Olena VYSOTSKA[1], Anatolii DAVYDENKO[2]

Scientific supervisor: Anatolii DAVYDENKO[3]

DOI: https://doi.org/10.53052/9788366249868.27

DODATKOWE UWIERZYTELNIANIE UPRAWNIONYCH UŻYTKOWNIKÓW WEDŁUG GEOMETRII ICH TWARZY W SYSTEMACH INFORMATYCZNYCH WYKORZYSTUJĄCYCH TECHNOLOGIĘ SINGLE SIGN-ON

Streszczenie: Artykuł przedstawia możliwość dodatkowego uwierzytelnienia uprzywilejowanych użytkowników systemów informatycznych przy użyciu technologii pojedynczego logowania. W tym celu proponuje się wykorzystanie technologii biometrycznej do rozpoznawania użytkowników po geometrii ich twarzy. Rozważane są etapy systemu uwierzytelniania opartego na proponowanej technologii biometrycznej. Na podstawie analizy wyników eksperymentów; określono celowość zastosowania tej technologii biometrycznej oraz określono warunki jej skuteczności w stagnacji.

Słowa kluczowe: uwierzytelnianie biometryczne, geometria twarzy, technologia jednokrotnego logowania, system informacyjny, uprzywilejowany użytkownik

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

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 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.

[1] National Aviation University, Department of Computerised Information Security Systems, lek_vys@ukr.net

[2] National Aviation University, Department of Computerised Information Security Systems, lek_vys@ukr.net

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

Keywords: biometric authentication, geometry of face, single sign-on technology, information system, privileged user

1. Introduction

Recently, a fairly common phenomenon is the use of single sign-on technology [1] when accessing various subsystems of large information systems. That is, by performing the authentication procedure when trying to access one subsystem of a large system, the user automatically gets the appropriate access to other subsystems of this system. Typically, such authentication is based on a password or other information known to the user. This method of access is acceptable in the case of ordinary users, whose access rights are usually minimal. However, applying an appropriate method of granting access to privileged users, who accordingly have a much wider range of rights to the system, increases the risk of violating the confidentiality, integrity and availability of information processed in this information system. In addition, it can also lead to a malfunction of the entire system. That is, if an attacker with a successful attempt to penetrate one of the subsystems immediately receives maximum access rights to the entire system, it can lead to significant harm to the organization in which the system operates, and for its employees. This fact explains the need and expediency of strengthening the authentication procedure for users from the privileged group in those systems that use single sign-on technology. It is advisable for users with extended access rights to use multi-factor authentication instead of one-factor authentication. The second factor can be checked either immediately, when logging in, or when trying to perform an action that requires extended access rights. As a second factor in this paper, it is proposed to use one of the biometric methods of authentication [2-7]. For greater convenience of use and expansion of the range of organizations in which this technology is effectively used, it is advisable to use those biometric technologies that do not require additional expensive equipment. In this paper, it is proposed to use geometry of face recognition as the second factor in authentication. An ordinary webcam, which is now available on almost all computers, is enough to implement this method.

2. Formulation of problem

To determine the feasibility of using a biometric method of user recognition by geometry of face to enhance the authentication of privileged users of the information system, which uses single sign-on technology, was:

- analyzed technologies that can be used to implement the authentication process on the selected biometric feature, and selected from them, which should be used to solve this problem;
- software developed on the basis of previously selected technologies;
- database assembled of training samples with the corresponding biometric characteristic;
- with the help of the developed software, a number of experiments were carried out, thanks to which it was:

- identified errors of the first and second kind in the recognition of system users;
- researched what conditions needs to be studied in case, it is necessary to adhere to increase probability of the correct recognition;
- researched what specific processing of samples must be performed for the correct application of this method of recognition.

3. Solving the problem

The operation of any biometric authentication system is impossible without the presence of a pre-assembled database of training samples of the relevant biometric characteristics of all potential users of the system.
On the basis of the assembled training (reference) samples, as a rule, the training of this authentication system is carried out.
Then you can directly perform the procedure of user authentication by geometry of face, which consists of the following 4 main stages:

1. Entering the user's login and read from the camcorder (webcam) the image on which the user's face is located.
2. Image pre-processing, which is necessary to increase the stability of the system and minimize errors.
3. Detection on the image directly of the user's face and the formation of his descriptor, meaning a sample of this person biometric characteristic.
4. Formation of descriptors for each, pre-processed, training (reference) sample, comparison of them with descriptor of the unknown sample and making a decision based on concerning results of performance of authentication procedure.

Consider the operation of this authentication system in more detail.
In this case, you can perform geometry of face authentication either immediately, when logging in, or when trying to perform a function that requires extended access rights. Accordingly, the user's login must either be entered during this authentication, or it is already entered by the user at the beginning of the current session in the information system.
To read an image of a user's face when working on a computer, a regular webcam that is already built into the computer or installed in the computer system as a separate device is sufficient. Given the principle of operation of the selected recognition technology and the fact that the user is at a short distance from the camera, there are no basic requirements for the webcam is not necessary. But for this recognition system to work properly, the image from the camera is transmitted to the computer screen so that the user can position his face so that the image of his face is in the specified area of the image.
In this work, Haar's features are used to recognize a person's face on a photo [9-11].
Haar features - are digital image features used to recognize patterns. The main advantage of using Haar features is the processing speed, thanks to which you can easily process even streaming video. This method is also flexible due to the ability to customize the search process. These features can be used to identify many objects, one of which is the human face. In order to adjust the signs to search for a specific object, ie a person's face, you need to create (perform training) a Haar cascade. This

process takes place using several hundred or thousands of samples (4000 in this paper), which are images of the object we need to find, as well as images of the environment in which the search will be performed, in the same number. This cascade will allow you to detect a face by applying a mask of Haar primitives on parts of the image with a step-by-step movement across the image until the desired object is found.

The creation of the Haar cascade is divided into the following 2 stages [9-11]:

- collection and preparation of the necessary samples that will participate in the training of the cascade;
- cascade training.

It is better to use photos with the faces of real employees to prepare samples, that are images of the object we need to find, because the more similar the samples are to real objects, the more stable the search will be. The photo should only have a face image without unnecessary elements. In addition, these photos must be of the same format. It is also very important to provide photography for learning in the environment where the search will be conducted, taking into account the lighting and angle of the camera, as this can also significantly affect the stability of the successful location of the object (hereinafter determined experimentally). Since the environment and lighting points are usually more or less stable in the conditions in which the use of this authentication system, these shortcomings will not have a significant impact. For stable operation of the cascade it is recommended to make 3000-4000 positive samples. This work used 4,000 photos, which show the object that will need to be searched in the future. For similar reasons, when filling the library of samples of images of the environment in which the search will be conducted, the photo should be taken at the point of recognition in working light and camera angle. It is also recommended to make 3000-4000 samples for stable recognition. The work used 4000 relevant photos.

The classifier is formed on Haar primitives by calculating the values of the features. Each Haar primitive consists of a light and dark fragment [9-11]. Haar's sign value is the difference between the sum of the brightness values of the dots that are closed by the light part of the primitive and the sum of the brightness values of the dots that are closed by the dark part.

A matrix identical in one size to the original image is used for the calculation. Each element of the matrix stores the sum of the intensities of adjacent pixels. Haar signs can be calculated quickly, over a constant time. The use of Haar features gives a point value of the brightness difference along the X and Y axes, respectively.

The created Haar cascade can be further used to detect images of faces of system users in the photo, during their authentication.

When recognizing a face, the correspondence of the image to the Haar primitives is determined by the difference of the sums of the brightness values of the pixels on the rectangular subregions of the Haar primitive. Since the Haar primitives in the cascade are created for a fixed-sized face, and the face itself will not be placed on the whole photo, it is necessary to apply Haar primitives on parts of the image with step-by-step movement and zooming at the end of the analysis. The moving window method is used to search for objects using the Haar cascade. Primitives from the Haar cascade are superimposed on part of the image, after which the brightness of the white and black areas is compared. The correctness of the face recognition result is influenced by the following cascade search parameters. The zoom scale cannot be less than one, but the higher this value, the stronger the search field at the end of the scan of the

whole photo. If this value is higher, the scan rate will be faster, but the chance of missing the desired object in the frame increases. The number of adjacent search squares cannot be less than one. A higher value for this parameter will allow for a more thorough analysis, but this will negatively affect the search speed, as the search field will move more slowly. The optimal value for this parameter is 3-6. The minimum dimension of the template determines the initial size of the area in which the search will be conducted. For the face it is better to take a square area of 30 by 30 pixels. There is also a maximum window setting, but if you ignore it, the window will enlarge until it fills the entire image, which will increase the search time, but also increase the chance of successful detection of the object.

But to identify a person only to determine the presence of the person will not be enough, you need to determine who specifically is trying to access the resource. To identify a person, you need to rely on something, namely certain features that are unique to each person. In the case of a human face, this information for identification may be characteristic points of the face. Namely, the points on the edges of the eyes, mouth, eyebrows, nose and the shape of the face, which together have a different location for each person.

These characteristic points can be identified by placing a mask with average statistical characteristic points on the image and aligning them to a specific face by using the Local Binary Pattern (LBP) method [12]. The LBP method is resistant to noise and texture variations in the image and faster in calculation. Thus, after applying a mask with average statistical characteristic points, these points are adjusted according to the found face, by moving the point to the nearest place where there is a sharp color difference in the photo, which in turn acts as the edge of the face (nose, mouth or eye). The standard mask of average statistical characteristic points is shown in Figure 1.

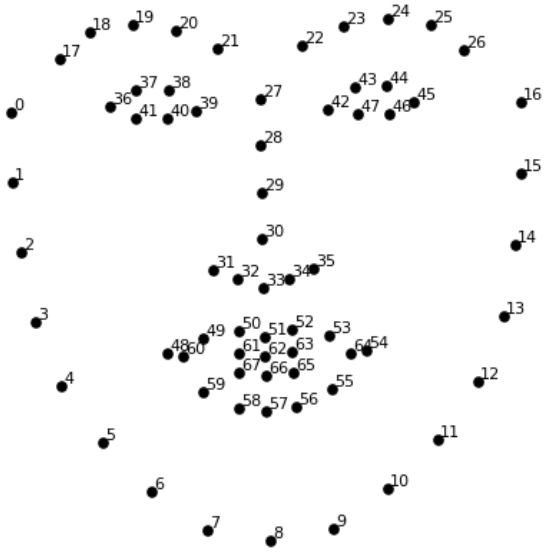

Figure 1. Mask of average statistical characteristic points

The LBP method allows you to determine in which direction the brightness decreases relative to the point in the photo on the normal. This operation will determine in which direction and how far the edges of the cheekbones (0-16 points), mouth (48-67 points), nose (27-35 points), eyes (36-47 points) and eyebrows (17-26 points). The calculation is made according to the formula:

$$LBP(g_{Px},g_{Py})=\sum_{p=0}^{P-1}S(g_P-g_C)\times 2^p \quad , \tag{1}$$

where g_c -is the intensity of the central pixel in the sample, and g_p - the intensity of adjacent pixels.

Function S is described in the following way:

$$S(x)=\begin{cases} 1, if \geq 0, \\ 0, if \ x<0, \end{cases} \tag{2}$$

These results are added to the binary number and converted to decimal. Then the histogram of dependence of intensity and deviation from the central point which is a point of a mask of characteristic points of the average statistical person is constructed. This deviation is built on the normal relative to the contour of the mask.

Thus, knowing the location of the reference points of the face, you can determine the identity of the person trying to enter the system.

After determining the characteristic points of the face depicted in the photo, it is necessary to determine the descriptor of the face. A descriptor is a set of characteristics that describe a person regardless of external factors, such as gender, age, hairstyle and the like. Special features are analyzed, namely the characteristic points of the face, which were identified earlier. That is, we can say that the face descriptor is a description of the face in the form of a vector, which consists of descriptors of characteristic points of the face.

The calculated face descriptor can then be used for comparison with the reference image descriptors to determine whether the training sample database contains data on the user to be authenticated, and whether it is really the privileged user whose login was entered in the current session. But before that, it is necessary to calculate the descriptors for all images of faces, whose images are stored in the database of training samples.

To compare the descriptor of the unknown sample with the descriptors of the reference samples from the database, in this paper used a method based on the calculation of the Euclidean distance. This method is to compare two data vectors, which allows you to determine their similarity.

The similarity of the vectors, meaning the distance of Euclid, can be calculated by the following formula:

$$d(p,q)=\sqrt{\sum_{k=1}^{n}(p_k-q_k)^2} \quad , \tag{3}$$

where n – is the number of elements in the vector, p_k –is the value k- number of the first vector, and q_k – is the value k- number of the second vector.

The smaller the value of Euclid, the more likely it is that the unknown face is the face of the same person depicted in the reference image. If the value is bigger than 0.6 (recommended threshold), then this person does not match the reference.
If the person matches the reference, then the next step is to compare the login that was entered earlier, whether it matches what belongs to the found person. If the result of the login comparison is positive, it means that this privileged user has passed the authentication procedure. If the result of the comparison of logins is negative, then it means that some other legal user, most likely with less access rights, is trying to access the resource on behalf of another legal user with more rights.
If the face did not match any reference, means the Euclidean distance was always greater than 0.6, it means that the system does not have samples of the geometry of the face of the user who is now trying to access the resource and, most likely, the violator.
In some cases, it may happen that the face image is either not found at all on the image transmitted from the webcam, or, conversely, several face images have been captured. This usually happens either if the lighting is very poor, or there are some external obstacles to highlighting the face image, or if the image captured by the webcam contains elements that are similar in shape to a person's face.
To minimize the chance of recognizing objects in the environment as human faces and to avoid double recognition if other people are nearby and their faces are in the camera's field of view, you need to process the images obtained from the webcam.
We implement this processing by blurring areas of the frame, which do not provide for the placement of the user's face. Because the position of the computer's head is usually about the same and the image of the face falls into the same area, it allows you to process (blur) the largest area and leave the smallest area to recognize. If the defined area of the face during processing and the actual placement of the face of the user will have deviations between them, the user can adjust the position of the head, by marking the area of future processing in the frame when reading photos from the webcam. To blur areas of the frame where the user's face is not planned, you need to create a photo that is completely filled with noise and a mask that will highlight the coordinates that need to be left without noise.
The blurring itself is as follows. The Core - is the size of the matrix that will be involved in calculating the pixel value. The pixel of the photo being calculated is the center of the matrix core. All pixels that fall under the influence of the matrix core are involved in the calculation, that is, if the core is 3 by 3, then all pixels that fall into the matrix of 3 by 3 with the center in the pixel to be calculated, will participate in the calculation. This area is selected from the photo, multiplied by the matrix core, after which all the obtained values are added to one whole, which is a new pixel value.
The larger the radius of the core, the stronger the admiration is created as a result of this calculation.
After performing the specified image processing, the process of finding the coordinates of the face using the Haar cascade will be much more stable, because the objects that the cascade could be confused with, are too blurred in the frame, and the only non-blurred object in the frame is the face that should be recognized.
Summing up we can say the following.
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).

4. 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.

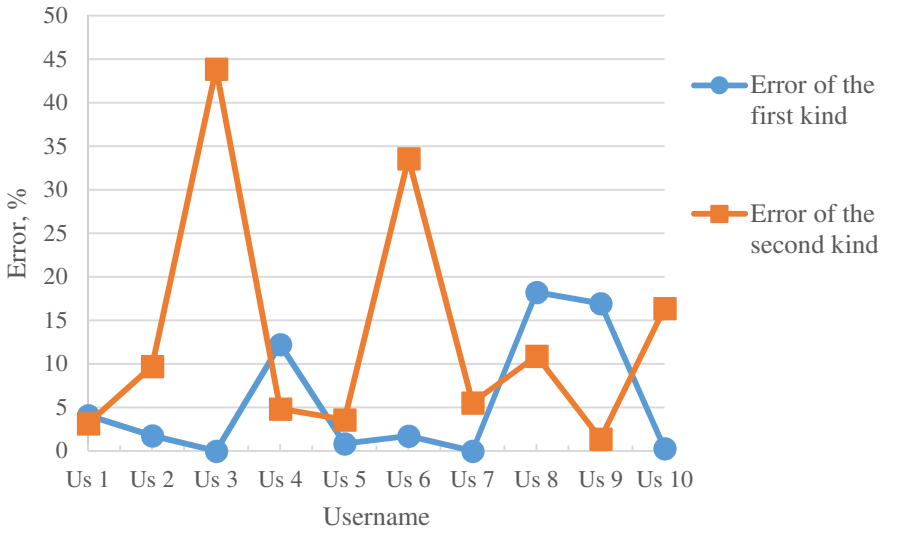

Figure 2. Errors of the first and second kind

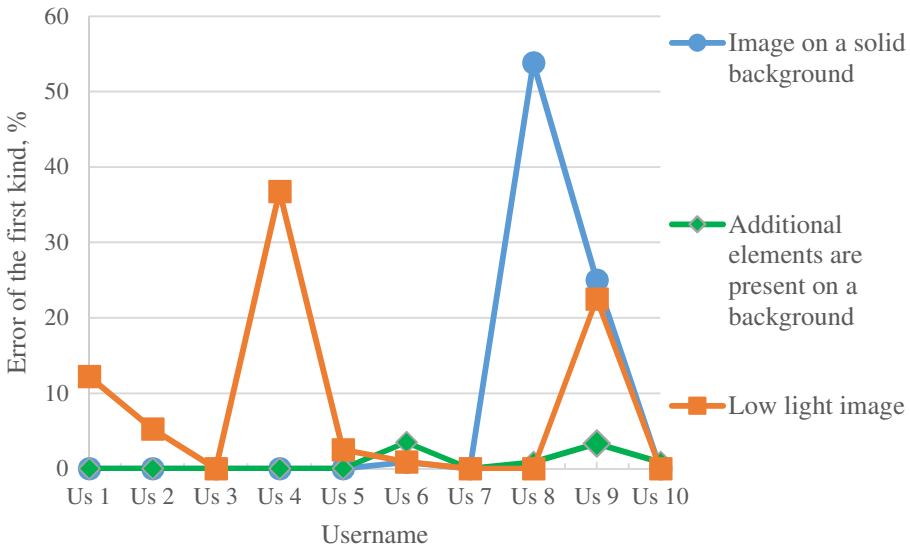

Figure 3. Dependence of the first kind error from environmental factors

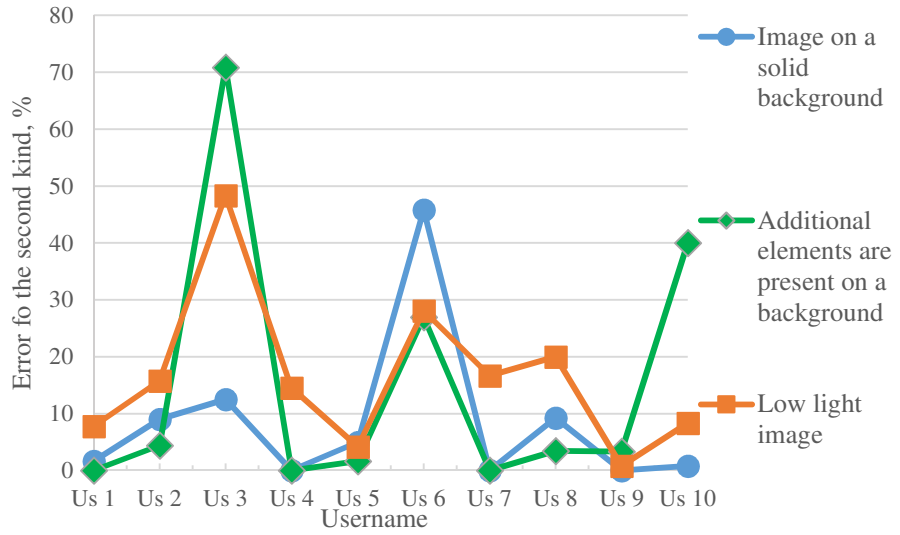

Figure 4. Dependence of the second kind of environmental factors

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

- 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.
- 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.
- If people work in the organization, in which there is a similar location of characteristic points, then in this case, when using the probability of a second kind error significantly increases.

5. 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.

REFERENCES

1. ROEBUCK K.: Single sign-on (SSO): High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors. Emereo Publishing 2016.
2. VYSOTSKA O., DAVYDENKO A.: Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing, **938**(2019), 356-368.
3. DAVYDENKO A., VYSOTSKA O., SHMELOVA T.: Methods of Primary Processing Handwriting Samples at User Authentication Using a Probabilistic Neural Network. 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine 2019, 723-735.
4. KORCHENKO O., DAVYDENKO A., VYSOTSKA O.: Authentication method of information systems user by their handwriting with multi-stage correction of primary data. Information Security, **21**(2019)1, 40-51. DOI: *https://doi.org/10.18372/2410-7840.21.13546.*
5. ZOUBIDA L., ADJOUDJ R.: Integrating Face and the Both Irises for Personal Authentication. International Journal of Intelligent Systems and Applications (IJISA), **9**(2017)3, 8-17. DOI: 10.5815/ijisa.2017.03.02
6. MUTHANA H. H., SAMAH K. A.: Biometric System Design for Iris Recognition Using Intelligent Algorithms. International Journal of Modern Education and Computer Science (IJMECS), **10**(2018)3, 9-16. DOI: 10.5815/ijmecs.2018.03.02.
7. SHANMUKHAPPA A. A., SANJEEVAKUMAR M. H.: Biometric Person Identification System: A Multimodal Approach Employing Spectral Graph Characteristics of Hand Geometry and Palmprint. International Journal of Intelligent Systems and Applications (IJISA), **8**(2016)3, 48-58. DOI: 10.5815/ijisa.2016.03.06.
8. MESSOM C.H., Barczak A.L.C.: Fast and Efficient Rotated Haar-like Features Using Rotated Integral Images. Australian Conference on Robotics and Automation (ACRA2006), 2006, 1–6.
9. LIENHART R., MAYDT J.: An extended set of Haar-like features for rapid object detection, ICIP02, **1**(2002), 900–903.
10. PHAM M.T. et al.: Fast polygonal integration and its application in extending haar-like features to improve object detection. 2010 IEEE

Computer Society Conference on Computer Vision and Pattern Recognition, 2010, 942–949.
11. HUANG C.-C., TSAI C.-Y., YANG H.-C.: An Extended Set of Haar-like Features for Bird Detection Based on AdaBoost. Signal Processing, Image Processing and Pattern Recognition SE – 17, Springer Berlin Heidelberg, **260**(2011), 160–169.
12. GUO Zh. ZHANG L.. ZHANG D.: A completed modeling of local binary pattern operator for texture classification. IEEE transactions on image processing, **19**(2010)6, 1657-1663.