Iris and Voice Signal Model for Remote Invigilation of Computer-Based Examination

Michael Olamide Gbale[1], Samuel Oluwatayo Ogunlana[2], Aliyu Ednah Olubunmi[3], Gabriel Babatunde Iwasokun[4], Olumide Olayinka Obe[5], Raphael Olufemi Akinyede[6]

[1,5]Department of Computer Science, Federal University of Technology, Akure

[2,3]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko

[3]Department of Software Engineering, Federal University of Technology, Akure

[4,6]Department of Information Systems, Federal University of Technology, Akure

DOI : https://dx.doi.org/10.47772/IJRISS.2024.8120018

Received: 03 October 2024; Accepted: 07 October 2024; Published: 27 December 2024

ABSTRACT

Computer-Based Examination (CBT) represents a growing trend in the assessment of knowledge and skills, utilizing computer technology to address many of the challenges associated with traditional, human-supervised examinations. These challenges include collusion, impersonation, unauthorized external assistance, and peeking. The research developed a comprehensive system that incorporates iris and voice recognition technologies to significantly reduce these problems, thereby enhancing the security, integrity, and reliability of the computer-based examinations. The system consists of the CBT module and the monitoring module. The CBT module includes a network infrastructure with a central server and several network-controlled workstations. The monitoring module was designed to monitor candidates in real-time and features an iris scanner that intermittently captures and analyzes the candidate's iris, triggering warnings or punitive actions if the system detects Behaviour such as peeking beyond a permissible range or other iris-related infractions. It also includes a voice processor that intermittently captures the candidate's audio signals, with similar consequences for violating audio intensity rules. The experimental study on the practical function of the system established its suitability for curtailing iris and voice-related infractions during CBT and the minimization of the costs associated with the screening, control, and management of CBT candidates.

Keywords: Computer-based examination, remote monitoring, iris recognition, face recognition, exam infraction

INTRODUCTION

An examination or test measures a candidate's knowledge, skills, abilities, or classification. It varies in structure, rigour, and requirements and can be administered orally, on paper, on a computer, or in a closed environment where candidates must complete the skills (Rovai, 2000). For instance, in a closed-book or written exam, the candidate relies on residual or memory-based knowledge to answer a particular question. In contrast, in an open-book exam or quiz, the candidate must use one or more additional tools, textbooks or calculators to answer specific questions. In the ever-evolving landscape of assessment methodologies, Computer-Based Testing (CBT) has emerged as a transformative approach, fundamentally altering how individuals are evaluated. This method, with its roots deeply embedded in the digital realm, has gained prominence owing to its efficiency, accuracy, and the unparalleled convenience it offers in the realm of examination administration (Ketab et al., 2023). Traditionally, the pen-and-paper format reigned supreme in the realm of testing. However, the advent of computer-based assessments revolutionized this age-old practice. In CBT, candidates engage with the test content through specialized software or web applications, projected onto the canvas of a computer screen. This shift from tangible to virtual reflects the progress of technology and signifies a paradigm shift in how we perceive and conduct assessments (Ketab et al., 2023). CBT is cost-

effective, swift in nature, often fortified with security features, all-inclusive and noted for high friendliness, flexibility, efficiency, accuracy, and adaptability (Iwasokun et al., 2019; Iwasokun et al., 2016; Okoro Dudu et al., 2023; Ketab et al., 2023; Potosky, 2008; Bridgeman et al., 2004). Human invigilators have been used during assessments to promote academic honesty and integrity through good identity management and the prevention of impersonation (Iwasokun et al., 2019). However, cases of connivance between human invigilators and examination takers to cheat are being reported (Sheard & Dick, 2003). Cheating refers to the Behaviour of candidates or their representatives to obtain false results by violating the examination rules and regulations. It undoubtedly reduces the reliability and integrity of examination results and scores. Many Nigerians had engaged in illegal activities at one stage or another of their education without being caught (Sheard et al., 2003). The situation is even worse in the e-learning environment with approximately 74% of students admitting to cheating during assessment because it is easier to cheat than in traditional tests (Apampa et al., 2010; Sabbah et al., 2012).

Most CBT systems that rely on human proctoring and the use of passwords, PINs, IDs, or tokens do not prevent candidates from illegal and illicit activities that could place them at any undue advantage. Such illegal activities include pimping, exchanging messages, spying on other candidates' screens, seeking external information, and other unlawful activities (Iwasokun et al., 2016). Current password or personal identification number (PIN)-based authentication, ID card or identification, and token swiping methods used to protect CBT systems are all susceptible to theft, transfer, loss, or forgetfulness. At present, most CBT centres are fitted with closed-circuit television (CCTV) which cannot provide capacity control and gives no consideration to data authenticity, confidentiality and strict access to authorized sites. This development has necessitated a growing interest in electronic invigilation (e-invigilation) or electronic proctoring (e-proctoring) through ICT-based monitoring and control of candidates during assessments. Electronic proctoring uses the Internet or intranet and other associated devices to prevent various suspicious behaviours of candidates and personnel during examinations or assessments. It is a user-centric system that monitors students with the best measures, provides security against external and internal threats, and provides controlled ability for storing, retrieving and processing (Ketab et al., 2016). Most e-invigilation systems adopt a Transparent Authentication Framework (TAF) to offer non-intrusive and unpredictable capturing, extraction and processing of biometric samples for verification and intelligent monitoring (Ketab et al., 2017; Iwasokun et al., 2019).

Online remote invigilation systems are often offered as a software-as-a-service solution that involves the preinstallation of special software that allows a third-party service provider to view or record webcam, microphone, and desktop locations during online assessment and measurements. Locked browsers are also used in some cases to prevent unauthorized access to information (Jefferies et al., 2017; Mellar et al., 2018). Online remote invigilation is an expensive, resource-intensive service and not scalable, it uses a network camera to monitor several students (Atoum et al., 2017; Fenu et al., 2018; Jefferies et al., 2017; Lilley et al., 2016). In asynchronous e-proctoring, candidates can complete assessments without a prior appointment and the evaluation process can be reviewed in real-time to provide a report flexibly. In synchronous remote invigilation, the examiner and the candidate meet virtually and concurrently during planned meeting times on a communication and collaboration platform (Atoum et al., 2017; Bedford et al., 2011; Fayyoumi et al., 2015; Hylton et al., 2016). The benefits of e-proctoring include enhanced security and convenience, cost-effectiveness, data-driven insights and global reach (Iwasokun et al., 2009; Ketab et al., 2023; Chowhan et al., 2011)

LITERATURE REVIEW

Levy and Ramin (2007) and Levy and Ramin (2009) introduced fingerprint-based theoretical models for biometric authentication in electronic-based examinations. The models offered a practical solution by integrating random fingerprint authentication for e-examinations but is susceptible to errors during instances of server downtime. Hernandez et al. (2008) developed a prototype fingerprint recognition system for student identification during electronic-based assessments. The system is integrated with a web-camera-based synchronized surveillance system to monitor student activities during exams. An experimental study of the system showed its ability to achieve recognition with high accuracy as well as its failure with network instability. Althoff et al. (2009) proposed a face and Haar-feature-based model for candidate authentication in

e-learning examinations. The Haar-feature component was used for eye detection alongside a Discrete Cosine Transformation (DCT) algorithm for the extraction of key features. An investigational study of the model established its ability to eliminate false positives through double-checking logical operations, though with increased complexity for continuous monitoring. Clark et al., (2013) adopted a Transparent Authentication System (TAS) model to e-invigilation. The model focuses on curbing impersonation, providing continuous verification, allowing identification of misuse and doing away with the requirement for specialized hardware over standardized PC hardware. Experimental study of the model justified its practical function in areas of authentication and prevention of impersonation as well as its capacity to handle voice-related infractions during CBT. Olawale et al. (2014) evaluated the current electronic examination systems in tertiary institutions in Nigeria and developed a fingerprint authentication and cryptography model for safeguarding the e-examination platform. The evaluation provided information on the staff and students' assessments of the systems and suggestions for improvement. A performance evaluation of the new model also confirmed its ability to prevent impostors from accessing the examination platform, though it experiences computational complexity. Haitham et al. (2013) proposed a model that leverages Elliptic Curve Cryptography (ECC) and multiple biometric modalities for enhancing security and reliability in computer-based examination. The model features components for biometrics enrolments, features extraction and binarization, matching and statistical analysis to achieve its objectives that include high performance. It is however faced with the challenge of limitation to 32-bit Windows platforms, the Internet Explorer (ActiveX) web browser, and a single-type operating system.

Iwasokun et al (2017) designed a fingerprint and iris-based framework for CBT invigilation. The framework comprised of modules for CBT, e-invigilation and control. The CBT module comprised of a network backbone, a server and several workstations. The e-invigilation module was designed to use high-definition and resolution iris scanners such as Iris Shield-USB MK and CMITech BMT series to capture the iris image of the candidates for processing. The system created edge points Θ_1 and Θ_2, in which when the iris is beyond these points, the system screen blinks and the admin receives a notification. The control module handles the tasks of fingerprint-based authentication of examinees with a view to making decisions on the eligibility of a candidate, process monitoring and relaying of situation reports. No consideration was given to voice-based infractions in the framework and it lacks experimental proof. Ketab et al., (2016) developed a mechanism for continuous authentication of candidates for e-assessments. The mechanism was created to monitor the exam taker and ensure that only legitimate students participated. A combination of face recognition, iris recognition, and head and eye movement formed the basis of the monitoring authentication. Depth information provided by an infrared camera was utilized as the main factor to enhance recognition and achieve continuous user identification. Facial recognition was via a peripheral F200 3D camera while voice recording was through a built-in microphone with noise-cancelation. An experimental study of the mechanism showed its ability to deliver the authentication and safety tasks with high precision, though susceptible to error. Kumar et al., (2020) developed a facial recognition model that analyzed multiple people in real-time recording scenes while writing an examination. This model relies on a face detection system that operates in real time. A Viola-Jones-related algorithm was used for face detection. The simulation of the models revealed its ability to achieve satisfactory verification, though still prone to unimodal threats.

Ojo et al., (2019) presented a face and deep learning model for CBT candidates' authentication. The model adopted image acquisition and feature extraction for the training phase, and face Recognition for the testing face. The face detector captures and stores the student face images while face recognition based on a deep learning algorithm was used to compare and match the images. The image database was based on a k-means/hierarchical algorithm model and the (expectation Maximization) EM algorithms were used to initiate and refine the database. A study of the model showed it only handles authentication with no consideration for the prevention of examination time infractions. It is established from the reviews that a significant gap is created from the limitations of the existing research works. The limitations include vulnerability to authentication or monitoring errors, authentication failures during network instability, complexity in implementing continuous invigilation, inability to process images with facial displacement or significant linearity, ineffectiveness in preventing various forms of examination malpractice, underperformance due to issues such as image corruption, and inability to detect examination time foul practices real-time. This research was therefore motivated by the need to fill the research gap by developing an iris and voice-based CBT real-

time monitoring system that addresses some of the stated limitations.

Proposed E-Invigilation Framework

The proposed e-invigilation framework intends to prevent a CBT candidate from looking at other candidates' screens as well as engaging in any voice-related. The framework is conceptualized in Figure 1 with components for computer-based tests and remote monitoring.

The computer-Based Test Module

The computer-based test module comprises a network backbone, a server and several workstations. The network requires a bandwidth with a minimum speed of 100Mbits/s for optimal performance of the server and workstation. For very reasonable computational speed at the experimentation level, Intel Xeon with specifications not below 3.6 GHz Processor and 4TB HDD for the server and 3 GHz Processor with 512 GB SSD and 128GB RAM with an iris scanner (high definition and resolution such as Iris Shield-USB MK and Citeh BMT series) and ports for audio devices are the minimal specifications.

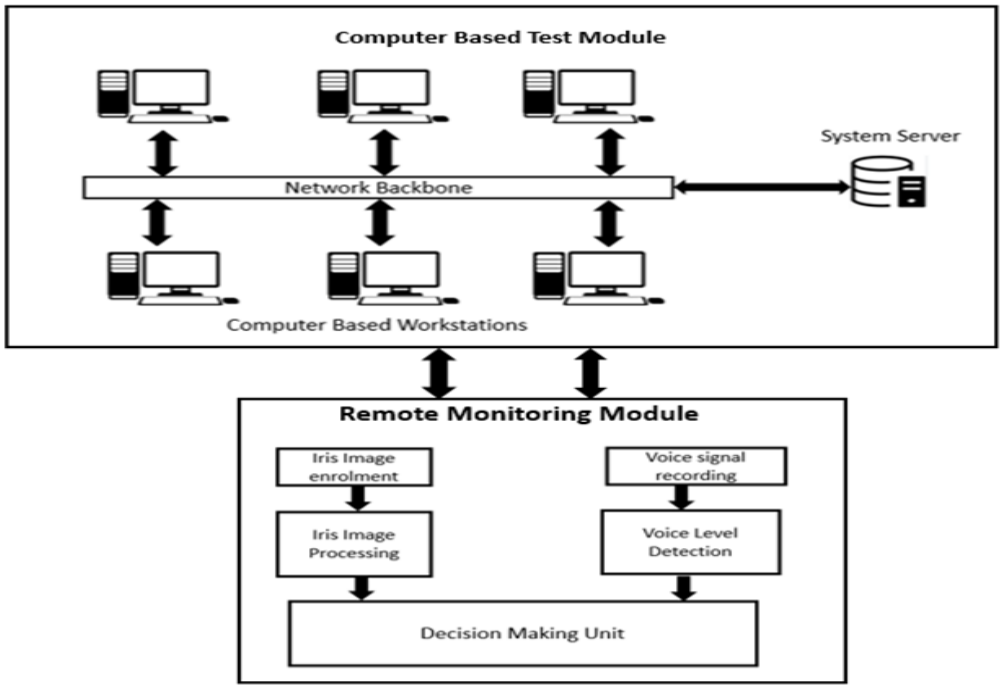

Figure 1: Conceptualization of the proposed framework

The Monitoring Module

This module consists of modules for iris and voice enrolment and processing. With a straddling iris scanner and other devices in each workstation, planned enrolments of the examination taker's iris image were carried out. The processing of the enrolled images for all the workstations takes place in synchronous mode with the measurement of the angular shift of the iris from the regular and the comparison of the measured value with the given threshold (allowable viewpoint) for both directions. The segmentation of the iris image and its feature extraction is performed with the motive of locating the inner and outer boundaries based on Daugman's intergrow-differential operator presented below (Chowhan et al., 2011):

$$\max(r, x_{0,} y_0) \left| \sigma * \frac{\partial}{\partial r} \int_{(r,\, x_0, y_0)} \frac{I(x,y)}{2\pi r} ds \right| \qquad (1)$$

r is the radius, x_o and y_o are coordinates of the canter point of image I, σ is the integration constant and x and y are the pixel values. The system setup will take cognizance of the inequality of the examinees' heights and ensure the iris scanners are mounted on stands that can be adjusted in line with the candidate's height. The

extraction of the relevant features was based on the principal component analysis method which captures local underlying information from the isolated image to yield a high-dimension feature vector (Chowhan et al., 2011). The arrows in Figure 2 illustrate the directional focus of the iris (from the binocular view) at any given time with Θ_1 and Θ_2 showing the permissible ranges. Θ_1 and Θ_2 are defined by points A and B respectively, and denote the edge points that must not be exceeded in any attempt by the candidate to look sideway from the screen. It is presumed that the exam taker is attempting to peek into another candidate's screen if the displacement angle exceeds the permissible range.

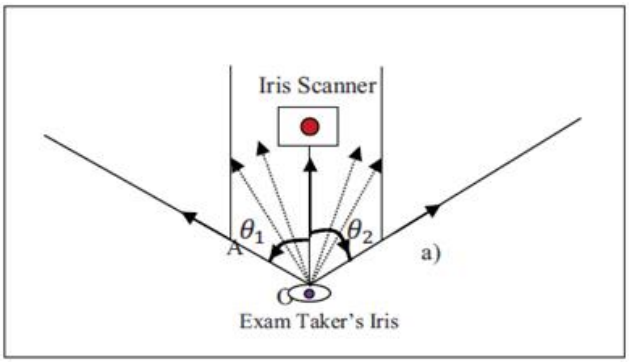

Figure 2: Examinee's angular facial displacement from the normal

The main objective of the acoustic unit is to lessen the instances of inappropriate verbal communication, thus creating a conducive atmosphere of the requisite silence required for examination purposes. This unit requires additional devices like Chrome Audio Device (CAD) and PC Audio Recorder (PAR) for enhancing the transfer of audio signals from the respective examinee through a mandatory mouthpiece or a microphone affixed to the workstations. During the processing of audio signals, the amplitude of the transmitted voice signal for every examinee is systematically compared with the pre-determined threshold. Notably, the magnitude of the vocal cord vibrations, quantified in decibels (dB), directly correlates with the energy carried by the sound wave. Consequently, a higher amplitude signifies an increased energy level within the wave, resulting in heightened intensity and audibility of the sound. The relationship between Amplitude (A) and Energy (E) carried by the sound wave is expressed as follows:

$$E = k.10^{(A/10)} \quad (2)$$

E represent the energy carried by the sound wave, K is a constant that depends on the specific, characteristics of the system. $0^{(A/10)}$ is the conversion of amplitude A from decibels to energy units If A < T, the energy E will be lower, indicating a sound within the permissible range and if A > = T, the energy will be higher, leading to noise from the candidate. If the energy E, contained within the wave exceeds the threshold, it is concluded that the candidate is practicing an unauthorized verbal exchange and appropriate measures or sanctions is promptly instituted. In addition, it is important to know that the intensity (I) of the transmitted signal tells of the rate at which energy (E) is propagated through a unit area (A), which is normal to the wave's trajectory within a medium characterized by a specified radius (r), as elucidated in Equation (3) (Felber, 2011).

$$I = \frac{E}{At} \quad (3)$$

$$A = 4\pi r^2 \quad (4)$$

For sound waves, $I \alpha P_0^2$ and $I \alpha S_0^2$. P_0 is the pressure amplitude and S_0 is the displacement amplitude. The loudness of the voice signal measured by the logarithm of the intensity against the hearing threshold intensity, I_0 is defined by Equation (5).

$$\beta = (10dB)\log(\frac{I}{I_0}) \quad (5)$$

d is the decibel which represents a tenth of a bel, and B which is used to quantify the reduction in audio level

over a specified range of transmission (Iwasokun et al, 2016). Upon the initial detection of any of the prohibited iris and voice-related infractions such as peeking or the vocal surpassing a permissible level, a warning message will be triggered in a manner visible to the exam taker. Another occurrence of any infraction will result in a temporary suspension of the examination session, marked by a brief blackout of the screen for a preset duration before the candidate is allowed to continue the examination. A third case of infraction will lead to the immediate termination of the exam taker's session and a permanent logout. The administrator will receive a notification on every instance of the infraction and the action taken towards ensuring a comprehensive oversight of the situation. To facilitate legitimate interactions between exam takers and monitoring personnel, an "attention call" protocol is provided for exam takers to call for assistance by clicking on a designated link. The monitoring personnel will respond to these calls in the order of arrival, ensuring fair and timely attention, in cases of multiple requests. Monitoring the entire CBT process requires a connection with the server to determine the total count of eligible candidates, candidates who remain logged in due to incomplete examination time, and candidates who log out after completing the allotted time. The operational flowchart of the proposed framework is presented in Figure 3.

Experimental Study

The experimental study of the model was carried out in an environment characterized by Python programming language as frontend and structured query language (SQL) as backend. The major purpose of the study was to convert the system design into source code, and each component of the design is implemented as a program module.

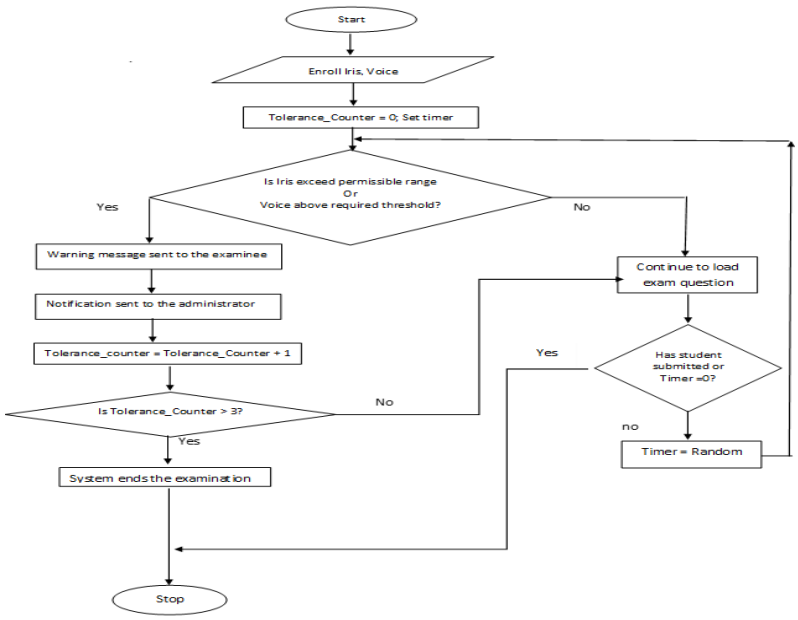

Figure 3: The operational flowchart of the proposed framework

The hardware requirements for the study include a Personal Computer with a 2.0 GHZ intel Core i3 Processor and pre-installed audio device, Iris Scanner and Microsoft HD Webcam. Intel Xeon 3.6GHz Server with 32GB RAM, Gigabit Router and Gigabit Switch also form part of the requirements. The software requirements include Windows 12, Microsoft Visual Studio, OpenCV Python, NumPy, Pyaudio, Dlib, and Pyinstaller. Microsoft Visual Studio is an Integrated Development Environment (IDE) for writing code as it supports coding in all kinds of languages including non-Microsoft languages and gives a huge number of features for software development. It was paired with C# programming language due to its wide range of support. Python also provides a powerful, open-source library for computer vision and image processing with an extensive range of tools for tasks like object detection, facial recognition, and image analysis. OpenCV is a cross-platform that works with most operating systems and programming languages to develop real-time applications. NumPy is an essential library for scientific computing in Python with a series of mathematical functions suitable for programming multi-dimensional arrays and matrices. It is widely used for numerical

computations, and data analysis, and gives foundational support to other Python scientific libraries including SciPy, pandas, and sci-kit-learn. PyAudio is a special Python library with attachments for Port Audio, which is a cross-platform audio input and output library that offers support for easy recording and playback of audio, streaming of audio data, and real-time processing of audio signals based on a straightforward API that interacts with audio hardware. Dlib is a modern C++ toolkit with machine learning algorithms and tools for creating complex software and extensive support of computer vision tasks, particularly facial recognition and landmark detection. It is suitable for the implementation of object detection, image processing, and machine learning algorithms with high accuracy and performance. PyInstaller is a robust utility dedicated to the conversion of Python scripts into standalone executable files. It also streamlines the deployment process and allows sharing of Python applications without the pre-installation of Python. Table 1 presents the configuration settings for the study.

Table 1: The configuration settings for the study

S/No	Configuration	Description	Setting
1	face_predictor_path	Pre-trained facial landmarks predictor model using dlib	shape_predictor_68_face_landmarks.dat
2	audio channels	1 means mono and 2 for stereo	Mono=1
3	audio rate	The sampling rate for audio capture in Hz	44100
4	audio chunk	The number of audio frames to process at a time. It will affect latency and processing load	2048
5	noise threshold	Used in voice detection to filter out low-level background noise. Audio data below this threshold is zeroed out.	100
6	voice threshold	The Sound Pressure Level (SPL) threshold above which voice is considered detected in decibels (dB) and can be adjusted base on environment and microphone sensitivity.	60
7	head_angle_threshold	The angle in degrees beyond which head movement is considered an infraction. It is used to control sensitivity to head movements.	20

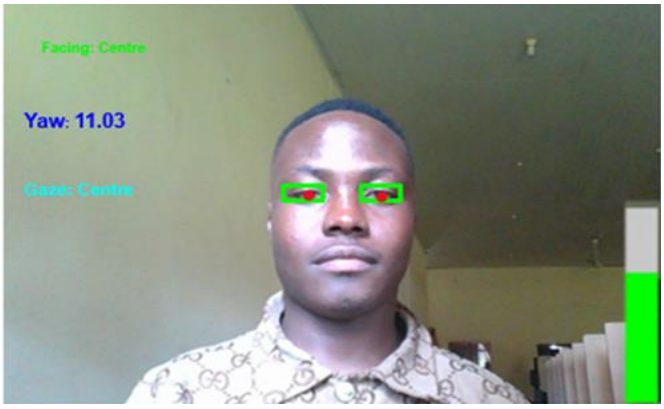

Figure 4: Iris and voice monitoring without any infraction

The system tracks both the iris and voice signals of the candidate, ensuring they are focused on the screen while the voice level remains within the defined threshold, as illustrated in Figure 4. First case of infraction is recorded as 1 of 3, the second case as 2 of 3 and the third case as 3 of 3. The image presented in Figures 5 and 6 demonstrate that face-based infractions were detected, indicating in each case that the candidate's gaze was directed outside the predefined boundaries.

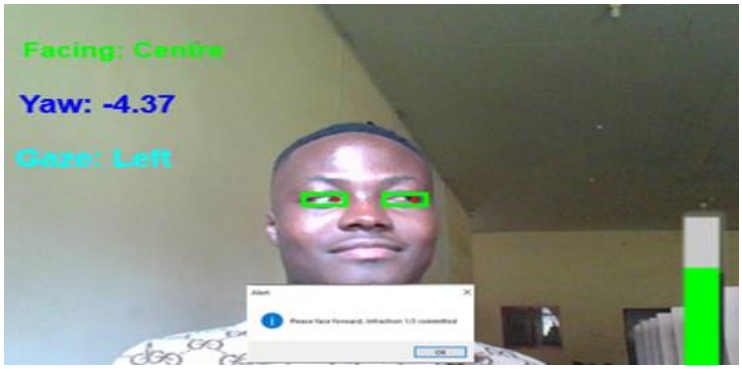

Figure 5: Candidate gazing outside the specified region with the infraction

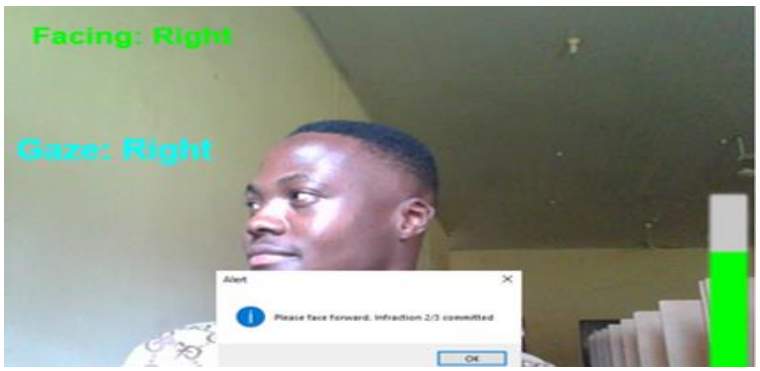

Figure 6: Candidate's gaze exceeding the outside right threshold second warning

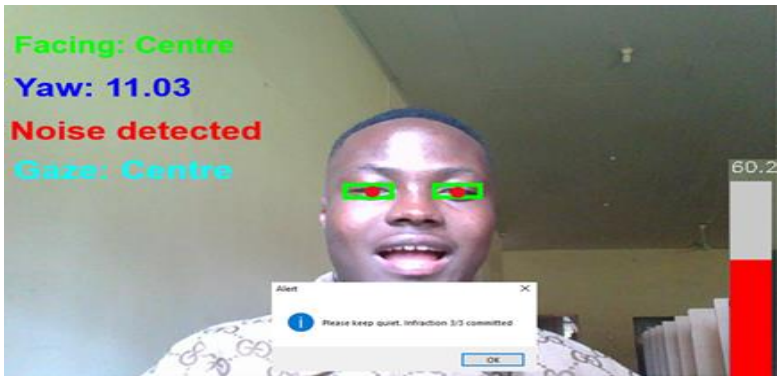

Figure 7: Third infraction committed with notification

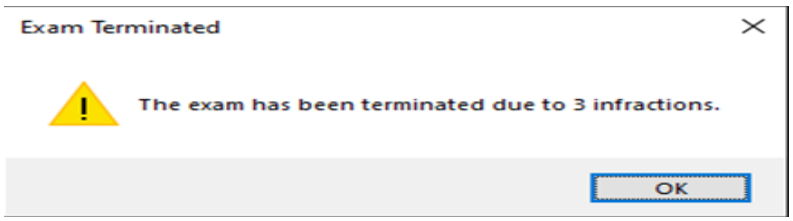

Figure 8: Termination of the candidate's exam after reaching

Figure 7 presents an infraction in which the candidate's voice level surpassed the established threshold. Accompanying this infraction is a counter indicating "3 infractions out of 3." Subsequently, Figure 8 presents a notification on the termination of the exam for the candidate due to the maximum allowable number of infractions being reached. Figure 9 details multiple cases of voice and iris infractions at different times by different candidates while interacting with the system.

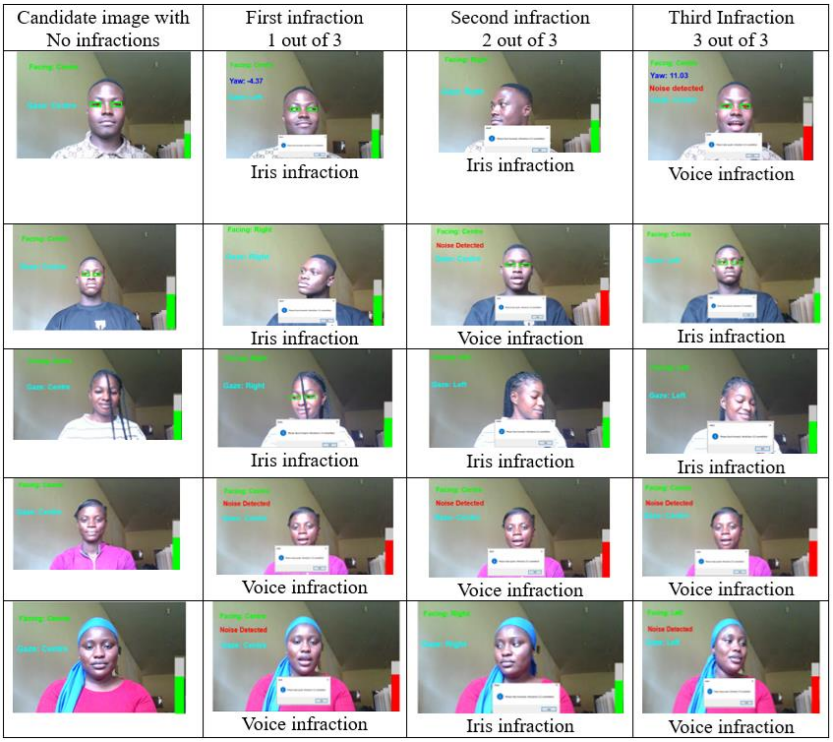

Figure 9: A number of students with infractions during the iris and voice-based

System Evaluation

The system's performance was assessed based on desired features and functionality through an online survey of 60 randomly selected participants in a pseudo-computer-based test. The participants were students from five agencies and institutions in Nigeria, namely the Joint Admissions and Matriculation Board (JAMB), Idris Premier College, Akure, Oloyemekun CBT Cenre, Akure, Adekunle Ajasin University, Akungba-Akoko, Bamidele Olomilua University, Ikere-Ekiti and The Federal University of Technology, Akure. The evaluation metrics include reliability, speed, security, effectiveness, usability, adaptability, user interface, experience, and ease of use. Based on an online questionnaire, the participants rated each metric on a five-point Likert scale (5: Excellent, 4: Good, 3: Average, 2: Fair, 1: Poor).

Table 2: Summary of the data collected through the online survey about the system pseudo exam.

	Parameters	**Excellent**	**Very Good**	**Average**	**Fair**	**Poor**
1.	To what extent did the iris-based voice system effectively monitor the test-taker's activity during the computer-based test?	20 (33.3%)	30 (50%)	10 (16.7%)	0 (0%)	0 (0%)
2	How comfortable were you using the iris-voice-based system?	18 (30%)	24 (40%)	18(30%)	0 (0%)	0 (0%)

3	How would you rate the system's impact on your test-taking experience?	18 (30%)	22 (36.7%)	20 (33.3%)	0 (0%)	0 (0%)
4	How user-friendly was the overall experience of using the iris-based voice monitoring system during the test?	17 (28.3%)	30 (50%)	13 (21.7%)	0 (0%)	0 (0%)
5	How would you rate the system's performance compared to traditional manual monitoring methods?	14 (23.3%)	25 (41.7%)	20 (33.3%)	1 (1.7%)	0 (0%)
6	How would you rate the overall user experience of the system?	12 (20%)	32 (53.3%)	15 (25%)	0 (0%)	1(1.7%)
7	How likely are you to recommend the use of this iris-based voice monitoring system for future computer-based tests?	13 (21.7%)	32 (53.3%)	15 (25%)	0 (0%)	0 (0%)

As presented in Table 2, most of the participants rated the system very good or excellent on each of the indices. On the system's ability to monitor test-taker activity, 40% of the respondents rated it 'Excellent' while one-sixth of them (16.7%) found it satisfactory ('Average'). Notably, no participants gave a "Fair" or "Poor" rating of the system on its ability to monitor the test takers. The user experience with the iris-voice system is predominantly positive as a third of the participants found the system exceptional, rating it 'Excellent', 40% of them considered it satisfactory, rating it 'Very Good' and another 30% found it acceptable, rating it 'Average'. Thirty per cent of participants rated the system's impact on test-taking experience as 'Excellent', 36.7% of them gave a 'Very Good' assessment and another 33.3% rated it 'Average' with no participant giving a ''Fare'' or 'Poor' assessment. On the system's friendliness in the on-the-spot monitoring of examination takers, 78.3%, of the respondents expressed deep satisfaction, with the rating of 'Excellent' or 'Good'. This suggests the participants had very smooth and hitch-free interactions with the system. The remaining 21.7% found the system acceptable, rating it 'Average' with no negative feedback. On the system's performance compared to traditional manual monitoring methods, 65% of the participants expressed an 'Excellent' or 'Very good' rating for the new system. This implies that most participants agreed the system did very well compared to the traditional method. 33% of them rated it 'Average' and 1.7% of them rated it 'Fair'. On the overall experience with the Iris-voice system, 73.3% of the participants expressed 'Excellent' or 'Good' feelings, 25% of them gave an 'Average' assessment with only 1.7% expressing 'Poor' feelings. 73.3% of the participants have an 'Excellent' or 'Very Good' disposition to recommend the iris-voice system for the monitoring of computer-based tests, 25% of them have an 'Average' disposition and 1.7% with 'Poor' disposition.

CONCLUSION

The conduct of computer-based examination and its resultant supervision has evolved while the use of innovative approaches has indeed been of great benefit to the effective management of an examination procedure. Stakeholders in academia and industry continually seek a platform that supports the seamless conduct of examinations. CBTs had over time brought about good resource management, space reduction and minimization of logistic time and cost. However, there is a need for precision in candidate management during examination sessions. This research implemented an iris and voice signal model as a means of addressing these concerns and establishing a seamless and remote control of computer-based examinations. The study involved a comprehensive study through various literature on examinations, computer-based tests (CBTs) and benefits,

integration of biometrics into CBTs and the various applications of biometrics-based technologies for CBT candidate authentication and control. An iris and voice model had been developed for optimizing the output and integrity of CBT. The model was designed to track the iris and voice signals of the candidate and, as a result, take punitive action when an infraction is established against the candidate. Sixty (60) participants in a CBT scenario evaluated the system and confirmed its good performance. This established that the system could serve as an application resource and be deployed on educational and non-educational agencies for the remote monitoring of computer-based examinations. For improved accuracy, further research that blends machine learning algorithms with a larger number of biometrics is recorded.

Availability of Data

Not Applicable

Competing Interests

The authors declare that there are no conflicts of interests

Funding

The support of the Nigerian government through the National Tertiary Research Trust Fund (TETFund) towards the success of this study is greatly acknowledged.

Authors Contributions

All the authors contributed to the review, documentation and proofreading

ACKNOWLEDGEMENT

The noble roles played by the Centre for Research and Development (CERAD), The Federal University of Technology, Akure, Nigeria is greatly acknowledged

REFERENCE

1. Althoff C. M, Takuya K., Nomura S., and Fukumura Y. (2009). An Access Control System for e-Learning Management Systems, Journal of Medical Informatics & Technologies, 3
2. Apampa K. M., Wills G., Argles D. (2010). Effects of Differentially Time-Consuming Tests on Computer-Adaptive Test Scores, 1(2).
3. Atoum Y., Chen L., Liu A. X., Hsu S. D, H., and Liu X (2017). Automated Online Exam Proctoring, IEEE Transactions on Multimedia, 19(7)
4. Bedford D. W., Gregg J. R., Clinton M. S. (2011). Preventing Online Cheating with Technology: A Pilot Study of Remote Proctor and an Update of Its Use, Journal of Higher Education Theory and Practice, 11(2), 41 – 59
5. Bridgeman B., Cline F. (2004). Effects of Differentially Time-Consuming Tests on Computer-Adaptive Test Scores, Wiley Online Library, 41(2).
6. Chowhan S. S., Kulkarni U. V., Shinde G. N. (2011). Iris Recognition Using Modified Fuzzy Hypersphere Neural Network with Different Distance Measures, International Journal of Advanced Computer Science and Applications, 2(6)
7. Clarke N. L. (2013). E-Invigilator: A Biometric-Based Supervision System for e-Assessments Centre for Security, Communications & Network Research, Plymouth University, United Kingdom; Security Research Institute, Edith Cowan University, Western Australia
8. 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, 4, 5-12
9. Felber F. (2011). An Automatic Volume Control for Preserving Intelligibility, Proceedings of 34th IEEE Sarnoff Symposium, Princeton, NJ, 3–4 May 2011
10. Fenu G., Marras M. and Borrato L. (2018). A multi-biometric system for continuous student

authentication in e-learning platforms", 113(8), 3-29
11. Haitham H. (2013). Discourse of Entrepreneurship in The White Tiger", ProQuest LLC
12. Hernández J. A., Ortiz A. O., Andaverde J., and Burlak G. (2008). Biometrics in Online Assessments: A Study Case in High School Students, Proceedings of the 18th International Conference on Electronics, Communications and Computers (conielecomp 2008), 2008, 111–116.
13. Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. Computers and Education, 92, 53–63
14. Iwasokun G. B, Akinyokun O. C, Alese B. K., and Olabode O. (2019), Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation, International Journal of Computer Science and Security, 5(4): 414-424
15. Iwasokun G. B, Akinyokun O. C., Angaye C. O, and Olabode O. (2012). A Multi-Level Model for Fingerprint Enhancement, Journal of Pattern Recognition Research, 7, 155-174
16. Iwasokun G. B, and Akinyokun O. C. (2016). Singular-Minutiae Points Relationship-Based Approach to Fingerprint Matching, Artificial Intelligence Research, 5(1), 78-86
17. Iwasokun G. B., Akinyede R. O., and Akinyokun O. K. (2016). Fingerprint-Based Authorization Platform for Electronic-Based Examination", Journal of Scientific Research & Reports, 2(6), 1-10
18. Jefferies M. T., Cox A. C., Shorning B. Y., Meniel V., Griffiths D. (2017). PTEN loss and activation of K-RAS and β-catenin cooperate to accelerate prostate tumorigenesis", The Journal of Pathology.
19. Ketab A. S. (2017). E-Invigilation of E-Assessments, University of Plymouth Research Theses.
20. Ketab A. S., El-Abbadi N. K. (2023). A Survey of Speech Recognition from Lip Movement", The Proceedings of the 2nd Conference for Pure and Medical Science
21. Ketab S. S., Clarke N. L., and Dowland P. S. (2016). The Value of the Biometrics in Invigilated E-Assessments, Conference Paper, 2016
22. Kumar, J. S., Spandan, G., and Kumar, N. N. (2020). Online Examination and Malpractice Detection. Journal of Xi'an University of Architecture and Technology, 12(4)), 2825-2832
23. Levy Y., and Ramim M. (2007). A Theoretical Approach for Biometrics Authentication of E-Exams, Chais Conference on Instructional Technologies Research, the Open University of Israel, Banana, Israel
24. Levy Y., and Ramim M. (2009). Initial development of a learners' ratified acceptance of multi-biometrics intentions model", Inter-disciplinary Journal of E-learning Learn. Objects, 5, 19.
25. Lilley M., Meere J., Barker T. (2016). Remote Live Invigilation: A Pilot Study, Journal of Interactive Media in Education
26. Mellar H., Peytcheva-Forsyth R., Kocdar S., Karadenis A. and Yovkova B. (2018). Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives", International Journal for Educational Integrity
27. Ojo, O., Yekini, N. A., Aigbokhan, E. E., and Onadokun, I. (2019). Deterring Malpractice in a Networked Computer Based Examination Using Biometric Control Attendance Register. International Journal of Advanced Networking and Applications, 10(06), 4061-4064.
28. Okorodudu R. I., Urien P., and Akpochafo G. O. (2023). Self Esteem as Correlation of Examination Cheating Behaviour (ECB) Among Secondary School Students in Delta State, International Journal of Novel Research and Development, 8.
29. Olawale A., Shafi'i M. A. (2014). E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity, International Journal of the Computer, the Internet and Management, 18(2)
30. Potosky D. (2008). A Conceptual Framework for the Role of the Administration Medium in the Personnel Assessment Process, Academy of Management Review, 33(3).
31. Rovai A. P. (2000). Online and Traditional Assessments: What is the Difference?", The Internet and Higher Education, 8(3)
32. Sabbah Y. Imane S., and Amira K. (2012). Synchronous Authentication with Bimodal Biometrics for e-Assessment, A Theoretical Model, Proceedings of the 6th International Conference in Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, 21-24 March 2012, 139 – 145
33. Sheard J., Dick M. (2003). Influences on Cheating Practice of Graduate in IT Courses: What are the Factors? ICCE 2003, Seoul, Korea, 2003