



Deep fake Face Detection Using Deep Learning

N SaiLakshmi Kumari¹, P Haritha², S Bhavitha³, P Pooja⁴, S S Sharmila⁵

^{*1} Professor, Department of ECE, Dr. Lankapalli Bullayya College of Engineering, Visakhapatnam, Andhra Pradesh, India.

^{*2, 3, 4, *5} Department of ECE, Dr. Lankapalli Bullayya College of Engineering, Visakhapatnam, Andhra Pradesh, India.

To Cite this Article: N SaiLakshmi Kumari¹, P Haritha², S Bhavitha³, P Pooja⁴, S S Sharmila^{*5}, "Deep fake Face Detection Using Deep Learning", Indian Journal of Electronics and Communication Engineering, Volume 02, Issue 01, January-April 2025, PP: 32-33.

Abstract: Advancements in artificial intelligence (AI) have significantly enhanced the ability to generate realistic deepfake videos, raising concerns about their potential misuse in domains such as political misinformation and cybercrime. To address this issue, our research presents a deep learning-based approach utilizing LBPNET, which integrates Local Binary Patterns (LBP) with Convolutional Neural Networks (CNNs). The proposed methodology involves extracting LBP features from images, training a CNN using these features, and developing a model capable of differentiating between real and fake images. The model is rigorously tested to evaluate its effectiveness in deepfake detection.

Key words: Deepfake Detection, LBPNET, LBP Features, CNN, Feature Extraction, Fake Images, Model Training, Classification.

I.INTRODUCTION

The rapid evolution of deepfake technology has made it increasingly difficult to detect manipulated images and videos. Various methods are available for identifying deepfake content, such as analyzing inconsistencies in facial structures, lighting anomalies, and unnatural eye-blinking patterns. Additional indicators include discrepancies between facial expressions and audio cues. Advanced deep learning models, including CNNs and RNNs, are widely utilized for deepfake detection. Supplementary techniques such as metadata analysis, reference data comparison, and blockchain-based authentication further strengthen the verification process. Although AI-driven tools are highly effective, human intervention remains crucial for detecting subtle anomalies that automated systems may overlook. A hybrid approach integrating AI-based detection with human oversight provides a more robust solution for deepfake identification.

II.METHODOLOGY

The proposed approach, illustrated in Figure 1, involves analyzing deepfake images sourced from both authentic and manipulated facial datasets. The dataset is divided into 90% training and 10% testing sets. The LBP method is optimized to enhance accuracy, and the CNN model is trained using these extracted LBP features. The performance of the trained model is then evaluated using the test data.

Steps in Model Development: Dataset Preparation: Collection of real and manipulated facial images.

Data Splitting: 90% of the dataset is used for training, and 10% for testing.

Feature Extraction: Application of the LBP method to improve accuracy.

Neural Network Training: CNN is trained using extracted LBP features.

Model Evaluation: Performance is validated using unseen test images.

III.MODELING AND ANALYSIS

Hardware Requirements: Processor: Dual-Core

RAM: 2 GB

Storage: 5 MB Hard Disk Space

Software Requirements: Python: A high-level, object-oriented programming language known for its dynamic typing, automatic memory management, and extensive library support, maintained by the Python Software Foundation.

The dataset used for model training and evaluation was obtained from Kaggle, contributed by Yonsei University's Department of Computer Science. It consists of manually labeled real and fake facial images, including:

133 real images

165 fake images

Local Binary Patterns (LBP): Local Binary Patterns (LBP) is a powerful texture descriptor widely used in computer vision tasks. It labels pixels based on their neighborhood values, generating binary numbers for classification. The LBP operator is highly effective due to its robustness against monotonic grayscale variations caused by illumination changes. Additionally, its

computational simplicity makes it ideal for real-time applications.

IV.RESULTS AND DISCUSSION

Our study employs LBPNET, a CNN-based architecture incorporating LBP features for deepfake detection. The process involves:

Feature Extraction: LBP features are extracted from images.

Model Training: CNN is trained using extracted descriptors.

Testing & Classification: The trained model classifies images as real or fake.

The model achieved high accuracy in detecting fake images, demonstrating its effectiveness. Further improvements can be achieved by expanding the dataset and periodically retraining the model. Additionally, real-time user testing can refine the model's performance by enabling it to adapt to new deep fake variations.

V.CONCLUSION

This research presents a deepfake detection approach utilizing a Common Fake Feature Network (CFFN) with pairwise learning. The CFFN integrates cross-layer feature representations into fully connected layers, significantly improving the precision and recall rates for identifying manipulated images. Experimental evaluations demonstrate that the proposed model surpasses conventional deepfake detection techniques. By leveraging pairwise learning, the model can effectively adapt to emerging deepfake trends, making it a valuable tool in digital forensics and media integrity verification.

REFERENCES

1. M. M. El-Gayar, M. Abouhawwash, S. S. Askar, and S. Sweidan, "A Novel Approach for Detecting Deepfake Videos Using Graph Neural Networks," *Journal of Big Data*, vol. 11, 2024, pp. 1-22, DOI: 10.1186/s40537-024-00884-y.
2. A. Brock, J. Donahue, and K. Simonyan, "Large-scale GAN Training for High-Fidelity Natural Image Synthesis," *arXiv Preprint, arXiv: 1809.11096*, 2018.
3. J. Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks," *arXiv Preprint*, 2017.
4. H. T. Chang, C. C. Hsu, and C. Y. D. S., "Image Authentication with Tampering Localization Based on Watermark Embedding in the Wavelet Domain," *Optical Engineering*, vol. 48, 2009, pp. 057002.