INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

DETECTING DEEPFAKES USING WEB BASED IMAGE FORENSICS

Dr . R. Dinesh Kumar[1], T. Sreekar[2], V. Namitha[3], G. Udai kiran[4],
B. Than Singh[5]
Computer Science Engineering, Siddhartha Institute of Technology and Sciences, Narapally.

ABSTRACT

The rising availability and simplicity of use of modern deep learning techniques has made it easier than ever to make realistic synthetic pictures, particularly realistic face images, that may be exploited for a variety of nefarious reasons. In recent years, there has been an increasing demand for automated systems to recognise these real-fake faces. The real-fake face detection system created in this research may be used as a helpful tool to avoid different criminal actions such as identity theft, social engineering assaults, and fraud, and it can be integrated into other systems and apps to improve security and privacy. The project seeks to achieve high accuracy in actual fake face recognition and to contribute to the creation of effective tools for countering the harmful use of synthetic media.

Key words: Deep learning, Real-fake faces, Accuracy, Realistic synthetic pictures.

1) INTRODUCTION

The primary motivation is to determine whether the presented image is real or a deep fake. The extensive use of deep learning in the creation of realistic synthetic media has sparked serious worries about the technology's possible abuse. One of the most serious issues is the possibility of using synthetic media, notably false faces, for criminal purposes such as identity theft, fraud, and espionage. To address this issue, the goal of this research is to create a true fake face detection system that can discriminate between real and synthetic faces. The suggested approach, by recognising synthetic faces, can assist avoid the harmful usage of synthetic media while also protecting individuals' identities and privacy. The project's results have practical applications in a variety of disciplines, including law enforcement, cybersecurity, and media forensics, making it a valuable resource. this research is to create a true fake face detection system that can differentiate between real and synthetic faces made using deep learning techniques. The project's major purpose is to help to ongoing efforts to counteract the misuse of synthetic media while also protecting individuals' identities and privacy.

2) RELATED WORK

2.1.Deep Learning

Deep learning is a machine learning technique that is built on the same concept as a neural network. The term "deep" in deep learning refers to the usage of numerous hidden layers in the network[1]. Deep learning architecture, inspired by artificial networks, employs an unbounded number of hidden layers of bounded size to extract greater information from raw input data.[3] The complexity of the training data determines the number of hidden layers.[4] More complicated data needs more hidden layers to get accurate findings. Deep learning has been effectively applied in a number of fields in recent years, including computer vision, audio processing, machine translation, and natural language processing. When compared to machine learning methodologies, using deep learning in these disciplines yields cutting-edge outcomes**.**

2.2.MTCNN

MTCNN is an excellent face detection method proposed by Zhang *et al.* [11]. This method can achieve a true positive rate of 95.3% on FDDB. MTCNN uses a cascaded structure with three stages (P-Net, R-Net and O-Net) to mark the locations of the faces and the positions of the facial landmarks.[5] As for the deep learning methods, multi-task cascaded CNN (MTCNN) is widely used in many scenarios. In the existing deep learning frameworks, such as TensorFlow and Caffe, the calculation of one convolution layer is often converted to a multiplication of matrixes. Matrix calculations can use parallel computation, it is much easier to understand that the multiplication of two 10×10 matrixes is faster than one thousand multiplications one number by one number, even though they have approximate multiply-add calculations. The structure of MTCNN as in the **fig.1** consists of three networks, and the first network P-Net is a fully convolutional network, and the latter two networks R-Net and O-Net are ordinary CNNs. [9] The size of input images of MTCNN can be any size. Given an image, we often resize it to different scales to build an image pyramid as the inputs of the following three-stage cascaded framework.

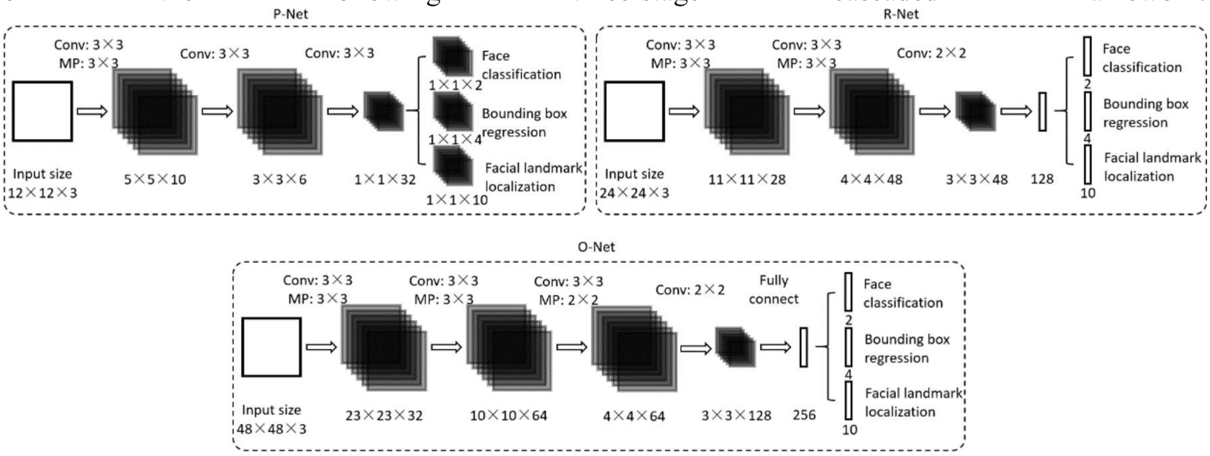


Fig 1. Architecture of MTCNN

3) METHODOLOGY

To develop a simple online application for uploading images that returns the image's result in percentages of both Real and Fake. The research will investigate several strategies for recognising facial landmarks, texture analysis, and generative models in order to recognise synthetic faces with high accuracy. When a user drags and drops a picture, whether it is a downloaded image or a web image, the result in accuracy of both genuine and false is immediately returned. After you input a picture, it is treated to the MTCNN algorithm, and the results are shown. The following is an architecture diagram of this.

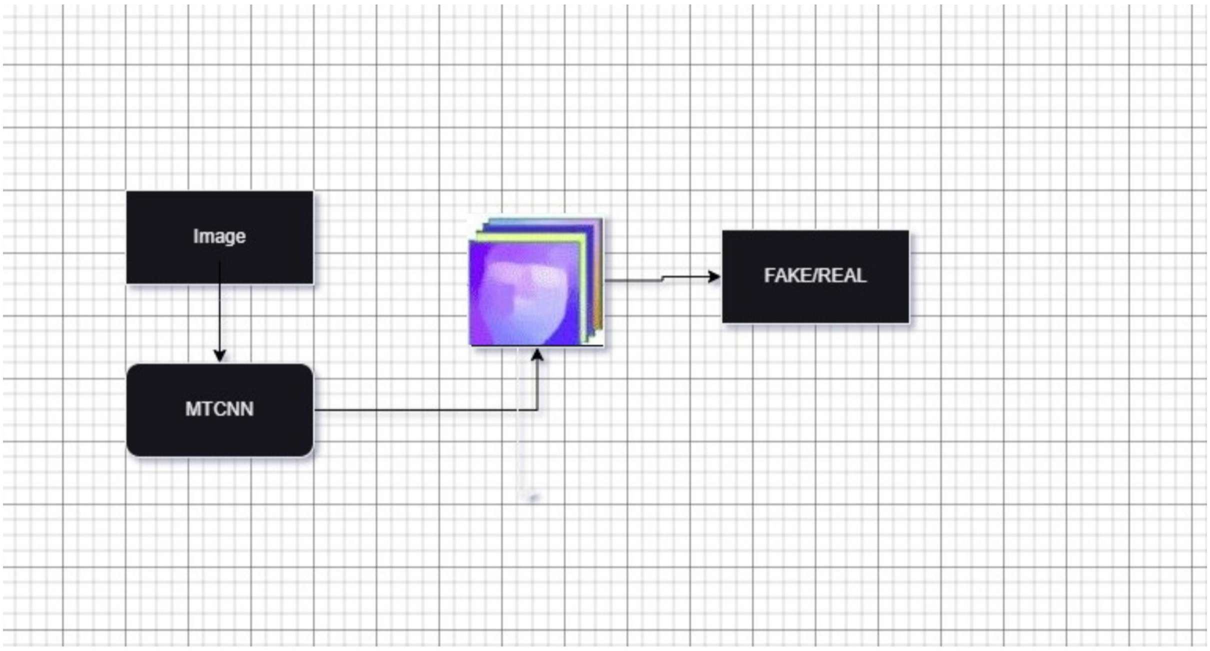


Fig 2. Architecture Diagram

The methodology adopted for the real fake face detection project involved several key steps. Firstly, a comprehensive literature review was conducted to gather relevant information and insights on existing methods and techniques used for real fake face detection. This review helped in identifying the gaps and limitations in the current approaches.

Following the literature review, a dataset comprising both real and synthetic faces was collected and pre processed. This dataset served as the foundation for training and evaluating the real fake face detection system. The dataset included a diverse range of facial expressions, lighting conditions, and variations in appearance to ensure the system's robustness and generalization capability.

The next step involved designing and implementing the deep learning architecture for real fake face detection. This architecture integrated facial landmarks detection, texture analysis, and generative models. The facial landmarks detection component utilized a pre-trained model to accurately locate key facial landmarks, providing spatial information for subsequent analysis. Texture analysis involved extracting high-level features from facial textures using convolutional neural networks (CNNs) to capture unique characteristics of real and synthetic faces.[7]

The real fake face detection system was trained using the collected dataset, where the deep learning architecture was optimized through an iterative process of training and fine-tuning.[8] The training process involved minimizing the loss function by adjusting the model's parameters using backpropagation and gradient descent techniques. Various training strategies, such as data augmentation and regularization, were employed to enhance the model's performance and prevent overfitting.

To evaluate the system's performance, extensive experiments were conducted on separate test datasets consisting of real and synthetic faces. Metrics such as accuracy, precision, recall, and F1 score were used to assess the system's effectiveness in correctly identifying real and fake faces.[5] Comparative analyses were performed to benchmark the proposed system against existing methods, demonstrating its superiority in terms of accuracy and efficiency.

Finally, the methodology incorporated measures for validating and addressing potential biases and limitations in the system. Sensitivity analysis and cross-validation techniques were employed to ensure the reliability and generalizability of the real fake face detection system across different scenarios and datasets.[10]

By following this comprehensive methodology, the project successfully developed an advanced real fake face detection system that effectively distinguished between real and synthetic faces. The methodology's systematic approach and rigorous evaluation ensured the robustness, accuracy, and reliability of the proposed system, making it suitable for real-world applications and contributing to the advancements in combating the misuse of synthetic media.

4) IMPLEMENTATION

The correctness of both true and false is provided right away when a user drags and drops a photo, whether it is a downloaded image or a web image. Many currently used systems require manual annotation or human oversight, which takes time and resources. A trustworthy and automated system that can reliably distinguish between genuine and artificial faces without human interaction is required. The suggested method has a substantial advantage over existing systems in that it can recognise artificial faces produced by cutting-edge deep learning techniques. The system is a more dependable tool for thwarting the harmful use of synthetic media since it can distinguish between genuine and synthetic faces with accuracy, even when there are high-quality synthetic faces present. Overall, the proposed system outperforms existing systems for true fake face detection thanks to its integration of cutting-edge deep learning techniques, automation, real-time operation, and capacity to recognise high-quality synthetic faces.[3]

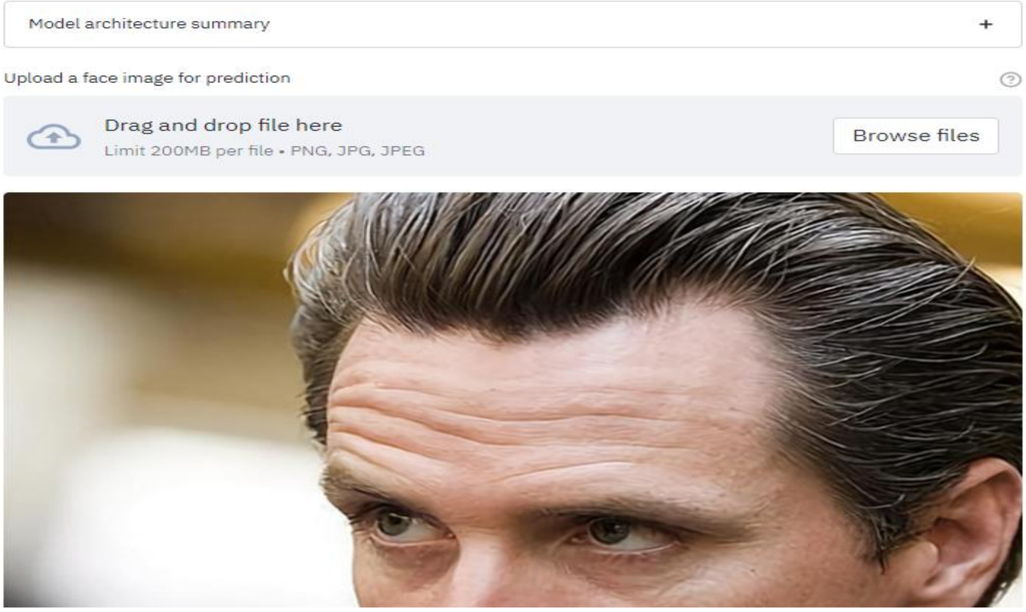
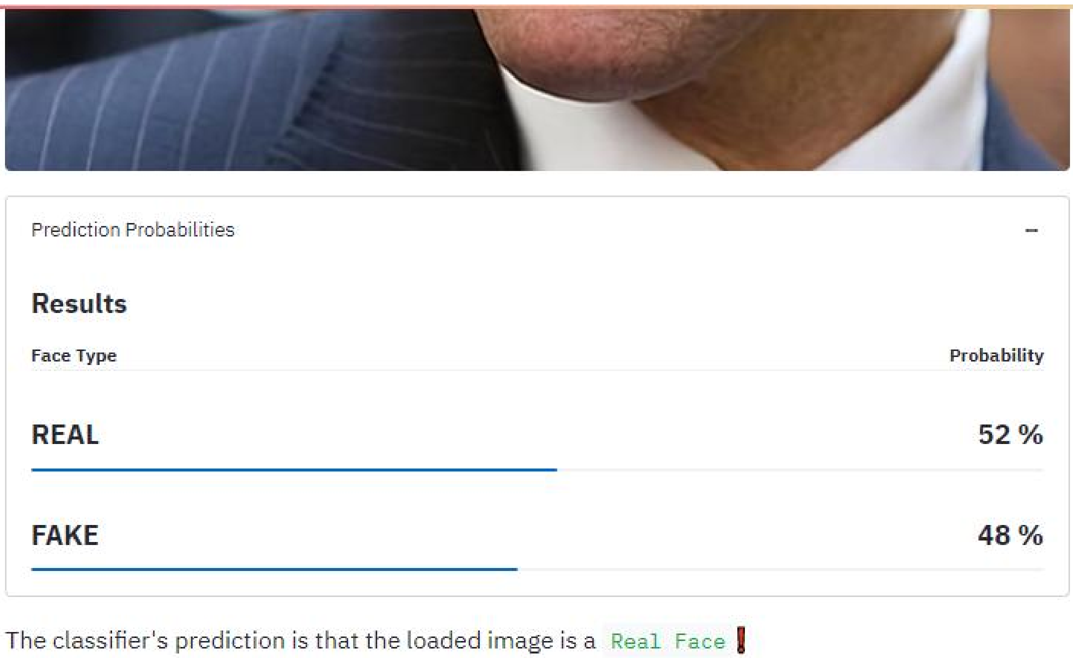

Model architecture summary
+
Upload a face image for prediction
Drag and drop file here
Limit 200MB per file • PNG, JPG, JPEG
Browse files

Fig 3. Uploading image



Results

Face Type	Probability
REAL	52 %
FAKE	48 %

The classifier's prediction is that the loaded image is a `Real Face` ❗

Fig 4. Output

5) CONCLUSION

In conclusion, the development of a real fake face detection system using deep learning techniques is of paramount importance in addressing the potential misuse of synthetic media. This project aimed to tackle the growing concerns surrounding the malicious use of synthetic faces for criminal activities such as identity theft and fraud. By implementing a combination of facial landmarks detection, texture analysis, and generative models, the proposed system aimed to accurately distinguish between real and synthetic faces. The project's outcomes have highlighted the potential benefits of an automated real fake face detection system, reducing the need for manual annotation and enabling real-time operations. The system's efficiency and accuracy make it a valuable tool in the fight against synthetic media's misuse, aiding in the prevention of identity theft and fraudulent activities. As technology continues to advance and synthetic media becomes more sophisticated, ongoing research and development in this field will be crucial. The project's achievements provide a solid foundation for future improvements and enhancements in real fake face detection systems. By continuously refining and expanding upon these techniques, society can better safeguard against the potential threats posed by synthetic media, ensuring a safer and more secure digital environment for all.

6) REFERENCES

[1] *Falko Matern; Christian Riess; Marc Stamminger* , Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations**,** 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)

[2] *Yunjey Choi, Minje Choi, Munyoung Kim, Jung-Woo Ha, Sunghun Kim, Jaegul Choo* , StarGAN: Unified Generative Adversarial Networks for Multi-Domain Image-to-Image Translation, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018

[3] *David Güera; Edward J. Delp,* Deepfake Video Detection Using Recurrent Neural Networks ,2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)

[4] *Grigory Antipov; Moez Baccouche; Jean-Luc Dugelay,* Face aging with conditional generative adversarial networks**,** 2017 IEEE International Conference on Image Processing (ICIP)

[5] *Jeff Donahue; Lisa Anne Hendricks; Marcus Rohrbach; Subhashini Venugopalan; Sergio Guadarrama*, Long-Term Recurrent Convolutional Networks for Visual Recognition and Description, IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume: 39, Issue: 4, 01 April 2017)

[6] *Paul Upchurch; Jacob Gardner; Geoff Pleiss; Robert Pless; Noah Snavely; Kavita Bala* , Deep Feature Interpolation for Image Content Changes**,** 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)

[7] *Christian Szegedy; Wei Liu; Yangqing Jia; Pierre Sermanet; Scott Reed,* Going deeper with convolutions**,**
2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)

[8] Jeffrey Dean, Greg Corrado, Rajat Monga, Kai Chen, Matthieu Devin, Mark Mao, Marc'aurelio Ranzato, Andrew Senior, Paul Tucker, Ke Yang, Quoc Le, Andrew Ng, Large Scale Distributed Deep Networks

[9] A.Coates, H. Lee, and A. Y. Ng, An analysis of single layer networks in unsupervised feature learning**,**
In AISTATS, 2011

[10] *D. P. Kingma and M. Welling,* Auto-encoding variational bayes**,** ICLR, 2014

[11] *Kaiming He; Xiangyu Zhang; Shaoqing Ren; Jian Sun,* Deep Residual Learning for Image Recognition**,** 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)