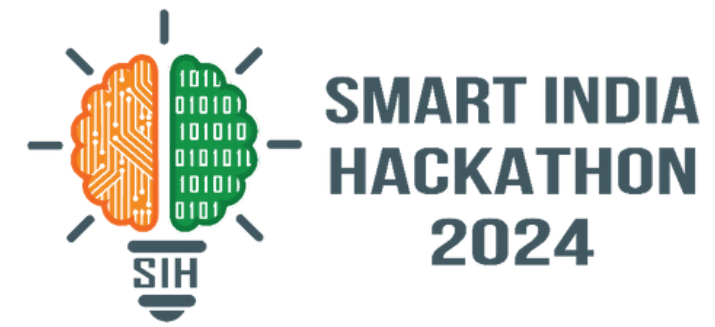


# SMART INDIA HACKATHON 2024



## DeepFake Detector

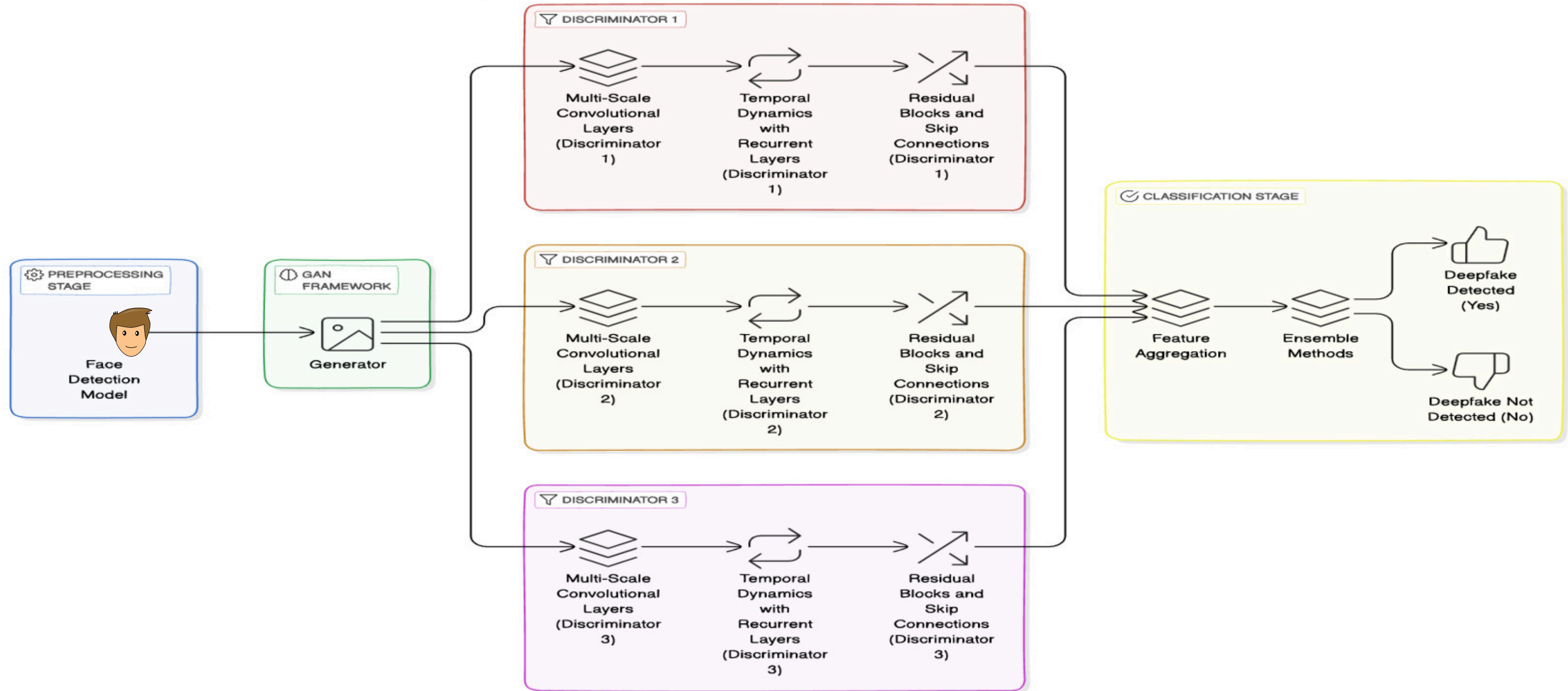
- Problem Statement ID – 1683
- Problem Statement Title: Development of AI/ML-based solution for detection of face-swap-based deep fake videos
- Theme – Miscellaneous
- PS Category – Software
- Team ID: 46402
- FakeFilter\_2024



## Proposed Solution

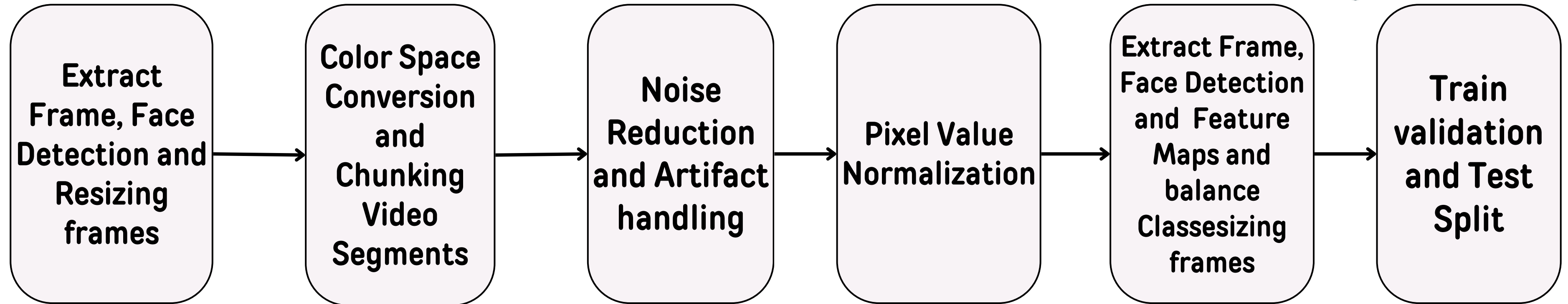
- **GAN-Based Series Discriminators:** We will utilize a Generative Adversarial Network (GAN) framework with a series of deep layered discriminators, each tailored to extract inconsistencies and relevant features and perform final classification for thorough image analysis.
- **Each discriminator contains:**
  - **Multi-Scale Convolutional Layers:** We will Implement parallel convolutional layers with varying kernel sizes to capture both detailed and broad image features, providing a richer input representation.
  - **Temporal Dynamics with RNN and LSTM:** We will use RNNs and LSTMs to process sequential feature maps, capturing subtle temporal inconsistencies crucial for detecting deepfakes.
  - **Enhanced Deep Network Architecture:** We will Incorporate residual blocks and skip connections within each discriminator to improve gradient flow, facilitate deeper architectures, and ensure efficient training and convergence.
- **Advanced Feature Synthesis and Ensemble Classification:** Aggregating features through a feedforward neural network for nuanced analysis, and combine outputs from multiple discriminators using ensemble methods for robust and accurate deepfake detection.

## Deepfake Detection Using GAN with Series Discriminators

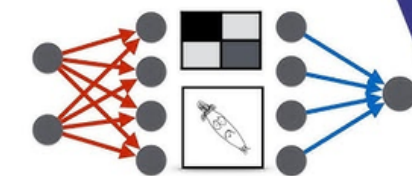
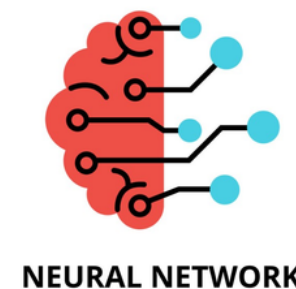
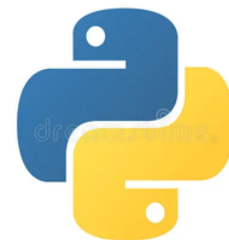
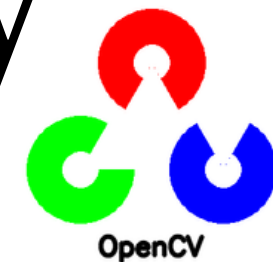


# Preprocessing Steps

Fake  
Filter\_2024



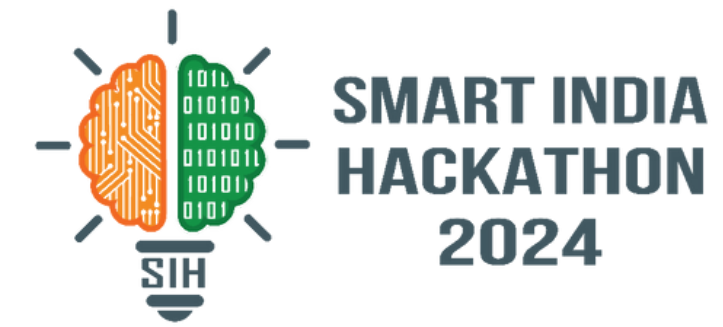
## Technology Stack



Generative  
Adversarial  
Networks



# FEASIBILITY AND VIABILITY



- **Feasibility:**

- The solution for detecting face-swap deepfakes is feasible with advanced machine learning, computational power, and datasets like FaceForensics++ and DFDC. Ongoing research and synthetic data help models adapt to evolving techniques. Though challenges like adversarial adaptation and accuracy persist, regular updates and ethical considerations can address these issues effectively.

- **Challenges:**

- Computation Requirements: Given the complexity (multi-scale convolutions, recurrent layers, multiple discriminators), the model could be computationally expensive to train and deploy, especially for real-time deepfake detection in videos.
- Training Challenges: Training multiple discriminators in a GAN-based system can be tricky, as GANs are notorious for stability issues.

- **Strategies to overcome challenges:**

- Residual Blocks & Skip Connections: Improves gradient flow, preventing vanishing gradients. Use in both generator and discriminators.
- Hyperparameter Tuning: Use learning rate schedules and optimal batch sizes for balance. TTUR (Two-Time Scale Update Rule) helps balance learning between generator and discriminator.
- Employing appropriate loss function(WGAN-GP, for improving gradient flow and stability)

The potential impact of deep fake detection on the target audience includes:

- **Increased trust:** Accurate detection tools restore public confidence in digital media by spotting forgeries.
- **Misinformation protection:** It shields users from manipulated content that could mislead or harm public opinion.
- **Privacy preservation:** Detecting deepfakes helps protect people from identity theft and defamation via falsified media.
- **Ethical awareness:** It promotes responsible media consumption and sharing, raising awareness about the dangers of deepfakes.
- **Content authenticity:** Detection systems ensure the integrity of information shared online.
- **Personal security:** Individuals can feel safer knowing their likeness won't be exploited or misused in deceptive ways.

# RESEARCH AND REFERENCES

**MesoNet:** [IEEE Paper Template in A4 \(V1\) \(arxiv.org\)](#)

**MaskGAN:** [1907.11922 \(arxiv.org\)](#)

**FaceForensics++:** <https://arxiv.org/abs/1901.08971>

**FSGAN:** <https://arxiv.org/abs/1811.00661>

**Other compiled dataset & research papers:**

- [1905.00582 \(arxiv.org\)](#)
- [1610.05586 \(arxiv.org\)](#)
- [1912.12396 \(arxiv.org\)](#)
- [1908.05932 \(arxiv.org\)](#)
- [enochkan/awesome-gans-and-deepfakes: A curated list of GAN & Deepfake papers and repositories. \(github.com\)](#)
- <https://github.com/Daisy-Zhang/Awesome-Deepfakes-Detection?tab=readme-ov-file>