DEVELOPMENT OF IMPROVED COPY MOVE IMAGE FORGERY DETECTION TECHNIQUES

By

Bisma Haider

00000274576/MSSE25

Supervisor

Brig Abdul Ghafoor

A thesis submitted to the faculty of Software Engineering Department,
Military College of Signals, National University of Sciences and Technology,
Islamabad, Pakistan, in partial fulfilment of the requirements for the degree of MS in
Software Engineering

August 2022

Copyright

DEDICATION

This thesis is dedicated to

ALL THOSE who raised my morale and prayed for my success

ABSTRACT

In this revolutionized world where images are being used as proofs, image authentication has become a challenge today. Easily available image editing tools and softwares have made it easy for people to forge an image. Some forgery techniques fail to detect small and overlapped forged region while other techniques are not able to accurately detect forgery if the forged part has undergone geometric transformations. To overcome these issues, this paper describes two proposed method to detect forgery for small, overlapped and multiple forged regions that has undergone geometric transformation. The duplicate detection approach and the robust detection method are combined in the first proposed copy-move detection. The features of each image block can be obtained differently using the two methods. The PCA is used as the image block features in the duplicate detection approach. The robust detection technique compares pixel values to determine the features in the second way. These qualities and attributes are kept in one container. A lexicographical sort is then used to order the container. The image block sets are then filtered to eliminate any pairs that don't reach a predetermined threshold. The remaining pair sets of an image block's coordinates are then used to construct an image of the detection result. The technique stands invariant to post region duplication process. The technique detects multiple and overlapped copy-move forgery. Second proposed method uses SIFT to detect keypoint features. DBSCAN clustering algorithm is then applied to cluster the matched groups. Afterwards, morphological operation is implemented after outlier removal process by median filter. Finally, forged regions are localized using Linear Spectral Clustering (LSC). Hence, the technique accurately detects multiple forged region with high efficiency and is invariant to scaling and rotation.

ACKNOWLEDGEMENTS

All praises be to ALLAH, Al-Muizz, Al-Kabeer, Al-Hadi and Al-Fattah

The successful completion of this thesis is accomplished by the devoted participation and cooperation of all guidance committee members. With gratitude and affection, I acknowledge- edge active and guided guidance of my honorable supervisor and co-supervisor, Brig Abdul Ghafoor, PhD and Dr. Muhammad Mohsin Riaz. They supported me in hours of need and channelized my way in hard times. Their motivation, guidance and supervision acted as the driving force that has enabled me to achieve my objective. I also admire and value participation of my respectable committee members; Assc Prof Dr. Naima Iltaf and Asst Prof Muhammad Imran for their time and advice. I am very grateful for the teachings of faculty members of Computer Software Engineering Department that has fueled my sense of continued determination over the years. I appreciate efforts of my all family members, friends and class fellows who raised my morale and their motivation opened new ways for me. Their prayers and ALLAH's help have enabled me to be the best version of myself.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

Human vision perceives visual imprints quite simply. When technology was more limited, the human brain was able to tell the difference between a fabricated image and an authentic one [13]. With technological breakthroughs, images have altered the globe. An image is worth a thousand words when it comes to conveying a complex idea [1]. They are therefore used as proof in court, in journalism, in health records, in bank records, etc. Additionally, technological advancement has made it possible for several image-altering programs to exist. These programs, like Adobe Photoshop, Corel Draw, and GNU image manipulation program (GIMP), are now commercially available for free or at a very cheap cost [14]. They allow editing in such an easy way that even a rookie user can actually build, alter and manipulate image without leaving any detectable evidence of these operations [13]. Data is manipulated to meet a specific requirement or to fabricate false information. This procedure degrades the data's legitimacy, making it more difficult to tell the difference between authentic and modified data. Because of their widespread use on the internet and social media, images have become a target for data falsification [33]. The use of image alteration software for various reasons of image tampering has become more convenient (e.g., shading selfie for pleasant visualization effects). Image forging is the practice of purposefully altering an image's data to make it appear to be a different object [2]. Image tampering is a form of image counterfeiting in which a portion or portions of an image's graphic content are altered [1]. Image manipulation has emerged as one of the most serious dangers, because the human eye has a difficult time detecting changes to graphical data. Forgers were able to conceal their tampering efforts with the use of new age technologies, making it difficult to tell when an image has been tampered with [20]. Humans have been shown in numerous studies [2] [3] to be unable to distinguish between a genuine and a forged image. Image manipulation [24] offers advantages, such as modifying

the graphical material on an image or video to enchant the human imagination, such as movies and ads. Aside from the fact that it might lead to legal issues in certain parts of the world, it has its drawbacks, including the need to detect manipulation in images. In order to prove the authenticity of a photograph in court, a solid forensic investigation is required [41].

1.1 Copy move forgery:

When an image's content is copied and pasted from one area to another, it is known as copy-move forgery. Technology, like the rest of the world, is advancing at breakneck speed. Using the internet to share data has never been easier than it is now, due to the advancement of new technology [30]. Instagram, Snap Chat, and WhatsApp popularity has skyrocketed because of these new technologies. The amount of data being exchanged on the internet is staggering. All kinds of data, including audios, movies, photos, and documents of all sizes, are part of the circulating data. It has become increasingly common for people of all ages to use digital platforms, which have become easier and more convenient to use [31]. The sharing of any data on these platforms was more convenient because it was so close to the user's fingertips [16]. The huge demand for data manipulation is a byproduct of the enormous use of data of all kinds. Over the course of the decade, this gave rise to a slew of data manipulation tools that may be used for good or bad ends, depending on the manipulation's goal [5].

1.2 Research motivation:

Nowadays where tampering is just few clicks away, sight has no longer stayed believing. In such a scenario, hiding truth, erroneously leading people, damaging someone's reputation by changing face, leading to wrong verdict by eliminating crucial items or persons from an evidence image is just few clicks away [9]. False photographs could be used in news reports to embellish the facts or deceive the public. The integrity of digital photos is now even more in jeopardy due to the prevalence of cheap, simple-to-use, yet effective desktop applications. This all is sending shockwaves in the digital world by leading to a serious situation where robust, precise and efficient counterfeit detection algorithms are needed to check image authenticity and trustworthiness [1] [7]. In order

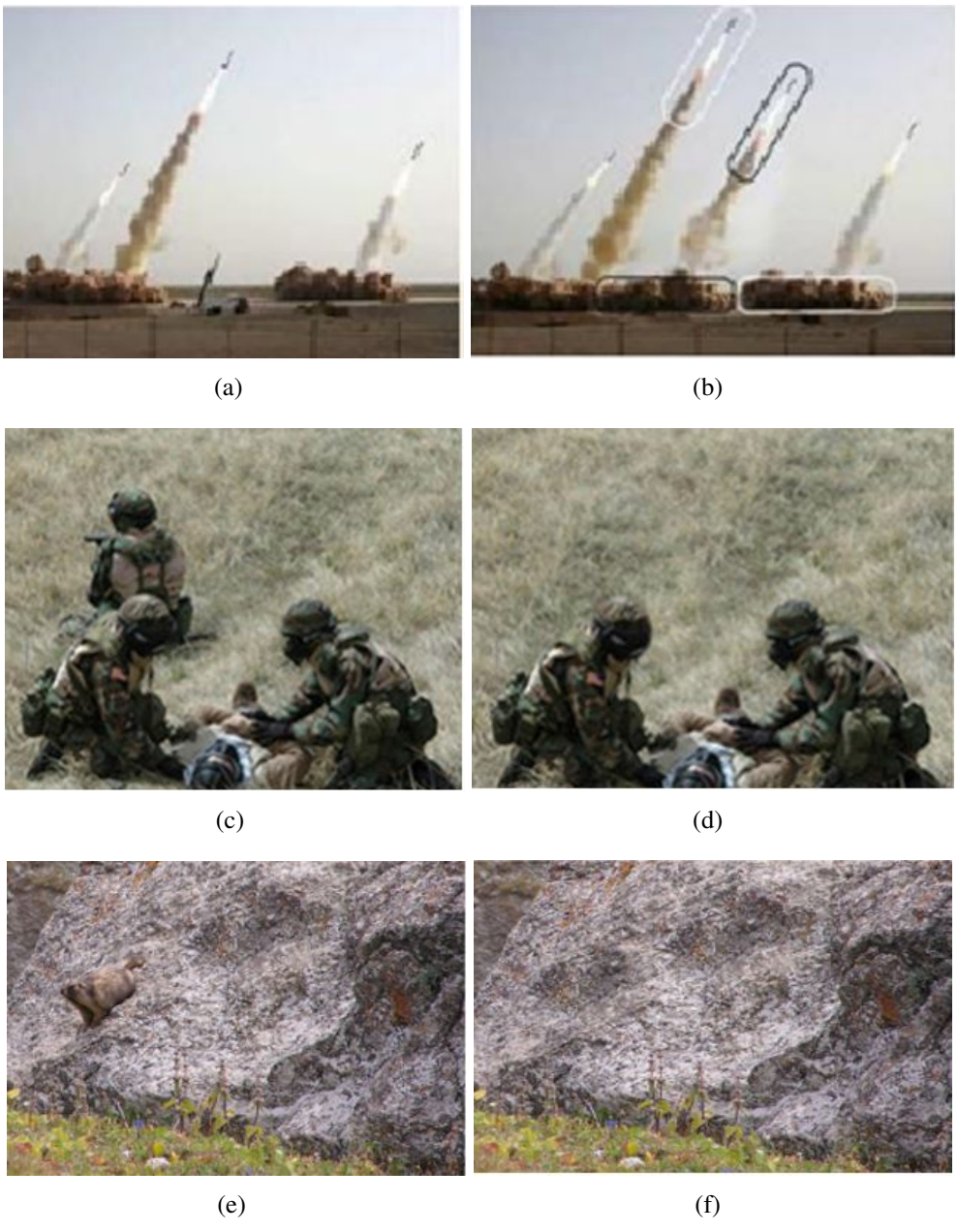


Figure 1.1: (a) Original image [18] (b) Forged image [18] (c) Original image [77] (d) Forged image [77] (e) Original image [77] (f) Forged image [77]

to investigate and completely examine proofs and signs left behind in digital data, such as digital photographs, as a result of an illegal effort, cyber-crime or forgery, digital image forensics [2] was developed. When a user does not have any prior knowledge of the data to be protected, it offers security and protection [8] [48]. Documents with images must be checked before making any conclusion for maintaining social stability and avoiding misjudgements [3] [9]. Some past examples show circumstances of copy move forgery detection (CMF). Iran has been held responsible of falsely altering an image from one of its missile tests almost ten years ago; the image was published in the press in July 2008, and Iran's Revolutionary Guard claimed that four missiles were fired and were shooting up to the sky concurrently, when in fact only three missiles were actually fired. The authentic and falsified versions of the photographs are shown in Figures 1.1 (a) and (b) correspondingly. Figures 1.1 (c) and (d) shows that a soldier was concealed in the image's background by copying and pasting it, however an item was then copied and pasted to change the image's item count. Same is the case with Figure 1.1 (e) and (f). Image forgery is a broad topic that is used in healthcare institutions to verify the validity of diagnostic exams and other related details to diagnose diseases as well as in courtroom to reject fake photographs as testimony to expose criminal activity. In order to solve the problem of the photos' lack of authenticity, image alteration should be avoided [21].

1.3 Problem statement:

Two methods are presented in this study for identifying the forged area in an image and demonstrating the validity and genuineness of images with higher F-measure (FM). It reduced CPU time when geometric changes and overlaps occurred. The first method is a PCA-based detection method. In this instance, the fabricated element is overlapped and repeatedly pasted, making it challenging to identify fraud, particularly when the faked part is too small. The second method, which is utilized in this work, is based on DBSCAN [73] [75] , and scale invariant feature transform (SIFT([35] to detect forgery in case of scaling and rotation. It employs an improved F-measure (FM) to demonstrate picture validity and originality while consuming less CPU time. In order to hide the

forging effects from the viewer, the forged region is regularly scaled, rotated, and pasted several times along with different operations like blurring, blending, compression, etc. in this case. Because of these processes, direct pixel mapping is no longer possible and is a laborious task. Some CMF detection algorithms discuss overlapping, scaling, some place a specific emphasis on rotation, and some take into account numerous clones, but there isn't a single method that addresses all these issues at once. A new method needs to be created in order to address each of these shortcomings. To lessen system complexity, two new, enhanced procedures have been created. To address the above stated problems the main objectives of this study are:

a) To recognize CMF if forged region is rotated, scaled, compressed and noisy using the proposed algorithm.

b) To detect small forged regions.

c) To diagnose copy move (CM) region with increased FM and efficiency.

d) To detect multiple and overlapped copy move parts.

e) To get better visual recognition of detected forged region.

f) To achieve more robustness.

1.4 Thesis contribution and dissertation organization:

For effective and accurate forgery region identification, two methods are suggested. The first model integrates pixel value comparison and Principal Component Analysis (PCA). The duplicate detection method first uses PCA as the image block characteristics. Pixel value comparisons are used in the robust detection approach to determine the attributes. The differentiating features of each approach are then collected into a single container for convenient access and storage. The block coordinate, the distinctive features of the first technique (i.e., the fundamental components), and the distinctive features of the second process (i.e., the pixel value comparison) are all stored in the container. After that, the container is arranged alphabetically. A filtering procedure is then used to remove any photos that do not meet a predetermined threshold. The next step is to create a detection result image using the remainder pairs of coordinates from each image block. Using this technique, copy-move forgeries that are multi-

plied and overlapped can be found. This approach allows for highly accurate forging region detection. The second method makes use of SIFT to extract features, which are subsequently grouped using the DBSCAN algorithm. Outliers are eliminated in post-processing, and then LSC segmentation is being used to optimize the findings. In the case of geometric transformations, this method excels. In comparison to state-of-the-art approaches, qualitative and quantitative study reveals that the suggested work has high FM and low CPU time.

This chapter serves as an overview, outlining the context, problem statement, goals, and importance of the study. This chapter also highlights the importance of copy move forgery detection. The remainder of this study is structured as follows. The thesis is divided into different chapters with numerous subheadings:

Chapter 2

The literature review is in the second chapter. This chapter serves as a refresher on the fundamentals of research. It reviews related studies that have already been published and evaluates their conclusions.

Chapter 3

The methodology of the research thesis is the subject of the third chapter. It explains why research methodologies and design are necessary. It explains the proposed method to overcome the issues.

Chapter 4

The results and findings are discussed in this fourth chapter. The analysis of these results, which includes a comparison to the literature and aids in the evaluation, is also provided in this chapter.

Chapter 5

The fifth and last chapter of the book. It restates the objectives, explains the results, and talks about the applications in real life, the limitations, and suggestions for further

study.

Chapter 2

LITERATURE REVIEW

As digital image forensics has grown in recent years, it is now possible to identify digital picture forgeries. In digital image forensics, the primary goal is to examine the images for the existence of forgeries using either active or passive (blind) techniques [54]. The active techniques such as watermarking and digital signatures rely on the information encoded in the photographs prior to their use. Active approaches, however, may not be used in practice because of the lack of knowledge. As a result, photographs that require no prior knowledge about them can be verified using passive techniques [10].

2.1 Types of forgery:

There has been a lot of digital picture falsification in recent years. Based on the steps taken to fabricate the fictitious image, each of these instances falls into one of three broad categories. Retouching, Splicing, and Copy-Move attack all fall under this category.

2.1.1 Retouching:

Color and tone correction, discoloration, and eye circles removal, as well as changes in brightness, contrast, and saturation, are all examples of photo retouching. 'Retouching,' in the context of post-processing and image editing in photography, is any procedure used to physically or digitally alter an image in order to improve the image's appearance. Figure 2.2 below shows the example of retouching.

2.1.2 Splicing:

Digital images can be altered by splicing, in which a portion of one image is put into another image. Images can be spliced together using image altering techniques such as local/global blurring, compression and scaling after the splicing procedure has been completed. Images from several sources are combined in a way called "image splicing" to produce a fictitious new image [44].

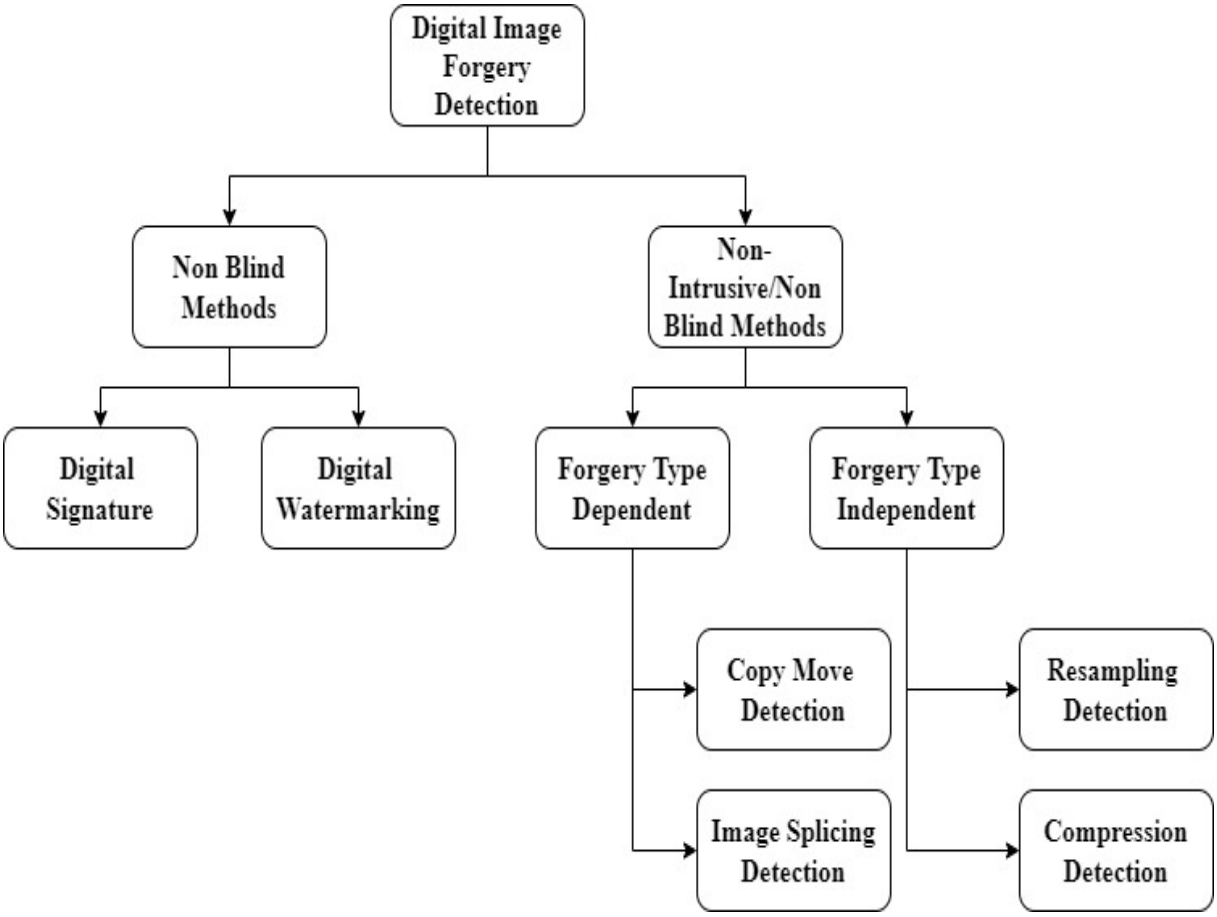


Figure 2.1: Classification of digital image forgery detection

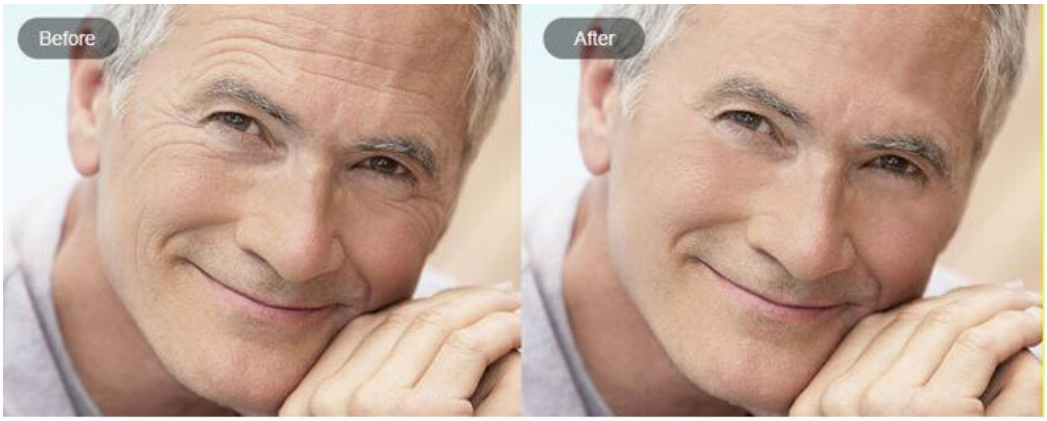


Figure 2.2: Image retouching [15]

2.1.3 CMF:

CMF [11] is tampering an image using the single image itself. A part is copied from the image and inserted in the same image followed by intermediate operations like rotation, scaling, reflection, chrominance and luminance changes. The image is then post pro-

Figure 2.3: Image splicing [16]

Figure 2.4: Copy move attack [17]

cessed by noise addition, JPEG compression, blurring or a combination of these [13]. Without any modification, such as affine transformations (like resizing, orientation, etc.) and parameter tweaks (i.e. brightness or contrast adjustments, background blending, retouching etc.), the CM region is simply pasted into the image [14]. Sometimes, the forger applies geometric and photometric transformations prior to pasting. This is plain CMF. Multiple CMF involves multiple pasting of copied region. After pasting, post processing operation [32] in image is done to make copied region to appear as original. Figure 2.4 is the example of copy move forgery attack.

2.2 CMF detection framework and techniques:

In the present era of images, the identification of image manipulation is a critical issue, making it important to verify its authenticity [59] [57]. To detect tampering in an

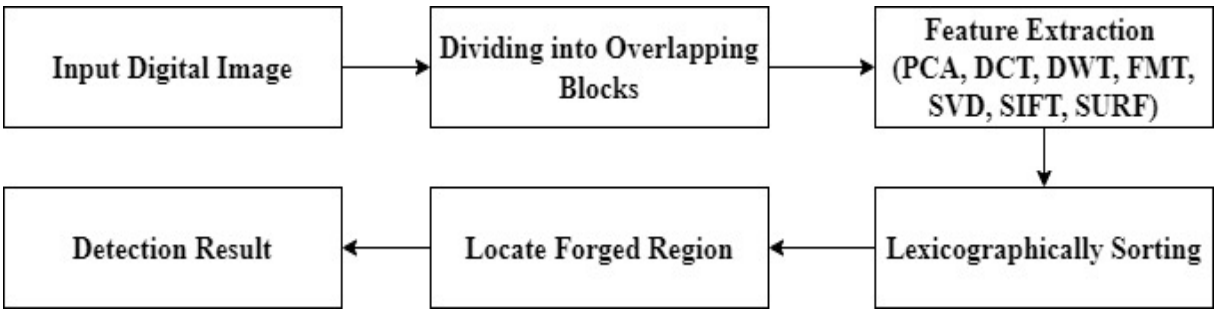


Figure 2.5: Basic process flow of CMF detection techniques

image, many detection methods have been developed, however they have not been able to detect other types. When it comes to detecting several sorts of image alteration, this has grown more difficult to do. Only a few features retrieved from the image have been presented for fusion to identify various tampering types on the image [46]. It's not just tampering detection that's the focus of some of the suggested fusion algorithms, but also a variety of manipulations. Image files in the JPEG format are some of the most commonly found and downloaded on the internet. Compression of an image using JPEG standards is known as JPEG compression [5]. In most cases, it is used to compress and store images in the JPEG format. When one alters a JPEG image, the tampered image is saved in the JPEG image, resulting in a second reduction in file size. The twofold quantization effect can be used to detect image manipulation in JPEG images that have been twice compressed [6]. For authentication, the altered images are used to extract special JPEG properties like discrete cosine transform (DCT) coefficients and Double quantization effects. Image tampering that does not originate in the JPEG image format was not addressed by these characteristics. Features invariant to JPEG compression are utilized in feature fusion to improve the reliability of tamper detection in JPEG images.

2.2.1 Block based CMF detection techniques:

Block based techniques split image into smaller blocks [47]. Features against each block are extracted using various methods i.e. moments based, dimensionality reduction based, intensity based, and frequency based etc. giving feature vector against each block. These blocks are matched using different methods. Lexicographical sorting [18]

is mostly used which is natural sorting based on alphabetical order; it helps to extracts similar block pairs. It brings similar blocks close to each other and their comparison takes less time. KD-tree, radix sort and other matching techniques are also in use [19]. The actual distance between matched blocks pairs is calculated to ensure that matching blocks might not be too close to each other. All block-based methods assume the size of blocks to be smaller than the size of doctored areas. As a result, very small tampered regions remain undetected because too much reduction of block size results in high computational time. These methods take more time to generate results but are more accurate than key point based methods [20].

2.2.1.1 Moment based method:

Lee at el. [71] proposed a blind forensic approach based on moment based method. A histogram is created after block segmentation of an image followed by Post-processing lexicographic sorting [31] of feature vectors and detection of duplicate image blocks. Experiment findings showed that this method was capable of detecting several occurrences of CMF and precisely locating the duplicated sections. The proposed method proved invariant to complex operation like scaling, rotation and translation [24] [25] and overlapped regions.

2.2.1.2 Patch match based detection:

Cozzolino et al. [28] developed a new technique for detecting and locating copy-move forgeries that makes use of densely calculated rotation-invariant characteristics [20]. The matching algorithm has improved in terms of its resistance to rotation and scale changes as a result of this modification followed by post processing strategy. According to the findings gained from testing the proposed was reliable and faster in many situations like scaling and rotation but didn't work in case of overlapped forged regions. Amiano et al. [6] extracted image features of videos which were invariant to various spatial, temporal, and intensity transformations. Afterwards, a video-oriented version of Patch Match [6] is used in conjunction with a multi resolution search strategy followed by post processing steps. A high degree of accuracy was achieved in the recognition and location of video copy-moves even in difficult settings using the pro-

vided strategy. This method remained invariance to all post processing operations like scaling, rotation and JPEG compression and didn't detect overlapped parts.

2.2.1.3 Dimensionality reduction-based methods:

Priyanka et al. [62] suggested a block-based DCT method. DCT on image blocks is applied after conversion of input image into grayscale and block wise segmentation. Singular value decomposition (SVD) is then applied followed by K-mean clustering. Finally, the forged regions are marked. The proposed technique was efficient in copy move forgery detection (CMFD) and provided robustness against transformations and high recall ratio. The resultant feature proposed in this paper can be further optimized by employing the convolution neural networks (CNNs) to improve robustness in case of geometric transformations and detecting overlapping doctored regions. Zhao at el. [8] presented a DCT based method. 2D-DCT and a quantization matrix are applied to each questionable image block followed by SVD. Feature vectors are then sorted and morphological open operation is applied to fill the holes in marked regions and remove the isolated blocks, then output the final detection result. The suggested scheme performed well in case of Gaussian blurring or additive white gaussian noise (AWGN) or JPEG compression or their combined processes and can detect multiple copy-move fraud. This method didn't work well in case of large compressions like scaling and rotation and overlapping.

Ahmed et al. [54] presented a block based method for copy move forgery detection. Initially image is divided into non-overlapping blocks after preprocessing it. Next, their means and standard deviations are calculated to get two different kinds of information. The feature vector matrix has been stored in lexicographic order for further use in locating pairings of comparable blocks after support vector machine (SVM) classifier. This method proposed better results but cannot identify and localize overlapping forgeries and didn't work in case of geometric transformations.

2.2.1.4 Frequency based methods:

Sharma et al. [19] presented a method based on three processes: feature extraction, Euclidian distance, and image marking. In the first step, discrete wavelet transform

(DWT) [70] and stationary wavelet transform (SWT) are combined. The gray level co-occurrence matrix (GLCM) algorithm is utilized for feature extraction using the Euclidian distance [13]. Lastly, morphological operations are used and to match and filter out the forged regions. The result showed that the presented method had high accuracy, peak signal to noise ratio (PSNR) and low mean square error (MSE) when it was compared to other method but didn't work in case of geometric transformations and overlapping. Hayat et al. [36] presented a combined DCT and DWT based CMF detection technique. The DWTed image must first be segmented, and each of those blocks must then have the DCT applied to it. In order to compare the blocks, correlation coefficients are employed. It turned out that the proposed approach, when compared to two other ways, produced some unexpected results. This method under performed in case of geometric transformation and didn't detect overlapped forged regions.

Li et al. [29] presented a CMFD system based on the polar cosine transform and approximate closest neighbor searching. The polar cosine transform's rotationally invariant and orthogonal qualities are used to extract robust and compact features from image patches. Once the patches with similar features have been identified, potential copy-move pairs can be discovered using an approach known as approximate nearest neighbor searching and implemented using locality sensitive hashing (LSH) [30] followed by post verification. It was found that the proposed approach was capable of producing accurate detection results, as well as a high level of robustness to various post-processing activities. This method failed to detect small and overlapped forged parts. Mahmood at el. [11] applied a CMD technique to the circular regions in order to better handle various post-processing activities that may occur. This method begins by computing the SWT of the preprocessed image. local binary pattern variance (LBPV) is implemented and finally features are matched and results are generated after filtering. In light of the findings, the proposed technique didn't detect forgery in case of scaling, rotation and non- affine transformations and didn't work for overlapped forged regions. Sheng at el. [42] introduced a method to detect forgery using ridgelet transform. The first step is to compute ridgelet transform on every sub-block and then computing the Hu-moments of every sub-block. Final step is to compute the Euclidean distance of

features corresponding to each pair of sub-blocks to find similar pairs. Even when photographs are compressed using JPEG, author's approach was effective at recognizing copy-move forged images, according to the results of experiments. This method failed to detect copy move forgeries in case of geometric transformations and other distortions like noise and blurring. Muhammad at el. [43] proposed a dyadic wavelet transform (DyWT) for the detection of copy move forgeries. The image is first decomposed using DyWT and then calculating Euclidean distance followed by block segmentation. Thus, pairs of blocks are arranged according to their high degree of similarity (LL1) and high degree of dissimilarity (HH1). The proposed stood invariant to all geometric distortions and failed in case of small and overlapped forged regions.

Khan et al. [4] proposed an approach using DWT for the detection of CMF. The compressed image is then split into overlapping segments of a predetermined size. If two blocks are similar to each other, the phase correlation criterion is used to determine which ones are similar to which others. At the end duplication map is used to demonstrate the forgery that has been discovered. The presented method had minimal CPU time and high accuracy of the procedure using this strategy. This method cannot find duplicate regions that have been resized or rotated through angles. Meena et al. [55] showed a method started by block wise segmentation followed by Tetrolet transform.. Each feature vector is then sorted using lexicographical order. Last but not least, the rotation-invariant and time-efficient outliers filtering strategy based on approximate nearest-neighbor searches is applied to MATCH LIST to remove the anomalies. The suggested method pinpointed copy-moved regions with high precision, speed and geometric alterations but didn't achieve results in case of non-affine transformations and overlapping.

Gani et al. [56] developed a reliable technique to extract features from each block using DCT. Following that, it is assumed that Cellular Automata will create feature vectors based on the DCT coefficients' sign information. In order to identify the duplicated portions in the image, feature vectors are matched using the nearest-neighbour searching technique based on kd-trees. The suggested technique performed remarkably well when post-processing effects were present. This method underperformed with affine

transformations and overlapping. Sekhar et al. [49] converted the input image into YCbCr color space. Features are then extracted using DCT after chopping the image into blocks. Finally, a lexicographic sorting of the feature vectors is used to make neighboring image blocks similar and to identify duplicated image blocks by comparing their Euclidean distance. The suggested method was capable of distinguishing between multiple copies of the same region in an image and even in the presence of minor rotations, JPEG compression and other minor distortions. This method was not able to detect major distortions, multiple and overlapped copy move forgery regions.
Kuznetsov et al. [50] proposed a new hash-based copy-move detection algorithm. A transform algorithm used in the second stage of this procedure (which does not include affine transforms). Adaptive linear contrast enhancement, image intensity range reduction, gradient computation, orthonormal basis expansion, and local binary pattern are just a few of the preprocessing methods that are put to the test. The proposed method's effectiveness was proved using a variety of fabricated photos in case of post processing operations. The method was not able to detect more complex forms of distortions and range of distortion parameters.

2.2.1.5 Hybrid schemes:

Hegazi et al. [74] presented a two-stage feature point detection scheme. In the first step, a feature point set for both regular and small smooth regions of the input image are settled. In the second step, feature points are extracted for both textured and smooth regions by using the multi-support region order-based gradient histogram (MROGH) and hue histogram (HH). MROGH is used for texture areas and the second one is used for smooth regions. Extracted features are then matched and falsely matched results are then filtered out. Finally, after the post processing step, a forgery detection map is generated to specify the doctored regions. This method performed well in case of joint photographic experts group (jpeg) compression and rotation but failed in case of high degree of scaling, translation, rotation and additive noise effects. Nguyen et al. [37] combined Radon transform with phase correlation technique. In the segmentation step, image is divided into overlapping blocks and RD is used for feature extraction which

are then stored lexicographically in order to reduce computational complexity. Finally, groups of same connected blocks are computed and the forged regions are located. Results showed that the presented technique was robust against rotation with the angles smaller than 4° and Gaussian noise addition with SNR values larger than 35 dB but didn't work in case of large angle of rotation, larger block size and overlapping parts.

Ardizzone et al. [27] employed triangles rather than blocks or single points, as in previous works. The image's focal points are detected, and triangles are utilized to model the objects that result from this identification. To match up the triangles, the local feature vectors produced from the vertices of the triangles and their shapes (interior angles) are utilized to align the triangles with one another. The scheme didn't work in case of affine, non-affine transformations and overlapping CM parts. Bayram et al. [3] proposed a method to use counting bloom filters as an alternative to lexicographic sorting. This is another frequent element of most suggested copy-move forgery detection techniques. The results of the experiments demonstrated that the proposed features were extremely effective in detecting duplicated regions, even when the copied region has undergone considerable visual modifications. The proposed method was far more robust to lossy compression, scaling, and rotation than previous methods but it was not able to detect forgeries in case of additive Gaussian noise and blurring type of operation, affine transformations and overlapped parts.

Moussa et al. [58] presented a technique with 2 stage algorithm. In the first stage, the five values of each pixel that arise from the calculation of the sum of the pixel intensities within each sub-block are saved in a feature vector. Feature vectors are then stored in a five-dimensional tree T (KD tree data structure) with 1-norm distance. In the second stage of the algorithm, input image is divided into non-overlapping blocks with a side length. For each node, the nearest neighbour node within the radius, corresponding to each block specified in previous step is determined. The corresponding blocks are marked as duplicates. The method was invariant to scaling and rotation and not able to detect multiple overlapped forged regions.

2.2.2 Keypoint based detection methods:

In contrast to block-based methods, image is viewed as a whole. Various feature detection and extraction techniques, including SIFT, Speeded-Up Robust Features (SURF), and others, are used to extract features from images. These descriptions and detectors retrieve edges, flat areas, or corners. Binary or string-based descriptors are both acceptable types of descriptors. Numerous matching algorithms are used for effective matching, including Best Bin First [11], Second Nearest Neighbour (2NN), Generalized Second Nearest Neighbour, and many others. They enable the use of feature vectors to locate matching keypoints [32]. Despite being less precise, these methods are faster than block-based CMF detection methods in terms of processing time. They also discover little altered areas. Emam et al. [34] outlined a technique using the scale invariant feature operator (SFOP) and MROGH descriptor which were used to describe the most important aspects of the story and generated a feature vector. In the feature matching step, kd-tree is used. To deal with multiple keypoints [10], generalized 2nd nearest neighbor (g2NN) method is used followed by random sample consensus (RANSAC) algorithm [71]. Finally, some morphological operations are done to obtain the final result. This method detected forgery in case of scaling but didn't work in case of rotation and multiple overlapped forgery.

2.2.2.1 SIFT based methods:

Hailing et al. [35] proposed a SIFT method which was used to detect copy-move fraud by keypoint features. The SIFT algorithm brings out unique features of local image patches which are invariant to scale and rotation and are robust to changes in noise, illumination, distortion and viewpoint. Forgery detection is improved by using the spearman relationship and ward clustering technique to determine the similarity between critical spots. The results of the experiments showed that the suggested method successfully achieved 99.56 percent accuracy and didn't detect small, multiple and overlapped forged parts. Liu et al. [59] proposed a CMF detection and location method combining both keypoint and patch match detection method. First keypoints are extracted using DOG. Two descriptors SIFT and local intensity order pattern (LIOP) are

then used for feature extraction followed by a new filtering strategy density grid based filtering (DGBF). The patch match is used to filter out the matched keypoints and to locate copy move forged regions. Aforementioned technique outperformed when compared to other techniques due to the combined descriptor but didn't detect multiple, overlapped and small forged regions.

Shandilya et al. [40] described a SIFT keypoint based CMF detection mthod. Division/segmentation of the image is done after keypoints extraction. Nearest neighbours of the block are then computed followed by D-distance computation. Euclidean distance algorithm is utilized to compute distance. Forged regions are then found after matching algorithm. The described method performed well on the detection of geometrically changed copy-moved image sections but didn't work for the identification of other forms of geometric transformations like reflection, as well as other image region transforms like grey level interpolation. Amerini et al. [18] proposed a SIFT based method for CMFD. These extracted keypoints are then matched using g2NN matching algorithm. To combine the matched keypoints, agglomerative hierarchical clustering is implemented. Afterwards, geometric transformations are estimated between matched and non-matched keypoints using affine transformation and finally mismatched points are filtered out using RANSAC algorithm [71]. This method worked well for geometric transformation parameters but didn't detect multiple cloning forgeries in case of uniform textured areas.

Su et al. [15] created low-dimensional feature descriptors by combining locality preserving projection (LPP) with the SIFT keypoints of an image. Keypoint matching is the last step. Lines are drawn between each matched keypoint pair in the image. These lines will obviously focus on two areas if the image has undergone copy-forged operations. Experiments showed that the suggested method was effective for post-processing forgeries including rotation, scale, and retouching as well as copy procedures. The future work will include to improve this method to make it valid in detecting copy forgery between different images. Shahroudnejad et al. [51] presented an affine scale invariant feature transform (ASIFT) based CMFD technique. The Presented method starts by finding matched ASIFT keypoints and then estimates all pixels within the duplicated

regions by using superpixel segmentation and morphological operations. The proposed scheme was efficient in case of severe transformations and common post-processing like adding noise and blurring but didn't detect forgery in case of grey level interpolation, JPEG compression and overlapping forged parts.

Huang et al. [25] segmented the forged image using simple linear iterative clustering (SLIC) and then used the SIFT to extract feature followed by clustering the key points. Helmert transformation is then implied to categorize these pairings depending on their spatial distance and geometric limitations. The zero mean normalized correlation (ZNCC) is used in matching step. Afterwards, authors improve forgeries and erase any errors or isolated sections by using morphological operations. Scaling, rotation, and compression forgeries can be more reliably countered with author's method. However, the current method was not robust against symmetric, recurring, overlapping and smooth patterns for forged regions. Meena et al. [63] utilized two strategies to find the counterfeit. After separating the first input image into flat and ridged sections, SIFT is applied. The g2NN algorithm is utilized in the matching phase, and then the outliers are eliminated using the RANSAC technique. In the second technique, the image is separated into blocks and the feature extraction is done using the Fourier-Melvin-Transform (FMT) with log-polar sampling. The generalized patch match technique is utilized for the matching process, while the dense linear fitting (DLF) algorithm is employed to filter outliers. The suggested method had very good results with several geometric changes and required less CPU time, however it failed with blurring, grey level interpolation, repeating, and overlapping.

JY Park et al. [64] proposed a method started by applying SIFT on the image to extract keypoints. Then a conventional 128-dimensional descriptor is generated. Next, pixel-wise local binary pattern (LBP) values are calculated for all the pixels in a 16×16 window centered at the keypoint location. Next, a histogram of the reduced LBP values is generated, and this 10-dimensional histogram is considered an additional descriptor. Both the descriptors are then combined. For the final output, the false matching removal step, followed by localization using the RANSAC algorithm [72] is performed. The proposed method didn't achieve results in case of geometric transformation and

multiple forged parts.

2.2.2.2 SURF based methods:

Sunitha et al. [38] described a hybrid feature extraction scheme. This method begins by dividing the image into equal patch or block size. Fusion method is used to extract features combining both speed up robust features (SURF) and SIFT. To match the extracted keypoints, agglomerative hierarchical clustering is applied and final step is to discard the false matches using RANSAC algorithm. This method was sensitive to post-processing effects such as noise and lossy JPEG compression, or even compound processing and overlapping. Xu et al. [39] made use of the SURF descriptors.. The SURF method comprises a keypoint detector and descriptor. Fast-Hessian Detector which is based on an approximation of the Hessian matrix for a given image point is used to extract keypoints. Before the keypoint descriptor is formed from the wavelet, the output of Haar wavelets is used for orientation assignment and finally forgery is detected. The mentioned technique was effective at detecting image region duplication and was resistant to both additive noise and blurring but didn't work on affine transformations, small and overlapped forged regions.

Wang et al. [17] presented an A-KAZE and SURF based technique for feature extraction. In the feature matching process, g2NN algorithm is used. K-d tree is used to perform g2NN which is based on Euclidean distance and used to evaluate similarity between keypoints. The affine transformation matrix is then computed using RANSAC. Finally, a new correlation coefficient map is calculated, filtering and mathematical morphology operations are combined. The proposed scheme was resistant to distortions and post-processing techniques such as noise addition and image blurring and was invariant to scaling and rotation and didn't detect overlapping. Liu et al. [59] discussed a SURF based technique. The SURF technique was used to identify significant features, and the kNN mapping algorithm was utilized to find similar features. The suggested method was superior to the typical SIFT implementation in terms of keypoint extraction from the suspected regions, the number of successful keypoint matched, and the number of incorrect matches but didn't achieve high accuracy and less CPU time.

Overlapping forged components were incompatible with the method.

Roy et al. [60] proposed the forgery detection methodology consisting of four major steps. First, keypoints are detected using SURF. After SURF, a 21×21 neighbourhood is selected and robust local binary pattern (RLBP) features corresponding to each SURF keypoints are then extracted in a circular neighbourhood. Then the RLBP histogram is taken as features. In the feature matching step, g2NN feature matching technique is applied. Next, an agglomerative hierarchical clustering is applied to identify possible similar areas. The approach was proven to be reliable in terms of the forgery's post-processing, although it didn't reach high precision, required little CPU time, or function on overlapped forged sections. Badr et al. [61] divided the entire grayscale image into four equal blocks to create a robust CMFD method. Each block's SURF features were then matched with one another using an NN searching algorithm to obtain matching keypoints. Next, the SLIC clustering algorithm with local colour feature (LCF) was applied to merge colour pixels in suspected regions (SRs) and obtain merged regions (MRs), and finally morphological close operation was applied. Robustness was demonstrated by running numerous tests against forgeries that included simple geometric adjustments, brightness alterations, colour changes, blurring, and noise additives. The presented method didn't provide results for small and overlapped forged regions.

Bilal et al. [73] developed a fusion technique for CMF identification. The fused features (SIFT and binary robust invariant scalable keypoints (BRISK)) are matched via hamming distance and second nearest neighbour after constructing a level-2 DWT, DBSCAN and RANSAC were then put into practice. The suggested method yields accurate and reliable results for single and multiple falsified areas even when post-processing attacks are evident with lower computational costs, but it failed to produce results for more complex post-processing attacks, such as increased scaling, smoothening, brightness change in the fraudulently portions, and overlapping. Studiawan et al. [16] presented a reliable duplicating approach. Using PCA and pixel value comparison, the differentiating characteristics are first calculated using this method. These features are then lexicographically recorded after which an outlier-removing filtering method is applied. This was not able to distinguish between tiny and overlapping doc-

tored portions and was invariant to all affine transformations.

Ramu et al. [52] put forwarded a hybrid block-based and feature point extraction-based technique. The input image is first subjected to DWT, after which super pixels are derived using SLIC. The (SIFT) technique is applied to the irregular blocks in order to obtain the features. The Dot products between unit vectors are then computed to match the characteristics. In addition, the (RANSAC) technique is used to find the counterfeit areas. The current method could not detect small and overlapped digitally altered portions and was insensitive to scaling and rotation.

This chapter discusses the types of forgery in detail. Explains the general framework for the detection of copy move forgery and already existing schemes related to copy move forgery, their basic methods, pros and their limitations. This chapter also presents the quantitative comparison of some existing techniques at the end of the chapter.

Table below summarises some of the existing schemes.

Table 2.1: Summary of the existing schemes

Techniques	**Pros**	**Cons**
SIFT and RANSAC [52]	Maximum features Detected	High FR (1.8)
Superpixel Segmentation and HT [25]	Refined CMF regions	High FR (1.94)
RD and Phase Correlation [37]	Improved robustness	High FR(2.032)
Self-Deep Matching and Super Glue [59]	Removed false alarmed regions	High FR(2.3)
AKAZE and Surf Features [17]	Detected duplicated regions	High FR (1.44)

Chapter 3

PROPOSED COPY MOVE IMAGE FORGERY DETECTION TECHNIQUES

There are two methodologies designed to detect forgery detection. First method is used to detect overlapped and multiple forged parts and the second method is proposed to detect scaled and rotated forged parts.

3.1 Proposed PCA-CMFD:

The robust detection method [66] and the duplication detection [67] are the two methods used in the design of the suggested method. Fist, both options are discussed before discussing suggested approach in the subsection that follows. This reliable duplicate detection method, which uses a block-based approach, is used to find overlapped forged parts.

3.1.1 Duplication detection technique:

Principal component analysis (PCA) [65] is used in the duplicate detection [67] method to identify the features of the image block. This technique initially creates overlapping blocks and each picture block's PCA is calculated, and it is regarded as a feature. In order to compute PCA for a color image, there are two options: either flatten the image block pixel to a two-dimensional array, or compute PCA for the features in the array [69]. Second, the block's eigenvalue to determine the number of dimensions is calculated. Then, by creating a new one-dimensional array, the principal component of an image block is ascertained [78]. Here is how the PCA approach is explained: Let's suppose, I be an input image of size $M \times N$ and an array storing the pixel values for a grayscale image is $L \times L$ in size. Where $L \times L$ is the size of overlapping blocks, which is 8 in this technique. Since PCA is used for dimensionality reduction [78], so let v_1^M be a D-dimensional vector of size M computed from an image I of size $M \times N$ and for the sake of simplicity, it's unit vector is defined and computed as $v_1^M v_1 = 1$.

Each image has it's data points, so let u_n be an image data point and $n = 1, 2, .., N$. This image's data point is then projected onto this new space $v_1^M u_n$. The mean of this projected data is:

$$\mu = v_1^M \bar{u} \tag{3.1}$$

where $\bar{u}$ is the sample set mean given by:

$$\bar{u} = \frac{1}{N} \sum_{n=1}^{N} u_n \tag{3.2}$$

Variance of the projected data is:

$$\eta^2(\bar{u}) = \frac{1}{N} \sum_{n=1}^{N} (v_1^M u_n - v_1^M \bar{u})^2 \tag{3.3}$$

where X is the data covariance matrix of the observed data of the image in original high dimensional space and is given as:

$$X = \frac{1}{N} \sum_{n=1}^{N} (u_n - \bar{u})(u_n - \bar{u})^T \tag{3.4}$$

The matrices are then sorted using a lexicographical manner according to the principal component of each image block in the following phase. As a result, image blocks with the same or comparable major components are situated adjacent to one another. The process then generates an array, incorporates it with a pair of the coordinates for the picture blocks. The process then calculates the offset of each array element. Every pair of coordinates in the array with an offset lower than the offset threshold which is set to 288, is discarded [16]. Additionally, the coordinate pairs with an offset magnitude lower than which is set to 25 are trashed out.

3.1.2 Robust detection technique:

The robust detection approach [66] determines how much of each image block's pixel value to utilize as its features. As a result of its repeated iteration over each pixel, this approach performs more complicated computations more slowly. Although the feature does not completely alter when a post region duplication takes place, this method is

more reliable when the input is a noisy or blurry image [16]. To begin, the $M \times N$ image is divided into $L \times L$ overlapping image blocks using this technique and L is set to 16 in this case. It's necessary to perform a feature extraction for each individual image block. RGB color space is used if the input image's color channel is not grayscale, so that the process can be more universal. The first three characteristics are then calculated $(c1, c2, c3)$. The sum of the red pixels is represented by $c1$, the total of the green pixels is represented by $c2$, and the sum of the blue pixels is represented by $c3$. There are no features assigned if the input image is a grayscale one. The approach then creates a variety of region borders, including vertical, horizontal, and diagonal borders, from each image block. Afterwards, it calculates the following four features $(c4, c5, c6, c7)$. Each feature's value is derived from the image's block. It calculates the following four features $(c4, c5, c6, c7)$

$$c_i = \frac{\sum(p_1(i))}{\sum(p_1(i) + p_2(i))} \tag{3.5}$$

where each region's parts p_1 and p_2 are derived whether it's horizontal, vertical or diagonal. The output then kept in an array along with each point for the image block. Additionally, lexicographical sorting is applied to order the matrix according to its seven features. As a result, the image blocks with the same feature are situated next to one another. The process then generates an array with the coordinates of an image block. The process also determines the difference between each feature and generates a histogram of a group of offsets. Only the offset with the highest frequency is used, and other coordinate pairs that don't match are discarded.

3.1.3 Robust duplication detection method analysis:

The division of the $M \times N$ input image into $L \times L$ overlapping chunks is a principle shared by the two approaches outlined above. Each image block's features are extracted after identifying the overlapping blocks from the image. The features of each image block can be obtained differently using the two methods. The PCA is used as the image block features in the duplicate detection approach. This approach is quite fast; however, it does not work well if the input image is noisy or blurry. The absolute value

is obtained from the offset computation in this manner. The same offset can be applied to a block with a negative distance. Tolerance is given to this procedure because of this absolute method. Due to the high tolerance, it is possible that a pair of blocks with the same offset value will be too close together, even if this is a false positive. The robust detection method offers comparing the pixel values to determine the features as the second approach. Using this method requires multiple memory accesses to acquire a single pixel value, which makes it significantly more time consuming. An offset frequency is measured using a histogram, then the offset with the highest frequency is taken. Because only one offset is chosen from a set of offsets, the approach can only discover one region of duplication [16]. However, even with no preprocessing, this approach is capable of working with photos of low quality. An image with a lot of noise or that has been blurred are two examples of low-quality input images. This is possible due to the fact that the characteristics are regarded to be resistant to image modification. The average method of blurring, for example, does not alter the region's overall number of pixels. Because the pixel value is compared to the characteristic feature value, the value is the same or similar to the characteristic feature value due to the fact that the overall number of pixels in the area stays the same. Because of this, the procedure can be regarded reliable. The proposing solution fixes the flaws of the others. In the first technique, the absolute operation from the offset calculation procedure is thrown away. Using this technique, the offset range can be extended or reduced (formerly only zero to infinity because of the absolute process). This offset must be able to distinguish between offsets with the same value but different types in order for it to be accurate (i.e., positive or negative). The second method, on the other hand, selects only the one offset with the highest frequency out of all possible offsets. The offsets that can be selected are then restricted by a frequency threshold variable. In this case, more than one offset is taken, as long as they all have an offset frequency greater than the threshold.

3.1.4 Proposed robust duplication detection method:

A new strategy is developed that combines two already-improved procedures while building a tolerance between them, preventing one method from ruling the other. This tolerance strategy applies a rounding procedure to the distinguishing characteristics, allowing almost all of them to participate in lexicographical sorting [68]. The robust-duplication detection procedure is shown in Figure 3.1 In order to begin the proposed copy-move detection, characteristic features from each of the two approaches are computed and simultaneously stored in a single container. As a result, the container includes three pieces of information: the block coordinate, the principal components from the first technique, and the characteristic features from the second method (i.e., the pixel value comparison). Each distinguishing feature undergoes a rounding procedure in order to achieve a particular level of precision. This round process appears to reduce the accuracy of each technique. However, every method's loss of dominance results in the development of a tolerance. Note that their characteristics have a lower precision. The tolerance effect is advantageous when features are sorted. After that, the container is ordered lexicographically according to the value of the features obtained from each approach. The close proximity of the image blocks with similar distinctive features throughout the sorting process suggests that those blocks may be identical or at least quite similar. Then pair sets of an image block from the sorted result is created that is close to another within a predetermined neighbouring distance threshold because identical or similar image blocks are always close to one another. The image block sets are then filtered to eliminate any pairs that don't reach a predetermined threshold. Only a pair of an image block that are further suspected to be identical or at least comparable remain after this filtering. At last, each coordinate of the remaining pair sets in an image block is used to construct an image of the detection result.

3.2 Proposed SIFT and DBSCAN method:

This proposed technique is feature based technique and proposed to detect scaled and rotated forged part. In this technique, SIFT feature extractor is used along with DBSCAN clustering [74] for the clustering the same features. It will help in forged

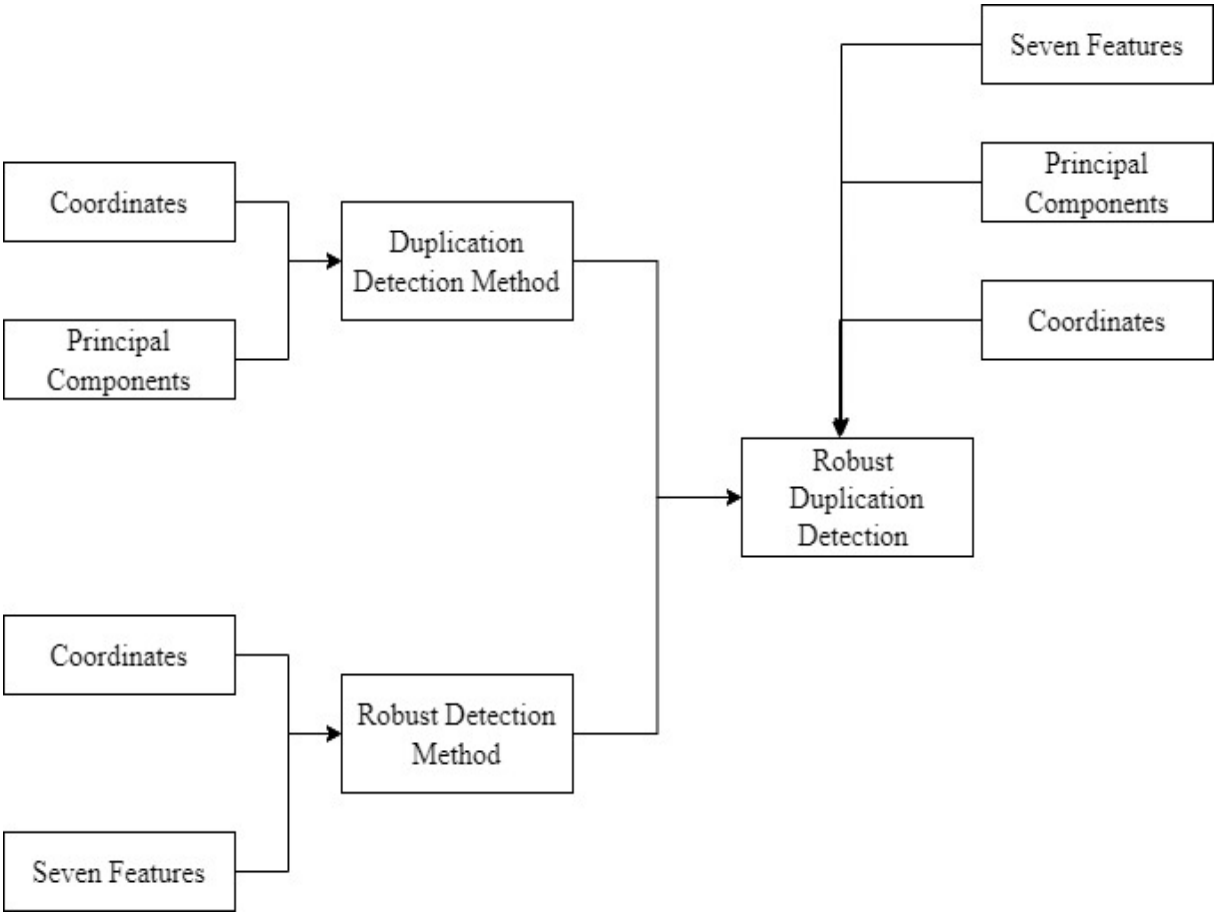


Figure 3.1: Block diagram of proposed PCA-CMFD method

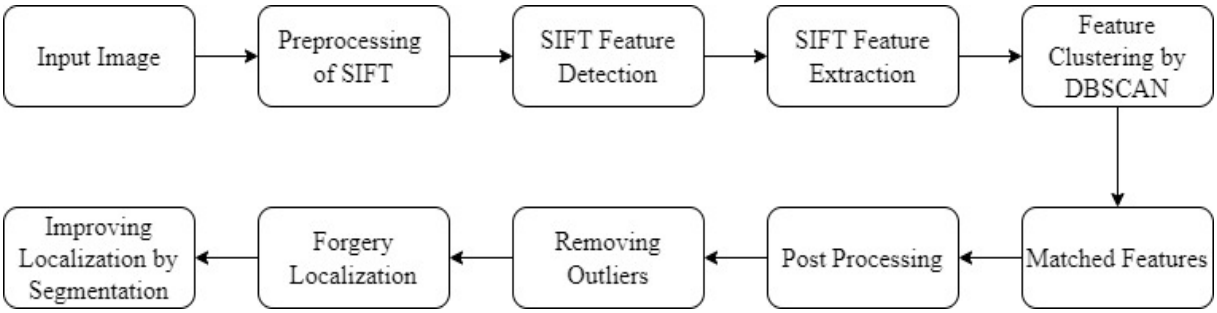
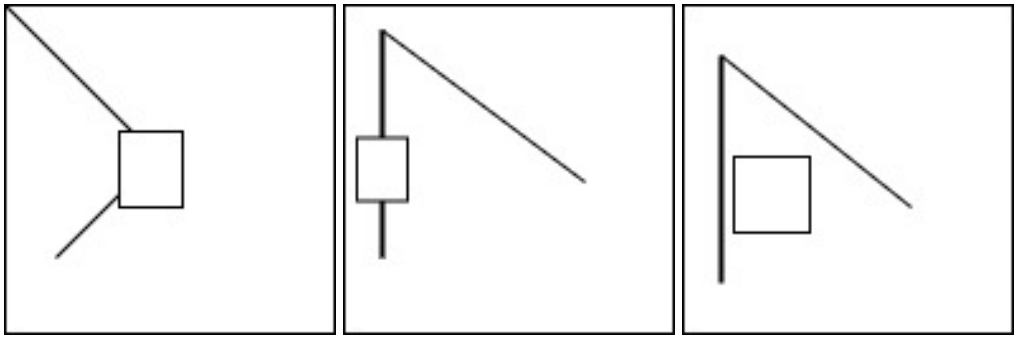


Figure 3.2: Block diagram of proposed SIFT and DBSCAN method

detection even the figure is rotated and scaled. An improved CM image forgery detection technique is proposed to detect CMF effectively in different cases (i.e. scale, rotation, illumination, brightness, contrast changes and noise addition).

Feature detectors:

The method of locating important areas in a picture by examining the distribution or consistency of the image's pixel grey levels (intensity values) is known as feature detec-



(a) (b) (c)

Figure 3.3: (a) Corner (b) Edges (c) Flat region

tion. They can be recognized in pictures by looking out a variety of windows. Corners (a), Edges (b), and Flat areas make up a picture (c). Flat areas retain their intensity, edges only modify it in the edge direction, and a corner point modifies intensity in all directions. Some feature detectors focus on the edges of the images, while others take corners into account or search for flat areas [83]. The most effective feature detectors for CMF detection are chosen.

Feature descriptors:

The best feature detectors or features for CMF detection are chosen. The best feature descriptors will yield impressive results when used against these feature detectors. Following are qualities of good feature descriptors (feature vectors):

1. **Replicability**: Features should retain their distinctiveness despite changes in the geometry and lighting conditions.

2. **Saliency:** Every feature must need a distinctive description.

3. **Efficiency and appropriateness:** Features should be few but comprehensive.

4. **Specificity:** Features should take up a tiny portion of the image and remain visible in the presence of clutter and occlusion.

3.2.1 Preprocessing of SIFT:

Preprocessed grayscale image $\breve{I}$ is provided to SIFT as an input. Key points are generated with certain steps.

3.2.1.1 SIFT feature detector:

The input image is converted into several smoothing versions by convolving it with a Gaussian function in order to produce features that are scale- and rotation-invariant. This is done by creating the scale space representation of an image [79]. Let $Z(u, v)$ be the part of the preprocessed grayscale image $\breve{I}(U, V)$ with coordinates u and v. Scale space representation of the image is then illustrated by:

$$N(u, v, \sigma) = G(u, v, \sigma) * Z(u, v) \tag{3.6}$$

where $N(u, v, \sigma)$ is the blurred image, $G(u, v, \sigma)$ is the Gaussian filter, $I(u, v)$ is the image. σ is the scaling parameter or the amount of blur. By increasing sigma, more and more details are removed from the image i.e. more blur [79].

The Gaussian filter is defined below:

$$G(u, v, \sigma) = \frac{1}{2\pi\sigma^2} e^2 \frac{-(u^2 + v^2)}{2\pi\sigma^2} \tag{3.7}$$

3.2.1.2 SIFT feature extraction:

Difference of gaussian (DOG) is then used to get stable feature points. The majority of dominating key points that hold steady after repeated soothing operations are considered potential key points. Taylor series on scale space is used to obtain scale and rotation invariance to all kinds of geometric and affine transformations. Extrema points with potential values below a predetermined threshold are rejected, leaving stable dominating key points in their place. Scale space extrema in the difference of the Gaussian function are used to identify keypoints [80]. When two different σ are used to blur an image, the difference of Gaussian is achieved. Let's assume that the two scaling/blurring parameters are $\sigma 1$ and $\sigma 2$. This procedure is carried out for various image octaves in the Gaussian Pyramid. [80]. Difference of Gaussian function is then computed as:

$$f(u, v, \sigma) = G((u, v, \sigma 2) - G(u, v, \sigma 1)) * Z(u, v) \tag{3.8}$$

(a) Input image (b) Ground truth

Figure 3.4: SIFT feature detector

$$f(u, v, \sigma) = N(u, v, \sigma 2) - N(u, v, \sigma 1) \tag{3.9}$$

$$\kappa(u, v) = \sqrt{(N(u+1, v) - N(u-1, v))^2 + N(u, v+1) - N(u, v-1))^2} \tag{3.10}$$

Orientation is assigned to each key point, $N(u, v)$; this assignment makes them invariant to rotation. In orientation assignment step, gradient magnitude and direction for each keypoints are calculated using finite differences [80]. Let $N(u, v)$ be a point of an image $\breve{I}(U, V)$, gradient magnitude and direction for this point is computes as::

$$\theta(u, v) = \tan^{-1} \frac{N(u, v+1) - N(u, v-1)}{N(u+1, v) - N(u-1, v)} \tag{3.11}$$

A 16 x 16 window is applied around each identified key point in order to produce extremely identifiable descriptors that can withstand changes in viewpoint and illumination. The image $\breve{I}$ is broken further into 16 subblocks, each measuring 4 by 4. A 128-dimensional feature descriptor is produced by 4 x 4 subblocks with 8 dimensional histograms against each subblock. Gradient orientations are used with feature vectors. Gradient orientations also vary when an image is rotated. By deducting the direction of each gradient from the orientation of the key point, rotation invariance is attained. The gradient orientation then changes to be relative to key point orientation.

Figure 3.5: Features clustering

3.2.1.3 Feature matching and clustering:

For densely packed points (those with a large number of adjacent neighbors), it uses a nonparametric technique for clustering, and outliers (those located alone in low-density areas) are marked as such (whose nearest neighbors are too far away). The DBSCAN [75] method basically requires 2 parameters. In order to be deemed a component of a cluster, a point's eps value must be less than a certain threshold. It signifies that two points are considered neighbors if their distance (in eps) is less than or equal to this value. Dense regions can be formed with as few as $minPoints$ points. If the minPoints option is set to 2, then a dense region must have at least 2 points. Now, two functions are written for constructing clusters and detection of forgery utilizing those clusters. This function will conduct DBSCAN clustering [76] [81] and the role of parameters $(eps, minsample)$ is mentioned above, it take another parameter which is basically SIFT descriptor of the image. For DBSCAN clustering algorithm, neighborhood of a point needs to be determined. This algorithm starts with an arbitrary point c, find all points that are density reachable from c. Cluster is found if c is a core point, if c is a border or noise point then no point is be reachable from it [81]. Let c and e be the two points of an image $\breve{I}$, with coordinates (u_1, v_1) and (u_2, v_2) where $(u_1, u_2) \in (U)$ and $(v_1, v_2) \in (V)$. The neighborhood of a point c is defined as:

$$N_{\in}(c) = e \in (M) : d(c, e) \leq \in \tag{3.12}$$

where $N_{\in}(c)$ denotes the neighbourhood of the point c if the distance between these two points c and e is less than the threshold value which is 60 in this case. A point c is directly density reachable from point e if point c belongs to the neighbours of point e. Let C_1 and C_2 be the two clusters, c be the part of first cluster and e be the part of second cluster, two clusters are merged if they are close enough [81]. Cluster distance is calculated as:

$$d(C_1, C_2) = \min_{c \in (C_1), e \in (C_2)} d(c, e) \tag{3.13}$$

In order to identify the forgery in an image, call locate forgery (img, clustering, and kps). This method uses image clusters and SIFT key points. It achieves it by creating lines between points grouped into the same groups. A verification procedure using a linear least squares solution for the parameters of the affine transformation [82] connecting the model to the image is then undertaken for each cluster that has been discovered. As can be seen below, the affine translation of the model point to the corresponding image point is given: Let $c(u_1, v_1)$ be the part of the found merged cluster and $(u_1, v_1) \in (U, V)$ and (o, p, q, r, s, t) are scalars for affine transformations [82], then the translation of the model (T) is defined by as:

$$T = \begin{bmatrix} ou_1 + pv_1 + q \\ ru_1 + sv_1 + t \end{bmatrix} \tag{3.14}$$

Pure scaling on the found cluster part is done, if $(p, q, r, t) = 0$.

$$T = \begin{bmatrix} ou_1 \\ \\ sv_1 \end{bmatrix} \tag{3.15}$$

The above equation shows that the found clustered part is purely scaled. Pure rotation on the found clustered part can be obtained if $(os = cos\theta)$, $(p = -sin\theta)$, $(r = sin\theta)$ and $(q, t) = 0$.

$$T = \begin{bmatrix} u_1 \cos\theta - v_1 \sin\theta \\ u_1 \sin\theta + v_1 \cos\theta \end{bmatrix} \tag{3.16}$$

Any number of additional matches can be added to this equation, each adding two rows to the first and last matrices. A solution can be found with a minimum of three matches.

3.2.1.4 Forgery detection localization and outlier removal:

Following stages further enhance identification of counterfeit regions that have been found. By using median filtering, rough edges are transformed into smooth edges. Hole filling is used to fill empty spaces.

3.2.1.5 Improving localization by segmentation:

After morphological processing, super pixel segmentation is performed using linear spectral clustering (LSC) for better localization of forgery region. It divides image into meaningful and dense super pixels with low computational cost. It uses normalized cuts to segment the image considering both color and spatial similarity between image pixel values preserving global image properties. Therefore, traditional Eigen based algorithm is replaced by approximate similarity metric which maps image to high dimensional feature space. DBSCAN clustering is also applied iteratively for better formation of segments. The detected image can be rotated or scaled as per the input features detectors. This algorithm can detect all three types of copy move forgery.

This chapter explains the need of the proposed schemes, highlights the issues of the existing techniques and then proposed two method to overcome the existing issues. First scheme is based on PCA and pixel value comparison. This is a block based technique used to detect the small and overlapped forged parts. The second one which is feature based uses SIFT and DBSCAN clustering for the detection of forgery.

Chapter 4

RESULTS AND ANALYSIS

4.1 Simulation setup and parameters :

Experiments are carried on a device with 2.70 GHz Intel(R) Core(TM) i7-7500U CPU, dual-core processor and 8.00 GB RAM using Jupyter Notebook on Windows 10 Pro Education. Qualitative and quantitative comparisons are recorded. FM and CPU-time in seconds of test images is stored. Qualitative analysis deals with comparison of visual qualities of results while quantitative analysis tells accuracy of results in numbers.

4.2 Datasets description :

Many academic datasets are available for detecting CMF, each covering different modifications of copied area [38]. They help in checking the effectiveness of CMF schemes in case the copied region is translated, scaled, rotated, compressed etc. To show the effectiveness of proposed technique with qualitative and quantitative analysis, datasets by [57] and [43] are used. Dataset by [31] contains images of 1000 × 700 or 700 × 1000 with corresponding GT images and is categorized in three subsets named as D0, D1-2 and D3. D0 contains only translated copies of pasted region, D1-2 is targeted to elaborate scale and rotation invariance. D0 includes 50 forged images, D1-2 is composed of 20 images to check rotation and scale changes. D1-2 covers rotation in ranges, [-25o, 25o] with step of 5o, [0o, 360o] with step of 30o and [-5o, 5o] with a step of 1o. Scaling is done in range [0.25, 2] with step 0.25 and [0.75, 1.25] with step 0.05. Every tampered image also contains corresponding binary mask. D3 contains pristine images without forgery.

4.2.1 CASIA dataset :

The modified CASIA dataset is constructed for the purpose of doing research on a variety of problems, including picture tampering detection, perceptual image hash, and user-device physical unlovable function, among others. The ground truth images were

Table 4.1: Dataset description

Dataset	Composition	Size	TR
MICC-F220	110 OI, and 110 TI	800 × 600 pix	1.2%
MICC-F2000	1300 OI and 700 TI	2048 × 1536 pix	1.12%

retrieved from the CASIA ITDE v1.0 database. CASIA image tampering detection evaluation database. This database includes pictures from eight different categories, including animal, architecture, article, character, nature, plant, scene, and texture, and their dimensions are either 384 x 256 or 256 x 384. Instead of directly using the tampered image set from CASIA ITDE v1.0, the tampered versions of those authentic images are selected from CASIA ITDE V2.0. These are more difficult and comprehensive tests because they take into consideration post-processing techniques such as blurring or filtering over the tampered regions to make the tampered images appear realistic to human eyes. The CASIA ITDE v2.0 dataset may contain several altered versions of the same authentic image, even though there is only one original.

4.2.2 MICC-F220 & 2000 dataset :

Hailing et al. [35] brought forward copy-move forgery dataset which contains 80 forged images with corresponding ground truth images. Images are kept of 768 × 1024 pixels having arbitrary sized forged regions as small as 1% of the image. The dataset does not cover scale and rotation changes. 30 test images taken from these datasets are of varying nature. The most prominent and useable datasets in the evaluation of copy-move forgery detection algorithms are MICC-F220 and MICC-F2000. These dataset details are provided in Table below. The altered photos in the MICC-F2000 dataset are classified into four categories based on the tampering activities they've undergone.

4.3 Test images:

20 images covering translated versions of copied region are taken from MICF2000 and MICF220. This set is named as Test images with 6 simple, 6 rotated and 6 scaled images.

4.3.1 Qualitative comparison of all strategies:

The copied part in image 1 is part of background and a detailed region. Ahmed et al. [54] has marked false matches with no accurate CMF detection and no CMF detection in case of scaling and rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected copied region with many false matches and no CMF detection in scaled and rotated images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52].

The copied part in image 2 is an object. Ahmed et al. [54] has marked various false matches in simple and scaled images and no CMF detection in case of rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected copied region with many false matches and no CMF detection in scaled and rotated images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52].

The copied part in image 3 is an object. Ahmed et al. [54] has marked false matches with no accurate CMF detection and no detection in case of scaling and rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected copied region with many false matches and

(a) Input Image I

(b) *Ahmed et al.* [54]

(c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD

(e) Proposed SIFT-DBSCAN

Figure 4.1: (a) Input simple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I

(b) *Ahmed et al.* [54]

(c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD

(e) Proposed SIFT-DBSCAN

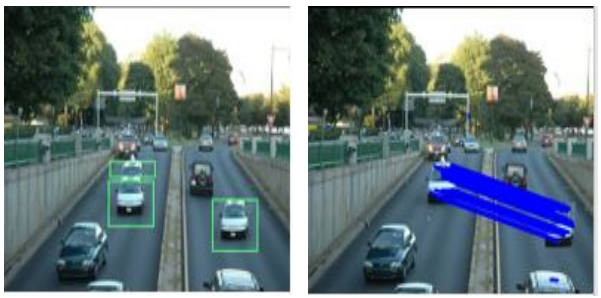
Figure 4.2: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.3: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]



(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.4: (a) Input simple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.5: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.6: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

no CMF detection in scaled and rotated images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52].

The copied part in image 4 is a blurred object. Ahmed et al. [54] has provided accurate CMF detection in simple tampered and no CMF detection in case of scaling and rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected accurate copied region in case of simple tampering and no CMF detection in scaled and rotated images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52] .

The copied part in image 5 is an object. Ahmed et al. [54] has marked no detection in simple tampered image and also no CMF detection in case of scaling and rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected no copied region in scaled, rotated and simple tampered images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery

(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

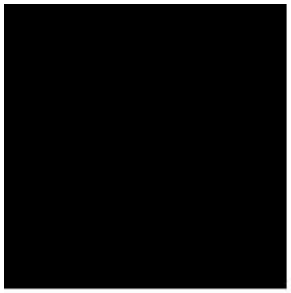
Figure 4.7: (a) Iimple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

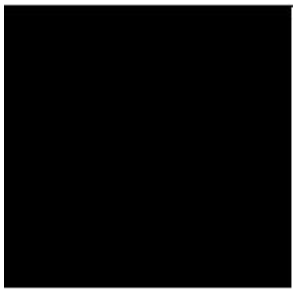
(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.8: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I



(b) *Ahmed et al.* [54]



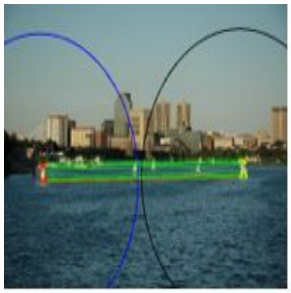
(c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD

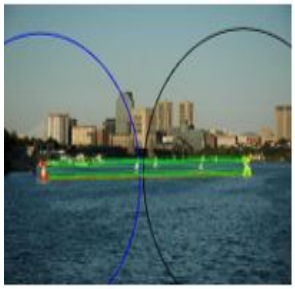
(e) Proposed SIFT-DBSCAN

Figure 4.9: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

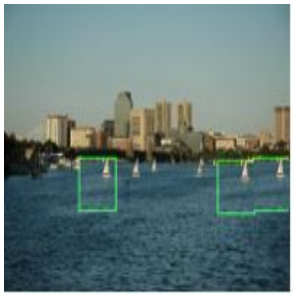
(a) Input Image I



(b) *Ahmed et al.* [54]



(c) *Ramu et al.* [52]



(d) Proposed PCA-CMFD

(e) Proposed SIFT-DBSCAN

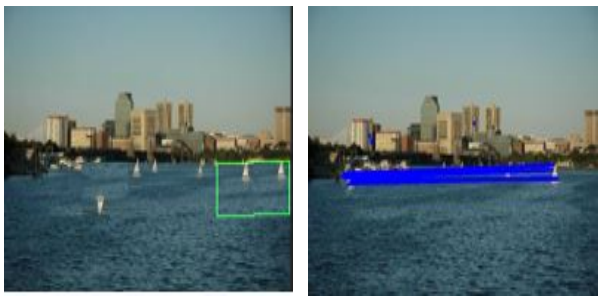
Figure 4.10: (a) Input simple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.11: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

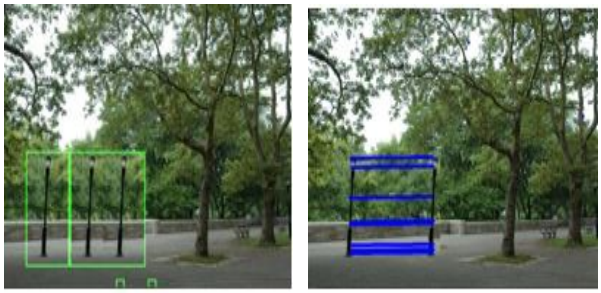
(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]



(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

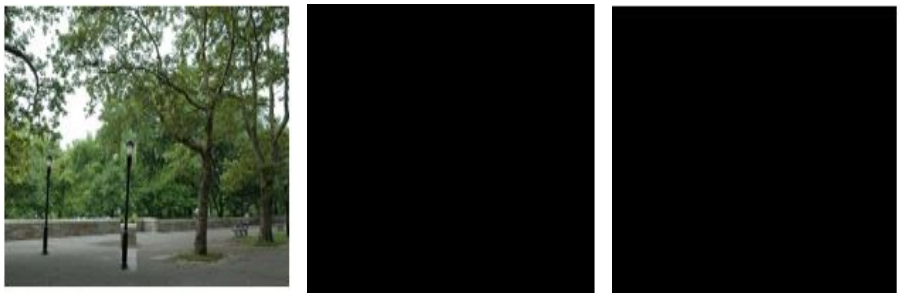
Figure 4.12: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

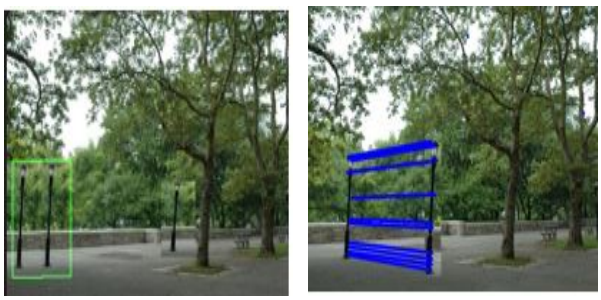


(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.13: (a) Input simple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

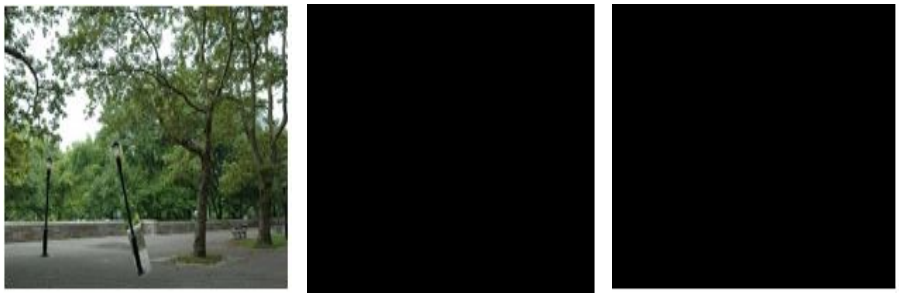


(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

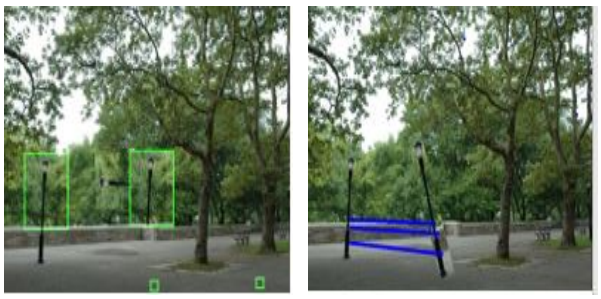


(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.14: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.



(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]



(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.15: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

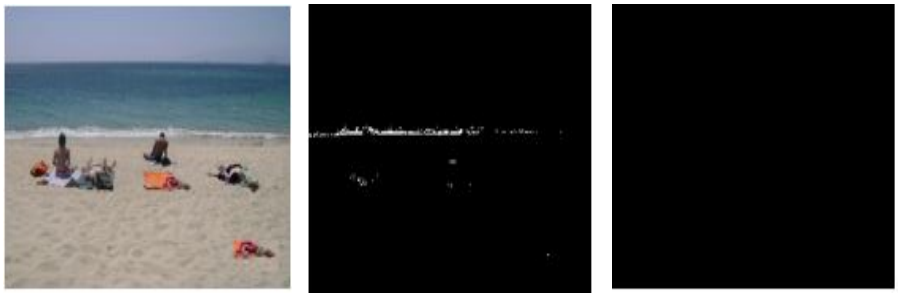
region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52] .

The copied part in image 6 is an object. Ahmed et al. [54] has marked no detection in simple tampered image and also no CMF detection in case of scaling and rotation as it uses image's statistical features like mean and standard deviation along with SVM classifier. Ramu et al. [52] has detected no copied region in scaled, rotated and simple tampered images by using SIFT and RANSAC. Fist proposed technique makes use of PCA and pixel value comparison and the second suggested technique makes use of SIFT detectors that have distinguishing and discerning properties. DBSCAN is used for matching and clustering since it provides the best matches quickly. The first presented method detects simple and overlapped forgery but doesn't give results in case of rotation and scaling and the second proposed techniques has nicely marked forgery region in case of scaling and rotation with high F-Measure and less CPU-time than Ahmed et al. [54] and Ramu et al [52] .

(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.16: (a) Input simple tampered image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.



(a) Input Image I (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.17: (a) Input scaled image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

(a) Input Image *I* (b) *Ahmed et al.* [54] (c) *Ramu et al.* [52]

(d) Proposed PCA-CMFD (e) Proposed SIFT-DBSCAN

Figure 4.18: (a) Input rotated image. (b) and (c) Results of existing techniques. (d) and (e) Results from the two proposed techniques.

4.3.2 Quantitative comparison of all strategies:

In quantitative analysis, false rates and accuracy are comparatively calculated on the basis of wrong copy detection. The proposed models have shown the lowest false rates with highest accuracy. False rate can be calculated as:

$$FalseRate = \frac{FalsePositive}{FalsePositive + TrueNegative} \tag{4.1}$$

Table 4.2 and 4.3 shows the comparative analysis of each strategy with false rates:

Table 4.2: F-Measure of test images

Cases	*Ahmed et al.* [54]	*Ramu et al.* [52]	Proposed PCA-CMFD	Proposed SIFT & DBSCAN
F-Measure (Simple Tampered Image)				
Image 1	0.95	0.67	-	0.3
Image 2	0.87	0.48	-	0.22
Image 3	0.98	0.86	0.98	0.4
Image 4	0.77	0.8	0.98	0.3
Image 5	0.85	0.75	0.75	0.1
Image 6	0.74	0.764	0.75	0.23
F-Measure (Scaled Image)				
Image 1	-	-	-	0.32
Image 2	-	-	-	0.4
Image 3	-	-	0.98	0.5
Image 4	-	-	0.98	0.11
Image 5	-	-	0.75	0.10
Image 6	-	-	0.75	0.12
F-Measure (Rotated Image)				
Image 1	-	-	-	0.21
Image 2	-	-	-	0.32
Image 3	-	-	0.98	0.3
Image 4	-	-	0.75	0.32
Image 5	-	-	0.98	0.3
Image 6	-	-	0.75	0.13

Table 4.3: CPU-time of test images

Cases	*Ahmed et al.* [54]	*Ramu et al.* [52]	Proposed PCA-CMFD	Proposed SIFT & DBSCAN
CPU-time for Simple Tampered Image (in seconds)				
Image 1	88	78	120	7
Image 2	69	90	150	9
Image 3	63.938	86	135	8
Image 4	76	89	133	8
Image 5	69	92	122	8
Image 6	78	91	130	8
CPU-time for Scaled Image (in seconds)				
Image 1	79	88	126	8
Image 2	85	88	140	8
Image 3	67	86	120	8
Image 4	77	90	120	8
Image 5	75	84	129	9
Image 6	77	99	140	9
CPU-time for Rotated Image (in seconds)				
Image 1	67	89	150	6
Image 2	79	86	129	8
Image 3	77	86	136	8
Image 4	77	86	126	8
Image 5	76	90	138	9
Image 6	87	92	136	9

All given tables in this chapter shows the FMs of test photos (with rotation and scaling). Compared to Ramu et al. [52] , Ahmed et al. [54] , and the first reported method, the second proposed technique exhibits significantly higher FM. This shows that there are low false matches using the second suggested strategy (i.e. false positives (FPs) and false negatives (FNs)). As a result, it will aid in accurately identifying fake copy-move areas. Ahmed et al. [54] do not perform as well as Ramu et al. [52] . The CPU-time for the second suggested solution is also listed in tables and is measured in seconds. This

second suggested technique demonstrates a significant time decrease. It has accurately detected the falsified portion while also requiring less computing effort.

This chapter includes dataset description, simulation parameters, working environment, and a comparison to the literature which aids in the evaluation of the proposed schemes. This chapter first provides qualitative comparison of the proposed schemes with the existing techniques and the presents quantitative comparison of these proposed techniques with the two existing schemes in terms of CPU time and false rates.

Chapter 5

CONCLUSION AND FUTURE WORK DIRECTIONS

5.1 Conclusion:

CMF detection has become a challenging task today due to rapid advances in science and technology have made it easier than ever before to access a wealth of data in a variety of formats across a wide range of media. Two approaches have been identified for efficient and precise forgery region identification. Detection of duplication and robustness are combined in the new copy-move method that we've presented. It uses PCA as the image block features in the duplicate detection approach. The robust detection approach uses pixel value comparisons to calculate the characteristics. Each method's distinguishing qualities are then combined into a single container for easy retrieval and storage. The container stores the block coordinate, the first method's distinguishing characteristics (i.e., the primary components), and the second method's distinguishing characteristics (i.e., the pixel value comparison). The container is then put in alphabetical order. Finally, a filtering process is carried out to delete a pair of images that does not meet a specific threshold. As a last step, a detection result image is generated based on the remaining pairs of coordinates in each image block. Multiplied and overlapping copy-move forgeries can be detected using this method. Forged regions can be detected with great accuracy using this method. Second approach uses SIFT as a feature detection and extraction which are then clustered using DBSCAN clustering algorithm. Outliers are eliminated during post-processing, and LSC segmentation is then used to enhance the results. This technique outperforms in case of geometrical transformations. Qualitative and quantitative analysis shows that the proposed work has high FM and low CPU time as compared to the state-of-the-art methods.

5.2 Future work directions:

The future would like to work on the improvement/advancement of these technologies by keeping in mind the importance of digital data and vulnerable attacks on it.

• Detecting copy-move forgery having combination of different effects like rotation, scaling, illumination changes, contrast adjustment, blurring, noise addition to make it cover all possible scenarios. This will need a detailed descriptor that will remain invariant to all these operations. Subsequently, a good matching algorithm will be required to encounter sufficient matches for improved accuracy.

• Detecting high scale changes in copied region. When copied region is scaled to a large value, its sufficient matches with its original part in image become low. This will need descriptors that consider a lot of scaled versions of image. As a result, such descriptor will consume a lot time in generation of descriptors.

• Detecting copy-move forgery in videos by localizing frames having copied region. Videos contain a lot of frame. All above mentioned CM scenarios will be considered with the addition of improved processing speed. Hence, feature detection, extraction and matching will be enhanced to give accurate result in less time.

• Detecting copy-move forgery having combination of overlapping and geometric transformations. This will need a detector that works if the forged region is overlapped and undergone geometric transformations like scaling, rotation and translation.

• Detecting copy-move fraud by enhancing the clustering-based filter technique, which would involve adding more parameters to the suggested platform in order to maximize its effectiveness for evaluation and comparison of photographic forgery detection.

BIBLIOGRAPHY

[1] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection," Journal of Inormation. Processing Syst, 2018, vol. 14, no. 1, pp. 6–31.

[2] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Science International, 2013, vol. 231, no. 1–3, pp. 284–295.

[3] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," ICASSP, IEEE International Conference Acoust Speech Signal Process, 2009, pp. 1053–1056.

[4] S. Khan and A. Kulkarni, "Robust method for detection of copy-move forgery in digital images," International Conference Signal Image Process. ICSIP, 2010, pp. 69–73, 2010.

[5] R. Oommen, M. Jayamohan, and S. Sruthy, "A survey of copy-move forgery detection techniques for digital images," International Journal of Innovations in Engineering and Technology, 2015, vol. 5, no. 2, pp. 419–426.

[6] L. D. Amiano, D. Cozzolino, G. Poggi, and L. Verdoliva, "A PatchMatch-based dense-field algorithm for video copy-move detection and localization," IEEE Transaction on Circuits and Systems for Video Technology, 2019, vol. 29, no. 3, pp. 669–682.

[7] S. Guleria and M. Kaur, "Copy move forgery detection in digital images and their analysis: -A review," International Conference on Small Data Intelligence, 2021.

[8] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, 2013, vol. 233, no. 1–3, pp. 158–166.

[9] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 8th IEEE International Workshop on Information Forensics and Security WIFS 2016.

[10] A. Diwan, R. Sharma, A. K. Roy, and S. K. Mitra, "Keypoint based comprehensive copy-move forgery detection," IET Institute of Engineering and Technology Image Processing, 2021, vol. 15, no. 6, pp. 1298–1309.

[11] T. Mahmood, A. Irtaza, and Z. Mehmood, "Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images," Forensic Science International, 2017, vol. 279, pp. 8–21.

[12] R. S. Dhanaraj and M. Sridevi, "A study on detection of copy-move forgery in digital images," Proceedings of 3rd International Conference on Intelligent Communication Technoligies and Virtual Mobile Networks, ICICV, 2021, pp. 900–905.

[13] R. S. Dhanaraj and M. Sridevi, “A study on detection of copy-move forgery in digital images,” Proceedings of 3rd International Conference on Intelligent Communication Technoligies and Virtual Mobile Networks, ICICV, 2021, pp. 900–905.

[14] N. Goel, S. Kaur, and R. Bala, “Dual branch convolutional neural network for copy move forgery detection,” IET Institute of Engineering and Technology Image Processing, 2021, vol. 15, no. 3, pp. 656–665.

[15] B. Su and K. Zhu, “Detection of copy forgery in digital images based on LPP-SIFT,” Proceedings 2012 International Conference on Industrial Control and Electronics Engineering ICICEE, pp. 1773–1776.

[16] H. Studiawan, R. N. Salimi, and T. Ahmad, Forensic Analysis of Copy-Move Attack with Robust Duplication Detection. Springer International Conference on Soft Computing and Pattern Recongnition, 2021, pp. 404-413.

[17] C. Wang, Z. Zhang, and X. Zhou, “An image copy-move forgery detection scheme based on A-KAZE and SURF features,” Symmetry (Basel), 2018, vol. 10, no. 12, pp. 1–20.

[18] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” IEEE Transactions on Information Forensics and Security, 2021, vol. 6, no. 3.

[19] P. Sharma and H. Kaur, “Copy-move forgery detection with GLCM and euclidian distance technique in image processing,” International Journal of Recent Technology and Engineering, 2010, vol. 8, no. 1C2, pp. 43–47.

[20] YE. Abdalla and S. John’s, “Detection of Copy-Move Forgery in Digital Images Using Different Computer Vision Approaches,” 2020.

[21] M. A. Elaskily, H.A. Elnemr and A.Sedik, “A novel deep learning framework for copy-moveforgery detection in images,” Multimed. Tools and Applications, 2020 vol. 79, no. 27–28, pp. 19167–19192.

[22] G. Kaur and M. Kumar, “Study of Various Copy Move Forgery Attack Detection Techniques in Digital Images,” International Journal of Research in Computer Applications and Robotics ISSN, 2015, vol. 3, no. 9, pp. 30–34.

[23] J. C. Lee, C. P. Chang, and W. K. Chen, “Detection of copy-move image forgery using histogram of orientated gradients,” International Journal of Information Science, 2015, vol. 321, pp. 250–262.

[24] I. A. Zedan, M. M. Soliman, K. M. Elsayed, and H. M. Onsi, “Copy Move Forgery Detection Techniques: A Comprehensive Survey of Challenges and Future Directions,” International Journal of Advanced Computer Science and Applications, 2021, vol. 12, no. 7, pp. 248–264.

[25] H. Y. Huang and A. J. Ciou, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation,” EURASIP Journal on Image and Video Processing, vol. 2019, no. 1.

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

[27] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-Move Forgery Detection by Matching Triangles of Keypoints," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 10, pp. 2084–2094.

[28] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 11, pp. 2284–2297.

[29] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," International Journal of Forensic Science, 2013 vol. 224, no. 1–3, pp. 59–67.

[30] A. Islam, C. Long, A. Basharat, and A. Hoogs, "DOA-GAN: Dual-Order Attentive Generative Adversarial Network for Image Copy-Move Forgery Detection and Localization," Proc. IEEE Confernece on Computer Vision and Pattern Recognition, 2020, pp. 4675–4684.

[31] G. Muzaffer and G. Ulutas, "A new deep learning-based method to detection of copy-move forgery in digital images," 2019 Scientific Meeting on Electrical-Electronics Biomedical Engineering and Computer Science EBBT 2019, pp. 1–4, 2019.

[32] S. F. Hajialilu, M. Azghani, and N. Kazemi, "Image copy-move forgery detection using sparse recovery and keypoint matching," IET nstitute of Engineering and Technology Image Processing, 2020, vol. 14, no. 12, pp. 2799–2807.

[33] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images," Mathematical Problem in Engineering, 2016.

[34] M. Emam, Q. Han, and H. Zhang, "Detection of copy-scale-move forgery in digital images using SFOP and MROGH," International Conference of Pioneering Computer Scientists, Engineers and Educators ICYCSEE, 2016, vol. 623, pp. 326–334

[35] H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application PACIIA, 2008, vol. 2, no. 4, pp. 272–276.

[36] K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," International Journal of Computer and Electrical Engineering, 2017, vol. 62, pp. 448–458.

[37] H. C. Nguyen and S. Katzenbeisser, "Detection of copy-move forgery in digital images using radon transformation and phase correlation," 8th International Conference of Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP, 2012, vol. 1, pp. 134–137.

[38] K. Sunitha and AN.Krishna, " Efficient keypoint based copy move forgery detection method using hybrid feature extraction", Preceedings of the 2nd International Conference on Innovative Mechnism for Industry Applications ICIMIA, 2020, pp. 670-675.

[39] B. Xu, J. Wang, G. Liu, and Y. Dai, "Image copy-move forgery detection based on SURF," International Conference on Multimedia Information Networking and Security MINES, 2010, pp. 889–892.

[40] M. Shandilya, R. Naskar, and R. Dixit, "Detection of geometric transformations in copy-move forgery of digital images," 2015 Annual IEEE India Conference (INDICON), 2015, pp. 1-6.

[41] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Processing: Image Communication, 2015, vol. 39, pp. 46–74.

[42] G. Sheng, T. Gao, Y. Cao, L. Gao, and L. Fan, "Robust algorithm for detection of copy-move forgery in digital images based on ridgelet transform," International Conference on Artificial Intelligence and Computational Intelligence AICI, 2012, pp. 317–323.

[43] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," International Journal of Digital Investigation, 2012, vol. 9, no. 1, pp. 49–57.

[44] C. M. Pun, B. Liu, and X. C. Yuan, "Multi-scale noise estimation for image splicing forgery detection," Journal of Visual Communication and Image Representation, 2016, vol. 38, pp. 195–206.

[45] I. T. Ahmed, B. T. Hammad and N. Jamil, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," 2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA), 2021, pp. 92-96.

[46] R. Dixit and R. Naskar, "Review, analysis and parameterisation of techniques for copy-move forgery detection in digital images," IET Institute of Engineering and Technology Image Processing, 2017, vol. 11, no. 9, pp. 746–759.

[47] Malti Puri and Vinay Chopra, "A Review: Block-Based Copy-Move Forgery Detection Methods," International Journal of Engineering Researcha nd Technology IJERT, 2016, vol. V5, no. 10, pp. 50–53.

[48] V. S. Kulkarni and Y. V Chavan, "Comparison of methods for detection of Copy-Move Forgery in Digital Images," Intwenational Journal of Engineering Science and Technology, 2014, vol. 1, no. 1, pp. 1–6.

[49] R. Sekhar and C. A. S, "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images," International Journal of Computer Applications, 2014, vol. 89, no. 8, pp. 28–33.

[50] A. Kuznetsov and V. Myasnikov, “A new copy-move forgery detection algorithm using image preprocessing procedure,” International Journal of Procedia Engineering, 2017, vol. 201, pp. 436–444.

[51] A. Shahroudnejad and M. Rahmati, “Copy-move forgery detection in digital images using affine-SIFT,” 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), 2017, pp. 1-5.

[52] G. Ramu and S. B. G. T. Babu, “Image forgery detection for high resolution images using SIFT and RANSAC algorithm,” 2017 2nd International Conference on Communication and Electronics Systems (ICCES), 2017, pp. 850–854.

[53] K.Liu, W.Lu, C.Lin, X.Huang, X.Liu, Y.Yeung and Y.Xue “Copy move forgery detection based on keypoint and patch match,” Multimedia Tools and Applications, 2019, pp. 31387–31413.

[54] I. T. Ahmed, B. T. Hammad and N. Jamil, ”Image copy-move forgery detection algorithms based on spatial feature domain,” 2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA), 2021, pp. 92-96.

[55] K.B. Meena and V.Tyagi, ”A copy-move image forgery detection technique based on Tetrolet transform” Journal of Information Security and Applications, 2020.

[56] G.Gani and F.Qadir, ”A robust copy move forgery detection technique based on discrete cosine transform and cellular automata” Journal of Information Security and Applications, 2020.

[57] K. Kaur, ”Efficient and fast copy move image forgery detection technique,” 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), 2018, pp. 986-990.

[58] A.M.Moussa, ”Kd-tree based algorithm for copy move forgery detection,” International Journal of Science and Technology Research IJSTR, 2020.

[59] Y.Liu, J.Wang, Y.Chen, H.Wu and H.Wang, ”A passive forensic scheme for copy-move forgery based on superpixel segmentation and k-means clustering” Multimedia Tools and Applications, 2020, pp. 477-500.

[60] A. Roy, A. Konda and R. S. Chakraborty, ”Copy move forgery detection with similar but genuine objects,” 2017 IEEE International Conference on Image Processing (ICIP), 2017, pp. 4083-4087.

[61] A. Badr, A. Youssif and M. Wafi, ”A Robust Copy-Move Forgery Detection In Digital Image Forensics Using SURF,” 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-6.

[62] Priyanka, G.Singh and K.Singh, ”An improved block based copy-move forgery detection technique,” Multimedia Tools and Applications, 2020, pp. 13011-13035.

[63] K.B.Meena, and V.Tyagi, ”A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms,” Multimedia Tools and Applications, 2020, pp. 8197-8212.

[64] J.Y.Park, T.A.Kang, Y.H.Moon and I.K.Eom, ”Copy move forgery detection using scale invariant feature and reduced local binary pattern histogram,” Symmetry, 2020, pp. 1-16.

[65] H.Studiawan, R.N.Salimi and T.Ahmad, ”Forensic analysis of copy-move attack with robust duplication detection,” Proceedings of 12th International Conference on Soft Computing and Pattern recognition SoCPaR, 2020, pp. 404-413.

[66] W.Luo, J.Huang and G.Qiu, ”Robust Detection of Region-Duplication Forgery in Digital Image,” 18th International Conference on Pattern Recognition (ICPR’06), 2006, pp. 746-749.

[67] A.C.Popescu and H.Farid, ”Exposing digital forgeries by detecting duplicated image regions,” Department of Computer Science, Dartmouth College (2004).

[68] D.Vogan, ”Lexicographic order,” Department of Mathematics.

[69] K.Sunil, D.Jagan and M.Shaktidev, ”DCT-PCA based method for copy move forgery detection,” ICT and Critical Infrastructure: Proceedings Convention of Computer Society of India, 2014, pp. 577-583.

[70] M.Zimba and S.Xingming, ”DWT-PCA (EVD) based copy-move image forgery detection,” International Journal of Digital Content Technology and its Applications, 2011.

[71] J.J.Lee and G.Kim, ”Robust estimation of camera homography using fuzzy RANSAC,” International Conference on Computational Science and Its Applications ICCSA, 2007, pp. 992-1002.

[72] Z.H.Nejad and M. Nasri, ”Adaptive stopping criteria-based A-RANSAC algorithm in copy move image forgery detection,” 2021 12th International Conference on Information and Knowledge Technology (IKT), 2021, pp. 107-111.

[73] M.Bilal, H.A.Habib, Z.Mehmood, T.Saba and M.Rashid, ”Single and multiple copy move forgery detection and localization in digital images based on the sparsely encoded distinctive feature and DBSCAN clustering,” Arabian Journal for Science and Engineering, 2020, 2021, pp. 2975-2992.

[74] A.Hegazi, A.Taha and M.M.Selim, ”An improved copy move forgery detection based on density based clustering and guaranteed outlier removal,” Journal of King Saud University-Computer and Information Sciences, 2021, pp. 1055-1063.

[75] F. I. Rahma, E. Utami and H. A. Fatta, ”The Using of Gaussian Pyramid Decomposition, Compact Watershed Segmentation Masking and DBSCAN in Copy-Move Forgery Detection with SIFT,” 2020 3rd Intern

[76] B.Soni and P.K.Das, ”Keypoints based enhanced CMFD system using DBSCAN clustering algorithm,” Studies in Computational Intelligence, 2022, pp. 69-83.

[77] B.Mahdian and S.Saic, ”Detection of copy move forgery using a method based on blur moment invariants,” 2007 Forensic Science International.

[78] A.Sankar, ”Principal Component Analysis Part 1: The Different Formulations,” 2021 Data Science.

[79] N.Ramchandani, ”Implementation of SIFT in CUDA,” 2012.

[80] D.Lowe, ”The SIFT (Scale Invariant Feature Transform) Detector and Descriptor,” 2004.

[81] R.Scitovski and K.Sabo, ”DBSCAN-like clustering method for various data densities,” 2020 Pattern Analysis and Applications.

[82] H.Donald and JC.Keyser, ”Foundations of Physically Based Modeling and Animation,” 2016 AK Peters/CRC Press.

[83] D. Mukherjee, Q. J. Wu, and G. Wang, “A comparative experimental study of image feature detectors and descriptors,” Machine Vision and Applications, vol. 26, no. 4, pp. 443–466, 2015