IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 8, August 2023

DOI: 10.17148/IJARCCE.2023.12801

LIVENESS FACIAL RECOGNITION SYSTEM FOR EXAMINATION HALL

Fatima Ahmed Abubakar[1], Atika Ahmad Jibrin[2], Ishaq Muhammad[3], Abdulrahman Abdulkarim[4], Zainab Aliyu Musa[5], Amatullah Yahaya Aliyu[6]

Lecturer, Computer Science Department, The Federal Polytechnic Bauchi, Nigeria[1-6]

Abstract The conduct of the examination is vital to the survival and reputation of that institution. Students are becoming smarter in the act of examination misconduct, therefore there is a need to curtail the act even before it occurs. Preventing the act can save a lot of resources which can then be channeled in solving other problems. Impersonation is one the disturbing examination misconduct and has proven to be difficult to eradicate. This implies bringing someone in place of the candidate to write the exam on the candidate's behalf. A security system aims to verify an individual's identity and prevent impostors from accessing protected resources. This work provides a solution to prevent the act of impersonation in examination halls. The facial liveness detection system was developed to identify candidates of a particular hall before entrance so that only the right candidates are allowed into the hall. The system also differentiated between real face (a live face) and fake face (picture or id card). When tested with 30 students, it was found to be 100% accurate.

Keywords: facial liveness detection system, facial recognition system, liveness detection, convolutional neural network.

I. INTRODUCTION

Examination as part of the evaluation in education is aimed at determining a learner's level of skill acquisition or intellectual competence and understanding after a given training [1]. An examination is considered credible only if it retains some key elements such as free, fair, devoid of partiality, cheating, and all forms of examination malpractices [2]. Examination malpractices are of major concern to any examination body. One of these problems is impersonation, where a candidate is being replaced by another to write the examination. This problem is hardly detected because of the lack of a reliable way of identifying candidates. A candidate can be identified by his/her identity card bearing his/her name, picture, and other relevant information. It has proven to be difficult in authenticating the originality of the picture in the card as fake ones can be obtained by the imposter.

A facial recognition system is one of the best ways to solve this menace, although it has its own limitations which is its inability to differentiate between real and fake or spoofed faces [3]. Face liveness detection attracts widespread consideration from many researchers who had proposed works in different sectors [4]. A real face in the physical world has a 3D structure, while a fake face from a photo or video is a 2D plane. A fake face image is easy to appear in mirror reflection and has a certain degree of shape deformation when compared with the real face. [5]. Although there are many improvements in face recognition systems, fraudsters always find a way of bridging security using fake faces.

Examination malpractice is a means by which an advantage or good grade is earned by the committers of the act implying awards confer to undeserving candidates. Undeniably, it has become a social problem for decades and the rate and manner at which performed these days advocate for a serious concern. The rate of this crime has become so widespread that there is virtually no examination anywhere at all levels and outside the formal school system that there is no one form of illegal practice or another [6]. Examination malpractices are common everywhere and every examination season witnesses the emergence of new and ingenious ways of cheating [7]. According to [8] existing examination systems are mainly concerned with image analysis techniques and biometric systems for identification, recognition, and classification of the candidates which might generally be prone to errors and easily bypassed [9], [10].

To overcome this grievous act, this research shall be carried out to produce a facial liveness detection system that can be installed in examination halls to detect genuine candidates for the examination and can also be used to identify the right candidates for the right hall. The main objective of this research work is to create a facial liveness detection system that will authenticate candidates for examination halls in The Federal Polytechnic Bauchi and can be achieved by building the image dataset which consists of real and fake face images extracted from videos; training the liveness

DOI: 10.17148/IJARCCE.2023.12801

detector network which shall be used to detect whether the person in front of the camera is alive or a picture is used and; incorporating the system to the database which will automatically create an attendance sheet for the successfully authenticated candidates.

II. METHODOLOGY

Creating the system involves data collection which involves students' information, courses, and examination halls. This can be achieved by collaborating with the ICT, exams and records, and the examination timetable committee. For each student, the live picture is taken in the form of a short video.

A CNN is then implemented using the dataset and this will be used to detect liveness. Thereafter, the network is trained using the students' dataset built. Below is the architecture of the model.

To build the liveness detector. There is the need to:

A. Build the image dataset which consists of real and fake face images extracted from videos.

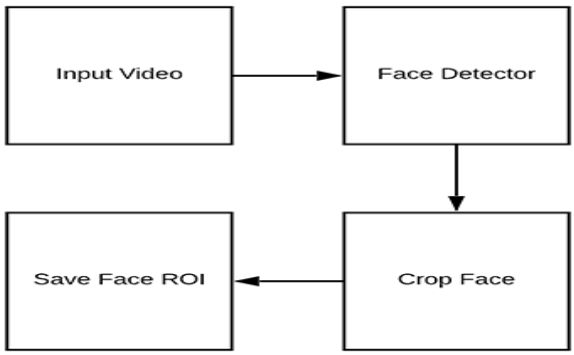

Fig. 1 Creating Dataset

To create the dataset with the faces and corresponding information of the students, there is a need to have a live image of each student. The face detector algorithm will be used to detect faces in the video and then cropped out. The corresponding image is saved with the features known as the region of interest (ROI).

B. Implement a CNN capable of performing face liveness detection.

The next stage is to train the convolutional neural network with the datasets. The convolutional layers as feature extractors learn the feature representations of the input images. Inputs are convolved with the learned weights in order to compute a new feature map, and the convolved results are sent through a nonlinear activation function. The neurons inside a feature map have equal weights but different feature maps within the same convolutional layer have different weights so that several features can be extracted at each location. More formally, the k^{th} output feature map Y_k can be computed as:

$$Y_k = f(W_k * x) \dots (1)$$

where x is the input image; the convolutional filter related to the k^{th} feature map is denoted by W_k; the multiplication sign in this context refers to the convolutional operator, which is used to calculate the inner product of the filter model at each location of the input image; and $f(\cdot)$ represents the nonlinear activation function [11].

The pooling layers are used to reduce the spatial resolution of the feature maps and thus achieve spatial invariance to input distortions and translations ([12][13].

The fully connected layers that follow these layers interpret these feature representations and perform the function of high-level reasoning [13]. For classification problems, it is standard to use the softmax operator on top of a CNN [14] – [16]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 8, August 2023

DOI: 10.17148/IJARCCE.2023.12801

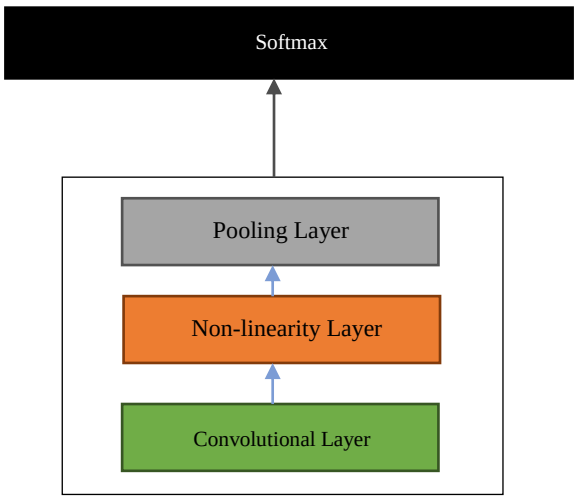

Fig. 2 CNN implementation for face liveness detection

C. Train the liveness detector network.

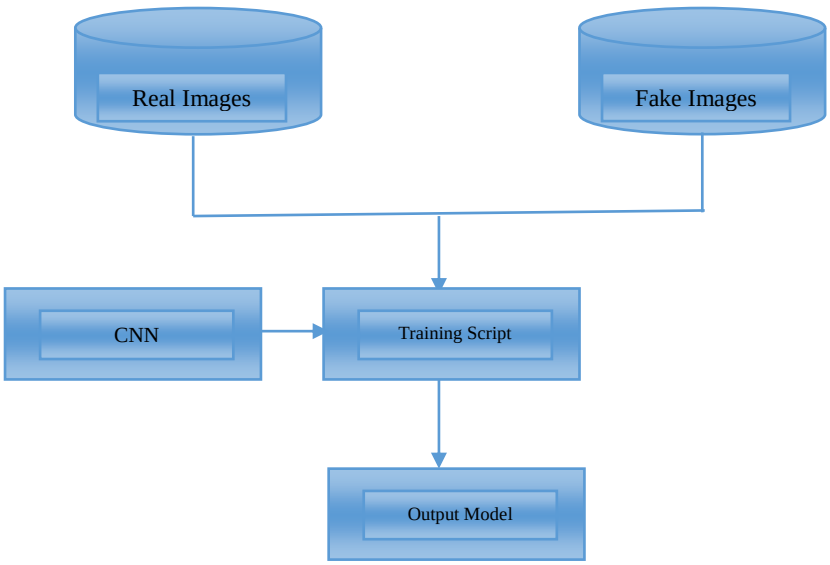

Fig. 3 Training Process

The last stage is to train the network to automatically detect the faces as either real or fake. After which the information about the student shall be the final output.

III. RESULTS AND DISCUSSION

A. Results

1) Registration and Authentication:

The Registration page of the Facial Recognition System is designed to capture students' information and images to create a database for facial recognition purposes. This page serves as a crucial step in the enrolment process, allowing administrators or authorized personnel to collect and store relevant data for each student. The "Generate Encoding" page in a facial recognition system is a crucial step in the process of creating unique facial representations, also known as face encodings, based on the captured images of individuals. These encodings serve as a numerical representation of facial features that can be used for subsequent matching and identification purposes.

The "Authenticating Students to Enter Examination Hall" page is a key component of a facial recognition system designed to verify the identity of students before granting them access to the examination hall. This page utilizes the webcam to capture the student's image in real-time and compares it with the stored facial encodings in the system's database. When students approach the entrance of the examination hall, they are directed to the Authenticating page.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 8, August 2023

DOI: 10.17148/IJARCCE.2023.12801

The page typically features the webcam interface, which is used to capture the student's face. The student will stand in front of the webcam, and the system will initiate the facial recognition process. After a successful authentication where a match is found, indicating that the student's face matches the enrolled face in the database, the system can display (Matched) as the visual indication or message to inform the student that they have been granted access to the examination hall. If the same user attempts to authenticate again after a successful attempt, the system displays a message indicating that the user has already been marked or authenticated. Figures 4-8 depict the different stages of authentication using the system.

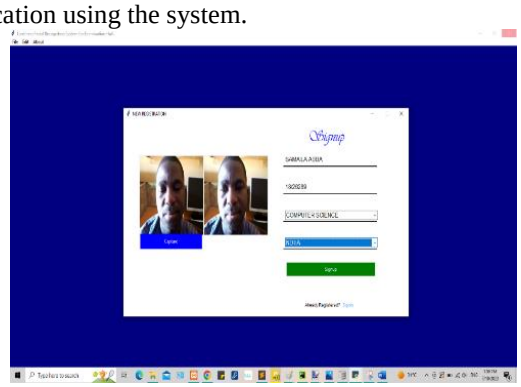

Fig. 4 Registration Page

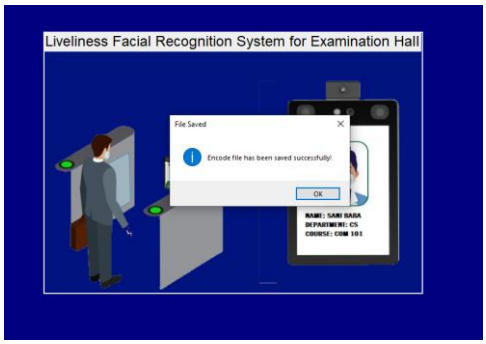

Fig. 5 Encode Generation

Fig. 6 Student Authentication Page

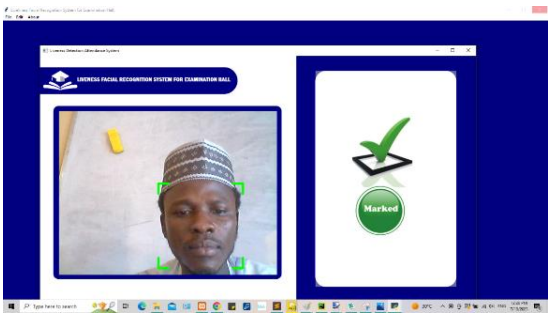

Fig. 7 Match Found

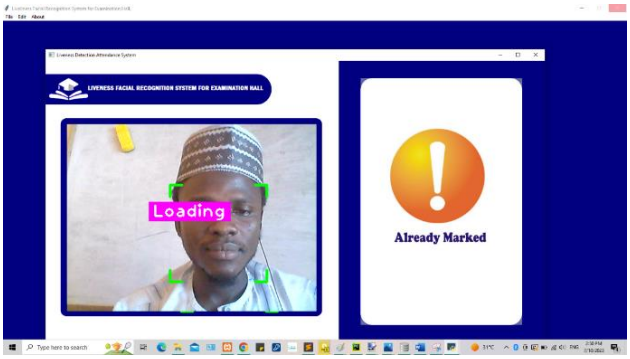

Fig. 8 Already Marked

2) Venue Mismatch:

A student at the wrong venue attempts to authenticate using the facial recognition system. The system can display a message indicating a "Venue Mismatch". This message serves as an alert to notify the student that they have attempted to access the wrong venue or location for their exam. The purpose of displaying the "Venue Mismatched" message is to prevent unauthorized access and ensure that students are directed to the correct examination venue based on their enrolment or assigned location.

3) Spoof detection:

Spoof detection refers to the capability of the system to identify and prevent spoofing attempts or fraudulent activities related. It is designed to ensure the accuracy and integrity of the system data by detecting and flagging any

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 8, August 2023

DOI: 10.17148/IJARCCE.2023.12801

unauthorized or deceptive actions. Whenever a spoof is detected, the system will display an alert saying "You are fake! Spoof detected".

Figures 9 and 10 below show the venue mismatched and spoof detection respectively.

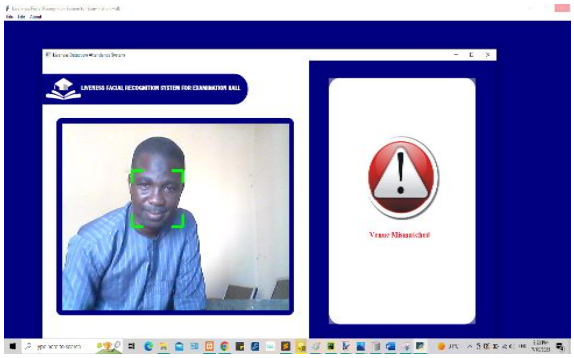

Fig. 9 Venue Mismatched

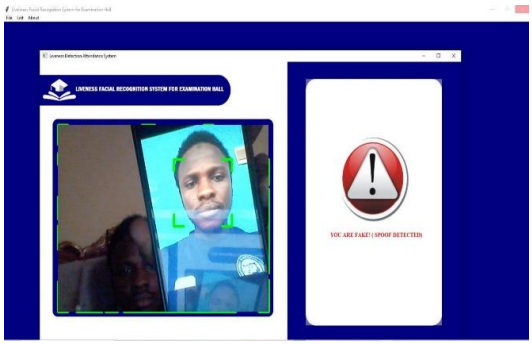

Fig. 10 Spoof Detection

4) *Settings:*

The setting page is a crucial component of the system that allows the system administrator to configure various parameters related to the examination. This page provides a user-friendly interface for the administrator to define and customize settings such as the exam hall venue, course information, and the date and time of the examination.

5) Download:

The Download page is a feature within the system that allows authorized users, such as administrators or invigilators, to download students' information along with their sign-in and sign-out details. This page provides a convenient way to access and retrieve data related to the examination process for further analysis, record-keeping, or reporting purposes. System settings and the download page are depicted below in Figures 11 and 12.

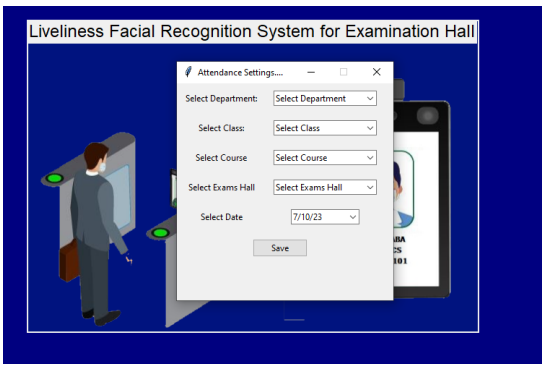

Fig. 11 System Settings

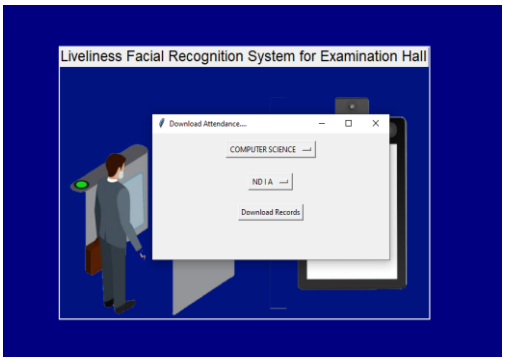

Fig. 12 Download Page

B. Discussion

To test the performance of the model, a dataset with 30 students was created, 10 students per exam hall. The model was tested for accuracy and proved to be 100% accurate as it was able to correctly authenticate students, match students with their right venue, detect spoofs (fake candidates), and mismatch venues. Table 1 below shows the summary of the performance of the model.

Venue	Number of Students Authenticated	Number of Students Matched	Number of Students Mismatched	Number of Fake Students	Error	Accuracy (%)
510 Hall	10	8	0	2	0	100
Twin Theater 1	10	7	2	1	0	100
SBS Complex Downstairs	10	10	0	0	0	100

From the table it can be deduced that the model was able to identify genuine students from impersonated students. It was able to deny access to students that went to the wrong exam hall.

DOI: 10.17148/IJARCCE.2023.12801

IV. CONCLUSION

Impersonation is one the disturbing examination misconduct and has proven to be difficult to eradicate. This implies bringing someone in place of the candidate to write the exam on the candidate's behalf. A security system aims to verify an individual's identity and prevent impostors from accessing protected resources. In this project, we were able to design a system that could authenticate students in an examination hall using liveness facial recognition. The system was able to differentiate between real and fake students and matched students with their right venues. The system was tested with 30 students in three different exam halls and was found to be 100% accurate.

ACKNOWLEDGMENT

This work was sponsored by the Tertiary Education Trust Fund (TETFund) Nigeria as a means of promoting research in tertiary institutions.

REFERENCES

[1] S. O. Emaikwu, "Assessing the Impact of Examination Malpractices on the Measurement of Ability in Nigeria.," *International Journal of Social Sciences & Education*, vol. 2, no. 4, pp. 748 – 757, 2012.

[2] M. M. Rufai, J. O. Adigun, and N. a Yekini, "A Biometric Model for Examination Screening and Attendance Monitoring in Yaba College of Technology," *World of Computer Science and Information Technology Journal (WCSIT)*, vol. 2, no. 4, pp. 120–124, 2012.

[3] S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, "Iris liveness detection for next generation smartphones," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 2, 2016.

[4] J. Yang, Z. Lei, and S. Z. Li, "Learn convolutional neural network for face anti-spoofing arXiv preprint," *arXiv:1408.5601*, 2014.

[5] G. A. O. Chenqiang, L. I. Xindou, Z. Fengshun, and M. U. Song, "Face Liveness Detection Based on the Improved CNN with Context and Texture Information ∗," vol. 28, no. 6, 2019, doi: 10.1049/cje.2019.07.012.

[6] M. U. Nnam and A. F. Inah, "Empirical Investigation into the Causes, Forms and Consequences of Examination Malpractice in Nigerian Institutions of Higher Learning," *International Journal of Novel Research in Humanity and Social Sciences*, vol. 2, no. 1, pp. 52 – 62, 2015.

[7] P. S. Ojonemi, W. Enejoh, A. Enejoh, and O. Olatunmibi, "Examination Malpractice: Challenges to Human Resource Development in Nigeria," *International Journal of Capacity Building in Education and Management*, vol. 2, no. 1, pp. 91–101, 2013.

[8] J. Kothapalli and A. Gudipati, "Automated Face Detection & Recognition for Detecting Impersonation of Candidate in Examination System," *Int J Sci Eng Res*, vol. 7, no. 3, pp. 149–158, 2016, [Online]. Available: http://www.ijser.org

[9] I. O. Izu-Okpara, O. C. Nwokonkwo, and A. M. John-Otumu, "An Implementation of K-NN Classification Algorithm for Detecting Impersonators in Online Examination Environment," *Journal of Advances in Computing, Communications and Information Technology*, vol. 1, 2021, doi: 10.37121/jaccit.v1.153.

[10] A. Vishal, T. Nitish Reddy, P. Prahasit Reddy, and A. Shitharth, "Detecting impersonators in examination halls using AI," 2022. doi: 10.1049/icp.2022.0367.

[11] D. Yu, H. Wang, P. Chen, and Z. Wei, "Mixed pooling for convolutional neural networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, pp. 364–375. doi: 10.1007/978-3-319-11740-9_34.

[12] M. A. Ranzato, F. J. Huang, Y. Boureau, and Y. LeCun, "Unsupervised learning of invariant feature hierarchies with applications to object recognition," *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1–8, 2007.

[13] M. A. Ranzato, "Image Classification with Deep Learning," 2015.

[14] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," *ImageNet Challenge*, pp. 1–10, 2014, doi: 10.1016/j.infsof.2008.09.005.

[15] B. Xu, N. Wang, T. Chen, and M. Li, "Empirical Evaluation of Rectified Activations in Convolution Network," *ICML Deep Learning Workshop*, pp. 1–5, 2015.

[16] A. Shrestha, T. Rakshit, R. Patra, and S. K. Jindal, "Experimental Design and Implementation of Fingerprint Based Exam Hall Authentication System with Temperature Sensing and Analysis using Internet of Things," in *Proceedings - 2020 International Conference on Interdisciplinary Cyber Physical Systems, ICPS 2020*, 2020. doi: 10.1109/ICPS51508.2020.00012.

[17] M. Kalbande, Y. Gaidhani, T. Panse, and M. Mahajan, "Cloud Based Examination Hall Authentication System Using Fingerprint Module," 2022. doi: 10.1007/978-981-19-0770-8_15.