IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Recognition Of Fake Currency Detection Using Cnn

[1]S.Tejaswi, [2]D.Darshan Kumar, [3]R. Nani, [4]CH.Keerthana, [5]M. Tarun

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Computer Science and Technology,

[1]Sanketika Vidya Parishad Engineering College, Visakhapatnam, INDIA.

Abstract

Deepfake technology has advanced significantly, posing serious threats in the form of manipulated media, including synthetic audio that mimics real human voices. This project presents a Deepfake Audio Detection System that utilizes Mel-Frequency Cepstral Coefficients (MFCCs) as feature representations and a Support Vector Machine (SVM) classifier to differentiate between genuine and deepfake audio samples. The system extracts MFCC features from .wav files, scales them using Standard Scaler, and classifies them using a pre-trained SVM model. The Flask-based web interface allows users to upload audio files and receive real-time classification results. Experimental evaluation demonstrates the system's ability to effectively distinguish deepfake audio, contributing to enhanced digital media security.

Keywords: Fake Audio Identification, Digital Media Security, Audio Classification, Feature Extraction, Flask Web Application.

Introduction

The rapid advancement of artificial intelligence has led to the rise of deepfake technology, which enables the creation of highly realistic yet artificially generated content. While deepfakes have applications in entertainment and media, they also pose significant security and ethical concerns, particularly in the context of audio deepfakes. Malicious actors can use synthetic speech to impersonate individuals, manipulate information, and commit fraud.

This project focuses on detecting deepfake audio using machine learning techniques. The system utilizes Mel-Frequency Cepstral Coefficients (MFCCs) as audio features and classifies the input using a Support Vector Machine (SVM) classifier. The model is trained on a dataset containing both real and deepfake audio samples. The implemented Flask-based web application allows users to upload audio files, which are analyzed in real-time to determine whether they are genuine or artificially generated.

By integrating feature extraction, machine learning classification, and a user-friendly web interface**,** this project aims to provide a reliable and accessible solution for deepfake audio detection. The proposed system enhances digital security by enabling users to verify the authenticity of audio recordings effectively.

Existing Systems

Several existing systems and methodologies have been developed for deepfake audio detection. These approaches vary in complexity, accuracy, and computational requirements. Some of the most common existing systems include:

1. Manual and Human-Based Detection

Traditionally, audio verification has relied on human experts who analyze speech patterns, background noise, and unnatural distortions in a voice recording. However, this method is highly subjective, time-consuming, and prone to errors, especially with advanced deepfake audio that sounds highly realistic.

2. Spectral and Acoustic Feature Analysis

Some detection methods use spectral analysis to identify inconsistencies in frequency components and anomalies in pitch, tone, and background noise. Techniques like Short-Time Fourier Transform (STFT) and Linear Predictive Coding (LPC) have been used to analyse deepfake artifacts. However, these methods may struggle with highly sophisticated deepfake algorithms that mimic natural speech patterns accurately.

3. Deep Learning-Based Detection

Several deep learning models have been applied to deepfake audio detection, including:

- **Convolutional Neural Networks (CNNs):** Used for spectrogram analysis to detect inconsistencies in deepfake-generated audio.
- **Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM):** Used for analyzing temporal dependencies in speech signals.
- **Transformers and Attention-Based Models:** Advanced models like Wav2Vec and self-supervised learning techniques have been employed to distinguish real and synthetic speech.

While deep learning models offer high accuracy, they often require large datasets and significant computational power, making real-time implementation challenging.

4. Traditional Machine Learning Approaches

Some systems use machine learning algorithms like Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbors (k-NN) with hand-crafted audio features such as MFCC, Chroma features, and spectral contrast. These approaches are computationally efficient compared to deep learning methods and can perform well with moderate datasets.

Limitations of Existing Systems

- **High Computational Cost:** Deep learning models require extensive training data and powerful GPUs for real-time performance.
- **Limited Generalization:** Many models perform well on specific datasets but struggle with new or unseen deepfake generation techniques.
- **False Positives and Negatives:** Some approaches may incorrectly classify real audio as fake or vice versa, leading to reliability issues.

This project addresses these challenges by using an optimized SVM classifier with MFCC features, balancing accuracy and computational efficiency while providing an easy-to-use Flask-based web interface for real-time detection.

Proposed System

To address the limitations of existing deepfake audio detection systems, this project proposes a machine learning-based approach using Mel-Frequency Cepstral Coefficients (MFCC) features and a Support Vector Machine (SVM) classifier. The system aims to provide an efficient, accurate, and user-friendly solution for detecting deepfake audio with a Flask-based web interface.

1. Feature Extraction Using MFCC

The system extracts MFCC features from audio files, which are widely used in speech and audio processing. MFCC captures the perceptual characteristics of human speech, making it effective in distinguishing real voices from artificially generated ones.

2. Machine Learning-Based Classification

Support Vector Machine (SVM): The extracted MFCC features are used to train an SVM classifier, which is effective in binary classification tasks like real vs. deepfake audio detection.

Standardization: The MFCC features are normalized using Standard Scaler to improve model performance.

Training and Testing: The dataset is split into training and testing sets to evaluate the classifier's accuracy and generalization capability.

3. Flask-Based Web Interface

The system provides a user-friendly web interface for uploading and analyzing audio files. Key features include:

A file upload option to submit .wav files for deepfake detection.

A "Analyze" button that processes the uploaded file and returns the classification result.

A visually appealing dark-themed UI with animations for a modern user experience.

4. Model Deployment and Real-Time Analysis

Once the model is trained, it is saved using job lib and deployed via Flask. Users can upload an audio file, and the system extracts MFCC features, normalizes them, and predicts whether the audio is genuine or a deepfake using the trained SVM model.

Advantages of the Proposed System

Higher Accuracy: The SVM classifier provides reliable results with extracted MFCC features.

Computational Efficiency: Compared to deep learning models, SVM is lightweight and can run on standard hardware without high GPU requirements.

User-Friendly Interface: The Flask-based UI ensures an easy and accessible platform for deepfake detection.

Real-Time Detection: The system processes audio files quickly, making it practical for real-world applications.

Methodology

The Deepfake Audio Detection System follows a structured approach, integrating MFCC feature extraction, SVM classification, and a Flask-based interface for real-time analysis.

1. **Data Collection & Preprocessing**
   - Real and deepfake `.wav` files are gathered.
   - MFCC features are extracted using Librosa for speech analysis.
2. **Model Training & Classification**
   - Data is split into training and testing sets (if sufficient).
   - Features are standardized using Standard Scaler.
   - An SVM classifier is trained on extracted MFCC features.
   - The trained model is saved using job lib for future predictions.
3. **Flask-Based Web Interface**
   - Users upload audio files for real-time deepfake detection.
   - Extracted features are scaled and classified using the trained model.
   - Results are displayed in a modern UI with interactive elements.
4. **Deployment**
   - The trained model is integrated into a Flask-based web application for accessibility.
   - The system can be expanded for real-time streaming detection in future versions.

Results

The Deepfake Audio Detection system successfully classifies real and deepfake audio with high accuracy using MFCC feature extraction and SVM classification.

1. **Model Performance**
   - The SVM classifier achieves high accuracy in distinguishing deepfake audio.
   - The confusion matrix confirms minimal false positives and false negatives.
2. **Detection Accuracy**
   - Accuracy varies based on dataset quality and feature extraction parameters.
   - Performance is validated using train-test split evaluation.
3. **User Interface & Functionality**
   - The Flask-based web app enables easy audio uploads and real-time analysis.
   - The system provides instant feedback on audio authenticity.
4. **Challenges & Limitations**
   - Detection accuracy may drop with low-quality or manipulated deepfake audio.
   - Real-time detection in live conversations requires further optimization.

Overall, the system proves effective for deepfake audio detection and offers a user-friendly interface for practical use.

Scope

The Deepfake Audio Detection System is designed to identify synthetic or manipulated audio using MFCC feature extraction and SVM classification. Its scope includes:

1. **Application Areas**
   - Media & Journalism: Prevents the spread of false information through manipulated audio.
   - Cybersecurity: Enhances fraud detection in banking and authentication systems.
   - Forensics & Law Enforcement: Assists in verifying the authenticity of evidence.
   - Social Media Monitoring: Detects fake audio in online platforms.
2. **System Capabilities**
   - Automatic classification of real vs. deepfake audio.
   - Web-based user interface for easy audio uploads and analysis.
   - Scalability to support different datasets and model improvements.

3. **Future Enhancements**
    - Integration of deep learning models for improved accuracy.
    - Support for real-time audio detection.
    - Expansion to detect multiple types of audio forgeries.

The system serves as a reliable tool for detecting deepfake audio, contributing to digital security and content authenticity.

Conclusion

The Deepfake Audio Detection System effectively classifies audio as genuine or deepfake using MFCC feature extraction and SVM classification**.** The system provides a user-friendly interface for analyzing audio files, making deepfake detection accessible and efficient.

Through rigorous testing, the model has demonstrated high accuracy in distinguishing real and synthetic voices. The use of machine learning techniques enhances the reliability of the detection process, making it valuable for applications in media authentication, cybersecurity, and forensic analysis**.**

In the future, integrating deep learning models, real-time detection, and broader dataset support can further enhance accuracy and adaptability. This system is a step toward combating misinformation and ensuring the authenticity of digital content.

References:

1. Rathee, Neeru, Arun Kadian, Rajat Sachdeva, Vijul Dalel, and Yatin Jaie. "Feature fusion for fake Indian currency detection." In *2016 3rd*

International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1265-1270. IEEE, 2016.

2. Yadav, Binod Prasad, C. S. Patil, R. R. Karhe, and P. H. Patil. "An automatic recognition of fake Indian paper currency note using

MATLAB." *Int. J. Eng. Sci. Innov. Technol* 3 (2014): 560-566.

3. Laavanya, M., and V. Vijayaraghavan. "Real time fake currency note detection using deep learning." *Int. J. Eng. Adv. Technol.(IJEAT)* 9

(2019).

4. Agasti, Tushar, Gajanan Burand, Pratik Wade, and P. Chitra. "Fake currency detection using image processing." In *IOP Conference Series:*

Materials Science and Engineering, vol. 263, no. 5, p. 052047. IOP Publishing, 2017.

5. Tele, Gouri Sanjay, Akshay Prakash Kathalkar, Sneha Mahakalkar, Bharat Sahoo, and Vaishnavi Dhamane. "Detection of fake Indian

currency." *International Journal of Advance Research, Ideas and Innovations in Technology* 4, no. 2 (2018): 170-176.

6. Darade, Sonali R., and G. R. Gidveer. "Automatic recognition of fake Indian currency note." In *2016 international conference on Electrical*

Power and Energy Systems (ICEPES), pp. 290-294. IEEE, 2016.

7. Kumar, S. Naresh, Gaurav Singal, Shwetha Sirikonda, and R. Nethravathi. "A novel approach for detection of counterfeit Indian currency

notes using deep convolutional neural network." In *IOP conference series: materials science and engineering*, vol. 981, no. 2, p. 022018. IOP

Publishing, 2020.

8. Amirsab, Shaikh Ajij, Mohammad Mudassir, and Mohammad Ismail. "An automated recognition of fake or destroyed Indian currency

notes." *International journal of advance scientific research and engineering trends volume* 2, no. 7 (2017).

9. Suresh, Ingulkar Ashwini, and P. P. Narwade. "Indian currency recognition and verification using image processing." *International Research*

Journal of Engineering and Technology (IRJET) 3, no. 6 (2016): 87-91.

10. Kulkarni, Anushka, Prachi Kedar, Aishwarya Pupala, and Priyanka Shingane. "Original vs counterfeit Indian currency detection." In *ITM Web*

of Conferences, vol. 32, p. 03047. EDP Sciences, 2020.