ISSN 2320 - 2602
Volume 7 No.4, March 2018
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst02742018.pdf
https://doi.org/10.30534/ijacst/2018/02742018

Advance Facial Recognition Using Liveness Estimation With Multi-Model Techniques

Engr Fahad Ali Khan
[1]Department of Computer Systems Engineering, University of Engineering and Technology, Peshawar, Pakistan
Email: engr.fahadalikhan@gmail.com

ABSTRACT

This research work focuses on the importance of facial biometric systems and their limitations. Biometric system is emerging technology that focuses on identifying a person on his/her physiological characteristics. Biometric systems are assumed to be better than password protected systems because of their authenticity. Facial Biometric systems have also some limitations. The proposed scheme took advantage of multi-model facial biometric techniques for liveness estimation. The liveness estimation is done by two different models. i.e. Detection of hand movement and letters recognition. The results based on real and artificial data proved that the scheme efficiency is 85% more effective as compare to the other schemes.

Keywords: Facial recognition, Biometirc systems, Multi-model Biometrics, object detection, alphabets recognition.

1. INTRODUCTION

The systems where passwords were being used for financial transactions, computer networks and other security systems are now replaced by Biometrics systems. Password protected security systems are easily available for unauthorized access by discovering other's security key and is available to imposters for unlawful actions. Biometric system is emerging technology that focuses on identifying a person on his/her physiological characteristics. It basically depends upon unique biological traits to work efficiently. As every person have unique biological characteristics for identification. Facial biometric system compares, a biometric data which is stored previously, with the current biometric data of query person to check whether the person has been registered or not, if it found that person is recognized correctly then authentication is given otherwise declined, so it is considered to be more secure as compared to the password protected security systems. In real time processing, a live facial biometric system works in such a way that it takes a single frame from real time video and detects face and recognizes it. If a picture of a registered person is shown to the facial biometric system then its security is bypassed and access is allowed to an imposter.

The proposed algorithm focuses on the identification and avoidance of false facial biometrics. Many researchers worked in this area to avoid face spoofing.

For liveness estimation Socolindky D. A [1] took advantage of using thermal infrared camera and came up with justified results but main drawback is usage of extra hardware and cost. In terms of software based techniques. Li[2] found that high frequency of live face is greater than high frequency of image. Liveness analysis tries to detect liveness in an image based on detection of movement organs that can't be noticed in a photograph. Eye blinking is a natural phenomenon G.pan [3] worked on eye blinking and come up with justified results. He calculated the degree of eye close and observed good results. Many researchers brought new ideas to avoid spoofing by using multi-model techniques and achieved their goals. Frischholz [4] combined face recognition with voice recognition for better results.

Purpose of this research work is to minimize the threat challenges encountered by facial biometric systems in order to allow access to real and live query person. This can achieved by adding multi-model software based techniques to defeat such fraudulent attempts.

2. LITERATURE REVIEW

If A high quality (HQ) or high definition (HD) picture is shown to facial biometric system. Its security can be broken and authentication can be accessed for unlawful purposes. This shows that facial biometric system has number of limitations and has vulnerability to spoofing attacks, which directly challenges its security measures.

With increase in technology it is well known fact that facial biometric system is taking place of password protected system. It has become important for facial biometric systems to overcome such type of problems.

This research is useful for liveness estimation of a human and motivation for researchers to work in this area of facial biometric systems to improve previous work.

Biometric system is emerging technology of present and future, researchers are working in his area to make facial biometric systems more defendable against spoofing attacks.

Our proposed methodology adds software based technique for liveness estimation, which can't be bypassed by any inanimate biometric.
Generally anti-spoofing technique is categorized into three main branches.

Hardware based Techniques

They are also known as sensor based techniques. In these technique special characteristics of a person is identified such as facial thermo gram, blood pressure and fingerprint.
Multi-model technique is introduced in hardware based biometric recognition in order to increase its robustness[5].
Thermal infrared camera is example of hardware based techniques.

Software based Techniques

They are also known as feature based techniques. Many researchers also worked in this area. Motion analysis is one of the examples of software based anti-spoofing technique. Using software based anti-spoofing technique B. Peixoto [6] worked on Gaussian filter and observed that edges of reacquired image are unclear with respect to genuine image.

Score level techniques

This is the combination of hardware-software based techniques. Combination of face recognition with voice recognition showed better results for anti-spoofing [4, 7]. Experiments show better results than single model techniques.

Object Detection

Object detection is a machine learning approach which is capable of obtaining high detection rates for detection of objects in an image.
For object detection Viola and jones algorithm has become standard. They introduced 'integral image' concept for fast feature evaluation which is capable of avoiding direct intensity computation. Small number of important features is grouped together for classification using using 'Adaboost'. Following are the components for detection of any object using Voila and jones algorithm[8].

- Haar feature.
- Integral image.
- Adaboost.
- Cascading.

Face Detection

Face detection is similar as object detection. Same steps are required for detecting different parts of face. Face detection classifier is trained by using positive and negative samples. Positive samples consist of faces and negative samples consist of non-faces. After training the classifier, it is capable to between faces and non-faces [9, 10].

Face Recognition.

A computer program which has ability to identify/classify from digital image is face/facial recognition.
Face recognition is same as object recognition; it specifically works upon recognizing certain objects that are trained to be classified by the classifier.
Following are the main points for recognition of facial biometric systems.

- Database.
- Extraction of facial features.
- Learning or modelling.
- Query image.
- Detection of face.
- Extraction of facial features of detected face.
- Classifier then identifies the query image and matches it with database.

3.METHODOLOGY

The first step of this scheme is based on face detection and then faces recognition. Liveness estimation is the core part of this scheme. MATAB is used for testing this scheme on real and artificial data (e.g. extraction of facial features, classification for identification with query face).

Workflow of proposed scheme is as follows

- Database for members.
- HoG features extraction of database members.
- Acquisition of image from live video and face detection and cropping for better results.
- HoG features extraction of query image.
- Matching extracted features of query image with extracted features of database members.
- Liveness estimation for further authentication.
- Liveness is detected by moving hand and then liveness is estimated by letters recognition.

Proposed scheme for biometric verification if identifies the query person as genuine and real person then access is allowed otherwise rejected.

Liveness is estimated with multi-model technique. First one is to order the user to move his/her hand and the other method is to ask the user to say M or O randomly. It can be achieved by training our classifier to differentiate between M and O. Both are detected using feature based techniques for object recognition with viola jones algorithm [9]. Flowchart of proposed scheme is shown below.

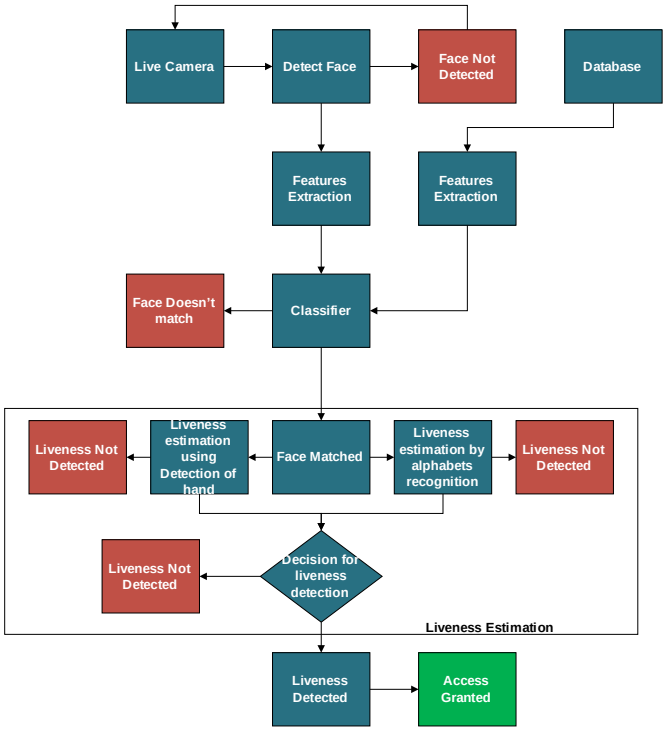

Figure1. Flowchart of proposed scheme

4.SIMULATION RESULTS ANS ANALYSIS

For achieving best results for face detection, voila jones algorithm is used and almost 97% accuracy is attained. Face recognition using HOG facial feature extraction[11] is found to be better in the circumstances with constant illumination than other face recognition algorithms.

The benchmarks scheme include face recognition using Hog features extraction and face recognition using principal component analysis (Eigen faces).

Database	No of faces per person	No of people	Faces for training	Faces for testing	HOG Recog Rate	PCA Recog Rate
FEI	15	15	12	3	89.1	82.10
AT&T	25	25	20	5	76.5	67.66
Yale databas	15	50	12	3	81.2	77.10
BIOiD	20	40	16	4	91	81

Detection of hand is achieved by voila and jones algorithm for object detection. As discussed earlier this approach is based training a classifier by giving thousands of positive images and negative images. After processing of haar features, integral image and adaboost classifier (for discarding useless features) then it comes cascade classifier. Cascade classifier consists of strong classifiers that contain information regarding specific objects feature. Each stage determines that whether the stage contains justified feature about an object or not, if yes then it move to the next step otherwise discarded [12].

The cascade classifier consists of stages, containing weak classifiers. Each stage is trained using a technique called boosting. A strong classifier is made up of weak classifiers.

Every step/stage of learner labels the area as positive or negative. Positive shows that the desired object was found and negative shows that desired object wasn't found. In case of negative, Classification is stop and indicates that region is complete. In case of positive, classifier passes the region to the next stage.

Stages with negative samples discard it quickly. Stages with positive samples made the conclusion that object is found at current location.

Following are the traits considered while working with these classifiers.

- When a positive sample is correctly classified, a true positive occurs.
- When a negative sample is misclassified as positive then false positive occurs.
- When a positive sample is misclassified as negative then false negative occurs.

False negative rate is set to low because if a positive sample is misclassified as negative then classification stops. False positive rate is set to high because if a negative sample is misclassified as positive it can be corrected in next stage.

Following are the trade-offs while setting up the parameters.

Condition	Consideration
While dealing with large amount of data	Increase false positive and number of stages
While dealing with small amount of data	Decrease false positive rate and number of stages
Reduction of missing an object	Increase true positive rate.
Reduction of number of false detections	Decrease false alarm rate or increase the number of stages

The better way to deal with cascade classifier is to give positive images with ROI (region of interest) in thousands and negative samples are not specified explicitly. Negative samples are almost double of positive samples.

In case of detection of hand in image, different trade-offs were applied and found the results shown in figure.

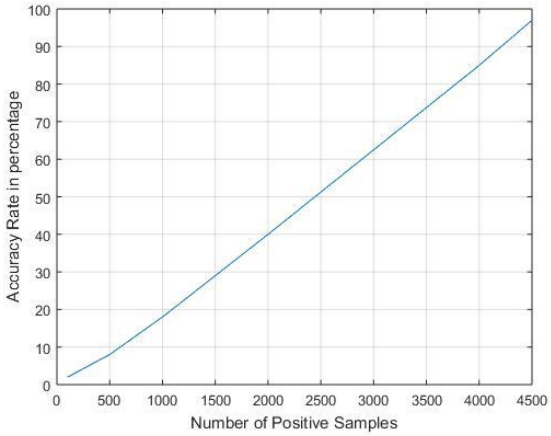

Figure2. Number of samples versus accuracy

Above figure shows that by increasing number of samples accuracy is increased and desired output is achieved.

Face Detection and face recognition results

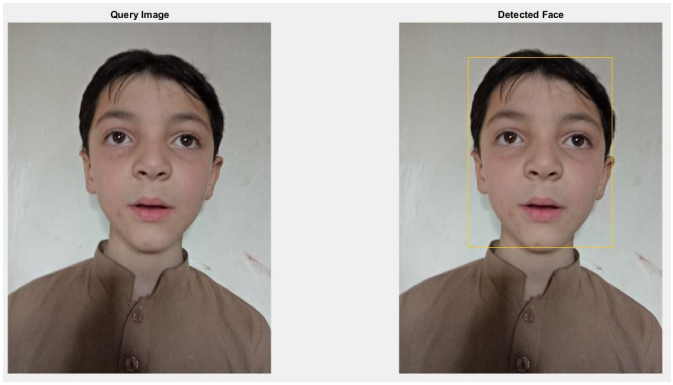

Figure a. Query Image and detected face

Figure a. shows the query person and detected face using voila and jones algorithm for frontal facial parts detection.

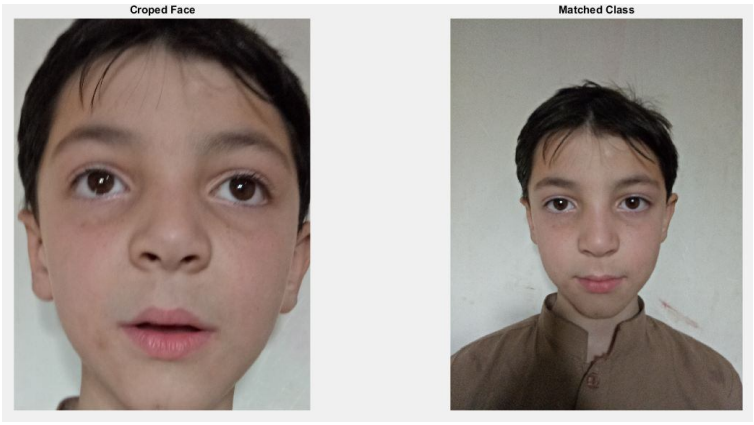

Figure b. Cropped Image and Matched Class

Figure b. shows the cropped image of detected face image and matched class with one of picture present in database for identification of person.

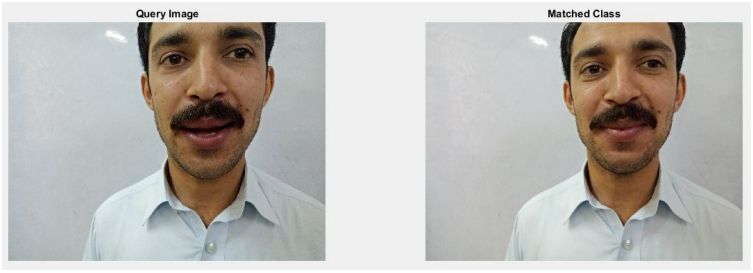

Figure c. Query Image and Matched Class

Liveness estimation

As discussed earlier that liveness is estimated by two methods. First one is detection of hand in an image.

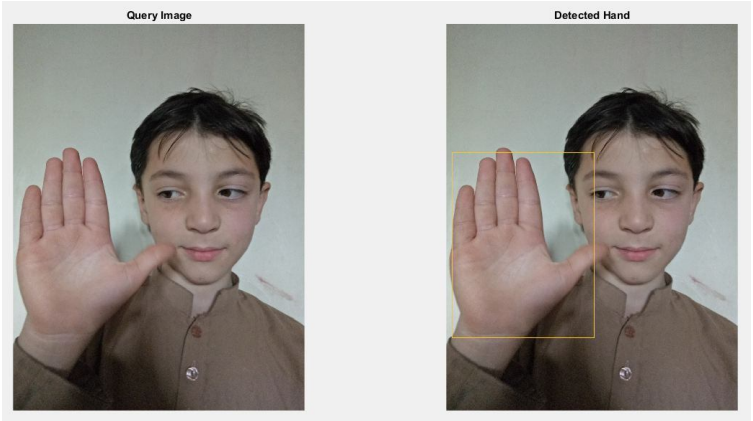

Figure3. Query image and detection of hand

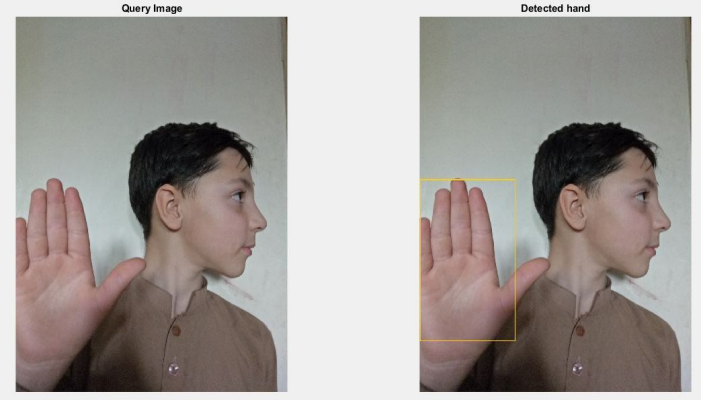

Figure4. Query image and detection of hand

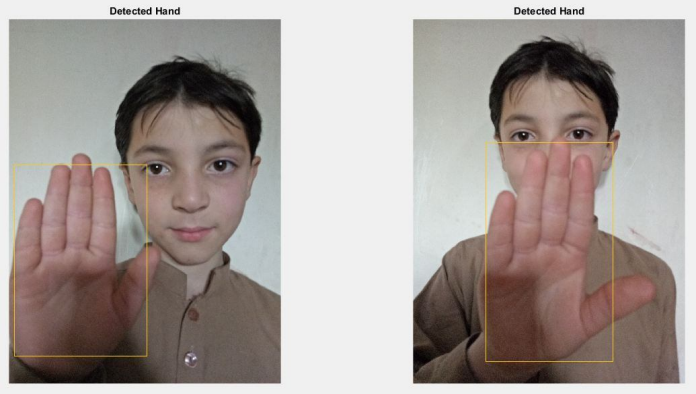

Figure5. Detection of hand

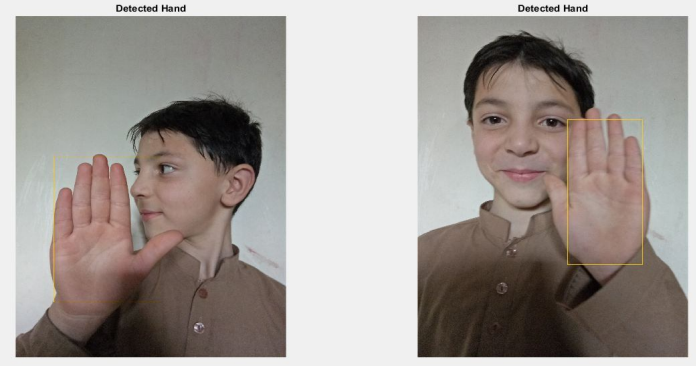

Figure6. Detection of hand

Alphabets recognition is another method for liveness estimation. Our proposed algorithm only works with two letters recognition i.e M and O. User is asked to say M and O randomly. We have trained our classier by giving thousands of positive images with detected lips and movement of lips in O and M style. Mouth detection and letters recognition is done by viola and jones algorithm for object detection [13].

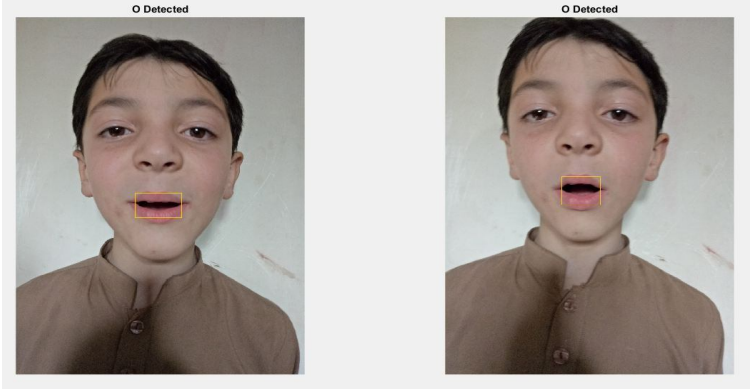

Figure7. Detection of letter O

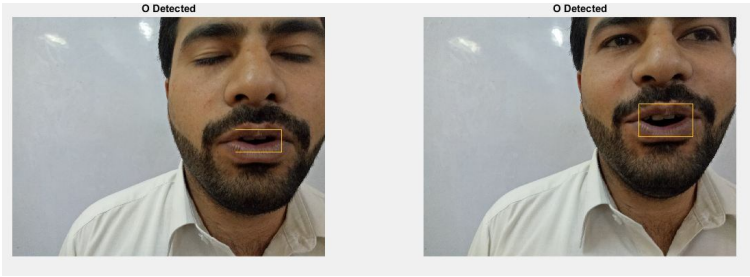

Figure8. Detection of letter O

Figure9. Detection of letter O

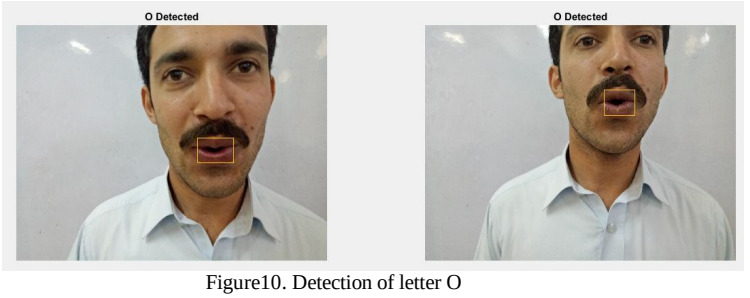

Figure10. Detection of letter O

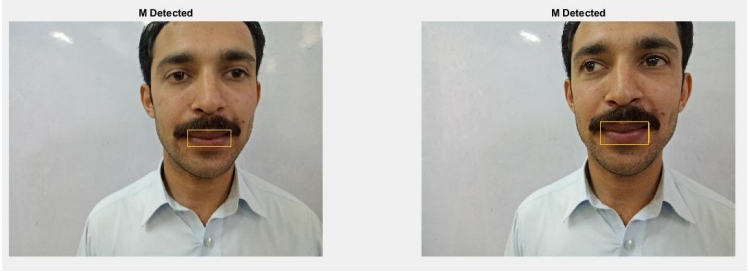

Figure11. Detection of letter M

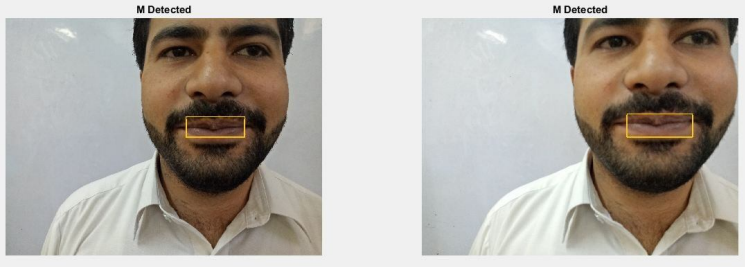

Figure12. Detection of letter M

Figure13. Detection of letter M

5.CONCLUSION AND FUTURE WORK

Results show that our proposed scheme is 98% efficient when tested on real time data. Multi-model technique has many advantages over single model technique. Chances of fake biometric reduce to 95% while using multi-model techniques.

Fraudulent attempts with 3D masks are still a threat to current facial biometric system. Our scheme also fails when dealing with 3D Mask spoofing.

New ideas in object detection such as emotion detection etc can be added into the future work for improving current facial biometric systems.

REFERENCES

1. Socolinsky, D.A.S., A. & Neuheisel, *Face Recognition with Visible and Thermal Infrared Imagery*. Computer Vision and Image Understanding,, 2003. **91**.
2. Li, J.W., Y. & Tan, T. & Jain. *Live Face Detection Based on the Analysis of Fourier Spectra, Biometric Technology for Human Identification*. in *SPIE*. 2004.
3. Gang Pan, Z.W.a.L.S., *Liveness Detection for Face Recognition.*
4. Frischholz, R.W.D., *U. Bio ID: A Multimodal Biometric Identification System.* IEEE Computer, 2000. **33**.
5. javier Galbally, Sébastien Marcel, and J. Fierrez, *Biometric Antispoofing Methods: A Survey in Face Recognition.*
6. B. Peixoto, C.M.a.A.R., *Face Liveness Detection under bad illumination conditions*, in *18th IEEE International Conference on Image Processing*. 2011.
7. Chetty, G.W., M, *Multi-level Liveness Verification for Face-Voice Biometric Authentication.* Biometric Symposium 2006, Baltimore, Maryland., 2006.
8. Jones, P.V.M., *Rapid Object Detection using a Boosted Cascade of Simple Features.* Mitsubishi Electric Research Labs Compaq CRL 201 Broadway, 8th FL One Cambridge Center Cambridge, MA 02139 Cambridge, MA 02142.
9. Paul viola, M.j., *Robust Real-Time Face Detection.* 2003.
10. Wang, Y.-Q., *An Analysis of the Viola-Jones Face Detection Algorithm.*
11. O.deniz, G.B., J.salido,F.Dela Torre, *Face recognition using histogramof oriented gradient features.* 2011.
12. Singh, H., *Object Detection using Haar-like Features.*
13. Hassankashi, M., *Combination of Speech Recognition with Lip, Face and Body Features for having Transparent Messages from Patients.* 2014.