Akademia Techniczno-Humanistyczna w Bielsku-Białej
WYDZIAŁ BUDOWY MASZYN I INFORMATYKI
Inżynier XXI wieku
XI Inter University Conference „Engineer of XXI Century" – 10 December 2021

ADDITIONAL AUTHENTICATION OF PRIVILEGED USERS BY THE GEOMETRY OF THEIR FACE IN INFORMATION SYSTEMS USING SINGLE SIGN-ON TECHNOLOGY

Olena Vysotska,
PhD, National Aviation University, Kyiv, Ukraine, Department of Computerised Information Security Systems, lek_vys@ukr.net

Anatolii Davydenko,
DSc, Pukhov Institute for Modeling in Energy Engineering of NAS of Ukraine, Kyiv, Ukraine, Department of Mathematical and Econometric Modeling;
National Aviation University, Kyiv, Ukraine, IT-Security Academic Department, davidenkoan@gmail.com

Summary

This work argues the expediency of performing additional authentication of privileged users of information systems using a single sign-on technology. To do this, it is proposed to use biometric technology recognition technology by geometry of their face. The stages of the authentication system based on the proposed biometric technology are considered; on the basis of analysis of the results of conducted experiments, the expediency of using this biometric technology is determined and the conditions for the effectiveness of its placement are indicated.

The proposed system of authentication by geometry of face operates in three modes:

1. Accumulation of a database of educational samples of the corresponding biometric characteristics of all users of the system.
2. Teaching the system to recognize the face of a person. This training consists in creating the Haar cascade based on the analysis of several hundred or thousands of samples, which are images of the object that we need to find (the person's face), as well as images of the environment in which the search will be conducted, in the same quantity.
3. Authentication of users by the geometry of their faces, on condition that the person who authenticate belongs to the group of privileged users and checking its first authentication factor was successful.

In authentication mode, algorithm of system work consists of the following steps:

1. Displaying the boundaries of the area in which the person's face should be located for correct recognition.
2. Reading images from a webcam.
3. Preprocessing an image by blurring areas of the frame that do not expect to accommodate the user's face.
4. Detecting the image of the user's face in the photo, using the cascade of Haar created during training.
5. Determination of characteristic dots on the detected face image by placing a mask with medium-statistical characteristic points on the image and trimming them to a specific face by using the Local Binary Pattern method.
6. The definition of a face descriptor, that is, a vector consisting of descriptors of characteristic points of the face.
7. Definition of face descriptors on all images stored in the database of training samples.
8. Comparison of the descriptor of an unknown sample with the handles of reference samples from the database, using a method based on the Euclides distance measurement. Based on the defined value of Euclid, the probability that the photo presented belongs to the person whose login was previously entered (the lower the distance, the greater the probability).

Experimental study

In order to determine the expediency of using the proposed user recognition technology for the geometry of the face and for empowerment of authentication for privileged users of the information system, which applies a single sign-on technology, and to determine the impact of environmental factors on the first and second kind of error factors, the accumulated database (reference) samples the corresponding biometric characteristics of tenth people. After that, a number of experiments were carried out, the main results of which are demonstrated in the following graphs (Fig. 2, Fig. 3, Fig. 4).

Teen people of different genders, the same age category (about 20 years) took part in the experiments. For each of these individuals, 120 photos were accumulated (several of them were discarded due to unsuitable image quality) for each of the three options (images on a monochromatic background; additional elements are present against the background of the image; images in poor lighting. During the experiments, for determine the errors of the first and second kind, each of the accumulated photos was used as an unknown sample. Experiments were conducted for each of the three specified options.

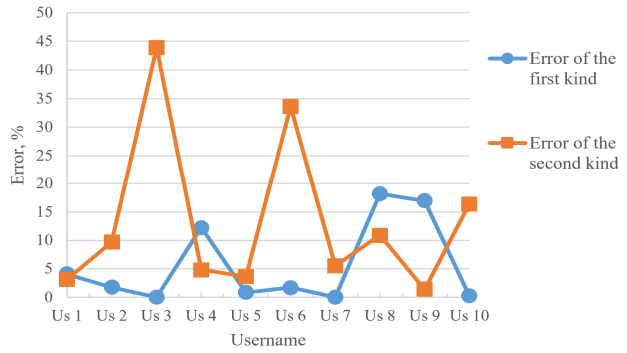

Figure 2. Errors of the first and second kind

After analyzing the results of experiments, the following conclusions can be drawn:

1. When using the proposed technology of biometric authentication by the geometry of face of the users, the probability of an error of the second kind is much higher than the errors of the first kind.
2. In most cases, the likelihood of correct recognition has a significant impact on environmental factors such as poor illumination and, in the absence of preliminary processing, the presence against the background of the image of additional elements.
3. If people work in the organization, in which there is a similar location of characteristic points, then in this case, when using the proposed technology, the probability of a second kind error significantly increases.

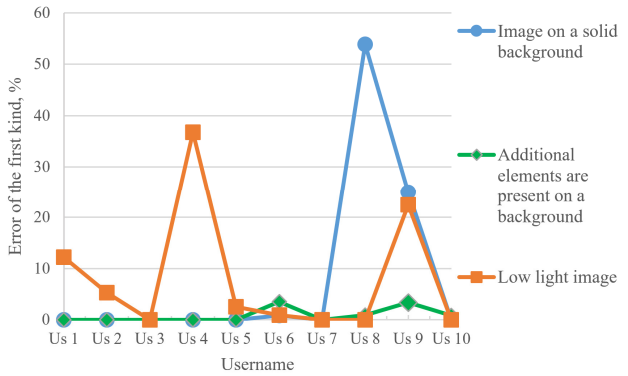

Figure 3. Dependence of the first kind error from environmental factors

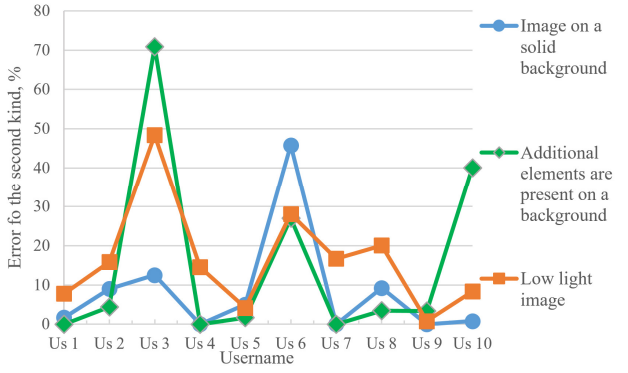

Figure 4. Dependence of the second kind of environmental factors

Conclusion

In this paper, it was proposed in authentication of privileged users in the information system that uses a single sign-on technology, to strengthen the protection of additional verification, namely to implement an additional authentication of the user by the geometry of the face. To determine the expediency of using this biometric method of recognition, the necessary software was developed by which a number of experiments were carried out. Based on the analysis of the results of experiments, we can say that the use of the proposed technology is expedient to solve the problem. But it should be noted that to increase the likelihood of correct recognition, it is necessary to adhere to certain rules when choosing an environment in which authentication is carried out and performed the processing of images that read from the webcam. With the correct use of proposed authentication technologies, privileged users will significantly increase the level of protection of the information system that uses the single sign-on technology.

In addition, it should be noted that technology of authentication by face geometry is contactless, comfortable for users and for now most workplaces have a webcam, does not require specialized equipment. Using the technology to recognize faces in photos and for their comparative analysis are quite effective and, unlike many other technologies (for example, the main component method, the Hopfield neural network), are not very difficult to implement and do not require to calculate the large computer productivity.

Ministerstwo Edukacji i Nauki
Dofinansowano z programu „Doskonała nauka" Ministra Edukacji i Nauki