Transactions of the VŠB – Technical University of Ostrava, Mechanical Series
No. 2, 2014, vol. LX
article No. 1991

Rastislav PIRNÍK[*], Ján HALGAŠ[**], Marián HRUBOŠ[*] and Jakub TRABALÍK[*]

DETECTION AND IDENTIFICATION OF PEOPLE AT A CRITICAL INFRASTRUCTURE FACILITIES OF TRAFIC BUILDINGS

DETEKCIA A IDENTIFIKÁCIA OSÔB V OBJEKTOCH KRITICKEJ INFRAŠTRUKTÚRY DOPRAVNÝCH STAVIEB

Abstract

This paper focuses on identification of persons entering objects of crucial infrastructure and subsequent detection of movement in parts of objects. It explains some of the technologies and approaches to processing specific image information within existing building apparatus. The article describes the proposed algorithm for detection of persons. It brings a fresh approach to detection of moving objects (groups of persons involved) in enclosed areas focusing on securing freely accessible places in buildings. Based on the designed algorithm of identification with presupposed utilisation of 3D application, motion trajectory of persons in delimited space can be automatically identified. The application was created in opensource software tool using the OpenCV library.

Abstrakt

Tento príspevok sa zaoberá problematikou identifikácie osôb vstupujúcich do objektov kritickej infraštruktúry a následnou detekciou ich pohybu v častiach objektov. Ozrejmuje niektoré technológie a postupy, ktoré sú pri spracovaní špecifickej obrazovej informácie, kde je použité stávajúce vybavenie budov. V článku je ďalej opísaný navrhnutý algoritmus na detekciu osoby. Prináša nový pohľad na detekciu pohybujúcich sa objektov (záujmových skupín osôb) na uzavretých plochách, pričom kladie dôraz na zabezpečenie voľne prístupných miest v budovách. Na základe navrhnutého algoritmu identifikácie s predpokladaným využitím 3D aplikácie je možné automatizovane identifikovať trajektóriu pohybu osoby vo vymedzenom priestore. Aplikácia bola vytvorená v opensourse softvérovom prostriedku s využitím knižnice OpenCV.

Keywords

IDS, identification of persons, motion trajectory, Face Recognition, low cost-intensity.

1 INTRODUCTION

Recognition of human faces is a complex task for new information technology and it is still being developed and improved as a method of identification of a specific person. It is natural for humans to recognize a familiar person, based on identification of a familiar face for various rotations,

[*] Ing. PhD, Department of Control and Information Systems, University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 01026 Žilina, Slovak Republic, (+421) 41 513 3351, rastislav.pirnik@fel.uniza.sk
[**] Ing. PhD, Division Intelligent transport systems, University Science Park in Zilina, University of Žilina, Univerzitná 1, 01026 Žilina, Slovak Republic, (+421) 41 513 3333, jan.halgas@uniza.sk
[*] Ing. Department of Control and Information Systems, University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 01026 Žilina, Slovak Republic, marian.hruboš@fel.uniza.sk
[*] Ing. Department of Control and Information Systems, University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 01026 Žilina, Slovak Republic, jakub.trabalik@fel.uniza.sk

various angles, various distances or backgrounds. This task is solved by different methods for information technology. The biometrics data converted into electronic form is a unique code for each person ant it is transferable and verifiable. This data (collected by biometric scanning) can be used for quick and reliable identification of individuals. The main advantage, compared to other methods of identification, is their versatility. Every person has a reference character (nose, eyes, ears etc.), but each person has a different set of unique characters. Comparison of these characters enables us to reliably identify a person. These characters are still in time and of constant shape except for extreme cases. Security systems based on biometric identification of individuals work in two modes; identification (e.g. aggressor recognition in the crowd) and verification (confirmation of identity) [4].

Systems for identification of moving people are inherent in the field of personal and cargo transport. They are mainly intended for surveillance, identification and control activities. In the context of static traffic surveillance camera systems are deployed mainly to control the situation around and in the building of critical infrastructures such as platforms, airport halls or areas reserved for parking a vehicle. The aim of these systems is to ensure the greatest possible reliability of the zone possible, providing oversight of unauthorized (suspicious) movement or finding people with possible identification of offenders. Therefore, we focus on an algorithm design for identification and recording of the vehicle trajectory together with recording of time sequence.

2 BIOMETRIC SECURITY SYSTEM

Recognition of a person's identity is performed on the basis of biometric features of human body which are consistently being recorded using a suitable sensor and then transformed to a numerical format. This format is subsequently available in the automatic recognition of persons. These biometric features can be divided into two groups [1], [2] and [3]:

- Physical characteristics – the most well-known biometric identifiers are a person's face and fingerprints. Other identifiers are eye iris, retina, hand geometry, ear, palm print, DNA and voice. This group includes static signs.
- Behavioral characteristics - features and habits of the people, thus characteristic for human behavior. It helps to distinguish a person from other people. Behaviors in various situations such as speed, slope and shape of the font in the signature, gait and. dynamic s of typing on the keyboard.

Level of security system is affected by a large number of factors [1], our design showing significantly the following two:

A) The accuracy and reliability of identification – parameters to evaluate the reliability are **FAR (False Acceptance Rate) -** the probability of false acceptance of unauthorized persons, i.e. acceptance of a person who is not registered in the database. **FRR (False Rejection Rate) -** the probability of wrong rejection of authorized persons and failing to accept a person from the database. The lowest value of these parameters determines quality of identification and functionality of the security system. The important element in this context is sensitivity of the system. Safety systems (not only for transport applications) require a certain degree of balance between FRR and FAR (fig. 1). Their optimal value is given by the value of the EER (Equal Error Rate). In our case it means that using a higher quality camera equals to a more sensitive identification. Then the algorithm of the system will focus on the details of facial features. The probability of incorrect acceptance of unauthorized persons (FAR) will be lower and the probability of incorrect rejection of authorized persons (FRR) will increase. Therefore, system should be set up in such a way that the FAR and FRR parameters are balanced, making the system optimized (ERR). Time of a person’s identification is less a significant parameter.

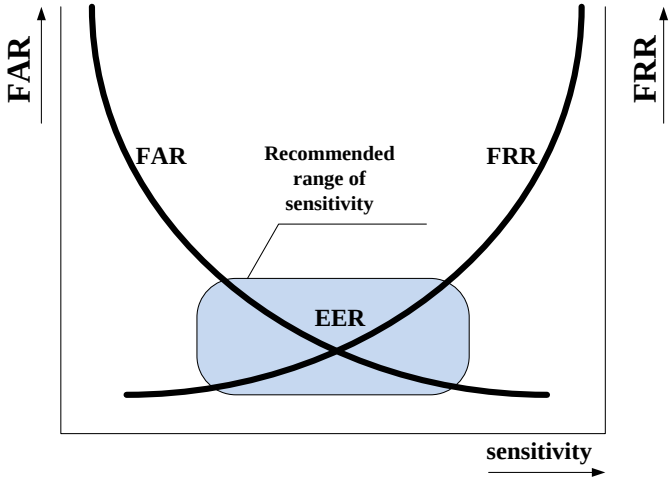

Fig. 1 Sensitivity range of biometric security systems

B) The total cost of implementing the security system into operation can divided into two groups - the initial investment in the selection of hardware and software of the system and introduction of the system into operation, creating a database of biometric data and training of the company as a professional staff. For our case we considered this factor because one of the requirements in the design of the security system was low cost-intesity.

3 METHODS FACE DETECTION IN IMAGE

The individual detection techniques can be classified into four categories based on the approach:

1. Knowledge-based methods. Methods based on knowledge of information on facial traits. This usually concerns relations between individual parts of face.
2. Feature invariant approaches. Methods based on invariant features of face such as mouth, eyes or skin color thanks to which the face is detected in the picture. These are predominantly relations between individual facial parts which do not change when the light or the rotation angle of face changes.
3. Template matching methods. Methods based on comparison with the template. These are templates describing the face or its parts and traits. Evaluation and assessment of existing face in the image is based on correlation between an input image and a template from the database set.
4. Appearance-based methods. These appearances/models are created on the basis of training classifiers. Facial detection is executed via comparing the input image with the given model from the training. The algorithm sets certain rules based on the training set during training. The whole process is depicted on fig. 2.

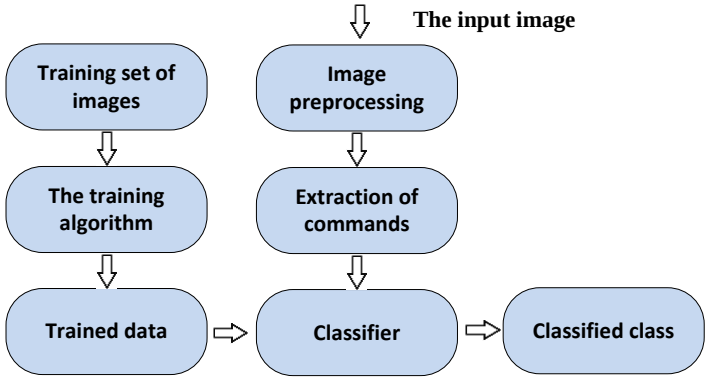

Fig. 2 A general scheme of human face detection in image by the appearance-based method

3.1 Face Recognition using Eigenfaces

Recognition of familiar faces is the most frequent activity of human brain. There is a large number of studies on facial recognition methods. For the needs of our application we have chosen the method of principal component analysis – PCA - using Eigenfaces. This method extracts facial traits from the image which are subsequently compared with facial traits from the central database. Training and test data are projected in a PCA subspace, i.e. in space created via its own vectors of convariance matrix created by training images. From the mathematic aspect it means searching for crucial facial points (eigenvectors) from the images of faces. Eigenvectos can be simplified as a file of qualities depicting interconnections between individual faces. They characterize each scanned face and are called eigenfaces. As with all appearance-based methods, the most significant part of PCA algorithm is a training set of images whose number is theoretically unlimited but finite. Processing images of this set results in eigenfaces. All images of the training set must be of the same proportions and the faces have to be centered. The core idea of this methods is based on the method described in detail in [2], [3], [4] a [6].

4 A DESIGN OF RECOGNITION UNIT WITH A LOW COST VIDEO RECORDER

One of the main parts of security systems of traffic infrastructure are camera systems/systems using video camera systems to secure an area or an object. They are based on recording input image which is subsequently analyzed. They identify persons recorded by the video cameras and then grant access or detain a suspicious one. This type of security system is mostly used in sports arenas, securing a crucial traffic infrastructure such as buildings and airport areas, railway or bus stations and all the places with a large number of people. Video camera systems for facial recognition are further used to secure objects of traffic regulation – various terminals granting access to traffic regulation systems only to employees with authorized access.

The designed algorithm has to provide security based on identification of persons based on recorded input image. The primary step is therefore detection and subsequent extraction of facial parts in the input image. After a successful facial detection the recorded person can be identified. The proposed algorithm basically proceeds in three basic steps:

1. Phase of “image database creation”.
2. Phase of “LEARNING” – training of input data.
3. Phase of “RECOGNITION” – identification of individual users.

4.1 Phase of "image database creation"

This phase represents image database creation of individual users' faces who will be provided with access through the access terminal. The whole process of facial image creation of a specific employee starting with scanning of the input image ending with saving the processed image in the database is depicted on the development diagram on Fig. 3.

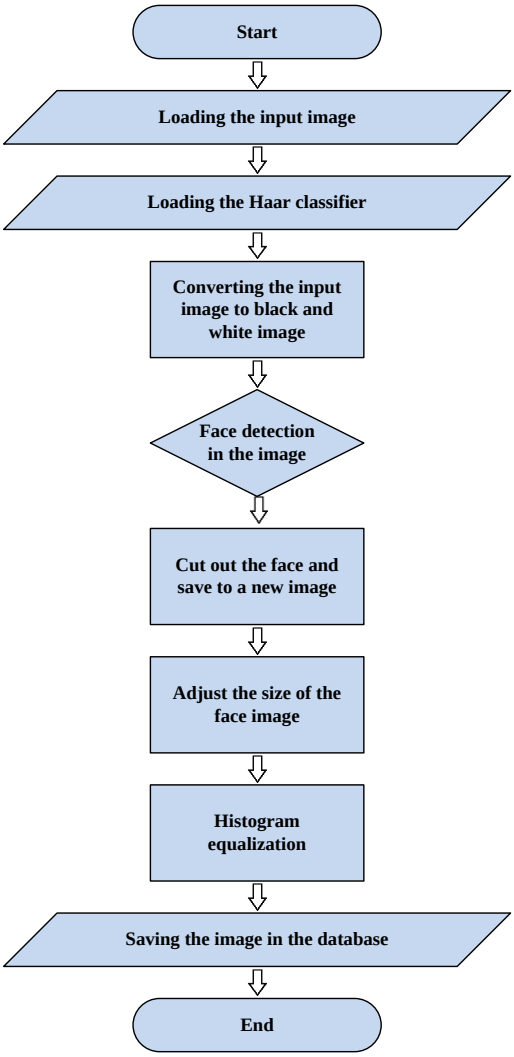

Fig. 3 Creation of image databases

The first diagram of algorithm requires recording an image of a person and the so-called Haar classifier (HC) into the system. HC, as depicted on the following figure, serves as detector of the face in the image in the next step.

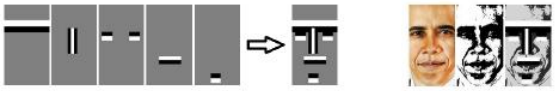

Fig. 4 Facial detection via HC

After detecting the probable area of face in the picture this area is extracted and saved in a new image in which the surroundings of the scanned person are no longer saved. Each of these facial images is subsequently transformed into a template of all faces. In our case the term "template" means transferring an image into a specific size, i.e. the facial image is comprised into the size of the chosen template of 100x100 pixels.

Fig. 5 Example of individual partial outputs executed by the designed algorithm

Subsequently, a histogram is equalized – a step visualizing facial traits which are then darker than the rest of facial skin color. It contributed to easier recognition/ability to differentiate between faces.

Before facial recognition it is necessary to convert the input image into black and white due to the detector used. The facial recognition is subsequently executed via Viola-Jones detector using Haar classifier/Haar wavelet for detection. The detector and its outputs are described in detail in [3] and [5].

Facial detection via Haar classifier in OpenCV is executed after setting the parameters via function **CvSeq* cvHaarDetectObjects(const CvArr*image, CvHaarClassifierCacade* cascade, CvMemStorage* storage, double scale_factor=1.1, int min_neighbors=3, int flags=0, CvSize min_size=cvSize(0,0), CvSize max_size=cvSize(0,0))**.

Figure 6 depicts an image of making an entry of the given function from OpenCV.

```
67  /*------------------------DETEKCIA TVARE POMOCOU HAAR KLASIFIKATORA------------------------*/
68
69  detegovana = cvHaarDetectObjects(obraz,     //vstupny obraz
70      cascade,                                //nahrany Haar Cascade klasifikator
71      storage,                                //pamatove miesto
72      1.1,                                    //zadanie detailov hladania tvare
73      3,
74      0,                                      //CV_HAAR_DO_CANNY_PRUNING
75      cvSize(30, 30));                        //najmensia vekost tvare, ktora bude zadetegovana
```

Fig. 6 Source code of facial detection in the input image – main function

4.2 Phase of „LEARNING“

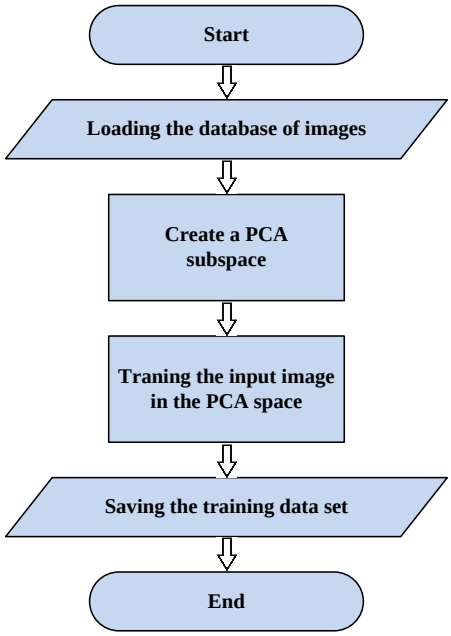

Fig. 7 Algorithm of phase of “LEARNING”

In the beginning of algorithm of LEARNING it is necessary to record the obtained input data which are subsequently processed. We are talking about images of faces of employees we had created and saved into the database of persons involved in the previous phase. For the purposes of our application we have chosen the PCA method using Eigenfaces for facial recognition within an image.

The core of Eigenfaces method is extraction of facial features from the saved images which are then compared with traits of trained faces in the database in the “RECOGNITION” phase. It is therefore necessary that all images from the training set are of the same proportions and faces in them are centered. Training and testing data are projected in the PCA subspace, i.e. subspace created via eigenvectors of convariance matrix which is created from training images of Fig. 7. Mathematically speaking, it means searching for crucial facial points (eigenvectors) from facial images.

Within this phase, the OpenCV library provides pre-written functions for creating PCA subspace as well as projection and training of facial images within this subspace. The first one is **void cvCalcEigenObjects(int nObjects, void* input, void* output, int ioFlags, int ioBufSize, void* userData, CvTermCriteria* calcLimit, IplImage* avg, float* eigVals**.

The cvEigenDecomposite() function calculates all coefficients of decomposition for the input training image via previously calculated eigenfaces and the average face. The whole form of the function is as follows: **void cvEigenDecomposite(IplImage* obj, int nEigObjs, void* eigInput, int ioFlags, void* userData, IplImage* avg, float* coeffs)**.

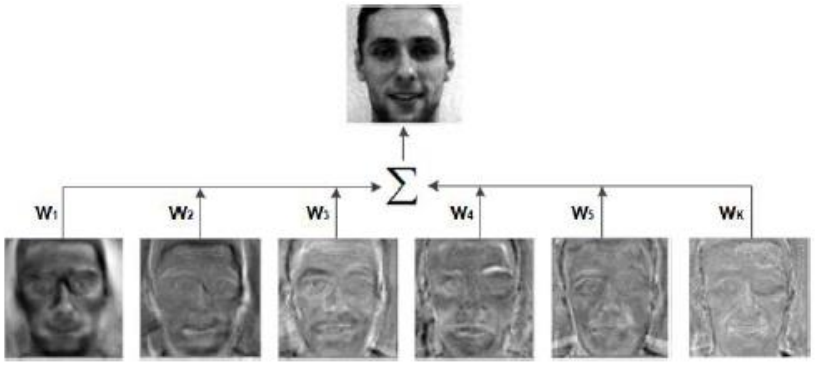

Fig. 8 Each of the facial images is a linear combination C of eigenvectors

```
55  /*-----------------------TRENOVANIE VSTUPNYCH OBRAZOV V PCA PODPRIESTORE-----------------------------*/
56
57  for (i = 0; i < nTrenTvar; i++){    //trenovanie obrazov v PCA, porovnavanie spolu s priemernym obrazom
58      cvEigenDecomposite(skupTvarP[i],
59          nEigen,
60          eigenVekP,
61          0,
62          0,
63          priemerTvar,
64          predpokladTrenTvarM->data.fl + i*nEigen);
65  }
66
67  ulozNatrenData();                   //ulozenie natrenovanych dat ako .xml subor
68  printf("Ulozenie vsetkych natrenovanych Eigenfaces do suboru 'trenovane.xml', pre rozpoznavanie.\n");
69
70  ulozEigenAkoObraz();                //ulozenie eigentvari do suboru ako obrazok
```

Fig. 9 Training of database images in PCA subspace

4.3 Phase of "RECOGNITION"

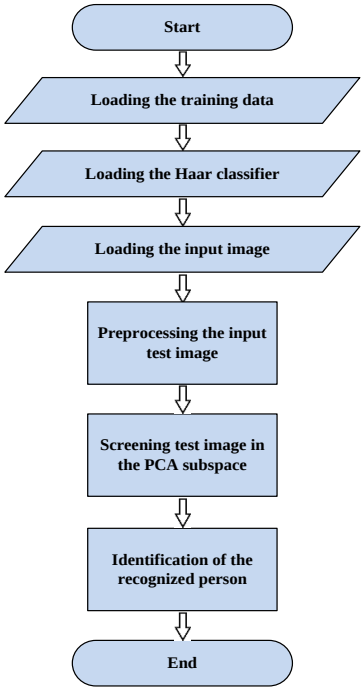

Fig. 10 Algorithm of "RECOGNITION" phase

Testing of algorithm began with scanning faces of several people who always faced the video camera during testing. Recording both input images of faces for training/creation of database and testing images was performed under different light conditions (except of IR lighting of the scene) and in various environments. All recorded images were of 640x480 pixel proportions and differenced in image quality were marginal.

Debugging the algorithm was executed under following conditions. 20 facial images of 8 persons were recorded. The first 10 images of every person were pre-processed, i.e. transferred into an image database in the first phase of software application resulting into a basic database of 80 images of faces of 8 different persons in the size of 100x100 pixels.

All these images were trained in the "LEARNING" phase. Further 10 images of tested persons were transferred into database of testing images including images recorded during previous phases. Subsequently, we selected 100 images which were tested and identified in the "RECOGNITION" phase.

```
/*-------------------------------------------------PREDPSRACOVANIE VSTUPNEHO OBRAZU-------------------------------------------------*/

IplImage *sedyObr = konvertujSeda(vstupObr);            //konvertovanie vstupneho farebneho obrazu na obraz sedy resp. cierno/biely

CvRect tvarOblast = detekujTvar(sedyObr, tvarCascade);  //dekegovanie tvare vo vstupnom obraze

IplImage *tvarObr = vyberTvar(sedyObr, tvarOblast); //vybratie oblasti z obrazu ktora je povazovana za tvar, a vlozenie do noveho obrazu

IplImage *velkostObr = nastavVelkost(tvarObr, tvarSirka, tvarVyska);//nastavenie rovnakej velkosti vstup.obr v porovnani s natrenovanym

IplImage *equalizObr = cvCreateImage(cvGetSize(velkostObr), 8, 1);
cvEqualizeHist(velkostObr, equalizObr);                 //aplikovanie ekvalizovaneho histogramu na vstupny obraz
IplImage *predspracovanyObr = equalizObr;               //snimok nadobudne standardny jas a kontrast, v pripade zleho kontrastu
```

Fig. 11 Example of debugged algorithm in the "RECOGNITION" phase

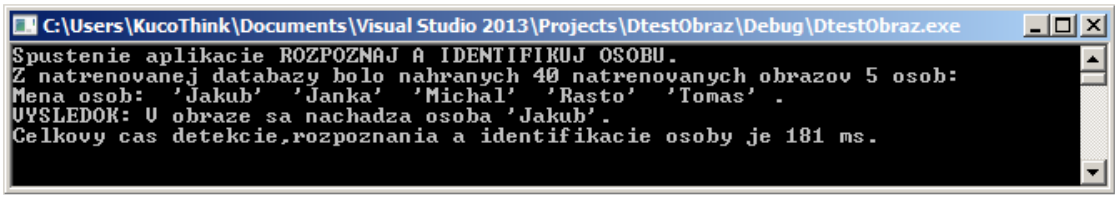

Fig. 12 Example of control output including overall time of identification in algorithm debugging phase

5 CONCLUSIONS

The average time of overall identification of tested faces is 427.89 ms with the overall correctness of recognition of people from the trained set off 88 %. Significantly better results as to time of identification – about 250 ms – were achieved during tests with a smaller number of trained images (e.g. 48 images of 6 different persons). However, it also means that with rising number of employees, i.e. new facial images, the time of identification rises. This problem can be solved by decreasing the overall number of images of one person for the phase of training, albeit for the price of lower correctness rate of personal identification.

ACKNOWLEDGEMENT

This paper is supported by the following project: University Science Park of the University of Zilina (ITMS: 26220220184) supported by the Research & Development Operational Program funded by the European Regional Development Fund.

REFERENCES

[1] NAGY, P. Biometrické identifikačné technológie. In Použitie automatickej identifikácie na ochranu objektov. [online]. Žilina. 2010. 40s. Dostupné na internete:<https://vzdelavanie.uniza.sk/moodle/mod/resource/view.php?id=31737>.

[2] SYNAK, M. Podobnostní vyhledávaní v biometrických charakteristikách. Diplomová práca. Brno. Masarykova Univerzita. 2010. 59 s. Dostupné na internete: <http://is.muni.cz/th/139888/fi_m/Podobnostni_vyhledavani_v_biometrickych_charakteristikach.pdf>.

[3] TRABALÍK, J. Hybridný pristupový terminál umožňujúci zaistenie bezpečnosti budov. Diplomová práca. Žilinská univerzita v Žiline. 2014. 85 s. ID: 28260220141028, Žilina

[4] MALACH, T. Detekce obličeje v obraze. Bakalárska práca. Brno. Vysoké učení technické v Brně. 2011. 67 s. Dostupné na internete: <https://dspace.vutbr.cz/bitstream/handle/11012/6586/Tobiáš%20Malach%20BP%202011.pdf?sequence=1>.

[5] OpenCV + Face Detection. [online]. Dostupné na internete: <http://www.cs.princeton.edu/courses/archive/fall08/cos429/CourseMaterials/Precept1/facedetect.pdf/>.