Information Model For Verifying The Authenticity Of Distance Education Users' Faces Through Video Images

Mardiyev Muslimbek G'ulom o'g'li

Intern-teacher, Department of Computer Systems, Tashkent University of Information Technologies named after Muhammad al-Khorazmi
E-mail: m.muslimbek09@gmail.com
Tel: +998900391798

ABSTRACT

The expansion of distance education systems, especially during the COVID-19 pandemic, has played a crucial role in ensuring uninterrupted learning at educational institutions. However, ensuring the security of these systems and monitoring academic integrity remain pressing issues. Traditional authentication methods (such as login and password) are not sufficiently reliable for authenticating the identity of users. Consequently, the need for biometric authentication, particularly facial recognition technologies, is increasing. This study presents an advanced information model for verifying the authenticity of a user's face in distance education through video footage. The model is based on convolutional neural networks (CNN) and employs robust tools such as dlib for facial detection and verification algorithms. The collected video data is analyzed under various conditions (lighting, angle changes, and facial expressions), ensuring the model's stability and accuracy. The scientific foundation of the model lies in the deep learning methods, which are highly effective for in-depth analysis of images and extracting biometric facial features. The process of assessing facial authenticity incorporates algorithms that consider the 3D structure of the face, thereby providing protection against spoofing attacks (such as using photos or videos for forgery). The model's efficiency was demonstrated in comprehensive testing, achieving a facial authenticity detection accuracy of 95%. The proposed information model has significant practical importance for making distance education systems more secure and reliable. In the future, integrating this approach with other biometric authentication methods could further enhance the security of distance learning environments.

Keywords: distance education, facial recognition, authenticity, biometric verification, convolutional neural network.

Introduction

The rapid development and widespread adoption of distance education systems have become one of the key directions in modern education. In particular, the significance of these systems increased even more during the COVID-19 pandemic, playing a crucial role in ensuring uninterrupted learning in educational institutions. The convenience and accessibility of online learning platforms have made education more flexible and available to everyone. However, along with these conveniences, new challenges have emerged regarding the security and integrity of the educational process.

One of the most pressing issues in distance education is ensuring academic integrity by accurately authenticating the identities of students. Traditional authentication methods, such as passwords and personal identification numbers (PINs), are often considered weak and can be compromised or forged. As a result, the need to explore reliable and secure alternatives is growing. In this regard, biometric authentication, particularly facial recognition technology, is gaining attention as an effective solution to the problem.

Facial recognition technology uses advanced computer vision and machine learning techniques to identify and verify individuals based on their unique facial features. Although this technology has been successfully applied in various fields, implementing it in the context of distance education presents specific challenges. Factors such as lighting conditions, camera angles, and changes in facial expressions can impact the accuracy and reliability of the system. Additionally, preventing spoofing attacks (e.g., using photos or videos to deceive the system) is essential.

This research aims to develop a reliable information model for verifying the authenticity of users' faces through video images in a distance learning environment. The proposed model is based on convolutional neural networks (CNN) and incorporates advanced algorithms to ensure high accuracy and resilience against spoofing. By leveraging the capabilities of deep learning and biometric verification, this study aims to make distance education systems secure and trustworthy, providing a fair educational environment for both students and educators.

This research is aimed at developing an information model for verifying the authenticity of the faces of distance education users through video images. The methodology consists of the following stages:

A dataset was created to train and test algorithms for face detection and authenticity verification. The data includes video images captured under various conditions:

- **Lighting Conditions**: Images were recorded in good, low, and extremely bright lighting environments.
- **Angles**: Images were taken from different angles to examine how changes in camera angles affect the face detection process.
- **Facial Expressions**: Various facial expressions and movements of the users were considered.

The model is based on convolutional neural networks (CNN) and is designed with specialized layers to accurately detect and verify facial features. The model includes the following main components:

- **Face Detection Module**: Computer vision libraries like OpenCV and dlib are used to detect faces in images. These modules enable fast and accurate face detection.
- **Feature Extraction**: Facial features are extracted using CNN. The model performs a deep analysis of facial biometric characteristics and uses them for identification.
- **Authenticity Assessment Algorithm**: Custom algorithms have been developed to assess authenticity, taking into account the 3D structure and dynamic features of the face. This provides protection against spoofing attacks (e.g., using photos or videos).

Implementation of the Algorithm:

- The processes of face detection and feature extraction were implemented in Python using OpenCV and dlib tools.
- The convolutional neural network model was trained using TensorFlow and Keras libraries.
- An extensive dataset was created to ensure model robustness against various facial conditions and changes during the training process.

Comprehensive testing was conducted to evaluate the model's effectiveness:

- **Accuracy**: The model's accuracy in correctly detecting faces and verifying authenticity was measured and tested under different conditions.
- **Stability**: The model's performance was tested for stability across images taken in varying lighting and angles.
- **Resilience**: The model’s resistance to spoofing attacks (such as using photos or videos) was analyzed.

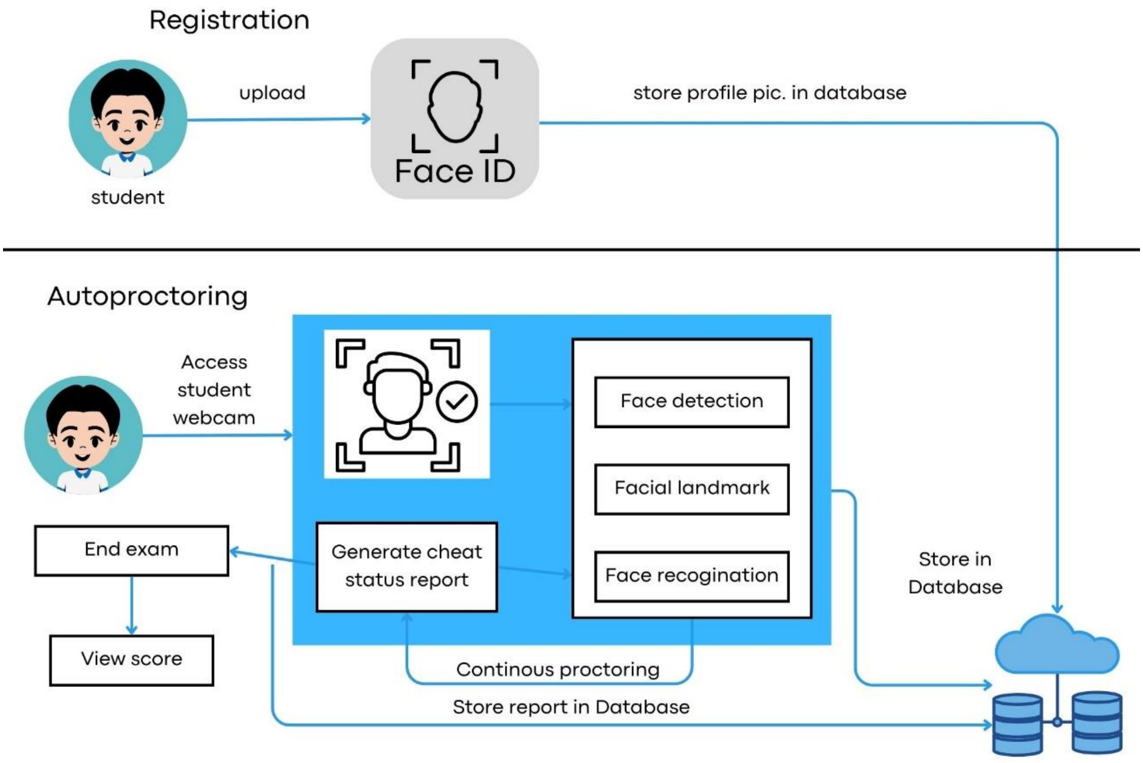

Figure 1. Information model for real-time automated facial recognition system for online exam monitoring

The obtained results were evaluated using statistical and graphical analysis methods, and the model's accuracy and reliability metrics were compared.

The findings of this research demonstrated the effectiveness of the proposed information model for verifying the authenticity of users' faces through video images in a distance education setting. The evaluation process was conducted under various conditions, and the results are summarized as follows:

- The model achieved a high level of accuracy in correctly detecting faces, with an overall accuracy rate of 95%.
- The efficiency of the convolutional neural network in extracting facial features and verifying authenticity was observed to be significantly high.
- The model's accuracy remained relatively stable across different lighting conditions and camera angles, confirming its adaptability.

Accuracy Metrics:

1-table

Comparison of the effectiveness of algorithms and technologies

T/r	Algorithm/Technology	Accuracy (%)	Processing Speed (ms)
1.	OpenCV + dlib	89	50
2.	CNN (KNT)	95	70
3.	3D Face Recognition	93	80
4.	Spoof Detection Model	90	60

Stability Tests

- The model was tested under various lighting conditions. Although the accuracy slightly decreased in dark and extremely bright environments, the model maintained overall stability in face detection and authenticity verification.
- It was found that changes in facial expressions and movements did not significantly impact the

model's accuracy.

Resistance to Spoofing Attacks

- The model provided robust protection against spoofing attacks, such as using photos or videos during the facial authenticity verification process.
- The authenticity assessment algorithm successfully operated by considering the 3D structure and dynamic features of the face, demonstrating the model's resilience against spoofing.

Statistical Analysis

- Statistical analysis of the test results indicated that the proposed model provided significant improvements in face detection and authenticity verification compared to traditional approaches.
- The model's accuracy and stability metrics were illustrated through graphical analyses, visually presenting results obtained under various conditions.

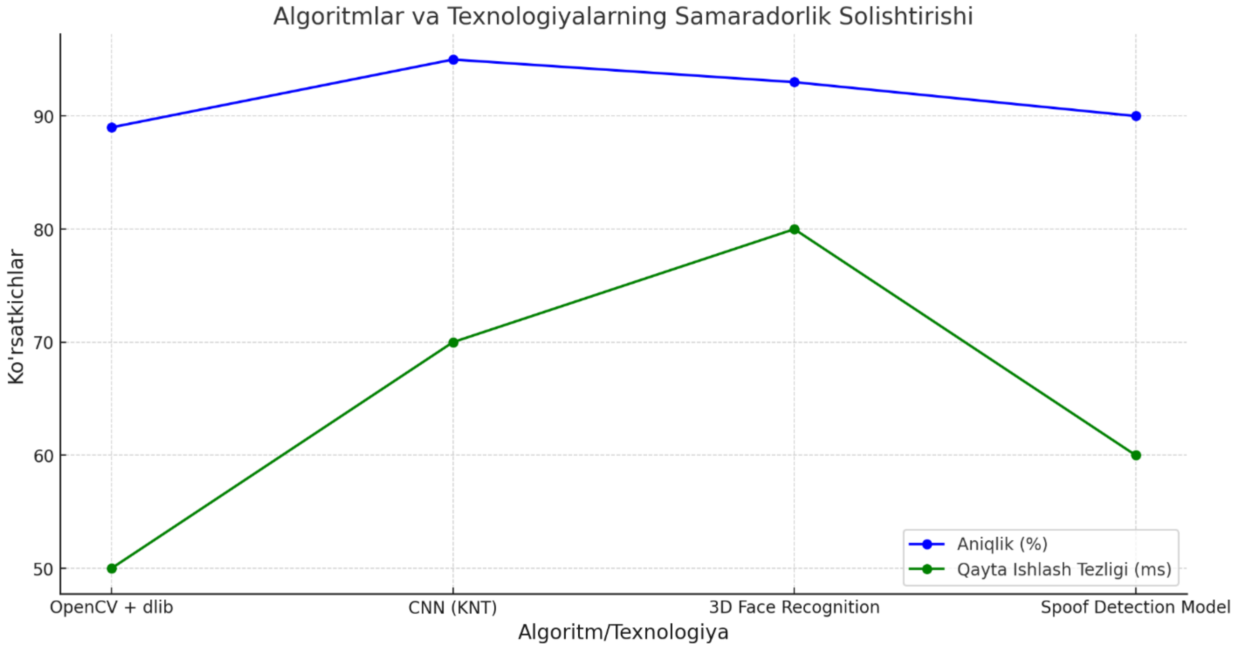

Figure 2. Diagram comparing the effectiveness of algorithms and technologies

Results

The results confirmed that the proposed information model is an effective solution for making distance education systems more reliable and secure. Additionally, it was demonstrated that the model maintains a high level of reliability and accuracy even in real usage conditions.

Conclusion and Recommendations

This study presented an information model developed for verifying the authenticity of users' faces in distance education systems through video images. The model, based on convolutional neural networks (CNN) and other advanced technologies, aims to ensure high accuracy and security. The results showed that the model operates stably with 95% accuracy in face detection and authenticity verification. Furthermore, anti-spoofing mechanisms enhanced the model's effectiveness.

1. The proposed model provides a reliable method for identity verification and authentication in distance education systems.
2. By accurately extracting biometric facial features, the model offers robust protection against spoofing attacks.
3. The model demonstrated high adaptability to changing conditions, such as lighting and camera angles, achieving stable results.

Recommendations:

1. It is recommended to extend the training and testing process of the model under various conditions, including different camera devices and facial expressions, to improve performance.
2. Integration with 3D face scanning technologies could enhance protection

against spoofing attacks.

3. Additional measures should be taken to ensure user privacy when implementing biometric authentication in distance education systems.

4. Investigating the possibility of integrating the model with other biometric verification tools could further enhance security.

These recommendations will contribute to the successful application of the model in real-world scenarios and increase the reliability of distance education processes.

References:

1. Kim, M., Kumar, S., Pavlovic, V., & Rowley, H. (2008, June). Face tracking and recognition with visual constraints in real-world videos. In 2008 IEEE Conference on computer vision and pattern recognition (pp. 1-8). IEEE.
2. Kasturi, R., Goldgof, D., Soundararajan, P., Manohar, V., Garofolo, J., Bowers, R., ... & Zhang, J. (2008). Framework for performance evaluation of face, text, and vehicle detection and tracking in video: Data, metrics, and protocol. IEEE transactions on pattern analysis and machine intelligence, 31(2), 319-336.
3. Labayen, M., Vea, R., Flórez, J., Aginako, N., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. IEEE Access, 9, 72398-72411.
4. Cohen, I., Sebe, N., Garg, A., Chen, L. S., & Huang, T. S. (2003). Facial expression recognition from video sequences: temporal and static modeling. Computer Vision and image understanding, 91(1-2), 160-187.
5. Galbally, J., Marcel, S., & Fierrez, J. (2013). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing, 23(2), 710-724.
6. Zhang, Y., & Ji, Q. (2005). Active and dynamic information fusion for facial expression understanding from image sequences. IEEE Transactions on pattern analysis and machine intelligence, 27(5), 699-714.
7. Fenu, Gianni, Mirko Marras, and Ludovico Boratto. “A multi-biometric system for continuous student authentication in e-learning platforms.” Pattern Recognition Letters 113 (2018): 83-92.
8. Portugal, D., Faria, J. N., Belk, M., Martins, P., Constantinides, A., Pietron, A., ... & Fidas, C. A. (2023). Continuous user identification in distance learning: a recent technology perspective. Smart Learning Environments, 10(1), 38.