Research Article Open Access

A New Smart Home Intruder Detection System Based on Deep Learning

Hiba Hameed Ali[1*], Jolan Rokan Naif[2], Waleed Rasheed Humood[1]

[1] Department of Computer Science, College of Education, Mustansiriyah University, 10052 Baghdad, IRAQ.
[2] Iraqi Commission for Computer & Information, Information Institute for Postgraduate Studies, Baghdad, IRAQ.

*Correspondent contact: hiba90ham@uomustansiriyah.edu.iq
https://orcid.org/0000-0001-7094-4574

Article Info

Received
29/11/2022

Accepted
31/01/2023

Published
30/06/2023

ABSTRACT

The security of home doors has become one of the necessities in this era. The Internet of Things (IoT) technology has also entered into building the smart home. Therefore, it has become necessary to develop a facial recognition system that can be implemented on IoT devices. This study presented a method to recognize faces using the efficientnet-b4. Transfer learning with fine-tuning was used here due to the small dataset size and high accuracy (accuracy of Top-1= 82.9% and accuracy of Top-5 = 96.4%) of EfficientNet-B4 and it has fewer parameters (19.5 M) than the previously known model and this is what we are looking for in order to implement it on the Raspberry Pi. After training and saving the model, it is converted into a lightweight model and transferred to the Raspberry to distinguish faces. The results showed that the model had an accuracy of 97%, despite the fact that the collected images were taken in different lighting, different places, and different facial expressions.

KEYWORDS: Smart home, deep learning, efficientNetB4, transfer learning.

الخلاصة

أصبح تأمين أبواب المنزل من الضروريات في هذا العصر حيث دخلت تقنية إنترنت الأشياء (IoT) في بناء المنزل الذكي. لذلك، أصبح من الضروري تطوير نظام للتعرف على الوجه الذي يمكن تنفيذه على أجهزة إنترنت الأشياء. قدمت هذه الدراسة طريقة للتعرف على الوجوه باستخدام EfficientNet-b4. تم استخدام transfer learning مع fine tuning هنا نظرًا لحجم مجموعة البيانات الصغير والدقة العالية لـ EfficientNet-B4 (Top1= 82.9% و Top5= 96.4%) وله معلمات أقل من النماذج المعروفة سابقًا (19.5 M) وهذا ما نبحث عنه من أجل تنفيذه على Raspberry Pi. بعد التدريب وحفظ النموذج، يتم تحويله إلى نموذج خفيف الوزن ونقله إلى Raspberry لتمييز الوجوه. وأظهرت النتائج أن دقة النموذج بلغت ٩٧٪ ، على الرغم من حقيقة أن الصور التي تم جمعها تم التقاطها في إضاءة مختلفة وأماكن مختلفة وتعبيرات وجه مختلفة.

INTRODUCTION

A home with smart technology installed is referred to as a smart home and is intended to offer people customized services. Smart technologies enable the monitoring, management, and assistance of inhabitants, thereby enhancing the quality of life and promoting autonomy. The application of smart home technologies remains an important part of the Internet of Things (IoT). Provides necessary life assistance and comfort to the elderly in the community [1, 2, 3]. The IoT paradigm dubs a system of interconnected, computationally capable, and capable of transmitting data via a network, without the need for human intervention. This paradigm is based on the idea that smart gadgets are widely used and work together and with people to accomplish common objectives [4,5,6,7,8]. As the likelihood of infiltration increases day by day, home security is becoming increasingly important in the modern world. To track the state of the house, closed circuit television (CCTV) is installed. But CCTV does not alert users in real time when interference is being recorded. If the homeowner does not watch the CCTV screen that has been installed, the homeowner will not be aware of the current state of the home [9, 10]. Facial Recognition is an application that detects, tracks, recognizes and verifies human faces in photos or videos obtained with a digital camera. Face recognition is used extensively in applications that are used in the real world, such as video surveillance, security systems, and human-machine interaction. Traditional systems based on shallow learning have faced obstacles such as position variation, facial disguises, scene lighting, the intricacy of the image background, and variations in facial expression as seen in references [11, 12].

Along with the advancement of technology, particularly in the IoT sector, the security of home entrances is becoming increasingly significant as it serves as the foundation for the simplest and most straightforward form of protection and is adequate to give homeowners a feeling of safety. Facial recognition technology has also been developed and is now being used in home door locking systems. This technology is an option that is pretty basic and straightforward to use, and it is quite accurate in detecting the faces of homeowners. Convolution neural networks (CNN's) advances in facial recognition has resulted in the creation of one of the face recognition systems that is simple to implement and has a high degree of accuracy when it comes to recognizing faces [13, 14].

Related Work

Research in the field of smart home automation has witnessed amazing progress, innovations, experimentation and implementation. This section provides a review of relevant literature on smart home automation. J. Patel, S. Anand, and R. Luthra [15] This paper presents a safe and reliable mechanism for unlocking Remote home doors using a mobile application. The prototype system consists of Amazon Web Services (AWS), a Raspberry Pi v2 camera module, a Raspberry Pi Model 3B+, a proximity sensor (infrared sensor), a switch (to simulate a doorbell), an LED (to simulate a door) and a liquid-crystal display (LCD) screen, and Android app. There are two situations that will activate the camera: either when someone presses the doorbell or when someone has been close to them for more than a preset amount of time. The captured image is uploaded to the cloud, where facial features are extracted and compared to "known" faces. Results - (whether known or unknown) are stored on the cloud, along with simultaneously sent to the user's application and email/recorded emails. The user is notified via an in-app notification, and has access to both the label and the image associated with it.

N. S. Irjanto and N. Surantha [13] the author presented a home door security design based on a face recognition system that uses CNN Alexnet, and the study suggests facial recognition when the door is opened. There are three stages to implementing this system: Homeowner data collection, data training, Facial recognition using raspberry pi. Facial data is collected from each family member. There are a total of five individuals present, and the data is separated into training and test groups. The training process phase was not implemented on the Raspberry Pi due to the Raspberry Pi's limited computational power, so the training phase was implemented separately using a computer with a CPU (control processor unit) based on the Intel Core i5 8500 and 8 GB Double Data Rate 4(DDR4) RAM, , the accuracy is 97.5%. R. A. Nadafa, S. M. Hatturea, V. M. Bonala, and S. P. Naikb [16] This work results in the design of a Raspberry Pi-based home security system. The raspberry pi, the touch screen, the camera, and the smartphone device are all necessary pieces of hardware for this system. opencv libraries, Python, and node.js are utilized when developing the software. The system that is being presented is meant to function like an intelligent mirror that can both deliver information and monitor the safety of a home. PythonAnywhere is one of the Amazon cloud services that can be used to upload the image of the intruder. The image will have its base64 format before being saved to the database. For easy image storage and retrieval, this conversion to a different format is necessary. The suggested system has two modes of operation: normal and on mode. In normal mode, it displays information on the mirror in real time. Touch commands or mobile phone commands can be used to put the system into on mode. When the system is on, it will work to detect human intrusion. When a human being is detected in this operating mode, the system takes the image of the individual and sends it via SMS to the owner.

I. G. M. Ngurah Desnanjaya and I. N. A. Arsana [10], the Raspberry Pi is utilized in the home security surveillance system that is proposed in this study. The system is able to observe the home for unfavorable occurrences like as theft, and it also notifies the user of any changes to the status of the home. Notifications are transmitted in the form of photographs depicting the circumstances of the room within the house, as well as the conditions of the gas density and the temperature. The system control center is raspberry pi. Raspicam is used to snap photographs when the PIR sensor senses objects entering a room. Gas and temperature sensors are utilized to monitor gas concentration and temperature conditions. And Telegram as a communication app to provide notifications to device users from Raspberry Pi.

O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi [17] introduce a smart home automation system to monitor environmental factors, control home appliances, and detect movement in and around the home. It is suggested to use a model that uses deep learning to recognize and classify motion based on the motion patterns that are identified. The walking pattern of a human being seen by a security camera helps determine whether that person is an authorized resident of the home or an unauthorized intruder. The prototype for the suggested method was created with a PIR motion sensor. A CNN model was used to conduct an empirical study of human movement patterns, and the results showed an accuracy of 99.8 percent. In this section, the latest work in building the smart home was explained, but there are not many works that depend on facial recognition using deep learning algorithms and implementing the system on the Raspberry Pi, in work [13], the researcher used the Alexnet, but by referring to the number of Alexnet parameters, we find it large, so we try to work on a pre-trained model with a lower number of parameters, so that the execution time is faster on the Raspberry Pi to distinguish faces.

MATERIALS AND METHODS

Proposed System

This article describes the design and execution of a home observation system that relies on detecting persons and then recognizing their faces using Raspberry Pi, a new, compact, and inexpensive technology. In addition to a pre-trained (CNN) model. this project includes a sensor capable of detecting human movement within an acceptable distance (PIR) sensor. In addition, the project includes a camera with an acceptable resolution. We will utilize a robust programming language which is simple to use, read, and write (python). and the smartphone. The sensor will function and transmit a signal to the raspberry pi if there is a person in front of the door. The camera is instructed to begin taking pictures when it receives a signal from the raspberry pi. The camera takes a picture of the person standing in front of the entrance. After the image is taken, it will be entered into the CNN model to perform facial recognition, If the person in the image is a family member or an intruder, If the person is an intruder, the raspberry pi will send an alarm to the homeowner via a Wi-Fi network connected to the raspberry pi, and if this person is a member of the house, the door is opened. A notification will be sent to the homeowner's mobile device via the mobile app (telegram bot). Wi-Fi allows the user to connect wirelessly to their home network and the internet. The Raspberry Pi acts as a microcontroller for the home environment. The home security system is enhanced with a deep learning (CNN) model that can recognize, classify and alert the user to the presence of an intruder; Figure 1 shows the hardware design of the proposed system. Figure 2 shows the system architecture.

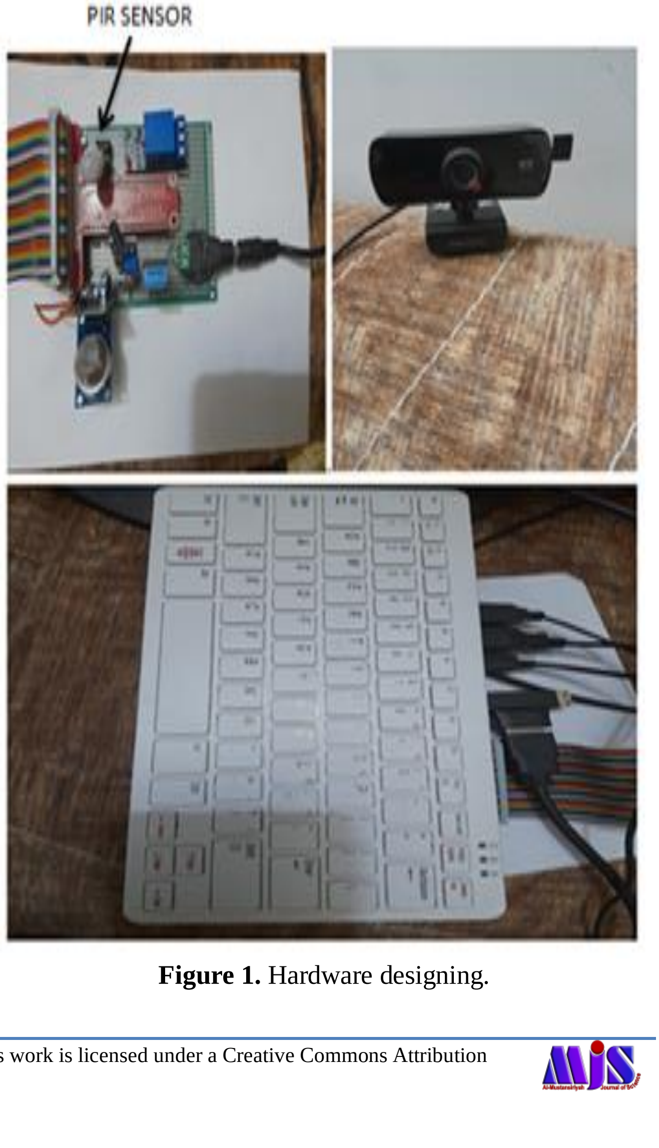


Figure 1. Hardware designing.

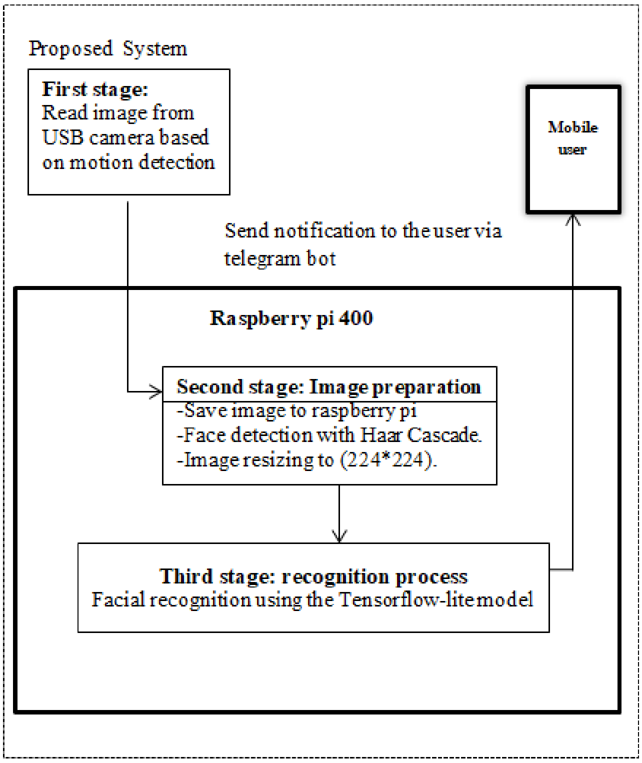
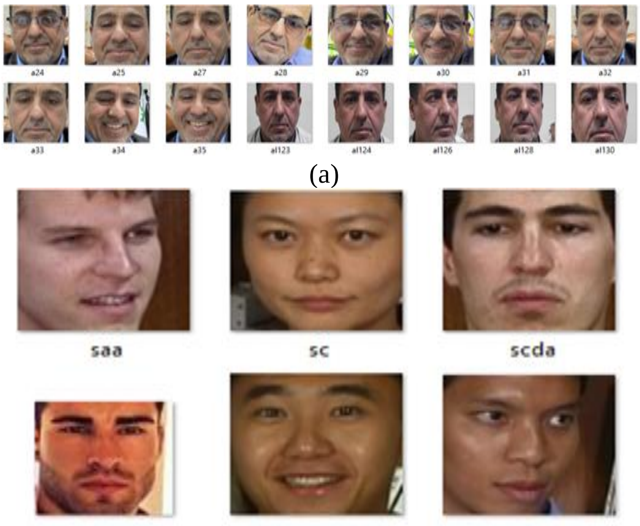

Proposed System
First stage:
Read image from USB camera based on motion detection
Mobile user
Send notification to the user via telegram bot
Raspberry pi 400
Second stage: Image preparation
-Save image to raspberry pi
-Face detection with Haar Cascade.
-Image resizing to (224*224).
Third stage: recognition process
Facial recognition using the Tensorflow-lite model

Figure 2. Proposed system.

Dataset Collection

The process of collecting photos was done manually, as the photos were taken by the mobile camera and the camera connected to the Raspberry. About 844 pictures were collected, distributed into 4 classes, three of which are family members, Figure 3(a) shows some image of family member. And the fourth class was called stranger, this class contains pictures of strangers of different ages, men, women and children, Figure 3(b) shows some images from this class. Table 1 shows how the datasets are distributed.



(a)

(b)

Figure 3. (a) pictures of family member and (b) pictures of stranger class.

Table 1. Dataset distribution

Class name	Number of images in each class	Distributed image
Hatam	186	Train 130 Validation 18 Test 38
Hiba	266	Train 186 Validation 26 Test 54
Lubna	138	Train 96 Validation 13 Test 29
Stranger	254	Train 177 Validation 26 Test 51

Preprocessing and augmentation

The suggested system starts pre-processing the images in the first step. The requirements of the pre-processing stage arise from the necessity of optimizing and preparing the input images [18].

- Detect and crop only faces image
- Distribute the pooled data set for training, validation and testing.
- Augmentation image data
- Resize the image to 224*224

After detecting and cropping only the faces image and saving the new images, the image data augmentation will be applied to the training, validation and testing dataset. Data augmentation is a way for increasing the amount of data by applying techniques such as flipping, rotating, and so on. Data augmentation makes the model more resistant to minor alterations, preventing overfitting [19].

Pre-trained models

Deep learning (DL) is a subsection of machine learning (ML) that consists of interconnected networks of units. In deep learning models, these modules are interconnected to form many layers, which enables them to create more high-level representations of the inputs [20]. DL has enabled significant advancements in a number of computer vision (CV) tasks, including object detection, action recognition, motion tracking, semantic segmentation, and human position estimation. Convolutional neural networks (CNNs), have established themselves as the preeminent form of DL technology since their outstanding success in the ImageNet competition. Image categorization is one of the most fundamental and essential CV fields [21,22].

DL is emerging as one of the most successful and relevant approaches that can be used for various elements of IoT security. In order to reduce the number of parameters required for image recognition tasks, CNN was developed to take the place of conventional artificial neural networks. The downside of a CNN is its high processing cost, making it difficult to execute on devices with limited resources, like those found in an IoT context, and frequently necessitating the use of edge computing devices [23,24]. 2019 saw the emergence of the EfficientNet model as the state-of-the-art in the largest image classification data set ImageNet. EfficientNet is a new baseline network developed by neural structure search (NAS), and a series of B1-B7 EfficientNet models are generated by scaling up When examining optimal combinations within a constrained resource range, eight models (models B0 to B7) displayed greater performance with less parameters. The EfficientNet shows exceptional transfer learning potential to different fields [25, 26, 27].

Using the EfficientNetB4 model, a CNN transfer learning application with fine tuning is created here. Fig. 4 shows the fine-tuning technique. The experiment is carried out using colab and the Python 3. Because EfficientNetB4 only supports photos with the dimensions (224, 224, 3), All images in the datasets are transformed to conform to these specifications. We use the transfer learning technique to build our system with an EfficientNet-b4 model and implement it on raspberry pi. Transfer learning provides a feasible method for alleviating the challenge of data hungry, and it has soon been widely applied to the field of computer vision (CV). When the training dataset is relatively small, transferring a CNN pre-trained by a large annotated dataset and fine-tuning it for a specific task can be an efficient method for achieving acceptable goals and lower training costs. Pre-trained CNNs are applied as the backbone of most state-of-the-art computer vision (CV) models [28, 29]. Training phase This stage includes feature extraction and recognition. The EfficientNet-B4 was chosen to train it to distinguish the faces of the owners of the house due to its accuracy in the Imagenet competition (accuracy of Top-1= 82.9% and accuracy of Top-5=96.4%) and the small number of its parameters compared to the rest of the pre-trained model (19.5 M), Because the proposed system is implemented on IoT devices, it is better that the model has a small number of parameters, the weights of the layers are not changed, but the classifier layer is modified to fit the number of class (persons) we have as in Figure 5.

The data is entered into a convolutional neural network, which is then processed and classified. Python-based Keras, a free and open-source deep learning library, was used to create a pre-trained model. Each image in the data set will go through a series of layers for facial recognition with probabilistic values between 4 classes, and label each class with the name of the person.

In our experiments, EfficientNet pre-trained on ImageNet was used as the backbone network in initial stage. The training phase is divided into two parts, the first part includes: freezing the weights of the network layer, excluding the classification layer. The second part is fine-tuning and retraining of the fully connected layer, replacing the 1000-dimensional softmax classification layer of EfficientNet with X-dimensional (number of persons) softmax classification layer, Figure 6 shows the modified classification layer.

Due to the small computing power of the raspberry pi, the training procedure is performed on a google colab, and Execution is on Raspberry Pi. After the model is trained, save the model and convert the Model to the Tensorflow-Lite model. Then use the model on the Raspberry Pi to distinguish the faces, Figure 7 shows the training process. The model initializes a value for all required parameters as in the Table 2.

Table 2. Pre-trained Model Parameters.

Parameters	Values
Activation function	Softmax
Gradient Descent Optimizer	Adam
Learning rate	0.0001
Epoch	700
Batch-size	50

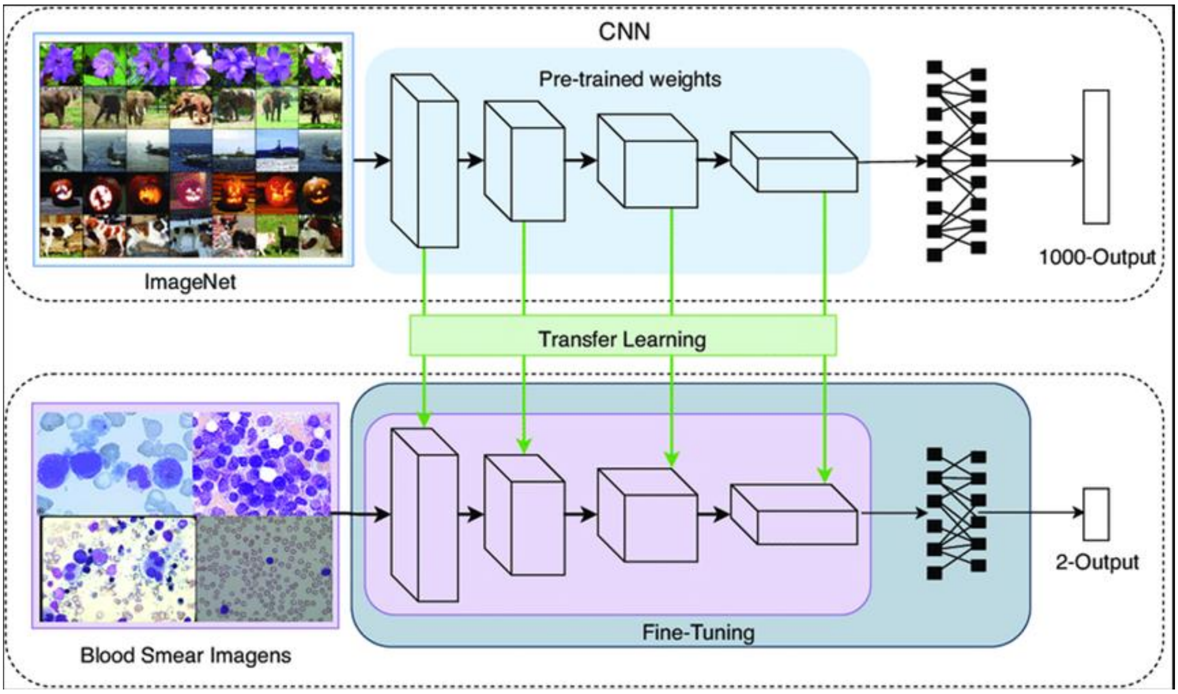


Figure 4. Fine tuning technique [30].

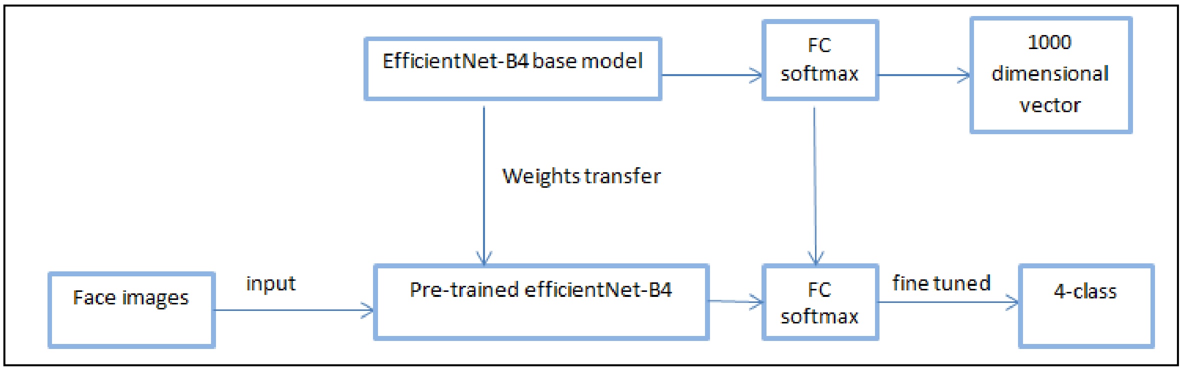


Figure 5. Fine tuning EfficientNetB4.

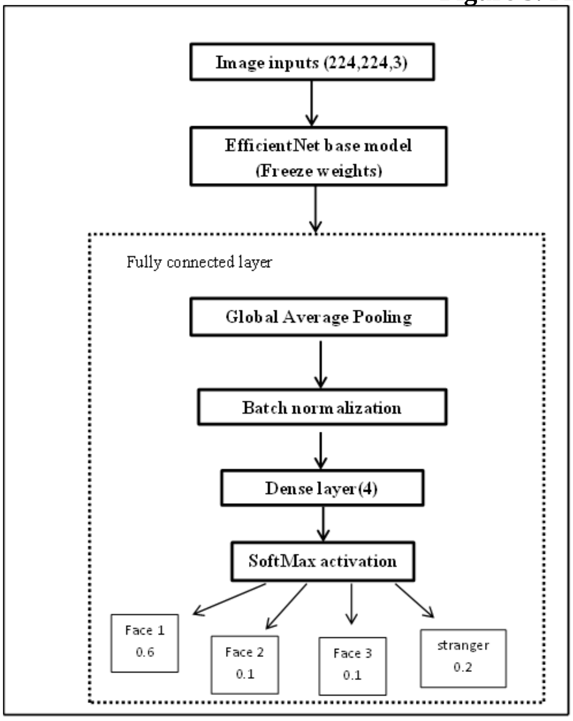


Figure 6. Design of fully connected layer.

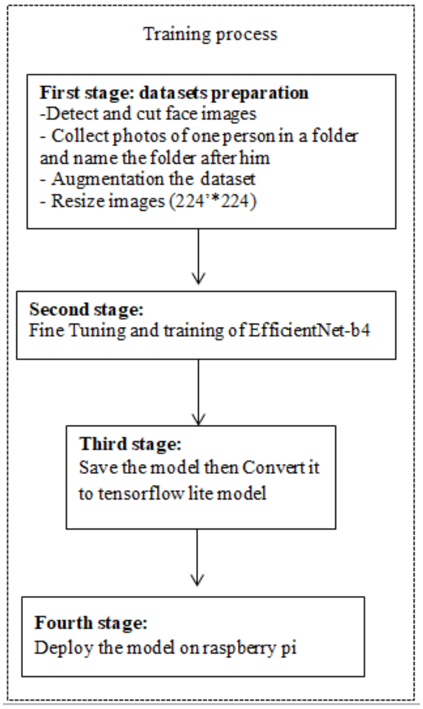

Training process
First stage: datasets preparation
-Detect and cut face images
- Collect photos of one person in a folder and name the folder after him
- Augmentation the dataset
- Resize images (224*224)
Second stage:
Fine Tuning and training of EfficientNet-b4
Third stage:
Save the model then Convert it to tensorflow lite model
Fourth stage:
Deploy the model on raspberry pi

Figure 7. Training process.

Evaluation metrics

Many measurements are used to define the classification algorithms efficacy like precision, recall, and F1-measure. Estimation of certain measures focuses mostly on the confusion matrix [31].

Confusion matrix: it is a description of the effects of a prediction over a classification problem. The correct and incorrect numbers of predictions are broken down by classes. The confusion matrix shows how confused the classification model is when it makes predictions [30].

Accuracy: The number of correct predictions is divided by the total number of predictions where TP = True positive class prediction, TN = True Negative class prediction, FP = False positive class prediction, FN = False negative class prediction [31].

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (1)$$

Recall: It is defined the number of real positive outcomes divided by the number of actual positive outcomes and calculated by (2) [31].

$$Recall = \frac{TP}{TP+FN} \qquad (2)$$

Precision: It is defined as the ratio of true positives to the total positives predicted by face recognition model and calculated according to (3) [31].

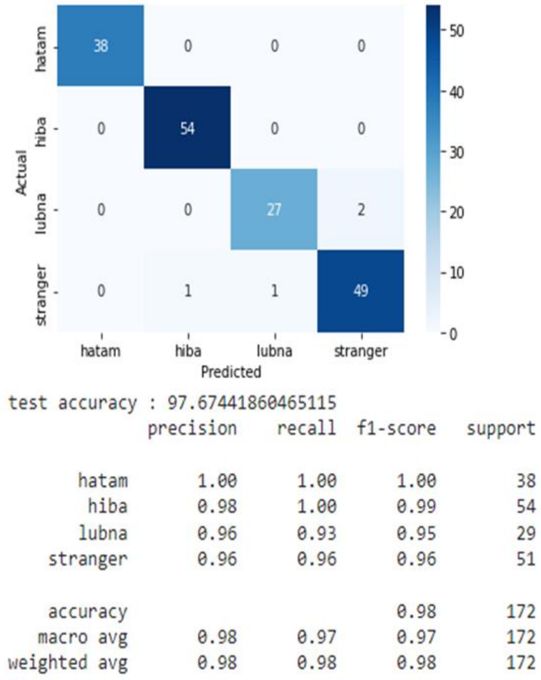
$$Precision = \frac{TP}{TP+TN} \qquad (3)$$

F1 Score [30]:

$$F1\,Score = \frac{2*(Precision*Recall)}{(Precision+Recall)} \qquad (4)$$

EXPERIMENTAL RESULT

The evaluation scales showed the following results, as shown in the Figure 8. Looking at the results of the studies as in table 3, several things appear that can affect the accuracy results of the proposed methods, and these matters are related to the dataset. In some datasets, the images for each person are 10 images, and when we have an algorithm training in deep learning or transfer learning, this number is considered to be a small number and the results cannot be relied upon and benefited from in real conditions and environment. In other studies, a pre-trained model with a very large number of parameters was used. In this study, we used a model whose parameter number is less than the well-known model. Dataset images were taken in unconstrained environments and with different expressions. The result was satisfactory, but the system needs more images in order to distinguish strangers and not classify them as a family member. In order to ensure that a stranger is not classified as a family member, a comparison is made on the Raspberry Pi if the similarity of the class in the softmax layer is less than 95%, the person is considered a stranger.



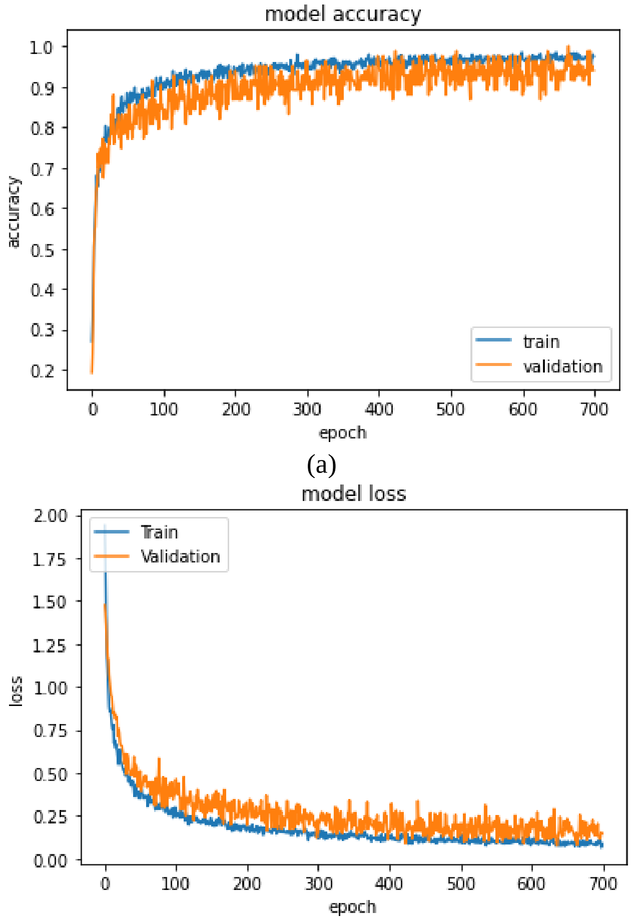
```
test accuracy : 97.67441860465115
              precision    recall  f1-score   support

       hatam       1.00      1.00      1.00        38
        hiba       0.98      1.00      0.99        54
       lubna       0.96      0.93      0.95        29
    stranger       0.96      0.96      0.96        51

    accuracy                           0.98       172
   macro avg       0.98      0.97      0.97       172
weighted avg       0.98      0.98      0.98       172
```

Figure 8. Performance evaluation

Table 3. Comparison with other studies.

Study	Method	Datasets	Accuracy
[13]	CNN (Alexnet)	Collected datasets	97.5%
[32]	CNN	AT&T database	98%
[33]	Facenet+ (SVM, KNN,RF)	LFW dataset	Facenet+SVM (99.7) Facenet+KNN (99.5) Facenet+RF (85.1)
Proposed method	EfficientNet-B4	Collected datasets	97.6

Figure 9 (a) shows the accuracy of the training and validation set, (b) shows the loss value of the training and validation set.

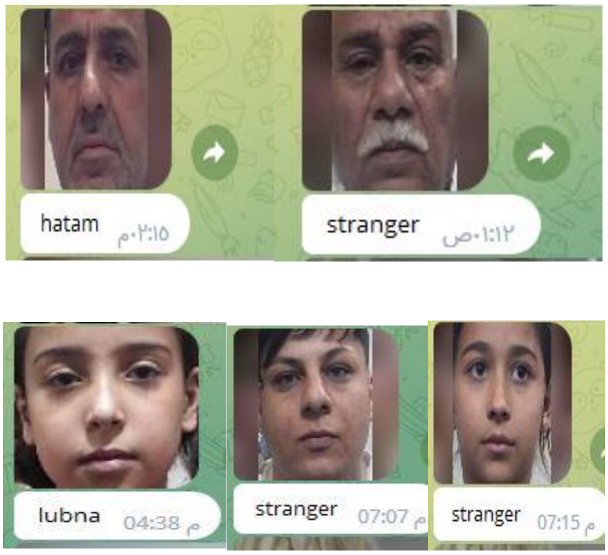


(a)

(b)

Figure 9. (a) Model accuracy (b) Model loss.

Figure 10 shows the implementation of the project, Where the image of the person standing in front of the door, after detecting his face, is sent to the homeowner via a telegram bot, and a message is sent with it. If the person is a family member, his name is written, and if he is an outsider, a stranger is written.



hatam ٠٢:١٥ م

stranger ٠١:١٢ ص

lubna 04:38 م

stranger 07:07 م

stranger 07:15 م

Figure 10. Shows an example of the system implementation.

CONCLUSIONS

The home monitoring system based on face recognition can be useful to notify the homeowner in the event of an intruder in front of the door without the need to monitor the house all the time through cameras. The study developed EficientNet-B4 to distinguish faces, and a high accuracy was obtained despite the lack of pictures, and they were taken in different conditions and different backgrounds and from more than one camera. As a prototype that can be started from and building a larger system for distinguishing faces that can be used in institutions based on EfficientNet-B4 where the number of parameters is less than the known pre-trained models, it is also possible to implement this system on edge devices after converting it to a light model.

Disclosure and Conflict of Interest: The authors declare that they have no conflicts of interest.

REFERENCES

[1] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," Technol. Forecast. Soc. Change, vol. 138, no. June 2018, pp. 139-154, 2019. https://doi.org/10.1016/j.techfore.2018.08.015

[2] K. Maswadi, N. B. A. Ghani, and S. B. Hamid, "Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly," IEEE Access, vol. 8, pp. 92244-92261, 2020. https://doi.org/10.1109/ACCESS.2020.2992727

[3] R. Khalaf, A. Mohammed, E. Essa, and H. Ali, "Controlling Smart Home Activities Using IoT," ICCISTA 2019 - IEEE Int. Conf. Comput. Inf. Sci. Technol. their Appl. 2019, pp. 1-6, 2019. https://doi.org/10.1109/ICCISTA.2019.8830664

[4] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," Inf., vol. 12, no. 2, pp. 1-21, 2021. https://doi.org/10.3390/info12020087

[5] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, 2017. https://doi.org/10.1155/2017/9324035

[6] A. H. Mohammed and R. M. A. Hussein, "Security Services for Internet of Thing Smart Health Care Solutions Based Blockchain Technology," Telkomnika (Telecommunication Comput. Electron. Control., vol. 20, no. 4, pp. 772-779, 2022. https://doi.org/10.12928/telkomnika.v20i4.23765

[7] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system," Period. Eng. Nat. Sci., vol. 8, no. 4, pp. 2333-2345, 2020. http://dx.doi.org/10.21533/pen.v8i4.1738

[8] V. C. Pathayapuram and A. A. Chikkamannur, "An Ameliorated Ensemble Approach for IoT Resource Feature Selection Based on Discriminating and Service Relevance Criteria," Int. J. Intell. Eng. Syst., vol. 14, no. 3, pp. 435-446, 2021. https://doi.org/10.22266/ijies2021.0630.36

[9] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology," Procedia Comput. Sci., vol. 183, pp. 4-13, 2021. https://doi.org/10.1016/j.procs.2021.02.023

[10] I. G. M. Ngurah Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," Indones. J. Electr. Eng. Comput. Sci., vol. 22, no. 3, pp. 1295-1302, 2021. https://doi.org/10.11591/ijeecs.v22.i3.pp1295-1302

[11] Z. M. Abood, G. S. Karam, and R. E. Haleot, "Face Recognition Using Fusion of Multispectral Imaging," 2017 2nd Al-Sadiq Int. Conf. Multidiscip. IT Commun. Sci. Appl. AIC-MITCSA 2017, pp. 107-112, 2017. https://doi.org/10.1109/AIC-MITCSA.2017.8722957

[12] P. Annamalai, "Automatic face recognition using enhanced firefly optimization algorithm and deep belief network," Int. J. Intell. Eng. Syst., vol. 13, no. 5, pp. 19-28, 2020. https://doi.org/10.22266/ijies2020.1031.03

[13] N. S. Irjanto and N. Surantha, "Home Security System with Face Recognition based on Convolutional Neural Network," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 11, pp. 408-412, 2020. https://doi.org/10.14569/IJACSA.2020.0111152

[14] G. Mubarak and E. Abdul Kareem, "In-Door Surveillance Module Based on an Associative Memory," AL-Rafidain J. Comput. Sci. Math., vol. 15, no. 2, pp. 13-26, 2021. https://doi.org/10.33899/csmj.2021.170005

[15] J. Patel, S. Anand, and R. Luthra, "Image-Based Smart Surveillance and Remote Door Lock Switching System for Homes," Procedia Comput. Sci., vol. 165, no. 2019, pp. 624-630, 2019. https://doi.org/10.1016/j.procs.2020.01.056

[16] R. A. Nadafa, S. M. Hatturea, V. M. Bonala, and S. P. Naikb, "Home Security against Human Intrusion using Raspberry Pi," in Procedia Computer Science, 2020, vol. 167, no. Iccids 2019, pp. 1811-1820. https://doi.org/10.1016/j.procs.2020.03.200

[17] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model," Wirel. Commun. Mob. Comput., vol. 2022, 2022. https://doi.org/10.1155/2022/9307961

[18] K. A. Hussein and Z. T. A. Al-Ani, "Iraqi License Plate Recognition Based on Neural Network Technique," J. Phys. Conf. Ser., vol. 2322, no. 1, 2022. https://doi.org/10.1088/1742-6596/2322/1/012025

[19] S. Karkra, P. Singh, and K. Kaur, "Convolution neural network: A shallow dive in to deep neural net technology," Int. J. Recent Technol. Eng., vol. 8, no. 2 Special Issue 7, pp. 487-495, 2019. https://doi.org/10.35940/ijrte.B1092.0782S719

[20] M. A. Mazurowski, M. Buda, A. Saha, and M. R. Bashir, "Deep learning in radiology: An overview of the concepts and a survey of the state of the art with focus on MRI," J. Magn. Reson. Imaging, vol. 49, no. 4, pp. 939-954, 2019. https://doi.org/10.1002/jmri.26534

[21] J. Chai, H. Zeng, A. Li, and E. W. T. Ngai, "Deep learning in computer vision: A critical review of emerging techniques and application scenarios," Mach. Learn. with Appl., vol. 6, no. August, p. 100134, 2021. https://doi.org/10.1016/j.mlwa.2021.100134

[22] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, "Deep Learning for Computer Vision: A Brief Review," Comput. Intell. Neurosci., vol. 2018, 2018. https://doi.org/10.1155/2018/7068349

[23] A. Thakkar and R. Lohiya, A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges, vol. 28, no. 4. Springer Netherlands, 2021. https://doi.org/10.1007/s11831-020-09496-0

[24] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security," Comput. Sci. Rev., vol. 40, p. 100389, 2021. https://doi.org/10.1016/j.cosrev.2021.100389

[25] D. Zhang, Z. Liu, and X. Shi, "Transfer learning on EfficientNet for remote sensing image classification," Proc. - 2020 5th Int. Conf. Mech. Control Comput. Eng. ICMCCE 2020, pp. 2255-2258, 2020. https://doi.org/10.1109/ICMCCE51767.2020.00489

[26] S. Gang, N. Fabrice, D. Chung, and J. Lee, "Character recognition of components mounted on printed circuit board using deep learning," Sensors, vol. 21, no. 9, 2021. https://doi.org/10.3390/s21092921

[27] A. W. Reza, M. M. Hasan, N. Nowrin, and M. M. Ahmed Shibly, "Pre-trained deep learning models in automatic COVID-19 diagnosis," Indones. J. Electr. Eng. Comput. Sci., vol. 22, no. 3, pp. 1540-1547, 2021. https://doi.org/10.11591/ijeecs.v22.i3.pp1540-1547

[28] X. Han et al., "Pre-trained models: Past, present and future," AI Open, vol. 2, no. August 2021, pp. 225-250, 2021. https://doi.org/10.1016/j.aiopen.2021.08.002

[29] K. S. Lee, E. Lee, B. Choi, and S. B. Pyun, "Automatic pharyngeal phase recognition in untrimmed videofluoroscopic swallowing study using transfer learning with deep convolutional neural networks," Diagnostics, vol. 11, no. 2, 2021. https://doi.org/10.3390/diagnostics11020300

[30] L. Vogado et al., "Diagnosis of leukaemia in blood slides based on a fine-tuned and highly generalisable deep learning model," Sensors, vol. 21, no. 9, 2021. https://doi.org/10.3390/s21092989

[31] A. S. Mahdi and S. A. Mahmood, "An Edge Computing Environment for Early Wildfire

Detection," Ann. Emerg. Technol. Comput., vol. 6, no. 3, pp. 56-68, 2022. https://doi.org/10.33166/AETiC.2022.03.005

[32] K. B. Pranav and J. Manikandan, "Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks," Procedia Comput. Sci., vol. 171, no. 2019, pp. 1651-1659, 2020. https://doi.org/10.1016/j.procs.2020.04.177

[33] A. S. Sanchez-Moreno, J. Olivares-Mercado, A. Hernandez-Suarez, K. Toscano-Medina, G. Sanchez-Perez, and G. Benitez-Garcia, "Efficient face recognition system for operating in unconstrained environments," J. Imaging, vol. 7, no. 9, 2021. https://doi.org/10.3390/jimaging7090161

How to Cite

H. H. Ali, J. R. Naif, and W. R. Humood, “A New Smart Home Intruder Detection System Based on Deep Learning”, *Al-Mustansiriyah Journal of Science*, vol. 34, no. 2, pp. 60–69, Jun. 2023.