Biometric Authentication using Face Recognition Algorithms for A Class Attendance System

Ahmad Syauqi Rahim and Maziah Mohamad*

School of Mechanical Engineering, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru
Johor, Malaysia

ABSTRACT

The paper is about developing an attendance system that is based on a biometric verification technique using a face recognition method that is expected able to avoid system manipulation in comparison to other attendance systems. Face recognition algorithm consists of two parts, namely, the training and testing components. The main focus of the study is on the feature extraction method in which the study proposes a face recognition algorithm using three types of features extraction methods which are the local binary pattern (LBP), principle component analysis (PCA) and histogram of oriented gradient (HOG) along with support vector machine (SVM) algorithm as the classifier. The performance analysis of each algorithm was carried out by testing the algorithms using multiple styles of facial images. The styles of the facial images are the frontal face, angled face, expression face and also low light illumination face images. The results show that the HOG+SVM algorithm obtained the highest accuracy in every test. Furthermore, it is also found that the HOG+SVM method can execute the recognition process efficiently and fast.

Keywords: *Biometric authentication*, *feature extraction methods*, *face recognition algorithms, attendance system*

1.0 INTRODUCTION

In an attendance system, particularly at the university, the student himself/herself must ensure that he or she should be present or in attendance in a class that he/she has registered. But sometime, it is typical that the students choose to be absent from attending class without permission due to some ridiculous and unacceptable reasons like the shuttle bus was late, oversleeping, a need to study for test or have no reasons at all. They are all aware that in order to qualify to sit for the final examination according to the stipulated academic regulation, their attendance ibn class must be at least 80% of the total class hours for every semester (for a typical 14-week semester). The existing conventional attendance system is through applying the personal signature method (by hand) has noticeable disadvantages, the main one of which is that the signature can be easily duplicated by other persons (students, friends or colleagues). This situation opens the door or opportunity to cheating, exploiting or manipulating the attendance system when the attendance itself is not properly monitored and controlled by the lecturer or teaching academic staff. In order to overcome this issue, a biometric authentication method for monitoring and controlling the attendance in class is proposed.

*Corresponding email: maziah@mail.fkm.utm.my

Biometric authentication is extensively known as the most effective type of authentication due to the fact that it is extremely difficult to transfer or emulate biological materials, traits or features from one individual user to another [1]. Biometric authentication method can be defined as a method for identifying and authenticating a person based on an identifiable identity or personal trait of that particular individual. Others defined it as a security process that relies on the unique biological characteristics of an individual to verify that he/she is who is says he/she is. Biometric authentication systems compare a biometric data set captured earlier to stored, confirmed authentic data in a specific database. If both samples of the biometric data match, then the authentication is confirmed or approved [2]. By implementing the biometric authentication, the ability to manipulate the attendance system can be greatly reduced or even totally eliminated. This is because it is extremely difficult to duplicate a biometric identity of a person knowing the fact that it is typically unique for each individual different person. There are many biometric identification (ID) or authentication methods that are practiced in the real-world applications that are particularly related to the security industry. In addition to the security provided by difficult-to-fake individual biological traits, the acceptance of a biometric verification technique has also been driven by convenience Amongst the popular biometric authentication approaches are those that are based on *handwritten signatures*, *retina scans*, *iris recognition*, *fingerscanning*, *finger vein ID*, *voice identification systems* and *facial recognition systems*, the last one of which is the main concern of the paper. A brief description of the methods is presented in the following paragraphs [2, 3].

Handwritten signature authentication method is based on systems for signature verification and signature identification. Whether the given signature belongs to a particular person or not is decided through a signature ID system, whereas the signature verification system makes decision if a given signature indeed belongs to a claimed person or otherwise [3, 4]. Retina scans produce an image of the blood vessel pattern in the light-sensitive surface lining of the individual's inner eye. Iris recognition is used to identify individuals that is based on unique patterns within the ring-shaped region surrounding the pupil of the eye. The earliest and most popular form of biometric authentication is the classic fingerprinting technique that utilizes ink-and-paper for various related applications. Fingerscanning is in fact the digital version of the fingerprinting process that works with details in the pattern of the raised areas and branches in a human finger image. Meanwhile, finger vein ID is another technique that is based on the unique vascular pattern in an individual's finger. Voice identification systems is yet another biometric approach that rely on the characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions. Last but not least, the facial recognition systems work with numeric codes called faceprints, which identify the nodal points on a human face.

The most common and an evolving type of biometric authentication involves facial scanning in which the facial scanning tools now have the ability to identify people and can be used for different types of security and authentication procedures [1]. Face as biometric identity has outperformed other popular biometric identity such as DNA, fingerprint, eyes (retina and iris), voice, hand and foot geometry as other methods are impractical to apply in many situations such as uncooperative scenario like surveillance setting. Face images/video are easy collectable and non-intrusive. Furthermore, the performance of automatic face detection is better than human performance [5]. The face recognition system is a method where computer detects the facial features/facial landmark and recognizes who the face belongs to. The examples of facial features are location of mouth, right and/or left eyebrows, right and left eyes, nose and jaw. These features can be readily detected by computer to distinguish the faces of persons.

The art of implementing the face recognition algorithm is an important topic of research interest where many researchers are arguing about the best type of algorithm for a face recognition system. Basically, the face recognition algorithm methods are focusing on the feature extractions of the human face and also the methods in which the computer can be taught and trained to distinguish those features [6].

2.0 FACE RECOGNITION ALGORITHM

Figure 1 shows the schematic diagram of a face recognition algorithm. There are two important processes in the face recognition algorithm with reference to the training and testing sets. The training set starts with all images (face) in the database that undergoes features extraction algorithm and then executing the learning/modeling algorithm which outputs the models of various persons involved in the study. In the testing process, the input image (test image) is required to undergo an image preparation process prior to the implementation of the feature extraction algorithm, followed by the application of the classification algorithm. The output of the face recognition algorithm is recognizing the face of a person in the input image and then comparing it that in the database [7].

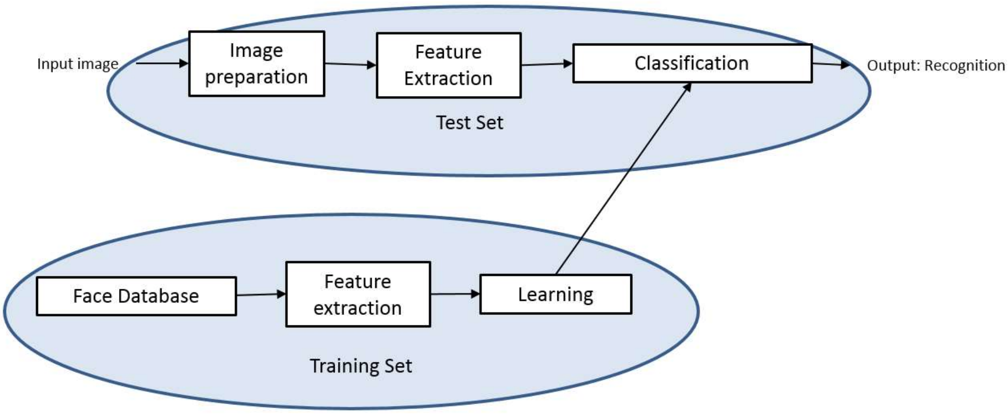

Figure 1: Basic face recognition algorithm flow process

Feature extraction is the process of getting useful information from face images such as face structure, texture, edges and also other biometric features like geographic distance of face. Basically, there are various method for features extraction such as linear discriminant analysis (LDA) [8], independent component analysis (ICA) [4], principle component analysis (PCA) [9], local binary pattern (LBP) [10] and also histogram of oriented gradient (HOG) [11]. This paper focuses on the comparative study of the performance results based on LBP, PCA and HOG feature extraction algorithms.

2.1 Local Binary Pattern (LBP)

LBP method is a method where computer compares a single pixel in the image with the neighbouring pixel. The comparison of this method is based on the grayscale colour intensity of the pixels. If the intensity of the neighbouring pixel is higher than the center pixel, the result equals to 1. Vice versa, it will be zero. The result of this process typically forms a binary pattern for example - 11001011. Figure 2 explains the formation of the binary pattern.

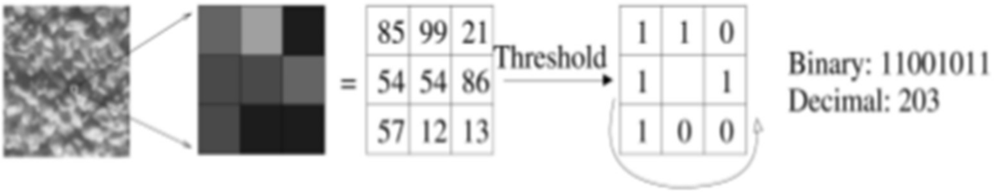

Figure 2: Binary pattern formation

2.2 Histogram of Oriented Gradient (HOG)

HOG method uses gradient vectors calculation from the grayscale image to obtain the value of the magnitude and the gradient between pixels in the images. The value of the gradient in *x* and *y* directions is calculated by subtracting the value from the right to left pixels and top to bottom pixels.

$$Magnitude = \sqrt{(xgradient)^2 + (ygradient)^2} \quad (1)$$

$$angle = Tan^{-1}(\frac{ygradient}{xgradient}) \quad (2)$$

The values can be plotted to illustrate the structure of the image as shown in Figure 3.

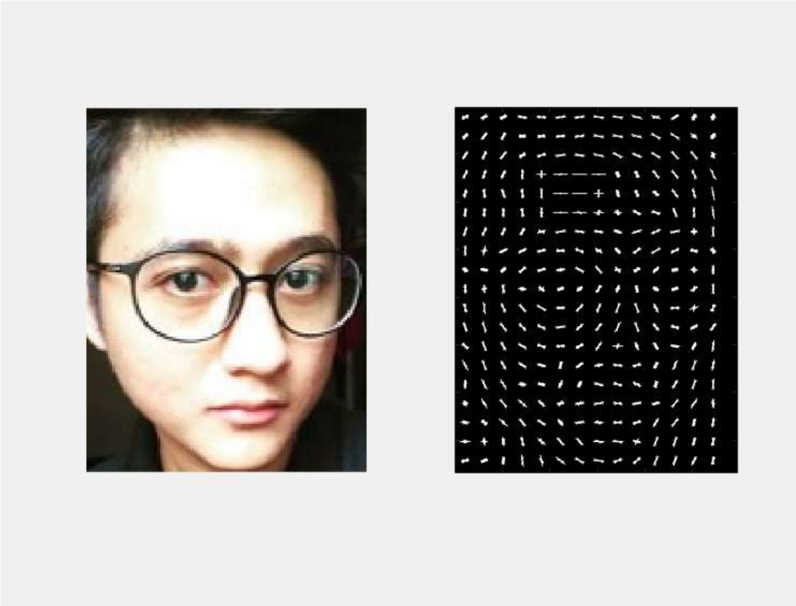

Figure 0: Gradient vector plot

2.3 Principle Component Analysis (PCA)

PCA feature extraction method is also known as eigenface algorithm method. This method was used to find the edges in the image as shown in Figure 4 by calculating the eigenvalues and eigenvectors of the image.

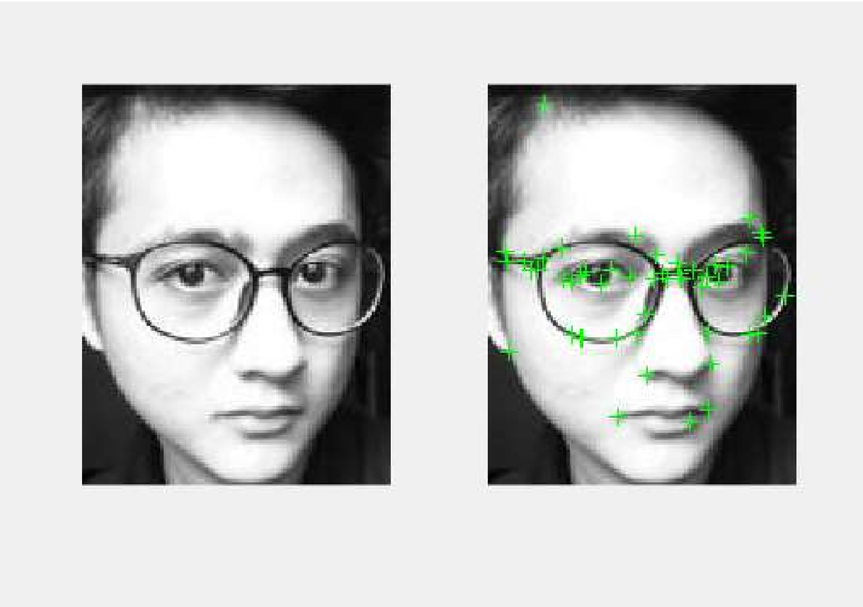

Figure 4: PCA feature extraction

2.4 Attendance System Database

The training database of the face recognition system that has been created consists of the captured images of eight UTM students as the subjects of interest. A total of 10 captured images were varied in terms of the facial and degree of lighting conditions. Each person creates four images of a *straight face*, two images of different *angled face* positions, two images of different *expression face* and two images of *low illumination face* conditions intended to measure the robustness of the proposed attendance system [12]. An example of the various image styles is shown in Figure 5.

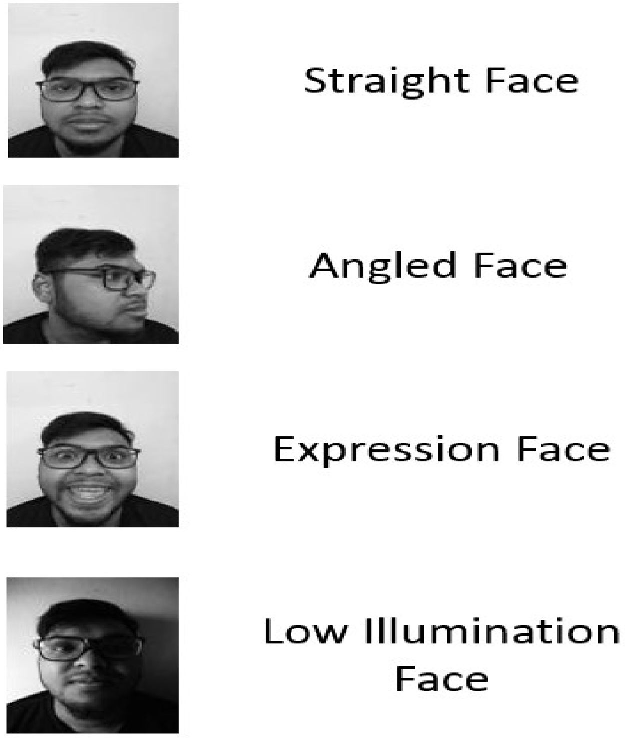

Figure 5: Different styles of the images of the subject's face used in the database

2.5 Face Recognition Algorithms

A number of face recognition algorithms was constructed using the LBP, PCA and HOG algorithms as the feature extraction methods together with an SVM and *Euclidean* distance as the classifier/learning algorithm as shown in Table 1.

Table 1: Face algorithm construction

Feature Extraction	Learning
LBP	SVM
PCA	*Euclidean* distance
HOG	SVM

The algorithms were tested using the images related to a *straight face*, *angled face*, *expression face* and *low illumination face* in order to evaluate its robustness. The algorithm performance is measured by the accuracy and the time taken for an algorithm to complete its task. The accuracy of the algorithm is calculated using Equation (3):

$$Accuracy = \frac{No.of\ match\ images}{Total\ no.of\ test} \tag{3}$$

3.0 RESULTS AND DISCUSSION

The performance of the face recognition algorithms using different feature extraction methods is measured based on the accuracy and efficiency of the algorithm in executing the tasks.

3.1 Algorithm Accuracy

Figure 6 shows that HOG is the best face recognition algorithm compared to PCA and LBP in terms of accuracy in all tests. The HOG+SVM algorithms obtains 100% accuracy for the *straight face*, *angled face* and *expression face*. LBP gets 100% accuracy on *straight face* and *expression face* while PCA is only able to get 100% accuracy on the *straight face* test only. The performance of all algorithms degrades when tested using low illumination image (62.5%) for HOG+SVM and only 25% for both LBP and PCA.

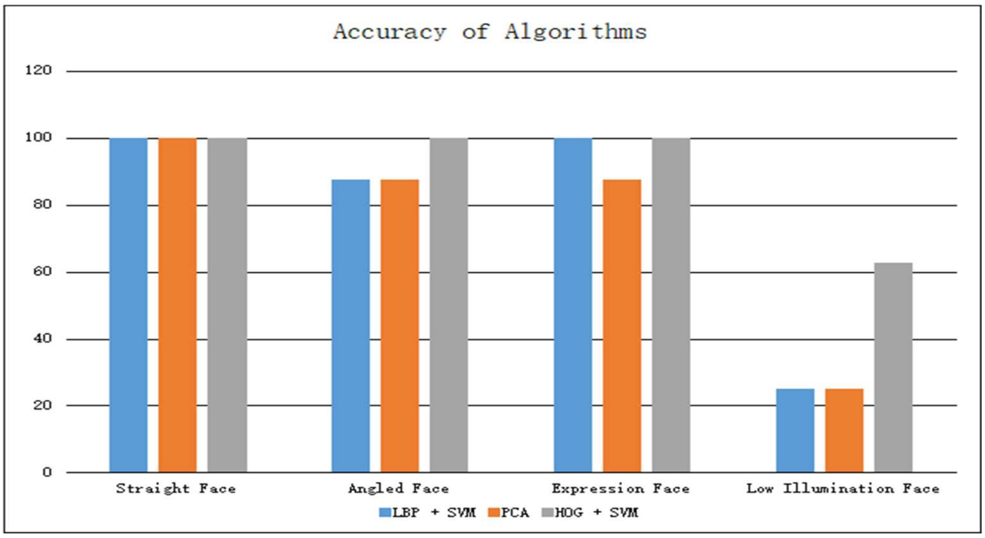

Figure 6: Comparison of attendance systems accuracy

3.2 Algorithm Efficiency

Table 2 shows that the most efficient algorithm is the PCA algorithm followed by the HOG algorithm and then LBP algorithm. As shown in the table, there is no such significant different in time taken for HOG and PCA algorithm which HOG slightly slower compared to PCA algorithm. However, there is a significant different of the time taken when using LBP methods.

Table 2: Overall results of face recognition algorithm

Algorithm methods	Straight face		Angled face		Expression face		Low illumination face	
	Accuracy (%)	Time taken (s)	Accuracy (%)	Time taken (s)	Accuracy (%)	Time taken (s)	Accuracy (%)	Time taken (s)
LBP + SVM	100	0.2080	87.5	0.2107	100	0.2091	25	0.2080
PCA	100	0.0377	87.5	0.0410	87.5	0.0407	25	0.0406
HOG + SVM	100	0.0422	100	0.0424	100	0.0419	62.5	0.0420

4.0 CONCLUSION

A number of face recognition algorithms (LBP, PCA and HOG) with a classifier/learning algorithm were implemented and tested using human subjects (eight UTM students) for the development of a biometric authentication class attendance system. From the results obtained, the performance of the algorithm is affected when tested on various angled, expression and low illumination faces of the subjects. The combined HOG+SVM algorithm was found to be the best algorithm based on robustness and efficiency tests. Therefore, this algorithm is suggested to be utilized in the development and implementation of the proposed attendance system.

REFERENCES

1. *Biometric authentication*, https://www.techopedia.com/definition/29824/biometric-authentication, [Accessed 27 September 2018].
2. *Biometric authentication*, https://searchsecurity.techtarget.com/definition/biometric-authentication, [Accessed 30 September 2018].
3. Pal S., Pal U. and Blumenstein M., 2014. Signature-Based Biometric Authentication, In Muda A., Choo Y-H., Ajith A., Sargur N.S. (Eds.), *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, 285-314.
4. Lim B.H., Mailah M., 2005. Intelligent Biometric Signature Verification System Incorporating Neural Network, *Jurnal Mekanikal*, 20: 22-41.
5. Bhatia R., 2013. Biometrics and Face Recognition Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5): 93-99.
6. Mudunuri S.P. and Biswas S., 2016. Low Resolution Face Recognition Across Variations in Pose and Illumination, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 38(5): 1034-1040.
7. Naeem M., Qureshi I. and Azam F., 2015. Face Recognition Techniques and Approaches: A Survey, *Sci.Int.*(Lahore), 27(1): 301-305.
8. Cao Z., Yin Q., Tang X. and Sun J., 2010. Face Recognition with Learning-based Descriptor, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, San Francisco, CA, USA

9. Paul L.C. and Sumam A.A., 2012. Face Recognition Using Principal Component Analysis Method, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(9): 135-139
10. Ahonen T., Hadid A. and Peitika M., 2006. Face Description with Local Binary Patterns: Application to Face Recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12): 2037-2041.
11. Dalal N. and Triggs B., 2005. Histograms of Oriented Gradients for Human Detection, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, San Diego, CA, USA.
12. Wagner A., Wright J., Ganesh A., Zhou Z., Mobahi H. and Ma Y., 2012. Toward A Practical Face Recognition System: Robust Alignment and Illumination by Sparse Representation, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(2): 372–386.