Multimedia Tools and Applications (2024) 83:67871–67902
https://doi.org/10.1007/s11042-023-18090-y

A survey on digital image forensic methods based on blind forgery detection

Deependra Kumar Shukla[1] · **Abhishek Bansal**[2] · **Pawan Singh**[3]

Received: 9 October 2022 / Revised: 26 September 2023 / Accepted: 29 December 2023 /
Published online: 29 January 2024

Abstract
In the current digital era, images have become one of the key channels for communication and information. There are multiple platforms where digital images are used as an essential identity, like social media platforms, chat applications, electronic and print media, medical science, forensics and criminal investigation, the court of law, and many more. Alternation of digital images becomes easy because multiple image editing software applications are accessible freely on the internet. These modified images can create severe problems in the field where the correctness of the image is essential. In such situations, the authenticity of the digital images from the bare eye is almost impossible. To prove the validity of the digital images, we have only one option: Digital Image Forensics (DIF). This study reviewed various image forgery and image forgery detection methods based on blind forgery detection techniques mainly. We describe the essential components of these approaches, as well as the datasets used to train and verify them. Performance analysis of these methods on various metrics is also discussed here.

Keywords Forgery · Copy-move · Cloning · Imaging device · Digital forensic · Deep-learning

✉ Pawan Singh
pawan.singh@curaj.ac.in

Deependra Kumar Shukla
deependrashuklag@gmail.com

Abhishek Bansal
abhishek.bansal@dhsgsu.edu.in

[1] Department of Computer Science, Indira Gandhi National Tribal University, Amarkantak, Madhya Pradesh 484887, India

[2] Department of Computer Science & Applications, Dr. Harisingh Gour Vishwavidyalaya, Sagar, Madhya Pradesh 470003, India

[3] Department of Computer Science, Central University of Rajasthan, Ajmer, Rajasthan 305817, India

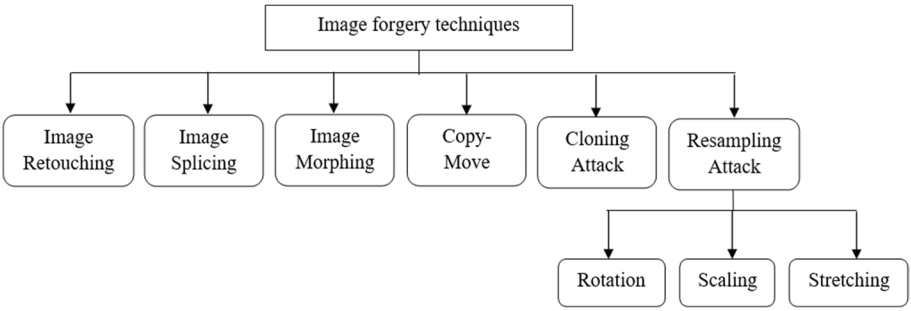

Fig. 1 Different image forgery methods

(a) Genuine image. (b) Image after retouching.

Fig. 2 Retouching image forgery [13]

1 Introduction

The term "digital image forgery" refers to the process of creating fake or altered images. Altering images is now effortless due to publicly available powerful image editing tools like Corel PaintShop Pro, Affinity Photo, ACDsee photo editor, and Adobe Photoshop [1–6]. We have used a systematic literature review methodology to write this review paper. We have identified and critically appraised relevant research for collecting and analysing data for blind forgery detection techniques.

Digital image fraud has occurred in several ways. On the basis of techniques used to generate fake images, all of these examples can be categorised into seven categories: Splicing, Retouching, Morphing, Copy-Move or Cloning, Inpainting, Resampling, and Deep-fakes [7–10]. Figure 1 demonstrates the various types of image forgery methods:

1.1 Image retouching

Maximizing or minimizing any particular feature of the image is called image retouching. This technique is less harmful and is commonly used by the magazine's photo editors. Most probably, all the magazine cover photos use this technique to enhance any particular image aspect to make it more attractive. At the same time, such modifications are unethical [10–12]. Figure 2 is an excellent sample of retouching forgery. Sub-image

(a) Genuine images (b) Spliced image

Fig. 3 Image splicing forgery [17]

(a) Original image (b) Morphed image (c) Original image

Fig. 4 Image morphing Forgery [21]

(a) is an authentic image, and sub-image (b) is an altered image created by retouching [13].

1.2 Image splicing

In image splicing, an altered image is created using the different portions of two or more images. To make spliced images, simple cut and paste method is used. This technique of creating fake images is very popular among attackers. These spliced images can be propagated on social media with bad intentions. Therefore, we can say that this method can create more trouble than image retouching [10, 11, 14–16]. Figure 3 demonstrates the image splicing.

Here, sub-image (a) is a genuine image, and sub-image (b) is the spliced version of the genuine image.

1.3 Morphing

The transformation of one image into another with the help of intermediate images is called image morphing. The goal is to create a series of intermediate images that indicate the transition from one image to another when combined with the originals [18–20]. Figure 4 shows the image morphing forgery. Sub-image (a) and sub-image (c) are the authentic images, whereas sub-image (b) is the morphed image of (i) and (iii) images [21].

(a) Authentic image. (b) Image created by a copy-move attack

Fig. 5 Copy- Move image forgery [25]

(a) genuine image (b) Masked image (c) Inpainted image

Fig. 6 Image Inpainting Forgery[28]

1.4 Copy-Move or Cloning attack

In the copy-move attack, the attacker copied from one region of the image and pasted that onto other regions of the same image to remove any specific portion from the image. This attack is used to create forged images [4, 8, 10, 11, 15, 22–24]. Figure 5 demonstrates the copy-move attack in digital photographs. Sub-image (a) is the authentic image, whereas sub-image (b) is the altered image created by a copy-move attack [25].

1.5 Image Inpainting

Generally, image inpainting is used to fill blank-spaces or corrupted regions whitin the image. Unfortunately, attackers used this approach to conceal a specific portion of the image with malicious intentions to create a fake image [26, 27]. Figure 6 demonstrate an excellent example of image inpainting. Figure 6 has three sections a, b, and c. Section a

contains two original images, section b contains the masked image of images in section a, then finally inpainted images corresponding to masked images are created in section c.

1.6 Resampling attack

Resampling involves generating a modified version of the original image through operations like stretching, rotation, and scaling [9]. To fraudulently geometrically change a digital image or a piece of a digital image, the resampling technique uses interpolation algorithms [29]. Figure 7 shows the Resampling forgery with flipping, scaling, and rotation operation.

Here in the Fig. 7, sub-image (a) is the authentic image, sub-image (b) is the resampled image by using the flipping operation, sub-image (c) is the resampled image with scaling, and sub-image (d) is the resampled image with the scaling and rotation operation [30].

1.7 Deep-fake images

Other than above mentioned traditional ways of forging images, currently new methods have been developed to create a fake image using Artificial Intelligence techniques called deep-fake. Deepfake images are computer-generated or altered pictures produced through advanced machine learning methods like Generative Adversarial Networks (GANs). These images convincingly depict individuals, objects, or environments that either never existed or have been substantially modified [27, 31].

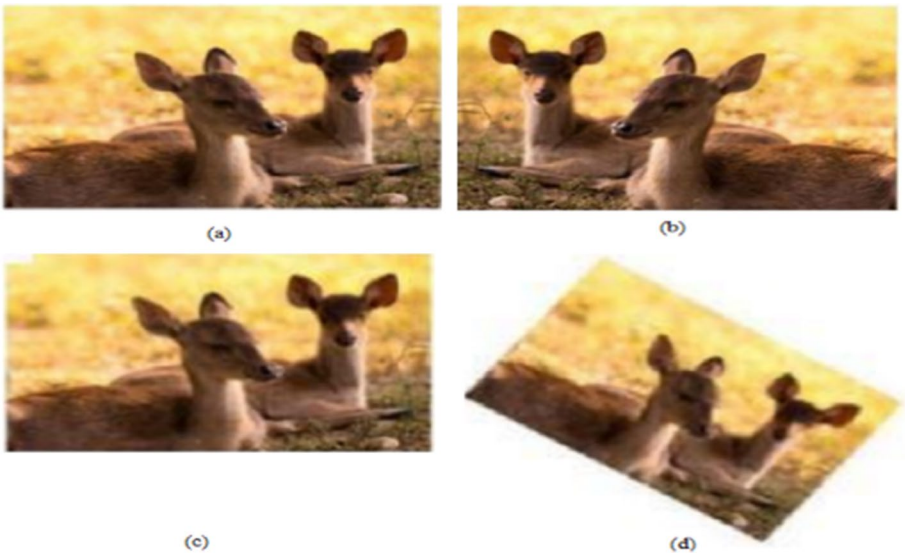

Fig. 7 Resampling Image forgery [30]

2 Digital image forensic

We have seen various ways to forge an image and destroy its integrity. So here, one crucial question arrives how to prove the image's purity and reliability? The answer to this question is Digital image forensics (DIF). DIF is the most recent field of research that solves two fundamental issues: imaging device identification and forgery or tamper detection [32]. In DIF, two methods are available to detect the alternation in the altered images. The first approach is the Active technique**,** and the second approach is the Inactive or Blind or Passive technique [33–36]. Figure 8 shows the different forgery detection techniques.

2.1 Active techniques

These techniques need previous knowledge about the image elements linked to the image, such as information related to steganography, water-marking or digital signature [8, 9, 27, 37, 38].

2.1.1 Steganography

In steganography, confidential data like text, images, or videos are hidden using the cover image. To achieve steganography, steganographic techniques are of two categories. The first is frequency domain methods, and the second is spatial domain methods [39–41].

2.1.2 Water-marking

Inserting a piece of confidential information in the digital image to preserve its integrity is known as water-marking. A water-mark in an image can be either visible or invisible [42, 43].

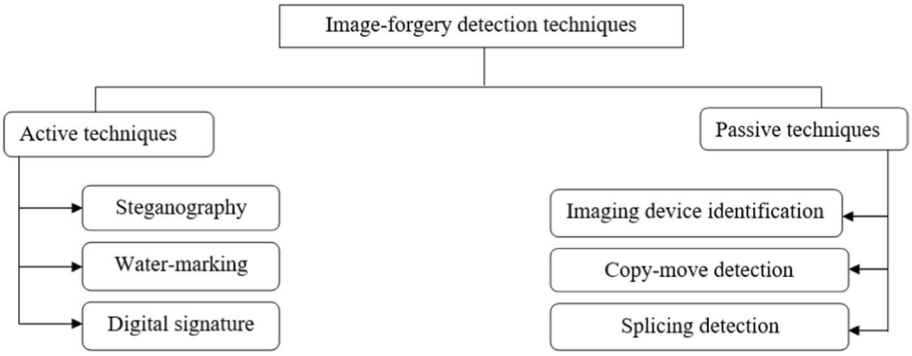

Fig. 8 Techniques of image fraud detection

2.1.3 Digital signature

Digital signatures can also be inserted into the image during its creation to preserve the purity of the image. Digital signatures can be extracted and compared to confirm the image's authenticity [10].

2.2 Passive Techniques

This technique does not require any previous knowledge related to image; therefore, this technique is also known as the blind technique [8, 9, 27, 37, 38]. Our primary focus in this survey is to study passive or blind forgery detection methods. Passive forgery detection includes Imaging device identification, copy-move detection, and splicing detection. Figure 9 demonstrate the different components of blind forgery detection methods [44].

All possible steps shown in Fig. 9 are widely explained in the following section.

Input: Suspicious images will be given as input to detect possible blind forgery [45].
Pre-processing: It is an optional step. Some images required it, and some did not. Some pre-processing operations are given as RGB to Gray-scale, RGB to YCbCr, RGB to HSV, Image resizing, etc. [45].
Feature extraction: Extraction of image features is essential for passive forgery detection. Some methods to extract features from the digital image are DCT, DWT, FMT, Zernike moments, SIFT, SURF, CNN, ResNet50, VGG19, contourlet transform, etc. [45].
Feature matching: Feature matching is employed to identify duplicated regions, where a strong resemblance between two feature descriptors serves as an indicator of such regions. Methods used for matching are PatchMatch, LSH, Lexicographical sorting, g2NN, k-d tree, Counting BloomFilters, etc. [45].
Filtering: This step is applied to minimize the probability of false matching [45].
Post-processing: Post-processing is applied to remove the false detection [45].
Output: In this step input image is classified as forged or genuine image.

2.2.1 Imaging device identification

Imaging device identification techniques recognize the inherent evidence left in the images by the corresponding imaging device or source camera used in the acquisition of the image [8, 46]. Imaging device identification techniques examine the footprints left behind during the acquisition of the image to frame a fingerprint that can recognize the imaging device or camera model. In particular, source camera authentication can offer helpful technological support for judicial verification. Imaging device identification plays a significant role in enhancing the security of photographs, settling copyright issues, avoiding false publicity, and combatting cybercrime along with compensation claims, child exploitation, and criminal proceedings [47]. This survey paper presents the performance of different methods in relation to precision, recall, F-1 score, and accuracy. Apart from these metrics we have provided details of other metrics like FPR, FNR, and TNR bot not utilized in this paper. These performance parameters are based on True

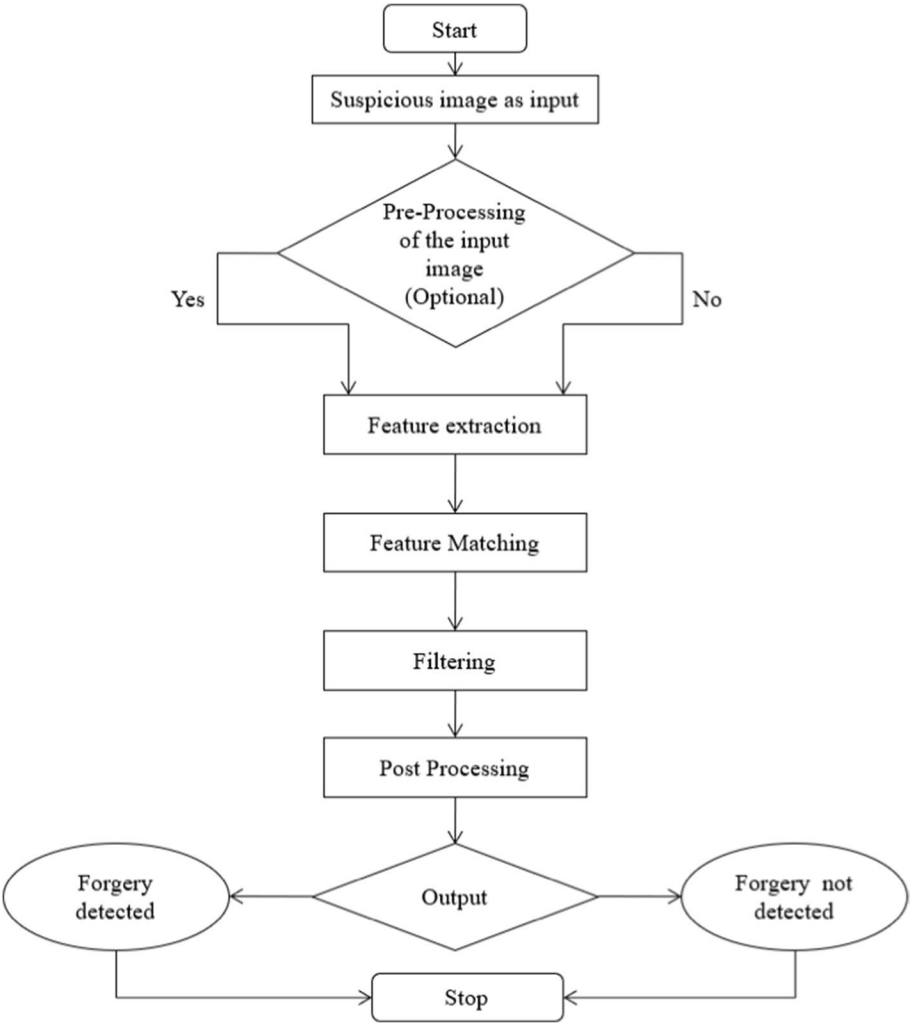

Fig. 9 Components of blind forgery detection

positive, True negative, False positive, and False negative. According to [22, 48] True positive, True negative, False positive, and False negative are defined as follows.

True positive (T_p): True positive means the number of correctly identified forgeries.
True negative (T_n): True negative means the number of correctly identified non-forgery.
False positive (F_p): False positive means the number of wrongly detected forgeries.
False negative (F_n): False negative means the number of un-detected forgeries.

Precision Precision shows us the percentage of correct positive predictions made. Precision can be calculated by using the Eq. (1) in terms of % [22, 48, 49]:

$$\text{Precision} = \frac{\text{Tp}}{\text{Tp} + \text{Fp}} * 100\% \tag{1}$$

Recall Recall shows us the percentage of positive predictions made out of all positive predictions. Recall can be calculated by using the Eq. (2) in terms of % [22, 48, 49]:

$$\text{Recall} = \frac{\text{Tp}}{\text{Tp} + \text{Fn}} * 100\% \tag{2}$$

F-1 Score The harmonic mean of precision and recall is the F-1 score. F-1 score can be calculated by using the Eq. (3) in terms of % [22, 48, 49]:

$$\text{F-1 score} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} * 100\% \tag{3}$$

Accuracy Accuracy shows us the percentage of correct predictions out of all predictions. Precision can be calculated by using the Eq. (4) in terms of % [22, 48]:

$$\text{Accuracy} = \frac{\text{Tp} + \text{Tn}}{\text{Tp} + \text{Tn} + \text{Fp} + \text{Fn}} * 100\% \tag{4}$$

False positive rate False positive rate is given by Eq. (5) in terms of % [50–52].

$$\text{Falsepositiverate(FPR)} = \frac{\text{Fp}}{\text{Tn} + \text{Fp}} * 100\% \tag{5}$$

False negative rate False negative rate is given by Eq. (6) in terms of % [50, 51].

$$\text{Falsenegativerate(FNR)} = \frac{\text{Fn}}{\text{Tp} + \text{Fn}} * 100\% \tag{6}$$

True negative rate True negative rate is given by the Eq. (7) in terms of % [51].

$$\text{Truenegativerate(TNR)} = \frac{\text{Tn}}{\text{Fp} + \text{Tn}} * 100\% \tag{7}$$

Figure 10 shows the primary methods used in imaging device identification.

i. Photo-response-noise-uniformity (PRNU) based methods

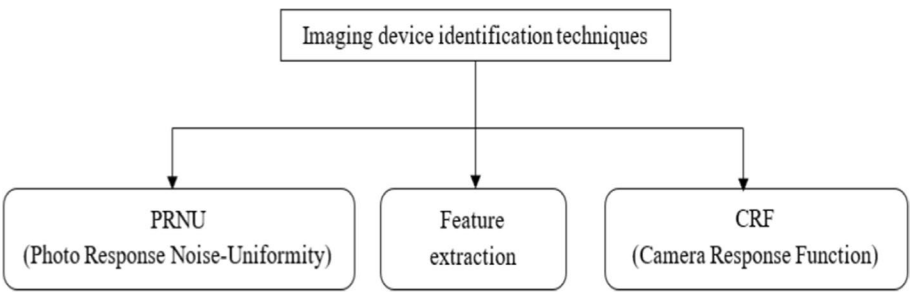

Fig. 10 Imaging device identification techniques

PRNU is used to recognize the corresponding imaging device from which the image is taken. PRNU noise pattern is extracted from the input image [53]. Here we have provided two PRNU-based imaging device identification methods.

- [54] Proposes a model to identify imaging devices based on PRNU extraction using a denoising filter. From acquired data like photographs or videos, the "Photo Response Noise Uniformity" is a unique pattern that can be utilized to identify the model of the source imaging devices. A reference pattern or fingerprint can be generated by averaging the obtained PRNU patterns from the image. The query image from the testing data is accurately classified after analysis of all the reference patterns of 25 devices by comparing the correlation values. The developed model is tested using 125 photos form Dresden Image Database. Since the correlation value is determined statistically, the accuracy is 100%. The suggested solution is tested on limited camera models and their images (25 camera models and 125 images) therefore accuracy of the suggested approach must be examined over bigger datasets. Robustness of the model's performance should also be examined over various image attacks.
- [55] Proposes a new approach that concentrates on the pixel that participates in sensor noise in the PRNU pattern to distinguish imaging devices (cameras) of the same type. The Jaccard coefficient is used to calculate the proportion of similar pixel locations shared between two devices' noise patterns. Their test findings demonstrate that using cameras of the same kind from the Apple iPhone 6, FujiFilm, Panasonic, and Sony cameras, the proposed system can correctly identify the device origin of the image. The suggested approach accurately distinguishes between two Apple iPhone 6 devices that are identical with 100% precision, With 100% accuracy, the FujiFilmXTlO, 97.50% accuracy for the Panasonic DMC-FZlOOO, and 98.73% accuracy for the Sony ILCE-6000. The Performance of the proposed solution is tested on only four camera models therefore system performance must be examined on more camera models. Apart from this, suggested solution can be extended for Source imaging device identification when image is taken from similar type of imaging device.

ii. Feature extraction-based methods

Feature extraction-based techniques uses the extracted feature from the image to identify the imaging device. Here we have provided a study that uses the extracted feature from the image to identify the imaging device. [56] Proposed a method for identifying the source camera using the texture features of the image, which are taken from selected color models and color channels. They separately extracted local binary pattern (LBP) features, the coefficient of the contourlet transform, and residual noise images from the original image in the recommended work. They also separately extract features of Local phase quantization (LPQ) from the residual and authentic images. Hue saturation value (HSV) color space is used to extract the LBP and LPQ characteristics. Then, they merge LPQ and LBP as distinct features to identify the camera source and input them into a "Multi-class Lib-SVM" classifier. The following are the primary benefits of the suggested method:

- Images taken with the same brand and model of imaging devices can nevertheless be distinguished from one another.
- It can withstand treatments that preserve content or geometric alternations such as scaling, rotation, and JEPG compression.

The experimental outcomes demonstrate that the suggested strategy achieves 99.76% of detection accuracy. The proposed model used the 300 images for training and 300 images for testing, therefore its performance must be examined over the bigger datasets. Apart from this suggested solution uses the fixed size images therefore this work can be extended for the variable size images.

iii. Camera response function-based methods

The camera response function is used to relate the scene radiance to the intensity value[57]. Here we have provided a study in which CRF is used to identify imaging devices. According to the literature [58], when luminosity occurs at a sensor, the sensor associates a pixel with the intensity value to the associated pixel in the image by camera response functions (CRFs). The nonlinearity of CRFs impacts a few techniques like de-blurring, photometric stereo, etc. The proposed work concluded in three remarks: Firstly, radiometric calibration is made simpler with the help of decreasing the number of basis vectors while preserving the same level of fit. Secondly, if CRFs can be predicted with high enough accuracy, they may still be useful for forensic purposes despite having less diversity. Finally, it demonstrated that the requirement to calibrate the imaging device prior to de-blurring radiometrically is substantially loosened in that ringing effects might frequently be avoided using an average CRF. In this study, they performed experiments and successfully differentiated with an average accuracy of 96% to distinguish between a film CRF and a digital camera CRF. The suggested solution uses a variety of digital camera models but the models performance can be examined by including the mobile camera's in the dataset (Table 1). Otherthan this one can aim to examine camera modes that employ tone-mapping techniques using specific pixel patch analysis.

2.2.2 Copy-move detection

The primary objective of these techniques is to identify the areas in an image where a copied part of the same image is pasted to detect the forgery [8, 10, 18]. The attacker can also alter the copied region. Hence, the primary objective of a copy-move operation is to remove or hide the elements of the picture to remove its legitimacy. After a copy-move process, the altered images could then go through further processing, including rescaling, filtering, and noise dispersion to hide the signs of forgery [8]. Figure 11 represents the methods of copy-move fraud detection.

a) **Key-points based methods**

Methods based on Key-Point to detect copy-move fraud bring out features or key points from the altered images, such as SIFT, geometric transformation, or robust noise. Key-point-based methods have a better time complexity than block-based methods[59].

- Scale-invariant feature transform (SIFT) is a key-point-based method. [60] proposed a new scheme to detect copy-move fraud based on key-points. This study used the SIFT method for key-point extraction because of the SIFT algorithm's rotation and scaling invariance characteristics. Sometimes SIFT algorithm is unable to bring out enough features from the smooth region. To overcome this drawback, they partitioned the image into texture as well as smooth areas. Using the SIFT algorithm, they bring out the features only from the texture regions whereas feature from the

Table 1 Summarizes the work related to imaging device identification

Title of the paper with citation	Publication year	Method used	Explanation of used method	proposed scheme Performance
"Source Camera Identification using Photo Response Noise Uniformity" [54]	2019	PRNU	This method uses the noise created by the imaging sensors during the process of acquisition which helps to construct a fingerprint or signature that identifies the model of the imaging device	Accuracy = 100%
"PRNU-based Source Camera Identification for Multimedia Forensics**"** [55]	2021	PRNU	In the Proposed work, The Jaccard coefficient is used to calculate the proportion of similar pixel locations shared between two devices' noise patterns	Accuracy = 100% for two apple iPhone 6, 100% for FujiFilmXTlO,97.50% for DMC-FZlOOO,and 98.73% for Sony ILCE-6000
"Source camera identification from image texture features" [56]	2016	Feature Extraction	These techniques use a set of attributes brought out from an image to identify signs in images captured with the same sensor	Accuracy = 99.76%
"Analyzing Modern Camera Response Functions" [58]	2019	CRF	The sensor collects luminance in a non-linear fashion, and the imaging device's signatures are made using information associated with this relationship	Average Accuracy = 96%

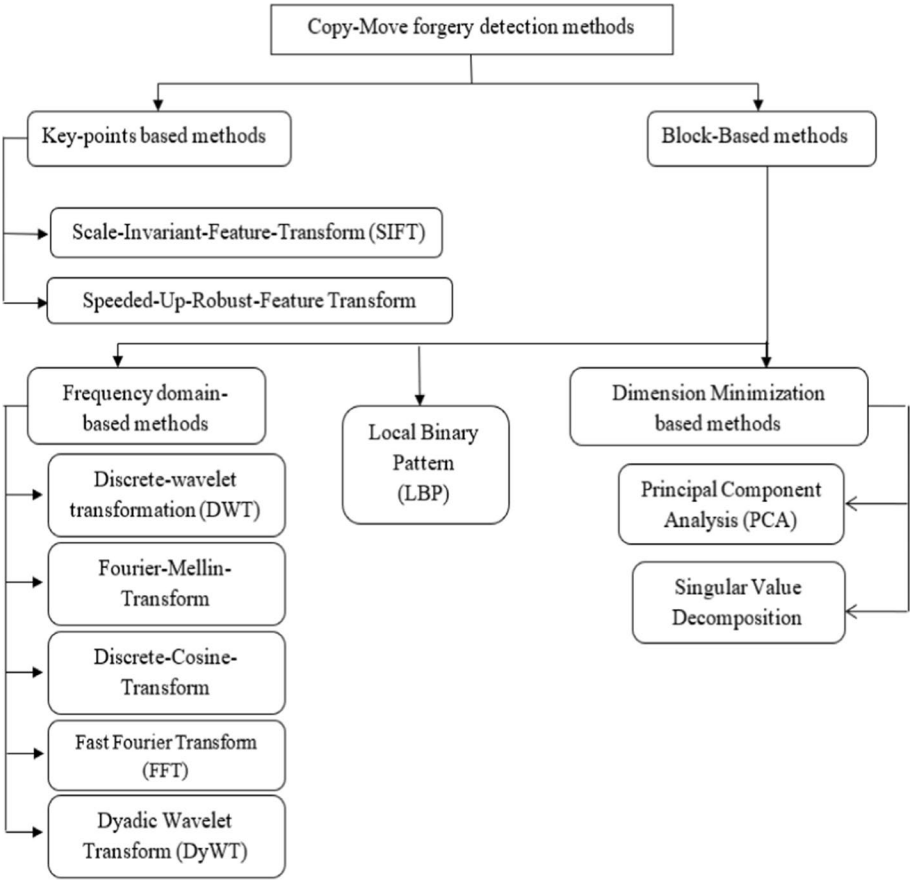

Fig. 11 Various methods for the detection of copy-move fraud

smooth regions were extracted using the Fourier Mellin Transform (FMT). The suggested models achieves 96.97% F-score. The suggested solution can be extended for detecting copy-move frauds in videos.

- SURF(Speeded-Up-Robust-Transform) is an efficient as well as a reliable technique for local representation of similarity-invariant and comparison of pictures. [61] used the SURF method in the proposed work for key-point identification and extraction, showing its performance among other methods. The proposed technique detected modified plain copy-move and duplicate regions on several datasets, including CoMoFoD, MICCF220, MICC-F2000, and MICC-F600, in 03.840 s with 91.95% accuracy. In addition to these findings on detection and accuracy, there is room for improvement in enhancing detection accuracy to address more intricate and challenging instances of copy-move forgeries. Moreover, the method should be extended to encompass various other forms of forgeries (Table 2).

Table 2 This table summarizes the work related to Key-point or feature-based methods

Paper Title	Publication year	Method used	Performance	Performance parameter
"A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms" [60]	2020	SIFT	96.97%	F-Score
"A Robust Copy-Move Forgery Detection In Digital Image Forensics Using SURF" [61]	2020	SURF	91.95%	Recall

b) **Block-based methods**

Copy-move fraud detection in block-based techniques, the frequency domain characteristics are identified by dividing the altered images into overlapped or non-overlapped blocks [59].

i. **Frequency domain-based methods**

Methods based on the frequency domain are used to transform an image in frequency domain from spatial domain to detect copy-move forgery [62]. Here we have discussed a few frequency domain methods to detect copy-move fraud. Generally, the following methods are used for the conversion of an image into a frequency domain:

- Discrete-wavelet transform
- Dyadic-wavelet transform
- Discrete-cosine transform
- Fourier-Mellin transform
- Fast-Fourier transform

Discrete wavelet transformation (DWT) splits the input image into four sub-blocks called Approximation coefficient block (A_C), Horizontal coefficient block (H_C), Vertical coefficient block (V_C), and Diagonal coefficient block (D_C) [63]. Figure 12 divides the input image into four sub-blocks (A_C, H_C, V_C, D_C) [63].

- [63] proposed an efficient technique to trace copy-move fraud using Discrete-wavelet-transform (DWT). Their study found that DWT is much better for identifying image properties on edges or sudden variations in color contrast than Fourier transform. Discrete-wavelet transform minimizes the image's size, leading to less time complexity. The result obtained in this study over the CoMoFoD dataset proved that this proposed technique could be utilized in copy-move fraud identification and localization with satisfactory performance. As author's come to the conclusion that the accuracy performance of the algorithms is affected by the dimensions of the altered regions.Therefore, still a need of improving the detection performance and examining the robustness of the model over other image attacks. Table 3 demonstrates the performance of the introduced method (Table 3).

Table 3 Demonstrates the performance of the introduced method

Method	Precision	Recall	F1-Score
DWT	98.678%	96.387%	97.523%

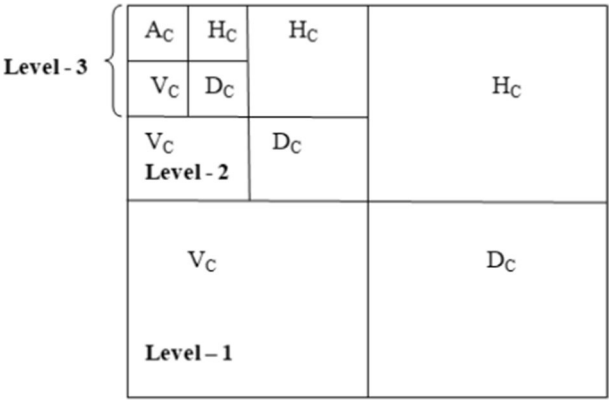

Fig. 12 Division of the image into sub-blocks using DWT

- Due to the scale-invariant and translation properties of the Fourier Mellin Transform (FMT), this method is used to extract features from the image during copy-move fraud detection [64]. [60] introduced a technique to detect copy-move fraud. To extract features from the smooth region of the image, they used Fourier-Mellin transform. In contrast, they used the SIFT method to bring out features from the texture region. The findings of this study are very promising. This proposed method has 96.97% performance in terms of F-measure. The suggested solution can be extended for detecting copy-move frauds in videos.
- Discrete Cosine Transform (DCT) transforms an image into the frequency domain. One profit of using DCT is that it is invariant to blurring [65]. [44] introduced an algorithm to detect copy-move fraud in this work, and they used DCT to bring out features of the photograph. In this study, copy-move fraud detection has the following four steps (See Fig. 13):

Experimental results of this study proved that the introduced way detected the altered regions of the image efficiently In the future, it is possible to expand the proposed research to identify manipulated sections within digital images using error-level analysis and quantization tables as the basis. There is an extreme concern in the proposed solution that the performance is tested over only 5 images so this issue must be taken into consideration.

- Fast-Fourier-Transform is used to quickly calculate the DFT, which means the matrix corresponding to an image is efficiently converted into Fourier coefficients (FFT). [66] Introduced a new method to identify the copy-move fraud in which they used Local features and Fast Fourier Transform of the altered photograph. The findings of this study demonstrate that the accuracy of the proposed technique (FFT-ELTP) was 86.62 percent on the compressed images of the used dataset. Due to the inclusion of intricate transformations like DCT and FFT in the proposed solution, the overall complexity of the methodology is heightened. Future research in the same vein may seek to minimize the requirement for

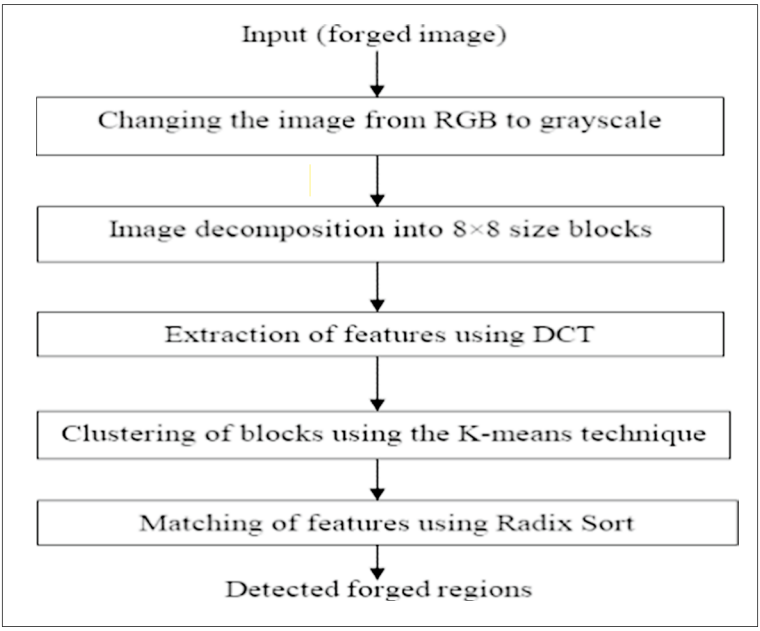

Fig. 13 Steps of the proposed forgery detection method

such intricate operations. Additionally, investigating the detection of image forgery's specific location is also an area to be delved into in further studies.

- [67] Proposed a new approach in which they used Discrete wavelet transform and Dyadic wavelet transform with Speeded-Up robust features (SURF). The experimental result of this study shows that Dyadic wavelet transform, when used with SURF, has better recall and precision but higher execution time than discrete wavelet transforms when used with SURF. The genuine significance of this suggested research would be fully recognized once it's adapted to identify video forgeries. Additionally, the authors are interested in evaluating how well this CMF detector performs on integrated platforms. Moreover, they aim to assess the effectiveness of alternative invariant feature transformations like PCA-SIFT when combined with wavelet transforms. Table 4 compares the two proposed methods of this study (Table 4).

Table 5 summarizes the different methods and their performance in copy-move fraud detection.

ii. **Local binary pattern**

Table 4 This table compares the two proposed methods of this study

Introduced Method	Recall	False Prediction rate	Execution time in seconds
DWT + SURF	64%	19%	2.05
Dyadic WT + SURF	76%	23%	63.122

Table 5 This table summarizes the techniques working on the frequency domain

Paper Title	Publication year	Method used	Performance	Performance parameter
"An Efficient Forensic Approach for Copy-move Forgery Detection via Discrete Wavelet Transform" [63]	2020	DWT	98.678%	Precision
"A Robust Copy-Move Forgery Detection In Digital Image Forensics Using SURF" [60]	2020	FMT	96.97%	F- score
"Block-based copy–move image forgery detection using DCT"[44]	2019	DCT	Efficient	In terms of execution time
"Detection of Digital Image Forgery using Fast Fourier Transform and Local Features" [66]	2019	FFT	86.62%	Accuracy
"Fast and Robust Copy-Move Forgery Detection Using Wavelet Transforms and SURF" [67]	2016	DyWT	76%	Recall

The local binary pattern (LBP) is the most effective local feature descriptor; it calculates the texture distribution rule of an image based on the signs of differences between adjacent pixels to achieve intensity and rotation-invariance [68]. Here we have discussed a simple Local binary pattern method. [69] discussed the passive forgery detection scheme using the LBP. LBP is an easy and economic texture operator generally used for texture classification. LBP is also utilized for counterfeit detection because Image fraud activities change the pixel values. This LBP label is created corresponding to every pixel of the residual image. Initially, every pixel which belongs to the residual image is assumed to be the center pixel then their 8-neighbours are examined. The intensity value of every pixel in the 8-neighborhood is compared with the value of a central pixel, and then a binary digit (0,1) is assigned corresponding to the following condition:

$$T_{a,b} = \begin{cases} 1, \mathbf{T_{a,b}} > \mathbf{C_{p,q}} \\ 0, Otherwise \end{cases} \tag{8}$$

In Eq. (8), $C_{p,q}$ is the pixel in the center of 8-neighbors, and $T_{a,b}$ is the pixel from the 8-neighbors with co-ordinates a and b. An 8-bit binary integer is generated by using the binary value of each neighboring pixel which is used for the label of the central pixel. These 8-bit binary numbers can be converted into decimal numbers for the purpose of better handling. This process will be used for creating the whole LBP image of the same size. The study's findings show that utilizing the BEST-q-CLASS feature selection approach to compute LBP using noise residuals and co-occurrence matrices leads to a model that performs effectively for practically any set of changes with an accuracy of 98.4%. In the future, we can enhance model performance by incorporating additional robust features using these approaches, creating more efficient models with improved performance. Furthermore, as we identify more types of forgeries, we can apply the scheme outlined to address them effectively.

iii **Dimension reduction-based methods**

Dimensionality reduction is the process of transforming data from a high-dimensional space to one with fewer dimensions so that the conclusions drawn from the reduced dataset are reasonably close to those drawn from the analysis of the original dataset [70]. Dimension reduction methods help to increase matching processing speed [71]. Here we have discussed the two famous dimensionality reduction methods; Principal component analysis (PCA) and Singular value decomposition (SVD).

- PCA decreases the dimensions of an extensive data set into smaller ones by reducing the number of variables. Principle component analysis decreases the variables in the data set while preserving as much information as possible. [71] Discussed new methods of copy-move fraud detection in which they used kernel PCA with DCT. Tables 6, 7, and 8 show the experimental result of the proposed study with additive white Gaussian noise (AWGN), JPEG compression, and Gaussian blurring, respectively. Nonetheless, the introduction of the segmentation module and dual-branch structure in SD-Net has increased the method's complexity. There is a need for future research to explore methods that can reduce complexity without compromising accuracy. Additionally, thoroughly investigating the detection of forgeries in regions that are similar but genuine is essential.

Table 6 Forgery detection result with Gaussian blurring

Performance parameter	Kernel size (ω) = 5 Blurring radius(δ) = 0.5		Kernel size (ω) = 5 Blurring radius(δ) = 1	
	24×24	40×40	24×24	40×40
Precision	00.9880	00.9980	00.9800	00.9950
Recall	1.0	1.0	00.9830	1.0
Tru positive rate	00.9340	00.9550	00.8590	00.8750
False positive rate	00.0350	00.0180	00.0540	00.0170

Table 7 Forgery detection result with additive white Gaussian noise (AWGN)

Performance parameter	SNR = 35 dB		SNR = 40 dB	
	24×24	40×40	24×24	40×40
Precision	00.9790	00.9930	00.9800	1.0
Recall	00.9840	00.9980	00.9910	1.0
Tru positive rate	00.9790	00.9920	00.9850	00.9950
False positive rate	00.0550	00.0460	00.0490	00.0270

Table 8 Forgery detection result with JPEG compression

Performance parameter	Quality factor Q = 80		Quality factor Q = 90	
	24×24	40×40	24×24	40×40
Precision	00.9190	00.9330	00.9700	00.9330
Recall	00.9250	00.9380	00.9750	00.9810
Tru positive rate	00.7910	00.9090	00.9570	00.9750
False positive rate	00.0170	00.0130	00.0130	00.0090

In Table 8, SNR stands for signal-to-noise ratio.
In Tables 6, 7 and 8, 24×24, and 40×40 is the forged area size in the image.

- [72] introduced a method of copy-move fraud detection in which they used PCA with SIFT and DBSCAN. The findings of this study show that the proposed approach successfully detects copy-move fraud in the MICC-F220 image data set with an accuracy of 97%. The suggested approach can be extended to detect other forgeries like splicing etc.
- [73] suggested a new clone identification method in digital images using Singular value decomposition (SVD) for data reduction. The SVD method is used to convert correlated variables into non-correlated variables, which can suitably explain the different relationships between various data items. According to this study, SVD is used for data reduction where a matrix T_{cr} is defined as:

$$\boldsymbol{T_{cr}} = \boldsymbol{O_{cc}} \times \boldsymbol{D_{cr}} \times \mathbf{H}_{\mathbf{rr}}^{\mathbf{T}} \tag{9}$$

In equation (9), O_{cc} is a matrix of size c × c, which is orthogonal in nature, the size of the D_{cr} matrix is c × r, which is diagonal in nature, and $H^{T}_{rr}$is a transpose matrix of a matrix H_{rr} of size r × r, which is orthogonal in nature. Findings of the proposed study show that the DWT-based technique optimizes the search time and accurately locates the forged region. Whereas DWT followed by the SVD approach further minimized the search time while preserving the accuracy. Nonetheless, these techniques prove ineffective in identifying alterations in images that have undergone JPEG compression. Regrettably, in the present day, the majority of images are accessible in JPEG format. One can expand this research to encompass the detection of tampering in JPEG images as well.

2.2.3 Splicing detection

Image splicing is a forgery algorithm for creating altered image using at least two images [74–76]. Here we have provided a few methods for splicing detection. Here we have discussed the machine learning-based splicing detection model and pre-trained residual network-based deep learning CNN techniques-based splicing detection model.

- [77] Proposed a ML based system for detecting splicing in digital images. This scheme creates a gray-level image from the (Red-Green-Blue) RGB image, and features are extracted from the image. A feature vector is created by joining these pertinent collections of characteristics. To train and categorize fake and real images, a machine learning classifier called logistic regression is utilized. Table 9 shows the correctness of the proposed method on the different data sets. In the future, the identification of manipulated objects within an image could potentially be achieved using a comparable feature set in combination with machine learning methods. Additionally, for identifying and pinpointing copy-move forgeries, utilizing the most relevant feature set in combination with a co-occurrence texture measure feature could be advantageous.

- [78] Proposed an approach to detect splicing in digital images. In this study, a pre-trained residual network-based CNN technique has been explored. Feature extraction has been performed using the RESNET-50 (a pre-trained residual network). This method trains the classifier model utilizing three classifiers: K-NN, Naive Bayes, and Multiclass Model using SVM Learner. In the proposed scheme, MATLAB is used to perform the experiment. Table 10 demonstrates the accuracy of the proposed approach corresponding to the different classifiers. The performance of the proposed solution must be examined when replacing the ResNet-50 with its alternative deep-learning models such as VGGNET and DewnseNet.

Table 9 Shows the accuracy of the proposed work

Paper Title	Data set	Accuracy achieved
"A technique for image splicing detection using the hybrid feature set" [77]	CASIA v1	98.3%
	CASIA v2	99.5%
	COLUMBIA	98.8%

Table 10 Demonstrates the proposed model's accuracy with all three classifiers

Paper title	Feature extraction	Data set	Classifiers	Accuracy achieved
"Image Splicing detection using Deep Residual Network" [78]	ResNet-50 (a pre-trained residual network)	CASIA v2	Naïve Bayes	59.91%
			K-NN	59.91%
			Multiclass model using SVM Learner	70.26%

Table 11 This table summarizes the techniques based on deep-learning

Paper Title	Publication year	Method used	Performance	Performance parameter
"Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network" [80]	2019	CNNs and GANs	95% (approx)	Accuracy
"Convolutional Neural Network for Copy-Move forgery detection" [81]	2019	CNN	90%	Accuracy
"Dual branch convolutional neural network for copy move forgery detection "[82]	2020	CNN	96%	Accuracy
"Digital Image Forgery Detection Using Deep Autoencoder and CNN Features" [79]	2021	Autoencoders and CNN	For JPEG 95.9% and for TIFF 93.3%	Accuracy
"CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature" [83]	2022	VGG16 CNN	90.5%	F1-score
"Image Forgery Detection Using Integrated ConvolutionLSTM (2D) and Convolution (2D)" [84]	2023	ConvLSTM and CNN	85%	Accuracy

3 Deep-learning based Image forgery detection

Apart form the traditional aproches to detect image forgery, recent advances in Artificial Intelligence (AI) and Machine Learning (ML) allows us to develop new methods which can successfully identify available forgeries in images. Recently Machine-learning models like Convolutional Neural Networks (CNNs) and Generative Adversarial Network (GANs), Support Vector Machine, Auto Encoders, and Convolutional Long Short-Term Memory (ConvLSTM) have been widely utilized in the area of image forgery detection [27].

- [79] introduced a deep-learning model to identify forgery (copy-move or splicing) in digital images by keeping in the mind that Image forgery method should be independent from the suspected image format. Suggested model utilized multiple structure stacked autoencoders (SAE) to identify forgery in images. To extract feature from the image the they used VGG!6 and AlexNet. Finally, for the classification purpose they used Ensemble Subspace Discriminant classifier. Form the experimnts performed over the CASIA verion 1.0 and 2.0 it has been observed that the introduced method obtained 95.9% and 93.3% for JPEG and TIFF images respectively. Apart from the accuracy this approach produces promising results in terms of execution time. This approach only classify the images as forged or genuine image but not localize the forgery in the image therefore this work can also be extended for the forgery localization which is an important issue in image forgery detection.
- [80] introduced a hybrid model to detect copy-move attack in digital images. Authors have utilized CNN and Generative Adversarial Network (GAN) for feature extraction and copy-move symptoms detection respectively. A linear Support Vector Machine (SVM) is used for the classification purpose. The proposed work has utilized CIFAR-10, MNIST, MICC-F600, Oxford buildings, and Image Manipulation (IM) data sets for training and testing purpose. Experiments of the study illustrates that the introduced scheme is trustworthy in copy-move detection and yield to accuracy of ~ 95%. Authors have recommended to include more dataset like ImageNet for the training of GAN to enhance the robustness of the proposed model.
- [81] introduces a purely CNN based model to trace the copy-moved regions in the suspected image if any. They added a pre-processing layer in their proposed model to obtain the satisfactory performance. The proposed model architecture contains a pre-processing layer, three convolutional layer, and two fully connected layer. Rectified Linear Unit (ReLU) is used as an activation function and Pooling layer uses the MaxPooling and AvgPooling strategy. Finally, SoftMax classifier is used for the classification purpose. Introduced work has utilized CIFAR-10, MNIST, MICC-F600, Oxford buildings, and Image Manipulation (IM) data sets for training and testing purpose. Experiments of the study illustrates that the introduced scheme is trustworthy in copy-move detection and yield to accuracy of 90% with a set iteration limit. Authors suggested that other network architectures could be investigated in related future research, and in-depth studies could be carried out by utilizing a larger dataset than the one employed here.
- [82] implemented an idea of dual branch CNN to detect copy-move forgery. They have used two different branches of CNN for feature extraction and forgery detection in the suggested model. This strategy is tested over the various kernel size combinations. Experimental results over the MICC F2000 data set illustrates that the suggested model is trustworthy in copy-move detection and yield to accuracy of 96%. Authors of the

study suggested that the proposed model can be examined and evaluated over datasets of different image sizes. This model can also be utilized in the detection of other forgery operations.

- [83] given a rotation invariant feature-based copy-move detection scheme using a pre-trained CNN model VGG16. The proposed technique consists of four basic modules: rotation invariant, extraction of feature, correlation, and mask decoder module. CoMoFoD, MICC-F2000, D, and COVERAGE data sets for training and testing purpose. Experiments of the study illustrates that the introduced scheme is trustworthy in copy-move detection and yield to F1 score of 90.5%. Suggested solution can be extended to detect other image forgeries like splicing etc.
- [84] developed a model for image forgery detection. Suggested model classify the suspected image as genuine or fake classes. For this purpose they have proposed two different ways of forgery detection. In the first way, ConvLSTM(1D) is utilized with Convolutional(2D). In the second way, ConvLSTM(2D) is utilized with Convolutional(2D). Both the approaches tested over the CASIA v.2.0 data set and it is found that second approach is efficient than first one in terms of accuracy as first approach results in 72% accuracy and second resultrs in 85% accuracy. Suggested approach must be extended for improving the accuracy, apart from this, suggested solution can be examined over various image alternation technioques (Table 11).

4 Image forensic data sets

In Digital image forensics, a dataset is a carefully managed collection of digital images that a researcher uses to train, test, and assess the effectiveness of the proposed algorithms for forgery detection [85]. It is observed that the same methods of forgery detection perform differently with different data sets. As researchers, we must develop methods whose performance does not depend on the data set. We have provided a few commonly used data sets to assess the performance of the proposed forgery detection methods (See Table 12). Table 12 has four columns, the first column **(Name of image dataset)** shows the name of the dataset with the citation where this dataset has been used, second column **(Dataset used for)** shows the purpose of utilizing dataset in mentioned citation, third column **(Performance)** shows the achieved performance when the dataset was used, and fourth column **(Dataset description)** describes the characteristic of the dataset in short.

Here we have provided the links to download publicly available datasets:

CASIA v1.0 and CASIA v2.0: https://www.kaggle.com/datasets/sophatvathana/casia-dataset
COLUMBIA: https://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm
CoMoFoD: https://www.vcl.fer.hr/comofod/download.html
MICC-F220, MICC-F2000, MICC-F8multi, and MICC-F600: http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/
GRIP: https://figshare.com/collections/Source-Destination_Forensics_CMFD_Dataset/6221192
CIFAR-10: https://www.cs.toronto.edu/~kriz/cifar.html
Copy-move hard: http://dx.doi.org/https://doi.org/10.6084/m9.figshare.978736
COVERAGE: https://github.com/wenbihan/coverage

Table 12 Comparison of various image data set

Name of the image dataset	Dataset used for	Performance	Dataset description
CASIA v1.0 [77]	Splicing detection	Accuracy = 98.3%	This data set has two image directories, Au and Sp, with 800 and 921 files, respectively [86]
CASIA v2.0 [77]	Splicing detection	Accuracy = 99.5%	This data set has three image directories, Au, Tp, and CASIA 2 Groundtruth, with 7492, 5125, and 5123 files, respectively [87]
COLUMBIA [77]	Splicing detection	Accuracy = 98.8%	The data set includes 1845 image blocks (128 × 128), of which 933 are authentic, and 912 are spliced image blocks [88]
CoMoFoD [89]	Copy-move detection	Precision = 96.845% Recall = 92.5% F1-score = 94.35%	CoMoFoD database contains 260 manipulated or altered photos, divided into two groups (small 512 × 512 and large 3000 × 2000) [90, 91]
MICC-F220 [92]	Copy-move detection	False positive rate = 3.1% Recall = 99.2%	Within this dataset, there are 220 images, with an equal split of 110 forged images and 110 authentic images [93]
MICC-F2000 [92]	Copy-move detection	False positive rate = 6.8% Recall = 98.5%	This dataset comprises 2,000 images, with 700 of them being forgeries and 1,300 being genuine/authentic images [93]
MICC-F8multi [92]	Copy-move detection	False positive rate = 6.9% Recall = 98.8%	This data set has eight altered images with realistic multiple cloning[94]
MICC-F600 [93]	Copy-move detection	Recall = 100% True negative rate = 100%	This data contains 440 authentic images, of which 160 are altered images, and 160 are ground truth images [93]
GRIP [95]	Copy-move	Precision = (91.76%)	80 legitimate and 80 altered images with a size of 768 × 1024 are used in the GRIP dataset [95]
Copy-move hard (CMH) [96]	Copy-move	The average accuracy on (CMH_{p1}) is = 96.19%	CMH data set has 108 images. Out of 108 images, 23 images are copy moved (CMH_{p1}), 25 Images rotate the copied region (CMH_{p2}), 26 images with resizing of the cloned area (CMH_{p3}), and 34 images use rotation and scaling (CMH_{p4}) [97]
Dresden Image Database [54]	Imaging device identificaT	Accuray = 100%	In total, there are over 14,000 images available, encompassing various camera configurations, environmental conditions, and specific scenes [98]
CIFAR-10 [80]	Copy-move	Accuracy = 95% (approx)	60,000 color images have been used in the CIFAR-10 dataset, each sized at 32 × 32 pixels, distributed across ten categories. 6000 images has been kept in each category. The dataset is further separated into 50,000 and 10,000 images for training and testing purpose respectively [99]

Table 12 (continued)

Name of the image dataset	Dataset used for	Performance	Dataset description
D data set [83]	Copy-move	F1-score = 90.5%	It consists of images of moderate size, with most being either 700 × 1000 or 1000 × 700 in dimensions, and it is additionally segmented into multiple datasets labeled as D0, D1, and D2. [100]
COVERAGE [83]	Copy-move	F1-score = 90.5%	A novel database has been created, which includes manipulated images where objects have been copied and moved, along with their authentic counterparts featuring similar but real objects. This database, known as COVERAGE, aims to emphasize and tackle the problem of uncertainty in tamper detection methods caused by the inherent similarity found in unaltered natural images [101]
Image Manipulation dataset [80]	Copy-move	Accuracy = 95% (approx)	The Image Manipulation Dataset serves as an authentic reference collection used to assess the accuracy of identifying alterations in images, such as tampering artifacts. It contains 48 primary images, distinct sections extracted from these images, and a software framework for producing accurate reference data[102]
MNIST dataset [81]	Copy-move	Accuracy = 90%	The dataset includes a training batch with 60,000 images and a testing batch with 10,000 images, all depicting handwritten digits. These images of digits have been standardized in size and positioned at the center, each occupying a consistent area of 28 × 28 pixels [103]

Image Manipulation Dataset (IMD): https://www5.cs.fau.de/research/data/image-manipulation/
Dresden image dataset: https://www.kaggle.com/datasets/hanjunyang1/dresden
D dataset: http://www.dicgim.unipa.it/cvip/ or by personal request to author.
MNIST dataset: https://figshare.com/articles/dataset/data/14132507

5 Conclusions

In this study, we have tried to provide a complete summary of various techniques used in blind forgery detection, especially Imaging device identification,copy-move detection, and splicing detection. We have been attempting to explore PRNU, CRF, and feature extraction-based methods to identify imaging devices. While for copy-move fraud detection, we have focused on the Key-point and Block based methods. In this survey paper, we have provided information about the data set in tabular form. To better understand this study for any reader, we have tried to summarize the survey by using various figures and tables. To preserve the importance of this study for future researchers, we have used the most recent and up-to-date references. In conclusion, we aspire that this study will prove beneficial to researchers within the digital forensics field, specifically those concentrating on blind or passive forgery detection.

Acknowledgements I am (Deependra Kumar Shukla) grateful to the UGC and the Government of India for granting me the UGC- (JRF/SRF) fellowship, which enables me to pursue my research endeavors.

Author Contributions The authors contributed equally to this work.

Funding No funding was received to assist with the preparation of this manuscript.

Data Availability No additional data or material has been used for this work other than the referenced papers.

Code Availability No code has been developed by the authors for this work.

Declarations

Conflict of Interests The authors declare that they have no conflict of interest.

References

1. Jana M, Jana B, Joardar S (2022) Local feature based self-embedding fragile watermarking scheme for tampered detection and recovery utilizing AMBTC with fuzzy logic, J King Saud Univ Comput Inf Sci, no. xxxx, 2021, https://doi.org/10.1016/j.jksuci.2021.12.011
2. Raju PM, Nair MS (2018) Copy-move forgery detection using binary discriminant features. J King Saud Univ Comput Inf Sci 34(2):165–178. https://doi.org/10.1016/j.jksuci.2018.11.004
3. Sekhar PC, Shankar TN (2023) An object-based splicing forgery detection using multiple noise features. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-16534-z
4. Verma M, Singh D (2023) Survey on image copy-move forgery detection. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-16455-x
5. Sushir RD, Wakde DG, Bhutada SS (2023) Enhanced blind image forgery detection using an accurate deep learning based hybrid DCCAE and ADFC. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-15475-x

6. Abir NAM, Warif NBA, Zainal N (2023) An automatic enhanced filters with frequency-based copy-move forgery detection for social media images. Multimed Tools Appl. https://doi.org/10.1007/s11042-023-15506-7
7. Li Q, Wang C, Zhou X, Qin Z (2022) Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. Sci Rep 12(1):14987. https://doi.org/10.1038/s41598-022-19325-y
8. Ferreira WD, Ferreira CBR, da Cruz Júnior G, Soares F (2020) A review of digital image forensics, Comput Electr Eng, vol. 85 https://doi.org/10.1016/j.compeleceng.2020.106685
9. Dhanaraj RS, Sridevi M (2021) A study on detection of copy-move forgery in digital images, in Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021, pp. 900–905. https://doi.org/10.1109/ICICV50876.2021.9388576
10. Uma S, Sathya PD (2019) A detailed review of copy-move forgery detection in digital image. Glob J Eng Sci Res. https://doi.org/10.5281/zenodo.2537823
11. Ansari MD, Ghrera SP, Tyagi V (Jan.2014) Pixel-based image forgery detection: A review. IETE J Educ 55(1):40–46. https://doi.org/10.1080/09747338.2014.921415
12. What is Photo Retouching? Why It's So Important to Retouch. https://www.imaginated.com/photography/photography-glossary/what-is-photo-retouching/ (accessed Sep. 20, 2022)
13. AlZahir S, Hammad R (2020) Image forgery detection using image similarity. Multimed Tools Appl 79(39–40):28643–28659. https://doi.org/10.1007/s11042-020-09502-4
14. Rajput A (2018) Image Splicing | Set 1 (Introduction) - GeeksforGeeks. https://www.geeksforgeeks.org/image-splicing-set-1-introduction/ (accessed Sep. 20, 2022)
15. Koul S, Kumar M, Khurana SS, Mushtaq F, Kumar K (2022) An efficient approach for copy-move image forgery detection using convolution neural network. Multimed Tools Appl 81(8):11259–11277. https://doi.org/10.1007/s11042-022-11974-5
16. Meena KB, Tyagi V (2023) Image splicing forgery detection using noise level estimation. Multimed Tools Appl 82(9):13181–13198. https://doi.org/10.1007/s11042-021-11483-x
17. Kaur N, Jindal N, Singh K (2020) A passive approach for the detection of splicing forgery in digital images. Multimed Tools Appl 79(43–44):32037–32063. https://doi.org/10.1007/s11042-020-09275-w
18. Kaur A, Rani J (2016) Digital Image Forgery and Techniques of Forgery Detection: A brief review. International Journal of Technical Research & Science 1(4):18–24
19. Raja K, Gupta G, Venkatesh S, Ramachandra R, Busch C (2022) Towards generalized morphing attack detection by learning residuals. Image Vis Comput 126:104535. https://doi.org/10.1016/j.imavis.2022.104535
20. Image Processing : Morphing (1997) https://www.owlnet.rice.edu/~elec539/Projects97/morphjrks/morph.html (accessed Sep. 20, 2022)
21. Thakur T, Singh K, Yadav A (2018) Blind Approach for Digital Image Forgery Detection. Int J Comput Appl 179(10):34–42. https://doi.org/10.5120/ijca2018916108
22. Hegazi A, Taha A, Selim MM (2021) An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. J King Saud Univ Comput Inf Sci 33(9):1055–1063. https://doi.org/10.1016/j.jksuci.2019.07.007
23. Vijayalakshmi NVSK, Sasikala KJ, Shanmuganathan C (2023) Copy-paste forgery detection using deep learning with error level analysis, Multimed Tools Appl, https://doi.org/10.1007/s11042-023-15594-5
24. Yang B, Li Z, Zhang T (2020) A real-time image forensics scheme based on multi-domain learning. J Real-Time Image Process 17(1):29–40. https://doi.org/10.1007/s11554-019-00893-8
25. Liu K et al (2019) Copy move forgery detection based on keypoint and patch match. Multimed Tools Appl 78(22):31387–31413. https://doi.org/10.1007/s11042-019-07930-5
26. Liu G, Reda FA, Shih KJ, Wang TC, Tao A, Catanzaro B (2018) Image inpainting for irregular holes using partial convolutions. In: Proceedings of the European conference on computer vision (ECCV), pp 85–100
27. Zanardelli M, Guerrini F, Leonardi R, Adami N (2023) Image forgery detection: a survey of recent deep-learning approaches. Multimed Tools Appl 82(12):17521–17566. https://doi.org/10.1007/s11042-022-13797-w
28. He L, Qiang Z, Shao X, Lin H, Wang M, Dai F (2022) Research on High-Resolution Face Image Inpainting Method Based on StyleGAN. Electron 11(10):1–18. https://doi.org/10.3390/electronics11101620
29. Qiao T, Zhu A, Retraint F (2018) Exposing image resampling forgery by using linear parametric model. Multimed Tools Appl 77(2):1501–1523. https://doi.org/10.1007/s11042-016-4314-1
30. Alamro L, Yusoff N (2017) Copy-move forgery detection using integrated DWT and SURF. J Telecommun Electron Comput Eng 9(1–2):67–71

31. Sharma P, Kumar M, Sharma H (2022) Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimed Tools Appl 82(12):18117–18150. https://doi.org/10.1007/s11042-022-13808-w
32. Koundinya Anjan K, Sunanda D, Mahesh G, Sneha S (2022) Characteristic overview of digital image forensics tools. In: Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2021. Springer, pp 157–162
33. Hosny KM, Mortda AM, Fouda MM, Lashin NA (2022) An efficient cnn model to detect copy-move image forgery. IEEE Access 10:48622–48632. https://doi.org/10.1109/ACCESS.2022.3172273
34. Fadhil JM, Trupti B (2022) An efficient technique for image forgery detection using local binary pattern (hessian and center symmetric) and transformation method. Scientific Journal Al-Imam University College 1:1–11
35. Manna N, Kumar S, Kakar R, Nayak S, Rout JK, Kumar Balabantaray B (2022) IFChatbot: Convolutional Neural Network based chatbot for Image Forgery Detection and Localization, in 2022 IEEE India Council International Subsections Conference (INDISCON), pp. 1–6. https://doi.org/10.1109/INDISCON54605.2022.9862926
36. Alhaidery MMA, Taherinia AH (2022) A passive image forensic scheme based on an adaptive and hybrid techniques. Multimed Tools Appl 81(9):12681–12699. https://doi.org/10.1007/s11042-022-12374-5
37. Kadam K, Ahirrao S, Kotecha K (2021) AHP validated literature review of forgery type dependent passive image forgery detection with explainable AI. Int J Electr Comput Eng 11(5):4489–4501. https://doi.org/10.11591/ijece.v11i5.pp4489-4501
38. Sai Achyuth P, Satyanarayana V (2021) Image forgery detection techniques: a brief review. In: Proceedings of Second International Conference in Mechanical and Energy Technology: ICMET 2021, India. Springer, pp 351–357
39. Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A (2021) Image Steganography: A Review of the Recent Advances. IEEE Access 9:23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998
40. Bansal A, Kumar V (2021) Steganography Technique Inspired by Rook, https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJISP.2021040103, vol. 15, no. 2, pp. 53–67, https://doi.org/10.4018/IJISP.2021040103
41. Bansal A, Muttoo SK, Kumar V (2016) Security against Sample Pair Steganalysis in Eight Queens Data Hiding Technique. Int J Comput Netw Inf Secur 8(8):39–46. https://doi.org/10.5815/ijcnis.2016.08.05
42. Begum M, Uddin MS (2020) Digital image watermarking techniques: A review, Information (Switzerland), vol. 11, no. 2. MDPI AG. https://doi.org/10.3390/info11020110
43. Ray A, Roy S (2020) Recent trends in image watermarking techniques for copyright protection: a survey. Int J Multimed Inf Retr 9(4):249–270. https://doi.org/10.1007/s13735-020-00197-9
44. Parveen A, Khan ZH, Ahmad SN (2019) Block-based copy–move image forgery detection using DCT. Iran J Comput Sci 2(2):89–99. https://doi.org/10.1007/s42044-019-00029-y
45. Meena KB, Tyagi V (2021) Efficient Passive Forgery Detection in Digital Images, Jaypee University of Engineering and Technology, Guna, [Online]. Available: http://hdl.handle.net/10603/338230. Accessed 25/09/2023
46. Liu Y, Zou Z, Yang Y, Law NFB, Bharath AA (2021) Efficient source camera identification with diversity-enhanced patch selection and deep residual prediction. Sensors 21(14):1–22. https://doi.org/10.3390/s21144701
47. Wang B, Wang Y, Hou J, Li Y, Guo Y (2022) Open-Set source camera identification based on envelope of data clustering optimization (EDCO). Comput Secur, vol. 113 https://doi.org/10.1016/j.cose.2021.102571
48. Shukla DK, Bansal A, Singh P (2022) Performance analysis of various copy-move forgery detection methods. i-Manager's Journal on Digital Signal Processing 10(2):1
49. Tahaoglu G, Ulutas G, Ustubioglu B, Nabiyev VV (2021) Improved copy move forgery detection method via L*a*b* color space and enhanced localization technique. Multimed Tools Appl 80(15):23419–23456. https://doi.org/10.1007/s11042-020-10241-9
50. Wei H, Kehtarnavaz N (2019) Semi-Supervised Faster RCNN-Based Person Detection and Load Classification for Far Field Video Surveillance. Mach Learn Knowl Extr 1(3):756–767. https://doi.org/10.3390/make1030044
51. Obeidat AA (2017) Hybrid approach for botnet detection using k-means and k-medoids with Hopfield neural network. Int J Commun Networks Inf Secur 9(3):305–313

52. Alhaidery MMA, Taherinia AH, Yazdi HS (2022) Cloning detection scheme based on linear and curvature scale space with new false positive removal filters. Multimed Tools Appl 81(6):8745–8766. https://doi.org/10.1007/s11042-022-12237-z
53. Fanfani M, Piva A, Colombo C (2022) PRNU registration under scale and rotation transform based on convolutional neural networks. Pattern Recognit 124:108413. https://doi.org/10.1016/j.patcog.2021.108413
54. Behare MS, Bhalchandra AS, Kumar R (2019) Source Camera Identification using Photo Response Noise Uniformity, in Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019, pp. 731–734. https://doi.org/10.1109/ICECA.2019.8822212
55. Flor E, Aygun R, Mercan S, Akkaya K (2021) PRNU-based Source Camera Identification for Multimedia Forensics, Proc. - 2021 IEEE 22nd Int. Conf. Inf. Reuse Integr. Data Sci. IRI 2021, pp. 168–175, https://doi.org/10.1109/IRI51335.2021.00029
56. Xu B, Wang X, Zhou X, Xi J, Wang S (2016) Source camera identification from image texture features. Neurocomputing 207:131–140. https://doi.org/10.1016/j.neucom.2016.05.012
57. Grossberg MD, Nayar SK (2003) Determining the camera response from images: What is knowable?, IEEE Trans Pattern Anal Mach Intell, vol. 25, no. 11, https://doi.org/10.1109/TPAMI.2003.1240119
58. Chen C, McCloskey S, Yu J (2019) Analyzing modern camera response functions, in Proceedings - 2019 IEEE Winter Conference on Applications of Computer Vision, WACV 2019, Mar, pp. 1961–1969. https://doi.org/10.1109/WACV.2019.00213
59. Sadeghi S, Dadkhah S, Jalab HA, Mazzola G, Uliyan D (2018) State of the art in passive digital image forgery detection: copy-move image forgery. Pattern Anal Appl 21(2):291–306. https://doi.org/10.1007/s10044-017-0678-8
60. Meena KB, Tyagi V (2020) A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms. Multimed Tools Appl 79(11–12):8197–8212. https://doi.org/10.1007/s11042-019-08343-0
61. Badr A, Youssif A, Wafi M (2020) A robust copy-move forgery detection in digital image forensics using SURF. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS). IEEE, pp 1–6
62. Introduction to Frequency domain (2022) https://www.tutorialspoint.com/dip/introduction_to_frequency_domain.htm (accessed Sep. 19, 2022)
63. Ashraf R et al. (2020) An Efficient Forensic Approach for Copy-move Forgery Detection via Discrete Wavelet Transform," 1st Annu Int Conf Cyber Warf Secur ICCWS 2020 - Proc, https://doi.org/10.1109/ICCWS48432.2020.9292372
64. Pourkashani A, Shahbahrami A, Akoushideh A (2021) Copy-move forgery detection using convolutional neural network and K-mean clustering. Int J Electr Comput Eng 11(3):2604–2612. https://doi.org/10.11591/ijece.v11i3.pp2604-2612
65. Jaiswal AK, Gupta D, Srivastava R (2020) Detection of copy-move forgery using hybrid approach of DCT and BRISK. In: 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, pp 471–476
66. Kanwal N, Girdhar A, Kaur L, Bhullar JS (2019) Detection of digital image forgery using fast fourier transform and local features. In: 2019 international conference on automation, computational and technology management (ICACTM). IEEE, pp 262–267
67. Hashmi MF, Keskar AG (2019) Fast and robust copy-move forgery detection using wavelet transforms and SURF. Int Arab J Inf Technol 16(2):304–311
68. Luo Q, Su J, Yang C, Silven O, Liu L (2022) Scale-selective and noise-robust extended local binary pattern for texture classification. Pattern Recognit 132:108901. https://doi.org/10.1016/J.PATCOG.2022.108901
69. Farooq S, Yousaf MH, Hussain F (2017) A generic passive image forgery detection scheme using local binary pattern with rich models. Comput Electr Eng 62:459–472. https://doi.org/10.1016/j.compeleceng.2017.05.008
70. Nsang AS, Bello AM, Shamsudeen H (2015) Image reduction using assorted dimensionality reduction techniques. CEUR Workshop Proc 1353(June):139–146
71. Chen H, Yang X, Lyu Y (2020) Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm. IEEE Access 8:36863–36875. https://doi.org/10.1109/ACCESS.2020.2974804
72. Mursi MFM, Salama MM, Habeb MH (2017) An Improved SIFT-PCA-Based Copy-Move Image Forgery Detection Method. Int J Adv Res Comput Sci Electron Eng 6(3):23–28
73. Mishra M, Chandra Adhikary M, Adhikary FMLt C (2014) Detection of Clones in Digital Images Digital Image Forgery Detection View project MAKE-meteorological analyser & knowledge

extractor View project Detection of Clones in Digital Images. [Online]. Available: https://www.researchgate.net/publication/264276516. Accessed 15/07/22
74. Jain I, Goel N (2021) Advancements in image splicing and copy-move forgery detection techniques: A survey, Proc Conflu 2021 11th Int Conf Cloud Comput Data Sci Eng, pp. 470–475, https://doi.org/10.1109/Confluence51648.2021.9377104
75. Rao Y, Ni J, Zhao H (2020) Deep Learning Local Descriptor for Image Splicing Detection and Localization. IEEE Access 8:25611–25625. https://doi.org/10.1109/ACCESS.2020.2970735
76. Ahmed B, Gulliver TA, S. alZahir (2020) Image splicing detection using mask-RCNN. Signal, Image Video Process 14(5):1035–1042. https://doi.org/10.1007/s11760-020-01636-0
77. Jaiswal AK, Srivastava R (2020) A technique for image splicing detection using hybrid feature set. Multimed Tools Appl 79(17–18):11837–11860. https://doi.org/10.1007/s11042-019-08480-6
78. Jaiswal AK, Srivastava R (2019) Image Splicing Detection using Deep Residual Network. SSRN Electron J. https://doi.org/10.2139/ssrn.3351072
79. Bibi S, Abbasi A, Haq IU, Baik SW, Ullah A (2021) Digital Image Forgery Detection Using Deep Autoencoder and CNN Features, Human-centric Comput Inf Sci, vol. 11, https://doi.org/10.22967/HCIS.2021.11.032
80. Abdalla Y, Tariq Iqbal M, Shehata M (2019) Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network, Inf, vol. 10, no. 9, https://doi.org/10.3390/info10090286
81. Abdalla Y, Iqbal MT, Shehata M (2019) Convolutional neural network for copy-move forgery detection. Symmetry 11(10):1280
82. Goel N, Kaur S, Bala R (2021) Dual branch convolutional neural network for copy move forgery detection, no. December 2020, pp. 656–665, https://doi.org/10.1049/ipr2.12051
83. Lee SI, Park JY, Eom IK (2022) CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature. IEEE Access 10(October):106217–106229. https://doi.org/10.1109/ACCESS.2022.3212069
84. Yogita S, Prashant S, Rawat CSD (2023) Image forgery detection using integrated convolution-LSTM (2D) and convolution (2D). International Journal of Electrical and Electronics Research (IJEER) 11(2):631–638
85. Maleve N (2019) An Introduction to Image Datasets | u n t h i n k i n g . p h o t o g r a p h y. https://unthinking.photography/articles/an-introduction-to-image-datasets (accessed Sep. 20, 2022)
86. Sovathana P (2018) Casia dataset | Kaggle. https://www.kaggle.com/datasets/sophatvathana/casia-dataset (accessed Sep. 02, 2022)
87. Goel D (2020) CASIA 2.0 Image Tampering Detection Dataset | Kaggle. https://www.kaggle.com/datasets/divg07/casia-20-image-tampering-detection-dataset (accessed Sep. 02, 2022)
88. Ng T-T, Chang S-F, Sun Q (2004) A data set of authentic and spliced image blocks. In: ADVENT Technical Report, vol 4. Columbia University
89. Niyishaka P, Bhagvati C (2020) Copy-move forgery detection using image blobs and BRISK feature. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-09225-6
90. Tralic D, Zupancic I, Grgic S, Grgic M (2013) CoMoFoD—New database for copy-move forgery detection. In: Proceedings ELMAR-2013. IEEE, pp 49–54
91. CoMoFoD (2013) https://www.vcl.fer.hr/comofod/ (accessed Sep. 02, 2022)
92. Soni B, Das PK, Thounaojam DM (2018) multiCMFD: fast and efficient system for multiple copy-move forgeries detection in image. In: Proceedings of the 2018 international conference on image and graphics processing, pp 53–58
93. Elaskily MA et al (2020) A novel deep learning framework for copy-moveforgery detection in images. Multimed Tools Appl 79(27–28):19167–19192. https://doi.org/10.1007/s11042-020-08751-7
94. Sadeghi S, Jalab HA, Wong K, Uliyan D, Dadkhah S (2017) Keypoint based authentication and localization of copy-move forgery in digital image. Malaysian J Comput Sci 30(2):117–133
95. Wang C, Zhang Z, Zhou X (2018) An image copy-move forgery detection scheme based on A-KAZE and SURF features. Symmetry (Basel) 10(12):1–20. https://doi.org/10.3390/sym10120706
96. Silva E, Carvalho T, Ferreira A, Rocha A (2015) Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. J Vis Commun Image Represent 29:16–32. https://doi.org/10.1016/j.jvcir.2015.01.016
97. Al-Qershi OM, Khoo BE (2018) Evaluation of copy-move forgery detection: datasets and evaluation metrics. Multimed Tools Appl 77(24):31807–31833. https://doi.org/10.1007/s11042-018-6201-4
98. Gloe T, Böhme R (2010) The dresden image database for benchmarking digital image forensics. J Digit Forensic Pract 3(2–4):150–159. https://doi.org/10.1080/15567281.2010.531500

99. CIFAR-10 and CIFAR-100 datasets (n.d.) https://www.cs.toronto.edu/~kriz/cifar.html (accessed Sep. 19, 2023)
100. Ardizzone E, Bruno A, Mazzola G (2015) Copy-move forgery detection by matching triangles of keypoints, IEEE Trans Inf Forensics Secur, vol. 10, https://doi.org/10.1109/TIFS.2015.2445742
101. Wen B, Zhu Y, Subramanian R, Ng TT, Shen X, Winkler S (2016) Coverage – a novel database for copy-move forgery detection. In: 2016 IEEE International Conference on Image Processing (ICIP), pp 161–165. https://doi.org/10.1109/ICIP.2016.7532339
102. Image Manipulation Dataset (n.d.) https://www5.cs.fau.de/research/data/image-manipulation/ (accessed Sep. 19, 2023)
103. MNIST - Machine Learning Datasets (n.d.) https://datasets.activeloop.ai/docs/ml/datasets/mnist/ (accessed Sep. 25, 2023)

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com