Analysis of Biometric Identification Methods Used in Auto-Proctoring

Anargul Bekenova, Sandugash Bekenova, Ainura Gumarova, and Gaukhar Kamalova

1 Introduction

The introduction of the distance learning format into the educational process has caused many different difficulties, one of which is the provision of remote control of exams. One of the control activities is the confirmation of the identity of the examiner, the primary need of which is when taking the exam. Since the teacher does not have the opportunity to remember all the students equally, the problem of identifying the identity of the examiners arises, as well as the need for regulatory support of the process [1]. In general, it can be characterized as a technology based on the implementation of control over the knowledge of students by specially trained people (proctors) who are not full-time employees of an educational institution. However, the possibilities of such methods of control are limited, primarily due to low bandwidth. In addition, the question of protecting the user's personal data is relevant [2]. The solution to such difficulties is the development of automation of identity identification when conducting control measures. Currently, not only a login-password is used as an identifier, but also biometric characteristics of a person. Today, the biometric identification approach is more effective because it reduces the student's chances of realizing deception or falsehood. We analyze the pedagogical applied resources of biometrics as a way of identifying a person based on physiological or behavioral characteristics [3].

A. Bekenova · S. Bekenova · A. Gumarova · G. Kamalova (✉)
Zhangir Khan West Kazakhstan Agrarian-Technical University, Uralsk, Kazakhstan

R. Bolgov et al. (eds.), *Digital Geography*, Springer Geography,
https://doi.org/10.1007/978-3-031-50609-3_5

2 Materials and Methods of Research

The study is aimed at determining the rationality of using the results in the proctoring system through a comparative assessment of various approaches to identifying the biometric identity of the student used in conducting remote control activities. In the course of the study, methods of analysis, comparative analysis, and analytical research were used [4].

3 Results and Their Analysis

Proctoring is a somewhat complex system, built separately, and then a flexible system of training or control [5].

Proctoring for remote control of exams was first used by ProctorU (USA) in 2008: The administrator tracked student examiners through a webcam and recorded any violations. Since then, digital technologies have improved significantly, many operations have been automated and introduced into the e-learning process, respectively; projecting has been carried out in three main ways [6, 7]:

1. Proctor: A human administrator monitors the progress of the exam through a webcam and records violations manually.
2. Auto-proctoring: The program independently checks the identity of the student, controls his behavior and the direction of his views, analyzes sounds in the room, removes violations on video, and prepares reports.
3. A person and a program – a mixed version: It can be implemented in two ways:
   (a) The whole process is controlled by the program and, in case of violation, sends a signal to the Proctor.
   (b) The test takers are controlled by the online administrator himself. The latter option is considered the most reliable, since any operation of the program can be disrupted [8].

At the same time, the proctor, thanks to the automation of the process, can simultaneously take exams from several students and not lose sight of anything [9].

The human biometric characteristics used in autoproctoring are numerous, and accordingly, so are the methods of identification. Each approach has its own priorities and vulnerabilities [10].

Modern biometric identification is based on two approaches:

- Static approach recognizes the physical parameters of a person throughout his life: from birth to death (fingerprints, eyeball feature, retina pattern, thermogram, face geometry, hand geometry, and even a fragment of the genetic code).
- Dynamic approach analyzes the characteristic features, features of user behavior displayed when performing any everyday action (signature, keyboard handwriting, voice, and much more) [11].

Despite the variety of biometric approaches, in practice, proctoring systems mainly use two: recognition by keyboard handwriting and face image (two-dimensional or three-dimensional (2D or 3D) image). However, some biometric identification methods have the potential to be used in proctoring systems [12–14].

3.1 Methods of Biometric Identification

Static approach is based on the physiological characteristics of a person present with him throughout his life:

- Fingerprint identification
- Face identification
- Identification by the iris of the eye
- Identification by hand geometry
- Identification by face thermogram
- Identification by DNA
- Identification based on the acoustic characteristics of the ear
- Identification by vein pattern

Dynamic ones take as a basis the behavioral characteristics of people, namely, subconscious movements in the process of repeating any ordinary action: handwriting, voice, and gait [15, 16].

- Voice identification.
- Identification by handwriting.
- Identification by keyboard handwriting and others.
- One of the priority types of behavioral biometrics is the manner of typing on the keyboard. When it is determined, the printing speed, the pressure on the keys, the duration of pressing the key, and the time intervals between presses are recorded [17].

A separate biometric factor can be the manner of using the mouse. In addition, behavioral biometrics covers a large number of factors unrelated to the computer – gait, features of how a person climbs the stairs [18, 19].

There are also combined identification systems using several biometric characteristics, which allows meeting the most stringent requirements for the reliability and security of access control systems.

To match by any parameter, the following conditions must be met:

- Parameter universality: Each person must have a measurable characteristic (except in unique isolated cases) [20].
- Uniqueness of the setting: The description must have sufficient differences between individuals.
- Parameter stability: The biometric characteristic does not change over time, for example, in the aging process [21].

3.2 Standardization of Biometric Identification Templates

Biometric authentication is a large-scale segment of the security systems market with high potential: both commissioning and development of new technologies. In fact, it is no exaggeration to say that every new biometric identification device can use new principles and algorithms of operation. Of course, this gives a huge scope for the creativity of developers, but it sharply raises the question for the user about the compatibility of equipment from different manufacturers and sometimes about the compatibility of equipment with different software versions [22, 23].

The Image Group is one of the main research organizations working on the standardization of biometric technologies. Members of the group serve on various standardization committees in INCITS/M1, ISO/SC 37 and have the support of the FBI and other government agencies around the world. The scope of the group's interests also includes testing algorithms for the operation of biometric devices using facial recognition technology, iris, and fingerprints. In particular, there is a free MINEX testing service for the latter. The test results are publicly available, which allows users and installers to get an additional assessment of the characteristics of the equipment they are interested in.

The biometric identification stage is based on a comparison of the data of the object to be identified and the biometric benchmark. Such a comparison is made by pre-recording and storing biometric information. A scanner for measuring a biometric characteristic and an algorithm that allows you to compare it with a pre-registered characteristic are the main tools of the automated biometric approach, an additional assessment of the character of interesting ones [24].

3.3 Biometric Identification Criteria

To determine the effectiveness of the access control and management system based on biometric identification, the following indicators are used [25]:

- FAR – false pass ratio
- FMR – the probability that the system incorrectly compares the input sample with an inappropriate template in the database
- FRR – false failure rate
- FNMR – the probability that the system is mistaken in determining the matches between the input sample and the corresponding template from the database
- ROC graph – visualization of the tradeoff between FAR and FRR characteristics
- Registration failure rate (FTE or FER) – the rate of unsuccessful attempts to create a template from input data (with low quality of the latter)

- Error Retention Rate (FTC) – the probability that an automated system is not able to determine biometric input data when they are presented correctly
- Template capacity –the maximum number of data sets that can be stored in the system

Most of the ways of biometric identification are faced with the same types of difficulties: choosing a mathematical algorithm for processing information that provides maximum accuracy; developing the most convenient and most effective hardware; and overcoming obstacles or distortions that occur when registering indicators. Since such difficulties are inherent in all biometric methods of identification and differ only in the degree of successful solution, we will dwell in more detail on the specific features of biometric technologies [26].

3.4 Identification by Fingerprints (Dactyloscopy)

Dactyloscopy is the most common technology used today in biometric access control systems. The technology is based on the uniqueness of papillary patterns on the fingers of people. The fingerprint obtained by the scanner is converted into a digital code and stored in the database and then compared with the previously entered and modified "fingerprint codes."

Advantages of biometric fingerprint access control in comparison with other biometric systems are user friendliness, ease of creation and use of algorithms, reliability of the approach, availability (including price) and speed of application, and high reliability of fingerprint scanning devices.

The main disadvantages of using this approach are destruction of the papillary pattern with small scratches, cuts, and chemical reagents and inability of some scanners to read the print with excessive dryness of the skin.

However, the use of this approach in the proctoring system is not effective, where attempts to deceive can be easily implemented, for example, a student can be identified by fingerprint, but another person can perform control measures [27].

3.5 Identification by the Structure of the Surface

Face recognition is divided into 2D and 3D approaches, which are distinguished by the possibility of spatial extrapolation and construction of a volumetric model of the face or the creation of a system of control points in a plane (2D) face image.

2D technology provides a smooth, two-dimensional image. The face recognition program reads the parameters of the face and gives the minimum aggregate images of physical and mathematical symbols.

Recognizing a person in his portrait is one of a number of tasks that are directly related to the analysis of a person's face. In addition to such tasks as automatic search for the area of the face in photographs and automatic selection of facial expressions, which can be considered as sub-areas of pre-processing of images when identifying people, other tasks that are not related to facial recognition have occurred [28].

The Advantages and Weaknesses of 2D Technology

2D algorithms are the most popular on the market due to their efficiency and budget. High demand pushes the developers of the technology to constantly improve it.

Currently, among the weaknesses of 2D algorithms, we can note high error margins: false pass – 0.1%; false pass – 2.5%.

The Advantages and Weaknesses of 3D Technology

3D creates a three-dimensional image and is characterized by the high quality of the created image. There are several ways to read the face: laser, scanners with backlight and digital processing of image bends, and working scanners with photogrammetric technology.

The main priority of 3D technology is high reading accuracy. The percentage of false passes is low, only 0.0005%, and the error failure rate is 0.1%. Other advantages of 3D technology can also be considered:

- Availability of equipment
- Non-contact
- Clarity of the procedure for the student
- Use of equipment to monitor the student's behavior during the exam
- The impossibility of falsification due to constant or periodic verification of the identity of the student

But this accuracy of work requires complex equipment and approaches to development. Therefore, among the weak points, the following can be distinguished: the need to purchase expensive cameras to support the 3D function; the lack of accumulated reserves of identified people significantly complicates the analysis of people in real time; and the percentage of differences in Twins for personality recognition is actually very low [29].

This direction of identification is developing most dynamically, is of interest to developers of mobile applications and devices, and is already used in proctoring systems. This technology is widespread due to the simplicity and wide distribution of the necessary equipment (video cameras), as well as the naturalness of human facial recognition [30].

A way of identification through the pupil of the eye. The structure of the pupil of the eye is recognized by it as the main biometric feature in these identification systems. Each person has a unique pupil structure (the structure of the left and right eyes is also different), so it is a reliable biometric sign.

The weak point of this approach is that in the process of pupil identification, many systems are currently unable to accurately recognize the image of the pupil, interfering conditions: eyelashes, eyelids, glare, corner of the eye, etc.

A special place among other ways of identification is occupied by writing, because for a long time the manuscript was the object of careful study and examination. As a rule, a handwritten signature is used when authenticating in administrative and financial institutions. Signing in writing depends on the psychophysical state of the signer and external circumstances. This process is recognized as the result of a complex process, such as its dependence on noise and distracting moments, for example, as the parameters of the recording device [31].

The ways to automatically recognize writing are as follows:

1. The static (offline) approach analyzes the graphic characteristics of the signature as a result; the characteristic features of writing individual letters and elements are recorded, and the signature is recognized as a graphic image.
2. The dynamic (online) approach uses a recording device that emits a signal during the recording process; in this case, the signature is a set of space-time characteristics of the recording process.

Touch screens or electronic pens, and sometimes virtual reality gloves, are used as registration tools. Signatures are recognized by image parameters (points, contour ratio, fragment orientation, and Gray level in pixel tone) or pen movement characteristics (pen position, strength, and direction of movement).

The advantage of this approach for the proctoring system is the ability to control the student's text writing and reduce the load on the proctor in case of unnecessary verification of the student's actions. However, such a system may require additional costs and improvements.

3.6 The Way of Identification Through the Entry on the Keyboard [32]

The principle of identifying an individual by keyboard handwriting consists in the ability to analyze the temporal characteristics of keystrokes when entering a password phrase.

Here, when entering the same phrase several times, a trained user usually performs most of the manipulations on the keyboard at an unconscious level. This creates the effect of keyboard handwriting, that is, the user forms a stereotype of automatic action when entering a password. The controlled keyboard input parameters are the time of pressing each key in the password, as well as the time interval between pressing adjacent keys.

A large-scale study of this area of recognition made it possible to make marginal estimates: The probability of correct recognition of users with stable skills of working with the keyboard is 98% [33].

Most importantly, the advantage of identifying the user through the keyboard handwriting is to combine it with the password phrase approach, that is, the password breaker must also know the password phrase and fake the characteristics of the keyboard handwriting.

However, this approach also has a disadvantage: the instability of the handwriting settings under different physiological conditions and the similarity of the handwriting settings of inexperienced users (entering the password slowly and with one or two fingers). This creates the need to restrict the approach to the authentication area of users, as the reference differences in a large database will be significantly related.

It should be noted that this method of identification is used in many proctoring systems; at the same time, the advantages of this approach are the absence of the need for additional equipment, simplicity for the user, and the ability to hide the identification process for entering a password.

However, this technology is more general and less accurate and less resistant to external influences.

3.7 Identification by Voice

There are two types of systems that identify a speaker by voice: analysis of the pronunciation of a code phrase or phoneme and fluency analysis. Here, speech analysis is used in computers and mobile devices to authenticate users, often with any other modality-face images, teeth, etc. This is a significant relief. The main problem of voice identification is the technical vulnerability of the registration system for interference and noise caused by both the external environment and the features of the microphone structure. The decrease in recognition accuracy makes it impossible to use this approach in another biometric modality without insurance of the identification system. The considered approach has the potential to be used in the proctoring system in solving technical problems related to noise and voice recognition algorithms [34].

Electrocardiogram Identification Method

Over the past few years, one can observe a number of publications suggesting the use of ECG as a biometric measurement. Electrocardiogram: The stability of the signal structure allows it to be used in multimodal biometric identification systems of subjects and in some cases as a single-modal system. There are several ways to analyze the electrocardiogram graph:

- Analysis of unique representations
- Analysis of differences between P, QRS, and T-complexes and their temporal characteristics
- Analysis of the vector structure of the cardiogram and analysis of the biodynamic signature (BDS)

The main problems of electrocardiographic identification are the relatively high error rate (5% or more) and the vulnerability of identification to physiological changes occurring in the human body over time (circadian rhythms and the consequences of diseases that change some parameters of the heart rate of the load). Advantages of this approach are: It is impossible to deceive the system with artifacts, it is impossible to imagine the electrocardiogram signal, the individual uniqueness of the electrocardiogram does not depend on external conditions, and the training factor is also excluded.

To this approach, T. W. Shen, W. J. Tompkins, and Y. H. Hu conducted a study on the feasibility of using an electrocardiogram as a new biometric identification method. As a result of their research, it was proved that the use of an electrocardiogram is sufficient to identify a specific person from a certain group of candidates. The exception here, unlike fingerprint identification, is the one-dimensional approach, in which the electrocardiogram is not two dimensional but imposes high requirements on the algorithms used [35].

Despite considerable efforts aimed at the development of the electrocardiogram as a biometric modality, several important questions remain: factors related to changes in heart rate, changes in time, and the peculiarities of a person's life.

Currently, this type of identification is recognized as one of the promising approaches. After all, it has a number of advantages:

- Dynamic parameter analysis is carried out, which allows continuous monitoring and authentication.
- In priority of compactness and convenience of devices, a small one sensor-bracelet is required.
- Possibility of integration with the body condition monitoring system.
- The impossibility of hacking the system.
- The ability to control the psychophysiological state of a person, which allows taking into account the real reaction of a person in his behavior.

Identification by Features of Eye Movements

Another way to establish identity in the identification process is to track users' eye movements. To use the approach, an eye-tracker, a device, a remote student account, and the direction of the approach to the device are required. During the experimental study, Nguyen Viet Cuong, Vu Dinh, and Lam Sang achieved an identification accuracy of 93.56%. The ability to track the orientation of the student's gaze is the main advantage of this approach. However, since this approach requires additional accurate and expensive equipment in terms of identification, its use in the proctoring system is inefficient. The fact is that currently systems using conventional cameras are prone to image distortion and have low accuracy.

4 Conclusion

Static biometric approaches are more accurate than dynamic ones, but they are easier to break because it is much easier to create a static human parameter. Static identification methods are minimally in demand in mathematical registration devices. The parameters fixed in these approaches have been studied in more detail. However, the requirements of static approaches to the required equipment are high, for example, the use of high-quality optics.

Currently, there is a huge amount of research on dynamic identification approaches, which makes it possible to assume that in the near future their shortcomings will be eliminated. It can be noted that the accuracy of all methods increases significantly when the user uses an authentication system (confirmation of a certain person), rather than an identification system (search for matches in the database). Thus, the system has the task of determining the probability that a particular person does not meet its biometric standard. This approach, as well as the multimodality of the system, allows us to confirm the identity of the student with very high accuracy, having various opportunities for interaction and control during the exam without compromising his finances and convenience.

Of course, the choice of a biometric authentication method for an access control system depends primarily on the requirements for it. However, a comparison of biometric methods by a combination of factors clearly showed their general advantages. We can see it in the comparative analysis of biometric identification techniques used in autoproctoring, shown in Table 1.

Acknowledgement This publication is the result of the project implementation ERASMUS+ ACeSYRI: Advanced Center for PhD Students and Young Researchers in Informatics reg.no. 610166-EPP-1- 2019-1-SK-EPPKA2-CBHE-JP.

Table 1 Comparison of biometric methods by a combination of factors

The biometric access control and management system uses:	FAR, %	FRR, %	Falsification	Strong authentication (one factor)	Immutability of the characteristic	Sensitivity to the influence of external factors	Authentication speed	Contactless authentication while driving	User comfort	Cost
Fingerprint	0,001	0,6	Possible	Possible	Low	High	High	Unsuccessful	Average	Low
2DFace Recognition	0,1	2,5	Possible	No	Low	High	Average	At a great distance	High	Average
3DFace Recognition	0,0005	0,1	Problematic	No	High	Low	Low	In the middle distance	Average	High
The iris of the eye	0,00001	0,016	Unsuccessful	Possible	High	Average	High	At a great distance	High	High
Retina of the eye	0,0001	0,4	Impossible	Possible	Average	High	Low	Impossible	Low	High
Vein pattern	0,0008	0,01	Impossible	Possible	Average	Average	High	At a small distance	Average	Average

References

1. Dunn, T.P., Meine, M.F., McCarley, J.: The remoteproctor: an innovative technological solution for online course integrity. Int. J. Technol. Knowl. Soc. **6**, 1–7 (2010)
2. Dobrovinsky, D.S., Lovetsky, I.V., Popov, M.A.: Proctoring as a tool for the development of distance education. Scientific, technical and economic cooperation of the APR countries in the XXI century. **2**, 27–32 (2018)
3. Shaushenova, A., Zulpykhar, Z., Zhumasseitova, S., Ongarbayeva, M., et al.: The influence of the proctoring system on the results of online tests in the conditions of distance learning. Ad. Alta J. Interdiscip. Res. **11**, 250–256 (2021)
4. Socolinsky, D.A., Selinger, A., Neuheisel, J.D.: Face recognition with visible and thermal infrared imagery. Comput. Vis. Image Underst. **91**(1), 72–114 (2003)
5. Karim, M.N., Kaminsky, S.E., Behrend, T.S.: Cheating, reactions, and performance in remotely proctored testing: an exploratory expiremental study. J. Bus. Psychol. **29**, 555–572 (2014)
6. Khoroshilov, A.D.A., Musabaev, R.R., Kozlovskaya, Y.D., Nikinin, Y.A., Khoroshilov, A.A.: Automatic detection and classification of information events in media texts. Autom. Doc. Math. Linguist. **54**, 202–214 (2020)
7. Tomasi, L.F., Figiel, V.L., Widener, M.: I have got my virtual eye on you: remote proctors and academic integrity. Contemp. Issues Educ. Res. **2**, 31–35 (2009)
8. Impedovo, D., Pirlo, G.: Automatic signature verification: the state of the art. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **38**(5), 609–635 (2008)
9. Nilchiyan, M.R., Yusof, R.B.: Improved wavelet-based online signature verification scheme considering pen scenario information. 1st international conference on artificial intelligence, modelling and simulation (AIMS), IEEE Conference, pp. 8–13, 2013
10. Abzalov, A.R.: Authentication of users by keyboard handwriting when using automatic proctoring systems. Nat. Interest Prior. Secur. **3**(384), 582–596 (2020)
11. Tumbinskaya, M.V., Bayanov, B.I., Rakhimov, R.Z., et al.: Analysis and prediction of malicious network traffic in cloud services. Bus. Inform. **1**, 71–81 (2019)
12. Bryukhomitsky, Y.: A.: verification of dynamic biometric parameters of personality on the basis of a probabilistic neural network. Izvestia of the Southern Federal University. Tech. Sci. **5**, 52–58 (2020)
13. Poh, N., Korczak, J.: Hybrid biometric person authentication using face and voice features. In: Audio- and Video-Based Biometric Person Authentication, pp. 348–353. Springer, Berlin Heidelberg (2001)
14. Kim, D.J., Hong, K.S.: Multimodal biometric authentication using teeth image and voice in mobile environment. IEEE Trans. Consum. Electron. **54**(4), 1790–1797 (2008)
15. Chiu, C.C., Chuang, C.M., Hsu, C.Y.: A novel personal identity verification approach using a discrete wavelet transform of the ECG signal. International conference on multimedia and ubiquitous engineering (MUE 2008), IEEE, pp. 201–206, 2008
16. Ababkova, M.Y., Pokrovskaya, N.N.: Biometrics as a method of studying advertising incentives. Bull. Acad. Econ. Law. **10**(3), 242–250 (2020)
17. Fang, S.C., Chan, H.L.: Human identification by quantifying similarity and dissimilarity in electrocardiogram phase space. Pattern Recogn. **42**(9), 1824–1831 (2009)
18. Odinaka, I., et al.: ECG biometric recognition: a comparative analysis. IEEE Trans. Inf. Forensics Secur. **7**(6), 1812–1824 (2012)
19. Cuong, N.V., Dinh, V., Ho, L.S.T.: Mel-frequency cepstral coefficients for eye movement identification. 2012 IEEE 24 th international conference on tools with artificial intelligence (ICTAI), 1, pp. 253–260, 2012
20. Brothen, T., Peterson, G.: Online exam cheating: a natural experiment. Int. J. Instruct. Technol. Distance Learn. **9**(2), 15–20 (2012)
21. Varma, S., Shinde, M., Chavan, S.S.: Analysis of PCA and LDA features for facial expression recognition using SVM and HMM classifiers. Techno-Societal 2018. In: Proc. 2nd International

Conference on Advanced Technologies for Societal Applications, vol. 1, p. 109–119 (2020). https://doi.org/10.1007/978-3-030-16848-3_11

22. Yin, D.B.M., Mukhlas, A.A., Chik, R.Z.W., Othman, A.T., Omar, S.: A proposed approach for biometric-based authentication using of face and facial expression recognition. In: Proc. IEEE 3rd International Conference on Communication and Information Systems (ICCIS 2018), Singapore, p. 28–33 (2018). https://doi.org/10.1109/ICOMIS.2018.8644974
23. Dino, H.I., Abdulrazzaq, M.B.: Facial expression classification based on SVM, KNN and MLP classifiers. In: Proc. International Conference on Advanced Science and Engineering (ICOASE 2019), Zakho Duhok, Iraq, p. 70–75 (2019). https://doi.org/10.1109/ICOASE.2019.8723728
24. Tripathi, A., Pandey, S.: Efficient facial expression recognition system based on geometric features using neural network. Lect. Notes Netw. Syst. **10**, 181–190 (2018). https://doi.org/10.1007/978-981-10-3920-1_18
25. Greche, L., Es-Sbai, N., Lavendelis, E.: Histogram of oriented gradient and multi layer feed forward neural network for facial expression identification. In: Proc. International Conference on Control, Automation and Diagnosis (ICCAD 2017), Hammamet, Tunisia, p. 333–337 (2017). https://doi.org/10.1109/CADIAG.2017.8075680
26. Tselikova, S.O., Gorozhankin, Y.P., Ivanov, A.O., Mironov, A.A., Akhremchik, Y.V.: Neural network technologies in automatic recognition of emotions. Young Sci. **26**, 59–61. https://moluch.ru/archive/264/61173/ (2019). Accessed 12 Dec 2019 (in Russian)
27. Stepanova, O., Ivanovsky, L., Khryashchev, V.: Deep learning and convolutional neural networks for facial expression analysis. DSPA. **8**(4), 170–173 (2018) (in Russian)
28. Talegaonkar, I., Joshi, K., Valunj, S., Kohok, R., Kulkarni, A.: Real time facial expression recognition using deep learning. In: Proc. of International Conference on Communication and Information Processing (ICCIP) (2019). https://doi.org/10.2139/ssrn.3421486
29. Jumani, S.Z., Ali, F., Guriro, S., Kandhro, I.A., Khan, A., Zaidi, A.: Facial expression recognition with histogram of oriented gradients using CNN. Indian J. Sci. Technol. **12**(24), 1–8 (2019) https://doi.org/10.17485/ijst/2019/v12i24/145093
30. Babu, D.R., Shankar, R.S., Mahesh, G., Murthy, K.V.S.S.: Facial expression recognition using bezier curves with hausdorff distance. In: Proc. IEEE International Conference on IoT and Application (ICIOT 2017), Nagapattinam, India, 8073622 (2017). https://doi.org/10.1109/ICIOTA.2017.8073622
31. Cao, H., Cooper, D.G., Keutmann, M.K., Gur, R.C., Nenkova, A., Verma, R.: CREMA-D: crowd-sourced emotional multimodal actors dataset. IEEE Trans. Affect. Comput. **5**(4), 377–390 (2014). https://doi.org/10.1109/TAFFC.2014.2336244
32. Alexandrov, A.A., Kirpichnikov, A.P., Lyasheva, S.A., Shleymovich, M.P.: Analyzing the emotional states of a person in an image. Her. Technol. Univ. **22**(8), 120–123 (2019) (in Russian)
33. Voronov, V., Strelnikov, V., Voronova, L., Trunov, A., Vovik, A.: Faces 2D-recognition and identification using the HOG descriptors method. In: Proc. 24th Conference of Open Innovations Association FRUCT, pp. 783–789 (2019)
34. Addison, P.S.: The illustrated wavelet transform handbook: introductory theory and applications in science, engineering, medicine and finance. CRC Press (2017). https://doi.org/10.1201/9781315372556
35. Nigam, S., Singh, R., Misra, A.K.: Efficient facial expression recognition using histogram of oriented gradients in wavelet domain. Multimed. Tools Appl. **77**(21), 28725–28747 (2018). https://doi.org/10.1007/s11042-018-6040-3