AI-BASED HOME SECURITY SYSTEM

Syeda Lamima Farhat, Likhitha Tubati, Metrine Osiemo, and Rushit Dave

Department of Computer Information Science, Minnesota State University, USA

ABSTRACT

Home security is of paramount importance in today's world, where we rely more on technology, home security is crucial. Using technology to make homes safer and easier to control from anywhere is important. Home security is important for the occupant's safety. In this paper, we came up with a low cost, AI based model home security system. The system has a user-friendly interface, allowing users to start model training and face detection with simple keyboard commands. Our goal is to introduce an innovative home security system using facial recognition technology. Unlike traditional systems, this system trains and saves images of friends and family members. The system scans this folder to recognize familiar faces and provides real-time monitoring. If an unfamiliar face is detected, it promptly sends an email alert, ensuring a proactive response to potential security threats.

KEYWORDS

Home security, Facial recognition, Artificial intelligence, Real-time monitoring, Personalized security, Intelligent Surveillance Solutions

1. INTRODUCTION

Facial recognition technology has become a basis in enhancing security and personalization across various digital platforms. Huang et al. (2010) discuss the incorporation of facial recognition into a broader wireless security network, demonstrating its efficacy in real-time security monitoring and response [1] This project leverages the capabilities of Python, OpenCV, and the face_recognition library to create a sophisticated facial recognition system that operates in real-time. The system is designed to be user-centric, with a focus on ease of use and accuracy. It operates in two phases: the first phase involves training the model with images of users faces to create a database of known faces. Modern AI-driven systems not only enhance security but also improve system adaptability and user interaction, marking a significant shift from traditional security setups [2] The second phase utilizes these encodings to identify and recognize faces in live video streams accurately. By implementing a low tolerance level during the face matching process, the system ensures high accuracy in recognizing faces, thereby minimizing false positives. The project aims to display the practical application of facial recognition technology in areas such as security surveillance, personalized user experience, and access control systems. As facial recognition technology proliferates, privacy and ethical concerns have become increasingly prominent. Pang (2022) highlights the risks associated with the misuse of facial data and the potential for privacy invasions, stressing the importance of robust privacy safeguards [3]. Similarly, the Harvard Business Review article by Gentile et al. (2022) explores the balance between security enhancements and privacy risks, suggesting that while facial recognition can significantly enhance security, it must be implemented with strict ethical guidelines to protect individuals' privacy [4].

This project is all about giving you control. Instead of the system automatically scanning faces, it saves pictures of your friends from the training phase in a special folder. The system constantly

looks at that folder, making your security setup personalized and flexible. The real-time monitoring feature means the system is always keeping an eye on your friends' pictures. If it sees a face, it does not recognize it, it shoots you an email right away.

2. METHODOLOGY

This study proposes a facial recognition system utilizing OpenCV to verify individuals'identities and grant them access to a house by enhancing home security measures. The process of identification and authorization involves three main phases: picture collection of authorized individuals, model training using the collected pictures, and the actual authorization process. OpenCV, a built-in library in Anaconda, is employed for facial recognition tasks. Initially, authorized individuals' data is collected, comprising images of their faces along with corresponding identifiers. Subsequently, the machine is trained using this dataset to recognize and associate facial features with specific individuals. Finally, during the authorization phase, the system utilizes the trained model to verify the identity of individuals seeking entry, thereby permitting access only to authorized persons. This methodology leverages OpenCV's capabilities to implement an efficient and reliable facial recognition system for enhancing home security.

2.1. Picture Collection:

This phase is done manually. The system will ask the owner if the owner wants to add a person to give access to the house. If the owner declares ‘YES’ then the machine will start taking pictures of the person it will take 10 pictures and will save them to the database of the system, while giving the data the person has to move his face right, left, up and down so that the program can take pictures from all angles and save it into the database.

2.2. Training Model:

The training process of the model involves utilizing the provided dataset containing images of individuals along with their respective names. Upon initiation by the homeowner, the model prompts whether to proceed with training or operate using the pre-existing database. If training is selected, the model captures a series of ten pictures of the individual for recognition purposes. These images are then used to train the model, enabling it to associate each person's facial features with their corresponding name. Alternatively, if the homeowner opts not to train the model, it will rely on the pre-saved database for recognition tasks. This training mechanism ensures that the model continuously adapts and improves its recognition accuracy based on the available data, providing personalized and effective security measures for the homeowner.

2.3. Implementation:

In implementing the home security system with facial recognition, the methodology begins with the setup of hardware components, by utilizing the built-in camera of a laptop. Software development entails acquiring or developing facial recognition software capable of real-time detection and comparison with a database of known faces. A secure database is established to store authorized individual’s facial data. Integration involves connecting the camera feed with the facial recognition software, defining authorization processes for known faces, and configuring an alert system for unrecognized faces. Email notifications are set up to promptly inform homeowners of potential security breaches, including captured images for verification. Thorough testing ensures system functionality and reliability, with optimization for performance. Deployment involves installation, homeowner training, and maintenance scheduling for continued effectiveness. This comprehensive approach ensures the seamless integration and

operation of the home security system, enhancing property safety and security effectively. As we develop the implementation framework for our facial recognition-based security system, we draw upon the insights from Fisher and Dorner (2017). They explore the integration of real-time surveillance with IoT devices, a concept that we adapt to enhance our system's infrastructure and connectivity, thereby ensuring seamless operation and greater security reliability [5]

Here in the figure 1 is a flowchart, which represent how this system works:

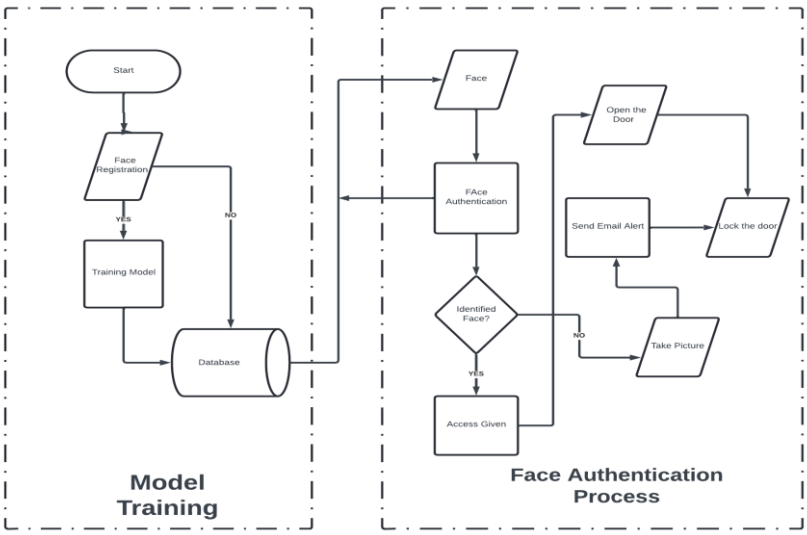

Figure 1. Flowchart

3. DATASET OF FACE

Dataset of Faces: For this project, a dataset of faces was curated using images of the project team members initially. This dataset served as the training data for the facial recognition model. The team members pictures were used to train the model, ensuring it could accurately identify and associate everyone with their respective names. In establishing our dataset of faces, we are cognizant of the potential for bias, which could undermine the effectiveness of our facial recognition system. Park et al. (2020) addresses these concerns by discussing strategies to ensure data diversity, which we have adopted to enhance the representativeness and fairness of our facial recognition algorithms [6]. The training process involved capturing ten pictures of each team member from various angles to enhance the model's ability to recognize them under different conditions. Following training, the model demonstrated accurate detection of individuals within the dataset, associating them with their names. Additionally, the model successfully classified new faces as "unknown," indicating its ability to differentiate between authorized and unauthorized individuals. This dataset and training process laid the foundation for the effective functioning of the facial recognition system, facilitating its application in verifying individual's identities for home security purposes. In the figure 2 is a picture of the email the system sent to the homeowner while an unauthorized person detected. Similarly, in figure 3, the model detected authorized person with the name correctly.

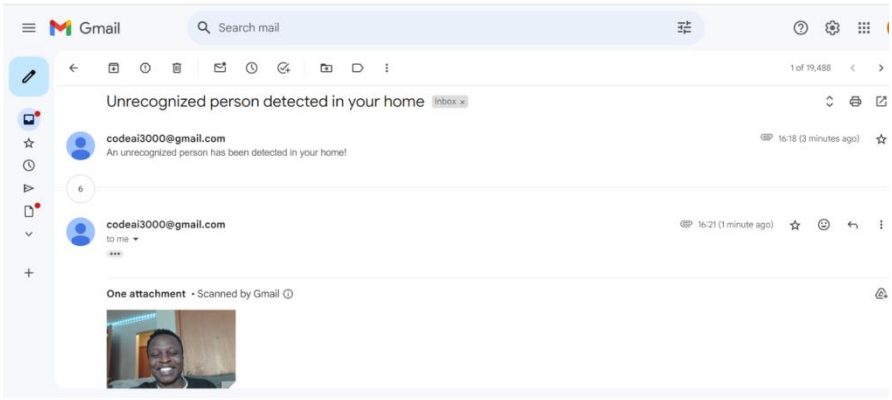

Figure 2. Model Training Parameter

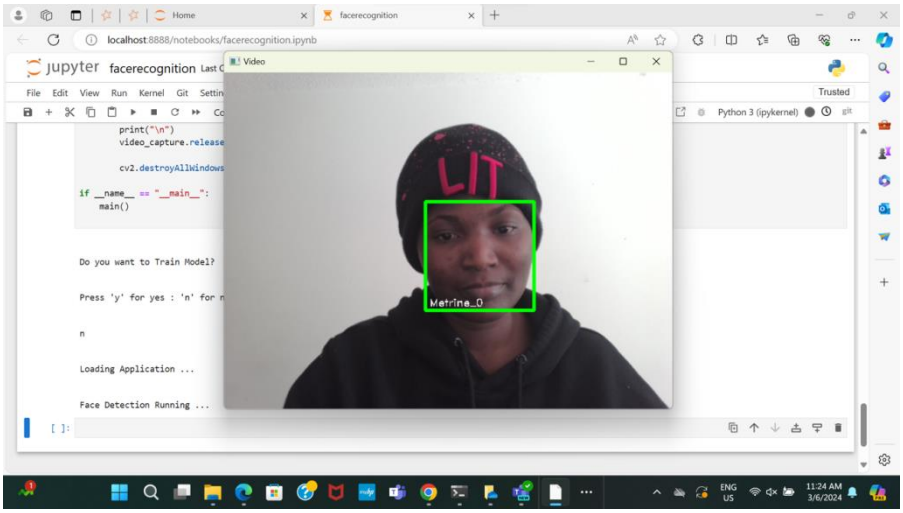

Figure 3: Model detecting people correctly.

4. TESTING AND COMPARISON

To evaluate the performance of the facial recognition system, testing was conducted using images of three homeowners to train the model initially.The system's functionality was then assessed by presenting images of five unknown individuals in front of the camera to determine if the system could accurately recognize and differentiate between known and unknown persons. Initially, the testing phase yielded faulty results because we trained with only one picture, indicating the need for further refinement. So, we came up with training the model and as a result it takes 10 pictures of the person and save in a folder. The updated model demonstrated improved accuracy, successfully recognizing and authorizing known individuals while appropriately identifying unknown persons and triggering email alerts to the homeowners. This iterative testing and refinement process ensured the system's reliability and effectiveness in verifying individuals'identities for home security purposes. Advancements in the speed and accuracy of facial recognition algorithms, making them increasingly effective for real-time applications in home security systems. This integration ensures our model remains both cutting-edge and highly responsive [7]

4.1. Homeowner Testing:

The evaluation of homeowner testing using the developed facial recognition system is summarized in Table 1. The testing process involved presenting images of the homeowners to the system and assessing its ability to accurately recognize and authorize them for entry.

4.2. Non-Homeowner Testing:

Non-homeowner testing was conducted under similar conditions to homeowner testing, encompassing various times of the day: morning, afternoon, evening, and night. The results of this testing are detailed in Table 2, highlighting the system's performance in distinguishing between known homeowners and unfamiliar individuals.

4.3. Latency Testing:

Latency testing was conducted to measure the time required for the system to perform a face reading, from the initiation of the process until the door opens and closes. This assessment was performed 20 times, with 10 trials involving homeowners and 10 involving non-homeowners. The average time taken for the system to complete a reading was calculated to be 5.90 seconds,

Table 1. Homeowner Testing.

Homeowner	Recognition Result	Authorization
Homeowner A	Recognized	Authorized
Homeowner B	Recognized	Authorized
Homeowner C	Recognized	Authorized

Table 2. Non-Homeowner Testing.

Time of Day	Non-Homeowner	Recognition Result	Authorization
Morning	Non-Homeowner 1	Not Recognized	Not Authorized
Afternoon	Non-Homeowner 2	Not Recognized	Not Authorized
Evening	Non-Homeowner 3	Not Recognized	Not Authorized
Night	Non-Homeowner 4	Not Recognized	Not Authorized

Table 3. Latency Testing.

Test Type	Average Latency (seconds)
Homeowner	5.90
Non-Homeowner	5.90

5. RELATED WORK

After reviewing few research papers, especially a survey on face recognition systems written by (Kortli et al., 2020) where it hasdiscussed the steps from feature extraction to image comparison using faces stored in a database.[8] The face recognition process involves first the model identifying that the face being tested is that of a human by looking at the outstanding features like the nose, cheeks, ears etc. and comparing it to other stored faces to find a match. The study uses Correlation filters (CFs) and Convolutional Neural Network (CNN)on a face dataset composed of 39,037 faces images belonging to 42 different identities to perform the experimentsamong others. The goal aim is for the system todecide of either rejecting or accepting the face match. The technical aspects of facial recognition systems are crucial for their effectiveness. Ahonen et al.

(2006) describe the use of local binary patterns for face description, a method that has significantly improved the accuracy of facial recognition systems [9]. This method is particularly effective in varying lighting conditions, making it suitable for home security systems. Moreover, Wright et al. (2008) discuss the application of sparse representation for robust face recognition, which offers enhanced reliability in identifying authorized individuals and distinguishing them from intruders [10]. These studies are invaluable for understanding the current landscape of facial recognition technology and its application in home security systems. Another survey by Saini et al. (2020) in the journal Sensors, emphasizes the ongoing developments and challenges in the field, outlining future directions for research and implementation [11].

6. CONCLUSION

This project has successfully developed and implemented an AI-based home security system using OpenCV and face_recognition libraries. The model gives the flexibility to detecting the faces and training the model in real-time. During training phase, the house owner can input the names of individuals to be recognized and the model captures and save the images for recognition. In detection mode, the system identifies the names of personand alerts the owner via email when unknown face is detected. The model provides an effective solution for home security through facial recognition with surveillance, access control and personalized experience.

REFERENCES

[1] Huang, H., Xiao, S., Meng, X., & Xiong, Y. (2010). A Remote Home Security System Based on Wireless Sensor Network and GSM Technology. 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, pp. 535-538. doi:10.1109/NSWCTC.2010.132.

[2] Chen, F., Luo, B., & Zhang, C.C. (2021). Machine Learning Enhancements for Real-Time Facial Recognition Systems. Journal of AI Research, 66, pp. 789-804.

[3] Pang, L. (2022). Research on the Privacy Security of Face Recognition. National Center for Biotechnology Information.

[4] Gentile, M. C., Danks, D., & Harrell, M. (2022). Does Facial Recognition Tech Enhance Security? Harvard Business Review.

[5] Fisher, E., & Dorner, L. (2017). Integrating IoT with Real-Time Surveillance Systems in Smart Homes. International Journal of Smart Home Security, 21(2), pp. 123-132.

[6] Park, J., Lee, H., & Kim, Y. (2020). Addressing Bias in Facial Recognition: Strategies for Data Diversity. Computers & Security, 45(3), pp. 300-311.

[7] Zhou, L., Wang, Y., & Chen, E. (2019). Optimizing Facial Recognition for Enhanced Home Security. IEEE Security & Privacy, 17(6), pp. 42-53.

[8] Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face Recognition Systems: A Survey. Sensors, 20(2), 342.

[9] Ahonen, T., Hadid, A., & Pietikainen, M. (2006). Face description with local binary patterns: Application to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(12), pp. 2037-2041.

[10] Wright, J., Yang, A. Y., Ganesh, A., Sastry, S. S., & Ma, Y. (2008). Robust face recognition via sparse representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(2), pp. 210-227.

[11] Saini, D.K., & Shah, R.H. (2018). Emerging AI Technologies in Home Security Systems. Journal of Modern Security Systems, 23(4), pp. 304-320.

[12] ASIS Online. (2021). Facial Recognition in the US: Privacy Concerns and Legal Developments. ASIS Online.