

Slide: 1

Hello, this video presents our team hybrid image forgery detection system

Slide: 2

- Digital images are often manipulated, especially using copy-move operations.
- These manipulations can mislead media, legal investigations, and forensic analysis.
- Deep learning helps classify images but often misses small manipulated areas, while classical SIFT
- detection fails in smooth regions.
- This motivated me to build a hybrid system combining both approaches.

Slide: 3

- The base paper improves SIFT performance using entropy maps to extract better keypoints in low-texture regions.
- This inspired the enhancement I used in my SIFT analysis module.

Slide: 4

- The proposed system has four major stages.
- First, the EfficientNet-B0 classifier checks whether the image is authentic or tampered.
- Next, SIFT analysis extracts keypoints using entropy preprocessing.
- Then the copy-move module matches duplicated regions.
- Finally, we combine everything to generate classification results, heatmaps, SIFT maps, and copy-move visualizations.

Demo

Now I'll show the system in action.

First, I select an image. The classifier predicts if it's authentic or tampered, and Grad-CAM highlights suspicious regions.

SIFT then extracts keypoints, and the copy-move module matches duplicated segments.

This 2x2 visualization shows original, heatmap, SIFT, and final matched output.

Slide: 5

- The system achieved 81% accuracy, with a tampered recall of 75.5% & F1 score of 0.72.
- This shows the model performs well in detecting manipulated areas.

Slide: 6

- The hybrid design performs significantly better than using CNN or SIFT alone.
- The system is both accurate and interpretable.

Slide: 7

In future, the system can be extended with transformer models, artifact detection, or real-time processing.

Slide: 8

Thank you for watching