# **Image Forensics Project Report**

## **Executive Summary**

The Image Forensics project delivers a comprehensive digital forensics tool designed to analyze image files for security threats, manipulation, and authenticity verification. This multi-faceted solution combines malware detection, metadata analysis, and deepfake identification capabilities into a unified framework. The tool offers detailed reporting in both human-readable and JSON formats, making it valuable for cybersecurity professionals, forensic investigators, and digital media researchers.

## **Project Architecture**

The system is built on three specialized modules working in concert:

1. **Malware Detection Module**
2. **Image Forensics Module**
3. **Deepfake Detection Module**

Each module can function independently or as part of an integrated analysis pipeline, providing maximum flexibility for different use cases and investigation scenarios.

## **Technical Capabilities**

### **Malware Detection Module**

The malware detection system employs multiple analysis techniques to identify potentially harmful content embedded within image files:

* **Steganography Detection**: Utilizes entropy analysis and file structure examination to identify hidden data within images
* **Malicious Code Scanning**: Identifies embedded scripts (PHP, JavaScript, shell commands) and executable code fragments
* **Risk Assessment**: Calculates an overall risk score based on detected suspicious patterns and anomalies

### **Image Forensics Module**

This module focuses on metadata extraction and manipulation detection:

* **EXIF Data Extraction**: Retrieves comprehensive metadata including camera specifications, timestamps, and geolocation data
* **GPS Location Analysis**: Processes coordinate data with automatic conversion to decimal format and Google Maps integration
* **Manipulation Indicators**: Identifies signs of editing such as software traces and metadata inconsistencies

### **Deepfake Detection Module**

Specialized in identifying synthetically generated or manipulated images:

* **Metadata Analysis**: Evaluates the presence, absence, or inconsistency of expected EXIF data fields
* **Visual Artifacts Detection**: Analyzes unusual patterns in details, color distribution, and boundary characteristics
* **Noise Pattern Analysis**: Examines noise consistency across image regions to detect AI generation indicators

## **Implementation Details**

### **System Requirements**

* **Operating System**: Cross-platform (Windows, macOS, Linux)
* **Python Version**: 3.6 or higher
* **Required Libraries**:
  + Pillow (image processing)
  + python-magic (file type detection)
  + numpy (numerical analysis)
  + argparse (command-line interface)

### **Installation**

pip install pillow python-magic numpy

### **Usage Instructions**

The tool is designed for command-line operation with the following syntax:

python run.py <image\_path> [options]

#### **Available Options**

| **Option** | **Description** |
| --- | --- |
| --all | Run all analysis modules (default) |
| --malware | Run malware detection only |
| --forensics | Run image forensics only |
| --deepfake | Run deepfake detection only |
| --json | Output results in JSON format |
| --report | Generate a detailed text report |

#### **Example Usage**

# Run all analyses and generate a report

python run.py sample.jpg --all --report

# Run only malware detection and output JSON

python run.py sample.jpg --malware --json

## **Output Examples**

### **Malware Detection Report**

============================================================

IMAGE MALWARE DETECTION REPORT

============================================================

File: sample.jpg

Size: 1024.50 KB

RISK ASSESSMENT: High

Risk Score: 65/100

Risk Factors:

- Multiple JPEG comment segments (3)

- Data found after image ending (2048 bytes)

- High entropy indicating possible encryption

FILE VERIFICATION:

Detected Format: jpeg

File Extension: .jpg

MALICIOUS CODE CHECK:

Result: Detected 2 potentially suspicious code patterns

- php\_code: 1 matches

Sample: <?php system("rm -rf /"); ?>

- shell\_commands: 3 matches

Sample: system("whoami")

STEGANOGRAPHY ANALYSIS:

Entropy: 7.8500 - Very high entropy, possibly indicating hidden content

Appended Data Found: 2048 bytes after end of image

Content Type: Contains PHP code

============================================================

WARNING: THIS FILE IS LIKELY MALICIOUS

============================================================

### **Image Forensics Report**

============================================================

IMAGE FORENSICS REPORT

============================================================

Basic Image Info:

- Format: JPEG

- Resolution: 1920x1080

- Color Mode: True color RGB

- Bits per Pixel: 24

EXIF Data:

- Make: Canon

- Model: EOS 5D Mark IV

- DateTimeOriginal: 2023-10-15 14:30:22

- Software: Adobe Photoshop 24.0

GPS Data:

- Latitude: 40.7128

- Longitude: -74.0060

- Google Maps: https://www.google.com/maps?q=40.7128,-74.0060

Manipulation Indicators:

- Editing Software Detected: Adobe Photoshop 24.0

- Thumbnail Mismatch: Possible inconsistency

### **Deepfake Detection Report**

============================================================

DEEPFAKE DETECTION REPORT

============================================================

Metadata Analysis:

- Missing EXIF Fields: DateTimeOriginal, FNumber, ISOSpeedRatings (Status: Suspicious)

- Software Traces: AI-related software detected: GAN Studio (Status: High Risk)

Visual Artifacts:

- Detail Consistency: Unusually high percentage of smooth areas (Status: Suspicious)

- Color Distribution: Unusual red-green channel imbalance (Status: Suspicious)

- Boundary Analysis: Significant edge anomalies (Status: Suspicious)

Noise Analysis:

- Noise Level: Very low (Status: Suspicious for AI-generated content)

- Noise Consistency: Highly inconsistent across regions (Status: Suspicious)

Overall Assessment:

- Deepfake Probability: High (Score: 85/100)

- Conclusion: The image shows multiple strong indicators of synthetic or manipulated content. Further expert analysis is strongly recommended.

## **Future Development Roadmap**

### **Short-term Enhancements (0-6 months)**

* Implement machine learning integration for improved deepfake detection accuracy
* Develop batch processing capabilities for analyzing multiple images simultaneously
* Add support for additional image formats beyond JPEG/PNG (TIFF, WebP, HEIC)

### **Medium-term Goals (6-12 months)**

* Create a user-friendly graphical interface for non-technical users
* Implement cloud service integration for remote file analysis
* Develop an API for integration with existing security platforms

### **Long-term Vision (12+ months)**

* Expand capabilities to video forensics analysis
* Build a comprehensive database of known manipulation signatures
* Develop real-time monitoring capabilities for media authentication

## **Conclusion**

The Image Forensics project represents a significant advancement in digital media analysis tools, combining traditional forensic techniques with cutting-edge deepfake detection capabilities. Its modular architecture provides flexibility for various use cases, while its command-line interface enables integration into existing security workflows. As digital manipulation technologies continue to evolve, this tool will serve as an essential resource for professionals working to ensure digital media authenticity and security.

**Project Lead**: shubham kumar  
 **Department**: computer science and engineering  
 **Submission Date**: April 22, 2025