AI-BASED CCTV & DIGITAL MEDIA FORENSIC ANALYSIS TOOL

Team members: Adwait Deshpande, Bhagyesh Worlikar, Parth Patil.

Problem Statement.

Nowadays, CCTV footage or seized digital evidence is crucial for police investigations. Manually combing through hours of video is inefficient, often inaccurate, and a waste of valuable manpower and resources. At the same time, digital images and videos can be tampered with. A system that can automatically identify people/vehicles in CCTV footage while also ensuring the authenticity of images and videos is desperately required. This tool will speed up investigations, reduce human fatigue, and give law enforcement a robust forensic workflow suitable for courtroom usage.

Proposed solution to the Problem statement.

We suggest a dual module forensic system.

1. Video Surveillance Analysis System.

- It recognizes and labels people and vehicles using computer vision techniques such as YOLOv8, OpenCV, and DeepSORT.
- This system keeps track of detections in the order of appearance, matching faces or license plates against offender/wanted databases with a recognition.
- Similarity search using embeddings compares files quickly.

2. Engine for Forensics in Digital Media.

- Uses ExifTool and python scripts for metadata extraction, including GPS, timestamp, camera/device info, and hash values.
- GPS/time-stamp discrepancies, alteration signs & hash differences show inconsistencies.
- Using noise or light patterns to check for tampering in media.
- Investigator's dashboard brings together findings: searchable timelines, side-by-side video assessments, and alerts on anomalies.
- The reports that are exported will get digitally signed in SHA256 hash and QR code to maintain the chain of custody. The whole system runs on local devices ensuring privacy and less cost in deployment.

Features of the Final solution to be designed.

- Detects people, cars, and other objects within bounding boxes and labels.
- Tweaked watchlist to help easily flag suspects and stolen vehicles.
- Exporting CSV/JSON log with a timestamp to the law enforcement records.
- Collecting GPS coordinates, device ID, hashes, date/time, forensic metadata.
- Detecting evidence of interference, such as altered frames and metadata.
- Integrated Control Panel.

- Look up by suspect, vehicle, or time.
- Analyse visuals from various camera sources.
- Visual signs of irregularities.
- Forensic Documentation.
- Court-ready PDF reports with embedded hash and QR code verification.
- Recording the chain of custody for controlling evidence.
- This is a stack that includes lightweight frameworks in python like Pytorch, OpenCV, Flask, Streamlit which allow on-premise deployment and are less reliant on cloud service providers.
- The use of a modular design for it can easily build on a greater number of AI models or foreign police databases.

Reasoning for Choosing This Problem Statement.

This task relates specifically to our M.Sc. Specialize in Digital Forensics and Information Security course. Getting to use all the knowledge about the computer vision, forensic verification, and secure documentation as a real-world law enforcement solution. CCTV footage is a staple of modern investigations. And the ongoing tussles over electronic manipulation in court, the proposed solution addresses a real world problem. This project is very feasible during the hackathon and can also scale to production grade police use in the future.

Previous Experiences.

- Assignments and projects focused on video manipulation detection, AI-driven intrusion detection, and digital forensics processes.
- Worked with various tools like OpenCV, Exiftool, Hashing, Volatility, Autopsy.
- Developed a malware identification framework while completing my studies.
- Experienced with CTF challenges like memory analysis, steganography, file forensics, video examination.