DOI: 10.38146/BSZ.SPEC.2020.3.2

Gergely Gárdonyi

# Still Image Face Recognition in Hungary

**Abstract**
The Still Image Facial Recognition System has been in operation for four years in Hungary. The present study details the experiences gained to date, as well as the possibilities, results and plans related to the subject. It briefly presents the history of still image face recognition, provides international outlook, describes the legal framework and the operation of the system, and finally outlines future development opportunities.

**Keywords:** face recognition, analysis, facial recognition system, biometric identification, expert

## Introduction

No significant study has been released on the Still Image Facial Recognition System (hereinafter: SIFRS) so far, even though the field itself is developing rapidly, achieving more and more objectively measurable success; the demand for the service, which plays more significant role in investigations each year, is increasing, and the subject nowadays attracts considerable attention also in scientific research. In Hungary, identification based on facial image has long been of concern to criminalists. As early as in 1887, only a few years after the criminal record system had been established, it was ordered that the records should be supplemented with photographs, and a photography studio was established in 1903 (Szigetvári, 2018, 169-180.). Meanwhile, for crime prevention, a separate manual record of traveling pickpockets was set and copied in 2000 counterparts during the preparation for the 1896 World Expo. The record, which included photographs of 685 persons, was sent to all police departments in Budapest and many police departments and gendarmerie stations in other towns of the country (Anti, 2017). After years of preparatory work, the National Criminal Records Office was established on 1 January 1909 (URL1). In

1958, a study was prepared on the means of identifying a person based on two photographs, i.e. on the factors that affect the quality of the images made for such purpose, the way the comparative analysis should be carried out, and the means to evaluate its results (Illár, 1958). Only a few years later, it was urged that a criminal record system based on facial images and facial features should be created, allowing for image prioritization (retrieving images from the database). A study notes that while approximately 1000 criteria can be determined and assembled precisely in individual facial recognition, approximately 40-70 of those criteria can be applied to achieve the identification of a high-quality facial image (Detrői & Déri, 1967). The National Police Headquarters made attempts to prepare an automated system already in the noughties (URL2), yet the first significant step in such regard was only taken in 2013 when the facial image profile record was established as a result of a decision rendered by the government in the same year. This was preceded by substantial examinations with regard to data protection, testing, and a procurement procedure, as well as the adoption and taking effect of Act CLXXXVIII of 2015 on facial image analysis database and facial recognition analysis system. The operation of the still image facial recognition system commenced on 15 March 2016, initially as the task of the then Central Office for Administrative and Electronic Public Services. Soon thereafter, on 1 January 2017, it was included among the functions of the Hungarian Institute for Forensic Sciences (hereinafter: HIFS) and has remained so to date.[1]

## Classification of facial recognition systems

Facial recognition systems have undergone significant development in recent years due to artificial intelligence and deep learning algorithms. Nowadays facial recognition systems are used in social media (e.g. the recognition of appearance on a photo), telecommunication, related to certain safety features (e.g. user identification for mobile phones), the private security sector (e.g. event security services), and public administration. Generally, two methods are applied in face recognition: the sample-based (or photometric) method on the one hand, in which the global features of the face or parts of the face (e.g. eyes, mouth) are compared with the stored samples, and the geometric-based method on the other hand, where certain details on a face (eyes, nose, chin, etc.) are analysed based on their position and dimensions in relation to each other (Németh & Tóth,

[1] Section 9 of Government Decree 350/2016 (XI. 18.).

2019, 129.). Facial image analyses may be carried out when one photograph is to be compared with another; in that case, the task is to determine whether a match between the persons on the photos can be confirmed or excluded (or to what extent can the match be supported). This is called 1:1 authentication (verification) in the literature. A different task is when one image is to be compared with a large number of photographs in the database, seeking to find out whether the person on the concerned photo is identical to any person appearing on the photos retrieved from the record. This is the so-called 1:N identification, which is essentially the activity carried out in the HIFS at the moment. The former method can be applied to identify a certain individual – who has already come to the attention of the authorities – while the latter can be used to identify, for example, an unidentified person who committed a robbery that was recorded by surveillance cameras, but may also be suitable in other cases, e.g. for the detection of forgery (whether any ID cards were issued previously, under a different name, for the person indicated on a given document). However, no publicly accessible facial image database exists so far that includes both images suitable for identification (e.g. ID photos) and images retrieved from real life (e.g. footage of surveillance cameras) (Dogshun et. al., 2019.). Facial recognition systems can be divided into two groups: image-based and video-based face recognition. Both types exist in Hungary, under the name standing image and video-based facial recognition, respectively. The latter operates within the framework of the Special Service for National Security and is not discussed in the present paper. The operation of the SIFRS is included among the tasks of the Ministry of Interior, and the facial recognition analysis belongs to the HIFS.

## International outlook

Facial recognition systems are considered highly controversial all over the world, primarily due to data protection concerns. Various examples can be seen, from full ban to a wide range of surveillance. In Europe, there is no uniform regulation (URL3), even though it is known that the extension of the Prüm legal framework is under development. The new regulation would allow for mutual retrieval from facial image databases (URL4). In the United States of America, state and local systems operate without federal regulation. According to a survey conducted in 2016, there are 18 states where databases including millions of driving licences are in operation (e.g. Utah, North Dakota), and 4 states where, beyond the aforesaid, records that include mug shots may also be used by the police (e.g. New Mexico). There are some states where the database is not available on a state level, yet few cities use it nonetheless (e.g. California – San Diego, Los Angeles) (URL5). In the United States, the application of Chinese and Russian facial recognition systems in the critical infrastructural systems and national security has been banned by law since 2019 (URL6). As regards the facial recognition systems of the American government, it can be seen that many cities seek to gain time and have prescribed a moratorium of a few years during which those systems cannot be set up in public spaces or applied by the government in the concerned cities (URL7). In India, the Aadhaar Program, i.e. the world's largest national identification system with the capacity to handle one million registrations per day, was launched by the government and has been fulfilled with data by identifying over 1.3 billion individuals. In the program, where each person receives a 12-digit unique identification number (Aadhaar), particular attention is paid to preventing any misuse (primarily seeking to prevent a registration under another person's name). That goal is sought to be achieved by applying fingerprint, face, and iris recognition technology (URL8). Japan uses one of the world's most renowned facial recognition systems (developed by NEC), nowadays used frequently also at several events. Its accuracy was proved to be over 99% on the ceremony that marked the 30th anniversary of Emperor Akihito's accession to the throne, and where the system was used to accelerate and support entries. As widely known, the same system will be used at the Olympics hosted by Japan (URL9). However, it should be noted that the said accuracy was achieved after pre-entering and recording the data of approximately 1000 persons who entered the event and whose identification was backed by several metadata. The facial recognition systems used in China became infamous rapidly as a tool of a repressing state. Indeed, China seeks to include every single citizen in the source record of the system. Moreover, it attempts to sell its software to as many countries as possible, with less success in the USA and in Europe, and with more in the developing world. According to an article published in the Financial Times in December 2019, there were 67 countries (primarily in Asia, Australia, and South America) at the time whose facial recognition system serving surveillance purposes was related to China – not including airports and border crossing points (URL10). All in all, as regards world tendencies, it can be said that facial recognition systems – with different tools, methods, and to various extents – have been or are planned to be introduced and applied extensively everywhere. Developed countries seek to find the line between the inviolability of privacy and the application of facial recognition systems supporting criminal and national security investigations. The most problematic legal issues primarily arise from the use of public space surveillance (CCTV). It appears that a solution that would be satisfactory for all social strata and political forces has not yet been found at any place of the globe (URL11).

## Legal framework

Act CLXXXVIII of 2015 on facial image analysis database and facial recognition analysis system (hereinafter: Facial Image Database and Facial Recognition Analysis System Act) appeared as a new element both in the Hungarian legal system and in public thinking in 2015. Even though some human rights defenders spoke out against the adopted law (URL12), the database was established and the activity related to it, commenced in the spring of 2016. The reasoning of the act points out that it has been a strategic objective since 2013 to include all Hungarian citizens into the Personal Data and Address Record, regardless of whether living in Hungary or abroad (URL13). The aims of the facial image profile database[2] include apprehending perpetrators of criminal offences; identifying persons convicted, or detained on the basis of other legal titles upon their acceptance to the prison service facility; tracing persons missing or wanted for any other reason; identifying the applicants in procedures seeking the issuance of identity cards or other documents suitable for identification; providing support for national security services, as well as for bodies entitled to carry out covert information gathering and apply undercover means, as regards such activities; providing support to the national security services at national security controls, as well as at their tasks prescribed by law related to investigation, national security defence and counterintelligence, intelligence, and control carried out in relation to national security, industry security, interior security and crime prevention, and at the operational protection of facilities; carrying out personal protection tasks prescribed by law; carrying out tasks prescribed by law in relation to the protection of priority bodies (institutions) and facilities; providing support to authorities abroad, for the purpose of crime prevention, criminal investigation and the conduct of criminal procedure, at identifying persons against whom such procedure is conducted; providing support in case of extraordinary death and in relation to body identification if the deceased is unknown; carrying certain tasks for the Witness Protection Service; identifying persons who intend to cross the state border; identifying persons who qualify as third-country citizens in the framework of alien policing procedures; identifying persons covered by the act on asylum and identifying the ap-

[2] Section 5 of the Facial Image Database and Facial Analysis System Act.

plicants in the procedures for acquiring Hungarian citizenship. As of 1 May 2020, further aims of the database are to identify individuals affected by police measures or to verify their identity, and to provide support, in the framework of customer identification, for verifying the identity of applicants at electronic administration, including applicants seeking for the issuance of identity cards or other documents suitable for identification. These tasks aim, on the one hand, at decreasing the number of cases when an individual is to be taken to the police department, since they allow for means of identification on-site, and, on the other hand, at providing more flexible solutions to people by broadening the scope of electronic administration. These activities are not covered by the present paper; the system serving such activities is currently under development and is not related to the facial recognition analysis carried out by the HIFS. The law provides an exhaustive list of the bodies entitled to request facial recognition analysis and the purposes for which it can be requested.[3] That list includes the bodies carrying out classic policing activities (i.e. the Police in the classic sense), the National Protective Service, the Special Service for National Security, the Counter Terrorism Centre, the Constitution Protection Office, the Information Office, the Military National Security Service, the Hungarian Prison Service Headquarters, the National Directorate-General for Aliens Policing, the National Tax and Customs Administration, the Parliamentary Guard, the Counter Terrorism Information and Criminal Analysis Center, as well as the prosecution service and the courts. Each time, the search in the image profile database is carried out only in relation to the given case and the body requesting the service must designate the purpose of the search accurately.[4] These data are not provided to the body who carries out the facial recognition analysis, i.e. the analyst is not aware of whose image he or she is analysing and for what purpose. Thus, the analyst's activity is confined to comparing identifying features and drawing conclusions as regards the degree of identity. The body who carries out the facial recognition analysis neither keeps any records of nor processes any personal data. The given photograph is erased by the system automatically, each time after the analysis is finished.[5] In the framework of data provision, the body entitled to data request only receives the connection code attached to the relevant facial image profile. That body can gain access to the personal data belonging to the connection code in a separate procedure initiated by it. Thus, the analyst is not aware of whose image he or she analyses and for what pur-

[3] Paragraph (3) of section 3 in the Facial Image Database and Facial Analysis System Act.
[4] Paragraph (1) of section 13 in the Facial Image Database and Facial Analysis System Act.
[5] Paragraph (10) in section 11 in the Facial Image Database and Facial Analysis System Act.

pose. The data of the person(s) sent as a match is received only by a member of the body who requested the analysis. Certain provisions of the Facial Image Database and Facial Recognition Analysis System Act are elaborated by Decree 78/2015. (XII.23.) BM of the Minister of Interior on the rules of operating the facial recognition analysis system. This Decree also regulates the conditions of requesting the service. In accordance with the said Decree, a cooperation agreement is to be concluded between the HIFS and the body entitled to requisition.[6] (The HIFS has already concluded the required agreement with each concerned body.) Provided such agreement exists, different entitlements can be requested at the Ministry of Interior to the co-workers of the bodies entitled to requisition. With the entitlement, they can turn directly to the body who carries out the facial recognition analysis, they can lodge images and accept responses (depending on the type of entitlement). The Facial Image Database and Facial Recognition Analysis System Act prescribes that the analysis shall be carried out within 8 working days,[7] and the said Decree obliges the HIFS to carry out the analysis within 24 hours[8] or even outside office hours within a 3-hour time limit if certain requirements are met.[9] The Decree also prescribes the necessary safety measures,[10] inter alia that the facial recognition analysis system is to be operated separately from all other systems, the premises and the facility (building) of the body who carries out the analysis shall be protected by electronic access control. The Decree also includes several other provisions ensuring impartial and secure analysis. Due to the hierarchy of legal norms, the general police authority (the National Police Headquarters) put a separate instruction into effect covering its own personnel, which prescribes their tasks in facial recognition analysis.[11] The instruction includes the procedure of requesting the analysis, the rules on photographing unidentified bodies, and the quality requirements of input images. The latter two sets of rules can be considered as obsolete, since the software used by experts evolved highly, thus, we made a proposal for the amendment thereof. The basis of the quality of images is provided by

[6] Paragraph (1) of section 8 in Decree 78/2015. (XII. 23.) of the Minister of Interior.

[7] Paragraph (6) in section 11 in the Facial Image Database and Facial Analysis System Act.

[8] Paragraph (1) of section 5 in Decree 78/2015. (XII. 23.) of the Minister of Interior *'[...] if risk is posed to a minor, a situation imminently and severely threatening public or national security occurs, or there is a priority law enforcement interest in the procedure serving as grounds for the application of facial recognition analysis'.*

[9] Paragraph (5) of section 5 in Decree 78/2015. (XII. 23.) of the Minister of Interior *'[...] if the facial recognition analysis is applied in order to carry out its tasks related to measures to be taken in special legal order or to the handling of a crisis due to massive immigration'.*

[10] Section 11 in Decree 78/2015. (XII. 23.) of the Minister of Interior.

[11] Instruction 11/2016 (IV. 29.) of the National Police Headquarters on the tasks related to the application of facial recognition analysis database and facial recognition analysis system.

input requirements of the manufacturer of the earlier software,[12] but practice shows that both the software and the analyst can handle images of much poorer quality as well. As a point of reference, we usually advise the following: '*If you recognised the person on the photo had you known him or her, the photo can be lodged.*' However, surprises also occur every now and then: sometimes an image appears to be completely unsuitable for analysis, but the software is nonetheless able to recognise a face and generate a relevant candidate list. Although it is a bit unusual that the amendment of a norm adopted by the National Police Headquarters is preceded by a series of empiric experiments, we considered it necessary in order to make a professionally well-founded proposal as regards photographing unidentified bodies. In the course of those experiments, my colleagues uploaded photos taken of 56 bodies to the system. In the case of 41 persons, there was at least one photo (with a certain setting), with which we were able to find a match in the candidate list. Furthermore, there were four parameters evaluated in the experiment (eyes, light, image plane, viewing angle); as for the position of the eyes, the main conclusion was that the best result can be achieved if the eyes remain untouched during the shoot (i.e. closed eyes are not opened). Manual opening of the eyes – that is, if one follows the procedure set out in the Instruction of the National Police Headquarters – proved to be counter-productive in the light of research results, due to the development of technology. Thus, we proposed the amendment of the procedural protocol and the National Police Headquarters Instruction. All in all, as regards Hungarian legal regulation, it can be ascertained that the SIFRS serves the investigations

[12] *'The image lodged for identification should, if possible, meet the following requirements:*
*a) each image lodged for identification should only display one person or, if the former is not possible, the facial image to be identified must be unambiguously designated in the brief description field connected to the photograph;*
*b) the person on the image to be identified must be in a front-view position, as follows:*
*ba) lateral rotation of the head shall not exceed 30°,*
*bb) vertical pitch of the head shall not exceed 10°;*
*c) the face shall be well-lit, with diffused light;*
*d) the face on the image should not be lit from the side, since the shadow cast by the nose may significantly deteriorate the success of identification;*
*e) on the image lodged for identification, the person to be identified:*
*ea) may not wear any hat, hood or other piece of clothing that covers his face,*
*eb) may not wear sunglasses,*
*ec) his eyes must be opened;*
*f) the image lodged for identification must be of good quality and as high-definition as possible, pursuant to the following data:*
*fa) acceptable format of the image lodged for identification is with 'jpg.' extension,*
*fb) the pupillary distance between the eyes of the person to be identified on the image lodged for identification shall not exceed 50 pixels,*
*fc) definition of the facial image shall not be less than 0,3 megapixels, where the mass of the person's face is two thirds of the image.'* (point 18 of Instruction 11/2016 (IV. 29.) of the National Police Headquarters)

carried out both by domestic law enforcement and national security agencies well, with proper safeguards, a database background of considerable size even on a European level, and a wide scope of users. Thanks to the still image recognition analysis activity, the number of requests increases steeply each year (URL14), and the success of the activity confirmed by the requesting bodies is increasing even more.

## Facial recognition analysis

The process of the still image face recognition commences with the lodging of the image (e.g. a still frame of a camera footage recorded of the suspect) by the body entitled to requisition via a closed system,[13] the file number of which includes no identifier that would reveal the lodging body or the case.[14] Thereafter, the task is assigned to two analysts, who work separately in the facial recognition analysis center, and who upload the image to the software. In case of an image suitable for analysis, the software generates a candidate list of the most similar images. The analysts, who work in different premises, not being aware of each other's activity, then choose the persons who, based on professional aspects, can be indicated as matches in the response given to the requesting body.[15] Before sending the response, the analysts develop a consensual, professionally well-grounded joint opinion. To improve the quality of the image, the analysts may edit any poor-quality images before uploading them to the software. Independence is ensured primarily by the organisational independence of the HIFS and the fact that the origin of the images, as well as the legal ground of the request is unknown by the analysts,[16] the analysis is carried out by two analysts (working separately in different premises)[17] who are obliged to promptly report any suspicious event that might hinder the uninfluenced nature of their activity or the security of data.[18]

As of 1 July 2020, the quality assurance of the still image recognition analysis is ensured in accordance with ISO 9001:2015 standard, thus, the aforesaid rules are guaranteed by an external certification body (URL15). The quality of the facial recognition analysis in Hungary is illustrated by the fact that the domestic

[13] Point 10 of Instruction 11/2016 (IV. 29.) of the National Police Headquarters.

[14] Point 12 of Instruction 11/2016 (IV. 29.) of the National Police Headquarters.

[15] Paragraph (7) of section 11 in Decree 78/2015. (XII. 23.) of the Minister of Interior.

[16] Point 12 of the Instruction 11/2016 (IV. 29.) of the National Police Headquarters.

[17] Paragraph (6a) of section 11 in the Facial Image Database and Facial Analysis System Act and paragraph (7) of section 11 in Decree 78/2015. (XII. 23.) of the Minister of Interior.

[18] Paragraph (5) of section 11 in Decree 78/2015. (XII. 23.) of the Minister of Interior.

facial recognition analyst service participated at the experiment carried out by ENFSI[19] in 2019 involving 27 countries, and achieved second-best result.

## Future tasks of the still image facial recognition

Continuous development is carried out in the facial recognition analysis system, from two directions: on the one hand, the manufacturer of the software carries out development and, on the other hand, the HIFS makes development proposals to the competent department of the Ministry of Interior, also supporting the operation of the system with helpful suggestions. The two organizations develop the IT system operating the SIFRS in close cooperation and propose the amendment of law if necessary. There is a serious potential in extending the source record by the front-view images of the criminal record of perpetrators,[20] as well as in allowing for international data exchange or in small amendments of the database structure to create scene-to-scene connections, similarly to that of dactyloscopy traces and DNA profiles. Further extension of preliminary image processing procedures, which are so far in a pilot phase, also pose good opportunities. Experts are working on the development of several other methods serving the facilitation and efficiency of analysis. Furthermore, the attempts as regards the quality assurance of the field should be extended, and accreditation would also be reasonable. The transfer of continuously innovated technologies and methods is essentially important to the members of bodies entitled to requisition. Equally important is the training of facial image analysts and the conduct of empirical research. In such regard, beyond the hard work of the co-workers, extensive international contacts in the working groups of Interpol and ENFSI can also be rather beneficial.

## References

Anti, Cs. L. (2017): A személyleírás története [The history of suspect description]. In Anti, Cs. L.: *A személyleírás [The personal description].* Semmelweis Kiadó, 11.

Detrői, E., Déri, P. (1967): Portré-teleidentifikáció – arcképnyilvántartás – arcképpriorálás [Portrait identification – facial image database – facial image prioritizing]. *Belügyi Szemle*, 15(5), 20.

[19] European Network of Forensic Sciences.

[20] Point 6 of annex 1 in Decree 12/2016. (V. 4.) of the Minister of Interior.

Dongshun, C., Guanghao, Z., Kai, H., Wei, H., Guang-Bin, H. (2019): Face recognition using total loss function on face database with ID photos. *Optics & Laser Technology*, 124(110), 227. https://doi.org/10.1016/j.optlastec.2017.10.016

Illár, S. (1958): Személyazonosítás fényképek szakértői vizsgálata alapján [Identification based on expert photograph analysis]. *Rendőrségi Szemle*, 6(3), 217-225.

Német, A., Tóth, G. (2019): Arcfelismerő rendszerek alkalmazása [The application of facial recognition systems]. *Belügyi Szemle*, 67(1), 129. https://doi.org/10.38146/BSZ.2019.1.10

Szigetvári, O: A magyar bűnügyi nyilvántartás kezdete [The beginning of the Hungarian criminal record]. In *Ünnepi parergák Boda József 65. születésnapja tiszteletére [Festive parerga to honour of the 65th birthday of József Boda]*. Salutem (4). Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság, 169-180. https://doi.org/10.31626/HU-EISSN2560094XTOMIV.169-180.pdf

## Internet references

URL1: *100 éves a bűnügyi nyilvántartás [100 years of criminal register]*. https://www.nyilvantarto.hu/archiv_honlap/tartalom/hirek_aktualitasok_hu_091116.html

URL2: *Instruction 58/2010. (OT 33.) ORFK of the National Police Headquarters on the introduction of Automatic Facial Image Recognition and Identification System*. http://www.police.hu/sites/default/files/58_2010_0.pdf

URL3: *At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals*. https://algorithmwatch.org/en/story/face-recognition-police-europe/

URL4: *Study on the Feasibility of Improving Information Exchange under the Prüm Decisions*. https://op.europa.eu/en/publication-detail/-/publication/6c877a2a-9ef7-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-130489216

URL5: *The Perpetual Line-Up*. https://www.perpetuallineup.org/

URL6: *Ban of Dahua and Hikvision Is Now US Gov Law*. https://ipvm.com/reports/ban-law

URL7: *Victory! Berkeley City Council Unanimously Votes to Ban Face Recognition.* https://www.eff.org/deeplinks/2019/10/victory-berkeley-city-council-unanimously-votes-ban-face-recognition

URL8: *Biometric Identification for Over 1 Billion People*. https://www.nec.com/en/case/uidai/index.html

URL9: *Japanese government to use facial recognition for Emperor's anniversary event access*. https://www.biometricupdate.com/201902/japanese-government-to-use-facial-recognition-for-emperors-anniversary-event-access;

URL10: *Chinese tech groups shaping UN facial recognition standards.* https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

URL11: *Activists Worldwide Face Off Against Face Recognition: 2019 Year in Review*. https://www.eff.org/deeplinks/2019/12/activists-worldwide-face-against-face-recognition-2019-year-review

URL12: *Álláspontunk az arckép profil nyilvántartásról [Our standpoint on face profile registration]*. https://tasz.hu/cikkek/allaspontunk-az-arckep-profil-nyilvantartasrol

URL13: *Jogtár [Legal register]*. https://jogtar.hu/uj-jogtar/

URL14: *Közérdekű adatigénylés [Applicatikon for data of general public interest]*. https://kimittud.atlatszo.hu/request/14537/response/21169/attach/3/1553%203%20V%20lasz%20k%20z%20rdek%20adatig%20nyl%20sre%20Dr.K%20m%20ves%20Bal%20zs.pdf

URL15: *Tanúsítvány [Certification]*. http://nszkk.gov.hu/content/minosegbiztositas/akkreditalt-modszerek-es-eljarasok/tan%C3%BAs%C3%ADtv%C3%A1ny_magyar_nszkk_iso9001v.pdf