IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

Deepfake Detection using Deep Learning

Dr. B. M Vidyavathi[1], Mr. Adnaan Faisal Ahmed[2], Ms. Lulu Ayain T[3], Mr. Mohammad Huzair[4], Ms. Syeda Mehraj Fatima[5]
Head of the Department, Department of Artificial Intelligence and Machine Learning[1]
Students, Department of Artificial Intelligence and Machine Learning[2,3,4,5]
Ballari Institute of Technology and Management, Ballari, Karnataka, India

Abstract: *The detection of deep fakes, which are synthetic media generated using deep learning techniques, has become increasingly important due to their potential to deceive and manipulate individuals, organizations, and society at large. This abstract explores recent advancements in deep fake detection methodologies, including machine learning algorithms, neural network architectures, and forensic techniques. Key challenges such as the rapid evolution of deep fake generation methods and the emergence of highly realistic forgeries are discussed. Additionally, the abstract examines the ethical implications of deep fake technology and the need for robust detection methods to mitigate its harmful effects. Finally, future directions in deep fake detection research are outlined, emphasizing the importance of interdisciplinary collaboration and the development of innovative approaches to combat this growing threat to information integrity and trust*

Keywords: deepfake

I. INTRODUCTION

Deep fake detection involves identifying manipulated or synthesized media, often using artificial intelligence. As technology advances, deep fakes, which are realistic-looking but fabricated content, pose challenges in various domains. Detection methods include analyzing facial inconsistencies and leveraging machine learning algorithms trained on authentic data to differentiate real from manipulated content. With the rapid advancement of deep learning techniques, the rapid increase of deep fake content has become a significant challenge in the digital era. This research proposes a novel approach for harnessing artificial intelligence (AI) in image classification, specifically targeting the identification and classification of deep fake images. The integration of deep learning models enables the development of robust systems capable of discerning authentic from manipulated visual content. This study focuses on enhancing the accuracy and reliability of deep fake classification, contributing to the ongoing efforts in mitigating the adverse impacts of synthetic media. Deepfake detection using deep learning relies on neural networks to distinguish between authentic and manipulated content. These models are trained on extensive datasets of both real and synthetic media, learning patterns and features indicative of manipulation. Common techniques include using convolutional neural networks (CNNs) for image analysis. By leveraging the power of deep learning, these systems aim to identify subtle inconsistencies or artifacts created during the deepfake generation process.

II. LITERATURE SURVEY

SL.NO	Title	Author(s) & Citation	Findings
[1]	DeepFake Detection Using convolutional Neural Networks	A. Singh, B. Singh, and M. Vatsa et al, IEEE Transactions on Information Forensics and Security, 2020	The paper proposes a method for detecting deepfakes using transfer learning on the VGG-16 model, focusing on facial manipulation detection. It emphasizes the need for continuous improvement in detection techniques due to the social and political impact of deepfakes. The proposed method performs well but highlights the need for better datasets and combined models, including temporal and audio analysis, to improve accuracy. Future

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

			research should explore ensemble learning and the aggregation of results for enhanced detection capabilities.
[2]	FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals	Y. Li, M. Chang, and S. Lyu et al.in Proc. IEEE Transactions on Image Processing, 2018.	The paper introduces a novel deepfake detector for portrait videos, leveraging biological signals as implicit descriptors of authenticity, which are not preserved in fake content. The proposed method achieves high accuracy by employing signal transformations and CNNs, outperforming baseline detectors and demonstrating robustness across various datasets and conditions. Additionally, an "in the wild" dataset of fake portrait videos is released for evaluation purposes.
[3]	DeepFake: A New Threat to Face Recognition? Assessment and Detection	N. Rössler, D. Cozzolino, and L. Verdoliva, IEEE International Conference on Computer Vision (ICCV), 2019.	This review provides an extensive overview of both indoor and outdoor navigation aids, focusing on location technologies and user feedback methods. The authors classify various types of assistive technologies, such as GPS-based systems and wearable devices, and assess their efficacy in real-world scenarios. The review highlights the importance of accurate localization, real-time data processing, and user-friendly feedback mechanisms for improving mobility. It also identifies the need for more robust data collection, user-centric design, and modular system architectures to adapt to varying environments.
[4]	An Experimental Evaluation on Deepfake Detection using Deep Face Recognition	N. Rössler, D. Cozzolino, and L. Verdoliva, IEEE(2020)	Significant progress in deep learning has achieved high accuracy rates in various computer vision applications. classification problem, using convolutional neural networks (CNNs) to distinguish authentic images or videos from fake ones.

III. METHODOLOGY

- **Input Image:** The image to be analysed for potential deepfake content. Preprocessing: Cleaning and standardizing the input image. This can involve tasks like resizing, noise reduction, or normalization.
- **Feature Extraction:** Extracting relevant features from the image. This step might include identifying facial landmarks, texture analysis, or statistical measures from specific regions of the image.
- **Detection Model:** Deep Features Extraction: Using convolutional neural networks (CNNs) or other deep learning architectures to extract high-level features that are indicative of manipulation.
- **Accuracy test:** To determine whether the image is real or a potential deepfake. This model utilizes extracted features to make a prediction.
- **Output (Real/Fake):** The final output indicating whether the input image is assessed as a real image or identified as a potential deepfake

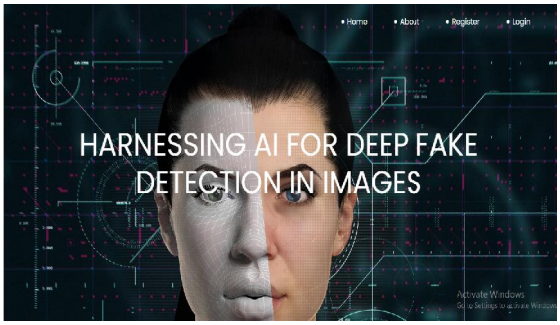
Block Diagram:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

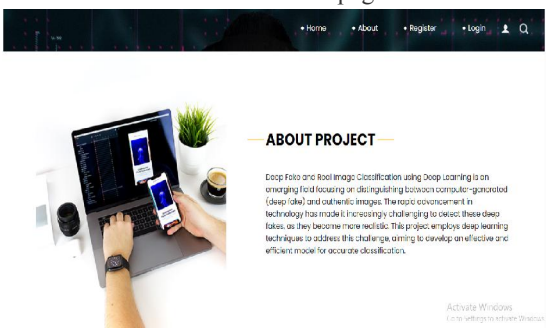
[1], Fig1BlockDiagramofDeepfake detection.

IV. RESULTS AND DISCUSSION

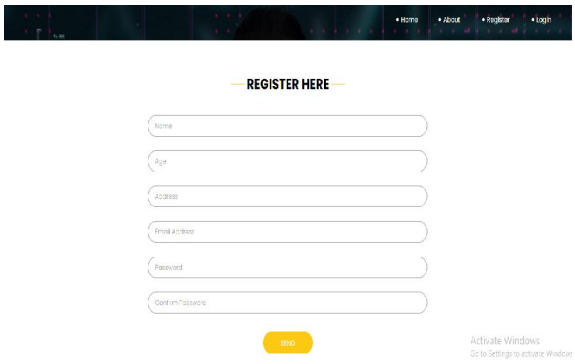
Home page:



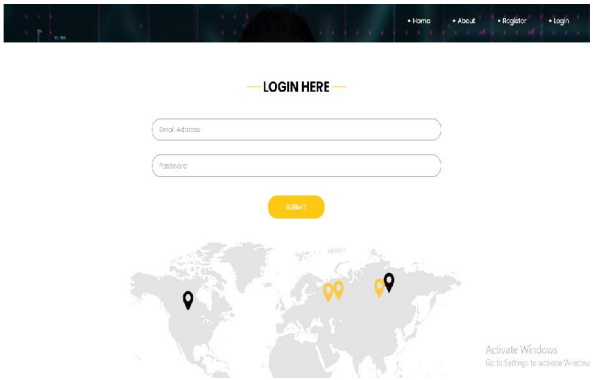
About page:



User registration form



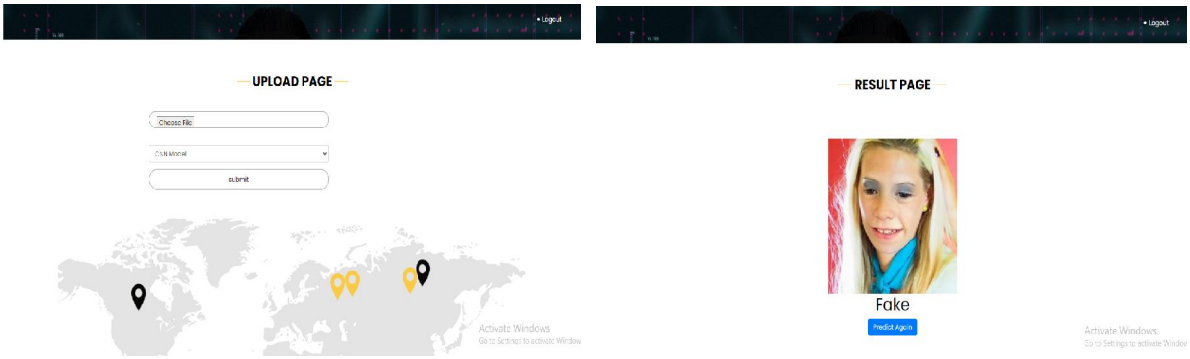
User login form



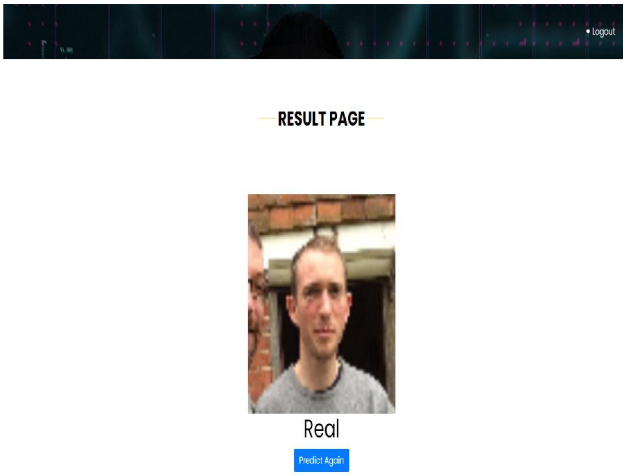
Uploadpage

Result : Fake

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024



Result : Real



V. ACKNOWLEDGEMENT

The satisfactions that accompany with the successful completion of project on "DEEP FAKE DETECTION" would be incomplete without the mention of people who made it possible, whose noble gesture, affection, guidance, encouragement and support crowned our efforts with success.

It is our privilege to express gratitude and respect to all those who inspired us in the completion of project phase-1. We are deeply indebted to our guide, Dr. B M VIDYAVATHI, Department of AIML, for consistently providing us with the required guidance to help us in the timely and successful completion of project .

VI. CONCLUSION

The project on "Deepfake detection", employing Deep fake, image Classification, Convolutional Neural Networks, Transfer Learning, CNN, Mobilenet, VGG16, Deep Learning, Artificial Intelligence aims on enhancing the accuracy and reliability of deep fake classification, Ethical considerations surrounding the use of deepfake technology and its potential societal impact should also be addressed, as the consequences of undetected deepfakes can be profound, ranging from misinformation and reputation damage to more severe threats such as cyber threats. Contributing to the ongoing efforts in mitigating the adverse impacts of synthetic media.

REFERENCES

[1] Lattas, A, Moschoglou, S., Gecer, B., Ploumpis, S., Triantafyllou, V., Ghosh, A., & Zafeiriou, S. (2020). AvatarMe: realistically renderable 3D facial reconstruction "in-the-wild". In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 760769).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, May 2024

[2] Deng, Y., Yang, J., Chen, D., Wen, F., & Tong, X. (2020). Disentangled and controllable face image generation via 3D imitative-contrastive learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5154-5163).
[3] MD SHOHEL RANA, MOHAMMAD NUR NOBI, BEDDHU MURALI, AND ANDREW H. SUNG, (Members, IEEE) (2022) Deepfake Detection: A Systematic literature review.
[4] https://www.kaggle.com/c/deepfake-detection-challenge/data
[5] ASADMALIK, MINORU KURIBAYASHI SANI M. ABDULLAH AND AHMAD NEYAZ KHAN, (Member, IEEE) (2022) Deepfake Detection for Human Face Images and Videos: A Survey