Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2022.020920

REVIEW

A Thorough Investigation on Image Forgery Detection

Anjani Kumar Rai* **and Subodh Srivastava**

Department of Electronics & Communication Engineering, NIT, Patna, India

*Corresponding Author: Anjani Kumar Rai. Email: anjanikumarr.phd19.ec@nitp.ac.in

Received: 19 December 2021 Accepted: 11 May 2022

ABSTRACT

Image forging is the alteration of a digital image to conceal some of the necessary or helpful information. It cannot be easy to distinguish the modified region from the original image in some circumstances. The demand for authenticity and the integrity of the image drive the detection of a fabricated image. There have been cases of ownership infringements or fraudulent actions by counterfeiting multimedia files, including re-sampling or copy-moving. This work presents a high-level view of the forensics of digital images and their possible detection approaches. This work presents a thorough analysis of digital image forgery detection techniques with their steps and effectiveness. These methods have identified forgery and its type and compared it with state of the art. This work will help us to find the best forgery detection technique based on the different environments. It also shows the current issues in other methods, which can help researchers find future scope for further research in this field.

KEYWORDS

Forgery detection; digital forgery; image forgery localization; image segmentation; image forensics; multimedia security

1 Introduction

Millions of digital documents are created and circulated daily through newspapers, magazines, websites, and television. Images are an excellent tool for communication in any of these information channels. These images, along with video and audio, can be easily collected using various devices or software. DIs serve as evidence or proof against crimes. Unfortunately, manipulating images with computer graphics and image processing tools is not difficult. The way we deal with photo modification raises many legal and ethical issues that need to be addressed [1]. However, before considering what action to take in response to a problematic image, one must first determine it has been altered. There are various ways to modify the content of an image, such as compression, splicing, copy-move, and retouching techniques [2–4]. One of the most typical picture alteration processes is image composition (or splicing) and retouching. Various applications can perform manipulations in images that humans cannot detect by just looking at them once. Therefore, there is a need for automated digital image forgery detection (DIFDs) techniques to perform these tasks very fast and effective. Image forgery detection has developed as a fantastic study in various DIPs applications (digital image processing), image forensics, criminal investigation, biomedical technology, computer

vision [5–7]. There are various digital image forgery detection techniques used to detect the different kinds of forgery. DIFDs can be broadly classified passively or actively [8], as depicted in Fig. 1. An active forgery detection technique requires pre-extracted or pre-embedded information.

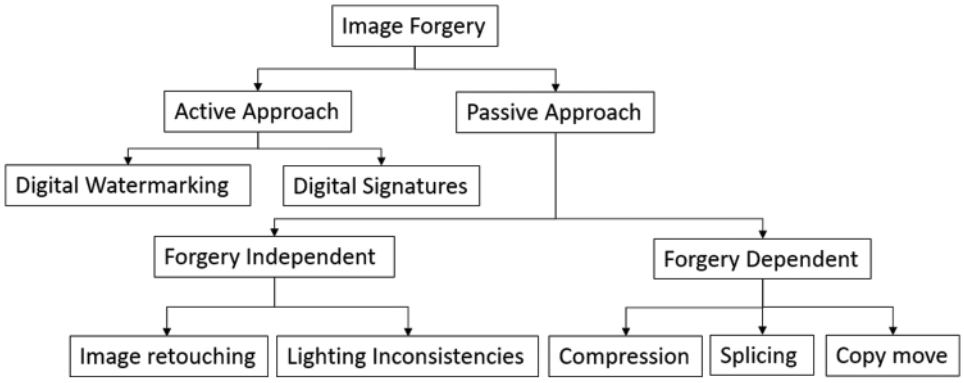

Figure 1: Categorization of image forgery detection techniques

1.1 Categorization of DIFDs

Active DIFDs necessitate the preparation of digital images, including watermarking, embedding and signature creations, limiting their practicality in applications. Passive DIFDs, unlike watermarks [9] and signatures [10], do not generate digital signatures or embedding from watermarks. DIFDs can be classified into five groups [11], as shown in Fig. 2. A few select DIFDs are presented for detecting passive image forgeries [12].

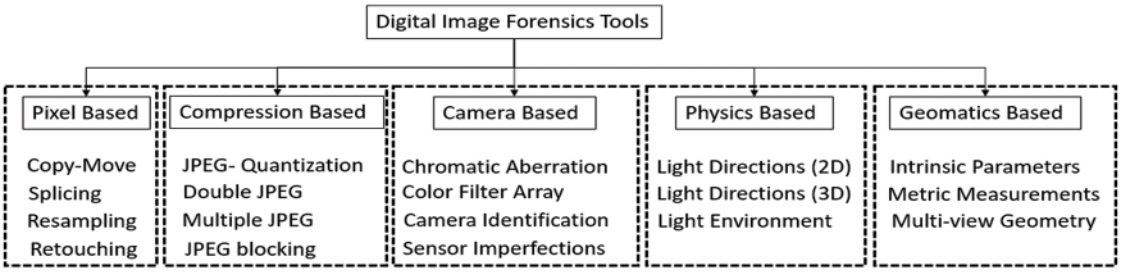

Figure 2: Digital image forgery detection techniques

Pixel-based DIFDs: Pixel-based approaches process DI pixels to statistically identify abnormalities that arise in image pixels due to tampering. The approaches also consider spatial or altered domain correlations between pixels that happen in the tampering of images. Copy-move, re-samples, re-touches, and image splicing are some of the approaches under this category. These are the most frequently used methods in DIFDs [13].

Format-based DIFDs: Forged images can also be detected based on their formats. They are used mainly in JPEG formats. Identifying fraud in compressed images is a complex task. However, structure-based approaches detect forgery even in compressed images. A modified, fabricated image that has been compressed (JPEG) makes forgery detections extremely difficult. Forensics investigations, however, use many characteristics of JPEG compression to discover manipulations. Format based DIFDs can be found on one of JPEG quantization [14], double JPEG compressions [15,16], multiple JPEG compressions [2,17], and JPEG blocks.

Camera-based DIFDs: A digital camera transfers acquired images from sensors to memory. They are quantized, color correlated, gamma-corrected, white balanced, filtered, and JPEG compressed. These processes are based on the different camera models and artefacts. Image captures undergo multiple stages of processing. Light enters the camera's lens, followed by the sensors' traversals through CFAs (Color Filter Arrays). The sensor's Photodetectors capture this incidental light and convert it to a voltage form, converted into digital data using A/D (Analog-to-Digital) conversions. Most current cameras use CMOS (Complementary Metal-Oxide Semiconductors), while a few use CCDs (Charged Coupled Devices). CFAs acquire color images from these sensors, which capture one color. At the same time, balance colors are computed using interpolations correlations that could be used to identify manipulations. Image Enhancement techniques are used to improve image qualities before storage. Artefacts generated at various phases of image generations can also be used to identify manipulations. These artefacts are generally estimated using chromatic aberrations, source camera identifications, CFAs, interpolations, and sensor noise errors where discrepancies indicate manipulations.

Physical environment-based DIFDs: Assuming fakes of two Hollywood stars rumored to be romantically connected through their beach images. Two individual photos can be superimposed to create a combined image but fail in mimicking the lighting effects of original images captured separately. Differences in illuminations throughout an image are proof of manipulations. These approaches are based on the lighting conditions of the captured original idea, as lighting is crucial to photography. They can be categorized into three groups. Discrepancies in light sources between certain items in the images assist in detecting manipulations in physics-based methods [18]. This approach was first developed by Kee et al. [18] and used three-dimensional surface geometries.

Geometry-based DIFDs: Geometry-based approaches measure object locations in the environment of the camera. Geometries can be faked using two sub-divided intrinsic camera parameters-based techniques, including multi-view geometries, focal lengths, primary points, aspect ratios, skews, and metrics. The main points or optical axis intersections and planes lie in genuine image centres. When tiny portions of images are moved or translated, copy-moves or images are merged, called spliced. It is not easy to retain main image points from the same perspectives [19].

DIP approaches have traditionally focused on altering image pixels. Hence, pixel-based DIFDs have been extensively utilized as the most basic and widely used forgery techniques. These approaches analyse inter-pixel correlations caused by direct/indirect image tampering. Copy-moves, Image splices, re-samples, and retouches are the most prevalent pixel-based DIFDs, as indicated explained in the introductory part of this work. In copy-moves, image parts are duplicated and/or within images, resulting in significant correlations in these areas, which can be utilized as evidence for DIFDs. However, developing effective characteristics or matching algorithms for DIFDs is a big issue.

2 Literature Review

DIFDs generally include pre-processing, feature extraction, and classification/detection techniques. These DIFD processes are examined by others researchers in previous works. The review consists of three sub-sections. Where the first section discusses processing methods. While subsequently, reviews of feature extraction approaches have been done. The third section review of classification and deep learning methods with its descriptions.

2.1 Preprocessing Methods

Forensic research mainly focuses on strong algorithmic creations to identify where altered image elements are present. Hence, image noise eliminations are the first step for clearly identifying forgeries.

A multitude of approaches exist in pre-processing, like color conversions, image smoothing, CEs (Contrast Enhancements), HEs (Histogram Equalizations), and MFs (Median Filters). In image forensics, it is critical to look at these processing processes, which are detailed below. Pre-processing step typically begins with color to grey scale conversions before the subsequent stage of feature extractions.

DIFDs for detecting copy-moves were proposed by Panzade et al. [20]. The scheme called CMFDs (Copy-Move Forgery Detections) converted RGB (Red Green Blue) images into HSVs (Hue Saturation Values) in their representations from faked photos. The study used SIFTs (Scale Invariant Feature Transforms) to extract key points and match them where they were clustered for final detection. Their comprehensive experimental findings demonstrate detection of cloned areas successfully. Their scheme also gave good results to geometrically transformed or multi-cloned images.

Many pre-processing methods were combined by Lonnie et al. [21] in their proposed scheme. Their pre-processing included HEs and filters (median, Gaussian and sharpening), processed using SIFTs. The study decreased false matches in identifying forged areas. SIFT key points such as identified counts, count of matches, and inaccurate match counts were displayed in the survey. Their scheme coupled SIFTs with pre-processing methods to reduce false matches in 30 tampered photos divided into three categories. Their optimum pre-processing strategy produced minimal false matches when tested on image databases.

A unique pre-processing method was proposed by Kuznetsov et al. [22]. Their work used hashing for the detection of copy-moves and could work on duplicated images. The work used initial image transformations to integrate modifications. In the second step, Image intensity range reductions, gradient computations, orthonormal expansions, Alces (adaptive linear contrast enhancements) and LBPs (local binary patterns) were compared during their tests on their ability to detect DIFDs.

CEs in DIPs can improve the dynamic range of image pixel values, as Chakraverti et al. [23] showed in their study for detecting copy-moves. Their ORB (Oriented FAST and Rotated BRIEF) approach was combined with modified Local CLAHEs (Contrast Limited Adaptive Histogram Equalizations), an alternative to SIFTs. Their experimental results revealed the success and betterment of their proposal when compared with other techniques in terms of FPRs (False Positive Rates) and TPRs (True Positive Rates).

Cao et al. [24] proposed two new methods using CEs for digital images that were modified. Their scheme concentrated on detecting global CEs, which were applied to JPEGs. Theoretically, histogram peak/gap artefacts caused by JPEG compressions or translation of pixels were examined, and zero-height gap fingerprints were identified for differentiation. It was followed by a novel method that detected composite images generated by enforcing contrast adjustments on source image regions. For detecting applied CEs in source areas, they were identified using block-wise peak/gap groupings. Image forgeries were detected by evaluating composition borders and the consistency of regional artefacts. Their extensive tests showed the efficacy of the proposed approaches. However, when CEs was the final post-processing step and failed on image compressions after executing CEs, it worked efficiently.

Yuan [25] proposed grey level cumulative distributions of image HEs. The distributions were represented as discrete identity functions on inherent fingerprints created by global HEs. The study has observed cumulative distributions matched well with their model. Their classifications recognized usage of global HEs. Compared to prior approaches, their proposed method differentiated global HEs from other types of CEs accurately. The proposal's effectiveness was exhaustively evaluated in identifying image HEs and resistance against attacks.

Powerful MFs were presented by Kang et al. [26] in their study where residuals of MFs (differences between original and filtered image versions) were examined statistically. The study fitted their MF residuals into an AR (Autoregressive) model for capturing statistical characteristics. Their model used AR coefficients as characteristics for detecting MFs, followed by a series of tests that evaluated the efficiency of their proposed MF based detections. Their results demonstrated that their proposed forensic methodology outperformed previous techniques, shallow FPRs and limiting characteristic counts.

MFs for DIFDs were also proposed by Gao et al. [27] using CFDIs (combined differences image characteristics). Their CFDIs were a combination of first-order JCPDFs (Joint Conditional Probability Density Functions) and Second-Order Difference Images. Dimensionality reductions were executed using PCAs (Principal Component Analyses) for obtaining final features for given threshold values. The study's experiments on single/compound databases showed that their proposed scheme outperformed other approaches on uncompressed/compressed image datasets, mainly on solid JPEG compressions and low-resolution images.

A different approach for detecting global CEs and copy-paste forgeries was proposed by Charpe et al. [28]. The study used contrast computations for detecting CEs in images. The proposed method was resistant to post-processing JPEG compressions, and features from the pictures in copy-paste duplicates were extracted using DCTs (Discrete Cosine Transforms). The scheme could detect tiny or medium, or large areas of fabrications in forged images with ease.

Sensor's pattern noise was used for DIFDs by Chierchia et al. [29] in their study. Their scheme recast forgery issue as a Bayesian estimation issue, used appropriate MRFs (Markov Random Fields) to describe the source's spatial solid dependencies, and judged each image pixel collectively. Subsequently, convex optimizations were used to produce globally optimum solutions, and non-local denoising enhanced PRNUs (Photo-Response Non-Uniformities) for estimations. Their simulation of genuine forgeries indicated that their proposed approach improved existing approaches successfully in a wide range of practical instances.

CNNs (Convolution Neural Networks) were used by Chen et al. [30], where the study presented convolution filters with an isotropic design. The scheme is minimized the number of CNN parameters and their proposed filter, rotation-invariant features using equal weights for image forensics. Their experiments demonstrated that their new rotation-invariant CNNs achieved significantly higher performances and fewer parameters, improving 13% in Gamma corrective forensics DIFDs. When compared to the popular BayarNet, it also produced considerably better generalization results on diverse databases, in addition to its resilience against JPEG compressions.

It may be noted that CLAHEs responsible for RGBs-HSVs conversions play a critical role in DIFDs pre-processing stages.

Picture enhancement entails methods that increase image quality, allowing for more accurate visuals for analyses. It is extensively utilized in various applications because it can overcome some image capture systems' constraints [31]. Image improvement processes include deburring, noise reduction, and contrast enhancement. CLAHEs [32,33] are standard approaches for enhancing local CEs that have proven practical and helpful in various applications [34–36]. CLAHE is a technique for increasing the visibility of a hazy picture or video.

CLAHE is an AHE variation that minimizes noise amplification. CLAHE has also been proven to be unsuitable for digital images with fine details. They combined global histogram modification with CLAHE in Histogram Modified (HM-CLAHE) [35]. Along with the usual CLAHE, local CEs

emphasized the small features buried in images and an enhancement parameter to adjust the amount of enhancement. As a result, combining Local Contrast Modification (LCM) with CLAHE yields optimum contrast enhancement with all local information of pictures that standard CLAHE may not fail.

The authors propose the LCM-CLAHE algorithm, which contains various steps: First, take the input image. LCM is provided with the original picture and the enhancement parameter as input. We alter the photo in LCM to generate the more delicate features concealed in the mammography image and then send that output image to CLAHE, enhancing image quality [37].

The initial step for image enhancements is an application of CEs to images where both global and local information are considered for image improvements. Local knowledge of images is captured by a window defined to the network's pixel widths. An equation can be used to express the transformation function Eqs. (1)–(2).

$$T = \frac{E.M}{\sigma} \tag{1}$$

$$g = T*(\mathrm{f} - \mathrm{m}) + m \tag{2}$$

E-parameter for enhancement, M–input image's global mean, g-enhanced image, f-input image, m-input image's local mean, σ local SD (standard deviation), E–constant in the interval [0, 1]. Eqs. (3)–(4) are used to calculate m and σ for a user-defined window width,

$$m(x,y) = \frac{1}{n*n}\sum_{x=0}^{n-1}\sum_{y=0}^{n-1} f(x,y) \tag{3}$$

$$\sigma = \sqrt{\frac{1}{n*n}\sum_{x=0}^{n-1}\sum_{y=0}^{n-1} (f(x,y) - m(x,y))^2} \tag{4}$$

Averages of windows are computed from the obtained standard deviation and local mean values utilized in Eqs. (1) and (2). The more delicate features of mammography pictures will be highlighted with this approach. This approach produces an improved image that is sent into CLAHE.

A picture received in RGB space is transformed into a color space with a brightness (Y) and two chrominance components (Cb, Cr) as shown in Eq. (5),

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112.000 \\ 112.000 & -93.786 & -18.214 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{5}$$

The two chrominance channels are separated, and the number of rectangular contextual tiles into which the image is split is determined for each chrominance channel. The best value for this is determined via experimentation. The contrast transform function is built based on a uniform distribution.

$$i_{c\_out} = [i_{c\_max} - i_{c\_min}]*F_k\left(i_{c_{in}}\right) + i_{c\_min} \tag{6}$$

Assuming i_{c_min} is minimum allowed intensity, i_{c_max} stands for maximum allowed intensity and optimal clipping limit is fixed and if F_k (i_{c_in}) represents cumulative distribution function for inputs i_{c_in}., then Eq. (6) mathematically depicts modified chrominance with uniform distributions. Inferences of pre-processing methods for forgery detection are discussed in Table 1.

Table 1: Inferences of preprocessing methods

Author	Algorithm	Merits	Demerits	Analysis and dataset
Panzade et al. [20]	RGBs to HSVs	Successful detection of cloned regions via color conversion	Noise present in the image is not removed. It may decrease the quality of the picture.	MICC-220, TPRs-7%, FPRs-100%
Lionnie et al. [21]	Histogram equalization, smoothing filter with median and Gaussian filter and sharpening filter	Pre-processing methods to reduce false matches	This system does not find suitable for some tampered images.	MICC F220, Mean Square Error (MSE), with Median Filter-36.2905 MSE with Gaussian Filter (sigma = 0.5)-7.2875 MSE with Gaussian Filter (sigma = 1)-55.0257
Chakraverti et al. [23]	LCM-CLAHE	The study's scheme showed promising results in terms of FPRs and TPRs	Filtering methods are not applied to remove noises presented from original images.	CoMoFoD, TPR-99.25% FPR-6.00% F_score-94.29%
Yuan et al. [25]	Histogram Equalization	Evaluations with HEs and resilience to attacks was good	Noise present in the image is not removed. Thus exact noise removal is not done correctly.	MICC-F2000
Kang et al. [26]	Median Filter Residual (MFR)-Autoregressive Model(AR) with subtractive pixel adjacency matrix (SPAM) features	The system performed better than similar techniques with reduced FPRs and minimized features	The work does not easily apply to higher-dimensional features.	Uncompressed Color Image Database TPRs-93.5%, FPRs-2.5%

(Continued)

Table 1 (continued)

Author	Algorithm	Merits	Demerits	Analysis and dataset
Gao et al. [27]	MFs based on combined feature differences (CFDI)	Achieves superior performance on the uncompressed image datasets	The improvement in detecting median filtering in heavily compressed images becomes a significant issue	UCID, Break Our Watermarking System (BOWS2), Dresden Image Database (DID) Area Under Curve (AUC) for JPEG compression with QF = 70-Combined Features Of Difference Image (CFDI)-0.986
Charpe et al. [28]	Global contrast enhancement	The technique can efficiently detect the small, medium and large size regions in the forged image	It could not see tampered images	Synthetic dataset, Robust against low, middle and high-quality JPEG compression
Chierchia et al. [29]	Photo-Response Non-Uniformity (PRNU) estimation and Markov Random Field (MRF)	It increased denoising results	Fails to improve spatial resolutions, which help detect smaller forged areas	Synthetic images, Mean CPU Time (S)-7.10 s, Standard Deviation-0.21

Note: The introduced method uses local CEs for highlighting minute image details and a parameter for controlling enhancements along with CLAHEs. This usage of LCMs (Local Contrast Modifications) with CLAHEs produced optimal CEs as more local image information was visible compared to normal CLAHEs.

As a result of the preceding, a variety of techniques to improve detection performance have been developed. The only difference between the following works is the characteristics utilized in the forgery detection method. Here, three main categories are introduced to categories these algorithms: Techniques based on space, transforms, and hybrid techniques [13] (see Fig. 3).

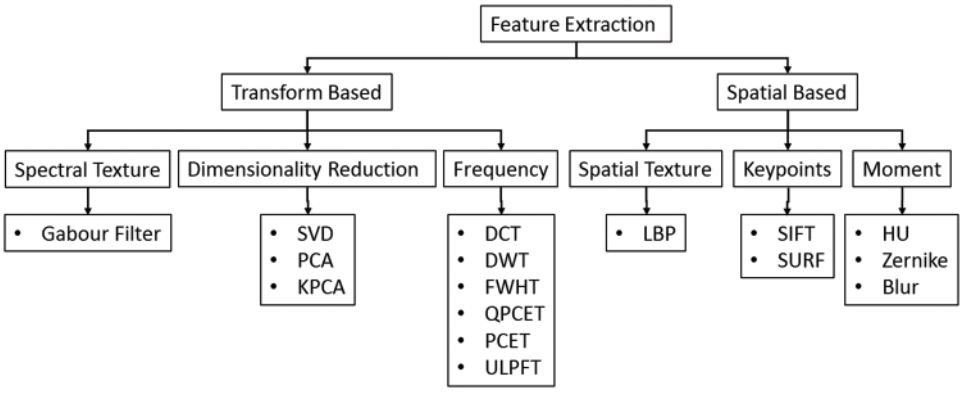

Figure 3: Classifications of feature extraction methods for copy-move forgery detection techniques

2.1.1 Spatial Domain Methods

The pixel location directly describes the content of a picture in a spatial feature space, where the energy is distributed evenly, and nearby pixels are highly associated. As a result, the matching procedure is highly computationally intensive. In spatial feature spaces, copy-moves can be based on moments or intensities or key points or textures.

Moment-based methods: Copy-move DIFDs can be assessed using Hue, blur invariance and Zernike moments. Liu et al. [38] detected duplicate locations in forged images by rotating the photos using circle block and Hu moments in their scheme. Their proposed method worked well against notions with noises, blurs, JPEG compressions and rotations.

Ryu et al. [39] proposed copy-move DIFDs detections using Zernike moments to locate duplicated areas. The presented approach detected forged areas amidst rotations as Zernike moment amplitudes show invariance in rotations. The proposed method is also resistant to deliberate distortions, including blurs, JPEG compressions, and the addition of white Gaussian noises. Their experiments showed that their technique was effective in identifying the faked region in copy-rotate-move forging.

Ryu et al. [40] suggested a forensic approach using Zernike moments of tiny picture blocks to locate duplicated image areas. To dependably reveal repeated measurements following arbitrary rotations, use rotation invariance characteristics. The block matching process is based on locality-sensitive hashing. It reduces false positives by looking at the phase of the moments, by using signal properties and differentiating between "textured" and "smooth" duplicated areas. The proposed approach beats prior art, especially when the repeated measurements are smooth. Experiments show that the system is resistant to JPEG compressions, blurs, additive white Gaussian noises, and modest scaling.

Singh et al. [41] proposed the No-Reference Image Quality Assessment (NR-IQA) technique, which employs simple spatial filtering operations and is computationally efficient. Laws' filters, which are effective in texture analysis, are used to calculate the features. A primary Generalized Regression Neural Network is used to predict the picture quality score (GRNN). Because of its low computational complexity, the proposed technique could be used in real-time applications. The proposed method produced good results amidst distortions with reduced computational cost when compared to most existing methods.

Intensity-based methods: Images were divided into distinct sub-blocks for computing their energies using various intensity-based copy-move DIFDs [42]. These techniques support both color and

grayscale pictures. However, all of these methods anticipated that the duplicated areas would not be subjected to post-processing, including scaling or rotations or JPEG compressions. The features mentioned above' rotation invariant characteristic has also been proved in a recent study [42]. Bravo-Solorio et al. [5,43] suggested methods for detecting reflections and rotation invariance in copy-moves. Pixel's Log polar transforms from overlapping picture blocks were used to determine the characteristics.

Key point-based methods: These techniques use high entropy areas to focus the entire picture. Das et al. [44] proposed a fast and robust detection method for this type of picture fraud. The image is first turned to grayscale. The grayscale picture is then divided into four parts using two-level SWTs (Stationary Wavelet Transforms). The key points were extracted by approximating components of a decomposed image using SIFTs. The matching pairs of key-points are then discovered. Then, using a variety of linking techniques, matching pairs of key-points are grouped.

SIFTs and reduced LBPs based histograms were used in Park et al. [45] method. The 256-level LBP values collected from local windows centered on key-points were then minimized. A 138-dimensional is created for each key point to detect copy-move fraud. While comparing the detection accuracy of the proposed algorithm with current techniques on many image datasets, findings showed that their proposed method outperformed other copy-move DIFDs in evaluations. Their scheme also exhibited uniform detections on a multitude of test datasets.

For feature extractions, Amerini et al. [46] proposed SIFTs that determined whether a copy-move attack has happened and retrieved the geometric transformation utilized for cloning. Extensive experimental data shows that the approach can accurately identify the changed region and estimate the geometric transformation parameters with high accuracy. This approach also handles multiple cloning.

Texture-based methods: The human visual system primarily interprets images through texture, divided into spatial texture and spectral texture properties. The pixel statistics are used to derive texture characteristics in the spatial domain. They may be computed from any data and are usually noise sensitive.

Li et al. [47] exploited textural characteristics using LBPs to manage geometrical changes. Images were low-pass filtered and subsequently divided into overlapped circular blocks, and finally, uniform rotation invariance LBPs were employed for extracting features in the pre-processing stage. The study was resistant to rotations, flips, noises, JPEG compressions, and blurs.

By collecting LBPs based Histogram Fourier Features of blocks, Soni et al. [48] detected copy-moves by proposing block-based blind DIFDs. The proposed approach is evaluated using the CoMoFoD dataset as a benchmark. Experiments indicate that the proposed technique decreases the time complexity of tamper detections and shows resistance to post-processing assaults such as blurs, brightness alterations, and contrast adjustments.

Kalsi et al. [49] proposed the Approximation Image Local Binary Pattern (AILBP) technique for feature extraction. A typical solitary picture is used to start the number of trials. The experiments show that the proposed system can provide exemplary performance in terms of speed and accuracy. Darmet et al. [50] proposed a method to disentangle source and target areas in copy-move based on local statistical model of image patches. Zhang et al. [51] proposed an end-to-end deep learning model for robust smooth filtering to identify multiple filtering operations simultaneously.

Yang et al. [52] proposed LBPs for rotation invariance in their DIFDs for detecting copy-moves. The study initially filtered and divided images into constant sized chunks that overlapped. LBPs

then extracted image characteristics from blocks and stored them as sorted feature vectors. Euclidean distance computations between blocks found block pairs. The study's shift-vector counter C identified tampered areas, thus demonstrating their DIFDs even on multiple copy-moves while resisting JPEG compressions, noises, blur rotations, and flips.

Adding an LBP histogram-based descriptor to the CMFD technique improves it [45]. LBPs for pixels centered on in 16×16 window key points were computed. The histogram of the 256 LBP levels is utilized as a new descriptor, and the histogram is decreased to 10 levels. A reduced LBPs histogram was used as additional descriptors to enhance key point pair matches.

LBPs are generic ways to extract textures from images. Their computations are simple with a higher level of discrimination. LBPs for pixels located at (p, q) can be computed using Eq. (7),

$$L(p,q) = \sum_{n=0}^{N-1} s(I_n - I(p,q))\, 2^n \tag{7}$$

where L(p, q)-centre pixel's LBP with (p, q) as its location and I_n is the intensity of neighboring pixel and I(p, q) represents the intensity of pixel located at (p, q), and N represents neighboring pixel count within a defined radius. Eight-bit LBPs are obtained by using a local window centred at (p, q)) and defined as s(x) in s(x) (8),

$$s(x) = \begin{cases} 1, & if\ x \geq 0 \\ 0, & else \end{cases} \tag{8}$$

Assuming $\Omega(x_i, y_i)$ represents pixels within (16×16) local window centred with k_i as t6he key point located at (x_i, y_i). LBPs are computed for all pixels at$(p, q) \in \Omega(x_i, y_i)$, LBP.

Features obtained using SIFTs carry information suitable for CMF detections. Hence, using complete LBPs may not be required. LBPs with a maximum of two transitions in 0→1 or 1→0 are categorized as uniform patterns (characterized by consecutive 1's) where 00110000 is an example. 01010100 six transitions or is a non-uniform pattern. Amongst 256 LBPs, only 58 were found to be uniform. Assuming Lc(p, q) (c = 0, 1, 2, …, 8) are LBPs with c consecutive 1's, then L0(p, q) = 00000000, and L8(p, q) = 11111111. For c = 1, 2, …, 7, Lc(p, q) can have 8 binary patterns or view as rotational shifts of the single pattern. Lnon(p, q) are patterns without consecutive 1's except for L0(p, q). 256 level LBPs can be divided into 10 groups where Lc(p, q) total nine and Lnon(p, q).

This work uses $L_c(p,q)$, $L_{non}(p,q)$ probabilities as CMFD descriptors. Further, the descriptor's rotation invariance is maintained by checking $L_c(p,q)$ the occurrences. Values from $L_{non}(p,q)$ might reflect variations occurring due to noises or modified backgrounds or errors in quantization within small windows. Non-uniform patterns are checked for reducing these effects of variations. A descriptor r_i with its corresponding keypoint k_i is depicted in Eq. (9),

$$r_i = \{R_0(x_i, y_i), \ldots R_8(x_i, y_i),\ R_{non}(x_i,\ y_i)\} \tag{9}$$

where $R_c(x_i, y_i)$ and $R_{non}(x_i, y_i)$ are the normalized number of occurrences of $L_c(p,q)$ and $L_{non}(p,q)$, respectively, in $\Omega(x_i, y_i)$. $R_c(x_i, y_i)$ is calculated by Eq. (10),

$$R_c(x_i, y_i) = \frac{\#[L_c(p,q)]}{|\Omega(x_i, y_i)|},\ for\ all\ \ (p,q) \in \Omega(x_i, y_i) \tag{10}$$

where $\#[L_c(p,q)]$ represents $L_c(p,q)$ pattern counts or cardinality in $\Omega(x_i, y_i)$ and Rnon(x_i, y_i) can also be found similarly. r_i is a ten-dimensional feature vector encompassing $L_c(p,q)$ and $L_{non}(p,q)$ Histograms.

Eq. (11) is used to get the SIFT based key point descriptor and to obtain a histogram of reduced LBPs,

$$g_i = \{f_i, r_i\} \tag{11}$$

where g_i represents CMFD's descriptor with 138-dimensional features as r_i in contrast to f_i is computed from larger areas and can robustly handle minute pixel changes and errors in quantization caused by compressions.

2.1.2 Transformation Based Approaches

Coefficients have lower correlations when transformed, and only a few coefficients have most of the energy. Hence, only these coefficients are used as features for overlapping blocks. Transformations can be in three forms, namely Frequencies, textures and reduced dimensions.

Frequency-based transformations: DIs were validated based on pixels by Parveen et al. [53] in their proposed DIFDs for copy–moves. Their study used five significant steps: (1) color images were converted to grey-scale images, (2) the converted images were then split into 8×8 overlapping blocks, (3) DCTs were used for extracting features based on feature sets, (4) the blocks were clustered by K-means clustering (5) features were matched using radix sorts. Their experimental evaluations showed that the scheme accurately detected forged areas in DIs.

Alahmadi et al. [54] suggested passive DIFDs based on LBPs and DCTs. First, discriminative localized features are extracted from the chrominance component of the input picture using 2D-DCTs. Detections were then carried out using a support vector machine. Experiments on three picture forgery benchmark datasets showed that their approach outperformed recently developed methods with better detection accuracies.

Hayat et al. [55] proposed DIFDs based on feature reductions using the DWTs and DCTs. After splitting the DWT images into separate blocks, the DCT is applied. The correlation coefficients are then used to compare the blocks. A mask-based tampering mechanism is also created as part of the studies to verify the detection approach. When compared to two other systems in the literature, the method yields intriguing findings.

Jwaid et al. [56] used DWTs and PCAs to do productive calculations in light of LBPs. Pre-process the image to convert it from RGBs to YCbCrs (Yellow, Green, and Blue). Second, the picture is compressed using the Discrete Wavelet Transform. The guess sub-picture comprises areas with low recurrence and the most severe data. Covering squares divide the LLs (Low Levels) sub-images. LBPs and PCAs matched chunks as part of the feature matching process. The final stage used SVMs (Support Vector Machines) to classify fakes.

Thajeel et al. [57] created novel stage-wise CMFDs based on QPCETs (Quaternion Polar Complex Exponential Transforms). The suspicious image is split into blocks that overlap. Second, QPCET is used to extract invariant characteristics for each block. Finally, k-dimensional tree (kd-tree) block matching is used to find duplicated picture blocks. Finally, a novel approach is proposed to decrease false matches caused by flat regions. Experimental results demonstrated the proposed approach's exact and efficient recognition capability of copy-moves on rotated, scaled, noises added, blurred, brightened, colors reduced, and JPEG compressed images. Furthermore, the proposed technique solves false matches and outperforms other methods in terms of accuracy and false-positive rate. The technique shown here might be used to conduct accurate digital image forensic investigations.

PCETs (Polar Complex Exponential Transforms) were suggested by Wo et al. [58] to detect copy-moves. The study extracted rotationally invariant and multi-scale features with PCETs which used multi-radii with graphic processing unit accelerations. For achieving coarse matches, lexicographical order matches optimized with minimum heap were used. The radius ratio and location information were applied to detect changes accurately. The proposed PCETs noticed forged sections created by rotations or scaling while resisting smoothing, JPEG compressions, and noise degradations.

Soni et al. [59] proposed an efficient block-based copy-move DIFDs based on FWHTs (Fast Walsh Hadamard Transforms) to reduce processing time in finding duplicated portions in a picture. Lexicographical sorting and an effective shift-vector technique are used to detect forged areas.

Park et al. [60] proposed a ULPFTs (Up sampled Log-Polar Fourier Transforms) based descriptors resistant to rotation, scaling, sheering, and reflection, among other geometric changes. The theoretical foundations of the ULPFT representation are first presented. Then, from the ULPF representation, a feature extraction technique is shown that can extract scale-invariant features and rotations. Analyzed common CMFDs (Copy-Move Forgery Detections) processing pipeline and modified a section to handle various forms of tampering assaults more effectively. Simulation findings show that the introduced feature descriptor outperforms other descriptors with established performance guarantees. Another benefit of ULPFT is that it has low computational complexity.

A new approach for CMFD of duplicated items was given by Hosny et al. [61]. The bounding rectangle is designed around the identified item to create a sub-image. The morphological operator is used to get rid of the tiny things that are not needed. For the identified objects, exact PECT moments were employed as characteristics and items were compared using Euclidian distances and correlations between feature vectors.

Emam et al. [62] used PCETs to extract block's invariant characteristics, resulting in PCETs based kernels representing blocks. Second, probable comparable blocks were discovered using LSH (Locality Sensitive Hashing) and Approximate Nearest Neighbor searches. Morphological techniques are used to eliminate the incorrectly similar blocks, making the method more resilient. The presented approach is resilient to geometric changes with minimal computing complexity, according to experimental data.

Zhu et al. [63] proposed using Gaussian scales and extracting key-points quickly using ORB features in scales. Subsequently, the input image coordinates of FAST key points were reverted, and hamming distances matched obtained ORB features between key-points pairs. In its final part, the scheme eliminated falsely matched key points using RANSACs (Random Sample Consensus). Their experimentations showed that their approach was effective in detecting geometric transformations, including rotations and scaling. Further, their system was robust to see forgeries even in Gaussian blurred, or Gaussian white noised or JPEG recompressed images with high accuracy.

Dimensionality reduction-based methods: Chihaoui et al. [64] suggested automatically detecting duplicated areas in the same picture where SIFTs identified local properties of the photographs (sites of interest), and SVDs matched identical features. The findings demonstrate that the proposed hybrid approach is resistant to geometrical changes and can detect duplicated areas accurately.

SWTs (Stationary Wavelet Transforms) was proposed by Dixit et al. [65] to detect copy-moves due to shifting invariance of SWTs, which assist in similarity detections (matches) and dissimilar detections (noises) due to blurs in image blocks. The study used SVDs (Singular Value Decompositions) for deriving image features represented in image blocks. Additionally, the color-based segmentation technique employed in this study aids in achieving blur invariance. Their experimental findings showed the suggested technique's effectiveness in detecting copy-moves of images using intelligent edge blurring while outperforming most other methods in the accuracy of detections.

To describe and detect duplicated blocks in a picture, Hilal et al. [66] proposed an approach that used PCAs and DCTs. The algorithm is optimized and tested on a database of forged images. The algorithm's flexibility and performance are demonstrated by comparing the obtained results to a reference technique.

Sunil et al. [67] also proposed using DCTs and PCAs to compress overlapping block feature vectors. The down-sampling of low-frequency DCT coefficients creates features that are invariant to local changes in intensity.

Images are initially split into overlapping square blocks by Mahmood et al. [68], then DCT components were for block representations. Gaussian RBF kernel PCAs reduced the dimensionality of the feature vectors, thus improving feature matching efficiency. Extensive tests were carried out to compare the proposed approach with other approaches. Experimental findings show that the proposed method accurately estimated CMFDs even when pictures were polluted using blurs or noises or compressions and could identify numerous CMFDs. As a result, the proposed methodology was computationally efficient and reliable for copy-move DIFDs and enhanced the trust of evidence-based applications. However, compared to linear PCAs, both KPCAs and SVDs were computationally inefficient. In contrast, methods described above effectively expressed 2nd order data, forgeries based on altering high-order statistics, complex to detect.

Several authors have used PCETs, and as a result, PHTs (Polar harmonic transforms) are a type of complex exponential transforms [6–71]. It is a signal representation technique that uses a superposition. Harmonics to represent a signal [72–74]. PCETs are beneficial tools for characterizing images.

In polar co-ordinates (r, θ), the function Hnm(r, θ), includes radial basis function Rn(r) and angular function exp(jmθ) by Eq. (12),

$$H_{nm}(r,\theta) = R_n(r)\exp(\mathrm{jm}\theta) \tag{12}$$

where $R_n(r) = exp(j2n\pi r2)$, n, m $= -\infty, \cdots, 0, \cdots, +\infty, 0 \le \mathrm{r} \le 1, 0 \le \theta \le 2\pi$. Rn(r) is orthogonal in a unit circle, as in Eq. (13),

$$\int_0^1 R_n(r)\, R^*_{n'}(r)\, rdr = \frac{1}{2}\delta_{nn'} \tag{13}$$

where $\delta_{nn'}$ is the Kronecker delta and $R^*_{n'}(r)$ is the conjugate of $R_{n'}(r)$. The function set Hnm(r, θ) is orthogonal in the unit circle as in Eq. (14),

$$\int_0^{2\pi}\int_0^1 H_{nm}(r,\theta)\, H^*_{n'm'}(r,\theta)\, rdrd\theta = \pi\delta_{nm}\delta_{n'm'} \tag{14}$$

where π is the normalization factor; δ_{nm}, $\delta_{n'm'}$ are Kronecker deltas; and $H^*{}_{n'm'}$ (r, θ) denotes the conjugate of $H_{n'm'}(r,\theta)$. n order PCETs with repetition m are as per Eq. (15),

$$\begin{aligned} P_{nm} &= \frac{1}{\pi}\int_0^{2\pi}\int_0^1 f(r,\theta)\, H^*_{nm}(r,\theta)\, rdrd\theta \\ &= \frac{1}{\pi}\int_0^{2\pi}\int_0^1 f(r,\theta)\exp\left(-j2n\pi r^2\right)\exp(-jm\theta)\, rdrd\theta \end{aligned} \tag{15}$$

Based on the theory of complete orthogonal function sets, images can be reconstructed by PCET coefficient's infinite orders ($|n| \leq n_{max},\ |m| \leq m_{max}$).

2.1.3 Hybrid Methods

Many new approaches based on merged methods have recently been introduced to improve the performances of copy-moves in images. Yang et al. [75] proposed KAZE, a robust interest point detector that may be used in conjunction with SIFTs to extract additional feature points where enhanced matches are employed to deal with numerous duplications, and n-best matches in features can be discovered. Then, to eliminate false conflicts, a practical filtering step based on picture segmentation is performed. Furthermore, an iterative approach for estimating transformation matrices and determining the presence of forgeries is devised. The duplicated areas may be found at pix using these matrices. According to experimental results, the presented approach accurately detected duplicate areas even after distortions, including rotations, JPEG compressions, noise additions, and scaling.

Lin et al. [76] proposed a hybrid feature and evaluation clustering-based region duplication detection technique. The proposed system is broken down into two stages: rough matching and precise matching. Rough matching begins with the extraction of hybrid key points from the input picture, then is characterized by unified descriptors. Second, the Neural Network (NN) approach matches those key points. Third, the introduced clustering based on evaluation groups those matching key points. Fourth, affine transformations between these groups are approximated, and Bag of Word (BoW) is utilized to filter inaccurate affine transformations to enhance pixel-level results. When no affine transformation can be found, each suspicious region is addressed independently in precise matching. Under various situations, their suggested approach outperformed most other methods.

CMFDs were proposed by Tinnathi et al. [77] based on both block and key point techniques. Adaptive watershed segmentation is utilized to split the forged picture into non-overlapping segments, and adaptive H-minima transform retrieves the markers. In addition, a AGSOs (Adaptive Galactic Swarm Optimizations) to find the best gap value when picking the tags can improve segmentation performance by eliminating unwanted regional minima. After that, using HWHTs (Hybrid Wavelet Hadamard Transforms), the features from each segment are retrieved. Adaptive thresholding was then used to accomplish feature matches. RANSAC's (Random Sample Consensus) eliminated false matches or outliers. Finally, the FREA (Forgery Region Extraction Algorithm) was used to detect the duplicated region from the host picture. The presented technique successfully detects the picture forgery region, according to the results of the experiments.

Sunitha et al. [78] proposed CMFDs using key-points, combined feature extractions, and hierarchical clustering to identify forgeries. According to their experimental results, their suggested DIFDs achieved considerably higher performances when compared to other methods, according to their experimental results.

A machine learning classification approach was presented by Jaiswal et al. [3]. Spliced and non-spliced pictures were divided into two categories using logistic regression. For this, a feature vector was created using a mixture of four handmade features taken from photos. Then, using a logistic regression classification model, these feature vectors are trained. The outcome was evaluated using a ten-fold cross-validation test assessment technique. Finally, the study's comparisons of their suggested approach with other methods on three publicly available datasets discovered that the acquired findings outperformed other techniques.

FMTs (Fourier-Mellin Transforms) along with SIFTs were used by Meena et al. [4] in their hybrid approach for DIFDs. The study separated smooth and rough parts of images followed by key point's extractions from image textures using SIFTs. FMTs were applied on softer image parts for extracting their features which were then compared for detecting forgeries. Their scheme outperformed CMFD algorithms when tested with post-processing procedures and geometric transformations within an acceptable amount of time. In Table 2, the inferences of feature extraction approaches for forgery detection are well described.

Table 2: Inferences of feature extraction methods

Author	Algorithm	Merits	Demerits	Dataset and analysis
Ryu et al. [39]	Zernike moments	Detected suspicious images.	Framing an appropriate data structure is complex.	Extended dataset from National Geographic, Precision-81.20%, Recall-72.50%, F1-measure-93.67%
Ryu et al. [40]	Zernike moments	Reduce false positives by examining the moments' phase	Does not focus on local image manipulations.	Erlangen 'Image Manipulation Dataset, Pixel Detection Accuracy (PDA)-99.93%, Pixel False Positive (PFP) rate-19.8% True Positive Rate (TPR)-99.4%
Das et al. [44]	SWTs and SIFTs	Improved accurate forgery detections with lesser FPRs	Increased computation time for extracting features from the images.	MICCF220, Sensitivity = 90%, Specificity = 96%, FPR = 4%, FNR = 10%, Accuracy = 93%
Park et al. [45]	SIFTs and reduced LBPs	Better estimation accuracy in CMF detections when compared to conventional approaches	Even after feature matches, FPRs could not be eliminated	MICC-F220, CMH, D, and COVERAGE, TPRs, FPRs, and accuracies MICC-F220 Dataset TPRs = 99.10%, FPRs = 5.45%, ACCs = 96.82% CMH Dataset TPRs = 95.68%, FPRs = 0.35%, ACCs = 97.66% CMH5 Dataset TPRs = 95.80%, FPRs = 0.36%, ACCs = 97.72%

(Continued)

Table 2 (continued)

Author	Algorithm	Merits	Demerits	Dataset and analysis
Li et al. [46]	LBPs	Robust LBPs in rotation forgeries.	Appropriate selection of the dimension of the features to make the method strong to Random region rotations	UCID-an Uncompressed Color Image Database Correct detection ratio, False detection ratio True detection ratio of 0.8 with < 0.1 false detection ratios.
Kalsi et al. [49]	Approximation Image Local Binary Pattern (AILBP)	Showed high performances in terms of accuracy and speed	It does not extend to detecting forged images with various types of post-processing.	Synthetic dataset, House Image 300×300-execution time-0.51 s
Jwaid et al. [56]	(LBPs with DWTs	The scheme matched blocks in feature matches	Does not applicable to the large image size	Copy-move forgery detection database (CoMoFoD), Accuracy-95.13% Image size-$23 \times 23 = 98.035\%$, 3.0981%
Thajeel et al. [57]	Quaternion Polar Complex Exponential Transform (QPCET)	Reduces the flat region-mediated false matches.	Quick and robust detections of tampering, including affine transformations and combination attacks	CMFD database, CDRs (correct detection ratios) $= 98.0\%$ and FDRs (false detection ratios) $= 2.3\%$ against blurring attacks against brightness change attacks-CDRs-99.2%, FDRs-1.4% against color reduction attacks-CDRs-98.9%, FDRs-2.7%
Wo et al. [58]	PCETs	Detected copied areas using rotations or scaling.	PCETs are highly complex in their use of multi-radius feature extractions.	Image manipulation dataset (IMD), precision (95.2%), recall (51.9%) and F1-Score (66.1%)-,
Emam et al. [62]	PCETs	a robust approach for detecting geometrical transformations with reduced complexity	Morphology eliminated small holes and isolated pixels but could not eliminate noises completely	Real-world dataset, Precision, recall, F1-Score

(Continued)

Table 2 (continued)

Author	Algorithm	Merits	Demerits	Dataset and analysis
Tinnathi et al. [77]	Hybrid Wavelet Hadamard Transform (HWHT)	Copied areas are detected in images and minimize computational complexities	Image forged regions were affected by attacks & geometrical transformations	MICC-F600 dataset, and Bench mark dataset It illustrates AGSOs ability to identify forged images with Precision = 95.31%; Recall = 96.89% and F1 = 95.28% on MICC-F600 Precision = 99.08%; Recall = 98.42% and F1 = 98.33% on Bench mark dataset under plain copy move at image level
Sunitha et al. [78]	Hybrid feature extractions using SURFs-detections and SIFTs-descriptors. Efficient key-point based CMFD (EKP-CMFD)	Efficient mismatch elimination and image transformation	Forged regions were indicated using lines without explicit demarcations of boundaries	MICC-F220 dataset EKP-CMFD-Recall-92.50%, FPR-8.90%, F1-Score-91.70%
Meena et al. [4]	FMTs and key point-based techniques using SIFTs	Detect the duplicated regions of the image	Feature extraction with more computation time	Image Manipulation Dataset (IMD), GRIP dataset, Precision, Recall, F-measure **Rotation attack** Precision = 93.88%, recall = 95.83% and F-measure = 94.85% **Scaling attack** Precision = 94.00%, recall = 97.92% and F-measure = 95.92% **JPEG compression** Precision = 94.12%, recall = 100% and F-measure = 96.97% **Additive noise** Precision = 91.67%, recall = 68.75% and F-measure = 78.57%

2.2 Review of Classification and Deep Learning Methods

The job of detecting picture fraud among legitimate and counterfeit photos is a binary classification example [79–83]. This part will go through the specifics of detecting forgeries using conventional matching and deep learning approaches.

Cozzolino et al. [84] suggested CMFDs and localization based on dense nearest-neighbor field computations in a short amount of time. The study's Patch Match was a recursive randomized method for nearest-neighbor search that uses image regularities to converge to a near-optimal and smooth field swiftly is utilized to do. Modify the fundamental algorithm to make it more resistant to rotations while maintaining its computational efficiency. Experiments demonstrate that the presented approach outperforms all evaluated reference procedures in terms of accuracy and speed nearly equally.

Copy–moves were detected in DIs by Bi et al. [85] with their proposed MLDDs (Multi-Level Dense Descriptors) based on Hierarchical Feature Matches. The study's descriptors (Color Textures and Invariant Moments) were extracted at several levels with MLDDs. Their Hierarchical Feature Matched identified forged areas in DIs after computing MLDDs for pixels. The pixels with comparable color textures were sorted into different neighbor pixel groups and geometric invariant moments of pixels identified a pixel's corresponding neighbors. Subsequently, Adaptive Distances and Orientations are used for Filtering superfluous pixels based on generated/matched pixel pairs. The study used morphology for their final outputs, where forged areas were identified. Their experiments demonstrated the scheme's sturdiness even under demanding conditions, including geometric transformations, JPEG compressions, noise additions, and down sampling compared to other CMFDs.

Key points identified forged smooth areas in DIs by Wang et al. [86] in their scheme based on CMFDs. Their scheme divided tampered DIs into non-overlapping/irregular super pixels before categorizing super pixels from smoothened, normal textured and strongly textured backgrounds based on local information entropies. Subsequently, adaptive feature point detectors extracted DIs key points from super pixels belonging to different textures and generated local visual characteristics (moment magnitudes) for these super pixel key points. A reversed generalized dual Nearest Neighbor Algorithm discovered key point's matches quickly. In the final stage, erroneous key-points were eliminated by random sample consensus and forged areas were normalized using zero-mean normalized cross-correlations. The scheme showed its superiority compared to other CMFDs in detecting copy-moves in DIs generated with geometric transformations, JPEG compressions, and additive white Gaussian noises.

Bi et al. [87] segmented host images into irregular but non-overlapping patches using multiple scales. The study used SIFTs to extract multi-scale feature points from these patches. Subsequently, APMs (Adaptive Patch Matches) identified suspicious/forged areas for the used scales. Matched Key points were merged, and suspect regions of multiple scales were combined in the final stage to identify forgeries. Their experimental evaluations outperformed other CMFDs in DIFDs on images forged with geometric transformations, JPEG compressions, and specific noise additions, including multiple copies and down sampling.

Li et al. [88] developed a quick and efficient CMFD method using hierarchical feature point matches. First, prove that reducing contrast thresholds and image rescales required key-points even in tiny or smoothened areas. Then, to handle more key point counts in matches, a unique hierarchical matching technique was devised. Unique iterative localizations decreased false alarm rates and precisely located tampered regions with the assistance of key-points' resilient features, including leading orientations, size information, and color information. Extensive experimental data are presented to illustrate the suggested scheme's improved performance in terms of efficiency and accuracy.

Wang et al. [89] proposed color invariance as the base for their DIFDs where SIFER (Scale-Invariant Feature Detector with Error Resilience) and FQRHFMs (Fast Quaternion Radial Harmonic Fourier Moments) were used for detecting copy-moves. Their scheme derived adaptively stable key points from super pixels by integrating block contents with SIFER color invariance after segmenting DIs into non-overlapping uniform super pixel blocks. The extracted key-points and local image features were used to build Delaunay triangles using FQRHFMs and gradient entropies. The proposal matched Delaunay triangles using CSHs (Coherency Sensitive Hashing) followed by DLFs (Dense Linear Fittings). Errors in Delaunay triangle matches were eliminated by localizing forged areas using ZNCCs (Zero Mean Normalized Cross-Correlations). The study's extensive tests assessed the scheme's efficacy in copy-move forgeries with positive finds.

Copy-moves were also detected by Yang et al. [90] in their study using multi granular super pixel matches. Their approach combined key point and block-based features for their DIFDs. The scheme extracted stable key-points in DIs from coarse granular super pixels after dividing DIs into non-overlapping/irregular coarse granular super pixel-based blocks. Each of these extracted super pixel's features was considered quaternion exponent moment magnitudes and used for rough granular super pixel matches where E2LSHs (Exact Euclidean Locality Sensitive Hashing algorithms) quickly identified forged areas. In the final step, finely granulated super pixels were separated and replaced by their key point matches followed by morphological operations on delicate granular super pixel neighboring areas, which were then combined to yield the identified forgery areas. When tested on publicly available online datasets, extensive experimental findings showed that the presented method performs well under a range of demanding situations compared to other techniques.

Liu et al. [91] proposed a new Key point and Patch Match-based CMFDs. To obtain trustworthy key-points, LIOPs (Local Intensity Order Patterned), robust key point descriptors was coupled with SIFTs. After matching the collected key points using g2NN, the redundancy matched key point pairs were eliminated using matched key point pair descriptions and filters based on density grids. Finally, an improved method for matching patches was used to evaluate key-point pair matches to detect forgeries properly. According to their experimental results, their presented technique accurately saw copy-moves in images better than existing methods and performed well even on deformed images processed by rotations, JPEG compressions, and noise additions and scaling.

Elhaminia et al. [92] proposed treating CMFDs as MRFs in labelling. Pre-processing included over segmentations to create super pixels which were treated markov network nodes for balancing precision and speed. The maximal a posteriori labelling can accurately map the forged areas while selecting unary and binary potentials intelligently. According to qualitative and quantitative comparisons with other methods utilizing public benchmarks, the presented technique can enhance accuracy while keeping processing demands low.

Cozzolino et al. [93] detected copy-moves accurately using rotational invariance, where these characteristics were computed based on localizations. The study's Patch Match was a dense-field approach that showed better performances when compared to key point approaches but took longer execution time in feature matches. The study computed dense fields in DIs and handled invariant characteristics more effectively, increasing resilience against rotation or scaling. Furthermore, based on the output field's smoothness, a dependable and straightforward post-processing technique was devised. According to their experimental research on available online datasets, their approach was accurate with greater resilience and quicker than most dense field references.

Ouyang et al. [94] proposed CNN based CMFDs. The proposed technique takes an already trained model from an extensive database, such as ImageNet, and tweaks the net structure significantly

with tiny training examples. Experiments demonstrate that the proposed approach produced good counterfeit images automatically using simple image copy-moves using computers.

Liu et al. [95] proposed that CMFD be performed using CKNs (Convolution Kernel Networks). CKNs are deep convolution architectures based on data-driven local descriptors. Because of its high discriminative capabilities, it can produce competitive results. Three essential modifications are made to better adapt to the situation of CMFD: First and foremost, CKN has been rebuilt for use with a Graphical Processing Unit (GPU). The GPU-based reconstruction achieves excellent efficiency and allows hundreds of patch matching in CMFD to be applied. Second, to create homogenously dispersed key points, a segmentation-based key point distribution technique is presented. Finally, an adaptive over-segmentation approach is employed. Experiments on publically available datasets are carried out to verify the proposed method's other performance.

Thakur et al. [96] concentrated on efficient splicing detection and CMFD pipeline design, which focuses on identifying the traces left by different Splicing and copy-move forgeries post-processing activities like JPEG compressions or noises or blurs or contrast adjustments. Their use of LFRs (Laplacian Filter Residuals) and SDMFRs (Second Difference of Median Filters) on images as one of the residuals were introduced jointly to suppress image content and focus solely on the traces of tampering activities.

Agarwal et al. [97] developed a deep learning-based approach for identifying the CMFD. The newly developed method uses the altered picture as the system's first input for detecting the tampered region. Segmentation, feature extraction, dense depth reconstruction, and ultimately seeing the tampered areas are all part of this method. The newly developed deep learning-based method may reduce computing time and improve the accuracy of duplicated region detection.

BRISKs (Binary Robust Invariant Scalable Key points) were used as Yang et al. [98] descriptors in their study. Their approach used adaptive uniform threshold value distributions to extract key-points of local features from DIs. The study then used the embedded random ferns approach for formulating needed matches, thus achieving discriminative classifications. Their local descriptors based on BRISKs matched image key-points. The study also used RANSAC's to eliminate erroneous key point pairs Normalized Intensity Correlations to detect tampers in DIs. Their experiments with other CMFDs showed their scheme's enhanced detection and localization accuracies even under adverse image conditions.

DCNNs (Deep Convolution Neural Networks) were exploited by Kao et al. [99] for offline hand signature verifications. The study used novel local feature extractions using SigComp on ICDAR (Document Analysis and Recognitions) 2011 dataset. Their training on the authenticity of signatures was used for testing unsaved fresh author's signatures.

Feng et al. [100] proposed a CNN based picture forgery detection method to achieve image pre-processing for the Columbia University picture mosaic detection dataset. SRM and high-pass filtering are introduced initially instead of the standard feature of extracting related features based on image content. The CNN then completed the training and verification processing. On the classification findings, the impacts of pre-processing and the number of convolution layers are thoroughly compared. Experiments indicate that the CNN approach described in this paper is successful and resilient in classifying picture forgeries.

Agarwal et al. [101] compared different deep learning-based forgery detection approaches with strategies that do not utilize NN architecture for feature extraction. To identify these photos as factual or fabricated, developing an effective image forgery detection system is necessary.

Zhong et al. [102] proposed a Dense-Inception Net-based image CMFD method. Dense-InceptionNet, which are multi-dimensional DNNs (Deep Neural Networks) with dense feature connections. Their DNNs learnt feature correlations in training and used their learning to match forgeries. The use of PFEs (Pyramid Feature Extractors), FCMs (Feature Correlation Matches) and HPP (Hierarchical Post-Processing) modules were a part of their Dense-Inception Nets. PFEs extracted dense multi-dimensional/scale features where each layer was linked directly to previous layers. FCMs learnt strong correlations amongst features for producing candidate matches as maps. HPP in the final stage used these maps to generate cross entropies using training's back propagations. Their experimental results showed that their Dense-Inception Net approach produced efficient DIFDs while proving to guard against most known assaults.

For Copy-Move Forgery Detection, Pun et al. [103] proposed a two-stage localization method CMFDs. SLIC (Simple Linear Iterative Clustering) divided images into meaningful patches in the first step, preliminary localization. The WLDs (Weber Local Descriptors) computed and extracted feature from each super pixel is then presented. The super pixel matches are then obtained using a matching threshold based on an experimental study. In the final step, weak super pixel's Euclidean distances were used to generate suspect approximations. The study's DAFMTs (Discrete Analytic Fourier–Mellin Transformations) extracted image characteristics at a blocking lever while localizations were given by sliding varying radii circular blocks in suspect areas. The study's generated candidate circular blocks were matched by LSHs (Locality-Sensitive Hastings). Poor matches were filtered and eliminated in identified areas to obtain final identified regions, and geometric morphological techniques were used. The extensive experimental findings show that the proposed approach outperformed other CMFD methods on available benchmark databases.

Silva et al. [104] proposed a new method to CMFD based on a digital image's multi-scale analysis and voting procedures. Extract interest points from a suspicious image resilient to scaling and rotation, then look for probable correspondences between them. Based on geometric restrictions, corresponding group points into regions. Following that, a multi-scale picture representation is built for each scale. The produced groups are examined using a highly resilient descriptor to rotation, scaling, and somewhat robust to compression, reducing the search space of duplicated regions yielding a detection map. The ultimate choice is made once all detection maps have been voted. Validate the approach using a variety of datasets that include both original and realistic picture cloning. Compare and contrast the proposed method with 15 others found in the literature and present promising findings.

Pun et al. [105] proposed an adaptive over-segmentation and feature point matching CMFD method. The proposed technique combined forgery detection methods based on blocks and key-points. The study's over segmentations adaptively divided DIs into non-overlapping/irregular blocks to extract feature points from blocks that were matched to identify labelled feature points, thus indicating forged areas in DIs. They replaced feature points in forged areas with tiny super pixels and combined neighboring blocks similar to feature blocks' local color characteristics, thus creating a merged region. As the last step, morphological operations identified forged regions from the merged regions. Their proposed scheme identified developed regions as very effective when compared to other DIFDs for copy-move detections. Their experimental results also showed that their copy-move forgery detection system produced considerably superior detection results under various demanding situations.

Li et al. [106] proposed a method for CMFD in images based on the extraction of key points. The study's approach differed from prior approaches in dividing DIs as semantically independent blocks

before key point extractions. Subsequently, these extracted patches were matched for identifying copy-moves. The study's matches used two steps where initially suspicious patch pairs included forged areas in the first step to estimate approximate affine transform matrices. EMs (Expectation-Maximizations) was used subsequently to refine the estimated matrices and establish their existence. Comparing the presented method to other strategies on public datasets, experimental findings showed that it performed well.

Bi et al. [107] proposed a new and fast reflecting offset-guided CMFD image searching technique. The features are retrieved, and feature correspondences are randomly allocated during the initialization step to get initial mapping offsets, while reflective offsets were computed in searches to obtain mapping offsets as copy-move forgery mapping offsets. Then copy-move forgery mapping offsets were disseminated to enhance mapping and reflective offsets based on priority feature matches. Finally, only a few iterations can completely detect the forgeries areas from the mapping offsets. According to experimental data, the presented approach for image copy-move DIFDs decreased computational complexities while providing higher detection results than other CMFD algorithms, even under challenging situations.

Bi et al. [108] proposed a method for detecting CMFDs for accuracy and resilience. To build feature correspondences in images, the study used an enhanced coherency sensitive hashing algorithm. A local bidirectional coherency error factor was used in iterations for improved accuracy and advanced feature correspondences. The iterative procedure ended when the local bidirectional coherency error fluctuations were less than a predefined threshold, suggesting that feature correspondences were stable. This error of each feature was used to recognize copy-moves from regular feature correspondences. Their experimental findings demonstrated that their proposed detection technique was successful in real-time/near real-time data and produced excellent detection results compared to other copy-move DIFDs even under challenging situations.

CNNs were used by Rao et al. [109] in their study for their CMFDs, where CNNs learnt RGB color image's hierarchical representations from DIs. Their CNNs spliced images for detecting copy-moves. Instead of randomizing weights, the study network's first layer was initialized by high-pass filter sets and residual maps computed for SRM (Spatial Rich Models). The model regularized DIs efficiently to suppress image effects and capture artefacts introduced in image tampers. The study's pre-trained CNNs extracted dense features of DIs, followed by feature fusions to explore discriminative features for classifying using SVMs. The scheme's experimental results on multiple datasets showed that their CNNs outperformed most other methods.

Fig. 4 depicts the suggested CNNs' architecture, including 8 convolutions, 2 pooling, and 1 fully-connected layer with a bi-way softmax classifier. Patches of $128 \times 128 \times 3$ (128×128 patch, 3 color channels) make up the CNN's input volume. The first and second convolution layers contain 30 kernels with a receptive field of 55, whereas the subsequent layers all have 16 kernels with a receptive field of 33. ReLUs (Rectified Linear Units) were applied to neurons for the activation function to preferentially react to relevant signals in the input using a size 22 filter, which resizes the input spatially and discards 75% of the activations. This is because the max-pooling process aids in the retention of additional texture data and improves convergence performance. Local response normalization is also used to the feature maps before the pooling layer to increase generalization, where the surrounding pixel values normalize the center value in each neighborhood. Finally, through "dropout," which sets the neurons in the fully-connected layer to zero with a probability of 0.5, the recovered 400-D features (5516)

are transferred to the fully-connected layer with a bi-way softmax classifier. This usage of the fully-connected layer at the end was different from other traditional CNNs using 2 or more fully connected layers, leading to overfitting, especially in small training sets.

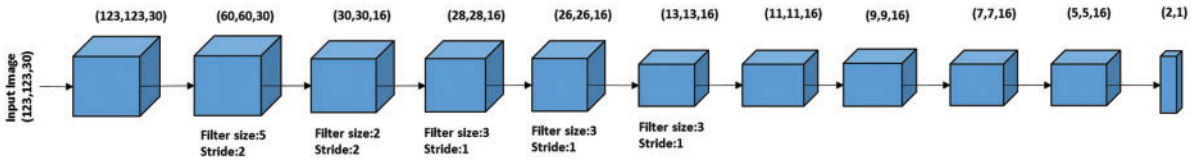

Figure 4: The architecture of the proposed 10-layer CNN

Wu et al. [110] also proposed end-to-end DNNs in DIFDs. The study's CNNs extracted block features from DIs and computed self-correlations between blocks with extracted feature points matched to rebuild forged/masked areas using de-convolutions. In contrast to traditional approaches, which needed multiple training and parameter tuning steps followed by post-process spans, the proposed method eliminated multiple training/parameter adjustments. The study's scheme was trainable as it combined forged mask reconstructions with loss optimizations. Their experimental results showed that their proposed scheme beat other traditional DIFDs based on their matching schemes and effectively against assaults, including affine transforms, JPEG compressions, and blurs.

Wu et al. [111] proposed BusterNet, a new DNNs for CMFD images. BusterNet is an accurate, end-to-end trainable DNNs system, unlike prior efforts. It has a two-branch design with a fusion module in the middle. The two branches, respectively, locate possible manipulation locations (by checking for visual artefacts) and copy-move regions (by evaluating visual similarities). This is the first CMFD algorithm that can identify source/target areas with discernibility to the best of our knowledge. Simple techniques for generating large-scale CMFD samples from out-of-domain datasets are shown, as well as stage-wise BusterNet training procedures. According to extensive tests, BusterNet considerably beats other copy-move detection algorithms on the two publicly accessible datasets, CASIA and CoMo-FoD, and is resistant against other known assaults. However, it is preferable to take these features into account directly. Thus BusterNet is recommended as a two-branch DNN architecture.

Dashed blocks are only activated during branch training. Output mask of the main task, i.e., M_c^X is colour coded to represent pixel classes, namely pristine (blue), source copy (green), and target copy (red). Output masks of auxiliary tasks, i.e., M_m^X and M_s^X are binary where white pixels indicate manipulated/similar pixels of interests, respectively. In dual branch DNN based CMFDs, dashed blocks are active only in training. The main outputs (M_c^X) are color codes representing pixel classes: pristine (blue), source copy (green), and target copy (red) where output's masks of auxiliary tasks (M_m^X and M_s^X) are white pixels in binary representing manipulated/similar pixels. An input image X's features are extracted using CNNs, and feature maps are scaled to original image sizes using Binary Classifier (Mask Decoder) to create manipulation masks. CNN Feature Extractor may be used with any CNN. Because of their simplicity, the first four blocks of the VGG16 design are employed here. The resultant CNN feature has a resolution of 1,616,512, significantly lower than that required by the modification mask.

Bunk et al. [112] detected altered imaging with two approaches based on a combination of deep learning and re-samples. The study's Radon initially transformed re-sampled images computed from overlapped image patches converted to heat-map using deep learning classifiers and Gaussian

conditional random field models. The approach used Random Walker segmentations to identify tampered areas in images. LSTMs (Long Short-Term Memories) used these overlapped images as inputs for localizations and classifications. Their experiment results demonstrated that both approaches successfully identified and localized forgeries in DIs in terms of detection/localization capabilities.

Qiao et al. [113] used a linear parametric model to examine the problem of picture resampling detection. First, reveal the one-dimensional 1-D resampled signal's rare artefact. The detector is built based on the likelihood of residual noise recovered from the resampled signal using a linear parametric model after dealing with the nuisance parameters and Bayes' rule. After that, focus on the characteristics of a resampled image. Meanwhile, it calculates the likelihood of pixel noise and creates a realistic LRT (Likelihood Ratio Tests). Numerical studies indicate the significance of the presented technique in recognizing uncompressed/compressed resampled pictures compared to another testing.

Amerini et al. [114] proposed a novel CMFD and localization schema based on the J-Linkage method, achieving robust clustering in the geometric transformation space. Experiments on several datasets demonstrate that the proposed method surpasses other comparable strategies for CMFD reliability and accuracy in the modified patch localization.

Bayar et al. [19] proposed a new CNN-based technique for camera model identification that is resampling and recompression resistant. A new low-level feature extraction method is presented that employs both a restricted convolution layer and a nonlinear residual feature extractor in tandem. These layers' feature maps are then concatenated and sent on to subsequent convolution layers for feature extraction. The presented technique improves camera model recognition performance in resampled and recompressed pictures according to experimental data. When CNN is employed without ACFM in experiments, we utilize the architecture which refers to as Non ACFM-based CNN. It's worth noting that the ACFM method may be extended and used to various types of nonlinear features to add variety to current features and improve CNN's resilience in real-world settings.

Non ACFM-based CNN [19] is for Convolution Feature Maps Augmentation; BN stands for Batch-Normalization Layer; TanH stands for Hyperbolic Tangent Layer; ET stands for Extremely Randomized Trees.

CNNs for use in forensics was proposed by Bayar et al. [115] in their study. CNNs learning for classifying features tend to be on the current state of images contents. The study defined a new CNN layer called the restricted convolution layer, which concealed image contents during learning and manipulations were detected adaptively to overcome this issue. The study showed that their restricted CNNs could learn about manipulations directly in a series of tests where experimental results outperformed current other general-purpose manipulation detectors in DIFDs. Moreover, in cases of source camera model mismatched between training and testing data, their restricted CNN could still identify picture alterations correctly. The proposed method is made up of four separate conceptual blocks that may be used to: (i) use a block of 11 convolution filters to jointly suppress an image's content and learn prediction error features while training, (ii) extract higher-level representations of previously learned image manipulation features, and (iii) learn new connections between feature mappings in a deeper layer. These filters learn a linear combination of features in the exact location but from a different feature map across channels. The classification block, which has three completely linked layers, receives the output of the latter block. The input layer of our CNN in this study is a grayscale picture patch with 256×256 pixels.

Bondi et al. [116] proposed a method for detecting and localizing image manipulation based on different camera types' distinctive imprints on pictures. The algorithm's logic is that all pixels in immaculate photos should be recognized as being captured by a single device. In contrast, evidence

of several devices can be identified when a picture is created by image composition. The proposed technique uses a CNN to extract typical camera model characteristics from picture patches. These characteristics are then examined using iterative clustering algorithms to determine if a picture is fabricated and pinpoint the foreign location.

In low-resolution pictures, Zhang et al. [117] proposed a Shallow Convolution Neural Network (SCNN) capable of identifying the borders of fabricated areas from original edges. SCNN was created to make use of Chroma and saturation data. Two methods based on SCNN have been developed to identify and localize picture forgery areas: Sliding Windows Detection (SWD) and Fast SCNN. The CASIA 2.0 dataset is used to test this model. The results demonstrate that Fast SCNN operates effectively on low-resolution pictures and outperforms the other significantly. Several works [7,118–120] utilized this CNN. A CNN [6,121,122] is a multilayered neural network with a unique design to detect complicated data characteristics. Pixels are the building blocks of images. A number between 0 and 255 [123] is assigned to each pixel. A neural network based analysis [124–126] for image forensics based on localization of features.

Introduce a Fast SCNN method that is quicker and more efficient than SWD, inspired by the Fast RCNN. The suggested Fast SCNN computes all of the image's CNN characteristics. After that, the features are sent to SCNN's fully linked layers. Table 3 clearly explains classification inferences and deep learning approaches for forgery detection.

Table 3: Inferences of classification and deep learning methods

Author	Algorithm	Merits	Demerits	Dataset and analysis
Cozzolino et al. [84]	Dense nearest-neighbor field, modified Patch Match and Zernike moments (M-PM + ZM)	Robust to rotations without losing computation efficiencies	Displacements were ineffective	GRIP dataset, F-measure = 98.12%, CPU-time = 54.73 s
Bi et al. [85]	Multi-Level Dense Descriptor (MLDD)	Generated final DIFDs	3-step pipeline for dense feature extractions were complex	CMFDA, CMFDPM Precision, Recall, F-measure on CMFDA-88.89%, 100.0%, 94.12% Precision, Recall, F-measure on CMFDPM-89.53%, 96.25%, 92.77%
Yang et al. [90]	Multi-granularity super pixels matching based algorithm	Showed good detection performances under many challenging conditions	Manipulation of DIs could have been hidden in post-processing of strong noise additions, high range scales, angle rotations	FAU, and GRIP, Pixel-level F-measure = 96.63% Image-level F-measure = 89.52%, computation cost = 2760 s

(Continued)

Table 3 (continued)

Author	Algorithm	Merits	Demerits	Dataset and analysis
Ouyang et al. [94]	CNN classifier	Achieve better performance in various datasets	The method could not detect real-world copy-moves in DIs	UCID, OXFORD, CMFD image database Error = 2.32%, 2.43%, 4.2% for UCID , OXFORD, CMFD image database, respectively
Liu et al. [95]	Convolution Kernel Network (CKN)	The GPU version was robust to varying conditions with good discriminations	Research had gaps between copy-moves and CNN features	MICC-F220, precision, recall and F1-measure = 59.27%, 82.20%, 63.18% CoMoFoD dataset = 55.99%, 78.25% 59.97%
Kao et al. [99]	Deep Convolution Neural Network (DCNN)	Higher sample counts could increase accuracy rates	Unfavorable conditions of small sample size	ICDAR 2011 SigComp dataset **VGG-19** = Training accuracy = 99.93%, Validation accuracy = 100%, Testing accuracy = 99.96% Test FRR = 0%, Test FAR = 0.22% **Inception V3** Training accuracy = 100%, Validation accuracy = 99.98%, Testing accuracy = 90.85% Test FRR = 2.83%, Test FAR = 16.31%
Guorui et al. [100]	CNN classifier	Effective and robust for image forgery classification	MLTs based feature extractions had the same disadvantages as block-based methods	Columbia University image mosaic detection dataset, Accuracy No pre-processing layer = 65.22% General filtering = 83.94% Combination of SRM filtering and general filtering = 91.80%

(Continued)

Table 3 (continued)

Author	Algorithm	Merits	Demerits	Dataset and analysis
Zhong et al. [102]	Dense-Inception Net	Achieved performances were good against attacks and could increase the efficiency of detections	Falsely identified foreground in real-time DIs	FAU, CASIA CMFD, and Comofodnew Dataset Precision, Recall, F1-Score = 70.85%, 58.85%, 64.29% for CASIA CMFD Precision, Recall, F1-Score = 46.10%, 42.20%, 44.41% for FAU
Rao et al. [109]	CNN classifier	The advantage of modelling residuals was original image pixels were suppressed while generating residual images	Fully connected layers with more parameters might lead to overfitting in small training sets	CASIA v1.0, CASIA v2.0 and Columbia grey DVMM Spatial Rich Model (SRM)-CNN, Xavier-CNN = 98.04%, 88.24% for CASIA v1.0 SRM-CNN, Xavier-CNN = 97.83%, 97.30% for CASIA v2.0 SRM-CNN, Xavier-CNN = 96.38%, 74.67% for DVMM
Wu et al. [111]	BusterNet	Discernibility to localize source/target regions	Shows robustness to attacks	CASIA and CoMo-FoD Image Level Evaluation Protocol = Precision, Recall, F-Score = 78.22%, 73.89%, 75.98% , Processing Speed = 0.62 s for CASIA Dataset Precision, Recall, F-score = 83.52%, 78.75%, 80.09% for CoMo-FoD dataset
Bunk et al. [112]	LSTMs	Effective in detecting and localizing digital image forgeries	No visual changes in manipulations in authentic images fail to perform well in segmenting manipulated regions	NIST Nimble 2016 Dataset, Accuracy = 94.86%, and AUC = 91.38%

(Continued)

Table 3 (continued)

Author	Algorithm	Merits	Demerits	Dataset and analysis
Bayar et al. [19]	Augmented Convolution Feature Maps (ACFM) based CNN classifier	Introduced significantly improved camera model identification performance in resampled and recompressed images	Lower identification rate since it is a suboptimal solution of the trained network with a constrained convolution layer	Dresden Image Database, Accuracy = 98.58%
Zhang et al. [117]	Shallow Convolution Neural Network (SCNN)	DIFDs by localizing image's tampered areas	Sharp edges are a good indicator for classifying tampered regions in high-resolution images; it is not effective in low-resolution images that are relatively smooth	CASIA 2.0 Dataset, Accuracy Fast SCNN = 85.35% (JPEG), 82.93% (TIFF)

There is also a deep fake based technology which is emerging and hottest branch of image forgery. In this GAN's network is used to learn the probability distribution based on examples and generate the images which are very similar to original images. Li et al. [127] proposed a method to detecting forgery in face images generated by unseen face manipulation. In this method author used face x-ray based on blending step. Li et al. [128] proposed a novel frequency-aware discriminative feature learning framework based on single-center loss. Haliassos et al. [129] proposed Lip Forensics technique which targets high-level semantic irregularities in mouth movements.

Shang et al. [130] proposed pixel-region relation network which exploit pixel wise and region-wise relations for face forgery detection. It is very helpful to detect deep fake face forgery detection. Hu et al. [131] proposed dynamic Inconsistency-aware Network which uses CRM to capture global and local inter-frame inconsistencies to detect deep fake forged video.

Image inpainting forgery is task to reconstructing some regions in the image. It is the used in applications like object removal, image manipulations. This type of forgery has been focused in Elharrouss et al. [132]. Where various method has been discussed based on this problem. Currently, various work has been done to improve image inpainting. To tackle this type of forgery [133] proposed method like impainting quality assessment tool using local features. Zhu et al. [134] proposed a encoder-decoder network to detect patch-based inpainting operation as shown in Fig. 5. Zhang et al. [135] proposed a feature pyramid network for diffusion-based image inpainting.

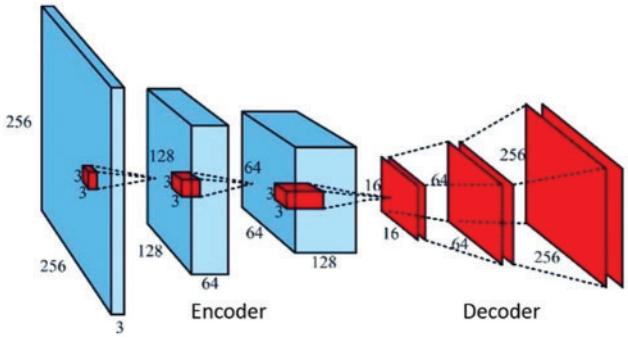

Figure 5: The layout, architecture and parameter settings of the CNN based on Encoder and Decoder network for inpainting forensics

Zhang et al. [135] proposed a Federated Learning to face forgery video detection, which is trained with decentralized data. Inconsistency-Capture module (ICM) [136] to capture the dynamic inconsistencies between adjacent frames of face forgery videos. Qian et al. [137] proposed a novel Frequency in Face Forgery Network taking advantages of frequency-aware decomposed image components, and 2) local frequency. Li et al. [138] proposed a novel feature learning framework for single-center loss which compresses mere intra-class variations of natural faces.

There are some other model which exploits the deep learning based approach such as DLFM-CMDFC [139], deep learning by recompression [140], copy-move image forgery [141], CNN by using the architecture of ResNet50v2 [142].

1) Convolution

A convolution is a two-function integration that demonstrates how one influences the other. The input picture, the feature detector, and the feature map are key components in this process as in Eq. (16),

$$(f * g)(t) \stackrel{def}{=} \int_{-\infty}^{\infty} f(\tau)\, g(t-\tau)\, d\tau \tag{16}$$

For input images, the feature detector (Kernel) could be a 3×3 or 7×7 matrix. The kernel multiplies matrix representations of the image elements to generate feature maps (convolved features or activation maps) to reduce image sizes and hasten to process. Though specific image characteristics might be lost, essential factors necessary for DIFDs are retained.

2) ReLu (Rectified Linear Unit)

This function boosts non-linearity in CNNs, and items that are not linear to each other are used to generate images. The primary use of ReLu is to handle image classification as a non-linear issue.

3) Pooling

The idea of spatial invariance states that the position of an object in an image has no bearing on the neural network's capacity to recognize its unique characteristics. CNNs Pooling (maximum/minimum) identifies image characteristics irrespective of illumination/camera angle differences s. A 2×2 matrix is placed on feature maps, and the most significant value in the box is selected while pooling. This 2×2 matrix is passed over the entire feature map from left to right, choosing the maximum value in each pass. These data are then combined to create a new matrix known as a pooled feature map. Max pooling helps to keep the image's key characteristics while shrinking its size. This helps avoid

overfitting, which occurs when the CNN is given too much data, especially if the information is irrelevant to categorizing the picture.

4) Flattening

After acquiring the pooled featured maps, they need to be flattened. The whole pooled feature map matrix is flattened into a single column, then given to the neural network for processing.

5) Full connection

The flattened feature map is then sent through a neural network after flattening. The input layer, the fully linked layer, and the output layer make up this stage. In ANNs, the completely connected layer is identical to the hidden layer, except it is fully linked in this case. The projected classes are the output layer. The data is sent via the network, and the prediction error is computed. The mistake is then sent back into the algorithm to enhance the prediction.

In most cases, the neural network's final values do not add up to one. However, it is critical to reducing these figures to integers between zero and one, which indicates each class's likelihood. By Eq. (17), the Softmax function plays this job,

$$\sigma : \mathbb{R}^K \to (0,1)^K,\ \sigma(z)_j = \frac{e^{z_j}}{\sum_{k=1}^{K} e^{z_k}}\ for\ j = 1, ..K \tag{17}$$

3 Challenges and Issues

The techniques above nevertheless have many drawbacks. First, rather than leveraging correlated information across patches. Most existing pixel-wise tampering detectors employ a patch-based approach. As a result, statistical information required for feature extraction is insufficient, particularly at the boundary of a forged region. Alternatively, to make assessing the validity of an inquiry patch simpler, the features of neighboring patches should be underlined.

Furthermore, the absence of statistical characteristics across flat sites (clear sky, Blue Ocean, etc.) generates estimation uncertainty, resulting in poor detection performance. In this case, the texture of the image content becomes an essential factor in enhancing detection accuracy. Furthermore, as image-editing software has advanced rapidly, the leftovers of alteration operations now behave similarly to the original (i.e., tampering traces are hard to detect). As a result, lowering the likelihood of detection mismatches and increasing localization resolutions (determined by the smallest unit of detection) remains an ongoing challenge.

Machine learning approaches that rely on block feature extraction, on the other hand, suffer from the same flaws as block-based methods. Furthermore, to counter forgeries, these algorithms only learn characteristics of a single recognized picture. Due to the lack of past information to handle forgeries in other images, the techniques must re-initialize the model and repeat many times. These approaches are significantly less efficient than deep learning methods.

4 Conclusion and Future Work

In terms of simulation, this article has examined the numerous processes involved in forgery detection approaches. It is clear from this paper that there would be two primary categories accessible in forgery detection. Several authors rely heavily on the passive voice. The passive-based forgery detection approaches are also discussed in this review paper, along with image processing processes such as preprocessing, feature extraction, and classification. Many writers have proposed numerous methods for picture preparation, but only a handful have solely concentrated on this phase. Several

scholars have worked on spatial domain approaches in feature extraction, but only a few have focused on transform and hybrid methods. Because of its high detection accuracy and quick calculation, Deep Learning-based feature extraction has made significant progress in forgery detection applications. Furthermore, the authors are attempting to enhance the accuracy of forgery detection, either by building a solo feature extractor or by inventing additional feature extraction. Finally, several detecting matching techniques are examined.

Funding Statement: The authors received no specific funding for this study.

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

References

1. Rocha, A., Scheirer, W., Boult, T., Goldenstein, S. (2011). Vision of the unseen: Current trends and challenges in digital image and video forensics. *ACM Computing Surveys, 43(4),* 1–42. DOI 10.1145/1978802.1978805.
2. Pasquini, C., Boato, G., Pérez-González, F. (2014). Multiple JPEG compression detection by means of Benford-Fourier coefficients. *2014 IEEE International Workshop on Information Forensics and Security*, pp. 113–118. Atlanta, USA.
3. Jaiswal, A. K., Srivastava, R. (2020). A technique for image splicing detection using hybrid feature set. *Multimedia Tools and Applications, 79(17),* 11837–11860. DOI 10.1007/s11042-019-08480-6.
4. Meena, K. B., Tyagi, V. (2020). A hybrid copy-move image forgery detection technique based on Fourier-mellin and scale invariant feature transforms. *Multimedia Tools and Applications, 79(11),* 8197–8212. DOI 10.1007/s11042-019-08343-0.
5. Bravo-Solorio, S., Nandi, A. K. (2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. *Signal Processing, 91(8),* 1759–1770. DOI 10.1016/j.sigpro.2011.01.022.
6. Zhang, R., Tan, S., Wang, R., Manivannan, S., Chen, J. et al. (2019). Biomarker localization by combining cnn classifier and generative adversarial network. *International Conference on Medical Image Computing and Computer-Assisted Intervention*, pp. 209–217. Shenzhen, China.
7. Wang, C., Deng, W. (2021). Representative forgery mining for fake face detection. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 14923–14932. Nashville.
8. Gill, N. K., Garg, R., Doegar, E. A. (2017). A review paper on digital image forgery detection techniques. *2017 8th International Conference on Computing, Communication and Networking Technologies*, pp. 1–7. Delhi, India.
9. Rosales-Roldan, L., Cedillo-Hernandez, M., Nakano-Miyatake, M., Perez-Meana, H., Kurkoski, B. (2013). Watermarking-based image authentication with recovery capability using halftoning technique. *Signal Processing: Image Communication, 28(1),* 69–83.
10. Wang, X., Xue, J., Zheng, Z., Liu, Z., Li, N. (2012). Image forensic signature for content authenticity analysis. *Journal of Visual Communication and Image Representation, 23(5),* 782–797. DOI 10.1016/j.jvcir.2012.03.005.
11. Ansari, M. D., Ghrera, S. P., Tyagi, V. (2014). Pixel-based image forgery detection: A review. *IETE Journal of Education, 55(1),* 40–46. DOI 10.1080/09747338.2014.921415.
12. Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications, 36(1),* 25–41. DOI 10.1016/j.jnca.2012.08.007.

13. Qureshi, M. A., Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication, 39,* 46–74.
14. Manjunatha, S., Patil, M. M. (2017). A survey on image forgery detection techniques. *Digital Image Processing, 9(5),* 103–108.
15. Bianchi, T., Piva, A. (2012). Image forgery localization via block-grained analysis of JPEG artifacts. *IEEE Transactions on Information Forensics and Security, 7(3),* 1003–1017. DOI 10.1109/TIFS.2012.2187516.
16. Bianchi, T., Piva, A. (2011). Detection of nonaligned double JPEG compression based on integer periodicity maps. *IEEE Transactions on Information Forensics and Security, 7(2),* 842–848. DOI 10.1109/TIFS.2011.2170836.
17. Milani, S., Tagliasacchi, M., Tubaro, S. (2014). Discriminating multiple JPEG compressions using first digit features. *APSIPA Transactions on Signal and Information Processing, 3(19),* 2253–2256. DOI 10.1109/ICASSP.2012.6288362.
18. Kee, E., Farid, H. (2010). Exposing digital forgeries from 3-D lighting environments. *2010 IEEE International Workshop on Information Forensics and Security*, pp. 1–6. Seattle, USA
19. Bayar, B., Stamm, M. C. (2017). Augmented convolutional feature maps for robust CNN-based camera model identification. *2017 IEEE International Conference on Image Processing*, pp. 4098–4102. Beijing, China.
20. Panzade, P. P., Prakash, C. S., Maheshkar, S. (2016). Copy-move forgery detection by using HSV preprocessing and keypoint extraction. *2016 Fourth International Conference on Parallel, Distributed and Grid Computin*, pp. 264–269. Solan.
21. Lionnie, R., Bahaweres, R. B., Attamimi, S., Alaydrus, M. (2017). A study on pre-processing methods for copy-move forgery detection based on SIFT. *TENCON 2017–2017 IEEE Region 10 Conference*, pp. 1142–1147. Penang.
22. Kuznetsov, A., Myasnikov, V. (2017). A new copy-move forgery detection algorithm using image preprocessing procedure. *Procedia Engineering, 201,* 436–444. DOI 10.1016/j.proeng.2017.09.671.
23. Chakraverti, A. K., Dhir, V. (2017). A new approach of copy move forgery detection using rigorous preprocessing and feature extraction. *International Journal of Computer Sciences and Engineering, 5(12),* 50–56. DOI 10.26438/ijcse.
24. Cao, G., Zhao, Y., Ni, R., Li, X. (2014). Contrast enhancement-based forensics in digital images. *IEEE Transactions on Information Forensics and Security, 9(3),* 515–525. DOI 10.1109/TIFS.2014.2300937.
25. Yuan, H. D. (2013, July). Identification of global histogram equalization by modeling gray-level cumulative distribution. *2013 IEEE China Summit and International Conference on Signal and Information Processing*, pp. 645–649. Beijing, China.
26. Kang, X., Stamm, M. C., Peng, A., Liu, K. R. (2013). Robust median filtering forensics using an autoregressive model. *IEEE Transactions on Information Forensics and Security, 8(9),* 1456–1468. DOI 10.1109/TIFS.2013.2273394.
27. Gao, H., Hu, M., Gao, T., Cheng, R. (2019). Robust detection of median filtering based on combined features of difference image. *Signal Processing: Image Communication, 72,* 126–133.
28. Charpe, J., Bhattacharya, A. (2015). Revealing image forgery through image manipulation detection. *2015 Global Conference on Communication Technologies*, pp. 723–727. Kanya Kumari.
29. Chierchia, G., Poggi, G., Sansone, C., Verdoliva, L. (2014). A Bayesian-MRF approach for PRNU-based image forgery detection. *IEEE Transactions on Information Forensics and Security, 9(4),* 554–567. DOI 10.1109/TIFS.2014.2302078.
30. Chen, Y., Lyu, Z. X., Kang, X., Wang, Z. J. (2018). A rotation-invariant convolutional neural network for image enhancement forensics. *2018 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2111–2115. Calgary.

31. Hiary, H., Zaghloul, R., Al-Adwan, A., Al-Zoubi, M. D. B. (2017). Image contrast enhancement using geometric mean filter. *Signal, Image and Video Processing, 11(5),* 833–840. DOI 10.1007/s11760-016-1029-8.
32. Yadav, G., Maheshwari, S., Agarwal, A. (2014). Contrast limited adaptive histogram equalization based enhancement for real time video system. *2014 International Conference on Advances in Computing, Communications and Informatics*, pp. 2392–2397. Delhi.
33. Stimper, V., Bauer, S., Ernstorfer, R., Schölkopf, B., Xian, R. P. (2019). Multidimensional contrast limited adaptive histogram equalization. *IEEE Access, 7,* 165437–165447. DOI 10.1109/Access.6287639.
34. Laksmi, T. V., Madhu, T., Kavya, K., Basha, S. E. (2016). Novel image enhancement technique using CLAHE and wavelet transforms. *International Journal of Scientific Engineering and Technology, 5(11),* 507–511.
35. Sundaram, M., Ramar, K., Arumugam, N., Prabin, G. (2011). Histogram modified local contrast enhancement for mammogram images. *Applied Soft Computing, 11(8),* 5809–5816. DOI 10.1016/j.asoc.2011.05.003.
36. Kim, S. E., Jeon, J. J., Eom, I. K. (2016). Image contrast enhancement using entropy scaling in wavelet domain. *Signal Processing, 127,* 1–11. DOI 10.1016/j.sigpro.2016.02.016.
37. Mohan, S., Ravishankar, M. (2012). Modified contrast limited adaptive histogram equalization based on local contrast enhancement for mammogram images. *International Conference on Advances in Information Technology and Mobile Communication*, pp. 397–403. Berlin, Heidelberg.
38. Liu, G., Wang, J., Lian, S., Wang, Z. (2011). A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications, 34(5),* 1557–1565. DOI 10.1016/j.jnca.2010.09.001.
39. Ryu, S. J., Lee, M. J., Lee, H. K. (2010). Detection of copy-rotate-move forgery using zernike moments. *International Workshop on Information Hiding*, pp. 51–65. Berlin, Heidelberg.
40. Ryu, S. J., Kirchner, M., Lee, M. J., Lee, H. K. (2013). Rotation invariant localization of duplicated image regions based on zernike moments. *IEEE Transactions on Information Forensics and Security, 8(8),* 1355–1370. DOI 10.1109/TIFS.2013.2272377.
41. Singh, V. K., Tripathi, R. C. (2011). Fast and efficient region duplication detection in digital images using sub-blocking method. *International Journal of Advanced Science and Technology, 35(93)*.
42. Christlein, V., Riess, C., Angelopoulou, E. (2010). On rotation invariance in copy-move forgery detection. *2010 IEEE International Workshop on Information Forensics and Security*, pp. 1–6. Seattle, USA.
43. Bravo-Solorio, S., Nandi, A. K. (2011). Exposing duplicated regions affected by reflection, rotation and scaling. *2011 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1880–1883. Czech Republic.
44. Das, T., Hasan, R., Azam, M. R., Uddin, J. (2018). A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform. *2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering*, pp. 1–4. USA.
45. Park, J. Y., Kang, T. A., Moon, Y. H., Eom, I. K. (2020). Copy-move forgery detection using scale invariant feature and reduced local binary pattern histogram. *Symmetry, 12(4),* 492. DOI 10.3390/sym12040492.
46. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security, 6(3),* 1099–1110. DOI 10.1109/TIFS.2011.2129512.
47. Li, L., Li, S., Zhu, H., Chu, S. C., Roddick, J. F. et al. (2013). An efficient scheme for detecting copy-move forged images by local binary patterns. *Journal of Information Hiding and Multimedia Signal Processing, 4(1),* 46–56.
48. Soni, B., Das, P. K., Thounaojam, D. M. (2017). Copy-move tampering detection based on local binary pattern histogram Fourier feature. *Proceedings of the 7th International Conference on Computer and Communication Technology*, pp. 78–83. Allahabad.

49. Kalsi, D. K., Rai, P. (2017). A copy-move forgery detection system using approximation image local binary pattern. *2017 International Conference on Recent Innovations in Signal Processing and Embedded Systems*, pp. 284–288. Bhopal.
50. Darmet, L., Wang, K., Cayre, F. (2021). Disentangling copy-moved source and target areas. *Applied Soft Computing, 109,* 107536. DOI 10.1016/j.asoc.2021.107536.
51. Zhang, Y., Yu, L., Fang, Z., Xiong, N. N., Zhang, L. et al. (2022). An end-to-end deep learning model for robust smooth filtering identification. *Future Generation Computer Systems, 127,* 263–275. DOI 10.1016/j.future.2021.09.004.
52. Yang, P., Yang, G., Zhang, D. (2016). Rotation invariant local binary pattern for blind detection of copy-move forgery with affine transform. *International Conference on Cloud Computing and Security*, pp. 404–416. San Francisco.
53. Parveen, A., Khan, Z. H., Ahmad, S. N. (2019). Block-based copy–move image forgery detection using DCT. *Iran Journal of Computer Science, 2(2),* 89–99. DOI 10.1007/s42044-019-00029-y.
54. Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G. et al. (2017). Passive detection of image forgery using DCT and local binary pattern. *Signal, Image and Video Processing, 11(1),* 81–88. DOI 10.1007/s11760-016-0899-0.
55. Hayat, K., Qazi, T. (2017). Forgery detection in digital images via discrete wavelet and discrete cosine transforms. *Computers & Electrical Engineering, 62,* 448–458. DOI 10.1016/j.compeleceng.2017.03.013.
56. Jwaid, M. F., Baraskar, T. N. (2017). Detection of copy-move image forgery using local binary pattern with discrete wavelet transform and principle component analysis. *2017 International Conference on Computing, Communication, Control and Automation*, pp. 1–6. Pune.
57. Thajeel, S. A., Mahmood, A. S., Humood, W. R., Sulong, G. (2019). Detection copy-move forgery in image via quaternion polar harmonic transforms. *KSII Transactions on Internet and Information Systems, 13(8),* 4005–4025.
58. Wo, Y., Yang, K., Han, G., Chen, H., Wu, W. (2017). Copy–move forgery detection based on multi-radius PCET. *IET Image Processing, 11(2),* 99–108. DOI 10.1049/iet-ipr.2016.0229.
59. Soni, B., Das, P. K., Thounaojam, D. M. (2017). Blur invariant block based copy-move forgery detection technique using FWHT features. *Proceedings of the International Conference on Watermarking and Image Processing*, pp. 22–26. Paris.
60. Park, C. S., Kim, C., Lee, J., Kwon, G. R. (2016). Rotation and scale invariant upsampled log-polar Fourier descriptor for copy-move forgery detection. *Multimedia Tools and Applications, 75(23),* 16577–16595. DOI 10.1007/s11042-016-3575-z.
61. Hosny, K. M., Hamza, H. M., Lashin, N. A. (2018). Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators. *The Imaging Science Journal, 66(6),* 330–345. DOI 10.1080/13682199.2018.1461345.
62. Emam, M., Han, Q., Niu, X. (2016). PCET based copy-move forgery detection in images under geometric transforms. *Multimedia Tools and Applications, 75(18),* 11513–11527. DOI 10.1007/s11042-015-2872-2.
63. Zhu, Y., Shen, X., Chen, H. (2016). Copy-move forgery detection based on scaled ORB. *Multimedia Tools and Applications, 75(6),* 3221–3233. DOI 10.1007/s11042-014-2431-2.
64. Chihaoui, T., Bourouis, S., Hamrouni, K. (2014). Copy-move image forgery detection based on SIFT descriptors and SVD-matching. *2014 1st International Conference on Advanced Technologies for Signal and Image Processing*, pp. 125–129. Sousse, Tunisia.
65. Dixit, R., Naskar, R., Mishra, S. (2017). Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD. *IET Image Processing, 11(5),* 301–309. DOI 10.1049/iet-ipr.2016.0537.
66. Hilal, A., Hamzeh, T., Chantaf, S. (2017, September). Copy-move forgery detection using principal component analysis and discrete cosine transform. *2017 Sensors Networks Smart and Emerging Technologies,* pp. 1–4. Lebanon.

67. Sunil, K., Jagan, D., Shaktidev, M. (2014). DCT-PCA based method for copy-move forgery detection. *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India*, vol. 2, pp. 577–583. Visakhapatnam, India.
68. Mahmood, T., Nawaz, T., Irtaza, A., Ashraf, R., Shah, M. et al. (2016). Copy-move forgery detection technique for forensic analysis in digital images. *Mathematical Problems in Engineering, 2016,* 1–13. DOI 10.1155/2016/8713202.
69. Wang, C. P., Wang, X. Y., Chen, X. J., Zhang, C. (2017). Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. *Multimedia Tools and Applications, 76(24),* 26355–26376. DOI 10.1007/s11042-016-4130-7.
70. Wang, X. Y., Li, W. Y., Yang, H. Y., Wang, P., Li, Y. W. (2015). Quaternion polar complex exponential transform for invariant color image description. *Applied Mathematics and Computation, 256,* 951–967. DOI 10.1016/j.amc.2015.01.075.
71. Singh, S. P., Urooj, S. (2015). Combined rotation-and scale-invariant texture analysis using radon-based polar complex exponential transform. *Arabian Journal for Science and Engineering, 40(8),* 2309–2322. DOI 10.1007/s13369-015-1645-6.
72. Singh, S. P., Urooj, S., Ekuakille, A. L. (2015). Rotational-invariant texture analysis using radon and polar complex exponential transform. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications*, pp. 325–333. Bhubaneswar, India.
73. Gao, Y., Kang, X., Chen, Y. (2021). A robust video zero-watermarking based on deep convolutional neural network and self-organizing map in polar complex exponential transform domain. *Multimedia Tools and Applications, 80(4),* 6019–6039. DOI 10.1007/s11042-020-09904-4.
74. Yang, H. Y., Qi, S. R., Niu, P. P., Wang, X. Y. (2020). Color image zero-watermarking based on fast quaternion generic polar complex exponential transform. *Signal Processing: Image Communication, 82,* 115747.
75. Yang, F., Li, J., Lu, W., Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence, 59,* 73–83. DOI 10.1016/j.engappai.2016.12.022.
76. Lin, C., Lu, W., Huang, X., Liu, K., Sun, W. et al. (2019). Region duplication detection based on hybrid feature and evaluative clustering. *Multimedia Tools and Applications, 78(15),* 20739–20763. DOI 10.1007/s11042-019-7342-9.
77. Tinnathi, S., Sudhavani, G. (2021). An efficient copy move forgery detection using adaptive watershed segmentation with AGSO and hybrid feature extraction. *Journal of Visual Communication and Image Representation, 74,* 102966. DOI 10.1016/j.jvcir.2020.102966.
78. Sunitha, K., Krishna, A. N. (2020). Efficient keypoint based copy move forgery detection method using hybrid feature extraction. *International Conference on Innovative Mechanisms for Industry Applications*, pp. 670–675. Bangalore, India.
79. Teerakanok, S., Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. *IEEE Access, 7,* 40550–40568. DOI 10.1109/Access.6287639.
80. Dixit, R., Naskar, R. (2017). Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images. *IET Image Processing, 11(9),* 746–759. DOI 10.1049/iet-ipr.2016.0322.
81. Abd Warif, N. B., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R. et al. (2016). Copy-move forgery detection: Survey, challenges and future directions. *Journal of Network and Computer Applications, 75,* 259–278. DOI 10.1016/j.jnca.2016.09.008.
82. Zhang, Z., Wang, C., Zhou, X. (2018). A survey on passive image copy-move forgery detection. *Journal of Information Processing Systems, 14(1),* 6–31.
83. Mushtaq, S., Mir, A. H. (2018). Image copy move forgery detection: A review. *International Journal of Future Generation Communication and Networking, 11(2),* 11–22. DOI 10.14257/ijfgcn.
84. Cozzolino, D., Poggi, G., Verdoliva, L. (2014). Copy-move forgery detection based on patchmatch. *2014 IEEE International Conference on Image Processing*, pp. 5312–5316. Paris.

85. Bi, X., Pun, C. M., Yuan, X. C. (2016). Multi-level dense descriptor and hierarchical feature matching for copy–move forgery detection. *Information Sciences, 345,* 226–242. DOI 10.1016/j.ins.2016.01.061.
86. Wang, X. Y., Li, S., Liu, Y. N., Niu, Y., Yang, H. Y. et al. (2017). A new keypoint-based copy-move forgery detection for small smooth regions. *Multimedia Tools and Applications, 76(22),* 23353–23382. DOI 10.1007/s11042-016-4140-5.
87. Bi, X., Pun, C. M., Yuan, X. C. (2018). Multi-scale feature extraction and adaptive matching for copy-move forgery detection. *Multimedia Tools and Applications, 77(1),* 363–385. DOI 10.1007/s11042-016-4276-3.
88. Li, Y., Zhou, J. (2018). Fast and effective image copy-move forgery detection via hierarchical feature point matching. *IEEE Transactions on Information Forensics and Security, 14(5),* 1307–1322. DOI 10.1109/TIFS.2018.2876837.
89. Wang, X. Y., Jiao, L. X., Wang, X. B., Yang, H. Y., Niu, P. P. (2019). Copy-move forgery detection based on compact color content descriptor and delaunay triangle matching. *Multimedia Tools and Applications, 78(2),* 2311–2344. DOI 10.1007/s11042-018-6354-1.
90. Yang, H. Y., Niu, Y., Jiao, L. X., Liu, Y. N., Wang, X. Y. et al. (2018). Robust copy-move forgery detection based on multi-granularity superpixels matching. *Multimedia Tools and Applications, 77(11),* 13615–13641. DOI 10.1007/s11042-017-4978-1.
91. Liu, K., Lu, W., Lin, C., Huang, X., Liu, X. et al. (2019). Copy move forgery detection based on keypoint and patch match. *Multimedia Tools and Applications, 78(22),* 31387–31413. DOI 10.1007/s11042-019-07930-5.
92. Elhaminia, B., Harati, A., Taherinia, A. (2019). A probabilistic framework for copy-move forgery detection based on markov random field. *Multimedia Tools and Applications, 78(18),* 25591–25609. DOI 10.1007/s11042-019-7713-2.
93. Cozzolino, D., Poggi, G., Verdoliva, L. (2015). Efficient dense-field copy–move forgery detection. *IEEE Transactions on Information Forensics and Security, 10(11),* 2284–2297. DOI 10.1109/TIFS.2015.2455334.
94. Ouyang, J., Liu, Y., Liao, M. (2017). Copy-move forgery detection based on deep learning. *2017 10th International Congress on Image and Signal Processing, Biomedical Engineering and Informatics*, pp. 1–5. Shanghai, China.
95. Liu, Y., Guan, Q., Zhao, X. (2018). Copy-move forgery detection based on convolutional kernel network. *Multimedia Tools and Applications, 77(14),* 18269–18293. DOI 10.1007/s11042-017-5374-6.
96. Thakur, R., Rohilla, R. (2019). Copy-move forgery detection using residuals and convolutional neural network framework: A novel approach. *2019 2nd International Conference on Power Energy, Environment and Intelligent Control*, pp. 561–564. Greater Noida.
97. Agarwal, R., Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. *Multimedia Tools and Applications, 79(11),* 7355–7376. DOI 10.1007/s11042-019-08495-z.
98. Yang, H. Y., Qi, S. R., Niu, Y., Niu, P. P., Wang, X. Y. (2019). Copy-move forgery detection based on adaptive keypoints extraction and matching. *Multimedia Tools and Applications, 78(24),* 34585–34612. DOI 10.1007/s11042-019-08169-w.
99. Kao, H. H., Wen, C. Y. (2020). An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. *Applied Sciences, 10(11),* 3716. DOI 10.3390/app10113716.
100. Feng, G. R., Wu, J. (2020). Image forgery detection based on the convolutional neural network. *Proceedings of the 2020 12th International Conference on Machine Learning and Computing*, pp. 266–270. New York.
101. Agarwal, R., Verma, O. P., Saini, A., Shaw, A., Patel, R. (2021). The advent of deep learning-based image forgery detection techniques. In: *Innovative data communication technologies and application*, pp. 679–693. Singapore: Springer.
102. Zhong, J. L., Pun, C. M. (2019). An end-to-end dense-inceptionnet for image copy-move forgery detection. *IEEE Transactions on Information Forensics and Security, 15,* 2134–2146. DOI 10.1109/TIFS.10206.

103. Pun, C. M., Chung, J. L. (2018). A two-stage localization for copy-move forgery detection. *Information Sciences, 463,* 33–55. DOI 10.1016/j.ins.2018.06.040.
104. 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. *Journal of Visual Communication and Image Representation, 29,* 16–32. DOI 10.1016/j.jvcir.2015.01.016.
105. Pun, C. M., Yuan, X. C., Bi, X. L. (2015). Image forgery detection using adaptive oversegmentation and feature point matching. *IEEE Transactions on Information Forensics and Security, 10(8),* 1705–1716. DOI 10.1109/TIFS.2015.2423261.
106. Li, J., Li, X., Yang, B., Sun, X. (2014). Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security, 10(3),* 507–518.
107. Bi, X., Pun, C. M. (2017). Fast reflective offset-guided searching method for copy-move forgery detection. *Information Sciences, 418,* 531–545. DOI 10.1016/j.ins.2017.08.044.
108. Bi, X., Pun, C. M. (2018). Fast copy-move forgery detection using local bidirectional coherency error refinement. *Pattern Recognition, 81,* 161–175. DOI 10.1016/j.patcog.2018.03.028.
109. Rao, Y., Ni, J. (2016). A deep learning approach to detection of splicing and copy-move forgeries in images. *2016 IEEE International Workshop on Information Forensics and Security*, pp. 1–6. France.
110. Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). Image copy-move forgery detection via an end-to-end deep neural network. *2018 IEEE Winter Conference on Applications of Computer Vision*, pp. 1907–1915. Lake Tahoe, NV, USA.
111. Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. *Proceedings of the European Conference on Computer Vision*, pp. 168–184. Munich, Germany.
112. Bunk, J., Bappy, J. H., Mohammed, T. M., Nataraj, L., Flenner, A. et al. (2017). Detection and localization of image forgeries using resampling features and deep learning.*IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1881–1889. Honolulu, HI, USA.
113. Qiao, T., Zhu, A., Retraint, F. (2018). Exposing image resampling forgery by using linear parametric model. *Multimedia Tools and Applications, 77(2),* 1501–1523. DOI 10.1007/s11042-016-4314-1.
114. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L. et al. (2013). Copy-move forgery detection and localization by means of robust clustering with J-linkage. *Signal Processing: Image Communication, 28(6),* 659–669.
115. Bayar, B., Stamm, M. C. (2018). Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection. *IEEE Transactions on Information Forensics and Security, 13(11),* 2691–2706. DOI 10.1109/TIFS.2018.2825953.
116. Bondi, L., Lameri, S., Guera, D., Bestagini, P., Delp, E. J. et al. (2017). Tampering detection and localization through clustering of camera-based CNN features. *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1881–1889. Honolulu, HI, USA.
117. Zhang, Z., Zhang, Y., Zhou, Z., Luo, J. (2018). Boundary-based image forgery detection by fast shallow cnn. *2018 24th International Conference on Pattern Recognition*, pp. 2658–2663. Beijing, China.
118. Marra, F., Gragnaniello, D., Verdoliva, L., Poggi, G. (2020). A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection. *IEEE Access, 8,* 133488–133502. DOI 10.1109/Access.6287639.
119. Kohli, A., Gupta, A., Singhal, D. (2020). CNN based localisation of forged region in object-based forgery for HD videos. *IET Image Process, 14(5),* 947–958. DOI 10.1049/iet-ipr.2019.0397.
120. Kuznetsov, A. (2019). Digital image forgery detection using deep learning approach. *Journal of Physics: Conference Series, 1368(3),* 032028. DOI 10.1088/1742-6596/1368/3/032028.
121. Zhu, Q., Zhang, P., Wang, Z., Ye, X. (2019). A new loss function for CNN classifier based on predefined evenly-distributed class centroids. *IEEE Access, 8,* 10888–10895. DOI 10.1109/Access.6287639.

122. Mai, X., Zhang, H., Jia, X., Meng, M. Q. H. (2020). Faster R-CNN with classifier fusion for automatic detection of small fruits. *IEEE Transactions on Automation Science and Engineering, 17(3),* 1555–1569. DOI 10.1109/TASE.8856.

123. Elleuch, M., Tagougui, N., Kherallah, M. (2016). A novel architecture of CNN based on SVM classifier for recognising arabic handwritten script. *International Journal of Intelligent Systems Technologies and Applications, 15(4),* 323–340. DOI 10.1504/IJISTA.2016.080103.

124. Bammey, Q., Gioi, R. G. V., Morel, J. M. (2020). An adaptive neural network for unsupervised mosaic consistency analysis in image forensics.*IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 14194–14204. Seattle, WA, USA.

125. Wu, Y., AbdAlmageed, W., Natarajan, P. (2019). Mantra-Net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 9543–9552. Long Beach, CA, USA.

126. Hu, X., Zhang, Z., Jiang, Z., Chaudhuri, S., Yang, Z. et al. (2020). SPAN: Spatial pyramid attention network for image manipulation localization. *European Conference on Computer Vision*, pp. 312–328. Glasgow, UK.

127. Li, L., Bao, J., Zhang, T., Yang, H., Chen, D. et al. (2020). Face x-ray for more general face forgery detection. *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 5001–5010. Seattle, WA, USA.

128. Li, J., Xie, H., Li, J., Wang, Z., Zhang, Y. (2021). Frequency-aware discriminative feature learning supervised by single-center loss for face forgery detection.*IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 6458–6467. Nashville, USA.

129. Haliassos, A., Vougioukas, K., Petridis, S., Pantic, M. (2021). Lips don't lie: A generalisable and robust approach to face forgery detection. *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 5039–5049. Nashville, TN, USA.

130. Shang, Z., Xie, H., Zha, Z., Yu, L., Li, Y. et al. (2021). PRRNet: Pixel-region relation network for face forgery detection. *Pattern Recognition, 116,* 107950. DOI 10.1016/j.patcog.2021.107950.

131. Hu, Z., Xie, H., Wang, Y., Li, J., Wang, Z. et al. (2021). Dynamic inconsistency-aware deepfake video detection. *International Joint Conferences on Artificial Intelligence*, Montreal, Canada. DOI 10.24963/ijcai.2021/102.

132. Elharrouss, O., Almaadeed, N., Al-Maadeed, S., Akbari, Y. (2020). Image inpainting: A review. *Neural Processing Letters, 51(2),* 2007–2028. DOI 10.1007/s11063-019-10163-0.

133. Rezki, A. M., Serir, A., Beghdadi, A. (2022). Blind image inpainting quality assessment using local features continuity. *Multimedia Tools and Applications, 81(7),* 9225–9244. DOI 10.1007/s11042-021-11872-2.

134. Zhu, X., Qian, Y., Zhao, X., Sun, B., Sun, Y. (2018). A deep learning approach to patch-based image inpainting forensics. *Signal Processing: Image Communication, 67,* 90–99.

135. Zhang, Y., Ding, F., Kwong, S., Zhu, G. (2021). Feature pyramid network for diffusion-based image inpainting detection. *Information Sciences, 572,* 29–42. DOI 10.1016/j.ins.2021.04.042.

136. Hu, Z., Xie, H., Yu, L., Gao, X., Shang, Z. et al. (2022). Dynamic-aware federated learning for face forgery video detection. *ACM Transactions on Intelligent Systems and Technology, 13(4),* 1–25. DOI 10.1145/3501814.

137. Qian, Y., Yin, G., Sheng, L., Chen, Z., Shao, J. (2020). Thinking in frequency: Face forgery detection by mining frequency-aware clues. *European Conference on Computer Vision*, pp. 86–103. Glasgow, UK.

138. Li, J., Xie, H., Yu, L., Gao, X., Zhang, Y. (2021). Discriminative feature mining based on frequency information and metric learning for face forgery detection. *IEEE Transactions on Knowledge and Data Engineering, 14(8),* 1–14.

139. Krishnaraj, N., Sivakumar, B., Kuppusamy, R., Teekaraman, Y., Thelkar, A. R. (2022). Design of automated deep learning-based fusion model for copy-move image forgery detection. *Computational Intelligence and Neuroscience, 2022,* 1–14, 8501738. DOI 10.1155/2022/8501738.

140. Ali, S. S., Ganapathi, I. I., Vu, N. S., Ali, S. D., Saxena, N. et al. (2022). Image forgery detection using deep learning by recompressing images. *Electronics, 11(3),* 403. DOI 10.3390/electronics11030403.

141. Koul, S., Kumar, M., Khurana, S. S., Mushtaq, F., Kumar, K. (2022). An efficient approach for copy-move image forgery detection using convolution neural network. *Multimedia Tools and Applications, 81,* 11259–11277. DOI 10.1007/s11042-022-11974-5.

142. Qazi, E. U. H., Zia, T., Almorjan, A. (2022). Deep learning-based digital image forgery detection system. *Applied Sciences, 12(6),* 2851. DOI 10.3390/app12062851.