The Vaccine's QR Code is in Your Eyes

Catalin Lupu, Corneliu-Octavian Turcu, Cornel Ventuneac and Vasile-Gheorghiță Găitan

"Ștefan cel Mare" University of Suceava, Romania

Summary
COVID-19 disease, caused by the SARS-CoV-2 virus, has led to many changes in the movement of people in different environments or even between different countries. Vaccines began to be administered more than a year after the pandemic has started. Following the administration of the vaccine, various ways were sought to identify the vaccinated people very quickly, in order to allow access to various areas, such as supermarkets or secure areas at airports. Thus, digital certificates were issued for attesting the vaccination, testing or recovery of that person. These certificates contain a QR code that can be scanned using an application installed on a mobile device. Research has sought to identify a more secure way to identify the holders of such a certificate. After vaccination, we consider it's useful to insert the biometric data of the iris or fingerprint in a national or international database, from where it can be accessed by all institutions authorized to verify the validity of such a certificate. During the research, the human iris was taken as a biometric feature, trying to find ways to scan it in real time and without a great interaction of the user with the video capture device. One of the biggest problems with such an approach is the exact connection between the person whose iris was scanned and the proof of having a COVID digital certificate. The idea was to replace the need to hold a certificate in printed or digital form with the image of the human iris, which in polar coordinates is quite similar to that of a QR code.

Keywords: *iris recognition, COVID-19, SARS-CoV-2, vaccination, digital ceriticate*

1. Introduction

The first coronavirus infections were announced in late 2019 in Wuhan, the capital of the Hubei region of China. The disease, called COVID-19, is caused by a virus called SARS-CoV-2, which means "severe acute respiratory syndrome coronavirus 2". The first coronavirus to produce SARS caused an epidemic in 2002-2004.
In principle, coronaviruses are a group of RNA viruses, which cause diseases in mammals and birds, manifested mainly by respiratory infections, which can range from insignificant to very important, some becoming lethal.
The main symptoms of coronavirus infection range from fever, cough, fatigue, loss of taste and smell, sore throat and severe seizures, such as respiratory failure, which often requires specialist care in the ICU (Intensive Care Unit).

Manuscript received April 5, 2022
Manuscript revised April 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.4.70

Given the huge increase in the number of people infected with SARS-Cov-2, the World Health Organization (WHO) has declared a public health emergency of international interest on 30 January 2020 and a pandemic on 11 March 2020. The WHO, founded on April 7, 1948, is headquartered in Geneva, Switzerland and is an international organization whose role is to maintain and coordinate the health of the world's population.
Healed people normally develop specific antibodies, which will protect the body from further reinfection or make it easier to bear, if it does occur. The concentration of antibodies decreases over time, and at some point, may even be insufficient to protect people who have been infected in the past.
This is one of the reasons why it has been tried since the beginning of this disease to find a vaccine that stimulates the immune system to produce antibodies specific to this coronavirus. Another reason is to provide antibodies to people who have not been through the disease and thus do not have natural antibodies.
The vaccines found were very helpful in preventing SARS-CoV-2 infection or, if the infection did occur, its symptoms were much milder than if the vaccine had not been given. In principle, the process of finding vaccines went in two directions: first, the use of a messenger RNA, which will cause the immune system to produce specific antibodies, and a classic method, which involves the use of inactivated viruses, which the body human recognizes them and against whom he tries to fight, while creating immunity. In the future "meetings" with the "intruder", this will be recognized and annihilated by the body.
As a result of vaccination, testing using RT-PCR or passing through the disease, the competent authorities in each country have issued certain certificates attesting this thing, in order to be able to differentiate people at lower risk of infection and transmission from others. In the first phase, vaccination certificates were issued in the countries of the European Union containing the data of the vaccinated person, the type of vaccine and the date on which it was administered, the dose number, the expiry date of the vaccine and information about the digital certificate with which that document was signed. This digital document could be printed for presentation to the requesting authorities. Subsequently, a QR code was generated by people who were vaccinated, tested, or

passed through the disease. In this way, the data could be read more easily using mobile devices, while increasing the security of this certificate.
This article will present a much more interesting approach to using the QR code, by scanning the iris of the person concerned, in order to validate its presence in a national or international database, created to be able to check in real time the situation of each person in part.

2. Theoretical Consideration

In this paragraph it will be presented the two aspects that will be used in the research conducted.

2.1. QR code generated for a test, vaccination or cure certificate

In fig. 1 it can be seen the QR code generated as a result of going through the disease. The QR code green check-mark was intentionally placed for reasons of personal data protection. It does not normally appear on the QR code.

Fig. 1. The digital certificate with the QR code issued for a person who has gone through COVID-19 disease

In Romania, the generation of the vaccination certificate and implicitly of the QR code is done by accessing the web address “https://certificat-covid.gov.ro”. After an email address is entered, a link will be received to this email for the connection to the application. After entering the personal data, the digital certificate containing the QR code will be generated, as shown in fig. 1.
When someone needs to check the QR code, he/she can use a dedicated app for that. In Romania, the application is called "Check DCC" and can be downloaded from the Google Play Store using the name "ro.sts.dcc". When the application is installed, it will be synchronized with the national backend, in order to successfully identify the QR codes, which contain a code that will be decrypted by the application, using a specific encryption key. In fig. 2 shows a photo of the application, which shows the successful verification of the certificate in Figure 1, after it has been photographed and processed. The application does not allow the execution of screen shots, because it is intended to be used only for validation or invalidation of the QR code, without the processed data to be stored on the local device. This figure shows that the validity limits of the scanned digital certificate appear. If all the data is valid, the application is colored in green and people can be allowed access in certain places, but if the certificate is not valid the application is colored in red and thus the permit is refused.

Fig. 2. Data read from the previous QR code

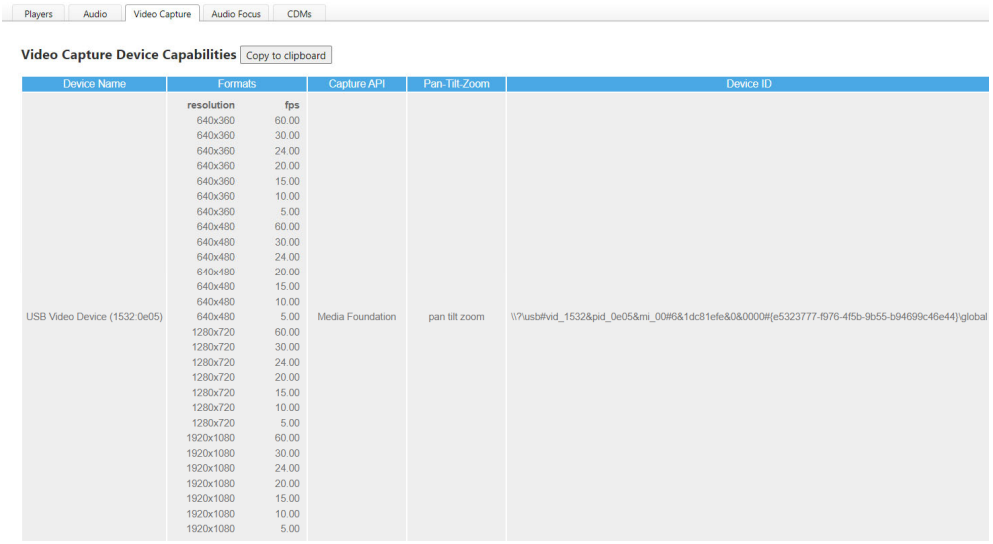
2.2. General information on the recognition of people using iris biometrics

A classic biometric system involves several steps, from taking the image from the camera to making a decision to enter the database or compare with other samples. In the first phase, an image of the iris and implicitly of the face is taken, of an acceptable quality, in order to extract appropriate samples from it. Samples are evaluated and, if they are not of the appropriate quality, it is possible to reject the captured image if sufficient data cannot be extracted from it. In this case, it returns to the previous step, when taking the image again. If sufficient data can be extracted, then move on to the next step, namely the module extraction module. If a new user is registered, a new template will be generated and entered into the database for future use. If the system instead works in the identification or verification mode, then it will move to the next verification module. It will compare the extracted characteristics of the downloaded image with those existing in the database in order to formulate a decision of acceptance or rejection of the user. This happens in the last mode, the decision mode.
In the case of an iris recognition system, follow the steps below, in the order in which they are presented:
- **taking the image** from the camera for iris recognition, for example Razer Kiyo Pro, or uploading it from a file (for example from iris databases such as CASIA (Chinese Academy of Sciences - Institute of Automation), MMU, UBIRIS, etc.);
- **graphics processing**, which aims to improve the image taken from the camera or file; it is done by applying various filters, by equalizing the histogram or by other methods of image processing;
- **image segmentation -** after obtaining a processed image with a maximum of useful information, it will be segmented in order to obtain the center and radius of the pupil and iris;
- **image normalization** - after segmentation, the normalization of the iris region involves framing the circular region in a rectangle of constant size so that it can be compared with other existing templates in the database or in a neural network;
- **coding** - extracting the iris code for registration in a database or for recognition;
- **entering data in a database**;
- **matching** - in case of identification or verification it will be tried to determine if the presented image corresponds to any of the database, based on 1:1 comparisons (in case of verification, when additional information about the user is provided - the question can be asked: “Image X shown corresponds to user Y?”) or 1:N (in case of identification, when the whole database is queried in order to obtain data about the user related to the presented image - the question is “Who is the user who presented the image of iris X?”). In case of registration this matching module may be missing; however, a type 1:N check can be made in the database to identify if the user is already registered, thus eliminating the possibility for a single user to use different credentials for authentication.

3. Experimental Consideration

In our research, we used the high-performance Razer Kiyo Pro FullHD camera, which is shown in Figure 3. Figure 4 shows the main features of the camera, resulting from accessing the URL version 100.0.4896.75 in the Chrome browser: “chrome://media-internals/”.
The selected camera has the advantage of being able to deliver 1080p quality images at a frequency of 60fps. Also, the optical zoom can be software controlled. It is well known that the optical zoom is much more performant than the logical one. For iris recognition, a high-quality image is needed because we have to take the picture of a very small object, that might have been moving while taking the photo. This is why we need a professional camera to take a high-quality picture. Also, this camera has a high-performance adaptive light sensor (for superior imaging in any lighting conditions), the lenses are wide-angle with adjustable FOV and has many flexible mounting options. Traditionally, the image was taken in near infra-red light, but with the performance of this camera we could manage to do successful iris recognition in normal light.

Fig. 3. Camera Ryzen Pro



Players | Audio | Video Capture | Audio Focus | CDMs

Video Capture Device Capabilities Copy to clipboard

Device Name	Formats		Capture API	Pan-Tilt-Zoom	Device ID
	resolution	fps			
	640x360	60.00			
	640x360	30.00			
	640x360	24.00			
	640x360	20.00			
	640x360	15.00			
	640x360	10.00			
	640x360	5.00			
	640x480	60.00			
	640x480	30.00			
	640x480	24.00			
	640x480	20.00			
	640x480	15.00			
	640x480	10.00			
USB Video Device (1532:0e05)	640x480	5.00	Media Foundation	pan tilt zoom	\\?\usb#vid_1532&pid_0e05&mi_00#6&1dc81efe&0&0000#{e5323777-f976-4f5b-9b55-b94699c46e44}\global
	1280x720	60.00			
	1280x720	30.00			
	1280x720	24.00			
	1280x720	20.00			
	1280x720	15.00			
	1280x720	10.00			
	1280x720	5.00			
	1920x1080	60.00			
	1920x1080	30.00			
	1920x1080	24.00			
	1920x1080	20.00			
	1920x1080	15.00			
	1920x1080	10.00			
	1920x1080	5.00			

Fig. 4. Features of the Razer Kiyo Pro camera from the Chrome browser

The main idea in our research was to use a high-performance camera (Razer Kiyo Pro) in order to take a very high-resolution image, which will be used to recognize people by the characteristics of the iris.

The use of iris recognition in the COVID-19 pandemic is presented in the papers [1] - [6]. Articles [7] and [8] provide information on verifying green certificates based on the iris image. Prevention of attacks on iris recognition can be found in papers [9] - [12]. For further information on real-time iris imaging, the articles [13] - [19] have been studied.

During the COVID-19 pandemic, the trend was to use contactless biometric systems, and of these I consider the iris to be the best feature, primarily due to the fact that the accuracy of human recognition is among the highest of all known characteristics. Facial recognition, for example, could not be taken into the account due to the use of the medical mask. The fingerprint can be taken from a short distance using a high-performance camera, but I find it much harder to do than in the case of the iris.

In our research, we have focused more on high quality image capture, because iris recognition can be done much better from a very clear image and a very high resolution. In the case of this camera, as can be seen in Figure 4, the maximum resolution is 1920x1680, at a frequency of 60 fps.

The main purpose of the article was to find a way to take the image in real time and automatically zoom in on that eye. In order to extract the maximum features of the iris from the captured image, we need a photo of extraordinarily good quality.

To test the camera's functionality and including iris recognition, the Visual Studio Code programming environment was used, where the "face-api" library was imported, being downloaded from github.com.

In Fig. 5 it is shown the Visual Studio Code interface with the code for “index.html”, and in Fig. 6 it can be seen a part of the code related to the JavaScript script "script.js".

Regarding the “index.html”, the following statements can be made:

- at the beginning are included the scripts “face-api.min.js” (from GitHub) and “script.js” (which contains the code of the application);
- a HTML table is created, in which three objects will be inserted: 1) a video taken from the video camera, 2) a “range” type control, which specifies the zoom level applied to the image and 3) a button for “Refresh” page

Part of the main script of the application ("script.js") is shown in Figure 6 and we can say the following:

- the “manualZoom” function performs the optical zoom of the device, depending on the “zoomVal” parameter. It usually ranges from 100 (no zoom) to 400 (4x zoom). The actual zoom is done by calling the following function:

```
track.applyConstraints({advanced: [ {zoom: zoomVal} ]});
```

- assignment "*input.value = zoomVal;*" moves the range control named “zoom” from “index.html” to the appropriate position;
- the zoom value is written in the console log, after which a 10ms sleep is executed.

When the browser starts downloading video images from the camera, it checks if the camera has the zoom facility, and if it does not exist, no further processing will continue (`if (! ('Zoom' in settings)) {`). In Figure 4, for the camera features, it can be seen that in the “Pan-Tilt-Zoom” column all 3 values are set, so the zoom value also appears in the settings, which means that the

camera can be used to run the application developed in Visual Studio Code programming environment.

With the help of the "face-api" application (https://github.com/justadudewhohacks/face-api.js) it can be found the coordinates of the left and right eye, the right and left eyebrow, the nose and the mouth, as well as the shape of the mandible. From all this data, we are only interested in the position of the eyes, to which we will try to zoom, followed by automatic focus. After that we have to take the image of the eyes in order to identify the iris. Using the other functions of the camera (*pan* and *tilt*), we can move the image horizontally or vertically, before zooming, in order to frame the irises as well as possible.

The system studied in this research has the main advantage that it adapts to the user. Classically, the image capture system is static and the user has to move in various positions so that the image capture of the iris is successful. In this case, the system detects the face, then in the face it finds the eyes and zooms and focuses towards this area, in order to successfully capture very high-quality images. It is recommended to have a light source next to the video camera, which will reduce the pupil and implicitly increase the size of the iris. The light source is also very useful for capturing the image with a very good brightness, given that the photos are no longer taken in infrared, but in natural light.

The iris image may be entered into a national or international database immediately after administration of the vaccine, after recovery from COVID-19 disease or after an RT-PCR test to determine the presence or absence of SARS-CoV-2 virus. Then, the user can go in front of such an imaging device and without his direct interaction the image of the iris will be taken, his situation will be checked in the respective database. After database check, a decision will be made on the continuation of his way. If the biometric data of the iris is found in the database, then it can be accessed in a store, airport or even in a country, and if it is not registered it will be asked for printed documents to prove whether it can continue the journey or not.

This also solves the problem of personal data protection (GDPR), because the “Check DCC” application presented above displays the name and date of birth of that person, which can be seen by the person making the verification. This is undesirable and often uncomfortable for people whose QR code is being scanned to allow or deny access to a particular area. The proposed application verifies that the iris is registered in the database and gives a ***Yes*** / ***No*** verdict, but without providing additional data on that person.

Even if there are not so many restrictions now, the idea is very good for any other event that will follow and will require the presentation of a document to validate access.

During the research, 1,734 images of the iris were taken from 10 people. From these images, 984 could be used, the rest being blurred or not having many features of the iris that could be extracted from them.

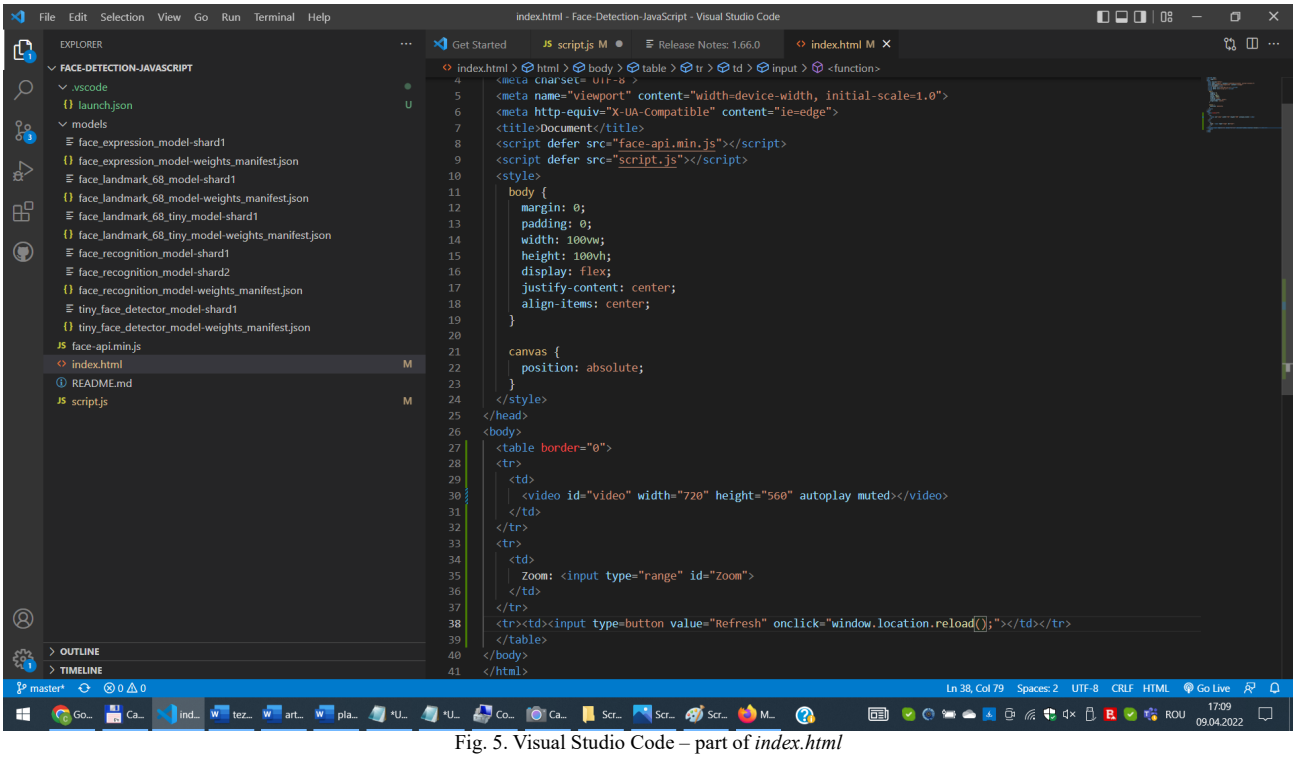


Fig. 5. Visual Studio Code – part of *index.html*

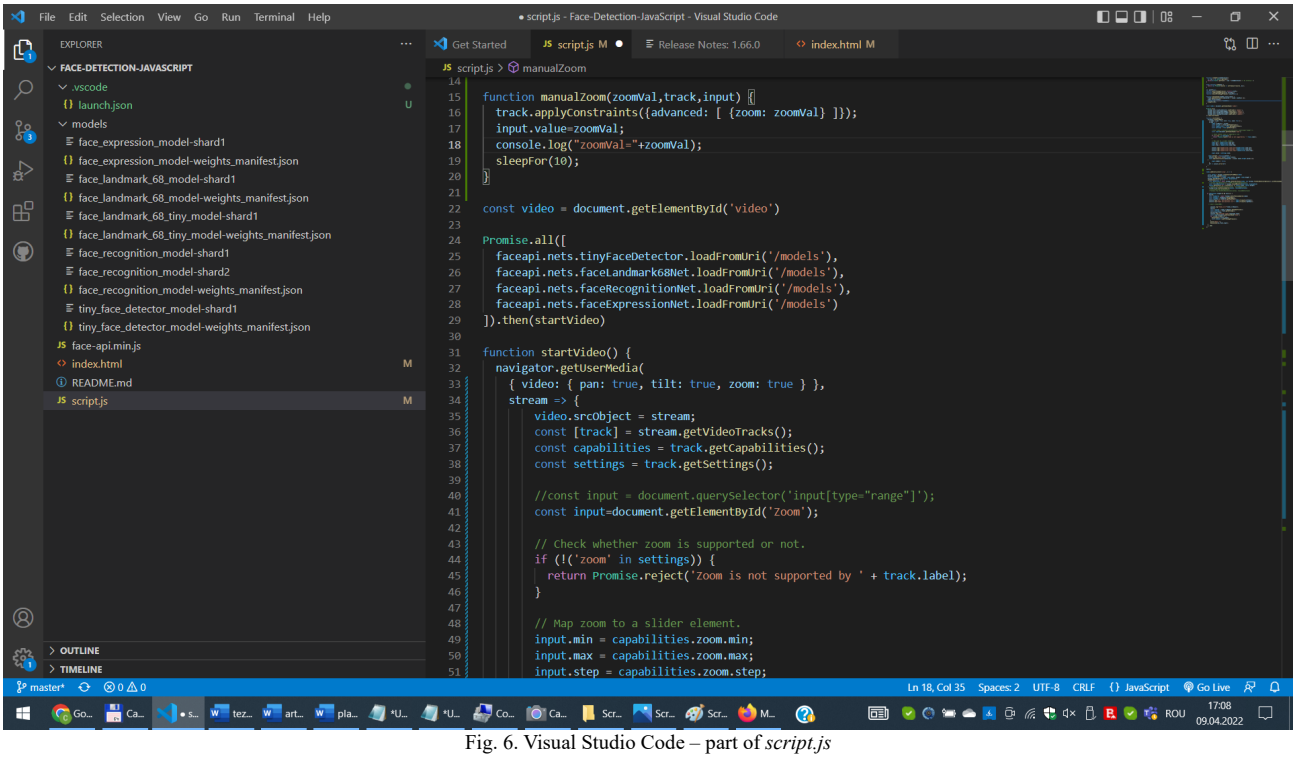


Fig. 6. Visual Studio Code – part of *script.js*

In fig. 7 it can be seen the page resulting from running the previous application, using the "Live Server" extension within Visual Studio Code. To do this, we have to right-click on "index.html", then "Open with Live Server". On the left it can be seen the face, with its features found using "face-api". On the right side it can be seen the console log with 2 positions of the iris of the right eye and the left eye. The position of each eye is given by 6 points and is obtained as follows:

```
const landmarks = await faceapi.detectFaceLandmarks(video)
const leftEye = landmarks.getLeftEye();
const rightEye = landmarks.getRightEye();
```

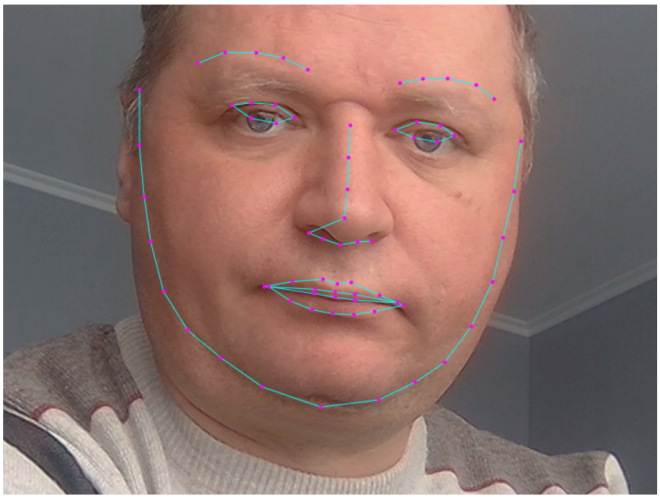


Fig. 7. The application and its console log

Biometrics can be integrated into the IIoT, both for authentication in cloud-based systems and for securing data transmission. Article [20] discusses the use of biometrics for authentication in IoT systems. In the case of the implemented application, encrypted information can be sent to an IIoT and we have to wait the response coming from it, in order to validate or invalidate the access of people in a certain place.

4. Conclusion

Research has led to the conclusion that iris recognition can be used successfully to allow or deny access to a person in a particular place or country. The idea was to use exclusively contactless biometric sensors, because people aren't very comfortable with the biometric sensor that has to be touched.
On the other hand, many more complex applications may be developed in the future, using even more biometric features to validate a person's identity with certainty.

Acknowledgment

This work is supported by the project ANTREPRENORDOC, in the framework of Human Resources Development Operational Programme 2014-2020, financed from the European Social Fund under the contract number 36355/23.05.2019 HRD OP /380/6/13 – SMIS Code: 123847.

References

[1] *"New Biometrics Trend in COVID-19"*, http://www.iritech.com/news-events/news/new-biometrics-trend-covid-19

[2] Liébana-Cabanillas, F., Muñoz-Leiva, F., Molinillo, S. et al. "*Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint",* Financ Innov 8, 22 (2022). https://doi.org/10.1186/s40854-021-00328-z

[3] *"Touchless authentication for the post-COVID world"*, https://www.hpe.com/us/en/insights/articles/touchless-authentication-for-the-post-covid-world-2010.html

[4] *"Biometric System Market with COVID-19 Impact Analysis by Authentication Type, Type, Offering Type, Mobility, Vertical & Region - Global Forecast to 2027*", https://www.reportlinker.com/p04397168/Biometric-System-Market-by-Authentication-Type-Component-Function-Application-and-Region-Global-Forecast-to.html

[5] *"2021 - How the pandemic pushes governments and the private sector to go further in the adoption of biometric technologies*", https://www.idemia.com/news/2021how-pandemic-pushes-governments-and-private-sector-go-further-adoption-biometric-technologies-2021-10-13

[6] Gomez-Barrero, Marta, et al. "*Biometrics in the era of COVID-19: challenges and opportunities*", arXiv preprint arXiv:2102.09258 (2021).

[7] Lupu, Catalin, and Corneliu-Octavian Turcu. "*Iris Recognition Used for the Implementation of a Green-Passports System Regarding the Vaccination against the SARS-CoV-2 Virus for the UE Citizens*", EIRP Proceedings 16.1 (2021), https://dp.univ-danubius.ro/index.php/EIRP/article/download/206/196

[8] Lupu, Catalin, and Corneliu-Octavian Turcu. "*Real-Time Iris Recognition of Individuals–an Entrepreneurial Approach*", EIRP Proceedings 16.1 (2021), https://dp.univ-danubius.ro/index.php/EIRP/article/download/208/197

[9] Rohit Agarwal, Anand Singh Jalal, "*Presentation attack detection system for fake Iris: a review*", Multimedia Tools and Applications (2021) 80:15193–15214, https://doi.org/10.1007/s11042-020-10378-7

[10] T. S R, A. Ojha, M. K and G. Maragatham, "*DeepIris: An ensemble approach to defending Iris recognition classifiers against Adversarial Attacks*", 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-8, doi: 10.1109/ICCCI50826.2021.9402404.

[11] M. Choudhary, V. Tiwari and V. U, "*Ensuring Secured Iris Authentication for Mobile Devices*", 2021 IEEE International Conference on Consumer Electronics (ICCE), 2021, pp. 1-5, doi: 10.1109/ICCE50685.2021.9427584.

[12] www.liveness.com

[13] Chen, Rui, Xirong Lin, and Tianhuai Ding. "*Liveness detection for iris recognition using multispectral images*" Pattern Recognition Letters 33.12 (2012): 1513-1519.

[14] Kanematsu, Masashi, Hironobu Takano, and Kiyomi Nakamura. "*Highly reliable liveness detection method for iris recognition*" SICE Annual Conference 2007. IEEE, 2007.

[15] Gragnaniello, Diego, Carlo Sansone, and Luisa Verdoliva. "*Iris liveness detection for mobile devices based on local descriptors*" Pattern Recognition Letters 57 (2015): 81-87.

[16] Czajka, Adam. "*Pupil dynamics for iris liveness detection*" IEEE Transactions on Information Forensics and Security 10.4 (2015): 726-735

[17] Hematian A., Chuprat S., Manaf A.A., Yazdani S., Parsazadeh N. (2013) "*Real-Time FPGA-Based Human Iris Recognition Embedded System: Zero-Delay Human Iris Feature Extraction*", The 9th International Conference on Computing and Information Technology (IC2IT2013). Advances in Intelligent Systems and Computing, vol 209. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37371-8_23

[18] E. P. Wibowo and W. S. Maulana, "*Real-Time Iris Recognition System Using a Proposed Method*" 2009 International Conference on Signal Processing Systems, 2009, pp. 98-102, doi: 10.1109/ICSPS.2009.9

[19] Dal Ho Cho, Kang Ryoung Park and Dae Woong Rhee, "*Real-time iris localization for iris recognition in cellular phone*", 6th ICSEAINPDC and First ACIS International Workshop on Self-Assembling Wireless Network, 2005, pp. 254-259, doi: 10.1109/SNPD-SAWN.2005.62

[20] Gaurav Meena & Sarika Choudhary (2019), "*Biometric authentication in internet of things: A conceptual view*", Journal of Statistics and Management Systems, 22:4, 643-652, DOI: 10.1080/09720510.2019.1609722

Cătălin LUPU received the B.Sc. degree from "Ștefan cel Mare University" from Suceava in 2003. He received the Dr. Eng. degree from the same University 14 years later, in 2017. He has been a research assistant and an university assistant at "Ștefan cel Mare" University from 2003 until now. His research interest includes biometric technologies, recognition of persons, iris and fingerprint matching and programming techniques.

Prof. Cornel Turcu was born in 1966 in Adjud, Romania. He received the B.Sc. and Ph.D. degrees in automatic systems, from the University of Iasi, Romania, in 1991, and 1999, respectively. He also holds a degree in Informatics (M.Sc.) from the University of Suceava, Romania. Since 1991, he has been with the Faculty of Electrical Engineering and Computer Science, University of Suceava (USV), where he is a full professor of System Theory and Intelligent Systems and also holds a joint appointment as head of Programmes Management Department. At USV he is also a supervisor for Ph.D. and M.S. theses. He has published over 70 research papers and 4 books. His research interests include intelligent systems, RFID systems and automatic control system design.

Cornel Ventuneac received the Bachelor Degree in Computer and Systems Science from "Stefan cel Mare University" from Suceava. He also received a master in Computer Science & Engineering from the same University. His research interest includes Internet of Things and local industrial networks. He is currently doing researches for his Ph.D. thesis in the field of Industrial Internet of Things.

Prof. Vasile-Gheorghiță Găitan has received his B.Sc. in 1984 and Ph.D. in 1997 from "Gheorghe Asachi" Tehchnical University of Iasi. Since 1990, he has been with the Faculty of Electrical Engineering and Computer Science, University of Suceava (USV), where he is a full professor of Microcontrollers. At USV he is also a supervisor for Ph.D. and M.S. theses. He has published over 60 research papers and 6 books. His research interests include intelligent systems, RFID systems, automatic control system design and microcontrollers.