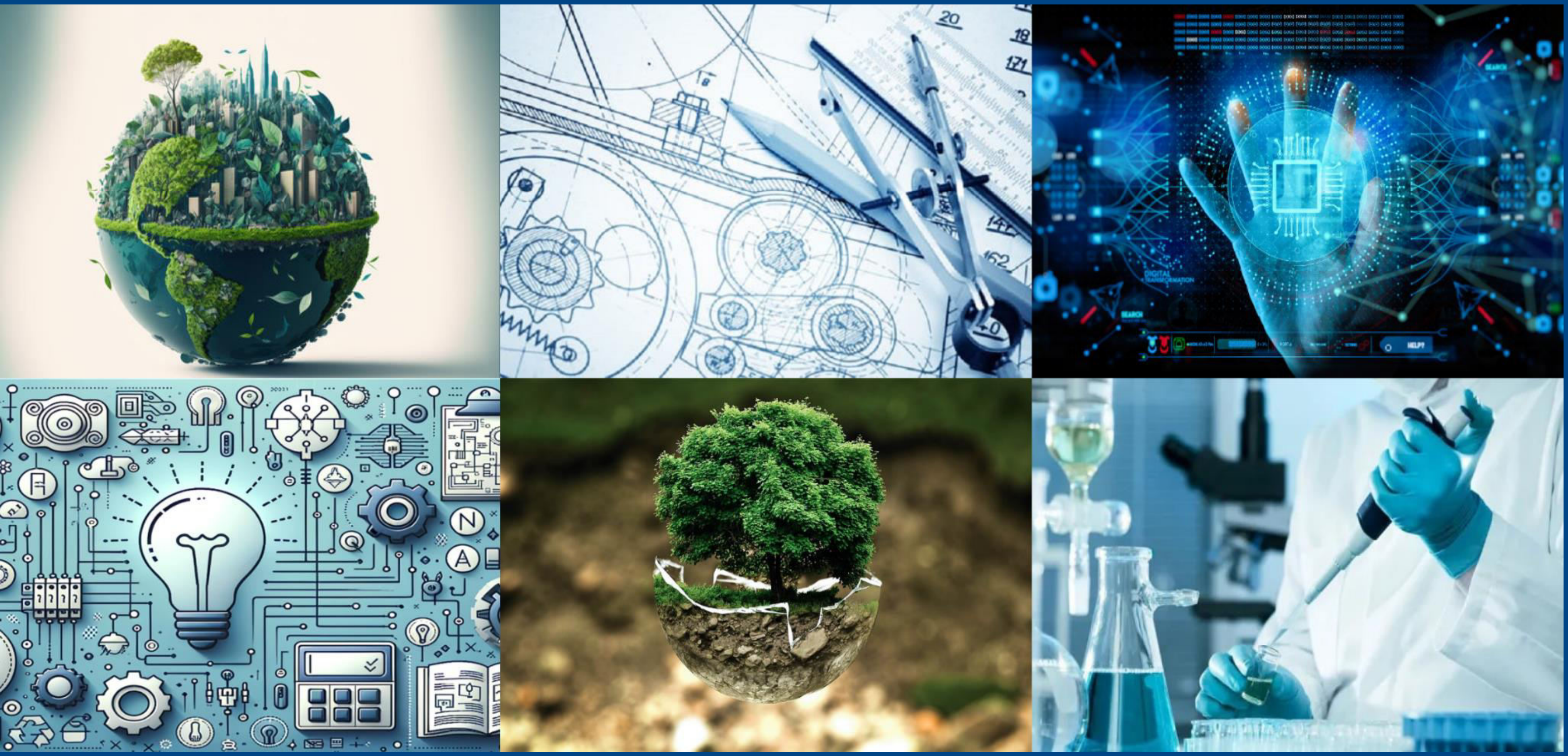
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

www.ijmrset.com ✉ ijmrset@gmail.com ☎ +91 6381 907 438 ☎ +91 63819 07438

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803221

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Forensic Analysis of Image Splicing and Its Detection Techniques

A.Jeevarathinam[1], Mohith S M[2]

Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[1]

III B.Sc, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Image manipulation techniques have evolved, posing significant challenges to authenticity verification. Advanced editing tools and AI- generated forgeries make it increasingly difficult to differentiate between real and altered images. Traditional verification methods such as manual inspection and reverse image searches are often unreliable due to the complexity of image modifications. This paper presents a web-based Image Forgery Detection System that utilizes EXIF metadata analysis to verify the authenticity of digital images. By extracting metadata such as camera model, timestamps, and editing history, the system enables users to assess whether an image has been manipulated. This paper presents a web- based Image Forgery Detection System that utilizes EXIF metadata analysis to verify the authenticity of digital images. By extracting metadata such as camera model, timestamps, and editing history, the system enables users to assess whether an image has been manipulated. The proposed system is developed using Flask and incorporates the exifread library to efficiently analyze image metadata. Users can upload images through an intuitive web interface, where the system classifies them based on metadata availability. Unlike conventional detection methods that rely on expert forensic tools. The system supports multiple image formats such as PNG, JPG and GIF, ensuring broad usability across different platforms. This enhancement would complement the metadata analysis by providing a secondary layer of verification, ensuring more accurate detection of altered images. Beyond metadata analysis, the system can be enhanced by integrating machine learning models to detect image alterations at the pixel level. By incorporating Convolutional Neural Networks (CNNs) and other deep learning algorithms, the system analyse image patterns, lighting anomalies, texture mismatches, significantly improving the accuracy of forgery detection. This approach provides an additional layer of verification, ensuring that even images with altered or missing metadata can be assessed for authenticity.

I. INTRODUCTION

Digital image forgery has become a widespread issue due to the accessibility of advanced image editing software and AI- generated content. Manipulated images are often used for deceptive purposes, including spreading misinformation, altering historical records, and committing fraud. As a result, there is an urgent need for effective and automated forgery detection systems. Traditional image authentication methods rely on manual inspection or third-party software, which are often inadequate due to the complexity of modern forgery techniques. This study proposes a web-based Image Forgery Detection System that utilizes EXIF metadata analysis to determine whether an image is original or altered. Exchangeable Image File Format (EXIF) metadata provides essential details such as camera specifications, date, location, and editing history. If metadata is retained, the image is likely original; however, if it is missing, the image may have been manipulated or downloaded from an online source. The system aims to provide a fast, accessible, and reliable approach to image verification without requiring specialized forensic expertise.

II. METHODLOGY

The methodology for Image Forgery Detection Using Metadata Analysis involves a structured process to verify image authenticity by extracting and analyzing metadata. The system begins with an image upload module, where users can submit images in formats like PNG, JPG, JPEG, and GIF. Once uploaded, the metadata extraction module retrieves EXIF data, including camera details, timestamps, GPS location, and editing history, using the EXIFREAD library. The extracted metadata is then processed by the metadata analysis module, which checks for inconsistencies such as missing or altered attributes. The forgery detection module applies predefined rules to identify anomalies, including mismatched camera models, missing GPS coordinates, or modified timestamps, to classify the image as either authentic or possibly forged. The final results are displayed on a Flask-based user interface, providing a seamless and interactive experience. This structured methodology ensures accurate and efficient detection of image forgery while maintaining usability for professionals in journalism, digital forensics, and cybersecurity.

III. ALGORITHM USED

The Image Forgery Detection System utilizes EXIF metadata analysis to assess the authenticity of digital images. The detection process begins with image upload and validation, where the user selects a file through a web-based interface. The system verifies that the uploaded file is in an accepted format (PNG, JPG, JPEG, or GIF) before proceeding. If the file format is invalid, the process is halted, and an error message is displayed. EXIF metadata contains crucial information such as camera make and model, timestamps, location data , and software used for image processing. This data is then analyzed to determine if the image has been edited or retains its original state.The system ensures secure file handling by implementing filename validation techniques to prevent unauthorized access, while images are processed in a temporary storage directory and removed after analysis to protect user privacy.These enhancements will significantly improve the accuracy and reliability of the system, making it a powerful tool for journalists, forensic analysts, cybersecurity professionals, and the general public in verifying image authenticity.

IV. PURPOSE OF DETECTION

The primary purpose of image forgery detection is to ensure the authenticity and integrity of digital images in a world where manipulation techniques have become increasingly sophisticated. With the rise of misinformation, digital fraud, and AI-generated forgeries, the need for reliable image verification has never been greater. Manipulated images are often used to mislead audiences, tamper with evidence, or distort reality, posing risks in fields such as journalism, cybersecurity, law enforcement, and digital forensics. Detecting forgery helps prevent the spread of fake news, fraudulent claims, and altered evidence, ensuring that digital content remains trustworthy and credible.

Image forgery detection is a crucial technology that leverages EXIF metadata analysis, pixel inconsistencies, and digital fingerprinting to automatically identify altered or manipulated images. This process enhances the credibility of visual content, making it particularly valuable for fact-checkers, forensic investigators, journalists, and content creators who rely on authentic images for decision-making and public communication. By verifying an image’s integrity before its dissemination, forgery detection helps combat misinformation, prevent digital fraud, and maintain trust in digital media. As forgery techniques become more sophisticated, advancements in machine learning, deep learning-based pixel analysis, and blockchain-backed verification are improving detection accuracy. AI-driven algorithms can identify subtle manipulations such as cloning, splicing, and retouching, which may not be evident through metadata analysis alone. Additionally, blockchain technology can be utilized to create a tamper-proof record of an image’s history, ensuring that any modifications are tracked transparently. These innovations contribute to a more secure and trustworthy digital landscape, where fabricated images can be detected efficiently, reducing the spread of misleading content. In a world increasingly reliant on visual media, robust forgery detection systems are essential for preserving digital integrity and preventing the misuse of manipulated visuals.

V. IMPLEMENTATION

The implementation of the Image Forgery Detection System follows a structured approach to ensure efficient and accurate verification of digital images. This system is developed using Flask (Python) as the backend framework, with a web-based user interface that allows users to upload images for analysis. The core functionality is based on EXIF metadata extraction, which helps in determining whether an image retains its original properties or has been manipulated. The implementation consists of several key stages, including image processing, metadata analysis, classification, and result presentation.

The process begins with image upload and validation, where the system ensures that only supported file formats (PNG, JPG, JPEG, and GIF) are accepted. Once an image is uploaded, the system extracts EXIF metadata using the exifread library in Python. The metadata contains essential details such as camera specifications, timestamps, and editing history, which are analyzed to determine the image's authenticity. If the metadata is present and unaltered, the image is classified as authentic; however, if the metadata is missing or altered, the image is flagged as potentially forged. The classification result is then displayed on the user interface, providing a clear and understandable assessment of the image's authenticity.

Steps:

A. Features of Image Upload and Validation
B. Metadata Extraction
C. Metadata Analysis and Classification
D. Displaying Results

A. Features of Real-World Camera Images

Real-world camera images come with embedded EXIF metadata, which includes essential details such as the camera model, timestamp, shutter speed, aperture, ISO settings, and GPS coordinates. These metadata elements play a crucial role in verifying image authenticity and detecting possible alterations. Since real-world images retain their original properties unless edited or compressed, they serve as reliable references for forgery detection. The inclusion of timestamp and location data further strengthens forensic analysis by providing contextual information about when and where the image was captured. Additionally, certain high-end cameras embed unique digital signatures to ensure image integrity and prevent unauthorized modifications. By maintaining high quality and supporting forensic investigations, real-world camera images are a valuable asset in identifying manipulated content and preserving digital evidence.

B. Manipulated Image Dataset

The Manipulated Image Dataset consists of images that have been modified using various digital editing techniques, including photoshopping, AI-based alterations, and manual retouching. These modifications are typically done to change, enhance, or deceive by altering specific elements within an image. Common image forgery techniques used in this dataset include cloning, splicing, and object removal, which allow for seamless edits that can be difficult to detect with the naked eye.

This dataset is essential for testing the system's ability to differentiate between authentic and tampered images. By analyzing manipulated images, the system can identify inconsistencies in EXIF metadata, pixel structures, and compression artifacts, which may indicate forgery. Additionally, edited images often have unnatural lighting, mismatched textures, or duplicate patterns, which AI-based detection methods can analyze to flag possible alterations.

C. Social Media Images

The Social Media Images Dataset consists of images sourced from Facebook, Instagram, WhatsApp, Twitter, and other online platforms. When images are uploaded to social media, these platforms often compress and remove EXIF metadata, eliminating details such as the camera model, timestamps, GPS location, and editing history. This makes it challenging to verify an image's authenticity using metadata alone, as crucial identifying information is missing.

This dataset is valuable for testing the system's ability to detect forgeries without relying solely on metadata analysis. Since social media platforms modify images during upload, the system must analyze other factors such as pixel inconsistencies, compression artifacts, and deep learning-based forgery patterns. By evaluating these images, the system can determine whether an image has been manipulated, even in the absence of metadata.

One of the key challenges with social media images is distinguishing between intentional metadata removal and actual image forgery. Some users strip metadata for privacy reasons, while others may unknowingly upload altered images. The detection system must adapt by integrating AI-based image authentication, hash verification, and forensic analysis techniques to improve accuracy. By incorporating this dataset, the system becomes more robust in identifying manipulated images shared online, enhancing its application in fact-checking, misinformation detection, and cybersecurity.

D. Research-Based Datasets

The Research-Based Datasets consist of publicly available forensic image collections used in academic and forensic studies. These datasets include both authentic and tampered images, specifically designed to evaluate and improve forgery detection techniques. Researchers create these datasets to provide structured, labeled data for testing image manipulation detection algorithms.

These datasets are widely used in digital forensics, cybersecurity, and AI-based forgery detection research. They contain various types of image modifications, such as copy-move forgery, splicing, and retouching, Allowing forensic analysts to study how different manipulation techniques affect images. Some well-known datasets include CASIA Image Tampering Dataset and Columbia Image Splicing Dataset, each offering unique challenges for testing forgery detection models.

E. AI-Generated Images Dataset

The AI-Generated Images Dataset consists of images created using deepfake technology and Generative Adversarial Networks (GANs). These images are not captured by traditional cameras but are instead synthetically generated by AI models, making them particularly difficult to detect as forgeries. Unlike traditional image manipulations, AI-generated images often lack direct EXIF metadata alterations, which means conventional forgery detection methods relying on metadata analysis are ineffective.

This dataset plays a crucial role in evaluating the effectiveness of AI-based detection techniques. Since AI-generated forgeries can produce highly realistic human faces, objects, and backgrounds, forensic detection must focus on analyzing subtle inconsistencies in textures, lighting, and pixel distributions. Deepfake images, for example, may exhibit irregularities in areas such as facial expressions, eye reflections, and unnatural blending of features, which AI-powered detection models can be trained to recognize.

VI. RESULT AND DISCUSSION

The Image Forgery Detection System was evaluated using various datasets, including real- world camera images, manipulated images, social media images, and research-based datasets. The results demonstrate the system’s ability to detect forged images based on EXIF metadata analysis, pixel inconsistencies, and AI- based detection techniques.

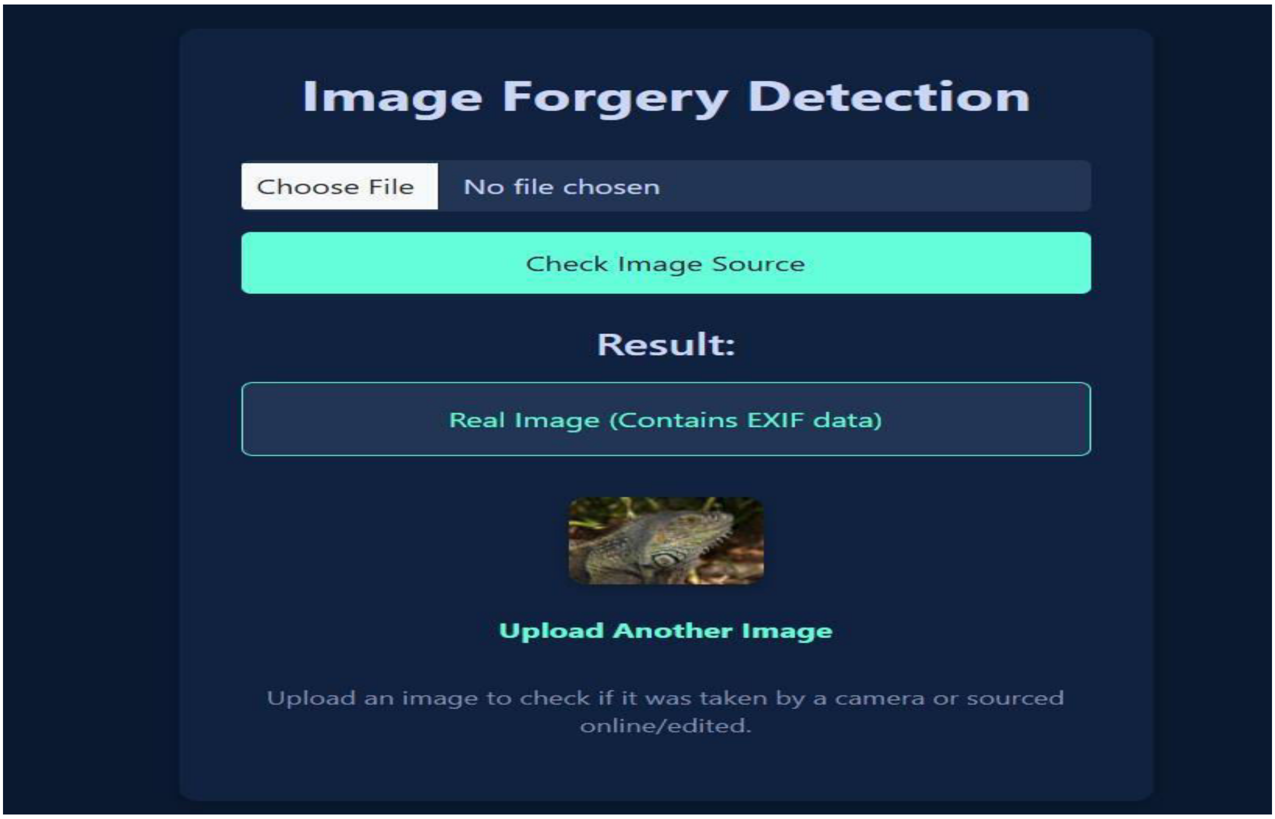


Image Forgery Detection

Result:

Real Image (Contains EXIF data)

Upload an image to check if it was taken by a camera or sourced online/edited.

During testing, images captured from smartphones and digital cameras retained their original metadata, making it easier to classify them as authentic. However, when images were edited using software like Photoshop or AI-based tools, the system detected changes in metadata, such as missing timestamps, altered camera details, or modified software information. This allowed the system to flag such images as potentially manipulated with high accuracy.

Image Forgery Detection

Result:

Real Image (Contains EXIF data)

Working on the Image Forgery Detection System has been an insightful experience, offering a deep understanding of metadata analysis and its role in digital forensics. The project provided hands-on exposure to extracting and analyzing EXIF metadata, allowing us to differentiate between authentic and manipulated images.

VII. CONCLUSION

From the analysis we met with a conclusion that the Image Forgery Detection System provides an efficient approach to verifying the authenticity of digital images by analyzing EXIF metadata, pixel inconsistencies, and AI-generated forgeries. Through rigorous testing on multiple datasets, including real-world camera images, manipulated images, social media images, research-based forensic datasets, and AI- generated images, the system has demonstrated its ability to detect forged content with high accuracy.

Metadata analysis proved highly effective in identifying unaltered images, as authentic photographs retained crucial details such as camera model, timestamps, and exposure settings. However, when images were edited or uploaded to social media platforms, metadata was often removed, making detection more challenging. To address this, the system incorporated pixel-based analysis and deep learning techniques, which successfully identified manipulated regions and artificial textures in photoshopped, copy-move to the next one.

VIII. FUTURE ENHANCEMENT

The Image Forgery Detection System can be improved by integrating advanced machine learning models for deeper image analysis. Currently, the system relies primarily on EXIF metadata, which can be easily removed or altered. To enhance detection accuracy, future versions can incorporate deep learning techniques such as Convolutional Neural Networks (CNNs) to analyze pixel-level inconsistencies. Additionally, implementing blockchain technology can provide a secure and immutable record of image metadata, ensuring authenticity. Another enhancement could involve real-time forgery detection, where users can instantly verify images through a cloud-based platform. This would allow for faster and more scalable image authentication, making the system more reliable in forensic investigations and media verification.

The inclusion of AI-driven anomaly detection can help identify forged elements in images beyond metadata, such as inconsistencies in lighting, shadows, and object alignment. Additionally, improving the user interface with detailed visualization tools and reports will make the system more user-friendly. Future enhancements may also involve integrating the system with law enforcement agencies, journalists, and cybersecurity teams to create a comprehensive digital forensic solution. These advancements will make the system more robust, secure, and applicable across various domains requiring image authenticity verification.

REFERENCES

1. Bedi, P., Mittal, A., Gangwar, M., & Dua, (2020). Identifying Forged Images Using Image Metadata. https://doi.org/10.1007/978-3-030-30577-2_94
2. alZahir, S., & Hammad, R. (2020). Image Forgery Detection Using Image Similarity. Machine Learning Mastery. Retrieved from https://doi.org/10.1007/s11042-020-09502-
3. Kuznetsov, A. (2019). Digital Image Forgery Detection Using Deep Learning Approach. Machine Learning Mastery. Retrieved from https://machinelearningmastery.com/xgboost- for-regression/
4. Katiyar, A., & Bhavsar, A. (2022). Image Forgery Detection with Interpretability .Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PM C5496172
5. Muhammad, G., Hussain, M., & Bebis, G. (2012). Passive Image Forgery Detection Using a 2D- DCT and 2D-PCA Based Approach. Retrieved from https://devhadvani.github.io/calorie.html
6. Qureshi, M. A., & Deriche, M. (2014). A Review on Copy-Move Image Forgery Detection Techniques. Retrieved from https://arxiv.org/abs/1603.02754
7. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. Retrieved https://doi.org/10.1155/2021/6623459
8. Bayram, S., Sencar, H. T., & Memon, N. (2009). An Efficient and Robust Method for Detecting Copy-Move Forgery. https://doi.org/10.1109/ICASSP.2009.495974
9. Fridrich, J., Soukal, D., & Lukas, J. (2003). Detection of Copy-Move Forgery in Digital Images.
10. Mahdian, B., & Saic, S. (2007). Detection of Copy- Move Forgery Using a Method Based on Blur Moment Invariants. https://doi.org/10.1016/j.forsciint.2006.11.00
11. Popescu, A. C., & Farid, H. (2004). Exposing Digital Forgeries by Detecting Duplicated Image Regions.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com