International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

Image Forgery Detection

Dr. Vikram S. Patil[1], Ms. Muskan Sayyad[2], Mr. Sangram Shinde[3], Mr. Salman Pathan[4], Mr. Shreyash Nikam[5]
[1]Principal, Yashoda Technical Campus, Faculty of Engineering, Satara, Maharashtra, India.
[2,3,4,5]UG Computer Science and Engineering, Yashoda Technical Campus, Faculty of Engineering, Satara, Maharashtra, India.
Email ID: *principalengg_ytc@yes.edu.in[1], muskansayyad2003@gmail.com[2], sangramsinhshinde9@gmail.com[3], salmanpathan.exe2003@gmail.com[4], nikamshreyash23@gmail.com[5]*

Abstract
In the digital age, the proliferation of image editing tools has made it easier than ever to manipulate images, raising concerns about the authenticity and credibility of visual content. This project focuses on the development of an effective and efficient image forgery detection system to address the growing challenges associated with digital image tampering. The proposed system leverages advanced techniques in computer vision and machine learning to detect common forms of forgeries, such as copy-move, splicing, and removal. Using feature extraction methods such as SURF, SIFT, and deep learning models, the system identifies inconsistencies in texture, lighting, and metadata. By employing a robust dataset of authentic and forged images for training and testing, the system achieves high accuracy in distinguishing tampered images from genuine ones. This project aims to contribute to areas such as digital forensics, content verification, and social media monitoring, ensuring trustworthiness in digital media. The results demonstrate the system's potential for real-world applications, providing an automated and reliable tool for image integrity verification.

Keywords: *Image Forgery Detection, Computer Vision, Machine Learning, Copy-Move & Splicing, Feature Extraction (SIFT & SURF), Digital Forensics.*

1. Introduction
The rapid advancement of digital imaging technologies and the widespread availability of sophisticated editing tools have made it easier than ever to manipulate images. While these technologies offer significant benefits in creative industries, they also pose serious challenges to the authenticity and trustworthiness of visual content. Image forgery, which involves the deliberate alteration of digital images, has become a widespread issue, affecting fields such as journalism, law enforcement, forensics, and social media. This has created an urgent need for reliable techniques to detect and prevent image tampering. Image forgery detection is the process of identifying whether an image has been altered and, if so, determining the nature and extent of the manipulation. Common types of forgery include copy-move (duplicating regions within the same image), splicing (combining parts of different images), and content removal (erasing or obscuring parts of an image). These manipulations often leave subtle traces, such as inconsistencies in lighting, texture, or compression artifacts, which can be analysed to reveal the forgery. This project aims to develop an automated image forgery detection system that leverages state-of-the-art techniques in computer vision and machine learning. By identifying and analysing telltale signs of tampering, the system seeks to enhance the reliability of digital media and support applications in digital forensics, copyright protection, and misinformation control. Through the exploration of feature- based methods and deep learning models, the project contributes to the growing efforts to combat image forgery and ensure the integrity of digital content. Detection of such manipulations relies on identifying inconsistencies in the digital footprint of an image,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

such as alterations in texture, color gradients, illumination patterns, or compression artifacts. Traditional feature-based methods like SIFT (Scale-Invariant Feature Transform) and SURF (Speeded-Up Robust Features) have been widely used to detect anomalies, but they often struggle with high-resolution, highly manipulated images. On the other hand, deep learning approaches have shown significant promise, enabling the automated extraction of complex patterns and irregularities. By providing a systematic approach to image forgery detection, this project aims to contribute to the growing body of tools used in digital forensics, ensuring that visual content can be trusted in an era of pervasive digital manipulation. Furthermore, the findings of this research hold potential applications in journalism, legal systems, and social media platforms, where the authenticity of images is of paramount importance. The Image Forgery Detection project is a web-based application designed to identify and analyze tampered or digitally manipulated images using advanced machine learning and image processing techniques. In today's digital era, where the authenticity of visual content is often questioned, this system plays a crucial role in detecting forgeries by comparing image patterns, textures, and structural inconsistencies. The project integrates technologies such as Java and Spring Boot for the backend, MySQL for secure data storage, Python-based ML models for analysis, and a responsive React.js frontend for user interaction. By utilizing methods like Structural Similarity Index (SSIM) and Support Vector Machine (SVM) classification, the system accurately flags suspicious regions and presents results visually through heatmaps.

2. Literature Survey

The paper provides a comprehensive review of deep learning techniques for image forgery detection. It contrasts traditional methods that rely on handcrafted features with newer deep learning approaches, which can automatically extract complex patterns from images. The paper also surveys publicly available datasets for training and testing deep learning models, comparing their effectiveness in detecting manipulated images. It highlights the improved accuracy of deep learning methods over traditional ones and presents insights into the application of these techniques in real-world scenarios. [1] The paper discusses a method for detecting copy-move image forgeries, where a part of an image is duplicated and placed elsewhere in the same image. This type of forgery is difficult to detect because the copied parts share similar attributes with the original image. The proposed solution uses Convolutional Neural Networks (CNNs) to extract features from image blocks and classify images as either original or forged. The model achieves an accuracy of 97.7% using the CASIA2 dataset, which contains both authentic and forged images. The approach effectively addresses challenges like image compression and resizing, which can mask alterations. The method offers real-time processing, making it suitable for applications in social media, legal, and academic contexts, where image forgery detection is critical. [2] The paper proposes a novel image forgery detection system using Convolutional Neural Networks (CNNs) to identify various types of image manipulations, including copy-move, splicing, and retouching. The system integrates Error Level Analysis (ELA) with deep learning to enhance detection accuracy. Tested on real-world images, it achieved a 93% detection accuracy, outperforming existing methods. This CNN-based system offers a robust solution for detecting image forgery in applications like forensics, security, and digital media analysis, addressing the growing concern of manipulated images in today's digital landscape.[3] The paper Image Forgery Detection using Deep Learning Model addresses the challenge of detecting image tampering, which can compromise the integrity of visual evidence, particularly in legal and forensic settings. The study proposes a deep learning solution using the VGG-19 architecture to identify forged images. The authors utilize a dataset from CASIA, containing both authentic and manipulated images. Preprocessing steps, including image resizing and denoising, are applied to prepare the dataset for training. The model is evaluated based on accuracy and loss, achieving more than 95% accuracy and a minimal loss value, which makes it highly efficient compared to other existing models. The

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

authors suggest that, in the future, the model could be deployed as a tool on a website, allowing the general public to easily detect image forgeries. [4] The paper Image Forgery Detection Using Machine Learning explores the increasing concern over the authenticity of digital images due to advancements in imaging technology and the widespread use of photo- editing software. With the rise of social media and the ease of altering images, the integrity of digital images has been compromised, creating a need for effective detection methods. The study employs a machine learning algorithm, specifically Support Vector Machine (SVM), to identify whether an image has been manipulated. The model also includes a feature to block users who attempt to upload altered images. This approach helps maintain the credibility of digital images, especially in fields that rely on them for decision-making, such as medicine and warfare. [5] Image is a powerful way to share information in the digital world. The sources of images are everywhere, magazines, newspapers, healthcare, entertainment, education, social media and electronic media. With the advancement of image editing software and cheap camera-enabled mobile devices, image manipulation is very easy without any prior knowledge or expertise. So, image authenticity has questioned. Some people use the forged image for fun, but some people may have bad intentions. The manipulated image may use by political parties to spread their false propaganda. Fake images use by people to spread rumours and stoking someone. In addition to harming individuals, fake images can damage the credibility of media outlets and undermine the public trust in them. The need for reliable and efficient image forgery detection methods to combat misinformation, propaganda, hoaxes, and other malicious uses of manipulated images. These are some known issues on digital images. The researcher, scientist, and image forensic experts are working on the development of fake image detection and identification tools. Presently digital image forgery detection is a trending field of research. The main aim of this paper is to provide the exhaustive review on digital image forgery detection tools and techniques. It also discusses various machine learning techniques, such as supervised, unsupervised, and deep learning approaches, that can be employed for image forgery detection it demonstrates the challenges of the current state of the work. [6] With the advent of powerful image editing tools, manipulating images and changing their content is becoming a trivial task. Now, you can add, change or delete significant infor mation from an image, without leaving any visible signs of such tampering. With more than several millions pictures uploaded daily to the net, the move towards paperless workplaces, and the introduction of eGovernment services everywhere, it is becoming important to develop robust detection methods to identify image tampering operations and validate the credibility of digital images. This led to major research efforts in image forensics for security applications with focus on image forgery detection and authenti cation. The study of such detection techniques is the main focus of this paper. In particular, we provide a comprehensive survey of different forgery detection techniques, com plementing the limitations of existing reviews in the literature. The survey covers image copy-move forgery, splicing, forgery due to resampling, and the newly introduced class of algorithms, namely image retouching. We particularly discuss in detail the class of pixel based techniques which are the most commonly used approaches, as these do not require any a priori information about the type of tampering. The paper can be seen as a major attempt to provide an up-to-date overview of the research work carried in this all important field of multimedia. [7] These days digital image forgery has turned out to be unsophisticated because of capable PCs, propelled image editing softwares and high resolution capturing gadgets. Checking the respectability of pictures and identifying hints of altering without requiring additional pre-embedded information of the picture or pre-installed watermarks are essential examine field. An endeavor is prepared to review the current improvements in the research area of advanced picture fraud detection and comprehensive reference index has been exhibited on passive methods for forgery identification. Passive techniques donot require preembedded information in the image. Several image forgery detection techniques are

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

arranged first and after that their summed up organization is produced. Author will review the various image forgery detection techniques along with their results and also compare the various different techniques based on their accuracy. [8] The digital image proves critical evidence in the fields like forensic investigation, criminal investigation, intelligence systems, medical imaging, insurance claims, and journalism to name a few. Images are an authentic source of information on the internet and social media. But, using easily available software or editing tools such as Photoshop, Corel Paint Shop, PhotoScape, PhotoPlus, GIMP, Pixelmator, etc. images can be altered or utilized maliciously for personal benefits. Various active, passive and other new deep learning technology like GAN approaches have made photo-realistic images difficult to distinguish from real images. Digital image tamper detection now focuses on determining the authenticity and consistency of digital photos. The major research problems use generic solutions and strategies, such as standardized data sets, benchmarks, evaluation criteria and generalized approaches. This paper overviews the evaluation of various image tamper detection methods. A brief discussion of image datasets and a comparative study of image criminological (forensic) methods are included in this paper. Furthermore, recently developed deep learning techniques along with their limitations have also been addressed. This study aims to comprehensively analyze image forgery detection methods using conventional and advanced deep learning approaches. [9]

3. Block Diagram

The block diagram (Figure 1) illustrates the end-to-end workflow of the Image Forgery Detection system, showcasing the interaction between the user interface, image processing modules, machine learning components, and the result visualization. Each component in this flow plays a crucial role in identifying and reporting image tampering.

3.1.User Interaction

The process begins with the user accessing the application through a web interface. The user uploads an image they suspect may have been altered or forged. Once the image is uploaded, the system initiates the detection pipeline.

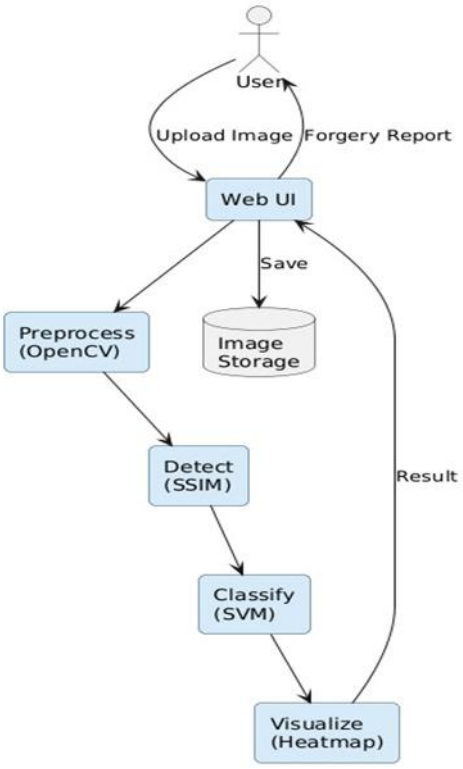

Figure 1 Block Diagram

3.2.Web UI

The Web User Interface (UI) serves as the front-facing layer of the application. It allows users to submit images and view results. The interface is built using HTML, CSS, JavaScript, and React for a seamless and interactive experience. Upon upload, the image is sent to the backend and simultaneously saved to a secure image storage database for further processing.

3.3.Image Storage

This component is responsible for persistently storing the uploaded images. It ensures that the image data is retained throughout the detection process. It also acts as a repository for analysis logs and results, allowing retrieval for future reference or audits.

3.4.Preprocessing (Open CV)

Before running any detection algorithms, the image undergoes preprocessing using Open CV. This step involves standardizing the image format, resizing, converting to grayscale if necessary, and enhancing features such as edges and textures. These operations prepare the image for more accurate analysis in the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

following stages.

3.5.Detection (SSIM)

The detection phase employs Structural Similarity Index (SSIM) to identify inconsistencies within the image. SSIM compares different regions of the image to spot anomalies in structure, brightness, and texture that may suggest tampering. This method is effective for detecting localized changes introduced during forgery.

3.6.Classification (SVM)

Once potential tampered areas are identified, they are passed to a machine learning classifier. In this system, a Support Vector Machine (SVM) is used to categorize the input as either 'authentic' or 'forged'. The SVM model has been trained on labeled image datasets to distinguish between genuine and manipulated image patterns with high accuracy.

3.7.Visualization (Heatmap)

The final output is visualized as a heatmap, which overlays color-coded regions on the original image. This highlights the areas most likely to be tampered. Red or warm-colored zones indicate high suspicion of forgery, providing users with an intuitive view of the results. The heatmap is displayed on the Web UI, completing the user feedback loop.

3.8.Forgery Report Generation

After visualization, a detailed report can be generated containing the classification result, SSIM scores, and annotated heatmaps. This report can be downloaded or shared for documentation or forensic use.

4. Proposed System

4.1.Preprocessing

In this initial phase, the input image is prepared for analysis. Preprocessing includes converting the image to a standard format, resizing to a fixed resolution, and enhancing features such as contrast and brightness to improve detection accuracy. This step ensures consistency across the dataset and removes potential noise that could interfere with further analysis.

4.2.Feature Extraction

The system utilizes advanced feature extraction techniques to identify unique patterns and irregularities in the image. Approaches like Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF) are employed to extract local features, which are crucial for identifying manipulated regions. For more complex forgery types, deep learning models are applied to learn intricate features that are not easily captured by traditional methods.

4.3.Forgery Detection

Once features are extracted, the system performs analysis to detect tampered regions.

- **Copy-Move Detection:** The system uses block- based or keypoint-based matching to identify duplicated regions within the same image. Techniques such as PatchMatch or exhaustive search are applied to detect overlapping blocks or identical feature points.
- **Splicing Detection:** Splicing often introduces inconsistencies in lighting and texture. The system examines discrepancies in color gradients, edge continuity, and chromatic aberrations to identify such manipulations.
- **Metadata Analysis:** The system may also analyze image metadata (e.g., EXIF data) to detect inconsistencies indicative of forgery.

4.4.Classification

The extracted features are fed into a classification model, such as a Convolutional Neural Network (CNN) or Support Vector Machine (SVM). The model is trained on a labeled dataset containing authentic and forged images, allowing it to distinguish between genuine and tampered regions. Transfer learning with pre-trained networks, such as VGG or ResNet, is used to improve detection accuracy for complex datasets.

4.5.Post-Processing and Visualization

To improve interpretability, the system highlights tampered regions on the image, providing a visual representation of the detected forgery. The system also outputs a confidence score indicating the likelihood of manipulation. This feedback can be used for further investigation or validation by forensic experts.

4.6.Evaluation and Optimization

The system undergoes rigorous testing on a diverse dataset of manipulated and genuine images. Metrics such as precision, recall, F1-score, and processing time are used to evaluate performance. Based on these metrics, the system is iteratively optimized to

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

enhance its robustness and generalizability to various types of forgeries and datasets.

5. Working

The image forgery detection system operates through a series of structured steps, each designed to identify and analyze tampered regions in digital images. The following outlines the workflow of the system.

5.1.Image Input and Preprocessing

- **Input Handling:** The system accepts a digital image as input in common formats such as JPEG, PNG, or BMP.
- **Preprocessing:** The image is standardized to ensure uniformity in size and format. This may involve resizing, grayscale conversion, and noise reduction to enhance clarity. Adjustments like contrast enhancement or histogram equalization may also be applied to improve feature visibility.

5.2.Feature Extraction

In this step, distinctive features of the image are extracted for analysis.

- **Traditional Methods:** Algorithms like SIFT (Scale-Invariant Feature Transform) and SURF (Speeded-Up Robust Features) detect keypoints and descriptors, which are critical for identifying duplicated or altered regions.
- **Deep Learning-Based Extraction:** For more complex forgery patterns, convolutional neural networks (CNNs) are used to automatically learn spatial and texture-based features that traditional methods might miss.

5.3.Model Design

Choose a model depending on your forgery type and approach.

Traditional Machine Learning:

- Extract features manually (using techniques like SIFT, LBP, etc.).
- Support Vector Machines (SVM)
- Decision Trees or Random Forest
- Logistic Regression or k-NN

5.4.Deep Learning-Based Feature Extraction Pretrained CNNs:

- Use models like VGG16, ResNet, or EfficientNet for feature extraction.
- Transfer learning enables leveraging large-scale training from other datasets.

5.5.Advanced Technique and Emerging Approaches

- Deepfake Detection
- Multi-Modal Detection
- Steganalysis for Hidden Information
- Forensic Watermarking
- Multi-Scale Approaches
- Hash-Based Verification
- Blind Forgery Detection

6. Output

Figure 2 Image Forgery Detection

The displayed image demonstrates the output screen of the “Image Forgery Detection” system after a successful comparison between two images (Figure 2 & 3). At the top, there is a user-friendly interface section labeled "Compare Two Images", which allows the user to upload two separate image files for analysis. In this example, the same file, bdaorg.jpg, appears to have been selected in both fields, indicating either a test for self-comparison or a verification step. Once the user clicks the "Compare Images" button, the backend system initiates the analysis process. A status message reading “Comparison completed!” confirms that the image processing and analysis steps have finished successfully. Below this, the result section is prominently displayed. Here, a "Highlighted Image" is shown, featuring red rectangular boxes over specific areas. These red boxes indicate regions that the system has flagged as suspicious or potentially tampered. The detection logic likely uses similarity measurement techniques (such as SSIM) or pixel-level analysis to identify differences or inconsistencies in the images. Notably, some text has been visibly altered or obscured, and the system has

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

accurately marked these areas for user review. The bounding boxes serve as a visual guide to help the user focus on questionable regions within the image. This interface effectively combines usability with technical precision, allowing users to not only compare visual content but also to quickly understand where changes might have occurred. Such a setup is particularly valuable in scenarios like document authentication, academic integrity checks, or digital forensics.

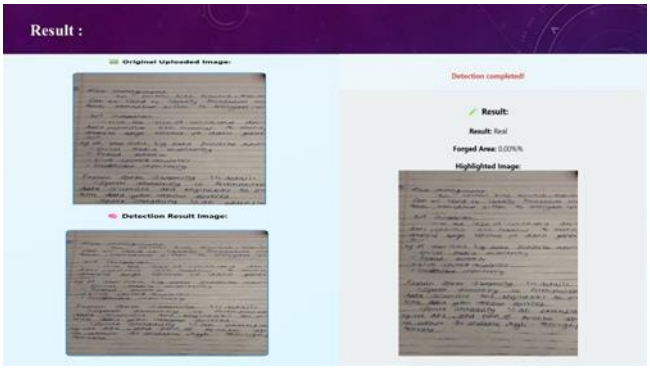

Figure 3 Compare Two Images

The displayed image represents the output interface of the Image Forgery Detection system, showcasing a completed analysis of an uploaded handwritten document. The interface includes three key sections: the original uploaded image, the detection result image, and the final detection summary. The system compares the input image against its internal forgery detection algorithms using techniques like OpenCV preprocessing and SSIM analysis. In this instance, the result indicates the image is "Real" with 0.00% forged area, meaning no signs of tampering were found. The highlighted image confirms this outcome, as it shows no red-marked or suspicious regions. This result panel provides users with a clear and trustworthy verification of image authenticity, combining visual evidence and statistical accuracy in a user-friendly layout.

Conclusion

The Image Forgery Detection System emerges as an essential tool in combating the rising challenge of digital image manipulation in today's media-driven world. By integrating advanced machine learning algorithms with forensic analysis techniques, the system provides a reliable, efficient, and user-friendly solution for detecting tampered content. Its versatility has proven invaluable across industries such as media, law enforcement, and research, ensuring the integrity and credibility of visual data. As the system evolves, with enhancements in accuracy, performance, and ease of use, it holds immense potential for future applications like video forgery detection and real- time monitoring, solidifying its role as a cornerstone in digital content verification.

Future Scope

1. Hybrid Models for Enhanced Robustness

One promising future direction is the development of hybrid detection models that combine traditional image processing techniques with advanced AI methods. Traditional approaches, such as analyzing noise patterns or frequency domains, excel at detecting physical inconsistencies, while AI-driven methods, especially deep learning, can adapt to complex and diverse forgery types. By integrating these techniques, hybrid models can overcome limitations of standalone methods, creating systems that are both accurate and versatile. For instance, preprocessing an image with wavelet transforms can enhance subtle tampering artifacts, which deep neural networks can then analyze for forgery detection.

2. Real-Time Detection for Practical Applications

As forgery detection becomes a critical need for social media platforms, surveillance systems, and journalism, the ability to detect tampering in real-time is essential. However, the computational demands of many current algorithms make this challenging. The future lies in developing lightweight, efficient algorithms capable of operating on edge devices like smartphones and cameras. Such systems would allow instant forgery detection during image uploads or live surveillance, ensuring content authenticity without delays. This real-time capability could also be a game-changer in live broadcasting, preventing the dissemination of tampered visuals.

3. Integration with Augmented Reality (AR) and Virtual Reality (VR)

As AR and VR technologies become mainstream, detecting manipulations in immersive environments will be crucial. Future forgery detection systems

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0383
e ISSN: 2584-2854
Volume: 03
Issue:07 July 2025
Page No: 2425 - 2432

could analyze 3D content for anomalies, such as inconsistent textures, lighting, or geometry. Integrating forgery detection with AR/VR tools could enable users to overlay detection results on immersive content, helping identify tampered elements in real-time within virtual spaces.

4. Explainable AI for Forensics

One limitation of many current AI-based detection systems is their black-box nature, which can undermine trust and reliability in critical scenarios like legal investigations. A future focus on explainable AI (XAI) can address this by making detection models interpretable. Systems that not only identify forgery but also provide visual and textual explanations for their findings—such as highlighting tampered regions or inconsistent metadata—will be more transparent and credible. This feature would enhance their applicability in courtrooms and other formal settings.

5. Proactive Detection with Embedded AI in Cameras

Embedding forgery detection algorithms directly into camera hardware is a proactive future direction. Such systems could analyze an image at the moment of capture, detecting any unauthorized alterations or inconsistencies. For example, AI-enabled cameras could flag potential tampering when saving an image or video.

Reference

[1]. Image Forgery Detection using Deep Learning: A Survey, April 2020 Authors: - Zankhana J. Barad, Mukesh M. Goswami
[2]. Image Forgery Detection, June 2023.Authors: Dipanshu Narayan, Himanshu, Rishabh Kamal.
[3]. Image Forgery Detection using CNN, August 2023. Authors: Meet Patel, Kartikay Rane, Niyati Jain, Praneel Mhatre, Shree Jaswal .
[4]. Image Forgery detection using Deep Learning Model, November 2022. Authors: Praveen Gupta, Chour Singh Rajpoot, T.S.Shanthi, Dvsssv Prasad, AshokKumar, S Sandeep Kumar.
[5]. Image Forgery detection using Deep Learning Model, December 2022.
[6]. Image forgery detection: comprehensive review of digital forensics approaches, April 2024. Authors: Satyendra Singh & Rajesh Kumar.
[7]. A bibliography of pixel-based blind image forgery detection techniques. August 2015, Muhammad Ali Qureshin, Mohamed Deriche
[8]. A review paper on digital image forgery detection techniques July 2017. Authors: Navpreet Gill, Amit Deogar.
[9]. Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation, October 2022. Authors: Preeti Sharma, Manoj Kumar, Hitesh Sharma.