IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier

Image Forgery Detection Techniques: Latest Trends And Key Challenges

POULOMI DEB[1], SUBHRAJYOTI DEB[2], ABHIJIT DAS[3] AND NIRMALYA KAR[1]
[1]Department of Computer Science and Engineering, National Institute of Technology, Agartala
[2]Department of Computer Science and Engineering, ICFAI University, Tripura
[3]Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India

Corresponding author: Abhijit Das (e-mail: abhijit.das@manipal.edu)

ABSTRACT The improvement and accessibility of high-resolution cameras have significantly increased image capturing by various media. Different editing tools are available that are frequently used to improve image quality, resulting in the alteration of images. So, determining the authenticity or integrity of the original image is a challenging task in any domain. Currently, an image or video is a critical source of legal data for digital forensics. Hence, the study begins with the primary objective of determining whether the digital evidence (image or video) associated with a legal case has been altered. Active forgery detection methods, such as digital watermarking and digital signatures, and passive forgery detection techniques, including copy-move, splicing, and retouching, are used to verify digital evidence. Recently, neural network (NN) based forgery detection has garnered notable attention due to its efficacy in detecting forgery on images. In order to assess the benefits and drawbacks of those models, this work starts by looking at different categories of forgery detection and how those classifications are implemented. We summarised and compared the different architectures that researchers had suggested, taking into account their respective specialised viewpoints, and then we analysed them according to quality. Most used methodologies in forgery detection are elaborated by mentioning the advantages and disadvantages of each technique. Additionally, the work examines the deployment of neural networks and machine learning (ML) techniques within forensic science to detect image forgery. We also underlined the present challenges and potential research directions that might help researchers fill the knowledge gaps.

INDEX TERMS Active Forgery; Passive Forgery; Digital Watermark; Digital Signature; Neural Network; Machine learning; Copy-move forgery (CMF).

I. INTRODUCTION

IN today's lifestyle, capturing an image and creating video content is very common because of the easy availability of various devices having inbuilt cameras like smartphones, tabs, laptops, etc. Sharing those images and videos on social media is also common. Most of the time to make those images lucrative and transparent, original images are forged using various editing tools or software like adobe photoshop, photo editor, etc. [1]. An image goes through many steps, from being captured initially to becoming forged. Identifying those forged images is a challenging task. An example of manipulation of a digitally captured image is depicted in Fig. 1, which was posted on a website where it seemed to be 4 (four) missiles. In contrast, three missiles were launched initially [2].

FIGURE 1: An example of CMF [2]

Digital image forgery detection is a topic of research that enables identifying the forged image, primarily concentrating on the origin of the actual image and its properties. Digital images and videos are vital legal data in digital forensics. The image's authenticity is always a question mark due to the computational advances that can quickly manipulate authentic images. When some parts of any image are intentionally modified with malicious intent, that manipulated image is identified as a case of image forgery. The practice

of manipulated image creation has increased daily in social media networks, leading to offering fake news. Due to these issues, researchers and scientists are motivated to focus on digital image forensics as well as detecting forgery.

Since the early 2000s, numerous methods and surveys have been created to identify image forgeries. Different methodologies are used to detect image forgery, and several references are explained in the upcoming section of this paper. Forgery detection based on image is often labeled into two types, namely active and passive forgery. The active forgery detection method relies on the idea of hiding data by inserting a small amount of code into an image at the time of image acquisition. Active forgery methods are watermarking and digital signature. Digital watermarking involves embedding a symbol to ensure owner authenticity in the image. Digital watermarking may not be available on all digital cameras, posing challenges for image authenticity. It is the major disadvantage of watermarking technique for digital images [54]. A digital signature is an encrypted authentication method that uses a hash function algorithm to authenticate digital information like images and electronic documents.

In contrast, the passive method analyses an image based on its statistics and semantics to determine whether any alteration has been done without considering any hidden information in an image. Copy-move, image splicing, and retouching are the categories of passive forgery detection methods [55]. Over the past decade, CMF has grown in popularity as an image manipulation technique. CMFD algorithms are subdivided into 8 categories DCT, LPT (Log-Polar transform) and others [56]. Ansari et al. [19] researched various methods for detecting pixel-based image forgery. Singh and Kaur [57] discussed about different subcategories of block-based CMF detection techniques. Zhang et al. [58] examined two CMFD technique frameworks in addition to the CMF mathematical model.

Most of the above research concentrated on traditional methods. On the other hand, recent developments in the domains of computer vision and digital image processing have demonstrated the revolutionary potential of deep learning (DL) techniques. They yield better results, particularly in the presence of a large training dataset. Furthermore, most surveys lacked information such as summaries of current and advanced approaches of DL, traditional approaches, and accessible datasets with their pros and cons, all in one location. We made an effort to compile all the CMFD related information in one location so that researchers could refer to this paper without requiring to study numerous papers.

Our main contribution in this paper addresses several key objectives in the investigation of image forgery detection. The work presents an exhaustive analysis of the currently used methods, with the techniques being divided into two categories: active and passive. A comparison analysis that takes into account the datasets frequently used in forgery detection research evaluates the advantages and disadvantages of both categories. The paper also investigates novel methodologies that capitalise on neural networks and machine learning models to improve detection accuracy. The performance metrics used to evaluate Copy-Move Forgery Detection (CMFD) schemes, both at the pixel and image levels, are thoroughly examined. The study also covers the challenges that are currently being faced in the field and makes suggestions for future approaches that may be taken to achieve better results in detecting image forgery.

A. PAPER ORGANIZATION

The structure of the organized paper is shown in Fig. 2.

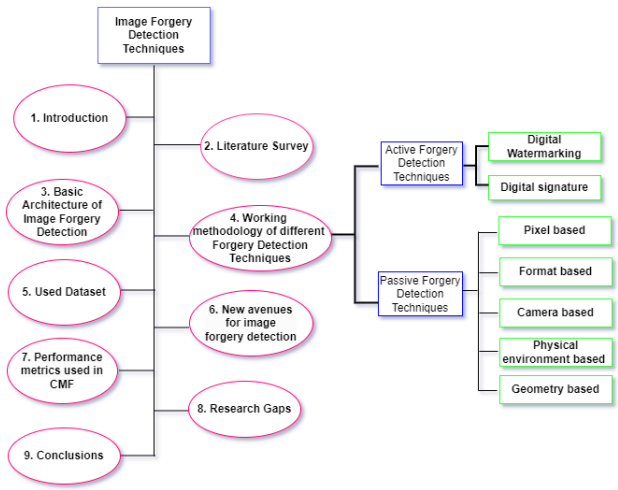

FIGURE 2: Roadmap for this survey paper

II. LITERATURE SURVEY

Based on the extensive literature survey, the initial classification of active and passive forgery detection is further subdivided into several parts based on the techniques deployed to detect any kind of manipulation. The detailed classification of different methods of image forgery detection is categorized in Fig. 3. We have mainly focused on the active part of the forgery detection technique in the present study.

For better understanding, a detailed analysis of the works is presented in the subsequent section.

A. ACCEPTANCE AND REJECTION CRITERIA TO GATHER RELEVANT DATA

To gather relevant studies for our systematic review, a variety of inclusion and exclusion criteria was considered, which is shown in Fig. 4. The selection criteria for selecting the articles for the present study were as follows:

- Papers must be composed in English.
- Contents must be relevance to the area of interest.
- Articles related to research questions and studies that only focus on image forgery detection.
- Other factors such as timeline, availability, impact, and quality of the paper are also considered.

Similarly, the exclusion criteria for articles were as follows:

- Remove duplicate articles identified via various databases.

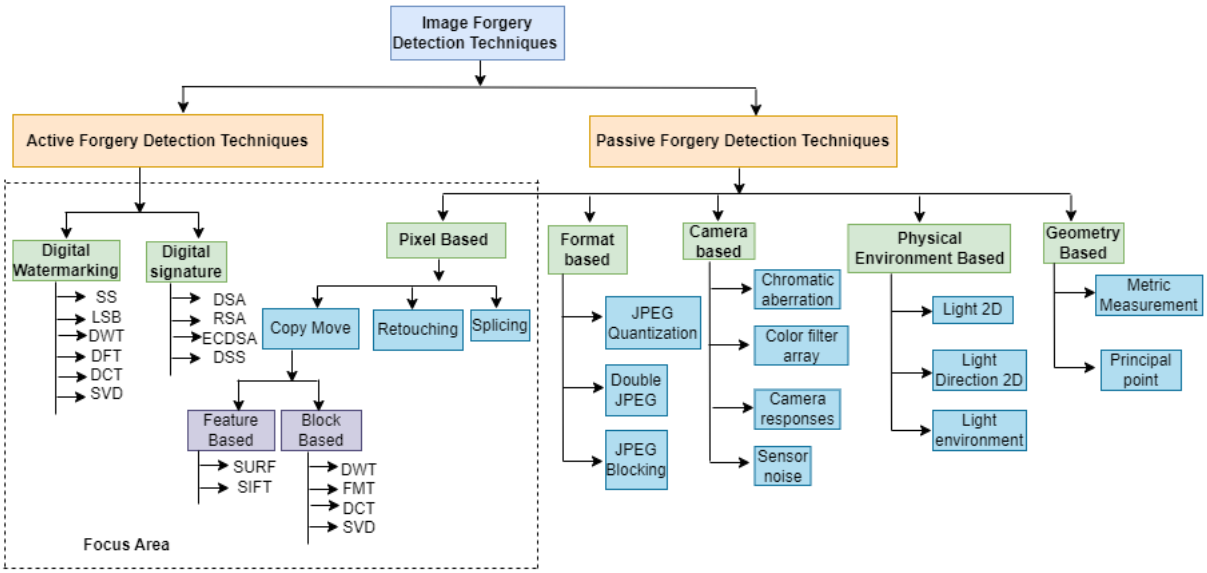

FIGURE 3: Categorization of different forgery techniques

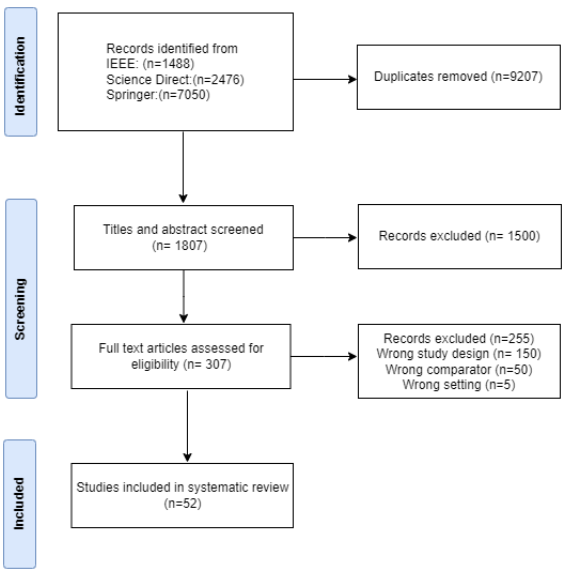

FIGURE 4: PRISMA classification for study selection process

- Irrelevant studies and paper is written in other languages.

III. BASIC ARCHITECTURE OF IMAGE FORGERY DETECTION

Generally, modification of an image can be labeled into multiple segments depending on the working principle.To Identify forgery in any image is always a binary response, i.e. yes or no response to the question that the given input image is real or altered [3] irrespective of the percentage of changes. A hierarchical structure of image forgery detection techniques used in forensic field and goal of these techniques has been shown in Fig. 5 for better understanding.

Input Image: In the initial step that concerns either the input image using digital or analog conversion, camera lens, color filter array (CFA), or not [4]. These are the important steps to detect any kind of manipulation or alteration has been done in an image.

Conversion of grayscale: In order to simplify the calculation, the input image is first acquired and then transformed into a grayscale.

Keypoint-based and block-based division: In this step, complexity is minimized on the grey scale image using keypoint and block-based algorithms.

Feature extraction: This step extracts all the features or characteristics from the image to detect forgery. Several techniques are used for feature extraction, such as diagonal-based features, chain code histogram, principal component analysis (PCA), Fourier descriptor, etc.

Feature sorting: This step includes storing extracted features in a matrix and all the matched blocks to be clustered later. Several algorithms are used to accomplish the feature of sorting.

Feature matching: It is used to determine identical blocks in an image using clustering, K-nearest neighbour (KNN), Euclidean distance, etc.

Forgery detection results: Various techniques such as robust clustering using J-linkage, convolutional neural network (CNN), DCT coefficient analysis, etc. and forgery detection have been identified.

IV. WORKING METHODOLOGY OF DIFFERENT FORGERY DETECTION TECHNIQUES

A. ACTIVE FORGERY DETECTION TECHNIQUES

This technique works on pre extracted and pre embedded confidential information in a digital image. The most popular method of active forgery techniques [5] are digital signature

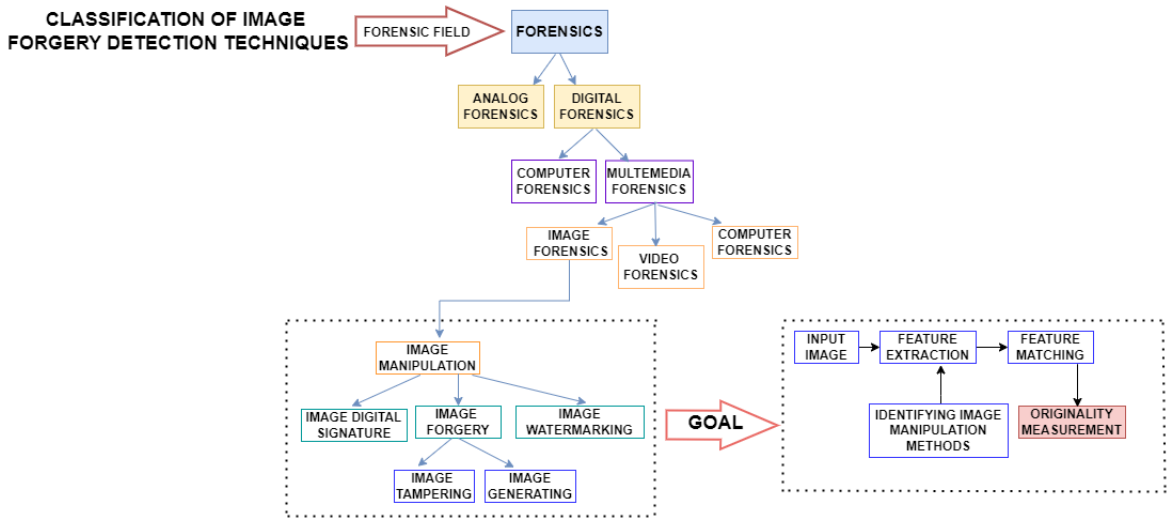

FIGURE 5: Hierarchical structure of image forgery detection techniques and its goal

and digital watermarking. Classification of forgery of a digital image under active detection technique: Firstly, the image is embedded using some authenticating information that can be further reverified with some authenticating technique to detect active forgery approach [6]. Table 1 shows the different classifications of forgery in digital images under active detection techniques.

1) Digital Watermarking

In this process, a symbol is used for owner authenticity, which is embedded in the image or video data. If any kind of alteration or modification is done in the data, the watermark gets destroyed, thus indicating data tampering. Watermarks are generally used for the protection of copyright as well as data rights. Urvoy et al. [7] described that watermarking technique concerns four crucial requirements i.e. security, capacity, robustness and invisibility. The watermarking method depends on both the spatial domain and the frequency domain, as shown in Fig. 6.

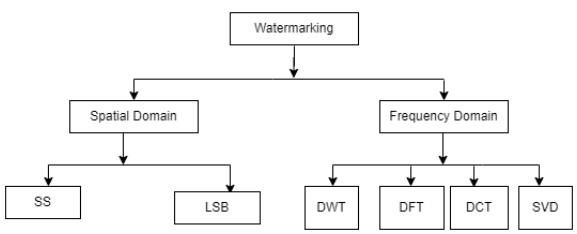

FIGURE 6: Watermarking techniques

Watermarking is done using Spread Spectrum (SS) as well as Least Significant Bit (LSB); both are based on the spatial domain. Two advantages of SS image watermarking are high imperceptibility and better watermark detection performance. There are two different kinds of SS embedding schemes: additive SS and multiplicative SS. In additive SS, watermark information spreads evenly with a fixed embedding strength; in multiplicative SS, watermark information spreads adaptively.

To support the generic framework for copyright protection, Bose and Maity [8] suggested a model based on SS to identify watermarks on the degraded compressed image in the presence of both multiplicative and additive impairments. An initial log-likelihood ratio model watermark detection threshold calculation is performed first. Then, under the restriction of detector reliability, the distortion minimization problem is expressed based on SS measurement calculation and the watermark embedding performance.

Bamatraf et al. [9] proposed an LSB method that involved flipping the watermark text's value in binary and shifting it to correspond to the image's odd as well as even number pixel value before inserting the watermark. The suggested algorithm can be modified depending on the watermark length. If the watermark text exceeds ((MxN)/8)-2 in length, the additional watermark text is inserted in the second LSB. This technique yields superior results after attacking the watermarked image with cropping and noise addition using LSB and inverse bit combinations. The new technique was tested for better results and then put up against traditional LSB using peak signal-to-noise ratio (PSNR) in the frequency domain. Based on the frequency domain, discrete Fourier transform (DFT), discrete wavelet transform (DWT), DCT and singular value decomposition (SVD) are the four techniques that the watermarking uses to operate. To identify the existence of watermarking in any digital image, Urvoy et al. [7] suggested a novel detection method involving perceptually-optimal visibility versus robustness. High levels of robustness to different attacks are displayed by this method. In the Fourier domain, a noise-like square patch of coefficients is inserted by replacement; the amplitude component adjusts the watermark's strength, and the phase component stores the image's watermark data. Makbol et al. [10] suggested block-based watermarking using SVD and the human visual system

TABLE 1: Classification of active detection technique

Sl.No.	Types	Description
1	Digital Watermarking [7]–[13]	Watermarks are generally used for protection of copyright as well as data rights
2	Digital signature [14]–[17]	Digital signature ensures the authenticity and integrity of the message using cryptography

in DWT. This method is block-based, as entropy and edge entropy are used as essential characteristics for choosing significant blocks inserted on the watermark. A. Kumar et al. [11] implement a modified buyer-seller watermarking protocol based on wavelets using DWT to manage the watermark in an image. A binary watermarked logo that has been embedded in a particular chosen sub-bands of a 3-level DWT that changed the original image. After that, a DWT sub-band is calculated, and the watermark bits sequences are embedded in the coefficients of the high-frequency sub-bands. The robustness of the watermarked image is assessed using PSNR and NCC metrics. Whereas Radhika Totla [12] presented a comparison study that used DCT and DWT to analyse watermarking. Ernawan and Kabir [13] proposed a watermark framework using an optimal DCT psycho-visual threshold for copyright protection. This method uses specific DCT frequency ranges where introducing watermark bits results in the least degree of image distortion. Table 2 shows some important information related to watermarking.

2) Digital signature

The generic implementation procedure of the Digital signature [14] is stated through following steps:

- The sender signs the image on one end, and the receiver validates the same on the other end.
- Unauthorized users are unable to falsify the signature.
- Digital signature provides integrity and gains non-reputation.
- Then the message is sent along with a digital signature.

A digital signature is an encrypted form of authentication stamp used to authenticate digital information such as images, electronic documents, etc. done by generating a hash function algorithm. Suppose there is any kind of alteration or modification in the image data, in that case, the hash function gets altered, indicating that the image has been manipulated, meaning image forgery. The digital signature ensures the authenticity and integrity of the message using cryptography. Several cryptosystem-based algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA), Rivet, Shamir, and Adleman (RSA), Digital Signature Algorithm (DSA) for digital signature are already proposed. Digital signature algorithms can be used for authentication by directly applying them to the message or by applying a hash value to generate a tag that can be used to ensure the message's authenticity. Xuan et al. [15] do research comparing various digital signature algorithms, including DSA, ECDSA and RSA, which are implemented using Java ME on mobile device emulators. Based on experimental comparative results, RSA is more appropriate for verifying the signature on mobile devices, whereas ECDSA is more practical for generating the signature. Zhang et al. [16] a novel digital signature scheme has been proposed by enhancing the original digital signature algorithm by implementing an elliptic curve cryptosystem. According to simulation results, this technique offers greater security than the original digital signature algorithm.

Digital signature systems (DSS) use public key cryptography techniques to produce digital signatures. Campbell [17] reviews supporting digital signatures with integrity and non-repudiation characteristics in mobile environments, where all methods and risks involved in producing digital signatures on workstations are examined. Table 3 shows some important information related to digital signatures.

B. PASSIVE FORGERY DETECTION TECHNIQUES

This technique works in image analysis based on its statistics and semantics to check whether any modification has been done without considering any hidden information in an image [18]. The most popular method of passive forgery techniques are ones based on pixels, formats, geometric, camera, physical evidence etc.

In the passive detection technique, [19], [20] forgery of an image can be detected based on the entire context that has been manipulated or if there is a particular modification in a few characteristics of the digital image. This approach is based on the principle of image analysis, mainly focusing on semantics and statistics to identify whether any manipulation has been done or any hidden information embedded in the image are not considered. Table 4 shows the different classifications of digital image forgery under the passive detection technique.

C. PIXEL-BASED FORGERY DETECTION

Determining any arithmetic modifications in pixels on an image is the primary concern of pixel-based techniques [19]. Any manipulation (if exists) in the form of statistical variations at the pixel level of the images are detected by using this technique. Table 5 shows the different classifications of pixel-based forgery detection under the passive detection technique. Further classification of these techniques is described below.

1) Copy-move forgery detection

Concerning digital image forgeries, the most popular one is copy-move technique [20]. Duplicating a portion of an image and subsequently pasting it in a different location within the same image falls under this manipulation category, as shown in Fig. 7. CMF is one of the simplest and most used ways to change images. Objective of CMF is to hide multiple

TABLE 2: Works related to Watermarking

Sl.No.	Technique	Description	Pros	Cons	Dataset Used
1	SS [8]	To identify watermarks present on diminished compressed images in the presence of both multiplicative and additive impairments, a model based on Spread Spectrum (SS) is proposed, offering a generic framework for copyright protection	Provides robustness against a broad range of common and deliberate signal processing operations, including geometric operations	Not suitable for copyright protection	A set of real images e.g. "Lena", "Cameraman", "Boat", "Mandrill", etc.
2	LSB [9]	presented an LSB approach that involved flipping the watermark text's binary values and shifting it to correspond to the image's pixel coordinates i.e. odd or even number, before inserting the watermark	The watermark's image quality is good after applying different attacks (cropping, adding noise)	Complex implementation	Dock, Forest, Waterfall, Toco Toucan
3	DFT [7]	A novel detection method involving perceptually optimal visibility versus robustness is suggested using DFT determining the presence of watermark in any digital image	Template matching is highly effective in identifying watermarks even when there are minor geometric variations, and it is also robust against printing and scanning. Moreover, it has shown superior performance in watermark detection.	The approach is not resilient to images that have extremely low quality scans	Baboon , Barbara, Boats, Fruits, Lena, Monarch and Peppers
4	SVD [10]	The use of SVD and the human visual system in DWT to implement a block-based watermarking methodology is proposed. This technique employs entropy and edge entropy to select important blocks for inserting the watermark	The scheme is highly secured	In certain geometrical attacks, the robustness's efficiency is reduced.	lena and pepper
5	DWT [11]	A modified buyer-seller watermarking protocol based on wavelets and using DWT to manage image watermarks has been proposed. The technique's resilience is assessed by measuring the PSNR and Normalized Correlation Coefficient (NCC) parameters	The technique is robust to a variety of attacks, including those using JPEG Rotation, Gaussian Noise, Compression, Median Filter, and Salt and Pepper Noise	Having security issue, as this protocol is depending upon the embedding and extraction of watermark	Lena , Cameramen, Baboon and House
6	DCT [13]	This approach presents a watermarking framework for copyright protection that employs an optimal DCT psychovisual threshold. The technique selects specific frequency regions of the DCT where the insertion of watermark bits results in minimal image distortion	Despite facing multiple attacks like image noise, lowpass filters, sharpening, median filters, JPEG, JPEG2000, and others, the watermark extraction process produces images of superior quality	Performance on resisting rotational attacks is unsatisfactory	Lena Image.

TABLE 3: Works related to Digital Signature

Sl.No.	Technique	Description	Pros	Cons
1	DSA, RSA and ECDSA [15]	Based on experimental comparisons of digital signature algorithms such as DSA, RSA, and ECDSA, it has been found that ECDSA is better suited for generating signatures while RSA is better suited for verifying signatures on mobile devices	In the context of mobile information systems, it is recommended to use 1024-bit RSA and 160-bit ECDSA for generating keys and signatures on the device to enable signature authentication	Research on digital signatures has been conducted less frequently
2	ECDSA [16]	By enhancing the original digital signature method with the help of an elliptic curve cryptosystem, a new digital signature scheme is proposed, provides better security	Algorithm is highly secured with less computation processing speed	Theoretical analysis only
3	DSS [17]	A review for supporting digital signatures having the characteristics of integrity and non-repudiation in mobile environments has been examined	Several techniques and concerns related to creating digital signatures on workstations, are investigated	The user's private key's security is not assured

TABLE 4: Classification of passive detection technique

Sl.No.	Terminology	Defination
1	Pixel based [21]–[33]	Any arithmetic modifications in pixels on an image are determined by pixel-based technique
2	Format based [34]–[36]	Format-based techniques deal with image formats, especially in the JPEG format.
3	Camera based [37]–[41]	This technique is based on the principle of detection of camera artefacts.
4	Physical environment based [42]	Identifying the forged region of the image using different types of lighting inconsistencies, shadows, reflection etc. is termed as physical environment-based forgery detection
5	Geometry based [21], [43], [44]	A precise geometric measurement and accurate position of any object in the world associated to the camera is known as geometric based forgery.

TABLE 5: Classification of pixel-based forgery detection technique

Sl.No	Terminology	Defination
1	CMFD [20]	The image is replicated in part, and the copied component is then pasted onto the original image in a different location
2	Retouching [21]	Retouching is the process of changing an image's visual characteristics such as color, sharpness, or other properties of the image
3	Splicing [22]	Splicing is another type of forgery detection, where multiple fragmented data are taken from numerous images and then merged into one image and the output image becomes indistinguishable

FIGURE 7: CMFD process

parts of the image, which renders the image's authenticity irrelevant. There are two methods to determine if a copy-move has occurred in an image: feature-based and block-based as shown in Fig. 8.

Local features such as corners, blobs, and edges are extracted from the tampered images using feature-based approaches. To detect copy-move attacks, the most commonly utilised key point features in CMFD are the scale-invariant feature transform (SIFT) and speeded-up robust features (SURF). Table 6 shows some important information related to CMFD.

The calculation of SIFT involves several aspects, including localising key points, detecting scale-space extrema, deter-

TABLE 6: Works related to CMFD

Technique	Description	Pros	Cons	Dataset Used
SIFT [23]	Digital images can be used to identify CMF using an efficient method that involves extracting SIFT descriptors from the image and comparing them with each other by computing Euclidean distance between the extracted descriptor vectors	Well performed against JPEG compression, rotation, noise, scaling,etc.	Less performance for detecting small size tampered region	Images collected from the internet.
SIFT [24]	Keypoint extraction algorithm (SIFT), used to reduce the number of points for better matching, has developed a key point based CMFD and localization process	Fast keypoint based forgery detection and localization technique	Bit complex	FAU, GRIP, MICC-F220, MICC-F600, CMH, COVERAGE.
SURF [25]	Depends on SURF descriptors, a fast method for identifying image CMF has been presented. First, SURF descriptors are extracted, and then matching is done between all of the descriptor's subsets	Unable to automatically identify the tampered-with region and its boundaries	Own dataset	
SURF [26]	A comparison of SURF and SIFT has been conducted, and it has been found that SURF's forgery detection algorithm operates more quickly than SIFT's. Due to the use of integral images and the Hessain matrix approximation, SURF can match data faster	The morphological operations for detecting transformation in the forged part give better results	Less secured	10 high resolution uncompressed PNG true color images.
DCT [27]	The study describes DCT coefficient-based methods that use shift vectors and lexicographical sorting of DCT coefficients to detect identical sections of an image	Even after the image has been saved in JPEG format, this technique can quickly identify the forged portion of the image	Provides false detection results also	Lenna image
FMT [28]	It has been proposed to use Fourier-Mellin Transform (FMT) to extract features from the image blocks in order to detect image forgeries, even if the image is compressed using JPEG, rotated, highly compressed, blurred, or added noise	Even if the forged image is rotated, resized, or heavily compressed, the CMF portion of the image is very accurately detected	The robustness of the detection method is reduced after improving the efficiency of the detection method	Lenna image
DWT [29]	A CMFD approach using a block matching algorithm is proposed. The method involves applying two-dimensional DWT on the tampered image and dividing it into blocks based on its approximate DWT coefficients	The proposed algorithm for candidate block selection helps to alleviate the computational strain involved in comparing all blocks during block matching operations	With the decrease in block size, performance of False Detection Rate (FDR) increases	MICC-F220
LBP [30]	The proposed approach suggests using rotation-invariant uniform local binary patterns (LBP) to preprocess the image, followed by dividing it into overlapping circular blocks, to detect instances of CMF	Provides robust performance for regions after rotation and flipping, as well as for JPEG compression, noise contamination, and blurring	If the forged section is rotated at arbitrary angles, detecting the forgery becomes challenging	Images source: internet.

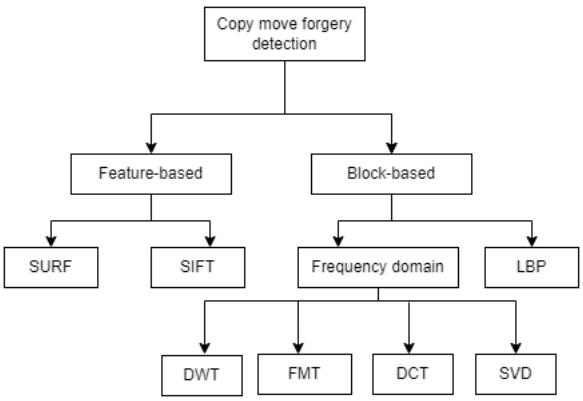

FIGURE 8: CMFD methods

mining orientation, and computing key point descriptors. Extracting SIFT descriptors from an image is insensitive to variations in rotation, scaling, lighting, and other factors. This approach can detect CMF by comparing the similarities between the copied and pasted regions. Huang H., Guo et al. [23] proposed an efficient method to identify CMFD in digital images. The process of obtaining SIFT descriptors from images involves calculating the Euclidean distance between the extracted descriptor vectors to perform matching. The performance of this approach is reasonable based on several post-image processing (JPEG compression, noise, rotation, scaling, etc.) and quantifying its robustness.

Li and Zhou [24] suggested a key point-based method for detecting and localising CMFD, which utilises the keypoint extraction algorithm (SIFT) to decrease the number of points, thereby enhancing the matching process. This approach is based on hierarchical feature point matching methods.

Bo, X, Junwen, et.al [25] has suggested a quick approach to detect image CMF, which relies on the SURF descriptors. The process involves extracting SURF descriptors and then performing matching between subsets of all the descriptors. This approach is helpful in detecting the duplicated region of the image and provides robustness to noise and blurring.

Jaseela and Nishadha [26] worked on SIFT and SURF for copy-move detectors and published a comparative study table by comparing the two techniques, where it is observed that forgery detection based on SURF algorithm works faster than SIFT based forgery detection algorithm. SURF has faster matching speed capacity because of Hessian matrix approximation and integral image.

To assess all the characteristics of a tampered image, block-based techniques are utilised by dividing the image into either overlapping or non-overlapping blocks. This division of blocks followed robust feature extraction of each block and feature matching with a pair of block. Matching is done after sorting or arranging the block feature by using the appropriate data structure. Frequency domain and LBP are the popular block based algorithms used in CMFD to identify copy-move attacks.

By using the frequency domain through signal transform duplicate region of an image is identified by offering signatures for the image blocks. Fast Fourier transform (FFT), DCT, FMT and DWT are the various frequency domain method. Fridrich, J., et al. [27] presented a study where duplicate regions of an image were detected by quantising a DCT coefficient-based approach employing shift vectors and lexicographic sorting of the DCT coefficient. Even when a tampered image is saved in a lossy format of JPEG or the copied region has been retouched to merge-in, this method can still detect the altered portion of the image.

Bayram, et al. [28] proposed an approach to extract features from image blocks which are used to identify fake images by using the FMT. The FMT features are robust even if the image is in JPEG compression, rotated, highly compressed, blurring, or noise addition. Furthermore, counting bloom filters rather than lexicographic sorting is used to shorten the detection timing.

Fattah, S.A., et al. [29] explained a block matching tech-

nique that is employed in a CMFD method. This involves applying two-dimensional DWT to the tampered image and dividing the approximate DWT coefficients into blocks. To reduce the computational burden, a similarity measure is used to select only a few candidate blocks from the non-overlapping blocks. A similarity criterion is introduced to detect the forged blocks of an image, which can detect CMF efficiently.

The spatial structure of an image is defined using a grayscale texture operator named LBP. Li., lL., et al. [30] proposed a method of detecting CMF that filters the image and then separates it into overlapping circular blocks. The circular blocks' features are extracted using rotation invariant uniform local binary patterns (LBP), and the relevant blocks are tracked to identify the forged regions. The LBP properties remain robust regardless of the image's characteristics, such as JPEG compression, blurring, noise contamination, region rotation, flipping, etc.

2) Retouching

Forgery detection often involves retouching, which can alter the visual attributes of an image, such as its color, sharpness, or other features [21]. Because of this, the image's visual presentation changes, which are reflected in the modified image in Fig. 9. This method is less harmless and less

FIGURE 9: Retouching forgery detection

malicious compared to other forgery methods. A good quality photo retouching tool is used for manipulating any image to improve the whole image or portion compared to the original image. This type of improvement or retouching, such as correction, sharpness, saturation etc., on an image is so accurate that it cannot be identified easily without a sophisticated detection tool. G. Cao et al. [31] proposed a technique to differentiate between single-source enhanced images and composite images that are enhanced using multiple sources. This is achieved by analyzing histogram peaks and gaps to detect any forgery artefacts. Whereas N. Zhu et al. [32] proposed an algorithm to detect forgery by examining histogram peaks and gaps in the image. The Canny operator is utilized first to detect the edges of the image, followed by applying the non-subsampled contourlet transform (NSCT) to categorize the edge points in the image. Table 7 shows some important information related to retouching.

3) Splicing forgery

Image splicing is a common and widely used method of image alteration. Splicing is one method of detecting forgeries, where multiple fragmented data are taken from numerous images and merged into one image. The final look of the output image is indistinguishable [22]. The output image having edges and corners are smoothed, color, sharpness and shifts are manipulated, which creates fake information Fig. 10.

FIGURE 10: Splicing forgery detection

Splicing is of two types - (1) Region-based splicing and (2) Boundary-based splicing. Various forensic techniques are applied to detect every form of distortion in the forged images. Fan et al., [33] defines a method combining five low-level statistics-based algorithms to estimate local illumination and detect image splicing. This method detects a spliced forgery region by estimating the variation in the illuminant color in the object region. To detect image splicing, Park et al., [34] proposed a wavelet domain inter-scale co-occurrence matrix is utilised by a method that employs characteristic function moments. Three well-known datasets, Columbia, CASIA1, and CASIA2, were used to evaluate their approach. Table 8 shows some important information related to splicing.

D. FORMAT BASED FORGERY DETECTION

It deals with image formats, especially in the JPEG format [35]. These detection methods are mainly based on statistical correlation. Correlations between any statistical units, such as pixels of the manipulated image, are established during its lossy compression. Table 9 shows some important information related to format based forgery detection.

1) JPEG quantization

JPEG (joint photographic expert group) is an image format, and its compaction is lossy based on how much compression is required. The image, which is in JPEG format is transformed into an RGB image, and the pixel values change based on low and high compression rates. The quantization is done by using DCT methods [35].

TABLE 7: Works related to Retouching

Technique	Description	Pros	Cons	Dataset Used
Retouching [31]	An algorithm has been suggested to differentiate between single source enhanced and both source-enhanced composite images. The method involves analyzing histogram peak/gap artifacts to detect any evidence of forgery	The proposed method can effectively identify image forgery when the last step of the manipulation involves contrast enhancement	If the image is highly compressed then it fails to detect forgery	BOSS public dataset and UCID.
Retouching [32]	Based on the overshoot artifact metric, an algorithm is applied to detect image sharpening operations	Detection accuracy is high	Not able to counter the anti-forensics of image sharpening	UCID.

TABLE 8: Works related to Splicing

Technique	Description	Pros	Cons	Dataset Used
Splicing [33]	A combination of five low-level statistics-based algorithms is utilized to estimate the illuminance of every vertical and horizontal band in order to accomplish image splicing detection along with local illumination estimate	This method may be used to accurately identify image splicing on the majority of image types	Slow performance	CASIA V2.0
Splicing [34]	A technique is suggested that utilizes the characteristic function moments for the inter-scale co-occurrence matrix in the wavelet domain	Best splicing detection accuracy for the Columbia image splicing detection evaluation dataset	Low performance for color splicing detection datasets	Columbia, CASIA1 and CASIA2

TABLE 9: Format based forgery detection

Sl.No	Terminology	Defination
1	JPEG Quantization [35]	It is generally a common image format, and its compression is lossy based on how much compression is required
2	Double JPEG [36]	JPEG image after manipulation, stored again in the format of JPEG after that modified and processed using the compression method twice.
3	JPEG blocking [37]	Once an image is re-compressed after cropping, a new set of blocking artifacts can be embedded which never aligns with the original boundaries.

TABLE 10: Camera based forgery detection

Sl.No	Terminology	Defination
1	Chromatic aberration [39]	Chromatic aberration means the improper focus of the light, while capturing an image; based on that outcome, aberration is disturbed, resulting image is forged.
2	Color filter array [40]	Color Filter Array (CFA) using interpolation process to create specific correlations between pixels if merged with other neighboring pixels
3	Camera responses [41]	Camera response function is used for mapping image irradiance into the intensity of the output image.
4	Sensor noise [42]	Sensor of digital image behaves like a unique identifier such as human fingerprint, skin blemishes etc.

2) Double JPEG

After processing, the manipulated image is saved again in the JPEG format, indicating that the image has undergone modification and compression twice. That's why this method is termed a double JPEG [36].

3) JPEG blocking

Once an image is re-compressed after cropping, a new set of blocking artefacts can be embedded, which never aligns with the original boundaries. JPEG provides an 8 by 8 pixel image block that will be compressed and quantized independently using DCT [37].

E. CAMERA BASED FORGERY DETECTION

This method is based on the principle of detection of camera artefacts. That means whenever an image has been captured using a digital camera; it is transferred from the camera's sensor to the camera's memory by following a sequence of processing stages, which include JPEG compression, gamma correction, filtering, color correlation, white balancing, and quantization. These steps may differ based on the camera model [38]. Table 10 shows some important information related to camera based forgery detection.

1) Chromatic aberration

Chromatic aberration means the improper focus of the light while capturing an image; based on that outcome, aberration is disturbed, resulting image being forged. It happens when an optical system fails to concentrate light from different wavelengths properly. This method is better modeled with high-quality image and produce good results [39].

2) Color filter array

A colored image needs at least three samples color at each pixel location, i.e., RGB, which stands for Red, Green, and Blue. The camera needs three different sensors in order to measure the image identically. However, modern cameras use interpolation to accomplish the same task using a single sensor coated with a colour filter array (CFA). This interpolation creates specific correlations between pixels if merged with other neighbouring pixels [40].

3) Camera responses

The source of an image can be identified solely based on the image itself, without requiring any information about the digital camera used to capture the image. Relationship with the quantity of light providing the corresponding pixel value

TABLE 11: Physical environment-based forgery detection

Sl.No.	Terminology	Defination
1	Physical Environment based Detection [43]	Identifying the forged region of the image using different types of lighting inconsistencies and the calculation of these inconsistencies can be done based on 2D and 3D surface for detecting forgery.

TABLE 12: Geometric based forgery detection

Sl.No	Terminology	Defination
1	Metric Measurement [21]	Analysis of various geometric parameters related to the image that can affect on the image clarity is termed as Metric Measurement.
2	Principal point [21]	The place where the center of the image is pointed means the principal point of an image.

TABLE 13: Frequently used dataset for image forgery detection

Dataset	Forgery Type	Resolution	No. of images	Format	Description
CMFDA	Copy-move	420 x 300 to 3888 x 2592	48	JPEG	Contains genuine and manipulated images that have undergone JPEG compression, scaling, and rotation
CoMoFoD	Copy-move	512 x 512 to 3000 x 2000	260	JPEG	contains both genuine and manipulated images that have been subjected to operations such as translation, rotation, scale distortion, or a combination of these
CPH	Copy-move	845 x 634 to 296 x 972	216	JPEG	Contains manipulated image created through some operations such as translation, rotation operation, scaling, compression etc.
CMH	Copy-move	845 x 634 to 1296 x 972	108	JPEG	Contains manipulated images created by applying various operations such as translation, rotation, scaling, compression, and others to produce cloned images
FAU	Copy-move	3000 x 2300	96	JPEG	Contains 48 genuine images and 48 manipulated images with realistic copy-move techniques
GRIP	Copy-move	768 x 1027	160	JPEG	The dataset consists of 80 authentic and 80 forged images. Some of the manipulated regions in the forged images are very smooth, which poses a challenge for copy-move forgery detection methods that use sparse sampling techniques such as SIFT
MICC- F600	Copy-move	800 x 533 to 3888 x 2592	600	JPEG	Contains authentic and manipulated images in this dataset which are selected randomly from the MICC-F2000 and SATS-130 datasets
MICC- F2000	Copy-move	2048 x 1536	2000	JPEG	Contains authentic and manipulated images in this dataset which are selected randomly from the MICC-F2000 and SATS-130 datasets
MICC- F220	Copy-move	722 x 480 to 800 x 600	220	JPEG	Dataset consists of authentic and manipulated image that are used for copy-move attack and geometric transformation
COVERAGE	Copy-move	Various	100	TIFF	Contains authentic and forged image that are used for identifying forged region
SBU-CM161	Copy-move	800 x 580	240	JPEG	Contains authentic image with rotation, compression, scaling, etc.
BOSS Public Dataset	Retouching	2000 x 3008 to 5212 x 3468	800	various	Contains unaltered photograph
UCID	Retouching	384 x 512	1338	TIFF	Contains uncompressed images used for natural scenes, man made objects and so on
SCUT-FBP	Retouching	384 x 512	500	TIFF	There are 500 images of female faces in the dataset and each image is accompanied by a score indicating their level of attractiveness
CISDE	Splicing	128 x 128	1845	PNG	Contains 912 authentic and 933 forged images, all are gray images
CUISDE	Splicing	757 x 568 to 1152 x 768	361	TIFF	Contains 181 authentic and 180 forged images, all are colored images
CASIA v1.0	Splicing	384 x 256	1725	JPEG	Contains 800 authentic and 925 forged images, all are colored images
CASIA v2.0	Splicing	240 x 160 to 900 x 600	12614	JPEG	Contains 7491 authentic and 5123 tampered uncompressd images, all are colored images
Columbia	Splicing	128 x 128	1845	BMP	The dataset consists of 933 authentic images and 912 manipulated images, all in BMP format

of the image exists in digital cameras. Camera response function is used for mapping image irradiance into the intensity of the output image. Using this process, the forensic investigator can determine what camera was used to take the image [41].

4) Sensor noise

Sensor of digital image behaves like unique identifier such as human fingerprint, skin blemishes etc. Different types of sensor defects or noise, including internal physical processes in cameras, environmental factors, and other potential influences on the image, are investigated by forensic analysts [42].

F. PHYSICAL ENVIRONMENT-BASED FORGERY DETECTION

Identifying the forged region of the image using different types of lighting inconsistencies, shadows, reflection etc. is termed physical environment-based forgery detection. The calculation of inconsistencies can be done based on two-dimensional (2D) and three-dimensional (3D) surfaces to detect forgeries [43]. This technique works based on the lighting environment. Table 11 shows some vital information related to physical environment-based forgery detection.

G. GEOMETRIC BASED FORGERY DETECTION

Precise geometric measurement and accurate position of any object relative to the camera is known as geometric based forgery [19]. Table 12 shows some important information related to geometric based forgery detection.

1) Metric measurement

If the location of an object changes, with respect to camera, an effect on the image clarity will be noticeable. Analysis of various geometric parameters related to image, is termed as metric measurement.

2) Principal point

An image having a principal point is the location where the image's centre is pointing at. Whenever the digital image is modified, the principal point of an image moves proportionally, which is used to detect forgery.

V. USED DATASET

Several datasets used during the analysis of forgery detection are shown in Table 13.

VI. NEW AVENUES FOR IMAGE FORGERY DETECTION

ML is a popular technology that allows a machine to learn automatically through experience. ML algorithms are widely

TABLE 14: Different ML techniques

Sl.No	Terminology	Defination
1	Supervised learning [51]	In this technique a ML model is being trained by using a labeled dataset of real as well as forged images. After training the model can determines either a new image is real or tampered.
2	Unsupervised learning [52]	In this technique a ML model is being trained by using a unlabeled dataset of real as well as forged images. Aim of unsupervised learning is to provide outcome by finding the patterns and relationship of image dataset without any prior knowledge about the dataset.
3	Reinforcement learning [53]	Reinforcement learning is similar to experience-based learning. The objective is to try new things and receive either rewards or penalties. The aim of this learning is to learn how to get the best rewards.

used in industries such as healthcare, education, traffic control, marketing, and finance [49]. ML algorithms have been utilized in digital image forensics to create tools for detecting and authenticating digital images. This method is effective at detecting image forgeries [50]. Some of the most commonly used ML techniques are illustrated in Fig. 11 and detail description is in table 14.

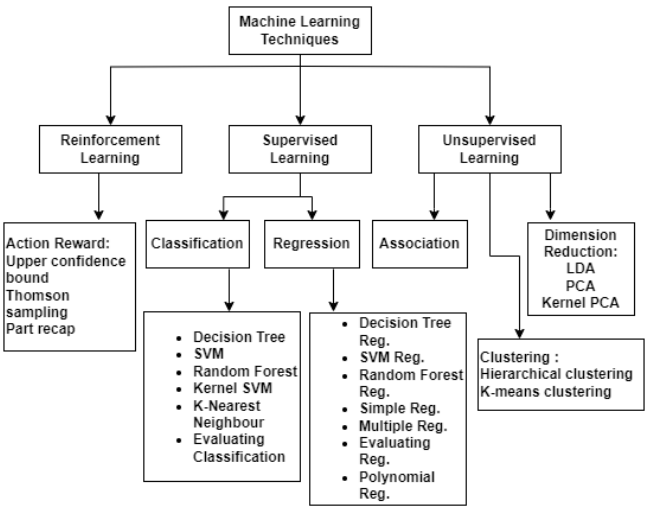

FIGURE 11: ML Techniques

This paper discusses several techniques for detecting image forgery, including active techniques such as digital watermarking and digital signature, as well as passive techniques like image splicing, copy-move, and retouching. While examining these techniques, drawbacks are found such as high computational complexity, vulnerability to various attacks, high false matching detection rates, and lower detection accuracy. In addition to the limitations mentioned earlier, these detection approaches are further limited in their scope of application. For example, an algorithm developed for detecting CMF cannot be used to identify other types of forgery, such as image splicing or retouching, and vice versa. Despite considerable research on the topic of image forgery detection, there is no single detection method that can reliably detect all types of forgery. Thus, there is a need for a robust and advanced forgery detection method that can overcome the limitations mentioned above.

Detecting image forgery using conventional methods becomes tough day by day. Different types of artificial intelligence (AI) based tools are used to forge an image that is a bit tough to detect using conventional methods. For this reason, to detect forgery different using ML tools such as NN or AI-based forgery detection techniques are used. So several AI-based forgery detection strategy have been stated in the present research work. NN or artificial neural networks are optimisation-based algorithms used for pattern recognition to identify the different object. CNN succeeded in digital forensics, used for searching patterns in digital media like image, video, etc. Fig. 12, shows the NN architecture with input features, hidden layers and output layer.

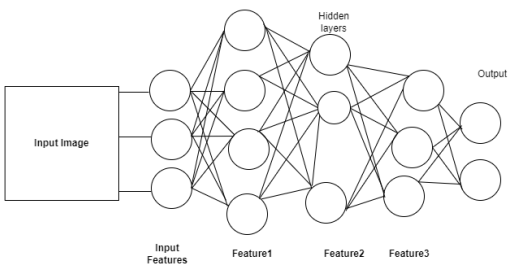

FIGURE 12: NN architecture

Currently, different approaches in active and passive methods of digital forgery detection use deep learning to produce promising results in identifying forged images. Regarding active forgery, watermarking is a popular method that uses CNN for detection. Zang et al. [44] proposed two-step mechanism for forged image detection. Firstly, the image is divided into patches, and each patch's features are then taught using a Stacked Autoencoder model. Furthermore, the next step is to obtain correct results, where each patch is updated with all relevant contextual data. A CNN design that Huang et al. [45] presented comprises a softmax classifier, two fully linked layers, and five convolutional layers. The stochastic gradient descent with momentum (SGDM) optimiser was utilised for gradient descent. The percentage of test images that were correctly identified was used to determine accuracy for the CASIA v1.0 dataset, which was split into training and testing sets. To detect and classify different types of forgeries, Rajini et al. [46] utilizing block discrete cosine transform (BDCT) in conjunction with ZM-polar (Zernike moment) and CNN. The image is first converted to YCbCr format. Next, BDCT and de-correlation are used to create

TABLE 15: Works related to Deep learning-based method for detecting image forgery

Technique	Model	Dataset	Accuracy
Copy-move [44]	Stacked-Auto-encoders (SAE)	CASIA v1.0, CASIA v2.0, Columia	91.09%
Splicing, Retouching, and Recompressing [45]	CNN	CASIA v1.0	95%(Spliced) 93%(Retouched) 71%(Recompress)
Copy-move and Splicing [46]	CNN	CASIA v1.0, CASIA v2.0	99.03%
Splicing [47]	rCNN	CASIA v1.0, CASIA v2.0, Columbia Image Forgery Database	97.62%(CASIA v1.0) 97.87%(CASIA v2.0) 96.38%(Columbia dataset)

TABLE 16: Performance evaluation metric

Sl. No.	Parameters	Description	Mathematical Equation
1	TPR (True positive rate) or R (Recall)	It is the proportion of accurately classified positive samples to the total number of positive samples	$\text{TPR} = \frac{\text{TP}}{\text{FN} + \text{TP}}$ (1)
2	TNR (True negative rate)	It is the proportion of negative samples to total negative samples that are accurately classified as negative	$\text{TNR} = \frac{\text{TN}}{\text{FP} + \text{TN}}$ (2)
3	FPR (False positive rate)	It is the proportion of incorrectly classified negative samples as positive samples to the total number of negative samples	$\text{FPR} = \frac{\text{FP}}{\text{TN} + \text{FP}}$ (3)
4	FNR (False Negative Rate)	It is the proportion of false negatives to the total number of actual positives	$\text{FNR} = \frac{\text{FN}}{\text{TP} + \text{FN}}$ (4)
5	P (Precision)	It is the proportion of accurately classified positive samples to predicted positive samples	$\text{P} = \frac{\text{TP}}{\text{FP} + \text{TP}}$ (5)
6	F1 Score	It is the harmonic-mean of Precision (P) as well as Recall (R)	$\text{F1} = \frac{2.\text{P.R}}{\text{R} + \text{P}}$ (6)
7	ACC (Accuracy)	It is the proportion of accurately predicted samples to the total number of samples	$\text{F1} = \frac{\text{TN} + \text{TP}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$ (7)

a feature vector set for the first CNN, which determines whether the image is real or tampered. To determine if an image is copy-moved or spliced, a CNN model is trained. The circular hough transform (CHT) is used to extract all features in the copy-move situation, and the patch method is used to train the CNN model. Yang et al. [47] proposed a rich model convolution neural network (rCNN) approach based on blocks for spliced images. The whole image is divided into processing blocks, each trained on a rCNN model. The rCNN model's seven convolution layers are applied to extract the desired features. Table 15 shows some vital information related to Deep Learning approaches.

After discussing all the existing methods, it may be concluded that the passive approach has the edge over the active approach, as there are some restrictions on the practical applications of digital signature and digital watermark under the active approach. Although passive approaches are more acceptable than active approaches, they still have some limitations, especially time complexity, for detecting the exact location of forgery. So a scope of future work exists to overcome those limitations. The main challenging task is to design a low-complexity algorithm, having the ability to detect forgery image efficiently and accurately.

VII. PERFORMANCE METRICS USED IN CMF

The performance of the suggested CMFD method can be understood by using test data and carefully analyzing the evaluation matrices, as indicated in Table 16. Researchers mainly use recall (R), precision (P), and F1 score to assess performance. With increases in R, P, and F1, the accuracy of the CMFD scheme gets better [48].

VIII. RESEARCH GAPS

Despite extensive research on image forgery, there are still numerous unresolved issues that require further investigation. Research indicates that while some methods can detect a single forgery, they often fall short when detecting multiple forgeries. Few writers have worked with multiple-forged region forgeries. Geometric transformations like rotation, scaling, and translation are not well-suited for use with block-based CMFD methods. Improved techniques and new approaches are needed to detect multiple forgeries. Block-based CMFD techniques are not robust to geometric transformations such as rotation, scaling, and translation. CMFD approaches based on keypoints have limited rotation and scaling capabilities. When images are rotated and scaled arbitrarily, existing methods struggle to perform well. An additional problem with Keypoint based approaches are struggle

to identify enough key points in flat or uniform regions. So keypoint based methods are ineffective for detecting CMF in consistent areas. To address this issue, block-based techniques can be combined with keypoint based methods. Traditional CMFD techniques require multiple parameters, making it necessary to automate the selection process. A method for automatically selecting customized parameters for each image is needed. Deep learning (DL) methods outperform traditional CMFD methods in terms of learning features. However, their use in CMFD is still relatively new and requires further research to improve performance. CMFD datasets lack sufficient images to support deep learning approaches is another issue.

IX. CONCLUSIONS

As an image becomes a vital source of legal data in the digital forensic department, forgery detection of an image is an essential topic in the research domain. This review shows a complete picture of image forgery detection, starting with basic architecture to the complete categorisation of image forgery. All the categorisations have been explained in an elaborate manner, with the corresponding research work proposed in the domain. This paper also discusses various existing approaches on different image forgery detection techniques. Qualitative analysis has been made and listed in a tabular form to better understand the presented work. A table containing frequently used dataset has been provided for the perspective researcher for image forgery detection work. Finally, the paper gives a direction on using neural networks with ML and DL based methods to identify any anomaly in an image for forensic evaluation.

REFERENCES

[1] Diwan, Anjali, and Anil K. Roy. "CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection." IEEE Access 12 (2024): 43809-43826.

[2] Verma, Mayank, and Durgesh Singh. "Survey on image copy-move forgery detection." Multimedia Tools and Applications 83, no. 8 (2024): 23761-23797.

[3] Kaur, Navneet, Neeru Jindal, and Kulbir Singh. "Passive Image Forgery Detection Techniques: A Review, Challenges, and Future Directions." Wireless Personal Communications 134, no. 3 (2024): 1491-1529.

[4] Singh, Satyendra, and Rajesh Kumar. "Image forgery detection: comprehensive review of digital forensics approaches." Journal of Computational Social Science (2024): 1-39.

[5] Mukherjee, Soumya, and Arup Kumar Pal. "A hybrid SWT-SVD based multiresolution features for robust image copy-move forgery detection." Multimedia Tools and Applications 83, no. 16 (2024): 48141-48163.

[6] El-Shafai, Walid, Mona A. Fouda, El-Sayed M. El-Rabaie, and Nariman Abd El-Salam. "A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends." Multimedia Tools and Applications 83, no. 2 (2024): 4241-4307.

[7] Urvoy, Matthieu, Dalila Goudia, and Florent Autrusseau. "Perceptual DFT watermarking with improved detection and robustness to geometrical distortions." IEEE Transactions on Information Forensics and Security 9, no. 7 (2014): 1108-1119.

[8] Bose, Anirban, and Santi Prasad Maity. "Spread spectrum watermark detection on degraded compressed sensing." IEEE Sensors Letters 1, no. 5 (2017): 1-4.

[9] Bamatraf, Abdullah, Rosziati Ibrahim, Mohd Salleh, and Najib Mohd. "A new digital watermarking algorithm using combination of least significant bit (LSB) and inverse bit." arXiv preprint arXiv:1111.6727 (2011).

[10] Makbol, Nasrin M., Bee Ee Khoo, and Taha H. Rassem. "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics." IET Image processing 10, no. 1 (2016): 34-52.

[11] Kumar, Ashwani, Satya Prakesh Ghrera, and Vipin Tyagi. "Implementation of wavelet based modified buyer-seller watermarking protocol (BSWP)." WSEAS Trans. signal process 10 (2014): 212-220.

[12] Totla, Radhika V., and K. S. Bapat. "Comparative analysis of watermarking in digital images using DCT & DWT." International Journal of Scientific and Research Publications 3, no. 2 (2013): 1-4.

[13] Ernawan, F., Kabir, M.N.: A robust image watermarking technique with an optimal dct-psychovisual threshold. IEEE Access 6, 20464–20480 (2018)

[14] Rani, Rajneesh, Akshay Kumar, and Amrita Rai. "A Brief Review on Existing Techniques for Detecting Digital Image Forgery." In 2021 Sixth International Conference on Image Information Processing (ICIIP), vol. 6, pp. 533-538. IEEE, 2021.

[15] Xuan, Zuguang, Zhenjun Du, and Rong Chen. "Comparison research on digital signature algorithms in mobile web services." In 2009 International Conference on Management and Service Science, pp. 1-4. IEEE, 2009.

[16] Zhang, Qiuxia, Zhan Li, and Chao Song. "The Improvement of digital signature algorithm based on elliptic curve cryptography." In 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp. 1689-1691. IEEE, 2011.

[17] Campbell, Scott. "Supporting digital signatures in mobile environments." In WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003., pp. 238-242. IEEE, 2003.

[18] Shukla, Deependra Kumar, Abhishek Bansal, and Pawan Singh. "A survey on digital image forensic methods based on blind forgery detection." Multimedia Tools and Applications (2024): 1-32.

[19] Alencar, Ancilon Leuch, Marcelo Dornbusch Lopes, Anita Maria da Rocha Fernandes, Julio Cesar Santos dos Anjos, Juan Francisco De Paz Santana, and Valderi Reis Quietinho Leithardt. "Detection of Forged Images Using a Combination of Passive Methods Based on Neural Networks." Future Internet 16, no. 3 (2024): 97.

[20] Shinde, Varun, Vineet Dhanawat, Ahmad Almogren, Anjanava Biswas, Muhammad Bilal, Rizwan Ali Naqvi, and Ateeq Ur Rehman. "Copy-move forgery detection technique using Graph Convolutional Networks feature extraction." IEEE Access (2024).

[21] Saber, Akram Hatem, Mohd Ayyub Khan, and Basim Galeb Mejbel. "A survey on image forgery detection using different forensic approaches." Advances in Science, Technology and Engineering Systems Journal 5, no. 3 (2020): 361-370.

[22] Kumari, Ritesh, and Hitendra Garg. "Image splicing forgery detection: A review." Multimedia Tools and Applications (2024): 1-39.

[23] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." In 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, vol. 2, pp. 272-276. IEEE, 2008.

[24] Li, Yuanman, and Jiantao Zhou. "Fast and effective image copy-move forgery detection via hierarchical feature point matching." IEEE Transactions on Information Forensics and Security 14, no. 5 (2018): 1307-1322.

[25] Bo, Xu, Wang Junwen, Liu Guangjie, and Dai Yuewei. "Image copy-move forgery detection based on SURF." In 2010 International conference on multimedia information networking and security, pp. 889-892. IEEE, 2010.

[26] Jaseela, S., and S. G. Nishadha. "Copy move image forgery detection using SURF feature point extraction." Int. J. Sci. Eng. Res 7, no. 7 (2016): 653-657.

[27] Fridrich, Jessica, David Soukal, and Jan Lukas. "Detection of copy-move forgery in digital images." In Proceedings of digital forensic research workshop, vol. 3, no. 2, pp. 652-63. 2003.

[28] Bayram, Sevinc, Husrev Taha Sencar, and Nasir Memon. "An efficient and robust method for detecting copy-move forgery." In 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1053-1056. IEEE, 2009.

[29] Fattah, Shaikh Anowarul, M. M. I. Ullah, M. Ahmed, Istak Ahmmed, and Celia Shahnaz. "A scheme for copy-move forgery detection in digital images based on 2D-DWT." In 2014 IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 801-804. IEEE, 2014.

[30] Li, Leida, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F. Roddick, and Jeng-Shyang Pan. "An Efficient Scheme for Detecting Copy-move

Forged Images by Local Binary Patterns." J. Inf. Hiding Multim. Signal Process. 4, no. 1 (2013): 46-56.
[31] Cao, G., Zhao, Y., Ni, R., Li, X.: Contrast enhancement-based forensics in digital images. IEEE transactions on information forensics and security 9(3), 515–525 (2014).
[32] Zhu, Nan, Cheng Deng, and Xinbo Gao. "Image sharpening detection based on multiresolution overshoot artifact analysis." Multimedia tools and applications 76 (2017): 16563-16580.
[33] Fan, Yu, Philippe Carré, and Christine Fernandez-Maloigne. "Image splicing detection with local illumination estimation." In 2015 IEEE international conference on Image processing (ICIP), pp. 2940-2944. IEEE, 2015.
[34] Park, Tae Hee, Jong Goo Han, Yong Ho Moon, and Il Kyu Eom. "Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain." EURASIP Journal on Image and Video Processing 2016 (2016): 1-10.
[35] Bhowal, Arundhati, Sarmistha Neogy, and Ruchira Naskar. "Deep Learning-based forgery detection and localization for compressed images using a hybrid optimization model." Multimedia Systems 30, no. 3 (2024): 128.
[36] Verma, Vinay, Deepak Singh, and Nitin Khanna. "Block-level double JPEG compression detection for image forgery localization." Multimedia Tools and Applications 83, no. 4 (2024): 9949-9971.
[37] Nikoukhah, Tina, Miguel Colom, Jean-Michel Morel, and Rafael Grompone von Gioi. "Local JPEG grid detector via blocking artifacts, a forgery detection tool." Image Processing On Line 10 (2020): 24-42.
[38] Kaur, Navneet, Neeru Jindal, and Kulbir Singh. "Passive Image Forgery Detection Techniques: A Review, Challenges, and Future Directions." Wireless Personal Communications 134, no. 3 (2024): 1491-1529.
[39] Elmaci, Mehmet, Ahmet Nusret Toprak, and Veysel Aslantas. "Detection of background forgery using a two-stream convolutional neural network architecture." Multimedia Tools and Applications 83, no. 12 (2024): 36739-36766.
[40] Liu, Lei, Peng Sun, Yubo Lang, and Jingjiao Li. "CFA-Based Splicing Forgery Localization Method via Statistical Analysis." IET Signal Processing 2024, no. 1 (2024): 9929900.
[41] El-Shafai, Walid, Mona A. Fouda, El-Sayed M. El-Rabaie, and Nariman Abd El-Salam. "A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends." Multimedia Tools and Applications 83, no. 2 (2024): 4241-4307.
[42] Alencar, Ancilon Leuch, Marcelo Dornbusch Lopes, Anita Maria da Rocha Fernandes, Julio Cesar Santos dos Anjos, Juan Francisco De Paz Santana, and Valderi Reis Quietinho Leithardt. "Detection of Forged Images Using a Combination of Passive Methods Based on Neural Networks." Future Internet 16, no. 3 (2024): 97.
[43] Ghai, Ambica, Pradeep Kumar, and Samrat Gupta. "A deep-learning-based image forgery detection framework for controlling the spread of misinformation." Information Technology & People 37, no. 2 (2024): 966-997.
[44] Zhang, Ying, Jonathan Goh, Lei Lei Win, and Vrizlynn Thing. "Image region forgery detection: A deep learning approach." In Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016, pp. 1-11. IOS Press, 2016.
[45] Awasthi, Divyanshu, and Vinay Kumar Srivastava. "Robust, imperceptible and optimized watermarking of DICOM image using Schur decomposition, LWT-DCT-SVD and its authentication using SURF." Multimedia Tools and Applications 82, no. 11 (2023): 16555-16589.
[46] Jordan, Michael I., and Tom M. Mitchell. "Machine learning: Trends, perspectives, and prospects." Science 349, no. 6245 (2015): 255-260.
[47] Mehraj, Samrah, Subreena Mushtaq, Shabir A. Parah, Kaiser J. Giri, and Javaid A. Sheikh. "A robust watermarking scheme for hybrid attacks on heritage images." Journal of Ambient Intelligence and Humanized Computing 14, no. 6 (2023): 7367-7380.
[48] Rakhmawati, L., Tjahyaningtijas, H.P.A., Yustanti, W., Wiryanto, W.: A block- based image characteristics robust watermarking with optimal embeddable ac coefficient. International Journal of Intelligent Engineering & Systems 16(4) (2023)
[49] Chowdhury, Rakibul Hasan. "Advancing fraud detection through deep learning: A comprehensive review." World Journal of Advanced Engineering Technology and Sciences 12, no. 2 (2024): 606-613.
[50] Huang, Zengyi, Haotian Zheng, Chen Li, and Chang Che. "Application of machine learning-based k-means clustering for financial fraud detection." Academic Journal of Science and Technology 10, no. 1 (2024): 33-39.
[51] Vaishali, Sharma, and Singh Neetu. "Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model." Multimedia Tools and Applications 83, no. 4 (2024): 10839-10863.
[52] Chowdhury, Rakibul Hasan. "Advancing fraud detection through deep learning: A comprehensive review." World Journal of Advanced Engineering Technology and Sciences 12, no. 2 (2024): 606-613.
[53] Verma, Mayank, and Durgesh Singh. "Survey on image copy-move forgery detection." Multimedia Tools and Applications 83, no. 8 (2024): 23761-23797.
[54] Huang, Yanping, Wei Lu, Wei Sun, and Dongyang Long. "Improved DCT-based detection of copy-move forgery in images." Forensic science international 206, no. 1-3 (2011): 178-184.
[55] Qazi, Tanzeela, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, and Cheng-Zhong Xu. "Survey on blind image forgery detection." IET Image Processing 7, no. 7 (2013): 660-670.
[56] Al-Qershi, Osamah M., and Bee Ee Khoo. "Passive detection of copy-move forgery in digital images: State-of-the-art." Forensic science international 231, no. 1-3 (2013): 284-295.
[57] Singh, Ratnam, and Mandeep Kaur. "Copy move tampering detection techniques: a review." International Journal of Applied Engineering Research 11, no. 5 (2016): 3610-3615.
[58] Zhang, Zhi, Chengyou Wang, and Xiao Zhou. "A Survey on Passive Image Copy-Move Forgery Detection." Journal of Information Processing Systems 14, no. 1 (2018).

POULOMI DEB is a Ph.D. Scholar in the Department of Computer Science and Engineering of the National Institute of Technology, Agartala. She has a B.Tech degree in Information Technology from West Bengal University of Technology (WBUT)(2013) and an Mtech in Computer Science and Engineering from Tripura University, Agartala (2015). Her research interests include cryptography, networking, information security, steganography and cybersecurity.

SUBHRAJYOTI DEB is working as an Assistant Professor in the Department of CSE at the ICFAI University Tripura, India. Prior to joining the ICFAI University, he was a Postdoctoral Visiting Scientist in the Applied Statistics Unit, ISI Kolkata, India. He has received his M.Tech and Ph.D from the NIT Agartala and NEHU Shillong respectively. He is Visvesvaraya PhD awardee under MeitY, Government of India. His research interests include Cryptography, Information security, Data Hiding Steganography, and IoT. He visited Japan under IRIS programme of the Embassy of Japan. Dr. Deb has one patent granted and nearly 30 publications in refereed journals, book chapters and conference proceedings. He has participated in many international conferences as an Organizer and Session Chair. Dr. Deb is an Editorial Board member and a Reviewer of many SCI indexed journals.

ABHIJIT DAS is an Assistant Professor - Senior Scale in the Department of Information Technology at Manipal Institute of Technology, Bengaluru. With over 17 years of experience, he specializes in Computer Networks Security, Operating Systems, Mobile Application Development, Data Structures & Applications, and Machine Learning. Abhijit holds a Bachelor of Engineering from National Institute of Technology, Agartala, a Master of Technology from Jawaharlal Nehru New College of Engineering, Shimoga, and a PhD from Visvesvaraya Technological University, Belgaum, Karnataka. His research interests include Cyber Security and Deep Learning, with numerous publications and patents. Abhijit has a commitment to academic excellence and practical application, having guided significant projects such as the Mobile Banking Project recognized in IBM-TGMC The Great Mind Challenge, 2007. He has also received awards for his expertise in C programming. His role as project coordinator on the VGST project funded by the Government of Karnataka from 2017 to 2019 further demonstrates his dedication to advancing research and innovation in his field.

DR. NIRMALYA KAR is an Assistant Professor in the Department of Computer Science and Engineering at the National Institute of Technology (NIT) Agartala. He also serves as the Chief Information Security Officer at the Institution. Having more than 18 years of teaching and research experience, Dr. Kar specializes in Information Security, Cryptography, Computational Intelligence and the Internet of Things (IoT). He has 2 patents and more than 60+ research contributions in refereed journals, book chapters, conference proceedings. Dr. Kar has been involved in various academic roles including Organising Chair and General Chair of International Conferences, Editor of Book Chapters, reviewer board of many SCI journals and transactions apart from other administrative roles like coordinating high-performance computing initiatives at NIT Agartala, Academic coordinator of UG curriculum etc.