Advances in Military Technology
Vol. 21, No. 2, 2026, pp. 463-479
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.02107

Facial Recognition Option at the Hungarian Technical Border Barrier

M. Majer*, and J. Káldos

Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Hungary

The manuscript was received on 13 March 2026 and was accepted after revision for publication as a case study on 26 September 2026.

Abstract:

The recognition of human faces is a constant need, as members of society identify each other mainly by their faces. Nowadays, when we have to face challenges, risks and threats, a need has arisen to automate the recognition of human faces. The possibility of digital facial recognition increases people's safety, because it can filter out one or more people who do not have the right to be in the place affected by the control. The Still Image Facial Recognition System has been operating in Hungary since 2017. The study presents the history of facial image analysis from a legal and practical perspective, as well as its use. It looks for areas where it is currently not working but would be useful.

Keywords:

facial recognition, identification, algorithm, technical border barrier

1 Introduction

People's desire for security requires them to be able to reliably identify a person who is using a service, arriving somewhere, moving somewhere, or being wanted [1]. In an average society, everyone has a photo ID, which in most cases is a passport, driver's license, ID card, or other document. When carrying out official procedures or entering countries, authorities check such a photo ID. This is how they decide that the person in the photo is actually there. Once identified, the cardholder can exercise the rights to which the document entitles them. Facial recognition is a dynamic process in which several features are determined. Identification methods are constantly evolving, both for the efficiency of citizens and companies, and for the benefit of official bodies.

An official organization, such as the police, can use facial recognition during criminal work to see if the face of a person in a photo is found in other records. In this way, the person's data can be determined based on the photo. Civilians can use facial

* *Corresponding author: Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Népszinház u. 8. Budapest, Hungary. E-mail: majermilan@gmail.com. ORCID 0009-0006-8451-5651.*

recognition when using home camera systems, but here it is necessary to upload a record in advance. In this way, doors can be opened after identification, without always having to carry a key or card. Identification increases the security of homes. Civilian companies can also use it when using camera systems, and here too a register must be uploaded. The system will then be suitable for monitoring the movement, entry and exit of employees. Identification increases security and profits, for example by using working hours effectively. Nevertheless, this study does not cover civilian applications.

2 The Process of Personal Identification Based on Facial Image Analysis

The best method for identifying people is biometric identification, which examines the unique, unchangeable, unforgeable, original characteristics of people [2]. Therefore, biometric data must always be unique, permanent, and of acceptable quality. Such data suitable for unique identification include fingerprints, irises, faces, and voices [3].

Human characteristics change continuously over time. Of course, the face also changes as we age. However, the unique characteristics of the human face always remain, so facial recognition can be used relatively continuously. The basic data required for facial image analysis is quick to obtain, as a photo or film can be taken relatively easily from a distance, and no physical contact is required. The analysis process is quick, provided that the appropriate records are available [4].

Face recognition processes can be divided into two groups. One group is still images, the other group is film recording, i.e. moving image analysis. In both methods, the currently recorded photo or film is compared with elements of images recorded in an existing registry. In the case of still image recognition, a finished photo is compared. In the case of moving image recognition, the comparison is made from a moving recording, for example, a recording taken during the operation of a camera [5].

Face recognition can be done in several ways. One way is verification, or checking, which the literature on the subject calls 1:1 analysis. In this case, the system compares one photograph with another to establish whether they depict the same person or two different people. In the other case, identification, or according to the literature, 1:N analysis is performed. Here, a photo is also compared, but with several photos in the registry to see if the person being searched for matches any of the people in the registry [6].

Two methods can be used to recognize a face. In one case, the features of the face are examined as a whole, using the similarities between the recorded and the examined face. In the other case, the system examines the shape and size of the recorded face and the elements on it, as well as their distance from each other. Elements on the face can be, for example, the mouth, earlobe, nose, eyes, eyebrows [7].

Facial recognition is also present in our homes; it is constantly developing. It does not necessarily require a full face, the system can also recognize people in sunglasses or a hat. Since the Covid epidemic, it can also recognize faces covered with masks. Of course, these systems are not official systems, but they are used as identification at home, for example, to unlock the phone screen. The best-known system is Apple Face ID. Another popular home facial recognition system is Google Photos, which helps organize stored photos. Apple Pay also allows electronic payments to be authorized only after the facial image has been recognized and identified. It is important that the user takes high-quality photos of themselves, scanned from multiple

positions, on the mobile phone before using facial recognition, as this will ensure the most secure identification.

3 International Perspectives on the Use of Facial Recognition Systems

Critically evaluating the suitability and legitimacy of such systems is challenging. The implementation of data protection regulations varies considerably across countries, ranging from complete prohibition to extensive deployment of facial recognition technologies. Furthermore, there is currently no harmonized legal framework governing the use of facial recognition within the European Union [8].

In the United States of America, micro and macro systems operate, in cities and states, but there is no uniform legislation. Mostly, with minimal differences, the authorities use the registration of photos of people with a driver's license or registered for committing a crime [9]. In China, the goal is to have the entire population registered in a registry that provides data for the facial recognition system [10]. In Japan, the system is already being used in a way that is suitable for large-scale events, such as sporting events. It helps with entry, controls movement in the area, and also achieves identification results independently. It is effective even when wearing sun-glasses or masks. It can also be used to check the body temperature of people entering a given place [11].

It can be said that facial recognition systems are operated or intend to be operated in almost all countries in the world [12]. Of course, only within legal limits, since illegally obtained data is useless in an official procedure in all developed countries [13].

4 The Legal Framework of the Hungarian Facial Recognition System in Relation to Law Enforcement Agencies

The primary legislation is the Act on the Facial Image Analysis Registry and the Facial Image Analysis System, which very clearly declares the concept of identification, the scope of those involved, the recording of data, and the provision of information [14]. The implementing legislation is the *Decree of the Minister of the Interior on the Detailed Rules for the Operation of the Facial Image Analysis System*, together with its annexes. This regulates the identification process [15].

The detailed rules for the facial image analysis are contained in a national police chief's order [16]. Of course, the domestic legislation on the subject generally complies with the 2018 EU General Data Protection Regulation (GDPR) [17]. which is closely related to the Act on Informational Self-Determination and Freedom of Information. In this, the protection of personal data is the primary concern [18].

Hungarian legislation (law, decree and instruction) defines in detail which bodies are authorized to use facial image analysis activities and for what purpose. Both the law enforcement bodies authorized to use them, and the expert institute may transmit facial images and perform facial image analysis activities exclusively for the purposes specified in the law, of course in full compliance with data protection rules. The legislation and human activity keep both the registry created from the photos and the analysis decisions under control, which is why the system is completely secure. Experts specialized in the activity carry out the comparative examination solely on the basis of anthropological characteristics. After that, only anonymous technical codes are returned to the body entitled to use the results in the hit list. It is important to note that the evaluation process must be independent of and completely free from influence

from all other factors. The expert cannot see any personally identifiable data belonging to the facial images. The analysts are also not provided with information on how the body requesting the analysis will use the results.

5 Implementation of the Analysis in Hungarian Law Enforcement Agencies

The Hungarian facial recognition system has been in use since 2016. It is called the Standing Face Recognition System (hereinafter abbreviated: 3AR). In Hungary, the 1:N method is used in such a way that the authorized law enforcement agency processes a photo on its own, closed network IT system, the Robotcop Neo Management and Case Processing System [19].

The first step in facial recognition is to upload the photo. After that, the uploaded photo and the request for identification are sent to the staff of the National Expert and Research Center, Facial Analysis Department [20]. The 3AR then analyzes the photo and determines relationships between the dimensions and the size, shape, and location of other parts of the face. It then generates a list of the most likely matching faces from the available records. The registry is currently managed by Idomsoft Private Limited Company [21].

The photos on the list are then manually compared by several employees, independently of each other, with the photo depicting the wanted person. The analysis department finally sends the results to the ordering agency. The analysis is usually carried out within a deadline of 8 days, however, in case of high law enforcement interest, serious situations, or in case of danger to a minor, the deadline is 24 hours.

There is another procedure that assists the work of police officers on duty in public areas. The first step here is that the police officer takes a photo of the person who cannot credibly identify himself and whose personal data cannot be determined with a smart device. The smart device is a mobile phone or tablet running the aforementioned Robot Cop Neo system application.

The police officer sends the photo to the system, which then also generates a hit list. The list and the person present are manually compared by the police officer leading the operation. If the identification is successful, no further action is required; if the identification is unsuccessful, the police officer takes the person to the nearest police station for further data determination.

6 Use of Facial Recognition System in Addition to Hungarian Technical Border Barrier

Based on decisions issued by the Hungarian Government in response to the extraordinary migration pressure, a technical border barrier was established along the Hungarian-Serbian border. The project included the construction of a patrol road in the border area [22] and the installation of other supporting infrastructure. The primary purpose of the barrier is to curb illegal migration, which intensified in 2015 and has continued to pose a challenge for both Hungary and the European Union [23].

The Hungarian technical border fence consists of several lines of metal fences installed in parallel, supplemented by an electronic signaling system. The fence also has cameras, which can be used remotely, manually, or automatically, activated by movement or temperature changes. The border fence signaling system is monitored by an open-source software called NAGIOS. The software is responsible for the absolute supervision of the infrastructures, during which it continuously monitors and evaluates

the availability of the devices, error signals, and measured values [24]. Such values can be movement received from the sensors, or temperature changes.

The use of 3AR is particularly important in the work of law enforcement agencies protecting the border fence. Determining the data of the person affected by the measure is an important goal, as it can be used to decide how the measure should continue. This method makes it easier to identify wanted people or those who have committed a crime. Facial recognition is also performed at the border fence using the 1:N method. The authorized ordering organization makes a screen recording from the film footage taken by its own camera system, uploads it, and finally receives the identification result. The result can be categorical when the identification is absolutely certain, or proves or excludes the identity. It can be list-based, when the people on the list are potentially suitable for identification. Or it can be exclusionary, when the customer receives the response that the uploaded photo is unsuitable for identification.

Several signaling devices have been integrated into the technical border fence. The devices operate many sensors during their intended operation. The sensors are compressed into lines, designed like a network. The wires connecting the sensors run along the entire length of the border fence and also have the ability to bend, so that they can adapt to the terrain conditions. The sensors are addressed, in the event of an operating error, the location of the problem can be determined precisely, so it can be localized easily and quickly, and there is the possibility of maintenance and resetting [25].

Furthermore, in the event of an alarm due to the movement of the fence, a 7-language information message will be played from the loudspeakers in the area affected by the alarm in English, French, Turkish, Arabic, Pashto, Farsi and Urdu. The loudspeakers will broadcast the following text: "I would like to warn you that you are at the Hungarian state border, at a border fence owned by the Hungarian state, which is equipped with an electronic protection system. Approaching or touching the border fence may cause injury and pain. If you damage the border fence, cross the border fence in an unauthorized manner or attempt to do so, you are committing a crime. I urge you to refrain from committing a crime! You can submit your asylum application at the embassy of Hungary outside the Schengen area."

The computer control system indicates each change with a separate alarm type. In the event of a communication error, the system can remain connected to the control device, but if a problem occurs in the operation of one or more sensors, the system searches for the possible source of the error. Usually, a sensor short circuit, breakage, contact error, misaddressing, power supply failure, or bus cable short circuit is responsible for the error, which can be repaired quickly and efficiently. A controller failure may occur when the system is unable to establish a connection. In such cases, a power supply, network, or controller error may occur, which can be easily repaired and detected.

The Hungarian technical border fence can also detect physical changes that occur during an illegal intrusion attempt in such a way that the location of the change can be precisely localized for human resources. The border fence is capable of providing its own physical protection and accurately localizing any damage. A camera system operates along the entire length of the border fence. In the case of cameras in a constant state, continuous spectral analysis operates in specific monitoring zones or lines. If someone or something passes through these or makes continuous movement, a video analytics alarm is generated. The evaluable daytime visibility range of laser cameras is more than 1 000 meters, and the nighttime visibility range is more than 100 meters. The evaluable visibility range of thermal cameras is 1 000 meters.

The protection is also supplemented by (using) drones. During patrols using the device, the state border area is mapped, possible illegal routes, resting places, possible tunnels are detected by the flying device, and in some cases, people who have committed illegal border crossings are also searched for. The most essential elements of the Ethernet communication network connecting the sensors have been placed in the infrastructure devices. Each device operates a router. The large number of routers enable the localization method of effective troubleshooting.

Each device, such as energy transmitters, controllers, input cards, thermometers, and other devices, is connected to the police network via routers. The task of the communication network is to ensure stable and secure communication between all the devices that make up the system. The correct operation of the communication network allows alarms and signals to reach the surveillance system, and these networks also guarantee the remote switching on and off devices, as well as their possible configuration.

The data transmission cables are connected to the system components performing various tasks through structures constructed in safe locations. A data transmission backbone runs parallel to the border, but within the territory of Hungary, and active data transmission devices have been installed at the low-voltage feed points. The communication network is based on Internet Protocol (IP). An IP address is a unique network identifier used to identify computers communicating with each other using the network protocol.

There is also remote monitoring software that continuously collects data on the operation of the border fence. The external and internal fence elements are displayed on the map with icons. There is also a separate server interface for selecting different stations and displaying data on up and down connections. In the control program, the application shows each object with a different icon and marks its exact location on the map. The colors and pictograms of the icons have different meanings. The icon of a location can be a county, a site, or any preset figure. It shows all the information about the current status of the devices under the icon.

From the point of view of the operation of the technical border fence, the main task of the established network is the monitoring and operation of the communication system, software, and infrastructure. Various services can also be run that alert when a preset extraordinary event occurs or when a certain limit value is exceeded. The monitoring program of the signaling system is suitable for continuous monitoring of operation and for the immediate recognition and localization of possible malfunctions or attacks, thus ensuring the efficient operation of the technical border fence.

7 Opportunities for Improving Facial Recognition Systems in Relation to Border Closures

Continuous development of facial recognition algorithms is necessary to ensure that the results already achieved are sustainable and improved [26]. One such development option would be to replace the cameras used to take the photos required for uploading. Replacing the existing cameras with higher-quality ones would be prohibitively expensive; therefore, it is more cost-effective to enhance the lower-quality images using image-processing algorithms.

There are two types of algorithms, one of which can be purchased or used on a subscription basis. The other type is the open-source algorithm, which is freely available and can be developed by the employing organization. Both versions are suit-

able for performing their tasks, however, in both cases special attention must be paid to ensuring that the algorithms are used exclusively on a closed network. Of course, in the case of the subscription version, a separate contract must be concluded for data protection.

The use of the 3AR system currently requires continuous use of human resources, therefore the number of people working in it can be increased, so the average 8-day deadline for identification outside of highlighted events could be reduced. Artificial intelligence is constantly evolving, so monitoring developments and continuously integrating innovations can also improve the operation of recognition algorithms. This integration may result in human resources being excluded from facial recognition over time, thus further reducing the time the system is used.

Since law enforcement agencies [27] in Hungary use the 1:N method for facial recognition, it is essential to keep existing records up to date and expand them. It is advisable to conclude as many agreements as possible, since the greater the possibility of immersion during identification, the greater the chance of achieving successful identification. Based on the recordings of currently operating cameras, merging the NAGIOS system and the Robotzsaru Neo system application version is a reliable way to increase efficiency.

If this is achieved, the camera operator takes a photo of the perpetrator at the border fence, which is uploaded to the 3AR system. The images of the people on the hit list are then compared in real time with the original photo.

8 Technological Challenges of Automated, AI-Assisted Facial Recognition System

Although the deployment of an AI-driven automated facial recognition system capable of providing instant identification represents the logical next step, the technological limitations of current AI-based facial recognition systems continue to pose significant challenges. These limitations also include data quality, environmental, algorithmic, infrastructure network integration and ethical issues, which can significantly affect the practical effectiveness of such systems.

The first and most important question is how efficiently the available learning machine algorithms are able to identify a given person based on images of different quality, and in this context, it is important to compare the performance of such systems with the efficiency of facial recognition with human intervention. Earlier simpler modelling algorithms that examined the morphological characteristics of the face with static descriptive data, which were able to recognize the face strictly on the basis of an image taken from a specific angle, are the currently widespread deep learning models for facial recognition, like the convolutional neural networks (CNNs) [28, 29], Deep Belief Networks (DBNs) [30] or Spatial Pyramid Pooling Net-work (SPP-Net) [31] are able to recognize and identify faces in photos and videos taken from different angles and in natural environments.

In different experimental situations (Tab. 1.), modern deep-learning face recognition algorithms achieve a rather high identification rate of over 90 %, depending on the resolution of the images and the nature of the learning-database, and even in the case of a rather low image size, there is a probability of over 98 % that the person under study will be the most accurate match among the 5 hits.

Based on an experiment conducted by Makhruskin et al. [32] on a small sample, these results far exceed the performance of human facial recognition capabilities, who

were able to correctly identify faces based on the available database in only 57.9 % of the tasks during the indicated experiment. Although the effectiveness of identification can be said to be quite effective based on the above data, it is important to emphasize that the above experiments – although they tried to reconstruct real situations – showed images taken at different angles and with different lighting – they were basically taken in a sterile, experimental environment and do not necessarily reproduce the conditions of a real border security situation.

Tab. 1 Overall face recognition rates with different models

Model	Size of pictures	Overall recognition rate		Source
		Top1 (%)	Top 5 (%)	
CNN (2017)	16 × 16	88.8	98.4	[28]
CNN (2017)	64 × 64	94.8	98.8	[28]
CNN (2024)	128 × 128	98.3		[29]
Deep Belief (2017)	-	93.1		[30]
CNN (2019)	96 × 96	94.9		[31]
SPP-Net (2019)	96 × 96	92.5		[31]
CNN (2017)	224 × 224	90–100		[32]
Human observer	224 × 224	57.9		

In real situations, especially in the case of an attempt at an illegal border crossing, it is common that the face of the person to be examined is only partially visible, which can significantly impair the effectiveness of automatic facial recognition. Various research studies [33–35] show that the performance of deep-learning facial recognition algorithms can be significantly increased with the help of targeted learning databases containing partial faces. For images where the upper part of the face is visible, with a properly trained database, identification is also available with an efficiency of over 90 %, similar to full-face image recognition. However, the experiment of Elmahmudi et al. [33] in this direction pointed out that the effectiveness of systems that are not trained for partial facial recognition can be radically reduced.

The result (Tab. 2) of a processing model using the Cosine Similarity method within the CNN model is presented from the scenarios examined in the aforementioned study. This illustrates the performance differences between the results of a student database that uses partial faces and a database that only uses full faces.

It is also important to consider how effectively facial recognition databases based on frontal facial images can identify individuals from profile-view images. Sengupta et al. [36] report that the identification accuracy of databases relying on frontal 2D facial images may decrease substantially – by 11% to 32% – when the query image depicts the subject in profile rather than from the front.

Partial facial occlusion should also be considered in this context. Studies have shown that the reduction in identification accuracy is relatively small (2–5 %) for databases trained to recognize faces with makeup [37, 38]. In contrast, for databases

that have not been trained on such variations, the decrease in recognition accuracy can exceed 15 %.

Tab. 2 Partial face recognition rate using Cosine Similarity method

	Recognition rate (%) [33]	
	learned full face database	learned on partial face-images
Full face	100	100
Right face	100	100
Top half	100	100
Bottom half	60	97
Eyes + Nose	40	90
Eyes	25	65
Nose	0	15
Forehead	0	30
Mouth	0	15
Cheek	0	15

In the case of other accessories – hats, beards, glasses, headscarves, the effectiveness of identification is basically determined by which part of the face and to what extent the costume covers it. Here it can be stated quite clearly that deep learning applications are much less sensitive to such modifying characteristics than human perception with culturally and situationally determined expectations. However, practical observations show that there are demonstrable algorithmic biases on gender and racial grounds [39], which are also interesting because the analysis algorithm is not influenced by cultural considerations or biases.

The explanation of the existing phenomenon can basically be traced back to three reasons. On the one hand, some of the databases on which machine learning is based are not balanced in terms of appearance and race, and people belonging to certain races are overrepresented in them [40]. As a result, the machine system will be more sensitive to differences between people of a given race, making the reliability of identification more accurate.

The NIST report [39] cited above explicitly states that facial recognition systems trained on Chinese datasets exhibit significantly lower false-positive rates for Chinese and other East Asian populations than for individuals from other populations. Similarly, systems trained on American datasets achieve the lowest false-positive and false-negative rates for individuals of Caucasian ancestry [41].

Another important reason that has been explored is the question of the quality of the data entered into the database and in part during the search. In the case of different skin-tones, different illumination and background can be used to take the most detailed photo, but during the creation of official photos – which make up the majority of the databases for identification, they can rarely take such aspects into account, and in the course of these – at least in the Western world, a systematic difference can be observed between image quality and skin color [42]. This is reinforced by the fact that the most commonly used image compression methods – e.g. when creating a jpeg file

– typically preserve more details from the lighter shades of the visible color range, so in the case of dark images or images of darker-skinned people, the compression process itself creates a racial bias.

The NIST report cited above explicitly states that facial recognition systems trained on Chinese datasets exhibit significantly lower false-positive rates for Chinese and other East Asian populations than for individuals from other populations. Similarly, systems trained on American datasets achieve the lowest false-positive and false-negative rates for individuals of Caucasian ancestry.

The third such reason is the context of the images related to cultural and social customs. For example, it can be shown that the difference in perceptual efficiency between women and men can be explained practically entirely by differences in the wearing of headgear and make-up habits [43]. Although it belongs to a different field from the point of view of interpretation, technically the same problem is represented by the difference in the image stock in the database and the age during the examination, which in technical sense means different variations in the appearance of the same person [44].

In connection with the efficiency of facial recognition systems and in addition to the measures of its general effectiveness, it is worth dealing separately with the two types of indicators of erroneous perceptions, the two consequences of sensitivity and specificity values. Sensitivity shows the rate of successful identification of the test subject, and specificity is the rate of false-positive feedback given by the system. The technological limitation here is not only a question of accuracy: a lower number of successful identifications can pose a security threat, and false-positive results lead to operational overload and unnecessary delays and examinations of innocent passengers from the point of view of border crossers. The latter case, if associated with ethnic or gender bias, also constitutes an explicitly unintentional discriminatory practice.

To illustrate the problem, let's take the case of the Röszke border crossing, where between 50 and 60 000 people turn up on a busy summer day, and let us assume that we use a system with an average efficiency of 98 %, and this % value is met for both indicators, specificity and sensitivity. If we assume that the number of people registered as suspicious or wanted for some reason is 1 per thousand, in the case of 50 000 people, this means 50 such people per day. A system with 98 % sensitivity will identify 49 of them. At the same time, the 98 % specificity also means that 2 % of the 49 950 unsearched people, i.e. 999 persons, will be incorrectly identified as wanted people, i.e. in reality, the system will filter out 1 048 persons, the vast majority, 95 % of whom will be incorrectly identified by an automatic system.

To address the problem outlined, appropriate processes must be put in place to reduce both the workload of security staff and the procedure for those who are misidentified. One of these possible solutions is the operation of parallel identification systems, which are trained in different learning databases, in some cases using different models. Those identified in the first step could be immediately included in the second automatic verification process. Sticking to the previous example, only 1 048 people are examined here, of whom 49 will be really wanted people. The system is again able to identify those who are wanted with 98 % of the results, so after the second round, 48 people are actually wanted in the system, while only 20 people remain in the system with false positive results from the people who were incorrectly identified in the first round. At the end of the two rounds of automatic search, there are a total of 68 people on the system, out of whom more than two-thirds are genuinely wanted persons.

9 Real Life Application of Face Recognition Solutions in Different Border Control Situations

Different border policing situations impose completely different conditions on face recognition systems.

Airports are one of the most ideal applications for biometric technologies. The environment is controlled, lighting conditions can be optimized, and passenger interaction is generally higher than in other border crossing situations. At airport border control, facial recognition is often carried out through automated gates, where passengers have to stop, look at the camera, and the system checks their face against the biometric data in the passport and other databases.

The accuracy of the systems used at airports is usually high, as the cameras are high-resolution, the lighting is controlled, and the position of the users is predetermined [45]. However, due to the high safety standards of the airport environment, the requirements for the systems are also very high. The guidelines set out by Frontex provide [46] for a sensitivity of 9.99 % and a specificity of 95 % for the effectiveness of the entire ABC system [47]. However, it is important to note that these regulations do not apply to facial recognition solutions per se, but to the identification system as a whole.

In airport border control, facial recognition can be used not only when crossing the border, but also at boarding, checking in baggage or at security. The concept of a fully biometric passenger route is becoming more and more common in such a way the passenger's face is recorded once and then automatically identified at each additional checkpoint. This significantly speeds up the process, but raises serious data protection issues, especially when it comes to data storage and sharing [48].

Face recognition during pedestrian border-crossing is relatively easier task in connection with small border traffic, as the movement of pedestrians is relatively predictable, so the cameras record the face more easily. However, training the system to recognize facial details significantly increases the efficiency of identification.

From a technological point of view, it is more critical to identify people crossing the border en masse during a crisis situation, which always sets individual requirements depending on the nature of the crisis. In such cases, it is not only the identification of faces, but also the determination of the number of people passing through which poses a challenge. Hence, effective facial identification can only work effectively in such cases if the system is also connected to a People Counting System that identifies human presence [49]. Crossing the border by car is a much more complex issue even in normal operation and it causes lots of problems that are difficult to overcome. Real-time identification of vehicle occupants while driving is only inefficient under current technological conditions and is easy to circumvent, as – especially passengers – can very easily find a position in which a fixed camera does not have a view of the face.

In addition, light reflections, reflections from the windshield and possible dirt also significantly impair facial recognition efficiency. The situation is different if the entry is not automatic during border control, facial recognition increases the efficiency of the work of the control unit. In such cases, the device that captures the image can be a portable camera (e.g. mobile phone) that transmits the taken photo to the central server, and the result of the deep-learning analysis is sent back to the same device. Over the past decade, several such systems have been introduced, achieving an identification result of around 98 % in practice [50].

The green border means a completely different environment for facial recognition systems. Here, technology does not work under controlled, but under unpredictable conditions, which significantly reduces the accuracy and reliability of recognition. In the case of a technical border fence erected at the southern border of Hungary, the identification of a specific person with the installed systems can only be carried out occasionally, with relatively low efficiency, even with deep learning tools.

In the case of such permanently installed systems, facial recognition is less capable of identifying repeat border violators than systems for recognizing movement patterns, the effectiveness of which, however, is currently far below the effectiveness of facial recognition systems even with adequate comparative data. At the same time, the identification of a repeat border violator with an efficiency of 70–80 % before apprehension can significantly increase the efficiency of border surveillance, assist apprehension, and prepare border guards for the nature of the threat they face [51].

In such a situation, however, the previously mentioned system of the staff performing border guards and apprehending the border violator, available on their mobile phones, is more important, which can be used to identify the apprehended person on the spot, so the procedures related to him or her can become significantly faster and more efficient.

10 Conclusions

To sum up, the development of the system elements can make the cameras installed next to the border fence suitable for the NAGIOS system to automatically take a photo of unknown persons appearing at the border fence, which is suitable for identification. As a result of automation, the uploaded image can be searched in the registers without using human resources. Successful identification enables the prompt apprehension of individuals involved in illegal border crossings or human smuggling, thereby facilitating the swift initiation and conduct of legal proceedings.

Based on the presentation of other systems operating at the border crossing, it can be stated that the IT network has been built and is capable of securely and efficiently transmitting facial images and then analyzing the data. Therefore, there is no need to build additional infrastructure.

The acceleration of facial recognition will result in a reduction in the investigation time in the long term, as the authorities do not have to spend time establishing the perpetrator's data. Due to faster procedures, Hungarian and European border protection will become more efficient. This would also make it more likely that illegal migration will be curbed and that migration will be redirected to legal channels. The results listed above can start a continuous process that will also increase the productivity of the Hungarian economy, because the 3AR system also makes the work of state-owned enterprises safer. The systems used by state-owned enterprises can also be transferred to multinational companies or domestic enterprises over time, of course only using the records containing the data necessary for the given task.

Among other applications, recordings from musical or sporting events can be processed using 3AR or similar civilian systems to identify individuals within a crowd who may be associated with criminal activity or whose presence at a particular location is prohibited. The main purpose of facial recognition by law enforcement agencies and the expansion and updating of facial image registers is to prevent, disrupt, deter, detect and prove crimes.

References

[1] GASPER, D. and O.A. GÓMEZ. Human Security Thinking in Practice: 'Personal Security', 'Citizen Security' and Comprehensive Mappings. *Contemporary Politics*, 2015, **21**(1), pp. 100–116. DOI 10.1080/13569775.2014.993906.

[2] IMAOKA H., et al. The Future of Biometrics Technology: From Face Recognition to Related Applications. *APSIPA Transactions on Signal and Information Processing*, 2021, **10**, e9. DOI 10.1017/ATSIP.2021.8.

[3] ELHOSENY, M., et al. Multimodal Biometric Personal Identification and Verification. In: A. HASSANIEN and D. OLIVA, (eds). *Advances in Soft Computing and Machine Learning in Image Processing. Studies in Computational Intelligence*. Cham: Springer, 2018. ISBN 3-319-63754-1.

[4] TÓTH, N.Á., et al. Innovation, Infocommunication and Digital Transformation in Sport Policing and Certain Aspects of Sports. *Journal of Infrastructure Policy and Development,* 2024, **8**(3), 2617. DOI 10.24294/jipd.v8i3.2617.

[5] KIS, K.B. and I. SZIJÁRTÓ. The Hungarian Face Recognition Technology in Light of EU Law. *Maastricht Journal of European and Comparative Law,* 2026. DOI 10.1177/1023263X261462828.

[6] PETRESCU, R.V. Face Recognition as a Biometric Application. *Journal of Mechatronics and Robotics,* 2019, **3**(1), pp. 237–257. DOI 10.2139/ssrn.3417325.

[7] PAOLUCCI, F. Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems. In: N.M. GONZÁLEZ and G. MOBILIO (eds). Next Democratic Frontiers for Facial Recognition Technology (FRT). Cham: Springer, 2025. ISBN 978-3-031-89793-1.

[8] KAYSER-BRILL, N. General Information: At Least 11 Police Forces Use Face Recognition in the EU [online]. 2020 [viewed 2025-11-01]. Available from: https://algorithmwatch.org/en/face-recognition-police-europe/

[9] GARVIE, C., A. BEDOYA and J. FRANKLE. The Perpetual Line-Up [online]. 2016 [viewed 2025-10-30]. Available from: https://www.perpetuallineup.org/

[10] GROSS, A., M. MURGIA and Y. YANG. Chinese Tech Groups Shaping UN Facial Recognition Standards [online]. 2019 [viewed 2025-10-20]. Available from: https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

[11] BURT, C. Japanese Government to Use Facial Recognition for Emperor's Anniversary Event Access [online]. 2019 [viewed 2025-08-30]. Available from: https://www.biometricupdate.com/201902/japanese-government-to-use-facial-recognition-for-emperors-anniversary-event-access

[12] GOPALAN, R.T. Forensic Investigations in Terrorism. In: B.E. TURVEY. *Forensic Victimology*. 3rd ed. Cham: Springer, 2023, pp. 267–287. ISBN 978-0-12-821768-9.

[13] ALEKE, N.T. and M. TRIGUI. Legal and Ethical Challenges in Digital Forensics Investigations. In: M. OMAR and H. ZANGANA (eds.). *Digital Forensics in the Age of AI.* Sohar: IGI Global Scientific Publishing, 2025, pp. 147–176. DOI 10.4018/979-8-3373-0857-9.

[14] *Act CLXXXVIII of 2015 on the Facial Image Analysis Registry and the Facial Image Analysis System* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://net.jogtar.hu/jogszabaly?docid=a1500188.tv

[15] *Decree 78/2015 (XII. 23.) of the Minister of the Interior on the Detailed Rules for the Operation of the Facial Image Analysis System* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://net.jogtar.hu/jogszabaly?docid=a1500078.bm

[16] *11/2016. (IV.29.) National Police Chief's Instruction* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://net.jogtar.hu/jogszabaly?docid=A16U0011.ORF&txtreferer=00000001.txt

[17] *Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv

[18] *Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [online]. [viewed 2025-08-11]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=hu

[19] *Normative Enabling the Development of the System: 14/2022. (IV.7.) National Police Chief's Instruction on the Regulation of IT Application Development Processes* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://njt.jog.gov.hu/jogszabaly/2022-14-B0-8E

[20] *Legislation Enabling the Operation: Government Decree 350/2016. (XI.18.) on the National Expertise and Research Centre (NSZKK)* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://njt.jog.gov.hu/jogszabaly/2016-350-20-22

[21] *General Information on the Operation of Idomsoft Private Limited Company* (in Hungarian) [online]. [viewed 2025-10-10]. Available from: https://idomsoft.hu

[22] *Government Decree No. 1401/2015 (VI.17.) on Certain Measures Necessary to Manage the Extraordinary Immigration Pressure* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://njt.jog.gov.hu/jogszabaly/2015-1401-30-22

[23] *Government Decree No. 1165/2016. (IV.5.) on Providing the Necessary Budgetary Resources for the Construction of the Maneuver Road to Be Built on the Hungarian-Serbian Border Section and to Ensure Reliable Power Supply* (in Hungarian) [online]. [viewed 2025-08-11]. Available from: https://njt.jog.gov.hu/jogszabaly/2016-1165-30-22

[24] RENITA, J. and N. EDNA Network's Server Monitoring and Analysis Using Nagios. In: *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).* Chennai: IEEE, 2017. DOI 10.1109/WiSPNET.2017.8300092.

[25] MAJER, M. Construction and Operation of the Hungarian Technical Border Barrier. Critical Infrastructure Protection: Advanced Technologies for Crisis Prevention and Response. In: T.A. Kovács and I. Fürstner (eds). *Critical Infrastructure Protection: Advanced Technologies for Crisis Prevention and Re-*

sponse. NATO ATC 2024. NATO Science for Peace and Security Series C: Environmental Security. Dordrecht: Springer, 2025. ISBN 94-024-2307-9.

[26] HILL, R.K. What an Algorithm Is. *Philosophy & Technology*, 2016, **29**, pp. 35–59. DOI 10.1007/s13347-014-0184-5.

[27] BESENYŐ, J. Fences and Border Protection: The Question of Establishing Technical Barriers in Europe. *Academic and Applied Research in Military and Public Management Science*, 2017, **16**(1), pp. 77–87. DOI 10.32565/aarms.2017.1.7.

[28] COSKUN, M., A. UCAR, O. YILDIRIM and Y. DEMIR. Face Recognition Based on Convolutional Neural Network. In: *2017 International Conference on Modern Electrical and Energy Systems*. Kremenchuk: IEEE, 2017, pp. 376–379. DOI 10.1109/MEES.2017.8248937.

[29] FIRMAN, A.M., Z. ZAINUDDIN and M. NISWAR. Performance Analysis of Face Recognition Using Machine Learning and Modified Deep Learning Methods. In: L. RAHAYU, et al. (eds.). *The 18th IMT-GT International Conference on Mathematics, Statistics and Their Applications.* Warsaw: Sciendo, 2024, pp. 111–116. DOI 10.2478/9788367405713-020.

[30] KANG, K. Comparison of Face Recognition and Detection Models: Using Different Convolution Neural Networks. *Optical Memory and Neural Networks*, 2019, **28**(2), pp. 101–108. DOI 10.3103/S1060992X19020036.

[31] FAN, R. and W. HU. Face Recognition with Improved Deep Belief Networks. In: *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).* Guilin: IEEE, 2017, pp. 1822–1826. DOI 10.1109/FSKD.2017.8393043.

[32] MAKRUSHIN, A., D. SIEGEL and J. DITTMANN. Simulation of Border Control in an Ongoing Web-based Experiment for Estimating Morphing Detection Performance of Humans. In: *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*. New York: Association for Computing Machinery, 2020, pp. 91–96. ISBN 1-4503-7050-0.

[33] ELMAHMUDI, A. and H. UGAIL. Experiments on Deep Face Recognition Using Partial Faces. In: *2018 International Conference on Cyberworlds*. Singapore: IEEE, 2018, pp. 357–362. DOI 10.1109/CW.2018.00071.

[34] WANG, Z., B. HUANG, G. WANG, P. YI and K. JIANG. Masked Face Recognition Dataset and Application. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2023, **5**(2), pp. 298–304. DOI 10.1109/TBIOM.2023.3242085.

[35] YO, M.C., S.C. CHONG and L.Y. CHONG. Sparse CNN: Leveraging Deep Learning and Sparse Representation for Masked Face Recognition. *International Journal of Information Technology*, 2025, **17**(8), pp. 4643–4658. DOI 10.1007/s41870-025-02415-1.

[36] SENGUPTA, S., et al. Frontal to Profile Face Verification in the Wild. In: *2016 IEEE Winter Conference on Applications of Computer Vision (WACV).* Lake Placid: IEEE, 2016. DOI 10.1109/WACV.2016.7477558.

[37] ENFES, E.I. and Ö. TOYGAR. The Effect of Disguise and Makeup in Facial Recognition. In: *2025 9th International Artificial Intelligence and Data Processing Symposium (IDAP).* Malatya: IEEE, 2025. DOI 10.1109/IDAP68205.2025.11222301.

[38] DANTCHEVA, A., C. CHEN and A. ROSS. Can Facial Cosmetics Affect the Matching Accuracy of Face Recognition Systems? In: *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. Arlington: IEEE, 2012, pp. 391–398. DOI 10.1109/BTAS.2012.6374605.

[39] KRISHNAPRIYA, S.K., K. VANGARA, M.C. KING, V. ALBIERO and K. BOWYER. Characterizing the Variability in Face Recognition Accuracy Relative to Race. In: *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. Long Beach: IEEE, 2019, pp. 2278–2285. DOI 10.1109/CVPRW.2019.00281.

[40] GROTHER, P., M. NGAN and K. HANAOKA. *Face Recognition Vendor Test Part 3: Demographic Effects* [online]. 2019 [viewed 2025-08-11]. DOI 10.6028/NIST.IR.8280. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[41] YUCER, S., F. TEKTAS, N. AL MOUBAYED and T. BRECKON. Racial Bias within Face Recognition: A Survey. *ACM Computing Surveys*, 2025, **57**(4), 105. DOI 10.1145/3705295.

[42] ISO/IEC 19794-5:2011ISO, *Information technology – Biometric Data Interchange Formats – Part 5: Face Image Data*.

[43] ALBIERO, V., K. ZHANG, M.C. KING and K.W. BOWYER. Gendered Differences in Face Recognition Accuracy Explained by Hairstyles, Makeup, and Facial Morphology. *IEEE Transactions on Information Forensics and Security,* 2022, **17**, pp. 127–137. DOI 10.1109/TIFS.2021.3135750.

[44] SAJID, M., et al. Deep Learning in Age-invariant Face Recognition: A Comparative Study. *The Computer Journal*, 2022, **65**(4), pp. 940–972. DOI 10.1093/comjnl/bxaa134.

[45] LABATI, R.D., A. GENOVESE, E. MUNOZ, V. PIURI, F. SCOTTI and G. SFORZA. Advanced Design of Automated Border Control Gates: Biometric System Techniques and Research Trends. In: *2015 IEEE International Symposium on Systems Engineering (ISSE).* Rome: IEEE, 2015, pp. 412–419. DOI 10.1109/SysEng.2015.7302791.

[46] *Guidelines for Processing of Third Country Nationals Through Automated Border Control* [online]. 2016 [viewed 2025-08-11]. DOI 10.2819/39041. Available from: guidelines_for_processing_of_third_country_nationals_through_abc.pdf

[47] LABATI, R.D., A. GENOVESE, E. MUÑOZ, V. PIURI, F. SCOTTI and G. SFORZA. Biometric Recognition in Automated Border Control: A Survey. *ACM Computing Surveys,* 2017, **49**(2), 24. DOI 10.1145/2933241.

[48] PATEL, V. Airport Passenger Processing Technology: A Biometric Airport Journey [Thesis] [online]. Embry-Riddle Aeronautical University, 2018 [viewed 2025-08-11]. Available from: https://commons.erau.edu/cgi/viewcontent.cgi?article=1384&context=edt

[49] HORVAT, G., S. RIMAC-DRLJE and D. ŽAGAR. Fade Depth Prediction Using Human Presence for Real Life WSN Deployment. *Radioengineering,* 2013, **22**(3), pp. 758–768. ISSN 1210-2512.

[50] GUPTA, D. and N. KUMAR Border Surveillance Using Face Recognition, Mobile OTP and Email. *IIUM Engineering Journal*, 2020, **21**(2), pp. 143–152. DOI 10.31436/iiumej.v21i2.1322.

[51] BATCHULUUN, G., R.A. NAQVI, W. KIM and K.R. PARK. Body-Movement-Based Human Identification Using Convolutional Neural Network. *Expert Systems with Applications*, 2018, **101**, pp. 56–77. DOI 10.1016/j.eswa.2018.02.016.