

International Journal for Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: https://doi.org/10.54692/ijeci.2026.1002/280

Research Article

Vol. 10 issue 2 Jul-Dec 2026

Image forgery detection in the era of generative editing: A structured review

Junaid Abdullah Mansoor[1], Rafaqat Alam Khan[2], Muhammad Nadeem Nadir[3], Muhammad Ishtiaq[2,4,*], Maryam Gulzar[5]

[1]Department of Data Science, University of the Punjab, Lahore 54590, Punjab, Pakistan

[2]Department of Software Engineering, The University of Lahore, Lahore 54600, Punjab, Pakistan

[3]School of Computer Science, Wuhan University, Wuhan 430072, Hubei, China

[4]School of Software Technology, Dalian University of Technology, Dalian 116024, Liaoning, China

[5]Department of Software Engineering, Lahore Leads University, Lahore 54000, Punjab, Pakistan

Corresponding Author: ishtiaqrai@mail.dlut.edu.cn

Received: November 1 ,2026, **Accepted:** November 15,2026; **Published:** November 25,2026

ABSTRACT

Image forgery detection has gained increasing attention due to its importance in digital forensics, multimedia security, and the fight against misinformation. Despite substantial progress, reliable detection remains challenging because modern manipulations can be visually subtle, benchmark datasets are often limited in scale and diversity, and existing methods may suffer from poor generalization and false detections under real-world conditions. This review examines image forgery detection techniques with emphasis on active and passive approaches, handcrafted feature-based methods, machine learning models, and deep learning architectures. Widely used datasets, including Chinese Academy of Sciences Institute of Automation (CASIA), Dresden Image Database, Copy-Move Forgery Dataset (CoMoFoD), and Image Manipulation Dataset 2020 (IMD2020), are reviewed with respect to their role in benchmarking detection and localization algorithms. The literature is organized through a structured taxonomy based on forgery type, detection strategy, dataset usage, and evaluation metrics. This paper further summarizes representative methods through comparative tables and identifies major research gaps, particularly in inpainting-based manipulation, deep learning generalization, and standardized evaluation. Finally, future directions are discussed, including multimodal analysis, explainable artificial intelligence, diffusion-aware detection, and the development of more diverse datasets and unified metrics to support robust digital media authentication.

Keywords: Image forgery detection, Digital forensics, Image tampering, Image inpainting, Multimedia

1. INTRODUCTION

In today's digital media and online information age, there is an unprecedented amount of visual information. It has been easy to create, manipulate and share images with high resolution due to the use of smartphones, computers and image editing software. This has revolutionized communication, journalism, entertainment and social interaction, but also questions the authenticity and integrity of visual information have been raised. Image forgery, also referred to as image tampering or manipulation, involves unauthorized changes to visual content, including the addition, removal, duplication, or modification of image regions [1]. Image forgery has become a serious problem because manipulated images can influence public opinion, conceal evidence, damage reputations, and support political, financial, or malicious objectives [2]. Manipulated content is a significant challenge to social media platforms to detect and remove from the system before it goes viral [3]. At the same time, ethical and legal questions about who is liable if fake visual information is shared leading to harm [4] are coming to the forefront. Human observers also are not reliable observers of manipulation, in that there are cognitive limitations that can impact visual perception including change blindness, where changes, however obvious, may not be noticed [1], [5]. These concerns highlight the need for reliable and reliable Digital Forensics techniques to be developed that can detect and trace the manipulation of images.

In 2008, for instance, a picture was published in an Iranian news agency of four missiles being fired. The image was posted on numerous major media platforms, but it was later revealed that there was a missile added in to hide a failed launch [6]. These events are all instances of how false images can deceive the viewer, abroad. But the danger to journalism, especially, to the reporting of legal evidence, science, law enforcement, and the public is not just about politics. Images have more impact on persuading people than text, because people believe what they see before reading it [7], [8].

In order to overcome this problem, researchers have proposed a variety of image forgery detection techniques. There are two general approaches to these: active and passive strategies. Active methods are those that need some sort of information to be embedded at the time of acquiring or distributing images, such as digital watermarking and digital signatures. Passive methods, or blind methods, do not need to be based on information that has been embedded prior and instead rely on inconsistencies created during manipulation. These inconsistencies can be seen in texture, noise pattern, illumination, compression artifacts, sensor traces or semantics. Over the past few years, machine learning and deep learning techniques have also been developed to further enhance the detection performance by learning discriminative forensic features directly from data.

Though these advancements have been made, there are still some questions unanswered. Existing datasets are frequently difficult to access, limited in variety, complexity and type of manipulation and even lack a realistic setting. Many methods are effective on their own held-out test sets but are not effective on other sets, compression techniques, post processing, or new manipulation tools. The swift advancements in deep learning, generative adversarial networks,

diffusion models, and image inpainting tools have significantly driven the realism and in detectability of the created content. Advancements in deep learning, generative adversarial networks, diffusion models, and image inpainting tools have made the created content more realistic and hard to detect. In particular, inpainting-based object removal and scene completion produce subtle inconsistencies, which may be missed by traditional forensic techniques. Thus, a structured review that helps to organize the existing body of research, compare data sets and techniques, and pinpoint research gaps is required. This paper is a summary of the main contributions as follows:

1. A structured study of image forgery detection, including active, passive, handcrafted feature-based, machine learning and deep learning approaches.
2. A taxonomy of image forgery detection methods for type of forgery, detection approach, type of dataset used and evaluation metrics.
3. Comprehensive overview of widely-used image forgery databases, their manipulation categories, advantages and disadvantages.
4. Representation of comparative analysis of representative detection methods with respect to datasets, evaluation metrics, strengths and weaknesses.
5. A critical analysis of unsolved problems, focusing on inpainting-based manipulation, generalization by deep learning and deployment in the wild.
6. Future research directions focusing on multimodal analysis, explainable artificial intelligence, diffusion-aware detection, standardized datasets, and unified evaluation protocols.

The remainder of this paper is organized as follows. Section 2 presents the review methodology, including the research questions, literature search strategy, inclusion and exclusion criteria, and classification framework. Section 3 introduces the fundamentals and taxonomy of image forgery detection. Section 4 reviews public datasets used for image forgery detection and localization. Section 5 discusses detection methods according to forgery type, including splicing, copy-move forgery, resampling, retouching, inpainting, and artificial intelligence (AI)-generated manipulation. Section 6 provides a comparative analysis of representative methods, datasets, and evaluation metrics. Section 7 discusses inpainting-based forgery detection as an emerging research gap and opportunity. Section 8 presents challenges and open issues. Section 9 outlines future research directions. Finally, Section 10 concludes the paper.

2. REVIEW METHODOLOGY

The paper is organized according to a structured review method for organizing the existing research on image forgery detection. The scope of digital image forensics has grown considerably, and a number of bibliometric and survey works have documented that there are various research directions, datasets, and techniques in digital forensics, along with a few unsolved challenges [9], [10]. The literature is thus organized by type of forgery, method of detection, type of data set used, and reported evaluation criteria. The aim is not to introduce a novel detection algorithm but to review the available methods, discuss some of the datasets that are most often used, and highlight areas of research that are open in image forgery detection.

2.1 Research Questions

The review is guided by the following research questions:

1. RQ1: What are the major categories of image forgery detection techniques, active vs passive?
2. RQ2: What are the most frequently used public datasets in image forgery detection and localization?
3. RQ3: What are the existing methods for detecting different types of forgery (image splicing, copy-move forgery, resampling, retouching, and inpainting) in the literature?
4. RQ4: What are the major advantages and drawbacks of hand-crafted feature-based, machine learning, and deep learning approaches?
5. RQ5: What research gaps are there, particularly in the realm of inpainting-based manipulation, diversity, robustness, and real-world deployment?

2.2 Literature Selection

The studies reviewed in this paper were selected based on their relevance to image forgery detection, digital image forensics, forensic datasets, and manipulation localization. Foundational works were included when they introduced important forensic concepts, benchmark datasets, or classical detection techniques. Recent studies were included when they addressed machine learning, deep learning, inpainting-based manipulation, or advanced detection and localization methods.

The reviewed literature was grouped into four main categories. The first category includes public datasets used for image forgery detection and benchmarking, such as Dresden, CASIA, CoMoFoD, and IMD2020 [11]-[14]. Other datasets, including MICC-F2000, RAISE, MFC, and CMFD, are discussed later in the dataset review section.

The second category covers active forensic methods. These methods include secure camera-based authentication, digital watermarking, and digital signatures, which require prior information to be embedded or generated before verification [15], [16], [17]. Such methods are useful when image acquisition and distribution can be controlled, but their applicability is limited when no prior authentication information is available.

The third category includes passive detection methods. These methods do not require prior embedded information and instead detect traces left by manipulation. Existing passive approaches cover image splicing [18], [19], copy-move forgery [20], [21], resampling [22], [23], and enhancement or retouching operations [24], [25]. These studies form the basis for comparing handcrafted feature-based, machine learning-based, and deep learning-based detection strategies.

The fourth category focuses on inpainting and deep learning-based forgery detection. Exemplar-based inpainting detection was among the early directions for identifying object removal [26]–[28]. Later studies used deep learning models, including convolutional neural network (CNN)based localization, transformer-CNN models, and feature enhancement networks, to improve the detection and localization of manipulated regions [29]-[32]. This category is significant because the manipulations based on inpainting can generate realistic object removal and completion of the scene, making it more difficult to detect. For this literature selection procedure to be better understood, the following Table 1 summarizes the sources of information searched, the terms searched, the screening procedure and the classification dimensions of the literature selected for this study.

2.3 Inclusion and Exclusion Criteria

The literature was included if it satisfied at least one of the following criteria:

1. It proposed or evaluated an image forgery detection or localization method;
2. It introduced or used a public dataset for image forgery detection;
3. It discussed active or passive image forensic techniques;
4. It addressed a specific manipulation type, including copy-move forgery, splicing, resampling, retouching, contrast enhancement, or inpainting;
5. It applied handcrafted features, machine learning, deep learning, or hybrid models to image forgery detection;
6. It reported detection or localization performance using quantitative measures such as accuracy, AUC, F-score, true positive rate, false positive rate, or related evaluation criteria.

Studies that discussed general image processing but were not related to forgery detection were excluded, as were studies that were not sufficiently methodologically detailed, did not discuss image-level manipulation, discussed copyright protection but didn't consider image manipulation detection, or focused solely on forgery detection. The exclusion criterion is crucial since copyright violations and image forgery are two distinct issues. Violation of copyright can be considered as the unauthorized use of an image, while image forgery refers to changing the visual information.

2.4 Classification Framework

For categorizing the selected papers, we have chosen the following four criteria: dataset, forgery method, detection method, and evaluation method. Under dataset-based classification, we categorize whether the paper utilizes any benchmark dataset such as CASIA, CoMoFoD, MICCF2000, IMD2020, RAISE, MFC, and CMFD. Under forgery-based classification, we classify the papers in categories of image splicing, copy move forgery, resampling, retouching, contrast manipulation, and inpainting manipulation. Under detection-based classification, we categorize the papers under active methods, handcrafted features-based method, classical ML methods, deep learning methods, and hybrid methods. This classification framework provides the basis for the taxonomy, dataset review, method comparison, and gap analysis presented in the following sections.

3. FUNDAMENTALS AND TAXONOMY OF IMAGE FORGERY DETECTION

Image forgery detection is a branch of digital image forensics that aims to determine whether an image has been manipulated and, in some cases, to localize the manipulated region. Image manipulation may involve adding, removing, duplicating, enhancing, or geometrically transforming image content. Depending on the application, the objective of a forgery detection method may be image-level classification, region level localization, or source-related verification. Image-level classification determines whether an image is authentic or forged, while localization identifies the specific tampered region. Source-related verification attempts to determine whether the image is consistent with a particular acquisition device, processing history, or authentication mechanism

3.1 Active and Passive Image Forensics

Image forgery detection techniques are commonly divided into active and passive approaches. Active approaches require authentication information to be embedded or generated before image distribution. These include secure camera mechanisms, digital watermarking and digital signatures [15]-[17]. These methods can be subsequently

authenticated by determining if the embedded authentication information (e.g. watermark, signature, authentication information for acquisition, etc.) is valid. When the image acquisition and distribution pipeline is controlled, active methods can offer robust verification. Their application is limited however, if the image is captured by a conventional device and shared without any prior authentication information.

Passive approaches are also known as blind forensic approaches, as they do not rely on embedded information or access to the image itself. Rather, they study traces added while manipulation. These can manifest as patterns of illumination, texture, edges, compression artifacts, or as patterns of information, sensor noise or semantic information. Passive methods are more flexible than active methods as they can be used with images captured from uncontrolled sources. They also are harder to design as manipulation traces can be weak, obscured by post processing or influenced by compression and resizing

Table 1 Search protocol used for selecting literature on image forgery detection.

Item	**Description**
Review type	Structured narrative review focused on image forgery detection, manipulation localization, datasets, detection strategies, and emerging generative-editing challenges.
Databases and sources	IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Google Scholar, arXiv, and publisher webpages of relevant journals and conferences.
Search period	Foundational studies were considered from earlier image forensic literature, while recent studies from 2023–2026 were emphasized for deep learning, transformer-based methods, inpainting, retouching, and generative-editing-aware detection.
Search terms	Search terms “image forgery detection”, “image manipulation localization”, “copy-move forgery detection”, “image splicing detection”, “image resampling detection”, “image retouching detection”, “contrast enhancement forensics”, “image inpainting detection”, “deep learning image forensics”, “transformer image forgery localization”, “diffusion image manipulation”, and “text-prompt image manipulation”.
Screening process	Papers were first screened by title and abstract, followed by full-text checking for relevance to image forgery detection, dataset usage, manipulation type, detection strategy, evaluation metric, and reported limitation.
Selection focus	Priority was given to studies introducing benchmark datasets, classical forensic concepts, representative handcrafted methods, machine learning and deep learning detectors, inpainting-related detection, and recent generative-editing-aware approaches.
Classification dimensions	Selected studies were organized by dataset, forgery type, detection strategy, evaluation focus, robustness, and research limitation.

3.2 Forgery Types

Image forgery can be categorized according to the type of manipulation applied to the image. The most common categories include image splicing, copy-move forgery, resampling, retouching, contrast enhancement, and inpainting-based object removal. Image splicing involves combining regions from two or more images to create a composite image. Since the inserted region may come from a different source, splicing can introduce inconsistencies in illumination, color, texture, noise, or camera response characteristics [18], [33].

Copy-move forgery involves copying a region from one part of an image and pasting it into another part of the same image. In such a forgery, the duplicated content or the hidden objects are typically identified by looking for duplicated areas, repeated key points, or similar local features [20], [21]. Resampling is the term for scaling, rotation, skewing or resizing a signal, which could cause interpolation artifacts and periodic statistical traces [22], [23]. Retouching and contrast enhancement are manipulations of the image, such as histogram, brightness adjustment, smoothing, and sharpening, that change the appearance of an image [24], [25].

Inpainting-based manipulation is capable of removing or filling parts of an image using either surrounding pixels or prior knowledge of images learned from a set of examples. This is particularly difficult due to the fact that modern inpainting techniques can create visually plausible images with low forensic signatures [26]–[28].

3.3 Detection Strategies

There are other ways to categorize forgery detection methods as well: by the forgery detection strategy used to detect the manipulation. The traditional approaches use handcrafted features for the detection of certain forensic features, including noise residuals, block similarity, texture inconsistency, interpolation artifacts or compression anomalies. Though sometimes they can be interpreted, their effectiveness can get compromised under targeted manipulation types, and it may be reduced if the manipulation is followed by compression, blurring, scaling or any other post-processing.

Machine learning-based methods use extracted features together with classifiers such as support vector machines or other supervised learning models. These methods are better at discrimination than strictly rule-based methods, but their discrimination performance is also highly dependent on the quality and generality of the features chosen. Deep learning-based methods learn forensic representations directly from the data, and have been used on image-level detection and pixel-level localization.

Several architectures such as convolutional neural networks, fully convolutional networks, residual networks and hybrid ones have been applied to recognize manipulated traces that are hard to be captured by hand [19], [29], [30]. Recent works have also addressed the detection and localization of inpainting-based manipulation using transformer-CNN [31], [32].

3.4 Proposed Taxonomy

Based on the reviewed literature, this paper organizes image forgery detection methods into a taxonomy with three connected levels. The first level is the forensic setting, which separates active and passive detection methods. The second level is the manipulation type, which includes splicing, copy-move forgery, resampling, retouching, contrast enhancement, and inpainting-based manipulation. The third level is the detection model, which includes handcrafted feature-based methods, classical machine learning methods, deep learning methods, and hybrid methods.

This taxonomy provides a structured basis for the remaining sections. The proposed taxonomy used to organize the reviewed literature is illustrated in Fig. 1. Public datasets are reviewed according to the manipulation types they support. Detection methods are discussed according to the type of forgery they address. Comparative analysis is then used to identify strengths, limitations, and open research gaps across datasets, methods, and evaluation settings.

4. PUBLIC DATASETS FOR IMAGE FORGERY DETECTION

The public datasets are important for the image forgery detection, since they serve as the benchmark images for training, testing and comparing with the forgery detection algorithms. The dataset should be diverse in image sources, in manipulation type (realistic), in ground truth, and in image content, resolution, compression and post processing conditions.

There is a wide variety of available datasets, however, with different designs and purposes. Some datasets contain authentic camera-native images and are mainly useful for camera identification or forensic feature analysis, whereas others provide manipulated images for evaluating copy-move forgery, splicing, retouching, inpainting, or general tampering detection. Therefore, dataset selection has a direct influence on the reported performance and practical reliability of forgery

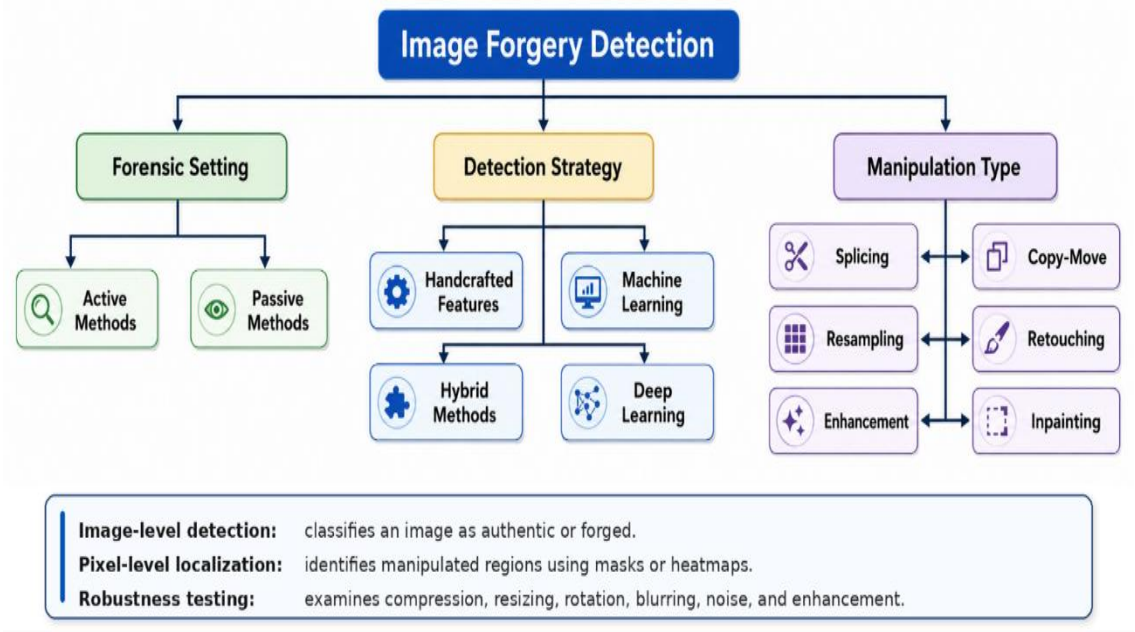

Fig 1 Proposed taxonomy of image forgery detection techniques. The taxonomy organizes the reviewed methods according to forensic setting, manipulation type, and detection strategy

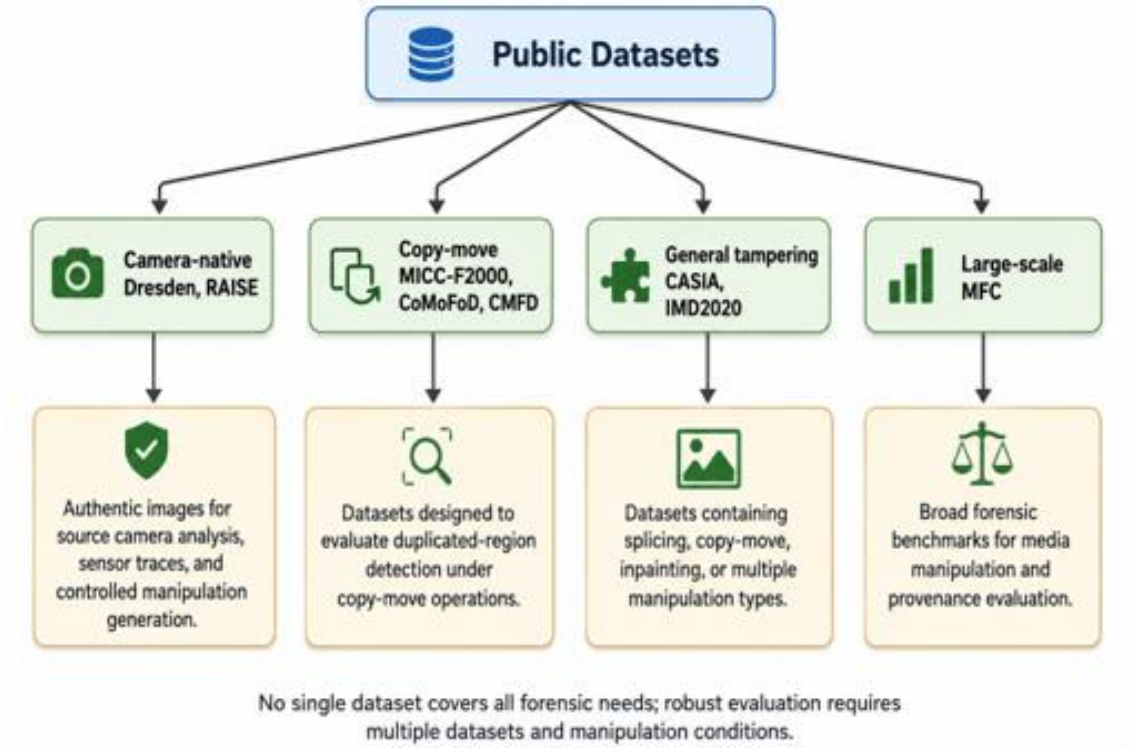

Fig. 2. Grouping of representative public datasets used in image forgery detection according to their primary forensic purpose, including camera-native datasets, copy-move datasets, general tampering datasets, and large-scale forensic datasets [11]–[14]

detection methods. A general grouping of the reviewed datasets according to their primary forensic purpose is shown in Fig. 2.

4.1 Camera-native and Authentic Image Datasets

The Dresden Image Database is one of the widely used datasets in digital image forensics. It contains high-resolution images captured using different camera models and devices under controlled conditions [11]. Although it is not primarily a tampering dataset, it is useful for analyzing camera-specific traces, sensor noise patterns, and acquisition-related forensic characteristics. Such characteristics are important for passive forensic methods that rely on source camera identification or inconsistencies in acquisition traces.

RAISE is another important dataset composed of higher solution RAW images collected from different cameras and real-world scenes [35]. Since the images are camera-native and uncompressed, RAISE is useful for studying original image statistics and for generating controlled manipulations. However, because it mainly provides authentic images, additional

manipulation generation or annotation is required when using it for direct forgery

4.2 Copy-move Forgery Datasets

Copy-move forgery datasets are designed to evaluate methods that detect duplicated regions within the same image. MICC-F2000 is commonly used for copy-move forgery detection and contains images where regions are copied and pasted into different locations of the same image [34]. This type of dataset is useful for evaluating keypoint-based, block-based, and feature-matching methods.

CoMoFoD is another important benchmark for copy-move forgery detection [13]. It includes manipulated images with different transformations and post-processing operations, such as scaling, rotation, blurring, noise addition, and JPEG compression. These variations make it useful for testing the robustness of copy-move detection methods under realistic image editing conditions.

The CMFD benchmark is also used for evaluating copy-move forgery detection methods [37]. It allows the comparison of algorithms in various transformations and post-processing. The copy-move forgery is hard to detect if the copied regions are resized, rotated, blurred, or compressed after the copy. Copy-move forgery is valuable because it can be difficult to detect when the copied regions are resized, rotated, blurred, or compressed after the copy.

4.3 General Tampering and Splicing Datasets

The CASIA is one of the most widely used image tampering datasets that are available for image tampering detection [12]. Includes real and manipulated images created with various manipulation methods such as image splicing and copy-move. The CASIA has been widely used, as it enables the benchmark of traditional and learning-based forgery detection methods. Its controlled manipulation settings may not, however, be representative of the complex real-world manipulation scenarios.

The more recent image manipulation detection dataset is called IMD2020 [14]. Includes real and manipulated images created with several manipulation types including high quality manipulation operations. The IMD2020 is more relevant for the assessment of modern image forgery detection techniques since it contains more challenging manipulation cases compared to previous datasets. It's especially suitable for the study of detection techniques that must cope with various and subtle tampering.

The Media Forensics Challenge (MFC) datasets offer media forensic research with large-scale benchmark data [36]. These datasets contain different manipulation scenarios and provenance information, thus they can be employed for assessing forensic algorithms in more realistic scenarios. However, because MFC is broad in scope and includes different media types and tasks, careful selection of image specific subsets is necessary when using it for image forgery detection.

4.4 Dataset Comparison and Limitations

Table 2 summarizes representative public datasets used in image forgery detection, including their primary forensic purpose, manipulation or content type, main forensic use, and major limitations. The table highlights that

no single dataset is sufficient for evaluating all types of image forgery. Camera-native datasets such as Dresden and RAISE are useful for acquisition-related forensic studies, while CASIA, CoMoFoD, MICC-F2000, IMD2020, MFC, and CMFD are more directly related to manipulation detection and localization.

Although public datasets have supported major progress in image forgery detection, several limitations remain. First, many datasets focus on a single manipulation type, such as copy-move forgery or splicing. This restricts their ability of assessing methods with mixed or complex manipulation situations. Second, procedures for manipulation may have to be controlled and may not accurately reflect actual editing processes. Third, there are differences in image resolution, compression quality, the format of the annotations, and the evaluation protocol between studies. Fourth, many datasets are unrealistic for modern editing operations such as those generated by inpainting or deep learning based editing techniques.

This restricts the performance of many methods to the set of data they were trained on, and is the reason why many methods work well on one set of data but fail on another. For strong image forgery detection, it is important to consider multiple datasets, multiple types of forgery operations, and various post-processing conditions. The need for dataset diversity and reliable ground truth, along with standardized evaluation protocols remain critical to future research on digital image forensics.

5. DETECTION METHODS ACCORDING TO FORGERY TYPE

Image forgery detection methods can be better understood when they are discussed according to the type of manipulation they are designed to detect. Different forgery types produce different traces. For example, image splicing may introduce illumination or camera-response inconsistencies, copy-move forgery may create duplicated regions, resampling may leave interpolation artifacts, and inpainting may generate unnatural texture or noise patterns. Therefore, this section reviews representative detection methods for major image forgery categories, including image splicing, copy-move forgery, resampling, retouching and enhancement, and inpainting-based manipulation. Representative examples of common image forgery types are shown in Fig. 3 and 4.

5.1 Image Splicing Detection

Image splicing is defined as the technique of creating an image by splicing or merging parts of two or more images together. In splicing, the spliced image may have originated from another image, hence, leading to inconsistencies of the illumination, color, texture, camera response, and statistics of the images. The early techniques for detecting splicing were based on manually crafted forensics, like illumination and color inconsistency [18], [33]. These methods are useful because spliced regions often do not share the same physical or acquisition conditions as the host image.

Table 2 Representative public datasets used in image forgery detection

Dataset	Primary Purpose	Manipulation / Content Type	Main Use in Forensics	Main Limitation
Dresden [11]	Camera-based forensic analysis	Authentic camera images	Camera model identification and sensor trace analysis	Not primarily designed as a tampering dataset
MICC-F2000 [34]	Copy-move forgery detection	Copy-move manipulation	Evaluation of duplicated region detection methods	Limited manipulation diversity
CASIA [12]	General image tampering detection	Splicing and copy-move manipulation	Benchmarking image level forgery detection and localization	Controlled manipulation may not represent all real-world cases
CoMoFoD [13]	Copy-move forgery detection	Copy-move with transformations and post-processing	Robustness testing under scaling, rotation, blurring, noise, and compression	Mainly focused on copy-move forgery
RAISE [35]	Camera-native image analysis	Authentic RAW images	Source image statistics and controlled manipulation generation	Requires additional manipulation and annotation for forgery detection
IMD2020 [14]	Image manipulation detection	Multiple manipulation types	Evaluation of modern tampering detection methods	Dataset-specific bias may affect generalization
MFC [36]	Media forensic challenge evaluation	Diverse media manipulation scenarios	Large-scale forensic benchmarking and provenance analysis	Image-specific subsets must be carefully selected
CMFD [37]	Copy-move forgery evaluation	Copy-move manipulation	Comparison of copy-move detection algorithms	Limited to copy-move related evaluation

The feature-based approach and machine learning techniques have also been applied for detecting splicing. For instance, texture features and classifiers have been used to classify genuine and spliced images based on statistical differences in their local areas [38]. The deep learning techniques have contributed further in detecting splicing through direct learning of discriminative features from images. CNN-based approaches have been used to detect splicing and copy-move forgeries by learning manipulation traces without relying entirely on manually designed features [19]. Mask-RCNN-based methods have also been explored for detecting spliced regions, showing the potential of object-level and region-level learning for

manipulation localization [3].

Example categories are based on commonly used forgery datasets and manipulation studies [12]-[14], [26], [27], [34] operations such as color correction, compression, blurring, and resizing can reduce visible forensic traces. In addition, when the source and target imageshave similar lighting conditions, camera characteristics, or texture distributions, the boundary between authentic and spliced content may become difficult to detect. Therefore, robust splicing detection requires methods that can jointly analyze low-level forensic artifacts and high-level semantic inconsistencies.

5.2 Copy-move Forgery Detection

Copy-move forgery is one of the most common forms of image manipulation. In this type of forgery, a region from an image is copied and pasted into another location within the same image. Since the copied region comes from the same image, its color, noise, illumination, and camera characteristics are often.

Copy-move forgery is one of the most common forms of image manipulation. In this type of forgery, a region from an image is copied and pasted into another location within the same image. Since the copied region comes from the same image, its color, noise, illumination, and camera characteristics are often

consistent with the rest of the image. This makes copy-move forgery more difficult to detect than some splicing operations. Detection methods usually focus

on identifying duplicated regions, repeated local features, or similar blocks within the image [20], [40].

Traditional copy-move forgery detection methods can be broadly divided into block-based and keypoint-based approaches. Block-based methods divide the

image into overlapping or non-overlapping blocks and search for similar blocks. These methods can localize duplicated regions accurately, but they may become computationally expensive for high-resolution images. Keypoint-based methods detect interest points and compare local descriptors to find duplicated regions. Such methods are often more efficient and more robust to geometric transformations, but they may fail in smooth or low-texture regions where few reliable keypoints are available.

Several methods have been proposed to improve robustness against transformations such as scaling, rotation, compression, and noise. SIFT-based and ORB-based methods have been used to detect duplicated regions under geometric changes [41], [42]. Transform-domain methods using techniques such as PCA, SVD, and FFT have also been explored for improving feature compactness and robustness [43]. More recent deep learning-based methods, including attention and residual refinement networks, have been used to improve copy-move forgery detection and localization [44], [45]. However, copy-move detection remains challenging when the duplicated region is small, heavily post-processed, or placed in a visually similar background.

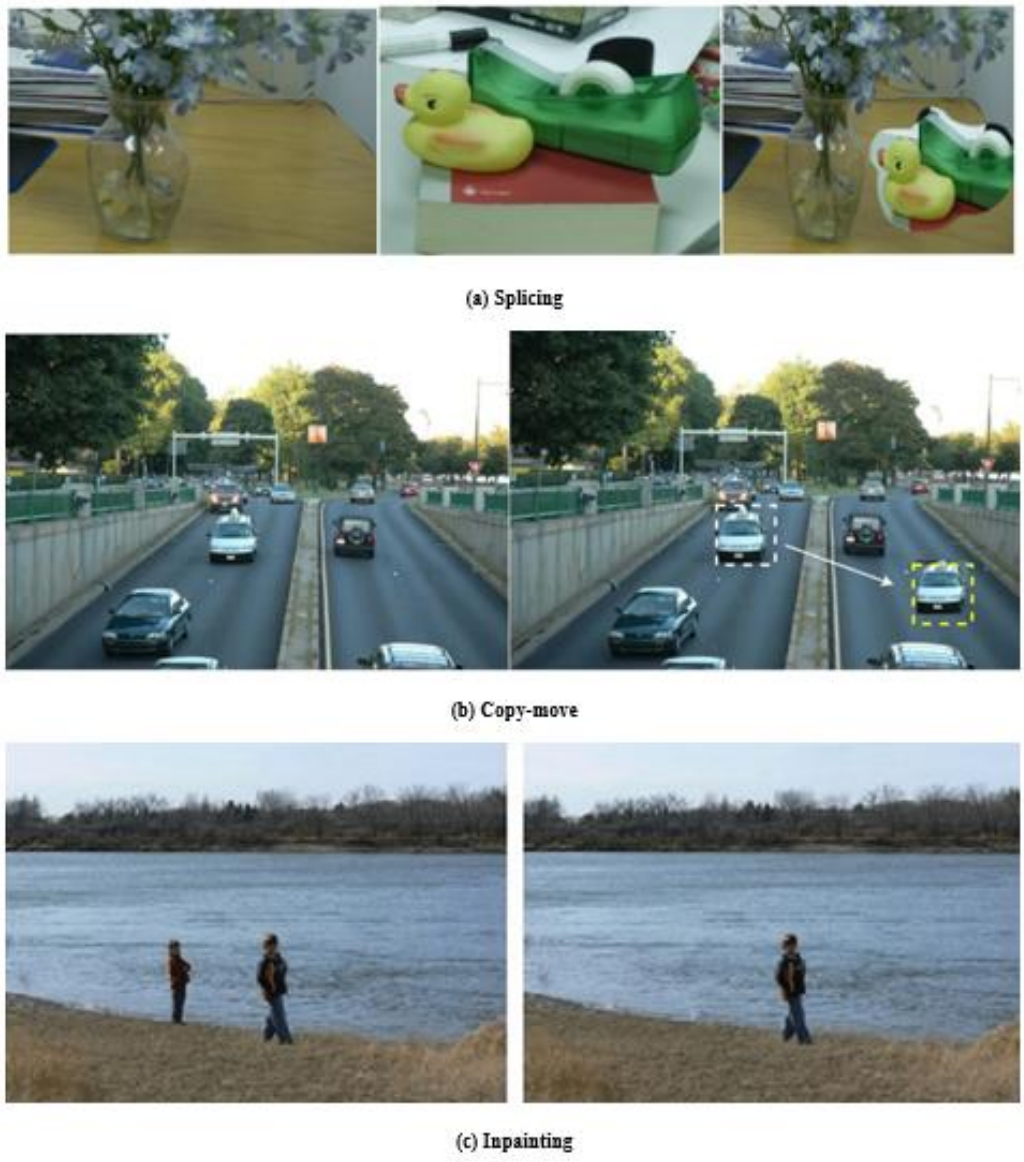

Fig. 3. Representative examples of common image forgery types: splicing, copy-move forgery, and inpainting-based manipulation.

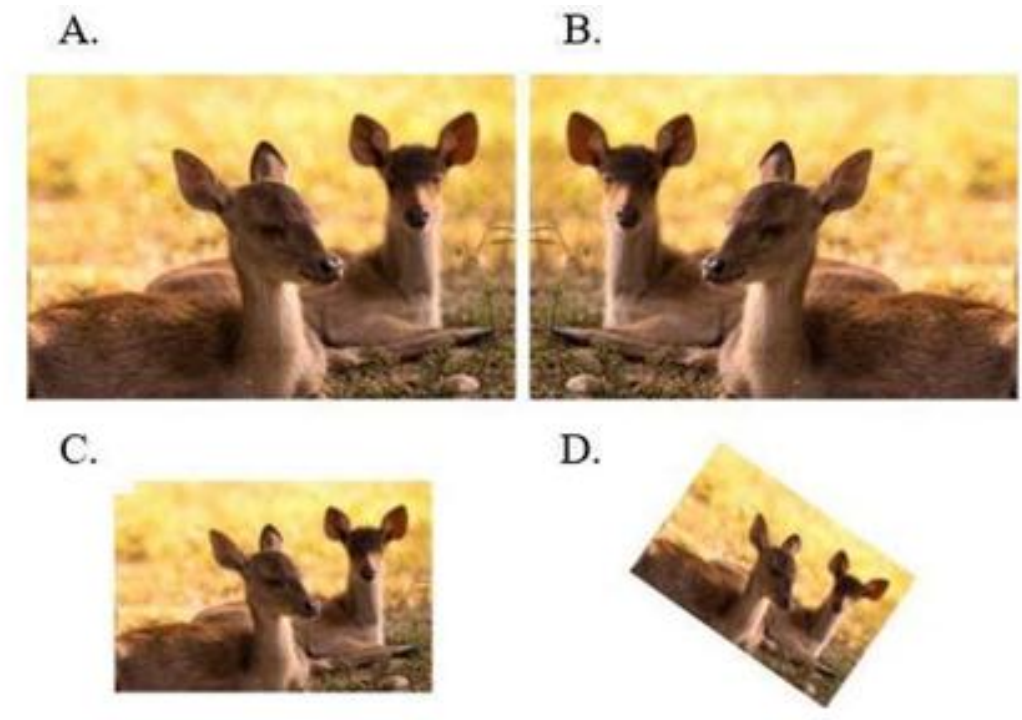

Fig 2 Representative examples of common image forgery types continued: resampling and retouching.

5.3 Resampling and Geometric Transformation Detection

Resampling occurs when an image or part of an image is geometrically transformed through operations such as scaling, rotation, skewing, stretching, or resizing. These operations often require interpolation, which may introduce periodic patterns or statistical traces in the image. Detecting such traces is important because resampling is frequently used during splicing, copy-move forgery, and object manipulation to adjust the size or orientation of inserted regions.

Traditional resampling detection methods attempt to identify interpolation artifacts and statistical dependencies introduced by geometric transformation. There are some methods that utilize mathematical models and statistical analysis to reveal resampling traces [22], [46]. Residual noise analysis or likelihood-based detection are other approaches adopted to distinguish resampled regions from real image regions [47]. When the interpolation traces are kept these techniques can work well, but can be less effective when JPEG compression or noise addition or other post-processing operations are performed.

Resampling detection is also a possible application of deep learning. Features related to resampling and post compression artifacts have been learnt using constrained CNNs and multi-patch aggregation models [23], [48]. These techniques can enhance detection performance over purely handcrafted methods, but still have generalization issues when evaluating images created by different transformation settings, compression levels, or editing tools. Thus, resampling detection is still a crucial but challenging aspect of passive image forensics.

5.4 Retouching and Enhancement Detection

Retouching refers to image modifications intended to improve appearance or conceal evidence of manipulation. Common retouching operations include sharpening, smoothing, contrast enhancement, brightness adjustment, histogram modification, and local editing. Unlike splicing or copy-move forgery, retouching does not necessarily add or remove semantic objects. Instead, it changes the visual quality or statistical distribution of an image. These changes may still be important in forensic analysis because they can hide manipulation traces or alter the meaning of visual evidence.

Several methods have been proposed to detect sharpening and contrast enhancement. Overshoot artifact analysis has been used for detecting image sharpening operations [49], [50]. Histogram-based and gradient-based techniques have been applied to identify contrast enhancement and related post-processing operations [24], [51]. Other literature has adopted local binary coding, CNN based approaches and multipath networks to improve the accuracy of sharpening detection and/or contrast enhancement [52],[53],[25]. The results indicate that enhancement operations can be detected in edges, histograms, and local image statistics.

But even retouching detection remains challenging as many retouching operations are visually subtle, and may also be done as part of the normal image processing. For instance, an auto-adjustment or sharpening feature may occur automatically by camera, mobile device or social media. For this reason, forensics techniques need

to differentiate between normal image enhancement and retouching. The detection of retouching is therefore highly context-specific, and relies on the design of the data set and the evaluation procedure.

5.5 Inpainting-based Manipulation Detection

Image inpainting masks missing or removed areas with surrounding pixels, texture propagation, or learned image priors. In the field of digital forensics, particularly in the context of image editing, inpainting plays a crucial role as it can be applied to mask objects, cover up evidence, or restore image regions in a plausible manner. Previous exemplar-based inpainting approaches produced repetitive patches or inconsistencies in structure, which were identified by a search for unusual patch similarity or separated areas [26]–[28].

With the development of machine learning and deep learning, inpainting methods have become more realistic. Context encoders introduced the idea of learning image representations through inpainting-based prediction [54]. Later deep inpainting techniques relied on the use of CNNs, generative models, Fourier convolutions and cooperative filtering to obtain visually satisfactory restoration [55]-[57]. The quality of inpainting increases as the quality of the forensic images increases, due to the fact that the manipulated areas might have less detectable inpainting artifacts.

Deep learning-based inpainting detection methods have been developed to address this challenge. Patch-based CNN models have been used for image inpainting forensics [29]. High-pass fully convolutional networks have been proposed to localize deep inpainting regions by emphasizing manipulation traces that may not be visible in the image content [30]. More recent models have explored transformer-CNN architectures and feature enhancement networks for detecting and localizing inpainting forgery [31], [32]. These studies show that deep models can capture subtle manipulation traces, but their performance may still depend heavily on the training data, inpainting method, mask shape, and post-processing conditions.

Image inpainting is one of the most critical open problems in image forgery detection. Modern inpainting is not limited to copy-move or splicing, and can create new content that is visually consistent with the rest of the image. This can make it hard to detect, particularly if the edited area is small, semantically reasonable or is edited and compressed. Thus, future inpainting detection methods must possess more power of generalization in terms of data sets, editing tools and post-processing conditions.

5.6 Summary of Detection Methods

Based on the reviewed detection methods, it can be concluded that the forgery type causes distinct forensic traces. The ability of the splicer to detect the splice is frequently based on inconsistencies between the inserted region and the host region. A tool called copy-move detection, which searches for duplicate images, is used to find duplicate content in an image. The focus of resampling detection is on artifacts of interpolation and geometric transformation. Changes in statistics about enhancements are detected in retouching detection. The goal of inpainting detection is to identify inpainted regions that may contain a low-level texture, noise or even a semantic error.

There is no single method that is effective in all types of forgery. The handcrafted technique can be informative and useful in some traces and useless in more complex post processing. Machine learning techniques enhance discrimination, but rely on good quality features. Deep learning techniques can learn representations that are better, but they require to be learnt with diverse data and they might not be well generalised across datasets. The observations give the impetus to a comparative analysis as described in the next section.

6. COMPARATIVE ANALYSIS AND DISCUSSION

It has been seen through the review of the literature that there are different targets of manipulation, image representations, data sources, evaluation measures, and robustness for the image forgery detection methods. Different methods can detect one type of manipulation such as copy move forgery or resampling and image tampering in general. Similar to that, traditional methods tend to be more focused on identifying certain forensic characteristics whereas the learning based methods focus on learning discriminative features from data. This section contrasts representative methods based on the type of forgery, the strategy used to detect it, the focus of the evaluation and the practical considerations.

6.1 Comparison across Forgery Types

Forensic artifacts are different for different types of forgery. When using image splicing, inconsistencies may occur between the inserted image and the background image with respect to illumination, camera response, image texture or noise mismatch [18], [33]. In copy-move forgery this is not the case, since the duplicated image region is part of the same image, and hence their color and noise statistics are more similar to the original image. Thus, the use of duplicated blocks, matched keypoints, or repeated local structures [20], [21] are typically used in copy-move detection methods. Resampling detection is based on interpolation and geometric transformation artifacts, and retouching detection is based on histogram, edge, and local statistics changes that are related to enhancement artifacts [22]-[25]. Finally, inpainting detection is harder since the inpainted area can be generated to concatenate seamlessly with the rest of the image, mimicking the visual characteristics of the original content [26], [29], [30]. The major characteristics of the most common forgery types, including the manipulation involved in creating them, forensic indications of forgery, representative detection methods, and key limitations are summarized in Table 3.

6.2 Comparison of Detection Strategies

The possible detection strategies can be classified as active ones, handcrafted passive ones, machine learning ones, deep learning ones, and hybrid ones. When watermarking, signatures, or secure acquisition mechanisms are available, then active methods can offer strong authentication [15]-[17]. But they are not appropriate for images that were not captured or shared with any authentication information. Passive methods are more flexible since they work directly on the image available to them, but they rely on the strength of the manipulation traces and how reliable of them they are. Handcrafted feature-based methods are often interpretable because they are designed around known forensic artifacts, such as duplicated

regions, interpolation patterns, histogram changes, and texture inconsistencies. Their weakness is that they usually target specific forgery types and may fail under unseen manipulation or post-processing. Machine learning methods improve classification by combining handcrafted features with classifiers, but their performance still depends on feature quality. Deep learning methods can learn complex manipulation traces directly from data and have shown strong potential for both image-level detection and pixel-level localization [19], [29], [30]. However, deep models require sufficient training data and may not generalize well across datasets or manipulation tools. Table 4 compares the main detection strategies used in image forgery detection, including active methods, handcrafted passive methods, machine learning, deep learning, and hybrid approaches.

6.3 Evaluation Metrics

The evaluation of image forgery detection depends on whether the task is image-level detection or pixel-level localization. Image-level detection determines whether the entire image is authentic or forged. Common metrics for this task include accuracy, precision, recall, F-score, true positive rate, false positive rate, and area under the curve. These metrics are useful for comparing classification performance, but they do not indicate where the manipulated region is located. Pixel-level localization evaluates whether the method can identify the forged region inside the image. Localization performance is usually assessed using region-based or pixel-based measures, such as overlap between predicted and ground-truth masks. Localization is more difficult than image-level classification because a method must not only identify that manipulation exists, but also accurately separate forged and authentic regions. This is especially challenging for small manipulations, blurred boundaries, inpainting-based object removal, and images compressed after editing.

A weakness in the literature is that different studies use different datasets, metrics, manipulation settings, and post processing conditions. Thus direct comparison is sometimes hard to make. A technique that works well on one data set might not work well on another data set. Thus, the evaluation needs to be done on various datasets, with both detection and localization performance reported and with robustness analysis considering common post-processing operations.

6.4 Robustness and Generalization

Robustness is one of the most critical problem to image forgery detection. Images taken in real life are frequently altered in size, compressed, blurred, and sharpened before being posted on the social media sites. These activities may also degrade or destroy forensic evidence. Copy-move techniques can perform poorly when duplicated regions are rotated, scaled or have undergone substantial compression. When the JPEG compression and/or the noise are high, resampling detectors can fail. Normal enhancement can be mistaken for malicious retouching by retouching detectors. It is possible for inpainting detectors to be misled when the inpainted portion is visually and statistically similar to the surrounding content.

Table 3 Comparison of major image forgery types and detection characteristics

Forgery Type	Main Operation	Common Detection	Cues Representative Methods	Main Limitations
Image splicing	Combining regions from different images	Illumination mismatch, camera response inconsistency, texture and noise differences	Illumination-based, camera response-based, texture-based, and CNN-based methods [18], [33], [19], [38]	Difficult when source and target images have similar visual and acquisition characteristics
Copy-move forgery	Copying and pasting regions within the same image	Duplicated blocks, repeated keypoints, similar local descriptors	Block-based, SIFT/ORBbased, transform-domain, and deep learning methods [20], [21], [41], [42], [44], [45]	Difficult for small, smooth, rotated, scaled, or heavily compressed copied regions
Resampling	Scaling, rotation, resizing, skewing, or geometric transformation	Interpolation traces, periodic artifacts, statistical dependencies	Statistical, residual-based, constrained CNN, and multi-patch aggregation methods [22], [23], [46]–[48]	Traces may be weakened by JPEG compression, noise, or repeated post-processing
Retouching and enhancement	Sharpening, smoothing, contrast adjustment, or histogram modification	Histogram artifacts, edge changes, overshoot artifacts, local statistical changes	Histogram-based, overshoot artifact-based, CNN-based, and multipath network methods [24], [49], [50], [53], [25]	Difficult to separate malicious retouching from normal camera or social media enhancement
Inpainting	Removing or filling image regions using surrounding content or learned priors	Patch repetition, texture inconsistency, noise mismatch, boundary artifacts, abnormal high frequency traces	Exemplar-based detection, patch-based CNN, high pass FCN, transformerCNN, and feature enhancement networks [26], [28]-[32]	Modern inpainting can generate visually realistic regions with weak forensic traces

Generalization is another major limitation. There are a number of methods that are trained and

tested on the same data set or on data sets that are manipulated in a similar manner. This can lead to high performance self-reported but low reliability in the real world. This is a specific challenge for deep learning methods, as they can learn artefacts in the data instead of general manipulation traces. Thus, the ability to detect forgeries produced under different post-processing conditions, an unseen type of manipulation, and different tools should be assessed through cross-dataset evaluation.

6.5 Practical Deployment Considerations

In practical application, image forgery detection techniques should be accurate, robust, efficient in computation and explainable. A detection system is used in legal, journalistic and forensic applications, where besides the classification of an image as a forgery, it is also required to give evidence that can be understood by human analysts. Localization maps, confidence scores, and visual explanations can assist analysts in gaining knowledge of why a method deems an image suspicious.

The complexity of the computations is also relevant. Some copy-move based techniques might be costly if applied to high-resolution images, and deep learning techniques might need a high-end device to train or inference. For real time screening, a lightweight approach might be more appropriate but might compromise localization accuracy or robustness. Therefore, future systems should balance detection performance, localization quality, computational cost, and interpretability.

6.6 Summary

As seen in the comparative analysis, image forgery detection is still a challenging problem as it is caused by different types of manipulations. When the manipulation trace to be targeted is well understood, classical methods can be useful, however, if the manipulation trace is complex for post-processing, classical methods may not work. Machine learning and deep learning techniques enhance detection capability, however, they require high diversity in the datasets and training settings. The inpainting-based manipulation is extremely challenging because today it is possible to produce content which is very realistic with very poor forensic signatures. These restrictions necessitate a specific inpainting-based forgery detection discussion and ongoing research challenges in the next section.

Although Table 4 compares broad detection strategies, recent studies have increasingly focused on stronger localization, robustness, attention-based feature learning, and generative-editing-aware manipulation detection. Table 5 summarizes representative recent studies, including text prompt manipulation datasets, splicing and copy-move localization networks, contrast-enhancement detectors, general manipulation localization frameworks, and inpainting specific methods.

7. INPAINTING-BASED FORGERY DETECTION: RESEARCH GAP AND OPPORTUNITY

Inpainting-based manipulation has become important research direction in image forgery detection because it can be used to remove objects, hide visual evidence, or reconstruct missing regions in a visually plausible manner. Unlike copy-move forgery, where duplicated regions may be detected through repeated

patterns, or splicing, where inserted regions may introduce source inconsistencies, inpainting attempts to fill the removed area using surrounding content or learned image priors. As a result, the manipulated region may appear natural to human observers and may contain fewer obvious visual artifacts. A general workflow for inpainting-based forgery detection is shown in Fig. 5.

7.1 Role of Inpainting in Image Manipulation

Image inpainting was originally developed for image restoration, object removal, and completion of missing or damaged regions. Classical exemplar-based inpainting methods fill missing areas by propagating patches from surrounding regions into the target region [27]. Although these methods can produce visually acceptable results, they may introduce repeated patches, disconnected structures, unnatural boundaries, or texture inconsistencies. Early forensic methods exploited these traces to detect object removal and exemplar-based inpainting manipulation [26], [28]

. With the development of deep learning, inpainting methods have become more realistic. Context encoders introduced learning-based image completion by predicting missing regions from surrounding context [54]. Later methods used deep generative models and advanced image completion strategies to produce more visually coherent results [55]-[57]. These developments make inpainting useful for legitimate restoration tasks, but they also increase the risk of misuse in image forgery. When an object is removed and the missing area is filled realistically, the manipulation may be difficult to detect using traditional forensic traces alone.

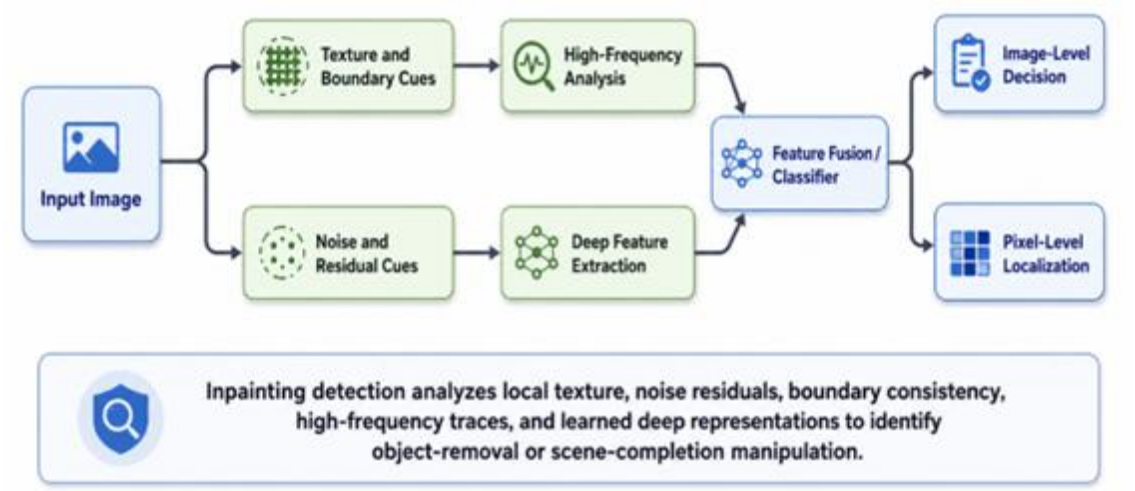

Fig. 5. General workflow of inpainting-based forgery detection. The input image is analyzed through forensic cues such as texture inconsistency, noise residuals, boundary artifacts, high-frequency traces, and learned deep features to detect and localize manipulated regions [26], [28]-[32]

Table 4 Comparison of major detection strategies in image forgery detection

Detection Strategy	Basic Idea	Strengths	Weaknesses	Typical Applications
Active methods	Verify embedded or generated authentication information	Strong verification when acquisition pipeline is controlled	Cannot be applied when no watermark, signature, or secure acquisition information exists	Watermarking, digital signatures, secure cameras [15]-[17]
Handcrafted passive methods	Detect manually designed forensic traces	Interpretable and effective for specific manipulation traces	Limited robustness under complex post-processing and unseen manipulations	Copy-move, splicing, resampling, enhancement detection [18], [20], [22], [24]
Machine learning methods	Use extracted features with supervised classifiers	Better discrimination than purely rule-based methods	Strongly dependent on feature design and training data	Splicing, copy-move, inpainting, and enhancement detection [19], [38], [58]
Deep learning methods	Learn forensic features directly from image data	Strong representation learning and localization capability	Requires large and diverse datasets; may suffer from poor cross-dataset generalization	Splicing, copy-move, and inpainting localization [19], [29]-[32]
Hybrid methods	Combine handcrafted cues, learning models, or multiple forensic traces	Can improve robustness by using complementary evidence	More complex and may require careful design and validation	General forgery detection and localization [44], [45], [32]

7.2 Forensic Traces Introduced by Inpainting

While today, there are in-painting techniques which can produce convincing content, they can leave behind forensic remnants. These traces may be found at several different levels. Locally, inpainted areas can have erratic texture continuity or repeated patches or boundary artifacts. The manipulated region can have inconsistencies of noise distribution, high frequency noise or residual noise patterns at the statistical level. The filled region may seem reasonable at the semantic level, but may have inconsistencies with the geometry of the scene, the structure of objects or the relationships among them. The traditional inpainting detection methods were primarily based on patch similarity and structural inconsistencies. For instance, exemplar-based object removal may lead to duplicated or disconnected patches that

may be detected by comparing the local image blocks [26, 28]. Deep learning-based detectors, however, attempt to learn more subtle features from manipulated images. Patch-based CNN models, highpass fully convolutional networks, transformer-CNN models, and feature enhancement networks have been proposed to detect or localize inpainted regions [29]-[32]. These methods show that learning-based models can capture manipulation traces that are difficult to design manually.

Table 5 Recent deep learning, attention-based, and generative-editing-aware studies relevant to image forgery detection and localization

Study / Year	**Forgery focus**	**Core idea**	**Evaluation focus**	**Main limitation / concern**
AutoSplice [59], 2023	Text-prompt local manipulation	DALL-E2-based automatic masked-region generation guided by text prompts; dataset for detection and localization.	Evaluates whether existing forensic models generalize to language-image generated manipulations.	Focused on DALL-E2-style manipulations; broader generative editing tools still require testing.
Feature enhancement and supervised contrastive learning [60], 2023	Splicing	Multi-level multi-scale feature enhancement and pixel-level supervised contrastive learning for forged-region localization.	Multi-scale splicing localization under noise and JPEG compression.	Mainly designed for splicing; broader manipulation generalization remains limited.
ZGS-based contrast enhancement detection [61], 2023	Contrast enhancement / retouching	Uses zero-gap spans as fingerprints to detect gamma correction, histogram equalization, and modified histogram equalization.	Image-level and patch-level detection of contrast enhancement manipulation.	Focused on contrast enhancement; does not address semantic local manipulation.
TruFor [62], 2023	General local forgery	Fuses RGB information and Noiseprint++ using a transformer-based framework to generate localization, integrity, and confidence maps.	Evaluated on cheapfakes, deepfakes, and varied local manipulations across several datasets.	More complex than lightweight detectors; deployment may require computational trade-offs.
D-Net [63], 2024	Splicing	Uses a dual-encoder structure combining	Pixel-level splicing	Designed mainly for splicing; not directly

		learned image fingerprints and fixed structural information, followed by global feature extraction.	localization on CASIA, Columbia, NIST'16, and Fantastic Reality datasets with robustness tests.	suitable for copy-move or removal forgeries.
CAMU-Net [64], 2024	Copy-move	Uses hierarchical feature extraction, feature matching, coordinate attention, and multi-scale feature-fusion upsampling.	Copy-move detection on CASIA V2, COVERAGE, and JPEG-compressed copy-move datasets.	Performance may depend on copied-region scale, transformation, and post-processing.
Similarity-based positional attention model [65], 2024	Copy-move	Uses lightweight MultiResUNet with similarity-based positional attention to locate duplicated regions.	Evaluated on CoMoFoD, COVERAGE, CASIA v2, and MICC-F600.	Patch-based attention may struggle with circular, irregular, very small, or highly complex forged regions.
Semi-supervised cropped-image detection [66], 2024	Cropping	Uses a teacher-student semi-supervised framework trained with a small labeled set and larger unlabeled data.	Cropped-image detection on BOSSbase, Alaska, and related cropped datasets.	Addresses cropping rather than classical splicing, copy-move, or inpainting localization.
Pixel-Inconsistency Modeling [67], 2024	General manipulation localization	Models global and local pixel dependencies using masked self-attention, difference convolution, feature fusion, and pixel-inconsistency augmentation.	Benchmarks 16 models across 12 datasets and evaluates robustness to unseen perturbations and AIGC manipulations.	Strong but complex; depends on careful training and multi-dataset validation.
Few-shot recaptured image detection [68], 2025	Recapturing / anti-forensics	Uses few-shot learning with multi-scale feature fusion and attention to detect recaptured images	Recaptured-image detection under limited-sample settings.	Recapturing is related to forensics but is not the central manipulation type in this review.

		with limited labeled data.		
Deep PatchMatch and pairwise ranking learning [69], 2025	Copy-move	Uses deep cross-scale PatchMatch for source-target matching and pairwise ranking for source/target discrimination.	Copy-move detection under challenging cloned-region and background-copy scenarios.	Computational cost and copy-move focus limit its use as a universal detector.
DeFI-Net [70], 2025	Inpainting	Uses dense feature interaction, multi-level feature fusion, edge guidance, and adaptive spatial weighting for inpainting localization.	Inpainting localization across seven inpainting datasets, including traditional and deep-learning-based inpainting.	Focused on inpainting; should be combined with broader detectors for mixed manipulation scenarios.
PeCA-DCNN [71], 2025	General forged/genuine classification	Combines pre-trained feature extraction with Pelican search optimization and adaptive self-boosted DCNN classification.	Image-level forged/genuine classification.	Less aligned with pixel-level localization and generative editing analysis.

Note: AIGC: artificial intelligence-generated content; ALASKA: steganalysis challenge dataset; AUC: area under the curve; BOSSbase: Break Our Steganographic System database; CAMU-Net: coordinate attention and multi-scale feature-fusion U-Net; CASIA: Chinese Academy of Sciences Institute of Automation; CNN: convolutional neural network; CoMoFoD: Copy-Move Forgery Dataset; COVERAGE: Copy-Move Forgery Database; DCNN: deep convolutional neural network; DeFI-Net: Dense Feature Interaction Network; D-Net: dual-encoder network; FCN: fully convolutional network; JPEG: Joint Photographic Experts Group; MICC: Media Integration and Communication Center; MICC-F600: MICC copy-move forgery dataset (600 images); NIST: National Institute of Standards and Technology; PeCA-DCNN: Pelican-search-optimized adaptive self-boosted DCNN; RGB: red-green-blue; U-Net: U-shaped convolutional neural network; ZGS: zero-gap spans.

7.3 Existing Inpainting Detection Approaches

Existing inpainting forgery detection methods can be grouped into three main categories: patch-based forensic methods, handcrafted or machine learning-based methods, and deep learning-based localization methods. Patch-based forensic methods are mainly designed for exemplar-based inpainting. These techniques apply to the search for repeated patches, or for

structural discontinuities from object removal, and abnormal block similarity [26], [28]. The benefits of their use is that they are interpretable, and that the detected traces can be sometimes associated with the inpainting process. But they are less effective for the modern deep inpainting techniques, where the content generated may not be easily detectable as duplication of a patch.

Handcrafted and machine learning techniques employ features like texture descriptors, gradient features, co-occurrence statistics, and local binary patterns that are used to distinguish between authentic and manipulated regions. Although these methods are more effective in detection than purely rules based methods, they are highly reliant on feature design and the type of inpainting technique applied to create the forgery.

Deep learning based techniques are gaining significance for detecting inpainting, as they can learn the manipulation traces directly from the data. A CNN-based patch-based method has been employed in the identification of inpainted regions [29]. There have been suggestions to use high-pass fully convolutional networks to focus on manipulation traces and localize the regions where deep inpainting should be performed [30]. Local and contextual features are used in combination to detect subtle inpainting artifacts with the help of transformer-CNN networks and feature enhancement networks [31] and [32]. But these approaches still need to be trained on a wide range of data and validated on various inpainting tools and data sets.

7.4 Current Limitations

In spite of the advances, forgery detection based on inpainting is still constrained in a number of aspects. First, many methods are tested using controlled data sets in which masks, regions of object removal or inpainting procedures are not defined. Does not accurately reflect actual editing practices. Second, the deep learning detectors might be trained to learn artifacts of inpainting method, thus making it less generalizable to untrained inpainting tools. Third, high frequency forensic information can be degraded during post-processing steps like JPEG compression, resizing, smoothing, and social media recompression. Fourth, small inpainted areas are hard to identify as they might exhibit only partial characteristics of the manipulation. Last but not least, pixel-level localization is still difficult if there is a smooth or coherent transition between real and generated content.

In Table 6, we list representatives of the various detection approaches for inpainting, from classical patch-based to deep learning, transformer enhanced, diffusion-aware, and text-based manipulation methods. This comparison makes the point that existing tools for patch repetition and boundary artefacts detection are not suitable for handling inconsistencies at a feature level which are more subtle than these.

7.5 Research Opportunity

A key challenge of inpainting based forgery detection is to devise methods that are applicable to multiple inpainting algorithms, inpainting datasets, mask shapes, image resolutions and post-processing settings. Future detectors should be able to extract more general artifacts, including inconsistencies in noise residuals, boundary continuity, high-frequency statistics, texture synthesis and semantic structure. The other direction is to incorporate image-level

detection with pixellevel localization to be able to say whether an image is forged and what is being manipulated. There should also be improved evaluation protocols for inpainting detection. The detector should be evaluated with several data sets, various inpainting techniques and postp-rocessing procedures. It also should report detection and localization performance. Failing to evaluate can mean that high performance on

Table 6 Summary of inpainting-based forgery detection approaches

Approach	**Main Detection Cue**	**Representative Methods**	**Strengths**	**Limitations**
Patch-based detection	Repeated patches, block similarity, disconnected structures	Exemplar-based inpainting detection [26], [28]	Interpretable and effective for classical object removal	Weak against modern deep inpainting methods
Handcrafted feature-based detection	Texture, gradient, co-occurrence, and local statistical features	Feature-based inpainting forensics [58]	Does not require very large training datasets	Depends strongly on feature quality and manipulation type
CNN-based detection	Learned local manipulation traces	Patch-based CNN and high-pass FCN methods [29], [30]	Better feature learning and localization ability	May learn dataset-specific or method-specific artifacts
Transformer-CNN and attention enhanced networks	Local and contextual manipulation features	Transformer-CNN and feature enhancement networks [31], [32]	Improved modeling of subtle and contextual traces	Requires diverse data and careful cross-dataset validation
Diffusion / generative inpainting localization	Multi-scale semantic traces, weak boundary artifacts, and feature-level inconsistency	DeFI-Net and related inpainting-localization networks [70]	More suitable for modern inpainting where copied patches or obvious boundaries are absent	Requires diverse inpainting datasets and cross-model evaluation
Text-prompt local manipulation detection	Language-image generated local edits, semantic consistency, and weak forensic traces	AutoSplice and generative-editing benchmarks [59]	Addresses emerging text-guided local manipulation produced by language-image models	Still limited by the specific generative model and prompt distribution used to create the dataset

Table 7 How generative editing weakens classical forensic assumptions and motivates future detection

Manipulation type	**Classical forensic assumption**	**Why generative editing weakens this assumption**	**Needed future direction**	**Manipulation type**
Splicing	Inserted regions often contain source mismatch, boundary inconsistency, or camera-response differences.	Modern harmonization and generative filling can reduce visible boundary and color inconsistencies.	Combine low-level fingerprint analysis with semantic and contextual inconsistency modeling.	Splicing
Copy-move	Duplicated regions create repeated blocks, keypoints, or strong visual similarity.	Post-processing, scaling, rotation, and background-copy scenarios can weaken explicit matching cues.	Use explicit matching with learned features, attention, and source-target discrimination.	Copy-move
Retouching / enhancement	Histogram gaps, edge changes, overshoot artifacts, or contrast traces reveal enhancement.	Mild enhancement can resemble normal camera or social-media processing, making intent difficult to infer.	Develop context-aware enhancement detection that separates malicious retouching from routine processing.	Retouching / enhancement
Inpainting	Removed regions may leave patch repetition, unnatural texture, or boundary artifacts.	Deep and diffusion-based inpainting can synthesize visually consistent regions with weak repeated-patch evidence.	Use dense multi-level feature interaction, boundary-aware learning, and cross-model inpainting benchmarks.	Inpainting
Text-prompt local editing	Manual local manipulation often leaves detectable editing artifacts or	Language-image models can generate semantically plausible local	Build text-guided manipulation datasets and evaluate detectors on unseen	Text-prompt local editing

	inconsistent composition.	edits that match scene style and lighting.	generative editing tools.	
General manipulation localization	A detector trained on one dataset can learn transferable manipulation traces.	Dataset-specific artifacts and model-specific generation traces reduce cross-dataset reliability.	Prioritize cross-dataset testing, perturbation robustness, confidence maps, and explainable localization.	General manipulation localization

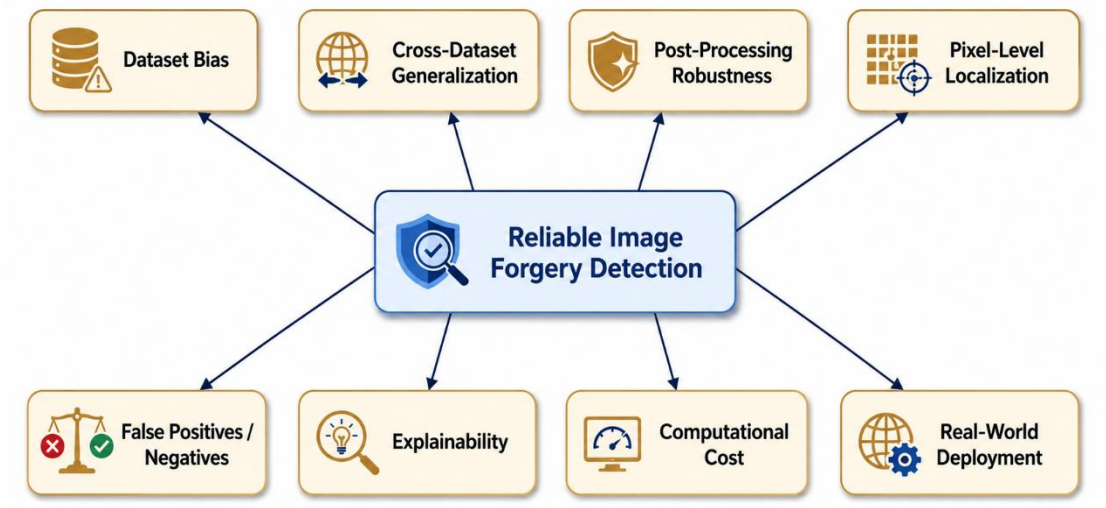

Fig. 6. Summary of major open challenges in image forgery detection, including dataset bias, cross-dataset generalization, robustness against post-processing, pixel-level localization, false detections, explainability, and practical deployment.

one data set does not necessarily mean that the system will be reliable in real-world applications. In conclusion, inpainting forgery detection is an important area of digital image forensics that should be investigated in the near future.

The limitations discussed above suggest that the main difficulty is not only detecting whether an image has been manipulated, but also understanding how modern generative editing changes the forensic traces left by manipulation. Compared with traditional splicing,

copy-move, or exemplar-based inpainting, text-guided and diffusion-assisted editing can generate visually coherent regions that reduce obvious boundary, texture, and duplication artifacts. Table 7 summarizes this shift by linking classical forensic assumptions to the

challenges introduced by generative editing and the future directions required for robust detection.

Overall, the transition from manual editing to generative manipulation suggests that future detectors should be evaluated not only by detection accuracy, but also by cross-dataset generalization, localization reliability, robustness to post-processing, and performance on unseen generative editing tools.

8. CHALLENGES AND OPEN ISSUES

Despite image forensics evolving from traditional manual techniques to machine and deep learning-based methods, many challenges still exist in this area that need to be addressed. Such challenges pose problems for the effectiveness of existing techniques in practical use cases when images have been altered through compression, resizing, post-processing, or manipulation by modern editing software. Some of the key challenges include the ones regarding dataset constraints, generalizability, robustness, localization, explainability, and deployment. The major open challenges identified from the reviewed literature are summarized in Fig. 6.

8.1 Dataset Bias and Limited Diversity

Public datasets have played an important role in the development of image forgery detection methods. However, there are many databases that can be constrained either in the kind of manipulation performed, in the type of images used, in the resolution and compression ratios, or even in the way annotations were created [11]-[14]. Therefore, techniques developed using one database may learn from peculiarities in this database, rather than learning forensic information in general.

It will be a huge challenge if an algorithm demonstrates good performance on benchmark images but is unable to perform well with real-life images. Real-life images can be captured using various cameras, from different social media platforms, using various editing software, at different resolutions, and with different compression techniques. In case a data set does not have such diversity, then chances are that the performance of the algorithm will overstate its practical reliability. Therefore, future datasets should offer more realistic manipulation pipelines, different sources for images, and different compression levels.

8.2 Cross-dataset Generalization

The major limitation of all current forgery detection techniques is cross-dataset generalization. A detector trained on one dataset cannot operate on another dataset due to differences between datasets in terms of image properties, manipulations used, and post-processing techniques. This challenge is relevant mainly for deep learning-based solutions because such models have a tendency to extract dataset-specific features rather than manipulation-invariant cues.

Another reason why generalization is problematic is that different forgery types create different artifacts. For instance, a model specialized in detecting copy-move forgery does not work for detecting splicing or inpainting. Likewise, a detector designed to operate on classical inpainting techniques will not be able to deal with deep inpainting. Thus, for evaluating forgery detectors it is necessary to use multiple datasets, forgery types, and post-processing

techniques.

8.3 Robustness against Post-processing

In practice, images from the real world may have to be post-processed prior to forensic analysis. Typical uses include compressing images in JPEG format, resizing, rotating, blurring, sharpening, adjusting contrast and adding noise. These operations may obliterate or impair manipulation trace. For instance, inpainting trace may be lost due to smoothing and recompression, copy-move similarity may be more difficult to match when the image is rotated or scaled, and compression may mask the presence of resampling artifacts [22], [23], [26], [29].

The robustness is particularly important because many forged images are distributed over the Internet, where resizing and recompression of images are common features. Hence, the detector should be able to maintain its reliability despite undergoing several stages of image processing. Therefore, its practical detector should be reliable even when the image goes through multiple stages of processing. Current techniques generally claim to perform well in realistically controlled environments, but the performance is not always robust in real social media or post-processing environments.

8.4 Pixel-level Localization

There are many applications in forensic science where image-level detection is not sufficient. In scientific image verification, legal evidence or journalism, it is sometimes essential to point to a specific manipulated area. The level of localization is pixel-level, which gives more forensic evidence as it indicates the location where the image was changed. But localization is harder than classification, since the detector has to correctly differentiate between manipulated and authentic regions.

Localization is particularly difficult when the area to be manipulated is small, the boundary is smooth, or the content being forged is similar to the surrounding content visually. Inpainting-based manipulation is a straightforward instance of this problem since current inpainting techniques can efficiently fill in missing area with realistic texture and structure [30]-[32]. Hence, future methods need to measure the image-level detection and pixel-level localization performance besides just classification accuracy.

8.5 False Positives and False Negatives

One of the major problems in image forgery detection is false detections. A false positive is when a genuine image is misidentified as a fake image, and a false negative is when a fake image is misrecognized as a genuine image. Both situations are troublesome. Misidentifications can undermine the credibility of the primary source of visual information, and a failure to identify can allow manipulated information to proliferate unchecked.

It tends to generate false positives when the images are processed into images that are normal but have been altered by some image processing functions like sharpening, contrast stretching, resizing or compression and are confused for malicious images. Manipulation traces, especially if weak, can be removed by post processing, or created by advanced editing tools, which result in false negatives. Hence, a detection system capable of accurately detecting

a target under realistic conditions should use minimal false alarms and minimize missed detections as well as maximize the accuracy.

8.6 Explainability and Forensic Reliability

Many algorithms with deep learning are black-box models. They might produce high accuracy on benchmark data, but it is hard to determine on which forensic traces they rely to make decisions. A severe drawback for legal, journalistic and forensic applications, where interpretation and defensibility are crucial. Sometimes a detection result with no explanation may not be enough for human analysts to corroborate or provide evidence.

Maps of the localization, confidence score, and clues to explain why an image is a manipulated image should be included in the explanation of a forensic system. These explanations can help analysts to distinguish between real manipulation traces and other normal image processing features. So, explainability should be considered as a key requirement and not just an optional one.

8.7 Computational Cost and Practical Deployment

In practice, the tradeoff is between accuracy, robustness, localization quality and computational costs. The traditional ones are computationally heavy, particularly in case of high resolution images for BDCMD. These deep learning algorithms can be demanding in terms of computing resources and data sets needed to train them. These requirements may restrict deployment for real-time monitoring, mobile or large scale online applications.

Any system of forgery detection should be efficient enough to be used on a large scale for screening and still reliable in its ability to localize the forgery and explain it. A light-weight model can be employed for initial screening, and a more complex forensic model could be used for suspicious images and detailed analysis. This multi-layer approach might be more practical than looking for a one-size-fits-all detector.

8.8 Summary of Open Challenges

Table 8 summarizes the main challenges in image forgery detection and their impact on practical forensic reliability. These challenges show that image forgery detection is not solved by high accuracy on a single benchmark dataset. Reliable forensic systems require diverse datasets, robust evaluation protocols, interpretable decisions, and strong generalization across manipulation types and real-world post-processing conditions

9. FUTURE RESEARCH DIRECTIONS

The challenges discussed in the previous section show that image forgery detection still requires significant improvement before it can be considered reliable for real-world forensic use. Future research should move beyond high accuracy on individual benchmark datasets and focus on robustness, generalization, localization, explainability, and practical deployment. This section summarizes important future directions for improving image forgery detection systems..

Table 8 Major challenges and open issues in image forgery detection

Challenge	Main Cause	Impact	Required Direction
Dataset bias	Limited manipulation types, image sources, and annotation formats	Weak real-world reliability and overestimated benchmark performance	More diverse datasets with realistic manipulation workflows
Cross-dataset generalization	Dataset-specific artifacts and training bias	Poor performance on unseen datasets and editing tools	Multi-dataset training and cross-dataset evaluation
Post-processing robustness	Compression, resizing, blurring, sharpening, and recompression	Loss or weakening of forensic traces	Robust detectors evaluated under realistic processing pipelines
Pixel-level localization	Small manipulated regions and smooth boundaries	Weak forensic evidence when only image-level labels are reported	Joint detection and localization with reliable ground-truth masks
False detections	Confusion between normal processing and malicious manipulation	False alarms or missed forgeries	Balanced evaluation using false positive and false negative analysis
Explainability	Black-box behavior of deep models	Limited trust in legal and forensic use	Interpretable localization maps and confidence-based evidence

9.1 Development of more Diverse Benchmark Dataset

Future datasets should include more diverse image sources, manipulation types, resolutions, compression levels, and post-processing conditions. Existing datasets such as CASIA, CoMoFoD, IMD2020, and MFC have supported important progress, but they do not fully cover the wide range of manipulations found in real-world images [12]-[14], [36]. New datasets should include mixed manipulation scenarios, realistic editing workflows, and high-quality ground-truth masks for pixel-level localization. Images uploaded via social media and online platforms should also be taken into account when developing datasets because they are likely to be compressed, resized, and stripped of metadata.

The presence of such conditions would allow researchers to assess whether or not a method is reliable after being used in the real world. However detection methods can be good in the lab, but poor in real forensic situations if they are not tested with a diverse set of datasets.

9.2 Standardized Evaluation Protocols

One of the drawbacks of the literature is the absence of a standard evaluation protocol. This makes it difficult to compare the results of different studies as they rely on different datasets, different train-test splits, different manipulation settings, and different performance metrics. Standardized evaluation setups with image-level and pixel-level detection and localization results are desired.

When the detection is done at the image level (image classification), accuracy, precision, recall, F-score, true positive rate, false positive rate, and AUC are good parameters to report. If ground-truth masks are available, then pixel-level or region-level overlap should be added for localization. Further, robustness tests should be conducted with typical post processing operations, for example JPEG compression, resizing, rotation, blurring, sharpening and noise addition. No method is reliable if it works well on one data set only.

9.3 Improved Cross-dataset Generalization

Methods should be tested on several datasets to quantify their generalizability to the test data. This is particularly true of deep learning methods, where models can learn artifacts from the dataset rather than general manipulation traces. This detector should be tested with other datasets with other image sources, manipulation tools and post-processing conditions.

In order to better generalize, future models should be trained on manipulation-independent forensic cues like noise inconsistency, boundary artifacts, high-frequency residuals, texture discontinuity and semantic inconsistency. Multiple training sets, multiple manipulation techniques and realistic post-processing pipelines can help lower the training dataset bias and increase the reliability in the real world.

9.4 Robust Inpainting-based Forgery Detection

The manipulation based on inpainting should be given more specific attention since it may be able to remove an object and reconstruct missing areas in a plausible manner. While classical exemplar-based inpainting may generate repetitive patches or structural artifacts, learning-based inpainting techniques may generate more realistic results, as shown in [26]–[30]. Hence, future detectors should not rely solely on the obvious duplication of patches or the existence of boundary artifacts.

In future, the inpainting detector should combine multiple forensic features, such as the noise residuals, frequency domain inconsistencies, texture continuity and semantic plausibility. They should also be compared with various inpainting techniques, mask configurations, object size and compression level. A good inpainting detector needs to be able to detect the classical object removal and more advanced deep inpainting manipulation.

9.5 Multi-modal and Multi-cue Forensic Analysis

Typically, one forensic clue is not enough to detect forgery. Future systems should integrate several types of evidence, including the content of the image, noise residuals, compression artifacts, metadata, consistency of illumination, and semantic relationships. This kind of multi-cue analysis can enhance the robustness of the technique, since the traces produced by different manipulation methods can be different.

There is also the possibility of using multimodal analysis to help in practical verification. For location maps, for example, the manipulated region can be identified and for image level detection it is determined whether the image is suspicious. The source of the photo or the steps in the photo's production process might be recorded in other evidence, including metadata, acquisition-related traces, etc. The combination of these cues may result in more accurate forensic conclusions than if only one detector is used.

9.6 Explainable Forensic Artificial Intelligence

In the legal, journalistic and forensic applications, the requirement for explainability should be an integral part of image forgery detection. The models in deep learning can give good classification performance but the decision may be challenging to interpret. A forensic system ought to offer extra than a faux or real label. It should describe the area in question and evidence that supports this decision.

Future methods should include localization maps, confidence levels and interpretable forensic cues. These outputs can be used by human analysts to verify the output and minimize the blind use of black box models. It is also important for explainable systems to reduce false positives which can be checked by the analyst as whether the traces detected are from malicious manipulation or normal image processing.

9.7 Lightweight and Practical Detection Systems

For real world deployment, there needs to be accurate methods with low computational costs. Large deep learning models can be beneficial for in-depth forensic analysis but can also be challenging to implement in real-time systems, mobile devices, and large-scale online platforms. Other lightweight models which are efficient in screening but with acceptable detection and localization performance should be investigated in the future.

One possible solution is a phased detection system. A lightweight detector can initially filter out a lot of images and be able to identify images that are suspect. Those cases can then be used to create more detailed localization and explanation with more complex forensic models. This would be a compromise between cost and accuracy and forensically reliable.

9.8 Summary

Having more powerful datasets, uniform evaluation, cross-dataset testing, and powerful inpainting detection, multimodal forensic analysis, explainable models, and practical deployment strategies are essential for future image forgery detection advancements. The field should no longer be based on benchmark approach, but include a more realistic manipulation and post-processing. The provided directions are crucial for creating effective and

dependable image forgery detection systems, which can play a vital role in digital forensics, media verification, and information security.

10. CONCLUSION

Image forgery detection is of paramount concern in digital image forensics, as falsified images can have a significant influence on journalistic work, legal evidence, public trust, and information security. This paper discussed the various methods of image forgery detection such as active approach, handcrafted approach, machine learning approach, deep learning approach and inpainting based approach. Datasets for the public image forgery detection were also discussed, highlighting their use for benchmarking image forgery detection and localization. The review demonstrates that there are different types of forensic traces of a forgery. These inconsistencies arise from the discrepancy between the spliced region and the host region in image splicing, the duplication of structures in the same image in case of copy-move forgery, the interpolation artifacts generated in resampling, the changes made in the local statistics of the image in case of retouching and the visually plausible image content generated through inpainting-based manipulation. Therefore, there does not exist one detection technique applicable for all forms of image manipulations. The comparative analysis has revealed that even in the modern times, the techniques used for the detection of image forgery still have several weaknesses including dataset bias, weak generalization between datasets, post-processing dependency, false detections, low localization accuracy, and lack of explainability. All these shortcomings are especially critical in the context of forgery detection using deep learning and inpainting as some techniques having very high performance in benchmarks fail in detecting the manipulation in practice. For future research, emphasis must be placed on diverse datasets, evaluation methodologies, robust cross-dataset tests, inpainting detection, multimodal forensics, explainable models and lightweight solutions. This progress will be key for developing reliable techniques of image forgery detection.

11. REFERENCES

[1] H. Luo and J. H. Mortimer, “Copyright infringement in the market for digital images,” Am. Econ. Rev., vol. 106, no. 5, pp. 140–145, May 2016, doi: 10.1257/aer.p20161017.

[2] C. Shen, M. Kasra, W. Pan, G. A. Bassett, Y. Malloch, and J. F. O’Brien, “Fake images: The effects of source, intermediary, and digital media literacy on contextual assessment of image credibility online,” New Media Soc., vol. 21, no. 2, pp. 438–463, Feb. 2019, doi: 10.1177/1461444818799526.

[3] D. Spohr, “Fake news and ideological polarization: Filter bubbles and selective exposure on social media,” Bus. Inf. Rev., vol. 34, no. 3, pp. 150–160, Sep. 2017, doi: 10.1177/0266382117722446.

[4] E. Goldman, “The complicated story of FOSTA and Section 230,” First Amendment Law Review, vol. 17, p. 279, 2018.

[5] V. Schetinger, M. M. Oliveira, R. da Silva, and T. J. Carvalho, “Humans are easily fooled by digital images,” Comput. Graph., vol. 68, pp. 142–151, Nov. 2017, doi: 10.1016/j.cag.2017.08.010.

[6] M. Verma and D. Singh, "Survey on image copy-move forgery detection," Multimed. Tools Appl., Aug. 2023, doi: 10.1007/s11042-023-16455-x.

[7] H. Farid, "Digital doctoring: How to tell the real from the fake," Significance, vol. 3, no. 4, pp. 162–166, Dec. 2006, doi: 10.1111/j.1740-9713.2006.00197.x.

[8] B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When seeing isn't believing [multimedia authentication technologies]," IEEE Signal Process. Mag., vol. 21, no. 2, pp. 40–49, Mar. 2004, doi: 10.1109/MSP.2004.1276112.

[9] A. Gokhale, P. Mulay, D. Pramod, and R. Kulkarni, "A bibliometric analysis of digital image forensics," Sci. Technol. Libr., vol. 39, no. 1, pp. 96–113, Jan. 2020, doi: 10.1080/0194262X.2020.1714529.

[10] F. Casino et al., "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," IEEE Access, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[11] T. Gloe and R. Böhme, "The 'Dresden Image Database' for benchmarking digital image forensics," in Proc. 2010 ACM Symp. Appl. Comput. (SAC '10), New York, NY, USA: ACM, Mar. 2010, pp. 1584–1590, doi: 10.1145/1774088.1774427.

[12] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in 2013 IEEE China Summit Int. Conf. Signal Inf. Process., Jul. 2013, pp. 422–426, doi: 10.1109/ChinaSIP.2013.6625374.

[13] D. Tralić, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—New database for copy-move forgery detection," in Proc. ELMAR-2013, Sep. 2013, pp. 49–54. [DOI not provided.]

[14] A. Novozamsky, B. Mahdian, and S. Saic, "IMD2020: A large-scale annotated dataset tailored for detecting manipulated images," in 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW), 2020, pp. 71–80.

[15] G. L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," IEEE Trans. Consum. Electron., vol. 39, no. 4, pp. 905–910, Nov. 1993, doi: 10.1109/30.267415.

[16] M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. CRC Press, 2004.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[18] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. de Rezende Rocha, "Exposing digital image forgeries by illumination color classification," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 7, pp. 1182–1194, Jul. 2013, doi: 10.1109/TIFS.2013.2265677.

[19] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in 2016 IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2016, pp. 1–6, doi:

10.1109/WIFS.2016.7823911.

[20] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," J. Vis. Commun. Image Represent., vol. 29, pp. 16–32, May 2015, doi: 10.1016/j.jvcir.2015.01.016.

[21] N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab, N.-S. N. Ismail, and R. Salleh, "A comprehensive evaluation procedure for copy-move forgery detection methods: Results from a systematic review," Multimed. Tools Appl., vol. 81, no. 11, pp. 15171–15203, May 2022, doi: 10.1007/s11042-022-12010-2.

[22] H. C. Nguyen and S. Katzenbeisser, "Robust resampling detection in digital images," in Communications and Multimedia Security, B. De Decker and D. W. Chadwick, Eds., Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2012, pp. 3–15, doi: 10.1007/978-3-642-32805-3_1.

[23] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in 2017 IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), Mar. 2017, pp. 2152–2156, doi: 10.1109/ICASSP.2017.7952537.

[24] X. Lin, C.-T. Li, and Y. Hu, "Exposing image forgery through the detection of contrast enhancement," in 2013 IEEE Int. Conf. Image Process. (ICIP), Sep. 2013, pp. 4467–4471, doi: 10.1109/ICIP.2013.6738920.

[25] W. Shan, Y. Yi, R. Huang, and Y. Xie, "Robust contrast enhancement forensics based on convolutional neural networks," Signal Process. Image Commun., vol. 71, pp. 138–146, Feb. 2019, doi: 10.1016/j.image.2018.11.011.

[26] Q. Wu, S.-J. Sun, W. Zhu, G.-H. Li, and D. Tu, "Detection of digital doctoring in exemplar-based inpainted images," in 2008 Int. Conf. Mach. Learn. Cybern., Jul. 2008, pp. 1222–1226, doi: 10.1109/ICMLC.2008.4620591.

[27] A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting," IEEE Trans. Image Process., vol. 13, no. 9, pp. 1200–1212, Sep. 2004, doi: 10.1109/TIP.2004.833105.

[28] Z. Liang, G. Yang, X. Ding, and L. Li, "An efficient forgery detection algorithm for object removal by exemplar-based image inpainting," J. Vis. Commun. Image Represent., vol. 30, pp. 75–85, Jul. 2015, doi: 10.1016/j.jvcir.2015.03.004.

[29] X. Zhu, Y. Qian, X. Zhao, B. Sun, and Y. Sun, "A deep learning approach to patch-based image inpainting forensics," Signal Process. Image Commun., vol. 67, pp. 90–99, Sep. 2018, doi: 10.1016/j.image.2018.05.015.

[30] H. Li and J. Huang, "Localization of deep inpainting using high-pass fully convolutional network," in 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 2019, pp. 8300–8309.

[31] X. Zhu, J. Lu, H. Ren, H. Wang, and B. Sun, "A transformer–CNN for deep image inpainting forensics," Visual Computing, vol. 39, no. 10, pp. 4721–4735, Oct. 2023, doi:

10.1007/s00371-022-02620-0.

[32] Y. Zhang, Z. Fu, S. Qi, M. Xue, Z. Hua, and Y. Xiang, "Localization of inpainting forgery with feature enhancement network," IEEE Trans. Big Data, vol. 9, no. 3, pp. 936–948, Jun. 2023, doi: 10.1109/TBDATA.2022.3225194.

[33] Y.-F. Hsu and S.-F. Chang, "Camera response functions for image forensics: An automatic algorithm for splicing detection," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 4, pp. 816–825, Dec. 2010, doi: 10.1109/TIFS.2010.2077628.

[34] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 1099–1110, Sep. 2011, doi: 10.1109/TIFS.2011.2129512.

[35] D.-T. Dang-Nguyen, C. Pasquini, V. Conotter, and G. Boato, "RAISE: A raw images dataset for digital image forensics," in Proc. 6th ACM Multimedia Syst. Conf. (MMSys '15), New York, NY, USA: ACM, Mar. 2015, pp. 219–224, doi: 10.1145/2713168.2713194.

[36] H. Guan et al., "MFC datasets: Large-scale benchmark datasets for media forensic challenge evaluation," in 2019 IEEE Winter Appl. Comput. Vis. Workshops (WACVW), Jan. 2019, pp. 63–72, doi: 10.1109/WACVW.2019.00018.

[37] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 6, pp. 1841–1854, Dec. 2012, doi: 10.1109/TIFS.2012.2218597.

[38] C. Shen, Z. Shi, and H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices," IET Image Process., vol. 11, no. 1, pp. 44–53, 2017, doi: 10.1049/iet-ipr.2016.0238.

[39] B. Ahmed, T. A. Gulliver, and S. alZahir, "Image splicing detection using Mask-RCNN," Signal Image Video Process., vol. 14, no. 5, pp. 1035–1042, Jul. 2020, doi: 10.1007/s11760-020-01636-0.

[40] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Sci. Int., vol. 231, no. 1, pp. 284–295, Sep. 2013, doi: 10.1016/j.forsciint.2013.05.027.

[41] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT," Multimed. Tools Appl., vol. 77, no. 1, pp. 837–855, Jan. 2018, doi: 10.1007/s11042-016-4289-y.

[42] Y. Zhu, X. Shen, and H. Chen, "Copy-move forgery detection based on scaled ORB," Multimed. Tools Appl., vol. 75, no. 6, pp. 3221–3233, Mar. 2016, doi: 10.1007/s11042-014-2431-2.

[43] K. B. Meena and V. Tyagi, "A copy-move image forgery detection technique based on tetrolet transform," J. Inf. Secur. Appl., vol. 52, p. 102481, Jun. 2020, doi: 10.1016/j.jisa.2020.102481.

[44] A. Islam, C. Long, A. Basharat, and A. Hoogs, "DOA-GAN: Dual-order attentive

generative adversarial network for image copy-move forgery detection and localization," in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 4675–4684.

[45] Y. Zhu, C. Chen, G. Yan, Y. Guo, and Y. Dong, "AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection," IEEE Trans. Ind. Inform., vol. 16, no. 10, pp. 6714–6723, Oct. 2020, doi: 10.1109/TII.2020.2982705.

[46] T. Qiao, A. Zhu, and F. Retraint, "Exposing image resampling forgery by using linear parametric model," Multimed. Tools Appl., vol. 77, no. 2, pp. 1501–1523, Jan. 2018, doi: 10.1007/s11042-016-4314-1.

[47] A. Peng, Y. Wu, and X. Kang, "Revealing traces of image resampling and resampling antiforensics," Adv. Multimed., vol. 2017, p. 7130491, Jan. 2017, doi: 10.1155/2017/7130491.

[48] M. Lamba and K. Mitra, "Multi-patch aggregation models for resampling detection," in ICASSP 2020—2020 IEEE Int. Conf. Acoust. Speech Signal Process., May 2020, pp. 2967–2971,doi: 10.1109/ICASSP40776.2020.9053005.

[49] N. Zhu, C. Deng, and X. Gao, "Image sharpening detection based on multiresolution overshoot artifact analysis," Multimed. Tools Appl., vol. 76, no. 15, pp. 16563–16580, Aug. 2017, doi: 10.1007/s11042-016-3938-5.

[50] G. Cao, Y. Zhao, R. Ni, and A. C. Kot, "Unsharp masking sharpening detection via overshoot artifacts analysis," IEEE Signal Process. Lett., vol. 18, no. 10, pp. 603–606, Oct. 2011, doi: 10.1109/LSP.2011.2164791.

[51] M. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in 2008 15th IEEE Int. Conf. Image Process., Oct. 2008, pp. 3112–3115,doi: 10.1109/ICIP.2008.4712454.

[52] F. Ding, G. Zhu, J. Yang, J. Xie, and Y.-Q. Shi, "Edge perpendicular binary coding for USM sharpening detection," IEEE Signal Process. Lett., vol. 22, no. 3, pp. 327–331, Mar. 2015, doi: 10.1109/LSP.2014.2359033.

[53] Q. Wang and R. Zhang, "Double JPEG compression forensics based on a convolutional neural network," EURASIP J. Inf. Secur., vol. 2016, no. 1, p. 23, Oct. 2016, doi: 10.1186/s13635-016-0047-y.

[54] D. Pathak, P. Krähenbühl, J. Donahue, T. Darrell, and A. A. Efros, "Context encoders: Feature learning by inpainting," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 2536–2544.

[55] R. Suvorov et al., "Resolution-robust large mask inpainting with Fourier convolutions," in 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022, pp. 3172–3182.

[56] P. Shamsolmoali, M. Zareapoor, and E. Granger, "Image completion via dual-path cooperative filtering," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), Jun. 2023, pp. 1–5,doi: 10.1109/ICASSP49357.2023.10097260.

[57] R. A. Yeh, C. Chen, T. Y. Lim, A. G.

Schwing, M. Hasegawa-Johnson, and M. N. Do, "Semantic image inpainting with deep generative models," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 5485–5493.

[58] L. Shen, G. Yang, L. Li, and X. Sun, "Robust detection for object removal with post-processing by exemplar-based image inpainting," in Proc. 13th Int. Conf. Nat. Comput., Fuzzy Syst. Knowl. Discov. (ICNC-FSKD), Jul. 2017, pp. 2730–2736, doi: 10.1109/FSKD.2017.8393211.

[59] S. Jia, M. Huang, Z. Zhou, Y. Ju, J. Cai, and S. Lyu, "AutoSplice: A text-prompt manipulated image dataset for media forensics," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), 2023, pp. 893–903.

[60] Y. Xu, J. Zheng, A. Fang, and M. Irfan, "Feature enhancement and supervised contrastive learning for image splicing forgery detection," Digit. Signal Process., vol. 136, Art. no. 104005, 2023.

[61] X. Bi, Y. Shang, B. Liu, B. Xiao, W. Li, and X. Gao, "A versatile detection method for various contrast enhancement manipulations," IEEE Trans. Circuits Syst. Video Technol., vol. 33, no. 2, pp. 491–504, Feb. 2023.

[62] F. Guillaro, D. Cozzolino, A. Sud, N. Dufour, and L. Verdoliva, "TruFor: Leveraging all-round clues for trustworthy image forgery detection and localization," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), 2023, pp. 20606–20615.

[63] Z. Yang, B. Liu, X. Bi, B. Xiao, W. Li, G. Wang, and X. Gao, "D-Net: A dual-encoder network for image splicing forgery detection and localization," Pattern Recognit., vol. 155, Art. no. 110727, 2024.

[64] K. Zhao, X. Yuan, T. Liu, Y. Xiang, Z. Xie, G. Huang, and L. Feng, "CAMU-Net: Copy-move forgery detection utilizing coordinate attention and multi-scale feature fusion-based up-sampling," Expert Syst. Appl., vol. 238, Art. no. 121918, 2024.

[65] A. Roy, S. Mohiuddin, and R. Sarkar, "A similarity-based positional attention-aided deep learning model for copy-move forgery detection," IEEE Trans. Artif. Intell., vol. 5, no. 9, pp. 4354–4363, Sep. 2024.

[66] I. Hussain, S. Tan, and J. Huang, "A semi-supervised deep learning approach for cropped image detection," Expert Syst. Appl., vol. 243, Art. no. 122832, 2024.

[67] C. Kong, A. Luo, S. Wang, H. Li, A. Rocha, and A. C. Kot, "Pixel-inconsistency modeling for image manipulation localization," IEEE Trans. Pattern Anal. Mach. Intell., vol. 47, no. 6, pp. 4455–4472, 2025.

[68] I. Hussain, S. Tan, and J. Huang, "Few-shot based learning recaptured image detection with multi-scale feature fusion and attention," Pattern Recognit., vol. 161, Art. no. 111248, 2025.

[69] Y. Li, Y. He, C. Chen, L. Dong, B. Li, J. Zhou, and X. Li, "Image copy-move forgery detection via deep PatchMatch and pairwise ranking learning," IEEE Trans. Image Process., vol. 34, pp. 425–440, 2025.

[70] Y. Yao, T. Han, S. Jia, and S. Lyu, "Dense feature interaction network for image inpainting localization," IEEE Trans. Inf. Forensics Secur., vol. 20, pp. 1636–1648, 2025.

[71] E. Tripathi, U. Kumar, and S. P. Tripathi, "An efficient digital image forgery detection using Pelican search optimisation-based DCNN," J. Exp. Theor. Artif. Intell., vol. 37, no. 8, pp. 1267–1292, 2025