Bilge International Journal of Science and Technology Research

Web : http://dergipark.gov.tr/bilgesci - **E-mail :** kutbilgescience@gmail.com

ISSN: 2587-0742
e-ISSN: 2587-1749
1(Special Issue), 1-5, 2017

Authentication with Iris Recognition Based on A 3-Tier Security Analysis Approach

Y. Sandal[1*], H. Kutucu[2]

Abstract: Audit controls are made using the tools such as ID, magnetic card, password, pin code to enable people to access to areas requiring access permission. This situation with increasing the number of security measures forces people to remember more than one password. In addition, it is becoming compulsory for a person to have more than one type of card in order to be able to identify himself / herself. Increasingly reliable and practical detachment of such measures has increased the interest of researchers in biometrics systems, which is the recognition method of self-identification by using their own structural features. The aim in this project is to authenticate with one of these biometric systems, iris recognition. Iris screening is one of the most reliable biometric scans. There is no need for physical contact between the user and the scanner. Being able to use even with glasses, easy integration into systems and being one of the most reliable designs of iris has been the main factors in choosing iris definition. In the project done, the security level is aimed to be authenticated in a short time and correct match with the algorithm produced based on the increased three layer security analysis. These layers in the project; eye color in the first layer, ratio of the area of the iris to the area of the eyeball in the second layer, and tissue analysis in the third layer. The difference between this project and other work that has been worked on before is that the authentication process is performed with a different algorithm approach by increasing the number of security layers. Thus, it is aimed to reach reality in a safer and shorter time. At this time, only studies of iris texture have been carried out in the examination of iris. Other factors have not been evaluated in studies. In this study, eye color and the ratio of the iris area to the eyeball are examined by adding the account. After these factors are correctly matched, iris tissue is examined. The project has two databases, one to record real-time data, and the other to contain data from the CASIA database. The real-time data base is created with the images we have obtained from different people with the piece of hardware we have developed. By using different image processing algorithms, images in these databases are processed and an iris code is created to see the key task. Snapshots taken from the live eye are compared through the created iris code to the database data to find out if there is a match. It is determined that the analysis of the three security layers is done in a short time and with high success rate. The version_01 of the CASIA database is used in the study. In this database, 50 images of eyes taken from different angles at different times were worked on. In the real time database there are 25 images. The success rates of both databases are calculated separately. The obligation of individuals must carry lots of card with them and memorizing many password in order to introduce themselves will be avoid with this work. It will provide savings time and financial gains to institutions and individuals. There is not much study about identification of iris in the country, and necessary software in this area is generally supplied from abroad. With this work, it is aimed to increase the interest of researchers in this field and to eliminate this deficiency in the country..

Keywords: Iris Recognition, Biometric Security.

1. Introduction

In recent years, especially in the last few years, the rapid development of technology in the field of access to information has increased the need for many field security. The need for individual secure access in developed applications brought with it the problem of smart person identification. One

[1]Karabük University, Engineering Faculty, Karabük, Turkey
*Corresponding author (İletişim yazarı):yseminsandal@karabuk.edu.tr

Citation (Atıf): Sandal, Y., Kutucu, H. (2017). Authentication with Iris Recognition Based On a 3-Tıer Security Analysis Approach. Bilge International Journal of Science and Technology Research, 1 (Special Issue): 1-5.

common method for person identification, which is a specific image, is now inadequate and unreliable in today's conditions. Moreover, these methods do not have much practicality. Many factors, such as loss of keys and ID cards, forgetting passwords, cause problems in using these methods. In order to overcome these problems, researchers have exploited the behavioral and physical characteristics of individuals to find new ways to identify people (Gürkan, 2015). As a result of these investigations, reliable and more practical methods called biometric measurements have been obtained.

Biometric recognition is a reliable method used to determine who is allowed to perform an action and who is not. The basis of the biometric definition is based on defining the behavioral and physical characteristics that are different for each person. These behavioral and physical properties that can be used as biometric measurements include the fragrance components of the human body, temperature distribution, facial features, iris and retina structures, palm and fingerprints, hand geometry, individual voice, for example (Tekyıldız et al., 2015). Despite the fact that voice recognition and fingerprinting are among the most popular among these biometric measurements over the last few years, changing demands have accelerated the work on iris recognition.

Iris is the name given to the colored region in the circle inside the eye. The iris recognition system was developed based on the fact that the iris did not change during human life. More than one reference point can be used in this system. For example, in a biometric system that uses fingerprint separation for absolute success, there are about 60 to 70 comparison points, while iris recognition has about 200 reference points for this comparison (Jain et al., 2004).

The iris recognition system is now available in many areas. First of all, outposts are preferred in areas requiring strict security measures such as airports. In addition, organizations, companies and universities benefit from the iris recognition system for students and staff follow-up (Abatea et al., 2017).

Iris is among the most preferred among other biometric recognition systems because it is one of the most reliable because it has its own characteristics and is not easily affected by external factors (Akçay and Çetinkaya, 2011). It is aimed to reduce the need for information such as PIN number and password, which are highly likely to be shared with the Iris recognition system and the risk of being forgotten.

In the case of biometric authentication, the user uses his / her own physiological or behavioral characteristics to access the system. When a person wishes to access a system that works in this way, the system takes the appropriate biometric data (voice, iris, fingerprint, retina etc.) of the individual (Kamal et al., 2015). This data is taken from the same individual and matched with the biometric data previously added to the database. If the matching result is positive, the identity of the individual is verified.

This study refers to the definition of iris, one of these biometric based security systems. Iris recognition is also one of the methods of digital identification. Iris recognition is a system based on studying by scanning iris with high resolution cameras and comparing it at the time of reading.

In this study, we present a three layered security level enhanced tissue analysis based method for person authentication with iris identification. However, it is aimed to contribute to these areas by providing benefits to the health fields such as entry and exit of the personnel, need for strict security control such as country borders, banks, and entrance to the operating theater.

This paper is organized as the following. Section 2 describes how the iris boundaries are detected and the blob counter and haugman circle algorithms used when determining these boundaries. In section 3, the security layers which is three are analyzed.. In the last section we present the conclusions

2. Detection of Iris Boundaries

Up to this day, studies on iris recognition have been made in different approaches such as phase information base, zero crossing basis and tissue analysis base for the analysis of iris (Yuanning et al, 2015). In this project, tissue analysis based on these approaches is used for iris recognition.

In this section, the aim is to determine the boundaries of the iris. The iris has two boundaries that must be determined, an outer boundary and an inner boundary that defines the middle pupil. For this, edge detection, filtering and segmentation

algorithms of the image processor are used. As a result of this operation, unnecessary fields in the image will be cleared and ready iris is obtained. The output the result of this operation illustrated in Figure 1.

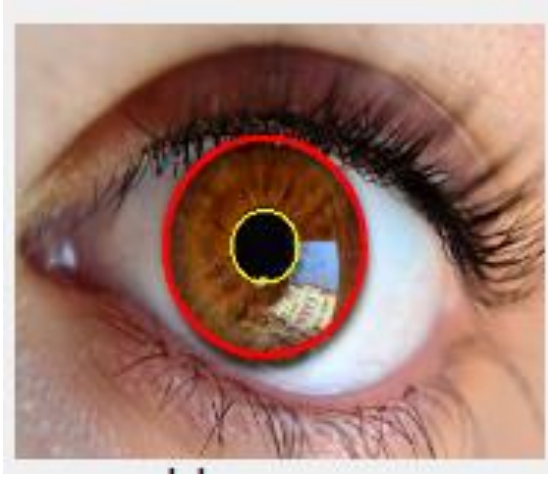

Figure 1. Detection of iris boundaries

Before determining the outer border of the iris, it is necessary to determine the inner border which forming the pupil. The image is passed through gamma correct and gaussian filters to remove noise from the original image. After the noise-free image is subjected to inverse processing, gray conversion is performed. The threshold is set by specifying a threshold value on the image that has been Gray transformed. The objects on the image are then detected after thresholding.

2.1. Blob counter

The blob counter is an algorithm that can find the objects in the image sent to it (Çakır et al., 2013.) After the threshold is set in the project, the image is sent to the blob counter algorithm to determine the objects in the image. As a result of the experiments, it is determined that the pupil has a value within the range of 10 to 50 pixels, so the blob counter is limited to these values to prevent unnecessary objects from being moved backwards. Figure 2 shows the view of the objects obtained from the image that comes to it as a result of the execution of this algorithm.

Figure 2. Objects found with blob counter

2.2. Haugman cırcle

The Haugman circle is an algorithm that finds objects that are similar to the circle sent to it (Erişti, 2010). We only need objects that look like circle because we try to find the pupil in our work**.** With this algorithm, the inner boundary of iris in other words the pupil is found. This algorithm is also used to find the outer boundary of the iris. If the pupil is the smallest, the diameter of the iris is 2.5 times the radius of the pupil. Starting from 2.5 times distance from the center of the pupil, the circle search is performed again with the haugman circle. Each time a search is made until a circle is found by reducing by 10%. As a result of these operations, the inner and outer boundaries of the iris are determined. The pupil with the haugman circle is shown in figure 3. The iris with boundaries is enclosed in a rectangular frame and cropped from the source image.

Figure 3. Pupil with haugman circle

3. Analysis of Security Layers

This study proposes a method based on a three-tiered security analysis with enhanced level of security for people recognition with the help of iris. Unlike other studies, this study carries out the identification of persons by examining factors such as eye color and iris diameter and eye diameter as well as iris texture. Eye color in the first layer, ratio of the diameter of the iris to the diameter of the eye blade in the second layer, and tissue analysis in the third layer is implemented. Once the boundaries of the iris are detected, this image is cropped from the original image to obtain an image that is only iris.

3.1. Analysis of first security layer

Once iris boundaries are detected, layers will be analyzed. The first layer of the project is color analysis. Colors are expressed as values between 0 and 255 The heat map is used for color analysis. The nearest value pixels are grouped and the standard deviation of these groups is taken and a value is obtained for the image The values of the color tone in the eye is determined and values obtained below and above this value is accepted by adding a certain tolerance value to the obtained value.

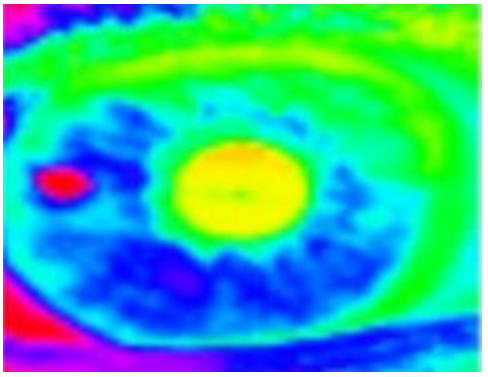

Figure 4. Analysis of iris color

3.2. Analysis of second security layer

In this layer, the area of the iris boundaries and the area of the eyeball are compared to obtain a value that is different for each eye. The presence of the iris domain is detected in the previous section. To find the area of eyeball the haar cascade eye class of the haar cascade library is used. Haar cascade is an algorithm that trains cascade objects and allows them to be found in the given image. In the image given in the study, eye scanning is done with haar cascade. The eye that is found is contained in the rectangle. Lastly, the ratio of these areas to each other is found. This ratio is shown in figure 5.

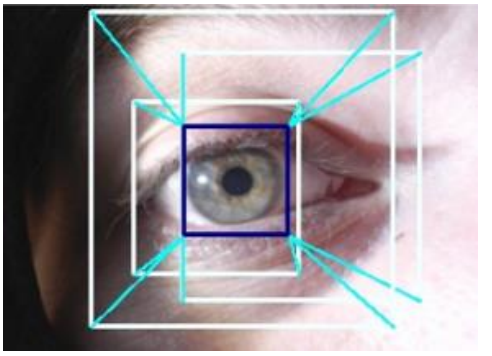

Figure 5. Analysis of proportion of areas

3.3. Analysis of third security layer

The last layer of analysis is the analysis of Layer 3 texture. This layer consists of the steps of normalization and feature extraction to determine the structure of the iris texture. In order to overcome the adverse effects of the images, all iris images must be expressed in equivalent dimensions and therefore iris normalization should be done. The extraction of the is performed using the normalized iris pattern.

Figure 6. Calculated iris code

Creation of Iris code: After the examination on 3 layers, the code to generate the key task is generated from the iris image obtained with the software produced. This allows the code generated database to perform a quick comparison with other codes. The code generated during these operations is encrypted.

Identification: In the test phase, an iris image taken with the camera from the live eye is obtained from the data obtained after passing through all the steps described above, and the identity of the iris is determined. The iris code generated from the live eye snapshot soon be able to map from the database containing another previously registered iris code**.** This comparison is performed by the hamming distance algorithm.

The algorithms generated in the working phase of this project are written in Emgu Cv platform which is an image processing library adapted to OpenCV C EmguCV is a library with image processing functions in net-based programming languages (Yang, et al., 2017). My Sql is also used for the database created from the images taken with the camera.

4. Conclusion

Detecting the iris in a noisy image is difficult process. So, first of all noise is removed by using gaussian and gamma correct algorithms from the original image. The inner and outer boundaries of the iris are determined with the blob counter and the haugman circle algorithms. In the first layer, color analysis is done using the heat map. In the second layer, the ratio of the iris are to eyeball are is calculated. Then, in the last layer, the iris tissue analysis is examined and the iris code is generated.

The proposed algorithm brought a different perspective to the recognition of iris. Parameters that are not previously considered in the recognition of iris are evaluated in this study and a study that yielded a fast match with high accuracy is obtained. The study consists of two databases. One of these contains data from the CASIA database. The other consists of the data obtained in real time. The study is tested on 50 images in the CASIA database and 88.7% success rate is achieved. In the real-time part, 25 people are tested and 84.6% success rate is achieved.

Acknowledgements

This work was supported by Research Fund of the Karabuk University. Project Number: KBÜBAP-17-YL-246. We would like to thank the Karabük University BAP Coordinator for their support.

References

Abate, A.F., Barra, S., Gallo, L., Narducci, F. (2017). Kurtosis and skewness at pixel level as input for SOM networks to iris recognition on mobile devices. Pattern Recognition Letters, 91, 37-43.

Akçay, M., Çetinkaya, H.H. (2011). Kampüslerde Uygulanan Yeni Biyometrik Sistemler, Akademik Bilişim Konferansları, 11, Malatya-Türkiye.

Çakır, A., Volkan, A., Akbulut, F.T. (2013). Iris Tanıma Sistemleri ve Uygulama Alanları. 5, Akademik Bilişim Konferansları, 13, Antalya-Türkiye.

Erişti, E. (2010). Görüntü İşlemede Yeni Bir Soluk, OPENCV 223-224 Akademik Bilişim, 10, Muğla-Türkiye.

Gorkan, G., Akan, A. (2005). A new iris recognition method based on texture analysis. In Signal Processing and Communications Applications Conference, 2005. Proceedings of the IEEE 13th (pp. 195-198). IEEE.

Jain, A. K., Ross, A., Prabhakar. S. (2004). An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, 14(1):4-20.

Kamal, H., Ujwalla, G., Yogesh, G. (2015). Neural Network Approach to Iris Recognition in Noisy Environment, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.

Tekyıldız, A., Güllü, M. K., Urhan, O. (2015). Irıs Recognıtıon System Based On Fast Irıs Localızatıon And Phase Correlatıon Mathchıng, İşaret Ve Görüntü İşleme Lab. (Kulis), 4-5.

Yang, H., Konstantinos, S., Gareth, H. (2017). A novel iris weight map method for less constrained iris recognition based on bit stability and discriminability, February, Pages 168–180

Yuanning, L., Fei, H., Xiaodong, Z., Zhen, L., Ying, C. (2015). The Improved Characteristics of Bionic Gabor Representations by Combining with SIFT Key-points for Iris Recognition. Journal of Bionic Engineering 12, 504–517.