AJIT-e: Bilişim Teknolojileri Online Dergisi
2020 Winter/Kış – Cilt/Vol: 11 - Sayı/Num: 40
DOI: 10.5824/ajite.2020.01.005.x

Date Received: 20.02.2020
Publishing Date: 3.05.2020

Dostroajan: Facial Recognition Based System Input Control Agent

Faruk AYATA, *Van Yüzüncü Yıl Üniversitesi, Başkale Meslek Yüksek Okulu, Öğr.Gör., farukayata@yyu.edu.tr, ORCID: 0000-0003-2403-3192*

Hayati ÇAVUŞ, *Van Yüzüncü Yıl Üniversitesi, Eğitim Fakültesi, Doç. Dr., hayatiicavus@gmail.com, ORCID: 0000-0001-5602-5221*

Mevlüt İNAN, *Van Yüzüncü Yıl Üniversitesi, Başkale Meslek Yüksek Okulu, Öğr.Gör., mevlutinan@yyu.edu.tr, ORCID: 0000-0002-9840-8404*

Ebubekir SEYYARER, *Van Yüzüncü Yıl Üniversitesi, Gevaş Meslek Yüksek Okulu, Öğr.Gör., eseyyarer@yyu.edu.tr, ORCID: 0000-0002-8981-0266*

Emre BİÇEK, *Van Yüzüncü Yıl Üniversitesi, Enformatik Bölümü, Araş. Gör., bicekemre@gmail.com, ORCID: 0000-0001-6061-9372*

Erol KINA, *Van Yüzüncü Yıl Üniversitesi, Özalp Meslek Yüksek Okulu, Öğr.Gör., erolkina@yyu.edu.tr, ORCID: 0000-0002-7785-646X*

ABSTRACT

Speed, time and safety are of great importance in many operations conducted today. There are standards such as ISO 27001, ITIL (Information Technologies Infrastructure Library), COBIT (Control Objectives for Information and Related Technology), which are globally recognized not only regarding access to information and the use of information but also information retention. Governmental institutions and many large companies use fingerprint, card reading, iris recognition and facial recognition systems in entrances and exits, regarding the protection of information.

The facial recognition system application developed within the scope of this study performs the facial recognition by using Convolutional Neural Networks (CNN), which is one of the deep learning algorithms and restricts the use of your personal computer by people you do not know. In addition to this restriction, it takes a photo of the person who wants to use your personal computer and sends this photo to the mobile phone of the owner of the computer, who was previously defined in the system and informs him/her.

Regarding the testing of the face recognition system application FEI (Faculdade de Engenharia Industrial- Faculty of Industrial Engineering) facial database was used. In this facial database, there are 14 different poses of 200 people (one is neutral, one is smiling, one is not smiling, and the others are at different angles). Trials were made to access the system with a total of 2800 photographs and as a result of the trials, success was achieved with a ratio of 76.31% in the worst angle and light and a ratio of 99.15% in the best angle and light.

Keywords : ***Information Security, Deep Learning, Image Recognition, Security Agent***

Dostroajan: Yüz Tanıma Tabanlı Sistem Giriş Kontrol Ajanı

ÖZ

Günümüzde yapılan birçok işlemde hız, zaman ve güvenlik büyük önem taşımaktadır. Bilgiye erişimin ve bilginin kullanımının yanı sıra bilginin saklanması noktasında küresel çapta kabul görmüş ISO 27001, ITIL (Information Technologies Infrastructure Library – Bilgi Teknolojisi Altyapı Kütüphanesi), COBIT (Control Objectives for Information and Related Technology - Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri) gibi standartlar vardır. Devlet kurumları ve birçok büyük şirket bilginin korunması hususunda giriş-çıkışlarda ve bu kurumların sistem odalarına erişimde parmak izi, kart okutma, iris tanıma ve yüz tanıma sistemleri kullanmaktadır.

Bu çalışma kapsamında geliştirilen yüz tanıma sistemi uygulaması derin öğrenme algoritmalarından biri olan Evrişimsel Sinir Ağlarını (Convolutional Neural Networks - CNN) kullanarak, yüz tanıma işlemini gerçekleştirip, istenmeyen kişilerin kişisel bilgisayarı kullanmasını kısıtlamaktadır. Bu kısıtlamaya ek olarak kişisel bilgisayarları kullanmak isteyen kişinin fotoğrafını çekerek bu fotoğrafı sistemde daha önce tanımlanmış olan bilgisayar sahibinin cep telefonuna mesaj olarak gönderip bilgilendirme yapmaktadır.

Yüz tanıma sistemi uygulamasının testi için FEI (Faculdade de Engenharia Industrial - Endüstri Mühendisliği Fakültesi) yüz veritabanı kullanılmıştır. Bu yüz veri tabanında 200 kişinin (biri nötr, biri gülümseyen, biri gülümsemeyen ve diğerleri de farklı açılarda olan) 14 farklı pozu bulunmaktadır. Toplamda 2800 fotoğraf ile sisteme erişim için denemeler yapıldı ve denemeler sonucunda en kötü açı ve ışık değerinde %76,31 ve en iyi açı ve ışık değerinde de %99,15 başarı sağlanmıştır.

Anahtar Kelimeler **:** ***Bilgi Güvenliği, Derin Öğrenme, Görüntü Tanıma, Güvenlik Ajan***

1. INTRODUCTION

Today, when the data increase rapidly, the security of the systems where these data are stored is very important. Many applications have been developed to prevent unauthorized access to systems and are still being developed. Developing technologies use different methods such as password usage, fingerprint reader, voice recognition, iris recognition and facial recognition regarding the protection of data. Along with the developments in artificial intelligence, many solutions (such as endpoint security, network security, password management, log management, e-mail security, system access controls) are offered in the field of information security. Advances in image processing, which is a common ground of the fields of artificial intelligence and information security bring along innovative solutions. One of these solutions is that the person can be identified based on his/her image. This process, known as facial recognition, is an important property of supervisory systems and computer-human interactive systems (Taşova, 2011, Kaplan, 2018).

Facial recognition is based on the ability to re-identify a person. The ability to re-identify a person depends on the working of many complex layers within a certain hierarchy. This identification process is quite complicated and difficult for reasons such as photographs taken

DOI: 10.5824/ajite.2020.01.005.x

at various times using various cameras, ambient light and differences in perspective. Two separate images of the same person may look quite different for the reasons mentioned above or the images of two different people may look very similar (Ahmed et al., 2015).

The redefinition of the image performed by classical artificial neural network modeling, the connections between the neurons and the layers and the learned parameters present great computational difficulties. At this point, convolutional neural networks come into play. In 2012, the deep learning model based on the evolutionary neural network was first presented by Krizhevski et al. in the ILSVRC'12 competition. They won the competition with a great percentage of identification accuracy with the work they performed. Since then, deep learning models based on convolutional neural networks have become more popular in the field of computer vision. The model fundamentally works on the basis of comparing two images and producing a similarity score as a result of this comparison or classification of the image.

In this study, facial recognition application was performed by using Convolutional Neural Networks, which is one of the deep learning algorithms based on image processing and an application was developed aimed at preventing unauthorized access to the systems. For the face recognition process to be performed, primarily, the images of the users authorized to use the system must be introduced to the system in advance. The image of the user attempting to access the system is captured by a camera connected to the system and matched with the previously recorded images. The user who succeeds in this matching process will be able to access the system. In case the pairing process fails, the image of the user attempting to enter the system is sent to the system authority by a text message. The application runs in the background of the system and does not show any signs of functioning while it is logged in. The application, which consumes a very small dimension (5.1 mb) of source in the memory, is activated as soon as the system is turned on.

2. Related Studies

There are many studies on facial recognition systems based on the re-identification of the person. Depending on the development of technology, it can be said that these studies continue increasingly.

In their study, Pala et al. (2018) compared the Haar Wavelet Artificial Neural Network model with the convolutional neural network model and proposed the Haar Wavelet Transform based neural network structure. In the study, where they used the MNIST data set, they found that the multilayered structure adopted in the design of the convolutional neural network increased the network depth and thus caused significant problems.

Erdem, M. E. and Topal, C. (2018), in their study, proposed the 2B patch warping based face pre-frontalization method, which has a simple but effective flow due to its low calculation cost. They found that "Face Fronting" technique increases the accuracy of face and motion recognition applications.

Kaplan, A. (2018), in his study, realized the determination of whether an image involves a face or not and the detection of the places of faces on the photograph by using image processing

techniques. He emphasized that the application he developed should work with high performance and speed as a real-time application.

Rashid, E. (2018), in his study, designed a personal security system with facial recognition using a Raspberry Pi-based camera system.

Zhang, Z. et al. (2018), in their study, proposed a new deep model called integration evolutionary neural network (ICNN) for the re-identification of the person in camera networks, in which they jointly learned universal and local characteristics. They evaluated the proposed ICNN in three large-scale databases. They obtained an accuracy of 92.13% in Market 1501, 61.4% in CUHK03 and 85.3% in Duke MTMC-re ID.

Sharma, R et al. (2019), in their study, proposed a new real-time face detection system that detects inclined, closed or differently illuminated faces. They proposed a system using Viola Jones and Modified Affin Transformation in order to overcome the problems of angle and light.

Chahar, H. And Nain, N. (2017) tried the studies on image and video based facial recognition in various data sets and the results of the study are shown in Table 1.

Table 1 Accuracy of different deep learning approaches for individual training on various image data sets (VIPeR, CUHK-01, CUHK-03, PRID, iLIDS,85etwo and Market-1501).

Authors/Year	**Evolution**	**VIPeR**	**CUHK-01**	**CUHK-03**	**PRID**	**iLIDS**	**Market-1501**
Yi [11]	CMC	28.23%	-	-	-	-	-
Li [12] (2014)	CMC	-	27.87%	20.65%	-	-	-
Wu [13] (2016)	CMC/mAP	-	71.14%	64.80%	-	-	37.21%
Xiao [14] (2016)	CMC	38.6%	66.6%	75.33%	64.0%	64.6%	
Chi-Su [15] (2016)	CMC/mAP	43.5%	-	-	22.6%	-	39.4%
Liu [16](2016)	CMC/mAP	-	81.04%	65.65%	-	-	48.24%
Varior [17](2016)	CMC/mAP	37.8%	-	68.1%	-	-	65.88%
Wang [18] (2016)	CMC	35.76%	71.80%	52.17%	-	-	-
Geng[19] (2016)	CMC/mAP	56.3%	-	85.4%	-	-	83.7%

Chahar, H. And Nain, N. (2017)

Yaman, A. U. & Samet, R. (2018) stated that the facial recognition systems used in their study could be overcome by displaying the image, video or three-dimensional artificial mask of the person concerned, and that such security weaknesses were aimed to be eliminated by affirming that the person is alive through the detection of his/her blink and mimics but the desired level of success could not be achieved and produce solutions to three-dimensional masks.

Sharma et al. (2016) conducted a CNN-based facial recognition using the dlib library. They performed the tests of the study based on the FAREC dataset and achieved 96% success.

Guo and Li (2016) used CNN for facial recognition in their study, but they used SVM (Support Vector Machine) as the classifier. They conducted the tests on the FERET dataset. As a result of the tests, they achieved a high recognition rate with less training time.

DOI: 10.5824/ajite.2020.01.005.x

Vinay et al. (2017) used F-CNN and G-CNN architectures in their face recognition application. They used the CMU, Grimace, Yale, Face 95 and FEI data sets to test the application and achieved an accuracy of 95%.

In the application developed by Cataline et al. (2017) for access to some special systems, facial recognition is performed in accordance with the 5sec video image taken from the camera and access is prevented if a second face, other than that of the person defined in the system is detected.

3. Data Set

FEI facial database was used for testing the system. This is a Brazilian face database containing a range of facial images taken at the FEI Artificial Intelligence Laboratory in Brazil between June 2005 and March 2006 by students and staff aged 19-40, choosing different images, hairstyles and accessories. In the FEI face database, there are a total of 2800 face images consisting of 14 different poses and light values of 200 people. All images were received rotating up to 180 degrees from the front in an upright position against a homogeneous background. Each of the subjects, which totally amount to 200 people have 14 different poses (one being neutral, one smiling, one not smiling, and the others at different angles) as shown in Figure 1. There is a change of approximately 10% between each exposure. The original size of each image is 640x480 pixels.

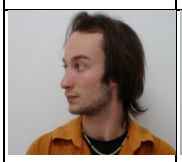
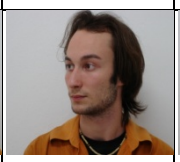
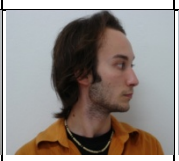
1.Pose	2. Pose	3. Pose	4. Pose	5. Pose	6. Pose	7. Pose
						
8. Pose	**9. Pose**	**10. Pose**	**11. Pose**	**12. Pose**	**13. Pose**	**14. Pose**
						

Figure 1. FEI face database.

4. Face Recognition Methods

Yan, Kriegman and Ahuja (2007) made a classification consisting of four main topics for face recognition methods. These are:

Method based upon knowledge

Knowledge-based method. There are certain set of rules and face detection is performed within the framework of the rules. It needs nose, mouth and eyes on the face for face detection. The

problem with this method is the creation of the appropriate set of rules. Whether the rules are detailed or general makes face recognition very difficult.

Feature-based method

This method detects the faces by removing the structural features of the face. These features may be light, head angle, facial tissue, skin color, etc. This method gave very good results in images containing more than one face.

Template-based method

It uses predefined or parameterized face templates for face detection. The human face can be divided into different definitions as nose, mouth, eyes and face circumference. The applicability of this method may be simple but insufficient for face detection.

Appearance-based method

It uses the learning set that includes various face patterns and makes face detection by learning human face models. It gives much better results than the other methods. It uses statistical analysis, machine learning, and deep learning techniques to detect face image. Appearance-based method uses the following methods for face recognition applications:

- Eigenface-Based
- Distribution-Based
- Neural-Networks
- Support Vector Machine
- Sparse Network of Winnows
- Naive Bayes Classifiers
- Hidden Markov Model
- Information Theoretical Approach
- Inductive Learning

5. Experimental Study

The facial recognition system application requires training regarding the images of the people who have access to the computer for establishing the control of whether the person who wishes to access the computer is among the people who have the right to access the computer. Therefore, the images of the people who were granted access to the folder specified as the first step should be discarded. In the absence of a previously captured image, the desired number of images can be recorded using the program provided below with the pseudo code and the interface (figure 2) to generate the test data.

Pseudo Code

İnput: Capture image from camera

DOI: 10.5824/ajite.2020.01.005.x

Output: Test image for dataset

1. test_folder /image dataset
2. Camera activated
3. While camera is open then
4. read key from keyboard
5. if key == 'q' then
6. test_folder= capture image and save
7. End if
8. Else if key== 'w' then
9. Close the camera
10. End else if
11. End while
12. Return test_folder

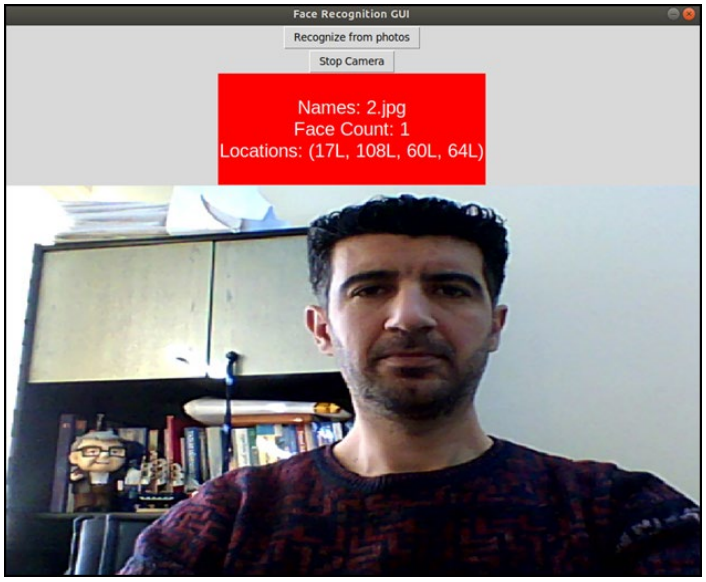


Figure 2. Training data creation program interface.

When logged on, the program starts running automatically and continues running in the background until the computer is shut down. The program uses a very small amount of the system resources.

The program, which starts to run when logged in, first takes a picture of the person using the computer and performs the identification process by applying face-recognition methods based on appearance on this image.

In this method, the techniques of statistical analysis, machine learning, and deep learning are used to detect face image. Face detection is performed on the image taken from the camera using Convolutional Neural Networks, which is one of the Deep Learning algorithms.

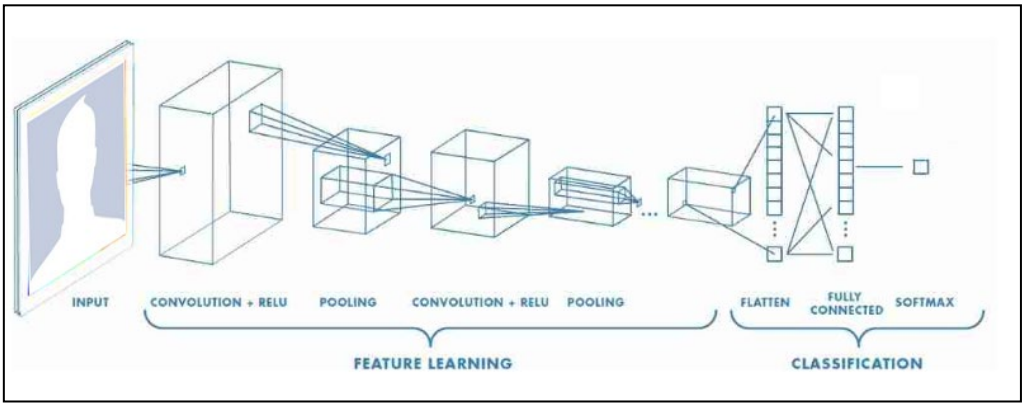


Figure 3. The logic of Convolutional Neural Network.

In the work of the Convolutional Neural Network, the image is fragmented. Each divided part is filtered. After the applied filter, the image shrinks. The pixels obtained after the reduction process are interpreted and the problem is solved (Cengil and Çınar, 2016).

As shown in Figure 3, the first few steps of the identification process consist of Convolution and Pooling layers. In the last stage, there is the Fully Connected layer and the Classification layer. In summary, this architecture consists of several trainable sections arranged one after the other. Finally, a final output is generated, and this output is used to be able to make comparison with the correct result. As a result of the comparison, an error occurs as much as the difference between the correct result and the final output. The back-propagation algorithm is used for this error to be transferred to all weights. Weights should be updated with each iteration to reduce the error (İnik and Ülker, 2017).

In the study, platform-independent Dlib library in C ++ programming language was used for face detection. The Dlib library is a library that has been developed since 2002, includes deep learning, machine learning and computer vision algorithms, and offers service to a wide audience through the C ++ and Python API.

DOI: 10.5824/ajite.2020.01.005.x

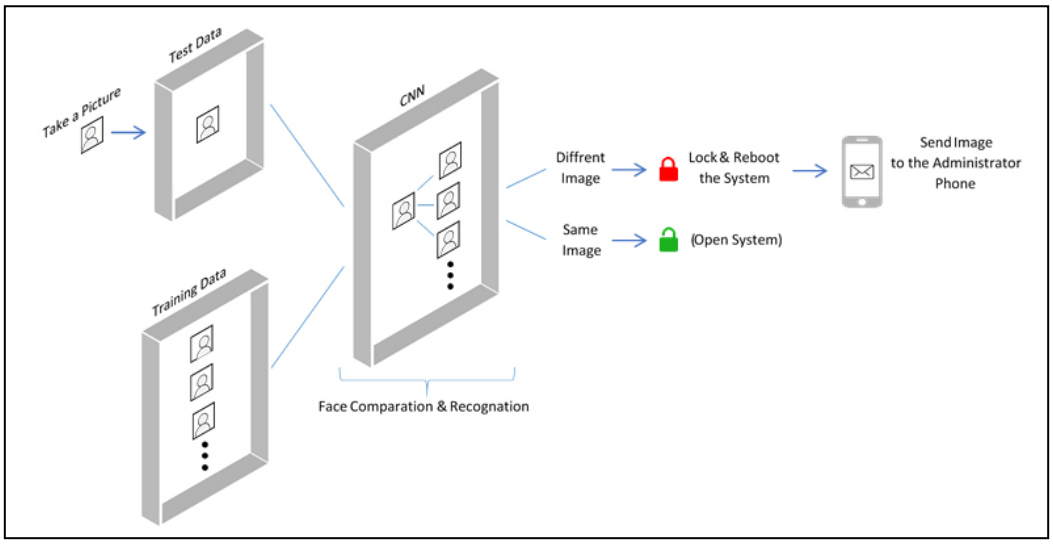


Figure 4. Block diagram of the developed system.

Figure 4 shows the block diagram of the system. Face detection, face recognition and face comparison operations are performed by using CNN structure of the image taken from the camera together with the images recorded in the system. The system is activated by the matching of people in the images; if there is no matching, the computer is restarted and informing is performed by sending the image of the person who wants to access the system to the mobile phone registered in the system.

Pseudo code

İnput: Capture image from camera

Output: Permission to system

```
I=[ ]  /test_folder
result = booleen
image= read image from camera
for j in ı do
    compare_value = image_compare(image, I)
    if compare_value == true  then
        result = true
        unlock system, break for
    end if
    else
        result = false
```

12. end else
13. end for
14. if result == false then
15. open ftp connection
16. save image to ftp server
17. send image to user via sms
18. shutdown system
19. end if

The pseudo code of the system developed above is seen. A snapshot of the person who wants to access the computer is taken and saved to the computer with a file name. Then, the image_compare function, the image of the person who wants to access the computer and the image of people who were previously recorded in the computer for testing the system and who have access to the system are analyzed using deep learning methods and comparison is made. If the result of the comparison is positive, the system is turned on, but if it is negative, the snapshot of the person who wants to access the computer is saved to the ftp server in the system, then the warning message information is sent to the specified mobile phone and finally the system is turned off. Figure 4 shows the message information sent to the mobile phone. By clicking on the link in the message, the photo of the unauthorized person is accessed.

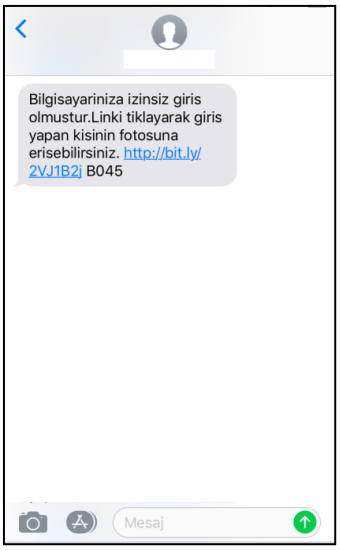


Figure 5. Intrusion system warning message information.

The program prepared was designed to run on Windows operating system. As shown in Figure 6, the program runs in the background of the computer and uses a very little amount of system resources.

DOI: 10.5824/ajite.2020.01.005.x

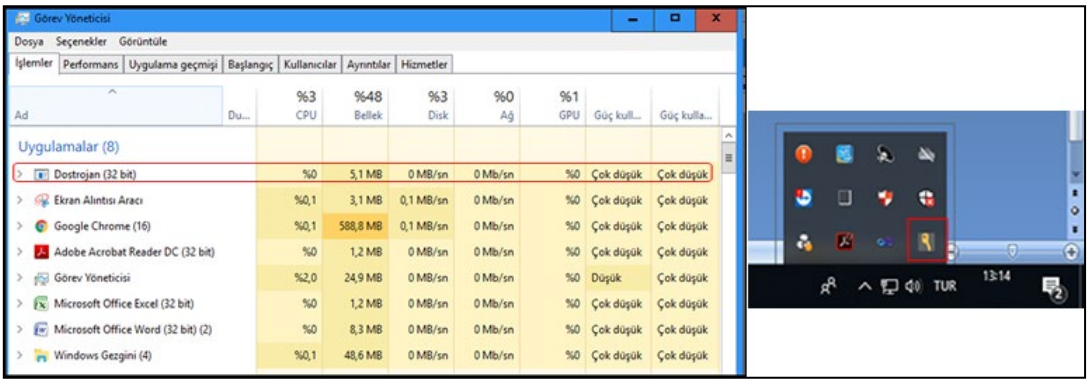


Figure 6. The image of the program working in the background.

FEI face database was used for the test of the system. Each photograph of the 200 people in the FEI face database taken in 14 different angles and lights was used for testing on the program.

6. Results

In this study, a prototype security system was developed for the security of personal computers. Face detection, face recognition and face comparison processes were performed with the video camera integrated in personal computers, and if the result of the comparison process was positive, the person was allowed to have access to the computer and if it was negative, a message was sent to the mobile phone of the person identified in the system and s/he was enabled to have access to the photograph of the person who requested access to the computer. That camera has become a standard equipment in today's laptops increases the usability of this system prepared.

In the software of this study, the image processing, machine learning and deep learning methods combined under Python programming language were used. For face detection, face recognition and face comparison operations, Python api, based on Convolutionary Neural Networks, which is one of the deep learning algorithms prepared independent of platform in Dlib library, was used.

FEI face image database was used for testing the system. The success rates for 14 different exposures are shown in figure 7. According to these results, the system achieved 99.15% success at the best angle and light and 76.31% success at the worst angle and light.

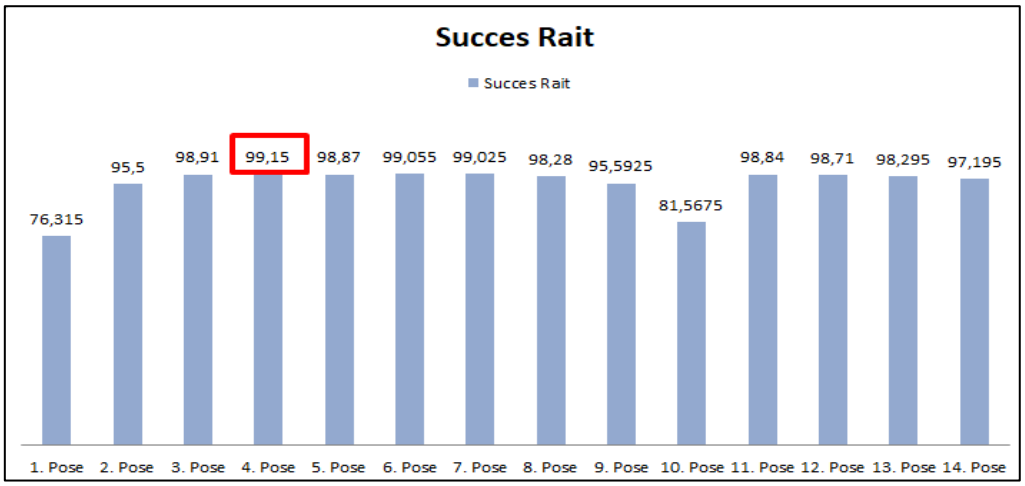


Figure 7. Program test success rates.

As a result, this system is expected to form the basis of the systems to be developed for the protection of personal computers, in today's world where information security and face recognition systems are crucial.

7. References

Ahmed, E., Jones, M., & Marks, T. K. (2015). *An Improved Deep Learning Architecture For Person Re-Identification.* In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 3908-3916).

Catalina P., Useche M., Javier O. Pinzo Arenas and Robinson Jimeez Moreno. (2018). *Face Recognition Access Control System using Convolutional Neural Networks*. Research Journal of Applied Sciences, 13: 47-53.

Cengil, E., Çinar, A.,(2016).“A New Approach For Image Classification: Convolutional Neural Network”, European Journal of Technique (EJT), 6 (2), 96-103.

Chahar, H., & Nain, N. (2017, December). *A Study on Deep Convolutional Neural Network Based Approaches for Person Re-identification*. In International Conference on Pattern Recognition and Machine Intelligence (pp. 543-548). Springer, Cham.

Erdem, M. E., & Topal, C. (2018, May). *Patch Warping Based Face Frontalization*. In 2018 26th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.

Geng, M., Wang, Y., Xiang, T., Tian, Y. (2016). *Deep Transfer Learning For Person Reidentification*. arXiv preprint arXiv:1611.05244 .

Guo S., S. Chen and Y. Li. (2016). *Face Recognition Based On Convolutional Neural Network And Support Vector Machine.* IEEE International Conference on Information and Automation (ICIA), Ningbo, 2016, pp. 1787-1792. doi: 10.1109/ICInfA.2016.7832107.

İnik, Ö., Ülker, E., (2017). “Derin Öğrenme Ve Görüntü Analizinde Kullanılan Derin Öğrenme Modelleri”, Gaziosmanpaşa Bilimsel Araştırma Dergisi , 6 (3) , 85-104.

Kaplan, A. (2018). *Gerçek ve Yarı Gerçek Zamanlı Yüz Tespit Etme/Face Detection On Real And Semi-Real Time.* Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Master Thesis. Elazığ.

DOI: 10.5824/ajite.2020.01.005.x

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). *Imagenet Classification With Deep Convolutional Neural Networks.* In Advances in neural information processing systems 25 (NIPS 2012) (pp. 1097-1105).

Li, W., Zhao, R., Xiao, T., Wang, X. (2014). *Deepreid: deep filter pairing neural network for person re-identification.* In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 152–159).

Liu, H., Feng, J., Qi, M., Jiang, J., Yan, S. (2016). *End-to-end comparative attention networks for person re-identification*, arXiv preprint arXiv:1606.04404.

Pala, T., Yücedağ, İ., Kahraman, H. T., Güvenç, U., & Sönmez, Y. (2018, September). *Haar Wavelet Neural Network Model.* In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP) (pp. 1-8). IEEE.

Rashid, E. (2018). *Raspberry Pi Ile Gerçek Zamanlı Yüz Tanıma Ve Kontrol Sistemi*. Doctoral dissertation, Selçuk Üniversitesi Fen Bilimleri Enstitüsü. Konya.

Sharma, K. Shanmugasundaram and S. K. Ramasamy. (2016). *FAREC — CNN based efficient face recognition technique using Dlib*. International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, 2016, pp. 192-195. doi: 10.1109/ICACCCT.2016.7831628.

Sharma, R., Ashwin, T. S., & Guddeti, R. M. R. (2019). *A Novel Real-Time Face Detection System Using Modified Affine Transformation and Haar Cascades*. In Recent Findings in Intelligent Computing Techniques (pp. 193-204). Springer, Singapore.

Su, C., Zhang, S., Xing, J., Gao, W., Tian, Q. (2016). *Deep attributes driven multicamera Person re-identification.* ECCV 2016. LNCS, vol. 9906, pp. 475–491. Springer, Cham Doi:10. 1007/978-3-319-46475-6 30.

Taşova, O., (2011). *Yapay Sinir Ağları Ile Yüz Tanıma.* Dokuz Eylül Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi. İzmir.

Varior, R.R., Haloi, M., Wang, G. (2016). *Gated Siamese convolutional neural network architecture for human re-identification.* ECCV 2016. LNCS (vol. 9912, pp. 791–808). Springer, Cham Doi:10.1007/978-3-319-46484-8 48.

Vinay A. et al., (2017). *G-CNN and F-CNN: Two CNN based architectures for face recognition*. International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), Chirala (pp. 23-28). doi: 10.1109/ICBDACI.8070803

Wang, F., Zuo, W., Lin, L., Zhang, D., Zhang, L. (2016). *Joint learning of single-image and cross-image representations for person re-identification.* In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1288–1296).

Wu, L., Shen, C., & van den Hengel, A. (2016). *Convolutional LSTM networks for video-based person re-identification*. arXiv preprint arXiv:1606.01609, 1(11).

Xiao, T., Li, H., Ouyang, W., Wang, X. (2016). *Learning deep feature representations with domain guided dropout for person re-identification.* In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1249–1258).

Yaman, A. U., & Samet, R. D. (2018). *Yüz tanıma sistemlerinin yanıltılmasına karşı bir yöntem: Yüz videolarında nabız tespiti ile canlılık doğrulaması*, Ankara üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Yang, M., David J. Kriegman, and Narendra Ahuja. (2002). "*Detecting Faces in Images: A Survey*", IEEE Trans. Pattern Anal. Mach. Intell. 24, 1 (January 2002), 34–58. DOI:https://doi.org/10.1109/34.982883.

Yi, D., Lei, Z., Liao, S., Li, S.Z. (2014). *Deep metric learning for person re-identification*. In: Proceedings of International Conference on Pattern Recognition (pp. 2666–2672).

Zhang, Z., Si, T., & Liu, S. (2018*). Integration convolutional neural network for person re-identification in camera networks*. IEEE Access, 6, 36887-36896.