AN IMPROVED METHODOLOGY FOR FRAUD DETECTION IN FACE RECOGNITION SYSTEMS

[1]TUGAY BOZIK, [2]NIHAN KAHRAMAN

[1,2]Yildiz Technical University, Electronics and Communication Eng. Dept.,Istanbul, Turkey
E-mail: [1]tugaybozik@gmail.com, [2]nicoskun@yildiz.edu.tr

Abstract - In this study, a method has been developed in response to the tricking movement which is a problem encountered in biometric systems. A method for more reliable applications has been developed by performing liveness analysis in face recognition systems. A security measure has been taken by following the movements performed during normal operations without understanding that the users are being followed. As an image processing library, the Dlib library, an open source library with machine learning, deep learning and computer vision algorithms, has been used. This library contains a detector which can find faces in an image. With this detector, we can predict the face area of the person standing in front of the camera. Then, from the face area obtained, we obtain two eye regions. The iris area in the eye is determined by moving iris kernel matrix over the eye images. After determining iris, the middle point is found and the eye is monitored. Users can watch the manuscripts by reading dynamically changing texts on the screen in a certain time without notice to the iris movements. As a result of all these results, liveness decisions are made by making comparisons according to the determined threshold values. This algorithm has been tested in volunteers. The volunteers selected to take into consideration the various situations are composed of both young and old individuals. As a result, the algorithm was tested on the volunteers and it can give liveness decision correctly and the success rate was 97%.

Keywords - Biometrics, Spoofing, Liveness Detection, Dlib, Facial Landmark

I. INTRODUCTION

Biometric recognition systems; Instead of passwords, cards or keys, face recognition, fingerprint, such as physical and behavioral features are used to identify the identity [1]. Biometric access systems according to card access systems are more preferred today because of their more secure and practical use. As an example of these practical biometric systems, it is possible to say iris recognition, fingerprint and face recognition systems.

Today, the issue of security plays an important role in the field of trade. Due to forgetfulness, we can say that security systems with card or key security create a security gap today [2]. For this reason, a more secure system has been entered into the search. This is more secure and practical biometric access control systems. Biometric systems that work with a person's physical or behavioral features minimize the security weakness and make the card, key etc. such as the load of vehicles can save us. However, the fragility of biometric authentication systems against spoofing attacks is now widely accepted. Such methods of fooling biometric systems are often referred to as spoofing attacks. A spoofing attack occurs when a fraud tries to mask as a real user by falsifying biometric data and thereby gaining legitimate access. A variety of viability detection methods have been proposed in the presence of a live human or an artificial copy in front of the biometric sensor. However, the problem cannot be solved due to the high level of difficulty in identifying effective features with low calculation costs to detect counterfeit attacks [3]. Face recognition is biometry easy in terms of spoofing, because data can be easily collected and it is not complicated to take pictures from online social media profiles. In addition, technical skills are not required for a spoofing attack, and even some attacks can be carried out by ordinary people [4].

In general, there are three ways to deceive a facial recognition system; to create a video of defined people, to take photographs or to create masks of current users. [5]

Liveness analysis is one of the most basic measures against attacks against facial recognition systems. The aim is to feel the signs of physiological life such as blinking, changes in facial expressions and mouth movements. Another method against anti-spoofing attacks consists of combining facial recognition with other biometric data such as walking and speaking. Some schemes in [6-8] have short researches against photo anti-spoofing attacks. Pan et al. [10] suggested an anti-spoofing method for blinking, while Kollreider et al. [9] presented an optical flow-based method for observing the movement of face images. Disadvantages of these methods can be seen when using a video or by simply shaking the camera. There are also databases and studies that identify liveness based on mouth movement [11-14], head movement or shape [15] for video attacks in the literature. Another method against anti-spoofing attacks is eye position tracking with controlling the LED direction [16].

In this study, a measure was developed in order to deceive the facial recognition systems by following the iris direction. In this study, simple solutions have been developed by using simple hardware. First, the

face area of the image is detected and then the eye region is located. The iris distinguishes the iris from the eye area and begins the follow-up. After confirming that the iris area has been captured several times, the user is expected to read them at different times in various parts of the screen. As soon as the user passes through the camera, iris movements are followed without being noticed. Several times the screen is written in different places. If the position information of the user's iris movements corresponds to the location of the post, the decision is made here. Also, this study has been tried by taking video and photos from mobile phone. The proposed algorithm and hardware are presented in Section 2. The rest of the study, the test results and the result are explained in Section 3.

II. PROPOSED ALGORITHM

For the systems that provide biometric authentication and access to the liveness analysis and the decision of the algorithm have 6 important steps.

- Face detection from the live camera image
- Removal of eye areas from detected face
- Finding the iris's coordinates to find the direction in which the person is looking
- Ensuring that the screen writings to be used in the decision of liveness can be released dynamically
- To make a direction verification by comparing the text on the screen with the iris coordinate
- Deciding the liveness if the direction is correct

Block diagram of proposed algorithm is given in Figure 1.

2.1 Face Detection

This step uses the Dlib library to mark the face area from the live camera image. Since the Dlib library is an open source library, it is easy to access the functions in it [17]. The face detection is done by using the face-matched face-detector and the face-to-face template matching logic of this library which contains the majority of image processing algorithms. This algorithm uses HoG (histogram of gradient and SVM (Support Vector Machine) when detecting faces. In more detail, the HOG algorithm repeats on each pixel of a given image, controls every pixel around it, and directly controls the pixels around it. then it will be plotted on each pixel, then it is divided into 16x16 pixels, where it indicates how many gradients in each main direction is replaced by the strongest arrow in that square. Then, using many faces, we can train the SVM (Linear Support Vector Machine) model to detect faces in an image.

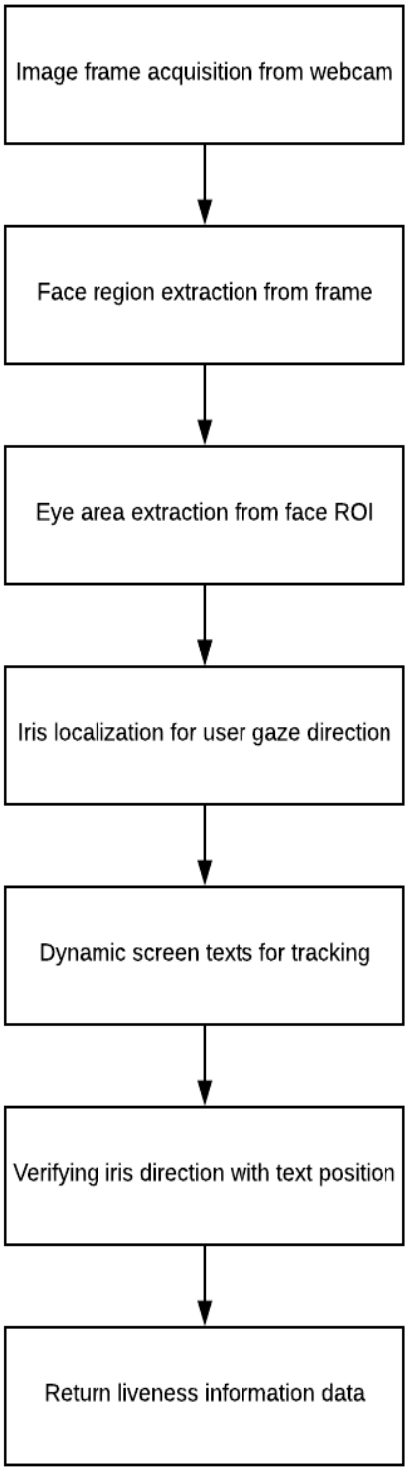

Figure 1:Block diagram of proposed algorithm

In this article we have used a pre-trained detector for the facial region.

2.2 Detection of The Eye Area

The face detector, which is located in the Dlib library, identifies a 68 percent point and returns the coordinates over these points [18].

For example; Parts of the face such as eyes, eyebrows, nose, jaw line, mouth can be easily found with this face detector. At the same time, face alignment, face change, eye blinking detection can be done in such operations.

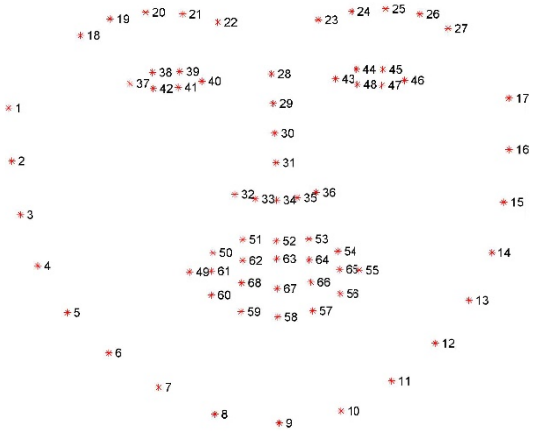

Figure 2: Facial Landmark 68 Markup

Each section is represented by specific points as can be seen on the Figure 2.
As can be seen here, there are different coordinates in two eyes. According to the desired application, a unilateral eye may be present or the two eyes can be removed and processed from the face picture at the same time.

2.3 Finding Iris Coordinates

It is passed through image processing filters with morphological processes to further clarify, enlarge and thin the features present on the image. We can easily find these morphological operations in the open source OpenCV image processing library [19]. Some morphological processes in the eye region found in the previous step are made and the iris is found in the eye frame.
First, a bilateral (two-sided) filter is applied in the eye image. Bilateral filter is a non-linear, edge protector and noise reduction softening filter for images. It modifies the density of each pixel with the mean density values that it calculates from nearby pixels. After this process, erosion process is performed. This operator applies an etching on the image. Erosion erodes the pixels in the specified area according to the parameters, and the distorted image, which is called noisy, is cleared from noise. All these events are mathematically defined and performed on arrays. After this, the threshold value is compared and the binary values of the pixels are found.The iris region is then estimated by finding contours within the eye frame passing through these processes.

2.4 Dynamically Output Screen Posts

In order to make a decision on liveness, users are displayed in 3 different areas on the screen to use in direction verification. This is done with the random function of the numpy mathematical library in Python. By learning the dimensions of the screen, we divide the x coordinate by 3 in a constant y coordinate. Within these coordinate regions that are divided, it is dynamically changed to see if users are looking at the right area. Thus, if direction verification is true, liveness decision is given.

2.5 Performing Direction Verification

After viewing the screen in the previous step, users' direction of view is determined. First of all, we know that the area in which the writings are displayed in different areas is checked for the iris movements.
A horizontal ratio is obtained by the ratio of the center of the X coordinate of the eyes in the eye frames. This rate is between 0 and 1. If the horizontal ratio is 0, the whole eye is looking to the right. If it is 0,5, the eye is looking at the midpoint.
On the screen, the coordinates of the written texts are compared and the direction of the direction obtained from the horizontal ratios of the eyes are compared and direction is confirmed. If the two direction information matches, the liveness information is returned to the system, if the direction information does not match after a certain number of attempts, the attack information is returned to the system.



Figure 3: Left Side Text and Verifying



Figure 4:Right Side Text and Verifying

III. RESULTS & CONCLUSIONS

The reliability of the system has been increased by using liveness analysis to prevent false access to biometric systems. This proposed algorithm can make existing old biometric systems more secure by modifying the software. In recent studies, the presence of face detection with the Dlib image processing library, which is quite remarkable, is

acceptable. However, it is possible to obtain more stable and precise results by training these algorithms with SVM algorithms. This algorithm has been tested on the volunteers. The entire algorithm which has been tested on volunteers the success rate of returning the live or fake information to biometric systems is 95%. In addition, the proposed algorithm was tested by putting videos and photos from mobile phones against the camera. In these trials, the iris could not find their centers and they showed that these entries were false. Further work will be to develop a more stable, facial region finding algorithm and a more stable iris center approach algorithm without being affected by the face. The presence of a more stable face and iris center will result in safer systems.

REFERENCES

[1] Jain, Anil K., Patrick Flynn, and Arun A. Ross, eds. Handbook of biometrics. Springer Science & Business Media, 2007.

[2] Jain, Anil K., Arun Ross, and SalilPrabhakar. "An introduction to biometric recognition."IEEE Transactions on circuits and systems for video technology 14.1 (2004).

[3] Akhtar, Zahid, Christian Michelon, and Gian Luca Foresti. "Liveness detection for biometric authentication in mobile applications."2014 International Carnahan Conference on Security Technology (ICCST).IEEE, 2014.

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

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

[6] S. G. Pan, Z. Wu, and L. Sun. "Liveness detection for face recognition". In K. Delac, M. Grgic, and M. S. Bartlett, editors, Recent Advances in Face Recognition, Chapter 9. IN-TECH, (2008)

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

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

[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] 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).

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

[13] 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).

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

[15] 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] Killioğlu, M., M. Taşkiran, and N. Kahraman. "Anti-spoofing in face recognition with liveness detection using pupil tracking."2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI).IEEE, 2017.

[17] King, Davis E. "Dlib-ml: A machine learning toolkit." Journal of Machine Learning Research 10.Jul (2009): 1755-1758.

[18] Amos, Brandon, BartoszLudwiczuk, and MahadevSatyanarayanan. "Openface: A general-purpose face recognition library with mobile applications." CMU School of Computer Science 6 (2016).

[19] Bradski, Gary, and Adrian Kaehler. Learning OpenCV: Computer vision with the OpenCV library." O'Reilly Media, Inc.", 2008.

★★★