Training Course on Deepfake and Synthetic Media Detection and Forensics

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid proliferation of **deepfake** and **synthetic media** poses unprecedented challenges to **digital trust** and **information integrity** across all sectors. Powered by advanced **AI** and **machine learning algorithms**, these manipulated forms of media, including hyper-realistic **video deepfakes**, **audio deepfakes**, and **synthetic images**, are increasingly used for **misinformation**, **disinformation**, **fraud**, and **reputational damage**. Training Course on Deepfake and Synthetic Media Detection and Forensics provides an essential deep dive into the **cutting-edge techniques** and **forensic methodologies** required to **identify, analyze, and mitigate** the threats associated with this evolving digital landscape, equipping professionals with the critical skills to combat **AI-generated deception** .

As the sophistication of **generative AI models** continues to advance, differentiating authentic content from **AI-manipulated media** becomes increasingly complex. This course will demystify the underlying **deep learning architectures** behind deepfake creation, such as **GANs (Generative Adversarial Networks)** and **autoencoders**, to better understand their inherent **digital artifacts** and **forensic fingerprints**. Participants will gain practical expertise in utilizing **advanced detection tools**, mastering **multimedia forensics**, and developing **robust verification strategies** to safeguard against the malicious exploitation of **synthetic content**.

Programme Curriculum

Training Course on Deepfake and Synthetic Media Detection and Forensics

Introduction

The rapid proliferation of **deepfake** and **synthetic media** poses unprecedented challenges to **digital trust** and **information integrity** across all sectors. Powered by advanced **AI** and **machine learning algorithms**, these manipulated forms of media, including hyper-realistic **video deepfakes**, **audio deepfakes**, and **synthetic**

images, are increasingly used for **misinformation**, **disinformation**, **fraud**, and **reputational damage**. Training Course on Deepfake and Synthetic Media Detection and Forensics provides an essential deep dive into the **cutting-edge techniques** and **forensic methodologies** required to **identify, analyze, and mitigate** the threats associated with this evolving digital landscape, equipping professionals with the critical skills to combat **AI-generated deception**.

As the sophistication of **generative AI models** continues to advance, differentiating authentic content from **AI-manipulated media** becomes increasingly complex. This course will demystify the underlying **deep learning architectures** behind deepfake creation, such as **GANs (Generative Adversarial Networks)** and **autoencoders**, to better understand their inherent **digital artifacts** and **forensic fingerprints**. Participants will gain practical expertise in utilizing **advanced detection tools**, mastering **multimedia forensics**, and developing **robust verification strategies** to safeguard against the malicious exploitation of **synthetic content** .

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Comprehend the foundational deep learning principles and generative AI models powering deepfake creation.
2. Identify the various types of synthetic media, including video deepfakes, audio deepfakes, and AI-generated images.
3. Recognize common digital artifacts, forensic traces, and inconsistencies indicative of AI manipulation.
4. Utilize state-of-the-art deepfake detection tools and AI-powered platforms for content authentication.
5. Apply multimedia forensics techniques to analyze and verify the authenticity of digital evidence.
6. Perform metadata analysis and EXIF data examination to uncover signs of digital alteration.
7. Conduct audio waveform analysis and spectral analysis for voice cloning and synthetic speech detection.
8. Implement facial landmark detection and biometric anomaly detection for visual deepfake analysis.
9. Develop robust verification workflows and counter-deepfake strategies for organizational resilience.
10. Assess the ethical implications, legal frameworks, and societal impact of synthetic media misuse.
11. Contribute to digital literacy initiatives and public awareness campaigns against disinformation.
12. Master techniques for reporting and documenting deepfake incidents for investigative purposes.
13. Stay abreast of the latest advancements in deepfake technology and AI-driven countermeasures.

Organizational Benefits

- Strengthened defenses against sophisticated AI-powered cyberattacks, phishing, and fraudulent impersonation.
- Proactive measures to protect brand image and public trust from deepfake-driven disinformation campaigns.
- Improved ability to collect and analyze digital evidence for legal proceedings involving synthetic media.
- Empowering leadership with the knowledge to navigate the complexities of AI-generated content and its implications.
- Minimizing disruptions and financial losses due to deepfake-enabled scams and identity theft.
- Upskilling teams in critical digital forensics and AI detection capabilities, fostering an innovation-driven workforce.
- Demonstrating a commitment to information integrity and combating online deception.

Target Audience

1. Digital Forensics Investigators
2. Cybersecurity Analysts
3. Law Enforcement and Intelligence Personnel
4. Journalists and Media Professionals
5. Risk Management and Compliance Officers
6. Legal Professionals and Attorneys
7. IT Security Teams and Network Administrators
8. Content Moderators and Social Media Platform Managers

Course Outline

Module 1: Introduction to Deepfakes and Synthetic Media

- Define Deepfakes, Synthetic Media, and AI-generated content.
- Explore the historical evolution of media manipulation to modern AI capabilities.
- Categorize different types: video deepfakes, audio deepfakes (voice cloning), image deepfakes.
- Discuss the societal impact: misinformation, disinformation, fraud, reputational damage.
- **Case Study**: The "Obama Deepfake" by BuzzFeed and Jordan Peele highlighting early awareness.

Module 2: The Science Behind Deepfakes: Generative AI

- Understand **Machine Learning** and **Deep Learning** fundamentals.
- Deconstruct **Generative Adversarial Networks (GANs)** and their role in deepfake creation.
- Examine **Autoencoders** and **Variational Autoencoders (VAEs)** for face swapping.
- Introduction to other generative models: **Diffusion Models** and **Transformers**.
- **Case Study**: Understanding how FaceApp's aging filter uses similar underlying AI principles.

Module 3: Visual Deepfake Detection Techniques

- Analyzing **facial inconsistencies**: blinking patterns, eye movements, facial landmarks.
- Detecting **lighting and shadow anomalies** and **geometric distortions**.
- Identifying **compression artifacts** and **pixel-level irregularities**.
- Exploring **optical flow** and **temporal inconsistencies** in video.
- **Case Study**: Analysis of the "Tom Cruise Deepfakes" on TikTok and subtle giveaways.

Module 4: Audio Deepfake Detection and Voice Forensics

- Understanding voice cloning and text-to-speech (TTS) synthesis.
- Techniques for audio waveform analysis and spectrogram interpretation.
- Identifying acoustic artifacts, speech rhythm anomalies, and background noise inconsistencies.
- Introduction to speaker verification and speaker diarization in forensics.
- **Case Study**: The **2019 UK energy firm CEO voice clone fraud** incident.

Module 5: Image Deepfake Detection and Manipulation Forensics

- Spotting inconsistencies in **image composition** and **object realism**.
- Utilizing **Error Level Analysis (ELA)** and **Noise Pattern Analysis**.
- Examining **EXIF data** and other **metadata** for signs of digital alteration.
- Detecting **cloning** and **splicing artifacts**.
- **Case Study**: Forensic analysis of manipulated images circulated during political campaigns.

Module 6: Deepfake Detection Tools and Platforms

- Overview of **AI-powered deepfake detection software** and online tools.
- Hands-on experience with selected **open-source and commercial solutions**.
- Understanding the strengths and limitations of current **detection algorithms**.
- Evaluating tool accuracy, **false positives**, and **false negatives**.
- **Case Study**: Comparison of various deepfake detectors on publicly available datasets like **FaceForensics++**.

Module 7: Digital Forensics Principles for Synthetic Media

- Establishing a **chain of custody** for digital evidence.
- Proper **acquisition, preservation, and handling** of suspected synthetic media.
- Forensic imaging and hashing for **data integrity**.
- Introduction to **forensic workstations** and their capabilities.
- **Case Study**: Reconstructing the digital trail of a deepfake spreading on social media.

Module 8: Advanced Forensic Analysis of Deepfakes

- Deep dive into **neural network architectures** for robust detection.
- Exploring **explainable AI (XAI)** in deepfake forensics.
- Utilizing **feature engineering** to enhance detection accuracy.
- Statistical analysis of **deepfake artifacts** for attribution.
- **Case Study**: Research papers on advanced AI models achieving high deepfake detection rates.

Module 9: Legal and Ethical Implications of Deepfakes

- Understanding current and emerging **legal frameworks** (e.g., **Deepfake Accountability Acts**).
- Discussing **privacy violations**, **defamation**, and **intellectual property** issues.
- The role of **deepfakes in cybersecurity threats** and **national security**.
- Ethical considerations for **AI development** and responsible **synthetic media use**.
- **Case Study**: Legal battles involving deepfake pornography and identity theft.

Module 10: Counter-Deepfake Strategies and Mitigation

- Developing **organizational policies** and best practices.
- Implementing **content authenticity initiatives** and digital watermarking.
- Strategies for **rapid response** to deepfake incidents.
- Public education and **digital literacy campaigns**.
- **Case Study**: Project Origin and the Coalition for Content Provenance and Authenticity (C2PA).

Module 11: Investigating Deepfake Incidents

- Establishing an **investigative methodology** for suspected deepfakes.
- Collecting **digital evidence** from various sources (social media, dark web).
- Working with **metadata** and **network traffic analysis**.
- Interviewing techniques and **intelligence gathering**.
- **Case Study**: The Hong Kong $25 million deepfake scam and the investigative steps taken.

Module 12: Reporting and Documentation

- Crafting comprehensive **forensic reports** for deepfake incidents.

- Presenting findings effectively to **non-technical stakeholders**.
- Guidelines for **admissibility of digital evidence** in court.
- Best practices for **preserving evidence** for future analysis.
- **Case Study**: Examples of effective forensic reports submitted in deepfake-related cases.

Module 13: Emerging Trends and Future Challenges

- The evolving landscape of **generative AI** and new deepfake techniques.
- The impact of **metaverse** and **virtual reality** on synthetic media.
- Future of **deepfake detection research** and **AI countermeasures**.
- The role of **blockchain** in content authentication.
- **Case Study**: Discussions on potential future applications and threats of deepfake technology (e.g., **AI assistants**, **synthetic influencers**).

Module 14: Practical Deepfake Forensics Lab

- Hands-on exercises in **identifying deepfake artifacts** using forensic tools.
- Simulated **deepfake detection challenges** with various media types.
- Practical application of **audio and visual analysis techniques**.
- Working with **deepfake datasets** for model evaluation.
- **Case Study**: Participants analyze a simulated deepfake case from beginning to end.

Module 15: Building a Deepfake Detection and Response Framework

- Developing an **integrated organizational framework** for deepfake resilience.
- Establishing **cross-departmental collaboration** (IT, Legal, PR).
- Creating **internal training programs** and awareness initiatives.
- Continuous monitoring and **threat intelligence sharing**.
- **Case Study**: Designing a hypothetical deepfake response plan for a major corporation or government agency.

Training Methodology

This course employs a blended learning approach, combining:

- **Interactive Lectures**: Delivering core concepts and theoretical foundations.
- **Hands-on Labs**: Practical exercises using industry-standard and open-source **deepfake detection tools**.
- **Case Studies**: In-depth analysis of real-world deepfake incidents and their forensic investigations.
- **Group Discussions**: Fostering collaborative learning and critical thinking on ethical and societal impacts.
- **Live Demonstrations**: Showcasing deepfake creation and detection processes.
- **Expert-Led Sessions**: Insights from leading professionals in **digital forensics**, **cybersecurity**, and **AI research**.
- **Q&A Sessions**: Addressing specific challenges and practical scenarios.

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
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now