

PAPER • OPEN ACCESS

Research on Intelligent Access Control System Based on Interactive Face Liveness Detection and Machine Vision

To cite this article: Wenfeng Shi *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **563** 052094

View the [article online](#) for updates and enhancements.

Research on Intelligent Access Control System Based on Interactive Face Liveness Detection and Machine Vision

Wenfeng Shi¹, Jun Li¹, Yuanjun Ding² and Kuan Zhou³

Sichuan Agricultural University, Yaan Sichuan 625000, CHINA

lijun@sicau.edu.cn

Abstract. With the improvement of people's safety awareness and the renewal of smart home technology, access control security has become a special concern of community, schools and enterprises. How to achieve efficient, convenient, safe and intelligent access control management is the main research direction in the field of smart home right now. Based on multi-task cascade convolutional neural network (MTCNN) and improved face recognition algorithm k-Nearest Neighbor (KNN), this paper proposes an interactive face liveness detection method by eye and mouth state. According to this method, an intelligent access control system based on machine vision is designed. The system solves the problem of identity forgery attacks by calling the camera to track the face in real time and issuing randomized action instructions to the user, after confirming that the object being detected is a living body and the face information matching is successful, the door lock will be opened. The experiment shows that the face recognition rate of the system can reach 98.3%, which has good practical significance.

1. Introduction

Access control system is one of the security facilities widely used in recent years. At present, the access control system on the market is mainly divided into inductive access control system and biometric access control system [1]. The technology involved in inductive access control system includes radio frequency identification technology, IC card technology, bar code, graphic ID, etc. In [2], the author combined RFID technology with IC card technology for designing the proximity card access control system, however, the security level of the system is not high, and there is a risk of loss of the sensor card and being duplicated. Usually used for parking fees, canteen consumption, etc. As people pay more and more attention to business intelligence and residential safety, it is obvious that inductive access control system can not fully meet people's living needs. In contrast, biometric access control system can better meet the needs of contemporary economic activities and security precautions, the technologies involved include fingerprint recognition, retina recognition, face recognition, etc. In [3], the author designed a smart access control system based on fingerprint recognition technology, the system has many advantages such as cheaply productive price, high reliability, but the direction and strength of finger pressing and the degree of dryness and wetness of the skin will affect the recognition accuracy of the system to some extent.

The application of face recognition technology in access control system is also a hot research topic, which has many advantages such as non-contact, easy data collection, low power consumption of processor, energy saving, low cost, easy installation, stable performance, etc [4]. At the same time, identity forgery attack has also been the corresponding occurrence, simple face recognition technology already has great risks. In this paper, considering the security and reliability of the access control system, MTCNN is used to realize real-time face tracking, and interactive face liveness detection



method is used to judge whether the current detection object is a living body or not. if it is, the advanced texture features of the human face will be extracted through the improved face recognition algorithm KNN, and matched with backstage face database to determine whether to open the electronic door or not. Thereby effectively reducing or even avoiding the security risks caused by identity forgery attacks.

2. Design of Intelligent Access Control System

2.1. Overall Design

The system is mainly divided into four modules: face training module, interactive face liveness detection module based on eye mouth state, video monitoring and face recognition module, control and management module. The main task of the face training module is to build the face information database. After collecting facial images of all users, image analysis and uniform labeling are carried out; The interactive face liveness detection module based on eye mouth state is mainly composed of four parts: face detection, eye and mouth feature location, face motion recognition and human-machine command interaction. Its main task is to use machine vision system to distinguish whether the current detection object has identity forgery attacks. The video monitoring and face recognition module mainly consists of three parts: image preprocessing, feature extraction and identity comparison. When the face image collected by the interactive module is transmitted to this module and the current detection object is confirmed to be a living body, this module will extract the feature points of each image, and finally compare it with the face information database in the face training module. Through the result of the comparison, we can judge whether the user is legitimate or not, so as to achieve the purpose of face recognition. In addition, this module can also play the role of real-time monitoring; The control and management module is mainly used to control the closing and opening of electronic lock. When the user is judged to be legitimate, the electronic door opens. The overall design flow chart of the system is shown in Fig 1.

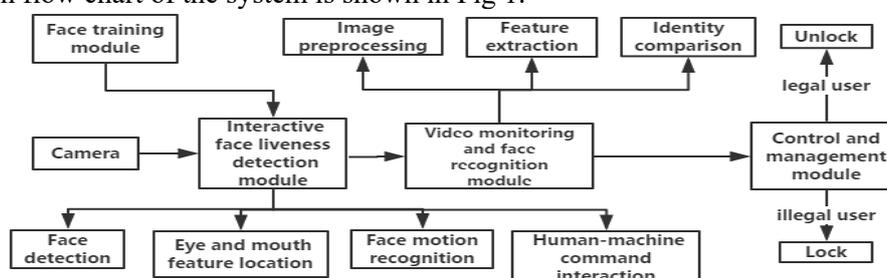


Fig 1. The overall design flow chart of the system

2.2. Face Training Module

In order to realize face recognition, firstly, we need to build a face image database and train the face images in the image database. Through training, we can extract the features of each person and get the data of face space, face image matrix and texture features. Then all the data are classified and identified and stored in the database for other modules to call. When there is a new resident living in, it is necessary to add this resident's face image samples to the face image database in time. At the same time, it is necessary to retrain all the sample images, so as to update the face database.

2.3. Interactive Face Liveness Detection Module Based on Eye and Mouth State

2.3.1. Identity Forgery Attacks

With the progress of science and technology, face recognition technology has been widely used in various fields: military, medical, civil and so on. Especially in the field of identity recognition, face recognition technology is playing an increasingly important role. But at the same time, identity forgery attack has also been the corresponding occurrence. There are three common attack

methods: photo face attacks, video face attacks and three-dimensional face model attacks.etc.Among them, photo and video face attacks are the most common at present. Because of the high technical requirements and high cost of three-dimensional face model attacks, this kind of attack is still less, but in the future it will become the main way of identity forgery attacks[5].The key problem of identity forgery attacks is how to judge the current recognition object is a living body.In order to solve this problem, in [6], the author proposed a method of combining blink detection and background analysis, which is simple and easy to operate, but it does not solve the problem of liveness detection directly .In [7],Wilder put forward a method of face detection using hot red imaging technology. This method can directly reflect the characteristics of living bodies, but the related hardware is expensive, so it is not suitable for wide-scale promotion.Robert W found a new way to judge the living body by human-computer interaction, which requires the living body to adjust its head posture[8]. This method has good real-time performance, but there are situations in which deceivers respond by posturing the same head postures with face photos. Therefore, this paper proposes an interactive face liveness detection method based on eye and mouth state.Firstly, face detection and eye and mouth location are realized by MTCNN, and then some random instructions based on eye and mouth motion are given by the system, and the detected object should make the appropriate posture according to these instructions,and the system determines whether the action is correct by tracking the face and uses it as the basis for the liveness detection.

2.3.2. Face Detection and Feature Point Location Based on MTCNN

In 2016, Zhang proposed a multi-task face detection framework, MTCNN[9],which has three network structures: Proposal Network (P-Net), Refine Network (R-Net), Output Network (O-Net).When the face image enters the P-net for processing,MTCNN will scale the image to form an image pyramid firstly, which achieves the goal of making image size the same. P-net is a full convolution network used to generate candidate windows and bounding box regression vectors,and it uses bounding box regression to calibrate, then uses non-maximum suppression (NMS) to remove a large number of repetitive candidate regions.R-net has one more full connection layer than P-Net, which can be processed in more detail.R-Net scales the face frame computed by P-Net, as input to itself, and the candidate boxes with scores below the threshold will be discarded, others will be merged by NMS, finally, the face frame selected from the P-Net result is obtained.O-net has one more convolution layer than R-Net. Its implementation principle is similar to R-Net, and it can output the landmark position of eyes, mouth and nose.Therefore, when inputting a face image, MTCNN can rely on the powerful third-order network to complete the tasks of face determination, boundary box regression, facial feature point location ,etc.Finally, the region image of human face can be obtained, in which the human eye region extracts $32 * 32$ from the human eye feature points, while the mouth region intercepts $60 * 50$ from the two corners of the mouth.

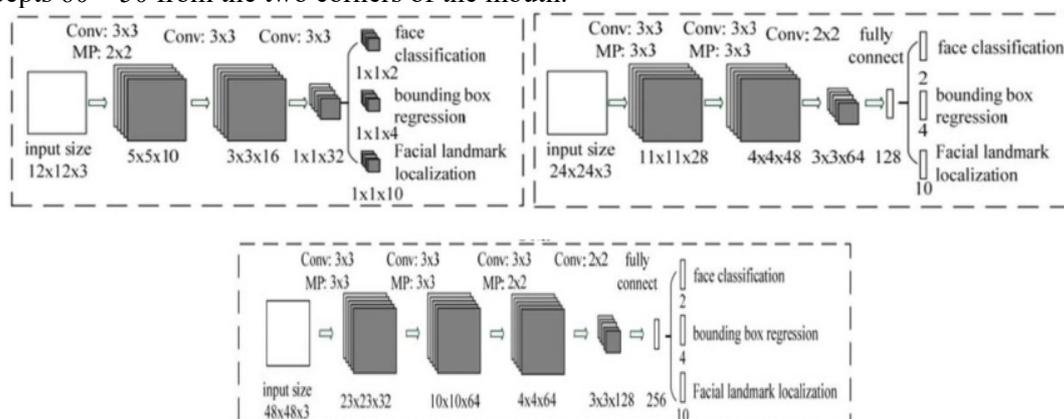


Fig 2. The structure of P-net,R-net and O-net

2.3.3. Recognition of Eye and Mouth State

Identifying the pose of a person's face requires determining the position of the face, eyes, and mouth and obtaining images of the eye and mouth area. In this paper, the open and close states of human eyes and mouth are identified by a convolutional neural network. As shown in Fig 3, a simple three-layer network structure is constructed, which has three convolution layers. Each convolution layer connects one pooling layer to reduce the size of the matrix, and the dropout layer is used to prevent over-fitting. The network structure can train two models for eye and mouth state recognition respectively.

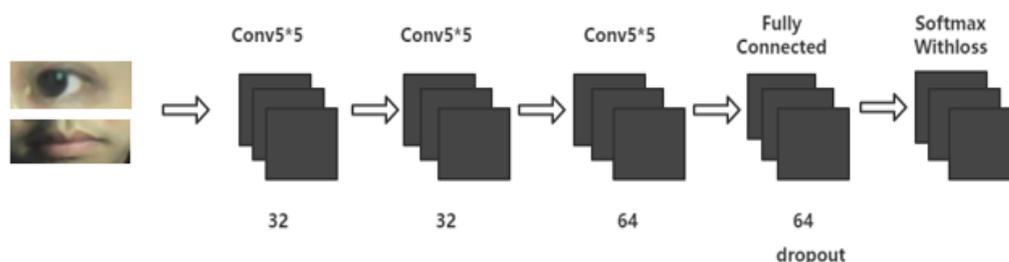


Fig 3. The structure of the convolutional neural network

2.3.4. Human-machine Instruction Interaction

As shown in Fig 4, this paper designs the following four instructions for users to complete: 1. Open and close your mouth, 2. Open your left eye and close your right eye, 3. Close your left eye and open your right eye, 4. Close your eyes. After the system has trained the eye and mouth state identification model, the system randomly selects two or more instructions from the above instructions and requires users to complete them in 5 seconds. Then, according to the position of the feature points, the system analyses whether the user has completed the specified action or not. Since each action is randomly selected from 4 instructions (the instruction does not appear repeatedly), and the number of instructions that need to be completed by the user is uncertain (≥ 2), there are a total of 468 possibilities. So the probability of using photos or pre-recorded videos to pass the authentication is extremely low.

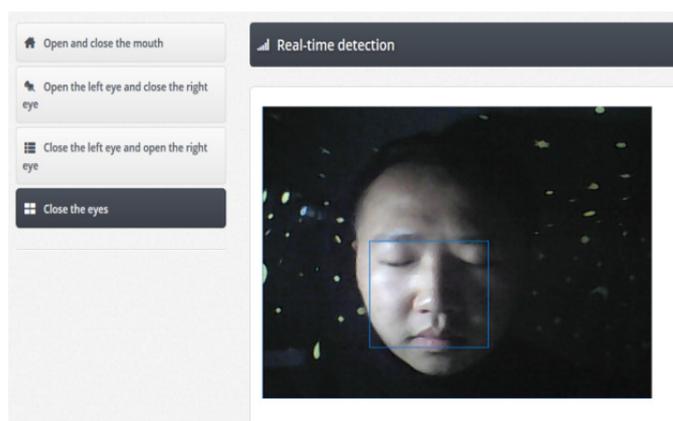


Fig 4. The Interface of human-machine Interactive

2.4. Face Recognition Module

2.4.1. Current Situation of Face Recognition Technology

After the success of liveness detection, the next task is to input the face images collected by machine vision system into the established face recognition model for face feature matching and decision recognition. Face recognition technology is a technology that uses computer to analyze face images and extract effective recognition information from them for identifying identity[10]. According to the

different research contents in each research period, the development process of face recognition can be divided into three parts: the algorithm based on geometric features, the algorithm based on artificial features and the algorithm based on deep learning. In [11], Zhang Shujun proposed a face recognition algorithm based on active appearance model (AAM). By comparing the Similarity of geometric feature vectors between the input image and the database image, the algorithm can effectively improve the face recognition speed and reduce the false positive rate. However, this method requires high-quality images, and the changes of facial posture and expression have a great impact on the accuracy of recognition. In 2013, Chen used artificial features for face recognition. Taking local binary pattern (LBP) as an example, he discussed the positive correlation between high-dimensional features and verification performance, that is, the higher the dimension of face, the higher the accuracy of verification [12]. The remarkable advantage of this method is that it is insensitive to illumination, but it still does not solve the problem of posture and expression. In [13], Taigman proposed a method of face recognition based on deep convolution neural network, DeepFace. In this paper, 3D model is used for face alignment task. And the deep convolutional neural network classifies the aligned face patches and achieves an accuracy of 97.35% on the LFW, but the algorithm is complex and the recognition speed is slow. In summary, face recognition technology has made great progress in recent decades. In order to make the access control system more real-time, this paper completes face recognition by improving KNN algorithm.

2.4.2. Improving KNN Algorithm for Face Recognition

When MTCNN realizes face detection and feature point location, it is necessary to select appropriate face recognition algorithm for further analysis. This paper improves the classical KNN algorithm to achieve the purpose of face recognition. KNN algorithm is one of the most widely used classification algorithms. It is often used in text classification, pattern recognition and other fields. Because of its simple, fast and easy to implement, KNN is also often used in the field of face recognition. The application of kNN algorithm in the field of face recognition can be summarized that give a sample of face image, find out the closest (most similar) K-images in the training image set and determine the category of the sample according to the category of the k-images. However, the traditional KNN algorithm has the disadvantage of slow classification, and is not suitable for real-time access control systems. Combining with the improvement directions of several algorithms proposed in [14] and the practical application scenarios of access control system, this paper improves KNN algorithm from the improvement of distance calculation. The traditional KNN algorithm mostly calculates the distance between two samples by Euclidean distance formula. Its disadvantage is that the weight of each attribute is the same, but the contribution of each attribute to the final result is different in the actual sample set. So, the main problem of KNN algorithm improvement is to determine which attributes are strongly correlated, weakly correlated and uncorrelated. Based on this, Chen Zhenzhou proposed a Feature-Weighted KNN algorithm based on Support Vector Machine (SVM), which can solve the dimension disaster problem brought by traditional algorithm very well [15]. In the field of image classification, Hou Yuting proposed a feature adaptive weighted natural image classification algorithm based on KNN. This algorithm weights the color and texture features of the image and gives color features higher weights, thus effectively improving the classification effect of natural images [16].

Compared with the complex and changeable natural image, the face image studied in this paper is more simple and intuitive. Selecting too many features to weigh will increase the complexity of the algorithm. Because of the high discriminability of face texture feature [17], this paper uses the multi-scale and multi-directional characteristics of Gabor wavelet to extract face texture feature by Gabor filter and regards it as the maximum correlation attribute of KNN model.

2.5. Control and management module

The control management module is the execution module of the system. The module is divided into three parts: the access control part, the client part, and the server part. The access control part is mainly composed of an electronic lock and related control components, and the client part is mainly used for

user management, such as adding and deleting users.the server part is the core part of this module. This part is mainly responsible for receiving the result data of face information comparison in face recognition module, then converting the result data into a level signal and transmitting it to the access control terminal, and controlling the switch of the electronic lock through the level signal.

3. Experimental Results and Analysis

The experimental environment:HD 1080P camera, MySQL version 5.5, Tomcat version 8.0, Python version 3.6, Windows 10 operating system.

3.1. Face Image Training

There are two parts in face image training: 1. Using improved KNN model to verify the accuracy of LFW database; 2. Testing improved KNN model on our own data.Firstly, we use LFW to train the improved KNN model. When the accuracy of face recognition reaches more than 95%, we save the model well.Then we simulate and build the training sample database of face image needed in this experiment. We set up a total of 10 people in the sample database, each person has 10 face images, and label each image separately, a total of 100 images.After training on our own data, a face image test sample library is established separately to test the recognition accuracy of KNN model. After testing, the face recognition rate of this model can reach 98.3%.



Fig 5. Some Data of Training Sample Database of Face Image



Fig 6. Part of Data of Face Image Test Sample and The Test Result

3.2. Face Detection and Feature Location

In order to verify the effect of MTCNN in face detection under the condition of insufficient illumination or facial occlusion in real application, the interference factors of dark background and wearing glasses are specially set in this experiment. As can be seen from Fig 7, MTCNN has good robustness to illumination and facial occlusion. It can be applied to all kinds of people even at night.

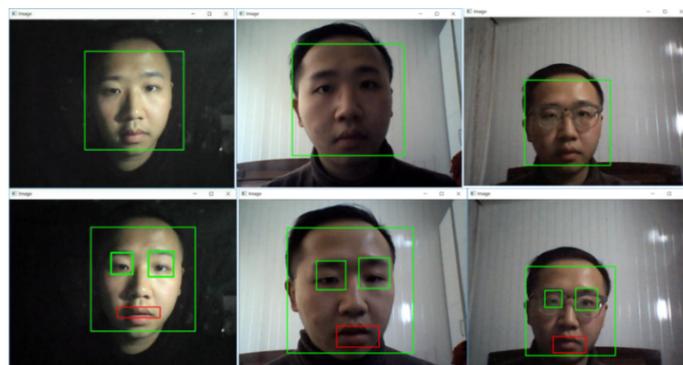


Fig 7. Face Detection and Feature Location

3.3. Face Recognition

In the face recognition testing process, the camera is first activated for face detection and recognition. As shown in Figure 8, if the face data to be recognized is not stored in the face image database, the person is determined to be illegal and appears "unknown people, No access". If the face to be recognized already exists in the face image database, the person is determined to be legitimate and appears "resident xx, Allow access".



Fig 8. Results of Face Recognition

4. Conclusion

In this paper, an intelligent access control system based on interactive face liveness detection and machine vision is designed. The key issues of our work are to avoid identity forgery attacks through human-computer instruction interaction and achieve face recognition using improved KNN algorithm based on texture features. Experiments show that this method can realize the basic functions of the access control system and effectively resist photos, and video face attack, but in the face of three-dimensional face model attack, the interactive face liveness detection method proposed in this paper only has very weak preventive ability, but it will be addressed in our future work.

Acknowledgments

This research was supported by Scientific Research Project of Sichuan Provincial Department of Education: Research on New Agricultural Internet of Things Intelligent Management System Based on Zigbee Technology (project number: 17ZB0336).

References

- [1] Lei Yu Tang 2007 The comparison and development of various access control systems[J] *Public Security in China (Market Edition)* pp 94-99 (in Chinese)
- [2] He Lifang, Fan Junbo 2004 Research and realization of sensor card access control system [J] *Information Technology* pp73-75 (in Chinese)

- [3] Wu Chengfeng and Zhao Zhenhua 2012 Research on intelligent access control system based on fingerprint identification technology [J] *Application of Microcomputer* pp 45-47 (in Chinese)
- [4] Li Jun, Meng Shige, Fan Quanchang and Chen Jin 2013 Design and implementation of access control system based on face recognition [J] *Automation and Information Engineering* pp30-34 (in Chinese)
- [5] Luo Hao 2015 Research on biological detection method in face recognition [D] *Hunan Normal University* (in Chinese)
- [6] Zhang Gaoming and Feng Rui 2017 Face-based biopsy detection system[J] *Computer system application* pp37-42.(in Chinese).
- [7] Wilder J and Phillips PJ 1996 Comparison of visible and infra-red imagery for face recognition[C] *Institute of electric and electronic engineer* pp182-187
- [8] Robert W,Frischholz and Alexander Werner 2003 Avoiding replay-attacks in a face recognition system using head-pose estimation[C] *IEEE International Workshop on Analysis and Modeling of Faces and Gestures* pp234-235
- [9] Zhang Kaipeng,Zhang Zhanpeng and Li Zhifeng 2016 Joint face detection and alignment using multi-task cascaded convolutional networks[J]
- [10] Zhang Cuiping and Su Guangda 2000 Overview of face recognition technology [J] *Chinese Journal of Image and Graphics* pp7-16 (in Chinese)
- [11] Zhang Shujun, Wang Gaofeng and Shifeng 2013 Face recognition algorithms based on AAM extracting geometric features [J] *Journal of Systems Simulation* pp2374-2380 (in Chinese)
- [12] Chen Dong,Cao Xudong and Wen Fang 2013 Blessing of dimensionality: high-dimensional feature and its efficient compression for face verification[C] *2013 IEEE Conference on Computer Vision and Pattern Recognition* pp3025-3032
- [13] Taigman, Yaniv,Yang, Ming,Ranzato and Marc'Aurelio 2014 DeepFace: closing the gap to human-level performance in face verification[C] *2014 IEEE Conference on Computer Vision and Pattern Recognition(CVPR 2014* pp1701-1708
- [14] Xiaomei Bi and Ruihua Bi 2009 A summary of knn algorithms [J] *Science and Technology Innovation Herald* (in Chinese)
- [15] Chen Zhenzhou, Li Lei and Yao Zhengan 2005 Feature-weighted KNN algorithm based on SVM [J]*Journal of Sun Yat-sen University (Natural Science Edition)* pp17-20 (in Chinese)
- [16] Hou Yuting, Peng Jinye, Hao Luwei and Wang Rui 2014 Research on feature adaptive weighted natural image classification based on KNN [J] *Computer Application Research* pp957-960 (in Chinese)
- [17] Yao Yongtian 2016 Face recognition based on image texture feature extraction [D]. *China University of Metrology* (in Chinese)