VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Jan Fabián

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV JAZYKŮ
DEPARTMENT OF FOREIGN LANGUAGES

ROZPOZNÁVÁNÍ OBLIČEJE VE VIDEU A JEHO VYUŽITÍ V POLICEJNÍ PRÁCI
FACIAL RECOGNITION IN VIDEO AND ITS APPLICATIONS IN LAW ENFORCEMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jan Fabián**
AUTHOR

VEDOUCÍ PRÁCE — **Mgr. Magdalena Šedrlová**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Angličtina v elektrotechnice a informatice**

Ústav jazyků

Student: Jan Fabián ***ID:*** 203147

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Rozpoznávání obličeje ve videu a jeho využití v policejní práci

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je popsat nejnovější trendy v technologii rozpoznávání obličejů (případně i vzorů chování) ve videu a její aktuální využití v práci policie a dalších bezpečnostních složek.

DOPORUČENÁ LITERATURA:

Blokdyk, Gerardus. Facial Recognition Technology A Clear and Concise Reference.

Christman, John H. and Charles E. Sennewald. Retail Crime, Security, and Loss Prevention: An Encyclopedic Reference.

Gates, Kelly. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillence.

Termín zadání: 6.2.2020 ***Termín odevzdání:*** 12.6.2020

Vedoucí práce: Mgr. Magdalena Šedrlová

doc. PhDr. Milena Krhutová, Ph.D.
předseda oborové rady

ABSTRACT

This bachelor thesis aims to describe the facial recognition technology and its use in practice. In recent years, facial recognition technology became a heavily discussed topic, whether in connection with the deployment of this technology in China or due to its general potential for law enforcement. Facial recognition technology is a perfect example of a two-sided coin, as it brings many new possibilities of crime prevention etc. but also has the risk of being used to invade personal privacy. This thesis is based on a literature survey of some of the available resources dealing with this topic. It focuses on the history of this technology, methods used by facial recognition and mentions some examples of the use of video-based facial recognition in practice along with the social risks of the application of this technology.

KEY WORDS

Facial recognition, technology, privacy, biometrics

ABSTRAKT

Cílem této bakalářské práce je popsat technologii rozpoznávání obličejů a její využití v praxi. Zejména v posledních letech se technologie rozpoznávání obličejů stala velmi diskutovaným tématem, ať už ve spojitosti s rozšířením této technologie v Číně nebo díky potenciálu této technologie pro bezpečnostní složky. Na jednu stranu technologie rozpoznávání obličejů přináší spoustu nových možností v oblasti prevence kriminality, ale na druhou stranu s sebou také nese riziko narušení soukromí jednotlivých osob. Tato práce se zabývá historií této technologie, metodami, jenž tato technologie používá a také popisuje příklady využití technologie rozpoznávání obličejů v praxi, spolu s riziky spojenými s uvedením této technologie do praxe.

KLÍČOVÁ SLOVA

Rozpoznávání obličejů, technologie, soukromí, biometrika

FABIÁN, Jan. *Rozpoznávání obličeje ve videu a jeho využití v policejní práci.* Brno, 2020. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/127167. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků. Vedoucí práce Magdalena Šedrlová.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Rozpoznávání obličeje ve videu a jeho využití v policejní práci jsem vypracoval samostatně pod vedením vedoucí semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

Jan Fabián, podpis

PODĚKOVÁNÍ

Rád bych poděkoval vedoucí mé bakalářské práce, Mgr Magdaleně Šedrlové, za odborné vedení, konzultaci a další cenné rady při zpracování této bakalářské práce.

CONTENTS

INTRODUCTION

As the modern society increasingly deals with the area of various methods of people's identification and identity verification, in past decades, research in this area focused on biometric characteristics as those are "biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition" (ISO/IEC 2382-37:2017). It may be the increasingly easy access to modern technologies and especially their continual development that stands behind the rising interest in facial recognition.

While the thought of facial recognition software first arose in post-war era, it was not until the late 70´s when first breakthroughs occurred. Even then, the programmes for facial recognition still faced many issues, which made them unreliable, and were not used much even after the 2000s. Gates (2011) describe the influence that the attacks of 11th September had on the first steps in using the video-based facial recognition in practice. Furthermore, they were also influenced by the rapid development in technology. This development removed some major problems in facial recognition in video such as low resolution of devices, low quality of recordings and high hardware requirements of these programmes.

Whereas the general technology used for video-based facial recognition is nowadays on a high and affordable level, many differences between the areas of research can be found. Facial recognition is based on comparison of the input with a database of faces. This may be the cause of commercial facial recognition focusing on identity verification instead of recognition as private subjects do not possess the resources or legal rights necessary to obtain extensive database of faces. On the other hand, most of the government and military subjects can probably obtain such database with ease.

The use of facial recognition software in practice still has its limitations, mainly of a social and political nature. While it is possible to use facial recognition in video by implementing it in the CCTV systems that are in every major city, the pressure from the society against this usage in the name of personal freedom has increased. A very relevant example of the problematics of the way facial recognition technology can be misused is

China. As is mentioned in the publication *Toward a Reputation State*, the facial recognition technology implemented in China helps to categorize the population into different social classes based on "social credit", which changes constantly thanks to almost ubiquitous surveillance of the citizens using facial recognition tools and other techniques (Dai, 2018). Due to this, the general public audibly opposes the implementation of this technology in the fear of 1984-like society and the possible misuse of this technology not only by government but also by private subjects.

The aim of this thesis is to briefly describe the history of facial recognition along with its expansion in recent years, mention its position in the field of biometrics recognition, provide an overview of how the technology works and describe some properties of facial recognition focusing on facial recognition in video. Furthermore, the methods of possible use of this technology by law enforcement are mentioned followed by examples from practical applications in some countries of the EU, USA, and China. In the end, the social risks of facial recognition technology are considered.

1 BRIEF HISTORY

What first started as a development of general pattern recognition by computers in the 1960s, slowly transformed into research aimed at computerized facial recognition. Regarding this research, Manuel De Landa (1991) noted: “the idea was not to transfer human skills to a machine, but to integrate humans and machines so that the intellectual skills of the former could be amplified by the latter.” (1991:193). Although the facial recognition promises great potential in military applications, the main idea behind its development was the potential that the techniques, which are used by facial recognition, had for automated image processing. Due to a growth in the volume of visual information, especially in medical, science and intelligence fields, automated image processing became necessary (Gates, 2011).

A significant role in the debates about facial recognition and its use for security purposes was played by the terrorist attacks on 11th September 2001. As Sennewald and Christman (2011) mention in their book on facial recognition, the use of facial recognition technology had been fairly successfully tested earlier that year during Super Bowl in Tampa, FL. This brought the attention of the public together with a question of whether face recognition software deployed at the airport´s camera system could have helped to prevent this. The major cause for this question was a picture from the Portland, Maine, airport that allegedly shows two of the hijackers (Gates, 2011).

1.1 World's Fair in Osaka, Japan

The World´s Fair that took place in Osaka in 1970 was highly successful in presenting Japan´s post-war technological boom. One attraction, named “Computer Physiognomy”, focused on facial recognition. At this attraction, a photo of a visitor was taken and then analyzed by a computer program. This programme located and extracted some important facial features, which were then used to classify the visitors´ face into one of seven categories that were based on famous persons (Gates, 2011).

Although the programme was simple and could not be considered very reliable, it

proved to be successful and popular among the visitors. Moreover, it provided a database of pictures that Takeo Kanade used for future research of facial recognition. This database consisted of pictures of people of various ages males and females, people with accessories (e.g. glasses etc.) as well as pictures with different head and face positions (Kanade, 1977).

2 FACE IN BIOMETRIC DETECTION TECHNOLOGIES

Among other forms of biometrics used for identification, facial recognition stands out as an especially challenging method but also as a unique method of identification of people. It is unique mainly due to the fact that this method can be conducted without the knowledge or consent of the people being identified. On the other hand, the challenges that this method is presented with are caused by the fact that faces, compared to for example fingerprints, are very complex, multidimensional and they can easily change (Gates, 2011).

In practice, the biggest challenge in using facial recognition is the development of software that can accommodate for changes of the faces that are given as an input. Other biometrics used for identification usually do not encounter many changes over time. Optical fingerprinting is much more reliable due to fingerprints not changing during life. They are also absolutely unique, which significantly lowers the rate of false positive or false negative results (Gates, 2011). With iris scanning (iris is a circular, coloured structure in the eye that is responsible for the control of the diameter of a pupil) the same advantages apply, moreover, iris scanning has even lower false result rates and can be done from a greater distance than fingerprints identification (Trader, 2016).

In their publication, Sennewald and Christman (2011) discuss that even despite the technological challenges, the method of people identification with facial recognition possesses certain advantages over other methods of biometric identification. One of the major set of advantages is the possible use of this method in all monitored places by implementing it into the already existing system of CCTV cameras. The first use of this

method was tested and documented during 2001 Super Bowl in Tampa, FL. The facial image of each person attending this event was matched against a database of criminal suspects.

Facial recognition software implemented in CCTV camera systems is nowadays used not only in China, although it is probably the most widely spread there, but also for example in Australia. In her article, Rebecca Turner (2019) describes a 12-month-trial of CCTV facial recognition in the city of Perth. With the right conditions and equipment, this method can be successfully conducted over a significant distance, in crowded places and without the knowledge of subjects (Sennewald & Christman, 2011).

3 FACIAL RECOGNITION TECHNOLOGY

In one chapter of the book *Recognition of Humans and Their Activities Using Video*, we can find the description of what the aim of facial recognition software is: "given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces." (Chellappa et al., 2005:7). From this statement alone, we are able to describe the process of facial recognition that starts with the first challenge presented to the software – detecting the face. The next step is dependent on the desired outcome. In the case of verification of a face, the input is compared to a specific photo as for example in the case of Windows Hello. Windows Hello is a Windows 10 feature enabling the users to log into their devices using biometrics, namely fingerprints and face (*Windows Hello*). With face identification, however, the whole process is more difficult due to the need of comparison of the input to an extensive database of photographs (Sennewald & Christman, 2011). These processes are also called one-to-one (verification) and one-to-many (identification) matching (Zhao & Chellappa, 2006).

Facial recognition technology can be generally categorized into two main categories. The first category is facial recognition software using photography or still images and the second category is software that uses either recorded video or live-feed video (Chellappa et al., 2005). Each category has its specific properties that are, together with the methods these categories use, described in this chapter.

3.1 Facial recognition using images

At the beginning of facial recognition technology, experiments with detection and identification of people in still images took place. This process requires software that is presented with still image input and is able to provide identity or verify the identity of a person in the given image, based on their face. It consists of three important steps: "(1) Detection and coarse normalization of faces, (2) feature extraction and accurate normalization of faces, and (3) identification and/or verification." (Chellappa et al., 2005:9).

The first two steps are the key for both the identification and verification purposes of facial recognition. When the software is presented with a picture it has to determine whether there is a face and mark it as such. This can be done with a few different approaches, such as using an algorithm that finds an area where the eyes most probably are and then tests the surrounding area for the presence of other typical facial features. If it gets a positive result it will mark this area as a face and will proceed to the second step (Sharma et al., 2017).

Other possible approaches are skin colour detection and template matching method. In their research, Tripathi and his colleagues (2011) tested the combination of both of these methods. The skin colour detection is based on the fact that colour clusters of the skin shades take up a relatively small part of chromatic colour space, which makes it perfect for detecting skin regions in the picture, thus, finding the part of a picture that contains a face. The template matching method works on a principle of matching parts of the input image to templates of faces. This method usually works together with a filter to extract the edges of a face and it has the advantage of being easy to implement.

During the second step, feature extraction, an algorithm with a role of not only locating specific facial features (i.e. nose and lips) but also describing their precise shape and texture is engaged. This step is not easy for the algorithm as it has to transpose a complicated three-dimensional face into a two-dimensional image; therefore, the precise location of facial features is very important. Iqtait, Mohamad and Mamat (2018) described in their study that the most widely used algorithm for precise feature extraction is the Active Appearance Model (AAM) which extracts not only the shape but also the texture of a specified object synchronously.

3.1.1 Classification of methods of identification

The techniques used by facial recognition software at the final step of the process of recognizing the face can be divided into three categories: (1) Holistic matching methods, (2) Feature-based matching methods and (3) Hybrid methods (Chellappa et al., 2005).

Holistic matching methods are based on identifying faces by their global representation as a criterion. This means that using the holistic approach, the face recognition software uses a description of a face that is based on the entire image as opposed to a description of local facial features. On the other hand, feature-based methods describe the face as computed geometric relationships between facial features (e.g. nose, eyes, mouth etc.), which significantly lowers the demands on the software that has to directly compare this description of a face with its database during both of these methods. Hybrid methods combine the use of the whole face region and the facial features for the process of face identification (Jafri & Arabnia, 2009).

3.2 Facial recognition using video

Since the early 2000s, fast advance in technology has ensued. This significantly changed the possibilities of facial recognition using video due to the elimination of some of the key factors that limit this technology such as low video quality (Zhao et al., 2003). The development in technology helped the facial recognition in video to be put into practice, furthermore, the possibility of implementing it into already existing CCTV systems is also a key feature of this technology. Thanks to this, the facial recognition in video has vast potential for use e.g. by retailers for the identification of known shoplifters (Sennewald & Christman, 2011). The facial recognition in video is currently being tested and used in many major airports around the world. One example of this may be the Václav Havel's airport in Prague. The facial recognition technology using video was implemented there in 2017 (*Pražští policisté „otevírají diskusi"…*, 2019).

The whole process of facial recognition using video does not significantly differ from the facial recognition using images. However, we can still say that thanks to specific properties of both of these technologies, facial recognition using video is better for identification of people as opposed to facial recognition using still images, which may

find better use in the field of identity verification. Chellappa and his colleagues (2005) mention video-based facial recognition utilizing the fact that, similar to humans' perception of faces, when the subject is in motion it is easier for the software to correctly detect a face. After the first step of the detection of the face in the video sequence, the software then exercises a technique of face segmentation and pose estimation. Because the face is not always in frontal view during the video sequence, which is the ideal view for the facial recognition software, these techniques find the visible facial features and then try to form a virtual front view of the face using the pose estimation technique. Another technique utilized in video-based facial recognition is called face tracking and is further described in the chapter 3.2.2.

3.2.1 Basic approaches

In the book *Recognition of Humans and Their Activities Using Video*, we can read that the programmes for facial recognition in video use a still image frames taken from a video sequence as it is technologically easier. These programmes mostly use a system of "voting" for the result. For this vote, the programme considers recognition results from all the used frames. However, the authors also mention that new algorithms utilizing a video sequences are beginning to develop. They reference an algorithm that aimed at facial recognition using a video sequence with a moving face using a probabilistic approach (Chellappa et al., 2005).

The mentioned algorithm not only detected faces from different frames of video sequence but also considered the previous frames, which helped the algorithm to compute the probability of transition of the face into a different pose (i.e. turning head from left to right), hence the name probabilistic approach. This approach also enabled the algorithm to deal with frames containing a partially covered face. The algorithm again took into account the previous frame of the sequence and was then able to estimate an area covered by an object and moreover, it was able to reconstruct the covered part of the face to some extent (Lee et al., 2003).

Since the publication of the *Recognition of Humans and Their Activities Using Video* in 2005, the methods for video-based face recognition evolved and many new approaches appeared. Zheng and his colleagues talk about these new approaches in a

chapter of the book *Handbook of Biometrics for Forensic Science*. This chapter, *Recent Developments in Video-Based Face Recognition*, mentions approaches that are currently being used by facial recognition programmes. These include sparse coding, geometrical model-based and dynamical model-based approaches. The further development of the probabilistic approach is also mentioned in this chapter (Zheng et al., 2017). *Recent Developments in Video-Based Face Recognition* is an especially interesting publication as we can use it to compare the development of approaches utilized by this technology in just 12 years since Rama Chellappa (one of the authors of *Recognition of Humans and Their Activities Using Video*) was also a member of the collective of its authors.

3.2.1.1 Sparse coding approach

This approach relies on dictionaries created from test video-sequences. Dictionaries are sets of faces or facial features extracted from these video-sequences with one dictionary corresponding to one set of images containing the same face. As these images of a face may vary during the video-sequence in lightning or the pose of the face, they are partitioned into various clusters that contain roughly the same pose and illumination of the face. A set of sub-dictionaries for these clusters is created this way. For identification, the video-sequence is also partitioned into clusters of images of the detected face which are then compared to the dictionaries. The use of sub-dictionaries in this approach enables the programme to handle video-sequences with large variations in illumination or in the pose of the face (Zheng et al., 2017).

3.2.1.2 Geometrical and dynamical model-based approaches

When analyzing a video-sequence using geometrical model-based approach, the programme firstly constructs geometrical models corresponding to the detected faces. The models constructed by this approach can have different forms, i.e. 3D head models or spherical head models. In the next step, texture map of the detected face is created and projected onto the model (see figure 1). Especially the use of spherical harmonic representation of the facial texture map projected onto a spherical head model proved to be potent. Lastly, the programme extracts the facial features and can proceed with the identification (Zheng et al., 2017).

Dynamical model-based approaches work with the video sequence as it is a dynamical system and they use individual video frames as the output of this system. This approach is sometimes used in a video-to-video face recognition but other than that, they are mostly used for activity or motion recognition applications (Zheng et al., 2017).

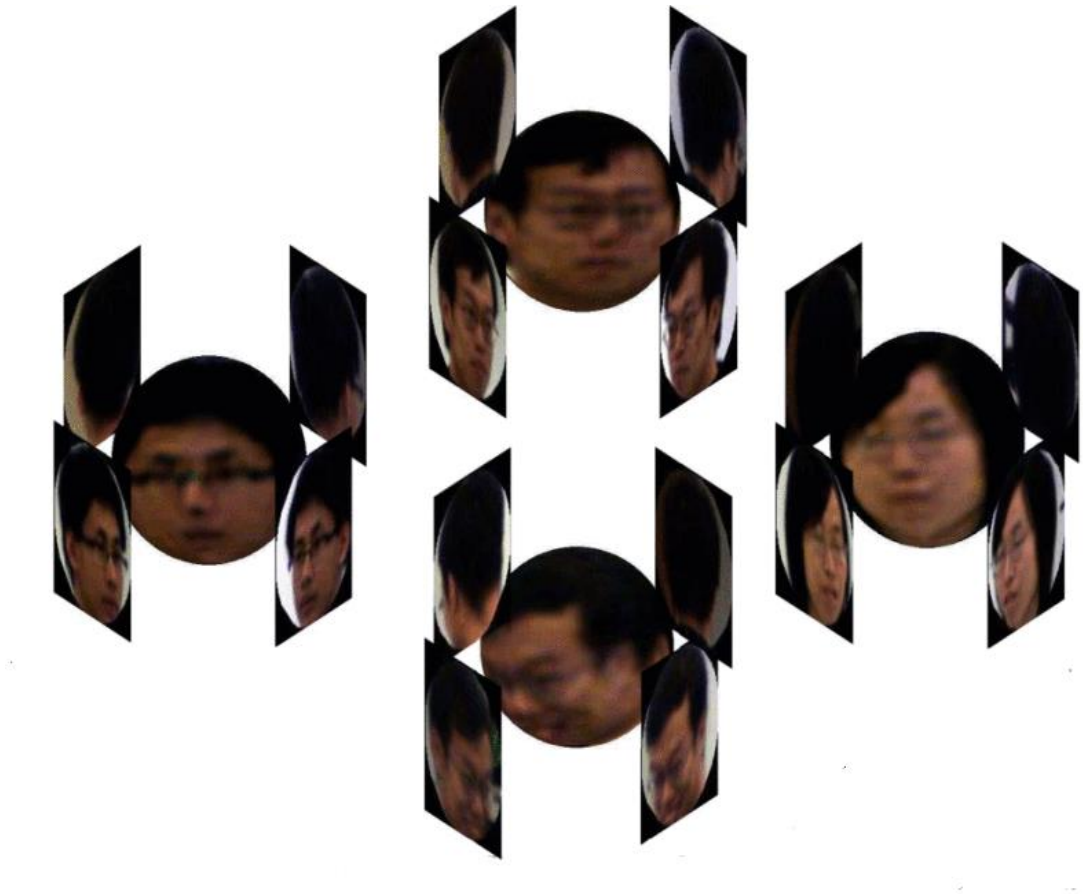

Figure 1 Texture map projections, reprinted from Du et al. (2014)

3.2.2 Face tracking & Snapchat

One especially important technique used by facial recognition software working with video sequences is called face tracking. Since the detected face is located in a different position in every frame of the video sequence, this technique is implemented to estimate the motion of the face and it essentially has to detect the face in every frame of the video. Facial tracking can track the position of the face region, just the position of facial features or it can use combination of both (Chellappa et al., 2005). The use of Active Shape Models (ASM) has proved to be very efficient when used for the tracking of a face and is

nowadays widely used together with this technique (Manousopoulos et al., 2007).

Active Shape Models are generally used for all kinds of shape tracking. The ones used in facial tracking are a statistical representation of a face made of a set of landmark points which correspond to the facial features (see figure 2). These landmark points are distributed by an algorithm utilizing a general face representation based on a training set of images with manually located landmark points. The algorithm then relocates some of the landmark points, so they correspond with the detected face as precisely as possible (Manousopoulos et al., 2007).

Figure 2 Landmark points (left) and Active Shape Model (right) placed on detected face, retrieved from Vox (2016)

An example of the use of Active Shape Models in practice is the mobile application Snapchat. This application offers a variety of filters that are not only able to augment still images of faces but also real-time video. The function of these filters is based on detecting the users' face and tracking the user's motion and even actions, such as opening their mouth or closing their eyes, using the Active Shape Models as a mask that can be projected onto or altered by the software in some way (e.g. adding a hat, adding colour effects or changing the shape of the face) (Vox, 2016).

4 FACIAL RECOGNITION IN PRACTICE

As mentioned in the previous chapters, especially in recent years, facial recognition has found its place in many commercial, police or military applications. One of the more interesting examples of commercial application is the possible use of this technology for locking and unlocking doors. In their paper *Smart Door Access using Facial Recognition*,

Deshwal and his colleagues (2019) propose both easy to implement and fully automated secure system of getting access through doors by face identification, going as far as implementing a function to notify the administrator when an unrecognized face is detected.

Eyedea Recognition, a Czech company offering a variety of products aimed at computerized pattern recognition, has made itself known in the market of facial recognition technology. Their software for recognition of faces is currently being used by Europol, Police of the Czech Republic and National Drug Headquarters of the Criminal Police and Investigation Service. One of the other products in the portfolio of this company is a product called Anonymizer. It detects faces and license plates and applies blurring filter on them, which is used for example by Seznam a.s. in their Panorama service. Another interesting software is the Video Matching. This is a software capable of finding a short video sequence in another video. This software can be used for video content detection or copyright protection (*Eyedea Recognition*).

4.1 Law enforcement

A major practical application of facial recognition in law enforcement is its use in forensic science. The main goal of forensics is to scientifically analyze data that were acquired by law enforcement agencies. In their paper, *Some challenges in forensics*, Jain and his colleagues (2011) talk about the necessity of the development of facial recognition technology to give forensics more ways of determining a person's identity. While the use of DNA and fingerprints are the most reliable methods, the ability to use for example surveillance cameras' footage is another great tool. In their paper, they describe the difference between forensic and automated facial recognition. Moreover, they mention some challenges for forensic facial recognition and few methods of its utilization (i.e. forensic sketch recognition, video-based facial recognition and near-infrared recognition).

As mentioned in *Some challenges in forensics*, two main differences between forensic and automated facial recognition can be described. The first is the quality of images or video sequences used. Although images in the law enforcements' databases are usually comparable to images used in automated facial recognition (frontal pose,

controlled illumination, and normal expression), the images of culprit etc. are not. This can be caused by low-quality surveillance cameras, different face poses or partially covered face of the culprit. The second difference is the involvement of humans in the process of forensic facial recognition (see figure 3) (Jain et al., 2011).

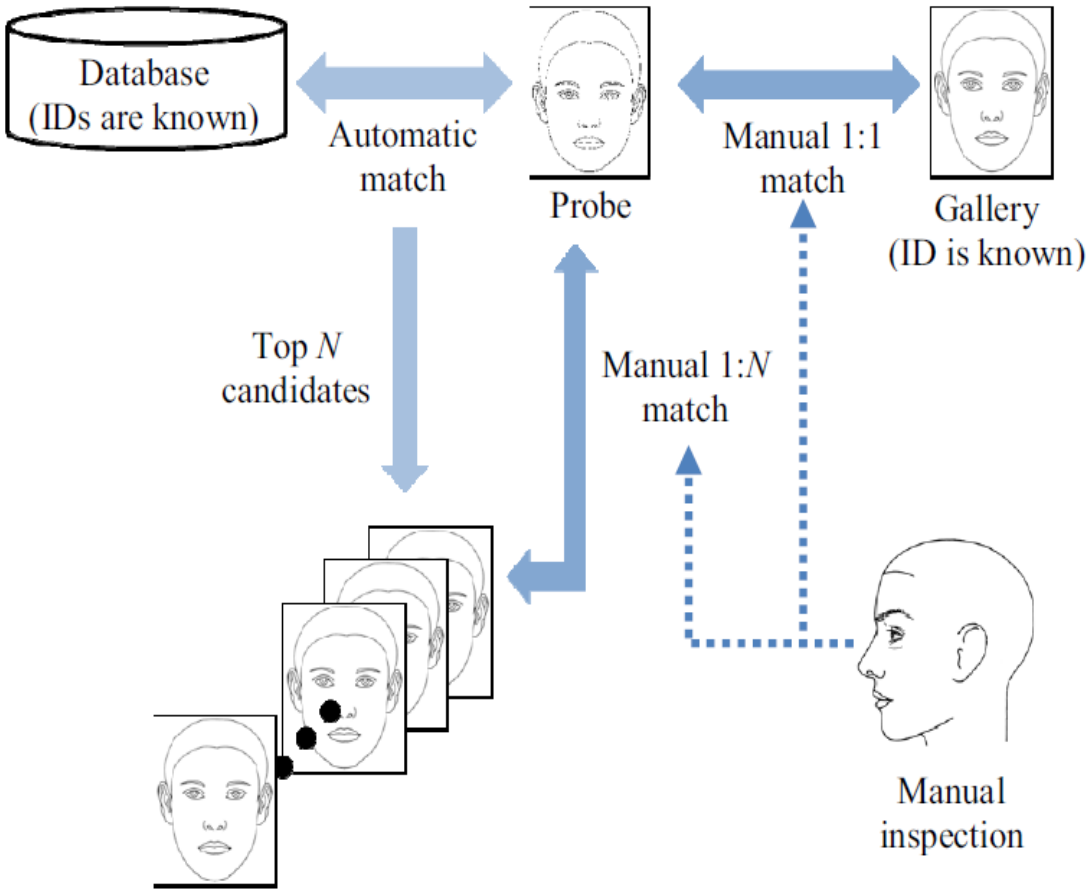

Figure 3 Schematic of the process of forensic facial recognition, reprinted from Jain et al. (2011)

Due to the nature of forensics and the consequences of falsely accusing someone of committing a crime, the automatic system chooses subjects from the database that are the most similar to the image of the culprit (the term probe is used by Jain and colleagues). These matches are then examined manually by forensic experts to determine the correct match. This is needed to be done partly due to law enforcement needing sound and most importantly correct evidence, and partly due to the differing quality of the probes (face sketches, low-resolution images, partially covered faces etc.) (Jain et al., 2011).

4.1.1 Face sketch recognition

One of the methods of forensic facial recognition that offers many new possibilities for law enforcement is face sketch recognition technology. Especially in cases with no surveillance footage available or with very limited information about the suspect, a sketch of the suspect based on the witness' description is usually made. This sketch can then be used to find possible suspects in the police databases using various approaches to face sketch recognition (Wan & Lee, 2017). However, traditional methods of facial recognition are not very suitable for this task as they do not give good results. This is mainly due to many issues such as inaccuracies in sketch images caused by the memory of the witness or miscommunication between the witness and the sketch artist. (Galea & Farrugia, 2017) New specialised approaches (i.e. FaceNet approach or the use of deep learning) greatly increase the success rate as opposed to traditional facial recognition methods, even though they also pose new challenges.

FaceNet is a system presented by Schroff and his colleagues in their publication *FaceNet: A Unified Embedding for Face Recognition and Clustering* (2015). It is a system that "directly learns a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity" (Schroff et al., 2015:815). This system is used in the work of Wan and Lee to propose a new approach to face sketch recognition. Firstly, they convert the images in the database to sketch style to reduce the difference between photograph and sketch. Secondly, the feature vectors of the sketches are obtained and can be used to find the probe sketch in the database (Wan & Lee, 2017).

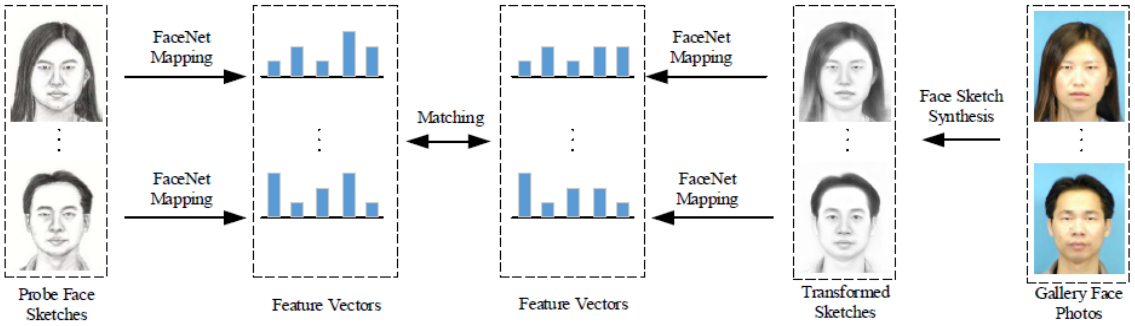

Figure 4 Schematic of FaceNet based face sketch recognition method, reprinted from Wan & Lee (2017)

Figure 4 shows the schematic of the method with an interesting part being the differences in probe sketches. Since the images come from public database (Chinese University of Hongkong face sketch database) that consists of one photograph and one drawn sketch of each face, we cannot say whether these differences can be caused by miscommunication as mentioned previously.

Another approach to the face sketch recognition that may prove to be very successful is the use of deep learning-based architecture (Galea & Farrugia, 2017). Deep learning is a technique used to teach computers to learn by example. It is a key technology for the development of software for driverless cars or voice control. With the use of deep learning, a computer model can learn to perform classification tasks from images. However, to achieve the state-of-the-art accuracy of the model's classification, they need to be trained by using extensive sets of data that are already pre-classified (*What is Deep Learning?*). In their research, Galea and Farrugia (2017) also describe the main advantage of using deep learning networks as the ability of such network to reliably compare even images with such differences as a photograph and sketch. However, they also mention one limiting factor of this system, which is the need to train deep learning networks on a large number of examples for them to be robust. Relatively few sketch images and photo-sketch pairs are publicly available, which together with the fact that usually only one sketch of each subject is made accounts for the problematic of creating examples to train deep learning network on.

4.1.2 Video-based facial recognition

As mentioned previously in this thesis, video-based facial recognition has proven to be a very invaluable tool for law enforcement. It has gained significantly more attention in recent years and various uses of this technology in practice emerged. Apart from the possible deployment of this technology in CCTV and other surveillance systems (*Pražští policisté „otevírají diskusi"…*, 2019), methods of mobile use of this technology such as body-worn cameras (Bromberg et al., 2020) or a mobile facial recognition van are also being tested (Fussey & Murray, 2019).

In a paper for the *Future Generation Computer Systems* journal, Sajjad and his colleagues (2017) propose Raspberry Pi assisted method of facial recognition that

promise cost-effective solution of public suspect detection. This method is based on a wireless camera connected through Raspberry Pi to a computational server running the facial recognition algorithm. The main benefit of this proposed method is a relatively simple solution that can help law enforcement agencies with real-time identification of suspects with the utilization of uniform-mounted cameras for police officers. (Sajjad et al., 2017) Body mounted cameras, providing visual evidence, moreover, having the capability of real-time facial recognition, were, for example, adopted in law enforcement agencies in the USA. Bromberg and his colleagues (2020) conducted a list experiment aimed at the level of public support for facial recognition utilized via body-worn cameras. In their findings, they mention that although the majority of respondents support this use of facial recognition in general, on an individual level, self-reported support of this technology by some of the respondents decreases.

4.1.2.1 The London Metropolitan Police Service's trial

The practical application of video-based facial recognition was trialled in the UK between 2016 and 2019. In total 10 test deployments of video-based facial recognition during policing operations were conducted by the Metropolitan Police Service. In those test deployments, either fixed position cameras or cameras mounted on a mobile van were used. The observation of camera feeds was done by police officers, who also discussed computer-generated matches similarly to the process in figure 3. Figure 5 shows the specific diagram of the process of decision making during these tests as depicted in the *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Fussey & Murray, 2019).

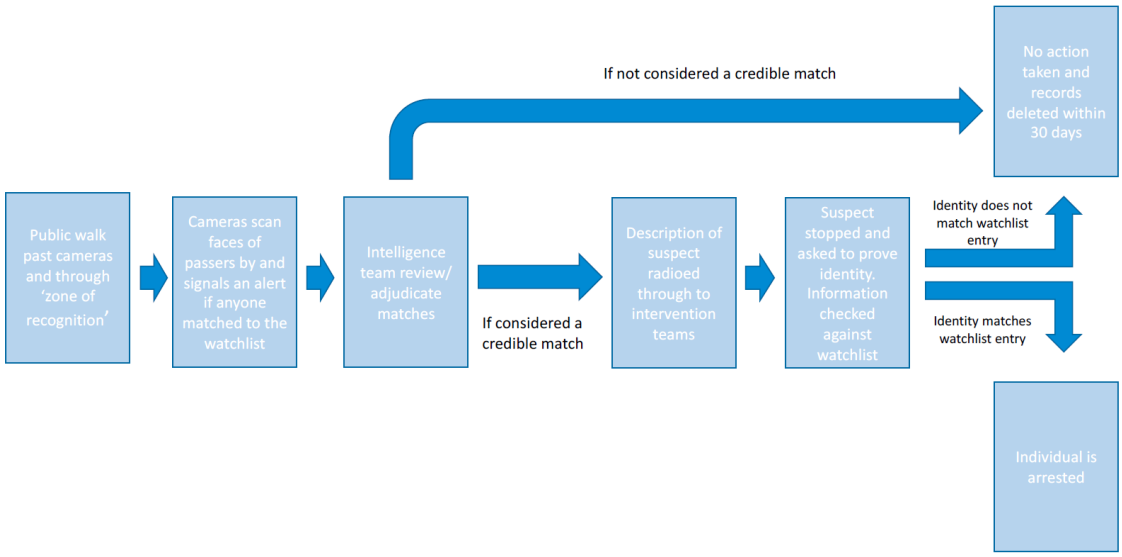

Figure 5 Schematic of the process of decision making during live facial recognition tests, reprinted from Fussey & Murray (2019)

In the case of a positive match, an alert was generated in the control room and on portable devices of officers near the site of deployment. This, however, led to situations in one of the tests, when the decision of the control room-based operatives not to intervene was "overruled" by street-based operatives with the reasoning of their separate access to the match information. During the six tests observed in the process of writing the report, the facial recognition system generated 46 matches (42 acceptable for analysis). The operatives ruled 16 of those matches as "non-credible" and ordered 26 identity checks based on the match, with 4 attempts unsuccessful as the individuals lost in a crowd. Of the 22 identity checks, 14 were verified as "false-positive match" and 8 as correct matches. This means that during the 6 observed trials, the facial recognition software had a 19.05% success rate (8 out of 42 matches) (Fussey & Murray, 2019).

4.2 Practical applications in the European Union

As of 2020, activities and experiments with facial recognition and other biometric technologies for surveillance were conducted in approximately 15 European countries. These include for example the Czech Republic, France, Germany, UK, Poland or Austria (see figure 6). However, many of these deployments of facial recognition technology have created a strong backlash from the general public and civil society organisations.

In May 2020, EDRi (European Digital Rights) association of European civil and human rights organisations published a document *Ban Biometric Mass Surveillance* in which they call on EU bodies and EU Member States to indefinitely ban the use of biometric surveillance technologies. The main reason for this is the concern that existing laws are not sufficient for the use of this technology by law enforcement and that the conducted trials can be considered unlawful (Jakubowska & Narajo, 2020). Similar concerns are mentioned in the *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Fussey & Murray, 2019).

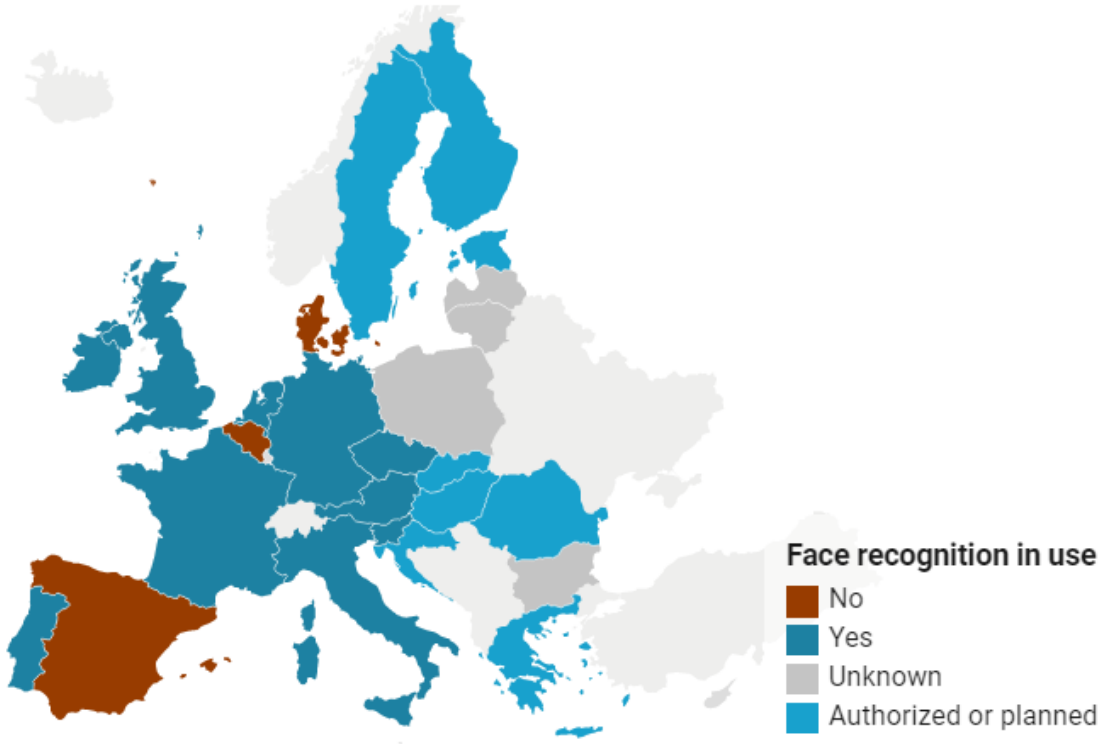

Figure 6 Use of facial recognition in law enforcement in the EU, reprinted from Kayser-Bril (2019)

4.2.1 Czech Republic

In the Czech Republic, the use of facial recognition technology was accentuated when the Prague police asked permission to use this technology in Prague's CCTV circuit. As of April 2020, no definitive resolution is given either by Prague or the Office for Personal Data Protection. This office, however, forbid the use of facial recognition technology for

identification of football hooligans in stadiums in 2019. Their reasoning was that insufficient legal grounds for the use of biometric personal data exists (*Kamery pro rozpoznávání obličejů…*, 2019).

Upon query regarding this thesis, no response about the use of facial recognition technology or possible future plans was received either from the Police of the Czech Republic or National Drug Headquarters. Spokesperson of the Brno Metropolitan Police responded that the facial recognition technology is currently not used by the Brno Metropolitan Police and there are no plans for future applications of this technology. Therefore, the only official deployment of this technology in the Czech Republic is currently the Václav Havel's airport in Prague (*Pražští policisté „otevírají diskusi"…*, 2019).

4.2.2 UK

As mentioned previously, trials of video-based facial recognition were conducted in the UK between 2016 and 2019. Following these trials, the Metropolitan Police adopted video-based facial recognition into their regular operations as the commissioner Cressida Dick stated in her speech on technology and its role in fighting crime (*Commissioner talks…*, 2020). Facial recognition is also used by police in South Wales. Their use of facial recognition technology was even brought to court in the autumn of 2019, however, the UK High Court ruled that the use of this technology by South Wales police is consistent with the data protection legalisation and the Human Rights Act (*Automated facial recognition*, 2019). On the other hand, the Police Scotland concluded that the facial recognition technology is not fit for their use in its current form and even though they initially planned to introduce facial recognition technology in 2026, they also stated that there would be no justifiable basis for them to invest in this technology in its current state (Lynch, 2020).

4.2.3 Poland

With the widespread of COVID-19 in early 2020, Poland developed and put into use the "Home Quarantine" smartphone application. The use of this application was made mandatory for every person that has been ordered 14 days quarantine after their return

from abroad. While crossing the borders, the person has to fill a localization form containing their personal information and address, where they were going to spend the quarantine period. After installing the application and matching their account to the database using phone number authentication, the user takes a photograph of their face that serves as a reference. Each day of the quarantine (randomly throughout the day) the user gets a notification to verify their identity and location. This is done by taking a selfie, which is matched to the reference photograph, and also by localization of the phone through the application. After the notification, there is a 20-minute time window to take the selfie. If the user does not make the selfie in time, they get a warning, and police might get a notice to check whether the quarantine is observed (*Aplikacja „Kwarantanna domowa"…*, 2020).

4.3 Practical applications in the USA

In 2016, Claire Garvie together with Georgetown University published an investigation on police use of facial recognition technology. In their publication (*The Perpetual Line-up: Unregulated Police Face Recognition in America*), they found out that at least 26 states already allow the use of facial recognition by law enforcement. For example, Florida and Texas use various systems of facial recognition and their law enforcement have access to extensive photo databases (Garvie, 2016). For the use of facial recognition in law enforcement in the USA, the FBI also provide Facial Analysis, Comparison and Evaluation (FACE) services. Those services offer a large database of photographs (approximately 640 million). While part of this database consists of mugshots, the majority is provided by state institutes such as driver's licence photographs provided by DMW, Visa applicant photographs or U.S. passport application photographs. (Bromberg et al., 2020)

One of the methods of the use of facial recognition by law enforcement in the USA are the body-worn cameras mentioned before (Bromberg et al., 2020). On some airports, the facial recognition technology is also used by the U.S. Customs and Border Protection agency, namely in New York (JFK), New Jersey (EWR), Miami (MIA) or Los Angeles (LAX) (*Biometrics*).

However, with the spread of the use of facial recognition by law enforcement, some states and cities have declared a ban on this technology. During 2019, California, Oregon and New Hampshire passed laws banning the use of aforementioned facial recognition technology in body-worn cameras (Samsel, 2019), and San Francisco, CA, Sommerville, MA, and Oakland, CA, banned city departments from using any form of facial recognition technology (Metz, 2019).

4.4 Practical applications in China

Since the beginning of the 21st century, China installed a large number of CCTV cameras, followed by smart cameras capable of assisting a software of pattern recognition, such as facial recognition etc. A portion of these systems are managed by private companies strongly supported by the government in the further development of these technologies. Some of the common examples of the use of facial recognition are cameras installed to fight against jaywalking and to monitor pedestrian traffic (Fieux-Castagnet & Santucci, 2020).

The facial recognition technology in China surveillance systems is functional approximately since 2010. In 2014, China's State Council introduced a plan to employ mandatory nationwide Social Credit System that should be fully operational by 2020. This system uses facial recognition technology as one of the means of tracking people and their activities and amending their social-credit scores. Based on their score, people can then be kept from using certain kinds of transportation, taking loans etc. Reportedly, 4.3 million people were restricted from travelling by high-speed railway based on their social-credit score in 2018 (Qiang, 2019).

Another use of cameras capable of facial recognition was especially apparent in the Xinjiang region, where the ability to categorise the ethnicity of people was used to identify people of Uyghur origin. Uyghurs are a heavily repressed minority in China, and it is probable that this technology was used in the Xinjiang region to assist the arrests and control of this minority by the government of China (Qiang, 2019).

5 SOCIAL RISKS

With the expanding use of facial recognition technology, the need to address the social aspects and influence on citizens arises. The deployment of facial recognition and other methods of biometric surveillance is often: accompanied by lack of transparency, without public engagement (i.e. public debates) or without sufficient guidelines and laws (Grimond & Singh, 2020). This may result in a violation of various human rights such as the right to privacy or the rights to freedom of expression.

One of the main points with regards to facial recognition technology and the right to privacy is the right to private life, in which the elements related to individual's identity and establishing relationships with the outside world are contained. Therefore, the issue can be described as whether the facial recognition technology in public space represents an interference with the right to privacy (Fussay & Murray, 2019). Sennewald and Christman (2011) address the topic of privacy as dependant on the purpose for which is the facial recognition technology used. They agree that the use of this technology for tracking people poses a serious threat. However, they also mention that the use of this technology for the prevention of shoplifting is less concerning with regards to the general public.

Another social aspect of facial recognition, especially the deployment of this technology in camera systems, is the impact on already over-surveilled groups. This is an issue with any monitoring conducted without prior suspicion of a specific target (mass surveillance) (Jakubowska & Narajo, 2020). For example, Fieux-Castagnet and Santucci (2020) describe the use of facial recognition to specifically identify the Uyghur minority in China. Fussay and Murray (2019) also mention the influence, knowledge of the deployment of facial recognition technology in public may have on individuals. They mention that due to a fear of possible consequences, individuals may be reluctant to go into public places, meet particular individuals or organizations or take part in protests. This is in contrast with the rights to freedom of expression and also right to freedom of assembly and association.

The possibility of misuse of the facial recognition technology is another commonly mentioned aspect. The potential of authoritarian abuse of this technology is strong, as it

can be used or re-deployed in more ways than people initially provided consent to. Some states showed, for example during the global coronavirus pandemic that, they may take advantage of available technology in more ways than necessary to manage the situation (Jakubowska & Narajo, 2020).

5.1 Social risks in the Czech Republic

For the time being, the use of facial recognition technology in the Czech Republic does not present a risk to the general public. It is used only on Václav Havel's airport, and as the Police stated after their proposal for the use in Prague, they primarily want to start a debate, which should be part of any plans revolving around the implementation of facial recognition by law enforcement.

In late 2018, the German state of Saxony announced a new plan of implementing facial recognition cameras, especially in border regions. This created a strong backlash from Czechs and Poles, with both heavily criticizing the use of this technology as it may represent a form of distrust towards foreign commuters (Mayhew, 2019).

One major issue arose when it came into light (in late 2019) that planned electronic vignette system for highways was supposed to have secret built-in features. Apart from the ability to recognize license plate and whether the user has valid vignette, the system was also supposed to store the images for possible use by law enforcement. This feature of the system was criticised as an intrusive into personal privacy (Nádoba, 2020).

CONCLUSION

With the constant development of technology, it is not very common nowadays to find ourselves out of the reach of some electronic devices. We carry our smartphones with us everywhere we go, most of us use laptops on a daily basis, and in every major city or places such as airports, we often find ourselves to be watched by large number of CCTV cameras. It was the aim of this thesis to acquaint readers with the process of the development of facial recognition technology, with the role of facial recognition in the field of biometrics detection, and moreover, to mention the possibilities and practical applications in law enforcement as well as the social risks this technology presents for citizens. This was achieved by making a survey of the available literature concerning this topic.

When talking about facial recognition, the methods it utilizes and its use in practice, we can talk about clear division of this technology into two main categories. This thesis deals with both facial recognition using images and video-based facial recognition. In conjunction with the video-based facial recognition, the difference between scientific publications from the year 2005 and from 2017, both dealing with new approaches in this technology, was discussed.

Furthermore, the specification of facial recognition in forensics, as mentioned in various literature, were discussed. After this, the approaches to the use in law enforcement and examples of practical applications of facial recognition technology in some countries of the EU, USA and China were described. Unfortunately, no response from various police bodies in the Czech republic was received after query regarding the facial recognition technology and possible plans for its deployment.

In the last chapter, we mention the social risks of this technology and its use, as this technology can have negative impact on human rights such as the right to privacy. Some occasions when facial recognition technology sparked controversy in the Czech Republic are also mentioned here.

In conclusion, the technology of facial recognition does not deal with as many technological issues nowadays as it dealt with just two decades back. What is an issue

that this technology encounters is a social pressure against the use of facial recognition technology in public. This is mainly due to the way China implemented this technology, the possible intrusion of human rights or lack of legal background for its implementation. These factors limit the use of this technology on a larger scale and are the cause of initiatives to heavily limit or ban facial recognition, especially in law enforcement.

ROZŠÍŘENÝ ABSTRAKT

Zejména v poslední dekádě se technologie na rozpoznávání obličejů stala velmi diskutovaným tématem. Je to v prvé řadě rychlý technologický vývoj, který stojí za odstraněním překážek bránicím praktičtějšímu využití technologie na rozpoznávání obličejů, jako jsou například nízké rozlišení a kvalita záznamů a vysoké nároky na použitý hardware. O této technologii se často diskutuje právě ve spojitosti s účely, pro které je rozpoznávání obličejů využíváno v zemích jako např. Čína nebo také díky potenciálu, který tato technologie nabízí bezpečnostním složkám. Ať už je tento potenciál možno využít v prevenci kriminality, nebo při policejním vyšetřování, jsou s touto technologií spojená také různá bezpečnostní a společenská rizika.

I přestože je současná technologie, která se pro rozpoznávání obličejů používá, na vysoké technologické a cenově dostupné úrovni, objevují se mnohé rozdíly mezi oblastmi jejího výzkumu. Základním kamenem technologie na rozpoznávání obličejů je porovnávání vstupního obrazu s databází obličejů. Právě toto může být důvodem pro komerční využití této technologie pouze k ověřování identity namísto identifikace neznámých osob, jelikož soukromé subjekty často nemají zdroje či pravomoci k vytvoření těchto značně rozsáhlých databází obličejů.

Cílem této bakalářské práce je zevrubně popsat historii technologie na rozpoznávání obličejů spolu s možnými důvody pro rozmach této technologie v posledních letech. Dále tato práce uvádí pozici, kterou technologie na rozpoznávání obličejů zaujímá v rámci detekce biometrik. Následně je v této práci obsažen přehled technologických postupů, na jejichž základě technologie na rozpoznávání obličejů funguje, včetně některých specifických vlastností této technologie. V praxi se nabízí spousta možností, jak využít tuto technologii pro policejní práci, ať už pro vyhodnocení záznamů v reálnem čase, či pozdější identifikaci osob na základě fotografií nebo policejních náčrtů. Nejen teoretické možnosti pro policejní složky a forenzní vědy, ale i některé příklady z praxe v Číně a ve vybraných zemích EU a USA jsou také zmíněny v této práci. Na závěr tato práce představuje společenská rizika spojená s použitím technologie na rozpoznávání obličejů včetně krátkého zaměření na Českou republiku. V rámci zpracování této práce bylo využito rešerše dostupné literatury zabývající se jak technologickými, tak i sociálními

aspekty technologie na rozpoznávání obličejů. Zajímavou částí bylo pozorování zmíněného technologického vývoje po roce 2000, což bylo obzvláště patrné na rozdílech v literatuře a popsáno v souvislosti s publikacemi R. Chellappy a kol.

V rámci technologie rozpoznávání obličejů, používaných metod a možných praktických aplikací, můžeme mluvit o jasném rozdělení této technologie na dvě kategorie. Tato bakalářská práce se zabývá oběma, a to jak technologií na rozpoznávání obličejů používající fotografie, tak technologií založenou na rozpoznávání obličejů ve videu. Rozdíly, jejich odůvodnění a další specifikace použití technologie na rozpoznávání obličejů ve forenzních vědách, jsou na základě odborné literatury také rozebírány v této práci. K reálnému využití technologie na rozpoznávání obličejů v práci policejních složek existuje spousta lišících se přístupů. Pro účely této práce byly popsány přístupy bezpečnostních složek v USA, využití technologie na rozpoznávání obličejů pro systém „společenského kreditu“ v Číně a praktické příklady z některých zemí EU. V rámci zpracování této bakalářské práce byly také osloveny vybrané bezpečnostní složky České republiky s dotazy o používání této technologie a případných budoucích plánech jejího využití. Tyto dotazy však bohužel zůstaly bez odezvy.

Poslední kapitola, zabývající se různými sociálními aspekty použití technologie na rozpoznávání obličejů bezpečnostními složkami, popisuje silný negativní dopad, který může implementace této technologie mít na lidská práva, jako například právo na soukromí nebo shromažďovací právo. V rámci této kapitoly jsou také zmíněny některé události spojené s technologií pro rozpoznávání obličejů, které v posledních letech vyvolaly kontroverzi v České republice.

Na závěr můžeme říct, že technologie na rozpoznávání obličejů se už zdaleka nepotýká s tolika technologickými problémy jako se potýkala ještě dvě dekády zpět, což umožnilo její silný rozmach. Technologické problémy však byly nahrazeny stále rostoucím společenským tlakem proti uvedení této technologie do praxe, zejména pro využití bezpečnostními složkami. Za tímto tlakem stojí především několik faktorů. Způsob, jakým tuto technologii implementovala např. Čína, možné narušení lidských práv a svobod anebo nedostatek právního zázemí pro odůvodnění použití této technologie v policejní práci. Jsou to také tyto faktory, které v současné době omezují praktické využití technologie na rozpoznávání obličejů ve větším měřítku a které jsou důvodem

různých iniciativ o silné omezení nebo úplný zákaz používání technologie na rozpoznávání obličejů v policejní práci a práci jiných bezpečnostních složek.

LIST OF REFERENCES

Aplikacja „Kwarantanna domowa" - ruszył proces jej udostępniania. *Gov.pl* [online]. 2020. Retrieved from: https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa--ruszyl-proces-jej-udostepniania

Automated facial recognition. In: *Gov.uk* [online]. 2019. Retrieved from: https://www.gov.uk/government/news/automated-facial-recognition

Biometrics. *U.S. Customs and Border Protection* [online]. Retrieved from: https://www.cbp.gov/travel/biometrics#What-does-it-mean

BROMBERG, Daniel E., Étienne CHARBONNEAU and Andrew SMITH, 2020. Public support for facial recognition via police body-worn cameras: Findings from a list experiment. In: *Government Information Quarterly* [online]. DOI: 10.1016/j.giq.2019.101415. ISSN 0740624X. Retrieved from: https://linkinghub.elsevier.com/retrieve/pii/S0740624X19300449

CHELLAPPA, Rama, Amit K. ROY-CHOWDHURY and S. Kevin ZHOU. Recognition of humans and their activities using video. San Rafael: Morgan, c2005. ISBN 15-982-9006-1.

Commissioner talks about how technology is helping to fight crime. In: *Metropolitan Police* [online]. http://news.met.police.uk, 2020. Retrieved from: http://news.met.police.uk/news/commissioner-talks-about-how-technology-is-helping-to-fight-crime-395188

DAI, Xin. Toward a Reputation State: The Social Credit System Project of China: The Social Credit System Project of China. SSRN Electronic Journal. 2018/01/01. DOI: 10.2139/ssrn.3193577.

DESHWAL, Amit, Mohnish CHANDIRAMANI and Umesh SURANA. Smart Door Access using Facial Recognition. International Journal of Trend in Scientific Research and Development. 2019/02/28, Volume-3, 442-443. DOI: 10.31142/ijtsrd21363.

DU, Ming, Aswin C. SANKARANARAYANAN and Rama CHELLAPPA, 2014. Robust Face Recognition From Multi-View Videos. *IEEE Transactions on Image Processing*. **23**(3), 1105-1117. DOI: 10.1109/TIP.2014.2300812. ISSN 1057-7149. Retrieved from: http://ieeexplore.ieee.org/document/6714452/

Eyedea Recognition [online], Retrieved from: https://www.eyedea.cz

FIEUX-CASTAGNET, Geneviève and Gerald SANTUCCI, 2020. *An Ethical Facial Recognition: An Oxymoron?*. Retrieved from: https://www.researchgate.net/publication/340846119_AN_ETHICAL_FACIAL_RECOGNITION_210420

FUSSEY, Peter a Daragh MURRAY, 2019. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*.

GARVIE, Claire, 2016. *The Perpetual Line-up: Unregulated Police Face Recognition in America*. Georgetown Law, Center on Privacy & Technology.

GALEA, Christian and Reuben A. FARRUGIA, 2017. Forensic Face Photo-Sketch Recognition Using a Deep Learning-Based Architecture. In: *IEEE Signal Processing Letters* [online]. s. 1586-1590 DOI: 10.1109/LSP.2017.2749266. ISSN 1070-9908. Retrieved from: http://ieeexplore.ieee.org/document/8025793/

GATES, Kelly A. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. NYU Press, 2011. ISBN 978-0814732090.

GRIMOND, Will and Asheem SINGH, 2020. *A Force For Good? Results from FOI requests on artificial intelligence in the police force*. Retrieved from: https://www.thersa.org/discover/publications-and-articles/reports/ai-police-force

ISO/IEC 2382-37:2017: Information technology — Vocabulary — Part 37: Biometrics.

IQTAIT, M., F. S. MOHAMAD and M. MAMAT. Feature extraction for face recognition via Active Shape Model (ASM) and Active Appearance Model (AAM). IOP Conference Series: Materials Science and Engineering [online]. 2018, 332 DOI: 10.1088/1757-899X/332/1/012032. ISSN 1757-8981. Retrieved from: http://stacks.iop.org/1757-899X/332/i=1/a=012032?key=crossref.09eab304dce016046d563966bbaf7acb

JAFRI, Rabia and Hamid R. ARABNIA. A Survey of Face Recognition Techniques. Journal of Information Processing Systems [online]. 2009, 5(2), 43-45 DOI: 10.3745/JIPS.2009.5.2.041. ISSN 1976-913X.

JAIN, Anil K., Brendan KLARE and Unsang PARK, 2011. Face recognition: Some challenges in forensics. In: *Face and Gesture 2011* [online]. IEEE, 2011 DOI: 10.1109/FG.2011.5771338. ISBN 978-1-4244-9140-7. Retrieved from: http://ieeexplore.ieee.org/document/5771338/

JAKUBOWSKA, Ella and Diego NARAJO, 2020. Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States. Brussels. Retrieved from: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

KAYSER-BRIL, Nicolas. At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals. In: *Algorithm Watch* [online]. 2019. Dostupné z: https://algorithmwatch.org/en/story/face-recognition-police-europe/

Kamery pro rozpoznávání obličejů zažívají celosvětový rozmach, Čína už jich nasadila 200 milionů. In: *Česká televize* [online]. 2019. Retrieved from: https://ct24.ceskatelevize.cz/veda/2991737-kamery-pro-rozpoznavani-obliceju-zazivaji-celosvetovy-rozmach-cina-uz-jich-nasadila-200

KANADE, Takeo, 1977. Computer recognition of human faces. Basel [etc.]: Birkhäuser. Interdisciplinary systems research, 47. ISBN 37-643-0957-1.

LANDA, Manuel. War in the Age of Intelligent Machines. 1991/12/26, p. 193. ISBN 0942299752.

LEE, Kuang-Chih, J. HO, Ming-Hsuan YANG and David KRIEGMAN. Video-based face recognition using probabilistic appearance manifolds. 2003/07/18, p. -313, I. DOI: 10.1109/CVPR.2003.1211369. ISBN 0-7695-1900-8.

LYNCH, Euan. The Use of Live Facial Recognition Technology in Scotland: A New North-South Divide? In: *UK Human Rights Blog* [online]. 2020. Retrieved from: https://ukhumanrightsblog.com/2020/02/25/the-use-of-live-facial-recognition-technology-in-scotland-a-new-north-south-divide/

MANOUSOPOULOS, Polychronis, Vassileios DRAKOPOULOS and Theoharis THEOHARIS, 2007. Fractal Active Shape Models. Computer Analysis of Images and Patterns. Berlin, Heidelberg: Springer Berlin Heidelberg, 645-652. Lecture Notes in Computer Science. DOI: 10.1007/978-3-540-74272-2_80. ISBN 978-3-540-74271-5. Retrieved from: http://link.springer.com/10.1007/978-3-540-74272-2_80

MAYHEW, Stephen. Czech, Polish and German rights groups criticize plan for facial recognition at border. In: *Biometric Update* [online]. 2019. Retrieved from: https://www.biometricupdate.com/201901/czech-polish-and-german-rights-groups-criticize-plan-for-facial-recognition-at-border

METZ, Rachel. Beyond San Francisco, more cities are saying no to facial recognition. In: *CNN Business* [online]. 2019. Retrieved from: https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html

NÁDOBA, Jiří. Dálniční e-shop měl mít tajnou funkci - špiclovat, kdo kde jezdí. In: *Respekt* [online]. 2020. Retrieved from: https://www.respekt.cz/agenda/respekt-dalnicni-e-shop-mel-mit-tajnou-funkci-spiclovat-kdo-kde-jezdi

Pražští policisté „otevírají diskusi" o technologii na rozpoznávání obličejů. Hřib je proti. In: *Česká televize* [online]. 2019. Retrieved from: https://ct24.ceskatelevize.cz/regiony/2982332-prazsti-policiste-oteviraji-diskusi-zda-vyzkouset-technologii-na-rozpoznavani

QIANG, Xiao, 2019. President XI's Surveillance State. In: *Journal of Democracy* [online]. s. 53-67 [cit. 2020-05-24]. DOI: 10.1353/jod.2019.0004. ISSN 1086-3214. Dostupné z: https://muse.jhu.edu/article/713722

SAJJAD, Muhammad, Mansoor NASIR, Khan MUHAMMAD, Siraj KHAN, Zahoor JAN, Arun Kumar SANGAIAH, Mohamed ELHOSENY and Sung Wook BAIK, 2020. Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. In: *Future Generation Computer Systems* [online]. s. 995-1007 DOI: 10.1016/j.future.2017.11.013. ISSN 0167739X. Retrieved from: https://linkinghub.elsevier.com/retrieve/pii/S0167739X17309512

SAMSEL, Haley. California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras. In: *Security Today* [online]. 2019. Retrieved from: https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

SCHROFF, Florian, Dmitry KALENICHENKO and James PHILBIN, 2015. FaceNet: A unified embedding for face recognition and clustering. In: *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* [online]. IEEE, 2015, s. 815-823 DOI: 10.1109/CVPR.2015.7298682. ISBN 978-1-4673-6964-0. Retrieved from: http://ieeexplore.ieee.org/document/7298682/

SENNEWALD, Charles A. and John H. CHRISTMAN. Facial Recognition Technology. Retail Crime, Security, and Loss Prevention: An Encyclopedic Reference. Elsevier, 2011, p. 454-456. ISBN 978-0080560823.

SHARMA, M., J. ANURADHA, H. K. MANNE and G. S. C. KASHYAP. Facial detection using deep learning. IOP Conference Series: Materials Science and Engineering [online]. 2017, 263 DOI: 10.1088/1757-899X/263/4/042092. ISSN 1757-8981. Retrieved from: http://stacks.iop.org/1757-899X/263/i=4/a=042092?key=crossref.e5802d9cc3d72d44beefb27ffa2f0b96

TRADER, John. Iris Recognition vs. Retina Scanning – What are the Differences? In: M2SYS Blog On Biometric Technology [online] 2016. Retrieved from: www.m2sys.com/blog/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/

TRIPATHI, Smita, Varsha SHARMA and Sanjeev SHARMA. Face Detection using Combined Skin Color Detector and Template Matching Method. International Journal of Computer Applications [online]. 2011, 26(7), 5-8 DOI: 10.5120/3119-4290. ISSN 09758887. Retrieved from: http://www.ijcaonline.org/volume26/number7/pxc3874290.pdf

TURNER, Rebbeca. City of Perth rolls out new facial recognition CCTV cameras, but is it surveillance by stealth? In: ABC News [online]. 2019, 8.6.2019 Retrieved from: https://www.abc.net.au/news/2019-06-08/city-of-perth-rolls-out-new-facial-recognition-cctv-cameras/11147780

VOX. How Snapchat's filters work. In: YouTube [online]. 2016 Retrieved from: https://youtu.be/Pc2aJxnmzh0

WAN, Weiguo and Hyo Jong LEE, 2017. FaceNet Based Face Sketch Recognition. In: *2017 International Conference on Computational Science and Computational Intelligence (CSCI)* [online]. IEEE, 2017, s. 432-436 DOI: 10.1109/CSCI.2017.73. ISBN 978-1-5386-2652-8. Retrieved from: https://ieeexplore.ieee.org/document/8560829/

What Is Deep Learning? 3 things you need to know, *MathWorks* [online]. Retrieved from: https://www.mathworks.com/discovery/deep-learning.html

Windows Hello: Discover facial recognition on Windows 10, Microsoft [online]. Retrieved from: https://www.microsoft.com/en-us/windows/windows-hello?SilentAuth=1

ZHAO, W., R. CHELLAPPA, P. J. PHILLIPS and A. ROSENFELD. Face recognition. ACM Computing Surveys. 2003, 35(4), 399-458. DOI: 10.1145/954339.954342. ISSN 03600300. Retrieved from: http://portal.acm.org/citation.cfm?doid=954339.954342

ZHAO, Wenyi and Rama CHELLAPPA, ed., 2006. Face processing: advanced modeling and methods. Amsterdam: Elsevier. ISBN 01-208-8452-6.

ZHENG, Jingxiao, Vishal M. PATEL and Rama CHELLAPPA, 2017. Recent Developments in Video-Based Face Recognition. Handbook of Biometrics for Forensic Science. Cham: Springer International Publishing, 2017-02-03, p. 149-175 ISBN 978-3-319-50671-5. Retrieved from: http://link.springer.com/10.1007/978-3-319-50673-9_7

LIST OF FIGURES