# Anti-Spoofing In Face Recognition with Liveness Detection Using Pupil Tracking

M. Kıllıoğlu*, M. Taşkıran*, N. Kahraman*

*Yildiz Technical University/ Electric and Electronics Department, Istanbul, Turkey
mehmetkillioglu@gmail.com, mrttskrn@yildiz.edu.tr, nicoskun@yildiz.edu.tr

***Abstract*—In this work, we focused on liveness detection for facial recognition system's spoofing via fake face movement. We have developed a pupil direction observing system for anti-spoofing in face recognition systems using a basic hardware equipment. Firstly, eye area is being extracted from real time camera by using Haar-Cascade Classifier with specially trained classifier for eye region detection. Feature points have extracted and traced for minimizing person's head movements and getting stable eye region by using Kanade-Lucas-Tomasi (KLT) algorithm. Eye area is being cropped from real time camera frame and rotated for a stable eye area. Pupils are extracted from eye area by using a new improved algorithm subsequently. After a few stable number of frames that has pupils, proposed spoofing algorithm selects a random direction and sends a signal to Arduino to activate that selected direction's LED on a square frame that has totally eight LEDs for each direction. After chosen LED has been activated, eye direction is observed whether pupil direction and LED's position matches. If the compliance requirement is satisfied, algorithm returns data that contains liveness information. Complete algorithm for liveness detection using pupil tracking is tested on volunteers and algorithm achieved high success ratio.**

***Keywords—eye location; liveness detection; face recognition; spoof-attack algorithm***

## I. INTRODUCTION

Access control systems generally uses traditional identification systems depend on a password to remember or a key to possess. In recent years, biometric recognition that needs automatic valuation of an individual's identity is used instead of these traditional methods because a biometric can't be lost or forgotten. However, there may be many fraud attempts on biometric systems, for example; one can steal any person's fingerprints, face or iris images, voice recordings, even the DNA which are used as private features in these systems. Therefore, it has to be sensitive to spoofing attacks where a person tries to masquerade as another one by falsifying data and thereby gaining an illegitimate advantage. As biometric recognition systems used in many places they perform better accuracies day by day, potential impostors may try to access to the system by directly interacting with the access system input device, like a genuine user would. Such methods of fooling a biometric systems are commonly referred as spoofing attacks.

Face recognition is the easiest biometrics to spoof because the data is easily collectable and furthermore uncomplicated to steal like taking photos from online social media profiles. Also for a simple attack, no specific technical skills are needed, even some attacks can be performed by ordinary people [1].

In general, there are three possible ways to generate a face spoof attack; taking a photo, reproducing a video, 3D model of a valid user [2].

Liveness detection is one of the basic countermeasure against spoofing. The purpose is to sense physiological life signs such as eye blinking, facial expression changes, mouth movements etc. Another existing countermeasure to spoofing attacks consists of combining face recognition with other biometric modalities such as gait and speech. Indeed, multi-modal systems are intrinsically more difficult to spoof than uni-modal systems [3].

Short surveys of some schemes against photograph spoofing attacks can be found in [4-8]. Pan et al. [10] proposed an eyeblink-based anti-spoofing method whereas Kollreider et al. [9] presented an optical-flow based method for observing motion of face images. The disadvantages of these methods can be seen when using a video or simply shaking the photograph before the camera. There are also mouth movement [11-14], head movement or shape [15] based liveness detection databases and studies for video attacks in the literature.

In this work we have developed a pupil direction chasing system for anti-spoofing in face recognition systems using a basic hardware equipment. We first obtained eye area in real time video ant then pointed the pupil and started to observe the pupil. We also used an Arduino to activate a random LED in a simple system that is used near face recognition system. After obtained a few pupil number, Arduino activates a random LED and eye direction is observed whether pupil direction and LED's position matches. If the requirement is satisfied the volunteer passes liveness detection part and then face recognition scheme starts. We have tested the system with both photograph and simply shaking the photograph before the camera. We also tried to test the system with real time video on a mobile phone.

The proposed algorithm and hardware are presented in Section 2. Rest of the work, test results and conclusion, is explained in Section 3.

978-1-5090-5655-2/17/$31.00 ©2017 IEEE

## II. PROPOSED ALGORITHM

The proposed algorithm that verifies liveness for biometric authentication systems has 5 important steps.

- Eye area extraction from live camera vision
- Eye area tracking using KLT algorithm [16-18]
- Pupil localization for finding person's eye direction
- Activating random LED on the square frame
- Verifying pupil direction

Block diagram of proposed algorithm is given in Fig. 1.

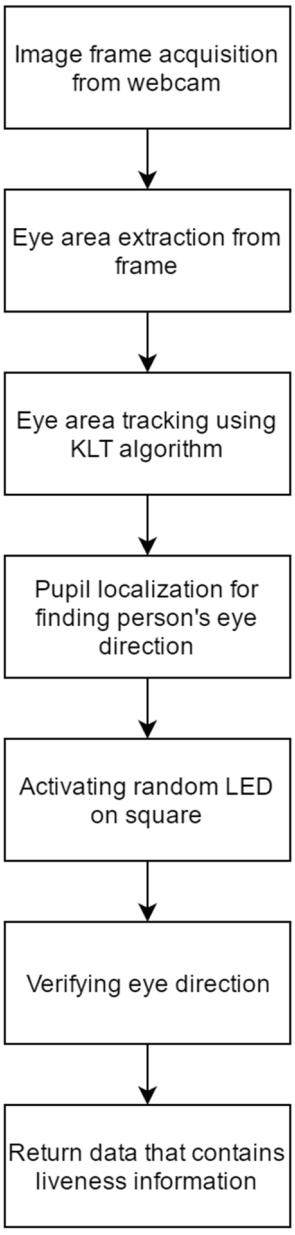


Figure 1. Block diagram of proposed algorithm

### A. Eye area extraction from live camera vision

Position In this step, Haar-Cascade Classifier that has already proven its success in detection algorithms is used for eye area extraction from real time frames. In this study, algorithm only uses Haar-Cascade Classifier when either its first iteration or there is not enough number of feature points for tracing eye area with KLT algorithm. Using specially trained classifier for eye detection, windows are being scanning through image for finding interest area. But this will require high processing power and time, to improve this method, Adaboost algorithm is used. Adaboost algorithm is mainly sum of weak classifiers to get strong classifier. This process will reduce computation time significantly. Adaboost related equation is given in (1).

$$F(x) = \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 + \cdots \quad (1)$$

$f_{\mathrm{n}}$ denotes weak classifiers in frame, while $F(x)$ denotes strong classifier and $\alpha_n$ are constants. To train a Haar-Cascade Classifier, sufficient number of images that contains and not contains desired area is required. In this paper, classifier that trained for eye area is used.

### B. Eye area tracking using KLT algorithm

In this method, algorithm should work at real-time to process eye movements from every frame captured from camera. Haar-Cascade classifiers are weak for using in every iterations. KLT-algorithm needs lower computational power and time, also can acquire desired area stable even if area is rotated with an angle. KLT algorithm finds feature points like corner points, stains or junction points to trace stabilized eye area in every frame that acquired from camera. Eigenvalue algorithm has used for finding these feature points. Each feature point has feature vector that gathered from neighbor pixels. Observing the movement of the feature points at desired region between two frames by using feature vectors provides us tracking eye area quickly and independent from person's movement.

$$G(x,y) = \sum_{wx}\sum_{wy}\begin{bmatrix} I_x^2 & I_xI_y \\ I_xI_y & I_y^2 \end{bmatrix} \quad (2)$$

$$\lambda_m = \min(\lambda_1, \lambda_2) \quad (3)$$

$$T = r * \max(\lambda_m) \quad (4)$$

In (2), G is autocorrelation matrix while $I_x$ and $I_y$ are the first-order derivative images that are located along the x axis at the pixel position (x,y). At the same time, $W_x$ and $W_y$ are the window sizes defining the number of pixels included in the computation. In (3), $\lambda_m$ means smallest values of two eigenvalues that expressed as $\lambda_1$ and $\lambda_2$. In (4), global threshold expressed as T while r is a constant value that changes between 0 and 1. KLT algorithm's flowchart is given in Fig. 2.[19]

### C. *Pupil localization for finding person's eye direction*

Eye map are constructed using morphological operations for finding pupil positions. For eye map construction, input frame's color space is changed from RGB to YCbCr. Y layer of YCbCr contains luminance component while Cb and Cr layers contain chrominance component. YCbCr color space provides us more information for finding pupil points. Eye center points are lighter on Cb layer while points are darker on Cr layer as seen in Fig. 3. EyeMapC is constructed using this difference between layers. EyeMapC construction equation is given In (5) [20].

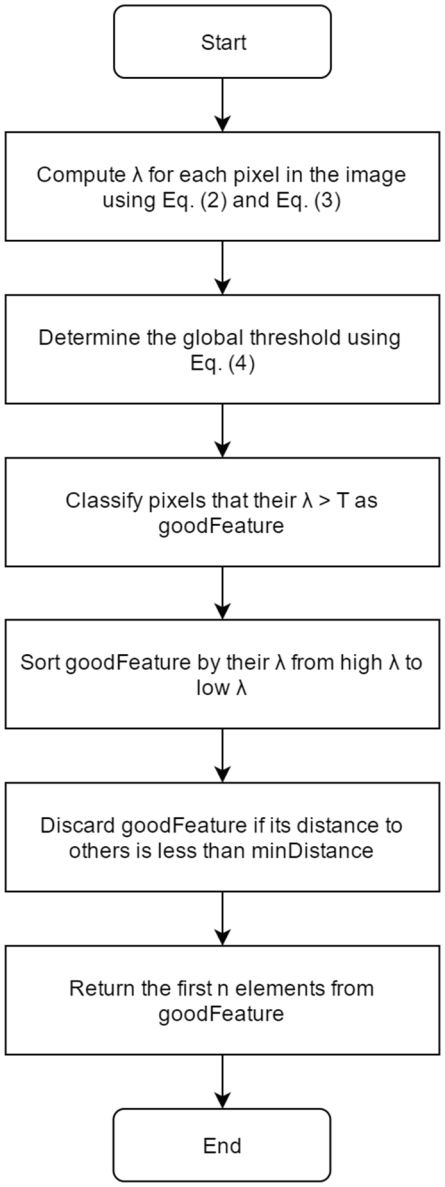


Figure 2. KLT algorithm's flowchart

$$EyeMapC = \frac{1}{3}\{Cb^2 + (255 - Cr)^2 + \frac{Cb}{Cr}\} \quad (5)$$

In (5), (255-Cr) denotes negative of Cr component while Cb and Cr presents chrominance component of YCbCr frame. In addition, $Cb^2, (255 - Cr)^2$ and $\frac{Cb}{Cr}$ values are normalized between [0,255] separately.

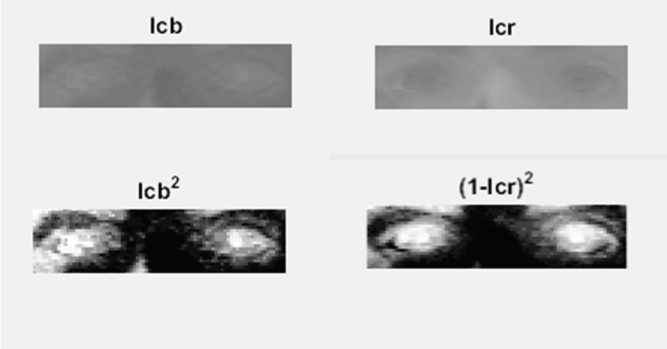


Figure 3. Eye features in YCbCr color space. Icb and Icr represents YCbCr frame's chrominance components Cb and Cr, respectively. $Icb^2$ denotes squared values of Icb and $(1 - Icr)^2$ denotes square of negative Icr frame.

Erosion and dilation morphological operations on Y layer are used for creating EyeMapL. Construction of EyeMapL is given in (6).

$$EyeMapL = \frac{Y(x,y) \oplus f(x,y)}{Y(x,y) \ominus g(x,y) + 1} \quad (6)$$

In (6), $\oplus$ denotes dilation operation while $\ominus$ denotes erosion operation. Y layer of YCbCr frame is expressed as $Y(x,y)$. Both $f(x,y)$ and $g(x,y)$ are circular structing elements. Radius selected as 1/20 of eye frame's width for $f(x,y)$ while 1/10 for $g(x,y)$. This radius ratios are estimately equal to gaze size in eye area frame. Plus one at divider is for preventing result of infinitive. As seen in Fig. 4, eye centers are brighter than other points in EyeMapC and EyeMapL. EyeMap is constructed by logical AND operation between EyeMapC and EyeMapL. Erosion and dilation morphological operations performed on EyeMap to get more accurate eye map. In final, eye center locations are acquired from EyeMap by selecting maximum point on each eye. In Fig. 5, results from eye location algorithm using The Extended Yale Face Database B are given.

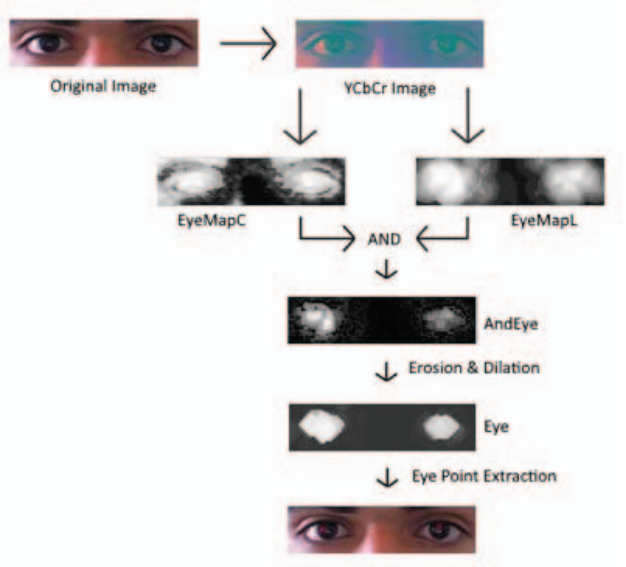


Figure 4. Processed results based on EyeMap method

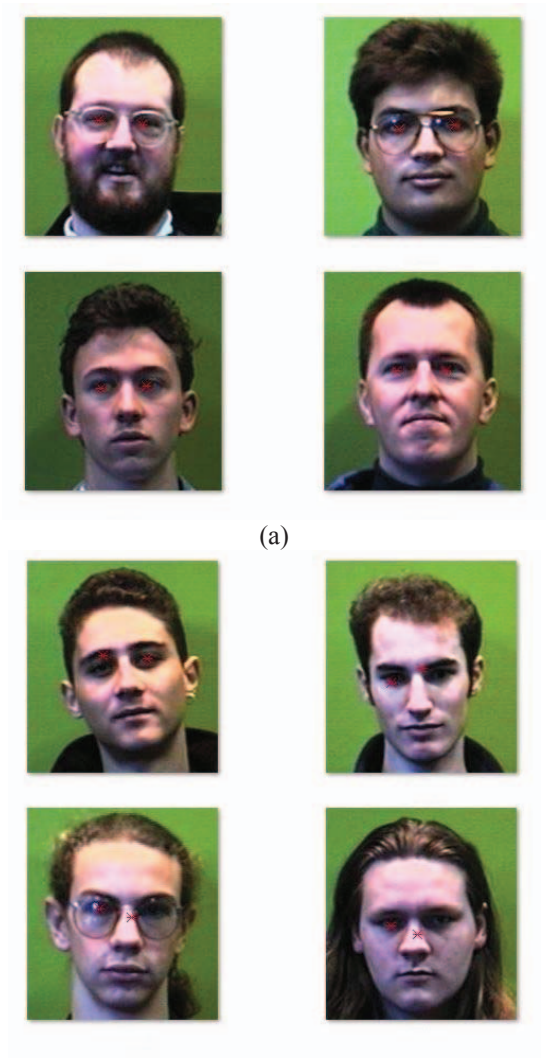

Figure 5. Eye location results on The Extended Yale Face Database B (Successful results in (a), failed results in (b))

### D. Activating random LED on square

In this work, face recognition system's security is improved by adding an extra layer of security. Following this stage, the one of the LEDs is activated randomly after determine the iris point and liveness test is realized to following the iris point movement according to LEDs. The one of the LEDs, which is placed at regular on rectangle frame, is activated randomly using serial communication between computer and Ardunio. The stage is the preliminary step to check the direction of the eye with LED direction.

### E. Verifying eye direction

In the previous stage, the suitability of the eye direction with the position of the activated LED is studied. A certain number of eye direction images are recorded. The liveness test will over if a certain fitness level between recorded data and LEDs direction is satisfied and the data about verification the liveness of the person are transmitted to the biometric system. The liveness test will restart with changing the LEDs direction, which will be activated, if a certain fitness level cannot be provided. When determining the level of compliance, basis vectors of the eye direction for each snapshot is collected according to eight different LEDs identified by four basic direction vectors. Four most approved directions in areas of basic vectors are selected to form the two main aspects of the eye vector. In generated eye vector, two main aspects are being processed. If difference of these two main aspects approve count is larger than threshold, vector is edited to have only one direction. Otherwise vector stands as it is. Verification algorithm's block diagram is given in Fig. 5. The liveness test's reliability depends on human reflexes that following the activated LED by eye movement.

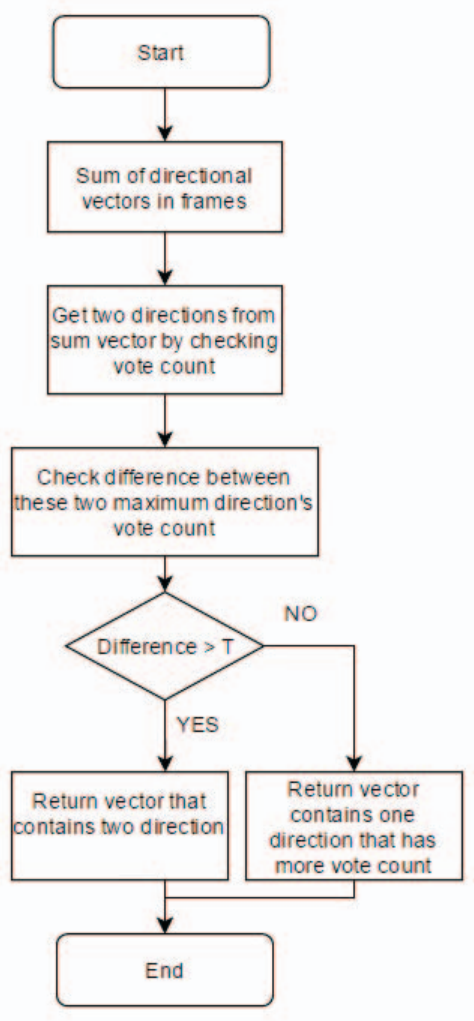


Figure 6. Verification algorithm's block diagram

## III. RESULTS AND CONCLUSION

The reliability of biometric system's security is improved with proposed method by checking liveness status of person to prevent Fake Face Movement. Proposed method can be used on an existed biometric verification system with small number of modification. Proposed method is a low-cost solution to improve security. One of the important issues in recent studies that providing a stable eye frame to algorithm is solved by using KLT algorithm which will also reduce the computation time to improve performance of algorithm. KLT algorithm also provides

stable eye frame even if person moves from current location. Eye location detection algorithm is tested on The Extended Yale Face Database B to get success ratio of algorithm. Success ratio on all database is 89.7%. Success ratio on database that excluded persons with glasses is 94.8%. Proposed eye location method compared with other methods in Table I. Runtime of proposed method for finding eye location from color image with 167x42 resolution is around 160 milliseconds. Complete algorithm is tested (alive or fake) on volunteers and algorithm achieved 98% success ratio.

Furthermore we have tested proposed algorithm with mobile real time videos and the system couldn't find the pupil centers therefore the result showed that attempt is fake. Future efforts will be directed towards improving eye location algorithm to get more accurate eye points. More accurate eye points will provide more secure algorithm. Test figures for proposed system are given in Fig. 7-15.

## ACKNOWLEDGMENT

This work is supported by Yildiz Technical University Scientific Research Coordination under project number 2016-04-03-YL03.

## REFERENCES

[1] J. Galbally, and R. Satta, "Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models", IET Biometrics,2015.

[2] C. Miyoung, Y. Jeong, "Face recognition performance comparison between fake faces and live faces", Soft Computing, 2016.

[3] J. Määttä, A. Hadid, M. Pietikäinen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis", *International Joint Conference on Biometrics*, 2011, pp.1-7.

[4] K. W. Bowyer, K. Chang, and P. Flynn, "A survey of approaches and challenges in 3D and multi-modal 3DC2D face recognition" in *Comput. Vis. Image Understand.,* vol. 101, no. 1, pp. 1-15, 2006.

[5] S. G. Pan, Z. Wu, and L. Sun. "Liveness detection for face recognition". *Recent Advances in Face Recognition*, Chapter 9. IN-TECH, 2008

[6] K. Nixon, V. Aimale, and R. Rowe. *Spoof detection schemes, Handbook of Biometrics*, pp. 403–4239, 2008.

[7] A. Hadid, "Face Biometrics under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues and Research Directions", *CVPR 2014*, 2014, pp. 113-118.

[8] J. Galbally, S. Marcel, J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition", *IEEE Access*, 2015, pp. 1530-1552

[9] K. Kollreider, H. Fronthaler, J. Bigun, "Verifying liveness by multiple experts in face biometrics". *Computer Vision and Pattern Recognition Workshops, CVPRW 2008*, IEEE, 2008

[10] S.G. Pan, L.Z. Wu, S. Lao, "Blinking Based Live Face Detection Using Conditional Random Fields*", ICB 2007*, *Springer*, pp. 252–260, 2007.

[11] K. Kollreider, H. Fronthaler, M. Faraj, J. Bigun, "Real time face detection and motion analysis with application in liveness assessment". *IEEE Trans. Infor. Forensics and Security, 2(part 2)*, pp. 548–558, 2007.

[12] G. Chetty, "Robust audio visual biometric person authentication with liveness verification". *Intel Multimedia Analysis for Security Appl*., pp. 59–78, 2010.

[13] S. M. Hatture, P. R. Karchi, "Prevention of spoof attack in biometric system using liveness detection", *Int. J. Latest Trends Eng. Tech*., *Special Issue-IDEAS*, pp. 42–49, 2013.

[14] C. Kant, N. Sharma, "Fake face recognition using fusion of thermal imaging and skin elasticity". *IJCSCIJ, 4(1),* pp. 65 –72, 2013.

[15] A. Lagorio, M. Tistarelli, M. Cadoni, C. Fookes, B. Clinton and S. Sridha, "Liveness detection based on 3D face shape analysis", *Proceedings of the IEEE International Workshop on Biometrics and Forensics (IWBF),* pp. 1–4, 2013

[16] B. D. Lucas and T. Kanade. "An Iterative Image Registration Technique with an Application to Stereo Vision". *International Joint Conference on Artificial Intelligence,* pp. 674–679, 1981.

[17] C. Tomasi and T. Kanade. "Detection and Tracking of Point Features". *Carnegie Mellon University Technical Report CMU-CS-91-132*, April 1991.

[18] J. Shi and C. Tomasi. "Good Features to Track". *IEEE Conference on Computer Vision and Pattern Recognition*, pages 593–600, 1994.

[19] Tomasi, Carlo, and Takeo Kanade. "Detection and tracking of point features." *Pittsburgh: School of Computer Science, Carnegie Mellon Univ.,* 1991.

[20] A. Datta, M. Datta, P. K. Banerjee, "Face Detection and Recognition: Theory and Practice",CRC Press, 2015

## APPENDIX A

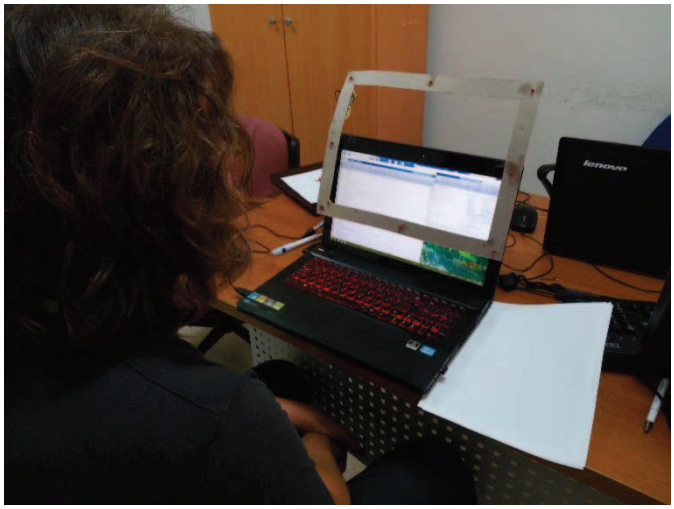

Figure 7. Test system.

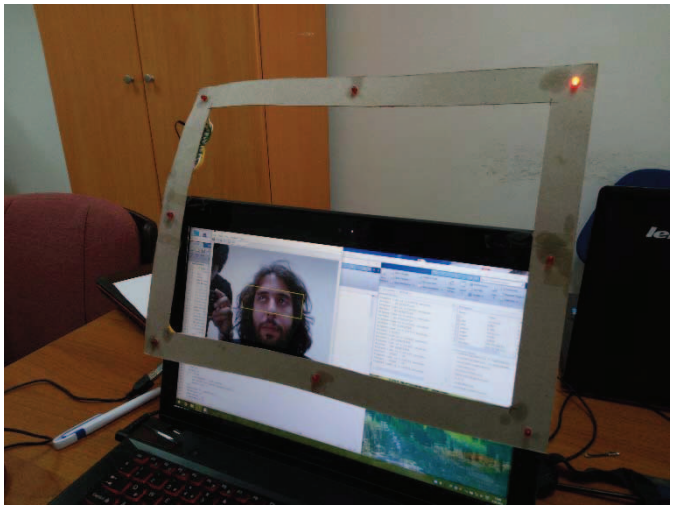

Figure 8. Right-up LED activated.

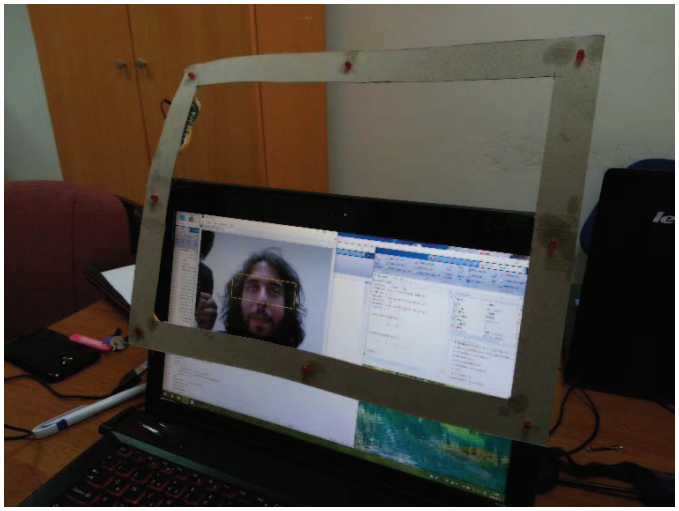

Figure 9. Test concluded successfully

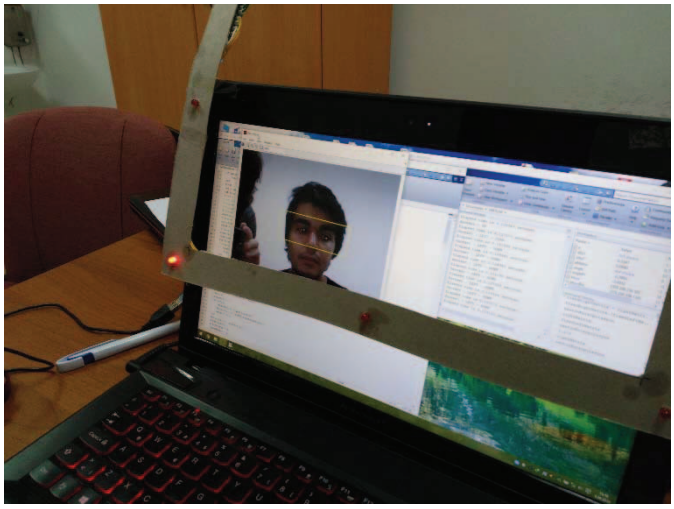

Figure 10. Left-down LED activated.

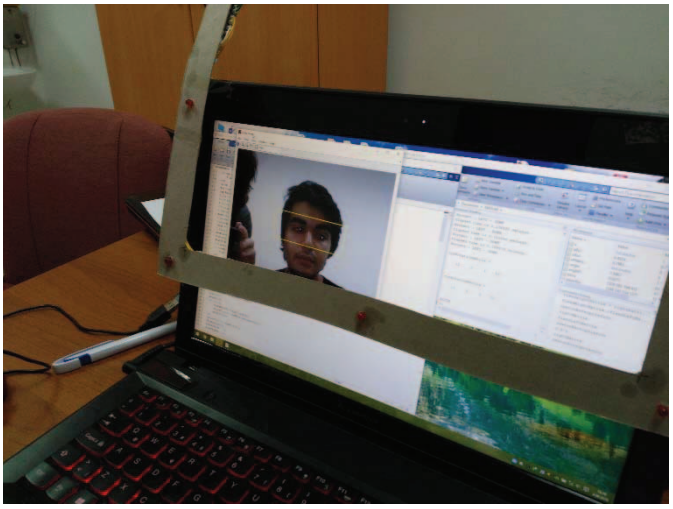

Figure 11. Test concluded successfully