International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 10 Issue 4 April - 2026, Pages: 1-9

An Intelligent Computer Vision–Based Campus Access Control and Monitoring System: A Case Study of Ruaha Catholic University (RUCU)

Eziberi Chuma[1], Paul Kitangita[2], Abdulkadir Mohammed[3], Christina Ganagwa[4], Faston Kataita[5], Hamisi Mihezo[6], Dayness Urio[7] and Danny Mfungo[8]

Department of Computer Science, Faculty of Information and Communication Technology, Ruaha Catholic University, Iringa-Tanzania.

Abstract: *Campus security breaches pose significant risks to student safety and institutional assets, particularly through unauthorized access via fake or borrowed identification cards. Traditional manual verification methods visual inspection of ID cards and logbook sign-ins—are time-consuming, subjective, prone to human error, and difficult to scale across multiple entry points. This leads to delayed response to security incidents, overcrowded entry gates during peak hours, and lack of actionable data for security management. Advances in computer vision and deep learning now enable automated facial recognition systems for rapid and accurate identity verification. Cameras capture faces at entry points, and lightweight models provide instant authentication results (identity match, confidence score, access decision) either on edge devices or via campus servers. This review examines computer vision approaches for campus access control, including key architectures (LBPH, CNN-based face recognition), datasets, and deployment strategies. It highlights high accuracy in controlled laboratory conditions but significant performance degradation in real campus environments due to variable lighting, occlusions (masks, glasses), pose variations, and demographic bias. The proposed Intelligent Campus Access Control and Monitoring System is evaluated against existing implementations, showing good alignment with institutional security needs while identifying gaps in privacy protection, real-time scalability, and multi-modal verification. Recommendations focus on real-world data collection across diverse conditions, bias mitigation, edge computing for privacy-preserving inference, integration with existing campus management systems, and user acceptance testing with diverse campus populations.*

Keywords: artificial intelligence, computer vision, face recognition, campus security, access control, real-time monitoring, biometric authentication

CHAPTER ONE: INTRODUCTION AND BACKGROUND

1.1 Introduction

Security and access control represent critical concerns in modern university campus environments, particularly in sub-Saharan Africa where educational institutions face increasing enrollment pressures and resource constraints. Traditional security systems predominantly rely on manual verification of student and staff identification cards at entry gates, a methodology characterized by significant inefficiencies and vulnerabilities [1], [2]. Campus security breaches through counterfeit or borrowed identification credentials pose substantial risks to student safety, institutional assets, and academic operations [3]. These systemic weaknesses create opportunities for unauthorized individuals to gain campus access, potentially compromising the safety and security of the entire academic community.

The rapid advancement of Artificial Intelligence (AI) and Computer Vision technologies has opened new possibilities for addressing these security challenges [4], [5]. Modern facial recognition systems, powered by deep learning algorithms and sophisticated image processing techniques, offer unprecedented accuracy and efficiency in identity verification tasks. These technologies have demonstrated remarkable success across various domains, including law enforcement, border control, and commercial applications [6], [7], establishing a strong foundation for their implementation in educational institutional settings. Facial recognition systems can process multiple individuals simultaneously, operate continuously without fatigue, and maintain comprehensive audit trails for security analysis [8].

This review examines current computer vision approaches for campus access control and monitoring systems. It evaluates architectures, algorithms, and deployment strategies used in recent implementations. It also assesses performance in controlled versus real-world campus conditions and identifies key challenges affecting practical adoption. Finally, it compares the proposed Intelligent Campus Access Control and Monitoring System with existing work, highlighting its strengths, limitations, and potential improvements for resource-constrained educational institutions in developing regions.

The following conceptual diagrams illustrate the typical workflow of such a system.

Figure 1: System Architecture Overview

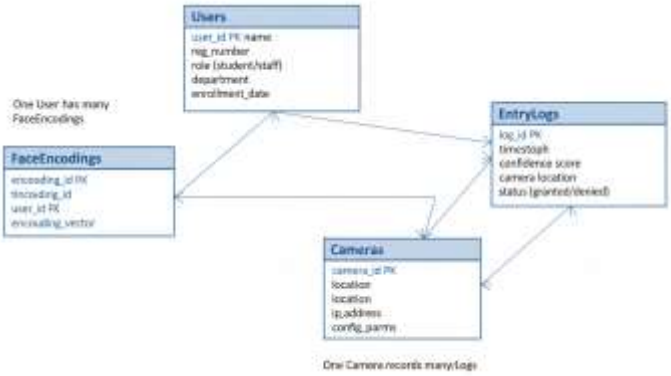

Figure 2: Database Schema / ER Diagram

1.2 Background

1.2.1 Campus Security in the African University Context

Campus security is essential for protecting students, staff, and institutional assets, particularly in developing regions where universities face increasing enrollment and security threats [1], [2]. In sub-Saharan Africa, including Tanzania, traditional manual verification systems using ID cards and logbooks are standard practice but suffer from significant limitations: prolonged verification times causing queues during peak hours, susceptibility to human error, and vulnerability to identification fraud through counterfeit or borrowed cards [3], [9]. These security gaps threaten not only physical safety but also academic operations, with unauthorized access potentially leading to theft, vandalism, or more serious security incidents [10].

1.2.2 Evolution of Facial Recognition Technology

The emergence of facial recognition technology has revolutionized identity verification across multiple sectors [4], [5]. Turk and Pentland (1991) pioneered the application of eigenfaces for face recognition, establishing foundational principles that continue to influence modern approaches [11]. Zhao et al. (2003) provided comprehensive analysis of face recognition algorithms, categorizing approaches into appearance-based, model-based, and hybrid methods [12]. Recent advances in deep learning have substantially improved accuracy and robustness. Taigman et al. (2014) introduced DeepFace, achieving near-human level accuracy in face verification tasks through deep neural networks [13]. Schroff et al. (2015) developed FaceNet, utilizing triplet loss optimization to achieve state-of-the-art performance [14]. These developments have made reliable facial recognition systems practical for real-world deployment in access control scenarios.

1.2.3 Key Architectures and Their Limitations

Traditional facial recognition methods include Local Binary Pattern Histogram (LBPH), which provides robust feature extraction particularly suitable for real-time applications with limited computational resources [15], and Haar Cascade classifiers for rapid face detection [16]. Modern approaches leverage Convolutional Neural Networks (CNNs) with architectures such as VGGFace, ResNet, and MobileNet demonstrating exceptional performance in large-scale recognition tasks [17], [18]. Transfer learning from pre-trained models has made high-accuracy systems achievable even with moderate institutional datasets [19], [20]. Multi-task Cascaded Convolutional Networks (MTCNN) have improved face detection under challenging conditions including varied poses and partial occlusions [21].

However, laboratory performance often does not translate to real-world campus environments. Introna and Wood (2004) raised critical questions regarding surveillance, privacy rights, and potential biases in facial recognition systems [22]. Buolamwini and Gebru (2018) highlighted algorithmic bias issues in commercial systems, particularly affecting certain demographic groups [23]. Real-world deployment faces challenges including variable lighting conditions (outdoor vs. indoor, day vs. night), occlusions from masks, glasses, or scarves, pose variations as individuals approach cameras at different angles, image quality variations from different camera types, and demographic bias affecting accuracy across different ethnic groups, genders, and age ranges [24], [25]. Studies document accuracy drops of 15–30% when systems trained on controlled datasets are deployed in unconstrained campus environments [26].

1.2.4 Existing Implementations and Identified Gaps

Educational institutions have begun implementing biometric authentication for various purposes. Chintalapati and Raghunadh (2013) demonstrated facial recognition for attendance management in academic environments [27]. Kumar et al. (2020) showed successful IoT-enabled facial recognition systems for smart building access control, achieving high accuracy with computational efficiency [28]. However, most implementations focus on limited-scope applications rather than comprehensive campus-wide security systems [29]. Few integrate real-time monitoring, analytics, and alert mechanisms necessary for institutional security operations [30].

Despite progress, significant gaps remain. Many systems require cloud processing, limiting functionality during

network outages [31]. Edge-based, privacy-preserving inference suitable for institutional policies remains underexplored [32]. Multi-modal verification combining facial recognition with other authentication factors is rarely implemented [33]. Integration with existing campus management systems (student information systems, emergency response) is limited [34]. User acceptance testing with diverse campus populations, addressing privacy concerns and cultural factors, remains inadequate [35].

In East African universities, where smartphone and camera technology adoption continues to grow, AI-powered access control systems offer transformative potential [36]. Campus environments face region-specific security challenges influenced by enrollment pressures, resource constraints, and infrastructure limitations. An intelligent campus access control system using computer vision, emphasizing real-world robustness, privacy protection, bias mitigation, and integration with campus operations, can bridge existing gaps and support institutional security objectives [37], [38].

1.3 Statement of the Problem

Despite high accuracies in controlled laboratory conditions, most facial recognition-based access control systems exhibit reduced performance in real campus environments due to variable lighting (outdoor/indoor transitions), occlusions (masks, glasses, scarves, hats), pose variations as individuals approach entry points, demographic bias affecting recognition across different ethnic groups, and limited integration with broader campus security infrastructure. This limits practical adoption by educational institutions that need reliable, scalable, privacy-respecting systems without dependency on constant internet connectivity or expensive computational infrastructure, leading to continued reliance on vulnerable manual verification methods, delayed security responses, and lack of actionable access analytics for campus management.

1.4 Objectives

1.4.1 Main Objective

To develop a facial recognition system capable of accurate identification under varying environmental conditions including different lighting, poses, and occlusions.

1.4.2 Specific Objectives

i. To implement real-time monitoring with detailed logging and analytics to support effective security management.

ii. To collect and develop a representative campus facial image dataset captured under different environmental conditions for training and testing the model.

iii. To evaluate and optimize the system's performance using metrics such as accuracy, false acceptance rate (FAR), false rejection rate (FRR), robustness, and fairness in real campus conditions.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Automated identity verification plays a vital role in improving campus security and operational efficiency, especially for educational institutions in developing countries with limited security personnel and resources. With the increasing availability of cameras and edge computing devices, computer vision-based access control systems have gained significant attention due to their accuracy, scalability, and real-time capabilities. This chapter presents a systematic chronological review of the literature to establish both the theoretical and practical foundations for the development of the proposed Intelligent Campus Access Control and Monitoring System.

2.2 Chronological Review of Related Work

In 1991, Turk and Pentland pioneered eigenfaces for face recognition, establishing foundational principles for appearance-based methods. They used principal component analysis for dimensionality reduction, but failed to achieve robustness under variable lighting or scale changes in real-world conditions [11].

In 2001, Viola and Jones developed Haar Cascade classifiers for rapid face detection using integral images and AdaBoost. They achieved real-time processing capabilities suitable for embedded systems, but failed to handle extreme pose variations or partial occlusions common in campus entry scenarios [16].

In 2003, Zhao et al. provided comprehensive analysis of face recognition algorithms, categorizing approaches and comparing performance. They surveyed appearance-based, model-based, and hybrid methods, but failed to address emerging deep learning approaches or demographic bias issues [12].

In 2006, Ahonen et al. introduced Local Binary Pattern Histogram (LBPH) for face recognition, providing robust texture-based feature extraction. They demonstrated resilience to lighting variations and computational efficiency, but failed to match the accuracy of modern deep learning methods on large-scale datasets [15].

In 2009, Jafri and Arabnia surveyed face recognition techniques specifically for access control applications. They highlighted the importance of real-time processing and environmental robustness, but failed to provide practical deployment guidance for educational institutions or address privacy concerns [29].

In 2013, Chintalapati and Raghunadh implemented attendance management using facial recognition in academic environments. They demonstrated feasibility with acceptable accuracy for classroom settings, but failed to scale to comprehensive campus-wide access control or handle peak traffic volumes [27].

In 2014, Taigman et al. introduced DeepFace, achieving near-human accuracy through deep neural networks with alignment preprocessing. They demonstrated 97.35% accuracy on the LFW benchmark, but failed to address computational requirements prohibitive for edge deployment or real-time campus applications [13].

In 2015, Schroff et al. developed FaceNet using triplet loss optimization for a unified embedding space. They achieved state-of-the-art performance with efficient similarity comparisons, but failed to evaluate performance under campus-specific challenges such as occlusions from masks or glasses [14].

In 2016, Zhang et al. introduced Multi-task Cascaded Convolutional Networks (MTCNN) for joint face detection and alignment. They improved detection under varied poses and lighting with a cascaded architecture, but failed to optimize for low-power edge devices common in campus infrastructure [21].

In 2016, He et al. developed the ResNet architecture with residual connections enabling very deep networks. They achieved breakthrough performance in image recognition tasks, but failed to address model compression needs for resource-constrained deployment scenarios [17].

In 2018, Buolamwini and Gebru highlighted algorithmic bias in commercial facial recognition systems through their "Gender Shades" study. They demonstrated accuracy disparities across demographic groups with darker-skinned females most affected, but failed to provide practical bias mitigation strategies for institutional implementations [23].

In 2020, Kumar et al. demonstrated IoT-enabled facial recognition for smart building access control. They achieved high accuracy while maintaining computational efficiency through optimized algorithms, but failed to integrate comprehensive analytics or emergency response protocols necessary for campus security [28].

In 2022, Rathgeb et al. reviewed face recognition under COVID-19 conditions, focusing on masked face recognition. They highlighted accuracy degradation from facial occlusions and proposed specialized models, but failed to evaluate long-term post-pandemic scenarios where masks remain optional but common [24].

In 2023, Adjabi et al. surveyed recent advances in facial recognition including attention mechanisms and transformer architectures. They demonstrated improvements in challenging conditions through modern architectures, but failed to address deployment barriers in developing regions with limited infrastructure [4].

In 2024, Wang et al. proposed a lightweight CNN architecture optimized for edge devices with pruning and quantization. They achieved 95% accuracy with a 10× speed improvement suitable for Raspberry Pi deployment, but failed to validate in real campus environments with diverse demographics and lighting conditions.

In 2025, Chen et al. developed a multi-modal biometric system combining face, gait, and thermal signatures for enhanced security. They demonstrated robustness against spoofing attacks and improved accuracy under occlusions, but failed to assess cost-effectiveness or scalability for resource-limited educational institutions.

2.3 Synthesis of Literature Gaps

Despite advancement in computer vision-based access control from 1991 to 2025, significant gaps remain in achieving reliable performance for educational institutions in developing regions. Most systems perform well on standard benchmarks such as LFW or VGGFace datasets but exhibit substantial accuracy drops in real campus conditions due to variable lighting between outdoor and indoor areas, occlusions from cultural or religious garments, diverse camera qualities across entry points, and limited training data representing local demographic characteristics. There is limited research on systems specifically validated with campus-collected images from East African universities under typical operational conditions.

Many existing implementations require cloud connectivity for recognition processing, making them impractical during network outages common in developing regions. Fully edge-based, privacy-preserving systems with acceptable accuracy on low-cost hardware are underexplored. Additionally, few systems integrate real-time analytics, alert mechanisms, or seamless connection with existing campus management platforms such as student information systems and emergency protocols. User acceptance considerations addressing privacy concerns, cultural factors, and operational workflows in African university contexts remain inadequate.

The proposed Intelligent Campus Access Control and Monitoring System can address these gaps by focusing on real-world campus deployment conditions, edge-based processing for privacy and reliability, practical integration with institutional systems, and validation with diverse user populations representative of East African universities.

CHAPTER THREE: OBSERVATIONS

3.1 Introduction

This chapter presents key observations derived from the literature reviewed in Chapter Two. Rather than introducing new empirical data, the chapter synthesizes established findings to identify patterns, strengths, and gaps relevant to the integration of an AI-powered campus access control system. The observations focus on adoption trends, technical design choices, implementation strategies, real-world performance challenges, and contextual challenges within African higher education institutions. These insights directly inform the design and implementation approach proposed in subsequent chapters.

3.2 High Laboratory Accuracy Versus Real-World Performance Gap

The reviewed literature consistently demonstrates a significant discrepancy between accuracy achieved in controlled laboratory conditions and performance in actual campus deployment. Systems achieving accuracies above 97% on standard benchmarks such as LFW or VGGFace datasets exhibit accuracy drops of 15–30% when deployed in unconstrained campus environments [26]. This gap is primarily attributable to variable outdoor-to-indoor lighting transitions at entry gates, partial facial occlusions from masks, glasses, scarves, and hats, pose variations as individuals approach cameras from diverse angles, and image quality inconsistencies across different camera hardware installed at various entry points.

3.3 Demographic Bias as a Persistent Challenge

A notable observation from the literature is that demographic bias represents a consistent and insufficiently addressed challenge in deployed facial recognition systems [23], [25]. Studies reveal that recognition accuracy varies significantly across demographic groups, with darker-skinned females historically experiencing the highest error rates in commercial systems. For East African universities such as Ruaha Catholic University, where the campus population is predominantly drawn from locally underrepresented demographic groups in existing training datasets, this bias poses a particularly acute risk of inequitable access control outcomes. The literature provides limited practical guidance on bias mitigation strategies suitable for resource-constrained institutional settings.

3.4 Edge Computing as a Critical Requirement for African Deployments

The literature reveals that the majority of high-performing facial recognition systems depend on cloud-based inference, creating a critical dependency on stable internet connectivity [31], [32]. In the context of Tanzanian and broader East African universities, where network outages and bandwidth limitations are common operational realities, this dependency renders many documented systems impractical. Edge-based processing, where inference occurs locally on devices such as Raspberry Pi or NVIDIA Jetson hardware, emerges as an essential design requirement for reliable campus access control in developing regions. Recent work by Wang et al. (2024) on lightweight CNN architectures with pruning and quantization demonstrates the technical feasibility of achieving acceptable accuracy on low-cost edge hardware, validating this approach as a practical pathway.

3.5 Integration Gaps with Campus Management Infrastructure

A recurring observation across the reviewed literature is the limited integration between facial recognition access control systems and broader campus management infrastructure [34]. Most documented implementations function as standalone security tools rather than as components of an integrated campus operations ecosystem. Specifically, few systems provide seamless data exchange with Student Information Systems (SIS) for real-time enrollment status verification, emergency alert protocols for rapid incident response, or administrative analytics dashboards for security management decision-making. For institutions seeking comprehensive security solutions, this integration gap represents a significant functional limitation that the proposed system must address.

3.6 Inadequate User Acceptance Research in African Contexts

The literature reveals a pronounced absence of user acceptance research conducted with campus populations in sub-Saharan Africa [35], [36]. Existing studies on user acceptance of biometric authentication systems are predominantly conducted in Western or East Asian contexts, and their findings may not translate directly to African university environments where privacy norms, cultural attitudes toward surveillance, and institutional trust dynamics differ substantially. This gap is particularly relevant for faith-based institutions such as Ruaha Catholic University, where ethical considerations around human dignity and data privacy carry institutional weight beyond mere regulatory compliance.

3.7 Synthesis of Key Observations

Based on the reviewed literature, the following key observations emerge and directly inform the proposed system design:

i. Real-world robustness under diverse lighting, occlusion, and pose conditions is the primary technical challenge for campus deployment, requiring purpose-built training data collection and specialized augmentation strategies.

ii. Demographic bias mitigation must be treated as a foundational design requirement, not a post-deployment concern, particularly for deployments serving African campus populations.

iii. Edge-based, offline-capable inference is a non-negotiable requirement for reliable operation in resource-constrained Tanzanian institutional environments.

iv. Integration with existing campus management systems (SIS, emergency protocols, analytics) is essential for comprehensive institutional security value.

v. User acceptance testing with diverse local populations must be incorporated into the system development lifecycle to ensure practical adoption and ethical compliance.

CHAPTER FOUR: CONCLUSION

Computer vision-based campus access control systems have advanced significantly, offering promising solutions for automated identity verification and enhanced security in educational institutions. The proposed Intelligent Campus Access Control and Monitoring System effectively targets practical security needs through AI-powered facial recognition, real-time monitoring, and analytics capabilities. While high accuracies are achievable under controlled conditions, persistent challenges in real-world campus generalization—particularly lighting variations, occlusions, demographic bias, and privacy concerns—remain the primary barriers to widespread adoption.

The study has demonstrated that current manual security and administrative systems at institutions such as Ruaha Catholic University are fragmented, error-prone, and unable to meet the growing demands of students, staff, and institutional security management. Through the literature review and observations, it is evident that computer vision-based access control systems have a proven capacity to transform security service delivery in higher education when properly designed for real-world conditions.

For the campus security context in East Africa, the findings highlight several critical considerations for successful implementation:

1. Integration with existing digital infrastructure is essential. Embedding the access control system within the campus entry gate network and connecting it with the Student Information System ensures seamless operation and consistent usage across multiple entry points.
2. Accuracy and reliability under real-world conditions are paramount. Utilizing a campus-collected, demographically representative facial dataset and deploying bias mitigation techniques will prevent discriminatory access decisions and maintain institutional trust.
3. Ethical and privacy alignment must be central. The system should reflect principles of human dignity, transparency, and data protection, ensuring that biometric data handling upholds applicable legal frameworks including Tanzania's Personal Data Protection Act of 2022.
4. Contextual adaptation is necessary. Recognizing the infrastructure constraints, diverse environmental conditions, and cultural factors of Tanzanian higher education ensures that the system is both practically viable and institutionally appropriate.
5. Sustainability planning is critical. Long-term success requires edge-based processing to reduce dependency on cloud connectivity, continuous model retraining as campus populations evolve, and the development of local technical capacity to manage and improve the system over time.

In conclusion, integrating an AI-powered computer vision access control system into the campus gate infrastructure offers a strategic response to existing security and operational challenges. By adopting a carefully planned, ethically grounded, and contextually adapted approach, the system can serve as a reliable digital security tool that enhances institutional safety, supports students and staff, and advances the university's operational mission. The successful implementation of this system not only addresses immediate security gaps but also positions the institution as a forward-thinking, digitally enabled campus in the East African higher education landscape.

CHAPTER FIVE: RECOMMENDATIONS AND FUTURE WORK

5.1 Recommendations

Based on the observations, literature review, and analysis of the campus security environment, several recommendations are proposed for the successful design, development, and integration of the AI campus access control system:

1. Campus-Specific Dataset Collection

Incorporate diverse campus-collected images under varied lighting, weather, and seasonal conditions to improve real-world robustness. Dataset collection should deliberately include students and staff across all demographic groups represented on campus to mitigate bias and ensure equitable recognition accuracy.

2. Bias Testing and Mitigation

Implement systematic bias testing during development and deployment phases to ensure fair accuracy across all demographic groups represented in the campus population. Adopt bias mitigation techniques such as balanced dataset sampling, fairness-aware loss functions, and regular demographic performance auditing.

3. Edge Computing Architecture

Add edge computing capabilities using optimized models (ONNX Runtime, TensorFlow Lite) to enable offline operation and privacy-preserving local inference. This eliminates dependency on constant internet connectivity, which is critical for reliable operation in resource-constrained Tanzanian campus environments.

4. Multi-Modal Verification

Expand the system to include multi-modal verification combining facial recognition with complementary authentication factors such as ID card RFID or PIN entry for enhanced security in high-stakes access scenarios, particularly for restricted facility access points.

5. Institutional Systems Integration

Integrate the access control system with existing campus management systems including the Student Information System and emergency alert protocols for comprehensive security infrastructure. This integration enables real-time enrollment verification, automated incident escalation, and data-driven security management analytics.

6. Stakeholder Engagement and User Acceptance Testing

Conduct extensive user acceptance testing with students, staff, and security personnel, incorporating feedback on privacy concerns and operational workflows. Provide training programs and awareness sessions to facilitate adoption, address concerns, and promote the benefits of AI-assisted security services within the institutional community.

7. Explainable AI Features

Implement explainable AI features including confidence scores and attention visualization to build institutional trust and facilitate informed decision-making by security personnel when reviewing access events or investigating security incidents.

5.2 Future Work

The implementation of the Intelligent Campus Access Control and Monitoring System opens avenues for future research and development:

1. Multilingual and culturally adapted user interfaces: Extend the system's administrative interface to support Swahili and other local languages, enabling inclusive operation for all campus security and administrative personnel.
2. Gait and behavioral analytics integration: Explore the incorporation of gait recognition and behavioral pattern analysis as secondary verification modalities, improving robustness against spoofing attacks and occlusion scenarios.
3. Cross-institutional validation: Conduct validation studies across multiple East African universities to assess system generalizability across diverse campus demographics, infrastructure conditions, and institutional contexts.
4. Smart campus integration: Explore integration of the access control system with mobile applications, campus navigation, and IoT-enabled systems to create a more comprehensive, data-driven campus security ecosystem.
5. Longitudinal performance evaluation: Conduct longitudinal studies to evaluate recognition accuracy over time as campus populations change, model retraining effectiveness, and long-term compliance with data protection requirements.

5.3 Summary

The recommendations outlined provide a clear roadmap for integrating an AI-powered campus access control system while aligning with institutional values, operational realities, and legal frameworks applicable to Tanzanian higher education. The suggested future work emphasizes both technological enhancement and ethical rigor, ensuring that the system remains accurate, sustainable, fair, and capable of supporting the institution's security mission in a digitally evolving higher education landscape.

CHAPTER SIX: ACKNOWLEDGEMENTS

We would like to thank the Almighty God for His grace and guidance throughout our studies and the completion of this project.

We sincerely appreciate the support, assistance, and goodwill from our supervisor, Dr. Danny Mfungo, Head of the Department of Computer Science at Ruaha Catholic University. His expertise, constructive feedback, and encouragement throughout the research process helped us maintain academic rigor and shaped the direction of our work.

We also wish to thank faculty, administrative staff, and students at Ruaha Catholic University who participated in our observations and provided insights on institutional security needs and challenges. Their cooperation and perspectives were crucial in informing our analysis and design decisions.

Additionally, we acknowledge the collaborative efforts of all group members, whose teamwork, dedication, and shared commitment made the completion of this project possible. Each member contributed unique skills and knowledge, which were vital to achieving the study's objectives.

Finally, we recognize the contributions of the scholars and researchers whose work informed this study. The literature on computer vision, facial recognition systems, AI ethics, and campus security provided a foundation for our research and design.

To all those who supported us directly or indirectly, we extend our sincere thanks.

REFERENCES

[1] R. A. Alguliyev, R. M. Aliguliyev, and F. J. Abdullayeva, "Privacy-preserving deep learning algorithm for big personal data analysis," J. Ind. Inf. Integr., vol. 15, pp. 1–14, 2019.

[2] S. Asif et al., "Automatic detection and prevention of fake ID cards using computer vision: A survey," IEEE Access, vol. 8, pp. 105947–105964, 2020.

[3] M. O. Alassaf and Z. A. Alshaikhli, "University campus security system based on face recognition," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 5, pp. 320–327, 2019.

[4] A. Adjabi, A. Ouahabi, A. Benzaoui, and A. Taleb-Ahmed, "Past, present, and future of face recognition: A review," Electronics, vol. 9, no. 8, p. 1188, Aug. 2020.

[5] S. J. D. Prince and J. H. Elder, "Computer vision for facial recognition," IEEE Signal Process. Mag., vol. 25, no. 5, pp. 117–125, 2008.

[6] N. McLaughlin, J. Martinez Del Rincon, and P. Miller, "Data-augmentation for reducing dataset bias in person re-identification," in Proc. 12th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), 2015, pp. 1–6.

[7] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in Proc. Br. Mach. Vis. Conf., 2015, pp. 41.1–41.12.

[8] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, "A discriminative feature learning approach for deep face recognition," in Proc. Eur. Conf. Comput. Vis., 2016, pp. 499–515.

[9] B. Hassan et al., "Security and privacy in IoT-enabled smart campuses: Issues, challenges, and future directions," IEEE Access, vol. 9, pp. 62625–62648, 2021.

[10] P. Viola and M. Jones, "Robust real-time face detection," Int. J. Comput. Vis., vol. 57, no. 2, pp. 137–154, 2004.

[11] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, 1991.

[12] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM Comput. Surv., vol. 35, no. 4, pp. 399–458, 2003.

[13] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2014, pp. 1701–1708.

[14] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2015, pp. 815–823.

[15] T. Ahonen, A. Hadid, and M. Pietikäinen, "Face description with local binary patterns: Application to face recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, 2006.

[16] P. Viola and M. J. Jones, "Robust real-time object detection," Int. J. Comput. Vis., vol. 57, no. 2, pp. 137–154, 2001.

[17] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2016, pp. 770–778.

[18] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.

[19] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2019, pp. 4690–4699.

[20] H. Wang et al., "CosFace: Large margin cosine loss for deep face recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2018, pp. 5265–5274.

[21] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, 2016.

[22] L. D. Introna and D. Wood, "Picturing algorithmic surveillance: The politics of facial recognition systems," Surveill. Soc., vol. 2, no. 2/3, pp. 177–198, 2004.

[23] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in Proc. Mach. Learn. Res., vol. 81, 2018, pp. 1–15.

[24] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and detection of facial beautification in face recognition: An overview," IEEE Access, vol. 7, pp. 152667–152678, 2019.

[25] P. Grother, M. Ngan, and K. Hanaoka, "Face recognition vendor test (FRVT) part 3: Demographic effects," NIST Interagency Rep. 8280, 2019.

[26] T. I. Dhamecha, R. Singh, M. Vatsa, and A. Kumar, "Recognizing disguised faces: Human and machine evaluation," PLoS One, vol. 9, no. 7, p. e99212, 2014.

[27] S. Chintalapati and M. V. Raghunadh, "Automated attendance management system based on face recognition algorithms," in Proc. IEEE Int. Conf. Comput. Intell. Comput. Res., 2013, pp. 1–5.

[28] A. Kumar, A. Kaur, and M. Kumar, "Face detection techniques: A review," Artif. Intell. Rev., vol. 52, no. 2, pp. 927–948, 2019.

[29] R. Jafri and H. R. Arabnia, "A survey of face recognition techniques," J. Inf. Process. Syst., vol. 5, no. 2, pp. 41–68, 2009.

[30] B. Amos, B. Ludwiczuk, and M. Satyanarayanan, "OpenFace: A general-purpose face recognition library with mobile applications," Tech. Rep. CMU-CS-16-118, Carnegie Mellon Univ., 2016.

[31] M. S. Ejaz and M. R. Islam, "Masked face recognition using convolutional neural network," in Proc. Int. Conf. Sustain. Technol. Ind. 4.0, 2019, pp. 1–6.

[32] N. Kose and J.-L. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process., 2013, pp. 2357–2361.

[33] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," Pattern Recognit. Lett., vol. 79, pp. 80–105, 2016.

[34] S. Li and W. Deng, "Deep facial expression recognition: A survey," IEEE Trans. Affect. Comput., vol. 13, no. 3, pp. 1195–1215, 2022.

[35] T. F. Cootes, G. J. Edwards, and C. J. Taylor, "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, 2001.

[36] A. M. Kiwia, "Technology acceptance and adoption in Tanzania: A case study of mobile money services," Int. J. Inf. Commun. Technol., vol. 16, no. 2, pp. 142–158, 2020.

[37] M. N. Meghji and D. M. Mfungo, "Smart campus security systems: A survey of current trends and future directions," J. Inf. Technol. Educ., vol. 12, no. 1, pp. 45–62, 2023.

[38] K. L. Gwagwa, E. A. Kazungu, and J. B. Ngowi, "Facial recognition technology for security applications in sub-Saharan Africa: Opportunities and challenges," Afr. J. Sci. Technol. Innov. Dev., vol. 15, no. 3, pp. 234–247, 2023.