

The rapid progress in the generation and manipulation of synthetic image has led to significant concerns for the implications towards the public. Creating realistic alterations in images is an active and challenging research area in computer vision and graphics. A recent twist on the disturbing problem of digital disinformation is falsified videos created by artificial intelligence technology, particularly deep neural networks. In such videos, the faces of a target person are replaced by the faces of a donor individual synthesised by DNN models, while the target's facial expressions and head positions are preserved as shown in the following figures.



Figure 1: Image Synthesis using DNN

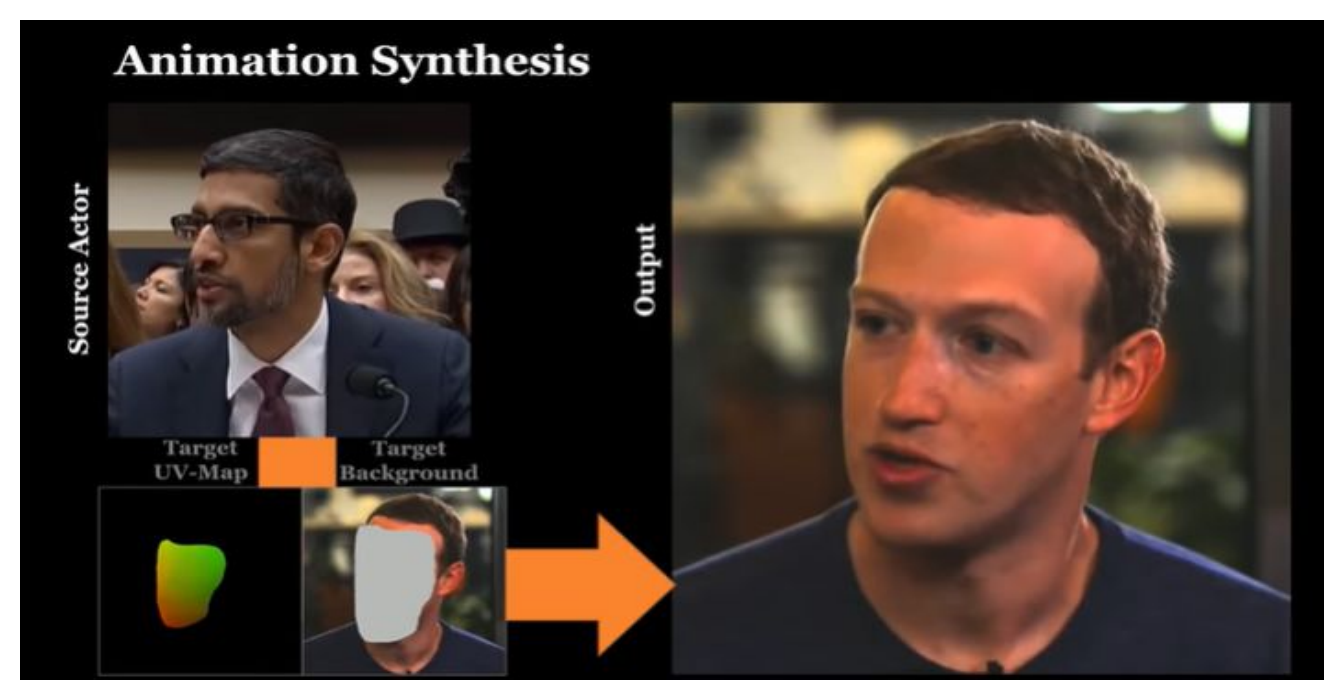


Figure 2: Video Forgery using Neural Textures

This leads to a loss of trust in digital content, and could potentially cause further harm by spreading false information or fake news.

Literature Review

In the FaceForensics++ [1] dataset, containing synthesized images from over 1000 Youtube videos having the tags "face", "newscaster" or "newsprogram", Rössler et al. considered two computer graphics-based manipulation approaches, namely Face2Face [2] and FaceSwap [3], in addition to two learning-based approaches, namely, DeepFakes [4] and NeuralTextures [5].

Rössler et al. [1] observed that even in the presence of significant compression, the use of additional domain-specific knowledge improved forgery detection to unprecedented accuracy, clearly outperforming human observers. They used the state-of-the-art face tracking method by Thies et al. [2] to track the face in the video and extract the face region of the image.

Jiang et al. [6] examined the classification performance on forged videos compressed at various quality settings. They observed that XceptionNet [8] recorded the best results in the task of classifying forged and pristine video sequences.

Methodology

As shown in figure 3, our domain-specific forgery detection pipeline for facial manipulations is the following:

The key-frames are extracted as images from the video input. Each image is then processed by a robust face tracking algorithm, which we use to extract the portion of the image that is covered by the face, which is then fed into a learned classification network based on XceptionNet [7], which produces the prediction. Finally, the forgery detection output is visualized as the input video, with the addition of a bounding box around the face area demonstrating the confidence levels of the classification results. Moreover, we divide the video sequence into pristine and manipulated sequences and extract the forged video sections as time intervals.

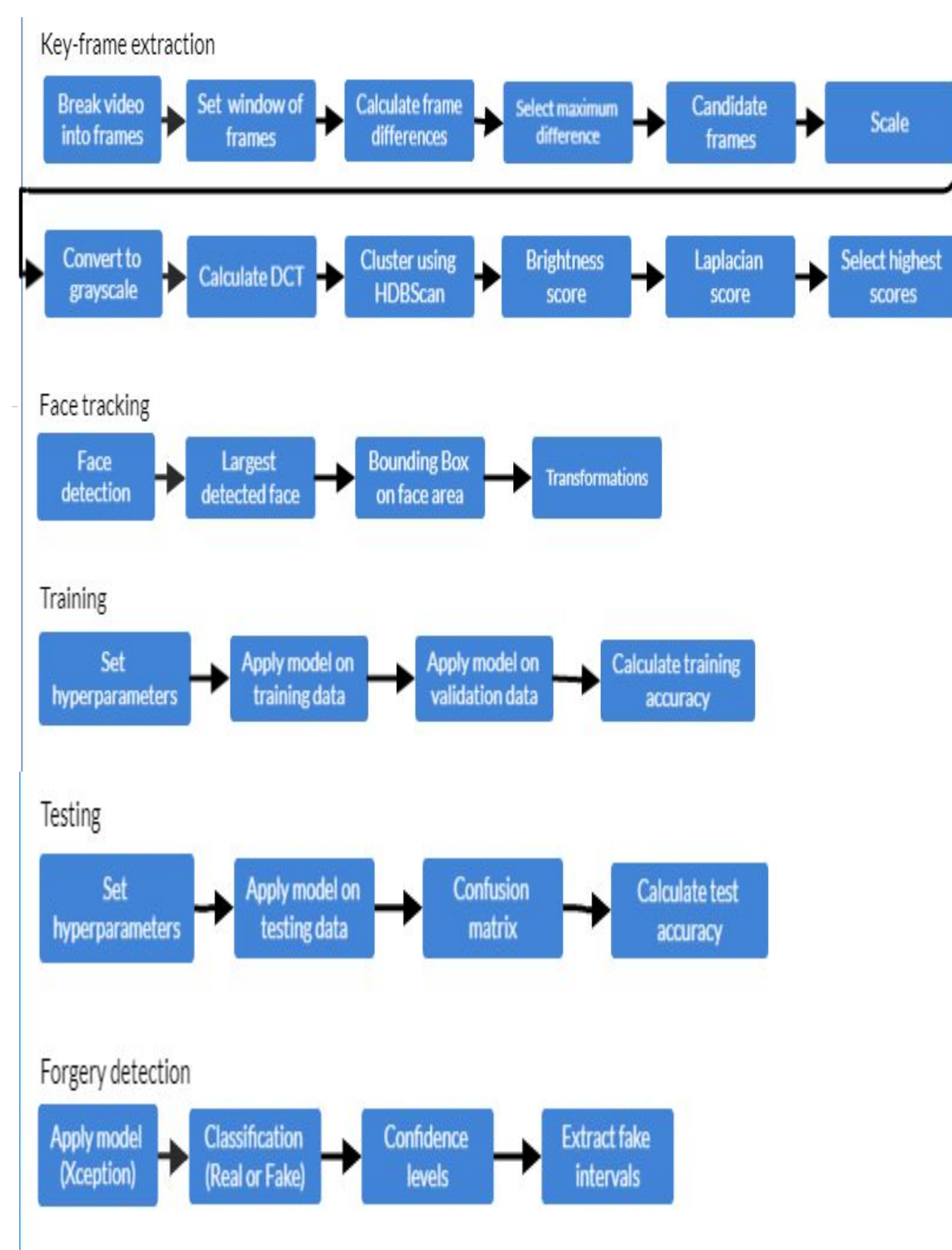


Figure 3: Video Forgery Detection Pipeline

Results

We trained and tested our network with pristine images from the Celeb-DF [8] and Youtube datasets along with manipulated frames from the DeeperForensics 1-0 dataset [6]. The following results were achieved.

TP	3,807
TN	4,124
FP	38
FN	31
Sensitivity	99.19%
Specificity	99.08%
Precision	99.01%
NPV	99.25%
F1 Score	99.1%
Accuracy	99.14%

Figure 4: Detection Accuracy

We compare the results of our binary forgery detection task using our network architecture evaluated on different manipulation methods both simultaneously and separately.

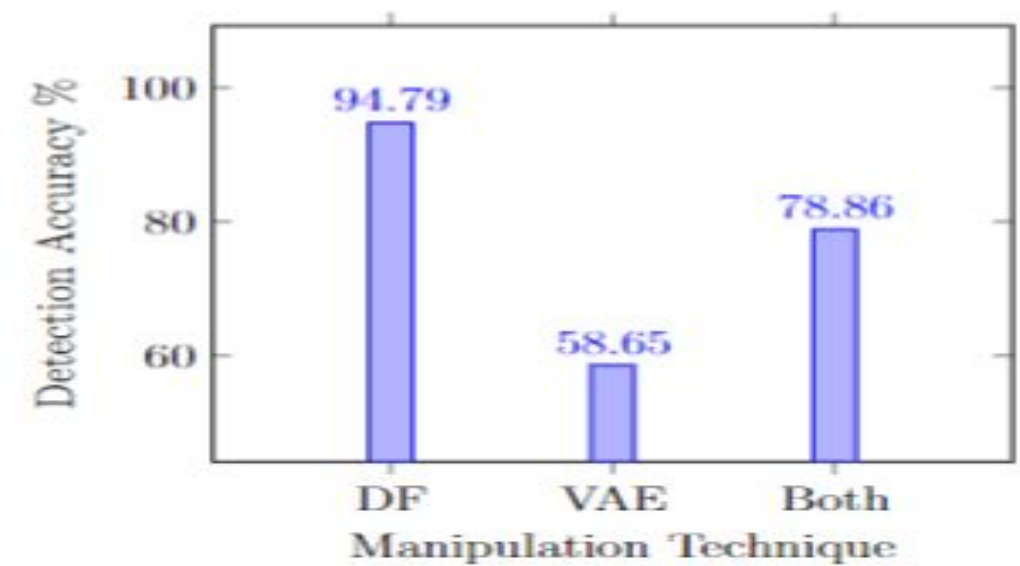


Figure 5: Comparison of the Detection Accuracy of the DL model trained on all manipulation methods

As per our results, we observe that the model achieves better performance when trained and tested on a single face manipulation method.

Conclusion

We succeeded in developing an algorithm that is able to detect video forgery caused by several manipulation techniques using deep learning and computer vision. Given a video sequence input, the system decides whether the video has been exposed to forgery while also identifying the detection confidence levels and the particular video section that has been tampered with.

Our deep learning architecture is capable of detecting video forgery with an accuracy surpassing that of human observers by a remarkable amount, therefore preventing them from becoming deceived or misled by false videos or fake news.



Figure 6: Classification of Real News Videos



Figure 7: Classification of Fake News Videos

References

1. A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "Faceforensics++: Learning to detect manipulated facial images," in Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 1–11, 2019.
2. J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, and M. Nießner, "Face2face: Real-time face capture and reenactment of rgb videos," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2387–2395, 2016.
3. I. Korshunova, W. Shi, J. Dambre, and L. Theis, "Fast face-swap using convolutional neural networks," in Proceedings of the IEEE international conference on computer vision, pp. 3677–3685, 2017.
4. M. Westerlund, "The emergence of deepfake technology: A review," Technology Innovation Management Review, vol. 9, no. 11, 2019.
5. J. Thies, M. Zollhofer, and M. Nießner, "Deferred neural rendering: Image synthesis using neural textures," ACM Transactions on Graphics (TOG), vol. 38, no. 4, pp. 1–12, 2019.
6. L. Jiang, R. Li, W. Wu, C. Qian, and C. C. Loy, "Deeperforensics-1.0: A large-scale dataset for real-world face forgery detection," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 2889–2898, 2020.
7. F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1251–1258, 2017.
8. Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-df: A large-scale challenging dataset for deepfake forensics," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3207–3216, 2020.