

No. 88

AI TRENDS

AI Detection

Spotting AI-generated text, images, audio and video, and what detectors can and cannot tell you, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 88

AI Detection

Spotting AI-generated text, images, audio and video, and what detectors can and cannot tell you, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

AI Detection

Spotting AI-generated text, images, audio and video, and what detectors can and cannot tell you, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SynthID is a trademark of Google LLC. Content Credentials and C2PA are associated with the Coalition for Content Provenance and Authenticity. Other product names mentioned are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why AI detection matters 5
2 Three approaches 6
3 How text detectors work 8
4 Accuracy and errors 10
5 Bias and fairness 12
6 How AI creates content 14

PART II · JUDGING CONTENT

7 Reading text critically 17
8 Images 19
9 Audio and voice clones 21
10 Video and deepfakes 23
11 Watermarks and Content Credentials 25
12 Verifying before you share 27
13 AI and misinformation 29

PART III · POLICY AND FAIRNESS

14 Schools and universities 32
15 Advice for students 34
16 AI content at work 35
17 Laws and labels 36
18 Disclosing your own AI use 38
19 Talking with young people 39

PART IV · PUTTING IT TO WORK

20 Scenarios 42
21 Tools 44
22 The future of detection 45

FREE SAMPLE · ojayo.com

23 Building good habits 46
Checklists 47
Glossary 48
Further reading 49

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

As AI writes essays, emails, news-style articles, photos, voices and videos, people increasingly ask: **was this made by AI?** Searches for AI detection reached an all-time high in early 2026, driven by teachers, students, employers, journalists and anyone worried about scams and fake news.

The honest answer is that **no tool can reliably tell you whether text was written by AI**, and the tools that try make serious mistakes, including falsely accusing people. For images, audio and video, detection is also hard, but **provenance** methods, such as invisible watermarks and signed Content Credentials, are improving, and new laws such as the EU AI Act's transparency rules now require AI providers to mark synthetic content.

This book explains, in plain language, how AI detection works, what it can and cannot do, how to judge content sensibly, and how schools, workplaces and families can respond fairly.

What this book covers

- How AI text detectors work, and their limits.
- Signs to look for in text, images, audio and video.
- Watermarks, Content Credentials and verification habits.
- Fair policies for education and work.
- Laws on labelling AI content, including EU AI Act Article 50.

FREE SAMPLE · ojayo.com

Who this book is for

- **Teachers, lecturers and students**.
- **Managers, editors and HR teams**.
- **Journalists and fact-checkers**.
- **Everyone** who wants to avoid being fooled by fake media.

How the book is organized

- **Part I — Foundations** (Chapters 1–6): why detection matters, the three approaches, how text detectors work, accuracy and errors, bias, and how AI creates content.
- **Part II — Judging content** (Chapters 7–13): reading text critically, images, audio and voice clones, video and deepfakes, provenance, verification, and misinformation.
- **Part III — Policy and fairness** (Chapters 14–19): schools and universities, students, workplaces, laws and labels, disclosing your own AI use, and talking with young people.
- **Part IV — Putting it to work** (Chapters 20–23): scenarios, tools, the future, and building habits.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How a method shows up in real tools.

WATCH OUT
Common mistakes and risks.

FREE SAMPLE · ojayo.com

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

Screens are **simplified illustrations**, not copies of real detection tools. Names in examples are invented.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why AI detection matters, the three main approaches, how text detectors work, how accurate they are, and who they treat unfairly.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why AI detection matters

AI-made content is everywhere, and the stakes of getting detection wrong are high.

Where the question comes up

- **Education**: was this essay the student's own work?
- **Work**: was this report, application or review written by a person?
- **News and social media**: is this photo or video real?
- **Scams**: is this really my relative's voice on the phone?
- **Publishing and hiring**: are reviews, articles or CVs genuine?

The stakes cut both ways

Missing AI content can let misinformation spread or scams succeed. But wrongly calling human work "AI" can damage a student's record, a job application or a writer's reputation.

The FBI's view of AI scams

The FBI's 2025 Internet Crime Report was the first to track AI use: more than 22,000 complaints referenced AI, with about $893 million in reported losses, including voice cloning and synthetic video.

KEY IDEA

"Is it AI?" is often the wrong question. "Is it true, is it fair, and who is responsible?" usually matters more.

FREE SAMPLE · ojayo.com

CHAPTER 2

Three approaches

There are three broad ways to judge whether content is AI-made.

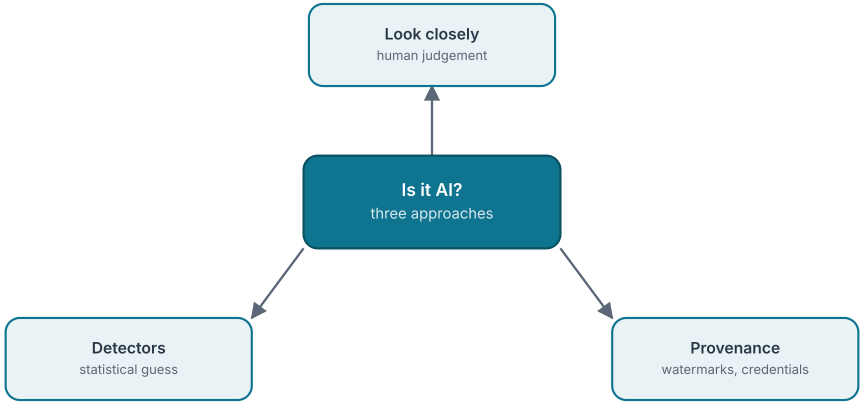


Figure 2.1 Human judgement, detectors and provenance

Human judgement

Looking closely for clues, checking facts and sources, and comparing with what you know about the author. Useful but slow and fallible; AI content is getting better quickly.

Detectors

Software that analyzes content and estimates the probability it is AI-made. Available for text, images, audio and video. Results are **guesses**, not proof.

FREE SAMPLE · ojayo.com

Provenance

Information attached to or hidden in content by the tool that made it: **watermarks** such as Google's SynthID, and **Content Credentials** based on the C2PA standard. When present and intact, provenance is much stronger evidence than a detector's guess.

Signal	Strength
Signed Content Credentials showing AI tool	strong
Watermark detected by vendor tool	strong for that vendor
Platform 'AI-generated' label	medium
Detector score	weak
Looks or sounds 'off'	weak

Figure 2.2 How strong is each signal?

TIP

Combine signals. No single clue should decide an important question.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection (you are reading this)

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

AI Detection

Enjoyed it? The full book has 54 pages and 23 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.