DA-221M Course project
Image Spoof Detection System

Jan 2025 - Apr 2025

1 Team Contributions

- Bipan Chandra(230102072):Module 1
- Pratik Ranjan(230123046):Module 2
- Rithvik Ponnapalli(230123052):Module 3
- Rehan Sherawat(230123077):Module 4

Abstract

This project implements a multi-stage image spoof detection system that integrates various detection techniques including deepfake detection, 3D mask spoofing detection, and 2D image forgery detection. The system is built with separate modules for each detection technique and integrated into a full pipeline.

2 Module 1: Data Acquisition and Preprocessing

We implemented a Flask-based web application that enables real-time image forgery detection by integrating both deep learning and traditional machine learning models. The backend supports three models: MobileNet, EfficientNet, and an SVM classifier trained on LBP features.

- **LTV Preprocessing:** The LTV model improves local texture clarity, aiding in better extraction of micro-texture features such as LBP, which are crucial for detecting subtle forgery patterns.
- **For MobileNet and EfficientNet**, the uploaded image is resized to 224×224 pixels and normalized to the $[0, 1]$ range to match the deep learning model input formats.
- **For the SVM classifier**, the image undergoes grayscale conversion, followed by Total Variation (TV) denoising using the Logarithmic Total Variation (LTV) model. This step enhances edge structures and suppresses noise prior to feature extraction.
- Local Binary Pattern (LBP) features are extracted from the denoised image and used as input to the SVM model for classification between real and fake.

- Each model generates a confidence score, which are averaged to produce a combined prediction score. The final output is determined using a fixed threshold(0.5).

3 Module 2: 2D Image Forgery Detection and Deployment

Data set: The Large Crowdcollected Face Anti-Spoofing Dataset (CASIA-FASD) is a widely-used benchmark for face anti-spoofing research. It includes real and spoof face videos captured under varying resolutions and attack types such as print, replay, and mask, providing a diverse and challenging dataset for evaluating spoof detection methods.

Model:

- A global average pooling layer to reduce the spatial dimensions of the feature maps.
- A dropout layer to prevent overfitting during training. A sigmoid output layer for binary classification (real or forged).
- A batch normalization layer to stabilize the learning process and speed up convergence.
- Fine-tuning of the deeper layers while freezing the initial layers to retain low-level feature extraction.Data augmentation techniques such as rotation, flipping, and scaling to increase the diversity of the training data and improve generalization.

Results: Performance of MobileNetV2: Accuracy (97.90%), Precision (99.69%), Recall (95.86%), F1 Score (97.73%).

4 Module 3: Deepfake Detection

Data set: The 140k Real and Fake Faces Dataset consists of 70k real faces from the Flickr dataset and 70k fake faces generated using StyleGAN. The images are resized to 256px and split into training, validation, and test sets. CSV files are also included for convenience. The dataset is designed to aid deepfake detection research. For more details, links to discussions on the real faces dataset and the 1 Million Fake Faces are provided

Model:

- Integrated Dlib for face detection and landmark extraction.Extracted head pose estimation features.Landmarks and pose vectors were extracted for both horizontal and vertical orientation stability.Detection focused on inconsistencies in facial dynamics and head movement.
- Fine-tuned an EfficientNetB0 model pre-trained on ImageNet to perform binary classification for image forgery detection.
- Extended the model with dense layers, batch normalization, LeakyReLU activations, and dropout.The first half of the base layers was frozen initially and trained for 2 epochs using Adam optimizer.

Results: Achieved strong performance on test data: Accuracy (98.23%), Precision (98.62%), Recall (97.83%), F1 Score (98.22%).

5 Module 4: 3D Mask Spoofing Detection

Data set: The system uses two datasets for training and evaluation: the Labeled Faces in the Wild (LFW) dataset for real face images and spoof faces generated from videos of individuals wearing silicon masks. The LFW dataset provides genuine face images, while the spoof faces simulate realistic presentation attacks.
Data augmentation techniques were applied to the spoof images to balance the dataset and prevent classifier bias.

Model:

- Focused on distinguishing real vs mask through micro-texture analysis.
- Used LBP techniques (Local Binary Pattern) to extract micro-texture features.Performed 'uniform' LBP with radius 3 and a radius of 24 sampling points.
- Converted images to grayscale and applied Total Variation denoising.Created and normalized LBP code histograms for each image.
- Implemented an SVM classifier with LBP feature sets and an RBF kernel.Dataset contains LFW image dataset for real faces and extracted frames from mask video sequences.

Results: Achieved strong performance on test data: Accuracy (95.63%), Precision (96.00%), Recall (96.00%), F1 Score (96.00%).

6 Results

The final prediction is computed as the average of the three model outputs. A threshold of 0.5 is used to make a binary decision of whether the image is original or a spoof(Dupilcate)

Figure 1: Home page

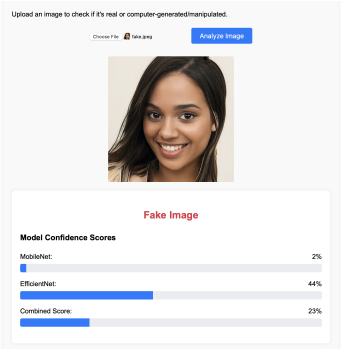

Figure 2: Results page

Conclusion

All modules were independently developed and integrated into a unified image spoof detection pipeline that classifies image authenticity by passing them through sequential checks. Techniques such as LBP for texture analysis and CNN models for forgery detection were crucial in improving accuracy.