



AI-Driven Digital Image Forensics System

Atharva Dhanshetti, Sugat Katke, Aditya Khose

Diploma in Artificial Intelligence and Machine Learning, D. Y. Patil Polytechnic, Pune, India

atharvadhanshetti69@gmail.com katkesugat@gmail.com adityakhose888@gmail.com

How to Cite this Article:

Dhanshetti, A., Katke, S. & Khose, A. (2026). AI-Driven Digital Image Forensics System. International Journal of Creative and Open Research in Engineering and Management, <i>02</i></i>(04). <https://doi.org/10.55041/ijcope.v2i4.100>

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.



<https://doi.org/10.55041/ijcope.v2i4.100>

ABSTRACT

This paper presents a study on AI-generated image detection using Artificial Intelligence. The main objective of this research is to accurately identify and classify digital images as AI-Generated or Human-Captured. In this work, deep learning techniques are applied through the SightEngine genai cloud API to analyze uploaded images for GAN fingerprints, diffusion artifacts, and texture inconsistencies. The results obtained show that the AI-based system can achieve reliable detection with a tiered confidence scoring mechanism. The study helps in combating misinformation and assisting professionals in verifying image authenticity. Finally, it is concluded that AI can play a significant role in reliable and efficient digital image forensics.

Keywords

AI-generated image detection, digital image forensics, deep learning, CNN, Flask



1. INTRODUCTION

AI-generated images are one of the most critical challenges in digital media today that require timely detection and verification. Traditional methods of image verification involve manual visual inspection by experts, which can be time-consuming and prone to errors. With the advancement in artificial intelligence, automated systems can now assist in analyzing digital images more efficiently.

The AI-Driven Digital Image Forensics System is designed to provide an AI-based solution for detecting AI-generated images. It allows users to upload images and get instant results. The system uses the SightEngine genai deep learning API to analyze images and identify synthetic patterns. The main objective of this project is to reduce the time required for verification and improve accuracy. The system also aims to provide an easy-to-use platform that can be accessed through a web interface.

Literature Review

Several research studies have been conducted on AI-generated image detection using deep learning techniques. Many researchers have used Convolutional Neural Networks (CNN) for analyzing synthetic images. These studies show that deep learning models can achieve high accuracy in detecting AI-generated content.

Some research papers focus on GAN fingerprint detection and frequency domain analysis to identify synthetic artifacts. Other studies highlight the importance of detecting diffusion model residues left by generators like DALL-E and Midjourney. It has been observed that CNN-based models outperform traditional forensic techniques such as error level analysis.

The existing systems demonstrate that AI can significantly improve the efficiency of synthetic image detection. However, many systems lack user-friendly interfaces or real-time processing. The AI-Driven Digital Image Forensics System aims to combine accuracy with usability by providing a complete web-based solution.

Methodology

The methodology of the AI Image Forensics System follows a structured approach using the Agile model. The development process includes multiple stages such as requirement analysis, system design, implementation, testing, and deployment.

Initially, the requirements of the system were identified, including image upload, AI-based analysis, and result display. Then, the system architecture was designed by dividing it into frontend, backend, and AI detection components. The frontend provides the user interface using HTML5, CSS3, and JavaScript, while the Flask backend handles data processing and communication.

The AI detection is powered by the SightEngine genai cloud API trained on millions of real and AI-generated images. When a user uploads an image, it is sent to the Flask backend, where validation and Pillow verification are performed. The verified image is then submitted to the SightEngine API which classifies it as AI-Generated or Human-Captured. The system also extracts ten forensic metadata points and assigns a confidence tier (High, Moderate, or Low). Finally, the result is displayed to the user. The system was tested using multiple image types to ensure accuracy and reliability.

Results

The AI Image Forensics System successfully detects AI-generated images with high reliability. The system provides results within a few seconds after image upload, making it fast and efficient. The user interface works smoothly and allows easy interaction.

The SightEngine genai model performs well in identifying synthetic patterns and classifying images correctly. The system was tested with authentic photographs, DALL-E 3 outputs, Midjourney v6 images, Stable Diffusion XL outputs, and StyleGAN face composites. The results showed consistent performance with appropriate confidence tier



assignments. The integration of frontend, backend, and AI detection layer works effectively, ensuring smooth operation of the system.

Overall, the project achieves its objective of providing a reliable and efficient solution for AI-generated image detection.

Conclusion

The AI-Driven Digital Image Forensics System demonstrates the successful application of artificial intelligence in digital media authentication. The system provides a fast, accurate, and user-friendly solution for detecting AI-generated images. It reduces manual effort and helps in early detection of synthetic content, which is important for combating misinformation.

Although the system has some limitations, it shows great potential for future improvements. The project can be enhanced by using Explainable AI heatmaps, video deepfake detection, and multi-model ensemble approaches. Overall, the system serves as a useful tool for verifying image authenticity and highlights the importance of AI in digital forensics.

References

Sr.No	Category	Title	Link	Description
1.	Research Paper	CNN-Generated Images Are Easy to Spot	https://arxiv.org/abs/1912.11035	Foundational CNN-based GAN detection theory (IEEE CVPR 2020).
2.	Research Paper	Detection of Synthetic Images by Diffusion Models	https://arxiv.org/abs/2211.00680	Diffusion model residues detection (IEEE ICASSP 2023).
3.	Research Paper	Are GAN Images Easy to Detect?	https://arxiv.org/abs/2104.02617	Benchmark for deepfake detection algorithms (IEEE ICME 2021).
4.	API Documentation	SightEngine AI Content Detection API	https://sightengine.com/docs	Cloud API for AI-generated image detection using genai model.
5.	Framework Documentation	Flask Documentation (Version 3.0)	https://flask.palletsprojects.com	Python web framework used for backend development.
6.	Library Documentation	Pillow Documentation (Version 10+)	https://pillow.readthedocs.io	Image processing library for verification and metadata extraction.
7.	Language Documentation	Python 3.8+ Documentation	https://docs.python.org/3/	Core language for system implementation.
8.	Library Documentation	Requests Library Documentation	https://requests.readthedocs.io	HTTP library for API communication.
9.	Library Documentation	Werkzeug Utilities Documentation	https://werkzeug.palletsprojects.com	WSGI library for secure filename handling.
10.	Academic Curriculum	MSBTE K-Scheme Capstone Project (316004)	https://msbte.org.in	Project documentation and evaluation framework.