**Systemy Logistyczne Wojsk**
Zeszyt 59 (2023)
ISSN 1508-5430, s. 287-298
DOI: 10.37055/slw/186380

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

**Military Logistics Systems**
Volume 59 (2023)
ISSN 1508-5430, pp. 287-298
DOI: 10.37055/slw/186380

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

# Electronic anti-theft protection for vehicles of people with special needs

# Elektroniczne zabezpieczenie antykradzieżowe dla pojazdów osób o szczególnych potrzebach

**Piotr Góral**
piotr.goral@put.poznan.pl, ORCID: 0000-0001-8999-693X
Division of Electronic Systems and Signal Processing, Institute of Automatic Control and Robotics, Poznan University of Technology, Poland

**Paweł Pawłowski**
pawel.pawlowski@put.poznan.pl, ORCID: 000-0001-5373-5148
Division of Electronic Systems and Signal Processing, Institute of Automatic Control and Robotics, Poznan University of Technology, Poland

**Wiktor Nowacki**
wiktor.nowacki@student.put.poznan.pl, ORCID: 0009-0002-8254-8717
Division of Electronic Systems and Signal Processing, Institute of Automatic Control and Robotics, Poznan University of Technology, Poland

**Jakub Wróbel**
wrobelkuba1455@gmail.com, ORCID: 0009-0007-8781-7281
Mechatronics Technician Profile, Józef Sieradzan Technical and Electronics School Complex in Kalisz, Poland

**Abstract.** The article presents an electronic anti-theft protection subsystem that was incorporated into the vehicle control system dedicated to people with special communication needs. The aim of the work was to design and test an electronic subsystem allowing for the acquisition and quick analysis of fingerprint images, checking whether they belong to the vehicle owner and generating a signal allowing the vehicle to be started. The following hypothesis was put forward: it is possible to use artificial intelligence for accurate, automatic

classification of fingerprint images acquired in a system with a single-chip microcomputer in order to identify a person. The research niche includes the use of biometrics in electronic anti-theft security adapted to people with special needs. This solution reduces the risk of theft and unauthorized use of special vehicles tailored to the owners' individual needs. The use of a commercial algorithm offered by the sensor manufacturer or the use of artificial neural networks for the classification of fingerprints was considered. The results of research on the accuracy of fingerprint recognition obtained from the developed subsystem are presented. The experiments performed based on the NASNetLarge artificial neural network model confirmed the possibility of achieving recognition accuracy for the test set of 99.99%. Additionally, practical aspects of the applicability of the presented device in an electric vehicle control system supporting the movement of people with physical and/or intellectual disabilities were discussed. The presented solution, after minor modifications, can be used in access security systems for protected rooms, as well as vehicles and military equipment.
**Keywords:** artificial intelligence, biometrics, electronic system, fingerprint sensor, anti-theft protection

**Abstrakt.** W artykule zaprezentowano elektroniczny podsystem zabezpieczeń przed kradzieżą, który został włączony w system sterowania pojazdu dedykowanego dla osób o szczególnych potrzebach komunikacyjnych. Celem pracy było zaprojektowanie i przebadanie podsystemu elektronicznego pozwalającego na pozyskanie i szybką analizę obrazów odcisków palców, sprawdzenie czy należą do właściciela pojazdu i generowanie sygnału zezwalającego na uruchomienie pojazdu. Postawiono następującą hipotezę: możliwe jest wykorzystanie sztucznej inteligencji do dokładnej, automatycznej klasyfikacji obrazów z liniami papilarnymi, pozyskanych w systemie z mikrokomputerem jednoukładowym, w celu identyfikacji osoby. Nisza badawcza obejmuje wykorzystanie obszaru biometrii w elektronicznych zabezpieczeniach antykradzieżowych dostosowanych do osób o szczególnych potrzebach. Rozwiązanie to pozwala na zmniejszenie ryzyka kradzieży oraz użytkowania przez osoby niepowołane pojazdów specjalnych dostosowanych do indywidualnych potrzeb właścicieli. Rozważono wykorzystanie algorytmu komercyjnego, oferowanego przez producenta czujnika lub wykorzystanie sztucznych sieci neuronowych celem klasyfikacji odcisków placów. Przedstawiono wyniki przeprowadzonych badań nad dokładnością rozpoznawania odcisków palców uzyskane z opracowanego podsystemu. Przeprowadzone eksperymenty w oparciu o model sztucznej sieci neuronowej NASNetLarge potwierdziły możliwość osiągniecia dokładności rozpoznawania dla zbioru testowego na poziomie 99,99%. Dodatkowo, omówiono praktyczne aspekty stosowalności przedstawionego urządzenia w systemie sterowania pojazdem elektrycznym wspomagającym poruszanie się osób z niepełnosprawnościami fizycznymi i/lub intelektualnymi. Zaprezentowane rozwiązanie, po niewielkich modyfikacjach, może zostać użyte w systemach zabezpieczeń dostępu do pomieszczeń chronionych, a także pojazdów i sprzętu wojskowego.
**Słowa kluczowe:** sztuczna inteligencja, biometria, system elektroniczny, czujnik linii papilarnych, zabezpieczenie antykradzieżowe

## Introduction

Over recent years, biometrics has become a much more extensive field than at the beginning of its existence. Researchers have begun to deal with various aspects of its development and are finding more and more innovative ways to use it. It is intensively developed in the field of medicine, where biometric systems combined with vision algorithms allow for the automatic identification of pathological lesions in the retina of the human eye (Marciniak et al., 2023), X-ray images of the lungs (Natashia, 2020), the recognition of cancer lesions in computed tomography images (Ma et al., 2020) and recognizing driver fatigue (Poliak et al., 2023). Application solutions dedicated to mobile phones are also available, allowing for deep learning of characteristic vein patterns from a 2D image obtained using a smartphone (Garcia-Martin and Sanchez-Reillo, 2021). Regardless of the current research on

the implementation of biometric systems, their inherent part is the use of methods that belong to the field of artificial intelligence (Berghoff et al., 2021). Automatic fingerprint recognition systems are widely known and are used in securing banking systems (Venkatraman and Delpachitra, 2008, Lisowska and Waściński, 2021) and in forensics (Rigano 2019). Other areas of application of biometric security include car anti-theft systems (Sadhukhan et al., 2017) and access control in buildings (Nexus Integra, 2023) or a convenient way of logging in to mobile devices (Priesnitz et al., 2023). The most common approach when designing biometric systems is to build hardware architecture and develop an identification or authorization algorithm from scratch. Recently, however, solutions that can be used have begun to appear in existing automation systems, as a subsystem improving the access control process (Bosch Security Systems 2023). A modern access control system can even be used to protect against theft of vintage cars. The value of vintage cars often equals or even exceeds the cost of purchasing a new vehicle. The electronic biometric subsystem is incorporated into the electrical circuit of the classic engine ignition system, preventing unauthorized engine starting. This type of modernization involves the use of an appropriate fingerprint sensor, which is mounted in a hidden but easily accessible place for the driver, and an electronic system that processes the signal representing the fingerprint. When the subsystem classifies the fingerprint as belonging to the owner, it generates a signal allowing the vehicle's engine to be started (Rajca and Sobczak, 2023).

Among the known methods used by biometric data processing algorithms, the main ones used are convolutional neural networks (CNN). Based on these architectures, both medical and fingerprint images can be processed (Jian et al. 2020). Algorithms from KNN (K-Nearest Neighnor) (Shamil et al. 2020) or others using SVM (Support Vector Machine) are also used to extract desired features from images. Recognition accuracy is therefore related to the accuracy of calculations that determine the degree of similarity that guarantees that the acquired fingerprints are recognized as the owner's fingerprints (Lula 2019). The use of convolutional neural networks allows for machine learning of feature representations and recognition. Deep learning architecture tune pre-trained model based on ImageNet (Minaee et al. 2023). Currently, research results are being published that indicate 100% accuracy in biometric image recognition using artificial intelligence algorithms. In (Nsaif et al. 2021), such accuracy was achieved thanks to the use of the Faster R-CNN (Region--based Convolutional Neural Networks) cascade with Gabor filters and the Baes model in eye detection. Multimodal experiments with CNN models also achieve high accuracies of 98.84% for the AlexNet and VGG-19 architectures (Wang 2022). However, such complex algorithmic structures require high computing power and an appropriate class of equipment.

This article presents the results of research on the accuracy of fingerprint recognition, which was carried out on an original photo database. The research was conducted based on

the NasNetLarge model and the Google Colab environment. The images were obtained as a result of the design and construction of an electronics subsystem containing a fingerprint sensor intended for inclusion in the vehicle start-up control system for people with special communication needs (Koniak et al. 2022, Hryciów 2022). Designed technological concept together with the research carried out, it constitutes a solution that, combined with the previously tested electric vehicle control system (Góral et al. 2019), allows us to isolate an extremely useful and important area of implementation of biometrics research.

## Electronic subsystem using a fingerprint sensor

Fingerprint sensors have been the subject of scientific research for many years and are being developed as part of research on the detection of biometric features and their practical application, e.g. in access control devices. There are various fingerprints detection methods: optical (analogous to taking a "photo" of a placed finger), capacitive (fingerprints create certain valleys on the skin and ridges that influence the change in capacitance), ultrasonic (changes are analyzed in the ultrasonic wave reflected from the fingertip), thermal (differences in depth between the ridge and valley of the fingerprint allow the line pattern to be detected by small measurable temperature differences on the thermistor array) (Nowak 2023), or even based on optical coherence tomography, which allows the internal copy of fingerprints to be imaged when the external skin is damaged (Korohoda et al., 2014).

The designed electronics subsystem uses a capacitive fingerprint reader from Waveshare (Waveshare 2023), which is presented in figure 1. The used capacitive sensor, due to its nature, cannot work in difficult environments - dusty, humid or with a dirty fingertip. The module can be used using a library to support the module in Python (for Raspberry Pi) and C++ (for Arduino or STM32).

Thanks to the use of available library functions, the program algorithm comes down to creating appropriate conditional statements. In a loop, Raspberry Pi waits for the sensor signal conditioning board to report that the measurement field has been touched. It is then possible to use the manufacturer's functions (closed source, which are contained inside the microcontroller within the sensor itself) or to send raw data (fingerprint images), which can be further processed, e.g. by testing other fingerprint analysis methods. Regardless of the chosen method, the result of processing the acquired data is the logical value "true" (the correct fingerprint of the vehicle owner) or "false" (the fingerprint of a stranger). Logical values are represented digitally through program variables. It allows for further processing of the obtained signal, which remains the responsibility of the programmer. The obtained signal, after software classification as owner/intruder, can be used to generate a sound or light signal or to control a relay.

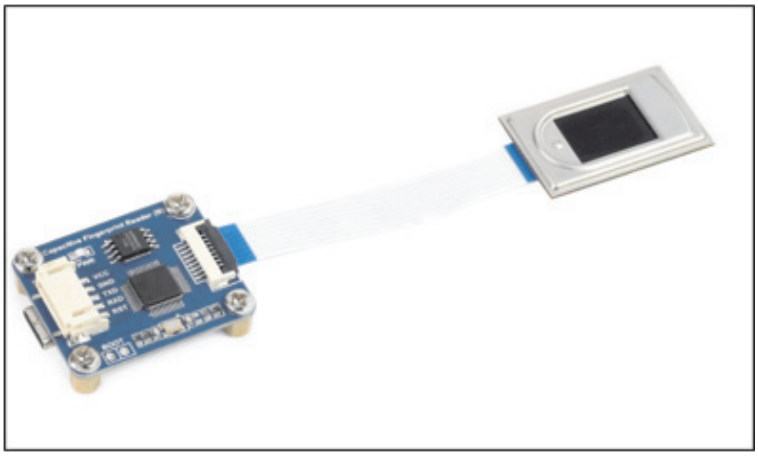

Fig. 1. Capacitive fingerprint reader
Source: Waveshare

Figure 2 shows a block diagram of the idea of using a capacitive fingerprint reader in an electronics subsystem containing a RaspberryPi microcomputer and an opto--isolated relay module. The presented electronics subsystem was developed as a concept for using an electric vehicle in the control system to support the movement of people with physical and/or intellectual disabilities, which includes a Siemens PLC controller in its hardware architecture (Koniak et al. 2022). In the presented concept, after activating the opto-isolated relay, a voltage signal of 24V is transmitted to the controller controlling the vehicle, which will take the appropriate action, e.g. allows/disallows to start the vehicle.

For preliminary experiments, a prototype system was assembled, shown in figure 3. In order to ensure the correctness of the software verification of the owner/ intruder fingerprint classification, sound and light signaling has been included. Turning on the green diode is identified with owner's fingerprint recognition. The obtained signal activates an opto-isolated relay, which transmits a signal to the PLC controller - permission to start the vehicle. The lighting of the red diode is identified with the recognition of the fingerprints of an intruder (potential thief). It activates an audible (alarming) signal and an opto-isolated relay transmitting a signal to the PLC controller - no permission to start the vehicle.

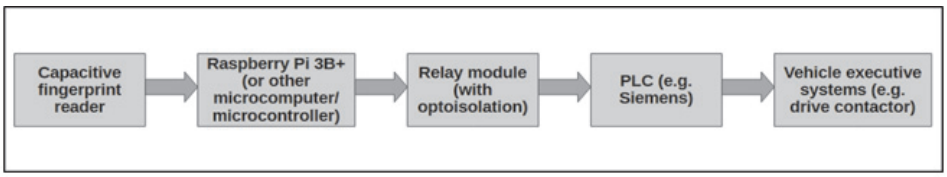


Fig. 2. An example concept of connections between individual components
Source: Own study

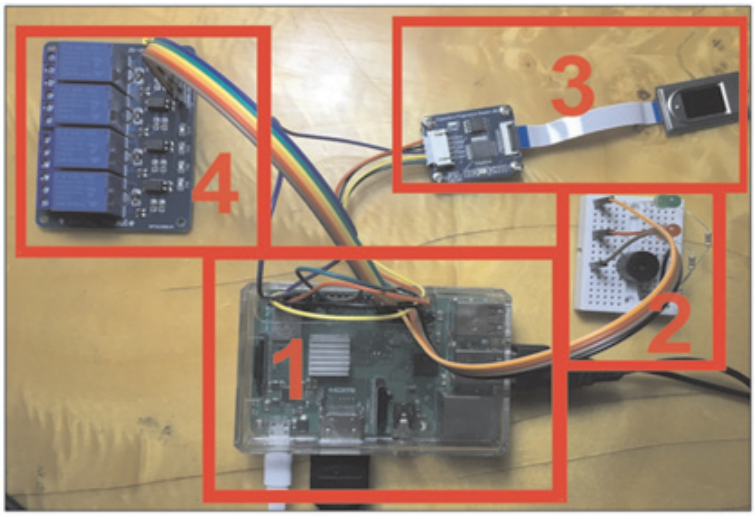


Fig. 3. Prototype of the system (1 - Raspberry Pi microcomputer with connected peripheral device cables; 2 - LEDs and buzzer as simple user-interface; 3 - actual Waveshare fingerprint sensor with a signal conditioning board; 4 - relay module)
Source: Own study

## Results of experimental studies

The designed electronics subsystem with a fingerprint sensor was used to conduct experimental research based on the convolutional neural network algorithm model called NasNetLarge. The acquired fingerprints were divided into two catalogs, each containing 1,000 photos. Catalogs of prints belonging to the owner and another person treated as an intruder (potential thief) were identified. Experimental tests were carried out using the Google Colab environment dedicated to machine learning due to the free provision of computing resources for educational purposes and graphic processors. Figure 4 shows sample images of the acquired fingerprints. These images were acquired in various lighting conditions, thus reflecting the actual conditions for

obtaining fingerprints on the target device (electric vehicle) where the capacitive fingerprint reader is to be installed.

Fig. 4. Sample images obtained from the electronics subsystem
Source: Own study

Then, a data augmentation technique was used on the acquired images, which consists in adding copies of them to the existing photos, which were subjected to various types of manipulation with random coefficients. This operation aims to avoid overfitting the convolutional neural network used and allows for expanding the existing training data set (Baby 2023). Figure 5 shows the resulting images subjected to the augmentation process - some transformations are visible, such as stretching, rotation and others.

Fig. 5. Sample images after augmentation surgery
Source: Own study

The accuracy results of fingerprint classification within 10 epochs (attempts to train the network) based on the NASNetLarge model are presented in the chart in figure 6. The „accuracy" parameter, i.e. accuracy, is calculated as the ratio of correctly recognized samples in relation to all samples that the network tried to recognize (Gad 2023). In order to prevent the phenomenon of model overfitting (Anon 2023)

and maintain reliability during testing, the photo database was also divided into training, validation and testing sets.

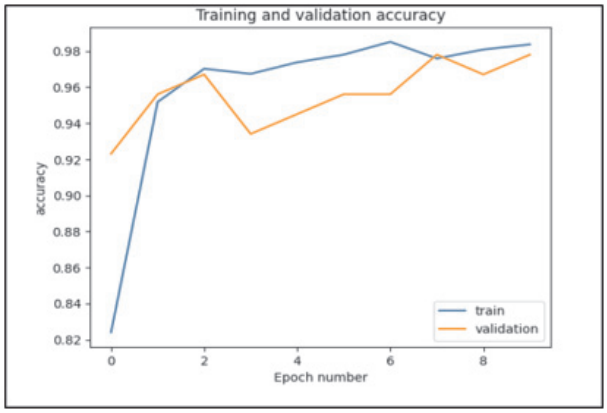


Fig. 6. Recognition accuracy plot for training and validation set
Source: Own study

The results of the sum of errors for the training and validation set are shown in figure 7. The „loss value" parameter - the loss function - is a coefficient trying to predict how often the network will make mistakes and it is one of the key values that determines the direction of evolution of the coefficient weights during learning process (Verma 2023).

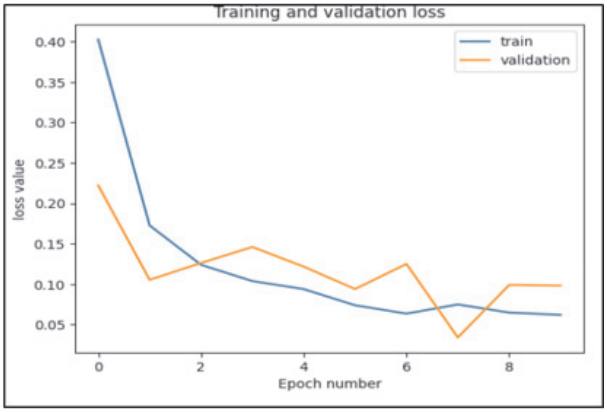


Fig. 7. The sum of errors for the training and validation sets
Source: Own study

## Conclusions

The presented solution allows us to connect the designed electronics subsystem with a fingerprint sensor to any PLC controller installed in a vehicle. We also presented a concept for using this solution in an electric vehicle adapted for people with special communication needs. This technology is intended to protect against theft or unwanted starting of vehicles by unauthorized persons, but in such a way that starting it by the owner - a person with special needs - is simple and does not cause difficulties.

The artificial convolutional neural network model was trained based on the author's database of fingerprint images obtained from the electronic anti-theft protection system. After 10 epochs, the network found relationships, details and nuances in the training data that allowed it to work with data that was not yet known.

After the training stage, the model used allowed to achieve recognition accuracy of 95.1% for the training set, 95.6% for the validation set and 99.99% for the test set. Data augmentation techniques were used, including multiple cross-validation, which means that each time a different part of the image database was used as a testing set. The obtained results of the sum of errors allow us to conclude that the training of the artificial network was completed at an adequate moment, i.e. when the network was neither undertrained nor overtrained.

The combination of the presented solutions allows for improved protection of vehicles adapted for the mobility of people with special needs and can be implemented in other areas. They are dedicated mainly to people with physical and/or intellectual disabilities, for whom the proposed solutions can strengthen their sense of security with specially adapted vehicles used. The scope of the presented research shows the useful use of artificial intelligence to improve the quality of life and can be expanded by using facial, eye or vein detectors.

It should be noted, however, that the applications of the proposed system are not limited only to issues related to vehicles dedicated to people with special needs, but (after adaptation) they can also be used in the field of access control, authorization of machine and equipment operators, or as a tool for efficient identification or quick confirming identity.

BIBLIOGRAPHY

[1] Anon., 2021. 7 Best Techniques To Improve The Accuracy of CNN W/O Overfitting. https://medium.com/mlearning-ai/7-best-techniques-to-improve-the-accuracy-of-cnn-w-o-overfitting-6db06467182f [24 September 2023].

[2] Baby, A. J. Building a CNN Model with 95% accuracy. https://www.analyticsvidhya.com/blog/2021/01/building-a-cnn-model-with-95-accuracy/ [24 September 2023].

[3] Berghoff, C., Neu M. and von Twickel A., 2021. The Interplay of AI and Biometrics: Challenges and Opportunities. Computer, vol. 54, no. 9, pp. 80-85, DOI: 10.1109/MC.2021.3084656.

[4] Anon., 2023. Bosch Security Systems, Biometric Access Control. https://www.boschsecurity.com/us/en/solutions/access-control-systems/biometric-access-control/ [24 September 2023].

[5] Gad, A. F., 2021. Evaluating Deep Learning Models: The Confusion Matrix, Accuracy, Precision, and Recall. https://blog.paperspace.com/deep-learning-metrics-precision-recall-accuracy/ [24 September 2023].

[6] Garcia-Martin, R. and Sanchez-Reillo, R., 2021. Deep Learning for Vein Biometric Recognition on a Smartphone. IEEE Access, vol. 9, pp. 98812-98832, DOI: 10.1109/ACCESS.2021.3095666.

[7] Góral, P., Pawłowski, P. and Dąbrowski, A., 2019. Wireless remote control system for an autonomous vehicle. Electrotechnical Review 2019, R. 95, 10, DOI: 10.15199/48.2019.10.25.

[8] Hryciów, Z., 2022. Bezpieczeństwo osób poruszających się na wózkach inwalidzkich w pojazdach silnikowych. The Archives of Automotive Engineering - Archiwum Motoryzacji, 97(3). https://doi.org/10.14669/AM/155001.

[9] Jian, W., Zhou, Y. and Liu, H., 2020. Lightweight Convolutional Neural Network Based on Singularity ROI for Fingerprint Classification. IEEE Access, vol. 8, pp. 54554-54563, DOI: 10.1109/ACCESS.2020.2981515.

[10] Koniak, K., Ciesielski, S., Buczkowski, K. and Przywara, Sz., 2022. Electric vehicle supporting the movement of people with physical and/or intellectual disabilitie, Competition project, Military University of Technology, Warsaw 2022.

[11] Korohoda, P, Dąbrowski A. and Pawłowski P., 2014. Optical Coherence Tomography for Fingerprint Acquisition from Internal Layer - A Case Study. Signal Processing Algorithms, Architectures, Arrangements and Applications, Poznań 2014.

[12] Lisowska, A. L. and Waściński, T., 2021. Bezpieczeństwo bankowości internetowej i mobilnej na rynku finansowym. Systemy Logistyczne Wojsk, 54(1). https://doi.org/10.37055/slw/140380.

[13] Lula, A., 2019. Ultrasound Systems for Biometric Recognition. Sensors 2019, 19, 2317. https://doi.org/10.3390/s19102317.

[14] Ma H, Liu ZX, Zhang JJ, Wu FT, Xu CF, Shen Z, Yu CH and Li YM., 2020. Construction of a convolutional neural network classifier developed by computed tomography images for pancreatic cancer diagnosis. World J Gastroenterol, 14;26(34):5156-5168, DOI: 10.3748/wjg.v26.i34.5156.

[15] Marciniak, T., Stankiewicz, A. and Zaradzki, P., 2023. Neural Networks Application for Accurate Retina Vessel Segmentation from OCT Fundus Reconstruction. Sensors 2023, 23, 1870, https://doi.org/10.3390/s23041870.

[16] Minaee, S., Azimi, E. and Abdolrashidi, A., 2019. FingerNet: Pushing The Limits of Fingerprint Recognition Using Convolutional Neural Network. https://arxiv.org/abs/1907.12956 [24 September 2023].

[17] Natashia, C., 2020. Chest X-rays Pneumonia Detection using Convolutional Neural Network. https://towardsdatascience.com/chest-x-rays-pneumonia-detection-using-convolutional-neural-network-63d6ec2d1dee [24 September 2023].

[18] Anon., 2023. Biometric recognition systems in buildings. https://nexusintegra.io/biometric-recognition-systems-buildings/ [24 September 2023].

[19] Nowak, K., 2023. How does a fingerprint reader work?. https://www.unicard.pl/news-jak-dziala-czytnik-linii-papilarnych [24 September 2023].

[20] Nsaif, A. K. et al., 2021. FRCNN-GNB: Cascade Faster R-CNN With Gabor Filters and Naïve Bayes for Enhanced Eye Detection. IEEE Access, 9, DOI: 10.1109/ACCESS.2021.3052851.

[21] Poliak, M., Beňuš, J., Hajduk, I. E., Demirci, E. and Nica, E., 2023. Test zmęczenia kierowców w transporcie drogowym towarów: badanie pilotażowe. The Archives of Automotive Engineering - Archiwum Motoryzacji, 101(3). https://doi.org/10.14669/AM/172910.

[22] Priesnitz, J., Huesmann, R., Rathgeb, C., Buchmann, N. and Busch, C., 2022. Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects. Sensors 2022, 22. https://doi.org/10.3390/s22030792 [24 September 2023].

[23] Rajca, N. and Sobczak, E., 2023. BIOMETRIC CAR ANTI-THEFT SECURITY IN A CLASSICAL IGNITION SYSTEM, Scientific Conference "21st century technology. Electromobility", Calisia Academy, Kalisz 2023.

[24] Rigano, C., 2019. Using Artificial Intelligence to Address Criminal Justice Needs. NIJ Journal 280, January 2019, https:// www.nij.gov/journals/280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.aspx.

[25] Sadhukhan, S., Acharyya, A. and Prasad, R., 2017. Car Security System using Fingerprint scanner and IOT. Indian Journal of Science and Technology. 10, 10.17485/ijst/2017/v10i40/109854.

[26] Shamil, M. A., Abdulelah, A., Ahmed, A., 2020. Multimodal Biometric System Iris and Fingerprint Recognition Based on Fusion Technique. https://www.researchgate.net/publication/340511996_Multimodal_Biometric_System_Iris_and_Fingerprint_Recognition_Based_on_Fusion_Technique [24 September 2023].

[27] Venkatraman, S. and Delpachitra, I., 2008. Biometrics in banking security: A case study. Information Management & Computer Security 16(4):415-430 doi:10.1108/09685220810908813.

[28] Verma, S., 2019. Understanding different Loss Functions for Neural Networks. https://shiva-verma.medium.com/understanding-different-loss-functions-for-neural-networks-dd1ed0274718 [24 September 2023].

[29] Wang, Y., Shi, D. and Zhou, W., 2022. Convolutional Neural Network Approach Based on Multimodal Biometric System with Fusion of Face and Finger Vein Features. Sensors 2022, 22, 6039. https://doi.org/10.3390/s22166039.

[30] Waveshare, Website of Waveshare module documentation https://www.waveshare.com/wiki/Capacitive_Fingerprint_Reader_(B) [24 September 2023].