BABCOCK UNIVERSITY
ILISHAN-REMO, OGUN STATE, NIGERIA

COLLEGE OF POSTGRADUATE STUDIES
2022/2023 PhD Thesis Abstract

Department of Computer Science

RFN: **Thomas Gbadebo AYANWOLA**
RD: **Computer Science**
RS: **Computing and Engineering Sciences**
RE: **ayanwola0529@pg.babcock.edu.ng**
RAE: **Thomas.ayanwola@mtn.com**
RP: **08032007204**

RT: **Face Spoofing Attack Detection Model Using Visual Geometry Group-19 Convolutional Neural Network**

MS: **Prof. Oudele AWODELE**
ME: **awodeleo@babcock.edu.ng**
SP: **08033378761**
CS: **Dr. Michel O. AGBAJE**
CE: **agbajem@babcock.edu.ng**
CP: **08052085154**

AB: Facial Verification and Authentication System (FVAS) has been found in device unlocking, automatic e-transactions, border security, airport control, attendance systems at colleges and universities, and in electronic polling. Spoofing Attack Detection (SAD) model is an integral part of FVAS which makes it impossible for an unauthorized user to disguise and outwit the face biometric device. However, poor generalization of face SAD model has negatively affected companies, banks, airports, national borders, and governments because successful face spoofing attacks had led to theft of valuables, unauthorized financial transactions, terrorism attack, and national border access. Previous studies have tried to solve the problem of loopholes created by this unsuccessful implementation in SAD models using Convolutional Neural Network (CNN) , but were unable to detect unseen face spoofing attacks in real time. Hence, this study developed a face SAD model using Visual Geometry Group (VGG)-19 CNN.

The face SAD model was developed using four variations of VGG-19 CNN: VGG-19A, VGG-19B, VGG-19C, and VGG-19D respectively. Six secondary face datasets were extracted from Nanjing University of Aeronautics and Astronautics, Chinese Academy of Sciences Institute of Automation, OUL University, Wide Multi Channel presentation Attack , 3D Mask Attack Dataset, and CASIA-Face-Africa containing 85,071 instances of face spoofing attacks images. The VGG-19 CNN was used to extract Red Green Blue and deep neural network features from the face datasets. The extracted features were normalized using different filter maps and dropout

regularization rates to overcome overfitting. The four VGG-19 CNN models were trained, validated and tested with the extracted normalized features. These were further evaluated using testing results, top-1 percent, threshold operation, quality test, fake face test, and overall test. The models were further benchmark in comparison with CNN and Support Vector Machine (SVM) techniques of previous results.

The validation results of the four VGG-19 face SAD models over unseen face datasets showed the accuracy of 97% (VGG-19A), 97.5% (VGG-19B), 98.8% (VGG-19C), and 97.5% (VGG-19D) respectively . VGG-19C performed better than the other models as shown in the validation results. Hence, it was evaluated, and the results of evaluation on low, normal, and high quality showed top-1 percent of 99%, threshold-operation of 99%, quality test of 97% and fake face test of 98%, while the average overall test was 98%. The average overall test result of (top-1 percent, threshold operation, quality test, and fake face test) on the existing face SAD models on low, normal, and high-quality datasets were 92%, 91%, and 90% respectively for SAD models. An improvement of 7% of overall test over the existing face SAD models was discovered.

In conclusion, the extracted normalized features of six face spoofing datasets were used to train and validate four VGG-19 SAD models. The models were evaluated using standard evaluation metrics. The validation and evaluation results of the implemented VGG-19 CNN face SAD model clearly demonstrated a strong generalization ability on unseen face images. Therefore, it was recommended that VGG-19C CNN face SAD model should be used by private and public institutions to secure their FVAS.

Keywords: Convolutional Neural Network, Face SAD, Generalization technique, SAD model, Spoofing attack, Visual Geometry Group-19

Word Count: 497

Abbreviations: RFN: Researcher's Full Name, RD: Researcher's Department, RS: Researcher's School, RE: Researcher's Email, RAE: Researcher's Alternate Email, RP: Researcher's Phone Contact, RT: Registered Title, MS: Main Supervisor, ME: Main Supervisor's E-mail Address, SP: Main Supervisor's Phone Contact, CS: Co-Supervisor, CE: Co-Supervisor's E-mail Address, CP: Co-Supervisor's Phone Contact, AB: Abstract

Suggested Citation: Ayanwola, T.G., Awodele, O. and Agbaje, M.O. 2023. Face Spoofing Attack Detection Model Using Visual Geometry Group-19 Convolutional Neural Network. PhD Thesis Abstract, College of Postgraduate Studies, Babcock University. **https://doi.org/10.61867/pcub.1(5).111**