Ascheulov Nikita Igorevich
Student
Ural Federal University
Russia, Yekaterinburg
Research adviser: Kurmanova Dilyara Ilshatovna

USING OF FACIAL RECOGNITION AS PART OF THE ACCESS CONTROL SYSTEM

Abstract: *In today's world, facial recognition is an integral part of personal and public safety. One of the ways of practical application of facial recognition algorithms is to use them as part of access control and control systems. The purpose of this article is to determine the possibility and assess the feasibility of integrating facial recognition into access control system. Several experiments are carried out, after each of which the system parameters are adjusted. Based on the results of the experiments, the convenience and expediency of joint use of the above-mentioned systems are evaluated.*

Keywords: *face recognition, biometric identification, security systems, access control.*

Ащеулов Никита Игоревич
Студент
Уральский федеральный университет
Екатеринбург, Россия
Научный руководитель: Курманова Диляра Ильшатовна

ИСПОЛЬЗОВАНИЕ СРЕДСТВ РАСПОЗНАВАНИЯ ЛИЦ В СОСТАВЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Аннотация: *В современном мире распознавание лиц – это неотъемлемая часть личной и общественной безопасности. Одним из способов практического применения алгоритмов распознавание лиц является использование их в составе*

систем контроля и управления доступом. Цель этой статьи – определить возможность и оценить целесообразность интеграции системы распознавания лиц в СКУД. Проводится несколько опытов, после каждого из которых параметры системы корректируются. На основании результатов экспериментов проводится оценка удобства и целесообразности совместного использования вышеназванных систем.

Ключевые слова: *распознавание лиц, биометрическая идентификация, системы безопасности, контроль доступа.*

Introduction.

The pace in development of technology is due to the fact that the computers are becoming more intelligent. These intelligent computers lead to computer-human interaction which helps in exploring various fields. Face detection, i.e. the sub domain of object detection is one of the fields based on computer-human interaction. Object Detection is a process that deals with detecting instances of objects from a particular class (such as people, cars, buildings or faces) in an image or video [**Ошибка! Источник ссылки не найден.**, p.1].

Today face recognition is widely applied in different areas of our life. Supermarkets and retail networks use face recognition systems for collecting various data about buyers and visitors. The most interesting data are age, gender, kinds of purchased goods, purchase amount and etc. But one of the most popular application of face recognition is security systems. In this paper we will review the application of access control system based on face recognition algorithms.

Equipment:

As an equipment for the experiments we used a camera LTV CNE-631 4G (it has 1/2.8” CMOS matrix, 3 Megapixels resolution and motorized zoom lens with focal length 9-22 mm). As a face recognition software, we used FindFace Security software package ver. 2.2.1 and ver. 4.0.3. This system is based on neuro nets. This soft gets the most expressed anthropometric traits of the face. It finds them in the recognized from on-line video stream face frame and compares them with a sample from dossiers. As an access control device, we used access controller SIGUR E500U and as a software

for this device we used SIGUR software package ver. 1.0.60.1. As a server for face recognition we used the virtual machine (CPU: Intel Xeon 4x physical cores processor, Integrated GPU, RAM: 10 Gbytes, OS: Ubuntu 16.04). As a server for SIGUR access control system we used the virtual machine (CPU: Intel Xeon 2x physical cores processor, Integrated GPU, RAM: 4 Gbytes, OS: Windows Server 2012 R2).

Experiments and methods:

As participants of the experiments we chose six men who work in the same office. For five days, during the working day, these people passed through the entrance, which faces the camera connected to the recognition system many times. Every day different parameters were corrected in the system, the software version was updated, additions and plug-ins were connected. Each day, we recorded the total number of passes of each person and the number of passes in which the person's identity was successfully recognized (the percentage of false-negative positives or errors of 1 kind is fixed). Next, we will separately consider the changes that occurred in each of the days, as well as the results of measuring the accuracy of the system:

1. The first day of the experiments (fig. 1).

The system was working in default mode after deploying. All parameters are set by default.

2. The second day of the experiments (fig. 2). On the second day of the experiments, the minimum image quality of the face was increased (men_score: -1), the maximum deviation of the face to the side was reduced (min_d_score: -2.5). Set the maximum number of faces in the frame for recognition (npersons: 2) (in order to save server resources). Experimentally we

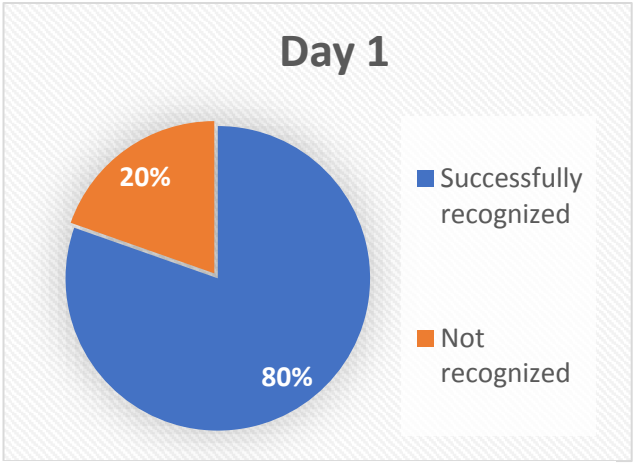

Fig. 3. Results of the first day of experiments

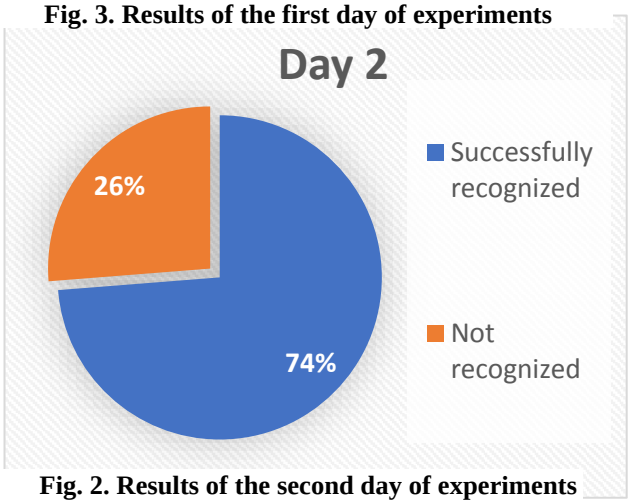

Fig. 2. Results of the second day of experiments

set the minimum size of the face in the frame for recognition (min_face_size: 130). This option allows you to limit the recognition area to the distance from the camera in order to prevent the recognition of unauthorized people in the background.

The changes resulted in a slight decrease in the percentage of successful recognition, but allowed you to configure the recognition zone and optimize the consumption of server resources.

3. The third day of the experiments (fig. 3).

On the third day of the experiments there was reduced the required percentage of similarity with the sample from 75% (default) to 70% in order to increase the probability of recognizing and checking the occurrence of errors of the second kind. There were no errors of the II kind during the whole period of testing.

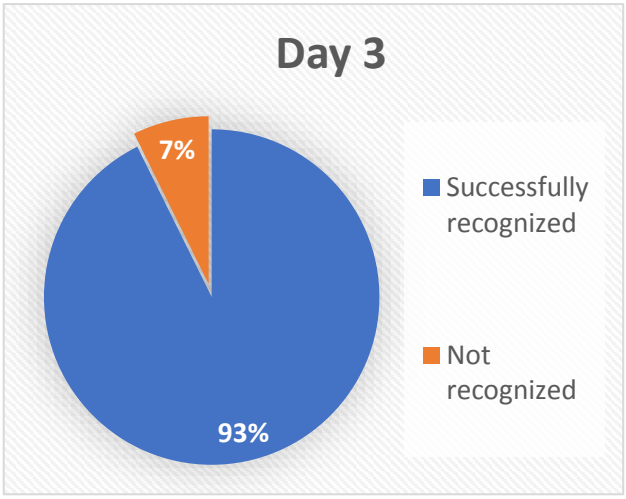

Fig. 4. Results of the third day of experiments

4. The fourth day of the experiments (fig. 4).

On the fourth day of the experiments, FindFace Security was updated from version 2.2.1 to version 4.0.3 in order to test the updated functionality (liveness and video wall for CPU-based systems). Liveness technology is designed to recognize the real person's face as opposed to a fake image on paper (photos).

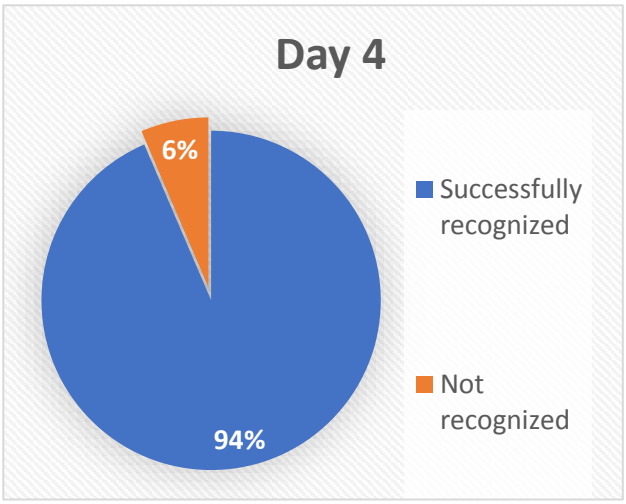

Fig. 5. Results of the fourth day of experiments

5. The fifth day of the experiments (fig. 5).

On the fifth day of the experiments, the liveness function was activated. After activation of the liveness function, a significant increase in server resource consumption was detected (RAM is constantly occupied by 95-97%). This led to a

violation of the stability of the system. Events took much longer to process. Not all events are transmitted to the SIGUR access control system, and there is also a significant delay (tens of seconds). Recognition accuracy decreased.

For the normal functioning of Liveness technology, it is necessary to increase the amount of RAM to 16 GB (minimum requirements), or deploy a GPU-based system (not lower than nVidia GTX 1080).

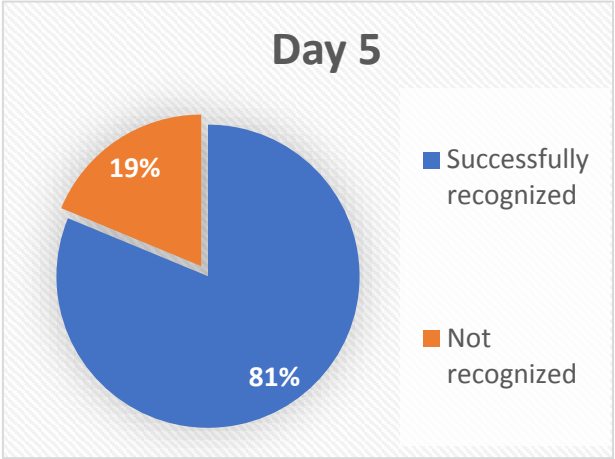

Fig. 6. Results of the fifth day of experiments

Conclusion:

Based on the results of the experiments carried out in this work, it can be concluded that the use of facial recognition algorithms as part of the access control and control system is possible provided that the necessary requirements for the server equipment are met.

If it is not possible to provide powerful and modern server equipment, the system can be used on small objects where there is no large flow of people, while modern functions of emotion detection, liveness technology and others will not work correctly, they will need to be disabled. In order to use the full functionality of the system and ensure high speed and performance of facial recognition, it is necessary to qualitatively work out the server architecture and provide a good supply of hardware resources.

REFERENCES

1. Kirti Dang. Review and Comparison of Face Detection Algorithms // 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence • January 12-13, 2017 • Noida, India.