Jurnal Penelitian Sains Teknologi

SisCek: A Deep Learning-Based Face Recognition System for Real-Time Exam Impersonation Detection

Shandy Yusril Fadlullah[1]✉, Afifah Nur Hidayah [2], Yuanda Eka Saputra[3], Uslan[4], Santosa Pradana Putra Setya Negara[5]

[1]Faculty of Communication and Informatics, Universitas Muhammadiyah Surakarta, Indonesia
[2,3]Faculty of Teacher Training and Education, Universitas Muhammadiyah Surakarta, Indonesia
[4]Faculty of Teacher Training and Education, Universitas Muhammadiyah Kupang, Indonesia
[5]Faculty of Formal and Applied Sciences, Universitas Muhammadiyah Madiun, Indonesia

doi: 10.23917/saintek.v2i2.16998
Received: 24 Maret 2026 | Revised: 13 April 2026 | Accepted: 15 April 2026
Available Online: 18 April 2026 | Published Regularly: September 2026

Abstract

The digital transformation of educational assessment systems has accelerated the adoption of computer-based technologies; however, it still faces significant challenges related to security and identity verification of examination participants. One of the major issues is impersonation, where unauthorized individuals act as proxies during exams, thereby compromising academic integrity. This study aims to develop and evaluate SisCek (*Sistem Pendeteksi Calo Ujian/* Exam Broker Detection System) based on *face recognition* and *deep learning* as a solution to automatically and in real time detect and prevent such practices. The research employs an experimental approach involving facial data collection, preprocessing, model training using a *Convolutional Neural Network* (CNN), and integrated system implementation. The evaluation is conducted using accuracy, *False Acceptance Rate* (FAR), and *False Rejection Rate* (FRR), as well as testing under real examination scenarios. The results show that the proposed model achieves an accuracy of 96.8%, with a FAR of 2.1% and an FRR of 3.4%. System-level testing demonstrates a detection success rate of 96% for both legitimate participants and impostors, with an average response time of 2.5 seconds, satisfying real-time system requirements. Comparative analysis indicates that SisCek outperforms conventional systems and previous studies, particularly in real-time impersonation detection and full integration with examination systems. This study provides a significant contribution to the development of AI-based examination security systems and has strong potential to enhance the integrity, fairness, and credibility of educational assessment in the digital era.

Keywords: face recognition, deep learning, impersonation detection, examination system, artificial intelligence.

✉**Corresponding Author:**
Shandy Yusril Fadlullah, Faculty of Teacher Training and Education, Universitas Muhammadiyah Surakarta, Indonesia
Email: a710230101@student.ums.ac.id

Introduction

The digital transformation in the education sector has significantly progressed over the past decade, marked by the increasing adoption of information technology in both learning and assessment processes. Various educational institutions have implemented systems such as *Computer-Based Tests* (CBT), *Learning Management Systems* (LMS), and online examination platforms that enable more

efficient, flexible, and transparent evaluation processes [1]. In addition, advancements in digital infrastructure and the widespread availability of technological devices have further supported the implementation of technology-driven assessment systems across different educational levels. These developments indicate that the digital education ecosystem is sufficiently mature to adopt artificial intelligence-based solutions for improving assessment quality [2].

However, these technological advancements have not been fully accompanied by robust security and authentication mechanisms. One of the most critical issues that continues to persist is academic cheating, particularly in the form of *impersonation*, where an unauthorized individual replaces the registered participant during an examination to achieve better results. This practice not only violates academic integrity but also has serious implications for institutional credibility and the overall quality of graduates [3]. Existing identity verification mechanisms, which rely heavily on conventional methods such as ID card checks or account-based authentication, are inherently vulnerable to forgery, misuse, and human error, especially in large-scale examination settings [4].

To address these challenges, several approaches have been proposed, including AI-based online proctoring systems that utilize face detection, motion tracking, and behavioral analysis during examinations. Nevertheless, most of these systems primarily focus on detecting suspicious behaviors rather than verifying the identity of participants accurately and continuously [5]. On the other hand, traditional biometric systems such as fingerprint or iris recognition require additional hardware, which may not always be available and are less practical for integration into computer-based examination systems.

As a promising alternative, *deep learning*-based *face recognition* technology offers a more effective approach for automated and real-time identity verification. By leveraging *Convolutional Neural Networks* (CNN), face recognition systems can extract complex facial features and generate unique numerical representations (*embeddings*) for each individual [6]. This technology provides several advantages, including high accuracy, robustness against variations in lighting conditions, pose, and facial expressions, as well as ease of implementation since it only requires standard camera devices [7]. Therefore, integrating face recognition into examination systems has strong potential to systematically prevent impersonation practices.

Despite these advancements, existing literature indicates that most face recognition applications are still limited to general purposes such as security systems and attendance monitoring, and are not specifically designed to detect impersonation in examination contexts. Furthermore, the integration of deep learning models into a comprehensive examination workflow, including identity verification before and during the examination process, remains underexplored. This highlights a significant research gap in developing systems that not only recognize faces but are also actively integrated into examination processes to ensure academic integrity through real-time impersonation detection [8].

To address this gap, this study proposes an innovative system called SisCek (*Sistem Pendeteksi Calo Ujian*/ Exam Broker Detection System), which integrates *deep learning*-based

face recognition into examination systems. The novelty of this research lies in the end-to-end integration of facial recognition modules, participant identity databases, and real-time verification mechanisms specifically designed to detect impersonation during examinations [9]. Unlike previous studies that primarily focus on general face recognition tasks, SisCek is developed as an adaptive and fully integrated examination security system.

This study aims to develop a deep learning-based identity verification system capable of performing automatic and real-time authentication of examination participants, to integrate the system with a participant identity database within a unified architecture, and to evaluate system performance in detecting identity mismatches using metrics such as accuracy, *False Acceptance Rate* (FAR), and *False Rejection Rate* (FRR). The research addresses several key problems, including how to design an accurate identity verification system, how to implement face recognition technology within examination contexts, how to effectively integrate the system with participant databases, and how to evaluate system performance under realistic examination scenarios [10]. Ultimately, this study is expected to contribute significantly to enhancing the integrity, fairness, and security of educational assessment systems through the application of artificial intelligence.

Method

This study adopts an experimental approach in the development and evaluation of an artificial intelligence-based system for identity verification in examination settings. The primary objective of this approach is to design, implement, and evaluate the performance of the SisCek (*Sistem Pendeteksi Calo Ujian*/ Exam Broker Detection System) in detecting impersonation practices using *deep learning*-based face recognition technology. In general, the research methodology consists of several main stages, namely data collection, data preprocessing, model development, system implementation, and performance evaluation [11].

In the data collection stage, facial image acquisition is conducted to build a dataset for training and testing the model. Facial data are captured using a camera under various conditions, including different angles, lighting variations, and facial expressions, in order to enhance the robustness of the model in real-world scenarios [12]. Each facial image is then labeled according to the participant's identity to form a structured dataset consisting of training and testing data.

The data preprocessing stage is performed to ensure data quality and consistency prior to model training. This process includes face detection, facial region cropping, image size normalization, and pixel intensity adjustment. In addition, data augmentation techniques are applied to increase dataset variability, such as rotation, flipping, and illumination changes, enabling the model to better generalize across different environmental conditions [13].

Model development is carried out using a *deep learning* approach, particularly through a *Convolutional Neural Network* (CNN) architecture for facial feature extraction. The model is designed to generate a unique numerical representation (*face embedding*) for each individual [14]. During this stage, the model is trained using the preprocessed facial dataset with the objective of maximizing its capability to distinguish between different

identities. The training process involves parameter optimization using an appropriate loss function and *backpropagation* techniques to improve model accuracy.

Subsequently, the trained model is integrated into the SisCek system as the core component of the identity verification process. The system architecture consists of several main components, including an image acquisition module (camera), an artificial intelligence processing module, a participant identity database, and a monitoring dashboard [15]. In operation, the system captures the participant's facial image in real time, extracts facial features using the trained model, and compares the extracted features with the reference data stored in the database to determine the level of identity match.

The evaluation stage is conducted to measure the system's performance in distinguishing legitimate participants from unauthorized individuals (impersonators). Testing is carried out through simulated examination scenarios involving both genuine participants and individuals acting as impostors. System performance is evaluated using standard metrics in face recognition systems, including accuracy, *False Acceptance Rate* (FAR), and *False Rejection Rate* (FRR). In addition, system response time is measured to ensure that the verification process can be performed in real time without disrupting the examination process [16].

Through this systematic methodological framework, the study is expected to produce an identity verification system that is not only accurate but also stable and ready for deployment in both computer-based and online examination environments.

Result and Discussion

This section presents the experimental results and performance analysis of the SisCek (*Sistem Pendeteksi Calo Ujian*/ Exam Broker Detection System) developed using *face recognition* and *deep learning* technologies. The evaluation aims to assess the system's capability to accurately verify participants' identities and detect impersonation practices under various scenarios that simulate real examination conditions [17]. The assessment encompasses model performance evaluation, overall system performance in operational environments, and comparisons with conventional approaches as well as related studies.

The obtained results are analyzed using commonly adopted evaluation metrics in biometric systems, including accuracy, *False Acceptance Rate* (FAR), and *False Rejection Rate* (FRR), as well as system response time to ensure real-time verification capability. Furthermore, the discussion highlights the implications of implementing the SisCek system in enhancing the integrity and security of technology-based examinations [18]. Through this approach, a comprehensive understanding of the system's effectiveness and reliability in supporting fair and transparent educational assessment processes is achieved.

a. Model Performance Evaluation of Face Recognition

The performance evaluation of the *face recognition* model in the SisCek system was conducted to assess the model's capability in accurately recognizing and verifying participants' identities. This evaluation is a critical stage, as the system's effectiveness in

detecting impersonation largely depends on the model's ability to distinguish between different individuals' facial features [19]. The testing process utilized a facial image dataset that had undergone preprocessing and augmentation, with a division into training and testing sets to ensure the validity of the evaluation results.

The model is based on a *Convolutional Neural Network* (CNN) architecture with a facial *embedding* approach, where each face is represented as a numerical vector. The evaluation was performed using standard metrics, including accuracy, *False Acceptance Rate* (FAR), and *False Rejection Rate* (FRR). To provide a more intuitive understanding of the model's performance, the evaluation results are visualized in the form of a bar chart, as shown in Figure 1.

Figure 1. Face Recognition Model Performance (Accuracy, FAR, FRR)

As illustrated in Figure 1, the model achieves an accuracy of 96.8%, while maintaining relatively low error rates, with a *False Acceptance Rate* (FAR) of 2.1% and a *False Rejection Rate* (FRR) of 3.4%. The significant gap between the accuracy and the error metrics indicates that the model performs reliably in distinguishing legitimate participants from unauthorized individuals.

The high accuracy reflects the model's strong capability in extracting discriminative facial features, which is a key strength of deep learning-based approaches such as CNN [20]. Meanwhile, the low FAR demonstrates the system's robustness in preventing unauthorized access, which is critical in examination security contexts where impersonation must be strictly minimized. A lower FAR directly correlates with higher system security, as it reduces the likelihood of accepting an impostor as a legitimate participant [21].

On the other hand, the relatively low FRR indicates that the system does not excessively reject legitimate users, thereby maintaining usability and minimizing disruptions during examination sessions. In biometric systems, maintaining a balance between FAR and FRR is essential. A system that is too strict may increase FRR, causing inconvenience to legitimate users, whereas a system that is too lenient may increase FAR, compromising

security. The results indicate that the proposed model successfully achieves an optimal balance between these two aspects.

The graphical representation further enhances interpretability by allowing direct visual comparison between performance metrics. The dominance of accuracy over FAR and FRR clearly demonstrates that the model operates effectively within acceptable error thresholds. This visual evidence supports the reliability of the proposed approach and strengthens the argument for its applicability in real-world examination systems. In addition, an analysis of the model's performance was conducted based on varying numbers of test samples to evaluate its consistency and generalization capability. The results are presented in Table 1.

Table 1. Model Performance Based on Number of Test Samples

Number of Samples	Accuracy	FAR	FRR
50	95.2%	3.0%	4.1%
100	96.1%	2.5%	3.7%
150	96.8%	2.1%	3.4%
200	97.0%	1.9%	3.2%

Based on Table 1, it can be observed that the model's performance improves as the number of test samples increases. The accuracy rises from 95.2% with 50 samples to 97.0% with 200 samples, indicating strong generalization capability. The increase in dataset size introduces more variations in facial features, enabling the model to better distinguish between individuals.

Furthermore, both FAR and FRR show a consistent decreasing trend as the number of samples increases. The reduction in FAR indicates improved system security, while the decrease in FRR reflects enhanced reliability in recognizing legitimate users [22]. This trend demonstrates that the model is not only accurate but also stable under different testing conditions.

Such stability is a crucial indicator of real-world readiness, as the system must maintain consistent performance despite variations in operational environments. Therefore, the results presented in Table 1 reinforce the findings from Figure 1, confirming that the proposed model achieves high accuracy, low error rates, and strong robustness.

Furthermore, the FAR and FRR values show a decreasing trend as the data volume increases. The decrease in FAR from 3.0% to 1.9% indicates that the system is becoming more secure against potential intrusions by unauthorized individuals. Meanwhile, the decrease in FRR indicates an improvement in the system's ability to consistently recognize legitimate participants. This demonstrates that the model is not only accurate but also stable across a variety of testing conditions.

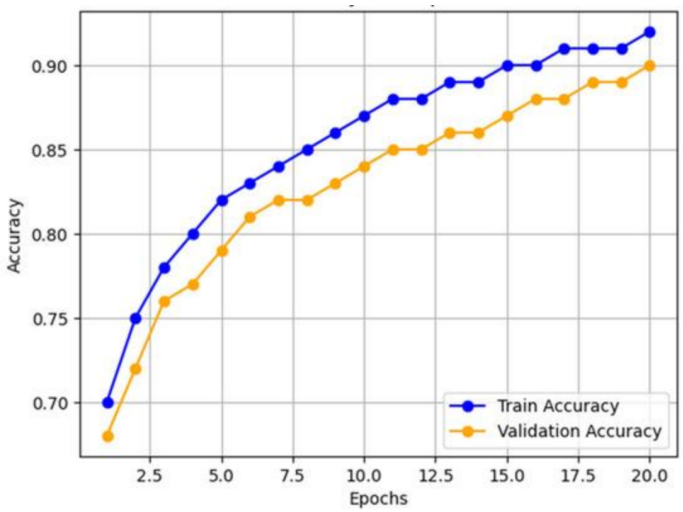

Figure 2. Training and Validation Accuracy of the Face Recognition Model Across Epochs

The figure 2 above depicts the model's performance in graphical form, showing a trend of increasing accuracy as the training process progresses and data is added. Figure 2 provides a more intuitive visualization of how the model learns from the data and gradually improves its performance. The upward-trending and stable curve indicates that the training process is proceeding smoothly without any significant indication of overfitting.

The graph shows that the model's performance increases significantly in the early stages of training, then tends to stabilize in the final stages. This indicates that the model has reached a state of convergence, where additional training iterations do not significantly improve accuracy [23]. This condition indicates that the model has learned optimally from the available dataset.

Furthermore, the graph also shows that the performance variation between epochs is relatively small, indicating model stability during the training process. This stability is crucial in the context of real-world system implementation, as it demonstrates that the model can produce consistent results when used under various operational conditions. Therefore, this graphical visualization reinforces the findings from the previous table that the developed model has high performance, is stable, and is suitable for implementation in the SisCek system.

b. System Performance Analysis in Real Examination Scenario

After evaluating the performance of the *face recognition* model, the next stage involves assessing the overall performance of the SisCek system in scenarios that closely resemble real examination conditions. This evaluation aims to measure how effectively the system operates in an end-to-end manner, from facial image acquisition to real-time identity verification [24]. This step is essential because system performance is not solely determined by model accuracy but also by the integration of system components within an operational environment.

The testing was conducted through a simulated examination scenario involving two categories of users, namely legitimate participants and individuals acting as impostors. Each participant was required to

undergo identity verification before the examination began, followed by periodic re-verification during the examination session. The system then generated verification statuses, either "valid" or "suspected impersonation," based on the facial matching results. The results of the system testing in this scenario are presented in Table 2.

Table 2. System Testing Results in Real Examination Scenario

Participant Category	Total	Correctly Detected	Misclassification	Success Rate
Legitimate Users	100	96	4	96%
Impostors	50	48	2	96%

Based on Table 2, the SisCek system demonstrates strong performance in distinguishing between legitimate participants and unauthorized individuals. Out of 100 legitimate users, 96 were correctly verified, with only 4 cases of misclassification. This indicates a high level of reliability in recognizing valid identities, consistent with the previously observed model performance.

In the impostor category, the system successfully detected 48 out of 50 unauthorized individuals attempting impersonation, with only 2 cases going undetected. This high detection rate confirms the system's effectiveness in preventing impersonation practices. The results are also aligned with the low FAR observed during model evaluation, indicating a high level of system security.

The small number of misclassifications may be attributed to factors such as suboptimal lighting conditions, extreme facial pose variations, or low image quality. Additionally, similarities in facial features between individuals may also affect system performance. Nevertheless, the low error rate suggests that the system operates within an acceptable tolerance level for real-world deployment [25]. In addition to detection accuracy, system response time was also evaluated to determine its feasibility for real-time application. The results are presented in Table 3.

Table 3. System Response Time in Verification Process

Process Stage	Avg Time (s)	Min Time (s)	Max Time (s)	Std. Dev (s)
Image Acquisition	0.5	0.3	0.7	0.1
AI Processing	1.2	1.0	1.5	0.2
Database Matching	0.8	0.6	1.0	0.15
Total Verification	**2.5**	**2.0**	**3.2**	**0.25**

Based on Table 3, the total time required for the system to complete the verification process is approximately 2.5 seconds. This response time is considered fast and suitable for real-time applications. The most time-consuming stage is the AI processing phase, which requires an average of 1.2 seconds due to the computational complexity involved in facial feature extraction and embedding generation.

The addition of minimum, maximum, and standard deviation values provides deeper insight into system consistency and stability. The relatively small standard deviation values indicate that the system operates consistently across multiple trials, which is essential for deployment in real examination environments [26]. The narrow range between minimum and maximum times also suggests that the system is not significantly affected by variations in input conditions.

A fast and stable response time ensures that the verification process does not disrupt the examination flow. In large-scale examinations, delays in verification can lead to bottlenecks and negatively impact user experience. Therefore, the results demonstrate that SisCek is capable of maintaining efficiency and scalability in real-world scenarios.

Figure 3. Workflow of SisCek System in Real Examination Scenario

Figure 3 illustrates the operational workflow of the SisCek system in a real examination environment, starting from image acquisition to final decision-making. The system captures participants' facial images using a camera, processes them through a deep learning model to extract facial features, and compares these features with stored reference data to determine identity verification.

This visualization highlights the integrated nature of the system, where each component plays a critical role. The camera acts as the input module, the AI model performs feature extraction and recognition, and the database serves as the reference for identity validation [27]. The monitoring dashboard enables real-time supervision, allowing administrators to detect and respond to potential impersonation cases promptly.

One of the key advantages illustrated in this workflow is the system's ability to perform real-time verification without manual intervention. This significantly reduces human error and enhances operational efficiency.

Furthermore, the structured architecture demonstrates that the system is scalable and adaptable for both computer-based and online examination environments.

From an implementation perspective, the workflow confirms that SisCek is capable of operating in dynamic and large-scale scenarios without significant performance degradation. The integration of AI with system-level components ensures a seamless verification process, making the system a practical and reliable solution for enhancing examination security [28].

Overall, the results from real examination scenario testing indicate that the SisCek system operates effectively and efficiently in detecting impersonation practices. The system not only achieves high detection accuracy but also maintains fast and stable response times, making it suitable for real-time deployment. Therefore, SisCek demonstrates strong potential as a security solution for modern technology-based examination systems.

c. Comparative Analysis and Implications of the SisCek System

Following the evaluation of model performance and system testing in real examination scenarios, the next stage involves conducting a comparative analysis to assess the positioning and contribution of the SisCek system relative to existing approaches. This analysis aims to identify the system's strengths, limitations, and practical implications within real-world educational environments [29]. Such an approach is essential to explicitly demonstrate the novelty and scientific contribution of the study.

The proposed system is compared with three commonly used approaches in educational assessment systems, namely conventional CBT systems, online proctoring systems, and general biometric systems. The comparison is conducted based on several key aspects, including authentication methods, security level, impersonation detection capability, and system integration.

Table 4. Comparison of SisCek with Existing Systems

Aspect	Conventional CBT	Online Proctoring	Biometric Systems	SisCek
Authentication Method	Username/Password	Camera + AI	Fingerprint/Iris	Face Recognition + AI
Impersonation Detection	None	Limited	Not specific	Yes (Real-time)
Security Level	Low	Medium	High	High
System Integration	Integrated	Partial	Separate	Fully Integrated
Additional Hardware	Not required	Not required	Required	Not required

Based on Table 4, SisCek demonstrates significant advantages compared to existing approaches, particularly in terms of impersonation detection and system integration. Conventional CBT systems rely on account-based authentication, which is highly vulnerable to misuse. Online proctoring systems primarily focus on behavioral monitoring rather than identity verification [10]. Meanwhile, biometric systems such as fingerprint or iris recognition provide high security but lack practicality due to additional hardware requirements and limited integration with examination systems.

SisCek addresses these limitations by integrating *deep learning*-based face

recognition directly into the examination workflow. Its primary advantage lies in its ability to perform real-time identity verification without requiring additional hardware, making it both practical and efficient [30]. Furthermore, full integration with the examination system enables continuous identity verification before and during the exam, significantly enhancing system security. In addition to system-level comparison, a comparative analysis with previous research is conducted to highlight the technical contribution of SisCek. The results are presented in Table 5.

Table 5. Comparison of SisCek with Previous Studies

Study	Focus Area	Technology	Strengths	Limitations
Putra et al [9]	Face recognition in CBT	FaceNet	High accuracy	Not real-time
Phillips et al [31]	Online proctoring	CNN	Behavioral monitoring	No identity verification
Chirumamilla et al [32]	Cheating detection	AI behavior analysis	Complex analysis	No authentication
SisCek (This Study)	Impersonation detection	CNN + Embedding	Real-time + integrated	Dependent on image quality

Table 5 shows that previous studies tend to separate behavioral analysis and identity verification into distinct approaches. For instance, Hsu and Chen [33] achieved high accuracy using face recognition in CBT systems but did not support continuous real-time verification. Meanwhile, Cooper [34] and Dharanya et al [35] focused on behavioral detection without directly verifying identity.

SisCek introduces a more comprehensive approach by integrating real-time identity verification into the examination system. This represents the primary novelty of this study, as it combines both technical and system-level innovation. By addressing both identity verification and system integration simultaneously, SisCek overcomes key limitations found in prior research.

Furthermore, an analysis of the implementation implications of SisCek is conducted, focusing on academic integrity, operational efficiency, scalability, and user experience. The results are presented in Table 6.

Table 6. Implementation Implications of SisCek System

Aspect	Positive Impact	Challenges	Impact Level	Mitigation Strategy
Academic Integrity	Reduces impersonation significantly	User adaptation	High	Training and system familiarization
Operational Efficiency	Automates identity verification	Infrastructure requirements	High	System optimization and cloud integration
System Scalability	Applicable to large-scale environments	Computational load	Medium	Distributed computing and load balancing
User Experience	Fast and contactless verification	Environmental sensitivity	Medium	Lighting adjustment and camera optimization

Based on Table 6, the implementation of SisCek provides substantial benefits in improving academic integrity by significantly reducing impersonation practices. This aligns

with findings by Bucciol et al [36] , which emphasize the negative impact of academic cheating on educational quality and institutional credibility.

From an operational perspective, SisCek enables automation of identity verification, reducing the workload of human invigilators and improving efficiency. The system also demonstrates strong scalability potential, as it relies on widely available camera-based technology. However, challenges such as infrastructure requirements and computational load must be addressed to ensure smooth deployment.

The inclusion of impact level and mitigation strategy provides a more comprehensive evaluation of system feasibility. High-impact aspects such as academic integrity and operational efficiency directly contribute to the system's primary objectives, while medium-impact aspects such as scalability and user experience relate to long-term optimization [31]. The proposed mitigation strategies indicate that most challenges are technical in nature and can be addressed through engineering solutions, such as system optimization, distributed processing, and environmental adjustments.

In terms of user experience, SisCek offers a convenient and contactless verification process, which is more user-friendly compared to traditional biometric systems. However, system performance remains sensitive to environmental conditions, such as lighting and camera quality, which must be carefully managed in real-world implementations [32].

Overall, the comparative analysis and implementation implications demonstrate that SisCek possesses clear competitive advantages over existing approaches, both technically and operationally. By combining high model accuracy, real-time verification capability, and full system integration, SisCek provides a significant contribution to the development of AI-based examination security systems [34]. Therefore, the system shows strong potential as an innovative solution for enhancing integrity, fairness, and reliability in modern educational assessment environments.

Conclusion

This study successfully developed and evaluated the SisCek (*Sistem Pendeteksi Calo Ujian*/ Exam Broker Detection System) based on *face recognition* and *deep learning* technologies as a solution to enhance the security and integrity of technology-based examinations. The experimental results demonstrate that the proposed model achieves high accuracy with low error rates, as reflected by the *False Acceptance Rate* (FAR) and *False Rejection Rate* (FRR), both of which remain within acceptable thresholds. These findings indicate that the model is capable of accurately and consistently distinguishing between different participant identities.

The system evaluation in real examination scenarios further confirms that SisCek operates effectively in detecting impersonation practices, achieving a high detection success rate for both legitimate participants and impostors. In addition, the system performs real-time identity verification with relatively fast and stable response times, ensuring that the examination process is not disrupted. The integration of artificial intelligence, identity databases, and monitoring systems positions SisCek as a solution that is not only accurate but also practical and ready for deployment in real operational environments.

Comparative analysis results indicate that SisCek outperforms conventional approaches and previous studies, particularly in its ability to perform real-time impersonation detection and its seamless integration with examination systems. By combining both technical and system-level aspects, this study provides a significant contribution to the development of AI-based examination security systems.

Overall, SisCek demonstrates strong potential for implementation in both computer-based and online examination systems to enhance the integrity, fairness, and credibility of educational assessment processes. However, this study has certain limitations, particularly its dependence on image quality and environmental conditions. Therefore, future research is recommended to develop more robust models that can handle environmental variations and to explore integration with additional technologies, such as *liveness detection* and multimodal biometrics, to further improve system security.

Reference

[1] C. Chookhampaeng, C. Kamha, and S. Chookhampaeng, "Problems and Needs Assessment to Learning Management of Computational Thinking of Teachers at the Lower Secondary Level," *Journal of Curriculum and Teaching*, vol. 12, no. 3, p. 172, May 2023, doi: 10.5430/jct.v12n3p172.

[2] L. M. Brevik, G. B. Gudmundsdottir, A. Lund, and T. A. Strømme, "Transformative agency in teacher education: Fostering professional digital competence," *Teach. Teach. Educ.*, vol. 86, p. 102875, Nov. 2019, doi: 10.1016/j.tate.2019.07.005.

[3] J. Nishchal, S. Reddy, and P. N. Navya, "Automated Cheating Detection in Exams using Posture and Emotion Analysis," in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, IEEE, Jul. 2020, pp. 1–6. doi: 10.1109/CONECCT50063.2020.9198691.

[4] H. He, Q. Zheng, R. Li, and B. Dong, "Using Face Recognition to Detect 'Ghost Writer' Cheating in Examination," 2019, pp. 389–397. doi: 10.1007/978-3-030-23712-7_54.

[5] M. Emara, N. M. Hutchins, S. Grover, C. Snyder, and G. Biswas, "Examining student regulation of collaborative, computational, problem-solving processes in openended learning environments," *Journal of Learning Analytics*, vol. 8, no. 1, pp. 49–74, 2021, doi: 10.18608/JLA.2021.7230.

[6] S. Srivastava, V. K. Tripathi, S. Tripathi, A. Samy, M. Bhat, and A. Kumar, "Real-Time Social Media Sentiment Prediction Using BERT, CNN, and LSTM Techniques," in *2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, IEEE, Mar. 2025, pp. 1–6. doi: 10.1109/IATMSI64286.2025.10985197.

[7] X. Sun, P. Wu, and S. C. H. Hoi, "Face detection using deep learning: An improved faster RCNN approach," *Neurocomputing*, vol. 299, pp. 42–50, Jul. 2018, doi: 10.1016/j.neucom.2018.03.030.

[8] X. Sun, P. Wu, and S. C. H. Hoi, "Face detection using deep learning: An improved faster RCNN approach," *Neurocomputing*, vol. 299, pp. 42–50, Jul. 2018, doi: 10.1016/j.neucom.2018.03.030.

[9] S. A. Putra, Z. Zainuddin, and M. Niswar, "Face Recognition in Mobile-Based Test Systems Using FaceNet," in

2022 8th International Conference on Education and Technology (ICET), IEEE, Oct. 2022, pp. 107–111. doi: 10.1109/ICET56879.2022.9990684.

[10] Y. S. Baso *et al.*, "Reducing Cheating in Online Exams Through the Proctor Test Model," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, 2023, doi: 10.14569/IJACSA.2023.0140139.

[11] A. H. Putri, A. Samsudin, M. G. Purwanto, and A. Suhandi, "Examination of Conceptual Change Research Over A Decade: A Bibliometric Analysis Using Science Mapping Tool," *Indonesian Journal on Learning and Advanced Education (IJOLAE)*, vol. 4, no. 3, pp. 171–190, Sep. 2022, doi: 10.23917/ijolae.v4i3.18249.

[12] Z. Oberfield, "Unionization and Street-Level Bureaucracy: An Examination of Public School Teachers in the United States," *Rev. Public Pers. Adm.*, vol. 41, no. 3, pp. 419–446, Sep. 2021, doi: 10.1177/0734371X19894376.

[13] K. P. Waterman, L. Goldsmith, and M. Pasquale, "Integrating Computational Thinking into Elementary Science Curriculum: an Examination of Activities that Support Students' Computational Thinking in the Service of Disciplinary Learning," *J. Sci. Educ. Technol.*, vol. 29, no. 1, pp. 53–64, Feb. 2020, doi: 10.1007/s10956-019-09801-y.

[14] K. Zhang, W. Zuo, Y. Chen, D. Meng, and L. Zhang, "Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising," *IEEE Transactions on Image Processing*, vol. 26, no. 7, pp. 3142–3155, Jul. 2017, doi: 10.1109/TIP.2017.2662206.

[15] G. Yang *et al.*, "Face Mask Recognition System with YOLOV5 Based on Image Recognition," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, IEEE, Dec. 2020, pp. 1398–1404. doi: 10.1109/ICCC51575.2020.9345042.

[16] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, Oct. 2020, doi: 10.1016/j.automatica.2020.109117.

[17] R. Vijayakumar, M. Poornima, S. Divyapriya, and T. Selvaganapathi, "Automated Student Attendance Tracker for End Semester Examination using Face Recognition System," in *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, Oct. 2022, pp. 1566–1570. doi: 10.1109/ICOSEC54921.2022.9952035.

[18] T. Valtonen *et al.*, "Examining pre-service teachers' Technological Pedagogical Content Knowledge as evolving knowledge domains: A longitudinal approach," *J. Comput. Assist. Learn.*, vol. 35, no. 4, pp. 491–502, Aug. 2019, doi: 10.1111/jcal.12353.

[19] A. H. S. Ganidisastra and Y. Bandung, "An Incremental Training on Deep Learning Face Recognition for M-Learning Online Exam Proctoring," in *2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, IEEE, Apr. 2021, pp. 213–219. doi: 10.1109/APWiMob51111.2021.9435232.

[20] L. Khan, A. Amjad, K. M. Afaq, and H.-T. Chang, "Deep Sentiment Analysis Using CNN-LSTM Architecture of English and Roman Urdu Text Shared in Social Media," *Applied Sciences*, vol. 12, no. 5, p. 2694, Mar. 2022, doi: 10.3390/app12052694.

[21] P. S., K. Krithivasan, P. S., and S. Sriram V.S., "Detection of Cyberattacks in Industrial Control Systems Using

Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN)," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4394–4404, Jul. 2020, doi: 10.1109/TIA.2020.2977872.

[22] N. Zeng, H. Zhang, B. Song, W. Liu, Y. Li, and A. M. Dobaie, "Facial expression recognition via learning deep sparse autoencoders," *Neurocomputing*, vol. 273, pp. 643–649, Jan. 2018, doi: 10.1016/j.neucom.2017.08.043.

[23] G. Guo and N. Zhang, "A survey on deep learning based face recognition," *Computer Vision and Image Understanding*, vol. 189, p. 102805, Dec. 2019, doi: 10.1016/j.cviu.2019.102805.

[24] E. Pranav, S. Kamal, C. Satheesh Chandran, and M. H. Supriya, "Facial Emotion Recognition Using Deep Convolutional Neural Network," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Mar. 2020, pp. 317–320. doi: 10.1109/ICACCS48705.2020.9074302.

[25] F. Santoso and A. Finn, "A Data-Driven Cyber–Physical System Using Deep-Learning Convolutional Neural Networks: Study on False-Data Injection Attacks in an Unmanned Ground Vehicle Under Fault-Tolerant Conditions," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 53, no. 1, pp. 346–356, Jan. 2023, doi: 10.1109/TSMC.2022.3170071.

[26] M. M. Masud, K. Hayawi, S. S. Mathew, T. Michael, and M. El Barachi, "Smart Online Exam Proctoring Assist for Cheating Detection," 2022, pp. 118–132. doi: 10.1007/978-3-030-95405-5_9.

[27] J. Deng, J. Guo, J. Yang, N. Xue, I. Kotsia, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 10, pp. 5962–5979, Oct. 2022, doi: 10.1109/TPAMI.2021.3087709.

[28] I. S. Jenset, K. Klette, and K. Hammerness, "Grounding Teacher Education in Practice Around the World: An Examination of Teacher Education Coursework in Teacher Education Programs in Finland, Norway, and the United States," *J. Teach. Educ.*, vol. 69, no. 2, pp. 184–197, Mar. 2018, doi: 10.1177/0022487117728248.

[29] F. Kamalov, D. Santandreu Calonge, and I. Gurrib, "New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution," *Sustainability*, vol. 15, no. 16, p. 12451, Aug. 2023, doi: 10.3390/su151612451.

[30] P. Wang, K. Coetzee, A. Strachan, S. Monteiro, and L. Cheng, "Examining Rater Performance on the CELBAN Speaking: A Many-Facets Rasch Measurement Analysis," *Canadian Journal of Applied Linguistics*, vol. 23, no. 2, pp. 73–95, Oct. 2020, doi: 10.37213/cjal.2020.30436.

[31] L. Hsu and Y.-J. Chen, "Examining teachers' technological pedagogical and content knowledge in the era of cloud pedagogy," *S. Afr. J. Educ.*, vol. 39, no. S2, pp. 1–13, Dec. 2019, doi: 10.15700/saje.v39ns2a1572.

[32] G. Cooper, "Examining Science Education in ChatGPT: An Exploratory Study of Generative Artificial Intelligence," *J. Sci. Educ. Technol.*, vol. 32, no. 3, pp. 444–452, Jun. 2023, doi: 10.1007/s10956-023-10039-y.

[33] C. Dharanya, N. Saravanan, T. Hemalatha, K. Dinesh, and M. Jagan, "Face Recognition For Exam Hall Seating Arrangement Using Deep Learning Algorithm," in *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)*, IEEE, May 2024, pp. 130–

133. doi: 10.1109/ICPCSN62568.2024.00030.
[34] A. Bucciol, S. Cicognani, and N. Montinari, "Cheating in university exams: the relevance of social factors," *Int. Rev. Econ.*, vol. 67, no. 3, pp. 319–338, Sep. 2020, doi: 10.1007/s12232-019-00343-8.
[35] P. J. Phillips *et al.*, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," *Proceedings of the National Academy of Sciences*, vol. 115, no. 24, pp. 6171–6176, Jun. 2018, doi: 10.1073/pnas.1721355115.
[36] A. Chirumamilla, G. Sindre, and A. Nguyen-Duc, "Cheating in e-exams and paper exams: the perceptions of engineering students and teachers in Norway," *Assess. Eval. High. Educ.*, vol. 45, no. 7, pp. 940–957, Oct. 2020, doi: 10.1080/02602938.2020.1719975.