Application of Biometric Technology in Academic Examinations

Qiman Huang

School of Mechanical Engineering, Tianjin University of science & technology, Tianjin 300000, China
hqm20815125549@outlook.com

Abstract. Educational examinations are critical for national talent selection. In recent years, the number of examinees has surged due to growing demands for academic advancement, professional title evaluations, and occupational qualifications. This expansion brings new management challenges, as conventional cheating—such as note-smuggling, technical violations, forged IDs, and proxy test-taking—persists despite bans. Manual verification worsens these issues, being cumbersome, time-consuming, and prone to subjective bias. Thus, curbing cheating via effective means is urgent, and biometric technology (integrating facial recognition, behavior analysis, and gaze detection) offers a solution for an anti-cheating system. The biometric framework in this study has two key functions. First, facial recognition's ultra-high-precision matching verifies examinees' identities against ID data, eliminating identity fraud (e.g., forged documents, proxy tests) at the source. Second, integrated behavior recognition and gaze tracking capture body movements and eye trajectories, enabling real-time pre-alerts for in-exam cheating (e.g., whispering, furtive glances) and overcoming traditional proctoring's latency. This research provides a rigorous theoretical basis for shifting exam administration from human-dominated to intelligent collaboration, plus feasibility analysis for technical deployment. Widespread use of this system will boost oversight precision and efficacy, safeguard exam fairness, strengthen the talent-selection mechanism's credibility, and build a more standardized, trustworthy exam ecosystem.

Keywords: Facial Recognition; Behavior Analysis; Gaze Detection; Examination.

1 Introduction

Educational examinations constitute a fundamental system for ensuring social equity and facilitating talent mobility. Their fairness maintains public trust in the talent selection mechanism. In recent years, the scale of educational examinations in China has experienced exponential growth. The annual number of examinees for occupational qualification certifications, such as the teacher qualification exam, has exceeded ten million. This expansion has not only increased the complexity of organizational management but also led to exhibiting new characteristics of diversification,

K. Subramanian (ed.), *Proceedings of the International Workshop on Advances in Deep Learning for Image Analysis and Computer Vision (IWADIC 2025)*, Advances in Computer Science Research 128,
https://doi.org/10.2991/978-94-6239-648-7_11

concealment, and technical sophistication. Traditional practices like smuggling notes and peeking coexist with the use of micro devices to transmit answers and impersonation using forged documents, posing a serious threat to the credibility of examinations.

Traditional manual verification models suffer from inherent shortcomings, including inefficiency, strong subjectivity, and missed or erroneous judgments. In-exam monitoring, which relies on human patrols, struggles to effectively address covert cheating behaviors. In this context, biometric technology, leveraging the timeliness, stability, and difficulty of counterfeiting inherent in human physiological features (e.g., face, fingerprint) or behavioral characteristics (e.g., gaze, posture), has emerged as a crucial technological support for resolving examination management difficulties. By reviewing application research on biometric technology in examination anti-cheating, this paper aims to construct a full-process technological framework encompassing "pre-examination verification, in-exam monitoring, and post-exam tracing," thereby providing a theoretical reference for the intelligent upgrading of examination management.

This paper focuses on the application of biometric technology to prevent cheating in academic examinations. It begins by highlighting the challenges stemming from the recent surge in exam participation, including the evolution of traditional cheating methods and the limitations of manual verification, thereby underscoring the need for this technology. The study then outlines the four key design principles and integration strategies for an anti-cheating system, detailing preliminary steps such as information collection and entry. Subsequently, it analyzes the application principles and practical effectiveness of three core technologies: facial recognition, behavior recognition, and gaze detection. Finally, the paper discusses the system's role in ensuring exam fairness, offers recommendations for implementation, and supports the advancement of intelligent exam management.

2 Design Principles of Examination Anti-Cheating Systems

The system design adheres to four major principles: Accuracy requires a facial comparison accuracy rate close to 100% and strict control over the misjudgment rate of behavior recognition; Efficiency ensures minimal delay; Privacy protects data security through encrypted storage, access control, and regular desensitization; Compatibility enables seamless integration with existing examination management systems and adaptation to various examination room environments. Technology integration adopts a strategy of complementary advantages. The identity verification stage implements multi-factor authentication, such as facial detection and comparison against a database. In-exam supervision integrates dual-dimensional analysis of behavior and gaze, enhancing the precision of cheating identification through data fusion.

3 Preliminary Preparation for Implementing Biometric Technology Applications

3.1 Information Collection

Information collection serves as the foundational step in the application of biometric technologies and necessitates the implementation of standardized protocols and a rigorous quality control system. Regarding the scope of collection, large-scale examinations typically prioritize facial feature extraction, whereas examinations requiring higher security levels may incorporate fingerprint or iris biometrics, with all data linked to candidates' personal information. Specific acquisition standards require that facial images be captured under uniform lighting conditions, without headwear or makeup, in a controlled examination environment equipped with consistent artificial illumination that remains unaffected by external weather or temporal variations [1]. Fingerprint acquisition necessitates specialized hardware to ensure feature completeness, with data formatted in a universally compatible manner. The collection process operates through dual online and offline channels: online via self-service mini-programs equipped with automated quality assurance mechanisms, and offline via staff-assisted terminals. Subsequently, manual random inspections are conducted to eliminate substandard samples, thereby ensuring the integrity of the database.

3.2 Information Entry

The information entry phase is centered on the construction of a secure and efficient biometric database. The database employs a distributed architecture, designed for high capacity and reliability. Data security is ensured through multi-layered encryption methodologies; biometric data is stored in encrypted form, transmission channels are protected via protocol encryption, and a stringent role-based access control mechanism is implemented to differentiate permissions among administrators, invigilators, and other stakeholders. All operations are recorded in comprehensive logs to ensure full traceability and accountability. Data integration is achieved through customized interfaces that connect the biometric database with the existing examination management system. This enables the linkage of examinee registration details with examination credentials, forming complete profiles, which are subsequently validated against public security identity databases to prevent fraudulent or duplicate registrations.

4 Biometric Recognition Technologies

4.1 Facial Recognition Technology

Facial recognition technology authenticates identity by extracting facial feature information and comparing it against pre-established database templates. Its core functionalities encompass three principal modules: face detection, feature extraction, and image matching. Guo Ming and colleagues developed an identity verification mechanism for English listening and speaking computer-based examinations that

utilizes facial recognition technology [2]. The process initiates with facial authentication during system login, followed by image capture and comparison at critical examination intervals, concluding with the real-time transmission of suspicious alerts to invigilators. Empirical results demonstrate that the system significantly strengthens anti-cheating measures, modernizes examination management, and upholds the fairness and credibility of the testing process. Wang Zongxin and collaborators designed a facial recognition-based identity verification system for examinees [3]. The system comprises a registration application, an invigilation application, and a management client. During registration, it captures candidate images, automatically detects facial regions, extracts distinctive features, and uploads the data to a cloud platform for management and examination room allocation. Invigilators may pre-download candidate data for their respective examination rooms to the invigilation client and perform identity authentication using offline facial recognition methods. Tests indicated that the system performs candidate identity verification efficiently with an accuracy rate of 99.3%. Additionally, the Seetaface facial recognition engine, proposed by Xiao Jin [4], contributes significantly to the detection of impersonation attempts.

4.2 Behavior Recognition Technology and Suspected Cheating Detection

A basis for determining whether a candidate is cheating by recognizing human behavior and detecting specified targets.

Human Pose Estimation Methods. Behavior recognition technology determines whether a candidate is engaging in cheating by analyzing human posture and conducting target detection. It relies fundamentally on human pose estimation methods, which consist of three core components: human data perception, behavior modeling, and behavior recognition. Xue Zhiyu conducted a comprehensive analysis of cheating behaviors in paperless examination settings, summarizing prevalent cheating techniques and their characteristics [5]. Moreover, an IoT-based management platform for paperless examination environments was designed, incorporating a cheating action detection model. This model autonomously monitors and analyzes the examinee's answering process, accurately identifying potential cheating behaviors. Experimental outcomes indicate that the system attains high accuracy in paperless examination contexts. Sun Xiujuan and her team integrated the YOLOv8 algorithm with the AlphaPose posture recognition model to construct an examination cheating detection system capable of rapidly identifying anomalous behaviors and accurately classifying cheating actions [6]. By refining the data structure and optimizing the network architecture—using exclusively body movement data for model training—the system became more adept at detecting cheating-related gestures, thereby improving its robustness and applicability. Experimental results reveal a practical cheating detection accuracy of approximately 95%, effectively distinguishing between normal and fraudulent behaviors, and offering substantial technical support for examination supervision. Luo Zuying and associates proposed an efficient hierarchical detection method for cheating behaviors capable of precise identification [7]. Experimental findings demonstrate that this method combines the rapid processing of 2D

Convolutional (C2D) networks with the high accuracy of C3D networks, rendering intelligent invigilation feasible.

Suspected Cheating Behavior Detection. Li Mengxiao and colleagues proposed using Alpha-Pose to obtain the real-time posture of candidates [1]. By identifying the conventional range of motion for the head and hands during normal examination states, and combining this with the real-time positions of the head and hands, the method judges whether there is suspicion of cheating. This method demonstrates good universality and can identify most exam cheating behaviors.

4.3 Gaze Detection System

Dai Chenggeng leveraged standard computer cameras to implement gaze detection technology for the purpose of examination monitoring, thereby researching and developing a novel networked surveillance system [8]. This system provides a cost-effective and efficient solution that contributes to the preservation of examination fairness and the prevention of cheating. Furthermore, Liu Xue and her research team employed gaze estimation techniques to extract structural features of the examinee's head from image frames captured in the examination environment and predict corresponding gaze locations [9]. Their methodology also incorporated face detection and object recognition algorithms. By integrating real-time gaze angle measurements and calculating the distance between the examinee and the visual target, they performed automated classification of behavior into three distinct categories: non-cheating, suspected cheating, and confirmed cheating. All relevant data pertaining to suspected and confirmed cases were systematically archived. Experimental validation demonstrated that this approach effectively filters out unrelated behavioral noise and achieves reliable detection of cheating attempts such as visual peeking. In a similar vein, Zhu Yuanzhi and colleagues applied a facial alignment technique based on HOG feature extraction and Ensemble Regression Trees (ERT) to accurately annotate facial landmarks, generate eye region masks, adaptively segment pupil boundaries, and compute both pupil position and gaze direction [10]. This visual tracking system significantly reduces dependency on specialized hardware and promotes the practical application of gaze-based monitoring in realistic testing scenarios.

5 Conclusion

This study investigates the application pathways and practical value of biometric recognition technology in examination anti-cheating contexts, focusing on the core challenges of frequent cheating incidents following the expansion of the educational examination scale and the inefficiencies of traditional manual supervision. At the technical level, facial recognition technology, utilizing engines such as Seetaface, achieves high-precision facial comparisons. From pre-examination identity verification to the capture of critical moments during the examination, it establishes an end-to-end defense against impersonation, effectively reducing document fraud and impersonation. Behavior recognition technology, employing algorithms like YOLOv8

and posture recognition models such as Alpha-Pose, focuses on the movement patterns of candidates' heads and hands. By establishing normal behavioral baselines and modeling anomalies, it accurately identifies cheating actions including whispering and item exchange. Certain systems achieve detection accuracy rates exceeding 95%, markedly decreasing the rates of missed and false judgments associated with human invigilation. The gaze detection system, accounting for specific examination room conditions, extracts candidate head features and calculates gaze angles and target distances. It classifies examination room behavior into three categories—non-cheating, suspected cheating, and confirmed cheating—successfully filters out interference from analogous behaviors, and efficiently identifies covert cheating methods such as lateral peering, through the use of HOG-based face detection and ERT algorithm regression trees for gaze analysis.

Collectively, this integrated biometric anti-cheating technology system enables end-to-end management, from pre-examination identity authentication and in-examination cheating prevention to post-examination tracing. It effectively addresses the complex coexistence of traditional and technologically sophisticated cheating methods. To facilitate more effective implementation, future efforts should focus on three critical areas: first, enhancing data security mechanisms through encrypted storage, access control, and periodic data desensitization to protect candidates' biometric privacy; second, advancing technical standardization by unifying protocols for data collection, algorithm accuracy, and interoperability to improve system compatibility; third, establishing a collaborative framework between technology and institutional systems, integrating technical safeguards with invigilator training and the refinement of examination regulations, to further reinforce examination fairness and maintain the credibility of national talent selection mechanisms.

References

1. Li, M., Wang, B., Dai, W., et al.: An intelligent detection method for cheating behavior in a standard examination environment. Information Technology and Informatization 10, 213–216 (2020)
2. Guo, M., Xu, W., Liu, X., et al.: Design of an identity verification system for computer-based English listening and speaking tests based on facial recognition technology. Information Technology and Informatization 10, 211–215 (2022)
3. Wang, Z., Jin, K., Bai, X.: Design of a candidate identity verification system based on facial recognition. Information & Computer (Theoretical Edition) 33(23), 166–169 (2021)
4. Xiao, J.: Research and implementation of an intelligent management system for in-person classrooms based on the Seetaface facial recognition engine. M.S. thesis, Jiangsu University (2019)
5. Xue, Z.: A study on cheating behavior detection in paperless examinations based on artificial intelligence. Changjiang Information and Communications 38(1), 159–161 (2025)
6. Sun, X., Fang, Y., Sun, H., et al.: Design and implementation of a cheating behavior detection system based on YOLOv8. Journal of Beijing Polytechnic 23(4), 17–22 (2024)
7. Luo, Z., Wan, Z., Li, Y.: A hierarchical detection method for cheating behaviors in examination videos. China Examinations 5, 45–52 (2023)

8. Dai, C.: Research and application of gaze detection in examination monitoring systems. M.S. thesis, Hubei University (2017)
9. Liu, X., Chen, Y., Ma, D., et al.: A cheating detection method in examinations based on gaze estimation. Journal of Taiyuan Normal University (Natural Science Edition) 21(3), 47–52, 96 (2022)
10. Zhu, Y., Lu, R., Li, J., et al.: Research on adaptive gaze detection and tracking algorithm. Computer & Telecommunication 10, 9–12, 24 (2020)