Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.066202

REVIEW

A Survey of Image Forensics: Exploring Forgery Detection in Image Colorization

Saurabh Agarwal[1], Deepak Sharma[2], Nancy Girdhar[3], Cheonshik Kim[4] and Ki-Hyun Jung[5,*]

[1]School of Computer Science and Engineering, Yeungnam University, Gyeongsan, 38541, Republic of Korea
[2]Department of Computer Science, Christian-Albrechts-Universität zu Kiel, Christian-Albrechts-Platz 4, Kiel, 24118, Schleswig-Holstein, Germany
[3]School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth, PL4 8AA, UK
[4]Department of Computer Engineering, Sejong University, Seoul, 05006, Republic of Korea
[5]Department of Software Convergence, Gyeongkuk National University (Andong National University), Andong, 36729, Republic of Korea

*Corresponding Author: Ki-Hyun Jung. Email: kingjung@gknu.ac.kr

Received: 01 April 2025; Accepted: 19 June 2025; Published: 30 July 2025

ABSTRACT: In today's digital era, the rapid evolution of image editing technologies has brought about a significant simplification of image manipulation. Unfortunately, this progress has also given rise to the misuse of manipulated images across various domains. One of the pressing challenges stemming from this advancement is the increasing difficulty in discerning between unaltered and manipulated images. This paper offers a comprehensive survey of existing methodologies for detecting image tampering, shedding light on the diverse approaches employed in the field of contemporary image forensics. The methods used to identify image forgery can be broadly classified into two primary categories: classical machine learning techniques, heavily reliant on manually crafted features, and deep learning methods. Additionally, this paper explores recent developments in image forensics, placing particular emphasis on the detection of counterfeit colorization. Image colorization involves predicting colors for grayscale images, thereby enhancing their visual appeal. The advancements in colorization techniques have reached a level where distinguishing between authentic and forged images with the naked eye has become an exceptionally challenging task. This paper serves as an in-depth exploration of the intricacies of image forensics in the modern age, with a specific focus on the detection of colorization forgery, presenting a comprehensive overview of methodologies in this critical field.

KEYWORDS: Image colorization; image forensic; digital image forgery; machine learning; convolutional neural network; deep learning; generative adversarial network

1 Introduction

The speedy development of editing tools in the modern period has dramatically aided the simplicity with which photos can be altered. As a result, it is now more difficult to tell the difference between real and manipulated photos. Digital images have become the prominent origin of information, attributable to not only sophistication but also accessibility [1] because of the extensive utilization of digital image forgery in diverse areas, namely military, law, medical images, media, worldwide web publications, and news photography. Other distinctive image editing techniques are available compared to traditional ones, namely image generation [2] and colorization [3]. Colorization typically involves adding plausible colors to grayscale images based on visual realism, which leads to errors when a particular object is required to be tracked. Eventually, the image generation approach typically builds a proper image out of a noise vector with or without the supplementary information, for instance, a class label. Li et al.'s [4] work is suitable for

color blind persons. They used a self-adapting recoloring strategy with an improved octree quantification method to detect significant color elements in an image adaptively. A screening platform for Color Vision Deficiency (CVD) datasets is then used to merge different recoloring methods. Through the assistance of this screening platform, a CVD dataset is constructed, containing 2313 sets of training images and 771 sets of test images. Different GANs, including pix2pix-GAN [5], Cycle-GAN [6], and Bicycle-GAN [7], are utilized for data conversion and are color-blind. Experimental results indicate that pix2pix-GAN effectively recolors unrecognizable colors for individuals with CVD, and it is predicted that this dataset will contribute to advancements in color-blind image recoloring. However, the traditional approaches can have substantial entertainment value or be utilized for other malicious purposes. For instance, the image retouching approach usually alters images using various systems. Copy-move and splicing approaches generally manipulate a part of a particular image and then perform object-level alterations.

To address the challenges above, a novel field called digital image forensics (DIF) has emerged, aiming to provide measurable evidence regarding the integrity and origin of digital images. DIF employs two distinct approaches: active and passive. The active approach involves implementing various processes, such as digital watermarking or signature embedding, to safeguard digital images against tampering [8,9]. This approach ensures that if a digital image has been tampered with, certain information cannot be extracted from it. On the other hand, the passive DIF technique is more demanding [10]. It involves authenticating and detecting the source of digital images without relying on any pre-embedded or pre-extracted information. While not applicable in every situation, the passive method offers a different approach to detecting specific instances of image tampering. This technique analyzes raw images by examining different statistical properties within the image content to identify the potential image manipulation [11,12]. A survey for forged colorized image detection (CID) is proposed by Salman et al. [13]. There are two widely used approaches to forged CID systems. The first approach utilizes traditional machine learning (ML) techniques that involve hand-crafted features extracted from the images for the discrimination of real and fake images. The second method employs deep learning (DL) methods as "end-to-end" architectures where manually designed features are not needed because the models learn them from the images directly. This work deals with different techniques and methods employed in detecting fake colorized images (CIs). The manuscript's main contribution is as follows:

- Exploration of image forensics approaches and techniques: This research paper investigates and presents an overview of existing image forensics approaches. It delves into various methods and techniques to detect image manipulations and forgeries. It offers valuable perspectives on the cutting-edge technologies employed in this domain.
- Focus on fake image colorization detection: This research paper covers general image forensics techniques and emphasizes fake image colorization detection methods. By providing a comprehensive overview of these techniques, the study addresses the growing concern of distinguishing between genuine and artificially colorized images.

The paper focuses on forgery detection methods, which are reviewed in Section 2. Moreover, other aspects of DIF are discussed in the same section. Section 3 analyzes detection approaches tailored explicitly for fake image colorization. These approaches can be broadly classified into ML-based and DL-based techniques. The section extensively explores the practicality and limitations of each category, offering valuable insights into the field. Finally, Section 4 serves as the paper's conclusion, summarizing the essential findings and limitations.

2 Digital Image Forensic Approaches

DIF examines the authenticity and integrity of images that have undergone retouching and colorization. Their other types are computer-generated images, fake images, and anti-forensic images. This involves analyzing whether some aspects of the image have been altered or enhanced, potentially to mislead viewers or present a modified version of reality. Experts in DIF use various techniques to detect and quantify the extent of retouching, helping to reveal whether the changes were legitimate or intended to deceive. CIs are scrutinized in DIF to ensure that adding color to a black-and-white or grayscale image has been carried out accurately and consistently. By analyzing color distribution, matching hues in the intended context, and assessing the overall coherence of colors, forensic experts can determine if the colorization aligns with the original scene or has been altered to manipulate perceptions. DIF addresses the distinction between images captured in the physical world and digitally generated through computer graphics. Forensic analysts employ specialized tools and techniques to identify telltale signs of computer-generated images, such as inconsistencies in lighting, shading, and patterns that might differ from what's expected in real-world images. This verification process is essential for assessing the credibility and provenance of CGI content. Anti-forensic refers to techniques used to subvert or evade digital forensic analysis. In DIF, it's crucial to understand anti-forensic methods that adversaries might employ to erase or alter traces of manipulation, thereby hindering the efforts of forensic experts. Understanding anti-forensic techniques is essential for developing more robust and reliable forensic tools and methods. DIF encompasses the detection and analysis of various types of image forgery. This includes detecting instances of copy-move forgery (where parts of an image are duplicated and placed in different areas), splicing (combining portions of different images), and other manipulations intended to deceive viewers. Forensic investigators use advanced algorithms and visual analysis to identify these forgeries, supporting the integrity of digital imagery. DIF covers multiple aspects, as presented in Fig. 1.

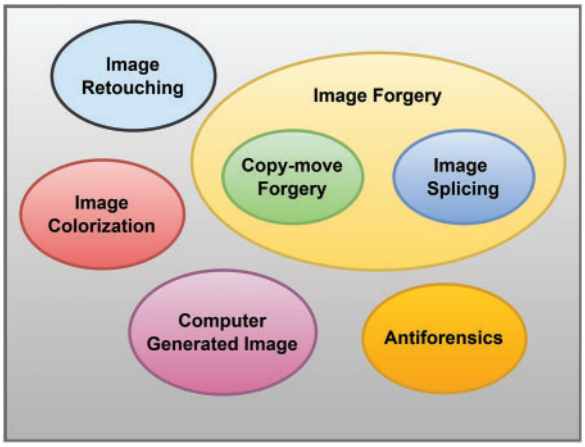

Figure 1: Categorical representation of digital image forensics

In general, research regarding image forgery implies that crimes of such particular kinds are conducted to publicize counterfeit information and take political advantage of bad publicity, which requires immediate attention. As a developing methodology, image forgery attempts to create the origin and validate digital media. DIF confirms the morals and legitimacy of massive data. It is used in diverse situations, such as medical fields, social media, and courts of law, which are becoming increasingly crucial.

Moreover, image forgery detection is classified into two categories: active image forgery and passive image forgery, also called blind image forgery detection. The active category comprises two sub-class

approaches: digital signature and watermarking. However, both of these methodologies necessitate prior knowledge of the image, which possibly happens to be embedded in the picture when it was captured or during image acquisition. Hence, the active forgery-based approaches are not entirely applicable when the images come from an unknown source. Instead, these approaches are pretty valuable for the forensic examination of digital images, such as crime scenes and fingerprint images, because such photos do not have signatures or watermarks. Alternatively, passive forgery-based approaches will unlikely need any pre-embedded knowledge regarding the picture. These approaches work by evaluating the different characteristics of the picture based on the determination of the source of the picture [14]. It established the notion of image forgery, including its types, datasets, schemes, constraints, and applications.

Fig. 2 depicts an extensive Mind map representing the intricate landscape of DIF. It provides a thorough overview of the demographic facets of the work conducted in this field. Mind map determines key participants and trends within the field of digital image forensics. It covers publication trends, sources of publications, research dimensions, keywords, key authors, organizations, and countries. The field of publication defines the number of papers published per year, the level of citation, and publication types. The Research Dimensions & Keywords section evokes some of the most notable areas like computer science, engineering, and telecommunications, and the visibility of the research to the community of academicians. The Key Authors, Organizations & Countries section focuses on efficient researchers and institutions. The illustration encompasses crucial information related to four distinct components:

2.1 Research Dimensions and Keywords

In this section, the Mind map highlights prominent research areas, indexing practices, and frequently used keywords within the realm of DIF. It covers a broad spectrum of research interests and author-associated keywords. According to the Web of Science (WoS), the top 5 significant research areas in the field of DIF are 'Computer Science' (1189 publications, 69.9%), 'Engineering' (926 publications, 54.44%), 'Telecommunication' (205 publications, 12.05%), 'Imaging Science Photographic Technology' (184 publications, 10.82%), and 'Optics' (53 publications, 3.12%). The top 5 WoS indexing categories are 'Science Citation Index Expanded' (SCI-Expanded) (845 publications, 49.68%), 'Conference Proceedings Citation Index-Science' (CPCI-S) (734 publications, 43.15%), 'Emerging Sources Citation Index' (ESCI) (130 publications, 7.6%), 'Social Sciences Citation Index' (SSCI) (7 publications, 0.41%), and 'Book Citation Index-Science' (BKCI-S) (5 publications, 2.9%). The most prevalent keywords in the domain of DIF are 'digital image forensics', 'image forgery detection', 'copy-move forgery', 'deep learning', and 'convolutional neural networks'.

2.2 Key Authors, Organizations, and Countries

This segment provides insights into the primary contributors, countries of origin, and institutions that play pivotal roles in advancing the field of DIF. The top 5 key authors in the DIF domain over the last decade are 'Shi YQ' (33 publications, 1.94%), 'Zhao Y' (29 publications, 1.71%), 'Barni M' (26 publications, 1.53%), 'Lu W' (25 publications, 1.47%), and 'Piva A' (25 publications, 1.47%). The top 5 major contributing organizations to the DIF domain include the Chinese Academy of Sciences, Beijing, China (69 publications, 4.06%); Sun Yat-Sen University, Guangzhou, China (66 publications, 3.88%); Indian Institute of Technology System, India (59 publications, 3.7%); National Institute of Technology System, India (48 publications, 2.82%); and University of Florence, Florence, Italy (39 publications, 2.29%). Furthermore, the top 5 contributing countries are 'China', 'India', 'USA', 'Italy', and 'South Korea'.

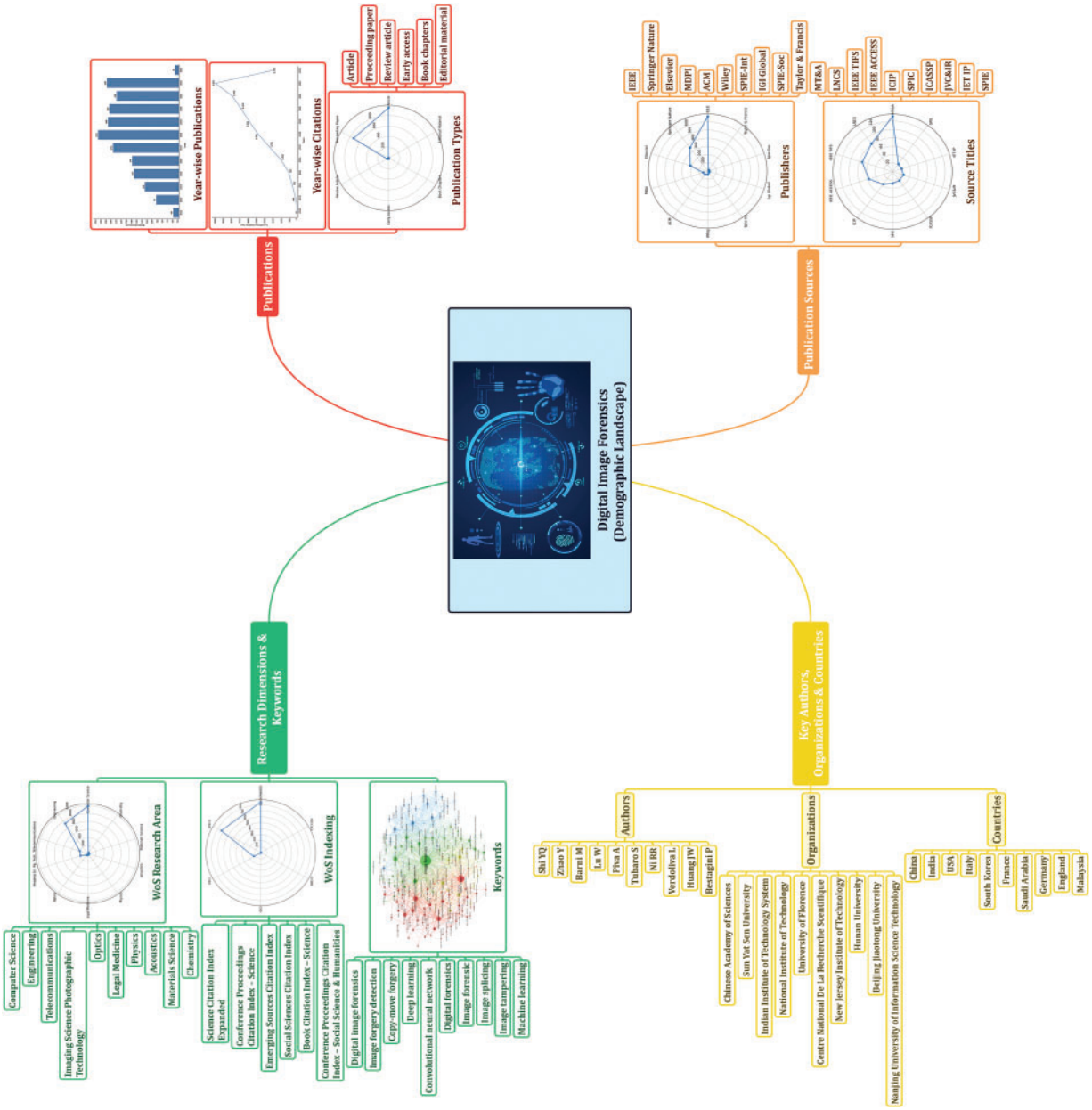

Figure 2: Mind map landscape of DIF

2.3 Publications

In this part, the Mind map provides comprehensive insights into the diverse types of publications resulting from research in DIF. It presents annual publication counts, shedding light on the field's growth and activity over time. Additionally, it furnishes information about citations spanning from 2012 to 2023, reflecting the influence and impact of the research. The highest citation count, 4981, was achieved in the year 2022. The major publication types encompass articles, conference proceeding papers, review articles, early access materials, book chapters, and editorial content. As depicted in the figure, the number of publications in the DIF domain has gradually increased, with 59 publications in 2012 and 188 in 2022. The maximum count of 205 publications was recorded in 2018 over the past decade.

2.4 Publication Sources

Within this component, the Mind map highlights significant publishers and source titles that play a crucial role in the field of DIF. This component assists in identifying key platforms where research findings are shared. Among the top publishers shown in the figure, the top 5 publishers in the domain of DIF are 'IEEE' (664 publications, 39.04%), 'Springer Nature' (353 publications, 20.75%), 'Elsevier' (215 publications, 12.64%), 'MDPI' (57 publications, 3.35%), and 'ACM' (54 publications, 3.16%). Similarly, the top 5 source titles are 'MT&A', 'LNCS', 'IEEE TIFS', 'IEEE ACCESS', and 'ICIP'.

In summary, Fig. 2 serves as a visual representation of DIF's multifaceted demographic landscape. It offers an in-depth insight into research dimensions, influential authors, institutions, publication trends, and authoritative sources within this dynamic field.

Image forensics, also termed passive image forensics, ascertains the picture authenticity along with the source, without relying on any pre-extraction data [15]. Image tampering tactics (device-independent) are utilized to modify a picture to achieve criminal intent [16]. A diverse range of image editing tools is used to create a fake image that, despite looking original, comprises complex hints of contradictions, for instance, distortions and overlapping loss of information, as evidence for image forensics. Passive forgery is generally divided into two categories: copy-move and splicing. In spite of the two categories, several other factors need to be considered in image forensics.

2.5 Copy-Move

This scheme of passive authentication is the most common picture tampering method. Still, it is also quite challenging to spot because a fraction of the picture is cloned and pasted into another section of the same image. The technique [17] encompasses four phases: pre-processing of the image, feature extraction, matching of image blocks, and visualization of the blocks, as illustrated in Fig. 3.

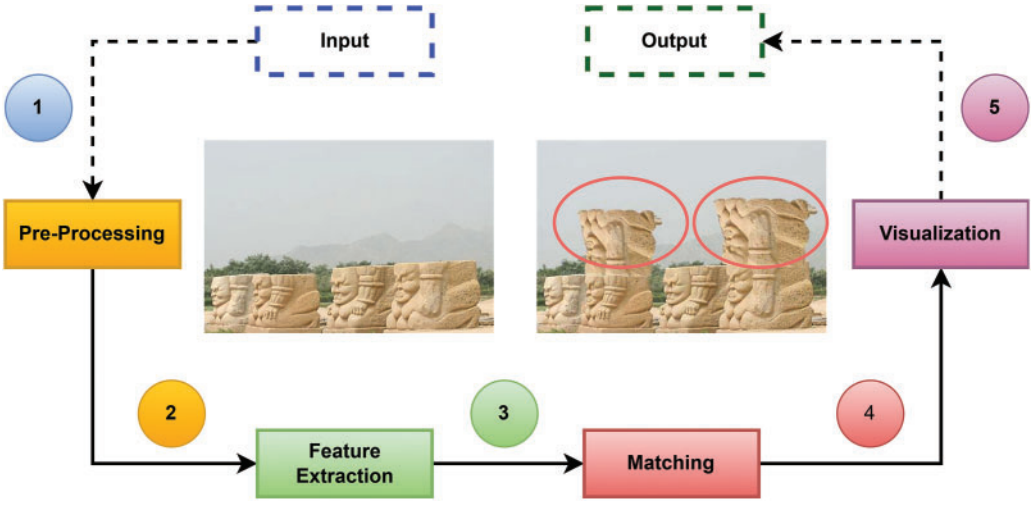

Figure 3: Workflow of copy-move

Moreover, a feature-based copy-move forgery detection (CMFD) scheme is presented by Yang et al. [18]. An adapted scale-invariant feature transform (SIFT) detector is employed to discover key points. A strategy based on key-point circulation was formed by circulating key-points over the picture. Eventually, the enhanced SIFT descriptor acknowledged key-points aimed at CMFD. Also, it grants comprehensive

experimental results to endorse efficiency. To detect the mistreatment of this kind, it also recognizes copied regions [19]. The SIFT relies upon that approach. It is an eminent, robust method that is proficient in detection and has identical features that apply to cloned areas. These coordinated features are positioned under a 2-level clustering scheme to ensure features are utilized for the geometric transformation of duplicated regions about specific clusters describing the comprised areas in the picture. For localization and detection of copy-move image forgery, a stationary wavelet transform (SWT) technique is utilized along with the discrete cosine transformation [20]. SWT is used considering its characteristics, such as spectral and spatial domain translation invariance and localization. Boundaries in CMFD are set forth by introducing a CNN design [21] that is sensitively crafted for the detection of even the subtlest manipulations, even for intricate image situations. In-depth knowledge of the properties of some key datasets—MICC-F220, MICC-F600, and their union variant—is furnished through rigorous study, thereby enlightening their influences on detection efficacy in previously untold ways. An all-around approach [22], a CMFD DRNet is given by Wang et al. The method aims to detect a pair of completely similar-structured regions in the copy-move fake image by ensuring complete extraction of semantically non-relevant shallow information. The DRNet is composed of two coupled modules: the coarse similarity and the shallow suppression similarity. Additionally, a higher-order self-correlation scheme is suggested to address the issue of noise introduction during the usage of shallow features. The experiments are conducted on the USC-ISI CMFD, CASIA [23] CMFD and CoMoFoD [24] public datasets, and 2.27%, 3.82%, and 4.60% improvement in the pixel-level F1 score, respectively, is observed when tested using DRNet. Li et al. [25] introduced an end-to-end CMFD framework, which combines the best of classical and DL techniques. More specifically, a strong cross-scale PatchMatch method designed for CMFD is built to detect copy-move regions. Compared with existing deep models, this technique utilizes features from high-resolution scales to scan for explicit and stable point-to-point matching between target and source regions. Moreover, a pairwise rank learning model is given to separate source and target regions. With the utilization of strong point-to-point prior, small variations are identified, and target vs. source discrimination is successfully achieved even if the target regions blend well with the background. Three main types of image forgeries are discussed [26]: recolouring, image splicing, and copy-move picture forgery detection. The copy-move image detection dataset applied in this study is MICC-220 and consists of 220 images captured in varying illumination conditions and camera settings. SIFT, the DBSCAN algorithm, and a deep convolutional neural network architecture are used in this study to identify recolored images. The CASIA V2 dataset of 4795 images is used to detect image splicing for the classification of tampered images and to identify different types of image forgery. Error level analysis in images and compression of images, along with a CNN, are included for identifying manipulated images.

2.6 Image Splicing

This approach, also termed image composition, is relatively tampering, clearly defined as a scheme that creates a single picture by copying and pasting different regions from different pictures [27]. There are two extensive splicing classifications: boundary-based and region-based [28]. Five low-level statistics-based algorithms [29] are introduced to evaluate the illuminance of horizontal and vertical bands. These algorithms leverage irregularities in illuminant color within the object area to identify area splicing fraud. Another approach focuses on illumination analysis, which proves effective in detecting image splicing [30]. Furthermore, a passive detection scheme for image splicing is presented in [31], utilizing the local binary pattern (LBP) in the discrete cosine transform (DCT) domain. Features are extracted from the chromatic channel to capture the tampered objects. Three key components are the backbone of the network [32]: feature extraction, augmented attention feature extraction, and tampered region detection. First, original tampered image features are mixed with the image residual features and then input into the backbone network to

extract features through the backbone network feature extraction module. Second, the tampered region area of the higher and lower layers is achieved through hierarchical encoding and decoding operations by the improved attention feature extraction module. Finally, the feature maps of each layer, which are derived, are input to the tampered region detection module, in which the loss of each feature map is collected to update the network parameters. Besides, a power image tampering dataset consisting of 552 samples has been created. Experiments demonstrate that the designed method compares favorably to current state-of-the-art approaches, with an improvement of 1% to 31% over evaluation measures, and is very insensitive to noise and JPEG compression attacks. A dual-encoder network for forgery detection from image splicing is presented by Yang et al. [33] to address these issues, employing an unfixed encoder and a fixed encoder. The unfixed encoder automatically learns the image fingerprints to separate tampered and non-tampered regions. The fixed encoder is utilized by design to embed structural information that is beneficial for understanding and forgery identification. The subsequent spatial pyramid global-feature extraction module is utilized to enlarge the global understanding of D-Net and further enhance discrimination among tampered and non-tampered regions. It is seen that D-Net, without pre-training or long training on a large set of forgery images, performs better than the other methods in pixel-level forgery detection. Additionally, it is demonstrated to be stably robust against various anti-forensic attacks. A dual-branch Multi-Scale Noise-Guided Progressive Network [34] is introduced by Zhang et al. The multi-resolution branch is utilized to extract the deep semantic image features and suppress redundant noise. A multi-scale noise-guided branch is utilized to identify more subtle tampering evidence and to lead the network to learn the spatial structure features better. The two branches are designed to constrain and complement each other. The properties of different scales are integrated through a progressive process, and the spatial channel feature aggregation module sums up feature expression. Various experiments show that it achieves better completeness and fewer false alarms in spliced image detection and localization. More precise detection results are achieved, and stability and robustness are shown. The method shows considerable performance relative to other state-of-the-art methods. The source code is available at https://github.com/Swag-Jiang/MSNP-Net (accessed on 01 January 2025). The approach [35] focuses on improving the accuracy of forged image classification. Enhanced DenseNet201 and VGG19 models are trained and fine-tuned for the CASIA 1.0 and CASIA 2.0 datasets, consisting of real and spoofed images. These models are used to identify instances of splice and copy-move forgeries. Leveraging the deep features learned by these models, the method is capable of achieving superior performance in identifying manipulated and real images. The summary of the above-discussed scheme is presented in Table 1. More studies of image splicing can be found in various survey papers [36,37].

Table 1: Image splicing detection schemes

Approach	Method/Model	Techniques used	Key features
Statistical analysis	5 Low-level algorithms [29]	Illumination inconsistency in horizontal & vertical bands	Detects tampering using irregularities in illuminant color
Illumination-based detection	Passive splicing detection [30]	Illumination analysis	Effective for splicing detection
LBP in DCT domain	Passive detection scheme [31]	LBP feature extraction in DCT uses chromatic channels	Captures tampered objects through local texture analysis

(Continued)

Table 1 (continued)

Approach	Method/Model	Techniques used	Key features
Deep learning network	Backbone network [32]	Feature extraction, attention module, tampered region detection	Shows 1%–31% improvement over other methods; robust to noise and JPEG compression
Dual-encoder network	D-Net [33]	Fixed & unfixed encoder; spatial pyramid feature extraction	High performance without pre-training; robust against anti-forensic attacks
Multi-scale dual-branch network	MSNP-Net [34]	Multi-resolution & multi-scale noise-guided branches; progressive spatial feature aggregation	High accuracy, low false positives, stable, and robust
Transfer learning with deep CNNs	DenseNet201 & VGG19 [35]	Fine-tuned on CASIA 1.0 & 2.0	Accurately classifies splice and copy-move forgeries

2.7 Image Retouching

Image retouching is quite productive for photography in films and magazines. At the same time, such adjustments are meant to beautify pictures and thus are not reckoned as forging. However, this technique is also included in this review because it comprises manipulations with the originality of the photo. Only specific areas of the photo are enhanced or beautified, such as removing wrinkles to have a better final shot. Fig. 4a illustrates the original photo, whereas Fig. 4b displays the retouched photo.

Figure 4: Image retouching

These techniques are moderately inoffensive and are measured as less malicious compared to other forgery approaches. Such manipulation is for good image retouching tools to help improve the whole photo or some parts. Retouching works, such as saturation, tone correction, noise corrections, and sharpness, are so detailed that such disparities cannot be recognized unless sophisticated tools are utilized to check. Xu et al. [38] suggest an algorithm based on a technique of 8-neighborhood quick sweeping. The study's results demonstrate a significant improvement in the rate of photo inpainting while preserving the overall effect quality. Kumar et al. [39] examine various pixel-based and physics-based forgery detection algorithms and compares these techniques. Additionally, despite variations in processing procedures and imaging devices, a consistent structure in the photo undergoes alterations when tampered with, deviating from its original state.

2.8 Image Resampling

Image resampling is basically a geometric alteration, such as flipping, stretching, rotation, scaling, and skewing. These modifications are done in specific areas requiring an astonishingly manipulated photo. The interpolation step is key in the resampling procedure. Meanwhile, it is familiar with substantial statistical variations. The image is resampled, which is familiar with exclusive periodic correlations. Liu and Sung consider [40] the association between the surrounding DCT coefficients. The implied procedure for enlarged JPEG and spliced pictures is frequently utilized in image forging. The adjacent joint density features of DCT coefficients are thoroughly removed. Also, features are detected by an SVM, besides the detection of resampling through integrating new tools and notions from random matrix theory (RMT) [41]. The RMT delivers valuable tools to model the performance of eigenvalues and singular values of random matrices. A way to detect and resample counterfeits in pictures with a linear parametric model was also suggested. First, resampling was detected in the 1-D signal and extended for the 2-D image. A primary quantization steps estimation method [42] for resized and double JPEG compressed images is presented. The distribution of DCT coefficients is examined first according to the inverse resized image. Then, a maximum likelihood function and a filtering scheme are designed to accomplish the primary quantization step on AC bands. Additionally, a prominent peak in the DFT spectrum of the DC coefficient distribution that depends nonlinearly on the step is discovered. Based on this observation, a geometric fitting-based mapping function is outlined to estimate the step in the DC band. An inexpensive feature extraction approach [43] for resampling detection in post-JPEG compressed images is suggested. In this strategy, the compression features are combined with resampling features and fed into various traditional conventional machine learning (ML) techniques like logistic regression, K-nearest neighbors, SVM, decision tree, and random forest to locate and classify tampered images in the scenario of re-compression. Table 2 presents a comprehensive comparison of various image forgery techniques, showcasing their respective performances and the datasets utilized in the corresponding research studies. This comparative analysis provides valuable insights into the effectiveness and suitability of different approaches in image forensics.

Table 2: Comparison of image forgery detection approaches

Forgery detection	Source	Approach	Datasets	Performance
Image forgeries, along with anomalous features, and a manipulation tracing system	[44]	Multibranch Input-Feature: Pixel values Filter: SRM, Bayar	COVERAGE [45], NIST [46], *ad-hoc*, CASIA, Dresden [47], Columbia color	81.7% accuracy & (CASIA), 79.5%
Copy-move forgery detection	[48]	Input-Feature: Key points background structure is its own location (pixel)	*Ad-hoc*, CoMoFoD, ROME patches [49]	Accuracy of 97.1%
Image forgery detection and hybrid LSTM	[50]	LSTM	NIST, COVERAGE, *Ad-hoc*, IEEE Forensics challenge	Accuracy of 94.8% (NIST)

(Continued)

Table 2 (continued)

Forgery detection	Source	Approach	Datasets	Performance
Based on LSTM and CNN	[51]	Input-Feature (Pixel values) background structure is its own location: Pixel with a box	UCID dataset [52] and an *Ad-hoc* dataset	Accuracy of 93.6%
Source-to-target localization, along with copy-move image manipulation	[53]	Input-Feature: Pixel values) background structure is VGG-16 location (pixel)	CASIA, CoMoFoD, *Ad-hoc*, SUN 2012, MS COCO	Accuracy of 78%
Patch-based photo inpainting	[54]	Input-Feature: High pass) background Structure is own location (pixel)	MIT Place dataset *Ad-hoc* dataset	Accuracy of 97.8%

2.9 Computer Graphics Image Detection

The approaches based on computer graphics usually create visually plausible photos of mythological scenes. Computer graphics images (CGI) are primarily utilized in 3D animation and virtual reality. Still, it might be used to manipulate information that can cause difficulties in real-life verdicts. Thus, the problem of discerning between a CGI and a real image has been investigated by many researchers in the past few years. Fig. 5 shows how difficult it is to differentiate these images with simple visual analysis [55].

Figure 5: The Image on the left is taken with a camera, and the image on the right is CGI

A deep neural network with a transfer learning-based approach was presented in [56]. Scheme [56] used the ResNet-50 model to categorize small patches of CGIs along with real photos taken with the camera, followed by another approach [57] that utilizes a CNN without pooling layers to cope with the CGI forensics issue. Maximal Poisson-disk Sampling was employed to extract patches from full-size photos in an end-to-end scheme, losslessly [58]. Another study [59] examined the application of an Attention-Recurrent Neural Network in a local-to-global fashion for categorizing computer graphics images under a sliding window scheme. Recently, a CNN-based method was introduced in [60] featuring a hybrid correlation module at the input stage, comprising a 1×1 convolution layer and three successive convolutional layers. This technique leverages pixel and channel correlations to detect CGIs. A shallow attention-based dual-branch CNN is presented [61], employing two inputs preprocessed with a Gaussian low-pass filter for

CGI classification. This preprocessing step enhances the network's ability to learn generalized patterns. An architecture combining a CNN with SRM filters and Gaussian random weights is outlined [62]. These filters and weights initialize the first layer within a two-branch framework. The research proposes creating negative samples through gradient-based distortion to enhance generalization for test images produced by unfamiliar graphic rendering engines.

Additionally, the CGI-based methods summarized in Table 3 demonstrate performance comparisons on the following datasets: Columbia CGI [63], Web-fetched images, ImageNet [64], Artlantis [65], Rahmouni [66], He [67], Corona [65], Vision [68], VRay [69], Autodesk [70], Tokuda [71], RAISE [72]. Patch-level accuracy is employed as the performance metric for both datasets, as it provides researchers with a controlled experimental setting featuring a balanced class distribution of natural images (NIs) and CGI patches. Larger patch sizes, as seen in [66], generally enhance CGI detection performance at the cost of increased computational requirements. However, in [62], HTER (half the total error rate, in %) is employed for performance evaluation [66].

Table 3: Summary of CGI-based approaches

References	Networks	Datasets	Input sizes	Performances
[57]	CNN	Columbia CGI, *ad-hoc*	32 × 32	98.0%
[56]	CNN-SVM	Tokuda, ImageNet	224 × 224	94.1%
[58]	CNN	Columbia CGI, RAISE	30 × 30, . . ., 240 × 240	94.8%
[59]	A-RNN	Columbia CGI, RAISE	30 × 30, . . ., 240 × 240	94.9%
[60]	CNN	He	96 × 96	94.2%
[61]	Two-input AD-CNN	He	32 × 32, 64 × 64	87.8%
[62]	Two-branch CNN	Corona, Autodesk, RAISE, VRay, Vision, Artlantis	233 × 233	HTER 1.31%

2.10 Camera Identification Issues

There are various approaches to addressing the challenge of determining the originality of a photo. One way is to consider whether it is possible to determine which camera model was utilized to capture the picture. The JPEG header or EXIF data typically contains information such as the camera model, date, and time. However, it is essential to note that this metadata is not always considered reliable or authentic, as it can be easily modified. Therefore, relying solely on this information may not provide a conclusive indication of the photo's originality. Moreover, the image acquisition process outlined in Fig. 6 consists of seven distinct steps. The initial step involves the lens capturing and redirecting the incoming light rays, possibly applying additional filters such as anti-aliasing. Subsequently, the color filter array (CFA) divides the light into red, green, and blue components for each pixel. Eventually, the de-mosaicing process reassembles the full-color scene using data collected in the prior step. Depending on the camera's software and model, diverse post-processing operations might be implemented after de-mosaicing. These operations can include gamma correction, JPEG compression, and color balancing. These post-processing steps are crucial in providing

specific characteristics and important cues within the forensic analysis of images. The final stage of the camera's image creation process involves fabricating a forgery, where intentional modifications are made to deceive the viewer. Consequently, traces of these post-processing steps can serve as significant indicators for the authentication and identification of the image's origin in image forensics research. Examining the hints and evidence left behind by the post-processing procedures executed by different cameras becomes a crucial source of information in determining the authenticity and source of an image.

Figure 6: Representation of forgery along with image acquisition

The initial approaches to camera identification based on DL were mainly focused on classifying patches generated via different camera models. The Bondi et al.'s model [73] based on CNN and SVM, was introduced to classify patches from unidentified cameras. The framework utilized the CNN output to identify photo anomalies and detect forgeries. Likewise, in the Tuama et al. method [74], a high-pass filter was employed at the initial CNN layer to limit the image's content. It enabled obtaining photo residuals as input, which favored training a shallow CNN model for learning and classifying different camera models. To ease the camera models issue, which can be difficult due to new models and requires an updated database, an open-set condition was presented [75] to predict an unseen camera. For the first layer, the methodology utilized a limited initialization to help infer, irrespective of the photo taken via an unknown camera model. Moreover, Cozzolino and Verdoliva [76] utilized a Siamese CNN model to extract the distinct fixed-pattern noise of a camera from the image's photo response non-uniformity. This technique helps classify cameras and identify device fingerprints for image forgery detection. A few-shot learning approach is utilized where annotated data, such as image samples, is limited [77]. This approach centers on acquiring a model through limited examples per class. A Siamese network is utilized to improve the classification accuracy of diverse camera models. The Siamese network forms pairs of photo patches from identical camera models for training enhancement. Both techniques harness the Siamese network, featuring multiple inputs with comparable architecture and initial weights for each sub-network. The core aim of this framework is to grasp the resemblance between inputs, with parameter updates synchronized across all sub-networks. Additionally, Table 4 summarizes the camera identification methodologies. The Dresden dataset [47] is utilized to compare the accuracy of the performance. The patch size was not the same for a similar number of cameras, making it complicated to pitch a reasonable compression of different approaches. Thus, the methods with 32 × 32 patch size or even smaller, merged with a wide range of camera models, exhibit a much more complex challenge because each patch offers inadequate information and a larger number of classes to classify.

Table 4: Summary of camera identification approaches

References	Network	Datasets	Input size	Input features	Performance
[73]	CNN-SVM	*Ad-hoc*, Dresden	64 × 64	Pixel values	93.00%
[74]	CNN	Dresden	256 × 256	High-pass residuals	98.00%

(Continued)

Table 4 (continued)

References	Network	Datasets	Input size	Input features	Performance
[75]	CNN-SVM, CNN-ET	Dresden	256 × 256	High-pass residuals	93.90%
[76]	Siamese	*Ad-hoc*	48 × 48	Pixel values	100.00%
[77]	Siamese	Dresden	64 × 64	Pixel values	87.03%

2.11 Anti-Forensics

Anti-forensics, also known as counter-forensics, is a practice that primarily focuses on thwarting forensic analysis methods used by determined adversaries. Its goal is to prevent photo alteration so that image forensics tools cannot provide valuable clues regarding falsification, tampering, and identifying source devices. Anti-forensics aims to make it difficult for forensic investigators to uncover evidence or trace the origins of a manipulated image by employing techniques that hinder traditional forensic analysis methods. The research presented in [78,79] suggested that CNNs are easy to target for adversarial attacks. The anti-forensic methods that relied on DL have been recapitulated rather than utilizing GANs to hide or reconstruct cues with the help of visually imperceptible distortions. A white-box condition is suggested by Chen et al. [80] in which the information on the camera model and the forensic tool is known. A proposal was made to use a GAN to modify traces used for camera model identification. A loss function was introduced to minimize photo distortion while simultaneously deceiving a CNN-based detector to distinguish between different camera models. In a follow-up work [81], the authors presented a GAN for two conditions: a data-independent requirement with no information and a data-dependent one with a known camera model. In addition, a GAN-based framework was created by Cui et al. [82] to assist in limiting the ability to detect CGIs and NIs accurately. Two Sobel filters were incorporated as the discriminator to direct the network's focus toward the texture information of the input image. The transferability of anti-forensic attacks was investigated by Barni et al. [83]. It was noted that most attacks could not be transferred, simplifying the development of appropriate countermeasures against anti-forensics. Table 5 concisely summarizes anti-forensic methodologies that leverage DL techniques. It highlights the critical components employed by these methods and the specific forensic issues they aim to address. This summary offers valuable information on using DL to combat various challenges in image forensics.

Table 5: Summary of anti-forensic approaches

References	Input size	Issues	Datasets	Strategy
[80]	256 × 256	Camera identification	Dresden	GAN
[81]	64 × 64, 227 × 227	Camera identification	Dresden	GAN
[82]	178 × 218	CGI detection	CelebA [84]	GAN
[83]	128 × 128	Attack transferability	Vision, RAISE	GAN

3 Overview of Fake Image Colorization Detection Approaches

The image holds a substantial role in several fields of the real world, such as surveillance systems, crime investigation, forensic investigation, sports, medical imaging, journalism, intelligence systems, and legal services. Image forgery is about fabricating illegitimate modifications in an original photo to closely mimic its legitimacy, making it difficult for the human visual system to differentiate between original and tampered

photos. To work on image forgery detection, determine whether the picture is authentic or tampered with. The most vital task is to localize the tempered section affected by different forgery operations executed by a forger. Image colorization is a new method of photo editing where grayscale pictures are colored with realistic colors, or, instead, the natural color picture is recolored for different purposes. Moreover, recent advancements in DL techniques have introduced a wide range of colorization models that have demonstrated innovative capabilities, including the successful utilization of Generative Adversarial Networks (GAN) [85] and brute force networks [86] to tackle the challenge of colorization. Colorization methods vary significantly, particularly in how data is handled and acquired. This is crucial for modeling the relationship between CIs and grayscale images. Techniques designed for detecting artificial CIs are also on the rise. Additionally, colorization extends beyond its practical applications in graphics and holds considerable potential. However, it remains a challenging problem due to the diverse conditions of images that require a single algorithm to handle. This challenge is particularly acute considering that two out of three image dimensions are missing, despite the inherent knowledge of scene semantics like green grass, blue sky, and white clouds, which are uncommon in human-made objects. In addition, the challenges of colorization are similar to those of image enhancement, such as changes in viewpoint, occlusion, and illumination variation. Recently, there have been two ways of detection, namely traditional and more modern ML-based and DL-based. The difference between these methods is illustrated in Fig. 7.

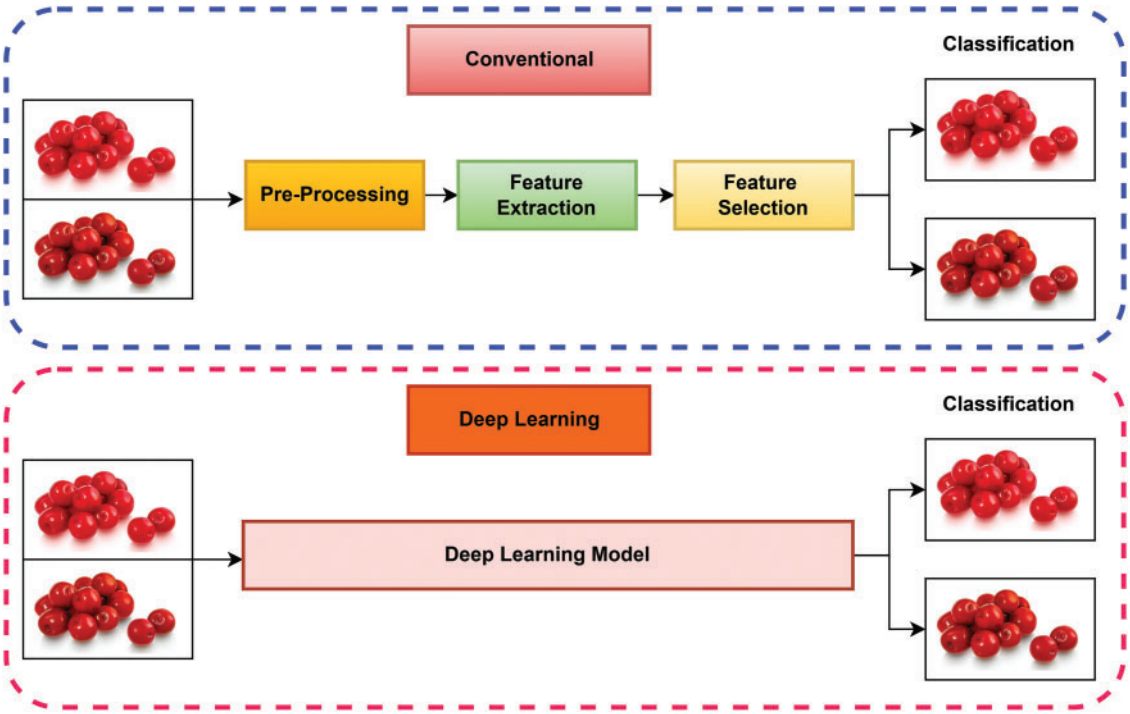

Figure 7: Fake colorization detection in traditional and DL comparison

3.1 Traditional Colorization Detection Approaches

In the traditional method, statistical data is taken from the photo during the feature extraction procedure, which is performed separately before the classification phase. In contrast, in the DL-based method, the classification and feature extraction are performed in the same step. Furthermore, adaptation to the appropriate luminance-chrominance color space is exploited by Welsh et al. [87]. However, in most scenarios,

no such color is available that might be suitable to relate to a specific gray object, such as clothing, balloons, or objects made from plastic. Hence, several objects that might have various colors and forms of colorization are a big challenge. This sort of complication offers consistent attention in the research community. In the initial phase of colorization methods [88], the approaches from that era comprised coloring a daguerreotype and a blend of pigments and gum Arabic [89]. After the digital revolution, colorization was moved to the computer domain after the advancement brought by the ML and DL approaches, and its usefulness in several applications of image processing and computer vision [90]. ML and DL can efficiently deal with an enormous amount of data, uncover hidden patterns, and produce an adequate estimation of potential knowledge. However, ML determines the rules of data by extracting features concerning a particular way of acquiring previous knowledge. In contrast, DL regularities can be extracted independently with the help of categorized-level artificial neural networks.

Hand-crafted methods like fake-colorized image detection (CID), which is based on histogram and feature encoding, outlined generalization issues, and utilized four features [91] for forgery detection, such as hue, dark channel, bright channel, and saturation features. The work substantially declines internal and external validation performance results. An LBP is utilized [92] by Agarwal et al. for feature extraction. However, a histogram of the resulting photo is used as a feature vector, and for binary classification, linear discriminant analysis is used as a classifier. The results offer an error value of 3.47%, but the outcomes were not compared with previous detection methods, a critical issue of the scheme. A different technique based on lateral chromatic aberration (LCA), along with histogram features, is applied for fraudulent detection [93]. A suggestion was made that recolored images (RIs) have fewer local color adaptation properties than NIs. A five-dimensional vector was employed to train SVM, resulting in promising but disparate outcomes.

Zhang et al. [94] extract chrominance texture features using the LBP operator. The LBP operator is used to extract local texture features from an image's chrominance components. The chrominance components are the color components that represent an image's hue and saturation, and they are often more sensitive to recoloring than the luminance component. A polycolor model binary pattern (PMBP) [95] is introduced to obtain good internal statistical features. Various color models like RGB, YUV, YCbCr, and HSV are investigated to achieve notable statistical information from an image. A PMBP is generated by utilizing the effective channels of different color models. The approach here produces promising results for non-compressed and highly compressed CIs. To detect imitated generated paintings by Bai et al. [96], imitated and original paintings are compared in the Fourier frequency domain, where statistical variations and artifacts appear. Based on these findings, fake-generated painting detection via frequency analysis is suggested by extracting three kinds of frequency-domain features. A digitally imitated painting detection database is also suggested for the method's evaluation. The directory of the original image by Castro et al. [97] contains 15 color images and 85 grayscale images. The tampered image directory contains 1050 images created by one of the four types of tampering: copy-move, cut-paste, retouching, and colorizing. For every pair of the original and tampered images, the corresponding true mask is provided in the mask directory (1380 masks). In the description file, image names (i.e., original, tampered, and mask), image description, photo location, type of tampering, and manipulated objects in the image are recorded.

An inter-channel correlation-based recolored image detection method [98] is suggested for both regular and hand-crafted recoloring scenarios. The inter-channel correlation of NIs is assumed to be disrupted by recoloring operations, as significant differences between the camera imaging model and recolored image modeling methods have been observed. Numerical analysis reveals that inter-channel correlation difference disparity can serve as an effective discriminative measure for distinguishing RIs from NIs. Based on such previous knowledge, a feature set of inter-channel correlation is computed from the first-order differential residues' channel co-occurrence matrix of the differential image. Besides, three detection modes

are considered based on real conditions, which are the appearance of matching and mismatching situations between training data and testing data, and a hand-crafted recoloring situation. The summary of traditional colorization detection approaches is presented in Table 6.

Table 6: Summary of traditional colorization detection approaches

S. No.	Scheme	Techniques used	Remarks
1	Welsh et al. [87]	Luminance-chrominance space adaptation	Limited by the unavailability of color references for gray objects
2	Daguerreotype + pigments/gum Arabic [88,89]	Manual blending techniques	The primitive approach before the digital era
3	Histogram & Feature Encoding [91]	Hue, dark/bright channel, saturation features	Suffers from generalization; poor validation results
4	Agarwal et al. [92]	Histogram of image → LBP → LDA for classification	3.47% error, but lacks comparison to baseline methods
5	Histogram + LCA [93]	5D vector for SVM classification	Recolored images show reduced local color adaptation
6	LBP on Chrominance [94]	LBP on hue/saturation components	Sensitive to color tampering; effective in detecting recoloring
7	Polycolor Model Binary Pattern (PMBP) [95]	RGB, YUV, YCbCr, HSV fusion	Good performance for both non- and highly-compressed images
8	Fake Painting Detection [96]	Fourier domain artifacts	Compares real vs fake paintings via three frequency features
9	Inter-Channel Correlation [98]	Co-occurrence matrix of differential image channels	Differentiates RIs from NIs effectively based on disrupted correlation

3.2 DL-Based Colorization Detection Approaches

A CNN-based fake image detection process [99] was conducted based on the distribution factor by Pillai et al. Hue, darkness, brightness, saturation, and the alpha channel were utilized. The estimation of the distribution factor of these features was performed using a Gaussian distribution. The model also employed Pearson correlation to ascertain whether the brightness of the synthetic and original edges correlates. To identify fake CIs, color information from three different color spaces—HSV, Lab, and YCbCr—is combined, and the most dissimilar channels from each color space are chosen to rebuild the image by Salman et al. [100]. Features are extracted from this representation using transfer learning with a pre-trained ResNet50 model. The SVM is employed for classification. A fuzzy classification model was employed to categorize the Pearson correlation, enhancing the overall model. A neural network-based methodology is presented in [101] with three phases to detect fake images. The work applies normalized histograms generated for value, red, green, blue, saturation, and hue channels during the first phase. It validates and assesses statistical changes between fake CIs and relevant originals. In the second phase, a cosine similarity scheme was applied to normalized histogram distributions of authentic and fake images in different channels for feature extraction. The model

is formed and trained in the last phase to identify tempered CIs. The outcomes demonstrate that the projected model excels in the approach presented in [91].

It is seen that the frequency spectrum of spurious visual data includes discriminative features that can be used for spurious content detection. In addition, the retained information in the frequency domain is seen to be dissimilar to that of the spatial domain. Based on these aspects, a two-stream CNN architecture is developed [102] to combine frequency and spatial domain features. The improved generalization of the suggested two-stream architecture to various unseen generation frameworks, datasets, and approaches is reported. The fusion of frequency and spatial domain streams enhances the detector's generalization further. The research work discussed [103] focuses on the development of an advanced network by leveraging DL methodology. Image preprocessing is done through DCT and YCrCb color space. It is a two-layered network, and pair-wise information is utilized as input. The network is trained to discriminate between fake and authentic images. Apart from this, a classification layer is inserted into it in order to classify an input image as forged or original. The flood fill algorithm is applied to stamp forged objects in images, and a DL-based method is introduced [104] for identifying fake images. A Twitter dataset is collected and used as input for DL models, which are trained to classify images as fake or real. To solve this problem, two models [105], namely a personalized architecture and a transfer-learning-based model, are designed based on CNNs to identify CIs (or colorized videos) rapidly. In experiments, the influence of three hyperparameters on the performance of a classifier is investigated by HTER. The best result is obtained with the Adam optimizer, a dropout rate of 0.25, and an input image size of 400 × 400 pixels. In terms of inference times per image, the custom model is 12 times faster than the transfer-learning-based model, yet in terms of precision, recall, and F1-score, the transfer-learning-based model is better than the custom model. Both models generalize better than other models reported in the literature.

Yang et al. [106] introduce a color tampering-based image detection method using Vector of Locally Aggregated Descriptors (VLAD) to represent multiple color channel features without watermarking. Several sets of common color channels in computer vision are tested, and the optimal one is selected. These features are then represented using VLAD, and an SVM model is learned based on the features represented. It is further observed that detection proves to be difficult for a massive group of image classes. DL is, therefore, applied to train a ResNet-based classification model and is used as a starting point to classify the dataset. Quan et al. [107] first automatically constructed negative samples through linear interpolation of NI and CI pairs. These adverse examples are progressively incorporated into the original training set, and learning in the network proceeds. Experimental results confirm that the enhanced training significantly improves the generalization performance of many CNN models. In another paper by Quan et al. [108], a sequence of experiments explores the impact of data preparation and the initial layer settings of an innovative CNN-based method on the forensic performance of the detector, particularly its generalization capability. Several intriguing conclusions are drawn, which are useful for designing image forensics experiments. A simple method is also presented to improve the generalization performance of CID by combining the decision results of CNN models with different first-layer configurations.

The study [109] investigated the shared correlations among various CFA algorithms instead of focusing on specific CFA patterns. Previous research demonstrates strong and similar correlations between high-frequency components across image color channels, typically ranging from 0.98 to 1. This correlation property is commonly utilized in CFA de-mosaicking techniques and leveraged in the method to detect RIs using the difference of images. The method also employs the Generalized Grayworld Estimates as the illuminant color estimator, based on the Grey-Edge hypothesis that assumes the average edge difference within a scene is achromatic. For image evaluation, the difference images (DI) and illuminant map (IM) are initially computed. Subsequently, the original image in RGB channels, the difference images, and the

illuminant map serve as inputs in the network. The network's backbone architecture is based on the 16-layer model of the VGGnet. In a similar approach [110], the input image undergoes an HSV color space transformation, and DI and IM are derived as evidence. The difference image represents inter-channel correlation and is essential for biased proposals and channel connections. RGB calculation is performed in the image, and it is incorporated into the method as a single information part. The illuminant mapping reflects the illumination color and is the same size as the original RGB image. Each pixel value indicates the estimated illuminant tone, aiming for consistency in illuminant colors. However, this objective may not be achieved after the recoloring process, as inter-channel relations and illuminant consistency are disrupted. All three image features are extracted and fused. The resulting fused image is fed into the input layer of the CNN as the initial step. Quan et al. [111] employ ensemble learning with multiple CNNs trained on the same dataset, each with different hyperparameters and initializations. It ensures diversity in learning features. A voting scheme combines CNN predictions, classifying an image as colorized if most CNNs agree. Negative sample insertion is also used, creating artificial images that resemble CIs but are natural. By training CNNs on NIs and negative samples, they effectively distinguish between the two image types and generalize to colorization techniques. Negative samples are generated by linearly interpolating between a natural and colorized image, controlled by an interpolation factor. A modified DenseNet architecture [112] is utilized in the first stage to extract features from the input image's hue, saturation, and value color channels. It modified the DenseNet architecture, fine-tuned on a dataset of genuine and forged CIs, demonstrating its effectiveness for image classification tasks. An ensemble learning approach is employed in the second stage to fuse the features extracted in the first stage. The fusion is performed using a voting classifier that predicts the image's class based on majority voting by individual models. The summary of deep learning-based colorization detection approaches is offered in Table 7.

Table 7: Summary of DL colorization detection approaches

S. No.	Scheme	Techniques used	Remarks
1	CNN-based detection [99]	Gaussian dist. of hue, brightness, alpha; Pearson correlation	Feature distribution used to detect inconsistencies
2	ResNet50 + SVM [100]	HSV, Lab, YCbCr fusion; transfer learning	Best channels fused, improves SVM classification
3	NN with Histogram & Cosine similarity [101]	Normalized histograms + cosine similarity	Outperforms earlier CID
4	Two-Stream CNN [102]	Combines frequency & spatial domain	Improves generalization to unseen datasets
5	Two-layer DL with DCT & YCrCb [103]	Pairwise input + classification layer	Detects forged vs authentic; flood fill used
6	DL on Twitter dataset [104]	Flood fill algorithm, DL	Social media-specific training
7	Custom CNN vs transfer learning [105]	Input size, dropout, optimizer tuning	Transfer learning = better precision; custom CNN = faster inference
8	VLAD + SVM [106]	VLAD on color channels; ResNet fallback	Detection is hard for large image classes
9	Negative sample insertion [107]	Interpolation of NI–CI pairs	Boosts CNN robustness to recolored images

(Continued)

Table 7 (continued)

S. No.	Scheme	Techniques used	Remarks
10	CNN layer configuration study [108]	Data prep + initial layer setup	First-layer fusion improves performance
11	VGG16 + Grayworld estimator [109]	CFA-based, inter-channel difference, illuminant map	Uses color channel correlation & illuminant consistency
12	HSV-Based difference image [110]	HSV transformation + fused features	Disrupted illuminant mapping helps detect recoloring
13	CNN Ensemble + Voting [111]	Multiple CNNs + negative sample insertion	Voting increases classification accuracy
14	Modified DenseNet + Voting [112]	HSV feature extraction + ensemble voting	Two-stage system with strong classification results

Image colorization detection confronts sophisticated AI-based methods, highly realistic manipulations, limited training data, generalization issues, vulnerability to adversarial tactics, evolving forgery techniques, complexities in model interpretability, human-authentic forgeries, sensitivity to minor alterations, wastefulness of resources, and ethical issues. These are addressed by ongoing research directed toward the development of robust detection methods that can evolve according to changes in manipulation practices.

4 Conclusion

In the present day, advancements in image editing technologies have catapulted the ease of image manipulation to unprecedented levels. Unfortunately, this progress has also paved the way for the misuse of fabricated images for various purposes. A fundamental challenge arising from this situation lies in the ability to distinguish between unaltered and modified images. This paper has provided a comprehensive survey of the established methods for detecting image forgery, shedding light on the diverse methodologies employed in this field. The paper has also explored a recent challenge in the domain of image forensics, with a primary focus on the detection of manipulated colorization. The process of image colorization involves predicting colors for grayscale images, thereby enhancing their aesthetic appeal. The advancements in colorization techniques have reached a point where it has become increasingly difficult for the human eye to differentiate between authentic and counterfeit images. Digital fake colorization can distort historical accuracy and influence public opinion. Its unethical use is a cause for concern about misinformation, cultural integrity, and the authenticity of visual evidence. It may be handled by explicitly labeling colorized images, using digital watermarks, and promoting ethical practices for transparency and preventing misinformation. In photojournalism and social media, imitative colorizations need to be traceable to uphold visual integrity and combat disinformation. In forensic science, accurate identification of pictures manipulated for misleading purposes can help establish proof. In medical imaging, color constancy is paramount to reliable diagnosis. Such enhancements aim to strengthen the technical applicability and societal value of reviewed methods.

Acknowledgement: We thank the anonymous reviewers for their valuable suggestions that improved the quality of this article.

Funding Statement: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3049788).

Author Contributions: Conceptualization, Saurabh Agarwal, Ki-Hyun Jung; methodology, Saurabh Agarwal, Cheonshik Kim; formal analysis, Saurabh Agarwal; investigation, Saurabh Agarwal, Deepak Sharma, Nancy Girdhar, Ki-Hyun Jung; resources, Ki-Hyun Jung; writing—original draft preparation, Saurabh Agarwal, Deepak Sharma, Nancy Girdhar, Ki-Hyun Jung; resources, Ki-Hyun Jung; writing—review and editing, Saurabh Agarwal, Deepak Sharma, Nancy Girdhar, Cheonshik Kim, Ki-Hyun Jung; resources, Ki-Hyun Jung; supervision, Ki-Hyun Jung. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Mahdian B, Saic S. A bibliography on blind methods for identifying image forgery. Sig Process Image Commun. 2010;25(6):389–99. doi:10.1016/j.image.2010.05.003.
2. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative adversarial networks. Commun ACM. 2020;63(11):139–44. doi:10.1145/3422622.
3. Zhuo L, Tan S, Zeng J, Lit B. Fake colorized image detection with channel-wise convolution based deep-learning framework. In: 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC); 2018 Nov 12–15; Honolulu, HI, USA. p. 733–6.
4. Li H, Zhang L, Zhang X, Zhang M, Zhu G, Shen P, et al. Color vision deficiency datasets & recoloring evaluation using GANs [Internet]. Multimed Tools Appl. 2020;79:27583– 614. [cited 2025 Jan 1]. Available from: https://link.springer.com/10.1007/s11042-020-09299-2.
5. Isola P, Zhu J-Y, Zhou T, Efros AA. Image-to-image translation with conditional adversarial networks [Internet]. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR); 2017 Jul 21–26; Honolulu, HI, USA. p. 5967–76. [cited 2025 Jan 1]. Available from: http://ieeexplore.ieee.org/document/8100115/
6. Zhu J-Y, Park T, Isola P, Efros AA. Unpaired image-to-image translation using cycle-consistent adversarial networks [Internet]. In: IEEE International Conference on Computer Vision (ICCV); 2017 Oct 22–29; Venice, Italy. p. 2242–51. [cited 2025 Jan 1]. Available from: http://ieeexplore.ieee.org/document/8237506/.
7. Zhu JY, Zhang R, Pathak D, Darrell T, Efros AA, Wang O, et al. Toward multimodal image-to-image translation. In: 31st Conference on Neural Information Processing Systems (NIPS 2017); 2017 Dec 4–9; Long Beach, CA, USA.
8. Wan W, Wang J, Zhang Y, Li J, Yu H, Sun J. A comprehensive survey on robust image watermarking. Neurocomputing. 2022;488:226–47. doi:10.1016/j.neucom.2022.02.083.
9. Begum M, Uddin MS. Digital image watermarking techniques: a review. Information. 2020;11(2):110. doi:10.3390/info11020110.
10. Lin X, Li JH, Wang SL, Liew AWC, Cheng F, Huang XS. Recent advances in passive digital image security forensics: a brief review. Engineering. 2018;4(1):29–39. doi:10.1016/j.eng.2018.02.008.
11. Fahmi H, Sari WP. Effectiveness of deep learning architecture for pixel-based image forgery detection. In: Proceedings of the International Conference on Engineering, Technology and Social Science (ICONETOS 2020); 2020 Oct 31; Malang, Indonesia.
12. Kashyap A, Parmar RS, Agrawal M, Gupta H. An evaluation of digital image forgery detection approaches. Int J Appl Eng Res. 2017;12:4747–58.
13. Salman KA, Shaker K, Al-Janabi S. Fake colorized image detection approaches: a review. Int J Image Grap. 2023;23(6):2350050. doi:10.1142/s021946782350050x.
14. Ye G, Wu H, Liu M, Shi Y. Image encryption scheme based on blind signature and an improved Lorenz system. Expert Syst Appl. 2022;205(322):117709. doi:10.1016/j.eswa.2022.117709.
15. Farid H. Chapter 1 photo fakery and forensics. In: Advances in computers. Amsterdam, The Netherlands: Elsevier; 2009. p. 1–55. doi:10.1016/s0065-2458(09)01201-7.

16. Kaur CD, Kanwal N. An analysis of image forgery detection techniques. Stat, Optim Inf Comput. 2019;7(2):486–500. doi:10.19139/soic.v7i2.542.
17. Meena KB, Tyagi V. Image forgery detection: survey and future directions. In: Data, engineering and applications. Singapore: Springer Singapore; 2019. p. 163–94. doi:10.1007/978-981-13-6351-1_14.
18. Yang B, Sun X, Guo H, Xia Z, Chen X. A copy-move forgery detection method based on CMFD-SIFT. Multimed Tools Appl. 2018;77(1):837–55. doi:10.1007/s11042-016-4289-y.
19. Abdel-Basset M, Manogaran G, Fakhry AE, El-Henawy I. 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimed Tools Appl. 2020;79(7):5419–37. doi:10.1007/s11042-018-6266-0.
20. Mahmood T, Mehmood Z, Shah M, Saba T. A robust technique for copy-move forgery detection and localization in digital images *via* stationary wavelet and discrete cosine transform. J Vis Commun Image Represent. 2018;53:202–14. doi:10.1016/j.jvcir.2018.03.015.
21. Kuznetsov O, Frontoni E, Romeo L, Rosati R. Enhancing copy-move forgery detection through a novel CNN architecture and comprehensive dataset analysis [Internet]. Multimed Tools Appl. 2024;83(21):59783–817. doi:10.1007/s11042-023-17964-5.
22. Wang J, Gao X, Nie J, Wang X, Huang L, Nie W, et al. Strong robust copy-move forgery detection network based on layer-by-layer decoupling refinement [Internet]. Inf Process Manag. 2024;61(3):103685. doi:10.1016/j.ipm.2024.103685.
23. Dong J, Wang W, Tan T. CASIA image tampering detection evaluation database. In: 2013 IEEE China Summit and International Conference on Signal and Information Processing; 2013 Jul 6–10; Beijing, China. p. 422–6. doi:10.1109/ChinaSIP.2013.6625374.
24. Tralic D, Zupancic I, Grgic S, Grgic M. CoMoFoD—new database for copy-move forgery detection. In: Proceedings ELMAR—International Symposium Electronics in Marine; 2013 Sep 25–27; Zadar, Croatia.
25. Li Y, He Y, Chen C, Dong L, Li B, Zhou J, et al. Image copy-move forgery detection via deep PatchMatch and pairwise ranking learning [Internet]. IEEE Trans Image Process. 2025;34(4):425–40. doi:10.1109/tip.2024.3482191.
26. Gadiparthi NSS, Kadha JS, Palagiri VDR, Chadalavada G, Kumba GK, Rajan C. Multiple image tampering detection using deep learning algorithm [Internet]. In: 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI); 2023 May 25–26; Chennai, India. p. 1–7.
27. Gill NK, Garg R, Doegar EA. A review paper on digital image forgery detection techniques. In: 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT); 2017 Jul 3–5; Delhi, India. p. 1–7. doi:10.1109/ICCCNT.2017.8203904.
28. Huynh-Kha T, Le-Tien T, Ha-Viet-Uyen S, Huynh-Van K, Luong M. A robust algorithm of forgery detection in copy-move and spliced images. IJACSA. 2016;7(3):1–8. doi:10.14569/ijacsa.2016.070301.
29. Fan Y, Carré P, Fernandez-Maloigne C. Image splicing detection with local illumination estimation. In: 2015 IEEE International Conference on Image Processing (ICIP); 2015 Sep 27–30; Quebec City, QC, Canada. p. 2940–4. doi:10.1109/ICIP.2015.7351341.
30. Hariri M, Hakimi F. Image-splicing forgery detection based on improved LBP and K-nearest neighbors algorithm. Electron Inf Plan. 2015;3:7.
31. Alahmadi AA, Hussain M, Aboalsamh H, Muhammad G, Bebis G. Splicing image forgery detection based on DCT and local binary pattern. In: 2013 IEEE Global Conference on Signal and Information Processing; 2013 Dec 3–5; Austin, TX, USA. p. 253–6. doi:10.1109/GlobalSIP.2013.6736863.
32. Xing J, Tian X, Han Y. A dual-channel augmented attentive dense-convolutional network for power image splicing tamper detection. Neural Comput Appl. 2024;36(15):8301–16. doi:10.1007/s00521-024-09511-6.
33. Yang Z, Liu B, Bi X, Xiao B, Li W, Wang G, et al. D-Net: a dual-encoder network for image splicing forgery detection and localization. Pattern Recognit. 2024;155(8):110727. doi:10.1016/j.patcog.2024.110727.
34. Zhang D, Jiang N, Li F, Chen J, Liao X, Yang G, et al. Multi-scale noise-guided progressive network for image splicing detection and localization. Expert Syst Appl. 2024;257(7):124975. doi:10.1016/j.eswa.2024.124975.
35. Singh S, Kumar R, Singh CK. Identification of splice image forgeries with enhanced DenseNet201 and VGG19. In: Computation of artificial intelligence and machine learning. Cham, Switzerland: Springer; 2025. p. 113–23. doi:10.1007/978-3-031-71481-8_9.

36. Zanardelli M, Guerrini F, Leonardi R, Adami N. Image forgery detection: a survey of recent deep-learning approaches [Internet]. Multimed Tools Appl. 2023;82(12):17521– 66. [cited 2025 Jan 1]. doi:10.1007/s11042-022-13797-w.
37. Kumari R, Garg H. Image splicing forgery detection: a review. Multimed Tools Appl. 2025;84(8):4163–201. doi:10.1007/s11042-024-18801-z.
38. Xu J, Feng D, Wu J, Cui Z. An image inpainting technique based on 8-neighborhood fast sweeping method. In: 2009 WRI International Conference on Communications and Mobile Computing; 2009 Jan 6–8; Kunming, China. p. 626–30. doi:10.1109/CMC.2009.369.
39. Kumar M, Srivastava S. Image forgery detection based on physics and pixels: a study. Aust J Forensic Sci. 2019;51(2):119–34. doi:10.1080/00450618.2017.1356868.
40. Liu Q, Sung AH. A new approach for JPEG resize and image splicing detection. In: Proceedings of the First ACM Workshop on Multimedia in Forensics; 2009 Oct 23; Beijing, China. New York, NY, USA: ACM; 2009. p. 43–8. doi:10.1145/1631081.1631092.
41. Vázquez-Padín D, Pérez-González F, Comesaña-Alfaro P. A random matrix approach to the forensic analysis of upscaled images. IEEE Trans Inf Forensics Secur. 2017;12(9):2115–30. doi:10.1109/TIFS.2017.2699638.
42. Zhang L, Chen X, Niu Y, Zuo X, Wang H. Robust primary quantization step estimation on resized and double JPEG compressed images. Multimed Tools Appl. 2025;84(12):11097–118. doi:10.1007/s11042-024-19376-5.
43. Kadha V, Das SK. An exhaustive measurement of re-sampling detection in lossy compressed images using deep learning approach. Eng Appl Artif Intell. 2024;129(11):107614. doi:10.1016/j.engappai.2023.107614.
44. Wu Y, AbdAlmageed W, Natarajan P. *ManTra*-net: manipulation tracing network for detection and localization of image forgeries with anomalous features. In: IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); 2019 Jun 15-20; Long Beach, CA, USA. p. 9535–44. doi:10.1109/cvpr.2019.00977.
45. Wen B, Zhu Y, Subramanian R, Ng T-T, Shen X, Winkler S. COVERAGE—a novel database for copy-move forgery detection [Internet]. In: IEEE International Conference on Image Processing (ICIP); 2016 Sep 25-18; Phoenix, AZ, USA. p. 161–5. [cited 2025 Jan 1]. Available from: http://ieeexplore.ieee.org/document/7532339/.
46. Bo X, Junwen W, Guangjie L, Yuewei D. Image copy-move forgery detection based on SURF. In: 2010 International Conference on Multimedia Information Networking and Security; 2010 Nov 4–6; Nanjing, China. p. 889–92.
47. Gloe T, Böhme R. The Dresden image database for benchmarking digital image forensics. J Digit Forensic Pract. 2010;3(2–4):150–9. doi:10.1080/15567281.2010.531500.
48. Liu Y, Guan Q, Zhao X. Copy-move forgery detection based on convolutional kernel network. Multimed Tools Appl. 2018;77(14):18269–93. doi:10.1007/s11042-017-5374-6.
49. Paulin M, Douze M, Harchaoui Z, Mairal J, Perronin F, Schmid C. Local convolutional features with unsupervised training for image retrieval [Internet]. In: IEEE International Conference on Computer Vision (ICCV); 2015 Dec 7–13; Santiago, Chile. p. 91–9. [cited 2025 Jan 1]. Available from: http://ieeexplore.ieee.org/document/7410376/.
50. Bappy JH, Simons C, Nataraj L, Manjunath BS, Roy-Chowdhury AK. Hybrid LSTM and encoder-decoder architecture for detection of image forgeries. IEEE Trans Image Process. 2019;28(7):3286–300. doi:10.1109/TIP.2019.2895466.
51. Lu M, Niu S. A detection approach using LSTM-CNN for object removal caused by exemplar-based image inpainting. Electronics. 2020;9(5):858. doi:10.3390/electronics9050858.
52. Schaefer G, Stich M. UCID: an uncompressed color image database [Internet]. In: Yeung MM, Lienhart RW, Li C-S, editors. Storage and retrieval methods and applications for multimedia. Bellingham, WA, USA: Society of Photo Optical; 2004. p. 472–80. [cited 2025 Jan 1]. Available from: http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=837905.
53. Wu Y, Abd-Almageed W, Natarajan P. BusterNet: detecting copy-move image forgery with source/target localization. In: Ferrari V, Hebert M, Sminchisescu C, Weiss Y, editors. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). Cham, Switzerland: Springer International Publishing; 2018. p. 170–86. doi:10.1007/978-3-030-01231-1_11.
54. Zhu X, Qian Y, Zhao X, Sun B, Sun Y. A deep learning approach to patch-based image inpainting forensics. Signal Process Image Commun. 2018;67(2):90–9. doi:10.1016/j.image.2018.05.015.

55. Anwar S, Tahir M, Li C, Mian A, Khan FS, Muzaffar AW. Image colorization: a survey and dataset. Inf Fusion. 2025;114(3):102720. doi:10.1016/j.inffus.2024.102720.
56. de Rezende ERS, Ruppert GCS, Carvalho T. Detecting computer generated images with deep convolutional neural networks. In: 2017 30th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI); 2017 Oct 17–20; Niteroi, Brazil. p. 71–8. doi:10.1109/SIBGRAPI.2017.16.
57. Yu IJ, Kim DG, Park JS, Hou JU, Choi S, Lee HK. Identifying photorealistic computer graphics using convolutional neural networks. In: 2017 IEEE International Conference on Image Processing (ICIP); 2017 Sep 17–20; Beijing, China. p. 4093–7. doi:10.1109/ICIP.2017.8297052.
58. Quan W, Wang K, Yan DM, Zhang X. Distinguishing between natural and computer-generated images using convolutional neural networks. IEEE Trans Inf Forensics Secur. 2018;13(11):2772–87. doi:10.1109/TIFS.2018.2834147.
59. Tariang DB, Sengupta P, Roy A, Chakraborty RS, Naskar R. Classification of computer generated and natural images based on efficient deep convolutional recurrent attention model. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops; 2019 Jun 15–20; Long Beach, CA, USA. p. 146–52.
60. Zhang RS, Quan WZ, Fan LB, Hu LM, Yan DM. Distinguishing computer-generated images from natural images using channel and pixel correlation. J Comput Sci Technol. 2020;35(3):592–602. doi:10.1007/s11390-020-0216-9.
61. He P, Li H, Wang H, Zhang R. Detection of computer graphics using attention-based dual-branch convolutional neural network from fused color components. Sensors. 2020;20(17):4743. doi:10.3390/s20174743.
62. Quan W, Wang K, Yan DM, Zhang X, Pellerin D. Learn with diversity and from harder samples: improving the generalization of CNN-based detection of computer-generated images. Forensic Sci Int Digit Investig. 2020;35(3):301023. doi:10.1016/j.fsidi.2020.301023.
63. Ng TT, Chang SF, Hsu J, Pepeljugoski M. Columbia photographic images and photorealistic computer graphics dataset ADVENT. New York, NY, USA: Columbia University; 2004.
64. Deng J, Dong W, Socher R, Li LJ, Kai L, Li FF. ImageNet: a large-scale hierarchical image database. In: 2009 IEEE Conference on Computer Vision and Pattern Recognition; 2009 Jun 20–25; Miami, FL, USA. p. 248–55. doi:10.1109/CVPR.2009.5206848.
65. Bouhamidi Y, Wang K. Simple methods for improving the forensic classification between computer-graphics images and natural images. Forensic Sci. 2024;4(1):164–83. doi:10.3390/forensicsci4010010.
66. Rahmouni N, Nozick V, Yamagishi J, Echizen I. Distinguishing computer graphics from natural images using convolution neural networks. In: 2017 IEEE Workshop on Information Forensics and Security (WIFS); 2017 Dec 4–7; Rennes. p. 1–6. doi:10.1109/WIFS.2017.8267647.
67. He P, Jiang X, Sun T, Li H. Computer graphics identification combining convolutional and recurrent neural networks. IEEE Signal Process Lett. 2018;25(9):1369–73. doi:10.1109/LSP.2018.2855566.
68. Shullani D, Fontani M, Iuliani M, Al Shaya O, Piva A. VISION: a video and image dataset for source identification. EURASIP J Inf Secur. 2017;2017(1):15. doi:10.1186/s13635-017-0067-2.
69. Budakov P. 3D-rendered images and their application in the interior design [Internet]. In: Encyclopedia of computer graphics and games. Cham, Switzerland: Springer International Publishing; 2024. p. 62–70. [cited 2025 Jan 1]. doi:10.1007/978-3-031-23161-2_262.
70. Qian LZ, Che H-Y. Computer graphics 3D and rendering practice design research [Internet]. In: 2nd International Conference on Computer Graphics and Image Processing (CGIP); 2024 Jan 12–15; Kyoto, Japan. p. 91–5. [cited 2025 Jan 1]. Available from: https://ieeexplore.ieee.org/document/10533417/.
71. Tokuda E, Pedrini H, Rocha A. Computer generated images *vs*. digital photographs: a synergetic feature and classifier combination approach. J Vis Commun Image Represent. 2013;24(8):1276–92. doi:10.1016/j.jvcir.2013.08.009.
72. Dang-Nguyen DT, Pasquini C, Conotter V, Boato G. RAISE: a raw images dataset for digital image forensics. In: Proceedings of the 6th ACM Multimedia Systems Conference; 2015 Mar 18–20; Portland, OR, USA. New York, NY, USA: ACM; 2015. p. 219–24. doi:10.1145/2713168.2713194.
73. Bondi L, Baroffio L, Güera D, Bestagini P, Delp EJ, Tubaro S. First steps toward camera model identification with convolutional neural networks. IEEE Signal Process Lett. 2017;24(3):259–63. doi:10.1109/LSP.2016.2641006.

74. Tuama A, Comby F, Chaumont M. Camera model identification with the use of deep convolutional neural networks. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS); 2016 Dec 4–7; Abu Dhabi, United Arab Emirates. p. 1–6. doi:10.1109/WIFS.2016.7823908.
75. Bayar B, Stamm MC. Towards open set camera model identification using a deep learning framework. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2018 Apr 15–20; Calgary, AB, Canada. p. 2007–11. doi:10.1109/ICASSP.2018.8462383.
76. Cozzolino D, Verdoliva L. Noiseprint: a CNN-based camera model fingerprint. IEEE Trans Inf Forensics Secur. 2019;15:144–59. doi:10.1109/TIFS.2019.2916364.
77. Sameer VU, Naskar R. Deep Siamese network for limited labels classification in source camera identification. Multimed Tools Appl. 2020;79(37):28079–104. doi:10.1007/s11042-020-09106-y.
78. Nguyen A, Yosinski J, Clune J. Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR); 2015 Jun 7–12; Boston, MA, USA. p. 427–36. doi:10.1109/CVPR.2015.7298640.
79. Szegedy C, Zaremba W, Sutskever I, Bruna J, Erhan D, Goodfellow I, et al. Intriguing properties of neural networks. In: 2nd International Conference on Learning Representations, ICLR 2014—Conference Track Proceedings; 2014 Apr 14–16; Banff, AB, Canada.
80. Chen C, Zhao X, Stamm MC. Mislgan: an anti-forensic camera model falsification framework using a generative adversarial network. In: 25th IEEE International Conference on Image Processing (ICIP); 2018 Oct 7–10; Athens, Greece. p. 535–9. doi:10.1109/ICIP.2018.8451503.
81. Chen C, Zhao X, Stamm MC. Generative adversarial attacks against deep-learning-based camera model identification. IEEE Trans Inf Forensics Secur. 2019; 99. doi:10.1109/TIFS.2019.2945198.
82. Cui Q, Meng RH, Zhou ZL, Sun XM, Zhu KW. An anti-forensic scheme on computer graphic images and natural images using generative adversarial networks. Math Biosci Eng. 2019;16(5):4923–35. doi:10.3934/mbe.2019248.
83. Barni M, Kallas K, Nowroozi E, Tondi B. On the transferability of adversarial examples against CNN-based image forensics. In: ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2019 May 12–17; Brighton, UK. p. 8286–90. doi:10.1109/icassp.2019.8683772.
84. Liu Z, Luo P, Wang X, Tang X. Deep learning face attributes in the wild. In: 2015 IEEE International Conference on Computer Vision (ICCV); 2015 Dec 7–13; Santiago, Chile. p. 3730–8. doi:10.1109/ICCV.2015.425.
85. Cheng Z, Meng F, Mao J. Semi-auto sketch colorization based on conditional generative adversarial networks. In: 2019 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI); 2019 Oct 19–21; Suzhou, China. p. 1–5. doi:10.1109/cisp-bmei48845.2019.8965999.
86. Žeger I, Grgic S, Vuković J, Šišul G. Grayscale image colorization methods: overview and evaluation. IEEE Access. 2021;9:113326–46. doi:10.1109/access.2021.3104515.
87. Welsh T, Ashikhmin M, Mueller K. Transferring color to greyscale images. ACM Trans Graph. 2002;21(3):277–80. doi:10.1145/566654.566576.
88. Weitz A. The basics of hand-coloring black-and-white prints. New York, NY, USA: B&H eXplora; 2020.
89. Gable G. Scanning around with gene: the miracle of photochrom, CreativePro network 2009. [cited 2024 Mar 18]. Available from: https://creativepro.com/scanning-around-gene-miracle-photochrom/.
90. ODSC-Open Data Science. Wonders in image processing with machine learning. San Francisco, CA, USA: Medium; 2019 [cited 2025 Jan 10]. Available from: https://odsc.medium.com/wonders-in-image-processing-with-machine-learning-9c6f2e070e99.
91. Guo Y, Cao X, Zhang W, Wang R. Fake colorized image detection. IEEE Trans Inf Forensics Secur. 2018;13(8):1932–44. doi:10.1109/TIFS.2018.2806926.
92. Agarwal S, Sharma D, Jung KH. Forensic analysis of colorized grayscale images using local binary pattern. In: Proceedings of the 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence); 2020 Jan 29–31; Noida, India. p. 507–10. doi:10.1109/confluence47617.2020.9057922.
93. Yu Y, Zheng N, Qiao T, Xu M, Wu J. Distinguishing between natural and recolored images *via* lateral chromatic aberration. J Vis Commun Image Represent. 2021;80(8):103295. doi:10.1016/j.jvcir.2021.103295.

94. Zhang Y, Chen N, Qi S, Xue M, Hua Z. Detection of recolored image by texture features in chrominance components. ACM Trans Multimedia Comput Commun Appl. 2023;19(3):1–23. doi:10.1145/3571076.
95. Agarwal S, Jung K-H. Forensic analysis and detection using polycolor model binary pattern for colorized images [Internet]. Multimed Tools Appl. 2024;83(14):41683–702. doi:10.1007/s11042-023-16675-1.
96. Bai Y, Guo Y, Wei J, Lu L, Wang R, Wang Y. Fake generated painting detection via frequency analysis [Internet]. In: IEEE International Conference on Image Processing (ICIP); 2020 Oct 25–28; Abu Dhabi, United Arab Emirates. p. 1256–60. [cited 2025 Jan 1]. Available from: https://ieeexplore.ieee.org/document/9190892/
97. Castro M, Ballesteros DM, Renza D. A dataset of 1050-tampered color and grayscale images (CG-1050) [Internet]. Data Brief. 2020;28(2019):104864. doi:10.1016/j.dib.2019.104864.
98. Chen N, Qi S, Zhang Y, Xue M, Hua Z. Image recolorization detection based on inter-channel correlation [Internet]. Chin J Netw Inf Secur. 2022;8(5):167–78.
99. Pillai N, Kanthe DA, Bhattacharjee S. Enriching fake colorized image detection. Int J Res Anal Rev. 2019;6(2):255–61.
100. Salman KA, Shaker K, Al-Janabi S. Fake colorized image detection based on special image representation and transfer learning. Int J Comp Intel Appl. 2023;22(3):2350018. doi:10.1142/s1469026823500189.
101. Li Y, Zhang Y, Lu L, Jia Y, Liu J. Using neural networks for fake colorized image detection. In: Peterson G, Shenoi S, editor. Advances in digital forensics XV. Cham, Switzerland: Springer International Publishing; 2019. p. 201–15. doi:10.1007/978-3-030-28752-8_11.
102. Yousaf B, Usama M, Sultani W, Mahmood A, Qadir J. Fake visual content detection using two-stream convolutional neural networks [Internet]. Neural Comput Appl. 2022;34(10):7991– 8004. [cited 2025 Jan 10]. doi:10.1007/s00521-022-06902-5.
103. Ananthi M, Rajkumar P, Sabitha R, Karthik S. A secure model on advanced fake image-feature network (AFIFN) based on deep learning for image forgery detection [Internet]. Pattern Recognit Lett. 2021;152(1):260– 6. [cited 2025 Jan 10]. doi:10.1016/j.patrec.2021.10.011.
104. Selva Birunda S, Nagaraj P, Krishna Narayanan S, Muthamil Sudar K, Muneeswaran V, Ramana R. Fake image detection in twitter using flood fill algorithm and deep neural networks [Internet]. In: 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence); 2022 Jan 27–28; Noida, India. p. 285–90. [cited 2025 Jan 10]. Available from: https://ieeexplore.ieee.org/document/9734208/.
105. Ulloa C, Ballesteros DM, Renza D. Video forensics: identifying colorized images using deep learning. applied sciences [Internet]. Appl Sci. 2021;11(2):476. [cited 2025 Jan 1]. doi:10.3390/app11020476.
106. Yang Z, Yu Z, Liang Y, Guo R, Xiang Z. Computer generated colorized image forgery detection using VLAD encoding and SVM [Internet]. In: 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC); 2020 Dec 13; Chongqing, China. p. 272–9. [cited 2025 Jan 1]. Available from: https://ieeexplore.ieee.org/document/9339027/.
107. Quan W, Wang K, Yan D-M, Pellerin D, Zhang X. Improving the generalization of colorized image detection with enhanced training of CNN [Internet]. In: 2019 11th International Symposium on Image and Signal Processing and Analysis (ISPA); 2020 Sep 23–25; Dubrovnik, Croatia. p. 246–52. [cited 2025 Jan 10]. Available from: https://ieeexplore.ieee.org/document/8868802/.
108. Quan W, Wang K, Yan D-M, Pellerin D, Zhang X. Impact of data preparation and CNN's first layer on performance of image forensics: a case study of detecting colorized images [Internet]. In: IEEE/WIC/ACM International Conference on Web Intelligence—Companion Volume; 2019 Oct 14–17; Thessaloniki, Greece. New York, NY, USA: ACM; 2019. p. 127–31. [cited 2025 Jan 1]. Available from: https://dl.acm.org/doi/10.1145/3358695.3360890.
109. Yan Y, Ren W, Cao X. Recolored image detection via a deep discriminative model. IEEE Trans Inf Forensics Secur. 2019;14(1):5–17. doi:10.1109/TIFS.2018.2834155.
110. Swathi B, Jhade S, Santosh Reddy P, Gottumukkala L, Subbarayudu Y. An efficient novel approach for detection of recolored image using deep learning for identifying the original images in public surveillance. In: Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems. Advances in Intelligent Systems and Computing. Singapore: Springer; 2022. p. 275–86. doi:10.1007/978-981-16-7330-6_21.

111. Quan W, Yan DM, Wang K, Zhang X, Pellerin D. Detecting colorized images *via* convolutional neural networks: toward high accuracy and good generalization. arXiv:1902.06222. 2019.
112. Shashikala S, Ravikumar GK. Ensemble deep learning fusion for detection of colorization based image forgeries. In: 2023 2nd International Conference for Innovation in Technology (INOCON); 2023 Mar 3–5; Bangalore, India. p. 1–9. doi:10.1109/INOCON57975.2023.10101337.