DIGITAL FORGERY IN THE AGE OF MISINFORMATION USING TECHNIQUES FOR RELIABLE IMAGE MANIPULATION DETECTION AND ASSESSING THEIR SOCIETAL IMPACT

Ayushi Tiwari [1], Kapil Shukla [2], Dr. Krishna Modi [2]

[1] Student at School of Forensic Science, National Forensic Sciences University, Gandhinagar, Gujarat, India
[2] Assistant Professor at School of Forensic Science, National Forensic Sciences University, Gandhinagar, Gujarat, India

Received 28 September 2025
Accepted 29 October 2025
Published 02 December 2025

Corresponding Author

Kapil Shukla, kapil.shukla@nfsu.ac.in

DOI
10.29121/DigiSecForensics.v2.i2.2025.68

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Digital image forgery has become a serious concern in today's information-driven society, as images rapidly circulate across social media, news platforms, and digital communication. As the creation of manipulated images becomes easier and their detection more difficult, the demand for reliable forgery detection techniques has become more urgent than ever. This review covers a wide range of methods that can be used to identify tampered images, with particular attention to metadata verification, hashing-based approaches, and learning-driven strategies. Metadata inspection remains among the simplest and earliest techniques, but it is usually vulnerable because metadata can be easily removed or altered. Hashing-based methods have much stronger robustness by generating unique digital signatures for images. However, they usually fail when minor edits are performed. Machine learning and deep learning techniques have significantly advanced the area, which primarily enables learning complex manipulative patterns automatically. These include convolutional neural networks, attention mechanisms, and hybrid models combining traditional features and deep features for superior detection accuracy. Some of the main focuses of current research are on hybrid architectures aimed at combining strengths for better performance against real-world forgeries, including sophisticated deepfakes. Besides technical advancements, this review highlights the societal importance of image integrity. Reliable forgery detection is important in journalism, forensic analysis, medical imaging, and national security-all those domains where misinformation or tampering could have dire consequences. While tremendous progress has been made, some challenges still remain, particularly with respect to how easily metadata can be tampered with or the realism of AI-generated content. Finally, the paper concludes by identifying future research avenues that have the potential to make forensic systems resilient and help rebuild trust in digital media.

Keywords: Image Forgery Detection, Metadata, Hashing, Machine Learning, Deep Learning

1. INTRODUCTION

Digital technologies have advanced rapidly, making images an integral element of communication, news reporting, healthcare, research, and law enforcement. Nevertheless, these perceive instruments have raised the possibility of easy manipulation of images. Nayyef and Al-Khanjari. (2015) Through techniques such as copy-move, splicing, retouching, and resampling, a Figure 1, unworthy visuals can be generated. Such forgery could lead to the dissemination of misleading

How to cite this article (APA): Tiwari, A., Shukla, K., and Modi, K. (2025). Digital Forgery in the Age of Misinformation Using Techniques for Reliable Image Manipulation Detection and Assessing Their Societal Impact. *Journal of Digital Security and Forensics, 2*(2), 76–87. doi: 10.29121/DigiSecForensics.v2.i2.2025.68

information, tarnishing of reputations, or distortion of real evidence. Tom et al. (2019). The field called digital image forensics has emerged to address this situation by detecting and analyzing image modifications. Some methods that have proven to be effective include checking the metadata files and performing a hash comparison, which are quick and resource-efficient. These methods are to be seen as preliminary steps toward authenticity and integrity assessment of an image. Shruthi et al. (2025).

1.1. MOTIVATION

Detection of forged images is the key to the establishment of credibility in our digital world. False photography can mislead, cause confusion, and potentially damage valuable segments such as scientific research or medical evidence. Manipulations are slight, with detection with the naked eye being untrustworthy; therefore, automation that produces clear and consistent findings is justified. Quick schemes such as verification of the metadata and of the hash value still hold a role in the preliminary check, accompanied by the use of sophisticated schemes such as the use of deep learning, to be a quick and precise method of verification. Kaur and Kanwal (2019), Marra et al. (2020).

1.2. OBJECTIVE OF THE RESEARCH

This research is guided to address current weaknesses in the detection of forgery images conducted with the intent to upgrade the tools of verifying digital photographs. The research presents the notable approaches utilized in image forgery detection, such as metadata analysis and hash functions, followed by stepwise development chronologies in classical schemes, machine learning schemes, and deep models. To that end, it makes comparisons among all the schemes with respect to different attacks, computational complexity, as well as effectiveness with the intent of real-world applications, with the outcome of mixed comparisons of the respective trade-offs required. The research concludes significant voids that, as it is, hamper all applicable uses and presents directions towards future works. The research suggests the development of hybrid systems through the integration of different schemes and future developments to enhance the scalability and reliability of forgery detection. Nagm et al. (2024), Tyagi and Yadav (2023).

1.3. SCOPE OF THE STUDY

The paper accounts for methods that can be used for the detection of forged images, as the methods make no use of watermarks or digital signatures. Figure 1, The paper accounts for the use of methods such as metadata analysis, hashing methods, as well as copy-move change or splicing detection. Table 1, It discusses machine learning and deep learning in their use to classify and localize such images. It compares programming environments such as Python, MATLAB, and C++. It sidesteps the problem of proactive watermarking, as it would be inoperable for already in-circulation images.

2. BACKGROUND AND BASICS

Prior to diving into the higher-order detection algorithms, one must be familiar with the basics of forgery in an image. This includes the knowledge of manipulations that happen as well as the most prominent forensic features pertinent to the right modes of detection. Some of the forgery that happens in the image will be evident in the section with some of the frequent use of the editing program. Being conversant with these crucial basics, such as the metadata, hashing as well as the processing of the signals, one can then picture that these form the very basis of forgery identification.

Figure 1

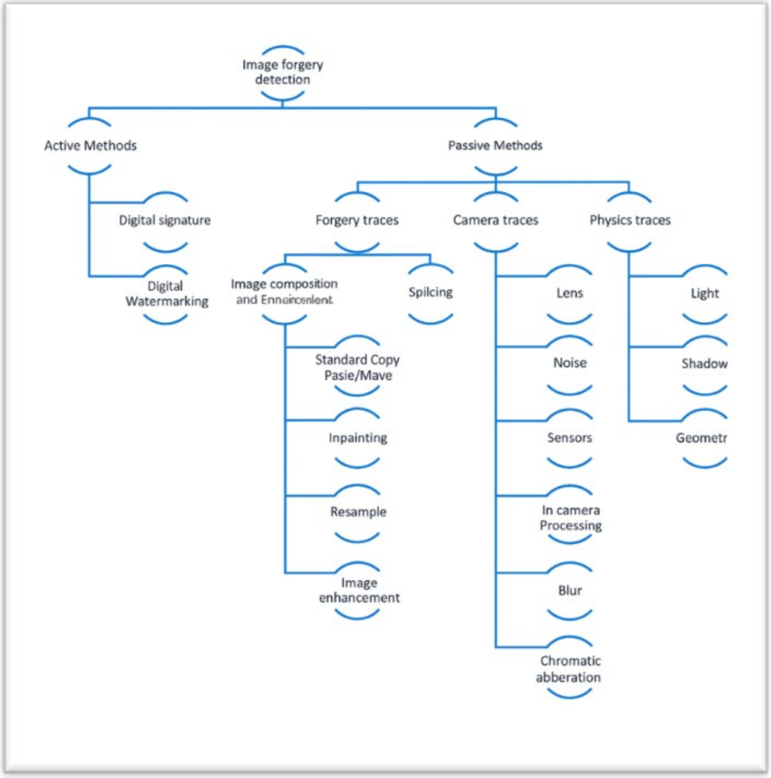

Figure 1 Overview of Image Forgery Detection

Table 1

Table 1 Types of Image Forgeries and Detection Hint.

Forgery Type	Description	Example	Detection hint
Copy-Move	Copying & pasting a region within the same image, often with rotation, scaling, or blurring	Duplicating soldiers in a battlefield photo	Key point analysis (SIFT, SURF), block matching
Image Splicing	Combining regions from multiple images	Placing a someone's head on another body	Noise, texture, and colour inconsistencies
Retouching/Enhancement	Subtle edits such as smoothing wrinkles, altering skin tone, or object removal	Beautifying faces in media	Lighting, texture, and boundary irregularities
Resampling/Scaling	Geometric transformations including rotation, resizing, interpolation	Resized objects to fit into an altered scene	Periodic artifacts in frequency/transform domain
Metadata Manipulation	Altering EXIF tags such as timestamps, GPS data, or camera details	Changing date on surveillance footage for false alibi	Inconsistencies in metadata vs. visual evidence
Deepfakes/AI Forgeries	Synthetic images/videos generated by GANs or deep learning	AI-generated fake celebrity videos	Deep learning-based detectors; physiological cues

Figure 2

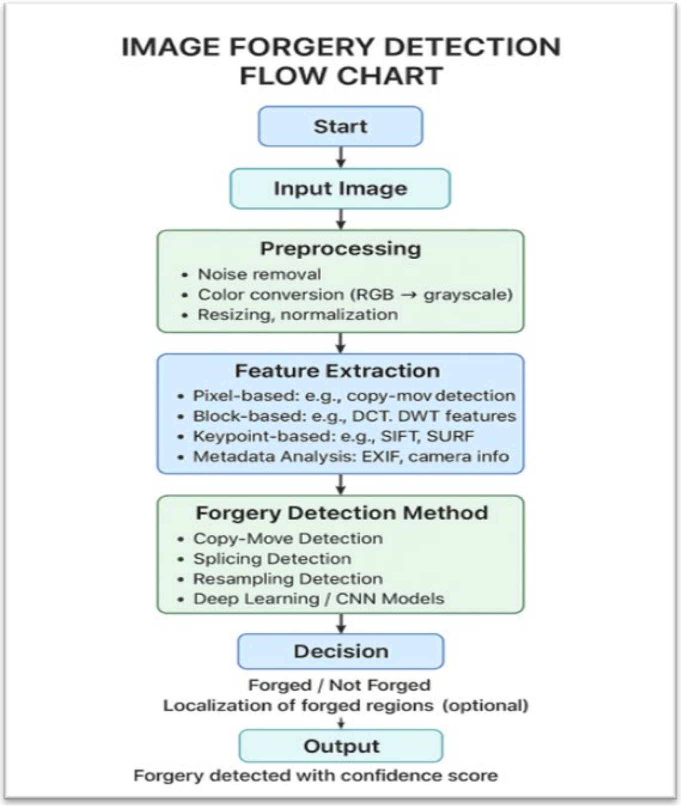
IMAGE FORGERY DETECTION FLOW CHART
Start
Input Image
Preprocessing
• Noise removal
• Color conversion (RGB → grayscale)
• Resizing, normalization
Feature Extraction
• Pixel-based: e.g., copy-mov detection
• Block-based: e.g., DCT. DWT features
• Keypoint-based: e.g., SIFT, SURF
• Metadata Analysis: EXIF, camera info
Forgery Detection Method
• Copy-Move Detection
• Splicing Detection
• Resampling Detection
• Deep Learning / CNN Models
Decision
Forged / Not Forged
Localization of forged regions (optional)
Output
Forgery detected with confidence score

Figure 2 Flow Chart of Image Forgery Detection

3. LITERATURE REVIEW

3.1. ANCIENT STRATEGIES AND CLASSICAL TACTICS

The first image forgery detection schemes were manual feature extraction schemes based on transforms and descriptors. Compared different schemes based on PCA, Scale Invariant Feature Transform (SIFT), Mistry and Banerjee (2025). Local Binary Patterns (LBP), and different schemes based on Discrete Cosine Transform (DCT) to detect forgery. Mali and Chavan (2025), Sadeghi et al. (2018). The classifiers that are based on the identification of forgery type, copy-move or splicing, will be the SVMs. Although these schemes had proved trustworthy with such forgery types, they had failed with noisy images as well as with manipulations of complex nature that prevented their generalizability to a wider extent.

3.2. HYBRID AS WELL AS KEY POINT-BASED TECHNIQUES

Hybrid methods have been developed that pair classical key point detection with machine learning with the aim of building a superior forgery detection. Diwan and Roy (2024), introduced a two-step hybrid framework that combines CenSurE key point detection with features extracted with the help of Convolutional Neural Networks (CNN) in a fusion classifier. The framework was evaluated over some datasets, namely CMFD, CoMoFoD, and CASIA-II Table 2, Dell'Olmo et al. (2025), Sedeeq (2025). with very impressive results in precision, recall, accuracy, and F1 scores. Additionally, it is resistant to geometric transform and to most of the post-processing strategies that are typically used to conceal the forgery. The cost and complexity were, however, the issues identified. Kumar et al. (2016).

3.3. DEEP-LEARNING-BASED ARCHITECT

Recent developments in deep learning have greatly revolutionized forgery detection because of the fully end-to-end trainable models. introduced a full-resolution, full-image CNN model that relies on the use of Xception networks as well as noise prints, Gardella et al. (2024) to express features, thus allowing localized forgery operation detection such as splicing, copy-move, Figure 1, as well as inpainting. Siopi et al. (2022). The model was trained on synthetic images (Vision, UCID, Dresden) and real images (DSO-1, Korus, NC2017) with high AUC values, therefore outperforming previous modelling but with the need to use vast computational power. Nande et al. (2021) incorporated conventional texture analysis with CNN classification. The procedure comprised preprocessing (histogram equalization and denoising) and segmentation (using the k-means clustering). Their method, tried on a set of 120 pairs of images (originals and transformed), Makandar and Javeriya (2024), yielded 96.4% accuracy-better accuracy compared to baseline SVM classifiers-but showed the power of deep learning, even with a relatively small set. Marra et al. (2020), One cannot possibly overstate the importance of large datasets for training and validating forgery detection models. In this regard, the Digital Forensics 2023 (DF2023) dataset stands out by presenting 1 million manipulated images from different, including splicing, copy-move, enhancement, and removal categories being ultimately sourced from Durusoy (2025) MS-COCO images. The sheer size along with the diverse contents allow for an objective benchmarking for the comparison of networks. Some notable alternate datasets are tampCoco, focusing on splicing and copy-move with nearly 800,000 images, and Defacto with around 190,000 images. These datasets contributed tremendously toward improving the model's generalization and robustness. Singh et al. (2024) PhotoHolmes, Noise Sniffer, Gardella et al. (2021). a MATLAB toolbox, and several Python libraries have eased experimentation since 2020 acts as a very powerful turn toward Python since it integrates nicely into machine learning and deep learning applications. C++ and, MATLAB maybe still be heard offered for quick prototyping or fine-tuning cycles, but Python is the obvious go-to.

3.4. METRICS

Trends were concerned, the majority of studies assessed models mostly in terms of accuracy, precision, recall, F1-score, and AUC. Bammey et al. (2022). Deep learning models usually manage well over 90% accuracy with respect to benchmark datasets, while detecting less manipulated or heavily processed areas is still rather difficult. Recent attempts involve novel strategies including dynamic histogram equalization, local descriptor transformations, and multisource feature fusion, all developed to improve small-forgery detection. These improvements may also accelerate detection and boost accuracy due to the incorporation of transfer learning utilizing previously trained models Hao et al. (2021) like VGG16 and Xception. Survey articles, on the other hand, show that the future direction of image forgery detection continues to centre on optimization of the deep learning architectures, combined data pools (such as metadata and image pixels), and computational cost with resistance to adversarial attacks. Nagm et al. (2024), Kaur and Kanwal (2019), Siopi et al. (2022), Akram et al. (2025). This research work aims at detecting forgery in images with particular concentration on deepfake face manipulation and splicing through hybrid means of deep learning models. Initially, we would create a balanced dataset comprised of real images and artificially produced images with a wide spectrum of forgery, using various types of deepfake generators as well as splicing. If possible, acquisition of the ground truth masks would indicate the specific areas where manipulations were conducted. Figure 2, Preprocessing includes face detection for deepfake cases along with resizing of images to a common size, colour normalization, and potentially conversion to other colour spaces such as RGB and YCbCr. Here we also propose a data augmentation such as compression, adding noise, rotation and scaling mechanisms for realistic image distortions while enhancing robustness of our models. The backbone model architecture comprises a CNN backbone model, Shruthi et al. (2025) easily one among Xception, Inception-ResNet or one among its peers, to derive high-level features but also features from the frequency domain or residual filters in another branch, -focused on artifact features. For localization purposes, we will link a segmentation head in an encoder-decoder or U-Net style to infer pixel-level masks. The loss function will comprise both image-level classification loss, which will be binary cross-entropy, plus localization loss like IoU or Dice loss if masks are added. For training, the dataset will be segregated into train, validation, and test data. This way, some types remain unseen fraud or data and will assess the generalization part. The final aspect of our model qualification will be an evaluation based on accuracy, precision, recall, and F1-score measures as per classification, whereas IoU and pixel-level accuracy measures are applicable as per localization. Additionally, we will also evaluate performance based on varied kinds of mild distortions such as compression and resizing, along with some computational measures such as model size as well as inference time. Figure 2, Lai et al. (2025), Diwan and Roy (2024).

Table 2

Table 2 Key Image Forgery Datasets: Merits and Demerits.

Dataset(s)	Merits	Demerits
CASIA 2.0	Large scale, diverse manipulations (splicing, copy-move), ground truth masks, standard academic benchmark	Limited postprocessing diversity, lacks modern synthetic techniques (deepfakes, GANs)
CoMoFoD v2	Pixel-level tampering masks, realistic post-processing, focuses on copy-move forgeries	Smaller scale than CASIA, limited to copy-move, less category diversity
MICC-F2000	Real-world handcrafted forgeries, high-resolution images, challenging splicing and copy-move scenarios	No pixel-level mask annotations, missing recent manipulation types
MFFI (2025)	Extremely large (1M+ images), advanced facial forgery, contemporary attack simulation, multi-level annotation	Specialized for facial forgery, less suitable for general scene tampering
Columbia Color DVMM	Established for splicing detection, color-based analysis	Small scale, outdated manipulation types, lacks annotation detail
So-Fake-Set (2025)	2M+ images, broad category scope, photorealistic generative sources, OOD benchmarks for cross-domain evaluation	Primarily focused on social media content, not all traditional forgery types covered
Real and Fake Images (Kaggle)	Authentic and forged samples, useful for simple benchmarking	Very limited scale and manipulation types, minimal annotation

4. WORKFLOW OF IMAGE FORGERY DETECTION

The strategy developed for detection of forgery images starts with data set-corpus collection of originals and fakes from repositories, e.g., CASIA, Hao et al. (2021), Dell'olmo et al. (2025), Nfor et al. (2024). Columbia, and CoMoFoD, by taking them and preparing them. Preprocessing would then be just arranging the image consistency through resizing, normalization, noise removal, and adjusting compression levels. For instance, if a forgery is to be detected, then it would be either copy-move, splicing, retouching, or GAN-produced deepfakes. Singh et al. (2024) All the above manipulations would determine detection methods. Feature extraction would then ensue to justify intelligibility with image qualities. There were conventional procedures in the case of manually curated features like frequency components of DCT or DWT, Mali and Chavan (2025) texture patterns, noise signatures such as PRNU and CFA, and primary statistics, but currently this is moving towards deep learning using embedding from CNNs, signal from GAN discriminators, Shruthi et al. (2025) and attention models. The real detection begins once the features have been extracted, with pixel analysis or statistical testing error level analysis, resampling detection, or ensuring light consistency. There are many classifiers that are used, including typical machine learning algorithms like SVMs, Random Forests, and KNNs and deep learning algorithms like CNNs, RNNs, Vision Transformers, and GANs (forgeries) detector models. Sedeeq (2025). At times, the hybrid method is used that utilizes metadata, visual features, and learned models. Classification would typically provide a binary response of real or fake or might have subclass categories of forgery. In certain instances, it would also involve localizing manipulated regions with the help of masks or heatmaps. Ultimately, the method employed is to evaluate detection model test performance using metrics such as accuracy, precision, recall, F1 score, ROC-AUC, Bammey et al. (2022). and localization metrics such as pixel accuracy or IoU. Robustness tests need to be conducted on multiple datasets and under diverse conditions: compression, addition of noise, scaling, and adversarial. Cross-dataset tests will reveal the generalization capacity of the methods. These include an outline detail on identification, classification, and their subsequent validation of image forgery. Durusoy (2025).

Dataset (CASIA/Deepfake) → Preprocessing → Feature Extraction (PRNU, CNN embeddings) → Detection Algorithm (ELA, SIFT, CNN) → Classification (SVM or Deep Network) → Evaluation (Accuracy, ROC–AUC, IoU). Lai et al. (2025). Figure 2.

4.1. COMPARATIVE ANALYSIS

Comparison of observations identifies the very first clear trends explain by various approaches; metadata and error-level analysis (ELA) Table 3, Nfor et al. 2024) are utilized thin-screening techniques but immensely shaky. Table 4 In contrast, copy-move detection remains stuck in solidity, particularly when enhanced using deep learning. While machine learning sowed the seeds, it was soon overshadowed by deep learning. Furthermore, deep learning has state-of-art accuracy but is hungry for resources. Hashing is extremely fast and scalable for integrity checking but is moderately robust. Its potential is further realized when paired with the power of deep learning. The shift of paradigm is from handcrafted features and traditional machine learning to deep learning, with transformer-based models experiencing a recent upsurge. This comparison contrasts the most significant techniques on the basis of their resistance to relative image manipulations, computational hardness, and usability in realistic scenarios. It also plots trends in tool usage and programming language usage and identifies practical change in the domain. Such comparison highlights the trade-offs between the forgery detection approaches. Even though they provide light-weight screening, metadata and error-level analysis are vulnerable when there is metadata removal or compression. Copy-move detection has gained highly explored methods with key points as well as deep learning techniques displaying great robustness against scaling and rotation. Patekar et al. (2023). Traditional methods were of average quality, but the deep learning techniques quickly took over from around all of them, boasting higher accuracy and localization, but at a cost. Hashing techniques are quick and optimum for bulk integrity checking but offer only medium resilience against tampering. They can be remarkably forensic consistent with image-device associations, but they are plagued by denoising and compression artefacts. Briefly, the most exciting are building deep learning and transformer-based approaches; Hao et al. (2021) integrated frameworks exist that bring together a number of methods to achieve maximum accuracy, efficiency, and resilience.

Table 3

Table 3 Evolution of Image Forgery Detection Techniques by Years.

Years	Researchers	Method	Key Technique	Dataset(s)	Performances
2016	Kumar et al. (2016)	Hybrid Keypoint-Based	SIFT + SURF + PCA features	MICC-F2000	Accurate for copy-move; fails under compression
2019	Kaur and Kanwal (2019)	Classical ML	DCT, PCA, LBP, SIFT; SVM classifier	CASIA	Baseline accuracy ~92% for splicing & copy-move
2020	Marra et al. (2020)	Deep Learning	Full-resolution CNN using Xception + Noiseprints	Vision, UCID, DSO-1	High AUC > 0.95; computationally expensive
2021	Hao et al. (2021)	Transformer-Based	TransForensics (Dense Self-Attention)	CASIA, Deepfake	Improved localization via attention maps
2021	Nande et al. (2021)	Texture + CNN Hybrid	CNN with histogram equalization, K-means segmentation	Custom 120-pair dataset	96.4% accuracy; robust under noise
2022	Siopi et al. (2022)	Multi-Stream Fusion DL	CNN-based multi-stream splicing localization	CASIA, CoMoFoD	Accurate localization; improved robustness
2023	Tyagi and Yadav (2023)	Lightweight CNN	MiniNet – concise deep CNN	CASIA 2.0	Efficient with small models (~93% accuracy)
2023	Guo et al. (2023)	Hierarchical CNN	Fine-grained image forgery localization	CVPR2023 Dataset	Excellent region-level detection
2024	Xu et al. (2024)	Explainable AI (XAI)	FakeShield: Multi-modal LLMs	Multiple benchmarks	Adds interpretability & cross-domain accuracy
2024	Nagm et al. (2024)	Hybrid ELA–CNN	Error Level Analysis + CNN Integration	Peer J Dataset	98.1% accuracy; metadata + visual fusion
2024	Diwan and Roy (2024)	Hybrid Feature Fusion	CenSurE + CNN Fusion Classifier	CASIA-II, CoMoFoD	High precision & recall; robust to transformations
2024	Gardella, et al. (2024)	Noise Analysis	Improved NoiseSniffer (noise inconsistency detection)	Public noise datasets	Fast & unsupervised; great for forensics
2024	Makandar and Javeriya (2024)	AI + ML	Hybrid deep neural approach	Custom Dataset	Robust against multiple forgery types
2025	Lai et al. (2025)	LLM-based Deepfake Detection	Multi-Agent LLM (Agent4FaceForgery)	Deepfake & So-Fake-Set	State-of-art deepfake face detection
2025	Akram et al. (2025)	Hybrid Framework	CNN + Copy-Move Pipeline	CASIA, CoMoFoD	High precision (99%); real-time capable
2025	Dell'Olmo et al., (2025)	Multi-Dataset CNN Comparison	Comparative CNN analysis	CASIA, MFFI, So-Fake-Set	Dataset dependency analysis for CNNs

Table 4

Table 4 Comparative Table of Image Forgery Detection Methods.

Techniques	Advantages	Disadvantages
EXIF tags (timestamp, GPS, device details), Metadata + ELA Processor	Simple, efficient, contextual data; useful for provenance and consistency verification	Can be easily removed, falsified, or stripped by social media platforms
Cryptographic & Perceptual Hashing, Image Hashing, SLIC	Excellent for duplicate detection and database indexing; scalable; perceptual variants tolerant to compression	Brittle under significant edits, transformations, or cropping; cryptographic hashes fail under minor changes
Block Matching, LBP, PCA, SVD	Simple and effective for detecting local copy-move forgeries; easy to implement	Sensitive to post-processing noise, filtering, and recompression
DCT, DWT, Fourier Transform, PCA	Captures frequency-domain and compression artifacts; strong for splicing and resampling	Requires parameter tuning; less robust against strong post-processing
SIFT, SURF, ORB	Robust to scaling, rotation, and partial tampering; effective for copy-move forgeries	May fail under heavy compression or low-texture image regions
PRNU, Sensor Pattern Noise, NoiseSniffer	Provides device fingerprinting and high forensic reliability; supports source attribution	Affected by compression, denoising, and resampling operations
DCT, DWT, Fourier, PCA	Foundational approach for periodic/frequency anomaly detection	Limited generalization; often requires expert manual interpretation
SVM, Random Forests, QCD, DCT/DWT feature learning	Balanced performance with moderate complexity; interpretable and efficient with smaller datasets	Poor generalization to unseen data; requires handcrafted features and preprocessing
CNNs, ResNet50, Vision Transformers (ViTs), BASNet	State-of-the-art accuracy, strong localization, learns hierarchical and abstract features	Computationally expensive, data-hungry, and less explainable
Multi-stream CNNs, Feature Fusion (Python → C++ pipelines)	Combines advantages of multiple domains; enhanced robustness and accuracy	Increased implementation complexity and training overhead

5. RESEARCH GAPS AND CHALLENGES

Nevertheless, some critical issues still remain for the practical application of forgery detection. One of the critical issues is with datasets, which are mostly not diverse enough. This aspect prevents the model from being able to handle already unseen types of forgery. Apart from this, most modern techniques are quite computationally expensive, and hence practically infeasible in most mobile applications, particularly where the response is required within seconds. Explainability is also a challenge; many deep learning models act as black boxes that are hard to break in Such openness diminishes trust—a bad situation, particularly in environments such as courtrooms and forensic analysis. Additionally, such models perform poorly with adaptive fakes, such as deepfakes or AI-generated forgeries, so they are quite the challenge to remain ahead of Finally, the integration of multimodal evidence using noise and content analysis with metadata, a task that has still not been accomplished, leaves the forensic infrastructure bare to sophisticated attacks.

6. FUTURE DIRECTIONS

Upcoming work must develop hybrid models that leverage metadata, offer hashing, and implement deep learning to make them more robust against all types of manipulation. We need light models that consume low power quickly due to deployment over mobile or resource-based settings. Explainable AI must also be encouraged because forensic usage demands transparency and accountability. Expansion and standardization are critical for datasets addressing generalization, particularly in dealing with new threats such as GAN-based deepfakes. Cross-disciplinary collaboration involving the domains of computer vision, cybersecurity, and law enforcement is necessary to take academic research and turn it into scalable and viable solutions for digital image forensics.

7. CONCLUSION

In the past, techniques like metadata check-ups and block-based copy-move detection were easy but easily breakable. The arrival of machine learning enhanced the systems' efficiency with handcrafted features, but Deep learning made a true breakthrough by providing the systems with the capability of automatically extracting features and reaching the desired level of accuracy. Transformer-based models have recently advanced these even further however, there is no one approach that can give its own distinct answer; hybrid approaches appear to achieve the most balance for robustness, velocity, and scalability. Even with the tremendous progress made, numerous issues still remain to be overcome, such as diversity in data, vast computational requirements, and the need for explainability since some of the fakes, like deepfakes, are so highly sophisticated. Therefore, light systems need to concentrate on processing an arbitrary data stream in an effort to improve the credibility of digital forensics. This would fill the gaps and instil confidence in digital media and help towards security, justice, and accountability within society.

CONFLICT OF INTERESTS

None .

ACKNOWLEDGMENTS

None.

REFERENCES

Akram, A., Jaffar, M. A., Rashid, J., Mahmood, K., and Ghani, A. (2025). Advanced Digital Image Forensics: A Hybrid Framework for Copy-Move Forgery Detection in Multimedia Security. Journal of Forensic Sciences. https://doi.org/10.1111/1556-4029.70076

Bammey, Q., Nikoukhah, T., Gardella, M., Gioi Colom, M., and Morel, J.-M. (2022). Non-Semantic Evaluation of Image Forensics Tools: Methodology and Database. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) (pp. 2383–2392). https://doi.org/10.1109/WACV51458.2022.00244

Dell'Olmo, P. V., Kuznetsov, O., Frontoni, E., Arnesano, M., Napoli, C., and Randieri, C. (2025). Dataset Dependency in CNN-Based Copy-Move Forgery Detection: A Multi-Dataset Comparative Analysis. Machine Learning and Knowledge Extraction, 7(2), 54. https://doi.org/10.3390/make7020054

Diwan, A., and Roy, (2024). Hybrid Model Integrating CensurE and CNN for Copy-Move Forgery Detection. Journal of Imaging Research, (3), 220–233. https://doi.org/10.1109/ACCESS.2024.3380460

Durusoy. (2025). Open-Source Datasets for Image Processing and Artificial Intelligence Research: A Comparison of ImageNet and MS COCO Datasets. International Journal of Sciences and Innovation Engineering, 2(5), 639–653. https://doi.org/10.70849/IJSCI0205202575

Gardella, M., Musé, P., Colom, M., and Morel, J.-M. (2024). Image Forgery Detection Based on Noise Inspection: Analysis and Refinement of the Noisesniffer Method. Image Processing on Line. https://doi.org/10.5201/ipol.2024.462

Gardella, M., Musé, P., Morel, J.-M., and Colom, M. (2021). NoiseSniffer: A Fully Automatic Image Forgery Detector Based on Noise Analysis. In Proceedings of the IEEE International Workshop on Biometrics and Forensics (IWBF) (1–6). https://doi.org/10.1109/IWBF50991.2021.9465095

Guo, X., Liu, Y., Ren, J., Grosz, S., Masi, I., and Liu, X. (2023). Hierarchical Fine-Grained Image Forgery detection and Localization. Arxiv Preprint. https://doi.org/10.48550/arXiv.2303.17111

Hao, J., Zhang, Z., Yang, S., Xie, D., and Pu, S. (2021). TransForensics: Image Forgery Localization with Dense Self-Attention. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). https://doi.org/10.1109/ICCV48922.2021.01478

Kaur, C., and Kanwal, N. (2019). An Analysis of Image Forgery Detection Techniques. Statistics, Optimization and Information Computing. https://doi.org/10.19139/soic.v7i2.542

Kintoh Allen Nfor, Tagne Poupi Theodore Armand, Hee-Cheol Kim, et al. (2024). A Holistic Approach to Image Forensics: Integrating Image Metadata Analysis and ELA with CNN and MLP for Image Forgery. Research Square Preprint (Version 1). https://doi.org/10.21203/rs.3.rs-4667372/v1

Kumar, J. V., Desai, S., and Mukherjee, S. (2016). A Fast Keypoint-Based Hybrid Method for Copy-Move Forgery Detection. Arxiv Preprint. https://doi.org/10.48550/arXiv.1612.03989

Lai, Y., Yu, Z., Wang, J., Shen, L., Xu, Y., and Cao, X. (2025). Agent4FaceForgery: Multi-Agent LLM Framework for Realistic Face Forgery Detection. Arxiv Preprint. https://arxiv.org/abs/2509.12546

Makandar, A., and Javeriya, S. B. (2024). Advanced AI Techniques for Detecting Forgeries of Diverse Data. IntechOpen. https://doi.org/10.5772/acrt.20240042

Mali, P. S., and Chavan, M. S. (2025). Evaluation of Image Forgery Detection Techniques Using DCT, DWT and QCD. International Journal for Modern Trends in Science and Technology, 11(6), 221–225. https://doi.org/10.46501/ijmtst.26.v11.i06

Marra, F., Gragnaniello, D., Cozzolino, D., and Verdoliva, L. (2020). Full-Image, Full-Resolution CNN for Image Forgery Detection. IEEE Transactions on Information Forensics and Security, 15, 2921–2931. https://doi.org/10.48550/arXiv.1909.06751

Mistry, D., and Banerjee, A. (2025). Comparison of Feature Detection and Matching Approaches: SIFT and SURF. Global Research Development (GRD), 2(3). https://doi.org/10.70179/3qhg4p03

Nagm, A. M., Moussa, M. M., Shoitan, R., Ali, A., Mashhour, M., Salama, A. S., and Abdul Wakel, H. I. (2024). Detecting Image Manipulation with ELA–CNN Integration: A Powerful Framework for Authenticity Verification. PeerJ Computer Science, 10, e2205. https://doi.org/10.7717/peerj-cs.2205

Nande, A., Rao, S., and Prasad, R. (2021). Multi-Semantic CRF-Based Attention Model for Image Forgery Detection and Localization. Pattern Recognition Letters, 142, 1–8. https://doi.org/10.1016/j.sigpro.2021.108051

Nayyef, A., and Al-Khanjari, Z. (2015). Detection Techniques of Digital Image Forgery By Using Images Metadata. Digital Investigation.

Patekar, S., Khan, S., Bhusare, D., Bhujbal, M., and Hegde, G. (2023). Image Forgery Detection. Journal for Basic Sciences. https://doi.org/10.13140/RG.2.2.32571.59680

PhotoHolmes Development Team. (2024). PhotoHolmes: A Python Library for Image Forgery Detection. Arxiv Preprint. https://doi.org/10.48550/arXiv.2412.14969

Sadeghi, S., Dadkhah, S., Jalab, H. A., et al. (2018). State of the Art in Passive Digital Image Forgery Detection: Copy-Move Image Forgery. Pattern Analysis and Applications. https://doi.org/10.1007/s10044-017-0678-8

Sedeeq. (2025). Image Forgery Detection Using Histogram-Oriented Gradients (HOG). Iraqi Journal of Science, 66(5), 2048–2058. https://doi.org/10.24996/ijs.2025.66.5.22

Shruthi, G., Soudhamini, B., Sandiri, S., Ramakrishna, R. V. V., and Deexit, Y. V. N. S. (2025). Image Forgery Detection Using Machine Learning. International Research Journal on Advanced Engineering Hub (IRJAEH), 3(4), 1164–1171. https://doi.org/10.47392/IRJAEH.2025.0166

Singh, S., Kumar, R., and Singh, C. (2024). Analysis on Recent Tools and Techniques for Image Forgery Detection. Advanced Research in Electrical and Electronic Engineering, 11(1), 12–20.

Siopi, M., Kordopatis-Zilos, G., Charitidis, P., Kompatsiaris, I., and Papadopoulos, S. (2022). A Multi-Stream Fusion Network for Image Splicing Localization. Arxiv Preprint.

Tom, N., Nandini, P., Princemary, and Ankayarkanni. (2019). An Improved Forgery Detection Method for Images. In IOP Conference Series: Materials Science and Engineering (Vol. 590, Article 012032). https://doi.org/10.1088/1757-899X/590/1/012032

Tyagi, S., and Yadav, D. (2023). A Detailed Analysis of Image and Video Forgery Detection Techniques. The Visual Computer, 39, 813–833. https://doi.org/10.1007/s00371-021-02347-4

Tyagi, S., and Yadav, D. (2023a). MiniNet: A Concise CNN for Image Forgery Detection. Evolving Systems, 14(3), 545–556. https://doi.org/10.1007/s12530-022-09446-0

Xu, Y., Zhang, H., Li, J., Tang, Z., Huang, J., and Jian, M. (2024). FakeShield: Explainable Image Forgery Detection and Localization Via Multi-Modal Large Language Models. Arxiv Preprint. https://doi.org/10.48550/arXiv.2410.02761