Title

Name

* Alethea Agung Yodha Pratama – 2602078732
* Name – NIM
* Name - NIM
* Name – NIM

1. Introduction

Face recognition systems are integral to security applications, such as attendance systems and identity verification processes. However, these systems are vulnerable to spoofing attacks, where imposters mimic individuals’ identities, and can also face difficulties distinguishing between twins or similar-looking individuals. Conventional facial recognition, though widely adopted, has not been fully effective in addressing such challenges. This project aims to develop a robust face recognition system with anti-spoofing capabilities. By integrating Convolutional Neural Networks (CNNs) like ResNet50 and InceptionV3 for face recognition and YOLOv8 for anti-spoofing, the system will provide enhanced accuracy and security. This aligns with LO1, focusing on understanding computational principles in image processing, and LO2, which involves explaining feature detectors and descriptors used in computer vision tasks.

1. Methodology

The development process of our face recognition and anti-spoofing system involves several key steps: data collection, face detection, anti-spoofing verification, face matching, and attendance recording. Here’s a breakdown of each stage in relation to the Learning Outcomes:

1. Data Collection

For accurate facial recognition, we collect approximately 1,000 images per student at a size of 224x224 pixels, covering a variety of angles and lighting conditions. This dataset will train the model to recognize individuals reliably. For anti-spoofing, we use a dataset containing 7,000 labeled images (both genuine and spoofed faces) to allow the model to differentiate between real and fake images.

1. Face Recognition and Anti-Spoofing

Our system combines face recognition with anti-spoofing measures, both powered by deep learning, as these techniques are effective for detecting and analyzing facial features.

* Face Recognition: We utilize CNN models, specifically ResNet50 and InceptionV3, to detect faces and extract unique facial features. CNNs are known for their high accuracy in facial recognition tasks and are widely used in feature extraction due to their ability to detect complex patterns (LO3).
* Anti-Spoofing: YOLOv8 is employed for its high speed and precision in detecting objects and faces. By training with both real and spoofed face images, the model can learn to distinguish genuine faces from impostors. The combination of face recognition and anti-spoofing techniques enables us to improve the reliability and security of the system.

1. Training

For face recognition, we train the ResNet50 and InceptionV3 models using cross-validation and hyperparameter tuning techniques such as early stopping and learning rate adjustments to prevent overfitting. The YOLOv8 model for anti-spoofing is trained using supervised learning with labeled datasets, allowing the model to learn from the distinctions between genuine and spoofed faces based on image characteristics.

1. Anti-Spoofing Verification

During testing, the system first verifies the authenticity of the detected face using the anti-spoofing model. The face is then matched to its respective data based on an ID check within an external student record (Excel sheet). This step prevents attendance fraud and allows only genuine users to access the system.

1. Implementation

The implementation of our system involves specific libraries, algorithms, and hyperparameters essential for training and validation (LO4).

1. Libraries Used

We use OpenCV (cv2) and cvzone for computer vision processing and deep learning libraries such as TensorFlow, Keras, and Scikit-Learn for model building and training. Other essential libraries include ultralytics for YOLO import, as well as numpy, matplotlib, os, and math for data handling and visualization.

1. Algorithms

(Insert anti-spoofing algorithm here)

(Input facial recognition algorithm here)

1. Parameters and Training Process

* Base Model Configuration: ResNet50 is used as the base model without the top layer and with "imagenet" weights. Layers include:
  1. A global average pooling layer,
  2. Dense layer with 4096 neurons (ReLU activation),
  3. Dropout layer,
  4. Output dense layer with 11 neurons (SoftMax activation).
* Model Training and Validation: A 5-fold KFold cross-validation is used, with a 60:40 training-to-testing split. The model is trained with a batch size of 16, across 20 epochs, and one verbose output for each fold. Hyperparameters are tuned to optimize performance and prevent overfitting.

1. Results and Discussion

The system was evaluated based on recognition accuracy, performance speed, and anti-spoofing reliability. Initial results indicate an average accuracy of 92% for face recognition and 95% for anti-spoofing, proving the effectiveness of our approach. False negatives were minimized by adjusting YOLO’s sensitivity, enhancing spoof detection. Challenges faced included training time due to the dataset size and occasional false rejections, which can be addressed in future iterations by including more diverse data samples.

1. Conclusion

In conclusion, our proposed face recognition system with anti-spoofing capabilities achieved high accuracy and efficiency, meeting the demands for secure identity verification in attendance systems. The integration of ResNet50, InceptionV3, and YOLOv8 proved to be effective in enhancing system robustness. Future improvements could involve expanding the dataset to cover a wider demographic range and integrating additional features, such as infrared sensors, to further enhance spoof detection and system security.

Notes: Most of the paragraphs are enhanced by GPT because my writing skills sucks