A Workflow paper on an effective approach for Face Spoofing Detection Using CNN

[1]Anushka Bagchi, [2]Shubh Malviya, [3]VGS Vishnu Priya, [4]Yashika Lalwani, [5]Prof. Aparna Pandey

[1,2,3,4]Student, [5]Assistant Professor
Dept. Computer Science and Engineering
Bhilai Institute of Technology

***Abstract*- The current facial biometric systems are vulnerable to spoofing attacks. A spoofing attack occurs when someone attempts to impersonate another person and gains unauthorized access by falsifying data. Face-spoofing attacks affect the high-security departments of corporations, government departments, and emerging SMEs. Several face spoofing countermeasures and live detection methods have been proposed, but the problem remains unresolved because of the difficulty in determining the characteristics and methods of spoofing attacks. It was recently shown that traditional facial biometric techniques are more vulnerable to spoofing attacks; therefore, the entire research community has had to focus more on finding solutions to spoofing attacks. The purpose of this study is to detail anti-spoofing methods and database evaluation. This research concludes that it is necessary to provide more general algorithms for detecting unpredictable spoofing attacks to increase system security, computational efficiency, and reliability.**

***Keywords*: Face Spoofing, Face Recognition, Anti-Spoofing, CNN, MobileNetV2.**

1. INTRODUCTION

Face spoofing is a type of cyber-attack that involves presenting a fake face or biometric trait to bypass facial recognition systems. Face spoofing attacks are becoming increasingly prevalent in the age of digital technology, posing a serious threat to security systems that rely on facial recognition for authentication and identification. To address this problem, researchers have developed various methods for detecting face spoofing attacks, ranging from traditional image processing techniques to more advanced machine learning-based approaches.

The purpose of this review paper is to provide an overview of the problem of face spoofing detection, its impact on security systems, and the various methods used for detecting spoofed faces. The paper will discuss the latest advances in face spoofing detection, including deep learning-based methods and the use of advanced features such as 3D face reconstruction and texture analysis. It will also discuss the various evaluation metrics used for assessing the performance of different face spoofing detection methods, and the challenges and open research questions in this field.

The review paper aims to provide a comprehensive and objective analysis of the current state-of-the-art in face spoofing detection, with a focus on the strengths and limitations of different methods. The paper will also provide recommendations for future research in this field, with a view to improving the accuracy and robustness of face spoofing detection methods and enhancing the security of facial recognition systems. Overall, this review paper will be a valuable resource for researchers, engineers, and practitioners working in the field of face spoofing detection and biometric security. The problem of face spoofing detection has become increasingly important in recent years due to the widespread use of facial recognition technology in various applications, including security systems, mobile devices, and social media platforms. Face spoofing is a type of cyber-attack that involves presenting a fake face or biometric trait to bypass facial recognition systems. This can be done using various techniques, such as printed photos, digital images, 3D masks, and videos.

To address the problem of face spoofing, researchers have developed various methods for detecting spoofed faces. Traditional image processing techniques such as Local Binary Patterns (LBP), Scale Invariant Feature Transform (SIFT), and Speeded-Up Robust Features (SURF) have been used for feature extraction and classification. However, these methods are often limited by their inability to handle complex variations in lighting, pose, and expression, and their susceptibility to noise and artifacts in the images.

More recently, machine learning-based approaches have emerged as a promising solution for face spoofing detection. These methods use deep learning architectures such as Convolutional Neural Networks (CNNs) and Multilayer Perceptrons (MLPs) for feature extraction and classification. They have been shown to be more robust and accurate than traditional image processing techniques, and can handle complex variations in the input data.

In addition to deep learning-based methods, researchers have also explored the use of advanced features such as 3D face reconstruction and texture analysis for face spoofing detection. These features can provide additional information about the spatial and textural characteristics of the face, which can improve the accuracy and robustness of face spoofing detection methods.

Overall, the development of face spoofing detection methods is an active area of research, with ongoing efforts to improve the accuracy and robustness of these methods. In the next section of this review paper, we will discuss the various methods used for detecting face spoofing attacks, including feature extraction, classification models, and evaluation metrics.

2. LITERATURE REVIEW

In recent years, detecting 3D mask face spoofing attacks has become a significant challenge that requires further research. However, due to the limited number of available databases and their deficiencies, only a few methods have been developed to address this issue. Most existing databases focus on countering various types of threats but neglect environmental factors in real-world implementations. [1] The paper proposes a 3D mask spoofing detection method that simulates real-world scenarios with different options. The proposed database consists of 440 videos, including 400 fake videos and 40 real videos, using 10 different subject masks (7 subject 3D latex masks, 2 subjects for 2D paper masks, and 1 half mask below the eye for testing). The authors intend to release this database to evaluate various methods, and it has been used for a deep convolutional neural network. The proposed system comprises three steps: video pre-processing, facial recognition, and output to determine whether the video is genuine or falsified. The suggested approach is stronger than most techniques and achieved high accuracy, with the MLFP dataset's accuracy obtained being 99.88. Future studies should focus on benchmarking experiments.

J. Kom. And M. Piet. In [2] states that the current biometric systems for facial recognition are prone to being compromised by spoofing attacks, which happen when an individual falsifies data to gain unauthorized access to a system while pretending to be someone else. To address this problem, we suggest approaching spoofing detection through texture analysis, inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection. Our proposed approach involves examining facial images to determine whether a live person is present or whether it is a face print, based on texture and local shape features. [8] We use a set of low-level feature descriptors, a fast linear classification scheme, and score-level fusion to analyze the texture and gradient structures of facial images. Our approach is unique in that it is robust and does not require user cooperation, unlike previous methods. Furthermore, the texture features used for spoofing detection can also be utilized for face recognition, creating a novel feature space that couples spoofing detection and face recognition. We conducted extensive experimental analysis on three publicly available databases, demonstrating that our approach outperforms existing methods.

Aneesa M P, Saabina M, Meera K in [3] propose that A Convolutional Neural Network (CNN) is an artificial neural network architecture that includes one or more convolution layers, commonly employed for image processing, segmentation, classification, and other types of auto-correlated data. Deep learning, a machine learning technique based on artificial neural networks, progressively extracts features from data through higher layers to identify objects in images. To recognize a face in an image, for instance, CNNs must be trained on human faces, as illustrated in the figure. CNNs have the advantage of developing an internal representation of a two-dimensional image, enabling the model to learn the position and scale of faces within an image. After training, the CNN is capable of recognizing faces in images. CNNs are a useful tool for processing image data, as they extract features from images.

M. B. Was., R. Mul., M. A. Az., and J. Bha. in [4] stated Accurate face recognition systems rely on face images as the most easily accessible biometric modality. However, such systems are susceptible to various presentation attacks. To prevent this, face anti-spoofing is a critical step before using face images in biometric systems. This paper introduces a novel two-stream CNN-based approach for face anti-spoofing that extracts local features and holistic depth maps from face images. [5] The local features enable the CNN to identify spoof patches regardless of their location on the face, while the holistic depth map verifies whether the input image has a face-like depth. The proposed approach is evaluated on challenging databases, including CASIA-FASD, MSU-USSA, and Replay Attack, and is compared to state-of-the-art techniques through extensive experiments.

Saankhya Mondal in [6] states that this paper focuses on the significance of detecting human faces and preventing spoofing in various security verification and law enforcement applications. To achieve high accuracy in classification and detection, deep learning is used to extract essential features from images. Convolutional Neural Networks (CNN) are particularly suitable for feature extraction from images without manual intervention. [7] The paper proposes a CNN-based real human face detection classifier, which is implemented on an embedded system for real-time detection. The classifier is capable of accurately predicting the presence of real human faces in camera frames.

3. PROPOSED METHODOLOGY

3.1 Data Pre-Processing

First of all, the dataset which will be used for the model is chosen. The dataset which be used in our model will contain ‘real’ and ‘spoof’ images. The new directory for dataset is created then the images will get copied on the new directory structure. In this step, the dataset will also get split into train and test datasets. After this step, Data exploration will take place which will divide the images on the basis of ‘real’, ‘spoof’, ‘train’ and ‘test’. The last step in Data Pre-processing is Dataset Visualization in which the images for training dataset will be displayed according to specified parameters.

3.2 Keras Framework

Keras is an open-source framework of written in python which is also a high level neural network API. In this project the Keras framework being used is of utmost importance because it is the base layer of the Convolutional neural network. It helps in building a defined and structured neural layer. The necessary libraries which will be used are: Dense, Dropout, Input, Flatten.

3.3 Image Augmentation

After choosing appropriate framework for our model, dataset will be loaded and image augmentation will be performed. In image augmentation the normalizing scales are decided like image rotation, brightness, width shift, height shift, shear, zoom etc. For training datasets these parameters for normalization will be defined and rescaling will be performed in valid dataset, 'rgb' colour mode will be used throughout the procedure for image augmentation. The suitable batch of images will be generated according to the specified conditions.

3.4 Model Selection

In this step, MobileNetV2 which is a pre-trained model will be used. MobileNetV2 is designed for accurate image classification task. It uses depth wise separable convolutions to reduce the computational complexity of the model while maintaining high accuracy. It also includes linear bottleneck layers and shortcut connections, which help to reduce the number of parameters and improve the flow of information through the network. Output layer and Prediction layers will be created in which we will use the flatten function to flatten the epochs. Along with flatten, dropout and dense functions will also be used.

3.5 Model Compilation and Checkpoints

In Model compilation the binary classification will be performed with help of a loss function called "Binary Cross-entropy. In binary cross-entropy, the predicted probabilities are typically generated by a sigmoid activation function, which maps any input value to a value between 0 and 1. The actual probabilities are usually represented as one-hot encoded vectors, where the target class is represented as a 1 and all other classes are represented as 0s. Model Checkpoint stores the weight of the model in different locations and only the best model is saved.

3.6 Model Training

The model will be trained continuously until it starts giving accurate results. After this step the model will be serialized to JSON.

3.7 Flowchart

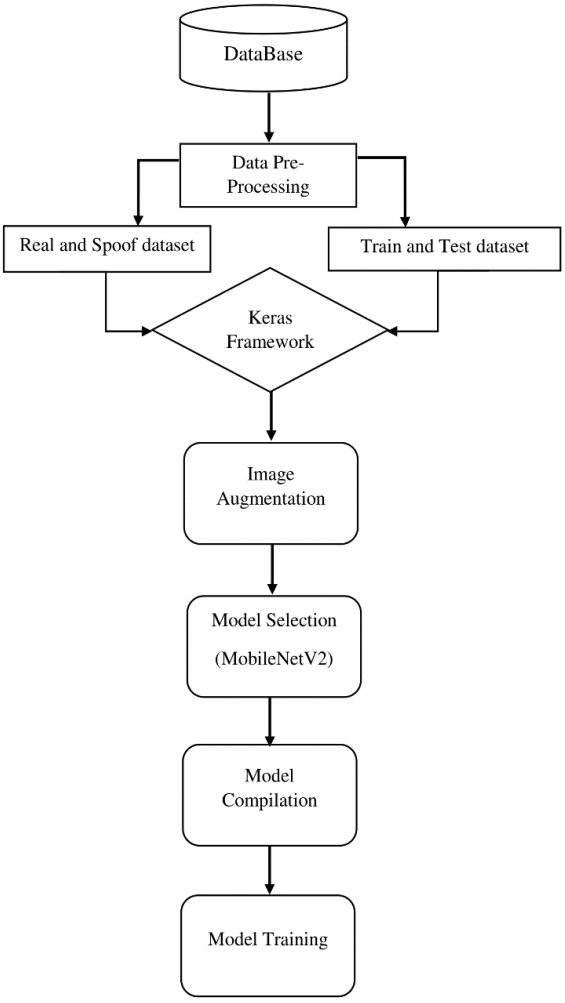

Figure 1 Flowchart for Proposed Methodology

4. CONCLUSION:

Personal data is an integral part of an individual's identity. Businesses must retain personal information. Systems that use facial recognition for authentication must be resistant to facial spoofing attacks. To create a secure facial recognition system that actually works, anti-spoofing technology should be a top priority from the beginning of the system design. Also it should be accurate in order to prevent the attacks from unknown sources. Face spoofing detection algorithms have been in market since the biometrics are used as passwords. More and more accurate models are launched in markets in order to keep users protected from spoof attacks.

REFERENCES:

1. Taha Hasan, Mohammed Akram Younus Face Spoofing Detection Using Deep CNN July 2021 (TURCOMAT)
2. Komulainen, Jukka & Hadid, Abdenour & Pietikainen, Matti. (2012). Face spoofing detection from single images using texture and local shape analysis. Biometrics, IET. 1. 3-10. 10.1049/iet-bmt.2011.0009.
3. Aneesa M P , Saabina N , Meera K, 2022, Face Recognition using CNN: A Systematic Review, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022),
4. Mohammed Badaruddin Wasef, Rehan Multani, Mohammed Abdul Azeem, Dr. J Bharathi Face spoofing detection using modified CNN May 2020 (JES)
5. Yousef Atoum Yaojie Liu Amin Jourabloo Xiaoming Liu Face Anti-Spoofing Using Patch and Depth-Based CNNs
6. S. Mondal, "Implementation of Human Face and Spoofing Detection Using Deep Learning on Embedded Hardware," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225495.
7. S. Mandol, S. Mia and S. M. M. Ahsan, "Real Time Liveness Detection and Face Recognition with OpenCV and Deep Learning," 2021 5th International Conference on Electrical Information and Communication Technology (EICT), Khulna, Bangladesh, 2021, pp. 1-6, doi: 10.1109/EICT54103.2021.9733685.
8. X. Han and Q. Du, "Research on face recognition based on deep learning," 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC), Beirut, Lebanon, 2018, pp. 53-58, doi: 10.1109/DINWC.2018.8356995.