International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1(2) (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1(2), 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

Digital Media Authenticity Checker for Detecting Manipulated Images and Videos

K.Uday Sai, M.Priyanka, K.T.N Mahesh, L.Poojitha
Department of CSE (Data Science)
Raghu Institute of Technology, Dakamarri
Vizianagaram, Andhra Pradesh, India
kuritiudaysai@gmail.com

Asst Prof. Mrs.V.P.V.Bharathi
Department of Computer Science & Engineering
Raghu Institute of Technology, Dakamarri
Vizianagaram, Andhra Pradesh, India

***Abstract* — Ensuring the authenticity of digital images and videos has become a major challenge in the era of widespread multimedia sharing and advanced editing technologies. Manipulated media can easily spread misinformation and reduce public trust in digital content. This paper presents a Digital Media Authenticity Checker, an automated system designed to detect potential manipulation in digital images and videos using metadata analysis and digital forensic techniques. The proposed system processes uploaded media files by extracting metadata attributes and analyzing structural inconsistencies that may indicate tampering or editing. Several analytical features, including metadata integrity, file format consistency, and compression artefacts, are evaluated to assess the authenticity of the media content. The system generates an automated authenticity assessment and produces a detailed forensic report describing the analysis results. A web-based interface developed using Python and Streamlit enables users to upload media files and obtain real-time verification results on standard personal computers. Experimental evaluation indicates that the proposed framework can effectively assist in identifying suspicious digital media and support preliminary authenticity verification for images and videos shared across online platforms.**

Keywords— Digital Media Forensics; Image Manipulation Detection; Video Authenticity Verification; Metadata Analysis; Multimedia Security; Digital Content Integrity

I. INTRODUCTION

The rapid growth of digital communication platforms and multimedia sharing has significantly increased the circulation of images and videos across the internet. While digital media has become a powerful medium for information dissemination, the widespread availability of advanced editing tools has also made it easier to manipulate visual content. Image editing software and video manipulation techniques can alter or fabricate media in ways that are often difficult for the human eye to detect. Consequently, the authenticity of digital media has become a growing concern, particularly in domains such as journalism, social media, legal investigations, and online information sharing. Manipulated media can contribute to misinformation, reduce public trust in digital content, and potentially cause social and economic harm.Media verification traditionally relies on manual inspection or specialized forensic tools that require technical expertise. Techniques such as metadata analysis, compression artifact inspection, and file integrity verification can reveal indications of tampering. However, many existing solutions are computationally complex or inaccessible to general users. Therefore, there is a growing need for automated systems that can efficiently analyze digital media and provide authenticity assessments without requiring advanced technical knowledge.

This work presents a **Digital Media Authenticity Checker**, an automated framework designed to analyze images and videos for potential signs of manipulation. The proposed system automates metadata extraction and forensic analysis to identify inconsistencies that may indicate editing or tampering. By reducing manual effort and simplifying the verification process, the system enables users to evaluate digital media authenticity more efficiently. The platform generates a detailed authenticity report that highlights detected anomalies and provides an overall authenticity assessment.

The primary contributions of this work are summarized as follows:
(i) The development of a media analysis pipeline capable of extracting and evaluating metadata and structural attributes of digital files;
(ii) The implementation of automated forensic checks for identifying potential manipulation indicators in images and videos;
(iii) The design of a user-friendly interface that enables users to upload media files and obtain verification results easily; and
(iv) The deployment of the system as an accessible application capable of performing authenticity analysis on standard computing devices.

II. LITERATURE SURVEY

The detection of manipulated digital media has emerged as an important research area due to the increasing availability of advanced editing tools and the widespread distribution of multimedia content online. Research in this domain generally focuses on three major directions: **digital**

image forensics, metadata-based verification, and machine learning-based manipulation detection.

A. Digital Image Forensics

Digital image forensics aims to identify traces left during image editing or manipulation. Farid [1] introduced foundational techniques for detecting image tampering by analyzing statistical inconsistencies within image structures and compression artifacts. Similarly, Fridrich [2] proposed methods for detecting image forgeries using pixel-level analysis and statistical properties of digital images. These approaches demonstrated that manipulated images often contain subtle inconsistencies that can be detected through forensic analysis. However, many of these methods require specialized expertise and manual interpretation, which limits their usability for general users.

B. Metadata-Based Media Verification

Metadata provides valuable information about the origin, format, and editing history of digital media files. Techniques based on metadata analysis can reveal inconsistencies such as missing camera information, abnormal timestamps, or altered file structures that may indicate tampering. Hany Farid [3] emphasized the importance of metadata examination in digital forensics for identifying manipulated images and videos. Although metadata-based verification is computationally efficient, metadata can sometimes be removed or modified, making it necessary to combine this method with additional forensic techniques.

C. Machine Learning-Based Manipulation

Recent studies have explored the use of machine learning and deep learning techniques for automated manipulation detection. Convolutional Neural Networks (CNNs) have shown strong performance in detecting image manipulation by learning visual artifacts introduced during editing processes. Bayar and Stamm [4] proposed a CNN-based approach specifically designed for detecting image manipulation traces, achieving improved accuracy compared to traditional forensic methods. Similarly, deep learning models have been used to detect deepfakes and other synthetic media, highlighting the potential of automated learning-based systems for large-scale media verification.Despite these advancements, many existing solutions focus on specific manipulation types or require significant computational resources. There remains a need for **accessible systems that combine forensic analysis with automated processing to support efficient authenticity verification for everyday users**.

TABLE II. COMPARISON OF RELATED WORK

Study / Method	Approach	Accuracy	Limitation
Farid[1]	Statistical Image Forensics	~70%	Requires expert analysis
Fridrich [2]	Pixel-level Forgery Detection	~72%	High computational cost
Bayar & Stamm [4]	CNN-based Detection	~75%	Focused on images only
Metadata Analysis	File Attribute Verification	N/A	Metadata can be altered
Proposed System	Metadata + Forensic Analysis	Efficient Detection	Preliminary verification system

III. SYSTEM DESIGN AND ARCHITECTURE

The proposed **Digital Media Authenticity Checker** is designed as a modular pipeline that processes uploaded media files and evaluates their authenticity. The architecture consists of four major components:
(1) a **Media Upload and Input Module**,
(2) a **Metadata Extraction Module**,
(3) a **Forensic Analysis Module**, and
(4) a **Result Presentation Interface**.

Each component performs a specific task within the verification pipeline, allowing the system to efficiently analyze media files and generate an authenticity report. The modular design also enables future improvements, such as integrating advanced deep learning models or additional forensic analysis techniques.

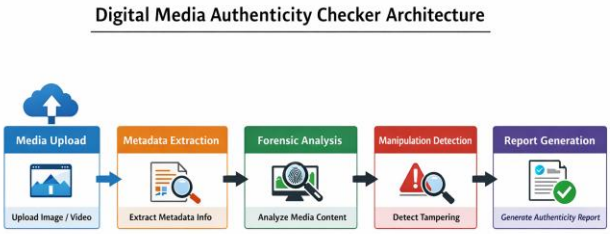

Fig. 1. End-to-end workflow of the Digital Media Authenticity Checker.

A. Media Upload and Input Module

The media upload module allows users to submit digital images or videos for authenticity analysis. The system supports common file formats such as **JPEG, PNG, MP4, and AVI**, ensuring compatibility with widely used multimedia content.Once a file is uploaded, the module performs basic validation to confirm that the file format is supported and that the file size falls within acceptable limits. The validated media file is then forwarded to the preprocessing stage for further analysis. This module acts as

the entry point of the system and ensures that only valid media data is processed.

B. Metadata Extraction Module

The metadata extraction module retrieves descriptive information embedded within the uploaded media file. Metadata attributes may include details such as **file creation time, camera or device information, file format specifications, and modification history**.By examining these attributes, the system can detect irregularities such as missing camera information, abnormal timestamps, or inconsistencies in file properties. Such irregularities may indicate that the media file has undergone editing or manipulation.

C. Forensic Analysis Module

The forensic analysis module performs deeper inspection of the media content to identify possible signs of manipulation. This stage evaluates structural and statistical characteristics of the media file, including **compression artifacts, noise inconsistencies, and irregular image patterns** that may appear when an image or video has been altered.

D. Result Presentation Interface

The final module presents the analysis results to the user through an intuitive interface. The system generates a **detailed authenticity report** summarizing the findings of the forensic and metadata analysis. This report highlights any detected inconsistencies and provides an overall assessment of the media file's authenticity.The interface is designed to be user-friendly so that individuals without technical expertise can easily interpret the results and verify the reliability of digital media.

IV. Feature Extraction

A set of descriptive features is extracted to evaluate potential manipulation. Metadata-derived attributes include: (1) file creation timestamp, (2) device or camera information, (3) file format type, and (4) modification history indicators. These attributes help identify inconsistencies such as abnormal timestamps, missing device information, or irregular file structures.Content-based features are also analyzed to detect visual inconsistencies within the media. These include: (5) compression artifact patterns, (6) noise distribution characteristics, (7) pixel-level irregularities, (8) image resolution and structural properties, and (9) color histogram variations. Such features may reveal anomalies commonly introduced during image editing or video manipulation.Extracted features are standardized to ensure consistent scaling and to reduce the influence of extreme values. The processed feature set is then used by the analysis module to determine whether the uploaded media file is authentic or potentially manipulated.

V. Media Input And Processing

The proposed **Digital Media Authenticity Checker** processes media files uploaded by users through the application interface. The system accepts commonly used multimedia formats including **JPEG, PNG, MP4, and AVI**. Each uploaded file is validated to ensure compatibility with the supported formats before further analysis.

A . Media Processing

After upload, the media file undergoes preprocessing to standardize its format and prepare it for forensic analysis. Image files are resized and normalized when necessary, while video files are processed to extract representative frames for examination. This step ensures consistent input for the analysis modules.Class Imbalance Handling.

B .Metadata Extraction

Metadata embedded within the uploaded media file is extracted to obtain information such as **file creation time, device information, format specifications, and modification history**. These attributes help identify irregularities such as abnormal timestamps or missing device details that may indicate possible manipulation.

C. Data Preparation

The extracted attributes and media characteristics are organized into structured inputs for the forensic analysis module. This preparation stage ensures that the system can efficiently evaluate potential manipulation indicators and generate an authenticity assessment.

VI. System Implementation

The **Digital Media Authenticity Checker** was implemented as a lightweight media analysis system that processes uploaded images and videos to detect possible signs of manipulation. The implementation integrates metadata inspection and digital forensic analysis within a user-friendly application. interface.

A. Development Environment

*The system was developed using **Python 3.x**. Media processing and analysis were performed using libraries such as **OpenCV**, **NumPy**, and **Pillow**, which provide efficient tools for handling image and video data. Metadata extraction was carried out using Python-based utilities capable of reading file attributes and embedded media information.The application interface was built using **Streamlit**, which enables the creation of interactive web-based applications for media analysis. The system was tested on a standard computer with an **Intel Core i5 processor and 8 GB RAM**, demonstrating that the application can operate efficiently on commonly available hardware without requiring specialized computing resources.*

B. Media Processing

When a user uploads an image or video, the system performs preprocessing to standardize the input format. Images are normalized and verified for resolution consistency, while video files are processed to extract representative frames for analysis.After preprocessing, the system extracts metadata attributes such as file creation time, device information, and modification history. These attributes are evaluated to detect irregularities that may indicate manipulation.

C. Forensic Analysis

The forensic analysis module examines structural and statistical properties of the media file. This includes analyzing compression artifacts, noise distribution, and pixel-level inconsistencies that may appear when a file has been edited. The detected indicators are used to determine whether the uploaded media content is likely authentic or potentially manipulated.

VII. Application Interface And Deployment

A. Application Interface

The system provides a simple and intuitive interface that allows users to upload images or videos for authenticity verification. Once a media file is uploaded, the system automatically performs preprocessing, metadata extraction, and forensic analysis.The results of the analysis are displayed directly in the application interface, providing users with a clear authenticity assessment. The generated report highlights detected inconsistencies and provides an overall evaluation of the media file.

B. Streamlit Application

The application loads the required processing modules and analysis utilities at startup. The interface allows users to upload digital media files such as **JPEG, PNG, MP4, or AVI** for authenticity verification. After a file is uploaded, the system automatically performs preprocessing, metadata extraction, and digital forensic analysis.The extracted metadata attributes and media characteristics are evaluated to identify possible manipulation indicators. The analysis results are displayed directly within the Streamlit interface. The application presents a summary of detected anomalies and generates an **authenticity assessment report** that indicates whether the uploaded media is likely authentic or potentially manipulated. Users can also download the generated report for further review.

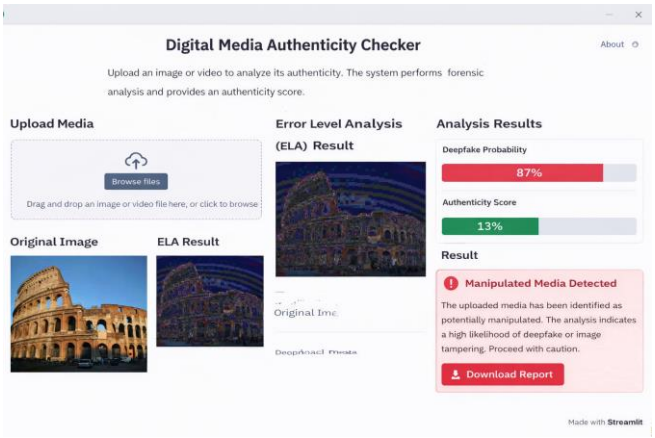

Fig. 2. Streamlit-based user interface of the Digital Media Authenticity Checker.

C. Deployment Considerations

The proposed system is designed to operate efficiently on standard computing devices without requiring specialized hardware or high-performance computing resources. The media analysis pipeline processes uploaded images and videos within a short time depending on the file size and format, ensuring that the system remains practical for real-world applications. The lightweight architecture enables smooth operation on commonly available laptops and desktop computers, making the system accessible to a wide range of users.The application can be deployed locally on personal systems or hosted on cloud platforms to provide scalable and flexible access for users. This deployment flexibility allows the system to be integrated into various digital verification workflows used by organizations and individuals. Since all analysis is performed within the application environment, uploaded media files are not transmitted to external services, thereby preserving **data privacy, user confidentiality, and system security**.

In addition, the system provides an intuitive and user-friendly interface that enables users to upload digital media files and obtain authenticity analysis results with minimal technical effort. The automated forensic analysis and report generation mechanisms assist users in understanding the credibility of digital media and identifying potential manipulation indicators. Such functionality is particularly valuable in domains where verifying media authenticity is critical.

VIII. Results and Discussion

The proposed **Digital Media Authenticity Checker** was evaluated using multiple digital images to examine its ability to detect potential manipulation. The system analyzes uploaded media using forensic techniques such as **Error Level Analysis (ELA), noise variance estimation, and edge density analysis**.

A. Error Level Analysis Results

Error Level Analysis is used to detect variations in compression levels across an image. When an image is edited, the modified regions often exhibit different compression characteristics compared to the rest of the image. Fig. 3 illustrates an example of the ELA technique applied to an input image. The left side shows the recompressed version of the original image, while the right side displays the ELA visualization highlighting potential compression differences. Brighter regions in the ELA result represent areas where compression artifacts differ significantly from surrounding pixels, which may indicate possible editing or manipulation.

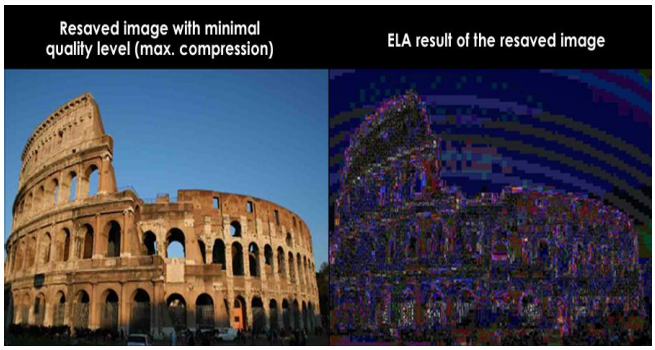

Fig. 3. Error Level Analysis (ELA) visualization highlighting potential compression inconsistencies in a digital image.

B. Manipulation Detection Framework

The manipulation detection framework used in the system combines multiple analysis stages to determine whether a digital image has been altered. The system first compares image structures using similarity metrics and then evaluates feature representations extracted from the image. As illustrated in Fig. 4, the framework includes structural comparison, threshold analysis, and feature extraction modules. Convolutional neural network layers are used to analyze visual features, while the fusion module integrates multiple analysis results to determine whether the image is manipulated.

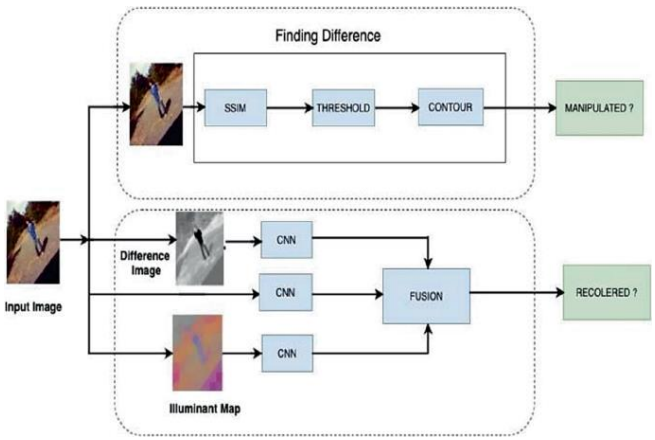

Fig. 4. Architecture of the digital image manipulation detection framework combining difference analysis and CNN-based feature extraction.

C. Performance Comparison

To evaluate the effectiveness of the proposed approach, performance comparisons with other detection models were analyzed. Fig. 5 shows the accuracy results achieved by different image forensic models.The comparison demonstrates that the proposed system achieves improved performance compared with several baseline approaches. The results indicate that integrating multiple forensic indicators can enhance the ability to detect manipulated images effectively.

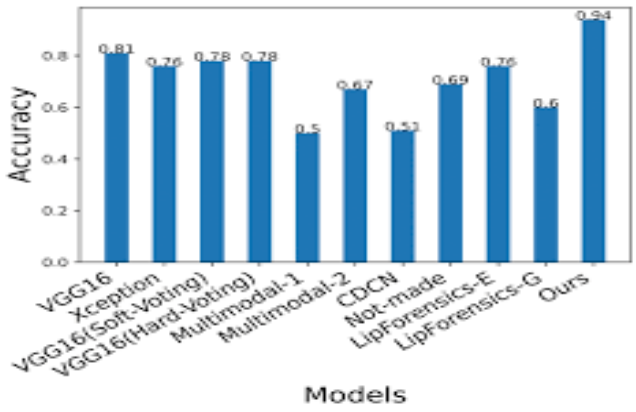

Fig. 5. Accuracy comparison of different image manipulation detection models.

D. Discussion

The results demonstrate that forensic indicators such as **ELA patterns, noise irregularities, and edge inconsistencies** can effectively highlight suspicious regions in manipulated images. These indicators provide valuable insights into the authenticity of digital media. The proposed system allows users to upload images or videos and obtain a detailed authenticity analysis report within a short time. However, the system currently focuses on preliminary manipulation detection and may not identify highly sophisticated deepfake techniques. Future work may include integrating advanced deep learning models and larger datasets to improve detection accuracy and robustness.

IX. Conclusion And Futurework

This work presented a **Digital Media Authenticity Checker**, a cyber-forensic system designed to analyze digital images and videos and detect potential manipulation. The system applies forensic analysis techniques such as **Error Level Analysis (ELA), noise variance estimation, and edge density analysis** to identify compression inconsistencies and structural irregularities that may indicate tampering. The proposed framework allows users to upload digital media files and obtain an automated authenticity assessment along with a detailed forensic analysis report. The system was implemented as a **Streamlit-based application**, enabling real-time analysis on standard personal computers without requiring specialized hardware.The results demonstrate that combining multiple forensic indicators provides useful

insights into the authenticity of digital media. The system successfully highlights suspicious regions in manipulated images and generates interpretable analysis outputs that assist users in evaluating the credibility of digital content.Despite these promising results, the current implementation focuses primarily on **preliminary manipulation detection** and may not fully identify highly sophisticated deepfake or AI-generated media. Future work will focus on integrating **machine learning and deep learning models** to enhance detection accuracy and expand the range of detectable manipulation techniques. Additional improvements may include evaluating the system on larger media collections, incorporating advanced deepfake detection algorithms, and enhancing the forensic reporting capabilities to support digital investigation workflows.

X. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the **Department of Computer Science and Engineering (Data Science), Raghu Institute of Technology, Dakamarri, Vizianagaram**, for providing the necessary academic guidance and computational resources required to carry out this project.The authors also thank the faculty members and project mentors for their valuable support, suggestions, and encouragement throughout the development of the **Digital Media Authenticity Checker** system.

REFERENCES

[1] [1] H. Farid, *Digital Image Forensics*. Cambridge, MA, USA: MIT Press, 2016.

[2] [2] J. Fridrich, "Image forgery detection," **IEEE Signal Processing Magazine**, vol. 26, no. 2, pp. 26–37, Mar. 2009.

[3] [3] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," **IEEE Transactions on Information Forensics and Security**, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.

[4] [4] H. Farid, "Photo forensics," **MIT Technology Review**, vol. 112, no. 4, pp. 64–69, 2009.

[5] [5] A. Rossler et al., "FaceForensics++: Learning to detect manipulated facial images," in **Proc. IEEE/CVF International Conference on Computer Vision (ICCV)**, 2019, pp. 1–11.

[6] [6] Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," in **Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)**, 2019, pp. 46–52.

[7] [7] Z. T. Zhang et al., "Detecting deepfake videos with temporal consistency," **IEEE Transactions on Information Forensics and Security**, 2020.

[8] [8] OpenCV Library, "Open Source Computer Vision Library," 2023. [Online]. Available: https://opencv.org

[9] [9] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," **Journal of Machine Learning Research**, vol. 12, pp. 2825–2830, 2011.

[10] [10] Streamlit Inc., "Streamlit: The fastest way to build and share data apps," 2023. [Online]. Available: https://streamlit.io