Face recognition using machine vision for Security system

F S A Saad¹, M V Lee¹ and S Basah¹
¹School of Mechatronic Engineering, Universiti Malaysia Perlis (UniMAP)

Abstract. The aim of this project is to design and develop a face recognition based security system using machine vision. In this paper, a face recognition system using Principal Component Analysis (PCA) with Euclidean distance classifier is proposed. PCA is selected as it is less sensitive to noise and interference, besides reducing the number of variables in face recognition which reduce computational time and increase accuracy. A number of experiments were done to evaluate the performance of the face recognition system. A training database of 20 students is created and used in this project. Overall, the face recognition system on static face images has 86% success rate and 14% error rate which is mainly due to the variation of pose orientation. It is also found that the threshold value is an important factor for the performance of face recognition. The distance of the person to the camera play a role as the further the person is away from the camera, the more blur the face image captured. As for the anti-spoofing approach, the proposed detection of eye blinking is successfully tested with training eyes open and eyes close images.

1. Introduction
Face recognition technology is the machine vision system that emulates the capabilities of human eyes to detect and recognise faces. Due to its nonintrusive nature, face recognition can easily be executed where it works with human face that is the most obvious individual identifier without the need of participation of that person [1]. The input image characteristics of a person’s face image will be analysed and necessary facial features are taken out from the face and retained in a database which will then be used as a comparison when a user stands before the camera [2]. This paper aim is to design and develop a security system using machine vision for face recognition using IoT. The best feature extraction and classification approach is chosen to develop a more robust system which yields more accurate results, meet the standard of security systems, besides being spoof-proof to take care of our privacy and safeguard our assets.

2. Methodology

2.1. Introduction
The security system developed consists of several components, which is face database component, motion detection component, face detection component, face recognition component, IoT and the anti-spoofing approach.

2.2. Facial database
A face database is required for comparison and scoring during the recognition process. For this project, 20 samples are taken for the creation of face database. 5 images are taken from each sample with 3 frontal face images of different facial expression and 2 more side face images. All 100 face images are
pre-processed on MATLAB, where it is converted from RGB to grayscale and then resized into resolution of 112 X 92 pixels.

2.3. Face detection component
The initial step of human face recognition system is face detection. The face detection algorithm used is the Viola-Jones Algorithm. Viola-Jones combined many weak classifiers to create a strong classifier. Four main concepts are introduced in the Viola-Jones algorithm, which are the Haar-like features, the integral image, the use of AdaBoost in machine training and a cascade of classifiers.

2.3.1. Haar-like features
At this stage, the Haar feature is found by calculating the difference of the pixels on the black portion to the pixels on the white portion [3]. There are few types of Haar feature, for instance the two rectangle, three triangle and four triangle Haar features.

![Figure 1. The type of Haar features](image)

2.3.2. Integral image
Next step is turning input image into integral image. Integral image is the intermediate form of the rectangular features of an image [4].

2.3.3. AdaBoost machine learning
AdaBoost is a machine learning boosting algorithm where large very number of features is reduced and a small set of features is selected. Adaboost develops the classifier that self learns and adapts the threshold value for selecting the features from the overall features to build a strong classifier [5].

2.3.4. Cascading
In the cascading step, the face area of the image is determined. The classifier uses the form of a degenerate decision tree, the window is either rejected or passed and this process is repeated to get accurate face detection. All the intermediate classifiers need to be passed. The weight given by AdaBoost determines the order on the cascade. The aim is to obtain the least false negative and to get low rates of error as set by AdaBoost thresholds value in default. Eliminating the undesired regions is the key to enhance the probability for the correct face detection.

2.4. Face recognition component
In the facial recognition component, the input face image is tested with the training image in the database. Both training image and test image goes through the principle component analysis (PCA) feature extraction, which is then classified using the Euclidean distance classifier.

![Figure 2. The general idea of the face recognition system](image)
2.4.1. Principal Component Analysis (PCA)
For feature extraction, PCA is chosen because it is good at reduction of dimension where data is compressed. By representing high dimension data of face images with lower dimension data, it reduces the complication and intricacy of sorting the images in groups. PCA defines original data with calculated eigenvectors and eigenvalues when it is projected onto a lower dimensional feature space. PCA captures the most distinctive data component from the face image which helps in maximising between-class data separation [7]. The detailed procedure of PCA algorithm is described in Figure 3.

Figure 3. The detailed procedure of PCA algorithm

2.4.2. Classification of face images
In this project, classification is performed by comparing the projection vectors of the training face images with the projection vector of the input face image based on the Euclidean distance classifiers between the faces classes and the input face image. The classifier computes the square root of distance between the coordinates of two objects.

2.4.3. Anti-spoofing approach
The anti-spoofing approach proposed in this system is by detecting blinking eyes. Eye blinking is detected from analysing one by one each sequence image to classify the state of either opened eye or closed eye. The eye area is detected by Viola-Jones method, while the blinking of eyes are detected using Histograms of Oriented Gradients (HOG) as features and Support Vector Machines (SVM) as binary classifiers.

3. Results and discussion

3.1.1. Static test
Test 1 is frontal face with normal expression, Test 2 is frontal face with smile expression, Test 3 is frontal face with other expression, Test 4 is left-sided face and Test 5 is right-sided face. The recognition rate is 86% with 14% error rate which is mainly caused by pose variation of face images. Side face image has parts of the face occluded affecting the feature extraction thus affecting the recognition process. Those highlighted are the false positive points, where the faces recognised is not that of the test face image but other identity.
### Table 1. Recognition result on static face images with variation of expression and pose

| Test Image | Test 1 | Test 2 | Test 3 | Test 4 | Test 5 |
|------------|--------|--------|--------|--------|--------|
| S1         | Min. Dist. | T/F    | Min. Dist. | T/F    | Min. Dist. | T/F    | Min. Dist. | T/F    | Min. Dist. | T/F    |
| S2         | 2.06E+13   | TRUE  | 3.14E+13   | TRUE  | 1.98E+13   | TRUE  | 2.42E+14   | TRUE  | 1.94E+14   | TRUE  |
| S3         | 8.54E+13   | TRUE  | 4.41E+13   | TRUE  | 4.33E+13   | TRUE  | 3.18E+14   | TRUE  | 4.23E+14   | TRUE  |
| S4         | 6.42E+13   | TRUE  | 5.39E+13   | TRUE  | 3.21E+14   | TRUE  | 2.03E+14   | TRUE  | 1.02E+15   | FALSE |
| S5         | 2.90E+14   | TRUE  | 2.24E+14   | TRUE  | 2.17E+14   | TRUE  | 2.96E+14   | TRUE  | 1.62E+14   | TRUE  |
| S6         | 2.13E+14   | TRUE  | 7.19E+14   | FALSE | 3.94E+14   | TRUE  | 1.91E+14   | TRUE  | 3.18E+14   | TRUE  |
| S7         | 3.37E+14   | TRUE  | 1.22E+14   | TRUE  | 2.34E+13   | TRUE  | 7.37E+14   | FALSE | 6.53E+14   | FALSE |
| S8         | 6.67E+13   | TRUE  | 4.70E+13   | TRUE  | 9.74E+13   | TRUE  | 9.48E+14   | TRUE  | 8.15E+14   | TRUE  |
| S9         | 2.98E+14   | TRUE  | 2.32E+14   | TRUE  | 2.57E+14   | TRUE  | 1.56E+14   | TRUE  | 3.27E+14   | FALSE |
| S10        | 2.76E+13   | TRUE  | 2.45E+13   | TRUE  | 2.49E+14   | TRUE  | 5.40E+14   | FALSE | 8.24E+14   | TRUE  |
| S11        | 4.24E+14   | TRUE  | 3.34E+14   | TRUE  | 2.69E+14   | TRUE  | 5.14E+14   | TRUE  | 3.71E+14   | TRUE  |
| S12        | 9.14E+13   | TRUE  | 7.14E+13   | TRUE  | 2.32E+14   | TRUE  | 2.10E+14   | FALSE | 8.63E+14   | TRUE  |
| S13        | 8.48E+13   | TRUE  | 8.90E+13   | TRUE  | 7.46E+13   | TRUE  | 4.16E+14   | TRUE  | 3.39E+14   | TRUE  |
| S14        | 2.96E+14   | TRUE  | 2.48E+14   | TRUE  | 1.28E+14   | TRUE  | 3.09E+14   | TRUE  | 9.74E+14   | FALSE |
| S15        | 2.20E+14   | TRUE  | 1.82E+14   | TRUE  | 2.11E+14   | TRUE  | 5.76E+14   | TRUE  | 9.82E+14   | FALSE |
| S16        | 5.08E+14   | TRUE  | 1.25E+13   | TRUE  | 2.09E+13   | TRUE  | 6.87E+14   | TRUE  | 1.12E+15   | FALSE |
| S17        | 8.14E+13   | TRUE  | 7.40E+13   | TRUE  | 3.54E+14   | TRUE  | 4.92E+14   | FALSE | 5.56E+14   | FALSE |
| S18        | 1.74E+14   | TRUE  | 2.60E+14   | TRUE  | 1.61E+14   | TRUE  | 9.90E+14   | TRUE  | 1.42E+15   | TRUE  |
| S19        | 3.62E+14   | TRUE  | 4.37E+14   | TRUE  | 3.58E+14   | TRUE  | 6.34E+14   | TRUE  | 4.82E+14   | TRUE  |
| S20        | 1.80E+14   | TRUE  | 1.74E+14   | TRUE  | 1.29E+14   | TRUE  | 2.56E+14   | TRUE  | 6.87E+14   | FALSE |

### Figure 3. Successfully recognised face

![Successfully recognised face](image1)

### Figure 5. Unregistered face which is not recognised

![Unregistered face](image2)

3.1.2 Real-time test

The distance of the camera to the person testing the system is being considered in the real-time test besides having the variables of facial expression and pose variation as in the static test. The distance between the camera to the person tested in real-time test is 90cm, 120cm and 150cm as shown in figure 6. When the distance of the person to the camera is further, the face image captured is blurer. Thus, the principal components extracted from blur face image is not accurate when compared to those of training images in the database. Besides, the anti-spoofing approach is successfully tested in real-time as shown in figure 7.
4. Conclusion
In conclusion, face recognition can be applied for security purpose, such as access control, immigration verification and even criminal identification. In this paper, a security system using machine vision for face recognition is developed using Viola-Jones method to detect face, Principal Component Analysis (PCA) for feature extraction and Euclidean distance classifier. The integration of Internet of Things (IoT) with the system is also proposed. The algorithm performs relatively well in terms recognition rate and computational time under controlled environment. The face recognition can be further improved by increasing the training image and using 3D image processing where the risk of spoofing is hugely reduced.

Acknowledgement
First and foremost, special appreciation goes to my student Mar Vin for his assistance and constant support. His dedicated involvement throughout the whole project contributed to the success of this
research and accomplishment of this paper. To those who indirectly contributed in this research, your kindness means a lot to me. Thank you very much.

References
[1] K. Dharavath, F. A. Talukdar, and R. H. Laskar, Study on Biometric Authentication Systems, Challenges and Future Trends. (IEEE Int. Conf. Comput. Intell. Comput. Res. image).
[2] N. Bakshi and V. Prabhu, Face recognition system for access control using principal component analysis, (ICCT 2017 - Int. Conf. Intell. Commun. Comput. Tech).
[3] I. Gusti Ngurah Made Kris Raya, A. N. Jati, and R. E. Saputra, Analysis realization of Viola-Jones method for face detection on CCTV camera based on embedded system, (Proc. 2017 Int. Conf. Robot. Biomimetics, Intell. Comput. Syst. Robionetics 2017),
[4] R. B. B and M. Sharmila Kumari, (Comparative Study on Face Detection Algorithms),
[5] M. Ayi, A. K. Ganti, M. Adimulam, and B. Karthik, Interfacing of MATLAB with Arduino for face detection and tracking algorithm using serial communication, (Proc. Int. Conf. Inven. Comput. Informatics).
[6] M. Saraswathi and S. Sivakumari, Evaluation of PCA and LDA techniques for Face recognition using ORL face database, ( Int. J. Comput. Sci. Inf. Technol).
[7] K. S. Sodhi and M. Lal, Face Recognition Using PCA, LDA and Various Distance Classifiers. (J. Glob. Res. Comput. Sci).