I.J. Modern Education and Computer Science, **2025, 3, 59-71**
Published Online on June 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2025.03.05

Information Security of Educational Portal Based on Face Anti-Spoofing Method: Effectiveness of Tiny Neural Network Machine Learning Model

Meruert Serik
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: serik_meruerts@mail.ru
ORCID iD: https://orcid.org/0000-0002-2801-432X

Danara Tleumagambetova*
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: danara1310@gmail.com
ORCID iD: https://orcid.org/0009-0007-4221-3900
*Corresponding Author

Alaminov Muratbay
Nukus State Pedagogical Institute, Nukus, Uzbekistan
E-mail: alaminov1962@gmail.com
ORCID iD: https://orcid.org/0009-0003-2946-7990

Received: 31 December, 2023; Revised: 14 February, 2024; Accepted: 16 March, 2025; Published: 08 June, 2025

Abstract: This article presents the implementation of a machine learning-based face anti-spoofing method to enhance the security of an educational information portal for university students. The study addresses the challenge of preventing academic dishonesty by ensuring that only authorized individuals can complete intermediate and final assessment tasks. The proposed method leverages the Tiny neural network model, selected for its efficiency in compact data processing, alongside the dlib system in Python and the LCC_FASD dataset, which enables precise detection of 68 facial landmarks. Using a confusion matrix to evaluate performance, the method achieved a 94.47% accuracy in detecting spoofing attempts. These findings demonstrate the effectiveness of the proposed approach in safeguarding educational platforms and maintaining academic integrity.

Index Terms: Information Security, Educational Portal, Machine Learning, Face Anti-Spoofing, Neural Network, Deep Learning

1. Introduction

Today, due to the transition of socio-economic sectors to digital transformation, "information" has become one of the most valuable assets. Cyber-attacks on the corporate network of various industries harm the operation of hardware and software, lead to the theft of important information, and disruption of the work process, resulting in reputational and financial losses.

Higher educational institutions are also comprehensively considering introducing the mechanisms of modern technological trends into the education system due to public demands. For this purpose, the creation of unified platforms for the optimization of the educational process, comprehensive use of digital transformation achievements, including data management, decision-making and forecasting capabilities based on artificial intelligence and machine learning, availability of proactive and predictive services to students, smart university system and cybersecurity issues are the main directions. At the same time, the information education portal developed based on the Faculty of Information Technologies of the Eurasian National University named after L.N. Gumilyov is a digital ecosystem based on strengthening the domestic innovative system and optimally and safely managing the educational process of students who are competitive in the international market, based on machine learning.

In our study, the aim was to improve the ways of biometrically implementing the protection of the educational information portal from cyberattacks and to determine the effectiveness of the anti-spoofing method as a result of the refinement of neural network models in machine learning.

Among cybercrimes, spoofing is one of the most modern malicious attacks that cause damage to network security. Many protocols in TCP/IP are vulnerable to spoofing if additional steps are not taken to identify message senders and recipients, as they do not provide authentication mechanisms. This requires in-depth analysis of data packets and user personal information using modern technologies such as machine learning. This type of attack provides unauthorized access to a system through the use of a user's image or video, leading to moral and material consequences. Therefore, for all sectors of society in the digitalization era, protection against this type of attack is crucial.

To prevent this attack, we can comprehensively study the methods and characteristics of presenting a false image of a legal person to ensure the security of facial biometrics and organize the reliable and secure operation of the system, using an anti-spoofing method based on machine learning in our research. The implementation of our research consisted of the following stages:

- Conduct a comparative analysis of the detector used in the face recognition system based on neural networks in machine learning.
- Implement steps to create and optimize a facial recognition system for user authentication on the educational information portal.
- Study the anti-spoofing system for face recognition to ensure the security of the facial recognition system, create a database for implementing the anti-spoofing system, and analyze the accumulated data.
- Train and analyze the results using machine learning algorithms and the Python language through video analysis.
- Calculate the accuracy of the security of the educational information portal.

1.1 Research hypothesis:

The implementation of a biometric face anti-spoofing system based on the Tiny Neural Network machine learning model in the educational information portal is expected to enhance the reliability and speed of user authentication. By leveraging the model's compact and efficient data processing capabilities, the system will enable electronic analytical devices to accurately detect and authenticate individuals within one to two seconds. This improvement in authentication speed and accuracy will contribute to a higher level of academic integrity among student users, as it will prevent unauthorized individuals from completing assessments on behalf of others. Additionally, the system will strengthen data protection on the server by minimizing identification errors and reducing vulnerabilities to malicious actors. The success of this method will be measured through metrics such as authentication accuracy (using a confusion matrix), processing speed, and the system's ability to detect spoofing attempts, with the goal of achieving a high detection rate (94%) while maintaining user convenience. The inherent advantages of biometric data, such as the impossibility of loss or forgetfulness, further support the system's practicality and effectiveness in securing the educational portal.

2. Literature Review

The Face anti-spoofing method is of great importance in ensuring the security of presentation attack detection systems. New innovative solutions are emerging based on the implementation of this type of machine learning-based information security.

Researchers consider various theoretical and practical issues related to information security and anti-spoofing, such as [1,4]:

- Detection of attacks in face recognition systems in the educational environment;
- Protection of DNS servers from attacks through multi-level defense;
- Utilizing anti-spoofing in detecting presentation attacks;
- Face anti-spoofing based on Deep Supervision;
- Methods and techniques for protection against spoofing.

For instance, many research works have considered anti-spoofing methods as a means of protection against fake surfaces on smartphones. To comprehend it, understanding the theoretical foundations of presentation attacks is paramount.

In research studies, approaches based on video sequence analysis are frequently used to counteract spoofing attacks. These approaches aim to detect natural facial changes, such as eye blinking, mouth movements, and head rotations. Specifically, the detection of eye blinking is determined based on a disoriented conditional graphical structure and the utilization of a video stream focused on the mouth region [5, 6]. Blink velocity vectors can be represented as an intuitive model, while statistical analysis of blink frequency and duration allows for assessing the naturalness of eye movements. As part of the study of methods for detecting fake videos, a work was examined that focuses on algorithms for automatic forgery detection based on blink analysis [7]. There, experimental work was carried out based on vocabulary, machine learning, and a hybrid approach.

In the following study, the correlation between the user's head movement and the background is proposed as a means of protecting against spoofing attacks. Although the anti-spoofing method is conceptually simple, it requires a sufficient number of frames to track page components. This necessitates increased detection time, additional user actions, and potentially increased communication channel load in the case of a remote API server [8]. In preventing spoofing attacks, a specific algorithm in the form of diffusion velocity mapping can also be applied to images obtained through adaptive non-linear filtering using specialized filters [9].

In addition, to fully master the methods of anti-spoofing in the face recognition system, the research work "A Survey on Anti-Spoofing Methods for Facial Recognition" by Raghavendra R was considered. The author considered Liveness cues (including Motion, rPPG), Texture cues (Static texture, Dynamic texture), 3D Geometric cues (3D shape, Pseudo depth map), Multiple cues, CNN based methods of detecting attacks. Considering the advantages and disadvantages of each method, the CNN method is recommended because it can analyze thirteen types of attacks, including impersonation and confusion [10].

Based on the analysis of existing research in this field, it is evident that the future development of face anti-spoofing methods will be centered around machine learning techniques.

3. Proposed Methodology

The integration of digitization into the educational process at the university is directly related to the successful implementation of informational educational portals. The advancement of this direction has become possible thanks to the integration of new directions in information technology, such as machine learning, artificial intelligence, big data, and web platforms. The informational educational portal presented by us is developed based on the L.N. Gumilyov Eurasian National University and includes three levels of education in higher education: bachelor's, master's, and doctoral programs, namely specialties “6B01511-Informatics”, “7M01511-Informatics”, “7M01525-STEM Education”, “8D01511-Informatics” intended to optimize the educational process. In the future, it is planned to cover future computer science teachers throughout the Republic of Kazakhstan.

The systematic organization of the security of the educational portal is a guarantee of its viability. In this study, we discuss the process of practical implementation of the face anti-spoofing biometric method based on machine learning, integrated into the informational educational portal. Biometric face recognition technology is the key to security. Finding a photograph or image of any person on a social network and using it for criminal purposes leads to serious problems. The development of a biometric registration system for the educational portal is a crucial measure in protecting it from malicious attacks, ensuring the security and confidentiality of the personal data of students and teachers, as well as guaranteeing the integrity and destruction of important data on the server. Two approaches were utilized for authentication in this system. Figure 1 shows the model of an information and educational portal.

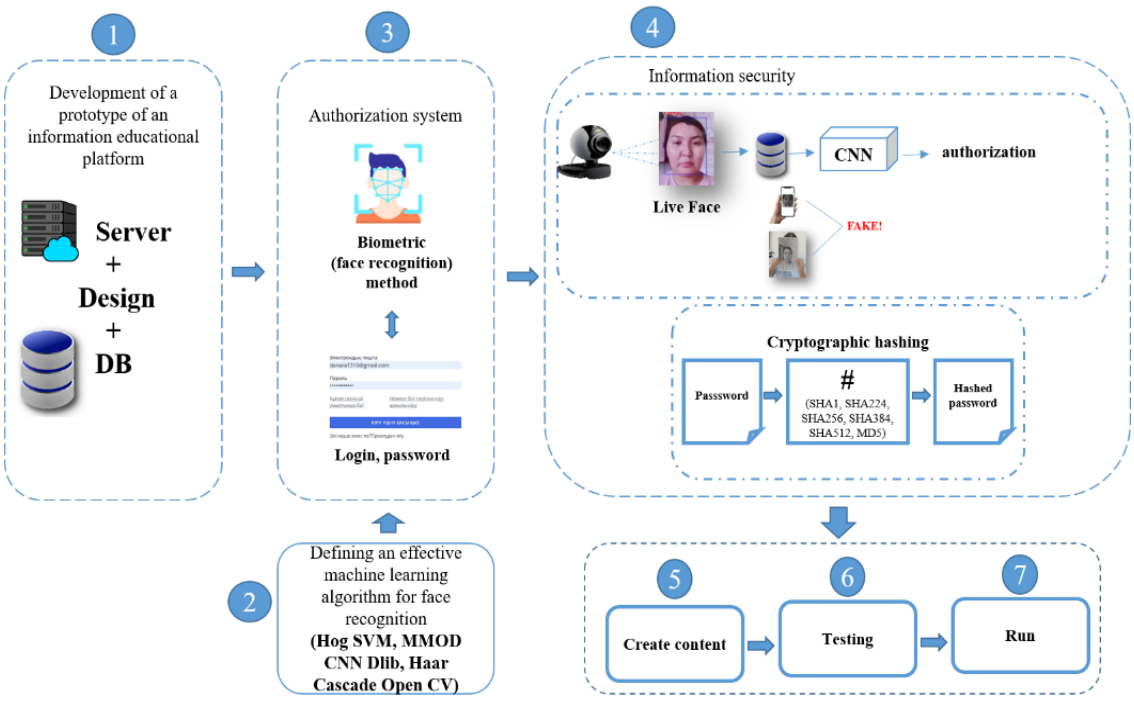

Fig. 1. The model of the informational education portal and the location of the biometric face anti-spoofing system in it.

The authors followed 7 basic steps to develop an informational education portal. First of all, a server (fornet.com), CyberPanel was selected, and an information and education portal was developed. To determine an effective face recognition algorithm (Hog SVM, MMOD, CNN, Dlib, Haar Cascade Open CV) real-time research was conducted. The first approach involves registration using daily login credentials and passwords, while the second approach utilizes authorization through a biometric facial recognition system. Cryptographic hashing was employed for securing login credentials and passwords, while a neural network-based anti-spoofing method was used in the biometric facial recognition system. One of the primary objectives of implementing the biometric facial recognition system on the educational portal is to prevent the presence of unauthorized individuals during the intermediate and final assessments through integration with proctoring systems, thus strictly adhering to academic integrity guidelines. As a result, an authorization system for the information educational portal has been developed (security.org.kz), as shown in Figure 2. Consequently, it was tested and implemented by registering students to the system.

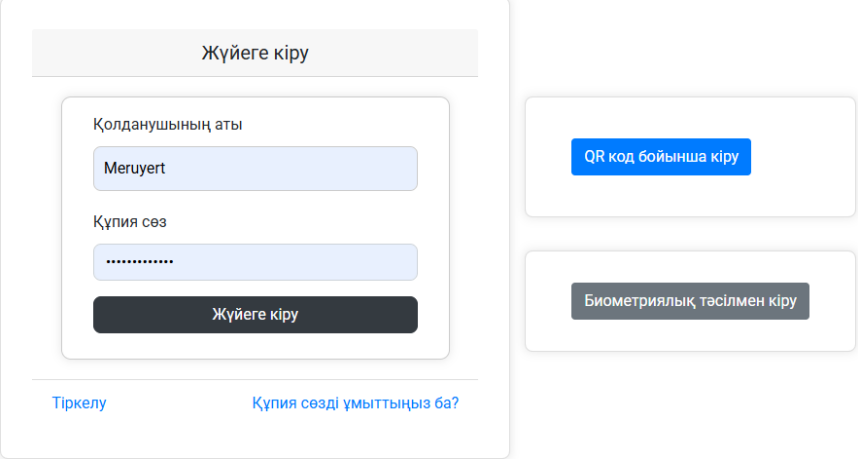

Fig. 2. The authorization page of the Information Education Portal.

Similar to this model, Z. Yu's “Deep Learning for Face Anti-Spoofing: A Survey” provides a model for using anti-spoofing methods in the development of a face recognition system. According to the authors' concept, attacks on the automatic face recognition system are divided into digital manipulation and physical representation attacks. Digital manipulations here include changing human facial features, and the other is presenting a human face image using physical media. In this article, the type of attack on the face recognition system through physical carriers of real face recognition is considered. Proposed two ways to detect attacks on the face recognition system using physical carriers: by comparing the data available in the system with the data detected during face recognition and by recognizing a fake face using face features immediately in the face recognition system. In addition, with the help of tools such as photography, electronic screens, and 3D masks, the full attack and the types of false attacks that change only facial features have been shown as a result of experiments [11].

So, P. Anthony's “A Review of Face Anti-spoofing Methods for Face Recognition Systems” presents the anti-spoofing model of the face recognition system by Anand and Gupta. The authors developed a face fake detection method using a hybrid algorithm combining SIFT(Scale-Invariant Feature Transform), genetic algorithm, and artificial neural network. Here, the SIFT descriptor was used to extract the key points and identify the facial region pattern. The genetic algorithm was then used as a feature optimization method to extract unique features and obtain normalized feature sets for each category of image data. Although the developed system showed 97.86% accuracy, errors were detected when identifying real persons [12].

As a result of comparing the two considered models with our proposed model, we can draw the following conclusions. Compared to previous researchers' works, our proposed model is used against image manipulation of users registering on the educational portal and determines whether real people are fake or true. The anti-spoofing method based on machine learning proved effective in generating compact datasets using a lightweight neural network model. The Python-based dlib system was employed to quickly and accurately detect 68 facial landmarks, enabling the research model to identify spoofing attacks carried out using physical mediums. Future enhancements aim to expand the system's capabilities to detect digitally manipulated fake faces, further improving its ability to counter advanced spoofing techniques.

3.1 Comparative analysis of the detector used in a neural network-based facial recognition system

At the initial stage of the research task, a comparative analysis of the performance and detector of the facial recognition system based on a neural network in machine learning for users of an educational information portal was conducted.

The facial recognition system consists of a facial recognition (facial landmark detection) block, a face preprocessing (alignment) block (cropping, scaling, transforming to a specified shape), a face feature extraction module (embedding vector), and classifiers [13].

The facial recognition method, based on deep learning through a neural network, is inclusive in feature selection and adapted to lighting conditions and rapid facial feature changes. The process of facial recognition can be implemented using the rich Python software library. In the first stage, images are loaded as NumPy arrays using the PIL library and the open () function. If the image has an alpha channel or is grayscale, its conversion to RGB is taken into account. Once the images (photos) are converted to arrays, we create the MTCN face detector class to detect all the facial landmarks. As a result, bounding boxes are created to determine the distance between facial features. These annotations are used for face classification. Surfaces can be aligned based on reference points. The aligned face is the output of MTCN and is passed to FaceNet as input. The FaceNet model determines the shortest L2 distance between facial features, transforming the 160x160x3 face image into a 128-length face input vector. In the process of facial recognition, the convolutional neural network model uses the triplet loss function, which assigns a lower value to similar images and a higher value to dissimilar images [14].

Investments on different surfaces here are referred to as positive, while investments on different surfaces are referred to as negative. The analyzed entity is called an anchor. To calculate costs, a triplet is formed, consisting of the anchor, positive, and negative embedding's, and their Euclidean distances are analyzed. The goal of the face recognition system is to reduce the distance between the anchor and the positive and maximize the distance between the anchor and the negative. Therefore, during the training of FaceNet, random vectors are created for each image and randomly chosen as positive anchors. However, the negative embedding perceives the image of another person. The FaceNet network parameters are adjusted by the system to ensure that the positive example is close to the anchor. As a result, it is observed that if the L2 distance in the embedding space is short, the face of the person is recognized, and if it is large, the face of another person is identified.

The next steps in creating a face recognition system are performed using a neural network or deep learning-based detectors. In our case, to analyze the performance of detectors, CNN Haar Cascade (OpenCV), HOG SVM, and MMOD Dlib were tested using a Python script for real-time face detection from a database of recorded images. The images shown in Figure 3 were obtained as a result of practical work.

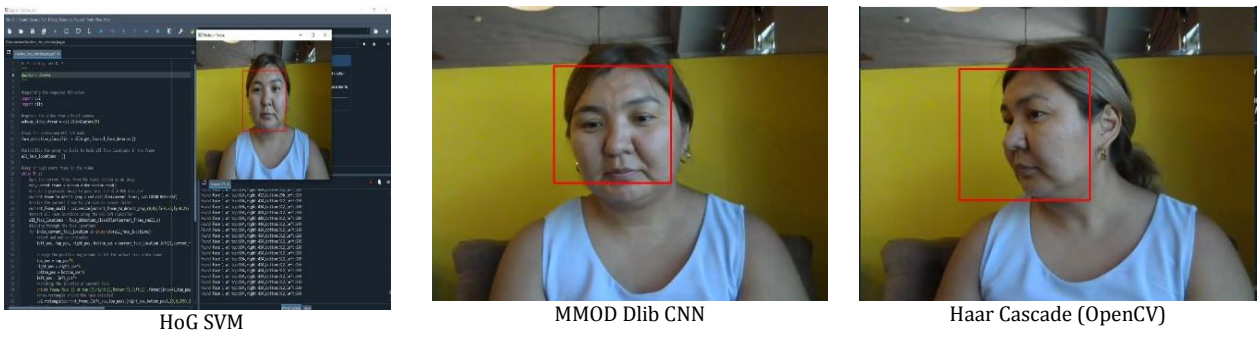

Fig. 3. A real-time face detection (HoG SVM, MMOD Dlib CNN, Haar Cascade (OpenCV)).

The HoG SVM detector operates very effectively in this context but encounters certain challenges in recognizing small-sized surfaces. The MMod Dlib CNN typically emerges as the most accurate algorithm, yet its inability to function without graphical processing acceleration can be considered a minor drawback. Conversely, the Haar OpenCV library efficiently resolves surface identification issues during experiments at high speeds; however, it often generates numerous errors. Furthermore, the DLL library contains functions and classes that cannot be implemented within the OpenCV library, specifically neural networks used for locating specific points on a human surface. During the comparative analysis of detector performance, the following advantages and disadvantages of the detectors were identified (Table 1).

Table 1. Comparative analysis of HoG SVM, MMOD CNN Dlib and Haar OpenCV

Algorithms	Advantages	Disadvantages
HoG SVM	Speed of use, the application is mainly used for objects;	The minimum surface size should be 80*80 pixels, the edge is not intended for side surfaces or exceeding the limits of non-frontal surfaces
MMOD Dlib CNN	Highly accuracy in detecting human faces in images, small model size	GPU cannot operate in real-time without acceleration
Haar OpenCV	High computational power, facial expression accuracy, rapid recognition	The accuracy level is still not high, there is a significant percentage of errors in facial recognition

Hence, for the biometric system's facial recognition and identification, the CNN MMOD dlib detector has been chosen.

3.2 Creating a Facial Recognition System for User Authentication on an Educational Information Portal

While the first stage of our research was dedicated to determining the methods used in the experiment, the subsequent stages involved experimental work on implementing information security.

During the second stage, a facial recognition system was created, and steps were taken to enhance information security.

At the initial stage of implementing the biometric authentication system on the educational information portal, certain issues arose, such as the appearance and slow functioning of facial recognition rectangles in incorrect locations during testing, and the "inability to convert the input image to a NumPy array" during the alignment phase. During the experiment, after checking the documentation of the NumPy module, it was found that the function of converting the image to a NumPy array requires image streams. With the help of the Numpy library, we can store the image (photograph) in the system as an array. Using the Numpy function for image processing from the beginning is efficient as the images are treated as array components. The possibilities of full implementation of the facial recognition system were examined during the initial test work (Table 2).

Table 2. Unit test

№	Aim	Implementation	Expected results	Test 1	Test 2
1	Face recognition	Person image	A rectangle is drawn	Done	incorrect location
2	Face recognition	The person's image was not identified	A rectangle is drawn	failed	done
3	Alignment	Reduced	Customized rectangle	failed	done
4	Face recognition	Sequence not detected	Zero	failed	done
5	Result	Entering the system	Entering the system	done	done

During the biometric authentication process, the possibility of program recognition of users from a photo was identified (Fig. 4). This means that there is a probability that unauthorized individuals can access the system using a photo or video. In Figure 4, various methods for detecting anti-spoofing during authorization on the educational information portal (security.org.kz) are shown.

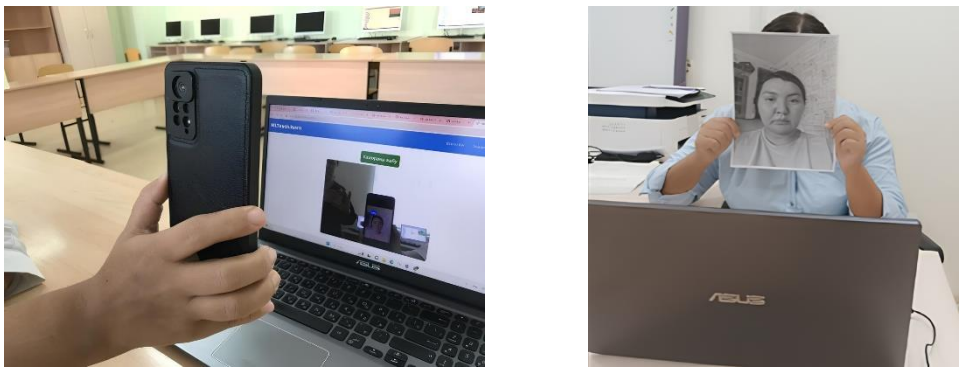

Fig. 4. A view of ways to authorize the system using a photo.

It is known that a facial recognition system is fully realized only if it operates in conjunction with additional security measures. For this reason, the system was constantly being enhanced using the face anti-spoofing method, based on machine learning.

3.3 Implementation of a face anti-spoofing system based on machine learning, creation of a video database

It is known that face anti-spoofing consists of traditional methods based on motion-based, texture-based, image quality analysis, and other signals. For example, motion-based methods are based on the movement of facial expressions (eyes, mouth), and texture-based methods consist of algorithms such as Local Binary Pattern (LBP). In the LBP method, the image is divided into several sectors so that the objects can be obtained. These objects consist of binary templates of pixels. Objects separated by sectors are combined in the form of a histogram and compared with the current image (for example, the distance between eyes). According to the results of research in the field of machine learning, Local Binary Pattern (LBP) has many advantages over other algorithms in terms of face recognition efficiency, speed, face rotation, and lighting conditions [15]. However, the LBP algorithm is inefficient when dealing with big data because:

- slows down the face recognition process as a result of creating very long histograms in big data;
- binary data generated during the face recognition process is sensitive to noise;
-its structure changes because the influence of the central pixel is not taken into account.

In our research work, this method was found to be inefficient due to the large amount of data used in the process of face recognition of users who register on the informational education portal.

Therefore, in addition to traditional methods, neural (convolutional) networks such as CNN are often used in the protection against spoofing. CNN algorithm uses a predefined classifier called a Support Vector Machine (SVM). The CNN algorithm automatically extracts features more than traditional algorithms, and also has high accuracy in image recognition and classification, and can process big data.

In the third stage of the research, to ensure the security of the facial recognition system, a study of the face anti-spoofing system based on machine learning was conducted, a database for its implementation was created, and the collected data were analyzed.

Attacks on the facial recognition system are called presentation attacks and have two categories: statistical 2D (image, photo), 3D (3D print, sculpture, mask), and dynamic 2D (displaying multiple images on the screen as a video), 3D (robots displaying faces) [16]. Currently, the widespread type of attack is 2D spoofing.

In this study, the anti-spoofing method primarily focused on addressing 2D presentation attacks, such as those involving printed photos and screen replays. However, spoofing techniques using physical carriers like masks or 3D models, which represent more sophisticated threats, were not fully explored. These types of attacks are particularly challenging due to their ability to mimic the depth and texture of real facial features [17]. In future work, the system will be extended to detect such threats by incorporating 3D face mapping and depth analysis. This enhancement will enable the biometric face recognition system to identify and mitigate the risks associated with advanced physical carrier spoofing attempts, thereby strengthening its security measures.

To address this issue, steps were taken to prevent spoofing attacks to enhance the security of the biometric authentication system on the educational information portal. This was achieved using the methods described below (Fig. 5). The data taken from the camera was transmitted to the preprocessing stage of the data in the facial recognition system to speed up the detection process and reduce the number of false positives. After the data is pre-processed, the main parts of the face (eyes, mouth) are determined. As a next step, during face recognition, the face images are compared with the template stored in the database. This level is carried out by the process of comparing and matching images with each other. If the match is found, you will be logged into the system, otherwise, information will be provided about the fake. Figure 5 presents the face recognition process for authorization and unlocking systems.

Fig. 5. A face recognition system with a spoofing detection module.

During the training process in the course of the experiment, we examined two types of attacks: photo and video. If the user's face does not match the model in the database, the system immediately blocks the action. To implement the face anti-spoofing system, a database of black and white photographs was developed. Figure 6 show images for data analysis within the framework of anti-spoofing tests aimed at detecting fraudulent face authentication attempts.

Fig. 6. Photo Database.

The dataset collected approximately 300-350 photographs per user. To improve the quality and reliability of the data, preprocessing steps were conducted, including image resizing, color normalization, and noise reduction to ensure consistency across samples. Images with poor lighting, blurriness, or significant occlusions were filtered out to maintain data integrity. Data augmentation techniques, such as flipping and brightness adjustments, were also applied to increase variability and improve model generalization. Subsequently, further work was carried out to prevent organized attacks during the system's authentication process. The data was normalized and classified into training and testing categories. The testing data was evaluated to determine system accuracy.

3.4 Training using machine learning algorithms and Python language on video

After preparing the dataset, the system extracts relevant features from images or video frames. These features demonstrate unique facial characteristics such as texture, color, shape, and motion. Once the data is gathered, we will proceed with the process of training the data using machine learning commands. 80% of the data is trained using machine learning, meanwhile, data validation is performed with the rest of the data to verify the correctness of any result.

When the labels are obtained, the system begins to classify samples as "genuine" or "spoof". During the data classification process, image quality analysis, texture analysis, motion analysis, and multimodal analysis (such as the integration of multiple sources of information such as depth data in 3D cameras or infrared images) are implemented [18].

In the fourth stage, after creating a database for accurate determination of real and spoof videos during facial recognition, machine learning algorithms for video and anti-spoofing algorithms for facial recognition systems are implemented using the Python language.

In the case of successful implementation of the algorithm, we can gain access to the content of the educational information portal. In case of failure to comply, the system automatically blocks the user.

4. Results

After the completion of a series of tasks mentioned above, we conduct testing to verify the security of the educational information portal's authentication system.

4.1 Result of effective Neural Network model determination

For the face anti-spoofing method based on machine learning, a highly precise neural network model, SSD MobileNet V1, was utilized. However, the image created based on this model amounted to approximately 5.4 MB. Thus, if around 300 photographs are taken for each individual for the facial recognition system to function effectively, then 300*5.4 MB=1.6 GB, and if the system involves 400-500 individuals, it will disrupt the operation. Therefore, facial recognition models were considered. A facial recognition model with a smaller volume and faster operation was examined to avoid hindering the educational information portal. Hence, SSD MobileNet V1 was replaced with the Tiny model. The capture volume of a single photo by the Tiny model is approximately 29 times smaller than the SSD MobileNet V1 model, and it is faster (Table 3).

Table 3. Comparison of neural network models for the Face Anti-Spoofing Method

Neural network models	The size of the quantized model	Time
SSD MobileNet V1	5.4 Mb	0.38 sec
Tiny model	190 Kb	0.24 sec

In addition to machine learning models, comparisons with traditional non-machine learning anti-spoofing techniques, such as motion analysis and texture-based approaches, were considered. These conventional methods, while effective in simple scenarios, often fell short in dynamic or large-scale educational environments, underscoring the advantages of the machine learning approach.

In the facial recognition system, only the statistical 2D category of presentation attack was considered.

During the research work, the Python library dlib was utilized, providing facial recognition and programming functions. Dlib can rapidly and objectively determine 68 points on the surface (Fig. 6). Dlib includes pre-trained models.

Additionally, a model for identifying human eye movement is employed. To determine the authenticity/falsity of the human eye in the facial recognition system on the educational platform, three photographs are taken in succession. In Figure 7, a person is depicted with contours overlaid on the face, highlighting key facial features, which can then be used for identification or facial expression analysis.

Fig. 7. Combining 68 points of facial features, inputting a 128-D value into the image.

The pre-processed facial expression created a 28-dimensional representation for sending data into the system. Based on this, the computer evaluates the image.

The system compares the data with 128-dimensional measurements in the database, generating this data. We used the LCC_FASD dataset to implement the Face Anti-Spoofing method. The dataset was selected for its comprehensive coverage of various face spoofing scenarios, making it a suitable choice for training and evaluating the face anti-spoofing model. This dataset includes images and videos featuring different types of spoofing attacks, such as printed photos, screen replays, and physical masks, captured under diverse lighting conditions. The dataset's structured design allows for effective categorization into training and testing sets, ensuring balanced representation of genuine and spoofed faces. Its extensive annotations and variety of attack types made it an ideal foundation for this research, enabling the model to generalize better and achieve higher detection accuracy in real-world applications [19].

These videos are pre-processed to remove unnecessary data and noise. The processed data is then classified as trained or test data. The classification of data into genuine/spoof was carried out using the Tiny model. Therefore, if the final data for the real-time modules are correct, the CNN classifier data is also correct. If any of the above-mentioned modules yield a negative result, then the image (photo) is considered a spoof.

4.2 Calculating the security accuracy of the educational information portal

To determine the effectiveness of the approaches investigated in the research work, 579 individuals participated. The data was calculated using the Confusion Matrix [20]. Before evaluating the research approach's effectiveness, all individuals who participated in the research were registered within the system (Table 4). The dataset was split into training and testing categories, with 70% of the data used for training and 30% for testing. Cross-validation was performed to ensure model generalization and avoid overfitting, where the dataset was divided into five folds, and the model was trained and validated on different data segments across iterations.

Table 4. Information about users' registration in the system

Individual Number	1	2	3	4	5	6	7	...	579
Actual Classification	1	0	1	0	1	1	0	1	1

To calculate the accuracy and error of the model according to a specific classification, data identification was performed as shown in Table 5.

Table 5. Data identification

	Predicted No	Predicted Yes
Actual No	TN=22	FP=15
Actual Yes	FN=17	TP=525

Where TP-True Positive, i.e., during the face recognition system, the person's face is correctly identified.
TN-True Negative, i.e., indicates that the face of a person who is not in the database is not identified.
FP-False Positive, i.e., the face of a person who is not in the database is identified.
FN-False Negative, an error where the face of a person in the database is not detected.
Therefore, the performance of the model under consideration is 94.47%, as in (1).

$$Accuracy = \frac{TN + TP}{total} = \frac{22 + 525}{579} \approx 94.47 \quad (1)$$

Its error in accordance with the model's performance, as in (2).

$$Error\_rate = 100 - Accuracy = 100 - 94.47 = 5.53 \quad (2)$$

To assess the statistical significance of the obtained accuracy of the model, a binomial test with a null hypothesis (H_0) was performed, assuming that the true accuracy of the model does not exceed 90% [21, 23] (3):

$$H_0 : p \le 0.90, H_1 : p > 0.90 \quad (3)$$

The total number of test samples was N=579, with 547 correctly classified cases (True Positives + True Negatives). The binomial test yielded the following results:

Accuracy p=94.47%

Hypothetical accuracy: p_0=90.00%

p-value (one-tailed binomial test): $p=7.69 \times 10^{-5}$

Since $p << 0.05$,the null hypothesis was rejected, indicating that the model's accuracy is statistically significantly greater than 90% at $\alpha = 0.05$ significance level.

Additionally, the 95% confidence interval for model accuracy was calculated as (4):

$$[92.61\%, 96.33\%] \quad (4)$$

Thus, we can state with 95% confidence that the true accuracy of the model falls within this range.

To further evaluate the model's classification performance, a Receiver Operating Characteristic (ROC) curve was plotted, and the Area Under the Curve (AUC) was calculated [24, 25]. The ROC curve illustrates the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) at different classification thresholds.

The key results are as follows:

AUC (Area Under the Curve): 0.960

Interpretation: An AUC value close to 1.0 indicates a high ability of the model to distinguish between positive and negative classes. Figure 8 shows the ROC graph.

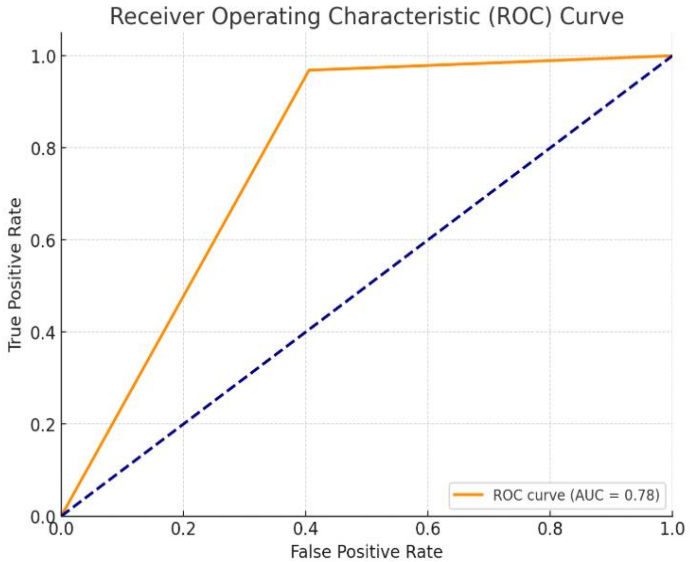

Fig. 8. The ROC curve.

The ROC curve (Figure X) demonstrates that the model maintains a high TPR while keeping the FPR low, confirming its effectiveness in classification tasks.

It can be observed that the developed face recognition system based on anti-spoofing, developed in accordance with the high accuracy of the model, can fully ensure the security of the educational platform and guarantee the preservation of academic integrity for students.

The results obtained from the study provide promising evidence for the practical applicability of the proposed face anti-spoofing method in real-world educational environments. Achieving an accuracy of 94.47% suggests that the system can reliably distinguish between authorized users and potential spoofing attacks, ensuring the integrity of the authentication process. This level of performance translates into increased security for online assessments, preventing unauthorized individuals from accessing the platform or attempting fraudulent activities. Moreover, the system's

efficiency in processing data using the Tiny model highlights its suitability for large-scale educational portals, where storage limitations and speed are critical factors. The significant reduction in image size without sacrificing accuracy addresses scalability concerns, allowing seamless integration into existing university systems. These findings underscore the model's potential to safeguard academic integrity by ensuring that exams and assessments are completed only by authorized students. This robust system can be a reliable solution for remote educational platforms and institutions seeking to implement secure authentication measures while maintaining user convenience.

5. Discussion

At the first stage of the implementation of the information and education portal, the availability of access to the system by using photos to the face recognition system was determined during the biometric authorization of users. To prevent this from the point of view of security and the principles of academic integrity, the anti-spoofing method has been improved and implemented based on machine learning. For this, a comparative analysis of the detectors used in the face recognition system based on a neural network was first performed, and MMOD Dlib CNN was selected as the most accurate algorithm. However, it should also be noted that it cannot work without GPU acceleration. During the experiment, access to the system by outsiders was checked by photo and video, and in case of non-compliance with the legal entity, a blocking operation was used. In the LCC_FASD dataset, approximately 300-350 photos per person were initially collected per user. The SSD MobileNet V1 convolutional neural network model, which was programmed using machine learning algorithms and Python language, and used in the analysis of the results, was a 1.6 GB dataset of photos taken for one person. The choice between the Tiny model, SSD MobileNet V1, and the dlib library was driven by the need to balance accuracy, storage efficiency, and processing speed. SSD MobileNet V1 initially showed high precision for detecting and classifying facial images in the anti-spoofing system. However, its significant storage requirements (5.4 MB per image) made it inefficient for large-scale deployment, particularly when handling datasets with hundreds of images per user. In contrast, the Tiny model demonstrated a remarkable advantage in terms of memory usage and speed. It required approximately 29 times less storage per image (190 KB) while maintaining competitive detection accuracy. This reduction in storage requirements made the Tiny model more suitable for environments where hardware limitations and scalability are critical, such as educational information portals. The dlib library was selected for its robust facial feature detection capabilities, particularly its ability to quickly and objectively identify 68 key facial landmarks. Despite its dependency on GPU acceleration for optimal performance, dlib provided essential tools for efficient pre-processing and dimensional analysis (28D and 128D representations) in the system. By adopting the Tiny model and leveraging the dlib library, the system achieved a more practical and efficient solution for real-world implementation, ensuring both scalability and reliable spoofing detection. In the future, it is planned to use an anti-spoofing method in the way of using a 3D mask for the biometric face recognition system.

6. Conclusion

In our study, ways of biometrically implementing the protection of the information education portal from cyberattacks were improved, and the flexibility of the Tiny model of neural network in machine learning in terms of data set storage and the efficiency of integration with the Python dlib system were determined. The implementation of the anti-spoofing method described in the article shows the ways to solve security problems in a practical sense as a result of the synthesis of traditional information protection methods, Python programming language, and machine learning, including neural network services, and is distinguished by the optimal organization of reliable protection of information of online portal users and system administrators.

This article covers research aimed at establishing a reliable and secure educational information portal system, enhancing the level of adherence to academic integrity among student users. In implementing information security, the face anti-spoofing method based on machine learning was applied. In the implementation of this method, the Tiny model neural network model, the dlib system of the Python language, capable of rapidly and objectively determining 68 surface points, and the LCC_FASD dataset were used.

As a result of the research work, the following works were performed:

- the Hog SVM, MODLib CNN, and HaarCascade (OpenCV) facial recognition detector was selected for our study;
- it was found that the speed of facial recognition obtained using the SD Mobile Net v1 neural network model is slower (especially when several users are logged into the system at the same time)than Tiny model;
- a step-by-step(data collection, preprocessing, face detection, function acquisition, face classification, face tracking) face anti-spoofing system was implemented using Photos, videos;
- an information and educational portal has been developed and tested(security.org.kz).

The research work was piloted among students enrolled in the educational programs 6B011500-Informatics, 7M011500-Informatics, and 8D01500-Informatics at the L.N. Gumilyov Eurasian National University, and the accuracy of the information security was calculated using a confusion matrix, demonstrating a 94.47% performance of the

developed system.

The findings of this study highlight the practical significance of the proposed anti-spoofing security system. Beyond academic applications, this approach can be integrated into digital portals, mobile applications, and corporate security systems across various industries, including banking, healthcare, and government authentication services. The lightweight architecture of the Tiny model makes it particularly suitable for real-time applications in resource-constrained environments. To further enhance the security of educational information portals, future research will focus on:

- exploring more advanced deep learning architectures for real-time face authentication.
- incorporating multi-modal biometric security, such as voice recognition and behavioral authentication, to improve overall robustness.
- analyzing adversarial attacks on face recognition systems and developing countermeasures.
- expanding the dataset to include diverse lighting conditions, facial expressions, and occlusions for improved generalization.

By addressing these aspects, we aim to develop a more reliable and adaptive model that can further strengthen the security of digital education platforms and beyond.

Acknowledgment

This paper is an output of the science project “Development educational portal on machine learning as an artificial intelligence's direction to improve the Informatic teacher's training in education globalization”. This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19677348 "Development educational portal on machine learning as an artificial intelligence's direction to improve the Informatic teacher's training in education globalization").

References

[1] Z. Akhtar and S. Kale, “Security Analysis of Multimodal Biometric Systems against Spoof Attacks,” Communications in Computer and Information Science, vol. 191, 2011. https://doi.org/10.1007/978-3-642-22714-1_62

[2] M. Saranya and P. Amudha, “Anti-Spoofing Method: A Survey on Biometric Face Recognition,” *World Scientific News*, vol. 41, pp. 92–98, 2016.

[3] S. Bharadwaj, T.I. Dhamecha, M. Vatsa and R. Singh, “Computationally efficient face spoofing detection with motion magnification,” In Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 105–110, 2013. https://doi.org/10.1109/CVPRW.2013.23

[4] R. Raghavendra and Ch. Busch, “Presentation Attack Detection Algorithm for Face and Iris Biometrics”, *Signal Processing Conference (EUSIPCO)*, 2014.

[5] G. Pan, L. Sun, Z. Wu and S. Lao, “Eyeblink-based antispoofing in face recognition from a generic Webcamera,” In Proc. IEEE 11th ICCV’07, pp. 14-20, 2007. https://doi.org/10.1109/ICCV.2007.4409068

[6] T. Amirsina and N. Nasrabadi, “3D Convolutional Neural Networks for Cross Audio-Visual Matching Recognition,” IEEE. Translations and content mining are permitted for academic research only, vol.5, pp. 22081-22091, 2017. https://doi.org/10.1109/ACCESS.2017.2761539

[7] Y. Li, M. Chang and S. Lyu, “In ictu oculi: Exposing AI created fake videos by detecting eye blinking,” In 2018 IEEE International workshop on information forensics and security (WIFS), pp. 1-7, 2018. DOI: 10.1109/WIFS.2018.8630787

[8] J. Kim, W. Luu and S. Palmisano, “Multisensory integration and the experience of scene instability, presence and cybersickness in virtual environments,” *Computers in Human Behavior*, vol.113, 2020. https://doi.org/10.1016/j.chb.2020.106484

[9] Y. Kim, J. Na, S. Yoon and J. Yi, “Masked fake face detection using radiance measurements,” *Journal of the Optical Society of America*, vol. 26, is. 4, pp. 760-766, 2009. https://doi.org/10.1364/JOSAA.26.000760

[10] R.J. Raghavendra, K.P. Jeevan, M. Likith, G. Manoj and D.S. Yashas, “A Survey on Anti-Spoofing Methods for Facial Recognition*,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 8(2), pp.259-268, 2022. https://doi.org/10.32628/CSEIT228248

[11] Z. Yu and Y. Qin, “Deep learning for face anti-spoofing: A survey,” *IEEE transactions on pattern analysis and machine intelligence*, no. 45(5), pp. 5609-5631, 2022. https://doi.org/10.1109/TPAMI.2022.3215850.

[12] P. Anthony, B. Ay and G. Aydin, “A review of face anti-spoofing methods for face recognition systems,” 2021 International Conference on Innovations in Intelligent SysTems and Applications (INISTA). IEEE, pp.1-9, 2021. https://doi.org/10.1109/INISTA52262.2021.9548404.

[13] R. Ranjan and A. Bansal, “A Fast and Accurate System for Face Detection, Identification, and Verification,” IEEE Transactions on Biometrics Behavior and Identity Science, 2019, pp. (99):1-1. https://doi.org/10.1109/TBIOM.2019.2908436

[14] D. Habrman, *“*Face Recognition with Preprocessing and Neural Networks,” M.S.thesis, Linköping University, Department of Electrical Engineering, 2016.

[15] Z. Ming, M. Visani, M. Luqman and J.C. Burie, “A survey on anti-spoofing methods for facial recognition with rgb cameras of generic consumer devices,” *Journal of imaging*, 6(12), p.139, 2020.

[16] S. Xiao and X. Zhao, “Discriminative representation combinations for accurate face spoofing detection*,” Pattern Recognition*, vol. 85, pp. 220-231, 2019. https://doi.org/10.1016/j.patcog.2018.08.019

[17] J. Galbally, S.Marcel and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *Ieee Access*, 2, pp. 1530-1552, 2020.
[18] N. Jahan and P.K. Bhuiyan, "Real Time Face Recognition System with Deep Residual Network and KNN," Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020), pp. 1122-1126, 2020. https://doi.org/10.1109/ICESC48915.2020.9155579
[19] D. Timoshenko, K. Simonchik, V.Shutov, P.Zhelezneva and V. Grishkin, "Large crowdcollected facial anti-spoofing dataset," *Computer Science and Information Technologies (CSIT)*, pp.123-126, 2019.
[20] V. Patro, and M. Patra, "Augmenting weighted average with confusion matrix to enhance classification accuracy," *Transactions on Machine Learning and Artificial Intelligence*, 2(4), pp.77-91, 2014.
[21] L. Wasserman, "All of statistics: a concise course in statistical inference," *Springer Science & Business Media*, 2013.
[22] A.Agresti and B. Finlay, "Statistical methods for the social sciences", 2009.
[23] T. Hastie and R. Tibshirani, "The elements of statistical learning", 2001.
[24] J.Eng, "Receiver operating characteristic analysis: a primer1," *Academic radiology*, 12(7), pp.909-916, 2013.
[25] J. Fan, S. Upadhye and A. Worster, "Understanding receiver operating characteristic (ROC) curves", *Canadian Journal of Emergency Medicine*, 8(1), pp.19-20, 2006.

Authors' Profiles

Serik Meruert, doctor of Pedagogical Sciences, she is a professor at the Department of "Informatics" at the L. N. Gumilyov Eurasian National University. She received her doctorate in Pedagogy in 2004. She is the author of more than 100 scientific papers, including articles in international peer-reviewed journals and conferences in the field of client-server technology, cloud technologies, machine learning, big data. She is the holder of the state educational grant "The Best University teacher-2008", an expert of the National Accreditation Center of the Ministry of Education and Science of the Republic of Kazakhstan, a member of the expert commission of the National Center for Testing and Standardization of the Ministry of Education and Science of the Republic of Kazakhstan.

Tleumagambetova Danara, Doctoral student of the educational program «8D01511 – Informatics», L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. She received her master's degree in 2013. She is the author of several peer-reviewed articles in local and international journals and conference proceedings. Her research areas include information security, big data, machine learning, and Olympiad problem programming.

Alaminov Muratbay, Doctor of Pedagogical Sciences, he is an associate professor at Nukus institute. His teaching experience inclides information technologies and netrwork technologies. His research interests include edicational technology, mathematical modelling and artificial intelligence.

How to cite this paper: Meruert Serik, Danara Tleumagambetova, Alaminov Muratbay, "Information Security of Educational Portal Based on Face Anti-Spoofing Method: Effectiveness of Tiny Neural Network Machine Learning Model", International Journal of Modern Education and Computer Science(IJMECS), Vol.17, No.3, pp. 59-71, 2025. DOI:10.5815/ijmecs.2025.03.05