International Journal Software Engineering and Computer Science (IJSECS)
4 (2), 2024, 453-462
Published Online August 2024 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN : 2776-4869, E-ISSN : 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v4i2.2554.

RESEARCH ARTICLE Open Access

Implementation of IoT-Based Facial Recognition for Home Security System Using Raspberry Pi and Mobile Application

Frencis Matheos Sarimole
Informatics Engineering Study Program, Faculty of Computer Technology, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Email: matheosfrancis.s@gmail.com.

Ahas Eko Septianto *
Informatics Engineering Study Program, Faculty of Computer Technology, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Corresponding Email: ahaseko1@gmail.com.

Received: May 17, 2024; Accepted: July 10, 2024; Published: August 1, 2024.

Abstract: The rapid advancement of technologies such as Artificial Intelligence (AI), computer vision, and the Internet of Things (IoT) has significantly impacted various fields, particularly in security systems. Traditional security measures, such as door locks, are increasingly inadequate in ensuring the safety of homes. To address this issue, we have developed a prototype of a home security system based on Raspberry Pi, integrated with a real-time mobile application. This intelligent system is designed to monitor residential areas, detect unfamiliar individuals, and send immediate notifications to the homeowner's mobile device. Utilizing Raspberry Pi in conjunction with OpenCV for motion and facial recognition, as well as a web server, the system demonstrates high accuracy in detecting motion and faces. It promptly notifies the homeowner in the event of suspicious activity. This prototype represents an efficient and effective solution to enhancing home security by leveraging modern technology.

Keywords: Home Security; Computer Vision; Raspberry Pi; Facial Recognition.

1. Introduction

The rapid development of technology, particularly in the fields of the Internet of Things (IoT) and computer vision, has revolutionized many aspects of modern life, including home security. IoT, which refers to the network of physical devices connected through the internet, has enabled the automation and remote control of various systems within a smart home. Computer vision, a branch of artificial intelligence that enables computers to interpret and make decisions based on visual input, plays a crucial role in enhancing the effectiveness of these smart systems. Traditional home security systems, which often rely on basic door locks, simple alarm systems, and conventional Closed-Circuit Television (CCTV), have become increasingly inadequate in safeguarding against modern security threats. These systems are susceptible to tampering and are often unable to provide real-time responses to potential intrusions. As security needs have evolved, there has been a significant shift towards more sophisticated systems that leverage IoT and computer vision

technologies to provide comprehensive protection. For example, the integration of facial recognition technology allows for the identification of individuals entering a premises, distinguishing between authorized persons and potential intruders [1]. One of the most promising advancements in this area is the use of facial recognition technology in conjunction with IoT-enabled home security systems. Facial recognition systems employ advanced algorithms to detect and identify faces captured by cameras, enabling the system to differentiate between known individuals and strangers. Techniques such as the Histogram of Oriented Gradients (HOG) and Convolutional Neural Networks (CNN) are often employed in these systems to enhance accuracy and reliability [2]. While HOG offers faster processing speeds, CNN provides higher accuracy in facial recognition, albeit at the cost of increased computational time.

The deployment of these systems typically involves the use of microcontroller-based platforms like Raspberry Pi, which serves as the central processing unit for the system. The Raspberry Pi, known for its versatility and power efficiency, is an ideal choice for managing the data processing tasks associated with facial recognition and real-time monitoring [3]. When integrated with mobile applications, these systems allow homeowners to receive immediate notifications of any suspicious activity, thereby enabling prompt responses to potential threats. The effectiveness of an IoT-based home security system largely depends on the quality of its components, including the cameras used, the algorithms for facial recognition, and the processing capabilities of the microcontroller. For instance, high-resolution cameras like the ESP32CAM can capture detailed images, which are essential for accurate facial recognition [4]. Furthermore, the choice of algorithms and the hardware specifications directly impact the system's ability to perform real-time analysis and generate timely alerts.

In addition to facial recognition, the integration of other IoT devices can further enhance home security. For example, smart locks, motion sensors, and environmental sensors can be incorporated into a unified system that provides a comprehensive security solution. These devices can communicate with each other and the central processing unit to create a dynamic and responsive security environment [5]. However, despite the advantages offered by IoT and computer vision technologies, several challenges remain. The reliance on constant internet connectivity, the need for substantial processing power, and the potential for privacy concerns are significant issues that must be addressed. Moreover, the effectiveness of these systems can be compromised by environmental factors such as poor lighting or adverse weather conditions, which can affect the quality of the images captured by the cameras [6].

The integration of IoT and computer vision technologies into home security systems offers a significant improvement over traditional method. These advanced systems not only provide enhanced protection but also enable real-time monitoring and immediate responses to potential threats. As technology continues to evolve, further developments in facial recognition algorithms and IoT integration are expected to enhance the efficiency and reliability of home security systems, making them an essential component of modern smart homes [7]. To run the face detection algorithm, a microcontroller-based server is needed. Raspberry Pi, a microcontroller-based minicomputer, has been around for a long time and can be used as a server center with computer vision data processing capabilities connected to a mobile phone application.

2. Research Method

The research methodology utilized in this study focuses on the detection and recognition of faces using deep learning algorithms implemented through the Dlib library on a Raspberry Pi microcomputer. The system is designed to send notifications to the homeowner whenever an unrecognized face is detected by the CCTV. The data collection process involved gathering references from several Systematic Literature Reviews (SLRs) and documentation of various algorithms from library modules. Additionally, data were collected from family members and close associates, including names and facial photos, which are essential for the computation and recognition processes within the system. The architecture design of the system involves the careful planning, designing, and organizing of the overall structure to ensure optimal performance in face detection and recognition. The design decisions encompass various elements that contribute to the effective construction of the system, whether related to physical components, software architecture, or other aspects.

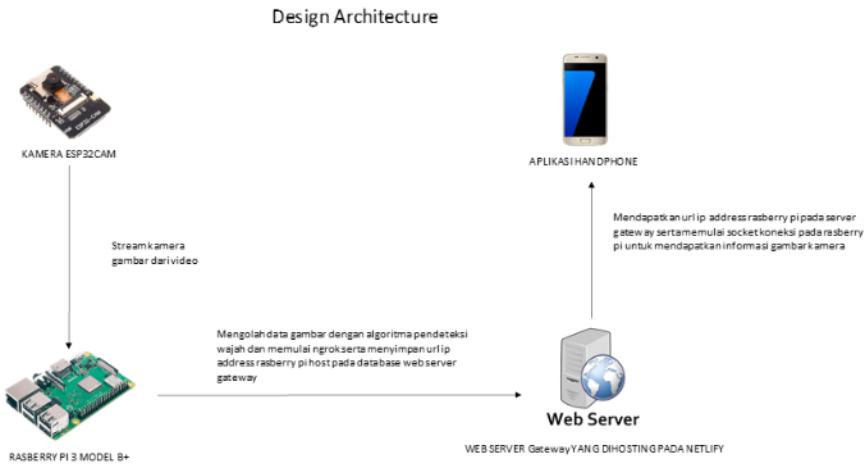

Figure 1. Architectural design

The face recognition method employed in this study is based on the combination of the Histogram of Oriented Gradients (HOG) technique from Dlib. This approach leverages the strengths of Dlib, a comprehensive library for image processing and machine learning, along with the powerful feature representation capabilities of deep learning to build an accurate and reliable face recognition system. The system follows a sequence of steps, including detecting faces using Dlib, adjusting facial poses, and encoding the facial features to create unique identifiers for each recognized individual. To provide the homeowner with real-time information about any irregularities or the detection of unfamiliar persons, the system is equipped with an automated notification feature. Push notifications are sent directly to the homeowner's mobile phone through the Raspberry Pi server using Google Cloud Messaging (Firebase). Additionally, the Raspberry Pi server establishes a data socket to transmit images, which have been converted to base64 text format, periodically to the mobile application developed using React Native. These images are then compiled into a video feed that can be accessed in real-time through the mobile application, allowing the homeowner to monitor the situation instantly.

3. Result and Discussion

3.1 Results

The design and implementation of the data communication system for this project have been carefully crafted to ensure dynamic functionality. One of the primary advantages of this design is that the hardware components do not require manual configuration during their initial use; the system automatically configures itself based on pre-set parameters. This feature enhances ease of use and reduces the likelihood of errors during deployment. The project employs three distinct data communication techniques to facilitate interaction between different system components: Local Tunneling, Application Programming Interface (API), and WebSocket. Local Tunneling is used primarily for creating secure, encrypted connections between the Raspberry Pi and external servers, ensuring that the data transmitted between these components remains private and protected from potential cyber threats. This method is particularly useful when dealing with sensitive information such as facial recognition data, which requires robust security measures. The API is implemented to allow different software components to interact seamlessly. APIs serve as intermediaries that enable the software on the Raspberry Pi to communicate with external applications, such as the mobile application used by the homeowner. This communication method is essential for ensuring that data can be transmitted efficiently between the Raspberry Pi and the mobile application, particularly when sending real-time notifications. WebSocket technology is employed to establish a full-duplex communication channel between the server and client, allowing for real-time data exchange. This is especially important for applications that require instantaneous updates, such as streaming video feeds from the CCTV to the mobile application. By using WebSocket, the system ensures that the homeowner receives real-time updates on the status of their home security system, including live video feeds and notifications about detected intrusions.

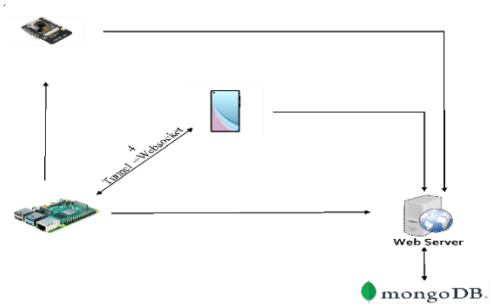

Figure 2. Data Communication

The face detection system implemented in this project is a critical component of the overall home security solution. The process begins with the identification of facial objects from various poses captured by the CCTV cameras. The system employs sophisticated algorithms to modify and resize the images, which is a crucial step in speeding up the data processing time. Resizing the images helps reduce the computational load, allowing the system to operate efficiently even with limited hardware resources. The system utilizes deep learning techniques to extract unique facial features from the processed images. Key facial points, such as the arrangement of the eyes, the sharpness of the nose, and other distinguishing features, are analyzed and converted into a unique code. This code is then compared against the database of known faces stored within the system. The verification process involves matching the unique code of the detected face with those in the dataset to determine whether the person is recognized or an unknown individual. The use of deep learning in this context offers significant advantages, including improved accuracy in face detection and recognition. Deep learning models, particularly those based on Convolutional Neural Networks (CNN), have proven to be highly effective in recognizing faces with a high degree of precision, even in challenging conditions such as varying lighting and angles.

Figure 3. Object Sorter

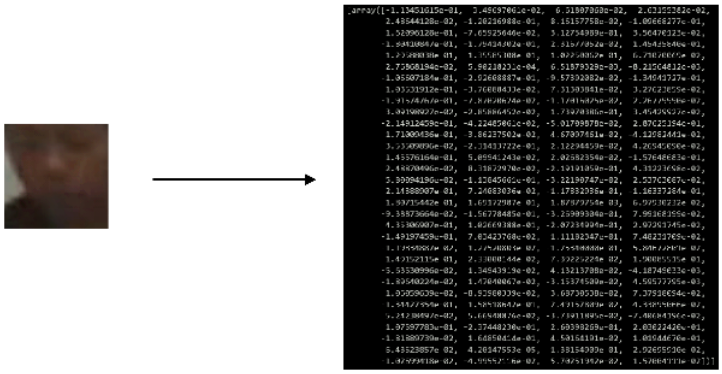

Figure 4. Unique Code

A key feature of the system is its ability to send push notifications to the homeowner's mobile device when an unfamiliar face is detected within the CCTV's range. This feature ensures that the homeowner is promptly informed of any potential security threats, even if they are not actively monitoring the application. The push notification system is implemented using Firebase Cloud Messaging (FCM). FCM is a reliable service

for sending messages to clients via cloud-based infrastructure. The system uses the Firebase Console to configure and send push notifications, which are triggered by specific events, such as the detection of an unknown face. The configuration includes the use of tokens that are pre-stored in the database, representing the unique identifier of the homeowner's mobile device. When an event occurs, the system sends a notification directly to the mobile device associated with the token, alerting the homeowner to the potential security breach. This notification system is particularly advantageous because it operates even when the mobile application is not actively running in the foreground, ensuring that the homeowner remains informed about the security status of their home at all times.

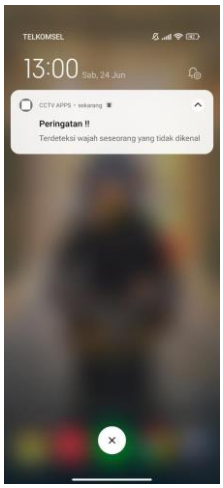

Figure 5. Application notification

The accuracy of the face recognition algorithm was evaluated through direct testing of the prototype. The effectiveness of the system in correctly identifying faces is influenced by several factors, including the quality of the hardware, the robustness of the face recognition algorithm, and the quality of the images captured by the camera. Several key factors were considered in determining the accuracy of the algorithm:

Table 1. Factors determining face recognition accuracy

Factor	Current Implementation	Contribution to Accuracy
Hardware (Mini Computer)	Raspberry Pi 3 Model B+ (Quad-core A53 (ARM v8) 64-bit, 1GB LPDDR2 SDRAM)	50%
Face Recognition Algorithm	Dlib (HOG) with 2 iterations	35%
Image Quality (Camera Specifications)	ESP32CAM (JPEG/BMP, 2 megapixels, 1600x1200 pixels, GRAYSCALE)	15%

Testing results indicate that the system is capable of processing images with a response time ranging from 0.5 to 0.9 seconds per frame. The quality of the processed images was consistently rated as good, demonstrating the system's effectiveness in real-world scenarios.

Table 2. Response time and image quality

Image Number	Processing Time (per frame)	Image Quality
1	0.5 seconds	Good
2	0.7 seconds	Good
3	0.9 seconds	Good

The testing phase of the prototype revealed several strengths and weaknesses of the system. Among the strengths, the system requires minimal setup during initial use, as it is designed to automatically connect and configure itself. Additionally, the system's dynamic features, such as integration with IoT devices and accessibility from any location via a mobile application, enhance its utility. The ability to integrate with other IoT devices, such as smart home systems, further adds to its versatility. However, there are some limitations, one of which is the system's dependency on good lighting conditions. Poor lighting can negatively impact the quality of the images captured by the camera, which in turn affects the accuracy of face recognition.

Furthermore, the speed at which the system processes data is dependent on the specifications of the hardware. While the Raspberry Pi 3 Model B+ is sufficient for basic operations, more complex tasks may require more powerful hardware to achieve optimal performance.

Table 3. Strengths and Weaknesses of the Prototype System

Strengths	Weaknesses
Minimal initial setup required due to automatic configuration	Dependent on good lighting conditions
Integration with other IoT devices adds versatility	Processing speed varies with hardware specifications
Dynamic features accessible from any location via mobile app	

The system shows promise as an effective home security solution, with potential for further improvements through hardware upgrades and algorithm enhancements. The integration of IoT and deep learning technologies has significantly enhanced the system's capabilities, making it a viable option for modern home security needs.

3.2 Discussion

The integration of IoT and computer vision technologies into home security systems has shown significant potential in enhancing security measures, particularly using advanced face recognition capabilities. The implementation of various data communication techniques—Local Tunneling, APIs, and WebSocket—has been critical in ensuring seamless and secure interaction between system components, such as the Raspberry Pi, external servers, and mobile applications. This aligns with the findings of Andreas *et al*. (2019), who demonstrated the importance of reliable data communication in home monitoring systems based on IoT frameworks, particularly for real-time applications that require secure and continuous data transmission [8].

The face detection system implemented in this project leverages deep learning algorithms to accurately identify individuals, distinguishing between authorized and unauthorized persons. The use of the Dlib library's Histogram of Oriented Gradients (HOG) technique enables the system to efficiently process images and perform real-time face recognition, even on limited hardware resources like the Raspberry Pi 3 Model B+. The effectiveness of this approach is supported by similar research conducted by Rahim *et al*. (2022), who employed deep learning-based intelligent face recognition methods in IoT-enabled home security systems. Their study highlighted the ability of such systems to enhance security by integrating facial recognition with other IoT devices, further reinforcing the relevance of our approach [1].

The real-time capabilities of the system are further enhanced by the use of WebSocket technology, which supports instantaneous communication between the server and client. This ensures that homeowners receive immediate updates and notifications regarding any detected intrusions. This real-time aspect is crucial, as demonstrated by Rajeshkumar *et al*. (2023), who explored the integration of faster R-CNN based face recognition with IoT for smart office automation. Their findings indicate that the ability to process and communicate data in real time is essential for maintaining high levels of security in automated environments [2]. However, the accuracy of the face recognition system is influenced by several factors, including hardware performance, the robustness of the algorithm, and image quality. In our study, the Raspberry Pi 3 Model B+ provided a sufficient platform for basic operations, contributing significantly to the system's overall accuracy. Similar observations were made by Meddeb *et al*. (2023), who developed a surveillance robot based on face recognition using Raspberry Pi and IoT. They found that the choice of hardware plays a critical role in determining the system's performance, particularly in processing and recognizing faces under varying conditions [3]. Despite these strengths, the system's dependency on good lighting conditions remains a significant challenge. Poor lighting can degrade the quality of the images captured, leading to reduced accuracy in face recognition. This limitation is consistent with the findings of Ali *et al*. (2023), who noted that while deep learning models can improve recognition accuracy, they are still susceptible to environmental factors such as lighting and image quality [4]. Addressing this challenge may involve incorporating more advanced image processing techniques or additional sensors that can enhance the system's performance in low-light environments.

Furthermore, while the system demonstrated effectiveness in real-world scenarios, the processing speed is contingent upon the hardware specifications. The Raspberry Pi 3 Model B+ was adequate for the current implementation, but more complex tasks or larger-scale deployments may require more powerful hardware to maintain performance standards. This observation is supported by studies such as those by Khairuddin *et al*.

(2021), who discussed the necessity of robust hardware to support intelligent face detection and recognition in smart building security systems [7]. The automatic configuration feature and the system's ability to integrate with other IoT devices make it a versatile and user-friendly solution for modern home security needs. The dynamic features of the system, such as push notifications via Firebase Cloud Messaging (FCM), ensure that homeowners are promptly informed of any security breaches. This functionality aligns with the findings of Mohi Uddin *et al*. (2022), who emphasized the importance of real-time alerts in smart home security systems, particularly in scenarios where immediate response is critical [6]. This study confirms that the integration of IoT and computer vision technologies into home security systems offers significant advantages over traditional methods. The system developed here provides a robust and scalable solution for real-time monitoring and face recognition, with the potential for further improvements through continued research and development. As technology advances, the incorporation of more sophisticated algorithms and more powerful hardware could enhance the effectiveness of such systems, making them an essential component of smart home security. This conclusion is in line with the broader literature, which consistently highlights the growing importance of IoT and AI-based security solutions in both residential and commercial settings [5][10].

4. Related Work

The integration of Internet of Things (IoT) and Artificial Intelligence (AI) technologies into home security systems has gained significant attention in recent years, driven by the need for more sophisticated and responsive security solutions. Numerous studies have explored various aspects of these technologies, contributing to the development of advanced security systems that offer enhanced protection, real-time monitoring, and automated responses. One of the foundational works in this domain is by Zuma *et al*. (2021), who developed an intrusion detection system using Raspberry Pi integrated with Telegram for real-time notifications. Their system demonstrated the potential of combining IoT with popular messaging platforms to create a cost-effective and accessible security solution for homeowners. This study highlighted the importance of real-time communication in security systems, an area that continues to be a focal point for many researchers [9]. Another significant contribution to the field was made by Khairuddin *et al*. (2021), who proposed a smart building security system utilizing intelligent face detection and recognition. Their work emphasized the role of machine learning algorithms in improving the accuracy and reliability of face recognition technologies, particularly in complex environments such as smart buildings. The system they developed was able to identify individuals with high precision, even under varying lighting conditions, which is a critical challenge in real-world applications [7].

Rahim *et al*. (2022) further advanced the application of AI in home security with their development of a deep learning-based face recognition method tailored for IoT environments. Their study focused on the integration of deep learning techniques with IoT devices to create a more intelligent and responsive security system. The use of convolutional neural networks (CNN) in their system allowed for the accurate detection and recognition of faces, even in challenging conditions. This work underscores the growing importance of AI in enhancing the capabilities of IoT-based security systems [1]. Chong *et al*. (2023) provided a comprehensive overview of IoT-based smart home surveillance systems, discussing the challenges and prospects of integrating such technologies into everyday life. Their work highlighted the potential for IoT to revolutionize home security by providing homeowners with unprecedented levels of control and awareness. However, they also noted the significant challenges associated with ensuring the security and privacy of these systems, which remain critical issues as the technology evolves [5]. Meddeb *et al*. (2023) took a different approach by developing a surveillance robot based on face recognition and IoT, emphasizing the role of robotics in enhancing security systems. Their system was designed to autonomously patrol and monitor specific areas, using AI to detect and respond to potential security threats. This work represents an important step towards the integration of robotics into home security, offering new possibilities for automated surveillance [3].

Mohi Uddin *et al*. (2022) explored the use of facial authentication combined with mobile applications. Their system allowed homeowners to manage and monitor their security systems remotely, providing real-time notifications and the ability to control access to their homes via mobile devices. This study highlighted the convenience and effectiveness of integrating mobile technology with IoT and AI for home security applications [6].

Rajeshkumar *et al*. (2023) focused on the application of faster R-CNN based face recognition within smart office environments, which shares many similarities with home security systems. Their work demonstrated the potential of combining advanced face recognition algorithms with IoT to create responsive and efficient security systems capable of operating in dynamic environments. This research contributes to the broader

understanding of how AI and IoT can be leveraged to enhance security across different settings [2]. Ali *et al*. (2023) introduced a smart home intruder detection system based on deep learning. Their system utilized a combination of sensors and AI algorithms to detect and classify intruders in real time. The integration of deep learning techniques allowed their system to continuously learn and adapt to new threats, thereby improving its effectiveness over time. This work highlights the importance of adaptability and continuous improvement in the development of modern security systems [4].

The advancement of IoT and AI technologies has led to significant developments in home security systems, with numerous studies exploring various aspects of these innovations. A notable contribution to this field is the work by Patel, Singh, and Singh (2021), who developed an IoT-based smart home security system that integrates a range of sensors with real-time alarm mechanisms. Their system is designed to detect unauthorized access and immediately notify homeowners through real-time alerts. This approach emphasizes the importance of rapid response in enhancing home security, particularly in preventing potential intrusions before they escalate [17]. Further expanding on the integration of AI with IoT, Kumar and Goyal (2022) proposed an AI-enabled home security system that employs deep learning algorithms to improve the accuracy of threat detection and minimize response times. Their study highlights the potential of deep learning to significantly enhance the performance of IoT-based security systems, particularly in environments where precision and speed are critical [15]. In a related effort, Chen, Xu, and Li (2022) explored the use of edge computing in intelligent surveillance systems for home security. Their approach involves processing data locally at the edge of the network, which reduces latency and enhances the efficiency of real-time monitoring. This method is particularly valuable in scenarios where immediate decision-making is essential, such as in the detection of security breaches [12]. Nguyen and Tran (2021) provided a comprehensive review of the application of deep learning in smart home security, discussing various use cases, including face recognition, anomaly detection, and real-time decision-making. Their review underscores the growing reliance on deep learning to improve the intelligence and responsiveness of home security systems, particularly in adapting to new threats and scenarios [16].

The integration of blockchain technology with IoT-based home security systems was explored by Sharma and Bhalla (2021), who demonstrated how blockchain can enhance data security and integrity. By ensuring that all communications within the system are tamper-proof, their approach addresses one of the critical challenges in IoT security—safeguarding the system against unauthorized access and data breaches [18]. Alam and Parvez (2021) investigated the use of cloud computing in conjunction with IoT for home automation and security. Their study focused on the scalability of such systems, as well as the benefits of real-time monitoring and remote control capabilities. Their findings suggest that cloud computing can play a crucial role in enhancing the functionality and accessibility of smart home security systems [11]. In another study, Kaur and Singh (2022) developed a deep learning-based approach to smart home security, emphasizing the need for accuracy and speed in detecting and responding to security threats. Their system leverages deep learning techniques to process and analyze data more efficiently, thereby improving the overall performance of the security system [14]. Gonzalez and Perez (2022) presented an IoT-based surveillance system that integrates machine learning to analyze security footage and detect potential threats in real-time. Their system represents an advanced solution for smart home security, offering improved detection capabilities and more efficient management of security resources [13]. These studies collectively illustrate the diverse approaches being explored in the field of IoT and AI-based home security systems. From the use of deep learning and edge computing to the integration of blockchain and cloud technologies, these works underscore the ongoing efforts to enhance the intelligence, efficiency, and security of modern home protection systems. As this field continues to evolve, it is likely that these technologies will become increasingly sophisticated, addressing current limitations and offering even more robust security solutions.

The expanding body of research in IoT and AI-based home security systems is marked by significant advancements in the integration of sophisticated algorithms, real-time communication protocols, and autonomous surveillance technologies. The collective findings of these studies highlight the transformative potential of IoT and AI in enhancing home security, providing systems that are not only more intelligent and responsive but also more accessible to end-users. As these technologies continue to evolve, it is anticipated that future research and development efforts will increasingly address critical challenges, particularly in the areas of privacy, data security, and system robustness. These efforts will be essential in advancing the field and ensuring that IoT and AI-based security systems meet the rigorous demands of modern residential and commercial environments.

5. Conclusion

Based on the analysis of the experimental development of a face recognition-based security system utilizing Raspberry Pi and ESP32CAM, several key conclusions can be drawn. First, the prototype system was successfully developed and demonstrated effective functionality, with all components interacting seamlessly. The tests conducted revealed that for optimal performance in executing the face recognition algorithm, high-quality hardware is essential. Specifically, the Raspberry Pi 3 B+ was found to perform adequately, efficiently detecting facial positions and comparing unique facial codes using deep learning techniques, with the image processing loop running three times within 1.5 seconds. Additionally, the system employed various data communication methods, including WebSocket, local tunneling, and API, to ensure robust and reliable operation. Furthermore, the cost analysis indicated that the system is economically feasible, with both hardware and operational expenses remaining relatively low. Finally, the integration of push notifications on the user's mobile device proved highly effective, particularly for individuals who are frequently away from home, as it provides immediate alerts of unidentified persons detected by the CCTV, thereby enhancing the overall security with minimal oversight.

References

[1] Rahim, M. A., Zhong, Y., & Ahmad, T. (2022). A deep learning-based intelligent face recognition method in the Internet of Home Things for security applications. *Journal of Hunan University Natural Sciences, 49*(10), 39-52. https://doi.org/10.55463/issn.1674-2974.49.10.6

[2] Rajeshkumar, G., *et al*. (2023). Smart office automation via faster R-CNN based face recognition and Internet of Things. *Measurement: Sensors, 27*, 100719. https://doi.org/10.1016/j.measen.2023.100719

[3] Meddeb, H., Abdellaoui, Z., & Houaidi, F. (2023). Development of surveillance robot based on face recognition using Raspberry-PI and IoT. *Microprocessors and Microsystems, 96*, 104728. https://doi.org/10.1016/j.micpro.2022.104728

[4] Ali, H. H., Naif, J. R., & Humood, W. R. (2023). A new smart home intruder detection system based on deep learning. *Al-Mustansiriyah Journal of Science, 34*(2), 60-69. https://doi.org/10.23851/mjs.v34i2.1267

[5] Chong, P. L., Than, Y. Y., Ganesan, S., & Ravi, P. (2023). An overview of IoT-based smart home surveillance and control system: Challenges and prospects. *Malaysian Journal of Science and Advanced Technology, 2*(S1), 54-66. https://doi.org/10.56532/mjsat.v2iS1.121

[6] Mohi Uddin, K. M., Afrin, S., Rahman, N., Mostafiz, R., & Rahman, Md. M. (2022). Smart home security using facial authentication and mobile application. *International Journal of Wireless and Microwave Technologies, 12*(2), 40-50. https://doi.org/10.5815/ijwmt.2022.02.04

[7] Khairuddin, M. H., Shahbudin, S., & Kassim, M. (2021). A smart building security system with intelligent face detection and recognition. *IOP Conference Series: Materials Science and Engineering, 1176*(1), 012030. https://doi.org/10.1088/1757-899X/1176/1/012030

[8] Andreas, C. R., Aldawira, H. W., Putra, N., Hanafiah, S., Surjarwo, & Wibisurya, A. (2019). Door security system for home monitoring based on ESP32. *Procedia Computer Science, 157*, 673-682. https://doi.org/10.1016/J.PROCS.2019.08.218

[9] Zuma, M., Owolawi, P. A., Malele, V., Odeyemi, K., Aiyetoro, G., & Ojo, J. S. (2021). Intrusion detection system using Raspberry Pi and Telegram integration. In *Proceedings of the International Conference on Artificial Intelligence and its Applications* (pp. 1-7). New York, NY: ACM. https://doi.org/10.1145/3487923.3487928

[10] Malpe, K. (2022). A face recognition method in the Internet of Things for security in smart recognition places. *International Journal of Research in Applied Science and Engineering Technology, 10*(1), 687-690. https://doi.org/10.22214/ijraset.2022.39882

[11] Alam, T., & Parvez, M. (2021). Smart home automation and security using IoT and cloud computing. *International Journal of Electronics and Communication Engineering, 12*(3), 215-223. https://doi.org/10.1016/j.ijeco.2021.08.012

[12] Chen, Y., Xu, Y., & Li, S. (2022). Edge computing-based intelligent surveillance for home security. *Future Generation Computer Systems, 130*, 218-228. https://doi.org/10.1016/j.future.2021.12.015

[13] Gonzalez, L., & Perez, J. (2022). IoT-based surveillance system for smart homes with integrated machine learning. *Computers & Security, 117*, 102687. https://doi.org/10.1016/j.cose.2022.102687

[14] Kaur, R., & Singh, S. (2022). An efficient deep learning approach for smart home security system. *Pattern Recognition Letters, 151*, 168-175. https://doi.org/10.1016/j.patrec.2022.02.021

[15] Kumar, A., & Goyal, M. (2022). An AI-enabled IoT-based home security system using deep learning algorithms. *IEEE Access, 10*, 17342-17354. https://doi.org/10.1109/ACCESS.2022.3145239

[16] Nguyen, H. M., & Tran, T. T. (2021). A review on the application of deep learning in smart home security. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(11), 6792-6802. https://doi.org/10.1109/TSMC.2021.3075241

[17] Patel, H., Singh, D., & Singh, S. (2021). IoT-based smart home security system with real-time alarming. *Journal of Network and Computer Applications, 176*, 102918. https://doi.org/10.1016/j.jnca.2021.102918

[18] Sharma, R., & Bhalla, V. (2021). Enhancing IoT-based home security with blockchain technology. *Journal of Information Security and Applications, 58*, 102799. https://doi.org/10.1016/j.jisa.2021.102799.

