AN OVERVIEW OF COPY MOVE FORGERY DETECTION APPROACHES

Gayathri K S[1] and Deepthi P S[2]

[1]Department of Computer Engineering, LBS Institute of Technology for Women, APJ Abdul Kalam Technological University, Mar Baselios College of Engineering and Technology, Trivandrum, Kerala
[2] LBS Institute of Technology for Women, Trivandrum, Kerala

ABSTRACT

Images have greater expressive power than any other forms of documents. With the Internet, images are widespread in several applications. But the availability of efficient open-source online photo editing tools has made editing these images easy. The fake images look more appealing and original than the real image itself, which makes them indistinguishable and hence difficult to detect. The authenticity of digital images like medical reports, scan images, financial data, crime evidence, legal evidence, etc. is of high importance. Detecting the forgery of images is therefore a major research area. Image forgery is categorized as copy-move forgery, splicing, and retouching. In this work, a review of copy-move forgery is discussed along with the existing research on its detection and localization using both conventional and deep-learning mechanisms. The datasets used and challenges towards improving or developing novel algorithms are also presented.

KEYWORDS

Copy Move Forgery, Splicing, Keypoint Detection, Image Forensics

1. INTRODUCTION

This Application of Digital images are visible in many fields like social media, the medical field, agriculture, journalism, forensics, etc. With their widespread use, there are also online tools to edit them. These manipulated images can be preprocessed or postprocessed to appear more realistic. The images can be forged such that they are difficult to identify as forged. The branch of cyber security that focuses on maintaining the integrity of digital images is image forensics. Image forgery can create serious problems in real life. As an example, the cancerous cells in the scan report image of a patient can be altered by hackers. Even surgeons could be misled by these scan reports, leading to misdiagnosis and insurance fraud. Image forgery related to politics can influence public decisions [20]. Forging digital images is considered a cybercrime, and authenticating the integrity of these digital images is a hot research area in cyber security.

Image tampering is classified into copy-move forgery (CMF), splicing, and retouching. CMF is imitating some image contents in areas within the image itself. Image splicing is done by merging parts of two or more images. The target image undergoes further processing to make the tampering invisible. Image retouching is a form of image enhancement. They are done to make the image more attractive by making small adjustments to the image [9]. Some examples of retouching are removing spots, fixing hair, clothes, etc.

The two methods for detecting forgery are passive and active, as shown in Figure. 1. In the active method, the image is embedded with additional information to help detect tampered images. Digital watermarking and steganography are the two active approaches. These methods are very accurate in determining image tampering, but most of the images on the internet may not have any embedded watermarks or signatures.

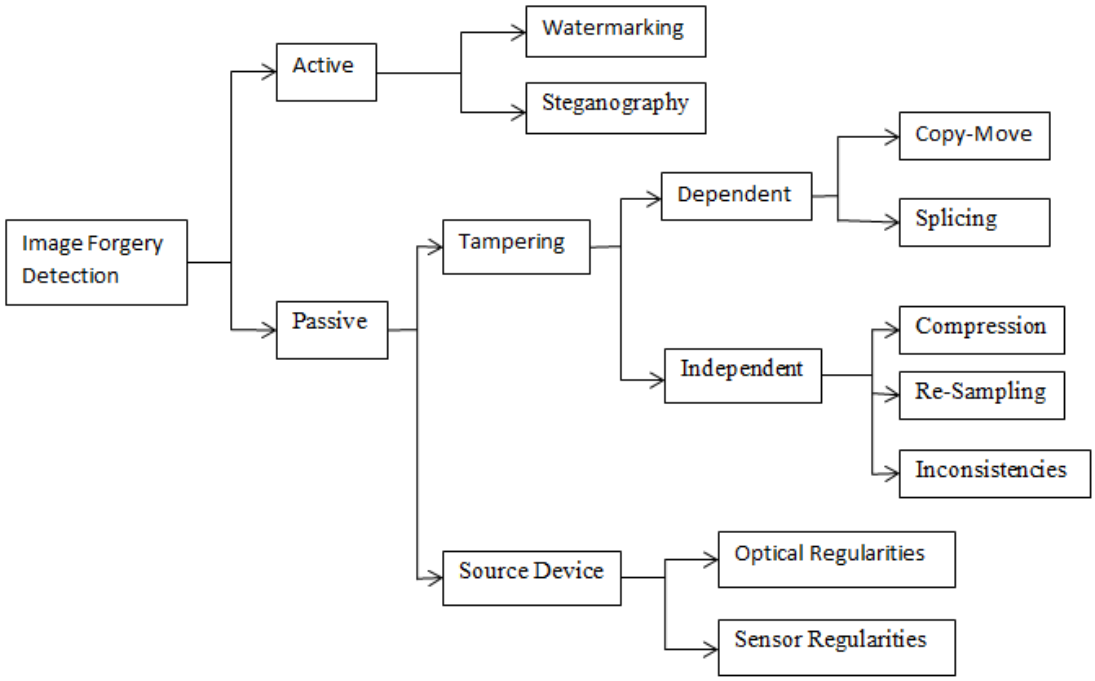

Figure 1. Categorization of Image Forgery Detection Techniques [2]

The passive approach does not rely on watermarks or signatures, but detection is based on extracting meaningful features from the image. Hence the method is also called the "blind detection method." The passive method is further divided into dependent and independent methods. In dependent forgery, modification is done to the image in the form of CMF or splicing, whereas in independent forgery, some properties of the image are altered. Some of the independent forgery techniques are retouching, resampling, compression, etc. Source device techniques are used to detect the source of the image based on optical and sensor regularities. The two main digital image forgeries now being researched widely are CMF and splicing. In this work, the survey of publications between 2019 and 2022 on CMF detection and localization (locating the forged portions in the image) methods is presented.

The remaining paper is arranged in the following manner: Section 2 focuses on CMF. Section 3 elaborates on the conventional methods for detecting CMF. Section 4 focuses on deep learning-based detection techniques. Section 5 summarises the challenges and research directions that should be pursued further. Conclusions follow in Section 6.

2. COPY MOVE FORGERY DETECTION

CMF is one of the most widely used forgeries. In CMF, tampering is done on the same source, i.e., imitating the contents of the same image. Grass, foliage, and fabric [2] are common areas for manipulation because their colour and texture blend well with the background. Also, if CMF is associated with attacks, then it becomes more difficult to identify the forged image. Attacks

associated with CMF are scaling, rotation, and translation, commonly called "geometric transformation attacks," and post-processing attacks like brightening, blurring, compression, etc., There are four steps in CMF detection (CMFD). These are pre-processing, feature extraction, feature matching, and visualization, as shown in Figure. 2. The preprocessing step is optional and is done to enhance image data. Commonly used CMFD pre-processing techniques are the conversion of RGB to grayscale, HSV, YCbCr, local binary pattern (LBP), principal component analysis (PCA), etc., which reduce image dimensionality and thereby increase processing speed or detection accuracy. Another technique used is block division [19]. Here, the image is chunked down into small partitions. Then block matching is done to find similar features. The feature extraction stage comes next. This is the crucial step in CMFD, as the accuracy of the entire detection depends on the features extracted. Features of interest are taken from the image. During matching, identified features are compared to determine their similarities. Finally, visualization is used to locate and display the forged parts of the image [8].

2.1. Feature Extraction Techniques

The methods for extracting relevant features of an input image are categorised into transformation, hashing, LBP, keypoint, histogram, color- and intensity-based techniques, etc. Transformation techniques convert images from spatial domain to frequency domain. Significant information about an image is carried by a few coefficients. Using these coefficients will enable an efficient detection process. High-frequency components like edges or irrelevant features can be eliminated from the image using transformation methods to emphasise low-frequency components, which are essential for the detection process. Some transformations used in literature are the discrete cosine transform, the stationary wavelet transform, the discrete wavelet transform, the polar complex exponential transform, Zernike moments, the polar cosine transform, the fourier mellin transform, the one-dimensional fast fourier transform, the diadic wavelet transform, the polar harmonic transform [2], etc.

The transform domain is also used to extract texture features. The Gabor filter can be used for this purpose, but it doesn't perform well when the image is compressed. LBP is used for texture analysis. It is a statistical method that converts a block of image data to texture information. LBP is applied to each pixel in the target image by comparing the intensities of its eight surrounding neighbours.

In spatial domain-based methods, the pixel locations in the image that contain interesting contents are considered. These points in the image are called key points. Key points are those that stand out from the crowd. They remain unaltered even though the image is rotated, scaled, or distorted. Key points can be detected based on edges, corners, and blobs in the target image. Harris Corner detection, Laplacian of Gaussian, Difference of Gaussian, Scale-Invariant Feature Transform (SIFT), and other key point detection methods are used in CMFD. However, SIFT has a high computation cost and is highly complex. So many variants of SIFT are used for CMFD, like binarized SIFT, OpponentSIFT, and Affine-SIFT. Other popular methods in research are speed-up reduced features (SURF) and mirror reflection invariant feature transform [2].

The feature of extraction based on the intensity of pixels is the most popular, as it extracts primary information from pixels. For grayscale images, the intensity is a single value, but for colour images, there are three intensity values. The spatial arrangement of colour or intensity in an image can be extracted for CMFD. Examples of these techniques are halftoning-based block truncation coding, Weber local descriptor, image binarization, LBP, etc. Moments are the weighted average of pixel intensities, which can be used as features to detect tampering in images. The invariant moments are features of an image that are not changed under rotation, scaling, etc. Two commonly used moments are the Hu moment and the Zernike moment.

Techniques like exponent moments, magnitude, Polar Complex Exponential Transform (PCET) moments, etc. are examples.

Finally, dimensionality reduction techniques are involved to minimise the volume of features extracted from the image, which helps in speeding up further matching and visualisation steps. Frequently used dimensionality reduction techniques are PCA, Kernal-PCA, Singular Value Decomposition, Locality Preserving Projection, Angular Radial Partitioning, Gray-Level Co-Occurrence Matrix, etc.

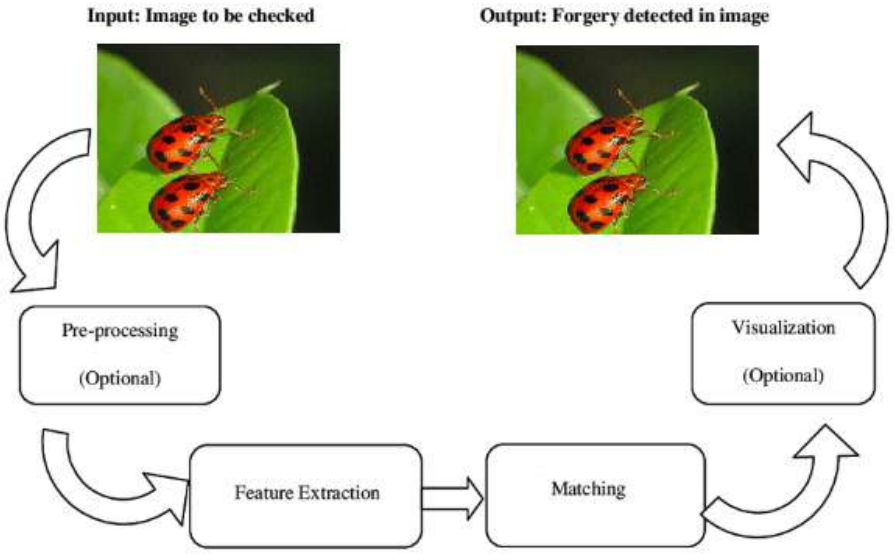

Figure 2. CMFD Model [2]

2.2. Matching

The matching process compares the similarity of tampered and original areas of the image using the features extracted in the previous step. Matching is categorised into two categories: searching methods and similarity measuring methods. Search methods are used to find matches between original and forged parts. Similarity methods are used to find similarity between two features [2]. A single image can generate a large number of features, and matching all these features is a computationally challenging task. Sorting is employed to make the matching process faster. Some sorting techniques used in CMFD are radix sort, colour texture descriptor-based sorting, lexicographical sorting, etc. Another popular matching technique is the nearest neighbour (NN). Two features are similar in the NN-method if the distance between their NN is less than a predefined threshold. Commonly used NN techniques are 2NN, generalised 2-nearest-neighbor (g2NN), and reversed g2NN. In hashing, the feature descriptor is processed into an easier-to-compare form, which improves the speed of the matching process. Traditional SIFT with hashing reduces the search space, thereby improving the accuracy and detection speed. Another hashing technique used is locality-sensitive hashing.

In hierarchical structure methods, relevant feature descriptors that are closely located in the hierarchy are grouped. The K-d tree is an example of a hierarchical structure-based method. Hence, this method minimises the computational load. The matching technique that has become popular in CMFD is the clustering and segmentation method. Segmentation is done to segment the target image into relevant patches. Hence, matching needs to be done only between the feature descriptors of different patches. Commonly used methods are the Gaussian mixture model

clustering, fuzzy C-Means clustering, etc. These methods result in reduced complexity, thereby speeding up the matching process. Other search-based matching techniques used in literature are priority-based matching, patch matching, symmetry matching, etc.

Search-based matching techniques find a suitable match by looking for the closest, or approximately closest, neighbours. Similarity-based techniques are used for the comparison of descriptors [2]. Euclidean distance is the most commonly used similarity measuring method. Other methods used to compute similarity measures between two feature descriptors are Manhattan distance, Euclidean with correlation technique, Euclidean with adaptive threshold, shift frequency threshold, and Euclidean distance threshold, and hashing with Hamming distance. The matching process most likely ends up with some false positives. That is, some non-forged parts are detected as forged parts. Methods for removing false positives need to be utilised to remove these faults. Some commonly used techniques are segmentation and clustering, threshold-based estimation, and transform-based estimation. Clustering or segmentation is a popular false match reduction technique that separates genuine and forged areas in the subject image. The presence of forgeries can be identified with the help of distance measurements between clusters. Some examples are agglomerative clustering and the Random Sample Consensus Algorithm (RANSAC) [19]. Simple linear iterative clustering segmentation is utilised in many CMFD processes to separate the target image into relevant segments. The threshold-based method utilises a predefined threshold value to detect image tampering. Two regions are considered to be a match if their distance exceeds the threshold.

3. CONVENTIONAL METHODS FOR IMAGE FORGERY DETECTION

Features needed for CMFD can be extracted either manually or automatically. Based on the feature extraction method, CMFD is performed in two ways: handcrafted feature-based and using approaches that use deep learning. The first approach can be implemented using 3 approaches: block-based, key-point-based, and hybrid approaches. Deep learning approaches incorporate deep networks like CNN that have the capability to automatically learn from the training samples and extract useful features that eventually help in detecting forgeries.

3.1. Block-based Approach

One of the most popular CMFDs is block-based forgery detection. Here, the entire image is broken down into small chunks, which can either overlap with each other or not overlap [2]. From each of these blocks, relevant features are extracted and compared for matches. The matched blocks indicate forged portions.

3.2. Keypoint-based Approach

In key point approaches, key points of the image are identified, and then features are extracted from the identified key points. Here, features like corners, edges, blobs, etc. are extracted from the image rather than divided into blocks. A set of descriptors is used to characterise each feature. Forged portions are identified by matching the extracted features and their descriptors. SIFT, Harris Corner Detector, and SURF are the commonly used key point feature extraction techniques.

Block-based CMF detection techniques incur a high computational cost, and they are unable to detect forgery with large-scale distortion. Key point-based methods are inefficient in addressing the detection of forgery in images with smoothing effects. Hence, fusion methods involving the best features of both of these techniques were used to detect forgery. To detect image tampering,

features extracted using key point methods and region matching using block-based methods are combined. But if the features are sparse, then again, the fusion methods cannot address the smoothing effect.

The authors [3] proposed two algorithms for the detection of forgery in official documents that are compressed. For CMFD, the authors extracted DCT coefficients and performed feature matching on coefficient values. For copy-paste forgery, the authors have used the averaged sum of the absolute difference. In [13], the authors have used a keypoint-based approach to detect CMF. Keypoints are detected using the Center Surround Extremas for Realtime Feature Detection and Matching (CenSurE) detector and Fast Retina Keypoint (FREAK) descriptors. Matching is done using k-NN, and agglomerative hierarchical clustering is used to eliminate false alarms in the images. The authors [14] detected CMFD by using SURF and SIFT. Keypoint matching is done using the nearest neighbour method to identify forged regions. In [15], the authors have used a keypoint-based approach for CMFD. SIFT features and descriptors are then extracted and matched using fast approximate nearest neighbor (FANN). Density-based Spatial Clustering of Applications with Noise (DBSCAN) is used to detect duplicate regions. The authors [17] developed an optimized technique to detect and locate CMF. They used the Steerable Pyramid Transform (SPT) to get the different orientations. An optimized support vector machine (OSVM) classifier is used. In [21], the authors proposed a keypoint CMFD method, namely, Second Keypoint Matching and Double Adaptive Filtering (SMDAF). The double adaptive filter is used to remove false alarms that are based on Adaptive Locally-Affine Matching (AdaLAM) and K-Average Nearest Neighbor DBSCAN (Kann-DBSCAN) clustering.

In [25], the authors have utilized optimization techniques to develop CMFD. Keypoints are extracted from the preprocessed image using the SIFT method. Football Game Optimization (FBGO) is used for clustering the features. Matches are identified by Euclidean distance. The authors [28] proposed a CMFD model that combines block and keypoint methods. FCM clustering with Emperor Penguin Optimization (EPO) is used to cluster the similar superpixels. The Gabor filter is used to generate feature descriptors. Then feature matching is done by computing the correlation coefficients of image blocks. The authors [29] proposed a CMFD algorithm using improved SIFT, feature label matching (FLM), and hierarchical segmentation. The authors [31] proposed a CMFD method involving Features from Accelerated Segment Test (FAST), Binary Robust Independent Elementary Features (BRIEF), and SIFT techniques. FAST extracts texture features like corners and edges. SIFT extracts features in smooth areas, and hence noise removal is done. Then, BRIEF is used to get the binary feature descriptors for FAST features. Matching is done with g2NN. Superpixel segmentation using linear spectral clustering (LSC) is done to improve the localization of forgeries. The authors [32] developed a robust method for CMFD. The proposed method uses the local binary pattern rotation invariant (LBP-Rot) to extract the structural texture information of the image. SIFT keypoints are identified in the textual image. Then keypoint matching is done using g2NN. Table I lists the comparisons.

Table 1. Conventional Methods of CMFD and Localization

Ref	Methods Used	Dataset	Performance	Remarks
[3]	Block based - DCT coefficients, Averaged Sum of Absolute Difference (ASAD)	CoMoFoD, Official Marks Card Dataset (OMCD)	Precision of 95.95%, a recall of 94.52%, and an F-score of 95.22% for CMF; precision of 80.45%, a recall of 89.05%, and an F-score of 84.53% for copy-paste forgery	Testing for the same marks in two subjects has not been done.
[13]	Keypoint based – CenSurE, FREAK, k-NN, Agglomerative Hierarchical Clustering	Coverage, MICC-F600, , CoMoFoD, Grip, CMFD, MICC-F220	F1-Measure of 97.61 for CMFD, 95.12 for GRIP, 97.50 for Coverage, 97.14 for MICC-F600, 98.43 for MICC-F220, and 98.43 for CoMoFoD	The method does not guarantee good results on highly smooth images. Also, poor results are obtained for combination attacks like rotation followed by scaling.
[14]	SIFT, SURF, Agglomerative Hierarchical clustering, RANSAC	MICC-F220	F1-score of 91.7 and recall of 92.5	The dataset is limited to only 220 images. Other standard datasets are not tested.
[15]	CLAHE, SIFT, DBSCAN, GORE and RANSAC	MICC-F220, Image manipulation dataset	Recall of 95.83%	Combination attacks are not tested. DBSCAN with high-dimensional data is complex.
[17]	SPT, GLCM, SPT, OSVM, Erosion, Dilation	CoMoFoD, CASIA	TPR and TNR of 99%; FPR and FNR of 1% without attacks	TPR and TNR values are lower when attacks are introduced. Combination attacks are not tested. The method was not tested with the addition of noise.
[21]	SIFT, AdaLAM, KANN-DBSCAN, Convex Hull, Padding	CASIA, MICC-F220, CoMoFoD, COVERAGE	FI-Score of 0.714 for CASIA, 0.904 for MICC-F220, and 0.711 for Coverage	Since a lot of computations are involved, the time for detecting forgery could have been measured. Combination attacks are not tested.
[25]	SIFT, DWT, FBO, RANSAC	500 samples from websites	Accuracy of 96	Samples used for training and testing are very limited. Attacks are not tested.
[28]	Turbo pixel, FCM clustering, Emperor Penguin Optimization, Gabor filter, RANSAC, Labelled Feature Points, FRE	MICC-F600	E-Measure of 95.06%	Double attacks and JPEG compression testing are not mentioned. The number of samples in the dataset is 600, which is very low.
[29]	SIFT, Feature Label Matching, Hierarchical Segmentation	Image manipulation dataset (IMD), CMH and GRIP	Precision of 91.15 %, 91.85% Recall and 91.50% F1-Score with CMH and 91.09%	Double attacks were not tested. Testing with other benchmark datasets like CASIA, COVERAGE, etc. is not done.

			Precision, 93.15% Recall and 92.11% F1-Score with GRIP	
[21]	SIFT, AdaLAM, KANN-DBSCAN, Convex Hull, Padding	CASIA, MICC-F220, CoMoFoD, COVERAGE	FI-Score of 0.714 for CASIA, 0.904 for MICC-F220 and 0.711 for Coverage	Since a lot of computations are involved, the time for detecting forgery could have been measured. Combination attacks are not tested.
[31]	FAST, BRIEF, SIFT, g2NN, Linear Spectral Clustering	Datasets of Ardizzone et al. and Lozzolino et al. and MICC-F8 multi datasets	0.9023 Precision, 1 Recall and 0.98864 F1-Score	Double attacks were not tested. Testing with other benchmark datasets is not done.
[33]	LBP-Rot, SIFT, g2NN, RANSAC, Ciratefi, Connected Component Labeling	GRIP and CMH	F-Measure of 96 with GRIP and an accuracy of 97.88 with CMH datasets	The method is complicated, as it includes two matching processes. Complexity analysis has not been done. Double attacks were not tested. Testing with other benchmark datasets is not done.

4. DEEP LEARNING BASED APPROACH

Deep learning uses an artificial neural network that resembles the human brain. Due to their generalization and automatic feature selection, deep learning models showed good performance in almost all domains. Deep learning networks can automatically learn needed features from the training data. Modern methods such as CNN, VGG models, ResNet, MobileNet, and others are used to automatically extract relevant features while being trained on image datasets.

Krishnaraj et al. [1] developed a fusion model using deep learning for CMFD and localization. They fused the outcomes of the GAN and DenseNet models as input to the Extreme Learning Machine (ELM) classifier. An artificial fish swarm algorithm is used to tune the parameters of the model. In [4], the authors have proposed a CNN-based model for copy-move and splicing forgery detection. The authors have converted the original images to Error Level Analysis (ELA). The ELA-preprocessed images are given to the VGG16 and VGG19 models for extracting the features, which are classified by a Softmax classifier with Root Mean Squared Propagation (RMSProp) optimization. In [6], the authors have created a serial deep learning detection and localization model to overcome the problems with the existing dual-branch Deep Neural Network (DNN) model, BusterNet. A serial network with a copy-move similarity detection network (CMSDNet) and source/target region distinguishment network (STRDNet) that are connected serially is introduced. CMSDNet detects similar regions in the image, and STRDNet distinguishes the tampered portions from the detected similar regions.

In [7], the authors presented a two-stage CMFD. First, a self-deep matching network is created as the backbone, which is constructed as an integration of atrous convolution, skip matching, and spatial attention. The backbone network creates a score map of suspected forged regions. The second is a keypoint matching method called Proposal SuperGlue. In [16], the authors used CNN to detect CMF. Three convolutional layers and two max pooling layers are used for extracting the

relevant features. Finally, a dense layer classifies the image as authentic or forged. RMSprop optimizer is used. The authors [20] developed an efficient approach towards CMFD and splicing forgery detection using Mask R-CNN and MobileNet V1. In [22], the authors used noise patterns as features to detect image forgery. The Fast Fourier Transform (FFT) transforms the image into the frequency domain. Using the Butterworth high-pass filter, only the high-frequency components, i.e., noise in the image, are extracted. Then an inverse FFT is performed to get the noise image. Then these noise patterns need to be encoded with the strength of orientation and edge information. For this purpose, LDRLBP is used. A Support Vector Machine (SVM) classifier is trained with FFT-DRLBP (Dominant Rotated Local Binary Patterns) descriptors to identify forged images.

The authors in [23] proposed AR-Net based on adaptive attention and residual refinement networks to detect CMF. Here, adaptive attention is used to fuse the spatial and channel attention features. Deep matching is done using self-correlation over the feature maps on multiple scales to locate similar regions. The authors have proposed a dense-inception-based CMF detection technique [24]. They claim that the proposed DNN-based solution is the first to detect untrained forgeries in the testing stage. Three Pyramid Feature Extractor (PFE) blocks are used to extract the dense features of the input image at multiple dimensions and multiple scales. Three feature correlation matching (FCM) modules are used to learn the correlation of hierarchical features. Finally, a Hierarchical Post Processing (HPP) module uses these hierarchical matching maps to obtain a set of cross-entropies. The authors have proposed a method to localise CMF by incorporating deep learning models. Here, the image and its binary localization map are given as input, which produces the tampering mask.

The author proposed an encoder-decoder model for CMFD [27]. First, the input image X is transformed into the DCT domain, which is further filtered to extract the low and high frequency components. Then IDCT is performed to obtain X_{low}, Xhigh, and X_{full}. With the ResNet architecture, U-Net is used as the encoder and decoder network structure. To highlight feature-channel relationships, these features are concatenated and fed into the Frequency Attention Module (FAM). Finally, region and edge prediction are derived from two individual convolutional layers. In [32], the authors fused both block and keypoint methods towards CMF detection and localization. Block- and keypoint-based fusion techniques are used for feature extraction. Here, Adaptive Over-Segmentation (AS) block-based and AKAZE and SIFT keypoint-based methods are used. Gray Level Co-Occurrence Matrix (GLCM), Gray Level Run Length Matrix (GLRLM), and Histogram are used for extracting the needed features. A SVM classifier is used for classification. The existing deep learning approaches are listed in Table II.

Table 2. Deep Learning based Methods

Ref	Methods Used	Dataset	Performance	Remarks
[1]	GAN, DenseNet, ELM Optimizer: Artificial Fish Swarm Algorithm	MNIST, CIFAR-10	Precision score of 97.25%, recall score of 96.46% and F-score of 96.06%	The proposed method for detection is not clearly explained. The fusion method is not mentioned.
[4]	VGG16, VGG19, ELA, Softmax Optimizer: RMSProp	CASIA-2.0, NC2016	Accuracy with ELA is 70.%, VGG16 is 71.6% and VGG19 is 72.9%	No testing is done to see what accuracy they will achieve without ELA.
[6]	VGG16 with fourth pooling layer replaced	Synthetic dataset, CASIA 2, CoMoFoD and	F-measure of 0.538, 0.511 and 0.677	Double attack testing is not mentioned.

	with atrous convolution, Pearson correlation BN-Inception, ASPP and attention mechanisms	COVERAGE		
[7]	VGG16, Atrous convolution, ASPP, Self correlation with Spatial attention	Synthetic dataset, MICC-F600, CoMoFoD, CASIA CMFD and MICC-F220	F1-score of 0.8216, 0.8312, 0.8059, 0.8118, 0.8412, and 0.7745 respectively for VGG16, ResNet50, ResNet101, MobileNetV2, MobileNetV3 and ShuffleNetV2	Double attack scenario testing is not mentioned.
[16]	3 LAYER CNN, Optimizer: RMSprop	MICC-F2000, MICC-F600, MICC-F220	Accuracy of 100%, F1-Score, Precision and Recall of 1.0.	Attacks are not tested.
[20]	MobileNet V1, Mask R-CNN, FPN	MICC-F600, MICC-F2000, COLUMBIA, COVERAGE, CASIA 1.0, CASIA 2.0, MICC-F220	F1-score of 70% on MICC-F600 for CMF and 64% on CASIA V1 for splicing. They also achieved an average precision of 90% on MICC-F2000 and COVERAGE for CMF and on COLUMBIA for splicing.	Testing on real-time images has not been done. Noise-related tests were not done. What if the image has a photo of twins? Will the method detect them as forgeries or authentic?
[22]	FFT, SVM, LDRLBP	CASIA 2.0, CoMoFoD, GRIP, CMH, CMEN, UNISA, IEEE IFS-TC	Average accuracy of 99.21%. Accuracy of 99.54% with CASIA 2.0, 99.13% with CoMoFoD, 99.74% with MICC-F220 and 97% with GRIP.	Double-attack testing is not mentioned, i.e., the image is scaled, rotated, and JPEG compressed.
[23]	VGG16, ASPP, Deep matching by self-correlation,	CASIA 2, Coverage, CoMoFoD	Precision of 58.32, Recall of 37.33 and F1 of 45.52 with CASIA 2. AUC of 0.8488 with Coverage. Precision of 54.21, Recall of 46.55 and F1 of 50.09 with CoMoFoD.	Some similar but genuine regions are identified as tampered by the method.
[24]	PFE, FCM, HPP	CMH, MICC-F220, MICC-2000, GRIP, Coverage, SUN, FAU, CASIA, Comofodnew		Double attacks are not tested.

[26]	Siamese Net, 4-Twins Net, 50 layer ResNet	CASIA, GRIP and USCISI	Accuracy of 97 with synthetic datasets and 91.56, 75.86 and 86.26 with USCISI, CASIA and GRIP	The model performed well on synthetic datasets, but it performed slightly worse on benchmark datasets. Attacks such as JPEG compression and noise are not tested with synthetic datasets. Multiple copy-move scenario testing is not mentioned.
[27]	DCT, ResNet, UNet, DFSAM, FAM	CASIA 1 and 2, Carvalho, Columbia, COVERAGE and IMD2020	CASIA v1 shows an F1-Score of 0.7730, CASIA v2 shows 0.7388, 0.9634 with Columbia, 0.6827 with IMD2020, 0.77 with Carvalho and 0.6910 with COVERAGE	The filter size was empirically derived based on the average synthetic region of the dataset. But, when forgery is applied in a wider sense, the filter size will be small compared to the forged region, and the features cannot be captured effectively.
[30]	Super-BPD segmentation, VGG16, ASPP,	USCISI, CoMoFoD and CASIA II	Precision of 59.11, a Recall of 57.69 and an F1-Score of 50.77 with CoMoFoD and a Precision of 57.48, a Recall of 51.25 and an F1-Score of 48.06 with CASIA II	The method is complex, with segmentation and a dual-branch structure. Forgery detection of similar but real regions was not tested. Also, multiple CMFs are detected, but there were some shadows due to similar backgrounds.
[32]	Adaptive over-Segmentation, SIFT, AKAZE, kNN	Image manipulation dataset (IMD), MICC-F220, COVERAGE, and GRIP	F1-Score of 99.5 with IMD, 99.53 with MICC-F220, 99.19 with COVERAGE and 99.56 with GRIP datasets	Rotation, scaling, and compression were not subjected to double testing. Testing is not done on real data. Testing to check for homogeneous regions simultaneously with the large scaling attacks has not been done.

5. CHALLENGES AND FUTURE SCOPE

Image forgery detection plays an important role as digital images are widespread everywhere. CMF and splicing are the two major passive techniques used to forge images. A lot of research is ongoing to find more accurate, efficient, and less complex methods to detect image forgeries. But still, there is a lot of scope for improvement. The feature extraction and matching stages of block-based methods are time-consuming. Key point-based approaches for CMF can detect forgery more accurately, but they suffer from high time complexity and fail if forgery is done on low-contrast regions or smooth regions. Block-based and keypoint-based methods have their own

strengths and weaknesses. A solution that can outperform all the existing methods in the literature in every working condition is not yet available.

Research can be incorporated to identify the limited number of relevant features needed, or some form of improvement can be made to the matching algorithms to reduce the time taken. Most existing CMFD methods are less effective in smooth regions of the image. Existing block-based and keypoint-based methods are incapable of providing effective feature extraction for homogeneous regions while also dealing with large scaling attacks. Also, the methods discussed in the literature so far are not efficient in differentiating tampering from retouching. Furthermore, existing detection methods only detect forgeries for which they were designed. They cannot detect other types of forgeries. Hence, there is a need for a unified detection method that can identify any type of image forgery.

Some research can be focused on extending the forgery detection mechanisms to detect forgeries in audio and video applications as well. Though methods with deep learning are widely used for detecting digital image fraud, these models appear to be complex. In the future, less complex and more accurate deep learning models may serve as the foundation for research. Optimizing the parameters of deep learning models requires a significant amount of effort. The CMFD methods incorporating CNN at the pixel level can be enhanced for improving performance accuracy, robustness, and differentiating the forged portions from the original ones. Now, the majority of researchers are concentrating on using deep learning for CMF detection. However, deep learning methods perform worse than block and keypoint methods because deep learning methods rely heavily on the amount and quality of training data available. In this digital era, CMF is performed in new ways with many unknown features not captured in training data. Also, these DL models require images to be reshaped to some specific size, which can result in the loss of image data.

6. CONCLUSION

The paper presents a comparative analysis of various CMF detection techniques. We have discussed the working stages of the copy-move forgery detection model. The detection approaches are categorised into block-based, keypoint-based, and deep learning-based. The paper summarises an overview of the recent research on these detection techniques. The paper also lists some fusion approaches involving keypoint and deep learning techniques. The challenges and the research directions to be focused on in the field of CMFD are discussed.

REFERENCES

[1] Krishanraj N, Sivakumar B, Ramya K, Yuvaraja T, Amruth R T, (2022) “Design of Automated Deep Learning - Based Fusion Model for Copy-Move Forgery Image Detection “, Hindawi Computational Intelligence and Neuroscience, pp. 1-13.

[2] Warif N B A, Wahab A W A, Idris M Y I, Ramli R, Salleh, R, Shamshirband S, Choo K R, (2016) “Copy-Move Forgery Detection: Survey, Challenges and Future Directions”, Journal of Network and Computer Applications, Vol. 75, pp. 259-278.

[3] Darem A, Al-hashmi A, Javed M, Abubaker A B, (2020) “Digital Forgery Detection of Official Document Images in Compressed Domain”, International Journal of Computer Science and Network Security, Vol. 20, pp. 115-121.

[4] Mallick D, Shaikh M, Gulhane A, Maktum, (2014) “Copy Move and Splicing Image Forgery Detection using CNN”, ICACC, 2022.Ansari et. al., “Pixel-Based Image Forgery Detection: A Review”, IETE Journal of Education, pp. 1-5.

[5] Ansari M D, Ghrera S P, Tyagi V, (2014) “Pixel- Based Image Forgery Detection: A Review”, IETE Journal of Education, Vol. 55, pp. 40-6.

[6] Chen B, Tan W, Coatrieux G, Zheng Y, Shi Y Q, (2021) "A Serial Image Copy-Move Forgery Localization Scheme with Source/Target Distinguishment", IEEE Transactions on Multimedia, Vol. 23, pp. 3406-3517.

[7] Liu Y, Xia C, Zhu X, Xu S, (2022) "Two-Stage Copy-Move Forgery Detection with Self Deep Matching and Proposal SuperGlue", IEEE Transactions on Image Processing, Vol. 31, pp. 541-555.

[8] Teerakanok S, Uehara T, (2019) "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis", IEEE Access, Vol. 7, pp. 40550-40568.

[9] Kaur C, Kanwal N, (2019) "An Analysis of Image Forgery Detection Techniques", Statistics Optimization & Information Computing, Vol. 7, pp. 486-500.

[10] Camacho I C, Wang K, (2021) "A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics", Journal of Imaging, Vol. 7, pp. 1-39.

[11] Qazi E U H, Zia T, Almorjan A, (2022) "Deep Learning-Based Digital Image Forgery Detection System", Applied Sciences, Vol. 12, pp. 1-17.

[12] Niu Y, Tondi B, Zhao Y, Ni R, Barni M, (2021) "Image Splicing Detection, Localization and Attribution via JPEG Primary Quantization Matrix Estimation and Clustering", IEEE transactions on Information Forensics and Security, Vol. 16, pp. 5397-5412.

[13] Anjali D, Sharma R, Roy A K, Mitra S K, (2021) "Keypoint based Comprehensive Copy-Move Forgery Detection", IET Image Processing, Vol. 15, pp. 1298-1309.

[14] Sunitha K, Krishna A N, (2020) "Efficient Keypoint based Copy Move Forgery Detection Method using Hybrid Feature Extraction", Proceedings of the 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 670-675.

[15] Aya H, Ahmed T, Mazen S M, (2021) "An Improved Copy-Move Forgery Detection based on Density-based Clustering and Guaranteed Outlier Removal", Journal of King Saud University – Computer and Information Sciences, Vol. 33, pp. 1055-1063.

[16] Hosny K M, Mortda A M, Fouda M M, Lashin N A, (2022) "An Efficient CNN Model to Detect Copy-Move Image Forgery", IEEE Access, Vol. 10, pp. 48622 – 48632.

[17] Babu T S B G, Rao S Ch, (2021) "An Optimized Technique for Copy-Move Forgery Localization using Statistical Features", Science Direct, ICT Express 8, pp. 244 – 24.

[18] Wu H, Zhou J, Tian J, Liu J, Qiao Y, (2022) "Robust Image Forgery Detection over Online Social Network Shared Images", IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 443 – 456.

[19] Kunj B M and Vipin T, (2019) "Image Forgery Detection: Survey and Future Directions", Data, Engineering and Applications, pp. 163-194.

[20] Kalyani D K, Ahirrao S, Kotecha K, (2022) "Efficient Apprach towards Detection and Identification of Copy Move and Image Splicing Forgeries using Mask R-CNN with MobileNet V1", Hindawi – Computational Intelligence and Neuroscience, pp. 1-21.

[21] Yue G, Duan Q, Liu R, Peng W, Liao Y, Liu J, (2022) "SMDAF: A Novel Keypoint based Method for Copy-Move Forgery Detection", IET Image Processing, Vol. 16, pp. 3589-3602.

[22] Asghar K,. Saddique M, Hussain M, Bebis G, Habib Z, (2022) "Image Forgery Detection using Noise and Edge Weighted Local Texture Features", Advances in Electrical and Computer Engineering, Vol. 22, pp. 57-69.

[23] Zhu Y, Chen C, Yan G, Guo Y, Dong Y, (2020) "AR-Net: Adaptive Attention and Residual Refinement Network for Copy-Move Forgery Detection", IEEE Transactions on Industrial Informatics, Vol. 16, pp. 6714 – 6723.

[24] Zhong J L and Pun C M, (2020) "An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection", IEEE Transactions on Information Forensics and Security, Vol 15, pp. 2134 – 2146.

[25] Uma S and Sathya P D, (2020) "Copy-move forgery detection of digital images using football game optimization", Australian Journal of Forensic Sciences, Vol. 54, pp. 1-22.

[26] Barni M, Phan Q T, Tondi B, (2021) "Copy-Move Source-Target Disambiguation Through Multi-Branch CNNs", IEEE Transactions on Information Forensics and Security, Vol. 16, pp. 1825 – 1840.

[27] Gu A R, Nam J H, Lee S C, (2022) "FBI-Net: Frequency Based Image Forgery Localization via Multitask Learning with Self-Attention", IEEE Acess, Vol. 10, pp. 62751 – 62762.

[28] Agarwal R, Verma O, (2021) "Robust Copy-Move Forgery Detection using Modified Superpixel based FCM clustering with emperor penguin optimization and block feature matching", Springer – Evolving Systems, Vol. 13, pp. 1-15.

[29] Yanfen G, Junliu Z, Chiman V, (2021) "A Novel Copy-Move Forgery Detection Algorithm via Feature Label Matching and Hierarchical Segmentation Filtering", Elsevier – Information Processing and Management, Vol. 59, pp. 1-21.

[30] Li Q, Wang C, Zhou X, Zhiliang Qin, (2022) "Image Copy-Move Forgery Detection and Localization based on Super-BPD Segmentation and DCNN", Nature Portfolio - Scientific Reports, Vol. 12.

[31] Baheesa F, Ghafoor A, Sohaib S, Riaz M, (2022) "FAST, BRIEF and SIFT based Image Copy-Move Forgery Detection Technique", Multimedia Tools and Applications.

[32] Kaur N, Jindal N, Singh K, (2022) "An Improved Approach for Single and Multiple Copy-Move Forgery Detection and Localization in Digital Images", Springer – Multimedia Tools and Applications.

[33] Tahaoglu G, Ulutas G, Gencturk B, Ulutas M, Nabiyev V, (2022) "Ciratefi based Copy Move Forgery Detection on Digital Images", Multimedia Tools and Applications.