Using Facial Movement for Face Recognition to Unlock the Personal Devices

[1] Ankit Dubey, [2] Shreya Golchha
[1] Assistant Professor, [2] Student
Department of Computer Science and Application
St. Aloysius' College (Autonomous), Jabalpur (M.P.), India

Abstract

Face recognition is one of the techniques used to protect the devices from an unauthorized access by recognizing the human faces. Facts suggest that it is not enough when access is gained by the unauthorized identity using the mask, photographs or video of the authorized user. To overcome this problem many methods have been devised. In this paper we have introduced a layer of facial movement on the top of the existing layer of facial recognition to provide a better security. Imitate of the facial expression (movement) is difficult and therefore unauthorised users can be easily detected.

Keywords: authentication, face recognition, facial movement, eyebrow movements, security

1. Introduction

In today's world where the data is termed as the most important asset. There is a need to secure the data. Many security algorithms have been devised to protect data from unauthorised access. Face detection is a technique that processes image. In this method, the human face is recognized by analysing and identifying human features. In a biometric approach like face recognition, is used in smart mobile devices and laptops which enables identity authentication. It is a challenging task in computer vision. The process used is machine learning algorithm taking dataset as input which identifies an object by taking into account several features like size, colour, height, width etc. These are expressed in form of numerals and are termed as feature vector. The algorithm understands the pattern and compares it with the new object. To unlocks personal device of the user if it detects that the credential is of the authorized.

Numerous researches that have been conducted so far studying human face perception clearly shows how face recognition technique can benefit from human facial expressions. Facial features are different and hence need to be extracted to recognize a person correctly [5]. The use of reverse engineering approach, demonstrated the use of facial features to recognize the familiar and unfamiliar faces [13]. A model for face recognition is proposed by applying approximation on Eigenfaces which resulted in the reduction of the arithmetic units without compromising the success rate [10]. During face perception, physiological features are extracted using face specific brain areas and consistent neural activity is stored. Dynamic signature can be used for face identification as like faces are easier to recognize in the moving sequence [2]. Hyperface detects faces simultaneously localizing landmarks, estimating head pose and identify gender [12]. The ability of human's facial expressions is not only an inborn biological characteristic, but also dependant on emotions [6]. Recognize six kinds of facial expression i.e. angry, disguist, worried, anxious, happy and sad with the satisfactory recognition rate [7]. A non-linear extension to the sparse representation classifier

adapted to real-world conditions that can be trained using single training sample [9]. Action unit is used for describing basic muscle movement of human face with neural network as classifier [1]. The extraction of face part can be identified using the colour based approach [4].

To improve the performance of face recognition is a challenging task. Its challenges are highly dynamic in their orientation, lightening, scale, facial expression and occlusion. However, a very important area has been also neglected so far which requires immediate attention i.e. vulnerability of spoofing attacks [3].
Detection of eye movement in face recognition would help to detect real faces and prevent pictures and mask of authorized to unlock the devices [8]. A mechanism to authenticate the user by allowing only the registered user to input the password hence avoiding the hacking of the password by non-legitimate user [11].

In this paper a method for user authentication, based on facial recognition and movements of eyebrows is proposed . Since each user makes a facial expression in a slightly different way, identities has been explored based on facial behaviours and patterns on facial movements. Movements and behaviours of face are inherent to each user and therefore they are more distinctive and cannot be easily replicated.

The paper is structured as following, the section 1 gives the introduction, section 2 briefs the problem definition and the basic requirements, the section 3 proposes a model for authentication, section 4 elaborates the algorithm for the proposed model and the section 5 contains conclusion and future prospects.

2. Problem Definition and requirements

The problem statement can be formulated as: given video images of a user's face to verify his/her identity by extracting a spatiotemporal facial pattern and comparing it with existing templates in a database also includes the count of eyebrow movement made with the variable count. Generally, it is expected to discriminate user's identity with dynamical facial characteristics which are distinctive and invulnerable to impersonation attacks.

The following are the requirements for facial recognition and pattern generation for eyebrow movements which include the tools/libraries of Matlab, Python (Open CV or cv2, pyautogui, numpy, sys, os, datetime) and Weka. A front facing camera enabled device required to take images of the face. The sample images are stored in a memory to be used by the algorithm for identifying the face taken by the camera.

3. Proposed Model

The personal data is at the risk of being stolen from the personal device. Using the current method the device can be unlocked by the person with similar face that of the registered user. Face Recognition along with facial expression pattern can be used to provide security, facial expressions are difficult to be replicated even if there exist two similar faces. Therefore unauthorized access can be eliminated also the pattern of facial expression provides a higher security.

3.1 Model Architecture

A model for eyebrow movement technique in association with face recognition is proposed to improve the application of cheating of screen unlocking by a human face. When the user operates the mobile device, it needs to use face recognition authentication to complete user's identity identification before the user can enter the mobile device

system. The model architecture can be divided into seven blocks, which are respectively face acquirement, face detection and recognition, face image database, eyebrow detection, eyebrow acquirement, eyebrow database and eyebrow pattern recognition. The function of each block is described as follows:

1. **Face acquirement:** The front facing camera of the device acquires face images.
2. **Face Detection & Recognition:** A face is located in the image using the human facial features. Then face recognition finds a face from an image with matching face samples on a face image database.
3. **Face Image database:** It stores the acquired face images and registered face images to be used as face samples for search.
4. **Eyebrow detection:** It locates the eye and eyebrow regions in the face image using any algorithm.
5. **Eyebrow acquirement**: It obtains the eyebrow movement features and counts the number of times the eye-brows moved. The eyebrows can be lowered, raised, middle-raised, middle-lowered and middle together. The basic eyebrow movements are explained below:
    1. **Lowered** – Lowering the eyebrow hide the eyes to a certain degree.
    2. **Raised** – The eyebrows are raised and the eyes are opened wide. Some people can raise only one eyebrow at a time.
    3. **Middle-together** – When the eyebrows are pulled together inwards, it slightly changes the shape of the eyebrows.
6. **Eyebrow database:** It stores the pattern formed by the face image to be used against the eyebrows movement acquirement.
7. **Eyebrow Pattern Recognition** - The eyebrow movements acquired from the face video images is matched against the samples of the eyebrow movements on a face video image database.

When the system starts, it will acquire one image in each second. Next, it will find a face from the face image with face samples on a face database to achieve user's identification. If she/he is identified, the eye-brow detection will start. Finally, the eye-brow movement acquirement counts the number of the eye-brow movements within the time set, and if it matches the eyebrow database the screen will be unlocked.

3.2 Face Detection and Recognition

Face feature database provided by Open CV is adopted and can be divided into a face detection function and a face recognition function. For the face detection function, through Haar feature, face features will be automatically detected to find a face so as to enhance automatic control on face recognition authentication to reduce the execution time. Eigenface and Fisherface are adopted to set up face image model, and Kth-Nearest Neighbor (KNN) is used to compare the featured points.

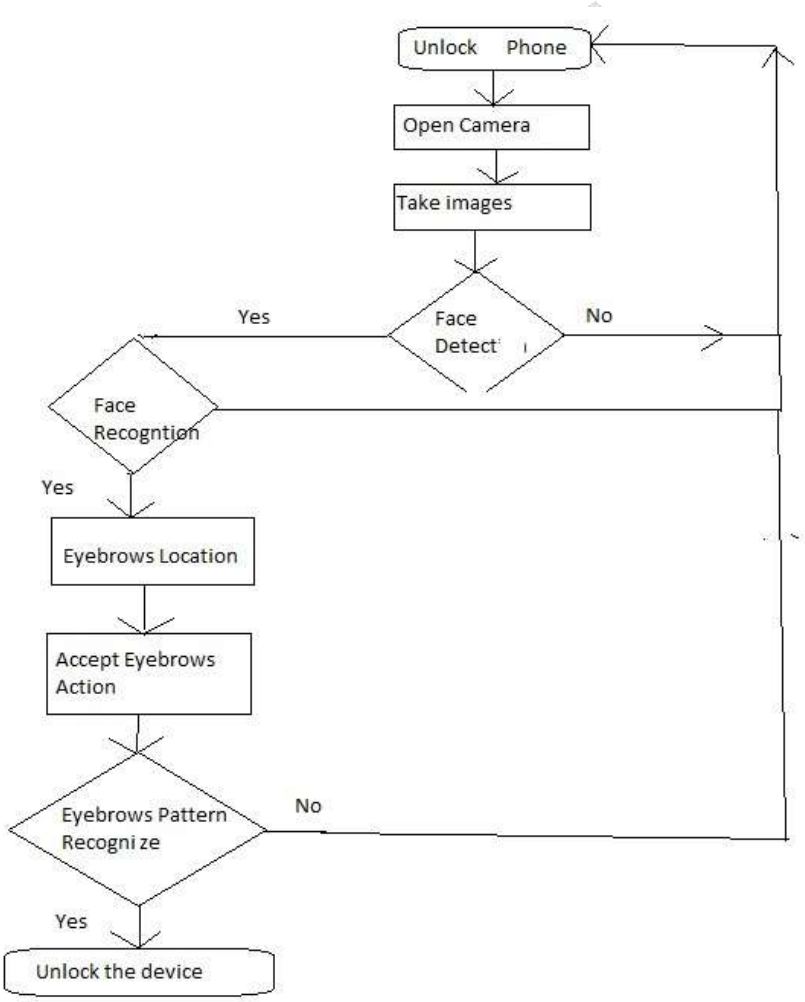
3.3 Eyebrow Detection and Pattern Recognition

This method can precisely locate the regions of eye and eyebrows by using an adaptive geometric ratio of a human face [12]. The binarization image of the user is detected, and the threshold value of black pixel of face is defined. Next, eyebrow detection model is added to capture continuously eyebrow information so that the system can own face detection and eye detection models to facilitate later eyebrow movements. After the face detection and recognition,

the method locates the position of eyebrows on the face image and record using the eyebrow acquirement function the sequence of actions performed by the eyebrows at the time period. Using the Eyebrow Pattern Recognition function these sequence of eyebrow movements is compared with the eyebrow database.

When an eyebrow moves affecting the different muscles results in the change in the size, shape and proportion of the eyebrow/s with respect to the eye. Different people have different shapes, size and proportion while performing different eyebrow expressions. The expression is difficult to copy and is used as a protection in this paper.

4. Flowchart



5. Conclusion

The method is proposed to overcome the existing problem of cheating the personal device by having the mask of the authenticated user or unlock of the device due to similarity of two faces. The face can be similar but the facial expression differentiates the person. In this paper, the security is provided by adding facial movement during the face recognition.

References

1. Kobayashi H and Haro F, "Analysis of neural network recognition characteristics at basic facial expression", Transactions of the Japan Society of Mechanical Engineers Series 222, 1994.
2. Haxby J, Hoffman E and Gobbini M, "The Distributed Human Neural System for Face Perception," *Trends in Cognitive Sciences*, vol. 4(6), pp. 223-233, 2000.
3. Jain A. K., Ross A. and Prabhakar S., "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14(1), pp. 4-20, 2004.
4. Kushwaha R & Nain N & Jangra P., "Extraction of Lip Contour from Face", International Journal of Current Engineering and Technology, vol 2(2), 2012.
5. Roy, M.S. and Podder, M.S., "Face Detection and its applications, International Journal of Research in Engineering & Advanced Technology", vol 1(2), pp 1-10, 2013.
6. Du S., Tao Y. and Martinez A. M., "Compound facial expressions of emotion", *PNAS, pp.* E1454–E1462, 2014.
7. Lia J, Zhanga D, Zhanga J, Zhang J, Teng Li, Yi Xia, Qing Yan, and Lina Xun, "Facial Expression Recognition with Faster R-CNN", Procedia Computer Science, vol. 107, pp. 135 – 140, 2017
8. Chu C. H. and FengY. K., "Study of Eye Blinking to Improve Face Recognition for Screen Unlock On Mobile Devices", J Electr Eng Technol, vol 13(1): pp. 1921-718, 2017
9. Ouanan H, Ouanan M and Aksasse B, "Non-linear dictionary representation of deep features for face recognition from a single sample per person" , Procedia Computer Science 127, pp. 114–122, 2018
10. Marso, K., & Nannarelli, A., "Face Recognition using Approximate Arithmetic", Dtu Compute Technical Report, Vol. 02, pp. 1-23, 2018
11. Shukla S, Helonde A, Raut S, Salode S, Zade J, "Random Keypad and Face Recognition Authentication Mechanism, International Research Journal of Engineering And Technology", vol 5, pp. 2395-0072, 2018.
12. Ranjan, R., Patel, V. M., and Chellappa R, Hyperface: "A Deep Multi-Task Learning Framework for Face Detection, Landmark Localization, Pose Estimation, and Gender Recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence", pp. 121 – 135, 2019.
13. Abudarham, N., Shkiller, L., & Yovel, G., "Critical Features for Face Recognition", Cognition, vol. 182, pp. 73–83, 2019