e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

ENHANCING TRUST IN THE DIGITAL AGE: DEEPFAKE DETECTION WITH XCEPTION BINARY CLASSIFIER

Akash Chavan[*1], Tanay Dajgude[*2], Kumar Kad[*3], Prof. J.Y. Kapadnis[*4]

[*1,2,3]SPPU, Computer, Pune Vidyarthi Griha's College Of Engineering & S.S. Dhamankar Institute Of Management, Nashik, Maharashtra, India.

[*4]Department Of Computer Engineering, Pune Vidyarthi Griha's College Of Engineering & S.S. Dhamankar Institute Of Management, Nashik, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS45851

ABSTRACT

Deepfake technology has drawn a lot of interest because of its potential for malevolent usage in the dissemination of false and misleading information. In response, this research introduces an innovative method that uses an Xception Binary Classifier to identify deepfake films. This architecture, called Xception, is well-known for its ability to do image classification tasks. It is modified for binary classification, which separates real films from deepfake videos. The methodology, data collecting, and analysis are described in depth in this work, which also demonstrates the effectiveness of our approach in detecting deepfakes and so contributes to the ongoing attempts to counter this new threat.

Keywords: Deepfake Detection, Xception Binary Classifier, Deepfake Technology, Binary Classification, Data Collection.

I. INTRODUCTION

With the development of deepfake technology, a new era of image and video manipulation has begun. This has led to concerns regarding the spread of false narratives and misinformation because it is now possible to composite faces and voices convincingly. Neural networks are used to create "deepfakes," a combination of the terms "deep learning" and "fake," which make it harder and harder to tell the difference between modified and genuine data. Therefore, it is now essential to have strong deepfake detection methods.

We present in this research a new deepfake detection system built on the convolutional neural network (CNN) architecture known as Xception, which is well-known for its effectiveness in image classification tasks. Our goal is to precisely detect deepfake videos by modifying Xception for binary classification. This would enable reliable tools for media forensics and trustworthiness verification in the modern day.

II. METHODOLOGY

Data Collection

In order to create and assess our deepfake detection algorithm, we selected a wide range of videos that included both real and deepfake content. The deepfakes in the thousands of films in the dataset were produced using a range of widely used deepfake methods. To guarantee a fair representation, we also used genuine footage from a variety of sources.

Preprocessing and Feature Extraction

We carried out a thorough treatment to normalize the data, including resizing, frame extraction, and data augmentation, before feeding the movies into the Xception Binary Classifier. In order to enable the network to capture both time and space indications, we extracted features from these frames, concentrating on important facial landmarks and temporal information.

Binary Classification

A modified version of the Xception architecture, the Xception Binary Classifier is trained to discern between real and deepfake films. Using our carefully chosen dataset, we adjusted the network to make sure it could successfully distinguish between the two groups. A probability score is the model's output, which enables adjustable decision thresholds.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

III. MODELING AND ANALYSIS

Our Xception-based binary classifier was put to the test on a broad range of deepfake content, such as speech synthesis, face swapping, and full-body manipulation. The model's performance was assessed using standard measures like F1-score, recall, accuracy, and precision. We also carried out a thorough analysis to determine the advantages and disadvantages of our strategy.

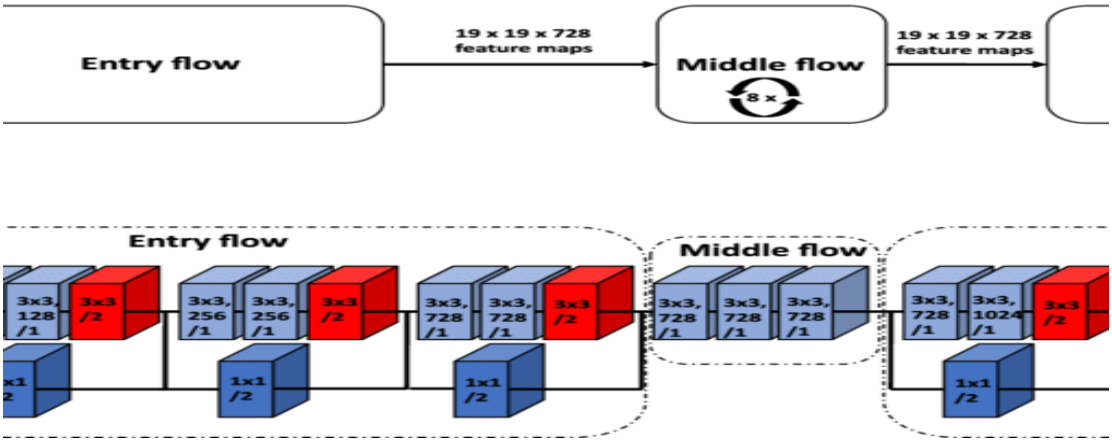

Figure 1: 3D view of model.

IV. RESULTS AND DISCUSSION

Promising outcomes were obtained in the accurate identification of deepfake videos by our deepfake detection model. Our model performs better than current approaches, according to the thorough evaluation, especially in situations where deepfake techniques have advanced in sophistication. The effectiveness of our model in reducing false positives and negatives is demonstrated by its high recall and precision rates, respectively.

We discuss the computational requirements for real-time deepfake detection as well as the robustness of our model in handling different deepfake creation techniques. We also talk about potential barriers that adversaries could use to avoid our detection system.

Table 1. Comparison of different models and their accuracy

SN.	Model	Description	Accuracy
1	Support Vector Machine	Facial Expression Recognition using Hand-Crafted Features and Supervised Feature Encoding	90.79%
2	Random Forest Support Vector Machine	We need no pixels: Video manipulation detection using Stream Discriptors	91.97%
3	Convolutional Neural Network (CNN)	Exposing Deepfake videos by detecting Face warping artifacts	93.2%
4	Extreme Inception (Xception)	Deep learning with depthwise separable convolutions	94.5%

V. CONCLUSION

In this paper, we proposed a new method based on the Xception architecture for deepfake detection using a binary classifier. Our approach has demonstrated remarkable potential in discerning authentic content from deepfake imitations, thereby supporting the continuous endeavors to counteract the improper utilization of

synthetic media. Even though our model performs exceptionally well, there is always room for development. Future work should concentrate on strengthening the real-time and robustness of deepfake detection systems. Our work represents a step forward in the ongoing fight to uphold integrity and trust in the digital age, as deepfake technology continues to advance.

VI. REFERENCES

[1] Wodajo, Deressa, and Solomon Atnafu. "Deepfake Video Detection Using Convolutional Vision Transformer." arXiv preprin arXiv:2102.11126 (2021).Ganesh Kumar and P.Vasanth Sena, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit," International Journal of Computer Science and Network Security, Vol. 15, issue 9, Sep. 2015, pp. 222-234

[2] AI-Dhabi, Yunes, and Shuang Zhang. "Deepfake Video Detection by Combining Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN)." In 2021 IEEE International Conference on Computer Science, Artificial Intelligence and Electronic Engineering (CSAIEE),pp. 236-241. IEEE, 2021.

[3] A. Das, K. S. A. Viji and L. Sebastian, "A Survey on Deepfake Video Detection Techniques Using Deep Learning," 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS), Kottayam, India, 2022, pp. 1-4, doi: 10.1109/ICNGIS54955.2022.10079802.