

Face Recognition on Bag Locking Mechanism

Mohamad Hafis Izran Ishak^{1*}, Nurul Hawani Idris² and Shafishuhaza Sahlan¹

¹School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia

²Faculty of Built Environment & Surveying, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia

*Corresponding author: hafis@utm.my

Abstract: With the emergent of biometric technology, people are no longer afraid to keep their important things in the safe box or room or even facility. This is because; human beings have unique features that distinguish them with other people. The scheme is based on an information theory approach that decomposes face images into a small set of characteristic feature images called ‘Eigenfaces’, which are actually the principal components of the initial training set of face images. In this report, thorough explanation on design process of face recognition on bags locking mechanism will be elucidated. The results and analysis of the proposed design prototype also presented and explained. The platform for executing the algorithm is on the Raspberry Pi. There are two artificial intelligent techniques applied to manipulate and processing data which is fuzzy logic and neural networks. Both systems are interdependent with each other, so that it can calculate and analyse data precisely. The receive image from the camera is analysed through the Eigenfaces algorithm. The algorithm is using Principal Component Analysis (PCA) method which comprise of artificial neural network paradigm and also statistical paradigm.

Keywords: face recognition, principal component analysis, eigenvectors, eigenfaces.

© 2019 Penerbit UTM Press. All rights reserved

Article History: received 1 June 2019; accepted 16 July 2019; published 31 August 2019.

1. INTRODUCTION

With the emergent of biometric technology, people are no longer afraid to keep their important things in the safe box or room or even facility. This is because; human beings have unique features that distinguish them with other people. Face recognition is one of biometric technologies that recognise a face based on the visual pattern. The system generally consists of four modules as depicted in Figure 1; detection, alignment, feature extraction, and matching, where localization and normalization which is face detection and alignment are processing steps before facial feature extraction and matching is performed.

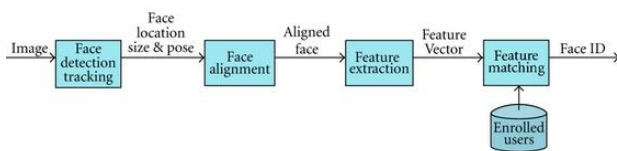


Figure 1. Face Recognition process flow

The scheme is based on an information theory approach that decomposes face images into a small set of characteristic feature images called ‘Eigenfaces’, which are actually the principal components of the initial training set of face images. Recognition is performed by projecting a new image into the subspace spanned by the Eigenfaces (‘face space’) and then classifying the face by comparing its position in the face space with the positions of the known individuals. The Eigenface approach gives us efficient way to find this lower dimensional space.

Eigenfaces are the Eigenvectors which are representative of each of the dimensions of this face space and they can be considered as various face features. Any face can be expressed as linear combinations of the singular vectors of the set of faces, and these singular vectors are eigenvectors of the covariance matrices.

The technology is suitable to be integrated with security technology in terms of hardware and software. An example is given in Figure 2. Besides security access control, locking mechanism that implements face recognition has been successfully preventing unauthorised person from accessing the content it’s protected such as safety box locking mechanism. In this report, thorough explanation on design process of face recognition on bags locking mechanism will be elucidated. The results and analysis of the proposed design prototype also presented and explained.



Figure 2. Face recognition on bags

2. PROBLEM STATEMENT

People are so careless when they are trying to keep something important especially when the thing is small for example key. The situation can be dent if the bearer is in rush and busy condition. All kind of bags that keeps people personal stuff have this type of locking mechanism. Not to mention, the mechanism would having technical problem which is hard to unlock during dire situation could be troublesome to the owner. By introducing face recognition bag locking mechanism on all types of bags, people are no longer suffering from all sorts of problem aforementioned.

In this work, the face recognition system is going to be implemented along with all sorts of bag. The platform for executing the algorithm is on the Raspberry Pi. By doing that, the following are the design objectives:

- 1) Running the face recognition algorithm successfully on the Raspberry pi.
- 2) Implement ambient light sensor by designing it using fuzzy logic control system as the assistive mechanism of the face recognition system.
- 3) Accurately and precisely identified the face prompted to unlock the system

Integrating fuzzy logic system with artificial neural network system on a single face recognition system.

3. PROJECT DESIGN

In this design, there are two artificial intelligent techniques applied to manipulate and processing data which is fuzzy logic and neural networks. Both systems are interdependent with each other, so that it can calculate and analyse data precisely. The decision making for the output of the system is fully determined by the neural network while the fuzzy logic system is only used as a decision support system.

3.1 Fuzzy Logic Design

The captured image accuracy is highly affected by the surrounding brightness level. Due to that, a fuzzy logic system has to be developed to determine and enhance the surrounding brightness. As the first step, the system input and output has to be identified first as shown in Figure 3. From the fuzzy sets, the inference rule can be developed for decision making.

Table 1. Inference Rule

Ambient light \ Camera angle	Dark	Medium	Bright
Negative Medium	High	Medium	Medium
Negative Small	High	Medium	Low
Zero	Medium	Medium	Low
Positive Small	Medium	Low	Low
Positive Medium	Low	Low	Low

The fired rule base is determined using the following Mamdani method of inference (Max-Min);

$$\mu_B^{(k)}(y) = \text{Max}\{\text{Min}[\mu_{A1}^{(k)}(\text{input}(i)), \mu_{A2}^{(k)}(\text{input}(j))]\} \quad (1)$$

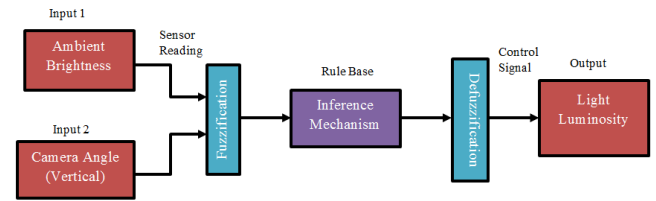


Figure 3. Block diagram of fuzzy logic controller

On the other hand, the determined inputs and output have the fuzzy sets as shown in Figure 4:

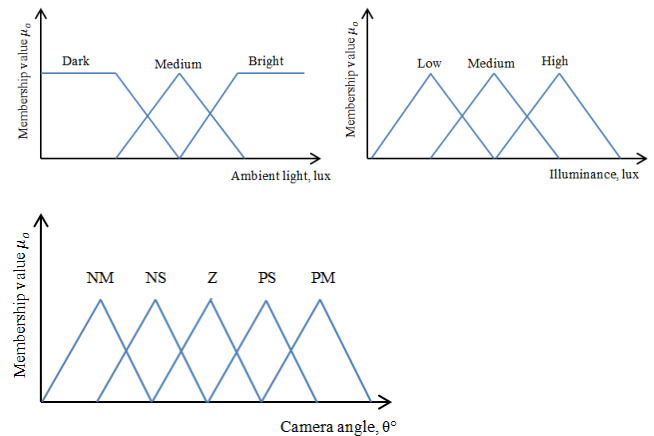


Figure 4. Fuzzy sets of designed inputs and output

The inference or firing with this fuzzy relation is achieved through the operations between the fuzzified crisp input and the fuzzy relation of the overall set of rules. As a result of the composition, the fuzzy set describing the fuzzy value of the overall control output is obtained.

After that, the obtained fuzzy value needs to be mapped from a space of fuzzy control actions into a space of non-fuzzy (crisp) control action to actuate the plant or in this case LED, this is because LED can only be operated using the crisp value. The process is known as defuzzification process; for this design, the defuzzification method used is the centre of gravity method. The formula is as follows;

$$Z^* = \frac{\sum \mu_z(z) \cdot z}{\sum \mu_z(z)} \quad (2)$$

3.2 Artificial Neural Network Design

In this design, the receive image from the camera is analysed through the Eigenfaces algorithm. The algorithm is using Principal Component Analysis (PCA) method which comprise of artificial neural network paradigm and also statistical paradigm. The PCA is a method of projection to a subspace and is widely used in pattern recognition. An objective of PCA is the replacement of correlated vectors of large dimensions with the uncorrelated vectors of smaller dimensions. Another objective is to calculate a basis for the data set. Main advantages of the PCA are its low sensitivity to noise, the

reduction of the requirements of the memory and the capacity, and the increase in the efficiency due to the operation in a space of smaller dimensions.

The strategy of the Eigenfaces method consists of extracting the characteristic features on the face and

representing the face in question as a linear combination of the so called ‘eigenfaces’ obtained from the feature extraction process. The face recognition algorithm flowchart is given in Figure 5.

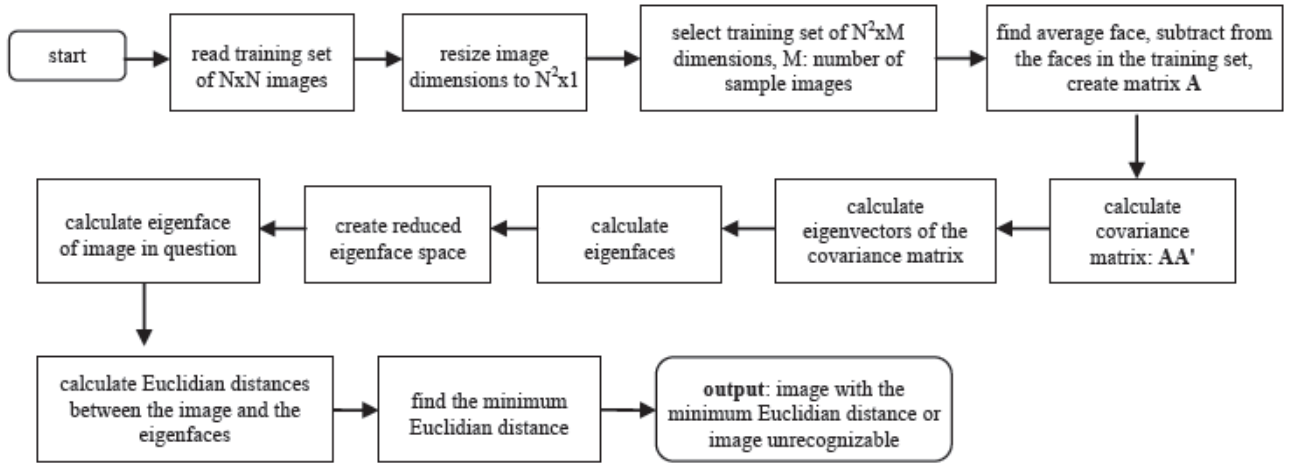


Figure 5. Face recognition algorithm flowchart

The principal components of the faces in the training set are calculated. Recognition is achieved using the projection of the face into the space formed by the eigenfaces. A comparison on the basis of the Euclidian distance of the eigenvectors of the eigenfaces and the eigenface of the image under question is made. If this distance is small enough, the person is identified. On the other hand, if the distance is too large, the image is regarded as one that belongs to an individual for which the system has to be trained.

Let $X = \{x_1, x_2, \dots, x_3\}$ be a random vector with observations which represent the receive image, $x_i \in R^d$.

Compute the mean μ ,

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i \quad (3)$$

Compute the the Covariance Matrix S ,

$$S = \frac{1}{n} \sum_{i=1}^n (x_i - \mu)(x_i - \mu)^T \quad (4)$$

Compute the eigenvalues λ_i and eigenvectors v_i of S ,

$$Sv_i = \lambda_i v_i, \quad i = 1, 2, \dots, n \quad (5)$$

Order the eigenvectors descending by their eigenvalue. The k principal components are the eigenvectors corresponding to the k largest eigenvalues.

The k principal components of the observed vector x are then given by:

$$y = W^T(x - \mu) \quad (6)$$

Where

$$W = (v_1 v_2, \dots, v_k) \quad (7)$$

The reconstruction from the PCA basis is given by:

$$x = Wy + \mu \quad (8)$$

Where

$$W = (v_1 v_2, \dots, v_k) \quad (9)$$

The Eigenfaces method are performs face recognition by projecting all training samples into the PCA subspace, projecting the query image into the PCA subspace and finding the nearest neighbor between the projected training images and the projected query image.

Next, imagine that there are given 400 images sized 100×100 pixel. The PCA solves the covariance matrix $S = XX^T$, wheresize $(X) = 10000 \times 400$ as mentioned before. It would end up with a 10000×10000 matrix, roughly $0.8GB$. Solving this problem isn't feasible, so we'll need to figure out different method. From linear algebra, a $M \times N$ matrix with $M > N$ can only has $N - 1$ non-zero eigenvalue. So it's possible to take the eigenvalue decomposition $S = X^T X$ of size $N \times N$ instead:

$$X^T X v_i = \lambda_i v_i \quad (10)$$

and get the original eigenvectors of $S = XX^T$ with a left multiplication of the data matrix:

$$XX^T(Xv_i) = \lambda_i(Xv_i) \quad (11)$$

The resulting eigenvectors are orthogonal, to get orthonormal eigenvectors, they need to be normalized to unit length. In Figure 6, the eigenfaces of the algorithm process is presented.

4. METHODOLOGY

4.1 Software

This project depends on the *OpenCV* computer vision library to perform the face detection and recognition. Unfortunately the current binary version of *OpenCV* available to install in the Raspbian operating system

through apt-get (version 2.3.x) is too old to contain the face recognition algorithms used by this project. However there is a later version of *OpenCV* that is available for download, compile, and install to access the face recognition algorithms. The Linux based operating system which is Raspbian is used to execute the instruction of the face recognition algorithm.

4.2 Hardware

The hardware made for this project is a prototype version of a briefcase. It has three major compartments for placing

the electronic components; battery, processing and lock mechanism. In this project, Raspberry Pi is used as the processing part of the face recognition algorithm and it is powered up by a battery of 5V and 2A. The lock mechanism is an electromagnetic lock that capable of providing 50N attract force to prevent unauthorized person to open the case. Figure 7 to Figure 9 show the prototype design.

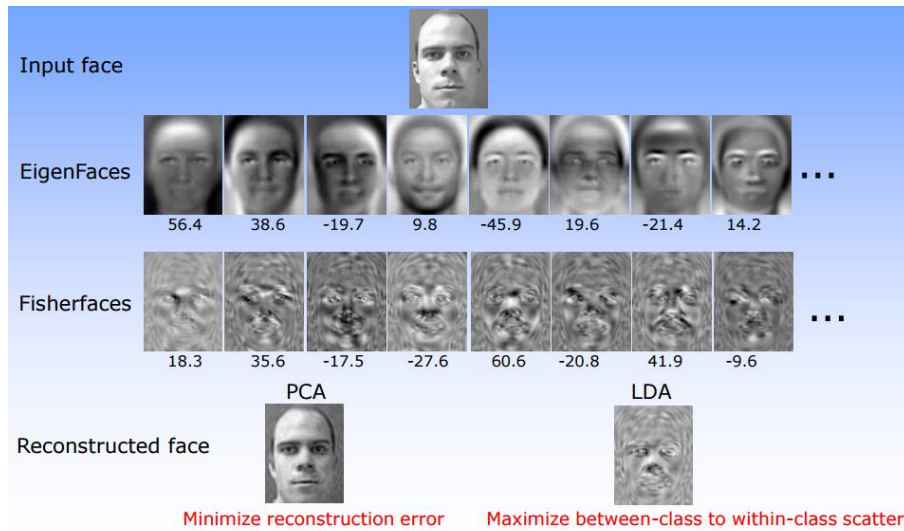


Figure 6. Eigenfaces algorithm process

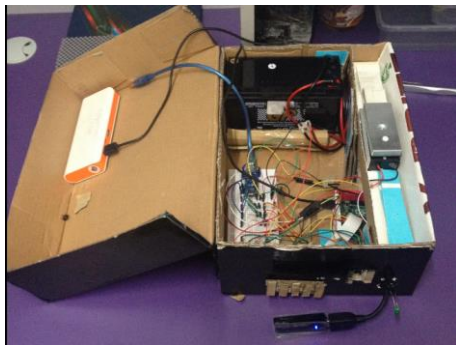


Figure 7. Prototype design of bag locking mechanism



Figure 9. External look of the design

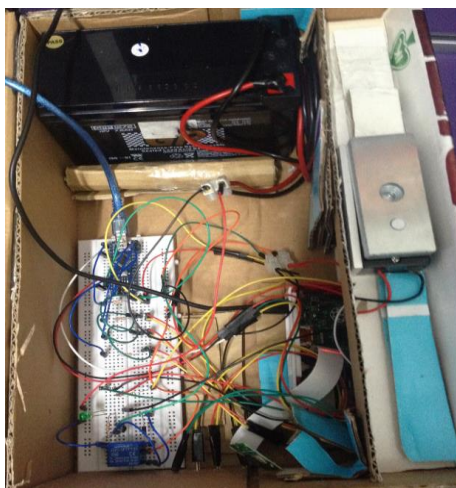


Figure 8. Internal part of the prototype design

4.3 Training Process

This project uses the eigenfaces algorithm in OpenCV to perform face recognition. To use this algorithm a set of training data need to be created with pictures of faces that are and are not allowed to open the bag.

There is a large set of face images included in the project that are tuned for training with the face recognition algorithm. This is the database of faces published by research AT&T Laboratories Cambridge in the mid 90's as shown in Figure 7. These faces make up the set of negative images which represent faces that are not allowed to open

the bag as shown in Figure 10. These images are stored in the training/negative subdirectory of the project.

To generate images of the person who will be allowed to open the box, or positive training images as shown in Figure 11, by executing the included capture-positives.py script. This script will take pictures with the box hardware and write them to the training/positive sub-directory which will be created by the script later.

With the hardware assembled and powered up the Raspberry Pi is connected in a terminal session and navigate to the directory with the project software.

5. RESULTS AND DISCUSSION

The prototype version of face recognition bag locking mechanism is executed by assembling all the hardware parts and run the programmed software.

The box will lock itself once the Raspberry Pi is powered and ready to unlock with face recognition. A message of “Predicted POSITIVE face with confidence 1321.35253959 (lower is more confident). Recognized face!” is shown when the person who allowed to open the briefcase pressed the push button. Likewise if the person is not allowed to open, a message like “Predicted NEGATIVE face with confidence 3987.76625152 (lower is more confident). Did not recognize face!” is shown. Figure 12 shows the messages obtained.



Figure 10. Negative images from the database

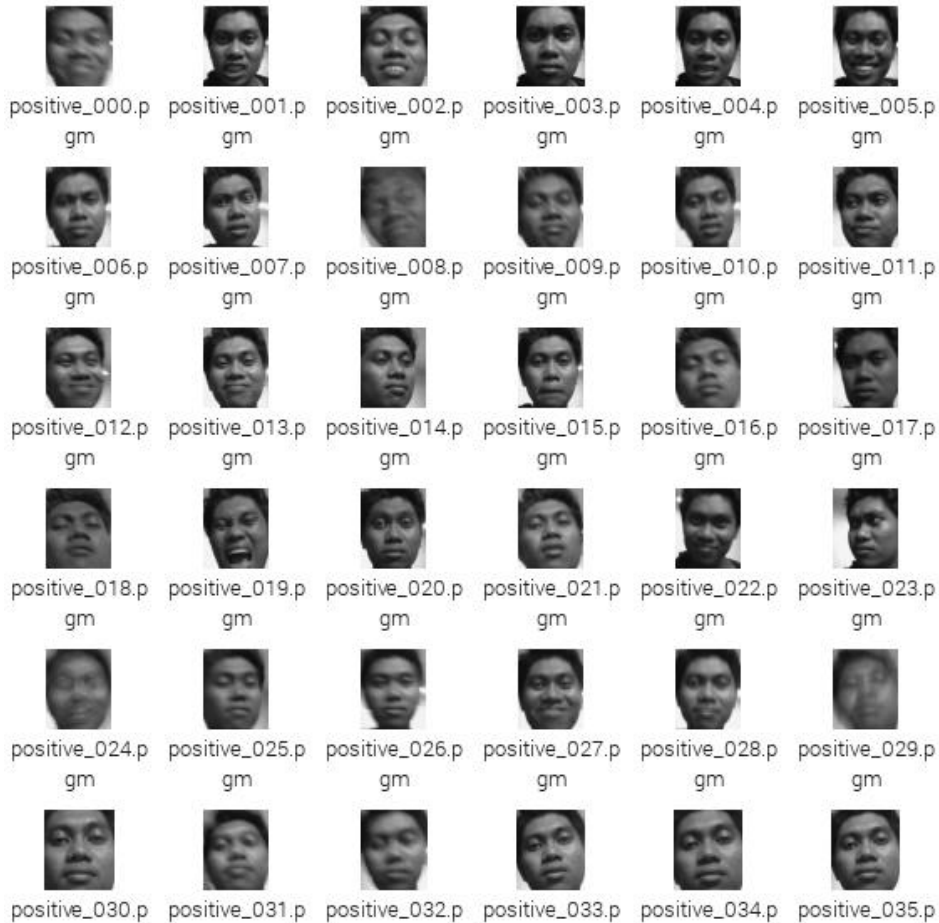


Figure 11. Positive training images

```

pi@raspberrypi: ~/pi-facerec-box-master
ptured and try again with only one face visible.
Button pressed, looking for face...
Could not detect single face! Check the image in capture.pgm to see what was ca
ptured and try again with only one face visible.
Button pressed, looking for face...
Could not detect single face! Check the image in capture.pgm to see what was ca
ptured and try again with only one face visible.
Button pressed, looking for face...
Could not detect single face! Check the image in capture.pgm to see what was ca
ptured and try again with only one face visible.
Button pressed, looking for face...
Could not detect single face! Check the image in capture.pgm to see what was ca
ptured and try again with only one face visible.
Button pressed, looking for face...
Predicted POSITIVE face with confidence 5015.86221493 (lower is more confident) .
Recognized face!
Box is now locked.
Button pressed, looking for face...
Could not detect single face! Check the image in capture.pgm to see what was ca
ptured and try again with only one face visible.
Button pressed, looking for face...
Predicted POSITIVE face with confidence 4735.2987804 (lower is more confident) .
Recognized face!

```

Figure 12. Messages responded from the Raspberry PI

When a face is found, the prediction message includes how the face was recognized which is matching either the positive or negative training data, or the confidence of the recognition. The confidence is a value like 1321.35 or 3987.77 above and represents the distance of the captured face from the predicted face in which a lower distance value means the captured face is more similar to the predicted face. To unlock the box, a captured face must be a positive prediction with a confidence value below the **POSITIVE_THRESHOLD** configuration value. By default the **POSITIVE_THRESHOLD** is 2000, so the positive prediction with confidence 1321.35 was considered a match and would have unlocked the box.

When the box is in an unlocked state, the button to lock the box is pressed again. Ideally the intended images of the positively trained face to be predicted as positive images with a low number for the confidence value. The eigenfaces recognition algorithm is sensitive to the lighting and orientation of the face, so similar conditions as when the positive training images were captured is very much needed.

5. CONCLUSION

From the results obtained in this work, the face recognition algorithm is successfully implemented and executed on the Raspberry Pi for the purpose of providing locking mechanism to all sort of bags. In addition, the assistive mechanism like ambient like sensor has been functionally helping improve the condition of the surrounding to minimize the threshold level or error. Not only that, face is identified precisely and accurately without performing any errors during the testing. This shows that, the fuzzy logic system has been successfully integrated with the artificial neural network system in the application of this work which is face recognition system.

REFERENCES

- [1] R. C. Gonzalez and R. E. Woods. "Digital image processing", Second Edition, published by Pearson Education, 2003.
- [2] W. Zhao, R. Chellappa, J. Phillips, and A. Rosenfeld, "Face recognition in still and video images: A literature survey", *ACM Comput Surv* vol. 35, pp. 399–458, 2003.
- [3] J. R. Solar, and P. Navarreto, "Eigen space-based face recognition: a comparative study of different approaches", *IEEE Transactions on Systems man And Cybernetics- part c: Applications*, vol. 35, no.3, 2005.
- [4] M. Turk, and A. Pentland, "Eigen faces for face recognition", *Journal cognitive neuroscience*, vol. 3, no.1, 1991.
- [5] W. Zhao, R. Chellappa, and A. Krishnaswamy, "Discriminant analysis of principal component for face recognition", *IEEE Transactions on Pattern Anal. Machine Intelligence*, vol. 8, 1997.
- [6] O. Deniz, M. Castrillion, and M. Hernfiandez, "Face recognition using independent component analysis and support vector machines", *Pattern Recognition letters*, vol. 24, pp. 2153-2157, 2003.
- [7] B. Moghaddam, "Principal manifolds and probabilistic subspaces for visual recognition", *IEEE Transactions on pattern Anal. Machine Intelligence*, vol. 24, no.6, pp. 780-788, 2002.
- [8] H. Othman, and T. Aboulnasr, "A separable low complexity 2D HMM with application to face recognition", *IEEE Trans. Pattern. Anal. Machie Inell.*, vol. 25, no.10, pp. 1229-1238, 2003.
- [9] M. Er, S. Wu, J. Lu, and L.H.ToH, "face recognition with radial basis function (RBF) neural networks", *IEEE Transactions on Neural Networks*, vol. 13, no. 3, pp. 697-710, 2003.
- [10] K. Lee, Y. Chung, and H. Byun, "SVM based face verification with feature set of small size", *Electronic letters*, vol. 38, no.15, pp. 787- 789, 2002.

- [11] M.J.Er, W.Chen, and S.Wu, "High speed face recognition based on discrete cosine transform and RBF neural network", IEEE Trans. On Neural Network, vol. 16, no.3, pp. 679-691, 2005.
- [12] D.L. Swets and J.J. Weng , "Using Discriminant Eigen features for image retrieval", IEEE Trans. Pattern Anal. Machine Intel, vol. 18, pp. 831-836, 1996.
- [13] P.N. Belhumeur, J.P. Hespanha, and D. J. Kriegman, "Eigen faces vs. Fisher faces: Recognition using class specific linear projection", IEEE Trans. Pattern Anal. Machine Intel., vol. 19, pp. 711-720, 1997.
- [14] D. Ramaeubramanian, and Y. Venkatesh, "Encoding and recognition of Faces based on human visual model and DCT", Pattern recognition, vol. 34, pp. 2447-2458, 2001.
- [15] X. Y. Jing, and D. Zhang, "A face and palm print recognition approach based on discriminant DCT feature extraction", IEEE trans. on Sys. Man & Cyb., vol. 34, no. 6, pp. 2405-2415, 2004.
- [16] Papoulis, and U. Pillai, "Probability, random variables, and Stochastic Processes", McGraw-Hill, 0073660116, New York, 2002.
- [17] Haykin, S. Neural Networks: A comprehensive foundation, Prentice Hall, 0-13-273350-1, New Jersey, 1999.