

Developing Facial Recognition Software to Control Access to Campus Facilities

Svetlana Devitsyna¹, Tamara Eletsckaya¹ and Andrey Meshkov¹

¹ Sevastopol State University, Institute of Radio-Electronics and Information Security, Information Security Department, 299053, 33 Universitetskaya Street, Sevastopol, Russia.
devitsyna@mail.ru, toma.eletsckaya@mail.ru,
world2000054@gmail.com

Abstract. The purpose of the proposed development is to improve the system for ensuring the safe functioning of the campus, and to determine the possibility of using an intelligent system of biometric identification of the subject to identify the disturber in the protected area, as well as to record attendance at classes and monitor working hours of employees. Computer technologies are widely used to organize the administration of the educational process of the University. The application of biometric identification methods to the organization of access to the campus is an actual and important task, the solution of which is presented in the form of software development based on the use of biometrics of students and employees of the educational institution. The Zorgo program is created using Python language tools and neural network algorithms of image recognition. Application of "Zorgo" software and its integration into the existing access control systems will increase the efficiency of the security service and improve the quality of the campus security system.

Keywords: Computer science, Computer technologies, Authentication, Biometrics, Computer vision, Digital signal processing, Machine learning, Python, Software, Campus, Administration of the educational process at the University.

1 Introduction

Information technology (IT) is successfully used in training to increase educational potential. At the same time, insufficient attention is paid to the application of modern computer technologies tools for the organization of the educational institution's activities, administration of the educational process. In modern educational campuses, as a rule, video surveillance and access control systems are widely used to implement security systems. Educational institutions belong to the category of objects with a permit system, so the issues of identification and authentication are relevant, and their solution significantly affects the security of not only the object, but also students and employees. Besides, at carrying out of certification of students the procedure of authentication which can be realised with use of an information technology is often required.

For access to the territory of an educational institution various systems of the physical access control system (PACS), and also photo- and video fixation, metal detectors

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

and turnstiles are used. All of these systems are usually poorly coordinated with each other and require additional time for comparing information about the subject of access.

The purpose of the proposed development is to improve the system for ensuring the safe functioning of the campus, and to determine the possibility of using an intelligent system of biometric identification of the subject to identify the disturber in the protected area, as well as to record attendance at classes and monitor working hours of employees. The developed software is easily integrated into the existing video surveillance system and allows to track the movement of people with the possibility of their authentication, that is, to determine the legality of the presence of the subject on the territory of the educational campus, or the legitimacy of the user of the automated system of the educational institution. The software is called “Zorgo” and translated from Esperanto as “The Keeper”.

2 Main body

Identification based on biometrics is now widely used, as it is effective and accurate. Biometric identification technologies previously used only at strategic sites to protect military secrets and critical commercial information are now used in various areas: banks, medical institutions, shopping malls, airports, company offices, etc. Biometrics make it possible to unambiguously identify a subject, so they belong to the category of personal data, the processing of which should be carried out only on a legal basis (Federal Law N 152-FZ ON PERSONAL DATA, 2006). When developing authentication systems using biometrics, it is important to take into account the requirements of regulatory documents to the procedure of personal data processing. The content and volume of processed data should correspond to the purposes of processing. The biometric database should be kept up to date, i.e. it should take into account not only changes and movements of the contingent (students and employees), but also the terms of personal data storage, if they are regulated by legislative acts. It is also necessary to take into account natural changes in biometrics, and periodically update the database. Incomplete or inaccurate data, as well as data of dismissed employees and expelled students, should be identified and deleted from the system. It is also necessary to apply organizational and technical measures for their protection during processing and storage in the organization using personal data processing systems, in accordance with the current regulatory requirements (Federal Law N 152-FZ ON PERSONAL DATA, 2006) (Order of FSTEC of Russia No.21, 2013). After performing the established organizational procedures and obtaining the consent of the subject to the processing of personal data, it is necessary to create a database with numeric codes of received biometrics.

As biometrics in this development, it was decided to use the image of the person being identified. Such a decision is conditioned by the following factors:

- The accuracy of the subject's identification by the image of the face is high in comparison with other methods, the level of recognition of three-dimensional photography is more than 90%, and two-dimensional image — more than 50%;
- The procedure of obtaining biometrics is usual for the subject, is contactless and fast (face image is used for passport and visa documents, passes);
- It is possible to use this biometric for remote automatic identification;

- Digital biometrics takes up little space in the storage (for example, three-dimensional photo takes up only 5 Kbytes);
- The cost of such a system, compared to, for example, retina recognition, is acceptable to educational institutions.

The practical use of biometric technology is based on two aspects: technical and algorithmic. The technical aspect involves the integration and use of hardware and software systems with basic biometric software modules such as biometric libraries. The algorithmic approach includes the integration of biometric technologies into an authentication or access control system. In this paper both aspects are applied, and also intellectual means on the basis of neural networks are used for training of system of recognition of faces of employees and trainees.

Any identification system works according to an algorithm:

- Record — obtaining an identifier;
- Selection — extraction of unique information from biometrics;
- comparison — comparison of the obtained identifier (biometric sample) with the standard stored in the database;
- Decision-making — getting a judgment about the coincidence of biometric images and the end of the identification procedure.
- Authentication procedure implies making a decision on subject's authenticity and rights of an identified subject in the system.

Thus, for creation of system of biometric identification at first it is necessary to create a database (DB) with biometrics of employees and trainees. Then, in real time mode, to carry out video monitoring of the campus territory, to recognize the subjects' faces on the received images, to compare them with the biometrics contained in the database, and to make a decision whether a person has the right of access to the territory of the educational institution.

To implement authentication at the first stage it is necessary to prepare the data for the procedure of identification (identification) of the subject. For this purpose, portrait photography of students and employees is carried out (the same way as for passes). On the electronic image, control points are identified (State Standard ISO/ITU 19794-5-2013, 2013), on the basis of which a "digital imprint" of the person of a legitimate subject, i.e., who has the right of access to the campus territory, is obtained

In the form of a numeric code the obtained biometric is placed in the database (DB), which the program will later refer to to implement the identification procedure.

The Zorgo program is created using Python language tools and neural network algorithms of image recognition. Neural networks can reproduce complex nonlinear dependencies with any accuracy, are able to learn and self-study, generalize the experience gained during the training, and are quite easily implemented on parallel computing tools.

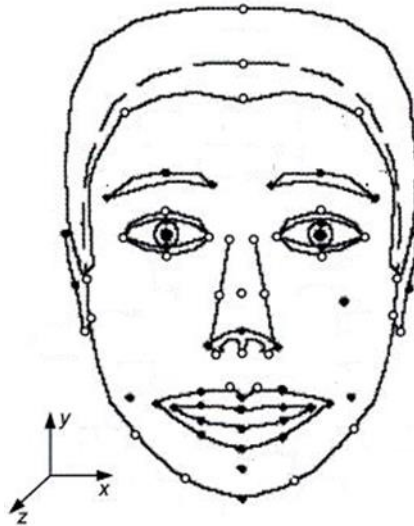


Fig. 1. Control points

Zorgo used intelligent methods based on the use of neural network technologies to teach the recognition system. The neural network system of pattern recognition consists of a subsystem of pattern extraction and a neural network classifier which performs the function of the decisive rule. An example of a neural network image recognition system block diagram is shown in Fig. 2 (Vasilev, 2017).

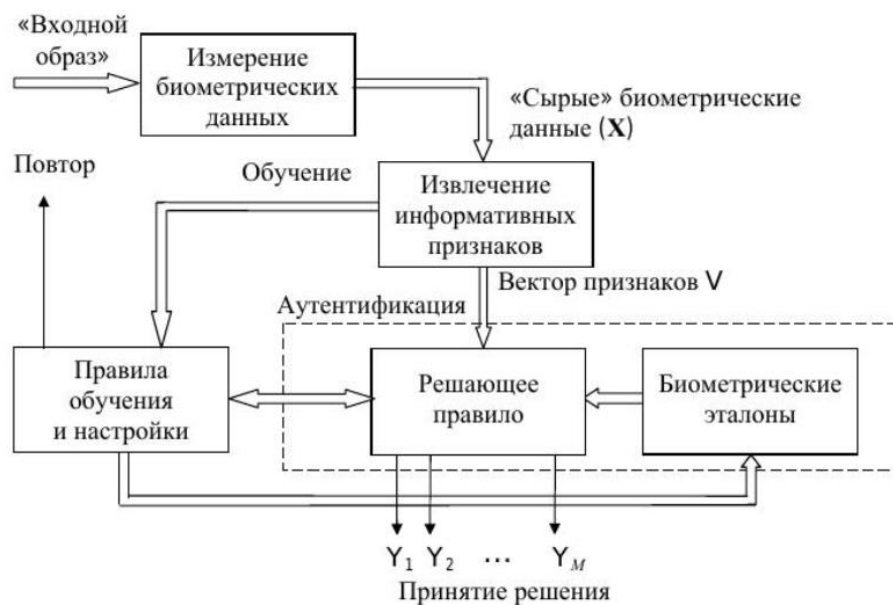


Fig. 2. Block diagram of neural network system of image recognition

When creating "ZORGO", we used two previously trained DLIB — a universal cross-platform software library — `dlib_face_recognition_resnet_model_v1.dat.bz2` (GitHub `dlib-models`). The first neural network defines the face area in the image. This generates a set of data for digital biometrics, these are the coordinates of the eye and mouth corners. When a face is detected on a video image, the neural network transmits the image of the second neural network's face selected according to its coordinates. The second neural network is preliminarily trained on the existing database. The task of the second neural network is to convert facial coordinates into a set of numerical data with 128 characters. Thus, the neural networks form a 128-long data array from the face image, which the system then works with to identify the accessed subject. So the database of the persons admitted to the territory of educational campus is created. The data array is saved, then the new array extracted by the neural network is compared with the existing one. The data warehouse in HDF5 format and computer vision methods are used for image analysis, implemented with the use of web-cameras.

For each subject, the database stores data about no more than ten facial images. The identifier for the array is UUID4 (universally unique identifier) — part of the Distributed Computing Environment (DCE).

Open Source Computer Vision Library (OpenCV) and NumPy are used for video processing. The Face_recognition layer for Python is also used, which allows to use the DLIB written in C++ (it is installed using the package manager pip).

The mechanism of implementation of the authentication procedure is as follows: in real time mode the video recording of the premises of the educational institution, or the entire territory of the campus is made. The resulting video image highlights the face area. The known methods of image recognition are used (Zhilyakov, 2007) (Balabanova & Devitsyna, 2018). Then the program searches for key points, obtains the biometric code and compares this code with the database. In case of coincidence, the program not only indicates to the observing operator that the subject has been identified successfully, but also shows his name and surname. If the subject is not identified, the operator sees a red frame on the image, the system informs about the presence of an unauthorized visitor on the territory, in this case the subject is considered an intruder.

To start the program, it is necessary to make preparations:

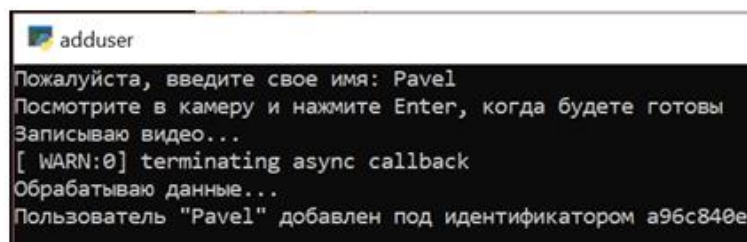
1. Install Python 3.6 in catalogue C: \Python36
2. With the help of the package manager "pip" we install the necessary libraries:
 - `dlib` is a C++ library that implements neural networks and `face_recognition`;
 - `numpy` — linear algebra methods and arrays;
 - `hdf5py` — library for working with HDF5 standard files;
 - `OpenCV` — library of computer vision.
3. Start working with the program.

Source files for working with the program:

- `adduser.py`; `Recognize.py` — programs that represent user functionality;
- `adduser` — shortcut that launches `adduser.py` program;
- `webcam` — launches `recognize.py` in webcam mode;
- `access` — launches `recognize.py` in text mode;

- `improcessing.py` — used to process images using `face_recognition` (which in turn is applied to `DLIB`). In this file the interface is implemented, which is used to input data into the predictor module;
- `predictor.py` — the core of the system, which is responsible for the search and comparison of persons in the `HDF5` database. The key method is `"predict_face"` - this method returns a list of persons similar in parameters to the transmitted image.

To start the biometric identification mechanism in `Zorgo` it is necessary to open the program `"adduser"`, and to carry out the procedure of adding a new user, the subject's name is entered and a picture of the face is taken with the help of a webcam.



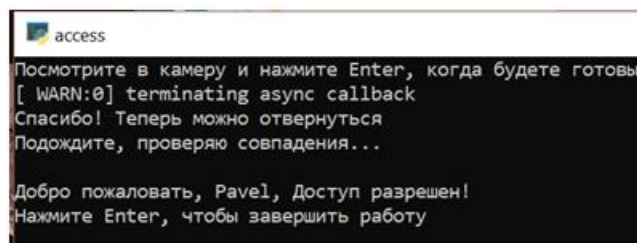
```

adduser
Пожалуйста, введите свое имя: Pavel
Посмотрите в камеру и нажмите Enter, когда будете готовы
Записываю видео...
[ WARN:0] terminating async callback
Обрабатываю данные...
Пользователь "Pavel" добавлен под идентификатором a96c840e

```

Fig. 3. Program window "adduser".

Next, open the program `"access"` and try to access the system (see Fig. 4). At the previous stage, when using the program `"adduser"`, the system has already received data about the entered name and the corresponding image of the person.



```

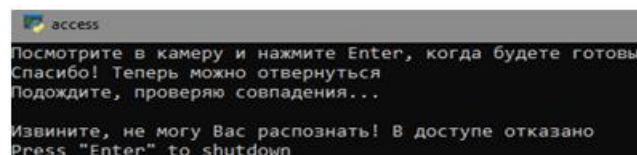
access
Посмотрите в камеру и нажмите Enter, когда будете готовы
[ WARN:0] terminating async callback
Спасибо! Теперь можно отвернуться
Подождите, проверяю совпадения...

Добро пожаловать, Pavel, Доступ разрешен!
Нажмите Enter, чтобы завершить работу

```

Fig. 4. Successful access to the system

If no data is entered into the system, it will deny access (see Fig. 5).



```

access
Посмотрите в камеру и нажмите Enter, когда будете готовы
Спасибо! Теперь можно отвернуться
Подождите, проверяю совпадения...

Извините, не могу Вас распознать! В доступе отказано
Press "Enter" to shutdown

```

Fig. 5. Denial of access

Thus, a database of employees and trainees is formed. To enter the data into the database, it is enough just to look at the screen once, tick the user's name and surname. This process takes about 15 seconds.

Then the trained and configured system can be used to control the perimeter of the campus. The information from the cameras is analyzed and as soon as the user's video image appears on the screen, the program, in case of successful identification, highlights the face area with a green frame, in which the user name is specified (see Fig. 6).

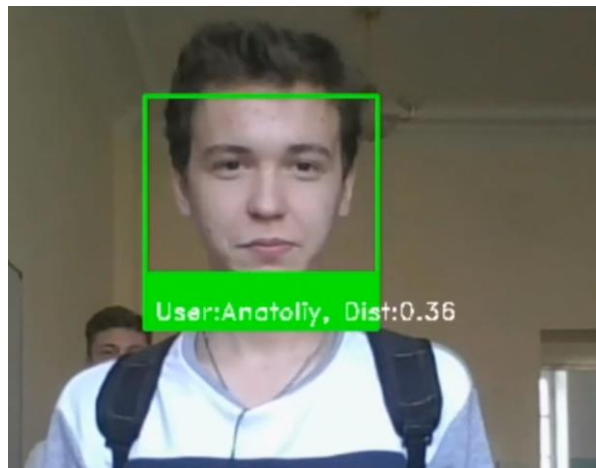


Fig. 6. Program window with successfully recognized subject

In the area of the frame that highlights the face on the video image, you can specify: User - user name, Dist:0.36 — metric distance. The smaller the metric distance is, the more precise the coincidence is.

The program carries out successful authentication even in the presence of the subject's headgear, glasses, beard, because the neural network, trained on a large data set, allows on the basis of artificial intelligence technologies to identify the required biometrics and accurately identify the subject (see Fig. 7).

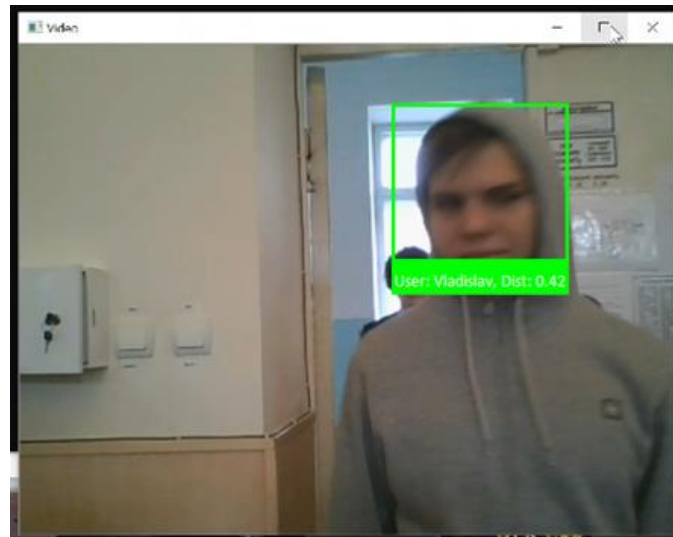


Fig. 7. Program window with successfully recognized subject in the headdress.

If the system does not find the subject in the database by its image, a red frame is automatically displayed to identify the intruder (see Fig. 8).

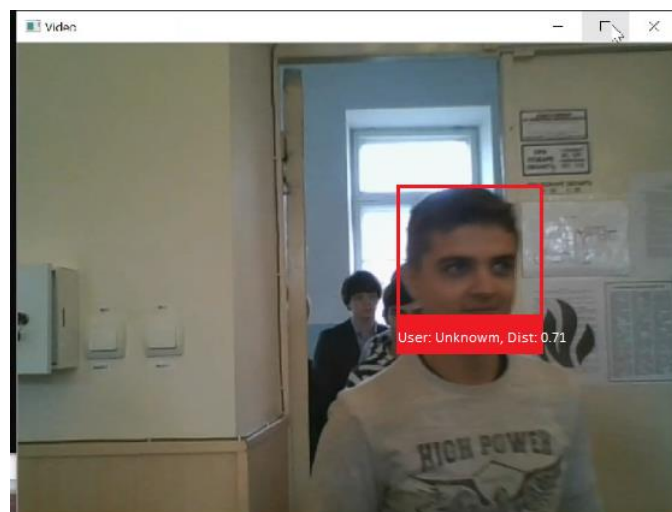


Fig. 8. Program window with unrecognized subject.

3 Conclusion

In this way, the programmer identifies those who violate access to the campus, thus preventing a number of threats, one of which is, for example, terrorist acts and the entry of unidentified persons into the protected area.

References

1. Balabanova, T., & Devitsyna, S. Search for Special Points when Creating a Panoramic Image. VII International Scientific and Technical Conference «Information Technologies in Science, Education and Production»: Conference proceedings, pp. pp. 36 – 41. Belgorod (2018).
2. Federal Law N 152-FZ ON PERSONAL DATA (2006). (In Russian).
3. Order of FSTEC of Russia No.21. "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems» (2013). (In Russian).
4. State Standard ISO/ITU 19794-5-2013 . Information technology (it). Biometrics. Formats of biometric data exchange. Part 5. The image data of the face (with Change No. 1) (2013).. (In Russian).
5. Vasilev, V. Intellektual'nye sistemy zashchity informacii [Intelligent information security systems]. Moscow: Innovative mechanical engineering (2017).
6. Zhilyakov, E. Variational methods of analysis and construction of functions from empirical data on the basis of frequency representations: Monograph (2007).