International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2063225

Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine (SVM)

Ngonadi I. Vivian[*1], **Orobor Anderson Ise**[2]
[*1]Department of Computer Science, Petroleum Training Institute, Effurun, Delta State, Nigeria
[2]Information and Communication Technology Directorate, Federal University of Petroleum Resources, Effurun, Delta State, Nigeria
ngonadi_iv@pti.edu.ng[1], orobor.anderson@fupre.edu.ng[2]

ABSTRACT

Article Info
Volume 6, Issue 4
Page Number: 11-20
Publication Issue :
July-August-2020

Article History
Accepted : 01 July 2020
Published : 07 July 2020

Impersonation in the context of examination, is a situation where a candidate sits in an examination for another candidate pretending to the real candidate. In many institutions in Nigeria, to mitigate this act, students are expected to present a means of identification before entering the examination hall. However, this approach is not sufficient to determine the eligibility of a student for an examination as these means of identification can easily be falsified. This paper therefore, develops a face recognition web service model for student identity verification using Deep Neural Network (DNN) and Support Vector Machine (SVM). The aim is to mitigate examination impersonation by simple face scan using mobile phone and also to make such a model accessible and re-usable for seamless integration with any kind of student identity verification project.

Keywords: Examination Impersonation, Student Verification, Face Recognition, Deep Neural Network

I. INTRODUCTION

Examination is one of the most used criterion for the assessment of individual knowledge. This method of assessment had in one way or the other suffered different form of malpractices including impersonation. Kanu and Ursula (2012) stated that impersonation in the context of examination, is a situation where a candidate sits in an examination for another candidate pretending to be the real candidate. It is a fundamental problem for examination that involves large number of students and this act compromises the integrity of any examination.

In many institutions, to mitigate this act, students are expected to present a means of identification which may be any of the following: student identity card, library card, clearance card, school fees payment receipt, course registration form etc. (Saheed *et al*, 2015; Abdullahi *et al,* 2018). However, none of these is sufficient to determine the eligibility of a student for an examination as these can easily be falsified.

This paper therefore, develops a face recognition web service model for student identity verification using Deep Neural Network (DNN) and Support Vector

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

Machine (SVM). The aim is to mitigate examination impersonation by simple face scan using mobile phone and also to make such a model accessible and re-usable for seamless integration with any kind of student identity verification project.

We believe that the fear of being suspected and scan for true identity before or during examination will mitigate examination impersonation by students.

II. RELATED WORKS

Examination impersonation happens both in face-to-face and online examinations. We studied existing works on both mode of assessment. Several researches have attempted solving this issue using either face recognition or fingerprint biometrics. The following table presents a summary of some of the existing researches.

TABLE 1. EXISTING RESEARCHES ON EXAMINATION IMPERSONATION

Author	**Biometric**	**Examination**	**App Type**
Ojo *et al,* (2019)	Face Recognition	Face-to-Face	Network
Sukmandhani and Sutedja (2019)	Face Recognition	Online	Web
Oyediran *et al* (2016)	Fingerprints	Face-to-Face	Embedded
Haruna (2018)	Fingerprints	Face-to-Face	Desktop
Shubha and Pushpa (2017)	Face Recognition	Face-to-Face	Desktop
Saheed *et al,* (2017)	Fingerprint	Face-to-Face	Desktop
Ketab *et al,* (2017)	Face Recognition	Online	Desktop
Anuradha *et al,* (2016)	Face Recognition	Face-to-Face	Desktop
Ogherohwo and Ezeoba, (2016)	Fingerprints	Face-to-Face	Embedded
Fayyoumi and Zarrad (2014)	Face Recognition	Online	Web
Kanimozhi, (2015)	Face Recognition	Face-to-Face	Experiment
Tejashwin (2017)	Face Recognition	Face-to-Face	Desktop

From the existing researches, proposed systems attempted to address this issue from one perspective (either face-to-face or online examination). However, any solution that can cater for both mode of assessment makes a lot of sense especially for institutions that operate both. Hence, the model proposed in this paper is adequate for both face-to-face and online examination student identity verifications. The model is quite different from the existing researches both in design and implementation. We focus more on an approach that is re-usable, accessible and without additional/ vendor dependent hardware for its implementation, both on client side or server side.

III. MATERIALS AND METHODS

A. Service Overview

In this paper, a student identity verification face recognition service model was proposed. The model is aimed at identifying suspected cases of impersonation during examination exercise. Although the service can also be used for full scale student identity verification before entering the examination hall, our main focus is on selective identity verification of suspected students.

Most time, suspected impersonator, when interrogated, will refuse to give or eventually gives false identity. The proposed model could adequately help in determining the true identity of the student in such case with quick and simple face scan. For this to be possible, the institution existing student portal have to be integrated with the service model through its web service Application Programming Interface (API). This will enable the portal to exchange students' records with the service for verification purpose.

B. Service Model Architecture

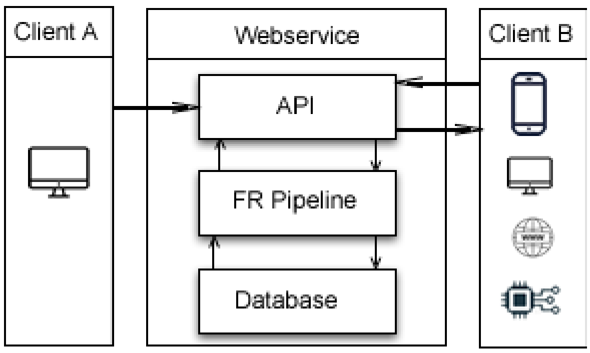

Figure 1. Service Model Architecture

From figure 1 above, the arrows indicate the flow of Hypertext Transfer Protocol (HTTP) request and response. Client A can be any existing online student portal extended to consume the service by synchronising its student's records such as Biodata, Courses Registration, Results etc. The records are stored in the service database to aid Client B verification.

Client B is a stack of different systems (mobile, desktop, web or embedded) that can be implementing to consume the service model. Each system can send a request to the service, in this case, face image.

On receiving the request, the face recognition pipeline service applies deep learning neural network in OpenCV library to perform several image processing and optimizations. OpenCV supports a number of deep learning frameworks, including Caffe, TensorFlow, and Torch/PyTorch. The service performs face detection, which is detecting the presence and location of a face in the image received. Extract from the detected faces, a 128-d feature vectors (called "embeddings") that quantify the face. Train a face recognition model on the face embeddings and then recognise the face in image. On valid recognition, the full details associated with the face is queried from the database and returned to Client B as JavaScript Object Notation (JSON) response as shown in Figure 3. A similar process is performed when Client A synchronises its data (student's photographs) with the service. The face recognition pipeline service is the core component of the proposed model.

C. Service Modelling

Unified Modelling Language (UML), a standard modelling language for visualising the design of a system was used. There are different UML diagrams. The sequence diagram amongst them was used to shows the interaction of the various objects in a system. The diagram present how different parts of the service model interact with each other to carry out their functions. Figure 2 depicts a sequence diagram of Client B web service model call.

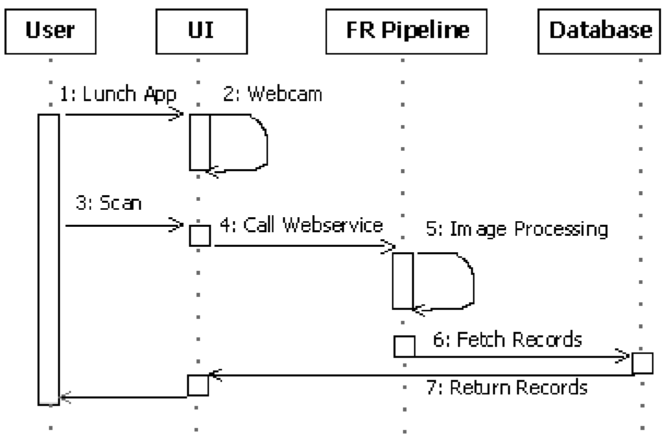

Figure 2. Sequence Diagram for Face Scanning

D. Web Service

A service is software that performs some computing function and has some type of underlying computer system. Web services is defined as a means to connect services together (Barry and Dick, 2013).

Web services allow various applications built with different technologies or platform to communicate and share data with each other through an acceptable standard. There are different options to adopt when building a web service. These include Simple Object Access Protocol (SOAP), Representational State Transfer (REST), JSON etc. This paper adopted REST in developing the service. REST is a style of architecture based on a set of principles that describe how networked resources are defined and addressed. It is the first alternative to SOAP (Barry and Dick, 2013).

With this architectural style, the proposed model is able to share business logic, data and processes through a programmatic interface across a network. It enables the underlay functionality of the face recognition pipeline to be exposed, allowing applications to consume the service through web service call.


```
{
 "bio_data":
   {
    "name" : "Smith Onyekachi",
    "gender" : "Male",
    "tel" : "070654386[redacted]",
    "email" : " smony[redacted]achi@gmail.com"
   },
   "academic_info":
   {
    "faculty" : "Engineering",
    "department" : "Mechanical Engineering",
    "level" : "300L",
    "matricno" : "ENG/2017/0[redacted]7"
   },
 "course_registration" : [
   {
    "code" : "MEE 314",
    "title" : "Strength of Material I",
    "unit" : "2",
    "status" : "Core",
    "semester" : "First Semester",
    "session" : "2019/2020",
  },
  {
    "code" : "MEE 316",
    "title" : "Thermodynamics & Heat Transfer",
    "unit" : "2",
    "status" : "Core",
    "semester" : "First Semester",
    "session" : "2019/2020",
   },
   .
   .
   .
```


Figure 3. REST response in JSON format

E. Face Recognition Pipeline

Face recognition is a prominent biometric technique that has been widely used in many areas for identity authentication (Wang and Deng 2019). Li and Jain (2011) noted that it is a broad task of identifying human face(s) in an image or video. Face recognition can be classified as a supervised predictive machine learning modeling task that is trained on dataset of face samples. In this task, the input is often an image with at least one face while its output varies based on the required prediction.

Generally, face recognition could be described as a four steps processes as shown in figure 4. These are:

- **Face Detection.** Locating one or more faces in the image and mark with a bounding box.
- **Face Alignment.** Normalizing the face to be consistent with the database, such as geometry and photometrics.
- **Feature Extraction.** Extracting features from the face that can be used for the recognition task.
- **Face Recognition.** Performing match of the face against one or more known faces in a database.

However, a specific implementation may have more separate modules for each step or combine some of the steps into a single module.

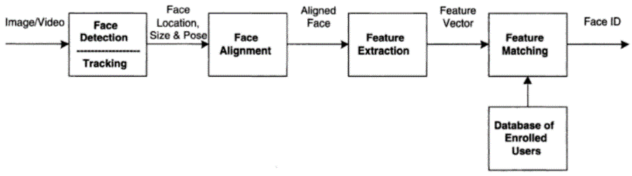

Figure 4. Face recognition process. Source: Li and Jain (2011)

In this paper, our face recognition pipeline was built using OpenCV and Scikit-learn implementation of Deep Neural Network (DNN) and Support Vector Machine (SVM) respectively.

Basically, a standard Neural Network (NN) consists of many simple, connected processors called neurons, each producing a sequence of real-valued activations (Schmidhuber, 2014).

Each node takes multiple weighted inputs, applies the activation function to the summation of these inputs, and in doing so generates an output. These structures can come in a myriad of different forms, but the most common simple NN structure consists of an input layer, a hidden layer and an output layer (Thomas, 2017). Figure 6 depicts a neural network with three layer.

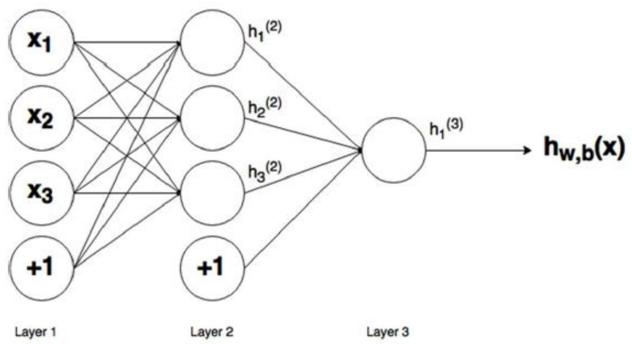

Figure 6. Three-Layer Neural Network. Source: Thomas, (2017)

From figure 6, Layer 1 represents the input layer, where the external input data enters the network. Layer 2 is called the hidden layer as this layer is not part of the input or output. This hidden lay can be more than one as the case may be. Layer 3 is the output layer. Each of these layers are connected together with its associated weight.

$$h_1^{(2)} = f(w_{11}^{(1)}x_1 + w_{12}^{(1)}x_2 + w_{13}^{(1)}x_3 + b_1^{(1)}) \quad \text{---------} \quad (1)$$
$$h_2^{(2)} = f(w_{11}^{(1)}x_1 + w_{12}^{(1)}x_2 + w_{13}^{(1)}x_3 + b_1^{(1)}) \quad \text{--------} \quad (2)$$
$$h_3^{(2)} = f(w_{11}^{(1)}x_1 + w_{12}^{(1)}x_2 + w_{13}^{(1)}x_3 + b_1^{(1)}) \quad \text{--------} \quad (3)$$
$$h_{w,b}^{(x)} = h_1^{(3)} = f(w_{11}^{(2)}h_1^{(2)} + w_{12}^{(2)}h_2^{(2)} + w_{13}^{(2)}h_3^{(2)} + b_1^{(2)}) \quad \text{--------------} \quad (4)$$

The equations above represent how the output is calculated from the input in neural networks. Where $f(\cdot)$ refers to the node activation function. $h_1^{(2)}$ is the output of the first node in the second layer, and its input are $w_{11}^{(1)} x_1$, $w_{12}^{(1)} x_2$, $w_{13}^{(1)} x_3$ and $b_1^{(1)}$. These inputs can be traced in the three-layer connection in figure 6 above. They are simply summed and then passed through the activation to calculate the output of the first node.

The concept of learning is simply finding weights that make the NN exhibit desired behaviour. Depending on the problem and how the neurons are connected, such behaviour may require long causal chains of computational stages. Deep Learning (DL) is about accurately assigning credit across many such stages (Schmidhuber, 2014).

Wang and Deng (2019) affirmed that DL applies multiple processing layers to learn representations of data with multiple levels of feature extraction. This occurs by repeatedly activating certain neural connections over others, and this reinforces those connections (Schmidhuber, 2014).

DL based facial recognition uses a technique called deep metric learning which output a real-valued feature vector 128-d (i.e a 128 real-valued numbers) which are used to quantify face(s) in an image or video.

Metric learning provides a new distance metric by analyzing data. Its aim is to learn a new metric to reduce the distances between samples of the same class and increase the distances between the samples of different class (Duan et al, 2018 as cited by Kaya and Bilge, 2019).

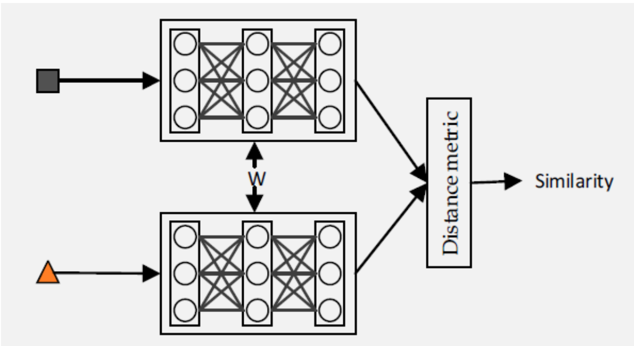

Figure 7. Deep Metric Learning. Source: Kaya and Bilge, (2019)

Let $X = [x_1, x_2, \ldots x_N] \varepsilon R^{dxN}$ be the training samples, where $x_i \varepsilon R^d$ is ith training example and N is the total number of training samples. The distance between x_i and x_j is calculated as:

$$d_M(x_i, x_j) = \sqrt{(x_i - x_j)^T M (x_i - x_j)} \quad \text{----------------------} \quad (5)$$

$d_M(x_i,x_j)$ is a distance metric, it must have the properties of non-negativity, the identity of indiscernible, symmetry, and the triangle inequality. M needs to be symmetric and positive semidefinite. All of the eigenvalues or determinants of M must be positive or zero to be positive semidefinite. When we decompose M, as follows:

$$\begin{aligned} M &= W^T W \\ d_M(x_i, x_j) &= \sqrt{(x_i - x_j)^T M (x_i - x_j)} \\ &= \sqrt{(x_i - x_j)^T W^T W (x_i - x_j)} \\ &= \|Wx_i - Wx_j\|_2 \end{aligned} \quad \text{--------------------} (6)$$

From equation 6, W has a linear transformation property. Euclidean distance in the transformed space is equal to Mahalanobis distance in original space for two samples. This linear transformation shows the reality in the infrastructure of metric learning.

The proposed model performs fast and accurate face detection with a pre-trained deep learning face detector model in OpenCV library. Being that face detection algorithm does not identify who is in the image analysed, the detected faces, is passed on to the face recognition algorithm for identification.

In a canonical face recognition algorithm. each individual is a class and the distribution of each face is estimated or approximated. In this method. for a gallery of K individuals. The identification problem is a K class problem and the verification problem is K instances of a two class problems. SVMs are a binary classification method formulated to solve a classical two class pattern recognition problem. It finds the optimal linear decision surface based on the concept of structural risk minimization (Phillips, 1999).

The input to a SVM algorithm is a set $\{(x_i, y_i)\}$ of labeled training data, where x_i is the data and $y_i = -1$ or 1 is the label. The output of a SVM algorithm is a set of N_s support vectors Si, coefficient weights αi, class labels y_i of the support vectors, and a constant term b. The linear decision surface is where $w \cdot z + b = 0$,

$$W = \sum_{i=0}^{Ns} \alpha iyiSi \quad \text{------------------------------(7)}$$

The support vectors are the data points that lie closest to the decision surface or hyperplane (Berwick, 2003).

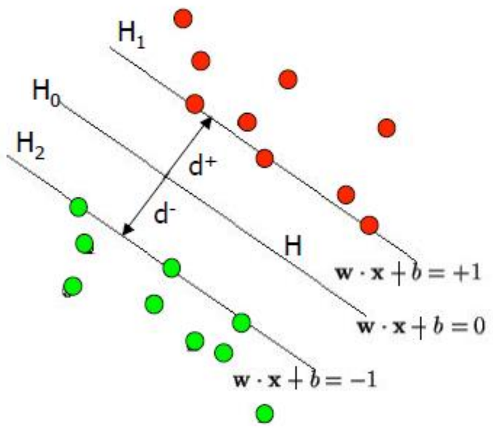

Figure 8. SVM hyperplanes. Source Berwick (2003)

Hyperplanes *H is* defined such that :
w.xi + b >= +1 where $y_i = +1$
w.xi + b <= -1 where $y_i = -1$
H1 and *H2* are the planes:
H_1: w.x_i + b = +1
H_2: w.x_i + b = -1

The plane H_0 is the median in between,
where $w \cdot x_i + b = 0$

d+ = the shortest distance to the closest positive point
d- = the shortest distance to the closest negative point
The margin (gutter) of a separating hyperplane is d+ + d–

The recognition algorithm dataset is built from student passport photograph captured during registration. See figure 11. For better accuracy, it is recommended that a minimum of 4 face image samples be captured for each student.

IV. RESULT AND DISCUSSION

A. System Implementation

As a proof of concept, the proposed model was developed as a web service that can be consumed by any application. The service model was developed using python, OpenCV DNN for face detection, scikit-learn SVM for face recognition and MongoDB for data storage.

A mobile app was developed using HTML, CSS, JavaScript and Cordova framework, targeting Android platform to consume the face recognition service model. The app enables users to perform simple face scan using their phone and get immediate responses on the full academic details of the student scanned. This provides a handy solution for student identity verification that can be used anytime and anywhere by invigilators/ investigators. With this approach, users mobile phone act as the face scanning device. Our assumption is that since most institutions already have an online student portal as well as proliferation of smart phones, the proposed service model can be leverage seamlessly without additional infrastructure.

A web interface that synchronise the student records with the service was developed in PHP since the existing student portal used during testing was developed using same.

B. System Interfaces

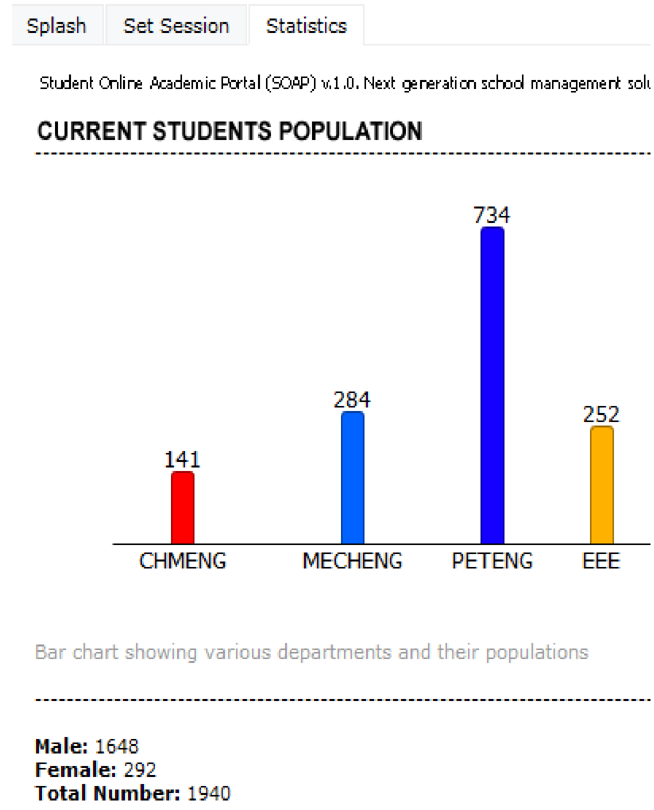

Figure 9. Web Application Interface

The above figure 9 depict part screenshot of an existing online student portal used in testing the model. The portal was extended to automatically interface and synchronise student records with the service model through its API.

Figure 10 and Figure 12 are results of student face scanned. When the Scan Button is tapped, the image streamed from the camera is captured and sends to the face recognition service pipeline for optimisation and recognition. On every valid face match, the student academic details are displayed. The result displayed can adequately guide the invigilator/ investigator in decision making. The following are more of the result obtained from the testing.

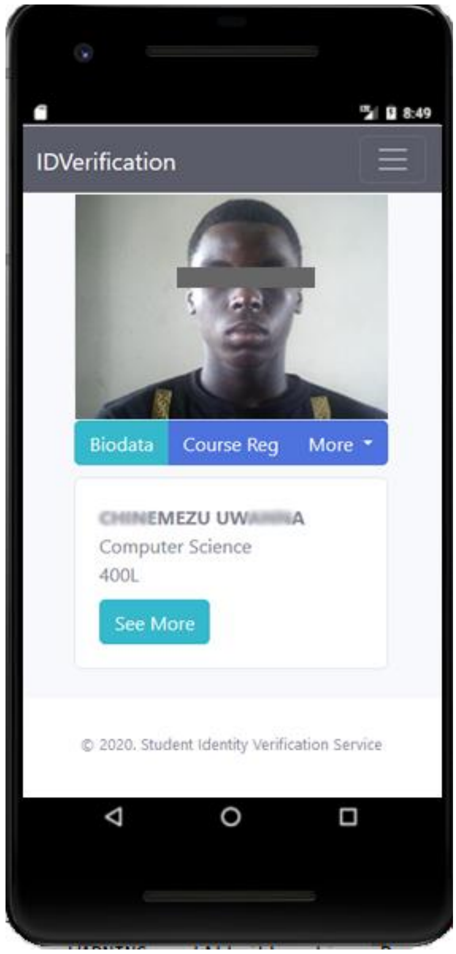

Figure 10. Scanned Student Biodata

Figure 11. Sample Faces Dataset

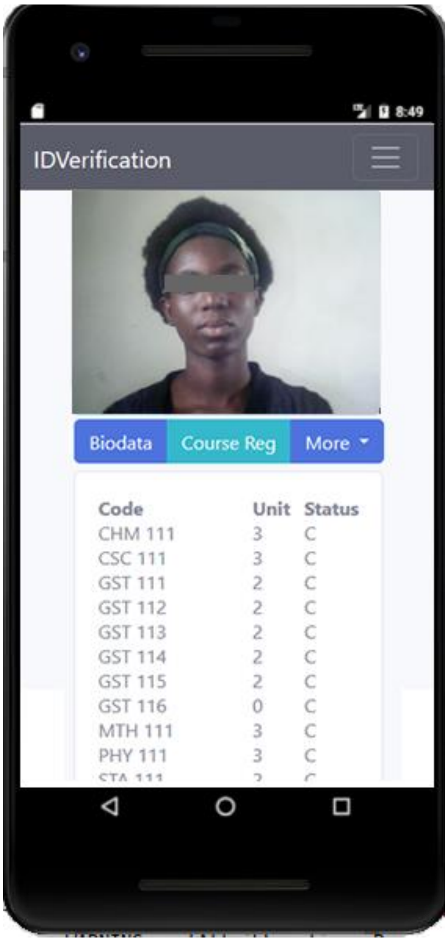

Figure 12. Sessional Course Registration Details

V. CONCLUSION

Examination impersonation is a familiar act to most students and academia. This paper presents a handy and sustainable solution to mitigate this practice. The proposed model provides a re-usable and accessible approach to reliably verify student true identity before or during examination whether on face-to-face or online mode.

Existing researches studied either requires additional hardware for implementation or lacks reusability, accessibility and flexibility. These were well addressed in the proposed model. The service model can be consumed through its API by different applications irrespective of their technology or platform.

The mobile verification app and web app implementation of the proposed model prove to be handy and adequate for any form of student identity verification when institution existing student portal is linked to the service model. However, the mobile device network can hamper the face scanning processing speed due to its network dependent.

VI. REFERENCES

[1] Kanu, S.I. and Ursula, N.A. (2012). Unethical Practices in The Nigerian Educational System. Interdisciplinary Journal of Contemporary Research in Business, 4(8), pp 451-464

[2] Tejashwini, S.G. (2017). Fraud Detection in Examination using LBP method. International Journal of Latest Engineering and Management Research (IJLEMR). International, 2(4), pp 28-35

[3] Saheed, Y.K, Hambali, M.A, Adeniji, I.A and Kadri, A.F (2017). Fingerprint Based Approach for Examination Clearance in Higher Institutions. FUOYE Journal of Engineering and Technology, 2(1), pp 47-50

[4] Shubha, G.S and Pushpa S.T (2017). Detection of Impersonation in Remote Online Examination. International Journal of Current Engineering and Scientific Research (IJCESR), 4(7), pp 61-64

[5] Barry, D.K. and Dick D. (2013). Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide (2ed): Morgan Kaufmann, USA

[6] Ojo, O., Yekini N. A., Aigbokhan E. E., Onadokun I. (2019). Deterring Malpractice in a Networked Computer Based Examination Using Biometric Control Attendance Register. International Journal of Scientific & Engineering Research, 7(3), pp 149-158

[7] Oyediran, M.O, Wahab W.B, Elegbede A.W and Enegbe T.J (2016). Development of an Examination Authentication Embedded System Based on Fingerprint Approach. International Journal of Computers & Technology, 17(1), pp 7164-7169

[8] Abdullahi, M.B., Nura, Z.M. and Jiya, L.M (2018). Examination Eligibility Verification and Attendance System Using Quick Response Code. Journal on Digital Signal Processing, 6(3), pp 1-4

[9] Sukmandhani, A. A. and Sutedja, I. (2019). Face Recognition Method for Online Exams. International Conference on Information Management and Technology (ICIMTech), Jakarta/Bali, Indonesia, 2019, pp. 175-179.

[10] Haruna, U. S. (2018), sVeriTool: A Verification Tool for Preventing Impersonation of Students in Examination Halls using Fingerprints. Afr. J. Comp. & ICT, 11(2) pp 37-52

[11] Ketab, S.S., Clarke, N.L., and Dowland, P.S. (2017). A Robust e-Invigilation System Employing Multimodal Biometric Authentication. International Journal of Information and Education Technology, 7(11), pp 796-802

[12] Anuradha, S.G, Kavya, B., Akshatha, S., Kothapalli J., Gudipati A. (2016). Automated Face Detection & Recognition for Detecting Impersonation of Candidate in Examination System. International Journal of Scientific & Engineering Research, 7(3), pp 149-158

[13] Ogherohwo, E.P. and Ezeoba, E.O. (2016) Design and Construction of a Biometric Examination Authentication Device. International Journal of Advanced Research in Physical Science (IJARPS), 3(5), pp 29-39

[14] Fayyoumi, A. and Zarrad A. (2014). Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. Advances in Internet of Things, 2014(4), pp 5-12

[15] Schmidhuber, J. (2014). Deep Learning in Neural Networks: An Overview. Neural and Evolutionary Computing, 61, pp 85-117

[16] Berwick, R. (2003) An Idiot's guide to Support vector machines (SVMs). Available at: https://web.mit.edu/6.034/wwwbob/svm.pdf. Accessed: 12 June, 2020

[17] Phillips, P.J. (1999) Support Vector Machines Applied to Face Recognition. Available at: https://papers.nips.cc/paper/1609-support-vector-machines-applied-to-face-recognition.pdf. Accessed: 12 June, 2020

[18] Thomas, A. (2017). An Introduction to Neural Networks for Beginners. Available at: https://adventuresinmachinelearning.com/wp-content/uploads/2017/07/An-introduction-to-neural-networks-for-beginners.pdf. Accessed: 08 June, 2020

[19] Duan, Y; Lu, J; Feng, J; Zhou, J. (2018). Deep Localized Metric Learning. IEEE Trans. Circuits Syst. Video Technology 2018, 28, 2644-2656

[20] Kaya, M. and Bilge, H.S. (2019) Deep Metric Learning: A Survey. Symmetry, 11(1066), pp 1-26

[21] Wang, M. and Deng, W. (2019) Deep Face Recognition: A Survey. Computer Vision and Pattern Recognition, pp 1-26

[22] Kanimozhi, K. (2015) Biometric Authentication for Online Examination. International Journal of Innovative Research in Computer and Communication Engineering, 3(9), pp 9075-9079

Cite this article as :

Ngonadi I. Vivian and Orobor A. Ise, "Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine (SVM)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 6 Issue 4, pp. 11-20, July-August 2020. Available at

doi : https://doi.org/10.32628/CSEIT2063225

Journal URL : http://ijsrcseit.com/CSEIT2063225