

DOI: 10.37943/LYFW8581

D. Muratuly

2nd year doctoral student of the educational program “Information Systems”
Muratulydidar@gmail.com, orcid.org/0000-0002-7821-811X
D. Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk,
Kazakhstan

N.F. Denissova

Candidate of physical and mathematical sciences, Vice-Rector for Research
and Digitalization
NDenisova@edu.ektu.kz, orcid.org/0000-0003-0525-730X
D. Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk,
Kazakhstan

Y.V. Krak

Doctor of Physical and Mathematical Sciences,
Head of the Department of Theoretical Cybernetics
Yuri.krak@gmail.com, orcid.org/0000-0002-8043-0785
Taras Shevchenko National University of Kyiv, Ukraine

K.S. Apayev

Head of System Administration and Educational Process Department
Kapaev@edu.ektu.kz, orcid.org/0000-0001-9292-4785
D. Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk,
Kazakhstan

BIOMETRIC AUTHENTICATION OF STUDENTS TO CONTROL THE LEARNING PROCESS IN ONLINE EDUCATION

Abstract. This article considers the relevant problem of biometric authentication of students in higher educational institutions. The authors present the results of using a turnstile system with a face recognition terminal, with the ability to provide unique biometric data in real time. The study was conducted among students of the D. Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk, Kazakhstan. The article presents the results of studies of one of the biometric methods of personality recognition. In this method, the process of proving and verifying the identity of the person can be carried out through the presentation by the user of his biometric image. The processing results are sorted and compared with typical images from the database. With its positive decision, the developed software issues the results of biometric authentication of a person who presented himself in front of a digital scanner. The applied value of the results of the work lies in the possibility of using them in the field of education, and various industries to make a decision on providing access to information resources. In the course of the study, a technology was developed to provide biometric authentication processes for university students. Domestic and foreign scientists who have made a significant contribution to the development of methods for processing facial images are noted. A review of biometric methods of recognition is carried out, and tools for electronic authentication and modern information security systems are described. Factors that significantly affect the probability of correct recognition of students' faces are determined. The analysis of ways to increase the probability of correct recognition of students by the image of the face is carried out.

Keywords: Biometric authentication, face recognition

Introduction. Trust-based e-assessment systems are becoming increasingly important in the digital age for academic institutions. Digitalization is one of the key solutions to current problems: it adds flexibility to higher education and makes higher education accessible to all students, regardless of their personal life situations, geographical location, exceptional local or global circumstances (for example, the world situation associated with COVID-19) [1].

While the digitalization process opens up more opportunities, it also poses a number of challenges for higher education institutions. Student authentication is recognized as an important issue in online education. In their article “Using Biometrics for User Authentication in Online Learning: A Systems Perspective,” Virginia Tech Professor Asad Moyni and University of Southern California Professor Azad M. Madni, founder and chairman of Intelligent Systems Technology, Inc., emphasized that students must pass authentication before they are given access to sensitive content such as tests, assignments, or personal notes. Therefore, with the development of online education and e-assessment methods, it is critical to improve student authentication. If universities can provide secure and convenient systems for electronic authentication, they can create a more secure environment in which they offer a variety of studies for all students [2].

The purpose of this study is to create an information technology for biometric authentication of students in the process of distance learning. The object of research is the task of increasing confidence and the use of methods used for video analytics tasks. The subject of the research is the analysis and implementation of a biometric authentication system in the process of distance learning.

To achieve this purpose, the following tasks are solved:

- analysis of known methods and algorithms for recognizing a person from a face image and confirming the authenticity of a recognizable object;
- substantiation of a mathematical model, a method for identifying faces in a video stream;
- development of information technology to ensure the process of recognition and authentication of a recognizable object.

Authentication refers to verification of the identity of a user, device, or process, and is often required before access to system resources is granted. Authentication can be performed either at the start of a session or as an ongoing process in which the user is continuously authenticated during the session.

Electronic authentication tools can be divided into three main types:

- 1 Knowledge – information that the subject knows (password, PIN code);
- 2 Possession – a thing that the subject possesses (electronic or magnetic card, token, flash memory);
- 3 Property possessed by the subject (biometrics, natural unique differences: face, fingerprints, iris, capillary patterns, DNA sequence) [3].

Table 1. Authentication methods for conducting exams (1)

Technique	Technique classification	Description
User ID	Knowledge Based Authentication	Based on personal information provided by the user.
Password		
Security question		
Mouse movement	Behavioral biometrics	Behavioral characteristics. Can be used with continuous authentication.
Keystroke dynamics		Voice test with a microphone. Can be used as continuous authentication.
Voice		Behavioral characteristics.
Signature		Behavioral characteristics. Identifies authorship by language styles of authors
Stylometry		
Handwriting		There are two types of handwriting-based authentication: one based on static information (letter width, density) and one based on dynamic information. Can be used for online exams.
Face recognition	Physiological biometrics	Can be used with continuous authentication
Fingerprint		Can be used for continuous user authentication; if it is included with other devices.
Eye tracking		Eye tracking feature to check users.
Binaural beats		ERP (Event Related Potential). Signals used to explain the cognitive information process.
Palm print		Physiological features. Requires additional scanning devices.
Smart card, memory card	Ownership-Based Authentication	Based on private objects owned by the user. Maybe stolen or duplicated
IP address	Other-mechanisms	Can be used to determine the user's possible location. The IP address can be used as an indicator of cheating during exams.

Online education and problems of student authentication.

With the rapid growth of online learning, students increasingly need easy and flexible access to learning content anytime, anywhere they choose. Verifying the identity of students and the authenticity of their work is becoming increasingly important to reduce academic abuse and for quality assurance purposes in education.

Information security is associated with ensuring the confidentiality, integrity and availability of information in all its forms [4]. There are many tools and methods that can support information security management. But a system based on biometrics has evolved to support some aspects of information security [5]. Using biometric data, teachers and specialists can determine how actively students are involved in learning activities [6].

The automatic behavior recognition system belongs to the class of real-time systems. This means that the correctness of its functioning depends not only on the logical correctness of the calculations, but also on the time during which these calculations are performed. At the same time, the most significant criterion for the effectiveness of the designed system (as a pattern recognition system) is the reliability of the recognition results. However, in practice, there are usually limitations that do not allow reaching this level without losing the performance of the recognition system.

Face recognition technology. Principles of the system.

In recent years, computer vision has gained popularity and has become a separate area. Developers create new applications that are used all over the world. Facial recognition has become widespread because the face plays an important role in conveying a person's identity in social interaction and requires neither advanced equipment nor physical contact to recognize it. Face recognition systems (FRS) use pattern matching to compare two faces and generate a match score reflecting their degree of similarity [7].

When solving the problem of face recognition in two-dimensional images, another important factor plays a role - these are the face projection angles that arise when photographing a student [8]. Thanks to the developed ball.py project, the ball moves along a predetermined trajectory and at this moment the webcam takes photos of the students.

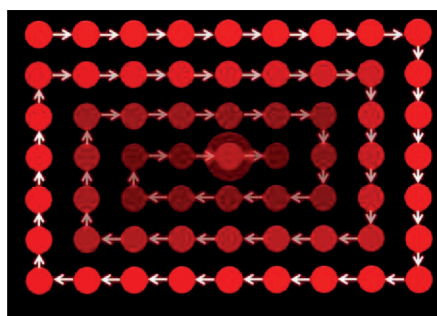


Figure 1. ball.py project for getting 2D images of a student's face

Students of the educational program 21-IS-1 and 21-CE-1 were assigned identification numbers, and 768 photographs of students' faces were taken for recognition. For the study, personal data of students with their own permission were used.

Table 2. List of students of the educational program 21-IS-1

Nº	Full name	ID Number
1	Brim Anna Igorevna	1411996
2	Zarifulin Artur Enverovich	1411994
3	Kiselev Viktor Sergeevich	1411991
4	Kolosov Andrey Sergeevich	1411993
5	Plotnikov Mikhail Antonovich	1411995
6	Sandybaev Asan Zineldinovich	1411997

Table 3. List of students of the educational program 21-CE-1

Nº	Full name	ID Number
1	Balashov Viktor Sergeevich	1412024
2	Bekshentaev Maksat Kazezovich	1412029
3	Golshtein Eduard Olegovich	1412028
4	Zakaria Islam Talgatuly	1412030
5	Kalinin Vladimir Andreevich	1412026
6	Moldakanov Madiyar Sungatuly	1412025

As a rule, a face recognition system is a software and hardware complex for automatic verification or identification of a person by a digital image (photo or video sequence frame).



Figure 2. The process of taking photographs of students

The functioning of the face recognition system begins with the construction of a person template according to the available biometric image. In face recognition systems, two-dimensional images or decompressed frames from a video stream are most often used as images [9].

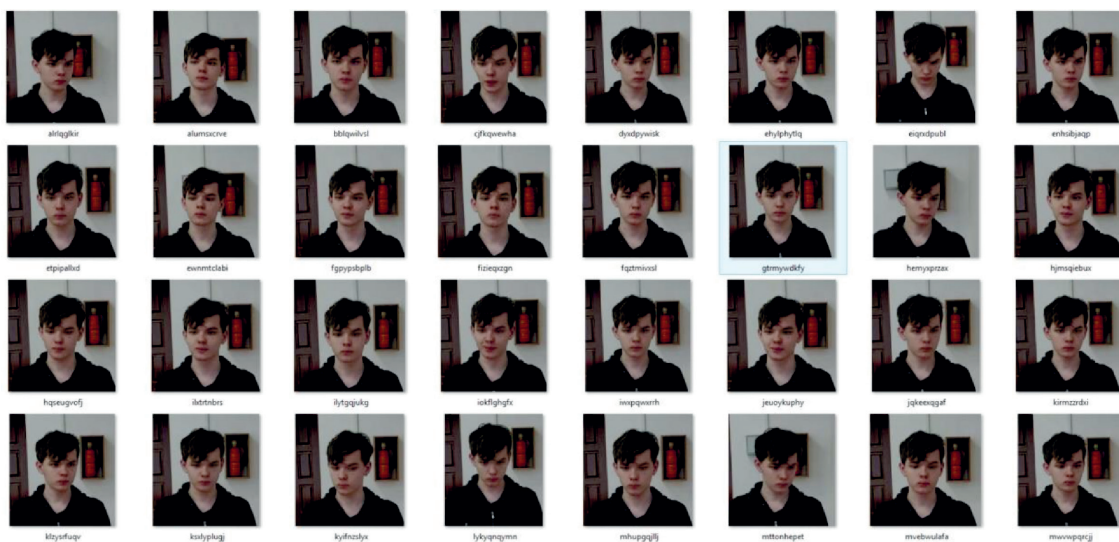


Figure 3. Two-dimensional images of students

Preparing a database for face recognition systems involves solving two problems: obtaining images suitable for processing, and marking them up. Obtaining images of faces can take place under controlled conditions, then the angles of rotation, tilt and deviation of the head are limited, special lighting and equipment for photography are installed, and the emotional coloring of the face is set [10].

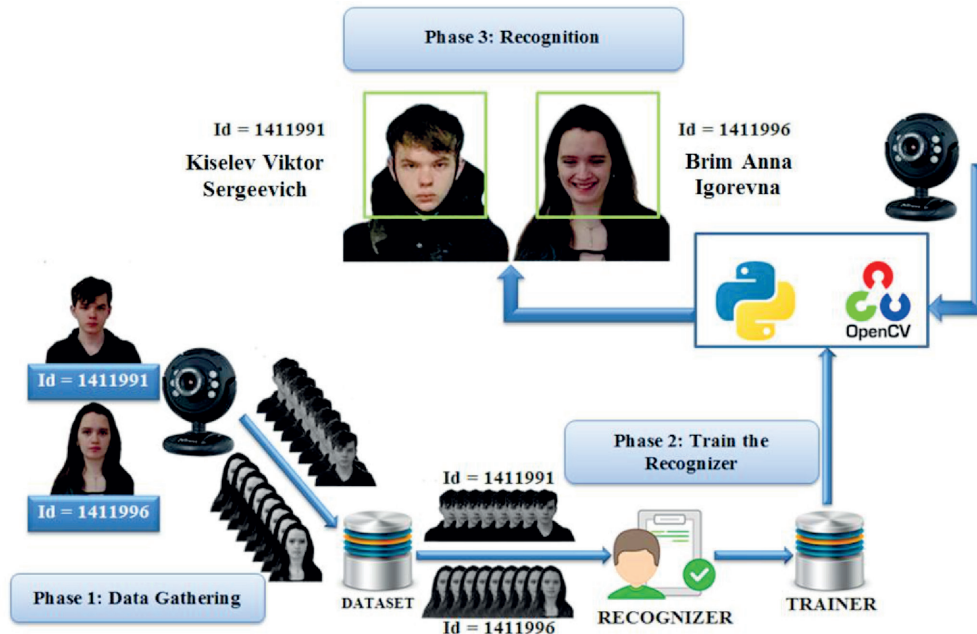


Figure 4. The main stages of real-time face recognition

At the first stage, face detection is performed from video data using the Viola–Jones object detection framework. A feature of this method is the processing of a video stream in real time. The Viola–Jones object detection framework allows you to classify various objects, but its main area of application at present is face recognition.

The work of the Viola–Jones object detection framework is based on the selection of features similar to Haar-like features and the use of a cascade classification model.

A feature of the Viola–Jones object detection framework is to work with an integral way of representing an image. Matrix elements are calculated using the following formula:

$$L(x, y) = \sum_{i=0}^x \sum_{j=0}^y I(i, j) \quad (1)$$

Where $I(i, j)$ is the brightness of the current pixel of the source image, (i, j) are the coordinates of the current pixel.

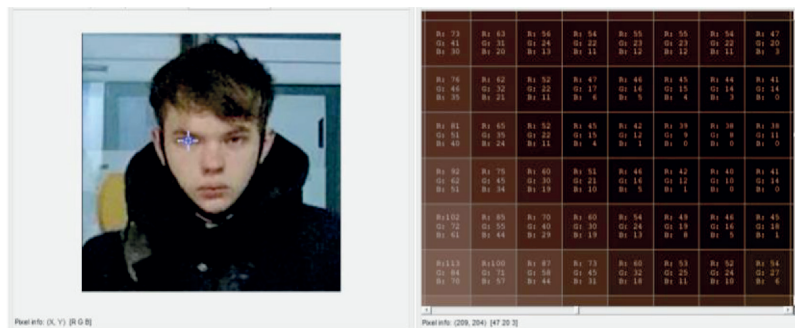


Figure 5. Pixel area on target image

The histogram of an image is one of the most informative characteristics. Based on the analysis of the histogram, one can judge the brightness distortions of the image, i.e. to tell if the image is dark or bright.

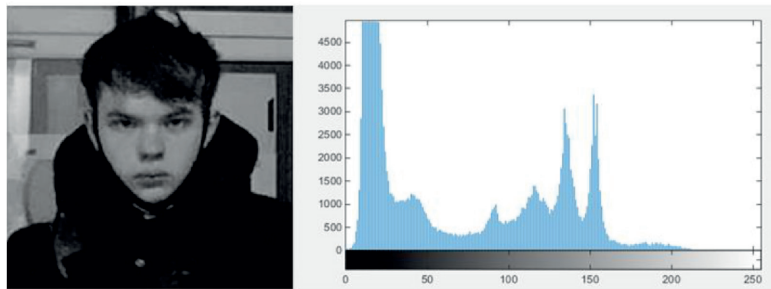


Figure 6. Source image for recognition

It is known that, ideally, a digital image should have equal numbers of pixels with all brightness values, i.e. the histogram should be uniform. The redistribution of the brightness of pixels in the image in order to obtain a uniform histogram is performed by the equalization method, which is implemented in the Matlab system as the `histeq` function.

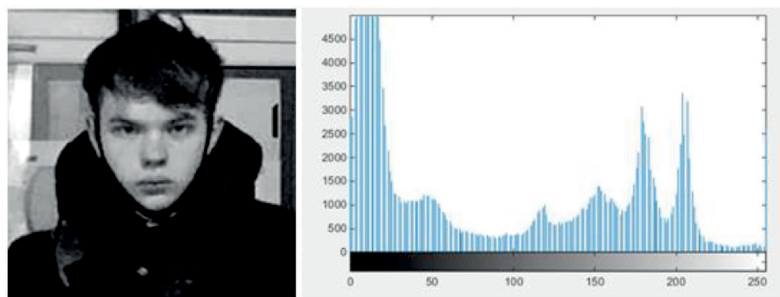


Figure 7. Processed image for recognition

Each element of the matrix L is the sum of the pixels in the rectangle from $(0,0)$ to (x,y) , i.e. the value of each pixel (x,y) is equal to the sum of the values of all pixels to the left and above the given pixel (x,y) .

Matrix calculation is possible by the formula:

$$L(x, y) = I(x, y) - L(x - 1, y - 1) + L(x, y - 1) + L(x - 1, y) \quad (2)$$

Using such an integral matrix, one can quickly calculate the sum of pixels of an arbitrary rectangle and an arbitrary area [11].

7	4	5	6	3	7	11	16	22	25
3	7	6	4	5	10	14	32	42	50
4	4	3	5	6	14	29	43	58	72
5	7	8	6	7	19	41	63	84	105
6	3	5	4	8	22	50	77	102	131

Figure 8. An example of working with an integral way of representing an image

The value of Haar-like features is calculated as the difference between the sums of pixels of image areas inside black and white rectangles of equal size.

$$F = X - Y, \quad (3)$$

where, X is the sum of the brightness values of the points covered by the light part of the feature, and Y is the sum of the brightness values of the points covered by the dark part of the feature.

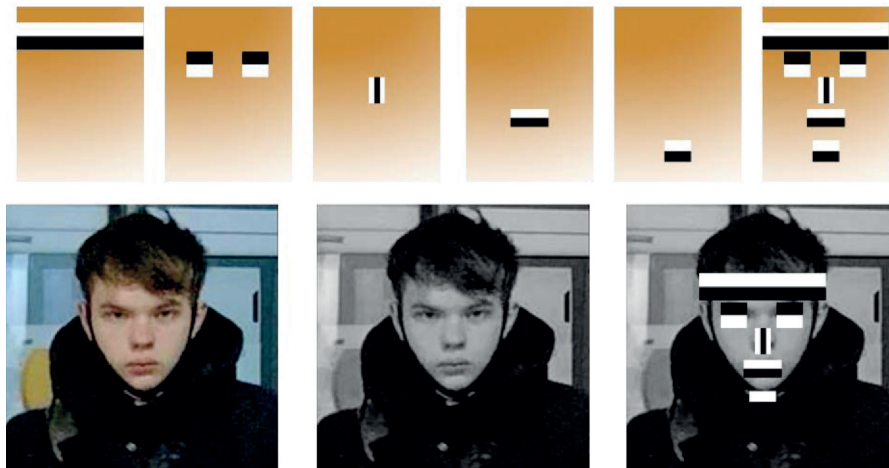


Figure 9. Face mask using Haar primitives

The Haar-like features in the Viola–Jones object detection framework are organized into a cascade classifier. The idea of cascading classification is to gradually increase the number of applied primitives, which increases the speed of the algorithm, filtering out regions in which the face was not found in the early stages.

Practical implementation. On the basis of D. Serikbayev East Kazakhstan Technical University, a turnstile system was developed with a face recognition terminal, with the ability to provide unique biometric data in real time. The system works in two modes: comparison with a database or with an ID. Both modes use high-definition cameras to capture the student's faces as they enter at the turnstile. This is done in order to create a biometric profile of the visitor from the received image, which is then immediately compared with the database [12].

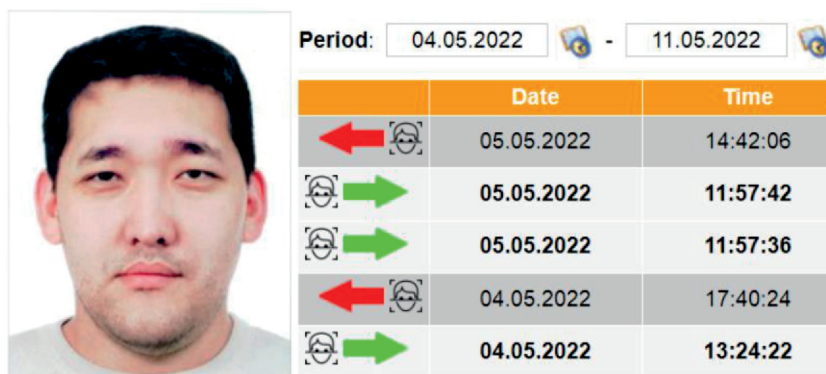


Figure 10. Passage through the checkpoint

The turnstile system with a face recognition terminal works according to a simple principle: using a terminal or a computer, pictures of students' faces are entered into the database and linked to their accounts. During each passage through the turnstile, the system analyzes the employee's access rights and makes a decision to allow the passage, registration is recorded in the system database, with reference to time.

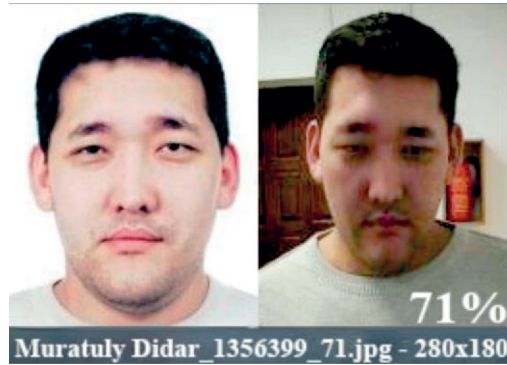



Figure 11. Face recognition result

The turnstile system with a face recognition terminal showed a high speed of face recognition, which ensures uninterrupted operation of the equipment even in conditions of heavy flow of people. The recognition accuracy is affected by the efficiency of the applied algorithm, the number of face and user templates in the terminal memory, as well as the parameters of the camera operation in different lighting conditions [13].

Table 4. Results of face recognition of students of EP 21-IS-1 and 21-CE-1

	ID number: 1411991 Last name: Kiselev Name: Victor Event date: 01-02-2022 Recognition accuracy: 0.7013295
	Id number: 1411993 Last name: Kolosov Name: Andrey Event date: 01-02-2022 Recognition accuracy: 0.68451077
	Id number: 1412025 Last name: Moldakanov Name: Madiyar Event date: 02-02-2022 Recognition accuracy: 0.6820017
	Id number: 1412028 Last name: Golshtein Name: Eduard Event date: 07-02-2022 Recognition accuracy: 0.69320565

	<p>ID number: 1412030 Last name: Zakaria Name: Islam Event date: 09-02-2022 Recognition accuracy: 0.6886546</p>
---	---

Research results.

The accuracy of the model created by using a turnstile system with a face recognition terminal, with the ability to provide unique biometric data in real time, depends on the number and status of uploaded images for model training. The greater the number of images and the more defects are applied to the image in different situations, the higher the accuracy of the model [14].

The model was trained on 40 epochs. The developed system divides the samples into two segments - for training and for testing. Training samples make up 85% of all samples. They are used to train the model to separate samples into generated classes. Test samples make up 15% of all samples. They are never used to train the model, but are needed for testing. Test samples allow you to evaluate how well the model copes with the classification of samples that it sees for the first time [15].

Conclusion

The use and diversity of electronic authentication technologies are important components of online education. Another topical issue of educational policy is the diversity of students in higher education institutions. The above questions are essential elements of higher education in the future [16].

The biometric authentication mode, in contrast, assumes a low level of trust in the person being authenticated. In biometric authentication, the applicant person must prove the authenticity of his claimed name by presenting his unique biometric images. It should be noted that biometric authentication is potentially vulnerable if it is used independently of classical authentication methods based on protocols using passwords and keys. A sufficient level of information security can only be ensured by combining classical and biometric authentication methods [17].

The introduction of student authentication and authorship verification technology is a relatively simple step in response to widely perceived threats, and therefore it could be a catalyst for further analysis of academic integrity leading to changes in institutional policy on academic integrity.

An analysis of the turnover of scientific papers in the world dimension was carried out, which allows you to see an objective picture of development and assess the relevance of this topic. A review of biometric authentication technologies in modern information sources has been carried out. The task is given and the main problems that can be used in the course of its solution are identified. The characteristic of frequently occurring cases of identification and identification of persons is given. An algorithm for determining informative features and confirming the reliability of an object is described. The results of the analysis of the grounds for the study and implementation of a comprehensive solution to the problems of using information resources. And also in the course of the developed study, information technology to provide biometric authentication processes.

New complex technology for face image preparation is proposed, which ensures the functioning of software systems for personality recognition in the video stream in real time in

automatic mode, the distinguishing features of the technology are the combination of known methods and the receipt of new results that lead to the solution of the tasks.

References

1. H. Farouk E.-S., Al, K. Alghatani T. A., (2013), 'The impact of cloud computing technologies in E-learning', *International Journal of Emerging Technologies in Learning (IJET)*, vol. 8,89, pp. 37–43.
2. Moini A., Madni A.M., (2009), 'Leveraging biometrics for user authentication in online learning: A systems perspective', *IEEE Systems Journal*, 3(4), pp.469–476, [https://doi: 10.1109/JSYST.2009.2038957](https://doi.org/10.1109/JSYST.2009.2038957).
3. Kashyap R., (2019), 'Biometric authentication techniques and E-learning', *Biometric Authentication in Online Learning Environments*, IGI Global, Hershey, PA, USA, pp.236-265, [https://doi:10.4018/978-1-5225-7724-9.CH010](https://doi.org/10.4018/978-1-5225-7724-9.CH010).
4. Kotwal D.V., Bhadke S.R., Gunjal A. S., (2016), 'Online examination system', *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 1, pp. 115–117.
5. Okada A., Whitelock D., Holmes W., (2019), 'E-authentication for online assessment: a mixed-method study', *British Journal of Educational Technology*, vol. 50, no. 2, pp. 861–875.
6. Atoum Y., Chen L., Liu A. X., Hsu S. D., Liu X., (2016), 'Automated online exam proctoring', *IEEE Transactions on Multimedia*, vol. 99.
7. Kausar S., Huahu X., Ullah A., (2020), 'Fog-assisted secure data exchange for examination and testing in E-learning System', *Mobile Networks and Applications*, pp. 1–17.
8. Cao Q., Shen L., Xie W., Parkhi O., Zisserman A., (2018), 'VGGFace2: A dataset for recognising faces across pose and age', in *Proc. 13th IEEE International Conference on Automatic Face & Gesture Recognition*, pp. 67-74.
9. Dang K., Sharma S., (2017), 'Review and comparison of face detection algorithms', *7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, Noida, India, Jan. 12-13.
10. Dundar A., Jin J., Martini B., Culurciello E., (2017), 'Embedded streaming deep neural networks accelerator with applications', *IEEE Transactions on Neural Networks and Learning Systems*, vol. 28, no. 7, pp. 1572–1583.
11. Pranav K.B; Manikandan J., (2020), 'Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks', *Procedia Computer Scienc*, Volume 171, pp. 1651-1659, <https://doi.org/10.1016/j.procs.2020.04.177>.
12. Liao S., Jain A. K., Li S.Z., (2016), 'A fast and accurate unconstrained face detector', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 2, pp. 211–223.
13. Zhao K., Xu J., Cheng M., (2019), 'Deep face recognition via exclusive regularization', In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp.1136–1144, <https://doi.org/10.1109/CVPR.2019.00123>
14. Schroff F., Kalenichenko D., Philbin J., (2015), 'A unified embedding for face recognition and clustering', In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 815–823.
15. Kumar A.; Kaur A.; Kumar M., (2020), 'Review Paper on Face Detection Techniques', *International journal of engineering research & technology*, 8, pp.32–33.
16. Rusyn B.P., Lutsyk O.A., Kosarevych R.Y., (2021), 'Evaluating the informativity of training sample for classification of images by deep learning methods', *Cybernetics and Systems Analysis*, Vol. 57, N6, pp.853–863, <https://doi.org/10.1007/s10559-021-00411-4>
17. Salamh A. B. S., & Akyüz, H. (2022), A New Deep Learning Model for Face Recognition and Registration in Distance Learning, *International Journal of Emerging Technologies in Learning (IJET)*, 17(12), pp.29–41., <https://doi.org/10.3991/ijet.v17i12.30377>