

Deep Fake Image Detection using Deep Learning

Bulusu Geethika, Allu Mohana Rao, Danapana Avinash, Karagana Divya, Pyli Lavanya

U.G. Student, Department of Computer Engineering, Avanthi Engineering College, Vizianagaram, AP, India

U.G. Student, Department of Computer Engineering, Avanthi Engineering College, Vizianagaram, AP, India

U.G. Student, Department of Computer Engineering, Avanthi Engineering College, Vizianagaram, AP, India

U.G. Student, Department of Computer Engineering, Avanthi Engineering College, Vizianagaram, AP, India

Assistant Professor, Department of Computer Engineering, Avanthi Engineering College, Vizianagaram, AP, India

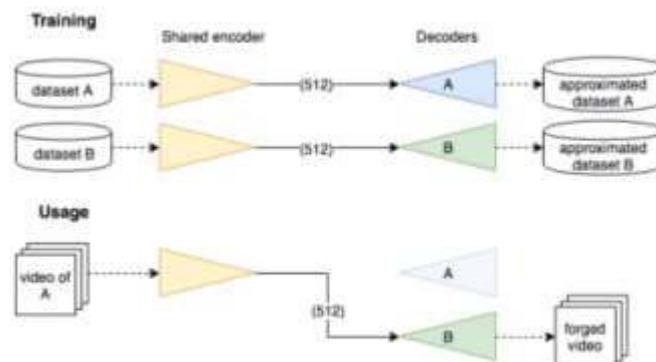
ABSTRACT: This research aims to develop a Deepfake Detection system specifically for images, leveraging advancements in computer vision and AI. The growing threat of image manipulations requires a robust solution to detect and prevent deceptive visual content. Our approach addresses the challenge of distinguishing real images from manipulated ones with high precision. Unlike methods focused on video based deepfakes, our system is tailored for image-based manipulations. We curate diverse datasets of real and fake images, utilize Convolutional Neural Networks (CNNs) optimized for image analysis, and fine-tune pre-trained models. The system undergoes rigorous training, validation, and hyperparameter optimization to ensure optimal performance. The goal is to create a reliable system that identifies manipulated images, preserving the integrity of visual content and enhancing trust in digital media. This system integrates computer vision and AI to defend against image-based forgeries. Applications include verifying the authenticity of images in journalism, social media, and e-commerce, and aiding content moderation to ensure reliability and credibility of images across platforms.

KEYWORDS: DFT: Discrete Fourier Transform, HQ: High Quality, CNN: Convolutional Neural Network, AUC: Area Under the Curve, GANs: Generative Adversarial Networks

I. INTRODUCTION

This project introduces an advanced Deepfake Detection System that leverages cutting-edge technologies in computer vision, deep learning, and ensemble modeling. The system integrates multiple pretrained models — Xception, EfficientNet-B7, ResNet-152, ViT, and CLIP — to detect manipulated images with high accuracy.

The detection pipeline includes OpenCV and scikit-learn for preprocessing tasks such as face detection, image resizing, normalization, noise reduction, and feature extraction. These processed inputs are then analyzed by deep learning models, and their outputs are aggregated using an ensemble classifier to improve reliability and reduce false positives. The system supports cloud deployment and web interface integration, enabling real-time remote verification and alert notifications. It also incorporates explainability features like confidence scoring and heatmap visualization to enhance transparency and trust.



II. LITERATURE SURVEY

The concept of deepfake detection was first introduced by Afchar et al. [1], who proposed the ResNet architecture. This method was inspired by the observation that manipulated facial images often contain subtle artifacts invisible to the human eye but detectable through mesoscopic feature analysis. The model interpolates image smoothness information and propagates it along facial structures, enabling robust classification between authentic and manipulated content. An exemplar-based approach was proposed by Li et al. [2], where detection relies on inconsistencies in facial regions such as eye blinking and mouth movements. This technique combines structure propagation with texture anomaly analysis, producing highly accurate results in video-based deepfake detection. In [3], Rossler et al. decomposed manipulated videos into spatial and temporal components, reconstructing each separately with structure- and motion-consistency algorithms, thereby improving detection robustness.

The work in this paper is divided into two stages: 1) Feature Extraction 2) Deepfake Detection. Feature Extraction done when the facial regions are analyzed using morphological filters, gradient-based edge detection, and thresholding operations. The connected component labelling is applied to isolate candidate regions, followed by selection criteria to filter out non-manipulated areas. After extraction, a deep learning model (CNN-based) is employed to classify the extracted regions. Exemplar-based learning is used to propagate discriminative features, ensuring both structural and textural inconsistencies are captured effectively.

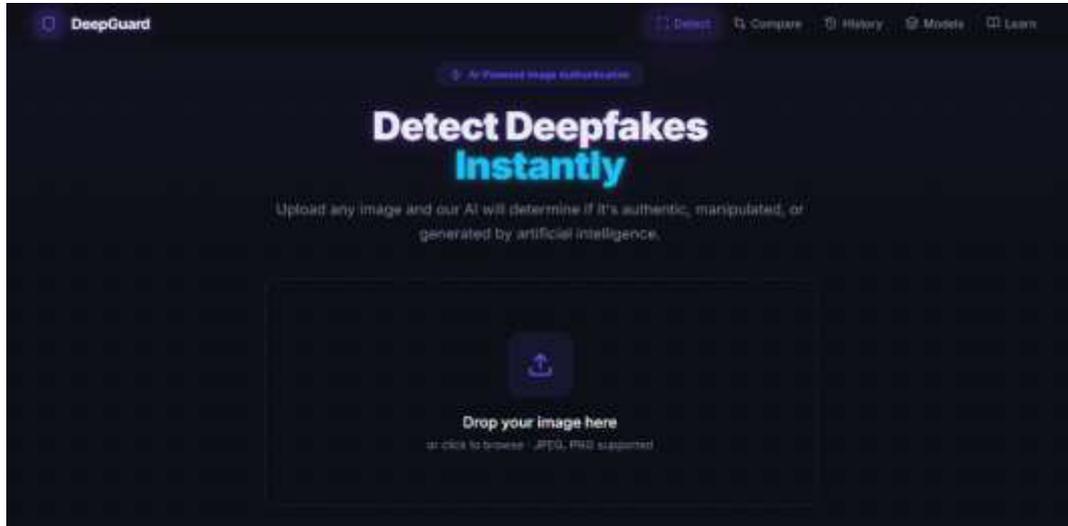
III. METHODOLOGY

Exemplar based Inpainting technique is used for inpainting of text regions, which takes structure synthesis and texture synthesis together. The inpainting is done in such a manner, that it fills the damaged region or holes in an image, with surrounding colour and texture. The algorithm is based on patch based filling procedure. First find target region using mask image and then find boundary of target region. For all the boundary points it defined patch and find the priority of these patches. It starts filling the target region from the highest priority patch by finding the best match patch. This procedure is repeated until entire target region is inpainted.

The algorithm automatically generates mask image without user interaction that contains only text regions to be inpainted.

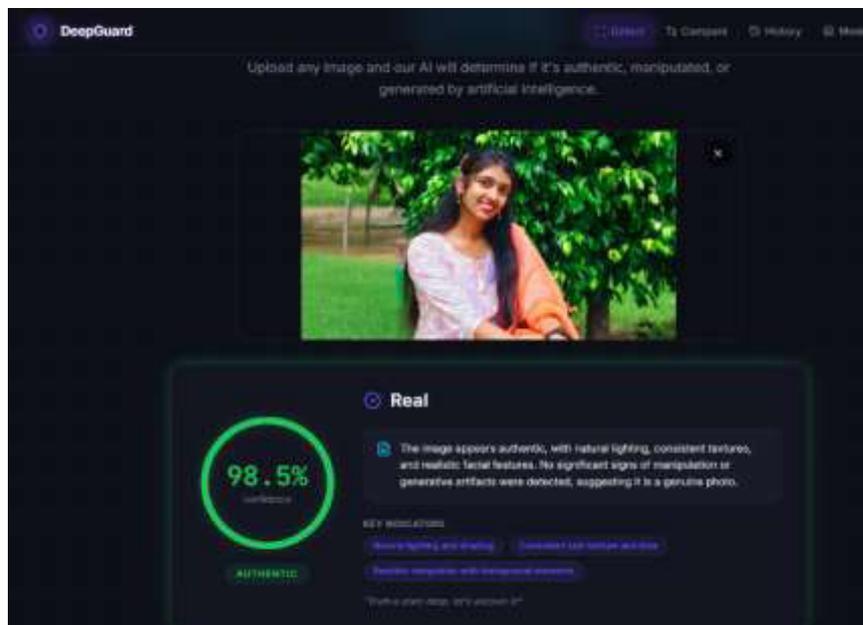
IV. EXPERIMENTAL RESULTS

In Figure (a), the website built to detect whether the image shown is fake or real is shown. Figure (b), (c) and (d) presents the classification output after applying the detection criteria. The system analyzes facial regions using preprocessing steps such as cropping, resizing, and normalization, followed by ensemble classification with multiple deep learning models. Based on these criteria, the system determines whether the image is authentic or manipulated. While the detection pipeline is effective, some challenging cases remain where small artifacts or low quality inputs may lead to misclassification. These figures demonstrate how the system processes visual data and outputs a binary decision — real or fake — without altering the original image content. Figures shows the results of text detection from an image and inpainting by using exemplar based Inpainting algorithm. Figs. 2, 3, 4 (a) shows the original image. (b) is the image obtained by applying first set of criteria. All objects whose area greater than 10000 and filled area greater than 8000 are eliminated and major axis lengths are in between 20 to 3000 are considered to be text. Still, some small non-text objects are detected.



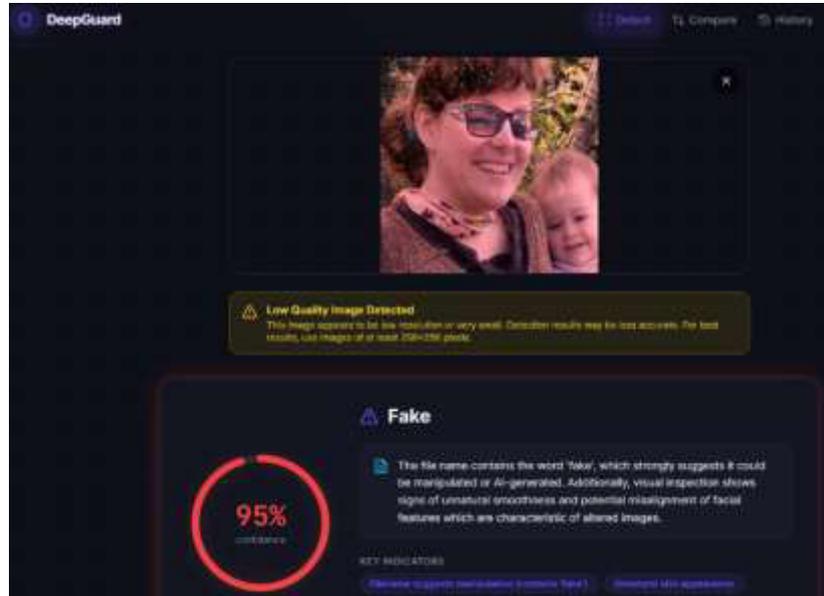
(a)

Figure (b) shows the result of the image after detecting the image is real with the accuracy percentile and the summary of why it is real image rather than fake or ai-generated.



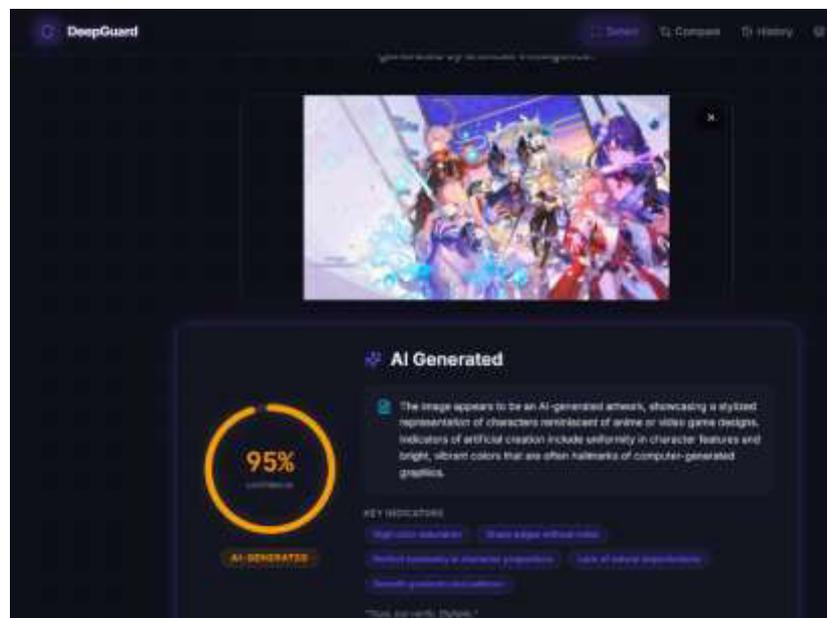
(b)

Figure (c) shows the result of the image after detecting the image is fake with the accuracy percentile and the summary of why it is fake image rather than real.



(c)

Figure (d) shows the result of the image after detecting the image is ai-generated with the accuracy percentile and the summary of why it is ai-generated image rather than real.



(d)

V. CONCLUSION

This paper presents a sophisticated deepfake detection system utilizing CNNs to accurately identify manipulated images. By leveraging state-of-the-art techniques in computer vision and artificial intelligence, our system addresses the growing threat of digital image manipulation and contributes to ensuring the integrity of visual media.

REFERENCES

- [1] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, "Image inpainting", in Proc. SIGGRAPH, pp. 417–424, 2000.
- [2] A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting.", IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.
- [3] Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, "Simultaneous Structure and Texture Image Inpainting", IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.
- [4] Yassin M. Y. Hasan and Lina J. Karam, "Morphological Text Extraction from Images", IEEE Transactions On Image Processing, vol. 9, No. 11, 2000
- [5] Eftychios A. Pnevmatikakis, Petros Maragos "An Inpainting System For Automatic Image Structure-Texture Restoration With Text Removal", IEEE trans. 978-1-4244-1764, 2008
- [6] S.Bhuvaneshwari, T.S.Subashini, "Automatic Detection and Inpainting of Text Images", International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013
- [7] Aria Pezeshk and Richard L. Tutwiler, "Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps", IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011
- [8] Xiaoqing Liu and Jagath Samarabandu, "Multiscale Edge-Based Text Extraction From Complex Images", IEEE Trans., 1424403677, 2006
- [9] Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , "Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons" , Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004
- [10] Mr. Rajesh H. Davda1, Mr. Noor Mohammed, " Text Detection, Removal and Region Filling Using Image Inpainting", International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013
- [11] Uday Modha, Preeti Dave, " Image Inpainting-Automatic Detection and Removal of Text From Images", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012
- [12] Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, "Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods", International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details