Training Course on Image and Video Forensics for Authentic Verification

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

In an era dominated by visual media, the ability to discern genuine images and videos from manipulated or fabricated content is paramount across legal, journalistic, and security sectors. The proliferation of sophisticated editing software and deepfake technologies has blurred the lines between reality and deception, making authentic verification a critical challenge. Training Course on Image and Video Forensics for Authentic Verification provides an immersive deep dive into image and video forensics, equipping digital forensic investigators, intelligence analysts, legal professionals, and media specialists with the advanced techniques required to detect tampering, establish provenance, and verify the integrity of visual evidence. Participants will master the scientific methodologies for identifying inconsistencies, analyzing metadata, and uncovering digital fingerprints that reveal manipulation.

This intensive program moves beyond basic visual inspection, exploring the intricate technical aspects of digital image and video acquisition, processing artifacts, compression analysis, and the unique challenges posed by social media distribution. Through hands-on labs with real-world manipulated media and cutting-edge forensic tools, attendees will gain proficiency in techniques such as Error Level Analysis (ELA), Noise Inconsistency Analysis, Metadata Reconstruction, and Deepfake Detection methodologies. By the end of this course, you will possess the expertise to provide authoritative assessments of visual media, building undeniable forensic evidence crucial for legal proceedings, journalistic integrity, and effective counter-disinformation efforts.

Programme Curriculum

Training Course on Image and Video Forensics for Authentic Verification

Introduction

In an era dominated by visual media, the ability to discern genuine images and videos from manipulated or fabricated content is paramount across legal, journalistic, and security sectors. The proliferation of sophisticated editing software and deepfake technologies has blurred the lines between reality and deception, making authentic verification a critical challenge. Training Course on Image and Video Forensics for Authentic Verification provides an immersive deep dive into image and video forensics, equipping digital forensic investigators, intelligence analysts, legal professionals, and media specialists with the advanced techniques required to detect tampering, establish provenance, and verify the integrity of visual evidence. Participants will master the scientific methodologies for identifying inconsistencies, analyzing metadata, and uncovering digital fingerprints that reveal manipulation.

This intensive program moves beyond basic visual inspection, exploring the intricate technical aspects of digital image and video acquisition, processing artifacts, compression analysis, and the unique challenges posed by social media distribution. Through hands-on labs with real-world manipulated media and cutting-edge forensic tools, attendees will gain proficiency in techniques such as Error Level Analysis (ELA), Noise Inconsistency Analysis, Metadata Reconstruction, and Deepfake Detection methodologies. By the end of this course, you will possess the expertise to provide authoritative assessments of visual media, building undeniable forensic evidence crucial for legal proceedings, journalistic integrity, and effective counter-disinformation efforts.

Course Duration

5 Days

Course Objectives

1. Understand Image & Video Fundamentals: Comprehend the underlying digital structures, formats, and compression techniques of images (JPEG, PNG, TIFF) and videos (MP4, AVI, MOV).
2. Master Metadata Analysis: Extract and interpret EXIF, XMP, and other embedded metadata from images and videos to determine device provenance, capture settings, and modification history.
3. Detect Image Manipulation (Basic): Identify common tampering techniques such as resizing, cropping, cloning, and simple object insertion/removal.
4. Perform Advanced Image Forgery Detection: Utilize scientific methods like Error Level Analysis (ELA), Noise Inconsistency Analysis, and JPEG Quantization Table analysis to uncover subtle manipulations.
5. Analyze Image Processing Artifacts: Identify and interpret artifacts introduced by cameras, scanners, and image editing software.

6. Assess Video Authenticity (Basic): Detect simple video edits, cuts, and frame insertions/deletions.
7. Conduct Advanced Video Forgery Detection: Employ techniques such as frame analysis, spatio-temporal consistency checks, and re-compression artifact analysis to identify manipulation.
8. Identify Deepfake & Synthetic Media: Understand the principles behind generative adversarial networks (GANs) and apply methods for detecting AI-generated synthetic media.
9. Analyze Compression & Re-compression Artifacts: Interpret the impact of lossy compression on image/video integrity and detect signs of multiple saves or re-encodings.
10. Evaluate Digital Fingerprinting: Understand unique sensor noise patterns (PRNU) and their application in linking media to specific cameras.
11. Address Social Media & Online Media Forensics: Acquire and analyze images/videos from social media platforms and assess the impact of platform-specific re-encoding.
12. Leverage Specialized Forensic Software: Proficiency in using commercial (e.g., Amped Authenticate, Adobe Photoshop Forensic tools) and open-source tools for image/video analysis.
13. Generate Actionable Forensic Reports: Produce clear, concise, and legally defensible reports on image and video authenticity assessments.

Organizational Benefits

1. Enhanced Authentic Verification: Ability to reliably determine the genuineness of visual media, crucial for evidence.
2. Mitigated Reputational Risk: Prevention of misinformed decisions or public statements based on fabricated media.
3. Improved Legal Case Strength: Providing irrefutable digital evidence from images and videos in court proceedings.
4. Faster Response to Disinformation: Rapidly identify and debunk manipulated visual content.
5. Stronger Insider Threat Detection: Uncover evidence of data manipulation or illicit activities captured visually.
6. Protection Against Fraud: Better detection of fraudulent claims supported by fake images/videos.
7. Optimized Investigative Efficiency: Streamlined processes for analyzing and verifying visual evidence.
8. Upskilled Forensic Team: Develop in-house expertise in a rapidly evolving and critical area of forensics.
9. Increased Public Trust: For organizations dealing with sensitive visual content (e.g., law enforcement, journalism).
10. Competitive Advantage: Position as a leader in media authenticity verification and digital integrity.

Target Participants

- Digital Forensic Investigators
- Law Enforcement Officers (Investigators, Detectives)
- Intelligence Analysts
- Legal Professionals (Attorneys, Paralegals)
- Journalists & Fact-Checkers
- Security Operations Center (SOC) Analysts
- Fraud Investigators
- Information Warfare Specialists
- Archivists & Curators of Digital Media
- Public Relations & Crisis Communication Professionals

Course Outline

Module 1: Foundations of Digital Images & Video

- **Image & Video Basics:** Pixels, resolution, color depth, frames, codecs.
- **Image Formats:** JPEG (lossy), PNG, TIFF (lossless), GIF.
- **Video Formats & Containers:** MP4, MOV, AVI, codecs (H.264, H.265).
- **Compression Techniques:** Understanding lossy vs. lossless compression and its forensic implications.
- **Case Study: Comparing Original vs. Heavily Compressed Visual Media**

Module 2: Metadata Analysis for Provenance & History

- **EXIF Metadata:** Camera make/model, date/time, GPS coordinates, capture settings.
- **XMP & IPTC Metadata:** Editing history, copyright information, embedded text.
- **Video Metadata:** Frame rates, duration, creation/modification times, encoding software.
- **Metadata Manipulation:** Detecting attempts to alter or strip metadata.
- **Case Study: Tracing an Image's Journey Using Metadata Forensics**

Module 3: Image Forgery Detection: Basic Techniques

- **Resampling & Resizing Detection:** Analyzing interpolation artifacts.
- **Cropping & Rotation Analysis:** Identifying inconsistencies at image edges.
- **Cloning & Copy-Move Forgery:** Detecting duplicated regions within an image.
- **Splicing & Compositing:** Identifying abrupt changes in light, color, or noise patterns.
- **Case Study: Unmasking a Simple Photo Manipulation in a Court Case**

Module 4: Advanced Image Forgery Detection

- **Error Level Analysis (ELA):** Detecting areas of differing re-compression, indicating tampering.
- **Noise Inconsistency Analysis:** Identifying unnatural noise patterns or absence of noise.
- **JPEG Quantization Table Analysis:** Uncovering re-compression or tampering based on quantization values.
- **Camera Ballistics & PRNU Analysis:** Linking images to specific camera sensors via Photo Response Non-Uniformity.
- **Case Study: Using ELA to Identify a Forged Document Image**

Module 5: Video Forgery Detection: Basic Edits

- **Temporal Discontinuities:** Detecting abrupt cuts, missing frames, or non-linear time progression.
- **Frame Analysis:** Examining individual frames for inconsistencies or inserted content.
- **Audio-Visual Desynchronization:** Identifying audio/video alignment issues as a sign of manipulation.
- **Scene Consistency Checks:** Analyzing lighting, shadows, and objects across frames.
- **Case Study: Identifying an Edited Security Camera Footage**

Module 6: Advanced Video Forgery & Deepfake Detection

- **Spatio-Temporal Consistency:** Analyzing how objects and light behave across multiple frames.
- **Re-compression Artifacts in Video:** Detecting multiple encoding passes and quality degradation.
- **Deepfake Fundamentals:** Understanding GANs, autoencoders, and deepfake generation techniques.
- **Deepfake Detection Methodologies:** Analyzing facial inconsistencies, eye blinks, artifacts specific to AI generation.
- **Case Study: Forensic Analysis of a Suspected Deepfake Video**

Module 7: Social Media & Online Media Forensics

- **Impact of Social Media Platforms:** Understanding platform-specific re-encoding, compression, and metadata stripping.
- **Acquiring Online Media:** Best practices for collecting images and videos from websites and social media platforms.
- **Authenticity Challenges:** Assessing the reliability of user-generated content from online sources.
- **Hashing & Digital Signatures:** Verifying content integrity after acquisition.
- **Case Study: Investigating a Viral Manipulated Image Shared on Social Media**

Module 8: Tools, Reporting & Future Trends

- **Image & Video Forensic Tools:** Hands-on with Amped Authenticate, Adobe Photoshop Forensic techniques, open-source tools (e.g., FotoForensics, ImageJ).
- **Forensic Report Generation:** Documenting methodology, findings, and conclusions for legal or public consumption.
- **Legal Admissibility:** Ensuring image/video evidence meets legal standards for authentication.
- **Emerging Trends:** AI in forensics, new manipulation techniques, ethical considerations.
- **Case Study: Preparing Expert Testimony for a Case Involving Manipulated Visual Evidence**

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.

- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com