DETECTION AND RECOGNITION OF PEOPLE BY CAMERA – RELIABILITY AND USE

VACLAV MACH, BARBORA KOTKOVA & MARTIN HROMADA

Abstract: *This article discusses the possibility of applying software evaluation for a person's detection and recognition in the inside and outside security areas. The methods of face detection and recognition, the methods used in practice are listed in the description. It also mentions manufacturers, Czech too, of software programs for face detection with a subsequent comparison with the database of persons and outlines methods of testing according to the international standard. Finally, the testing of these software programs is described with a focus on their reliability according to predetermined scenarios. The results of their reliability conclude the article.*

Key words: *Camera, Detection of people, Identification of people, Software*

Authors´ data: Mach, V[aclav]; **Kotkova**, B[arbora] & **Hromada**, M[artin], Tomas Bata University in Zlín, Faculty of Applied Informatics Nad Stráněmi 4511 760 05 Zlín, CZ, v2mach@utb.cz, b_kotkova@utb.cz

This Publication has to be referred as: Mach, V[aclav]; Kotkova, B[arbora] & Hromada, M[artin] (2019). Detection and Recognition of People by Camera – Reliability and Use, Chapter 18 in DAAAM International Scientific Book 2019, pp.233-240, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-24-2, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2019.18

1. Introduction

Recognizing individual objects, things, people and perceptions is one of the basic human abilities. The human senses are adapted to allow one to orient and make the right decisions. In fact, through vision, we acquire new information or verify information already obtained. We create various important databases in memory that are interconnected with each other and which are constantly filled with new data and compared with the data already stored.

Around 1970, digital image processing took place, and in the years to come, scientists gradually deal with 3D structure of objects. Gradually, the area develops in multiple directions, one of which has been object detection and person detection. In 2019, we recognize object recognition and human detection every day. [1]

2. Possibilities of using data from the camera system

Social perception of monitoring people and collecting personal information is a very sensitive topic. Most residents do not want their photographs or biometric data to be stored in the databases of different companies, and it is therefore necessary to ensure that the legal conditions regarding personal data are observed. [1]

In commercial areas, the FR is already being used to identify persons at the perimeter level in terms of whether an unauthorized person is trying to penetrate the object of interest. If such a situation is identified, there is sufficient time for operators to respond adequately to the potential risk of misuse of information or damage to company assets. [1]

- identification of goods, products, valuables for insurance purposes, sales and registration, e.g. in museums
- property management and service
- monitoring of production processes with focus on their control
- applications for finding and recognizing faces (casinos, hotels, etc.)

A typical case is when an unauthorized person enters the area. Using the CCTV, images of a person are obtained, which are then sent to a server with installed Face Recognition software, which performs a comparison and, if the person is placed on a “Black List”, sends this information to the security system operator. [1]

- access systems to company
- unlock mobile phone with face ID

Some incidents do not, by their severity and scope, meet the parameters for taking action by the Public Order and Security System, but for the soft objective alone, they are so seriously interfering with routine that it is appropriate to apply procedures for major security incidents. [2]

The next category is the use of Files in the area of security. The security situation is deteriorating from the point of view of terrorism and extremism in Europe, and there is an increase in terrorism-like, not ideologically motivated, violent attacks, just like the terrorist ones, on soft targets in order to hurt accidentally present persons. [2] However, the area of personal identification is also widely used by police authorities, intelligence services or public authorities. The Police of the Czech Republic has the legal opportunity to monitor public space, which is also actively used and in each police vehicle is integrated at least two cameras, which continuously record. [1]

- protection of property, persons and legitimate interests
- detecting, preventing and sanctioning crime
- taking evidence against criminals
- city camera and surveillance systems
- recognition of license plate and vehicle speed
- prevention of vandalism
- support for the fire alarm system
- detection of a suspicious object

3. Procedure to Identify the Person

Before we begin to identify people, we need to solve the problem of their detection in the video. It is not only necessary to detect movement, but also to determine the exact position of a person and to determine which pixels match them. [3]

- Pre-processing - image cleansing from optical errors and noise
- Segmentation - dividing the image into individual segments, assigning the index number segment. It separates important parts of the image from the unimportant ones. Methods - edge detection, neural networks, thresholding and more.
- Object description - division of found objects into classes according to size, colour, location and shape.
- Face detection - using methods (depending on image processing, shooting method) or algorithms, in practice also combinations thereof.
- Face comparison - based on the input data is searched for the identity of the person in the database, signing identity and evaluating success

Problems in detecting people close together appear as one figure after background reading. Another problem may be the incorrect detection of one person. There could be a situation where, after subtracting the background, we see one person divided into multiple parts. When designing the system, it is appropriate to take into account the layout of the cameras. Improper detection of foreign objects could become an unpleasant thing. Phenomena such as opening and closing doors can be identified as a short movement at one point in the scene. It may happen that the system will try to identify the door as a person. This can be avoided either by searching for a person's role model for each part, or by requiring some movement from the person. [3]

4. Methods used for Detection and Identification

There are many methods for detecting a face in an image. In this chapter, it is possible to get acquainted with theirs The following sub-chapters describe some of them. According to publication [4] of 2002, by Yang, Kriegman, and Ahuja, methods for face detection were divided into the following four basic groups [5]:

- Knowledge-based methods - These methods use the knowledge of a typical human face. The rules capture the relationships between typical facial features.
- Feature invariant methods - These methods look for typical features that are independent of the angle of rotation of the head and light conditions.
- Template matching methods - Face detection is based on the correlation between the input image and the pattern face or parts of it.
- Appearance-based methods - In contrast to the pattern-based method, a model is created with this method sets containing a variety of possible facial expressions.

Methods used for face recognition - automated person identification systems can, therefore, be solved by two basic one's approaches:

- structural - recognition of individual dominant parts of the face (eyes, mouth, nose…) of the presented pattern, measuring anthropometric quantities, their normalization due to expected interference (noise, interference, position in the scene, size…), comparison with a database of known photos using classification algorithms, statistical decisions about the relative similarities with the selected set of images.
- holistic - comparison, sample identification using global representations again with a subsequent statistical evaluation of the relative probability. Typical for this approach are combinations of the backpropagation method neural network feedback), basic component analysis component analysis (PCA) and singular value decomposition value decomposition (SVD). The concept of reductionism is a general practice in development of intelligent systems - design of solutions to complex problems through the gradual decomposition of the task into subsequent modules. Addressing the task of identifying stakeholders can be a combination of both. [6]

5. Software manufacturers

There are many products on the market with different algorithms. It is not unusual that two different software manufacturers use the same algorithm with different set parameters. To measure the performance and quality of facial recognition algorithms, the US National Institute for Standards and Technology (NIST) has introduced methodologies that test the capabilities of software from different vendors. [7] Selected producers from Czech Republic:

- Eyedea Recognition s.r.o. - Eyedentity recognizes faces in photos and videos, Vehicle Type recognizes car models, Number Plate and license plates. Anonymize offers anonymization, where it cooperates, for example, with Seznam.cz, to which it supplies a system for face blurring in photographs from Mapy.cz. [8]
- Quantasoft s.r.o.– specialize in object and person recognition technologies. It develops its products for shops, cities, hotels and restaurants (VIP clients, Unwanted, Black list etc.)

They advertise a breakthrough in healthcare in the predictive diagnosis of eye diseases. [9]

6. National Institute of Standards and Technology

NIST (US National Institute for Standards and Technology) to measure the performance and quality of facial recognition algorithms, the American Institute has introduced methodologies that test the capabilities of software from different vendors. [10] The tests are carried out on very large databases containing more than 1.8 million people and their photographs. The tests assess the accuracy, speed, memory and storage consumption and durability of these technologies. The best-performing companies ranked the best performing algorithms. NIST measures many technical parameters in different lighting configurations, but to evaluate the overall recognition success, the key values are:

- FMR (False Match Rate) FMR is the percentage of images where a person was found in the database, but the person was not actually the database.
- False Non-Match Rate (FNMR) FNMR is the percentage of frames where a person was not found in the database but the person was in the database. Evaluation of algorithm capabilities of various manufacturers is published in well-arranged tables, according to which users can make decisions in the design of the end system.

In November 2018, the results of NIST Interagency Report 8238 were published that the best results were achieved by the algorithms of the American company Microsoft Corporation.

7. Comparison of selected Software

There are many types of software that have different procedures and outputs. However, the conclusion must always be the same - the person being compared is located / not in the database. As an example of data processing and its outputs, user testing of two software from Japanese company NEC Corporation (its product Neo Face Watch is used at Václav Havel International Airport in Prague to verify biometric data in travel document) and IsVision company AnyVision (its product Better Tomorrow) is installed at Domodedovo International Airport). The purpose of the testing was not to verify all the declared functions, but the testing was aimed primarily at verifying the reliability of detection and identification of persons.

For testing was used database, which was used about 13 000 Mugshots type. The database includes men and women aged 15-80 years and of different ethnicities, with men and women of Caucasian origin being the most represented. However, some photographs were intentionally taken in situations where it was already difficult for a person to determine whether they were indeed the person to be found in the default database. Both products had their own friendly user interface. First, you had to connect to the default database (a database of 13,000 photos). Subsequently, a reference photo of the person we were looking for was uploaded to the default database. [1]

The testing focused on different types of environments and situations. In the first test, the systems were to detect a seated man at the age of 23, and the following test set was aimed at a white woman. In addition, a black man of approximately 50-55 years was selected. The last test set was aimed at a woman with Asian roots. Person detection and identification for Better Tomorrow and Neo Face Watch are only part of the data tested. the input images were intentionally taken in reduced quality or in situations where the wanted persons are in different positions on the border of the declared algorithm possibilities. [1]

With Neo Face Watch, 38% of the images tested were correctly identified in a predetermined scenario. Better Tomorrow's success rate was 53%. Although Better Tomorrow had a lower match than Neo Face Watch throughout the testing, it was able to correctly assign identity to multiple people. It follows that the score cannot be taken as a decisive parameter for determining which algorithm to be tested is more reliable. [1]

The Neo Face Watch software has always suggested several candidates that match the person on the embedded image. The searched person was, in the vast majority of cases, nominated among the top five candidates, and most often it was the first candidate, the highest probability of being the same person as the reference image. With Better Tomorrow, there was no opportunity to see other candidates with a lower match, and only one candidate was introduced to the tester, but it was 99% correct. Both manufacturers declare in their marketing materials a rate of correct identification of greater than 99% and a misidentified person of less than one 1% per day. From the test results, it can be concluded that the declared value manufacturers are achievable provided the requirements for image quality and visibility of the major minutiae of the face are respected. [1]

8. Conclusion

During the testing it was found that if the algorithm can correctly detect a person's face in the image, the subsequent identification against the reference image is at a very high level.

These results were obtained based on a single image that was embedded in the software. CCTV systems are used to monitor areas in the security area. Current cameras capture the scene in high definition and the frame rate has increased. In the case of installing a CCTV system and simultaneously identifying software, people acquire much higher quality input photos than if a single photo is used for comparison. [1]

The results will be affected by whether the images are taken indoors or outdoors. A high-resolution camera, outdoor, low visibility, and poor weather conditions (rain, snow, or fog) does not necessarily guarantee an increased likelihood of identifying the person. Another aspect that will affect the image quality of detected people is whether the images will be obtained from a collaborative or non-cooperative scene. The images taken from the security corridor, which people enter individually, will surely be better than images from a busy street with several dozen people. [1]

When building a surveillance system designed to identify persons, certain principles must be followed to achieve the highest possible reliability. The basic prerequisite is a quality recording device. The use of black and white cameras is not permitted. An important parameter in video cameras is the colour stability of the image. The ideal condition is all cameras from the same manufacturer, so there is a higher probability of the same colour rendering from all cameras. With the camera's resolution, of course, the more, the better, but too high a resolution is very computer-intensive. The cameras must be placed statically and the background image must be as static as possible. [2]

9. Acknowledgements

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Program Project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech ED2.1.00/03.0089 and by the Internal Grant Agency of Tomas Bata University under the project No. IGA/CebiaTech/2019/003.

10. References

Gabko, L. (2018). Testování spolehlivosti software určeného pro detekci osob. Available from: http://hdl.handle.net/10563/44437.

Lapkova, D., Kotek, L. & Kralik L. (2018). Soft Targets – Possibilities Of Their Identification. Katalinic, Branko, ed. Proceedings of the 29th International DAAAM Symposium 2018. DAAAM International Vienna, pp. 0369-03. DOI: 10.2507/29th.daaam.proceedings.053. ISBN 9783902734204.

Hopjan, T. (2010). Identifikace osob pro kamerový systém. Available from: http://hdl.handle.net/11012/53000.

Ming-Hsuan, Y., Kriegman D.J. & Ahuja N. (2002). Detecting faces in images: a survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. vol. 24, issue 1, pp. 34-58. DOI: 10.1109/34.982883.

Jablonski, P., Szewczyk R., Kulesza Z., Napieralski A., Moreno M. & Cabestany J. (2002) Automatic people identification on the basis of iris pattern - image processing and preliminary analysis. 23rd International Conference on Microelectronics. pp. 687-690. DOI: 10.1109/MIEL.2002.1003351. ISBN 0-7803-7235-2.

Ponzer, M. (2009). Detekce a rozpoznávání obličeje. Available from: http://hdl.handle.net/11012/2006.

Wu, W., Yin Y., Wang, X. & Xu D. (2019). Face Detection with Different Scales Based on Faster R-CNN. IEEE Transactions on Cybernetics. 49(11), pp. 4017-4028. DOI: 10.1109/TCYB.2018.2859482. ISSN 2168-2267.

Wu, Y., Wang W., Jung S., Hoermann S. & Lindeman R. (2019). Towards an articulated avatar in VR: Improving body and hand tracking using only depth cameras. Entertainment Computing. DOI: 10.1016/j.entcom.2019.100303. ISSN 18759521.

Prabhakar, S., Pankanti S. & Jain A.K. (2003). Biometric recognition: security and privacy concerns. IEEE Security & Privacy, 1(2), pp. 33-42. DOI: 10.1109/MSECP.2003.1193209. ISSN 1540-7993.

Bourlai, T. & Cukic B. (2012). Multi-spectral face recognition: Identification of people in difficult environments. IEEE International Conference on Intelligence and Security Informatics. pp. 196-201. DOI: 10.1109/ISI.2012.6284307. ISBN 978-1-4673-2104-4.