Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

AI-BASED DETECTION AND FORENSIC ANALYSIS OF DEEPFAKE IMAGES

HARINE P.R

B.Sc FORENSIC SCIENCE FINAL YEAR

Ms. ATHULYA PRABHAKRAN

Abstract - Deepfake images created using artificial intelligence have become a serious challenge in the modern digital world. These images are generated or manipulated using advanced AI technologies to produce highly realistic fake visual content. The misuse of deepfake images may lead to misinformation, identity theft, cybercrime, social manipulation, and digital fraud. As AI-generated images become more realistic, it becomes difficult to distinguish fake images from genuine images through normal visual observation. Therefore, digital forensic analysis plays an important role in identifying manipulated or AI-generated images. This study focuses on the AI-based detection and forensic analysis of deepfake images using different forensic examination techniques. A total of twenty sample images, including ten real images and ten AI-generated images, were analyzed using AI image detection tools, Error Level Analysis (ELA), clone detection, and metadata analysis. The forensic examination was conducted to identify visual inconsistencies, editing traces, image manipulation artifacts, and metadata variations between real and AI-generated images.

The analysis revealed that AI-generated images often contain abnormal compression patterns, inconsistent image regions, missing metadata information, and signs of digital manipulation when compared to real images. Real images generally showed natural compression levels, original metadata details, and fewer editing artifacts. The findings of the study indicate that forensic techniques are effective in differentiating authentic images from AI-generated deepfake images. This research highlights the importance of digital forensic tools and AI detection systems in image authentication and cyber investigation. The study also emphasizes the growing need for advanced forensic technologies to prevent the misuse of deepfake content in digital platforms and maintain the authenticity of digital media.

KEYWORDS

Deepfake Images, Artificial Intelligence, Digital Forensics, AI Detection, Error Level Analysis, Clone Detection, Metadata Analysis, Image Authentication, Cybercrime, Digital Image Examination.

INTRODUCTION

Artificial intelligence has rapidly transformed digital media technologies, especially in the field of image generation and manipulation. One of the most significant developments in this area is the creation of deepfake images. Deepfake images are digitally generated or manipulated images produced using artificial intelligence techniques such as deep learning, machine learning, and generative adversarial networks. These images are designed to appear realistic and visually convincing, making it difficult for ordinary viewers to identify whether the image is real or fake.

The increasing use of deepfake technology has created serious concerns in society because manipulated images can be used for spreading misinformation, creating fake identities, damaging reputations, cyber harassment, and digital fraud. Digital forensic analysis plays a major role in detecting manipulated images and identifying traces of digital editing. Various forensic techniques such as AI image detection, Error Level Analysis (ELA), clone detection, and metadata examination help forensic experts analyze suspicious images scientifically. These techniques assist investigators in identifying image inconsistencies, compression artifacts, editing traces, and hidden manipulation patterns.

This study focuses on the forensic comparison between real images and AI-generated deepfake images. The research aims to identify the observable differences between authentic and manipulated images using forensic analysis tools. The study also examines the effectiveness of digital forensic techniques in detecting deepfake image manipulation and improving image authentication methods.

STATEMENT OF THE PROBLEM

The rapid advancement of artificial intelligence technologies has increased the creation and distribution of deepfake images across digital platforms. These AI-generated images are often highly realistic and difficult to distinguish from genuine photographs. As a result, deepfake images can be misused for cybercrime, misinformation, identity theft, social manipulation, and online fraud. In forensic investigations, identifying whether an image is authentic or AI-generated has become a major challenge. Traditional visual examination methods

are often insufficient to detect modern deepfake images because AI technologies can create highly detailed and realistic content. Although several forensic tools are available, there is still a need to study the effectiveness of AI-based detection methods and forensic analysis techniques in identifying manipulated images accurately.

Therefore, this study attempts to analyze and compare real images and AI-generated deepfake images using forensic examination techniques such as AI detection, Error Level Analysis, clone detection, and metadata analysis to understand their reliability and forensic significance.

OBJECTIVES OF THE STUDY

1. To study the characteristics of real and AI-generated deepfake images.
2. To analyze deepfake images using AI detection tools.
3. To examine image manipulation using Error Level Analysis (ELA).
4. To identify cloned or duplicated regions in manipulated images.
5. To compare metadata information between real and AI-generated images.
6. To understand the forensic importance of deepfake image detection in digital investigations.

SCOPE OF THE STUDY

The scope of this study is limited to the forensic examination and comparison of real images and AI-generated deepfake images using digital forensic analysis techniques. The research mainly focuses on analyzing image authenticity through AI detection tools, Error Level Analysis, clone detection, and metadata examination.

The study is useful in the field of digital forensics, cybersecurity, and forensic image analysis. The findings may help forensic experts, researchers, cyber investigators, and students understand the characteristics of manipulated images and improve image verification methods. The research also contributes to the growing field of AI-generated content detection and digital media authentication.

REVIEW OF LITERATURE

Digital image forensics has become an important area of research due to the rapid development of image editing software and artificial intelligence technologies. Researchers have studied various forensic methods used to detect manipulated images and identify digital alterations. Studies explain that image manipulation leaves certain forensic traces such as compression inconsistencies, editing artifacts, cloned regions, and metadata modifications, which can be identified using forensic tools.

Several researchers have focused on AI-generated deepfake detection techniques. Earlier studies observed that deepfake images created using deep learning algorithms often contain visual inconsistencies, unnatural textures, abnormal lighting patterns, and irregular pixel distributions. These characteristics can help forensic experts distinguish manipulated images from authentic images.

Research related to Error Level Analysis explains that manipulated images usually show uneven compression patterns compared to original images. Similarly, clone detection techniques help identify duplicated image regions created during editing or manipulation processes. Metadata examination is also considered an important forensic method because AI-generated images often lack original camera information and editing history.

Recent studies indicate that combining multiple forensic techniques improves the accuracy of deepfake image detection. AI detection systems and digital forensic tools together provide reliable methods for identifying manipulated content and preventing the misuse of AI-generated media.

RESEARCH METHODOLOGY

Research methodology refers to the systematic procedure used to conduct the study and achieve the research objectives through organized data collection and analysis. In this study, a descriptive and comparative research design was adopted to examine the differences between real images and AI-generated deepfake images.

A total of twenty sample images were selected for forensic analysis. Among them, ten were real images collected from original image sources, and ten were AI-generated images created using artificial intelligence image generation tools. The images were analyzed under similar conditions to ensure accurate comparison and observation.

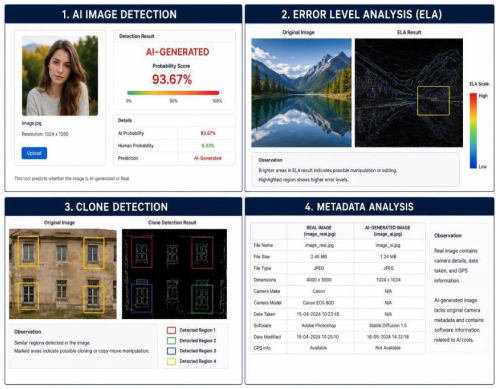
The study mainly used primary data obtained directly from image samples. Secondary data was referred from journals, research articles, forensic science books, and online resources related to digital image forensics and deepfake detection.

The forensic examination was conducted using the following techniques:

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

- AI Image Detection
- Error Level Analysis (ELA)
- Clone Detection
- Metadata Analysis

Each image was uploaded into forensic analysis tools to identify signs of digital manipulation. The obtained results were carefully observed and compared to determine the forensic differences between authentic and AI-generated images.



DATA ANALYSIS AND INTERPRETATION

The collected real and AI-generated images were analyzed using different forensic techniques to identify image manipulation characteristics and forensic artifacts. The examination helped in understanding the differences between authentic images and deepfake images.

Analysis of AI Detection

The AI image detection tool was used to determine whether the selected images were human-generated or AI-generated. Most real images were identified as authentic images, whereas the AI-generated samples were classified as manipulated or artificially generated content.

Interpretation

The AI detection tool successfully differentiated most deepfake images from real images based on image texture, pixel patterns, and AI-generated artifacts. This indicates that AI detection systems can support forensic image authentication.

Analysis of Error Level Analysis (ELA)

Error Level Analysis was performed to identify compression inconsistencies and edited regions within images. Real images generally displayed uniform compression levels, while AI-generated images showed irregular patterns and uneven error levels in certain regions.

Interpretation

The irregular ELA patterns observed in deepfake images indicate possible image manipulation and artificial generation. Uniform compression in real images suggests natural image formation without significant digital editing.

Analysis of Clone Detection

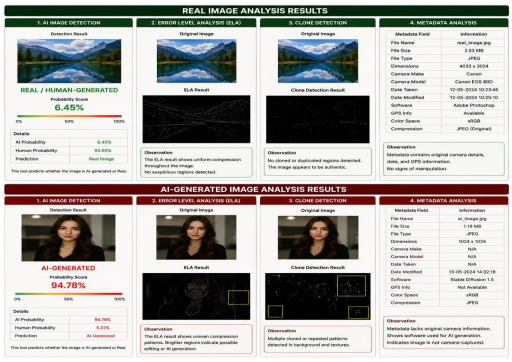
Clone detection analysis was conducted to identify duplicated or manipulated image regions. Most real images showed no significant cloned regions, whereas some AI-generated images displayed repeated textures and duplicated patterns.

Interpretation

The presence of duplicated regions and repeated image structures in AI-generated images indicates digital manipulation and artificial image synthesis. Clone detection is therefore useful in identifying suspicious image modifications.

Analysis of Metadata

Metadata analysis examined information such as camera



details, image creation history, software information, and editing traces. Real images contained original camera metadata and image properties, while many AI-generated images lacked metadata details or showed software-generated information.

Interpretation

The absence of original metadata information in AI-generated images suggests artificial image creation and digital processing. Metadata examination therefore acts as an important forensic indicator during image authentication.

FINDINGS OF THE STUDY

- AI-generated deepfake images showed noticeable forensic differences when compared to real images.
- AI detection tools successfully identified most manipulated images as AI-generated content.
- Error Level Analysis revealed irregular compression patterns in deepfake images.
- Clone detection identified duplicated regions and repeated textures in manipulated images.
- Real images contained original metadata information, while AI-generated images often lacked metadata details.
- Combining multiple forensic techniques improved the accuracy of deepfake image detection.
- Digital forensic analysis plays an important role in identifying manipulated visual content

SUGGESTIONS

1. Future studies may include a larger number of image samples for more accurate analysis.
2. Advanced AI detection software may be used to improve deepfake identification methods.
3. Researchers may analyze video deepfakes in addition to image-based deepfakes.
4. Digital forensic laboratories should adopt modern forensic tools for image authentication.
5. Awareness programs related to deepfake misuse and cyber safety should be encouraged.
6. Further research may focus on real-time deepfake detection systems for social media platforms.

CONCLUSION

The study on AI-based detection and forensic analysis of deepfake images highlights the growing importance of digital image forensics in the modern technological world. Artificial intelligence has made image generation and manipulation highly advanced, creating serious challenges in distinguishing real images from AI-generated content.

The forensic examination conducted in this study identified several differences between authentic images and deepfake images through AI detection, Error Level Analysis, clone detection, and metadata analysis. Deepfake images showed irregular compression patterns, missing metadata information, duplicated image structures, and artificial image characteristics when compared to real images.

The findings confirm that digital forensic tools and AI detection systems are effective in identifying manipulated images and supporting image authentication. The study also emphasizes the importance of combining multiple forensic techniques for accurate deepfake detection.

Overall, this research highlights the role of forensic science in preventing the misuse of AI-generated content and improving digital evidence verification. As deepfake technologies continue to develop, advanced forensic methods will become increasingly important in cybersecurity, criminal investigation, and digital media authentication.

LIMITATIONS OF THE STUDY

1. The study was limited to a small number of sample images.
2. Only image-based deepfake analysis was conducted, and video deepfakes were not included.
3. The analysis mainly depended on available forensic tools and software.
4. Some AI-generated images may closely resemble authentic images and reduce detection accuracy.
5. Environmental factors such as image quality and compression may influence forensic analysis results.
6. Advanced deepfake technologies may require more sophisticated forensic examination methods.

REFERENCES

1. Hany Farid, “Digital Image Forensics,” IEEE Signal Processing Magazine, 2009.
2. Chesney, R., & Citron, D., “Deepfakes and the New Disinformation War,” Foreign Affairs, 2019.
3. Verdoliva, L., “Media Forensics and Deepfake Detection,” IEEE Journal, 2020.
4. Fridrich, J., “Image Manipulation Detection,” Digital Forensic Research Workshop, 2012.
5. Zhang, X., et al., “Detecting AI-Generated Fake Images Using Deep Learning,” Journal of Artificial Intelligence Research, 2021.
6. Research articles related to deepfake detection and digital image forensics.
7. Academic materials related to cybersecurity and forensic image analysis.