# Developing a Facial Landmark Analysis Pipeline for Real Time Scene Authentication to Protect Against Deepfake Attacks

Kelly Yen, Hadleigh Schwartz, Dr. Xia Zhou
Columbia University, MobileX Lab

**Introduction**: "Deepfake" content refers to visual and auditory media that has been generated by an artificial intelligence (AI). The most recent deepfake technology is capable of generating content that's indistinguishable from real media, introducing a new class of security threats. Efforts to distinguish deepfake videos from real videos typically involve training a secondary AI algorithm to recognize specific artifacts or physiological cues. However, these countermeasures assume that deepfake generating algorithms won't continue to evolve and improve. To circumvent a deepfake generation vs detection arms race, we propose a real time scene authentication tool that authenticates an entire scene happening in the real world. This Summer's project focused on developing a facial landmark analysis pipeline to be used in both the scene and video authentication components of this project.

**Method:** Using Google Mediapipe's Facial landmark extraction tool, we can extract and track 478 landmarks on any individual's face and encode that information into a signal that's projected onto a scene with imperceptible light. We built a landmark data processing and testing pipeline in Python using the Matplotlib, Scipy, Numpy, and Pandas libraries.

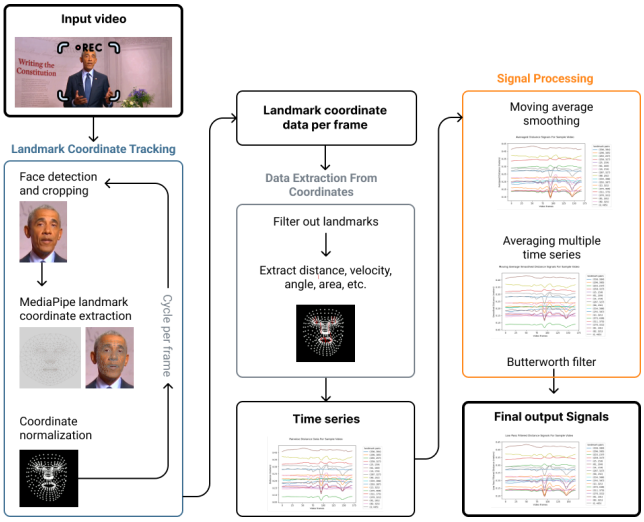


*Figure 1. An overview of the pipeline*

**Results**: The main outcome of this Summer is a modular landmark processing and testing pipeline that can be used to determine which landmarks best represent the unique facial movements and identity of a speaker. This pipeline can also be used to determine an optimal sequence for data processing. The current iteration of the pipeline produces the following results:

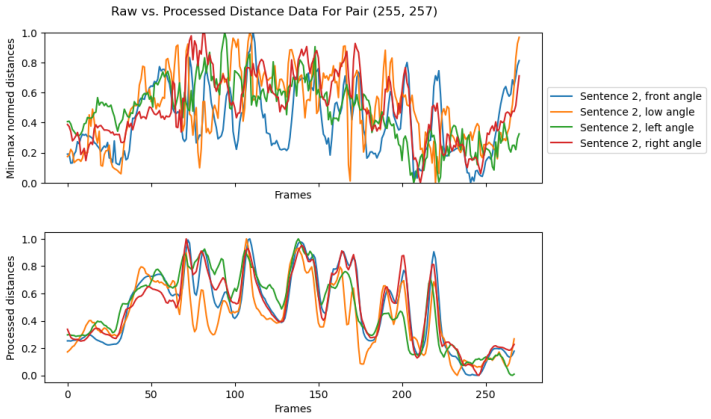


*Figure 2. Passing distance signals through the pipeline results in converged signals for videos capturing the same scene.*

**Future Work**: The landmark analysis pipeline needs to be tested on video test data collected from subjects of different age, race, and gender identities. Once more data has been collected, the pipeline can be used to finalize the feature extraction and processing component of the scene authentication project.

**References:**

1) Danielle K. Citron & Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security , in 107 California Law Review 1753 (2019).
2) Rahdari, F., Rashedi, E. & Eftekhari, M. A Multimodal Emotion Recognition System Using Facial Landmark Analysis. Iran J Sci Technol Trans Electr Eng 43 (Suppl 1), 171–189 (2019). doi: 10.1007/s40998-018-0142-9
3) F. Noroozi, M. Marjanovic, A. Njegus, S. Escalera and G. Anbarjafari, "Audio-Visual Emotion Recognition in Video Clips," in IEEE Transactions on Affective Computing, vol. 10, no. 1, pp. 60-75, 1 Jan.-March 2019, doi: 10.1109/TAFFC.2017.2713783.
4) Ryumina, E., & Karpov, A. (2020). Facial expression recognition using distance importance scores between facial landmarks. Proceedings of the 30th International Conference on Computer Graphics and Machine Vision (GraphiCon 2020). Part 2. https://doi.org/10.51130/graphicon-2020-2-3-32
5) Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes. ACM Computing Surveys, 54(1), 1–41. https://doi.org/10.1145/3425780

**Acknowledgements**: This project was funded by the Amazon Summer Undergraduate Research Experience program at Columbia University, and supported by Dr. Xia Zhou and Hadleigh Schwartz from the Mobile X Lab.