A Survey on Efficient Multi-Factor Authentication Approaches for Smart Door Lock Systems

S.V.V.D. Venu Gopal[1], P. Mohan[2], K. Naga Praveena[3], D. Datha Sai[4], M. Vamsi Varma[5] A. Siva Rama Rao[6]

[1,2,3,4,5,6]Department of Computer Science

Abstract

In a smart environment smart door lock is very important because previously they carried the traditional methods like carrying keys etc. after that they developed a biometric method for security for the users in different sectors because they are unique characters and that are also involved in hacking and using less quality component .and It is most important in present environment because the technology is very fast and they are not carrying key because if they lose the key it is hard to break the lock and it give high security for safety purpose because if we add smart door lock your home means it gives notification to your phone directly open or lock the door if any person came in front of the door if you are in another place it is easy to allow the person .there are so many methods used for smart door lock system but even though there are still having the challenges for security and photography. This summarized all the existing methods for solving the problem using iris recognition. By observing all the existing solutions Iris gives high security compared to other biometric.

Keywords: Face Detection, Iris Recognition, Image Processing, Deep Learning, Raspberry Pi

1. Introduction

Face recognition-based biometric authentication systems were proven that high in security and give better accuracy for many sectors like workplaces places, and home applications. When compared to security procedure this is applied to various authentication challenges with high security. But keeping the security without any hacking and maintaining the high accuracy is the biggest challenge [1-4]. To solve this challenge for security dual authentication schemes were proposed because using dual authentication gives high security especially in the home application and at the workplace so that the hackers cannot allow for photography and other cyber-crime. This way we can protect the system called dual authentication.

Dual authentication is important in the present environment for security purposes. Because by carrying manual keys we can use duplicate keys for opening the door of the targeted person. If same like if we use the fingerprint and pin and password it is easy to hack and enter the buildings, etc. The goal of using dual authentication is to provide high security and it can adaptable to any environment and any help in any sector making it the hacker hard to allow to gain access now, a day people are habituated to an easy life and easy money without work, and this causes the rapid growth of the attacking knowledge about the simple encrypted techniques so that they are not providing the sufficient security [5-8].

As a result of face recognition smart door locks. There are so many methods are exist for the smart door lock most of them are based on supervised algorithms of machine learning and the hardware components and fingerprint this is the most common type of biometric smart lock. It works by scanning the user's fingerprint and comparing it to a stored database of fingerprints. If the fingerprint matches, the lock unlocks. The next one is Facial recognition this type of lock uses a camera to scan the user's face and compare it to a stored database of facial images. If the face matches, the lock unlocks. And another existing method is voice Recognition t this type of lock uses a microphone to listen to the user's voice and compare it to a stored database of voice recordings. If the voice matches, the lock unlocks.

Some are combinations of fingerprint and pins or face recognition and pins adding an extra layer that gives high security so it is better to use combinations because we do need to carry the keys we do need the tension like any robbery happens to us.

Here some existing methods are used like iris recognition this type of lock uses a camera to scan the user's iris and compare it to a stored database of iris images. Iris recognition is one of the most accurate biometric authentication methods, but it can be more expensive to implement. [9-12]Next one is Palm vein recognition this type of lock uses a sensor to scan the user's palm vein and compare it to a stored database of palm vein images. Palm vein recognition is becoming more affordable and is being used in some high-end smart door locks.it is not adopted in all countries because of the lack of knowledge.

It was observed from the literature that there is no support for the high security and challenges that exist. Using this face and fingerprint and passwords and traditional methods gives certain security but not highly because using low-cost components [13-14] affects the pattern identification and faces of the authentication users. Observing from related work. I conclude that using dual authentication of face and iris gives high security compared to other biometric authentication [15] by using a convolution neural network it gives the best performance and Python programming open source in all platforms by using this for embedded systems it gives maximum performance.

The rest of the papers contain briefly about II. Related work, III. Analysis and discussion, IV. Conclusion.

2. Related work

a. Face recognition based Smart Lock System

The Authors Mishra *et al*. [16] have developed a face-recognition smart door lock system. The problem addressed by this paper was detecting faces for home security in the real world. This proposed method identified that the CNN algorithm gives the best result compared to other algorithms because CNN helps in image processing. The measures in this model are The FAR (False Accept Rate) is the probability of the system incorrectly identifying an unauthorized person as an authorized person. The data set used in this paper is Labeled Faces in Wild (LFW) this takes the face images of 13000 images of 5,700 people from this the accuracy of this model is 94.4%. The advantage of this is it is more useful in COVID-19 time because of the spreading of this virus through contact with touching keys etc. This will help for the users.

Similarly, another new approach was given by Jayanta Paul *et al*. [17] have used three algorithms local binary pattern histogram (LBPH), Eigen face, and Haar cascade for Face recognition door lock system for home security. The problem addressed from this model is recognizing the face for door locking. He develops three algorithms from that the results show that LBPH algorithm give the best performance compared to Eigen face and Haar cascade. And the dataset used in this paper is publicly available it contains different faces from different conditions from this they get the accuracy rate from 95% to 97%. And LBPH is a good choice when lighting and pose is critical, and Haar cascade is a good when speed is critical and Eigen face is a good when accuracy is critical. The advantage of this system is less mistaken in face recognition.

The Researcher Purushothaman *et al*. [18] he use two algorithm local binary pattern histogram (LBPH) and Viola- Jones detection algorithm for developing pose and illumination face recognition Automation door lock system. The problem addressed from this model pose and illumination of the automatic door lock. and the Viola-Jones detection algorithm used for detect face images but it will not give more accuracy and LBPH is used for extract features from face and by combining this two algorithms maintain the high level accuracy and the measures of this model is the accuracy, recall, and precision are all important measures of performance. The dataset used in this model is their own data for creating this model. The advantage of this system is identifying the face in different pose and recognizing face at lighting conditions.

The author Khalimov *et al*. [19] have used combination of three algorithms for face recognition smart door lock using Face recognition algorithm this is used for extracting features from stored database and Face detection algorithm this is used for identifying facial features like nose eyes mouth. And decision making algorithm is used for grant permission and Feature extraction algorithm is used for extracting features from the dataset. For extracting it uses LBPH and Eigen faces, and Fisher faces. And the measures from this model are use of high quality camera and enrolling multiple images of each person. And dataset used in this model is LFW (Labeled Faces in the Wild) this takes 13,000 images from web and CASIA web dataset this contains 40,000 face images in web it give the accuracy of 97%..The advantage of this model is needs to go in front of the camera and get quick access to the room and eliminate the handling the keys.

The author Orna *et al*. [20] used an deep learning algorithms for object detecting he use Haar's cascade algorithm this is used for face detection and Mobile Net-SSD this is use for object detection and Open Vino it is a software kit used for deep learning model on embedded system and also used python programming which is more popular for embedded system development. And the measures from this paper are true positive rate means how correctly the face is recognized. False positive rate means how much incorrectly face is not identified. The dataset used in this model is LFW (Labeled Face in the Wild) it takes 13,000 images of face and labeled with their names of the person in the image and gives the accuracy 88.75%. The advantage of this model is a low-cost embedded facial recognition system for controlling an electromagnetic lock and it provide low error rate .and provide more security for the authorized user.

The Researcher Waseem *et al.* [21] developed an Hierarchical Network for face recognition door lock system he use some algorithms PCA(Principle Component Analysis)this is used to extract most important feature from the data set and SVM(Support Vector Machine) this is used for classification and regression and HOG(Histogram of Oriented Gradients) used for extract features from images and Gabor filter it is a filter extract features from images and deep neural network this is used to learn complex patterns from data. The measures from this paper are Precision means it is percentage of images that are classified and Recall, F1 score. The dataset used in this model ORL dataset it take 400 face images from 40 different people it give the accuracy 97.5% and it also take Yale Face Database it take 165 images of face from 15 different people and give accuracy is 95% and Labeled Faces in the Wild (LFW) dataset it take 13,233 face images from 5,749 different people and provide the accuracy is83.3% over all it give the 90% accuracy from this model .The advantage of this model is it can used in home and office and work places.

The author Purohit *et al*. [22] have developed a Histogram of Oriented Gradients (HOG) algorithm and support vector algorithm (SVM) and Blink detection are used for anti-spoofing door lock using face recognition of real person not photograph. The Problem addressed in this paper is face recognition and blink detector for home application. The measures from this model is Accuracy and Recall and precision and F1score. The dataset used for this model is publicly dataset from Labeled Faces in the Wild (LFW) contain 13,000 face images and also take from Mega Face dataset it contain 1millon face images. From this the accuracy we get 92.68 %.The advantage of this system is providing the enhanced security, convenience, and adaptability and fast and inexpensive.

Similarly the researcher Jahnavi *et al*. [23] has developed three algorithms for smart door lock system. Those are Viola Jones algorithm and Feature extraction uses Local Binary Pattern (LBP) algorithm and for Face recognition uses Principal Component Analysis (PCA) algorithm. The problem identified from this paper is smart anti-theft door lock system for improving security. The dataset in this Labeled Faces in the Wild (LFW) and mega face dataset from this the accuracy we get 97.23%. The advantage of this model is provide detection of the location of the face points in an image and increase the security.

The Researcher Nikhilendra *et al*. [24] have proposed a Passive Infrared (PIR) sensor and Pi camera and Open CV and Telegram application for door lock system. The problem addressed and identified in this paper is automatic detecting and recognizing the face images for door lock. The problem addressed in this data set used in accuracy of this model is fast. The accuracy is 95%. The advantage of this model is provide performance of the system efficiency is high and the limitations of this model is vulnerable to hacking, raising concerns about the security of access control systems, especially if not properly secured.

b. Iris recognition based Smart Lock System

The authors Lozej *et al*. [30] have proposed three main algorithms. Those are DeepLabV3+ and mobile net and Exception. The main problem addressed in the paper is the impact of iris segmentation on the performance of deep learning models for iris recognition. The authors address the problem of using deep learning models for iris recognition in real-world applications .Receiver operating characteristic (ROC) curve, Area under the curve (AUC) , Equal error rate (EER). There are some measures which are used for this paper is iris recognition can achieve highly competitive performance even without iris segmentation.

The CASIA-Thousand dataset and the SBVPI datasets are used and we get the accuracy of this model 97.46% Advantages on this paper was having high accuracy, Robustness, scalability.

The Researcher Patil *et al*. [31] have developed a Hough transform and Gabor filters and Support vector machines (SVMs) and Log-Gabor filters and Integer Wavelet Transform (IWT) and Daugman's algorithms. The paper discusses techniques for removing occlusions from iris images. This is a challenging problem because the occlusions can vary in size, shape, and location. Segmentation, Feature extraction, Matching, Spoofing resistance, Real-time performance these are the measures used in this particular paper. The datasets are CASIA Iris Image Database (CASIA-Iris), IIIT-D Iris Image Database, NTCIR Iris Image Database, Bio ID Iris Image Database .The accuracy we get 98.8%. Advantages are High accuracy, Uniqueness, Non-intrusive, Robustness, and Scalability.

The Author Andrej Hafner *et al*. [32] have proposed a Convolutional Neural Network (CNN) for Deep Iris Feature Extraction door lock system. The problem addressed from this paper is Iris recognition. It is the process of identifying an individual based on the unique patterns in their iris and it is widely used in applications such as security and access control. The measures from this paper is Recognition accuracy and False match rate (FMR) and False non-match rate (FNMR).and the dataset used in this model is CASIA-Iris it contains 20,000 iris images collected by an IKEMB-100 camera and it also collect the 10 left and 10 right eye images from each and some contains eyeglasses from this we get the accuracy 97.3%.The advantages from this model give the high performance in both open and closed set recognition.

Similarly the another new approach was proposed by Rana *et al*. [33] have used Convolutional neural networks (CNNs) and he used some techniques like batch normalization and Dropout, Rectified linear units (RLU).and the problem addressed and identified from this paper is IR is a biometric technology that uses the unique patterns in the iris of the human eye to identify individuals. But it is challenge to implement in real world due to non-ideal image quality and sensor interoperability. The dataset used in this model is ND-iris-0405. This ND-iris-0405 database contains 64,980 iris images from 356 different conditions and capture by using LG2200 iris images camera and it also use ND- CrossSensorIris-2013. This ND-CrossSensorIris-2013 database contains 29,986 images from 676 subjects. The image captured by using two different sensors: LG2200 and LG4000 from this we get the accuracy 97.4%.The advantage of this model is it give high accuracy and give more security.

The authors Hegde *et al*. [34] have used discrete wavelet transform (DWT) this DWT is a mathematical transform that decompose signal into different frequency bands. And also used Radon transform that can transform images into different domains. The problem identified from this model is iris recognition algorithms can be susceptible to noise and an illumination variation leads to reduce the accuracy in real world conditions. The dataset used in this model is Phoenix Iris Database. This database contains 800 iris images from 200 subjects. These images were captured using a commercial iris camera and also used IIT Delhi Iris Database This database contains 1125 iris images from 225 subjects. This image was captured by using a prototype iris camera.

The Authors Talha *et al*. [35] have developed Local Gabor binary pattern (LGBP) and Zero-crossing wavelet transform (ZCWT) and Fourier transform (FT) and Support vector machines (SVMs) and Neural networks . The problem addressed and identified the problem domain of iris recognition using multi-algorithmic approaches for cognitive internet of things (CIOT) framework. The measures from this model are using robust iris recognition algorithm, Use a fusion of different iris recognition algorithms, and Use privacy-preserving iris recognition techniques. The datasets used in model is that these datasets contain images captured under different illumination conditions, with varying head poses.

3. Analysis and Discussion

In several articles face recognition has been analysed using a variety of techniques. For face identification used accuracy and different data sets. For the purpose of detecting face recognition we have used both software and hardware combination.

Here there we have used machine learning algorithms, python for face recognition and there are so many parameters used for machine learning techniques to identify face recognition and accuracy has shown in the table below.

In this table CNN, LBPH and SVM perform best to identify the face recognition

TABLE I. PERFORMANCE OF EXISTING FACE RECOGNITION SYSTEM

Authors	Model/Algorithms	Accuracy
Mishra *et al.* [16] (2020)	A Convolutional Neural Network(CNN)	94.4%
Jayanth *et al*.[17] (2020)	Local Binary pattern histogram(LBPH)	95%
Khalimov *et al*.[19] (2020)	Face detection algorithm	97%
Orna *et al*.[20] (2020)	Haar’s cascade algorithm	88.75%
Waseem *et al*.[21] (2020)	Principle Component analysis and SVM(Support vector Machine)	97.5%
Purohit *et al*.[2] (2021)	Support Vector Machine and HOG(Histogram Oriented gradients)	92.68%
Jahnavi *et al*.[16] (2019)	Local Binary Pattern	97.23%
Vidhyasri *et al*.[19] (2013)	Network Model Management System	85%

TABLE II. PERFOMANCE COMPARISION OF EXSING SYSTEM FOR IRIS RECOGNITION

AUTHORS	**MODEL/ALGORITHMS**	**ACCURACY**
LOZEJ[23] (2019)	DEEPLABV3+	97.46%
PATIL[24] (2014)	NTEGER WAVELET TRANFORM (IWT) AND DAUGMAN’S	98.8%
ANDREJ HAFNER[25] (2021)	CONVOLUTION NEURAL	97.3%
RANA[26] (2016)	CONVOLUTION NEURAL	97.4%

4. CONCLUSION

The proposed system detects and identifies the face for different pose and illumination. Hence using face recognition and iris for door access is a great way to ensure security. In future, the system can be implemented in real time by using microcontroller instead of laptop. Also the owner can be given alert via SMS/email if any attempt of unauthorized access occurs. The researchers developed a face recognition-based building entry system that is more accurate and intelligent than existing systems. However, the system is limited by the Raspberry Pi's memory space and processing speed. The researchers plan to improve the system's accuracy and performance by using a more powerful processor and by implementing multi-parameter recognition. They also plan to integrate the system with a mechanical locking system .Face recognition technology is powerful but can be biased and can be used to track people without their consent. Organizations

References

5. Zhiguo, Zhu; Cheng, Yao (2020). Application of attitude tracking algorithm for face recognition based on Open CV in the intelligent door lock. Computer Communications, (), S0140366419317219–. doi:10.1016/j.comcom.2020.02.003
6. Liu, X. Shen and H. Ren, "FDAR-Net: Joint Convolutional Neural Networks for Face Detection and Attribute Recognition," 2016 9th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, China, 2016, pp. 184-187, doi: 10.1109/ISCID.2016.2051.
7. Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multifactor door locking systems: A review. Materials Today: Proceedings, 46, 7973–7979. doi:10.1016/j.matpr.2021.02.708 10.1016/j.matpr.2021.02.708
8. Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door Security System for Home Monitoring Based on ESP32. Procedia Computer Science, 157, 673–682. doi:10.1016/j.procs.2019.08.218 10.1016/j.procs.2019.08.218
9. S.Tiwari, S. Thakur, D. Shetty and A. Pandey, "Smart Security: Remotely Controllable Door lock," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 979-984, doi: 10.1109/ICICCT.2018.8473161
10. Rameswari, R.; Naveen Kumar, S.; Abishek Aananth, M.; Deepak, C. (2020). Automated access control system using face recognition. Materials Today: Proceedings, (), S2214785320333113–. doi:10.1016/j.matpr.2020.04.664
11. Novita Hanafiah;Collin Power Kariman;Nicky Fandino;Edwin Halim;Felix Jingga;Wiedjaja Atmadja; (2021). Digital Door-Lock using Authentication Code Based on ANN Encryption. Procedia Computer Science, (), –. doi:10.1016/j.procs.2021.01.079
12. Areed, M. F. (2019). A Key less Entry System Based on Arduino Board with Wi-Fi Technology. Measurement. doi:10.1016/j.measurement.2019.02.028
13. Singh, G., Singh, R. K., Saha, R., & Agarwal, N. (2020). IWT Based Iris Recognition for Image Authentication. Procedia Computer Science, 171, 18681876.doi:10.1016/j.procs.2020.04.20010.1016/j.procs.2020.04.200
14. Hu, Qingqiao; Yin, Siyang; Ni, Huiyang; Huang, Yisiyuan (2020). An End to End Deep Neural Network for Iris Recognition. Procedia Computer Science, 174(), 505–517. doi:10.1016/j.procs.2020.06.118
15. Liu, Xiao Nan; Bai, Yuchen; Luo, Yuwen; Yang, Zhengwei; Liu, Yan (2019). Iris recognition in visible spectrum based on multi-layer analogous convolution and collaborative representation. Pattern Recognition Letters, 117(), 66–73. doi:10.1016/j.patrec.2018.12.003
16. Galdi, Chiara; Dugely, Jean-Luc (2017). FIRE Iris Recognition on mobile-mobile phones by combining color and texture features. Pattern Recognition Letters, (), S0167865517300314–. doi:10.1016/j.patrec.2017.01.023
17. Gad, Ramadan; Talha, Mohammed; El-Latif, Ahmed A. Abd; Zorkany, M.; EL-Sayed, Ayman; EL-Fishery, Nawal; Muhammad, Ghulam (2018). Iris recognition using multi-algorithmic approaches for

cognitive Internet of things (CIoT). Future Generation Computer Systems, (), S0167739X18306915–. doi:10.1016/j.future.2018.06.020

18. De Marsico, Maria; Petrosino, Alfredo; Ricciardi, Stefano (2016). Iris Recognition through Machine Learning Techniques: a Survey. Pattern Recognition Letters ,(), S0167865516000477–. doi:10.1016/j.patrec.2016.02.00
19. Galdi, Chiara; Nappi, Michele; Dugelay, Jean-Luc (2015). Multi modal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity. Pattern Recognition Letters, (), S0167865515003190 doi:10.1016/j.patrec.2015.09.009
20. Mishra A .Ransingh M. K. Behera and S. Chakravarty, "Convolutional Neural Network Based Smart Door Lock System," 2020 IEEE India Council International Subsections Conference (INDISCON), Visakhapatnam, India, 2020, pp. 151-156, doi: 10.1109/INDISCON50162.2020.00041
21. J. Paul et al., "Evaluation of Face Recognition Schemes for Low-computation IOT System Design," 2020 24th International Symposium on VLSI Design and Test (VDAT), Bhubaneswar, India, 2020, pp. 1-6, doi: 10.1109/VDAT50263.2020.91905

A. Purushothaman and S. Palaniswamy, "Pose and Illumination Invariant Face Recognition for Automation of Door Lock System," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1105-1108, doi: 10.1109/ICICCT.2018.8473103

22. R. Khalimov, Z. Rakhimbayeva, A. Shokayev, B. Kamalov and M. H.Ali "Development of Intelligent Door Locking System Based on Face Recognition Technology," 2020 11th International Conference on Mechanical and Aerospace Engineering (ICMAE), Athens, Greece, 2020, pp. 244-248, doi: 10.1109/ICMAE50897.2020.9178866.
23. G. Orna, D. S. Benítez and N. Perez, "A Low-Cost Embedded Facial Recognition System for Door Access Control using Deep Learning," 2020 IEEE ANDESCON, Quito, Ecuador, 2020, pp. 1-6, doi: 10.1109/ANDESCON50619.2020.9271984.
24. M. Waseem, S. A. Khorana, R. K. Ayyasamy and F. Bashir, "Face Recognition for Smart Door Lock System using Hierarchical Network," 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, pp. 51-56, doi: 10.1109/ICCI51257.2020.9247836
25. R. Ganjoo and A. Purohit, "Anti-Spoofing Door Lock Using Face Recognition and Blink Detection," 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2021, pp. 1090-1096, doi: 10.1109/ICICT50816.2021.9358795
26. S. Jahnavi and C. Nandini, "Smart Anti-Theft Door locking System," 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 2019, pp. 205-208, doi: 10.1109/ICATIECE45860.2019.9063836

A. Nag, J. N. Nikhilendra and M. Kalmath, "IOT Based Door Access Control Using Face Recognition, IOT Base" 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 2018, pp. 1-3, doi: 10.1109/I2CT.2018.8529749.

27. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga and S. Bojewar, "Intelligent security lock," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, India, 2017, pp. 713-716, doi: 10.1109/ICOEI.2017.8300
28. I.Yugashini, S. Vidhyasri, K. Gayathri Devi(2019)Design and implementation of automated door accessing system with face recognition, Int. J. Sci. Modern Eng.(IJISME) 01 (12) (2013) 10–12.

29. K. P. Bhattarai, B. P. Gautam and K. Sato, "Authentic Gate Entry System (AuthGES) by Using LBPH for Smart Home Security," 2018 International Conference on Networking and Network Applications (NANA), Xi'an, China, 2018, pp. 191-196, doi: 10.1109/NANA.2018.8648705
30. Gulzar, Jun Sang and O. Tariq, "A cost effective method for automobile security based on detection and recognition of human face," 2017 2nd International Conference on Image, Vision and Computing (ICIVC), Chengdu, China, 2017, pp. 259-263, doi: 10.1109/ICIVC.2017.7984557.
31. R. P. Rizki, E. A. Z. Hamidi, L. Kamelia and R. W. Sururie, "Image Processing Technique for Smart Home Security Based On the Principal Component Analysis (PCA) Methods," 2020 6th International Conference on Wireless and Telematics (ICWT), Yogyakarta, Indonesia, 2020, pp. 1-4, doi: 10.1109/ICWT50448.2020.9243667.
32. Lozej et al. (2019) Lozej J, Stepec D, Struck V, Peer P. Influence of segmentation on deep iris recognition performance. 7th International Workshop on Biometric and Forensics, IWBF.20
33. Patil, S. Gudasalamani and N. C. Iyer, "A survey on Iris recognition system," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 2207-2210, doi: 10.1109/ICEEOT.2016.775
34. Andrej Hafner;Peter Peer;Ziga Emersic;Matej Vitek; (2021). Deep Iris Feature Extraction. 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), (), – . doi:10.1109/icaiic51459.2021.9415202
35. Rana et al. (2019) Rana HK, Azam MS, Akhtar MR, Quinn JMW, Moni MA. A fast iris recognition system through optimum feature extraction. PeerJ Computer Science. 2019;5:e184
36. Dhage et al. (2015), Hegde SS, Manikantan K, Ramachandran S. Dwt-based feature extraction and Radon transform based contrast enhancement for improved iris recognition. Procedia Computer Science. 2015; 45(2):256–265. Doi: 10.1016/j.procs.2015.03.135.
37. Gad et al. (2018) Gad R, Talha M, El-Latif AAA, Zorkany M, EL-SAYED A, EL-Fishery N, Muhammad G. Iris recognition using multi-algorithmic approaches for cognitive internet of things (CIoT) framework. Future Generation Computer Systems. 2018;89 (7):178–191. Doi: 10.1016/j.future.2018.06.020