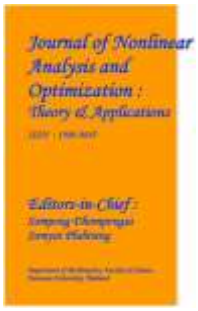
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**



FACE SPOOFING ATTACK DETECTION USING DEEP LEARNING

K. JAYA KRISHNA [1], JILAKARA VIJAY [2]

[1]Associate Professor, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

[2]PG Scholar, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT— The Liveness face detection is essential for modern biometric systems, ensuring that input data is genuine and not derived from a false image or video. Liveness face detection in today's biometric systems will ensure that input comes from a real, live person rather than a manipulated image or video. The novelty of this study lies in combining deep learning models with local interpretable model-agnostic interpretation (LIME) to enhance the interpretability and transparency of facial liveness detection systems. This technology is necessary for preventing spoofing attacks and attempts by hackers to break the security feature via pictures, videos, masks, etc. Spoofing refers to the compromise of a biometric system by providing it with untruthful material, photographs, videos, or masks to gain access. The objective of this research is to test the different pre-trained models to detect spoofing attacks and to use LIME to explain the model's predictions

Index Terms – Explainable artificial intelligence (XAI), liveness detection, LIME, pre-trained models, spoof attacks.

I. INTRODUCTION

With the increasing reliance on facial recognition technology for security and authentication purposes, the threat of face spoofing attacks has become a significant concern. Face spoofing involves presenting a fake image, video, or mask to the facial recognition system to gain unauthorized access. To counter this threat, robust face spoofing attack detection mechanisms are essential. Face spoofing attack detection using OpenCV and deep learning leverages

the strengths of both computer vision and advanced machine learning techniques. OpenCV, an open-source computer vision library, provides a wide range of tools for image and video processing, making it a suitable choice for real-time applications.

Deep learning, with its powerful feature extraction and pattern recognition capabilities, enhances the accuracy and reliability of spoofing detection systems. In this approach, the system typically consists of two main stages: feature extraction and classification.

During the feature extraction stage, the system analyzes facial images to capture distinguishing characteristics that differentiate between real and spoofed faces. This involves techniques like texture analysis, motion analysis, and frequency domain analysis. OpenCV aids in pre-processing tasks such as face detection, image resizing, and filtering, which are crucial for preparing the data for deep learning models. The classification stage employs deep learning models, such as convolutional neural networks (CNNs), to learn and identify patterns associated with spoofing attacks. CNNs are particularly effective in this domain due to their ability to automatically extract hierarchical features from raw images. The trained model can then classify incoming facial images as either genuine or spoofed based on the learned features.

This integration of OpenCV and deep learning not only enhances the system's ability to detect sophisticated spoofing attempts but also ensures real-time performance, which is critical for practical deployment in security-sensitive environments. As face spoofing techniques continue to evolve, ongoing research and development in this field are vital to stay ahead of potential threats and ensure the robustness of facial recognition systems.

II. LITERATURE SURVEY

A. An overview of face liveness detection

Face recognition is a widely used biometric approach. Face recognition technology has developed rapidly in recent years and it is more direct, user friendly and convenient compared to other methods. But face recognition systems are vulnerable to spoof attacks made by non-real faces. It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. A secure system needs Liveness detection in order to guard against such spoofing. In this

work, face liveness detection approaches are categorized based on the various types techniques used for liveness detection. This categorization helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of the latest works regarding face liveness detection works is presented. The main aim is to provide a simple path for the future development of novel and more secured face liveness detection approach.

B. Real masks and spoof faces: On the masked face presentation attack detection

Face masks have become one of the main methods for reducing the transmission of COVID-19. This makes face recognition (FR) a challenging task because masks hide several discriminative features of faces. Moreover, face presentation attack detection (PAD) is crucial to ensure the security of FR systems. In contrast to the growing number of masked FR studies, the impact of face masked attacks on PAD has not been explored. Therefore, we present novel attacks with real face masks placed on presentations and attacks with subjects wearing masks to reflect the current real-world situation. Furthermore, this study investigates the effect of masked attacks on PAD performance by using seven state-of-the-art PAD algorithms under different experimental settings. We also evaluate the vulnerability of FR systems to masked attacks. The experiments show that real masked attacks pose a serious threat to the operation and security of FR systems.

C. Face spoofing detection from single images using micro-texture analysis

Current face biometric systems are vulnerable to spoofing attacks.

A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access. Inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. Indeed, face prints usually contain printing quality defects that can be well detected using texture features. Hence, we present a novel approach based on analyzing facial image textures for detecting whether there is a live person in front of the camera or a face print. The proposed approach analyzes the texture of the facial images using multi-scale local binary patterns (LBP). Compared to many previous works, our proposed approach is robust, computationally fast and does not

require user-cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

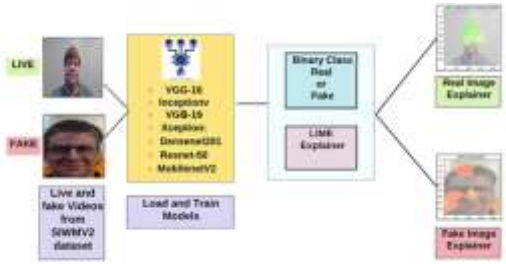


Fig. 1: System Overview

Implementation Modules

User Module

- In this module, user start the web cam to capture the video, once capture the video he can check the liveness of the video, and detect the any spoof attack.

Open Camera Module

- In this module, we are enable the system camera module using the Opencv library in python. This library is used to handling the image or video data effectively. Using the module we capture the live video data for further verification process.

Check liveness

- In this module, we are check the liveness of the video. In the recent time it is very common attack system different type of attacks in which spoofing the biometrics data. This attack was performing by using the photostat copies of images or pre record data. So we need check the liveness of the data is important to detect and mitigate the spoofing attack effectively.

Detect Spoof

- In this module, we collect liveness data from the above module and then classify whether the data spoofed or not.

IV. RESULTS

Fig. 2: Home Page

Fig. 3: Registration

Fig. 4: Login

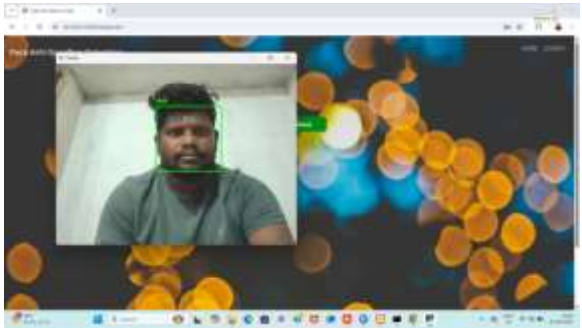


Fig. 5: Detecting Results

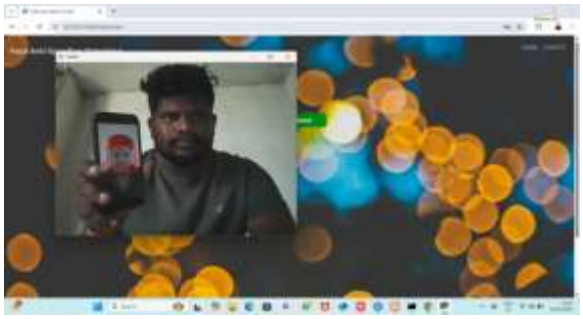


Fig. 5: Detecting Results

V. CONCLUSION

At present, upper ocean dynamics can be monitoring by several sensors, i.e., sea surface wind from scatterometer and spaceborne polarimetric microwave radiometer and sea surface wave from altimeter and SWIM. However, the spatial resolution of these products (i.e., >10 km) does not satisfy the requirement of complicated air–sea interaction in TCs. In this article, more than 2000 dual-polarized S-1 images obtained in IW and EW mode during 200 TCs are collected, which are matched with hindcasted wave parameters using WW3 model, in which H-E wind, CMEMS sea surface current and CMEMS sea level are applied as forcing fields. The SWH, MWL, and MWP simulated by WW3 were validated against the measurements of NDBC buoys, and the RMSE of SWH was 0.35 m, COR was 0.96, and SI was 0.18; the RMSE of MWL was 13.86 m, COR was 0.87, and SI was 0.26; and the RMSE of MWP was 0.73 s, COR was 0.88, and SI was 0.17. The difference sea states result show that the entire dataset under four different sea state condition demonstrates satisfactory results in terms of statistical results.

REFERENCES

[1] R.C.Beardsley, A.G.Enriquez, C.A. Friehe, andC.A.Alessi,“Intercom parison

of aircraft and buoy measurements of wind and wind stress during SMILE," J. Atmospheric Ocean. Technol., vol. 14, no. 4, pp. 969–977, Aug. 1997.

[2] T. W. Group, "The WAM model—A third generation ocean wave predic tionmodel,"J.Phys.Oceanogr.,vol.18,no.12,pp. 1775–1810,Dec.1988.

[3] M. A. Shaik, A. Fatima, M. Parveen, A. Soumya Rani, A. Mohammad and A. Rahim, "Dual-Model Approach for Lung Disease Classification Using Convolutional Neural Networks and Support Vector Machines," 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS), Kalaburagi, India, 2024, pp. 1-6, doi: 10.1109/ICIICS63763.2024.10860090.

[4] S. H. Ou, J. M. Liau, T. W. Hsu, and S. Y. Tzang, "Simulating typhoon waves by SWAN wave model in coastal waters of Taiwan," Ocean Eng., vol. 29, no. 8, pp. 947–971, Jul. 2002.

[5] M. Ali Shaik, P. Sairam, P. Rahul, T. Sadhvik and P. Nithin, "Titanic Survival Predictor Using Machine Learning Algorithms," 2024 4th Asian Conference on Innovation in Technology (ASIANCON), Pimari Chinchwad, India, 2024, pp. 1-6, doi: 10.1109/ASIANCON62057.2024.10837935.

[6] X. H. Li et al., "Tropical cyclone wind field reconstruction and validation using measurements from SFMR and SMAP radiometer," Remote Sens., vol. 14, no. 16, Aug. 2022, Art. no. 3929.

[7] M. A. Shaik and E. Ravithreyini, "Enhanced BreastNet Architecture and Comparison with State-of-the-Art Models," 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India, 2024, pp. 604-608, doi: 10.1109/ICDICI62993.2024.10810949.

[8]G.Z.Liang,J.G.Yang,andJ.C.Wang,"AccuracyevaluationofCFOSAT SWIM l2 products based on NDBC buoy and Jason-3 altimeter data," Remote Sens., vol. 13, no. 5, Mar. 2021, Art. no. 887.

[9] I. Ali, S. Cao, V. Naeimi, C. Paulik, and W. Wagner, "Methods to remove the border noise from Sentinel-1 synthetic aperture radar data: Implications and importance for time-series analysis," IEEE J. Sel. Top ics Appl. Earth Observ. Remote Sens., vol. 11, no. 3, pp. 777–786, Mar. 2018.

[10] A. Pleskachevsky, S. Jacobsen, B. Tings, and E. Schwarz, "Estimation of sea state from Sentinel-1 synthetic aperture radar imagery for maritime situation awareness," Int. J. Remote Sens., vol. 40, no. 11, pp. 4104–4142, May 2019.

AUTHORS Profile

Mr. K. Jaya Krishna is an Associate Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai, and his M.Tech in Computer Science and Engineering (CSE) from Jawaharlal Nehru Technological University, Kakinada (JNTUK). With a strong research background, he has authored and co-authored over 90 research papers published in reputed peer-reviewed Scopus-indexed journals. He has also actively presented his work at various national and international conferences, with several of his publications appearing in IEEE-indexed proceedings. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. Jilakara Vijay has received him BCA and degree from ANU 2023 and pursuing MCA in QIS College of Engineering and Technology affiliated to JNTUK in 2023-2025