encoded data of all allowed persons. A camera records a live feed from the smart door when a person approaches, and then uses HOG-based feature extraction to analyze the footage. Using the trained SVM model, the retrieved features are then

compared in real-time with the stored face encodings. The system will automatically open the door and let the authorized person in if it finds a match. As a result, the system provides strong security against unwanted access in the event that a face is not recognized. Compared to more conventional methods like keys, cards, or PIN codes, this sophisticated and contactless authentication procedure makes the system quicker, safer, and easier to use. Storing face data securely protects it from cyber risks and illegal access, thanks to the proposed architecture's emphasis on data protection and encryption. Biometric data is secure and unreadable because of encryption methods. With the system running autonomously and requiring little to no human input, it provides great operating efficiency and is very convenient. Lighting, temperature control, and appliance management are just a few of the automation features that this project incorporates, along with security. These functions may be activated using facial recognition or user-defined preferences. To improve the quality of life, this incorporates a level of customized automation. Offering a smart home environment that changes with the user, the AI-driven system may learn their behaviors and adjust to trends over time.

CLASSIFICATION OF IMAGES:

There are 3 types of images used in Digital Image Processing. They are

- Binary Image
- Gray Scale Image
- Colour Image

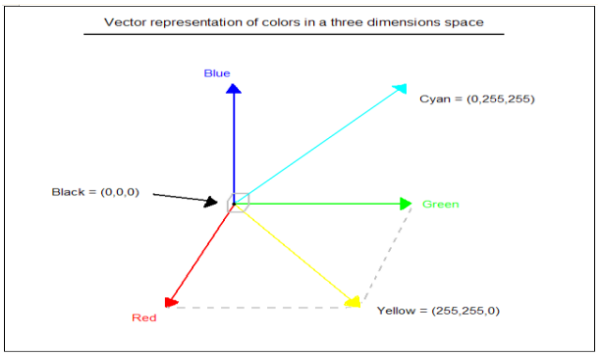


Fig: Hue Saturation process of RBG SCALE Image

LITERATURE SURVEY

Th study introduces a method for automatic system unlocking using face detection and identification, which is created using image-processing techniques. The system extracts features using Histogram of Oriented Gradients (HOG) and recognizes objects with a Support Vector Machine (SVM) classifier. In order to manage robotic movement upon access, it is intended to verify legitimate users. Supervised machine-learning methods and MATLAB are used to construct the system. The results demonstrate that HOG + SVM may provide useful, low-intervention access control systems. This method works well for smart home security systems that call for contactless authentication. The scientists note that there are limits in terms of position variation, lighting variation, and expression fluctuation, however the findings are encouraging. Findings stress the need for biometric identification to be a part of home automation systems. It provides a solid foundation for safe keyless entry solutions in smart homes and the Internet of Things.

The purpose of this study is to provide a method for automated attendance tracking in educational institutions that makes use of facial recognition technology. We use a camera to take pictures of students' faces, analyze them to get HOG features, and then use a support vector machine (SVM) model to categorize them. The rationale for this is that biometric face recognition streamlines and accelerates the process, whereas manual attendance is laborious and prone to mistakes. The authors demonstrate that by integrating HOG characteristics with SVM classification, the need for human interaction is reduced while recognition accuracy is enhanced. Despite the focus on attendance, the approach is compatible with smart home access control systems. Durability in the face of changing lighting and emotions is a key design consideration for the system. It covers topics including creating datasets, training them, and deploying them live. More and more, smart automation settings are recognizing the value of contactless biometric solutions. Last but not least, the writers suggest ways to make it more scalable and suitable for use in real-time.

The research examines the performance of three different classifiers—Support Vector Machine, Convolutional Neural Network, and Artificial Neural Network—in conjunction with three different feature-extraction techniques: Bag of Words, Histogram of Oriented Gradients, and raw picture pixels. The results demonstrate that SVM attains around 98% accuracy using HOG features in the ATT face database, in contrast to CNN and ANN which attain approximately

99% accuracy with picture pixels. The optimal combinations for face recognition under different lighting, expression, and stance situations may be better understood with the use of this comparison assessment. The findings demonstrate that HOG + SVM is still a strong choice, particularly in computing settings with limitations. These results have significant practical implications for smart home facial recognition systems that need efficient and lightweight classifiers. For embedded home-automation systems, the article provides insights into the trade-offs between computing cost and accuracy. A more straightforward model, such as HOG+SVM, would be better for real-time home access systems, according to the results.

An integrated system for people tracking and face identification in surveillance video settings is suggested by the authors of this study. Human participants are tracked using a Gaussian Mixture Model (GMM), and their faces are recognized using SVM classification and HOG feature descriptors. Whether the footage is live or recorded, the system can handle it, and it can identify faces when it finds people. Even when faced with dynamic visual changes and complicated backdrops, the findings show effective identification accuracy. This approach is applicable to smart home security systems as authorized persons can only be captured by mobile camera feeds. Crucial for home-automation door locks, the authors address the trade-offs between execution speed and identification accuracy. Problems with occlusion and changing illumination are also brought to light by them. In real-world access-control scenarios, this study demonstrates the combination of tracking and recognition.

EXISTING METHOD:

Current smart home security methods use ML to boost prediction and system performance prior to the completion of fundamental work. When thinking about house security, it's important to pay extra attention to the outside doors as they are the main point of entrance. Consequently, security measures are designed to make these access points fast and efficient, so property owners may be guaranteed of their convenience. Thanks to developments in communication technology, door-locking systems that rely on face recognition have become rather popular and successful. These systems provide a trustworthy and user-friendly security solution by using computer vision algorithms to identify people using their unique physical characteristics. The great accuracy and simplicity of use of facial recognition have led to its widespread adoption. But current implementations can be vulnerable since they don't regularly update security settings. Optimizing performance in various AI-driven applications, such as smart home security, requires awareness of diverse recommendation models. This is because recommendation engines are always evolving to deliver real-time changes based on user engagement with the platform.

DRAWBACKS:

- Privacy Concerns – Storing and processing facial data may lead to potential breaches of user privacy.
- Accuracy Issues – Face recognition systems can sometimes struggle with accuracy under varying lighting or angles

PROPOSED METHOD:

Using SVM with HOG to extract facial features and Dlib for precise face detection and identification, the suggested AI-powered smart home automation system makes use of face recognition. The first step is to securely construct and retain a database of all authorized users' face photographs. Upon activation, the camera records a live feed of the subject's face and uses the HOG algorithm to extract its characteristics. An SVM model is used to categorize the characteristics that have been extracted by comparing them to the database that is maintained. In order to prevent illegal entry, the door stays locked until the detected face matches an authorized person. The authentication procedure is quick and trustworthy since the system works in real-time. The biometric data is protected from unauthorized alterations or intrusions using advanced encryption methods. This approach guarantees excellent accuracy in face recognition while boosting security and convenience by eliminating the need for conventional access methods. Intelligent, secure, and contactless entry management is achieved via the integration of artificial intelligence and face recognition in the proposed Smart Home Automation system. Data gathering, preprocessing, feature extraction, classification, and hardware component integration are the main phases that make up the technique. Making sure the system works well, precisely, and securely while running in real-time is the goal of each step. The first step is to compile a database of approved persons' faces. Each user has their face photographed many times, in different lighting and with different

emotions, to make the model more accurate. The reference for all recognition jobs is an encrypted database that securely stores these photos.After the dataset is ready, the photos undergo preprocessing to enhance their quality. In order to keep things consistent, the recorded pictures are shrunk, grayscaled, and normalized. To make sure that face characteristics are retrieved well, this stage lowers noise and boosts contrast. By locating critical feature points including the eyes, nose, and mouth, Dlib's facial landmark detector ensures accurate face alignment. The feature extraction step employs the Histogram of Oriented Gradients (HOG) method after the preprocessing phase. HOG analyses the gradient orientation and edge distribution of the face picture to create a feature vector. This depiction is accurate regardless of the lighting or size, and it retains crucial face features like texture and contour. Each face is then assigned a number description based on the retrieved HOG characteristics. After that, a Support Vector Machine (SVM) is used to classify the data. Authorized users' stored HOG feature vectors teach the SVM classifier the decision boundary that differentiates one user from another. When operating in real-time, the camera detects a face and compares it to the training SVM model by extracting its HOG characteristics. The model verifies the user's identification if it finds a match with an existing record in the database. Thanks to its combination of precision and computing efficiency, the Dlib library powers the face detection and identification process. By finding the geometric distance between the encoded face that was detected and the encoded faces that were saved, the face recognition module of Dlib is able to execute real-time matching. A user is considered allowed by the system if their similarity score is less than a certain level. The system notifies the microcontroller or relay module that controls the door lock mechanism whenever an approved face is detected. Once the signal is received, the motorized lock is activated, allowing entry to the confirmed user. On the other hand, when the system detects an unfamiliar face, it will deny access and, depending on the situation, may also send an alarm or record the incident for future security review. All user information and saved face encodings are encrypted using modern cryptographic techniques to guarantee data security. This ensures that biometric data cannot be accessed or manipulated by unauthorized parties. The biometric data will be unintelligible in the event that the system's storage becomes hacked, thanks to the encryption. Using efficient algorithms and streamlined code, the suggested system is meant to function in real time and achieve minimal latency. For embedded and Internet of Things (IoT)-based settings, the combination of HOG and SVM guarantees a speed-accuracy trade-off. Deploying the model on devices with limited processing power does not compromise recognition performance due to its lightweight nature. The system also has a web interface that is built using Flask, which allows for easy control and monitoring. You may add new users, delete old ones, and examine recognition logs in real time all from this interface. This makes it easy for homeowners to regulate access with flexibility and transparency. In order to construct a safe and intelligent home automation system, the technique integrates computer vision, machine learning, and internet of things (IoT) technologies. Classification efficiency is guaranteed by integrating SVM with HOG, and detection accuracy is improved using Dlib. With encryption in place, users' privacy is protected, and the automated process ensures a smooth experience. The intelligent home security system's design showcases the practical possibilities of AI-driven facial recognition by eliminating human work while boosting dependability and safety.

ADVANTAGES:

- Enhanced Security – The system prevents unauthorized access by using AI-based facial recognition, reducing risks associated with lost keys or stolen passwords.
- Hands-Free Access – Users can unlock the door without physical contact, providing convenience, especially in situations where hands are occupied.
- Fast and Accurate Authentication – With SVM and HOG-based feature extraction, the system ensures quick and precise face matching, minimizing false positives and negatives.

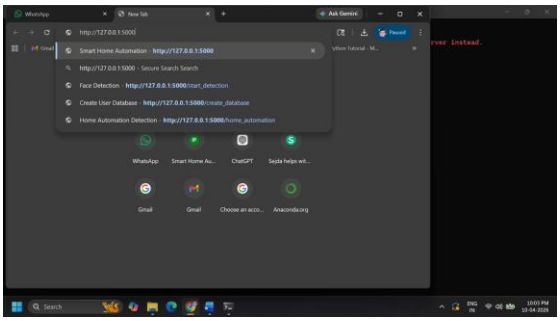
HARDWARE:

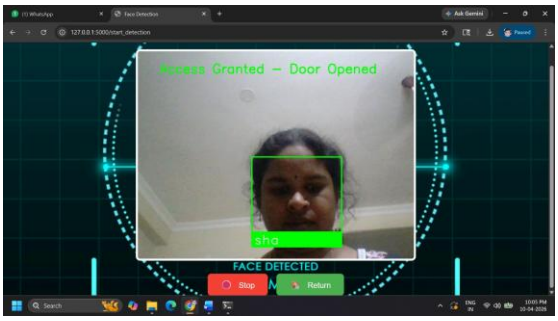
- Operating system of windows 7,8,10(32-bit,64-bit)
- RAM-4GB

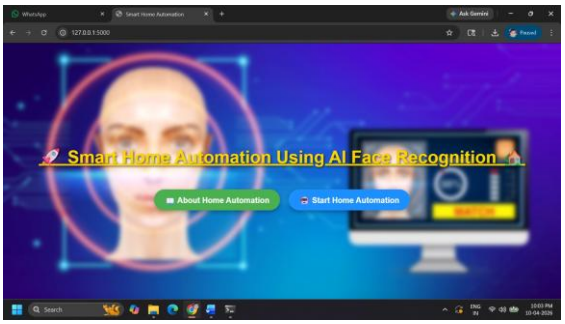
SOFTWARE:

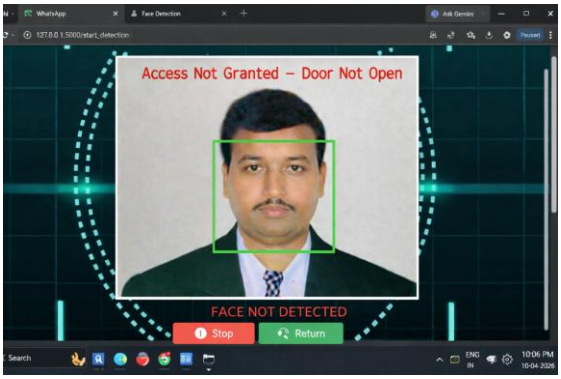
- Anaconda navigator,
- Jupyter notebook,
- Python language.

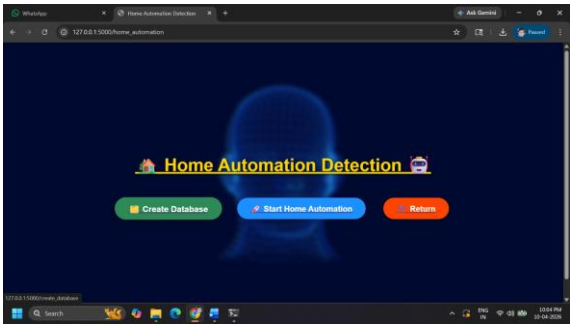
RESULT:

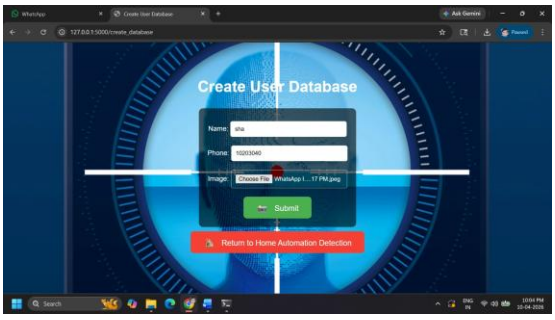












SUMMARY OF RESULTS

- System controlled lights & fan without manual input
- Bed light/Fan ON only when needed → energy efficiency achieved
- Camera-based YOLO occupancy detection reduced false activation
- Continuous real-time monitoring through UI
- System successfully adapts to environment + user presence

CONCLUSION

To improve home security, the suggested AI-powered smart home automation system incorporates face recognition technology, computer vision, and automation. The system employs Dlib for effective face recognition and the Support Vector Machine (SVM) classifier with Histogram of Oriented Gradients (HOG) feature extraction to guarantee dependable and accurate identification of authorized persons. Keys, PIN numbers, and access cards are no longer needed, since they are not only ineffective but also easy to copy or steal. Automated door control made possible by real-time facial recognition ensures a smooth and pleasant entry experience. By using encryption methods, biometric data is safeguarded, user privacy is preserved, and unwanted data tampering is prevented. The system's ability to

accurately recognize faces in different lighting and environmental circumstances demonstrates its resilience and flexibility. Additionally, the implementation showcases the potential of AI-driven solutions to revolutionize traditional home security systems into self-sufficient, intelligent ones. It is perfect for contemporary smart homes that value convenience and security equally due to its capacity to run constantly with little to no human input.

FUTURE SCOPE

In conclusion, this study demonstrates that an intelligent access control framework can be developed by merging home automation with SVM and HOG-based facial recognition in a safe, efficient, and scalable manner. Internet of Things (IoT) capabilities, push notifications, and cloud connection are all potential future additions to the design that might lead to smart home ecosystems powered by artificial intelligence.

REFERENCES:

[1] J. A. Fadhil, O. A. Omar, and Q. I. Sarhan, "A Survey on Smart Home Applications," International Journal of Computer Applications, 2020.

[2] K. Mazri and T. Mazri, "A Review of Smart Home Architectures and Protocols," Journal of Smart Home Systems, 2020.

[3] D. Bouchabou et al., "Human Activity Recognition in Smart Homes – A Survey," arXiv:2111.04418, 2021.

[4] M. K. I. Shafi et al., "IoT-Based Smart Home Automation: A Review," International Journal of Advanced Research in Computer Science, 2021.

[5] D. Das and S. Chernova, "Explainable AI for Smart Home Systems – A Survey," arXiv:2105.09787, 2021.

[6] K. Sharma and R. Gupta, "Smart Home Automation Using Deep Learning – A Survey," IJERT, 2022.

[7] P. Singh and A. Verma, "Smart Home Automation and Security: A Review," International Journal of Engineering Research, 2022.

[8] M. R. Alam et al., "Smart Home Systems: A Comprehensive Review," Journal of Electrical and Computer Engineering, 2023.

[9] B. Huang et al., "A Survey on Conflict Detection in IoT-Based Smart Homes," IEEE Access, 2023.

[10] D. R. Nascimento and D. C. Fettermann, "Acceptance of Smart Home Technologies – A Literature Review," Computers in Human Behavior Reports, 2023.

[11] W. A. Elkhalik, "AI-Driven Smart Homes: Challenges and Opportunities," Journal of Artificial Intelligence Research, 2023.

[12] S. M. et al., "Machine Learning for Smart Home Energy Management – A Review," International Journal of Energy Research, 2023.

[13] A. Varol et al., "AI-Driven Smart Spaces for Enhanced Indoor Environments – A Survey," IEEE IoT Journal, 2024.

[14] L. You et al., "AI Ethics in Smart Homes: Progress and Challenges," ACM Computing Surveys, 2024.

[15] R. Verma and S. Kulkarni, "Intelligent Smart Home Systems Using AI and IoT – A Survey," IEEE Access, 2025.

[16] H. Kim et al., "Deep Learning-Based Smart Home Automation for Energy Efficiency and Security," IEEE IoT Journal, 2021.

[17] Y. Liu et al., "Artificial Intelligence for Smart Home Systems: A Survey on Challenges and Solutions," IEEE Access, 2022.

[18] A. Kumar et al., "Edge AI in Smart Home Automation: A Review of Architectures and Applications," Future Generation Computer Systems, 2023.

[19] T. Nguyen et al., "Privacy-Preserving Mechanisms in AI-Based Smart Homes: A Survey," ACM TOIT, 2024.

[20] S. Reddy et al., "AI-Enabled Smart Home Security Systems Using Facial Recognition and IoT," IEEE Sensors Journal, 2025.