



Iris-based human identity recognition with machine learning methods and discrete fast Fourier transform

Maciej Szymkowski¹ · Piotr Jasiński¹ · Khalid Saeed¹

Received: 10 January 2021 / Accepted: 10 March 2021 / Published online: 26 March 2021
© The Author(s) 2021

Abstract

One of the most important modules of computer systems is the one that is responsible for user safety. It was proven that simple passwords and logins cannot guarantee high efficiency and are easy to obtain by the hackers. The well-known alternative is identity recognition based on biometrics. In recent years, more interest was observed in iris as a biometrics trait. It was caused due to high efficiency and accuracy guaranteed by this measurable feature. The consequences of such interest are observable in the literature. There are multiple, diversified approaches proposed by different authors. However, neither of them uses discrete fast Fourier transform (DFFT) components to describe iris sample. In this work, the authors present their own approach to iris-based human identity recognition with DFFT components selected with principal component analysis algorithm. For classification, three algorithms were used— k -nearest neighbors, support vector machines and artificial neural networks. Performed tests have shown that satisfactory results can be obtained with the proposed method.

Keywords Biometrics · Iris · Identity recognition · Discrete fast Fourier transform · Principal component analysis · Support vector machines · Artificial neural networks

1 Introduction

Recent research [1] is showing that on average every 39 s hacker attack on computer infrastructure is observed. By this statement we can conclude that importance of security systems is increasing. However, it was also proven that simple security approaches based on login and password are not efficient enough [2]. It is mostly connected with the fact that a part of users selects typical, easy to guess, nicknames, PINs or passwords. Moreover, some of them writes their credentials on credit cards or sticks them to their computers. It can lead to another statement—the user is the weakest element in the whole computer system. The main question is how it can be changed?

The solution for such problem is really easy. The well-known answer is biometrics. It is the science that identifies (or verifies) human on the basis of his measurable traits (e.g., fingerprint, iris, retina, keystroke dynamics). These features can be divided into three main groups—physiological (connected with our body and proper measurements), behavioral (these are the traits that we can learn—e.g., signature) or hybrid that consists of traits that are physiological and behavioral at the same time (e.g., voice). We can conclude that each computer system (with security system based on biometrics) user will not provide any additional passwords because he will be a real password by his measurable traits.

Diversified experiments and research are showing that one of the most important traits that can guarantee high accuracy, efficiency and recognition rate is iris. This feature consists of more than 250 unique elements. Each of them is used to describe human identity (in the form of feature vector). In the literature, it was also proven that such feature vectors are completely different for both eyes of one person (left and right), and moreover it is true, even in the case of twins. Each of them has different irises (feature vectors are completely different). The most important is that iris is really hard to spoof. In the literature, we can find only a couple of research papers [3] that provide some

✉ Maciej Szymkowski
m.szymkowski@pb.edu.pl

Piotr Jasiński
jasinski.life@gmail.com

Khalid Saeed
k.saeed@pb.edu.pl

¹ Faculty of Computer Science, Białystok University of Technology, Białystok, Poland

vital evidence that such spoofing procedure was finished with the success. However, it also has to be claimed that in these works, only simple iris-based biometrics systems were used. It means that such solutions are not considering iris liveness and are vulnerable to print attack (with iris photo). On the other hand, iris has one huge disadvantage—it is really hard to collect high-quality iris sample without specialized devices. In some cases, even an assistance of experienced ophthalmologist is needed to complete such task. Of course, iris samples can also be collected with novel smartphones (e.g., Apple iPhone 12 Max or Samsung Galaxy S20+) with high-quality cameras. However, once again an assistance of second person is needed. If we want to collect such images by our own, we can use specialized sensors that are available on the market. Nevertheless, their prices are really high and some of them even needs special light conditions to obtain precise, high-quality images.

In this work, the authors present their own, novel approach to iris-based human identity recognition. The most important part of the work is that the authors used discrete fast Fourier transform (DFFT) to analyze each sample and to construct feature vector based on a part of its components, selected with principal component analysis (PCA) method. As it is presented in the further parts of this paper, the proposed idea provided satisfactory results in really short time. Of course, the algorithm starts with iris segmentation and then preprocessing stage in which the authors performed some operations to enhance image quality and to highlight some parts of it. In the next steps, DFFT is used and finally feature vector is created with PCA method. For classification, the authors used three well-known approaches: k -nearest neighbors, support vector machines (SVM) and artificial neural network. Each of them was compared in the terms of accuracy. It was proven that the best results were obtained on the basis of SVM algorithm.

Significant part of this work is also connected with testing procedure used in the quality verification process. At the beginning, the authors used Scrum methodology to work out the solution by a step-by-step manner to increase algorithm precision. In each stage, we tested the created solution quality. It was the main indicator by which we observed whether the progress was made or not.

This work is organized as follows: in Sect. 2, the authors described some interesting approaches and solutions connected with iris-based human recognition that were recently published in the literature. In Sect. 3, the idea and its main points were presented and precisely described (each step was shown and discussed). Section 4 contains information about performed experiments, especially about tools used during solution testing. Finally, the conclusions and future work are given.

2 How others see it

In the literature, one can easily find diversified approaches and algorithms connected with iris-based biometrics identity recognition. Huge amount of works regarding this subject is caused by high efficiency and accuracy that can be guaranteed by this measurable trait. One of the most important solutions is Daugman's algorithm [4]. In this approach, random patterns visible in iris are encoded in a real time with selected distance measure. Then, test of statistical independence is applied to these vectors. We have to claim that this is one of the well-known solutions and most of novel ideas are compared with it. Moreover, this algorithm is also mentioned as a standard in diversified works and systems.

Another interesting algorithm was presented in [5]. In this work, the authors used principal component analysis (PCA) and discrete wavelet transform (DWT) for the extraction of iris optimum features and to reduce the processing time of image. The authors claimed that their solution should run in real time. In the case of this work, frequencies were also used to describe the sample; however, in comparison with our approach, different features were obtained. In the paper, the authors claimed that algorithm reached 95.4% of accuracy when it was tested on 100 iris images only. The most important question connected with this work is why the authors did not test their idea on more samples.

The next worth-reading solution was described in [6]. In this paper, the authors mainly consider a concept of negative iris recognition. In the analysis process, they used negative iris databases. Moreover, the main aim of this work is to check whether protection techniques applied to iris templates can make it unrecoverable for hackers. The summary of the work is that recently used approaches do not guarantee requested efficiency and accuracy (especially in the case of bank accounts or sensitive data). This work is not directly dealing with iris recognition. However, the main goal of this work is interesting because we should also know what the ways are to protect iris feature vectors placed in the databases.

Another idea that has to be considered during iris-based security systems design is prevention from spoofing. Mostly observed susceptibility in biometrics systems is positive recognition on the basis of printed images rather than real samples. Especially it is connected with iris-based systems. This problem was deeply described in [7]. In the paper, the authors presented that print attack images of live iris, use of contact lenses and conjunction of both can have huge influence on false-positive recognition by the system. All experiments were realized with IIIT-WVU iris dataset. Moreover, the authors presented a novel approach to prevent such attacks with a deep convolutional neural network.

Another interesting work was presented in [8]. In this paper, the authors described their own, novel approach to iris-based human identity recognition. However, they considered only low-quality images. Their idea is based on lifting wavelet transform. Authors claimed that their solution can guarantee high accuracy for CASIA V1 dataset. However, they did not provide any results calculated with other databases. The way in which the algorithm accuracy was calculated makes hard judgment of the solution real efficiency. It is connected with the fact that usage of only one database cannot guarantee that in the case of samples from different sets, the solution efficiency and accuracy will be the same.

In the work presented in the paper [9], the authors proposed an idea to calculate the quality of iris image. At the beginning, it was claimed that poor quality samples can have a huge influence on false rejection rate (FRR) increment as well as decrease in the system performance (in terms of accuracy). The authors proposed their own algorithm for iris image quality assessment. The metric described in the paper was based on statistical features of the sign and the magnitude of local image intensities. This is interesting work because on the basis of the information about quality we can decide whether we should use regular algorithm for iris recognition or whether some additional stages for enhancing image quality are required.

A novel approach to iris recognition was proposed in [10]. In this work, the authors used postmortem samples to recognize human identity. The main point of their work was to use deep learning-based iris segmentation models to detect highly irregular areas in iris texture. In the work, it was claimed that the proposed algorithm can guarantee higher accuracy than the currently used solutions for postmortem iris recognition. The authors also pointed out that their work is only a first step in the process of efficient forensic system creation for postmortem iris recognition. The proposed algorithm can be useful especially in the case of people recognition with unknown identity (e.g., without documents as ID card).

One of the trends in biometrics is to use deep learning and machine learning methods in the process of measurable traits classification. This term is also true in the case of iris. During the research performed in different databases (IEEE, Scopus, SpringerLink), the authors found papers in which iris-based human recognition was realized with convolutional neural networks [11, 12], support vector machines [13] as well as deep learning methods [14, 15]. We have to claim that all these approaches are really interesting; however, all of them needs huge databases (at startup) as well as high computing power and resources. Of course, they can guarantee satisfactory accuracy and efficiency, but the cost of it is really high. Moreover, it is nearly impossible to use such solutions in the case of mobile devices, e.g., smartphones or wearable devices.

3 Proposed solution

The proposed approach consists of two main modules. The first of them is connected with iris preprocessing and segmentation, whilst the second one is responsible for classification (identity recognition). However, before the system will be presented, the authors would like to show their motivation to work under iris-based human identity recognition.

As it was presented in the second chapter, in the literature one can observe different ideas and algorithms connected with biometrics and especially with the main topic of this paper. However, in some approaches descriptions there are no significant details provided. For example, in part of them it is really hard to understand how iris image was preprocessed and what kind of algorithms were used to extract the most important information. Sometimes there is even no answer on the vital question—how the feature vector was constructed? Moreover, in the case of artificial intelligence-based approaches, in part of them there are no details regarding the way in which such tools were tuned or how they were learned (number of epochs or even the structure of neural network is missing). At times, it is also hard to understand why the results were so precise. In these works, there are no premises that can lead to high recognition rates. (It means that there are no scientific reasons why such algorithms gain high accuracy values.) By these reasons, the authors would like to propose their own idea regarding iris-based human identity recognition.

In this paper, all stages of the worked-out approach are given. At the beginning, preprocessing stage is described, whilst at the end different classification methods are provided. The description of the whole recognition process is detailed, and all used algorithms are given.

The main aim of the worked-out solution described in this chapter is to use discrete fast Fourier transform (DFFT) components to create the descriptive iris-based feature vector that will be used in the human identity recognition process. The most important factors are selected with principal component analysis algorithm (PCA). This solution can guarantee that the most descriptive elements will be selected. It is a novel idea as in the literature we did not find any similar approaches. Moreover, the authors would like to check whether it is possible to get satisfactory recognition ratios with the proposed feature vector structure. The authors would like to claim that they used Scrum methodology to work out the solution. It allowed us to precisely step-by-step observe whether quality (in terms of efficiency and accuracy) of the proposed algorithm is satisfactory or not. This indicator was the most important, so that in each stage we could take significant steps by which we increased it. The authors considered here additional algorithms that can increase image quality or some changes in feature vector.

The proposed approach was implemented in the form of a real computer system. It was run in the development environment on both Microsoft Windows and Linux. All steps of the approach were implemented with Python programming language and frameworks available in this environment (e.g., TensorFlow, Keras and OpenCV). As it was claimed before, the proposed approach consists of two main components—iris segmentation and classification. At first, the details connected with the first part are given, and then, all information about the second part is presented.

3.1 Iris segmentation

The first stage of iris segmentation is connected with redundant artifacts removal (e.g., light reflections). This operation is needed due to the fact that some of them can be easily observed after sample acquisition process. To provide efficient and accurate results, Otsu binarization [16] algorithm is used at first. As the next algorithm, dilation is applied. It is done because another part of artifacts can be removed by then. After these two operations, the image is cleared and does not have any additional distortions that can have an influence on final feature vector result.

As the next step, Top-hat operation is used. Its main aim is to identify and highlight iris edges. In this stage, real iris region has to be extracted. Just after this algorithm is applied, two additional filters are used. The first of them is median filtering. It was used to remove some additional pixels that are not needed in the image. By this stage, all distortions in the form of salt and pepper are removed. In the next step, Gaussian filter is applied in image. It is connected with the fact that the visibility level of unnecessary details has to be reduced. The most important for us is to observe iris edges.

The next part of iris segmentation algorithm can be divided into two main substages. The first of them is connected with pupil detection. At the beginning, Canny edge detection algorithm is applied into image. By this step, we can observe all edges (in fact, detected elements are not only connected with iris). Following operation is Hough transform. It is used for circles detection by which we can observe pupil coordinates.

In the final stage, Hough transform is used once again. This time it is done for all circles detection. By this operation, external border of pupil can be detected. It also has to be claimed that the detection stage has to consider circle radius. Pupil radius has to be lower than external one. Original iris sample and image with the segmented iris are presented in Fig. 1.

3.2 Feature vector creation

In this stage, feature extraction and descriptive vector creation are performed. All stages of the proposed process are shown in Fig. 2.

The algorithm starts with image normalization based on Daugman's rubber sheet model [17]. This method uses information about centers and radiuses of iris and pupil. This solution was used because it can guarantee presentation clarity as well as it was much easier to work on transformed sample rather than the original iris sample. It is connected with the fact that it was much easier to analyze such samples.

Before we will be ready to obtain all significant information and create sufficient feature vector, preprocessing algorithms have to be applied in the normalized image. All these actions are required because iris sample is not adapted to easily extract the most important features. At the beginning of the preprocessing stage, we used histogram equalization. After this operation, we obtained the image in which

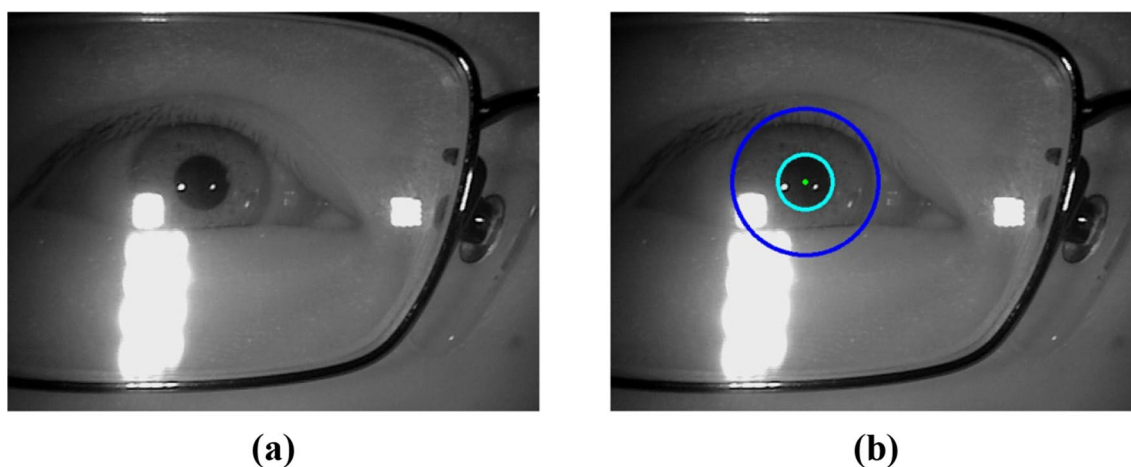
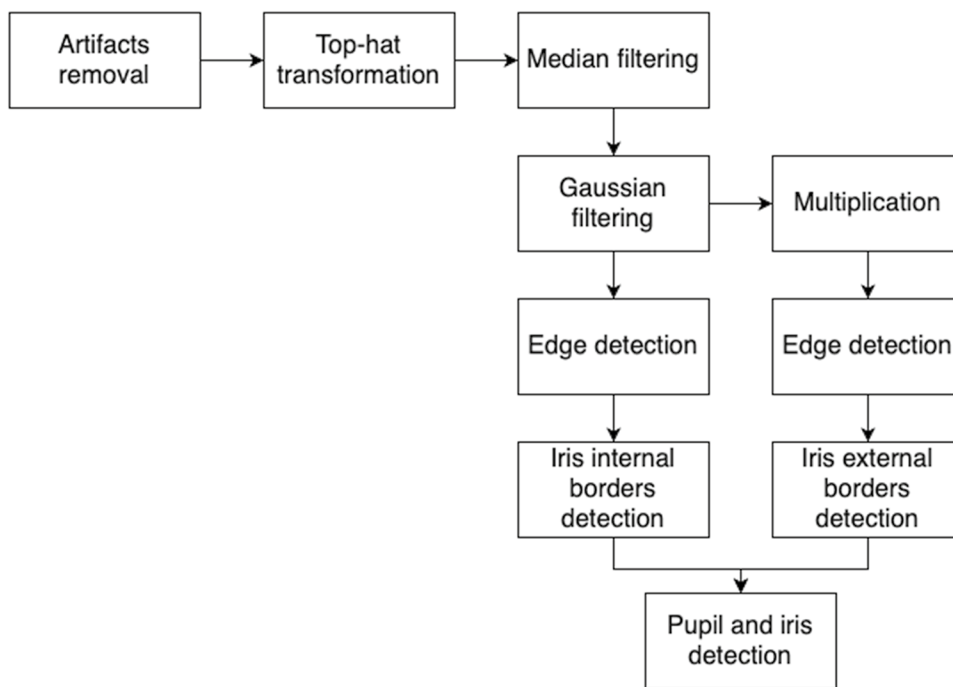


Fig. 1 Original image (a) and detected iris (b)

Fig. 2 Steps of feature extraction stage



the most significant iris points have been strengthened. (It is connected with the fact that the proposed operation can highlight the most important parts of the processed image.) This step allowed to observe them even by human eye. The images after normalization and after histogram equalization are presented in Fig. 3.

The third stage of the proposed algorithm was connected with the removal of unnecessary elements from the analyzed sample. The authors considered here some additional pixels that can form a kind of noise. For this aim, we used well-known algorithm that is median filtering. By this step, we got clear image without any additional distortions. During this stage, we also considered diversified possible solutions—for example, one of them was Gaussian filtering. However, on the basis of the results obtained in the further steps of our idea, the final results were much clearer when simple median filtering was used rather than any other tested algorithm. (We think here about higher accuracy of human iris-based identity recognition.)

In the next step, we used Gabor filter. This algorithm is a well-known linear filter for extraction information about

edges. We used it due to its efficiency and high accuracy. In the case of our idea, this datum was connected with the most important parts of the analyzed iris. Images after distortions removal and edges detection are presented in Fig. 4.

As the last step of our solution, we obtained information about frequencies occurring in image with discrete fast Fourier transform (DFFT). It was calculated as in (1). The frequency distribution generated in this step is presented in Fig. 5a.

$$X_k = \sum_{n=0}^{N-1} e^{-2\pi i k \cdot (\frac{n}{N})} \cdot x_n \tag{1}$$

where x_n is an array, consisting of n pixel values of previously preprocessed iris image—obtained after Gabor filtering, that is transformed by d -dimensional vector of indices $n = (n_1, n_2, \dots, n_d)$ by a set of d nested summations. We can also say that it is composition of a sequence of d sets of one-dimensional DFT performed one-by-one dimension.

On the basis of [18], we know that the most important information is placed in the effective area of the

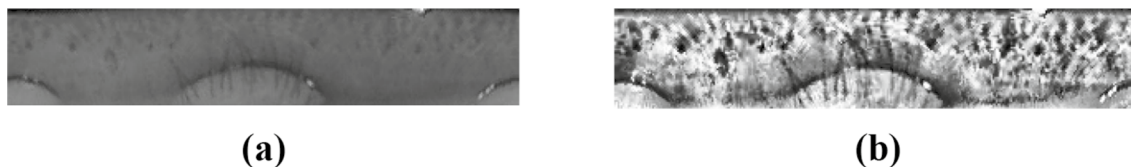
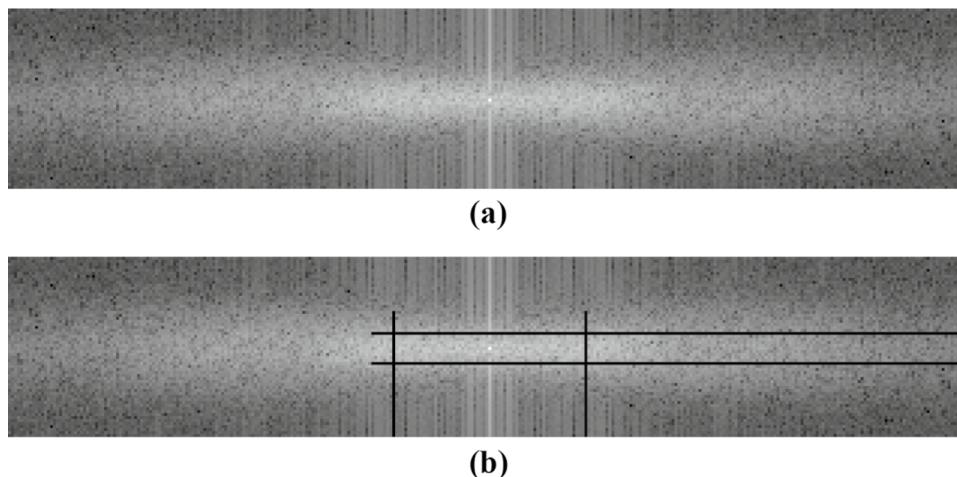


Fig. 3 Image after normalization stage (a) and after histogram equalization (b)



Fig. 4 Image after distortion removal with median filtering (a) and after edges detection with Gabor filter (b)

Fig. 5 Discrete fast Fourier transform of the sample after Gabor filtering (a) and the selected region (b)



transform—it means they are placed in 55% of obtained image width and 20% of its height. For further analysis, we used the data placed in the previously mentioned image region. The region is shown in Fig. 5b. However, we did not yet create final feature vector. To get the most important parts of each characteristic, we used principal component analysis (PCA) algorithm [19]. In fact, this solution allowed the authors to reduce the size of the dataset as well as to increase variance of each remain variable. After this operation, we calculated the final dataset that was then used during experiments. Finally, each sample was described by 200 parameters. During the experimental phase, it was observed that without feature reduction with PCA, the accuracy of the system was not satisfactory—it was nearly 20% less in comparison with the results obtained on the basis of reduced feature space with the previously mentioned method.

4 Results

During experiments, three main databases were used to evaluate algorithm accuracy. These are: UPOL [20], MMU [21] and CASIA-IrisV4 [22]. Moreover, the authors also used samples collected in Medical University of Białystok, Department of Ophthalmology. All experiments were made with 510 iris photographs. (Each person was described by 10 samples.) During all tests, the databases were divided into two main groups—training and testing. In the first set,

90% of samples were placed, whilst the rest of the database was moved to testing set. It has to be claimed that each experiment was repeated 100 times. Each set was created randomly. During the experiments, the authors also tested different splits as 50:50 (50% testing set and 50% training set, respectively) as well as 25:75, 75:25 and even 10:90. However, neither of them provided as satisfactory results as those obtained with the previously described split (90:10). The main observation regarding database sample splits is connected with the fact that much more samples are required to properly learn each classifier. It is why the 90:10 split provided the most accurate results.

Before the results of classification will be described, the authors would like to point out one more significant information. Each experiment was done on the basis of rules and recommendations connected with biometrics testing. The most important works in this topic are [23, 24]. In [23], different approaches to biometrics algorithms testing were shown, whilst [24] is connected with best practices connected with biometrics hardware testing.

During performed experiments, three well-known approaches were used. The first of them is k -nearest neighbors. This algorithm is classified as simple machine learning approach. In the case of this algorithm, the authors used an approach based on weights. Each weight was assigned to vector from the database on the basis of the distance between analyzed sample and vector from database. During experiment, different metrics were used—e.g., Manhattan,

Chebyszew, Euclidean, Minkowski and Bray–Curtis. The results obtained with this algorithm are shown in Table 1.

The results of the experiments in the case of k -nearest neighbors have shown that the most important for such solution is the way in which the database was divided. The authors would like to claim that this algorithm can be used in real environment due to its simpleness, efficiency as well as accuracy. The best result reached more than 92% of accuracy.

Support vector machine (SVM) is the second algorithm used for classification. Sample representation in 2D space is presented in Fig. 6. This algorithm was also selected due to its high efficiency. Moreover, the authors also proven its usefulness in their previous research [25]. During experiments, the authors observed that linear classification is much

more accurate than nonlinear. It is the opposite conclusion to the one we made in the case of retina. The best result obtained with this algorithm was 98%, whilst the average one is 86,6%. Once again, it has to be claimed that iris recognition with SVM as a classifier can be used in real environment. As it was in the case of k -NN, this approach also is simple and efficient. Moreover, it can also guarantee high accuracy results.

The third algorithm used for classification is artificial neural network (ANN). The scheme of the network is presented in Fig. 7. It is a simple network that consists of four layers. The first of them (input) consists of 200 nodes. (It is connected with the number of parameters obtained after pre-processing stage.) Next two layers consist of blocks responsible for data normalization, ReLu activation and dropout. Each block output consists of 720 neurons. The last layer is activated with Softmax function. Its main aim is connected with classification (51 neurons due to number of classes). The summary of nodes number and dropout values is presented in Table 2. It also has to be claimed that the authors used Adam algorithm for learning process optimization. At the beginning, learning rate was equal to $1e-4$, whilst decay parameter was $1e-6$. The network was learned in 100 epochs. The best classification result was 94.1%, whilst the average one equals 78.7%.

During experiments, the authors also considered diversified classification algorithms. For example, these were evolutionary algorithms and deep convolutional neural networks. Both these solutions did not provide satisfaction results. In the case of the second classifier, the authors think that the number of samples in the database was too low.

Table 1 k -nearest neighbors results

Selected metric	Parameter k	Average recognition rate (%)	The best recognition rate (%)
Euclidean	5	76.8	92.2
Euclidean	10	77.5	88.2
Manhattan	5	75.5	88.2
Manhattan	10	76.2	90.12
Chebyszew	5	41	58.8
Chebyszew	10	39.8	60.9
Minkowski	5	76.8	92.2
Minkowski	10	77.5	88.2
Bray–Curtis	5	81.6	96
Bray–Curtis	10	82.8	92.2

Fig. 6 Sample representation in two-dimensional space

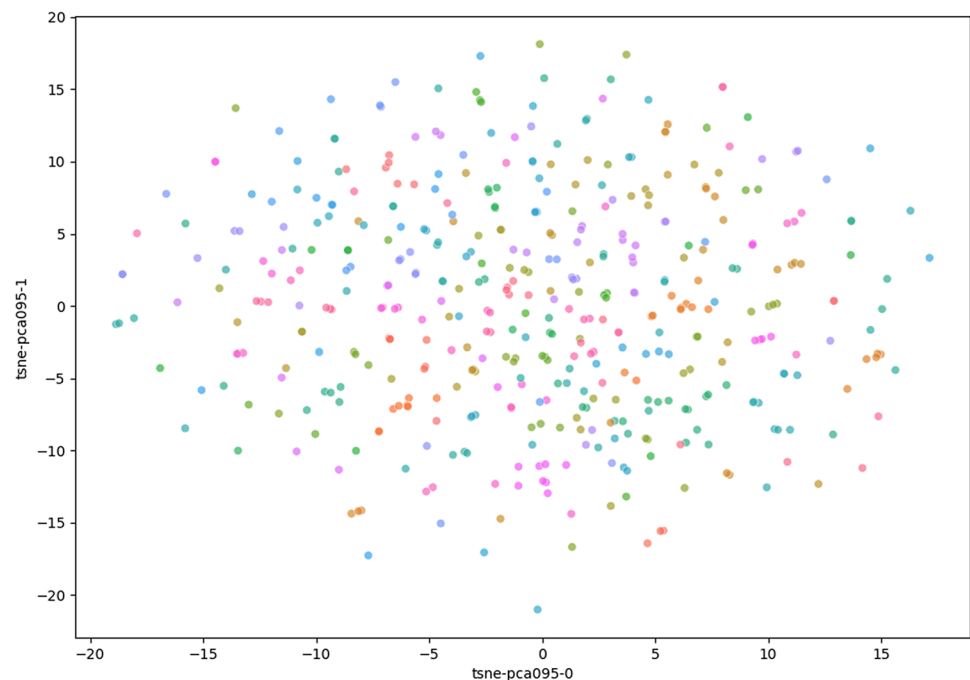


Fig. 7 Scheme of artificial neural network

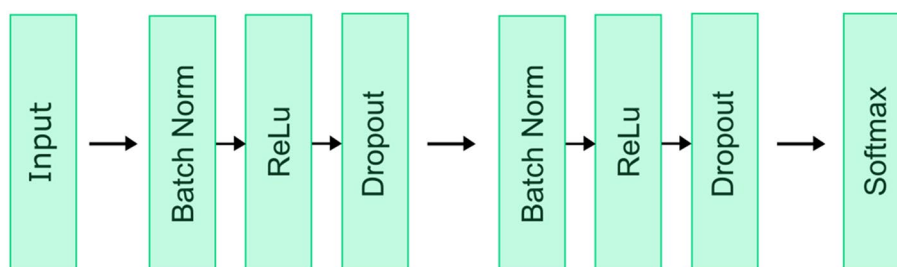


Table 2 Time needed to obtain the results with selected modules

Layer	Number of neurons	Dropout value
1	200	N/A
2	720	0.5
3	720	0.5
4	51	N/A

Table 3 Summary of the experiments

Method	Recognition rate (average/the best)
<i>k</i> -nearest neighbors	82.8%/92.2%
Support vector machines	86.6%/98%
Artificial neural network	78.7%/94.1%

Probably, this solution can guarantee much more precise results when samples' number was much more enlarged.

Before the results of the experiments will be concluded, the authors would like to claim that each algorithm was implemented by their own with Python programming language and frameworks that are available for this language. This environment was used because it provides multiple, diversified tools connected with machine learning and artificial intelligence as well as each operation can be implemented even with a couple lines of code. Moreover, the authors selected *k*-nearest neighbor, SVM and neural networks due to their simplicity and efficiency observed in the previously performed experiments (with diversified biometrics images and samples). Each method is also easy to implement with hardware designing languages such as VHDL. For future work, the authors would try to move their approach into FPGA-based solutions to check whether further acceleration is possible.

The summary of the experiments is presented in Table 3. The authors observed two main parameters connected with each algorithm. The first was the average value of the proposed classification accuracy. It was calculated on the basis of all observed results (their sum) divided by number of experiments (in each case it is 100). The second parameter is called "The best." It is the most precise result for each

algorithm individually observed in the collective set of all gathered accuracies.

It has to be claimed that the most precise results were observed in the case of support vector machine algorithm. This algorithm accuracy reached 98% (in the case of the best result), whilst the average recognition rate was 86.6%. These results are satisfactory and can guarantee proper recognition rate in the case of the implementation in real environment. Of course, to use this solution for security of sensitive data, some additional modules have to be provided.

The other two methods also reached interesting results. Especially it is observable in the case of *k*-NN method. Really simple algorithm that only compare proper feature vectors provided satisfactory results. As it was claimed before this solution can also be used in real environment while maintaining the same assumption as in the case of SVM.

5 Conclusions and future work

During the last few years, one can easily observe that human identity recognition based on biometrics was made one of the top technologies. In particular, it is observable in the case of mobile devices where face or fingerprint is used. However, in the next few years, iris can take their place. It is connected with the fact that novel devices have much more precise cameras as well as iris is really hard to spoof. On the basis of diversified sources, one can claim that iris can be described by more than 250 specific elements. It is much more than in the case of fingerprint or face.

The idea proposed in this paper has one specific goal. It is connected with creation of efficient and accurate iris-based human recognition algorithm that will not need specialized components or high computing power. It is why the authors used discrete fast Fourier transform components selected by principal component analysis (PCA) algorithm. Each user was described by 10 samples. Feature vector that represents each sample consisted of 200, the most informative parameters. On the basis of observations made during experiments, we can claim that it is clearly possible to get satisfactory accuracy results when feature vector consists of these values only. The most precise results were obtained with support vector machine (SVM) algorithm. However, two other tested

solutions (k -nearest neighbors and artificial neural network) also provided results by which we can claim their usability in the real environment. Each classification algorithm was tested with the database consisting of 510 samples. Training set and testing set were divided in the ratio of 90% to 10%.

As the future work, we would like to simplify our algorithm for mobile devices (as smartphones) or embedded systems (e.g., based on ARM microcontrollers). On the other hand, we would like to precisely test some other classification algorithms as deep convolutional recursive neural networks. However, to deal with such task we have to enlarge our database. The authors are working under collection of much more samples—at least 1000 of additional images have to be added to the database. In the future, we will also try to implement multimodal biometrics system with our iris algorithm. This experiment will provide us an evidence whether the multimodal solution can guarantee better recognition in short time (or comparable to the time needed in the case of iris).

Acknowledgements This work was partially supported by grant W/WI-IIT/2/2019 and subvention for scientific work for Institute of Technical Informatics and Telecommunications WZ/WI-IIT/4/2020 from Białystok University of Technology and funded with resources for research by the Ministry of Science and Higher Education in Poland.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- <https://www.cybintsolutions.com/cyber-security-facts-stats/>. Accessed 2 Jan 2021
- Sun H-M, Chen Y-H, Lin Y-H (2012) oPass: a user authentication protocol resistant to password stealing and password reuse attacks. *IEEE Trans Inf Forensics Secur* 7(2):651–663
- Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofing using print attack. In: *IEEE 2014 22nd international conference on pattern recognition*, Stockholm, Sweden, 24–28 August 2014. <https://doi.org/10.1109/ICPR.2014.296>
- Daugman J (2004) How iris recognition works. *IEEE Trans Circuits Syst Video Technol* 14(1):21–30
- Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA (2019) A fast iris recognition system through optimum feature extraction. *PeerJ Comput Sci* 5:184
- Ouda O, Chaoui S, Tsumura N (2020) Security evaluation of negative iris recognition. *IEICE Trans Inf Syst* 103(5):1144–1152
- Arora S, Bhatia MPS (2020) Presentation attack detection for iris recognition using deep learning. *Int J Syst Assur Eng Manag*. <https://doi.org/10.1007/s13198-020-00948-1>
- Mohammed NF, Ali SA, Jawad MJ (2020) Iris recognition system based on lifting wavelet. In: Mallick P, Balas V, Bhoi A, Chae GS (eds) *Cognitive informatics and soft computing*. Springer advances in intelligent systems and computing, vol 1040, pp. 245–254. Springer, Berlin
- Jenadeleh M, Pedersen M, Saupe D (2020) Blind quality assessment of iris images acquired in visible light for biometric recognition. *Sensors* 20(5):1308
- Trokielewicz M, Czajka A, Maciejewicz P (2020) Post-mortem iris recognition with deep-learning-based image segmentation. *Image Vision Compu* 94:103866. <https://doi.org/10.1016/j.imavis.2019.103866>
- Jalilian E, Uhl A, Kwitt R (2017) Domain adaptation for CNN based iris segmentation. In: *IEEE proceedings of 2017 IEEE international conference of the biometrics special interest group (BIOSIG)*, Darmstadt, Germany, September 20–22, 2017. <https://doi.org/10.23919/BIOSIG.2017.8053502>
- Hofbauer H, Jalilian E, Uhl A (2019) Exploiting superior CNN-based iris segmentation for better recognition accuracy. *Pattern Recognit Lett* 120:17–23
- Roy K, Bhattacharya P (2006) Iris recognition with support vector machines. In: Zhang D, Jain A (eds) *Proceeding advances in biometrics, international conference, ICB 2006*, Hong Kong, China, January 5–7, 2006, Springer lecture notes in computer science, vol 3832, pp 486–492.
- Minaee S, Abdolrashidi A (2019) DeepIris: iris recognition using a deep learning approach. [arXiv:1907.09380](https://arxiv.org/abs/1907.09380) [cs.CV]
- Arora S, Bhatia M (2018) A computer vision system for iris recognition based on deep learning. In: *IEEE proceedings of 2018 IEEE 8th international advance computing conference (ACD)*, Greater Noida, India, December 14–15, 2018. <https://doi.org/10.1109/IADCC.2018.8692114>
- Bangare S, Dubal A, Bangare P, Patil S (2015) Reviewing Otsu's method for image thresholding. *Int J Appl Eng Res* 10(9):21777–21783
- Prashanth CR, Shashikumar DR, Raja KB, Venugopal KR, Patnaik LM (2009) High security human recognition system using iris images. *Int J Recent Trends Eng* 1(1):647–652
- Miyazawa K, Ito K, Aoki T, Kobayashi K, Nakajima H (2006) A phase-based iris recognition algorithm. In: Zhang D, Jain A (eds) *Proceedings of advances in biometrics, international conference, ICB 2006*, Hong Kong, China, January 5–7, 2006, Springer lecture notes in computer science, vol 3832, pp 356–365
- Mishra S, Sarkar U, Taraphder S et al (2017) Multivariate statistical data analysis—principal component analysis (PCA). *Int J Livestock Res* 7(5):60–78
- <http://phoenix.inf.upol.cz/iris/>. Accessed 11 Jan 2020
- <http://andyzeng.github.io/irisrecognition>. Accessed 11 Jan 2020
- <http://www.cbsr.ia.ac.cn/china/Iris%20Databases%20CH.asp>. Accessed 15 Dec 2020
- Moore B, Iorga M (2009) Biometrics testing. *NIST handbook* 150-25
- Mansfield AJ, Wayman JL (2002) Best practices in testing and reporting performance of biometric devices. Centre for Mathematics and Scientific Computing, National Physical Laboratory. <http://www.idsystgroup.com/ftp/BestPractice.pdf>. Accessed 15 Jan 2020
- Szymkowski M, Saeed E, Omieljanowicz M, Omieljanowicz A, Saeed K, Mariak Z (2020) A novelty approach to retina diagnosing using biometrics techniques with SVM and clustering algorithms. *IEEE Access* 8:125849–125862. <https://doi.org/10.1109/ACCESS.2020.3007656>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.