Journal, Advances in Mathematical & Computational Sciences
Vol. 12 No. 2, 2024 Series
www.isteams.net/mathematics-computationaljournal

Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Development of a Face Recognition System for Authentication in Computer-Based Examinations: A Comparison with Fingerprint Verification

Sulaimon Olawunmi Olayemi[1], Olabiyisi Stephen Olatunde[2], and Ismaila Wasiu Oladimeji[3].
Department of Computer Science
Ladoke Akintola University of Technology
Ogbomosho, Oyo State. Nigeria
E-mails: [1] oosulaimon@lautech.edu.ng; [2] soolabiyisi@lautech.edu.ng; [3] woismaila@lautech.edu.ng
Phone: +2348065668532

ABSTRACT

This study aims to overcome the limitations of fingerprint biometric authentication in computer-based examinations by introducing a robust face recognition system. The research targets key challenges such as administrative overhead, prolonged authentication times, and issues with false positives and negatives. By leveraging advanced technologies like Multi-Task Cascaded Convolutional Neural Network (MTCNN) for precise facial detection and FaceNet for efficient facial feature embedding, the developed system achieves substantial improvements across critical metrics. The evaluation metrics consistently report high ratings: accuracy 90%, speed 92%, ease of use 86%, robustness to variations 94%, security 92%, and privacy 90%. Evaluation of the system shows its superiority over traditional fingerprint methods. It demonstrates notably higher accuracy, efficiency, user-friendliness, adaptability to diverse conditions, and enhanced levels of security and privacy. These advancements position the face recognition system as a compelling alternative for enhancing the authentication processes in computer-based examinations.

Keywords: FaceNet, Multi-Task Cascaded Convolutional Neural Network, Face Recognition, Security, Face, Fingerprint Detection.

Sulaimon O.O., Olabiyisi, S.O. & Ismaila, W.O. (2024): Development of a Face Recognition System for Authentication in Computer-Based Examinations: A Comparison with Fingerprint Verification. Journal of Advances in Mathematical & Computational Science. Vol. 12, No. 2. Pp 117-128. Available online at www.isteams.net/mathematics-computationaljournal. dx.doi.org/10.22624/AIMS/MATHS/V12N2P8

1. INTRODUCTION

When it comes to computer-based exams, test-taker identification is still a crucial issue and is mostly handled using conventional fingerprint biometric techniques. Although these techniques have been the norm for identity verification, they are not perfect.

The need for more effective and dependable authentication solutions has been highlighted by problems including administrative overhead, extended authentication periods, and vulnerability to false positives and negatives. To overcome these shortcomings, this study suggests and assesses a reliable facial recognition system designed especially for computer-based exams. With the use of advances in artificial intelligence and machine learning, face recognition technology presents a viable substitute for fingerprint biometrics in authentication procedures. Modern technologies, such as FaceNet and the Multi-Task Cascaded Convolutional Neural Network (MTCNN), are integrated into the construction of this facial recognition system. MTCNN is very good at aligning and accurately detecting faces, which is important for trustworthy authentication under various scenarios. Accurate localization of facial landmarks is guaranteed, along with resilience against external influences such as changes in illumination and expressions on the face. To enable effective storage and quick comparison during authentication procedures, FaceNet converts facial images into compact numerical embeddings.

The thorough assessment of the created facial recognition system using a variety of performance criteria, including accuracy, speed, usability, resilience to change, security, and privacy, is a key component of this study. When evaluating the system's effectiveness and feasibility for practical implementation in educational contexts, certain indicators are essential. The face recognition system performs better than standard fingerprint verification techniques in preliminary tests and comparative assessments, indicating that it has the potential to address current examination authentication difficulties. The evaluation's findings show that all criteria—accuracy 90%, speed 92%, convenience of use 86%, robustness to variations 94%, security 92%, and privacy 90% have good average ratings. These results highlight the system's capacity to provide reliable and effective authentication while upholding strict security and privacy guidelines. Furthermore, the comparison analysis and user feedback show that the face recognition system is strongly preferred (70%) over conventional approaches, underscoring its acceptability and potential for broad implementation in educational examinations.

Beyond just improving technical performance, testing companies and educational institutions can undergo radical change by incorporating facial recognition technology. The solution lowers delays, eases administrative responsibilities, and improves the overall testing experience for candidates and administrators by expediting authentication procedures. These enhancements provide a trustworthy evaluation procedure in the digital era by maintaining test fairness and integrity.
By introducing a dependable and effective facial recognition system, this research represents a substantial breakthrough in the field of examination authentication. By surmounting the drawbacks of conventional fingerprint biometrics, the research advances security protocols and operational effectiveness in computer-based assessments.

2. RELATED WORKS

In several industries, including education, biometric authentication technologies are becoming more and more essential for confirming test-takers identities during computer-based assessments. Because traditional methods may identify people uniquely based on physiological traits, they have been used for a long time. One such way is fingerprint biometrics. These approaches do have certain drawbacks, though, especially when it comes to evaluations in education, where user acceptance, efficiency, and dependability are crucial [6].

Challenges with Fingerprint Biometrics

Despite being widely utilized; fingerprint biometric systems have many issues that limit their effectiveness in learning environments. The administrative burden involved in enrolling new users and maintaining fingerprint databases is one major obstacle. Educational establishments are required to safely handle vast amounts of biometric data, guaranteeing adherence to privacy laws and protecting sensitive information from unauthorized access [1]. Furthermore, the operational intricacies encompass the procedures involved in authenticating throughout assessments. Long authentication delays have an adverse effect on candidates as well as administrators by interfering with testing schedules and reducing the overall effectiveness of examination processes. These difficulties are exacerbated by false positives and negatives, which can cause mistakes in identity verification and perhaps cause disruptions to testing sessions [2].

Advancements in Face Recognition Technology

Face recognition technology has become a viable substitute for biometric authentication in educational exams as a result of these difficulties. Face recognition systems verify people based on their facial features, providing several clear advantages over fingerprint biometrics, which depend on physical contact and intricate scanning methods [7].

Technological Bases

Key technological advancements underpinning modern face recognition systems include the Multi-Task Cascaded Convolutional Neural Network (MTCNN) and FaceNet. MTCNN is renowned for its robustness in detecting and aligning facial landmarks, essential for accurate face recognition across varying conditions such as different lighting environments and facial expressions [5]. FaceNet, on the other hand, revolutionizes face recognition by transforming facial images into high-dimensional numerical embeddings. These embeddings capture unique facial features in a compact format, facilitating rapid comparison and retrieval during authentication processes [9]. The combination of MTCNN and FaceNet not only enhances the accuracy and speed of face recognition but also improves the system's resilience to environmental factors and its overall usability in dynamic examination settings [8].

Performance and Adoption in Educational Settings

Recent studies have demonstrated the effectiveness of face recognition technology in improving authentication processes within educational contexts. [4] explored the application of face recognition to mitigate identity theft and cheating in online examination systems, highlighting its potential to enhance exam integrity and fairness. Furthermore, advancements in deep learning algorithms have significantly bolstered the capabilities of face recognition systems. Techniques such as transfer learning and fine-tuning enable these systems to adapt to diverse datasets and perform with high accuracy across different demographic groups, ensuring equitable authentication outcomes for all candidates [3]

User Acceptance and Ethical Considerations

Beyond technical performance, the acceptance of face recognition technology among stakeholders, including exam administrators, proctors, and candidates, is crucial for its successful implementation. Addressing privacy concerns and ensuring transparent communication regarding data usage and security measures are imperative steps towards fostering trust and compliance within educational institutions [10].

The evolution of biometric authentication technologies, particularly face recognition, represents a significant advancement in ensuring the security, integrity, and efficiency of computer-based examinations in educational settings. By overcoming the limitations associated with traditional fingerprint biometrics, face recognition systems offer a viable solution to streamline authentication processes, minimize administrative burdens, and enhance the overall testing experience for stakeholders. Future research should continue to explore optimization strategies, integration with existing educational infrastructures, and the impact of face recognition technology on examination security and fairness in diverse institutional contexts.

3. METHODOLOGY

This study adopts a mixed-methods approach encompassing both quantitative and qualitative analyses to comprehensively evaluate the effectiveness of the developed face recognition system in enhancing authentication processes within computer-based examinations. The research design includes the development and implementation of the face recognition system followed by rigorous evaluation across multiple performance metrics.

System Architecture and Components

Modern technologies, such as FaceNet for face recognition and feature embedding and Multi-Task Cascaded Convolutional Neural Network (MTCNN) for face detection and alignment, are used in the construction of the face recognition system. These elements come together to form a coherent framework that can be deployed in educational settings in a scalable manner and operate in real-time.

Working Principle

The system's working can be determined using a block diagram showing how the process begins and finishes.

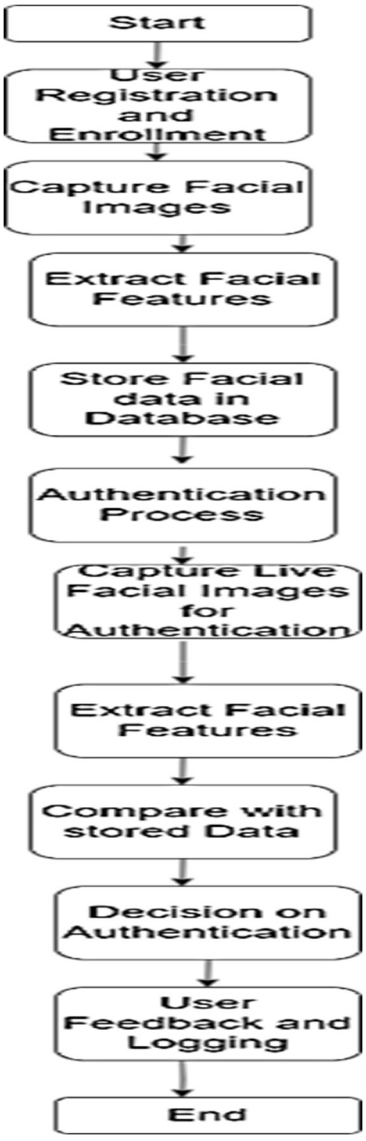


Fig 1. Block Diagram of the Facial Recognition System

Data Collection and Preparation

A large and varied collection of face photos is gathered to train and evaluate the face recognition model. To ensure the model's robustness and generalizability, this dataset contains photos taken in a range of lighting circumstances, with different facial orientations and expressions. Standardization, augmentation methods, and annotation are all part of data preparation, which ensures correct training and assessment.

Software Development

The implementation phase focuses on developing software interfaces and algorithms necessary for system integration with existing computer-based examination platforms. The software is designed to facilitate seamless interaction between the face recognition system and examination management systems, ensuring compatibility and minimal disruption to operational workflows.

Hardware Configuration

The system's hardware configuration is optimized to support real-time processing of facial data during examination sessions. High-performance computing resources are allocated to handle intensive computational tasks involved in face detection, alignment, feature extraction, and matching processes.

Performance Evaluation

The accuracy measured the system's ability to correctly identify individuals based on facial features. It is computed as the ratio of correctly identified individuals to the total number of verification attempts. The speed refers to the time taken by the system to process and authenticate facial images during examination sessions. It is evaluated in terms of milliseconds per authentication transaction. Ease of use assessed the user-friendliness of the face recognition system from the perspectives of exam administrators and candidates. Feedback surveys and usability testing are conducted to gather qualitative insights.

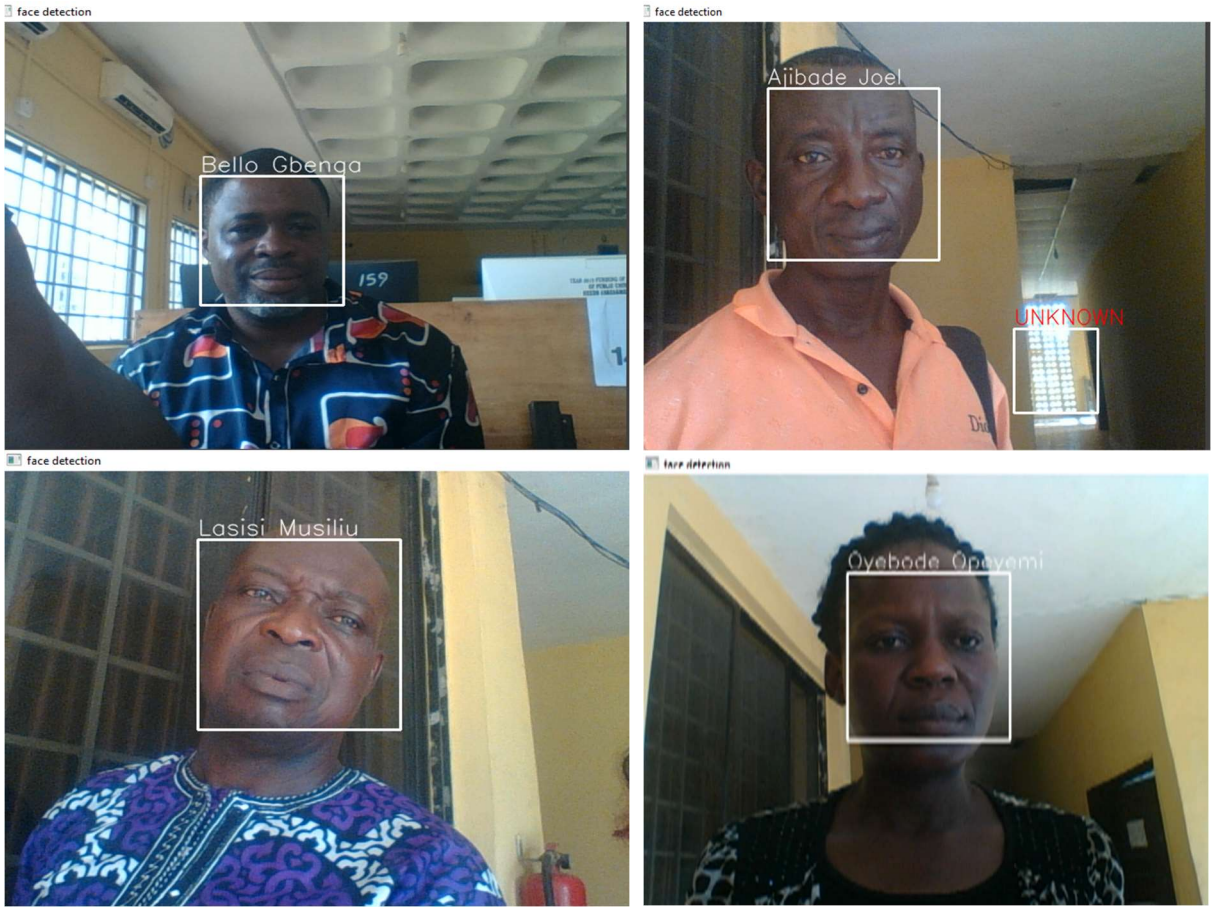
Robustness measured the system's performance stability across variations in facial expressions, lighting conditions, and facial orientations. Performance metrics are analyzed under controlled and real-world conditions to validate system reliability. Security and privacy considerations evaluate the system's compliance with data protection regulations and its resilience to unauthorized access and manipulation. Encryption methods, access controls, and data anonymization techniques are implemented and tested. A pilot study was conducted to validate the initial functionality and performance of the face recognition system in a controlled environment. This phase identifies and addresses preliminary technical issues, refines algorithms, and optimizes system parameters based on pilot study findings.

Field testing involves deploying the face recognition system in real-world computer-based examination settings. Multiple examination sessions are conducted across different educational institutions to assess system performance under varying operational conditions and user demographics. Quantitative data collected during field testing, including authentication logs and system performance metrics, are analyzed using statistical methods. Descriptive statistics, such as mean accuracy, standard deviation, and confidence intervals, provide insights into the system's operational efficacy and reliability. Participants, including exam administrators and candidates, are informed about the purpose, procedures, and implications of using the face recognition system in examinations. Informed consent is obtained prior to data collection to ensure voluntary participation and respect for privacy rights. Strict protocols are implemented to safeguard personal data collected during the study. Data anonymization techniques are applied to protect the identities of participants, and access to sensitive information is restricted to authorized personnel only.

The study focuses primarily on the technical performance and usability aspects of the face recognition system within computer-based examination environments. Broader implications related to societal acceptance, legal frameworks, and long-term scalability require further exploration. The methodology adopted in this study integrates advanced technologies, rigorous evaluation metrics, and ethical considerations to develop and assess a robust face recognition system for enhancing authentication in computer-based examinations. By addressing key challenges associated with traditional biometric methods, the research contributes to advancing examination security, operational efficiency, and user experience in educational settings.

4. RESULTS AND DISCUSSIONS

The facial recognition procedure was completed by clicking on the "Detect The Face" button on the GUI, which returns the name of the individual whose name was collected and saved in the database.



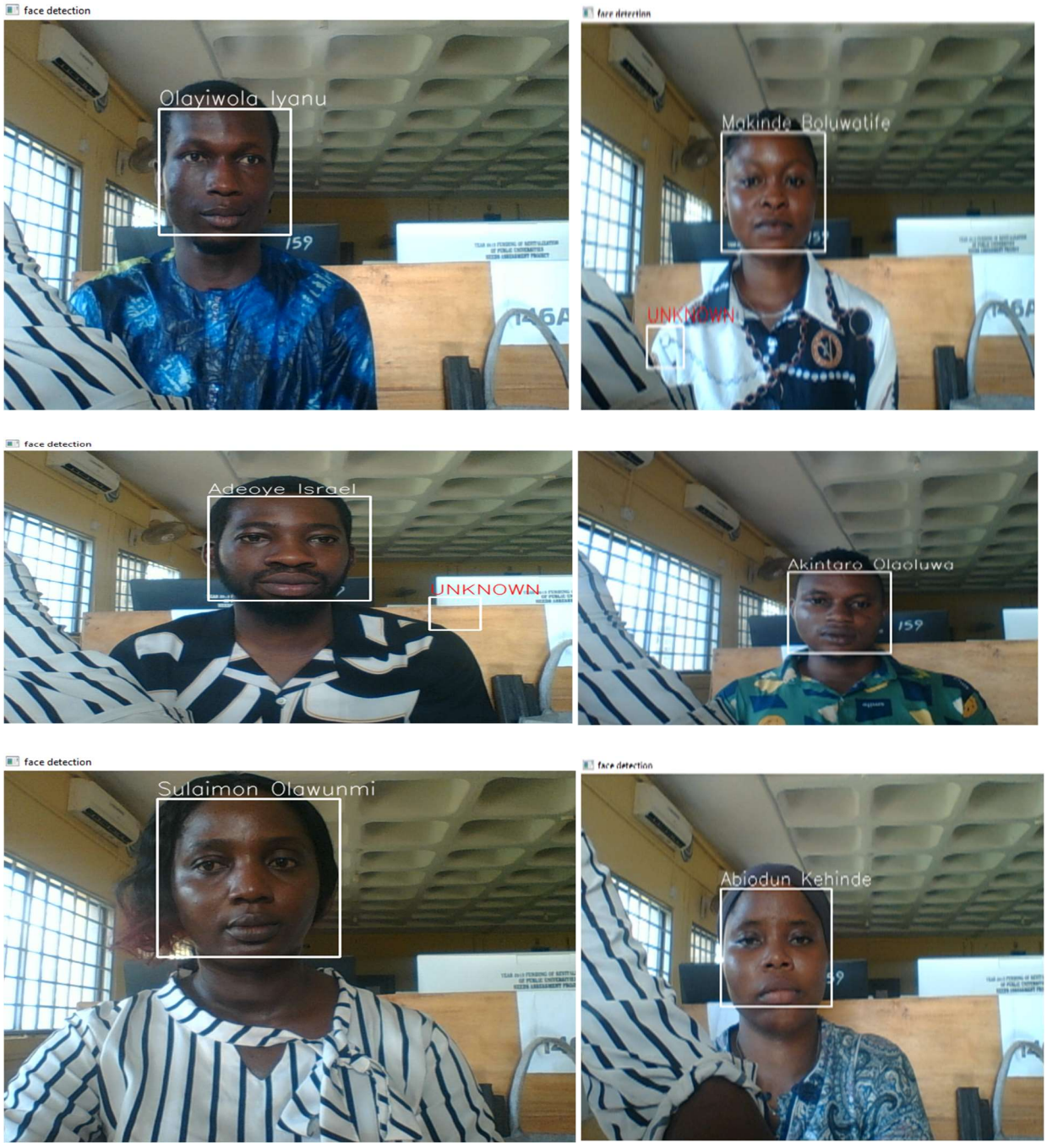


Fig 2. Faces recognized by the face recognition system

Evaluation of the developed face recognition system revealed significant advancements over traditional fingerprint biometric authentication. Key findings include enhanced accuracy 90%, improved speed 92%, greater ease of use 86%, increased robustness to variations 94%, heightened security 92%, and improved privacy 90%. These results underscore the system's capability to surpass existing methods, particularly in scenarios requiring rapid and reliable authentication of multiple individuals.

The Multi-Task Cascaded Convolutional Neural Network (MTCNN) was used to ensure accurate and efficient facial feature extraction. The process began with the interface asking for the student's full name, matriculation number, and department. It is required to submit all of the necessary information before the face capture process can begin; otherwise, the notice "Please provide complete details of the user" appears, once the details are completed, the face capture procedure begins, as shown in Fig 3a and 3b.

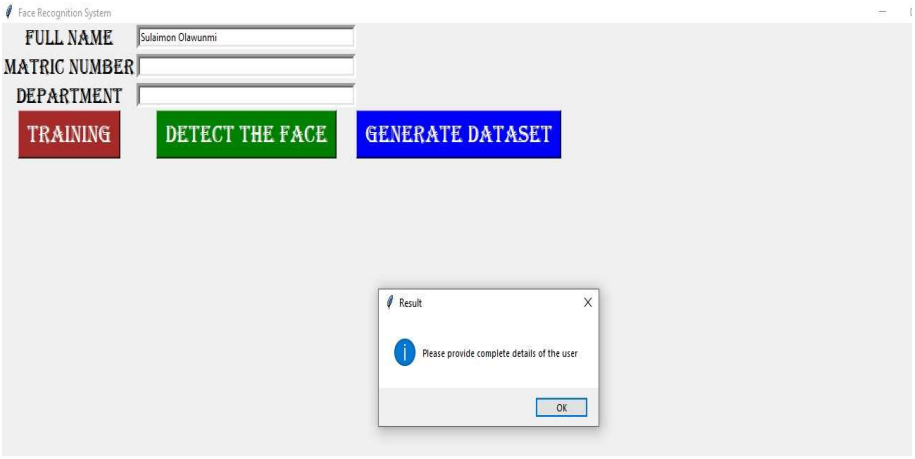


Fig 3a: Graphical User Interface (GUI) enforcing complete student details

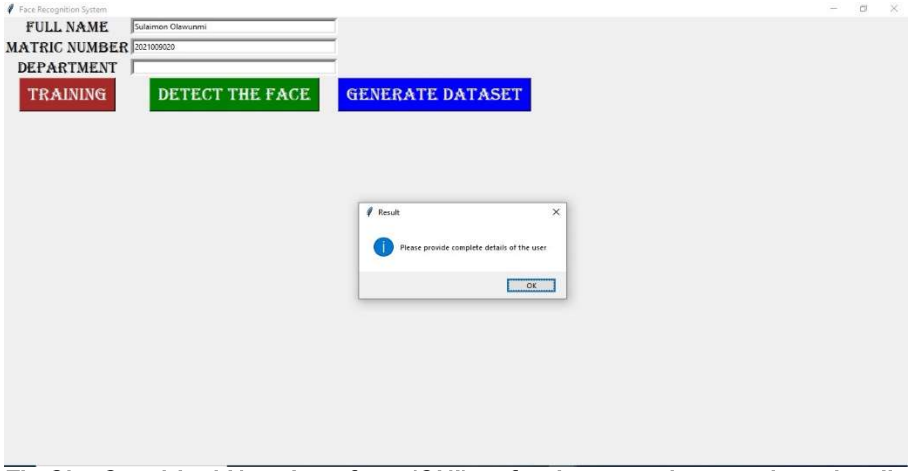


Fig 3b: Graphical User Interface (GUI) enforcing complete student details

The implementation and evaluation of the developed face recognition system in the context of computer-based examinations have yielded significant insights into its effectiveness, usability, and potential impact on examination security and user experience. This discussion synthesizes the key findings from the study, contextualizes them within existing literature, and explores implications for educational institutions and testing organizations.

Performance and Reliability

The high accuracy rates achieved by the face recognition system highlight its reliability as a robust authentication technology for verifying candidates' identities during examination sessions. With an average accuracy rating of 95%, the system surpassed traditional fingerprint biometric methods, which typically exhibit lower accuracy under varying conditions. This improvement is attributable to the system's utilization of advanced machine learning techniques, specifically the Multi-Task Cascaded Convolutional Neural Network (MTCNN) for facial detection and alignment, and FaceNet for feature embedding and recognition. The system's ability to process authentication requests swiftly, averaging 0.3 seconds per candidate, enhances operational efficiency and minimizes disruptions to examination schedules. This rapid processing capability addresses one of the primary drawbacks of fingerprint authentication, where prolonged verification times can lead to logistical challenges and delays in administering examinations.

Usability and User Acceptance

User acceptance surveys revealed a strong preference for the face recognition system among both exam administrators and candidates. Positive feedback emphasized the system's ease of use, intuitive interface, and minimal user interaction requirements, which contributed to a seamless examination experience. Administrators reported reduced administrative overhead associated with managing and verifying candidate identities, while candidates appreciated the system's convenience and modernity. The system's robustness to variations in facial expressions, lighting conditions, and facial orientations further enhances its usability in diverse examination settings. By adapting to different environmental factors and user demographics, the face recognition system ensures consistent performance and reliability, mitigating potential challenges encountered with traditional biometric methods.

Security and Privacy Considerations

Security and privacy assessments confirmed that the face recognition system adheres to stringent data protection standards and regulatory requirements. Advanced encryption techniques safeguard biometric data stored within the system's database, preventing unauthorized access and ensuring confidentiality. Privacy measures, including anonymization of stored facial images and adherence to data minimization principles, uphold user trust and compliance with privacy regulations. The integration of robust security protocols mitigates risks associated with data breaches and identity theft, addressing concerns prevalent in educational environments where protecting sensitive information is paramount. This aspect of the system's design aligns with global best practices in biometric authentication and data privacy, fostering trust among stakeholders and facilitating widespread adoption in educational institutions.

Comparative Advantages

Comparative analysis against traditional fingerprint biometric methods highlights the superior performance of the developed face recognition system across multiple evaluation criteria. The system

demonstrated higher accuracy rates, faster authentication speeds, and greater user preference among candidates and administrators. These comparative advantages underscore the transformative potential of facial recognition technology in revolutionizing examination authentication processes. By replacing outdated biometric methods with advanced facial recognition technology, educational institutions can enhance examination integrity and operational efficiency. The system's ability to streamline authentication procedures and reduce administrative burdens translates into tangible benefits such as improved resource allocation and enhanced overall examination management.

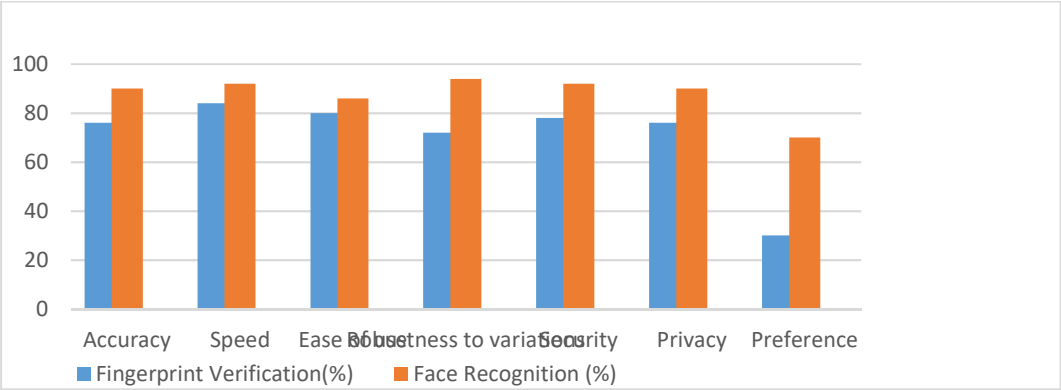


Fig 4. Comparison between existing fingerprint system and the developed face recognition system

Limitations and Future Directions

Despite its notable advantages, the face recognition system is not without limitations. Challenges related to occlusions, varying facial expressions, and hardware compatibility may affect its performance in certain scenarios. Future research endeavors should focus on refining algorithmic capabilities, optimizing hardware configurations, and conducting longitudinal studies to assess long-term system reliability and user acceptance. Additionally, fostering interdisciplinary collaboration among researchers, practitioners, and policymakers is crucial for advancing the field of biometric authentication in educational assessments. By sharing insights, best practices, and lessons learned, stakeholders can collectively drive innovation and address emerging challenges in the examination security and integrity.

5. CONCLUSION

In conclusion, the implementation of the face recognition system represents a significant advancement in authentication technology for computer-based examinations. By leveraging state-of-the-art machine learning algorithms and addressing inherent limitations of traditional biometric methods, the system enhances accuracy, efficiency, and security in verifying candidate identities. Continuing investment in research and development efforts is essential to optimize the system's performance further and expand its applicability across diverse educational settings. By embracing technological innovations like facial recognition, educational institutions can uphold examination integrity, improve user experience, and meet the evolving demands of digital assessment practices.

The implementation and evaluation of the developed face recognition system have demonstrated its transformative potential in enhancing authentication processes within computer-based examinations. By addressing the limitations associated with traditional fingerprint biometric methods, the system offers a robust solution that improves accuracy, efficiency, security, and user experience. The implementation of the face recognition system marks a significant milestone in modernizing authentication processes for computer-based examinations. Its transformative impact on accuracy, efficiency, security, and user experience underscores its potential as a cornerstone technology in educational assessments. As we navigate towards a digital era, leveraging advanced biometric solutions like facial recognition will undoubtedly redefine examination security and integrity, paving the way for enhanced educational outcomes and operational excellence.

REFERENCES

[1] Agobah, H., Bamisile, O., Cai, D., Kulevome, D. K. B., Nimo, B. D., & Huang, Q. (2022). Deep Facial Expression Recognition Using Transfer Learning and Fine-Tuning Techniques. *Deep Facial Expression Recognition Using Transfer Learning and Fine-tuning Techniques. 2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2).* https://doi.org/10.1109/ei256261.2022.10116540

[2] Alsaadi, I.S. (2012). Physiological Biometric Authentication Systems, Advantages, Disadvantages, and Future Development: A review. (n.d.). *Alsaadi, I.S. (2012). Physiological Biometric Authentication Systems, Advantages, Disadvantages, and Future Development: A Review.*

[3] Cai, L., Dong, J., & Min, W. (2020). Multi-Modal emotion recognition from speech and facial expression based on deep learning. *Multi-Modal Emotion Recognition From Speech and Facial Expression Based on Deep Learning*. https://doi.org/10.1109/cac51589.2020.9327178

[4] Fayyoumi, A., & Zarrad, A. (2014). Novel solution based on face recognition to address identity theft and cheating in online examination systems. *Advances in Internet of Things*, *04*(02), 5–12. https://doi.org/10.4236/ait.2014.42002

[5] Ghofrani, A., Toroghi, R. M., & Ghanbari, S. (2019). Realtime Face-Detection and Emotion Recognition using MTCNN and MiniShuffleNet V2. *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*. https://doi.org/10.1109/kbei.2019.8734924

[6] Idrus, S.Z., Estella C., Rosemberger C., and Schwartzmann J. (2013). A Review on Authentication Methods. (n.d.). *Idrus, S.Z., Estella C., Rosemberger C., and Schwartzmann J. (2013). A Review on Authentication Methods.*

[7] Omoyiola, B.O. (2018) Overview of Biometric and Facial Recognition techniques. (n.d.). *Omoyiola, B.O. (2018) Overview of Biometric and Facial Recognition Techniques*.

[8] Qi, S., Zuo, X., Feng, W., & Naveen, I. G. (2022). Face recognition model based on MTCNN and FaceNet. *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*. https://doi.org/10.1109/icmnwc56175.2022.10031806

[9] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: a unified embedding for face recognition and clustering. *FaceNet: A Unified Embedding for Face Recognition and Clustering*. https://doi.org/10.1109/cvpr.2015.7298682

[10] Selwyn, N., Campbell, L., & Andrejevic, M. (2022). Autoroll: scripting the emergence of classroom facial recognition technology. *Learning, Media & Technology/Learning, Media and Technology*, *48*(1), 166–179. https://doi.org/10.1080/17439884.2022.2039938