SMART SECURITY SYSTEM ON RASPBERRY PI WITH FACE RECOGNITION AND OBJECT DETECTION

Sa-nga Songmuang
Lecturer, Faculty of Science and Technology, Kasem Bundit University
60 Romklao Road, Minburi District, Bangkok 10510, Thailand,
sa-nga.son@kbu.ac.th

ABSTRACT

The smart Security System presented in this research harnesses the capabilities of Raspberry Pi to provide a comprehensive solution for home security and control. The system integrates three main functions aimed at enhancing user safety and convenience. The system employs a camera module to detect and recognize faces in its field of view. In the event of an unauthorized person attempting to enter the premises, the system captures the intruder's face and promptly sends the image to the user's mobile phone. This real-time notification ensures swift awareness and response to potential security threats. The camera is configured to detect and monitor various objects, such as vehicles or individuals, stationary for more than five minutes in front of the home. Upon detection, the system captures images of the objects and transmits them to the user's mobile phone. The system provides users with the capability to remotely control electronic devices within the home. Through the application or system interface, users can turn on or off specified devices. The primary goals of the system include the development of a reliable application for smart home security and control and the evaluation of its performance in real-world scenarios.

KEYWORDS: Raspberry Pi, Face Detective and Recognition, IoT, Mobile Application

1. Introduction

Traditionally, security systems relied on physical locks and alarms, providing a basic level of protection. However, with the rapid advancement of technology and myriad innovations, face detection algorithms have been addressed in many papers such as Haar Cascades [1], Kalman Filter [2] and applied in various fields [3-5]. Besides, OpenCV is a robust open source that supports many methods to detect faces. Face recognition and face

matching were conducted using the OpenCV image processing library. Face detection is not only necessary for the camera node detecting the face but also helpful in pre-processing the input data. Face recognition technology has made remarkable strides in recent years, driven by advancements in machine learning and artificial intelligence [6]. The integration of face recognition and object detection into smart security systems [7-9] stands out as a transformative paradigm [10], promising a robust shield for safeguarding homes. Parallelly, the integration of object detection fortifies the system's surveillance capabilities. Building on the works of Garcia et al [11, 12], which highlight the critical role of real-time monitoring in security systems, the inclusion of object detection extends the vigilant eye of the smart security system. Whether it be identifying parked vehicles or monitoring prolonged stationary activity, object detection augments the system's situational awareness.

In recent years, security cameras have been widely accepted by society as a security system, and the introduction of security cameras to shops, downtown areas, public facilities, etc. is proceeding [13]. It is important to prevent unauthorized use of photo data by the administrator of the security camera [14]. This security camera system is created using Raspberry Pi [15], a credit-card-sized computer, that has revolutionized the realm of DIY electronics and programming. Its affordability, versatility, and compact size have made it a favored choice for various projects, including security systems that provide a comprehensive solution for home security and control.

The intersection of face recognition, object detection, and remote device control forms the cornerstone of this study. Motivated by the promising prospects outlined in the existing literature, this paper aims to contribute to the discourse on smart security systems by presenting a novel implementation on the Raspberry Pi [16]. The primary research objectives encompass the development of a reliable application for smart home security and control, coupled with an in-depth evaluation of its real-world performance through user feedback. By addressing these objectives, this study endeavors to extend the frontier of knowledge in the realm of smart security systems while providing practical insights into the application of Raspberry Pi technology in residential settings.

Haar-feature-based cascade classifier for object detection has proved to be an effective classifier [17, 18]. A smart security system's integration of face and object detection is based on the convergence of advanced technologies including computer vision, artificial intelligence (AI), and the Internet of Things (IoT). Real-time face and object identification and recognition

are made possible by the system's utilization of deep learning models and sophisticated algorithms. It consists of multiple parts, including computer vision and image processing. By using computer vision techniques, the system analyzes live video feeds from cameras and extracts relevant environmental data. Algorithms for image processing are used to identify faces and objects in the photographed frames. The development and deployment of the system with integrated face and object detection follow a systematic and structured methodology such as requirement analysis, system design, data collection and processing, model training, integration and testing, deployment and evaluation, and interactive improvement. By following this methodology, the system is developed, evaluated, and refined to deliver reliable, efficient, and user-friendly security solutions. AI algorithms, especially deep learning models like Convolutional Neural Networks (CNNs) [19, 20], are trained on artificial intelligence and machine learning data. Mobile application and user interface design which is the main interface for communicating with the smart security system is a user-friendly mobile application. Real-time warnings, remote control capabilities, and historical data access are all offered by the program.

The first step is detecting faces within the camera's field of view. This involves analyzing the image or video feed to identify areas containing faces. Usually, camera 1 is positioned close to the entrance where authorization is required. The camera will take a picture and process it further if someone requires entrance to the home. Parallelly, camera 2 is configured to detect and monitor various objects, such as vehicles or individuals, stationary for more than five minutes in front of the home. Upon detection, the system captures images of the objects and transmits them to the user's mobile phone. This feature adds an extra layer of surveillance, aiding in the monitoring of activities around the property.

2. Methodology

2.1 Hardware Setup

The Smart Security System (shown in Figure 1) presented in this research harnesses the capabilities of Raspberry Pi3 to provide a comprehensive solution for home security and control. To build a face recognition security system, we'll need a Raspberry Pi3 board, a compatible camera module, and a display (optional). The camera module captures images, which are then processed for face recognition.

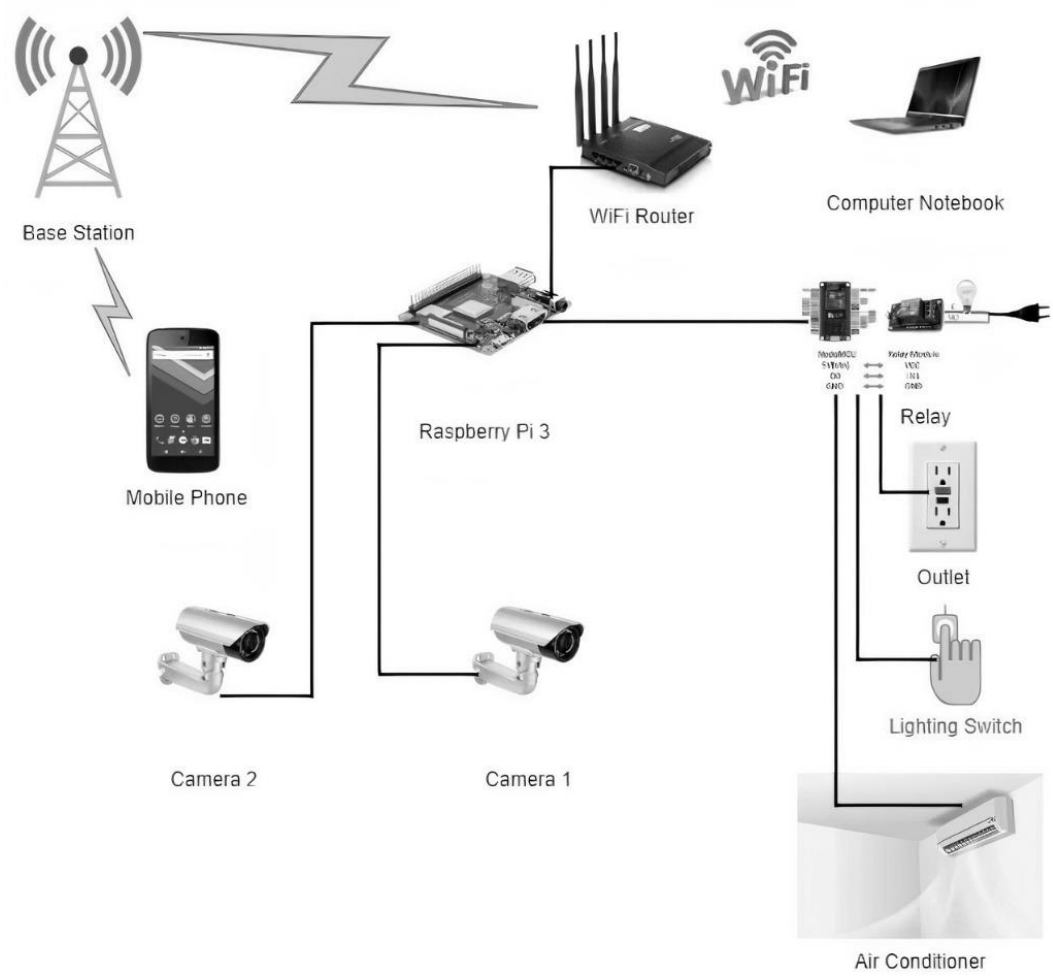

Figure 1 The Smart Security System

Base Station and Wi-Fi Router provide the network infrastructure for all devices to communicate. We connected the Wi-Fi router to the internet and configured it to ensure strong and secure wireless connectivity. The base station will act as the central hub, connected to the Wi-Fi network. Raspberry Pi3 acts as the main processing unit for face and object detection algorithms. It is connected to the Wi-Fi network. Camera 1 and camera 2 captured video footage for processing by the Raspberry PI (For cameras placement in a real-world setting are shown in Figure 2). We connected the cameras to the Raspberry Pi3. Position the cameras strategically around the property for optimal coverage. The cameras utilized in our smart security system are equipped with a 1/3" progressive scan image sensor, offering a maximum resolution of 1280 x 960 pixels and a frame rate of 30fps, ensuring high-

quality video capture. Each camera features a 4mm lens with an aperture of F/2.0, providing a 45.3-degree angle of view, and is mounted using an M12 lens mount. For optimal day and night functionality, the cameras include an IR cut filter with an auto-switch mechanism. They offer a wide horizontal view angle of 88 degrees and a vertical view angle of 65 degrees, effectively covering extensive areas. Additionally, these cameras can focus on objects as close as 0.5 meters, making them versatile for various security applications. Install cameras at the house with a height of 2.8 meters outside to provide the system with a wide-angle vision. With 88^{o} horizontal and 65^{o} vertical view angles provided by the cameras' wide-angle lenses, this arrangement optimizes coverage and reduces blind spots. To guarantee that the monitored area, including the ground directly below, is optimally covered, adjust the horizontal tilt between 0^{o} and 45^{o} and the vertical tilt between 10^{o} and 30^{o}. Adverse weather conditions such as heavy rain and fog can obscure the cameras' view and reduce detection accuracy. Even with optimal placement, cameras have a limited field of view. Wide-angle lenses provide broader coverage but may introduce distortion at the edges, affecting detection accuracy. Overlap the fields of vision of neighboring cameras to close any gaps and guarantee sufficient lighting to improve the quality of the images. This configuration lowers blind areas, increases face and object identification accuracy, and guarantees thorough monitoring. Computer Notebook used for monitoring, configuring, and maintaining the Raspberry Pi3 and system software. Ensure the notebook is connected to the same Wi-Fi network and has software installed to access and monitor the Raspberry Pi3. We used a relay to control the power supply to various electronic devices such as outlet, lighting switch, and air conditioner. These are the devices that will be controlled by the smart security system for automated responses. We connected these devices to the relay, enabling the Raspberry Pi3 to control them. The mobile phone provides remote monitoring and control capabilities to the user. It installed a mobile application that can receive notifications and control the system remotely.

Figure 2 The cameras placement in a real-world setting

2.2 Software Implementation

The software aspect involves installing, developing, and configuring the necessary libraries and frameworks (shown in Figure 3). Open-source libraries like OpenCV and dlib provide the tools needed for face detection and recognition. Machine learning models can be trained on a dataset of faces to ensure accurate recognition.

Figure 3 The smart security application or system interfaces

2.3 Face Recognition

The methodical approach used in the development and implementation of the smart security system with integrated face recognition and object detection includes 1) requirement analysis, which collects information about the required features and functionalities of the smart security system, defines the hardware and software requirements, including performance metrics like detection accuracy, response time, and power consumption. 2) system design, which is based on the requirements analysis and comprises choosing the right technologies and algorithms for face recognition and object identification in addition to specifying the system's components, interfaces, and interactions. 3) data collection and

preprocessing to gather and prepare the data required for training and testing models, which guarantee quality and consistency. Collecting images and videos of faces from various sources such as publicly available datasets and custom recordings and gathering images and videos of common objects in the targeted environment (e.g., vehicles, packages) from sources like custom datasets. Labeling the collected data with appropriate tags (e.g., bounding boxes for faces and objects) using annotation tools. Applying transformations such as rotation, scaling, and brightness adjustments to increase the diversity of the dataset improves model robustness and standardizes the image sizes and pixel values to ensure consistency. 4) model training, in which the machine learning models for face and object detection. Using algorithms like Multi-task Cascaded Convolutional Networks for initial face detection. Using deep learning frameworks like TensorFlow and employing deep learning models for feature extraction and recognition, splitting the dataset into training validations and test sets, and training the models using techniques like transfer learning, starting from pre-trained weights and fine-tuning on my specific dataset. 5) feature encoding and matching, in which the system encodes the extracted facial features into a compact representation known as a face embedding or descriptor. To find comparable faces, these embeddings are compared with those kept in a database using similarity metrics such as cosine similarity or Euclidean distance for setting a threshold to determine matches and non-matches [21] and use the trained face recognition model to extract feature vectors (embeddings) from detected faces. 6) database management, managing the storage and retrieval of facial embeddings and identities. Using a robust system (e.g., MySQL) depending on the scale of the application. Storing facial embeddings, identities, and metadata (e.g., timestamps, image paths). 7) real-time identification and verification, capturing live video feeds from cameras and process frames in real-time using the trained models. Identifying recognized faces and objects, and triggering alerts or actions if unknown or suspicious entities are detected. The system authenticates after identification and then either grants access or sets off notifications under pre-established regulations. 8) integration and testing, which verify the system's robustness, functionality, and performance under varied circumstances, the trained models are integrated into the framework of the smart security system along with other parts like cameras, Internet of Things (IoT) devices, and the mobile application. Conducting intensive testing in both controlled and real-world environments. Test for different scenarios, lighting conditions, and angles to ensure robustness. In low-light or nighttime, cameras may struggle

to capture clear and detailed images, which can hinder the accuracy of object detection algorithms. The lack of sufficient light can cause images to appear grainy or dark, making it difficult for the system to differentiate between objects, identify edges, or recognize patterns. The cameras include an IR cut filter with an auto-switch mechanism which can enhance image quality in darkness and algorithms will be optimized for low-light performance to improve detection accuracy during nighttime conditions. 9) implementation and assessment, which completed system is implemented in residential properties, which are real-world settings. Continuously monitor system performance, including detection accuracy, response time, and user interactions. The accuracy of face and object detection in our system is significantly influenced by the distance between the camera and the monitored objects. At close distances (0.5 to 2 meters), the cameras capture high-detail images, ensuring precise recognition, though extreme close-ups may cause distortion. Medium distances (2 to 5 meters) provide a balanced view, maintaining high accuracy with clear and identifiable features. At longer distances (5 to 10 meters), the detail reduces, leading to moderate accuracy as environmental noise increases. Beyond 10 meters, significant detail loss and environmental factors like lighting and obstructions further decrease detection reliability, making accurate recognition challenging. Optimal camera placement, high-resolution sensors, and advanced algorithms are essential to mitigate these issues and maintain accuracy across varying distances. In a controlled test, the system was tasked with detecting a person's face 50 times. The results were impressive, achieving a 100% accuracy rate, meaning that every instance of face detection resulted in the corrected identification of the individual.

The system employs the camera module to detect and recognize faces in its field of view. Once faces are detected (shown in Figure 4), the system employs a trained machine-learning model to compare the captured face with stored facial features of members in the home. If a match is found, access is granted; otherwise, appropriate actions, like sending alerts, can be triggered. In the event of an unauthorized person attempting to enter the premises, the system captures the intruder's face and promptly sends the image to the user's mobile phone. This real-time notification ensures swift awareness and response to potential security threats (shown in Figure 5).

Figure 4 Face detection and recognition

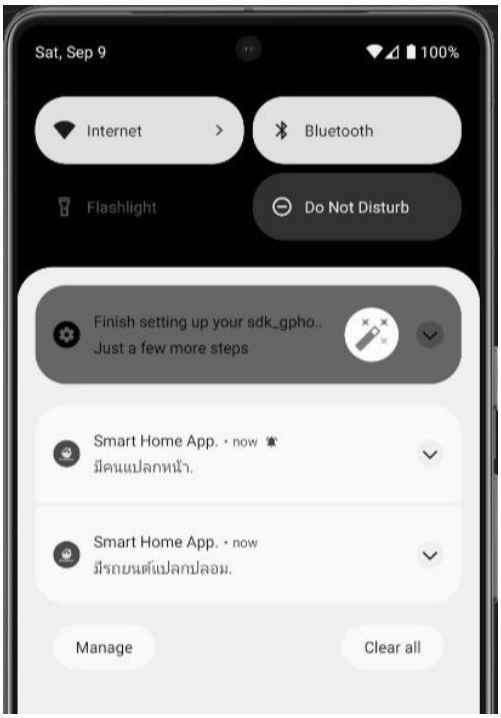

Figure 5 Real-time notifications

2.4 User Management

The system can be programmed to manage authorized users. New users can be enrolled by capturing their images and adding them to the database. Parallelly, the system provides users with the capability to remotely control electric devices within the home. The owner can operate electric devices with the help of their smartphone or other mobile device. This study represents a simple system where the Raspberry Pi3 controls three electronic devices such as lighting, air conditioning, and outlet using a relay (shown in Figure 6). Through the application or system interface, users can turn on or off specified devices, offering not only security but also enhanced energy management and convenience.

Figure 6 The interface for controlling electric devices

3. Conclusions

This Smart Security System on Raspberry Pi3 represents an innovative approach to residential security, combining facial recognition, object detection, and remote device control. These integrated features aim to provide users with comprehensive and user-friendly home security solutions. The study's success is contingent on user feedback that serves as a crucial indicator of the system's effectiveness in meeting these aims. By analyzing user responses (shown in Figure 7), the research aims to gauge the system's usability, reliability, and overall contribution to home security and automation.

The following are the key takeaways from the user feedback: 1) System performance evaluation, the main goal of user feedback is to assess how well the smart security system performs in practical situations. by requesting input on a range of topics, including ease of use, efficacy in detecting intrusions, dependability in object identification, and practicality in controlling devices remotely. 2) Evaluation of user experience, evaluating the user experience that the smart security system offers is one of the main goals of the user feedback. User perceptions of the system's usability, compatibility with daily activities, and notification response time. 3) Validation of research hypotheses, in addition, user input confirms the research goals and hypotheses that guided the creation and implementation of the smart security system. Researchers can determine the system's effectiveness in accomplishing its goals and providing value to users by contrasting users' perceptions and experiences with the system's planned outcomes.

On the user feedback gathered from the questionnaire, the following conclusions can be drawn: 1) Moderate User-Friendliness, the average response for user-friendliness is 4.35 indicating a moderate level of user-friendliness. It falls within a range where improvements or refinements may enhance the overall user experience. 2) Positive Perception of Intruder Detection, users express a positive perception of the system's effectiveness in intruder detection with an average response of 4.62. This suggests that the face recognition feature successfully identifies potential intruders contributing to a sense of security among respondents. 3) High Reliability in Object Detection, the system's reliability in detecting and capturing images of objects receives positive feedback with an average response of 4.58. This indicates that users find the object detection feature dependable contributing to effective surveillance around the home. 4) Moderate Convenience in Remote Device Control, users rate the convenience of the remote device control feature moderately with an average

response of 4.38. While the system provides a degree of convenience. There may be areas for improvement to further enhance the user's experience in controlling electronic devices remotely. 5) Positive Perception of Notification Response Time. The system's notification response time receives positive feedback with an average response of 4.62. Users appreciate the system's promptness in sending notifications contributing to a timely awareness of security events. 6) Moderate Integration with Daily Routine. The integration of the smart security system into users' daily routines is perceived moderately with an average response of 4.50. This suggests that the system is making strides in becoming a seamless part of users' lives. There may be opportunities for further integration. And 7) Positive Overall Satisfaction. The overall satisfaction with the smart security system is positive with an average response of 4.62. Users express contentment with the system indicating that it successfully meets their expectations and contributes positively to their sense of security.

In summary, the smart security system on Raspberry Pi with face recognition and object detection is generally well-received by users. The system demonstrates effectiveness in intruder and object detection with positive feedback on notification response time. While there are areas for improvement, particularly in user-friendliness and convenience in remote device control, the overall satisfaction level suggests that the system is meeting user expectations and contributing positively to their security and daily routines.

The benefits of the system are as follows; 1) Enhanced security that offers a robust authentication method that is difficult to forge, providing a higher level of security compared to traditional methods like PINs or keys. 2) Convenience-authorized users can access secured areas without the need for physical keys or remembering complex passwords. 3) Real-time alerts. The system can be programmed to send real-time alerts via notifications to the owner’s smartphone when unauthorized access is detected. 4) Data logging. The system can maintain logs of all access attempts, providing a record of who entered the premises and when. 5) Remote monitoring. Raspberry Pi-based systems can be accessed remotely, allowing homeowners to monitor their property even when they are away. And 6) Remote control of electric devices. The system provides users with the capability to remotely control electric devices within the home via the application or system interface.

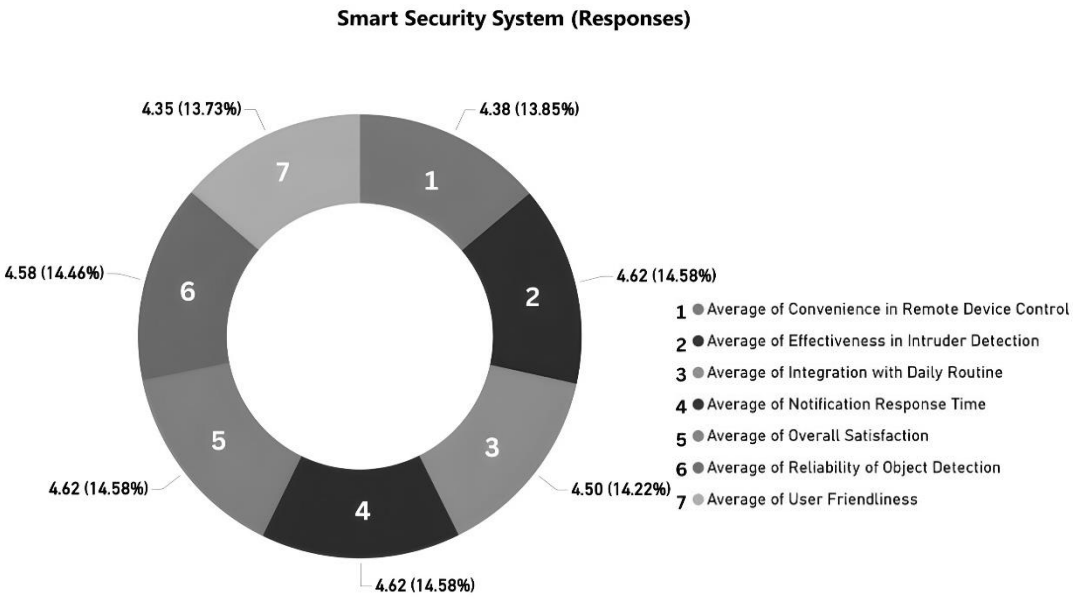

Figure 7 The user feedback gathered from the questionnaire

4. Discussion

The proposed smart security system on Raspberry PI with integrated face recognition and object detection offers several unique aspects and improvements that differentiate it from existing commercially available systems. While features such as face recognition, object detection, and remote device control are indeed common in various security systems, this research aims to innovate and improve upon these functionalities in several key areas:

1) Open-Source and Customizability. The proposed system leverages open-source software and libraries, such as Open-CV for computer vision and TensorFlow for machine learning. This open-source allows developers to customize and extend the system according to their specific needs, offering a level of flexibility and adaptability. 2) Cost-Effectiveness and Accessibility. Utilizing the Raspberry PI as the core platform significantly reduces the cost of the system compared to proprietary hardware solutions. 3) Enhanced Privacy and Data Security. The system can be configured to process data locally on the Raspberry PI minimizing the need to transmit sensitive data to external servers. This local processing is unauthorized access common with cloud-based commercial systems. 4) Integration of Multiple Functionalities on a Single Platform. This integration ensures coherent interaction between different functionalities, optimizing system performance and user experience. While

many commercial systems offer integrating features seamlessly on a single Raspberry PI platform is a notable achievement. 5) Scalability and Expandability. The design of the system allows for easy scalability and expandability. Users can add more cameras, sensors, and devices as needed without significant reconfiguration. And 6) User-Centric Design and Feedback Loop. By actively engaging with users and iteratively improving the system based on real-world usage and feedback, the proposed system aims to provide more user-friendly and effective solutions tailored to the specific needs of its users.

These unique aspects collectively contribute to a comprehensive and innovative security solution that addresses the limitations of current commercial systems and meets the evolving needs of users. It also faces certain limitations that may impact its overall performance and reliability such as 1) Accuracy in Face and Object Detection. Face recognition and face matching were conducted using the OpenCV image processing library. For face recognition, a classifier that uses the Harr features-based cascade function is used to identify faces in real-time. The algorithm employs a series of classifiers trained on positive and negative images to detect facial features with high accuracy. It uses 30 images of each person with a tilted face angle to trim everything except the face and divide them into each person. For our experiment, the detection rate for one mage was 99.73%, and the detection rate for one sequence was 100%. The metric that is used to confirm an authorized person is the similarity score between the facial embeddings of the detected face and the stored embeddings of authorized individuals. The system calculates the similarity between the extracted feature vector and the stored feature vectors of authorized individuals using cosine similarity metrics. Distinguishing between a photo and a real person is crucial for preventing spoofing attacks in face recognition systems. We used liveness detection to determine if the face being captured by the camera is of a live person or a static image, and motion analysis was used to track head movements and facial feature shifts. The system is highly dependent on the quality of the trained models and the dataset used for training. While deep learning models (Convolutional Neural Networks or CNNs) are employed to enhance detection accuracy, the system may still experience challenges in correctly identifying faces and objects under various conditions. Factors such as low-resolution images, partial occlusions, and variations in lighting and angles can reduce the accuracy of detection and recognition. 2) Potential for False Positives and Negatives. The system may produce false positives (incorrectly identifying a non-threat as a threat) and false negatives (failing to identify an actual threat).

False positives can lead to unnecessary alerts and inconvenience for users, while false negatives pose a significant security risk by allowing unauthorized access or failing to detect suspicious activity. The balance between sensitivity and specificity is crucial, and fine-tuning this balance is an ongoing challenge. 3) Processing Power and Latency. While the Raspberry PI is a powerful and cost-effective platform, it has limited processing power compared to dedicated high-performance computing systems. Real-time processing of video feeds to face and object detection can be resource-intensive, potentially leading to latency issues. 4) Susceptibility to Environmental Factors. Environmental factors play a significant role in the performance of the face and object detection algorithm. Changes in lighting conditions, such as bright sunlight, shadows, or low light, can adversely affect the system's ability to accurately detect and recognize faces and objects. And 5) Limited Database Capacity. The system's capacity to store and manage the facial embeddings and identities in its database is limited by the storage and memory constraints of the Raspberry PI. As the number of recognized individuals increases, maintaining an efficient and fast database query process becomes challenging.

In conclusion, while the proposed system offers several benefits, it is important to acknowledge and address these limitations to enhance its reliability, accuracy, and overall user satisfaction. Continuous research, development, and user feedback will be essential in mitigating these challenges and improving the system's performance in real-world applications.

Acknowledgment

I would like to acknowledge and give my warmest thanks to Prof.Yusaku Fujii who invited me to join his team for a research collaboration at Gunma University, Japan. His guidance and sharing me in-depth in the security camera carried me to share the knowledge with my students and led us to produce this study. I would also like to give special thanks to Kiattisak Singthong and Titinan Engbunmeesakul (my students) as a collaborative study and led us to complete this study.

References

[1] Wilson PI, Fernandez J. Facial feature detection using haar classifiers. Journal of Computing Sciences in Colleges 2006;21:127-33.

[2] Qian RJ, Sezan MI, Matthews KE. A robust real-time face tracking algorithm. Proceedings of 1998 International Conference on Image Processing (ICIP98) vol. 1; 1998 Oct 7; Chicago, USA. Piscataway, USA: IEEE; 2002. p. 131-5.

[3] Do HM, Mouser C, Liu M, Shaeng W. Human-robot collaboration in a mobile visual sensor network. Proceeding of 2014 IEEE International Conference on Robotics and Automation (ICRA); 31 2014 May 31 - June 7; Hong Kong, China. Piscataway, USA: IEEE; 2014. p. 2203-8.

[4] Sheng W, Ou Y, Tran D, Tadesse E, Liu M, Yan G. An integrated manual and autonomous driving framework based on driver drowsiness detection. Proceeding of 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems; 2013 Nov 3-7; Tokyo, Japan. Piscataway, USA: IEEE; 2014. p. 4376-81.

[5] Tran D, Tadesse E, Sheng W, Sun Y, Liu M, Zhang S. A driver assistance framework based on driver drowsiness detection. Proceeding of 2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems; 2016 Jun 19-22; Chengdu, China. Piscataway, USA: IEEE; 2016. p. 173-8.

[6] Kundu T, Saravanan C. Advancements and recent trends in emotion recognition using facial image analysis and machine learning models. Proceeding of 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques; 2017 Dec 15-16; Mysuru, India. Piscataway, USA: IEEE; 2018. p. 1-6.

[7] Amit Y, Felzenszwalb P, Girshick R. Object detection. In: Ikeuchi K, editor. Computer Vision. Cham, Switzerland; Springer: 2021. p. 875-83.

[8] See J, Lee SW. An integrated vision-based architecture for home security system. IEEE Transactions on Consumer Electronics 2007;53(2):489-98.

[9] Ravishankar V, Vinod V, Kumar T, Bhalla K. Sensor integration and facial recognition deployment in a smart home system. Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications; 2021 Mar 28-29; Hyderabad, India. Singapore: Springer; 2022. p. 759-71.

[10] Hilbert M. Digital technology and social change: the digital transformation of society from a historical perspective. Dialogues in Clinical Neuroscience 2020;22:189-94.

[11] Usamentiaga R, Lema DG, Pedrayes OD, Garcia DF. Automated surface defect detection in metals: A comparative review of object detection and semantic segmentation using deep learning. IEEE Transactions on Industry Applications 2022;58:4203-13.

[12] Carranza-García M, Torres-Mateo J, Lara-Benítez P, García-Gutiérrez J. On the performance of one-stage and two-stage object detectors in autonomous vehicles using camera data. Remote Sens 2021;13:89.

[13] Lijima T, Takita A, Fujii Y. Try to improve safety and security by utilizing security cameras considering privacy protection which is led by the municipality. Proceedings of International Conference on Technology and Social Science 2017; 2017 May 10-12; Kiryu, Japan.

[14] Kato S, Takita A, Yoshiura N, Ohta N, Maru K, Ueda H, et al. Development of security camera with privacy protection and, social experiment using the security camera with privacy protection. Proceedings of the 4th IIAE International Conference on Industrial Application Engineering 2016; 2016 Sep 22-24; Tokyo, Japan. p. 356-9.

[15] Faisal F, Hossain SA. Smart security system using face recognition on Raspberry Pi. Proceedings of 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA); 2019 Aug 26-28; Island of Ulkulhas, Maldives.

[16] Wang F, Zheng R, Li P, Song H, Du D, Sun J. Face recognition on Raspberry Pi on MobileNetV2. Proceeding of 2021 International Symposium on Artificial Intelligence and its Application on Media; 2021 May 21-23; Xi'an, China. Piscataway, USA: IEEE; 2021. p. 116-20.

[17] Shivappriya SN, Priyadarsini MJ, Stateczny A, Puttamadappa C, Parameshachari BD. Cascade object detection and remote sensing object detection method based on trainable activation function. Remote Sensing 2021;13:200.

[18] Zhuang X, Kang W, Wu Q. Real-time vehicle detection with foreground‐based cascade classifier. IET Image Processing 2016;10(4):289-96.

[19] Archana R, Jeevaraj PSE. Deep learning models for digital image processing: a review. Artificial Intelligence Review 2024;57:11.

[20] Shin HC, Roth HR, Gao M, Lu L, Xu Z, Nogues I, et al. Deep convolutional neural networks for computer-aided detection: CNN architectures, dataset characteristics and transfer learning. IEEE Transactions on Medical Imaging 2016;35(5):1285-98.

[21] Wang L, Zhang Y, Feng J. On the Euclidean distance of images. IEEE Transactions on Pattern Analysis and Machine Intelligence 2005;27(8);1334-9.

Author's Profile

Asst.Prof.Sa-nga Songmuang: Vice-Dean for Administration Affairs and Student Affairs, Kasem Bundit University, Faculty of Science and Technology, 60 Romklao Road, Minburi District, Bangkok 10510, Thailand. E-mail: sa-nga.son@kbu.ac.th

Article History:

Received: February 19, 2024

Revised: October 3, 2024

Accepted: October 4, 2024