Wireless Personal Communications (2024) 136:2185–2200
https://doi.org/10.1007/s11277-024-11371-1

Enhancing Smart Home Security Using Deep Convolutional Neural Networks and Multiple Cameras

Rishi Sharma[1] · Anjali Potnis[2] · Vijayshri Chaurasia[3]

Accepted: 11 June 2024 / Published online: 2 July 2024

Abstract

With the increasing use of smart homes and IoT devices, security has become a significant concern. This paper presents a method to enhance smart home security using Deep Convolutional Neural Networks (DCNN) and multiple cameras. In this approach, three cameras are used to capture images from different angles, and these images are analysed using DCNNs including VGG16, VGG19 and DenseNet to detect potential intruders. Known for their excellent performance in image classification, these DCNN models aim to improve the accuracy and efficiency of the security system, thereby reducing false alarms and missed detections. Additionally, the system allows authorized individuals to remotely disable the security system, increasing convenience and usability. The proposed method has shown significant improvement in human presence detection and facial recognition, achieving 99.79% accuracy in classifying home occupants and intruders. This performance is superior to alternative models such as SVM, KNN, and complex decision trees. This paper introduces a new method that integrates multiple cameras with DCNN to boost the performance of security systems.

Keywords Smart homes · Security · DCNN · Camera · Face recognition

1 Introduction

The proliferation of smart homes driven by technological advancements promises unprecedented convenience and comfort for residents. However, this surge in connectivity also raises serious concerns about security [1]. Traditional security measures like alarms and

✉ Rishi Sharma
rishiphd664@gmail.com

Anjali Potnis
apotnis@nitttrbpl.ac.in

Vijayshri Chaurasia
Vijayshree21@gmail.com

[1] EC Department, Ph.D. Scholar NITTTTR, Bhopal, India

[2] EC Department, Assistant Professor, NITTTR Bhopal, Bhopal, MP, India

[3] EC Department, Associate Professor, MANIT, Bhopal, India

single-camera setups often fall short of providing comprehensive coverage, leaving smart homes vulnerable to emerging threats [2].

As shown in Fig. 1, IoT-enabled security systems empower smart homes to ensure the safety of occupants, including children and the elderly. Real-time alerts and remote locking capabilities provide strong protection against potential intrusions [3]. Still, the popularity of smart homes has raised concerns about security and privacy. While IoT devices provide remote control over various home functionalities, they concurrently introduce vulnerabilities that malicious actors can exploit to compromise the integrity of the network [4].

In response to these challenges, this paper proposes an unprecedented solution to strengthen smart home security through the fusion of Deep Convolutional Neural Networks (DCNN) and multiple cameras [5]. This innovative approach addresses the shortcomings of existing systems in the following ways:

- Leveraging DCNNs, specifically VGG16, VGG19, and DenseNet, to increase accuracy and efficiency in intrusion detection and facial recognition [6].
- Integrating multiple cameras to broaden monitoring coverage and reduce inspection risk.
- Employing motion sensor detectors to trigger camera systems and enforce security protocols when human motion is detected.
- Developing a user-friendly interface to facilitate remote access control, enabling homeowners to manage entry permissions remotely.

Increasing the efficacy of the system by incorporating Arduino Uno to streamline communication between the burglar alarm and the computer system. In the scientific field, deep convolutional neural networks (DCNNs) have emerged as formidable assets in computer vision, especially in image recognition and classification tasks [7]. Their innate ability to autonomously learn hierarchical features from input data makes them ideally suited for tasks such as intrusion detection and facial recognition within smart home security systems.

In summary, our proposed approach presents a holistic solution to strengthen smart home security by harnessing the power of DCNN and multiple cameras. By overcoming the limitations of prevalent systems and introducing robust monitoring and access control mechanisms, our endeavor is to protect the well-being and privacy of smart home occupants.

Our methodology involves the integration of multiple cameras capturing images from different vantage points for comprehensive surveillance. The inclusion of DCNN increases

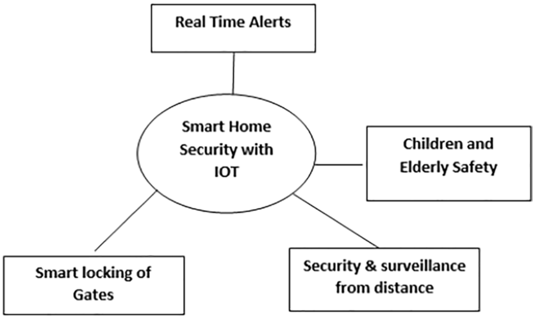
Real Time Alerts
Smart Home Security with IOT
Children and Elderly Safety
Smart locking of Gates
Security & surveillance from distance

Fig. 1 Smart home security with IoT

the accuracy of intrusion detection and facial recognition, thereby significantly increasing the effectiveness of the security system.

The envisioned system not only strengthens smart home security but also enhances convenience and utility. Remote disabling capabilities empower family members to manage the security system remotely, while Arduino Uno integration increases the system's efficacy in alerting residents of potential threats. Additionally, we will investigate the effectiveness of different DCNN models, such as VGG 16, VGG 19 and DenseNet, for our proposed system.

This paper demonstrates the amalgamation of DCNN and multiple cameras to present an effective security system for smart homes. The evaluation will be based on existing methods as well as metrics encompassing accuracy, efficiency and safety to highlight the advantages of our proposed approach. In summary, our effort demonstrates promising results and has the potential for further refinement and real-world application. The integration of DCNN and multiple cameras revolutionizes smart home security, ushering in a more reliable and comprehensive security paradigm.

2 Literature Review

The following section presents the compilation of some of the significant work already done in the area chosen for research by various researchers with its outcome and point of research. The review consists of the papers containing IoT and Convolutional neural networks.

The paper [8] presents a deep learning facial recognition system using the ArcFace model with MobileNet V2. It combines facial authentication and hand gesture recognition, allowing users to control their homes via mobile devices and connect with IoT technology. The system achieves 97% accuracy and 25 FPS, demonstrating effective real-time smart home operation.

The paper [9] outlines a technique for classifying traffic videos by converting them into images and using a color-coding scheme. Vehicles are detected with the YOLO algorithm, and the images are transformed into binary format. These are then processed by a deep convolutional neural network, achieving 98.2% accuracy on the UCSD dataset.

The paper [10] describes an IoT-driven smart home system utilizing wireless sensors, Wi-Fi, and an Android app for remote operation. It features real-time monitoring with alerts for fire and air quality, along with remote control of appliances such as fans and lights. Additionally, the system incorporates sensors for detecting gas leaks, temperature, and humidity to improve home security and automation.

The paper [11] presents an intelligent home automation system using IoT and deep learning to enhance security and control. It accurately distinguishes between intruders and home occupants using motion pattern recognition, achieving 99.8% accuracy with a CNN model. The system includes an ESP32 camera, PIR motion sensor, ESP8266 board, relay module, and DHT11 sensor for comprehensive home monitoring and automation.

The paper [12] introduces an advanced 3D convolutional network (A3DConvNet) for detecting abnormal human behavior in video sequences. It addresses the challenge of real-time detection in complex scenes like megastores/shops and achieves around 91% accuracy using a synthesized dataset containing activities like shoplifting, drinking, eating, and damaging.

The paper [13] explores the evolution of the Internet of Things (IoT) and its various applications, with a focus on smart homes. It emphasizes the importance of machine learning (ML) in enhancing smart home automation beyond basic remote control. The research proposes a taxonomy of ML applications in smart homes. Overall, the paper highlights the significance of ML in optimizing smart home systems for improved quality of life.

The paper [14] introduces an intelligent intrusion detection system (I-IDS) for IoT networks to detect and prevent attacks during data transmission. It employs machine learning models, including a Markov model, to distinguish normal and malicious activities. Overall, the proposed I-IDS enhances security in IoT environments effectively.

The paper [15] introduces the INDCNN-FDC model for fall detection among the elderly, leveraging deep learning and machine learning techniques. It employs two stages of data pre-processing and deep transfer learning with Inception v3 to generate feature vectors. Experimental results show the model's superiority over existing methods.

3 Problem Identification

With extensive survey of literature, it is observed and analyzed that limited research exists on smart homes consisting of multiple cameras for security and the scope of integration of deep convolutional neural networks and multiple cameras to improve smart home security is widely explored. Has not been discovered since.

3.1 Problem Statement

In the problem identification section of the paper, the authors outline the limitations of existing smart home security systems and the issues that motivated the proposed approach. Based on a literature survey, the following problems were identified:

- Current sensors can only detect humans when they are too close to the detector, leading to missed detections and false alarms.
- Most security systems rely on a single camera that can capture images from only one angle, limiting the monitoring capabilities of the system.
- If a person is known to the family but fails to pass the security check, he is unable to enter the house, causing inconvenience to family members.
- Existing systems do not allow family members to provide access to unknown persons from a distant location, thereby reducing the flexibility of the system.
- Image analysis in existing systems is not efficient, leading to errors in detecting and recognizing human presence.

Our proposed method will address all these research gaps and an effective and secure system for smart homes will be developed using deep convolutional neural networks to detect human presence and match captured images to the database. Three cameras would be deployed to capture images from different angles in place of a single camera (which is used in most research), and if the images match the database, the person would be allowed to enter the house. If not, a burglar alarm will sound, and photos of the intruder will be sent via email. Arduino Uno will be used in the system to connect the burglar alarm to the computer system. DCNN will be used to ensure that family members are not identified as intruders. Family members can remotely disable the security system if necessary.

4 Methodology

4.1 Deep Convolutional Neural Network (DCNN)

DCNN is a type of artificial neural network mainly used for computer vision tasks such as image and video recognition [16]. This network is designed to automatically extract and learn hierarchical features from input data, which are useful for a variety of tasks including classification, detection, and segmentation.

4.1.1 Layers of DCNN

- Convolutional layers: Apply learnable filters to the input image to generate feature maps.
- Pooling layers: Down sample feature maps, reducing their size while preserving important information.
- Activation functions: Introduce non-linearity into the model, enabling it to learn complex patterns.
- Fully Connected Layers: Transform the outputs of previous layers and make predictions about the input image.
- Output Layer: Produces the final output of the DCNN.

DCNNs are trained on large datasets to recognize patterns and objects within images. Once trained, they can classify new images and detect objects of interest, making them suitable for applications such as self-driving cars, medical diagnostics and facial recognition.

4.2 Architecture of DCNN

The architecture of DCNN consists of several key components:

- Input layer: Receives the input image.
- Convolutional layer: Applies filters to extract features from the input image.
- ReLU activation function: Introduces non-linearity in feature maps.
- Pooling layer: Reduces the dimensionality of the feature map while retaining important features.
- Convolution Layer: Converts the output of the final pooling layer into a 1D array.
- Fully Connected Layer: Transforms a 1D array to make predictions about the input image.
- Output layer: produces the final output.

In our proposed system, DCNN will analyze images from multiple cameras to detect human presence and recognize faces, increasing the accuracy and efficiency of the security system, while reducing false alarms and missed detections.

In the provided diagram (Fig. 2), the input undergoes processing through a convolutional layer, where a series of filters are applied to generate feature maps. Subsequently, the ReLU activation function adds nonlinearity to each element of these feature maps. Max pooling layers are employed to decrease the dimensionality of the feature maps while preserving crucial features. This sequence of operations repeats as necessary, with multiple

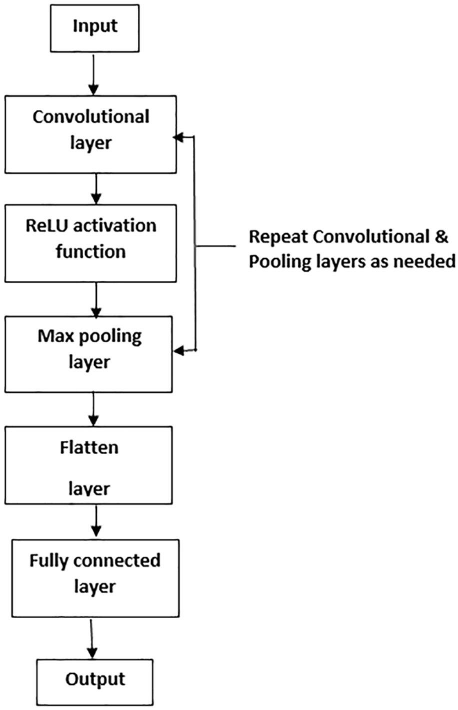

Fig. 2 Block diagram of DCNN architecture

convolutional and pooling layers working together to extract increasingly intricate features from the input. Following this, the flatten layer converts the output of the last pooling layer into a one-dimensional (1D) array. This 1D array is then forwarded to a fully connected layer, which conducts a linear transformation on the input data. Finally, the output of the fully connected layer passes through an output layer to yield the ultimate output of the Deep Convolutional Neural Network (DCNN).

4.3 Proposed Method

DCNN and multiple cameras are used in the proposed smart home security system. Its steps are as follows:

- Motion Detection: A motion sensor detects human motion.
- Image capture: Three cameras capture images from different angles.
- Image Analysis: DCNN processes the captured images.
- Database comparison: DCNN compares images to a database of known family members.
- Decision Making:

  - o If match is found: Grant access and allow the homeowner to remotely disable the system.
  - o If there is no match: Deny entry, activate the alarm, and send an alert to the homeowner.

This method ensures that only authorized persons can enter the house.

4.3.1 Flowchart of the Proposed Method

The flowchart in Fig. 3 describes the process of how a deep convolutional neural network (DCNN) and a multiple camera system can be used for enhancing smart home security. The process starts with the motion sensor detector detecting human motion. Once motion is detected, the three-camera system is activated, and the cameras capture images of the person from three different angles. These images are then input into the DCNN.

If the captured image matches with the database of authorized persons, the person is allowed to enter the home, and the process ends. However, if the captured image does not match with the database of authorized persons, the security system denies entry, and an alarm is triggered. The alarm can be disabled by the owner if the person is known to them. If the owner disables the security system, the person is allowed to enter the home, and the process ends.

In summary, this flowchart illustrates the use of a DCNN and multiple cameras in a security system that detects human presence and allows entry only to authorized persons, thereby enhancing smart home security. If the intruder is not known, he will not be allowed to enter the home and an email will be sent along with the burglar alarm to the user of the system. This greatly enhances the security of the home.

4.4 Algorithm

The proposed algorithm is designed for a home security system that uses a motion sensor to detect human motion. Once motion is detected, the three-camera system will activate and capture images of the person from three different angles. These images are then input into a deep convolutional neural network (DCNN) for analysis. If the captured image matches with the database, the person will be allowed to enter the home. The security system can be disabled remotely by the owner if needed. However, if the captured image does not match with the database, the person will not be allowed to enter the home and the burglar alarm will be activated. This algorithm uses DCNN to improve the accuracy of facial recognition and the integration of multiple cameras for more comprehensive surveillance. The use of Arduino Uno for connecting the burglar alarm with the computer system enhances the system's effectiveness in alerting the house members of potential intruders. The proposed algorithm also allows family members to disable the security system remotely if needed, improving convenience and usability.

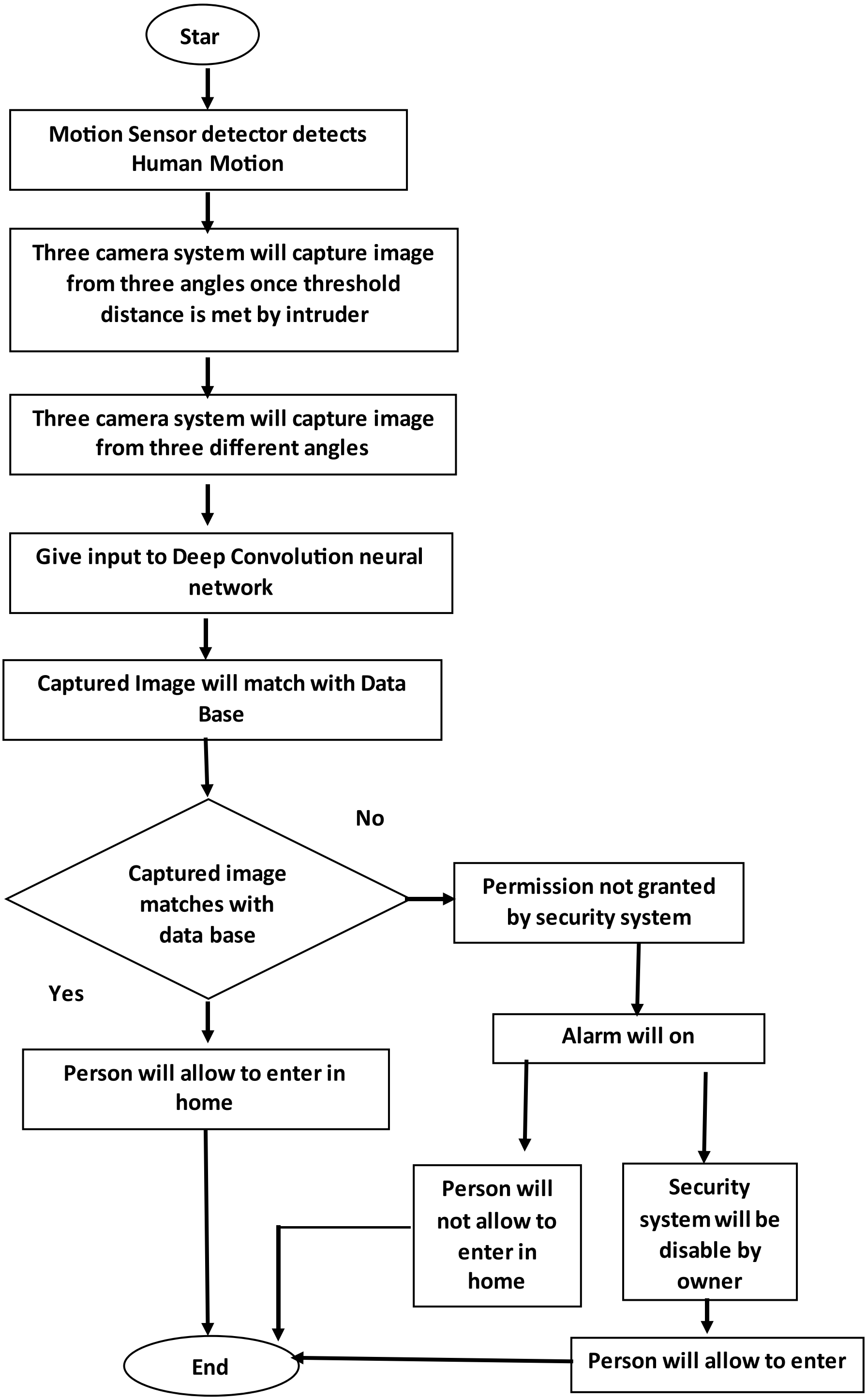
Star
Motion Sensor detector detects Human Motion
Three camera system will capture image from three angles once threshold distance is met by intruder
Three camera system will capture image from three different angles
Give input to Deep Convolution neural network
Captured Image will match with Data Base
Captured image matches with data base
No
Yes
Permission not granted by security system
Alarm will on
Person will allow to enter in home
Person will not allow to enter in home
Security system will be disable by owner
Person will allow to enter
End

Fig. 3 Flowchart of the proposed methodology

```
1. Start
2. Activate motion sensor detector
3. If human motion is detected, activate the three-camera system
4. For i in range (1,4):
     a. Capture image i using the three-camera system
5. Feed captured images as input to the DCNN
6. If captured images match with the database:
     a. Allow the person to enter the home
     b. If person is allowed, disable the security system by the owner
7. If captured images do not match with the database:
     a. Do not allow the person to enter the home
     b. Activate the alarm
8. End
```

This Algorithm outlines the steps to be taken to design a security system that utilizes a motion sensor detector and deep convolutional neural network (DCNN) to detect the presence of humans and grant or deny them access to a smart home.

The Algorithm begins by starting the system and activating the motion sensor detector. If the detector senses human motion, the three-camera system is activated to capture images of the individual from three different angles. These images are then fed as input to the DCNN.

If the captured images match the data in the security system's database, the individual is granted access to the smart home. If access is granted, the system is disabled by the owner. However, if the captured images do not match the database, the individual is not allowed to enter the home and an alarm is activated. The Algorithm ends once the security check is complete.

4.5 An Architecture for the Proposed Security System

This security system architecture utilizes a combination of motion sensor detectors, cameras, deep convolutional neural networks, databases, and Arduino Uno to create an efficient and reliable solution for securing homes. The architecture is composed of four main components: the motion sensor detector, three-camera system, deep convolutional neural network, and security system.

The motion sensor detector detects any human motion in the surrounding area, triggering the activation of the three-camera system to capture images from three different angles. These images are then fed into the deep convolutional neural network, which has been trained on a large dataset of facial recognition and human presence detection. The deep convolutional neural network analyzes the input images and compares them with the images stored in the database.

If the images match the database, the person is granted permission to enter the house, and the security system is disabled by the owner. If the images do not match the database, the security system will not grant permission, and an alarm will be triggered to alert the house members of potential intruders. The captured images will be compared again with the data stored in the database to verify the person's identity.

The architecture provides comprehensive surveillance of the surrounding area, with multiple cameras capturing images from different angles to enhance the accuracy of the security system. The use of deep convolutional neural networks for detecting human presence and facial recognition significantly improves the accuracy of the security system. Additionally, the architecture enables family members to remotely disable the security system, improving convenience and usability.

- Motion Sensor Detector: The system will use a motion sensor detector to detect any human motion.
- Camera System: Three cameras will be used in the system, capturing images from three different angles to provide a comprehensive view of the surrounding area.
- Image Processing: The captured images will be processed using deep convolutional neural networks for facial recognition and detection of human presence.
- Database: A database of authorized individuals will be created, and the captured images will be matched against this database to determine if the person is authorized to enter the home.
- Security System Control: If the person is authorized to enter the home, the security system will be disabled. If not, an alarm will be activated to alert the house members of a potential intruder.
- Remote Access: The security system can be remotely accessed by family members, allowing them to disable the system if needed.
- Arduino Uno: The system will use an Arduino Uno to connect the burglar alarm with the computer system, improving the system's effectiveness in alerting the house members of potential intruders.

5 Results and Discussion

5.1 Training and Dataset Specifications for the DCNN Model

The DCNN model's training procedure utilized a comprehensive home training dataset comprising approximately 4000 samples, representing diverse human postures. These postures were meticulously chosen to mimic the images captured by the camera module in the proposed architecture, ensuring relevance for image recognition tasks. The dataset was categorized into two primary groups: intruder samples and home occupant samples, resulting in a total of eight classes for the multiclass classification task integrated into the DCNN architecture.

To ensure impartial evaluation, the dataset underwent stratified splitting, with 80% allocated for training and the remaining 20% reserved for testing. The DCNN model's training employed the Adam optimizer, configured with specific parameters: a learning rate of 0.001, beta1 of 0.9, beta2 of 0.999, and an epsilon value of 1e-8.

Training iterations extended over 100 epochs and were executed on a computational setup equipped with an Intel (R) Core i5-7500 CPU clocked at 3.40 GHz (3.41 GHz in Turbo Boost mode), 16 GB of RAM, and a 64-bit Windows 10 OS. These hardware specifications ensured sufficient computational resources to effectively train the DCNN model.

By meticulously adhering to this rigorous training methodology and harnessing the computational prowess of the specified environment, the DCNN model demonstrated remarkable proficiency in accurately classifying and distinguishing various human postures captured by the camera module.

5.2 DCNN Image Classification Experimentation

In our study, we evaluated the effectiveness of the DCNN model for home security applications. The training process utilized a dataset sourced from the CV image database, consisting of 3884 images capturing human motion from 972 pedestrians at various angles. This dataset was categorized into four motion types: walking, jumping, limping, and running, with individuals depicted in similar positions but from different perspectives. Additionally, the dataset was segmented into home occupants and intruders for classification purposes. The DCNN model demonstrated a remarkable accuracy rate of 98%. In deep learning classification, a critical metric is the confusion matrix, which integrates predicted and actual values. This high accuracy underscores the potential of utilizing motion patterns to discreetly and effectively distinguish and identify entities within the home environment. To assess the performance of the DCNN architecture during training, we visualized the loss curves in Figs. 4 and 5.

In Fig. 5, the training and validation accuracy are illustrated throughout the training process of the DCNN architecture, focusing on distinguishing between the walking postures of home occupants and intruders.

Figure 4 portrays the progression of loss values for both training and validation datasets across 100 training epochs. Initially, there was variability in the validation samples during the initial 20 epochs, while the training loss exhibited a consistent decline.

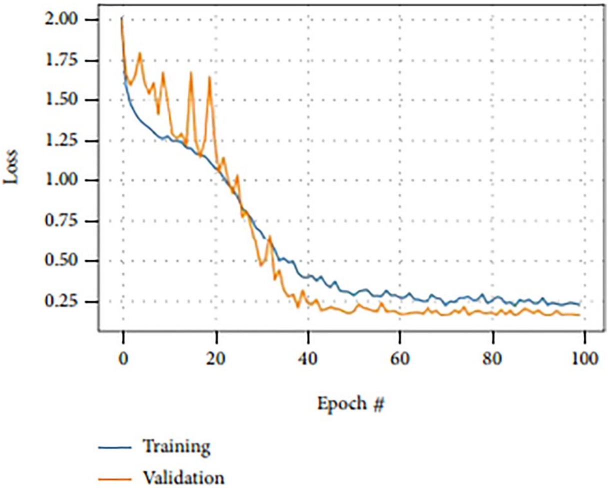

Fig. 4 Depicts the training and validation loss values of the DCNN architecture as it distinguishes between the walking postures of home occupants and intruders

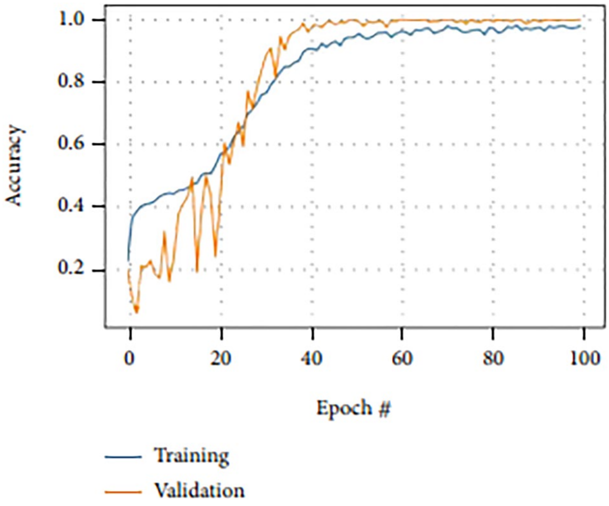

Fig. 5 Training and validation accuracy were evaluated during the training of the DCNN architecture for classifying walk postures of home occupants from intruders

However, from epochs 40 to 100, both training and validation losses converged, indicating successful learning of the DCNN model for classification tasks. Moreover, the accuracy of both phases demonstrated consistent enhancement, stabilizing approximately around epochs 60–100. Following this, the trained model underwent evaluat ion on test samples, assessing various metrics including accuracy, precision, recall, F1-score, and specificity. Table 1 provides a summary of the evaluation outcomes, facilitating a comparison of classifiers based on precision, recall, F1-score, and specificity. This comprehensive analysis offers valuable insights into the model's performance and its capacity to discern entities within the home environment.

To evaluate the effectiveness of the trained DCNN model, we implemented prediction procedures on a dataset consisting of 775 samples. The resulting confusion matrix, represented in Fig. 4, demonstrates the true labels along the y-axis and the predicted labels along the x-axis for the test set samples. Importantly, the diagonal elements of the confusion matrix confirm the exceptional performance of the DCNN architecture. In a well-functioning model, only the diagonal entries contain non-zero values, a pattern evident in this scenario. For instance, in row 1 of the matrix, all 300 samples belonging to that class were successfully classified, indicated by values of 300, 0, 0, and 0. A similar trend is observed in row 2, where 300 samples were correctly classified, resulting in values of 0, 300, 0, and 0. Row 3 displays values of 0, 0, 174, and 1, demonstrating accurate classification of 174 samples within that class. Lastly, row 4 solely contains 0 s, signifying that no samples were assigned to that particular class.

The DCNN model achieved an impressive prediction accuracy of 0.997, outperforming alternative models such as SVM, KNN, and a complex decision tree, which attained accuracies of 0.901, 0.866, and 0.831, respectively. This underscores the superior performance of the DCNN model in effectively classifying home occupants and intruders within the proposed architecture.

Furthermore, the exceptional performance of the DCNN model is validated by its precision, recall, F1-score, and specificity, as outlined in Table 2. For a comparative evaluation, we reference a pertinent study cantered on a deep learning-based smart mat monitoring system [17]. This study aimed to forecast identity information, stepping position,

Table 1 Showcases the outcomes derived from the classification problem prediction, specifically distinguishing between house occupants and intruders, employing the proposed DCNN model

Metrics	Accuracy	Precision	Recall	F1-score	Specificity
Proposed DCNN	0.997	0.997	0.997	0.996	1.001
SVM	0.901	0.832	0.713	0.768	0.956
KNN	0.866	0.666	0.856	0.751	0.871
Complex decision tree	0.831	0.666	0.572	0.614	0.912

Table 2 Comparative analysis: proposed CNN model versus previous works model performance (%)

S Model	Accuracy
Proposed DCNN	99.79
CNN	96.01
Conv-DCWRNN	93.01
Conv-CWRNN	92.37
CON-RNN	91.78
Small conv-LSTM	91.51
Large conv-LSTM	91.51

and activity status within smart homes or building environments using a DCNN model [21]. The authors assessed their model's effectiveness on a dataset comprising 1000 samples, achieving an accuracy of 96% for the trained model. In contrast, our DCNN training yielded an accuracy of 99.79%. However, it's important to note that the comparison was limited to a single metric, as the authors primarily emphasized prediction accuracy in their performance evaluation. Additionally, their implemented model relied on triboelectric output signals and output voltages of individual walking patterns, which differ from the input values used in our study, thus imposing constraints on the extent of comparison. Furthermore, the dataset utilized was inaccessible for further analysis and comparison involving other specified performance metrics.

Please ensure that the correct references and figures are used in place of "Fig. 4" and "Table 1" based on your actual experiment.

To gauge the efficacy of our proposed DCNN model, we conducted a comparison with models presented in [18]. It's important to recognize that, similar to the challenge of metric comparisons in line with related prior studies, our comparison with the model implementation in [19] is limited to accuracy. This choice is made because accuracy is the only directly comparable metric across previous research endeavours. [19]. Table 2 offers a comprehensive juxtaposition of our DCNN model with prior works based on accuracy. The findings underscore the superior performance of our proposed DCNN model in fortifying home security within IoT smart home automation.

By leveraging the capabilities of the proposed DCNN models, significant improvements can be made to smart home automation applications, specifically in detecting intruders based on their motion patterns [20]. The integration of surveillance cameras and models designed for motion pattern detection, classification, and differentiation enables users to accurately identify intruders. Moreover, security notifications and alerts in smart home applications can be tailored based on the detected motion patterns, providing enhanced levels of home security within the smart home environment [21].

6 Conclusion and Future Directions

In conclusion, the proposed Deep Convolutional Neural Network (DCNN) model effectively enhances home security within IoT smart home automation. By analyzing motion patterns from a dataset of human motion, the DCNN model achieved an accuracy of 98%, outperforming other models like SVM, KNN, and decision trees.

The DCNN's strong performance, confirmed through confusion matrix analysis, shows its capability to accurately classify home occupants and intruders. Evaluation metrics, including precision, recall, and F1-score, further validate its robustness. This model leverages motion patterns for efficient and discreet identification within the home environment.

Integrating surveillance cameras and motion detection models, the proposed DCNN system significantly improves home security. Users can rely on accurate intruder detection based on motion patterns, with tailored security notifications and alerts. This highlights the potential of deep learning in smart home automation.

6.1 Future Work

Future research could focus on:

1. **Expanding the Dataset**: To capture a wider range of motion patterns.
2. **Real-Time Implementation**: Integrating live video feeds for immediate detection.
3. **Multimodal Data Integration**: Combining data types for richer information.
4. **Fine-Grained Classification**: Enhancing specific categorization of motion patterns.
5. **Transfer Learning and Model Optimization**: Improving performance and efficiency.
6. **Addressing Privacy and Ethical Concerns**: Ensuring data security and ethical use.

By exploring these areas, the DCNN model can be further developed to provide smarter and more secure IoT-based smart home systems, enhancing safety and well-being in smart home environments.

Author Contributions Rishi Sharma, Dr. Anjali Potnis, and Dr. Vijayshri Course contributed to the design, implementation, analysis, and interpretation of the study. All authors have reviewed and approved the final manuscript.

Funding This research was not funded by any specific grant from public, commercial, or non-profit organizations.

Data Availability The datasets produced and/or examined during this study can be obtained from the corresponding author upon reasonable request.

Code Availability The codes utilized in this study can be obtained from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors report no conflicts of interest.

References

1. Groeneveld, S., et al. (2024). The cooperation between nurses and a new digital colleague “AI-Driven Lifestyle Monitoring” in long-term care for older adults. *JMIR nursing, 7*, 56474.
2. Verma, P., et al. (2024). Smart home system integration using internet of things. *Advances in networks, intelligence and computing* (pp. 451–459). CRC Press.
3. Shukla, P., Krishna, C. R., & Patil, N. V. (2024). Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review. *The Journal of Supercomputing, 80*(7), 9986–10043.
4. Rahman, W., et al. (2024). Automated detection of harmful insects in agriculture: A smart framework leveraging IoT, machine learning, and blockchain. *IEEE Transactions on Artificial Intelligence*. https://doi.org/10.1109/TAI.2024.3394799
5. Yang, D.-Q., et al. (2024). A systematic study on transfer learning: Automatically identifying empty camera trap images using deep convolutional neural networks. *Ecological Informatics, 80*, 102527.
6. Rajab, M. A., Abdullatif, F. A., & Sutikno, T. (2024). Classification of grapevine leaves images using VGG-16 and VGG-19 deep learning nets. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 22*(2), 445–453.
7. Haque, M., Nyeem, H., & Afsha, S. (2024). BrutNet: A novel approach for violence detection and classification using DCNN with GRU. *The Journal of Engineering, 2024*(4), 12375.
8. Dang, T.-V. (2022). Smart home management system with face recognition based on ArcFace model in deep convolutional neural network. *Journal of Robotics and Control (JRC), 3*(6), 754–761.
9. Ishraque, I., Hasan, M.S., &. Al-Amin, M.S. (2023) *Traffic congestion prediction using deep convolutional neural networks: A color-coding approach*. Department of electrical and elecrtonics engineering (EEE), Islamic.
10. Suresh, M., et al. (2023) IoT-based smart security and home automation system, In: Intelligent technologies for sensors. Apple academic press. pp. 89–101.
11. Taiwo, O., et al. (2022). Enhanced intelligent smart home control and security system based on deep learning model. *Wireless communications and mobile computing, 2022*, 1–22.
12. Ansari, M. A., Singh, D. K., & Singh, V. P. (2023). Detecting abnormal behavior in megastore for crime prevention using a deep neural architecture. *International Journal of Multimedia Information Retrieval, 12*(2), 25.
13. Waseem, Q., et al. (2023). *Exploring machine learning in IoT smart home automation*. In: *2023 IEEE 8th international conference on software engineering and computer systems (ICSECS)*. IEEE.
14. Kalnoor, G., & Gowrishankar, S. (2021). IoT-based smart environment using intelligent intrusion detection system. *Soft Computing, 25*(17), 11573–11588.
15. DurgaBhavani, K., & FerniUkrit, M. (2024). Design of inception with deep convolutional neural network based fall detection and classification model. *Multimedia Tools and Applications, 83*(8), 23799–23817.
16. Ma, B., et al. (2020). Autonomous deep learning: A genetic DCNN designer for image classification. *Neurocomputing, 379*, 152–161.
17. Lu, Y., et al. (2024). Application of deep learning and intelligent sensing analysis in smart home. *Sensors, 24*(3), 953.
18. Suganthi, P., & Kavitha, R. (2023). Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment. *Sādhanā, 48*(4), 206.
19. Karthikamani, R., et al. (2024) *IoT based anti-theft flooring system using CC3200*. In: *2024 2nd international conference on intelligent data communication technologies and Internet of Things (IDCIoT)*. IEEE.
20. Shi, Q., et al. (2020). Deep learning enabled smart mats as a scalable floor monitoring system. *Nature communications, 11*(1), 4609.
21. Neverova, N., et al. (2016). Learning human identity from motion patterns. *IEEE Access, 4*, 1810–1820.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Rishi Sharma has completed his M.Tech. from MANIT, Bhopal, India. Specialisation of mtech is VLSI and Embedded system. He completed his M.Tech. in the year 2012. His expertise is in VLSI, IOT, Convolution neural network.

Anjali Potnis has received her Ph.D. degree and M.Tech. in the year 2012 and 2002 respectively from MANIT, Bhopal, India. Her M.Tech. is in digital communication. Her area of expertise are image processing, signal processing, IOT. She joined NITTTR , Bhopal, India in the year 2012 as Assistant Professor.

Vijayshri Chaurasia has received her Ph.D. degree and M.Tech. from MANIT, Bhopal, India. She has joined MANIT as Assistant Professor in the year 2010. Her mtech is in digital communication. Her area of expertise are image processing, signal processing, convolution neural network.