International Journal of Power Electronics and Drive System (IJPEDS)
Vol. 11, No. 1, March 2020, pp. 417~424
ISSN: 2088-8694, DOI: 10.11591/ijpeds.v11.i1.pp417-424

IoT based facial recognition door access control home security system using raspberry pi

A. R. Syafeeza[1], M. K. Mohd Fitri Alif[2], Y. Nursyifaa Athirah[3], A. S. Jaafar[4], A. H. Norihan[5], M. S. Saleha[6]
[1,3,4,5] Fakulti Kejuruteraan Elektronic and Kejuruteraan Komputer, Universiti Teknikal Malaysia, Malaysia
[6] Fakulti Teknologi Kejuruteraan, Universiti Teknikal Malaysia Melaka, Malaysia
[2] School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, Malaysia

Article Info

Article history:

Received Aug 19, 2019
Revised Nov 27, 2019
Accepted Dec 11, 2019

Keywords:

Deep learning
Facial recognition
Home security system
Internet of things (IoT)
Raspberry pi

ABSTRACT

The home security system has become vital for every house. Previously, most doors can be open by using traditional ways, such as keys, security cards, password or pattern. However, incidents such as a key loss has led to much worrying cases such as robbery and identity fraud. This has become a significant issue. To overcome this problem, face recognition using deep learning technique was introduced and Internet of Thing (IoT) also been used to perform efficient door access control system. Raspberry Pi is a programmable small computer board and used as the main controller for face recognition, youth system and locking system. The camera is used to capture images of the person in front of the door. IoT system enables the user to control the door access.

Corresponding Author:

Syafeeza Ahmad Radzi,
Fakulti Kejuruteraan Elektronik and Kejuruteraan Komputer,
Universiti Teknikal Malaysia,
Jalan Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
Email: syafeeza@utem.edu.my

1. INTRODUCTION

Nowadays, home security system is a crucial issue. Indeed, this system is to ensure properties and loves ones is always safe and protected. For the past few years, it is important to have a solid security system for home, which can secure in the most ideal and safe way [1]. Many countries are step by step deployed home security system [2]. The important part of any home security system is the person identification to enter and exit the house. Previously, people use the traditional method for their home security system. The traditional security system relies on the use of external things such as key, password and ID card to gain access [3]. However, due to some limitation, biometric takes place to deliver such a promising security system. The biometric is a unique and quantifiable parameter for individual recognition [4]. Biometric system required the used of specialized hardware such as fingerprint scanner, palm print scanner, DNA analyzer and etc. Furthermore, this specific machine required the target to touch the hardware to acquire data of human unique features. Biometric technology is viewed as a standout among the most secure verification system accessible, by giving a more elevated amount of security than conventional method [1]. Face recognition is the most famous method in biometric technology besides fingerprint characteristics [2]. This is due to more stability as face contains more features [3]. Besides, it is considered highly secure as face cannot be stolen, borrowed or forge in order to enter the house. Face recognition is likely the most natural approach to perform biometric verification between individuals [2]. Face detection is the first step of the face recognition system.

Face pictures can be caught at a distance with the use of a web camera. The individual can be recognized without physical contact on any special hardware to perceive the person's identity.

Face recognition using deep learning technique is used. Deep learning is a piece of the more extensive group of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be managed, semi-directed or unsupervised. With the deep learning, the system is improved from time to time. Some images of authorizing user are used as the database of system and the system will train the face recognition automatically. Thus, the accuracy is increased. Home security is an example of an Internet of Things (IoT) applications. IoT refers to the network of associated physical objects that can interact and trade information among themselves without the need of any human intervening [5]. IoT is a futuristic technology where devices and internet is interconnected. It is different from the internet due to internet exceed connectivity by allowing any embedded circuit to communicate with each other using the current internet infrastructure. No doubt IoT helps users to control one or more devices and capabilities to automate with many daily chores. By using IoT, it can help in controlling the door access and also sent notification throughout the internet. In this system, Blynk apps are used. Blynk apps is an app that enables us to control the door access by designing the graphical interface in the apps according to the specific function to perform. It also able to send notification to computer, smartphone and other smart devices.

2. LITERATURE REVIEW

2.1. Face recognition technology

Currently, the number of thefts and identity fraud have frequently been reported and has become significant issues. Traditional ways for personal identification requires external element, such as key, security password, RFID card, and ID card to have access into a private asset or entering public space [1]. Many processes such as drawing out money from banks requires password. Other such parking in private space would also need parking ticket. For some houses, the house key is very important. However, all this method also has several disadvantages such as losing key and forgetting password [3]. When this happens, it can be hassle to recover back. This method is slowly taken over by biometric methods as it is the possible way to solve those problems. This technique required to use the special hardware such as fingerprint scanner, palm print scanner, DNA analyzer to gather information for the vast majority of the biometric applications and the target objects have to touch with the hardware to acquire information [6]. As biometric is a technique that distinguishing physical highlights of people accordingly it has an extensive variety of utilization in security frameworks and it is viewed as one of the most secure methods [1]. Basically, biometrics can be classified in two categories which are physical and behavioral. Recently, the face recognition technology has engaged an overwhelming number of researchers and it is gradually supplanting other biometric security frameworks [7]. Face recognition is also known as image matching. It is a rapidly growing field where it is heading in a direction such that it will replace the traditional method. Face recognition is more stable among others biometric identification method as it is using the human face that results in high accuracy, lowest false recognition rate and it does not change in people's life [3]. Thus, this method is much practical for a lot of usage, including face recognition for the unlocking house door.

2.2. Method used for face recognition

In this new era, face recognition plays an important role in security and observation. Consequently, there is a requirement for a proficient and cost-effective system. Face recognition is a technique that is able to identify and verify peoples [8]. According to [9], face recognition, define as steps to identify, distinguish and processed face is compared with the images that stored in the database to verify who the person is. This face recognition has become a significant technique for user identification [10]. There are many techniques that can be used for face recognition but the Principle Component Analysis (PCA) is one of the most popular techniques used for face recognition. This method involves a mathematical procedure to transform a number of possibly correlated variables into a number of uncorrelated variables known as principle component [10]. Generally, the PCA technique for face recognition will utilize the use of Eigenfaces [6]. It is the effective and efficient ways to represent pictures into Eigenfaces component as it can reduce the size of the database of the test image. Numerous method is developed and deployed in order to improve the performance of face recognition technology.

2.3. Deep learning

Deep learning has benefited the human kind for years now. In the modern society, a deep learning technique, especially convolutional neural network used in many applications such as license plate recognition , finger-vein identification [6-11], gender recognition [6], face recognition [8-12] , emotion

recognition [13] , and other applications. Based on [9], deep learning technique is highly used for computer vision application. By using Convolutional Neural Network (CNN), it results in better performance for face detection and face recognition [11]. There are many advantages by using CNN as it can perceive patterns with high variability and robustness to distortions and simple geometric transformations like translation, scaling, rotation, squeezing, stroke width and a noise [12]. Besides, Oriented FAST and Rotated BRIEF (ORB) also as one of the techniques used for face recognition. It is used for feature extraction, which utilizes a fast binary descriptor dependent on BRIEF and is rotationally invariant. Typically, Deep Learning is based on supervised learning. The aim of Deep Learning is to make a machine capable to correctly classify images. Thus, during the supervised learning Raspberry pi are shown an image to produce an output in the form of vectors scores, with each category one.

2.3. Face recognition in raspberry pi

The first research on face recognition goes way back in 1950 in the field of psychology. The actual work of automatic machine recognition of faces really started in 1970 [14]. From all the research done, there two types of face recognition method which are the image-based face recognition and video-based recognition. Video-based face recognition is the process of finding 3D images from its 2D while the image-based recognition method, is the process by which human train the machine using a camera by showing the camera sets of still images. A Face Recognition System is a framework which consequently recognizes and additionally checks the identity of a person from digital images or a video outline from a video source [15].

Many researchers choose to use embedded device called as Raspberry Pi for training and identification purpose. The fundamental reasons why they have picked this particular component because it has high handling limit, low cost, and its capacity adjusts in various programming modes [1]. By using Raspberry Pi, it helps to resolve the limitation of PC such as its weight, size and high power consumption [3]. Raspberry Pi is a device that can divide the software part into three parts which are recording images, training and face recognition [1]. According to [1] and [3] as they deployed the used of Raspberry Pi for image capturing system, the system becomes littler, lighter and has lower power utilization. So it is more convenient compared to PC-based face recognition system.

2.3. IoT in face recognition

IoT has been applied in face recognition in many applications such as unmanned arial vehicle [16], smart classroom [17], home security system [2, 18], smart house [19], smart surveillance and many more applications. The previous implementation of IoT in face recognition are using conventional method such local binary pattern [20], neural network [21, 22], support vector machine [23], and k nearest neighbor [24]. However, in this research deep learning was being used.

3. METHODOLOGY

3.1. Overview

This project will design face recognition for real-time use. It is integrated with IoT to perform smart home security system. A deep learning technique is used in this project. In order to ensure the expected result are obtained, several major steps need to be conducted such as data collections, implementing, testing, and troubleshooting. These steps are used to analyze the data and output. With these steps, this project are able to be evaluated.

3.2. Face recognition

The prototype is built by combining the part of face recognition and IoT together. Face recognition is operated at first place. There are five steps in face recognition, which are collecting images, creating database, pre-processing images, training images and testing images.

Firstly, images are collected. These images are obtained by capturing using camera and used the existing images. This image is used for training purpose for the system to be more accurate when dealing with new images. A total of five persons, each with five pictures is taken from different positions. Each picture is approximately 268 x 350 pixels of height and width. Images that are collected are stored in the database as shown in Figure 1.

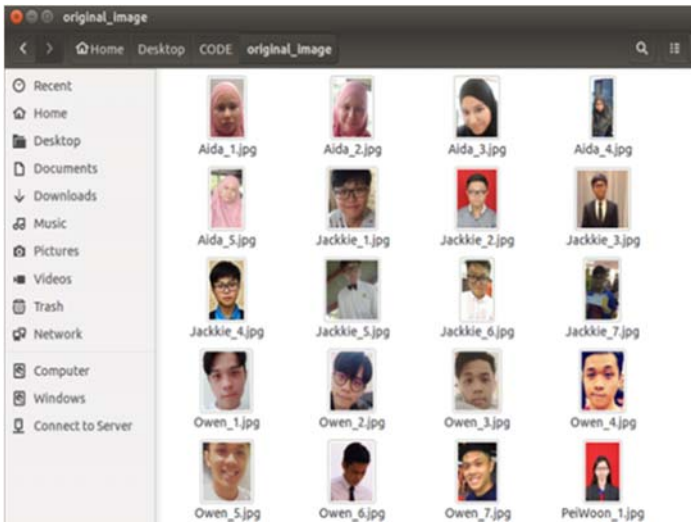
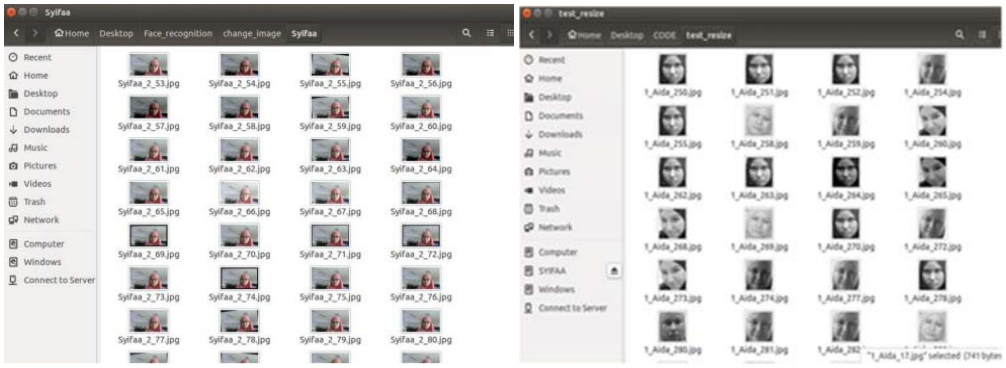


Figure 1. Numbered and labeled images

Since face recognition framework a need large number of images, existing images have been augmented. This is done by using an algorithm. Each picture per person will augment into 100 pictures, resulting 2500 images stored in database. The images vary in brightness, colour, intensity, and angle. This is to ensure that face recognition system can detect even in different conditions. Figure 2 (a) shows the transformation from the original image in the database into the processed photo. The result of each person categorized into each folder. Next, the cropping process takes place. This process will crop the exact face from the images. This process is carried out by using an algorithm. The pixel of each picture is reduced to 48 x 48 pixels of height and width. Figure 2(b) shows extract features by separating the face from the background.



(a) (b)

Figure 2. (a) Data augmentation of Images (b) Exact Face Obtained

3.3. Deep learning

Existing architecture was used in the training process. Images were train using deep learning method using Convolutional Neural Network (CNN) technique. The current architecture used is AlexNet which consist of eight layers. This architecture builds with several layer and activation function such as Convolution, Maxpooling, Flatten, Dense, Activation and Dropout. The entire neural network approach was implemented in Python language and Keras library [25]. The training involves 100 epochs at first and repeated with 20 epochs after the testing phase. Figure 3 will illustrate the training process of the dataset. After training process was done image testing is required to determine the accuracy achieved by the system. In this stage, image that are not in the database are used as test images. There are ten images tested for each

labeled which are recognized and unrecognized person. Each image tested will labeled the image with name or as an unknown.

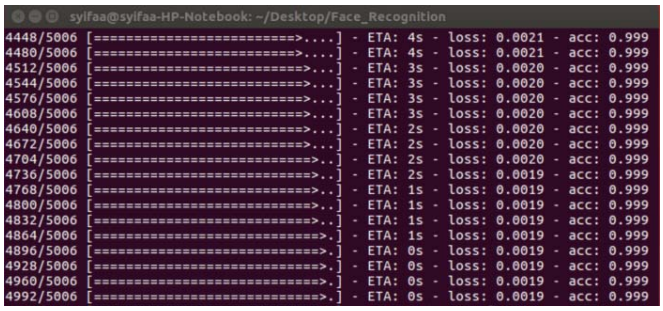


Figure 3. Training the dataset

3.4. Internet of things (IoT)

Blynk is a famous apps since it has been downloaded more than 100 thousand users. Blynk is a platform for iOS and Android apps that managed to control Raspberry pi and many other microcontrollers. It is a digital dashboard that designed for the user to create their own graphic interface for the project. It is easy and simple to use as the user can simply drag and drop the widgets that they need according to their project type. This app is used in IoT part. Blynk start online as the Raspberry Pi connected to the internet over Wi-Fi. Besides, it is also will get online by link to the internet through the Ethernet or the new ESP8266 chip. For condition where face cannot be recognized, that person can press the doorbell and notification are sent to smartphone of house owner. Hence, live streaming video will appear to identify the person trying to unlock the door.

4. RESULT AND ANALYSIS

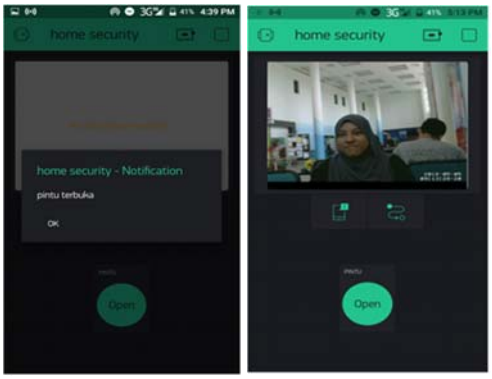
Face recognition is tested on two types which are by testing image and real-time to determine the system accuracy. For testing image, there are ten images that are not in the database are tested for each label which are authorized and unknown person. The tested image will have labeled the image with names for authorized person while unknown for unauthorized person. Figure 4 (a), (b), (c) and (d) shows the tested image with positive and negative results for authorized and unknown. Real-time face recognition is performed using web camera. An authorized person can be recognized through the system and vice versa. The name of the user will be shown below their face as shown in Figure 5 (a) while unauthorized person is shown in Figure 5 (b).

(a) (b) (c) (d)

Figure 4. (a) Positive result for authorized (b) Positive result for unknown
(c) Negative result for authorized (d) Negative result for unknown

(a) (b)

Figure 5. (a) Authorized person labeled with name (b) unauthorized person labeled with the unknown



(a) (b)

Figure 6. (a) Notification send through Blynk (b) Video streaming in Blynk

Face recognition and IoT are integrate and build in prototype. When person face can be recognized by the system, the door will open automatically as shown in Figure 4.9. If face cannot recognize by the system, door will remain closed as illustrated in Figure 7 (a) and (b). Door access can also be controlled through IoT using Blynk app.

(a) (b)

Figure 7.(a) Door is unlocking (b) Door is locked

5. CONCLUSION

As a conclusion, security system by using face recognition combined with IoT is successfully done. The face recognition is able to recognize the face and able to send notification to a user when an unknown being has been detected through IoT. On the other hand, this project is this project still has a big room of improvement to be done, especially in the efficiency of the image processing part. Due to the module used which is Raspberry Pi 3, the processing time of the coding took a long time so process the image taken and take action. By using another better module, this project can be improved greatly.

ACKNOWLEDGEMENTS

The authors would like to thank Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Education for supporting this research under PJP/2018/FTK(9D)/S01603.

REFERENCES

[1] Y. Januzaj, A. Luma, Y. Januzaj, V. Ramaj., "Real time access control based on face recognition," in *International Conference on Network security & Computer Science (ICNSCS-15)*, pp. 7-12, 2015.
[2] M. Sahani, C. Nanda, A. K. Sahu, B. Pattnaik., "Home security system based on face recognition,"" *2015 Int. Conf. Circuits, Power Comput. Technol. [ICCPCT-2015]*, pp. 1–6, 2015.
[3] G. Senthilkumar, K. Gopalakrishnan, V. S. Kumar., "Embedded image capturing system using raspberry pi system," vol. 3, No. 2, pp. 213-215, 2014.
[4] M. R. Mulla., "Facial image based security system using PCA," pp. 548-553, 2015.
[5] M. H. Jusoh & F. Bin Jamali, "Home security system using internet of things," 2017.
[6] S. S. Liew, M. Khalil-Hani, S. Ahmad Radzi, R. Bakhteri., "Gender classification: A convolutional neural network approach," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 24, No. 3, pp. 1248-1264, 2016.
[7] M. Sajjad *et al.*, "Raspberry pi assisted face recognition framework for enhanced law-enforcement services in smart cities," *Futur. Gener. Comput. Syst.*, 2017.
[8] A. R. Syafeeza, S. S. Liew, R. Bakhteri., "Convolutional neural networks with fused layers applied to face recognition," *Int. J. Comput. Intell. Appl.*, vol. 14, No. 3, 2015.
[9] A. R. Syafeeza, M. Khalil-Hani, S. S. Liew, R. Bakhteri., "Convolutional neural network for face recognition with pose and illumination variation," *Int. J. Eng. Technol.*, Vol. 6, No. 1, pp. 44-57, 2014.
[10] K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, W. H. Bin Mohd Saad., "A review of finger-vein biometrics identification approaches," *Indian J. Sci. Technol.*, vol. 9, No. 32, 2016.
[11] S. Ahmad Radzi, M. Khalil-Hani, R. Bakhteri., "Finger-vein biometric identification using convolutional neural network," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 24, No. 3, pp. 1863-1878, 2016.
[12] S. Ahmad Radzi., "A MATLAB-based convolutional neural network approach for face recognition system," *J. Bioinforma. Proteomics Rev*, vol. 2(1), pp. 1-5, 2016.
[13] M. K. M. F. Alif, A. R. Syafeeza, P. Marzuki, A. N. Alisa., "Fused convolutional neural network for facial expression recognition," in *Symposium on Electrical, Mechatronics and Applied Science 2018 (SEMA'18)*, vol. 2018, no. November, pp. 73-74, 2018.
[14] T. Tat, M. Student, L. C. Wing, P. M. Number., "Image-Based Face Detection System,".
[15] P. Kamencay, M. Benco, T. Mizdos, R. Radil, "A new method for face recognition using convolutional neural network face recognition system - state of the art," pp. 663-672, 2017.
[16] N. H. Motlagh, M. Bagaa, T. Taleb., "UAV-based iot platform: a crowd surveillance use case," *IEEE Commun. Mag*, vol. 55, No. 2, pp. 128-134, 2017.
[17] C. H. Chang., "Smart classroom roll caller system with IOT architecture," in *Proceedings - 2011 2nd International Conference on Innovations in Bio-Inspired Computing and Applications, IBICA 2011*, pp. 356-360, 2011.
[18] J. See & S. W. Lee, "An integrated vision-based architecture for home security system," *IEEE Trans. Consum. Electron*, vol. 53, No. 2, pp. 489-498, 2007.
[19] L. Y. Mano *et al.*, "Exploiting IoT technologies for enhancing health smart homes through patient identification and emotion recognition," *Comput. Commun*, vol. 89-90, pp. 178-190, 2016.
[20] Y. P. Chen, Q. H. Chen, K. Y. Chou, R. H. Wu, "Low-cost face recognition system based on extended local binary pattern," *2016 Int. Autom. Control Conf. CACS 2016*, pp. 13-18, 2017.
[21] N. A. Othman & I. Aydin, "A face recognition method in the Internet of Things for security applications in smart homes and cities," in *Proceedings - 2018 6th International Istanbul Smart Grids and Cities Congress and Fair, ICSG 2018*, pp. 20-24, 2018.
[22] S. H. Oh, G. W. Kim, K. S. Lim., "Compact deep learned feature-based face recognition for Visual Internet of Things," *J. Supercomput.*, 2018.
[23] N. Funabiki, D. Pramadihanto, R. Arridha, S. Sukaridhoto., "Classification extension based on IoT-big data analytic for smart environment monitoring and analytic in real-time system," *Int. J. Space-Based Situated Comput*, vol. 7, No, 2, pp. 82, 2017.
[24] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, M. Stanley., "A brief survey of machine learning methods and their sensor and IoT applications," *2017 8th Int. Conf. Information, Intell. Syst. Appl. IISA 2017*, vol. 2018-January, pp. 1-8, 2018.
[25] F. Chollet., "Keras: The Python Deep Learning library," *Keras.Io*, 2015.

BIOGRAPHIES OF AUTHORS

Mohammad Fitri Alif Mohammad Kasai currently is a PhD candidate in Electrical Engineering from Universiti Teknologi Malaysia. He received B.Eng degree in Mechatronics Engineering in 2011 from Universiti Selangor and his M.Eng degree in Mechatronics and Automatics Control in 2013 from Universiti Teknologi Malaysia. His PhD research is Facial Expression Recognition and Deep Learning.

Syafeeza Ahmad Radzi received her B.Eng degree in Electrical-Electronic Engineering in 2003 and her M.Eng degree in Electrical - Electronic & Telecommunication Engineering in 2005 from Universiti Teknologi Malaysia. She also received her PhD degree in Electrical Engineering from the same university in 2014. She is currently a Senior Lecturer at the Faculty of Electronic Engineering and Computer Engineering, Universiti Teknikal Malaysia Melaka (UTeM). She has been an academician in UTeM since 2006. She dedicate herself to university teaching and conducting research. Her research interests include embedded system, pattern recognition, machine learning, deep learning, image processing and biometric.