Biometric Authentication Using Facial Recognition

Mozammel Chowdhury[1(✉)], Junbin Gao[2], and Rafiqul Islam[1]

[1] School of Computing & Mathematics,
Charles Sturt University, Bathurst, Australia
{mochowdhury,mislam}@csu.edu.au

[2] Discipline of Business Analytics,
The University of Sydney Business School, Sydney, Australia
junbin.gao@sydney.edu.au

Abstract. Biometric authentication has been gaining popularity for providing privacy and security in many applications including secure access control, surveillance systems, user identification and many more. This research proposes a robust scheme for biometric authentication by analyzing and interpreting facial image using a neural network. Human face has become as the key attribute for biometric authentication over the recent years due to its uniqueness and robustness. Our system focuses on efficient detection and recognition of user's face for precise authentication. The facial features of a user are compared with a face database in order to perform matching for authentication and authorization. The proposed system estimates the face by analyzing skin color components in the facial image. The facial edge features are then extracted from the detected face skeleton. A neural network is employed and trained with the extracted edge features to recognize the user face by comparing with the facial database. Once the user is identified, authentication is granted. Experimental evaluation demonstrates that our proposed system provides better performance meeting accuracy requirements and less computation time.

Keywords: Biometric authentication · Secure access control · Surveillance system · Facial recognition

1 Introduction

Biometric authentication has become very popular nowadays in security and privacy preserving applications such as, access control, surveillance system, visa processing, border checking and so on. Biometric authentication is a technique that relies on the unique biometric characteristics of individuals to verify user identity for secure access to electronic devices or systems [1]. Biometric features such as, fingerprint, face, facial components, palm print, hand geometry, iris, retina, gait and voice are common form of key attributes in biometric authentication [2]. In recent years, human faces are widely used as the most distinctive key attributes for biometric authentication due to their uniqueness, robustness, availability, accessibility and acceptability characteristics [3].

R. Deng et al. (Eds.): SecureComm 2016, LNICST 198, pp. 287–295, 2017.
DOI: 10.1007/978-3-319-59608-2_16

User authentication is crucial in secure access control that provides the safety and security of any system. User authentication is traditionally performed based on the following arrangements: (a) something that the user knows (such as, a PIN, a password) or (b) something that the user holds (typically a key, a token, a smart card, a badge, or a passport). These traditional methods for the user authentication have deficiencies that restrict their applicability in security systems. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Biometric authentication or simply biometrics, on the other hand, authenticates users properly and reliably [4]. Biometric characteristics are unique and not duplicable or transferable. Biometric authentication identifies and authorizes a person based on the physiological or behavioral characteristics such as a fingerprint, an iris pattern, face or a voice sample [5].

The interest of doing research on biometrics is very significant due to its immense importance in the privacy and security community. This paper aims to develop an efficient scheme for biometric authentication based on facial recognition using a neural network. The system works with visual and geometrical information of the user's face in an image and detects the face skeleton using the similarity measure of the colour components of the image in the YC_bC_r colour space. Once the face is detected, the edge features of the face skeleton are then extracted and fed into the neural network to teach the network in order to identify the user face. Once the user is identified by facial recognition, authentication is granted to access the secure system. The proposed technique can treat images with different lighting conditions and complex backgrounds.

The rest of the paper is organized as follows. In Sect. 2, we present an overview of facial recognition. Section 3 demonstrates the architecture of our proposed facial recognition system. Experimental results are reported in Sect. 4. Finally, Sect. 5 concludes the paper.

2 Facial Recognition

Human face plays an important role in person recognition in vision-based surveillance system. Facial recognition is a technique for automatically identifying or verifying a person from an image or a video frame. Compared with other biometrics, face recognition has the potential to recognize uncooperative subjects in a non-intrusive manner. It has now become the most common and widely used means of biometric identification [6].

Facial recognition technology has been developed based on two arrangements: facial metrics and eigenfaces [7]. Facial metrics relies on the measurement of the facial features such as, eyes, nose, mouth. Eigenfaces refers to an appearance-based approach to face recognition that seeks to capture the variation in a collection of face images and use this information to encode and compare images of individual faces in a holistic (as opposed to feature-based) manner. In the facial recognition technique, the system captures the face image of the user by a camera or sensor and extracts the features from the face. The features are then compared with one which is stored in a face database, and if there is a match, the user's face is identified.

The face recognition process generally consists of the following steps. The initial task of facial recognition is to locate the face within the image sequence. Then the detected face block is normalized and extracted. The facial features are then extracted from the selected face block. Finally, the face is recognized.

A tremendous amount of research works have been done for automatic detection and recognition of human face over the last couple of decades [8, 9]. To name a few, good surveys exist for illumination invariant face recognition [10], face recognition across pose [11–13], video-based face recognition [14], and heterogeneous face recognition [15], face recognition using multi-scale Local Binary Patterns (LBP) [16], Locally linear regression based face recognition [17], and face recognition based on Dual-Cross Patterns (DCP) features [18].

Facial recognition techniques mentioned above have some deficiencies. The dependency on the light, resolution and facial expression reduces the accuracy of the facial recognition. We therefore, have employed facial edge features in recognition process which are independent of the variation of pose and illumination.

3 Proposed System Architecture

The general architecture of the proposed biometric authentication scheme is shown in Fig. 1. The scheme comprises of the following steps: (i) Pre-processing of the face image, (ii) Face detection, (iii) Facial features extraction, (iv) Feature matching, (v) Face identification, and (vi) Authentication.

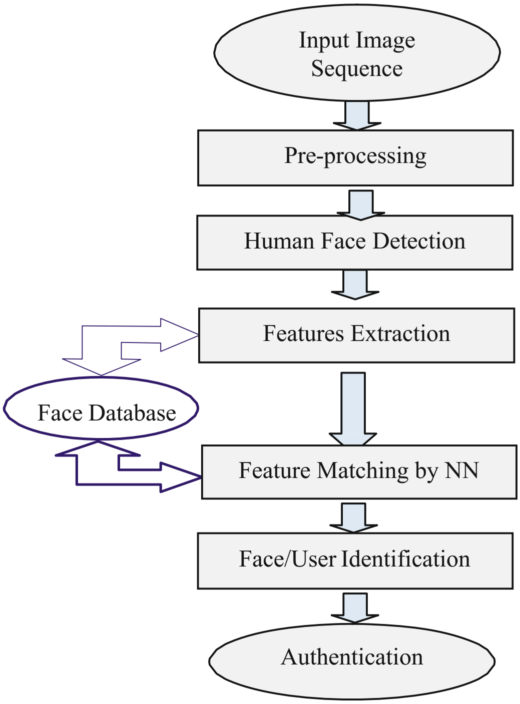


Fig. 1. Architecture of the proposed biometric authentication system.

3.1 Preprocessing of the Face Images

In computer vision systems, there may be significant amount of noise in the captured images. We therefore, employ a fuzzy median filtering technique [19] for refining the facial images corrupted by noise. This filter employs fuzzy rules for deciding the gray level of the pixels within a window in the image.

3.2 Face Detection

The most important part of the facial recognition is detecting the face in the image. Face detection is concerned with determining the part of an image which contains face. Several techniques have been developed for face detection in last couple of years, which includes: geometric modeling, genetic approach, neural network, principal component analysis, color analysis and so on [20–26].

In this paper, we have employed a fast and robust face detection technique based on skin color segmentation [27]. The face skeleton is detected from the largest connected area of the skin color segmented image. The method considers the frontal view of the face in color scale image. The detected face image is normalized and cropped with a dimension of 180 × 160 pixels. The steps of the face detection method are demonstrated in Fig. 2. The outcomes of face detection and normalization process are shown in Fig. 3.

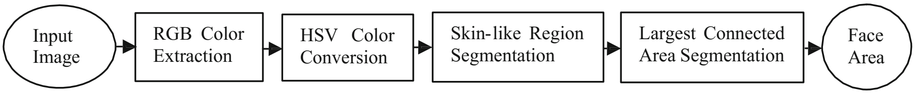

Input Image
RGB Color Extraction
HSV Color Conversion
Skin-like Region Segmentation
Largest Connected Area Segmentation
Face Area

Fig. 2. Block diagram of the face detection method.

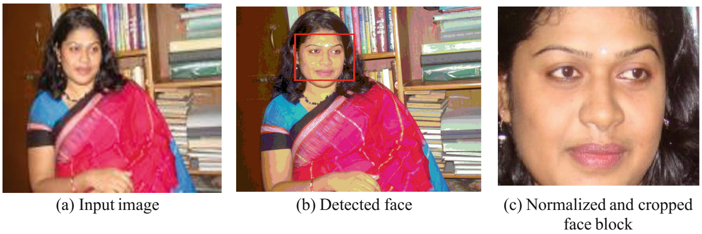

(a) Input image
(b) Detected face
(c) Normalized and cropped face block

Fig. 3. Face detection and normalization process for a real image sequence.

3.3 Facial Features Extraction

One of the key tasks underlying facial recognition is the features extraction. Once the face is detected, the facial features are then extracted from this face block for matching with the one stored in the face database. This paper extracts the edge features from the face region, since the edge features are invariant to pose variation and illumination changes. The extracted facial edge features are then fed into a back propagation neural network (BPNN) to train the network for recognizing the face.

Edge or gradient histogram corresponds to the spatial distribution of the edge features in the image. The gradient of an image *f*(*x*, *y*) can be expressed by,

$$\nabla f = \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{bmatrix} = \begin{bmatrix} G_x \\ G_y \end{bmatrix} \tag{1}$$

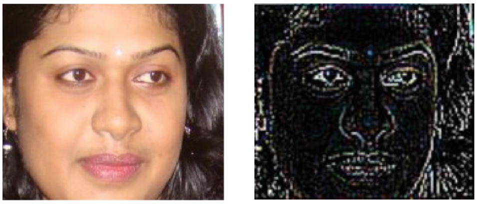
where $G_x = \frac{\partial f}{\partial x}$ is the gradient in x direction, and

$G_y = \frac{\partial f}{\partial y}$ is the gradient in y direction.

The gradient direction can be calculated by the formula:

$$\theta = \tan^{-1}\left[\frac{G_y}{G_x}\right] \tag{2}$$

We use Sobel edge detector to extract the edge features from the images. Figure 4 shows the edge features extracted from the face image.



(a) Face image (b) Detected Edge points

Fig. 4. Facial edge features extraction.

3.4 Facial Recognition with Neural Network

Facial recognition is achieved by employing a backpropagation neural network. The architecture of the neural network is illustrated in Fig. 5.

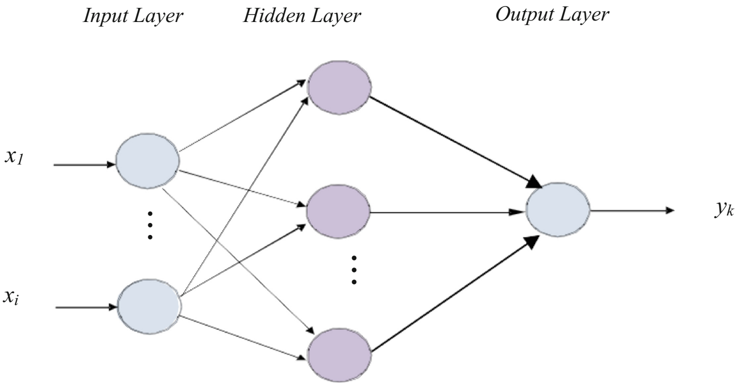


Fig. 5. Architecture of the back propagation neural network.

The nodes in the input layer receive the edge features. In this network, the layers are connected with each other through their neurons with specific weights. The input signals transmit from left to right directions while the error signals propagate from right towards left. Back propagation algorithm presents a training sample to the neural network and compares the obtained output to the desired output of that sample. It calculates the error in each output neuron. The BPNN adjusts the weights of each neuron for minimizing the error value. The minimum error margin is set to 0.001 for experimental evaluation.

4 Experimental Evaluation

In order to evaluate the effectiveness of the proposed method, experiments have been carried out for real images at different illumination conditions. We have performed experiments on three different face databases (Face 94, Face 95 and Face 96) of the University of Essex [29–31] with different poses and illuminations. Figure 6 demonstrates some sample images of these face databases. The features of the face databases are summarized in Table 1.

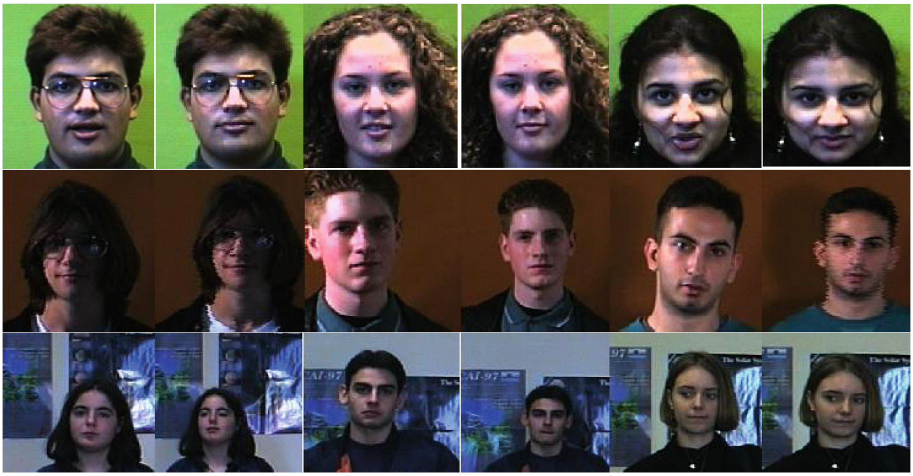


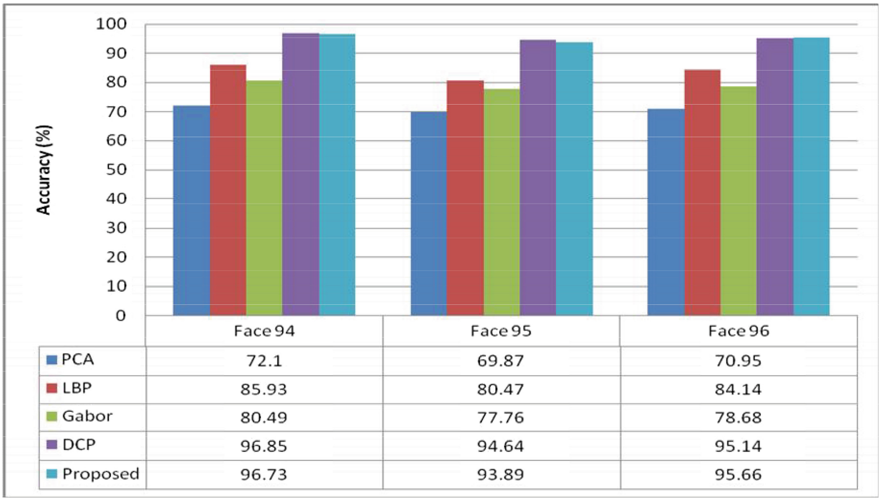
Fig. 6. Face image database of Essex: Face 94 (top), Face 95 (middle), Face 96 (bottom) with different poses and illuminations.

Table 1. Features of the face databases

Data Set	Total Images	Resolutions	Individuals
Face 94	3078	180 × 200	153
Face 95	1440	180 × 200	72
Face 96	3016	196 × 196	152

Experiments are carried out on a computer with 2.2 GHz Intel Core i5 processor and 4 GB RAM. The algorithm has been implemented using Visual C ++. Half of the images of the each face database are used as a training dataset and the remaining images are used as probe images in the recognition test. The extracted facial edge features are used to train the neural network.

We have performed experiments to compare our proposed algorithm with other existing methods including, principal component analysis (PCA) [11], Gabor [28], LBP [16], and DCP [18]. The results as furnished in the Fig. 7 and Fig. 8.



	Face 94	Face 95	Face 96
🟦 PCA	72.1	69.87	70.95
🟥 LBP	85.93	80.47	84.14
🟩 Gabor	80.49	77.76	78.68
🟪 DCP	96.85	94.64	95.14
🟦 Proposed	96.73	93.89	95.66

Fig. 7. Recognition accuracy (%) of different methods for three datasets

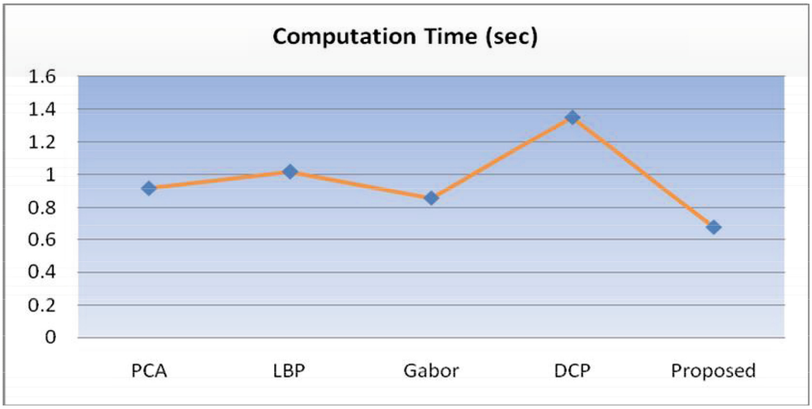


Fig. 8. Computation time for different recognition methods.

Experimental results demonstrate that our approach achieves almost similar recognition accuracy comparable to the state-of-the art method, while taking significant less amount of computation time. We believe that our method can be applicable in real time commercial environment where computational efficiency is a major concern.

5 Conclusion

In this paper we propose an effective and robust biometric authentication scheme based on facial recognition. The scheme employs a neural network with back propagation algorithm to recognize the user face. The system authenticates a user based on the correct matching of his/her face with a face database. Experimental evaluation demonstrates that the proposed system achieves a significant recognition performance with fulfillment of a tradeoff between accuracy and speed. The effectiveness of the proposed system has been justified using standard face databases with different poses and illuminations in complex and simple backgrounds. Our system is able to employ in real time applications where computation speed is a crucial. Our next approach is to extend the algorithm for multi-face detection and recognition.

References

1. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. IEEE Trans. Inf. Forensics Secur. **1**(2), 125–144 (2006)
2. Ahmed, I.T.: Continuous Authentication Using Biometrics: Data, Models, and Metrics. IGI Global, Hershey (2012)
3. Park, U., Jain, A.K.: Face matching and retrieval using soft biometrics. IEEE Trans. Inf. Forensics Secur. **5**(3), 406–415 (2010)
4. Kar, B., Kartik, B., Dutta, P.K.: Speech and face biometric for person authentication. In: Proceedings of IEEE International Conference on Industrial Technology, India, pp. 391–396, December 2006
5. Dabbah, M.A., Woo, W.L., Dlay, S.S.: Secure authentication for face recognition. In: Proceedings of IEEE Symposium on Computational Intelligence in Image and Signal Processing, USA, pp. 121–126, April 2007
6. Gopalan, R., Jacobs, D.: Comparing and combining lighting insensitive approaches for face recognition. Comput. Vis. Image Underst. **114**(1), 135–145 (2010)
7. Turk, M.A., Pentland, A.P.: Face recognition using eigenfaces. In: Proceedings of the IEEE, pp. 586–591 (1991)
8. Ding, C., Tao, D.: A Comprehensive Survey on Pose-Invariant Face Recognition (2015) arXiv:1502.04383v2
9. Barr, J.R., Bowyer, K.W., Flynn, P.J., Biswas, S.: Face recognition from video: a review. Int. J. Pattern Recognit. Artif. Intell. 26(5) (2012)
10. Zou, X., Kittler, J., Messer, K.: Illumination invariant face recognition: a survey. In: Proceedings IEEE International Conferenfce on Biometrics, Theory, Appl. Syst., pp 1–8 (2007)
11. Zhang, H., Zhang, Y., Huang, T.S.: Pose-robust face recognition via sparse representation. Pattern Recogn. **46**(5), 1511–1521 (2013)

12. Zhang, X., Gao, Y.: Face recognition across pose: A review. Pattern Recogn. **42**(11), 2876–2896 (2009)
13. Zhang, Y., Shao, M., Wong, E.K., Fu, Y.: Random faces guided sparse many-to-one encoder for pose-invariant face recognition. In: Proceedings IEEE International Conference on Computer Vision, pp. 2416–2423 (2013)
14. Beveridge, R., Zhang, H., Draper, B., et al.: Report on the fg 2015 video person recognition evaluation. In: Proceedings IEEE International Conference on Automatic Face and Gesture Recognition (2015)
15. Ouyang, S., Hospedales, T., Song, Y.Z., Li, X.: A survey on heterogeneous face recognition: sketch, infrared, 3D and low resolution (2014). arXiv preprint: arXiv:14095114
16. Chen, D., Cao, X., Wen, F., Sun, J.: Blessing of dimensionality: high-dimensional feature and its efficient compression for face verification. In: Proceedings IEEE Conference on Computer Vision Pattern Recognition, pp. 3025–3032 (2013)
17. Chai, X., Shan, S., Chen, X., Gao, W.: Locally linear regression for pose-invariant face recognition. IEEE Trans. Image Process. **16**(7), 1716–1725 (2007)
18. Ding, C., Choi, J., Tao, D., Davis, L.S.: Multi-directional multi-level dual-cross patterns for robust face recognition, August 2015. arXiv:1401.5311v2
19. Satter, A.K.M.Z., Chowdhury, M.M.H.: A Fuzzy algorithm for de-noising of corrupted images. Int. J. Comput. Inf. Syst. (IJCSI) **6**(4), 15–17 (2013). Silicon Valley Publishers (SVP), United Kingdom
20. Li, H., Lin, Z., Shen, X., Brandt, J., Hua, G.: A convolutional neural network cascade for face detection. In: CVPR 2015, pp. 5325–5334
21. Uddin, J., Mondal, A.M., Chowdhury, M.M.H., Bhuiyan, M.A.: Face detection using genetic algorithm. In: Proceedings of 6th International Conference on Computer and Information Technology, Dhaka, Bangladesh, pp. 41–46, December 2003
22. Shinn-Ying, H., Hui-Ling, H.: Facial modeling from an uncalibrated face image using a coarse-to-fine genetic algorithm. Pattern Recogn. **34**(8), 1015–1031 (2001)
23. Kukenys, I., McCane, B.: Support vector machines for human face detection. In: Proceedings of the New Zealand Computer Science Research Student Conference (2008)
24. Viola, P., Jones, M.: Fast and robust classification using asymmetric AdaBoost and a detector cascade. Adv. Neural Inf. Process. Syst. **2**, 1311–1318 (2002)
25. Heisele, B., Serre, T., Poggio, T.: A component-based framework for face detection and identification. Int. J. Comput. Vision **74**(2), 167–181 (2007)
26. Talele, K.T., Kadam, S., Tikare, A.: Efficient face detection using Adaboost. In: IJCA Proceedings of International Conference in Computational Intelligence (2012)
27. Chowdhury, M., Gao, J., Islam, R.: Human detection and localization in secure access control by analysing facial features. In: Proceedings of IEEE Conference on Industrial Electronics and Applications (ICIEA), China, June 2016
28. Khatun, A., Bhuiyan, M.A.: Neural network based face recognition with gabor filters. IJCSNS Int. J. Comput. Sci. Netw. Secur. **11**(1), 71–76 (2011)
29. Face Recognition Data. University of Essex, UK, Face 94. http://cswww.essex.ac.uk/mv/allfaces/faces94.html
30. Face Recognition Data. University of Essex, UK, Face 95. http://cswww.essex.ac.uk/mv/allfaces/faces95.html
31. Face Recognition Data. University of Essex, UK, Face 96. http://cswww.essex.ac.uk/mv/allfaces/faces96.html