ISNN 3030-3907

2026/3
VOLUME 8

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/3 VOLUME 8

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

ALGORITHM FOR DETECTING SPOOF ATTACKS IN BIOMETRIC DATA RECOGNITION SYSTEMS

Makhmudova Shakhzoda Yorkinovna
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Phd student
E-mail: shaha080599@gmail.com
Saydazimov Javlonbek
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Phd student
E-mail: javlonbek2020@gmail.com
Rajabov Kamoliddin Kayumovich
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi Phd student
E-mail: harrissoshka1234@gmail.com

Abstract. In this paper, an algorithm for detecting facial liveliness based on deep learning and image analysis methods is proposed. The algorithm includes the stages of face detection, image preprocessing, feature extraction using a convolutional neural network, and subsequent image classification into live and spoof classes. To evaluate the effectiveness of the developed method, experimental studies were conducted on a test dataset containing images of live faces and substitution attacks. The experimental results show high classification accuracy and confirm the effectiveness of the proposed approach to improve the security of biometric authentication systems. The developed algorithm can be used in access control systems, mobile authentication and other information security applications.

Keywords: biometric authentication, facial recognition, aliveness verification, spoof attacks, spoofing attack detection, convolutional neural networks, deep learning, computer vision, biometric security systems.

Аннотация. В этой статье предлагается алгоритм определения живости лица, основанный на методах глубокого обучения и анализа изображений. Алгоритм включает этапы распознавания лица, предварительной обработки изображения, выделения признаков с помощью сверточной нейронной сети и последующей классификации изображений на классы живых и поддельных. Чтобы оценить эффективность разработанного метода, были проведены экспериментальные исследования на тестовом наборе данных, содержащем изображения живых лиц и атаки подмены. Результаты экспериментов показывают высокую точность классификации и подтверждают эффективность предложенного подхода для повышения безопасности систем биометрической аутентификации. Разработанный

ISSN 3030-3907

алгоритм может быть использован в системах контроля доступа, мобильной аутентификации и других приложениях для обеспечения информационной безопасности.

Kalit so‘zlar: biometrik autentifikatsiya, yuzni aniqlash, tiriklikni tekshirish, soxta hujumlar, soxta hujumlarni aniqlash, konvolyutsion neyron tarmoqlari, chuqur o‘rganish, kompyuterni ko‘rish, biometrik xavfsizlik tizimlari.

Annotatsiya. Ushbu maqolada chuqur o‘qitish va tasvirni tahlil qilish usullariga asoslangan yuzning jonliligini aniqlash algoritmi taklif etiladi. Algoritm yuzni aniqlash, tasvirni oldindan qayta ishlash, konvolyutsion neyron tarmog‘i yordamida xususiyatlarni ajratib olish va tasvirni jonli va soxta sinflarga bo‘lish kabi bosqichlarni o‘z ichiga oladi. Ishlab chiqilgan usulning samaradorligini baholash uchun jonli yuzlar va almashtirish hujumlari tasvirlarini o‘z ichiga olgan test ma’lumotlar to‘plamida eksperimental tadqiqotlar o‘tkazildi. Tajriba natijalari yuqori tasniflash aniqligini ko‘rsatadi va biometrik autentifikatsiya tizimlarining xavfsizligini yaxshilash bo‘yicha taklif qilingan yondashuvning samaradorligini tasdiqlaydi. Ishlab chiqilgan algoritmdan kirishni boshqarish tizimlarida, mobil autentifikatsiya va boshqa axborot xavfsizligi ilovalarida foydalanish mumkin.

Ключевые слова: биометрическая аутентификация, распознавание лиц, проверка на живучесть, спуфинг-атаки, обнаружение спуфинг-атак, сверточные нейронные сети, глубокое обучение, компьютерное зрение, биометрические системы безопасности.

INTRODUCTION.

Biometric technologies have become widespread in various fields of information security in recent years. They are actively used in access control systems, mobile devices, banking services, government information systems and other applications where reliable identification of the user is required. Unlike traditional authentication methods based on passwords or identification cards, biometric systems use unique physiological and behavioral characteristics of a person, which significantly increases the level of security and ease of use.

One of the most common and convenient methods of biometric identification is face recognition. This method is widely used due to its contactless principle of operation, high data processing speed and the possibility of using standard cameras. Modern facial recognition algorithms based on machine learning methods and deep neural networks make it possible to achieve high identification accuracy even in difficult lighting conditions and at various angles of the face.

However, despite the high efficiency of such systems, vulnerability to spoofing attacks remains one of the major problems. As part of such attacks, an attacker tries to deceive the biometric authentication system using photographs,

ISSN 3030-3907

videos, masks, or other means of imitating the user's appearance. Such attacks can significantly reduce the reliability of the system and lead to unauthorized access.

To increase the resilience of biometric systems to such threats, liveness detection methods are used. The main task of aliveness verification algorithms is to determine whether the presented biometric image is real and belongs to a living person, or whether it is a fake object used to attack the system. Modern methods of detecting liveliness are based on the analysis of image texture characteristics, dynamic features of the face, as well as the use of deep learning methods.

The purpose of this work is to develop and study an algorithm for detecting substitution attacks in face recognition systems based on deep learning methods. The paper considers the architecture of the proposed algorithm, its mathematical model, software implementation, as well as the results of an experimental study of the effectiveness of the developed method in classifying images into classes "live face" (live) and "substitution" (spoof).

2. Analysis of existing methods

2.1 Biometric authentication

Biometric authentication is a method of identifying an individual based on a person's unique physiological or behavioral characteristics. Unlike traditional authentication methods such as passwords, PIN codes or identification cards, biometric systems use individual characteristics of a person that are difficult to fake or transfer to another person. This makes biometric technologies one of the most promising areas in the field of information security.

The most common biometric characteristics include fingerprints, iris, facial geometry, voice, as well as behavioral characteristics such as signature dynamics or keyboard typing features. Among these methods, face recognition occupies a special place, which has become widespread due to its convenience and the possibility of contactless use.

Modern facial recognition systems are based on computer vision and machine learning methods. They allow you to automatically detect a face in an image, extract the characteristic features and compare them with the data stored in the database. The use of deep learning methods and convolutional neural networks has significantly improved recognition accuracy and resilience to various lighting conditions, camera angles, and changes in user appearance.

The main advantages of facial recognition are ease of use, high data processing speed, and the ability to integrate into various security systems. Due to these characteristics, facial recognition technologies are widely used in access

ISSN 3030-3907

control systems, mobile devices, banking services, video surveillance systems, and government information systems.

2.2 Substitution attacks in facial recognition systems

Despite the high efficiency of modern facial recognition systems, they remain vulnerable to various types of spoofing attacks. The purpose of such attacks is to deceive the biometric authentication system using fake or simulated biometric data.

One of the most common types of attacks is the use of photographs. In this case, the attacker presents the system with an image of the user's face, printed on paper or displayed on the screen of an electronic device. In the absence of additional mechanisms for checking liveliness, the system may mistake such an image for a real face.

Another common type of attack is video attacks. In this case, the attacker plays a video recording of the user's face in front of the camera of the recognition system. Such attacks can be more effective because the video contains dynamic information, which makes it more difficult to detect spoofing.

Attacks using three-dimensional masks are also possible. In this case, the attacker uses a mask that mimics the user's face, which makes it possible to reproduce the three-dimensional structure of the face and significantly complicates the detection of substitution by traditional methods.

To increase the resilience of biometric systems to such attacks, special substitution detection algorithms are being developed to determine whether the presented biometric image is real or fake.

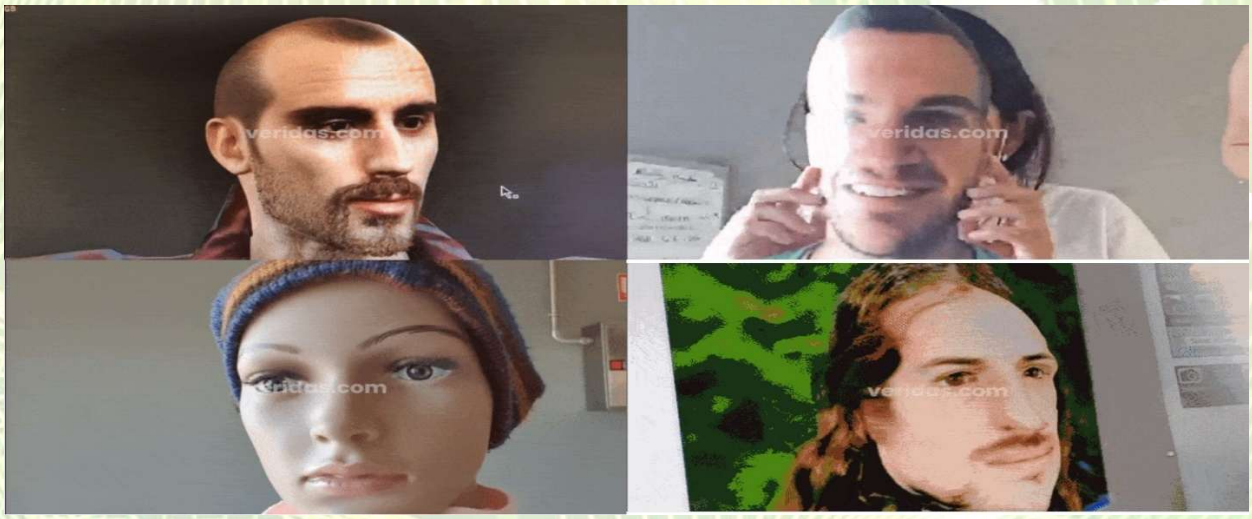


Figure 1 — The main types of substitution attacks in face recognition systems (photo, video and 3D mask).

2.3 Methods for detecting liveliness

ISSN 3030-3907

Liveness detection methods are used to enhance the security of biometric facial recognition systems. The main task of such methods is to determine whether the presented image belongs to a real person or is an attempt at a substitution attack. The existing methods of detecting liveliness can be roughly divided into several main categories.

The first category includes methods for analyzing the textural characteristics of an image (texture analysis). These methods are based on the analysis of the microtexture of the face image. Fake images obtained using photographs or device screens have distinctive textural features that differ from the texture of real skin. To identify such differences, various image analysis algorithms are used, including local binary templates (LBP) and other texture processing methods.

The second category includes motion analysis methods. These methods are based on the analysis of dynamic facial characteristics, such as eye blinking, head movement, or facial expression changes. The presence of natural facial movements may indicate that there is a real person in front of the camera, rather than a static image.

The third category of methods is based on the use of deep learning methods. These approaches use convolutional neural networks (CNNs), which are able to automatically extract informative features from images and effectively distinguish between real faces and substitution attacks. The use of deep neural networks can significantly improve the accuracy of detecting spoof attacks and is one of the most promising areas for the development of modern biometric systems.

3. The proposed algorithm for detecting facial liveliness

3.1 General system architecture

To increase the resilience of biometric authentication systems to spoofing attacks, this paper proposes an algorithm for detecting facial aliveness based on image analysis using deep learning methods. The proposed algorithm is designed to determine whether the presented image is a real face of the user (live) or an attempt at a substitution attack (spoof).

The algorithm includes several sequential stages of processing the input image. At the first stage, face detection is performed on the input image obtained from the device's camera. To do this, computer vision techniques are used to highlight the area of the face in the image.

At the second stage, image preprocessing is performed, including dimensional normalization, face alignment, and image conversion to a format suitable for neural network processing. Pre-processing makes it possible to increase the algorithm's resistance to various lighting conditions and face angles.

ISSN 3030-3907

At the third stage, feature extraction is performed using a convolutional neural network (CNN). The neural network automatically identifies the characteristic features of the image, allowing you to distinguish between real faces and fake images.

At the final stage, the image is classified into two classes: "live face" and "spoof attack". The classification result is used to make a decision about the user's authenticity.

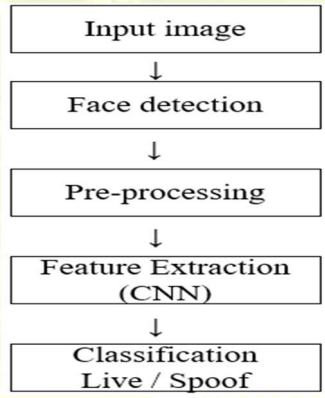


Figure 2. Architecture of the face liveliness detection algorithm

3.2 Mathematical model of the algorithm

Consider the input image of a face as a two-dimensional function of brightness:

$$I(x,y)$$

where x and y are the coordinates of the pixels in the image.

After preprocessing, the image is fed to the input of a convolutional neural network that performs feature extraction. The result of the neural network is a feature vector:

$$F=CNN(I)$$

where F is the feature vector obtained after image processing by the neural network.

To classify an image, the softmax function is used, which calculates the probability of an image belonging to one of the classes:

$$P(y|F)=Softmax(WF+b)$$

where

W is the weight matrix of the classifier,

b is the bias vector,

y is the image class (live or spoof).

The model is trained using the cross-entropy loss function:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

ISSN 3030-3907

where

N is the number of training examples,

y_i is the true class label,

$\hat{y}_i$ is the predicted probability of the class.

Minimizing the loss function allows you to optimize the parameters of the neural network and improve the accuracy of image classification.

4. Software implementation of the algorithm

The developed algorithm for detecting facial liveliness was implemented using modern image processing tools and deep learning methods. Python was used as the programming language, due to its wide capabilities and the availability of specialized libraries for computer vision and machine learning.

The following libraries were used to implement the individual steps of the algorithm: OpenCV for image processing and face detection, and PyTorch (or TensorFlow) for building and training a convolutional neural network. The use of these tools has made it possible to ensure high efficiency and flexibility of the system being developed.

The software implementation of the algorithm includes several successive stages. At the first stage, an image is obtained from the camera or an image is downloaded from the database. Next, the face is detected using standard computer vision techniques, after which the selected area of the face is reduced to a fixed size and normalized.

At the next stage, the preprocessed image is fed to the input of a convolutional neural network trained on the task of classifying images into classes "live face" and "substitution attack". The neural network extracts the informative features of the image and generates a feature vector, which is then used by the classifier to determine whether the image belongs to one of the classes.

The result of the algorithm is a binary solution: the image belongs to the "live" or "spoof" class. The result obtained can be used in access control systems to make a decision on granting or denying access to the user.

ISSN 3030-3907

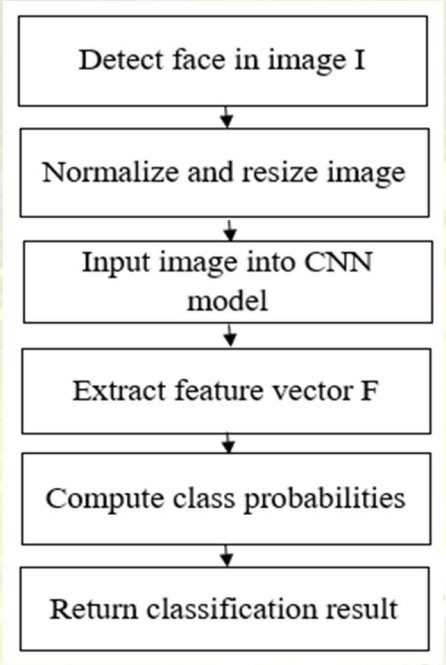


Figure 3. Algorithm Liveness Detection Input: Image I Output: Live or Spoof

5. Experimental results

To evaluate the effectiveness of the proposed algorithm for detecting facial liveliness, experimental studies were conducted on a test dataset. The dataset included images of two classes: real faces (live) and spoofing attacks (spoof).

The total volume of the test sample was 200 images, of which 100 images belong to the "live face" class and 100 images belong to the "substitution attack" class. The experiments were conducted to evaluate the classification accuracy and the algorithm's resistance to various types of attacks.

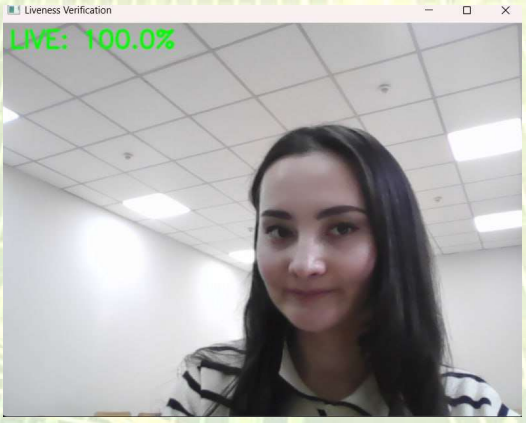


Figure 4 — Live face detection



Figure 5 — Spoof attack detection

CONCLUSION.

In this paper, an algorithm for detecting spoofing attacks in biometric authentication systems was developed. The proposed method is based on the use of convolutional neural networks to analyze facial images and determine signs of liveliness. Experimental results have shown high accuracy in classifying images

ISSN 3030-3907

into live and spoof classes. The developed algorithm can be used in access control systems and mobile applications. In the future, it is planned to expand the data set and increase the algorithm's resistance to various types of attacks.

REFERENCES

1. Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embedding for face recognition and clustering // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2015. URL: https://arxiv.org/abs/1503.03832
2. Wang H. et al. CosFace: Large margin cosine loss for deep face recognition. URL: https://arxiv.org/abs/1801.09414
3. Deng J. et al. ArcFace: Additive angular margin loss for deep face recognition. URL: https://arxiv.org/abs/1801.07698
4. InsightFace Project. URL: https://github.com/deepinsight/insightface
5. Zhang Z. et al. CASIA Face Anti-Spoofing Database // 2012 International Conference on Computer Human Interaction. DOI: 10.1109/CHCI.2012.6518181
8. Wen D., Han H., Jain A. Face Spoof Detection with Image Distortion Analysis // IEEE TIP. 2015.
9. A. Ross, K. Nandakumar and A. K. Jain, Handbook of Multibiometrics (Springer-Verlag, 2006).
10. V. K. N. Kumar, ”Performance of Personal Identification System Technique Using Iris Biometrics Technology”, International Journal on Image, Graphics and Signal Processing, vol. 5, no. 5, pp. 63-71, Apr. 2013.
11. A. Chikhaoui, B. Djebbar, and R. Mekki, ”New Method for Finding an Optimal Solution to Quadratic Programming Problem”, Journal of Applied Sciences, vol.
12. Y. Yin, L. Liu, and X. Sun, ”SDUMLA-HMT: A Multimodal Biometric Database”, In Chinese Conference on Biometric Recognition (CCBR 2011), Springer Berlin Heidelberg, pp. 260–268, Dec. 2011.
13. N. Wang, L. Lu, G. Gao, F. Wang, and S. Li, ”Multibiometrics Fusion Using Aczél-Alsina Triangular Norm”, KSII Transactions on Internet and Information Systems(TIIS), vol. 8, no. 7, pp. 2420-2433, Jul. 2014

ISSN 3030-3907