Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 11, Number 7 (2018) pp. 567-596

http://www.ripublication.com

# A Brief Review: Copy-Move Forgery Detection

**Gurpreet Kaur[1*], Dr. Rajan Manro[2#]**

*[1*]Research Scholar: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India.*

*[2#]Associate Professor: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India.*

**Abstract**

One of the most common methods of digital image forgery is Copy-move forgery (CMF). For copy-move forgery, the copied region may be rotated or flipped to fit the scene better. In copy–move image forgery, a region from some image location is copied and pasted to a different location of the same image. To better hide the forgery, post-processing is applied. Using keypoint-based features, like SIFT features, for detecting copy–move image forgeries has produced promising results. In this paper, various methods of Copy-Move Forgery have been studied, which are classified into Block-based methods and Feature-based methods. Then, the key techniques of Copy-Move Forgery Detection (CMFD) are demonstrated. The goal of copy-move forgery detection is to find duplicated regions within the same image. Copy-move detection algorithms operate roughly as follows: extract blockwise feature vectors, find similar feature vectors, and select feature pairs that share highly similar shift vectors. Rotation or scale invariant features that can be more easily integrated in the CMFD pipeline have been studied.

**Keywords:** Copy Move Forgery, Block Based Forgery Detection, Keypoint Based Forgey Detection, Textual Features etc.

## I. INTRODUCTION

In this day and age, through the popularity of digital media cameras, digital images have turn out to be an intimate part of human life. Nonetheless, some image editing

tools (such as Photoshop and 3DMax) aid some convicts easily interfere with digital images, generally for malicious ins and outs. The digital images are access and modified by anyone without leaving visible clues, consequently it has come to be a severe risk to security. Nowadays, there are innumerable sorts of image forgery, attention is being paid by progressively more investigators to the problematic of digital image forgery. The utmost widespread exploration in the arena of image forgery detection is passive (or blind) detection technology [1], [2].

The furthermost communal method of operation in image forgery is Copy-move (or cloning or copy-paste) forgery, where on the identical image but into alternative location parts of an image are copied and reinserted. By replication some regions, objects can be unseen exaggerated a part. Though in some cases numeral of simple operations are obligatory, certain supplementary image processing, such as noise addition, JPEG compression, and geometric destruction, etc., is frequently smeared for considerable forgeries. The significant and prevalent matter in image forensics is turned out to be copy-move forgery detection (CMFD), with the huge approachability of sophisticated image manipulation tools [3], [4]. To notice and trace the copy-move forgery numerals of patterns have been offered over the ancient era. As formerly, block-based approaches and keypoint-based approaches are the two elementary types. The individualities of local patches of them are paralleled which refer to copy-move forgery discovery of an image [5], [6]. The local patch selection and feature description methods are basic metamorphoses amid the offered approaches.

Block-based approach is the most mainstream CMFD approach in the existing schemes, perhaps due to it is suitable for various feature extraction techniques and has high matching performance at the same time. The block-based methods generally split the image into overlapping or non-overlapping square blocks, and may be divided into circular blocks in order to increase the effect of resisting the geometric transformation. Subsequently, the features are extracted commencing these image blocks and are paralleled the resemblances amid the image blocks with each other to conclude the doubtful regions. As soon as the matched image blocks are noticed, it is directed that they are the noticed forgery region [7], [8]. A robust CMFD methodology has been projected by Ryu et al. [9] to confine replicated image sections, and Zernike moments as features of image blocks are smeared. A block-based organization, where histogram of oriented gradients (HOGs) descriptors is castoff to excerpt image features and then, it is engaged as confirmation to confirm copymove manipulation is planned by Lee et al. [10]. Wu et al. [11] accessible a procedure which usages the Fourier-Mellin Transform process with scale invariance to extract the image block features. The Patch Match algorithm is adapted by cozzolino et al. [12] to pact with rotation actions, and a randomized methodology is industrialized to sense analogous image patches in an image. A new copy-move forgery exposure way is defined in Wang et al. [13], founded on invariant quaternion

exponent moments (QEMs) feature descriptor and circular image blocks. The histogram of orientated Gabor magnitude (HOGM) is exploited in Lee et al. [14] to direct image block feature, and a perceiving copy-move forgery and authenticating images method is projected. It is demonstrated that block-based approaches are exceedingly operative in CMFD, but they frequently have various intrinsic downsides, for instance serious fragility to geometrical transformations, high computational complexity, etc.

Keypoint-based approaches are usually much faster than block-based approaches because their work concentrates on a relatively small set of pixels instead of dense block matching. The keypoints can effectively resist some image transformations in the whole image, so that duplicate regions can also be recognized in the modified image. A robust keypoint-based CMFD approach is projected by Pan et al. [15], where they service the SIFT features to resist diverse sorts of geometric falsification. Here, Cartesian coordinates analyzes the affine transformation matrix. Harris sensor is exploited to extract image keypoints, and the feature vectors are placid by shredding the sector statistic of a minor circular region nearby each Harris interest point in Chen et al. [16]. An innovative attention fact detector is offered by Zandi et al. [17] in which the concentration of attention facts is inevitably accustomed to generate it additional applied in the CMFD domain and suspicious regions are engendered. A newfangled CMFD scheme based on voting procedures and multi-scale investigation is advanced by Silva et al. [18], where it excerpts the robust keypoints and inventions probable correspondences. The Order-based Gradient Histogram (MROGH) descriptor and Hue Histogram (HH) are castoff in Yu et al. [19] to implement two-stage feature detection in command to attain restored feature proficiency and upsurge the matching enactment. Three novel curious detectors are familiarized in Costanzo et al. [20] grounded on irregularities in the delivery of attention facts subsequent operation, worldwide or local keypoints can be detached by them.

An innovative CMFD methodology is developed by Pun et al. [21] grounded on SIFT and SURF, in which they service adaptive keypoint matching and over-segmentation. A firsthand CMFD approach is presented by Ardizzone et al. [22] that is constructed on the examination of triangles of local keypoints. Amerini et al. [23] developed a new CMFD method by the J-Linkage algorithm, that can meritoriously cluster SIFT matching sets, and mend the detection fallouts. Semantic-independent patches are designed by dividing the image, and then confined the replicated image sections by reckoning the transform matrix with an EM-based algorithm has been similarly planned. In all-purpose, the matched keypoints can be located by the keypoint-based approaches quickly, that are superior to block-based methods in time.

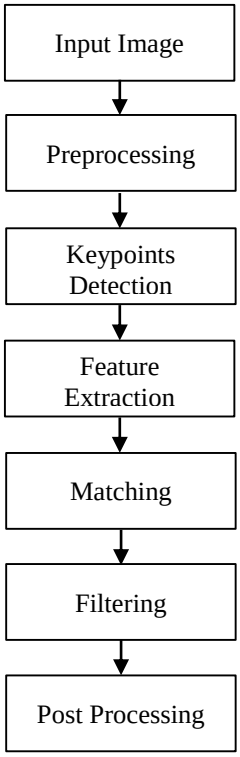


**Figure 1:** Basic block diagram for key-point based CMFD

However, most of them cannot locate regions very precisely; thus, they cannot often achieve satisfactory test results. In addition, a small region or duplicated regions with a little number of texture structures may be completely neglected.

## II. LITERATURE SURVEY

There are many existing works on copy-move forgery. Most existing methods differ in terms of features and emphasize on different aspects of the problem.

In the paper, **Zheng et al. (2013) [24]** present an automatic replication image region detection algorithm founded on LBP. It works in the absence of digital watermarking and does not requisite any former evidence about the tested image. Likened with preceding mechanisms, less features has been used in their algorithm to represent each block, and was more effective. Moreover, the effects of different block size fluctuating from 4 9 4 and 8 9 8 pixels on the enactment in terms of FP and FN has been studied in **Alkawaz et al. (2016) [25]**. In order to investigate the effect of block size on FP and FN, the block-based copy-move image forgery detection approach is considered using DCT coefficients with numerous block sizes. Basically, three objectives are carried out centered on the execution method that is using DCT coefficients with different block size, in order to achieve the accuracy to sense the tinkered region. However, a fast yet robust technique has been introduced in **Sachdev et al. (2017) [26]** to perceive copy move forgery using SURF key points. No

overlying super pixels are formed by subdividing the image and their SURF key points are equated. The method has a precise low computational complexity. Copy moved areas are detected even in the presence of processing operations like rotation, scaling, etc. A fast and efficient technique has been proposed in **Fadl et al. (2014) [27]** for fast-tracking CM forgery detection. Fan search method is projected instead of extensive block matching. By paralleling only the neighbors of suspected similar blocks, CM forgery detection is fastened through FS. The replicated regions of tempered images are sensed by their method even under the impact of blurring and JPEG compression. Furthermore, A novel CMFD approach engaging multi-granularity super pixels matching is advanced in **Jiao et al. (2017) [28]**. The foremost originality of the projected procedure depends on introducing color invariance based image key-points detector, robust QEMs-based CMFD features, and multiple granularity super pixels detection. A chain of simulation trials were implemented to indicate that our presented method has good performance in both detection accuracy and effectiveness. Besides this, the pattern also exhibits a very strong robustness, although the tempted image is subjected to various attacks; consist of common image processing operations for example AWGN and JPEG compression, and geometric transforms like rotation and scaling. Nonetheless, image manipulation can be hidden by methods of greater sophisticated postprocessing, such as strong noise addition, high range scaling, great angle rotation, or a combination thereof. This makes the CMFD far more challenging. An innovative procedure is proposed by **Zhihua et al. (2017) [29]** to notice copy-move forgery built on the CMFD-SIFT. It is represented by the investigational outcomes that the recommended scheme can precisely notice the replicated sections; and is incapable to overwhelm the problem of dearth of key-points by expending the key-points dispersal strategy for key-points selection. Furthermore, the invariance to mirror transformation and rotation is enriched by the proposed algorithm by using an improved descriptor. Besides this, by adaptive combination of keypoint-based method and block-based method, **Tingge et al. (2016) [30]** presented a well-worn fusion based methodology for image forgery detection. For each image, an applicable initial size of regions is determined by this system and it can divide the image into smooth region and keypoints region. Their method can effectually notice forgery from both plane regions and no plane ones whilst dropping the computation cost by smearing different methods to these two types of regions. The selection of threshold D has a great influence on the results while detecting forgery in smooth regions. Looking forward, **Osamah et al. (2017) [31]** looked at between four coordinating strategy that have been utilized in copy-move forgery detection. For reasonable examination, similar highlights and same check step have been utilized as a part of the investigations. The test comes about shows diverse reactions of the four techniques in view of the kind of activities associated with making the copy-move forgery. In addition, the four techniques demonstrated an extensive variety of general exactness, 34.88– 67.38, estimated by F1 measure. We can presume that coordinating strategy significantly affects the precision of recognition of copy-move forgery. Moving further, **Qershi et al. (2016) [32]** went for proposing an upgraded coordinating technique that can improve the execution LSH-based strategy regarding precision and speed. At the point when the picture pieces are grouped before

coordinating utilizing LSH, the coordinating procedure is performed between squares have a place with a similar bunch. The squares have a place with a similar group are nearer to each other which expands the likelihood of finding the copied pieces, i.e. expands the genuine positive proportion, and diminishes the false positive proportion. Whereas, a new CMFD method is proposed in **Jichang et al. (2016) [33]** consuming SURF in the opponent color space to extract local geometric and color invariant features. The assessment comes about show the adequacy of OwSURF in recognizing the level duplication districts with different postprocessing activities. In spite of, **Doyoddorj et al. (2013) [34]** projected a robust copy-move forgery detection scheme for a apprehensive image. To abstract invariant robust features of a certain image, they smeared dual-transform. The extricated highlights are spoken to by lexicographically requested DCT coefficients on the recurrence area from the Radon space, that each covered picture pieces are anticipated by the segments of a grid with the quantity of the characterized points ϑn on the Radon area. In the work of **Hasoon et al. (2017) [35],** It is considered that Copy-Move forgery is incorporating translation and rotation. Another division strategy was recommended to portion the Copy-Move questions in a more predictable manner than SLIC. They acquired great outcomes on interpretation and sensible outcomes with pivot. The Segment Gradient Orientation Histogram (SGOH), which was propelled by SIFT, was utilized to depict the angle for each section (sporadic square). The hysteresis method was utilized to develop the identification region(s) and enhance the essential discovery result. Additionally, our technique can recognize CMF in pictures with obscuring, shine change, shading lessening, JPEG pressure, and varieties interestingly and included commotion. Moving further, an enhanced matching process is proposed in **Osamah et al. (2014) [36]** that can be utilized to detect copy-move forgery based on Zernike-moments. By partitioning the squares into pails and embracing relative mistake rather than Euclidean separation, the proposed strategy improved the location exactness altogether. The precision is improved as a result of the strength of the proposed technique against turning and scaling. Besides this, **Malviya et al. (2016) [37]** developed an effective copy move tampering detection technique. The element extraction techniques actualized in the plan have been utilized broadly for content based picture recovery before. The proposed conspire presents three diverse location systems for duplicate move fraud recognition, which is less intricate and gives heartiness to change and commotion. Auto Color Correlogram demonstrates viable discovery with most astounding exactness when the proposed framework is affirmed on pictures from the database. The recognition strategy is likewise compelling in identification of fraud on occasion of scaling and numerous cloning in a similar picture. Looking forward, a new block-based method is presented by **Tralic et al. (2016) [38]** for detection of duplicated image regions that pools LBP with CA to complete a powerful configuration depiction. Recognizable proof of copied regions is expert by breaking down nearby changes of pixel luminance esteems in a roundabout neighborhood. Pixel esteems are changed to twofold esteems utilizing LBP to shape a decreased portrayal of a square and the double esteems are utilized as a contribution to CA. The created include vector shows the utilization of a particular arrangement of examples in the square surface, so comparable picture regions should deliver

comparable component vectors. FLANN is connected to the element vectors set to discover the k closest neighbors for each component and another hunt technique is connected to choose the copied squares. Illustrations of such forgeries in real world setups has been presented in **Manu et al. (2016) [39]** and developed an efficient algorithm that can detect them even if some postprocessing is prepared to counter the detection. They utilized a mix of division and SURF keypoints for location of duplicate move imitations in pictures by grouping the keypoints. They tried our technique on two datasets-the datset utilized as a part of and CoMoFoD. The reason for utilizing the previous was to test the execution based on exactness, review and precision and the last to confirm its resilience towards postprocessing activities in the wake of playing out a copy-move forgery. Performance-wise, a study on a novel approach is performed in **Shaji et al. (2016) [40]** for copy-move forgery detection. As a result of the high computational multifaceted nature of square based techniques, key-point-based strategies are picking up fame. In any case, the wastefulness of key-indicate based techniques perform well on account of little produced areas and pictures with little structure incited the scientists to consider other better alternatives. DAISY descriptor was observed to be powerful for a wide range of picture controls and it was ended up being to be better than SIFT. A rotational invariant portrayal of DAISY descriptor is exhibited in their work. Last year, an efficient block-based method for CMFD is presented by **Young et al. (2017) [41]**. First of all, a supplementary coincided circular block is acquainting with to swap the rectangle block to split the forged image. In polar coordinate, the overlay circular block is suitable for the RHFMs. The DRHFMs commencing the apprehensive image excerpt the local and inner image feature of the every single circular block. Then, 2NN test explore the extracted alike feature vectors of blocks. To filter these features, Euclidean distance and correlation coefficient is laboring to take away the incorrect matches. Then, to obliterate inaccessible points or regions for auxiliary matting, morphologic operation is employed. However, an innovative technique is emphasized for CMFD based on feature enrichment by **Zhang et al. (2016) [42]**. For the first while, image tampering forensics is prepared by CLAHE algorithm. Contrasted and existing work, the paper coordinates the CLAHE calculation into the SURF based structure to identify duplicate move falsification. Utilizing these upgrade design pictures, the qualities acquired are exceptionally ideal, expanding considerably the quantity of keypoints found in the pictures particularly in level or smooth areas. Furthermore, a new SIFT-based CMFD procedure is projected in **Joon et al. (2017) [43]** for the effectual detection of CMF. It has theoretic solid background and its definite performance is grander to prevailing processes grounded on SIFT features. The simulation comes about exhibit that the proposed calculation accomplishes an exceptionally stable identification execution for four CMF situations: revolution, scaling, JPEG pressure, and AWGN. Also, the handling time of the proposed calculation is the least among the SIFT-based CMFD calculations. Subsequently, we emphatically suggest the utilization of the proposed calculation for the applications that need to identify CMF. Particularly, the proposed calculation can be used to give quantitative measures of picture legitimacy in criminal examination, item investigation, news coverage, insight administrations, and observation frameworks.

In addition to all, an effectual forensic technique grounded on the scaled ORB is proposed by **Xuanjing et al. (2016) [44]** for noticing copy-move forgery in digital images. The proposed technique identifies copied locales as well as decides the geometric changes and post preparing connected to the manufactured areas. Likewise, when finding the copied areas of which SIFT and SURF can't distinguish, the proposed calculation additionally performs well. Notwithstanding, the strategy is still tedious for imitation discovery of high determination pictures. Besides this, a different policy is projected in **Yanfen et al. (2016) [45]** to sustenance copy–move forgery detection created on discrete analytical Fourier-Mellin transform. They complete a considerable measure of examination and exchange on DAFMT. They build the geometric minute invariant and concentrate geometric invariance with an assistant plate format. They at that point apply lexicographic arranging to sort the invariance in extraordinary arranging. Spearman rank relationship coefficient is proposed to assess and examine the consequences of lexicographic arranging. At long last, they find and show suspicious copy– move locales. A substantial number of investigations are performed to assess and show the prevalent execution of our DAFMT, in identifying interpretation, scaling falsification tasks, as well as in recognizing turned imitation activities. The predominant execution of our DAFMT isn't just constrained to distinguish the copy–move forgery images, yet in addition to perceive the first images effectively. Looking forward, **Xiamu et al. (2016) [46]** propose a feature point-based copy-move forgery detection method that is equipped for managing the imitations occurred at smooth, particularly little smooth districts. For highlight location, they exhibit a two-arrange include point identification plan to get adequate component point scope for both finished and smooth locales in a suspicious picture. They utilize the MROGH descriptor as highlight descriptor for customary areas in the picture, for the little smooth locales, they abuse include combination to upgrade the discriminative energy of the component descriptor. Their technique separates the highlights in a denser way, in this way the running time of our strategy is substantially higher than of the SIFT and SURF-based strategies. As far as identification capacity, their technique beats the cutting edge strategies for plain duplicate move recognition; moreover, the power against jpeg pressure and pivot are likewise tasteful. Their strategy can oppose direct level of scaling, added substance clamor and joined impacts, however the execution decreases quickly when these assaults are solid, because of the shakiness of the Harris Corner Detector under these conditions. The use of thick intrigue focuses or relative covariant element indicators may help. Moreover, **Emam et al. (2016) [47]** planned an effectual scheme meant for copy-move forgery detection that can distinguish tampering and localize the disagreed region in a digital image. Rather than utilizing the thorough piece coordinating technique, ANNs is gathered by territory touchy hashing LSH. To show signs of improvement recognition comes about, morphological activities are connected to evacuate little openings and dispose of detached pixels. Our technique can identify the copied locales of altered pictures even affected by geometric changes, for example, pivot, scaling, commotion expansion, and JPEG pressure. In the work of, **Qingxiao et al. (2017) [48]** propose a copy-move forgery detection technique based on Convolutional Kernel Network. The fundamental commitments can be closed as takes

after: the CKN appropriation in duplicate move phony discovery and GPU-based CKN remaking, the division based keypoint dispersion (SKPD) technique and GPU-based versatile over division (COB). Besides this, **Pandey et al. (2014) [49]** proposed a procedure to perceive Copy-Move Forgery to provision image forgery detection. The outcomes were recorded utilizing three distinctive picture includes to be specific SURF, HOG and SIFT among which SIFT gave best outcomes as exactness and accuracy. By applying same technique on various highlights they have demonstrated that how one component gives better outcomes in contrast with others. In the wake of considering half and half highlights (SURF-HOG or SIFT-HOG), they are showing signs of improvement result for CMFD in contrast with SIFT or SURF or when HOG is utilized alone. As well as in the work of **Rosin et al. (2014) [50]** CA has been smeared on every single overlying block of forged image with the intention to cause a set of procedures. This procedure can be available as a determination of a subset of standards that depict the surface of square from every single conceivable run the show. Use of a CA on a greyscale image prompts an expansive number of conceivable tenets and a much bigger number of conceivable subsets of those guidelines. Diminishment of number of guidelines can be refined by an appropriate paired portrayal of picture, bringing about just two conceivable estimations of cells states (rather than 256 on the off chance that when a greyscale picture is utilized). Thresholding of a greyscale picture by worldwide limit prompts paired picture where much data about surface is lost, and use of double planes is very clamor delicate. With a specific end goal to explain these issues, another portrayal of the picture in light of nearby parallel example (LBP) is presented. LBP characterizes twofold estimations of neighborhood pixels in view of a distinction amongst focal and neighborhood pixels. Subsequently, LBP jelly nearby data yet additionally keeps enough worldwide pictures' data. Recognition of duplicate move fabrication is expert utilizing straightforward 1D CA where the area for each pixel is characterized as a gathering of pixels from the line over the pixel under thought. In contrast of **Khayeat et al. (2016) [51]** copy-move forgery has been considered integrating rotation and translation. Another strategy was recommended to distinguish CMF/CRM forgery. They acquired amazing outcomes on interpretation and great outcomes on revolution. They enhanced the precision of the pivot strength of DSIFT; along these lines, they accomplished preferred outcomes over for Zernike minute in turn. Another strategy for evacuating false coordinating was produced and broadly tried. On the other hand, **Farukh et al. (2014) [52]** gauged altered forms of forgery techniques and definite an algorithm for distinguishing the utmost communal copy-move forgery. They inspected diverse methods and calculation grew beforehand for the same. They proposed a DyWT based strategy in mix of SIFT calculation. In the work of **Shuo et al. (2017) [53]** presented a novel keypoint-based copy-move forgery detection for minor plane sections. The fundamental oddity of the work comprises in presenting the superpixel content based versatile element point's identifier, hearty EMs-based keypoint highlights, and quick Rg2NN based keypoint coordinating. They show the viability of the proposed approach with a substantial number of trials. Accordingly, **XiuLi et al. (2018) [54]** propose an innovative multi-scale feature extraction and adaptive matching method to notice the copymove image forgery. In the proposed plot, to

begin with, they section the host image by SLIC in multiscale, to create multi-scale patches; at that point they apply SIFT to patches in every one of the scales, to remove highlight focuses. Next, the Adaptive Patch Matching calculation is in this manner proposed for finding the coordinating which can demonstrate the suspicious fashioned locales in each scale. Lastly, the suspicious districts in all scales are combined and some morphological activities are connected to create the recognized imitation locales. As a rule, they have four fundamental commitments in the proposed conspire: 1) they supplant the covering squares of normal shape in conventional fraud location calculations, with singular unpredictable patches, which can better parcel the host images into non-covering pieces. 2) They fragment the host image into patches in different scales, from which the component focuses are separated individually. The proposed multi-scale include extraction strategy can separate more precise component focuses. 3) Instead of falsely setting the fix coordinating limit ahead of time, they propose to adaptively ascertain the coordinating edge for better component acknowledgment. What's more, 4) amid the post-preparing, they propose to utilize the predefined little superpixels to supplant the coordinated keypoints and they apply some morphology tasks into the consolidated locales to produce all the more precisely identified fabrication districts. Also, **HaiBin et al. (2014) [55]** proposed a unique forensic method to notice and localize duplicated regions that have experienced rotation by random angles, even after JPEG compression. With a specific end goal to extricate rotationally invariant highlights, covering blocks of pixels are deteriorated first by utilizing DT-CWT which has both the shift invariance and directional selectivity. At that point channel energies are extricated from each subband at every deterioration level utilizing the L1 standard. At long last, the anisotropic rotationally invariant highlights are separated utilizing sizes of discrete Fourier transform for these channel energies. Moreover, the rotationally invariant element vector removed from each covering square of pixels can be utilized to lessen the computational cost of the pursuit arrange, and the duplicate pivot move location calculation is tended to in detail. Broad investigations have been led to assess the power of the proposed technique. Above all, a new hybrid method is implemented in **Oommen et al. (2016) [56]** by the strength of fractal dimension along with singular value decomposition. Exploratory outcomes demonstrate that the technique is powerful in pictures even after post-replicating controls. The main test with the technique is the high calculation time required for evaluating fractal measurement, which we have effectively lessened to an extraordinary expand limiting the correlation ventures by influencing utilization of B+ to tree plan of picture squares arranged in the request of neighborhood fractal measurement. Afterwards, a novel copy–move forgery detection method is defined in **Hong et al. (2016) [57]** which is concentrated on circular image blocks and invariant QEMs feature descriptor. They exhibit the adequacy of the proposed approach with an expansive number of trials. Exploratory outcomes demonstrate that the proposed approach can accomplish better location comes about for copy– move forgery images if the produced picture is pivoted, scaled or very packed. They contrasted the strength of our technique and the beforehand proposed plot which utilize Zernike minutes as highlights, and they demonstrated that their strategy is more vigorous to different kinds of preparing. Anyhow, **HangJun et al. (2013) [58]** introduced two foremost

contests like robustness against geometric transforms including time complexity, rotation, and scaling, specifically to a superiority of forgery images. They audit these calculations and talk about its vigor and time multifaceted nature. Block-matching techniques are best for phony location and powerful to JPEG lossy compression, obscuring, or commotion expansion, however not very many of them are successfully vigorous against geometrical assaults (turn, scaling, contortion) and tedious. Sift-matching techniques still have a constraint on location execution since it is just conceivable to separate the keypoints from unconventional purposes of the picture. Hence, how to blend two systems is future research course. In contrast, **George et al. (2014) [59]** measured the difficulty in copy–move image forgery detection. Their accentuation was on recognizing robustness. The proposed approach utilizes another arrangement of keypoint-based features, called MIFT, for finding comparative areas in a picture. To evaluate the relative change between comparable districts all the more precisely, they have proposed an iterative plan which refines the relative change parameter by discovering more keypoint coordinates incrementally. To lessen false positives and negatives while separating the copied area, they have proposed utilizing thick MIFT includes in conjunction with hysteresis thresholding and morphological tasks. On the other hand, the act of dissimilar projected approaches are assessed in **Sadeghi et al. (2017) [60]** and offered the compensations and negatives of existing approaches. Their basic advances were additionally clarified. All of these techniques can verify the image and find copied zones without being influenced by general changes, for example, turn, scale, or commotion expansion. In light of the order of all techniques as indicated by keypoint-based and piece age strategies, the outcomes demonstrate that keypoint-based techniques are greatly improved on the grounds that their computational time is low and their recognition execution is great. Also, copy-move image forgery detection is proposed in **Gaobo et al. (2016) [61]** that put accent on detecting duplicated regions with flipping or rotation. The rotation invariant uniform local binary patterns are engaged in proposed approach to excerpt block-based features. Exploratory outcomes demonstrate the benefits of the proposed approach. Be that as it may, like existing piece based recognition approaches, the proposed approach still does not function admirably if the copied district is to a great extent scaled or pivoted. At last, **Jihoon et al. (2016) [62]** offered an innovative feature descriptor for the effectual detection of CMF. The proposed ULPF descriptor has a strong hypothetical foundation and its real execution is unrivaled than existing descriptors. Particularly, the proposed descriptor accomplishes an exceptionally stable discovery execution over the whole scope of revolution edges. Furthermore, the proposed highlight vector structure and AZS request can be used in an extensive variety of uses managing images in the Fourier domain.

## III. RELATED WORKS

To yield accurate replication, doubling and pasting are customarily not sufficient; numerous supplementary procedures are engaged to plug this condition. i.e, if individual anticipates obscure a component by overlying it by a texture-like segment (water, sand, etc.), the segments requisites to be contested with its section. By

rotating, blurring, flipping or resizing the copied region, it possibly will be consummated before drubbing it. Graphic suggestions of altering are also condensed by these conversions. Additionally, as the replicating is terminated, the author could supplement Gaussian noise or shield the image in a lossy compression format like JPEG. The CMFD level stiffer would be generated to undertake it visually and by processor approaches. So as to report the problem, numerous approaches have been established by investigators that are sub-divided into two foremost modules: block-based and feature-based.

- **Block-based methods**

Blocks are associated and deliver invariance to selected conversions by Block-based techniques in an appropriate way. Fridrich et al. separated an image into overlying blocks of equivalent magnitude primarily in [63]. Afterward, factor of every block was mined by distinct cosine transform (DCT). To conclude, quantized factors are coordinated to discriminate the replicated regions which are lexicographically systematized. The time complexity of the PCA-based approach is lessened in process of [64] by overwhelming a discrete wavelet transform (DWT), but does not boom geometrical transformations. Undedicated Wavelet Transforms (UWT) initiated image forgery detection in [65]. The guesstimate and inclusive coefficients of the UWT are experienced by the journalist from overlying blocks of an image to paragon the resemblance among the blocks. Multi-Hop Jump (MHJ) algorithm and Fast Walsh-Hadamard Transform (FWHT) is castoff in [66].

- **Feature-based methods**

While block-based approaches appear operative to perceive duplicated regions, the accurateness of these classes of approaches is still inacceptable while execution on the geometrical altered objects [67]. To overwhelm this matter, feature-based procedures are preferred to match features in the image. The feature-based methods generally are smeared to two images: a target and a test image in pattern recognition [68]. But in the situation of CMFD, the feature-based methods are smeared to one image only. Keypoints excavated in the image will be relatively alike to the novel ones; consequently, a matching amongst key-points can be castoff to notice which fragment was copied and which geometric transformation was smeared [69]. Lately, feature-based CMFD procedures have been prompted, as forgeries have developed more resounding with several transformations. In [70], [71], SIFT feature is originally castoff for CMFD. Forgery decision is achieved whereas a numeral SIFT features are matched. In [72], Speeded-Up Robust Features (SURF) features [73] is extracted as an alternative of SIFT. Conversely, the detection consequence is scarcely amended meanwhile the transformation invariance of SURF is slight additional than SIFT [74]. Transform-invariant features are attained from the MPEG-7 image signature tools in [67]. Such CMFD approach find a feature matching exactness in excess of 90% crossways postprocessing processes and are competent to notice the cloned regions

with a high true positive rate and lower false positive rate. Lately, ORB features are castoff in [75]. Forgery decision is ended by toning the orientated FAST key-points which is grounded on the SVM technique [76], [77], [78]. Dense-field techniques are castoff in [79] to expressly agreement with the occlusive forgeries in which fragments of circumstantial copied elsewhere the dense-field. Technique [80] parts the image into semantically independent patches, such that the CMFD delinquent can be explained by fractional matching between these segmented patches. EM-based algorithm is then castoff to guesstimate the transform matrix. But the subsequent stage of matching necessitates supplementary computational cost. In [81], the multi-scale image hashing technique is projected to perceive the several content-preserving tempering. However, the engendered hash must be committed to the image before transmission, which would bind this method to organized surroundings. Though these feature-based approaches are competent to detect the forgery operated by geometric transformation, the accurateness of CMFD is still incapable to be castoff as indication.

## IV. BACKGROUND

In this division we concisely present the methods and techniques.

- **Zernike Moments**

Moments and invariant utilities of moments have been comprehensively castoff for invariant feature extraction in an eclectic series of digital watermarking applications, and pattern recognition, etc. [82]. Amongst the numerous sorts of moments originate in the nonfiction, Zernike moments have been demonstrated to be greater to the others in standings of their insensitivity to image noise, information content, and skill to deliver realistic image representation [83].

- **Matching Based on Lexicographical Sort**

This technique is the utmost widespread matching technique since it is modest, effectual, and upfront [84]. In this matching technique, the set of feature vectors,Z, is organized lexicographically which is alike to dictionary sort. The sorted set is represented as $\hat{Z}$ . Since the set $\hat{Z}$ , the Euclidean distance among adjacent pairs of $\hat{Z}$ is considered. If the distance is smaller than the pre-defined threshold$D_1$, they ruminate the queried blocks as a pair of aspirants for the forgery. Due to the statement that the neighboring blocks might consequence in somewhat alike Zernike moments, the distance between the actual blocks conforming to the pair of vectors is considered. If the considered distance is grander than a pre-defined threshold $D_2$, the corresponding blocks are well-thought-out as copy-move blocks. To enrich the presentation of the matching process, every vector is equated with the next r vectors.

- **Matching Based on Lexicographic Sort and Grouping**

The goal behindhand suggesting this technique is the point that vectors conforming to

alike blocks are not at all times head-to-head to each other after lexicographical sorting. It means that matching a vector with the succeeding r vectors may be not adequate to catch comparable vectors, and this may condense the true positive ratio (TPR) [85]. To overwhelmed that subject, a grouping method familiarized in [86]. In its place of matching all vectors with each other, the vectors are main divided consistently into G groups. Formerly G buckets are formed so that the i bucket comprises the vectors from group i, group i − 1, group i + 1. Every vector will be positioned into 3 buckets excluding the vectors in the leading and last groups which are positioned in only two buckets. Match the vectors with all vectors inside the similar bucket. The matching jerks with arranging Z by means of lexicographical sort. Then the resultant $\hat{Z}$ is separated into G groups and G buckets are generated. Contained by each bucket B, vectors are combined, and the actual distance between combined blocks is calculated as $D_A$. A novel set of combined vectors is formed as:

$$P_i = \left\{\left(B_{i_j}, B_{i_k}\right)\right\}, j \neq k \forall i = 1...G \tag{1}$$

$$If\ D_A(\mathrm{B}_{i_j}, \mathrm{B}_{i_k}) > \mathrm{D}_1 \tag{2}$$

Within every set Pi, the comparative fault is considered between vectors of each pair as the proportion of the absolute fault and the lowest rate of the two mechanisms. If entirely the comparative faults are beneath threshold $D_1$, the two conforming blocks are well-thought-out as contender forgeries. Otherwise, the pair of vectors is mislaid from Pi.

- **Matching Based on k − d Tree**

Bentley familiarized the k − d tree as a binary tree that provisions k-dimensional facts. Alongside the relatively effectual in its storage necessities, a substantial benefit of this arrangement is that a solitary data organization can switch many forms of inquiries very proficiently [87]. The k − d tree preprocesses data into a data structure that permits production effectual kind probes. It provisions facts of a k-dimensional space in the leaves. In direction to overwhelmed the downsides of upfront lexicographic arrangement, which is thought to be too penetrating to the transformations and yields a lower false positive rate, investigator adopted k − d tree [88]. Associated to lexicographical organization, k − d tree creates consistent consequences and lower false negative rates. In totaling, investigators exploited k − d tree to lessen the computational rate [89].

- **Matching Based on Locality Sensitive Hashing**

Locality-sensitive hashing (LSH), anticipated by Indyk and Motwani [90], is an estimated resemblance exploration method that mechanisms proficiently even for high-dimensional data. It has extended specific regard for copy-move detection [91], [92], by means of it is supplementary robust to image dispensation and can be still

quite fast. The purpose of LSH is to crack the (r, $\epsilon$)-NN resemblance exploration problem in sub-linear while. If, for a point q (query) in d-dimensional space, there occurs an indexed fact p such that (p, q)r, then LSH will, with extraordinary odds, yield an indexed fact p′ such that d(p′, q)(1 + $\epsilon$)r. If no indexed point lies surrounded by (1 + $\epsilon$)r of q, at that moment LSH will yield nonentity with high odds. This is attained by dint of a set of distinct hash functions. The hash functions content the instinctive conception that the odds of a hash impact for two facts be linked to the likeness (distance) among the facts. LSH diminishes the false negatives level by means of multiple hash functions in equivalent.

## V. COPY-MOVE FORGERY (CMF)

Copy-move Forgery (CMF) is most common technique that is used in digital image forgery [93]. The working is depend on the partition of an image, in which every part of image is first copied and then moved to another place in the similar image. There are two main reasons behind this forgery: first to hide and image and another to add content. However, forged region has been accessed from the same image, it is not probable to use the properties of statistical, for instance: camera noise or illumination conditions for forgery detection, the reason behind this, within the image, the forgery detection is well matched. Simplification of forgery process has also been defined by taking the forged region from the same region, for the reason that it is easier to fitting the forged region into the image due to the correspondence of properties of the copied region and the rest of image.

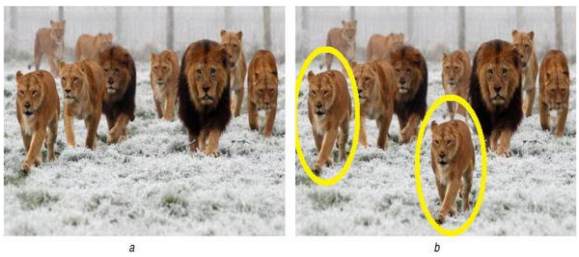

**Figure 2:** Example of copy move forgery

The main type of forgery is Plain copy-move forgery in which the working is depend on the translation, i.e. copied area is to be translated to a new space in the similar image, but with one condition, i.e. no changes in properties of the copied area. Hence, in that type of forgery, two identical areas are to be contained in the image which creates plain copy-move forgery detection rather easy to implement.

More complex categories of forgery can be done by transformation of a copied region before translation to a new location. Below are the possible transformations of copied regions:

1. scaling – expanding or shrinking of a copied area by an equal scale factor in all directions,

2. rotation – circular moving of a copied area around a middle of rotation by an arbitrary angle,
3. distortion – expanding or shrinking of a copied area by a scale aspect that is not the same in all directions,
4. combination – application of more than one transformation of a copied area.

The outcome of transformations by applying is a change in the copied area's properties. Therefore, searching for forgeries is not as simple as in the situation of plain CMF. There are some instances of CMFs from the CoMoFoD database [94].

By applying some post-processing methods, various forgery traces are to be hiding. By this, it is probable to apply a post-processing technique on the whole image after forgery, but sometimes post-processing is applied only on copied region borders to assure better fitting with the new background. In post-processing methods, commonly used in digital image forgery methods are JPEG compression, addition of noise and image blurring.

## VI. COPY-MOVE FORGERY DETECTION (CMFD)

Recognition of copy-move forgery has been extensively investigated [95]. Established approaches for copy-move forgery detection can be regarded as as keypoint-based and block-based methods. Keypoint-based methods embrace scanning of the entire image with the target of verdict points of attention (for example, point with high entropy). Those opinions are then examined to select only point with the identical possessions and distinguish analogous zones in the image. Various prevalent instances of keypoint-based methods are SIFT (Scale-invariant feature transform) [96] and SURF (Speeded Up Robust Features) [97].

Block-based approaches comprise separating an image into insignificant overlying blocks as a leading phase of the process. A set of features is then intended for each definite block, and those features are castoff for detection of analogous blocks in the image. Diverse sets of features, for instance DCT (Discrete Cosine Transform) [95] / DWT (Discrete Wavelet Transform) [98] factors, Zernike moments [100] or PCA (Principal Component Analysis) [99], have been projected for practice in block-based methods, but the usage of cellular automata for this drive is a wholly new methodology.

- **Block-Based Method for CMFD**

In general all block-based copy move forgery detection approaches track analogous phases:

1. First the image is pre-processed since most algorithms necessitate only the luminance component evidence, and so it is required to alter images to grayscale space. From time to time Gaussian pyramid decomposition is also smeared (as, in [101]).

2. Afterward pre-processing, an image is alienated into overlying blocks by gliding a predefined window by one pixel through the whole image. The size of the window is frequently insignificant (for illustration, 8×8, 16×16, 24×24 pixels) to guarantee recognition of zones of all magnitudes. Distributing an N×M image into overlying blocks of size b×b leads to a very bulky numeral of altered blocks affording to equation (3) (for illustration: distributing a 512×512 image by means of a 8×8 window yields 255,025 dissimilar blocks).

$$N_b = (N - b + 1) \times (M - b + 1) \tag{3}$$

3. For each definite block a feature vector f is intended by identical process. The feature vector is castoff as a condensed depiction of a block since it comprehends evidence about texture, shape, orientation or certain other assets of a block. The scale of the feature vector hinges on a selection of way for its deviousness.
4. Smearing brute-force exploration to catch analogous blocks by communal evaluation of all pairs of blocks entails a proportion of computational time and assets. Consequently, altogether feature vectors are warehoused in one matrix that is organized by particular procedure (for sample, lexicography categorization) to undertake assemblage of analogous blocks. Alongside categorization, several supplementary ways and means for vindicating analogous blocks can be pragmatic, for instance, kd-tree.
5. Neighbor feature vectors in the organized matrix are than paralleled by scrutinizing the correspondence among them, via the Euclidean distances concerning feature vector elements rendering to equation (4). All pairs of blocks with remoteness v advanced than certain predefined threshold Ts are detached from the set of probable outcomes. Assortment of threshold Ts contingent on the category of forgery, for specimen, it can be agreed to zero for plain CMF, or it has to be attuned to specific higher values if any transformations/post-processing procedures are smeared. Afterward this phase only analogous pairs of blocks are held in reserve as probable outcomes.

$$v = \sqrt{\sum_{i=1}^{size(f)} (f_1(i) - f_2(i))^2} \tag{4}$$

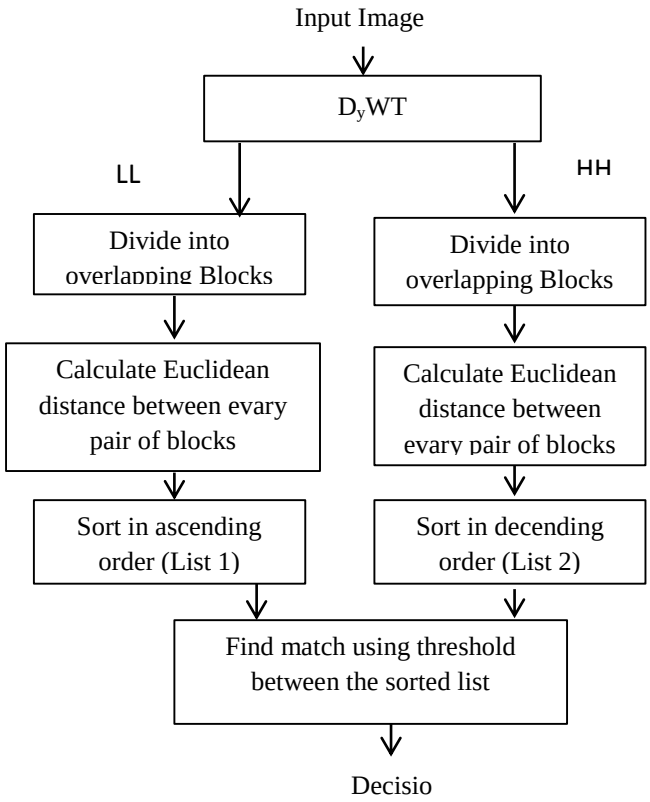


**Figure 3:** Block based method for CMFD

6. The set of probable grades is scrutinized another time and Euclidean distance d is intended among coordinates of blocks of every pair conferring to equation (5). Altogether pairs with distance d lesser than predefined threshold Td are unconcerned from the set of potential consequences. Threshold Td is frequently demarcated conferring to a selection of block dimensions (for specimen, k×b, where k is certain slight positive constant) to eradicate all close by blocks (it can be presumed that a block is progressed more than Td pixels). Subsequently these pace only alike pairs of blocks that are not close by to each other are retained as potential matches.

$$d = \sqrt{(x_{f1} - x_{f2})^2 + (y_{f1} - y_{f2})^2} \tag{5}$$

7. The recognition image is engendered by coloration all enduring pairs of blocks. Some meek post-processing can be pragmatic to take away insignificant, deceitfully perceived zones in the image (for specimen, morphological opening).

- **Possible Feature Vectors**

Outlining an applicable feature set is a communal delinquent in block-based approaches, since features have to return similar outcomes for redid blocks regardless of the alteration of the imitative area or smeared post-processing approaches. Dissimilar sets of feature vectors for block-based CMFD have been anticipated [102].

One of the principal tactics used quantized frequency factors of the Discrete Cosine Transform (DCT) [95] as features. Appreciations to the possessions of DCT, it contributes good consequences in circumstances of added compression, noise, and retouching. An analogous methodology is accessible by Bashar et al. [98], where the factors of a DiscreteWavelet Transform (DWT) by means of Haar-Wavelets were familiarized. Bayram et al. [103] endorsed expending the Fourier-Mellin Transform (FMT) aimed at engendering feature vectors.

Popescu and Farid [99] totaled Principal Component Analysis (PCA) to condense the feature set dimensions. This depiction is stout to compression and adding of noise, but any transformation of the imitative region (for specimen, rotation, scaling) would upset the eigenvalues. Far along this methodology is prolonged by distributing every block into 4 sub-blocks expending the Discrete Wavelet Transform (DWT) [104]. An analogous methodology to [99] was anticipated in [105], where Singular Value Decomposition (SVD) was castoff.

Luo et al. [106] acquaint with features grounded on the concentration of pixels in blocks. The leading three values of the feature vectors encompassed the average of the red, blue and green color modules. The respite of the feature vector was demarcated by isolating of the block into 2 identical parts in 4 directions and manipulative the proportion of each fragment's intensity as regards the intensity of the entire block. Bravo-Solorio et al. [107] recycled the same three constituents as in the preceding technique with the accumulation of the entropy of a block. A analogous methodology is untaken in [108] where every block was alienated into 4 sub-blocks and the feature vector is demarcated as a proportion of intensities of those sub-blocks. In the circle methodology, projected in [101], the image is main condensed in measurement by Gaussian pyramid disintegration and every block is alienated into four concentric circles. The feature vector is intended as a mean of the image pixel rate in each one circular region of each block.

Wang et al. [109] make known to the first four Hu moments as features. The image is first condensed in measurement by Gaussian pyramid disintegration, and the Hu moments are figured from the overlying blocks of the low-frequency image. The practice of Zernike moments of grade 5 as features was projected by Ryu et al. [100].

## VII. ROTATION INVARIANT FEATURE

- **LBP Operator**

LBP operator is an operative texture depiction operator. It has been efficaciously smeared in image processing zones these ages. Subsequent, familiarize how to

evaluate the LBP value. In 3 × 3 window, the gray value of the midpoint point of the frame as a threshold value, supplementary pixels in the frame do binarized handling, engenders an 8-bit binary string. Then, conferring to the dissimilar locations of the pixels, acquire the LBP value of the frame by weighted summing. It can be figured by

$$LBP = \sum_{i=0}^{7} s(g_i - g_c)2^i, where\, s(\mathrm{x}) = \begin{cases} 1\ x \geq 0 \\ 0\ x < 0 \end{cases} \quad (6)$$

Here $g_c$ is the center pixel of the frame, $g_i$ symbolizes adjoining pixels. In general the direction of the neighboring pixels is underway by the pixel to the right of the center pixel, counterclockwise patent. The LBP value can imitate the texture evidence for the province [24]. LBP can be extended to a circular neighborhood. Expending (P, R) to designate the neighborhood, where P symbolizes the number of sampling points, R is the radius of the neighborhood. The gray values of neighbors which do not fall accurately in the center of pixels are projected by exclamation.

- **Rotation Invariance**

The $LBP_{P,R}$ operator yields $2^P$ dissimilar output values, conforming to $2^P$ different binary patterns that can be made by the P pixels in the neighbor set. When the image is rotated, the gray values $g_i$ will transfer along the perimeter of the circle. After rotation, a particular binary pattern consequences in a dissimilar $LBP_{P,R}$ value. This does not smear to patterns encompassing of only 0 (or 1) which persist constant at all rotation angles. To eradicate the influence of rotation, allocate a unique identifier to each rotation invariant local binary pattern, it is demarcated as:

$$LBP_{P,R}^{ri} = \min\left\{ROR(\mathrm{LBP}_{P,R,i}), i = 0,1,....\mathrm{P}-1\right\} \quad (7)$$

where ROR(x,i) accomplishes a circular bit-wise right shift on the P-bit number x i times, superscript ri means rotation invariant. $LBP_{P,\mathrm{R}}^{ri}$ quantifies the existence statistics of individual rotation invariant patterns conforming to certain features in the image, hence, the patterns can be well-thought-out as feature detectors. In the instance of P = 8, $LBP_{P,\mathrm{R}}^{ri}$ will produce 36 different values or 36 patterns. Let vector V symbolizes the manifestation number of individual patterns. When block is rotated, $V'$ is mined. It is anticipated that V and $V'$ are analogous, the correlation coefficients between them is adjacent to 1. Associate the resemblance between V and $V'$, it is tranquil to recognize the replicated blocks.

$$corr2(\mathrm{V},\mathrm{V}') = \left(\sum_m\sum_n (\mathrm{V}_{mn} - \bar{\mathrm{V}})^2\right) / \sqrt{\left(\sum_m\sum_n (\mathrm{V}_{mn} - \bar{\mathrm{V}})^2\right)\left(\sum_m\sum_n (\mathrm{V}'_{mn} - \bar{\mathrm{V}}')^2\right)} \quad 8)$$

## VIII. CONCLUSION

In this, based methods and feature based methods has been studied. It is found that there are different sets of features, such as DCT (Discrete Cosine Transform) / DWT (Discrete Wavelet Transform) coefficients, PCA (Principal Component Analysis) or Zernike moments, use in block-based methods, but the cellular automata is a completely new approach. Block-based approaches is effective to detect duplicated regions, the accuracy of these kinds of methods is still unsatisfactory while performing on the geometrical transformed objects. To overcome this issue, feature-based techniques are used to match features in the image. In this, the transformations that can be applied to copied regions i.e. scaling, rotation, distortion and combination has been studied. It is found that these transformations change the properties of copied area. The popular examples of key-point based methods has also been studied such as SIFT (Scale-invariant feature transform) and SURF (Speeded Up Robust Features). The Rotation Invariant Feature has also been studied in which LBP operator and rotation invariance is analyzed in detail.

## REFERENCES

[1] Christlein, V., Riess, C., and Jordan, J., 2012, "An evaluation of popular copy-move forgery detection approaches," IEEE Transactions on Information Forensics and Security Vol.7, Issue.6, pp.1841–1854.

[2] Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., and Ren, K., 2016, "A privacy-preserving and copy-deterrence content based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security Vol.11, Issue.11, pp.2594–2608.

[3] Zhili, Z., Nung, Y. C., and Xingming, S., 2016, "Effective and efficient image copy detection with resistance to arbitrary rotation," IEICE Transactions on Information and Systems Vol.99, Issue.6, pp.1531–1540.

[4] Zhou, Z., Wang, Y., and Wu, Q., 2017, "Effective and efficient global context verification for image copy detection," IEEE Transactions on Information Forensics and Security Vol.12, Issue.1, pp.48–63

[5] Pandey, R., Singh, S., and Shukla, K., 2016, "Passive forensics in image and video using noise features: a review," Digital Investigation, Vol. 19, pp.1–28

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

[7] Bi, X., Pun, C.M., and Yuan, X.C., 2016, "Multi-level dense descriptor and hierarchical feature matching for copy move forgery detection," Inf Sci Vol.345, pp.226–242

[8] Cozzolino, D., Poggi, G., and Verdoliva, L., 2015, "Efficient dense-field copy–move forgery detection," IEEE Transactions on Information Forensics and Security Vol. 10, Issue.11, pp.2284–2297

[9] Ryu, S.J., Kirchner, M., and Lee, M.J., 2013, "Rotation invariant localization of duplicated image regions based on Zernike moments," IEEE Transactions on Information Forensics and Security, Vol.8, Issue.8, pp.1355–1370

[10] Lee, J.C., Chang, C.P., and Chen, W.K., 2015, "Detection of copy–move image forgery using histogram of orientated gradients," Information Sciences, Vol.321, pp.250–262

[11] Wu, Q., Wang, S., and Zhang, X., 2011, "Log-polar based scheme for revealing duplicated regions in digital images," IEEE Signal Process Lett Vol.18, Issue.10, pp.559–562

[12] Cozzolino, D., Poggi, G., and Verdoliva, L., 2014, "Copy-move forgery detection based on patchmatch," I.E. International Conference on Image Processing (ICIP), Paris, France, pp.5312–5316

[13] Xiang-yang, W., Yu-nan, L., Huan, X., Pei, W., and Hong-ying, Y., 2018, "Robust copy-move forgery detection using quaternion exponent moments," Pattern Analysis and Applications, Vol. 21,Issue. 2,pp. 451–467

[14] Lee, J.C., 2015, "Copy-move image forgery detection based on Gabor magnitude," Journal of Visual Communication and Image Representation, Vol. 31, pp.320–334

[15] Pan, X., and Lyu, S., 2010, "Region duplication detection using image feature matching," IEEE Transactions on Information Forensics and Security Vol.5, Issue.4, pp.857–867

[16] Chen, L., Lu, W., and Ni, J., 2013, "Region duplication detection based on Harris corner points and step sector statistics," J Vis Commun Image Represent Vol.24, Issue.3, pp.244–254

[17] Zandi, M., Mahmoudi-Aznaveh, A., and Talebpour, A., 2016, "Iterative copy-move forgery detection based on a new interest point detector," IEEE Trans Inf Forensics Secur Vol.11, Issue.11, pp.2499–2512

[18] Silva, E., Carvalho, T., and Ferreira, A., 2015, "Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes," Journal of Visual Communication and Image Representation, Vol.29, pp. 16–32

[19] Yu, L., Han, Q., and Niu, X., 2016, "Feature point-based copy-move forgery detection: covering the non-textured areas," Multimedia Tools and Applications, Vol.75, Issue.2, pp.1159–1176

[20] Costanzo, A., Amerini, I., and Caldelli, R., 2014, "Forensic analysis of SIFT keypoint removal and injection," IEEE Transactions on Information Forensics and Security, Vol.9, Issue, 9, pp.1450–1464

[21] Pun, C.M., Yuan, X.C., and Bi, X.L., 2015, "Image forgery detection using adaptive over segmentation and feature point matching," IEEE Transactions on Information Forensics and Security, Vol.10, Issue.8, pp.1705–1716

[22] Ardizzone, E., Bruno, A., and Mazzola, G., 2015, "Copy-move forgery

detection by matching triangles of keypoints," IEEE Transactions on Information Forensics and Security, Vol.10, Issue.10, pp.2084–2094

[23] Amerini, I., Ballan, L., and Caldelli, R., 2013, "Copy-move forgery detection and localization by means of robust clustering with J-linkage," Signal Processing: Image Communication, Vol.28, Issue.6, pp.659–669

[24] Zheng, N., Wang Y., and Ming, X., 2013, "A LBP-Based Method for Detecting Copy-Move Forgery with Rotation," Multimedia and Ubiquitous Engineering, pp. 261-267

[25] Alkawaz, M. H., Sulong, G., Saba, T., and Rehman, A., 2016, "Detection of copy-move image forgery based on discrete cosine transform," Neural Computing and Applications, pp, 1–10

[26] Sachdev, K., Kaur M., and Gupta, S., 2017, "A Robust and Fast Technique to Detect Copy Move Forgery in Digital Images Using SLIC Segmentation and SURF Keypoints," Proceeding of International Conference on Intelligent Communication, Control and Devices, pp. 787-793

[27] Sondos, M. F., Semary, N. A., and Hadhoud, M.M., 2014, "Fan Search for Image Copy-Move Forgery Detection," Advanced Machine Learning Technologies and Applications pp. 177-186

[28] Yang, H., Niu, Y., Jiao, L., Liu, Y., Wang, X., and Zhou, Z., 2017, "Robust copy-move forgery detection based on multi-granularity Superpixels matching," Multimedia Tools and Applications., pp. 1–27

[29] Yang, B., Sun, X., Guo, H., Xia, Z., and Chen, X. 2018, "A copy-move forgery detection method based on CMFD-SIFT," Multimedia Tools and Applications, Vol.77, Issue.1, pp 837–855

[30] Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., and Yang, H., 2016, "Fusion of block and keypoints based approaches for effective copy-move image forgery detection," Multidimensional Systems and Signal Processing, Vol.27, Issue.4, pp.989–1005

[31] Osamah, M., Qershi, A., and Khoo, B. E., 2017, "Comparison of Matching Methods for Copy-Move Image Forgery Detection," 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, pp.209-218

[32] Osamah, M., Qershi, A. and Khoo, B. E., 2016, "Copy-Move Forgery Detection Using on Locality Sensitive Hashing and k-means Clustering," Information Science and Applications (ICISA) pp. 663-672

[33] Jiachang, G., and Guo, J., 2016, "Image copy-move forgery detection using SURF in opponent color space," Transactions of Tianjin University, Vol. 22, Issue.2, pp 151–157

[34] Doyoddorj, M., and Rhee, K. H., 2013, "Robust Copy-Move Forgery Detection Based on Dual-Transform," International Conference on Digital Forensics and Cyber Crime pp. 3-16

[35] Retha, A., Khayeat, H., Rosin, P. L., and Sun, X., 2017, "Copy-Move Forgery Detection Using the Segment Gradient Orientation Histogram," Scandinavian Conference on Image Analysis, pp. 209-220

[36] Osamah, M., Qershi, A., and Khoo, B. E., 2014, "Enhanced Matching Method for Copy-Move Forgery Detection by Means of Zernike Moments," International Workshop on Digital Watermarking IWDW 2014: Digital-Forensics and Watermarking pp. 485-497

[37] Malviya, A., and Ladhake, S., 2016, "An Image Forensic Technique for Detection of Copy-Move Forgery in Digital Image," International Symposium on Security in Computing and Communication SSCC 2016: Security in Computing and Communications, pp. 328-335

[38] Tralic, D., Grgic, S., Sun, X., and Rosin, P. L., 2016, "Combining cellular automata and local binary patterns for copy-move forgery detection," Multimedia Tools and Applications, Vol.75, Issue.24, pp.16881–16903

[39] Manu, V.T., and Mehtre, B.M. 2016, "Detection of Copy-Move Forgery in Images Using Segmentation and SURF," Advances in Signal Processing and Intelligent Recognition Systems, pp. 645-654

[40] Sekhar, R., and Shaji, R.S., 2016, "A Study on Segmentation-Based Copy-Move Forgery Detection Using DAISY Descriptor," Proceedings of the International Conference on Soft Computing Systems, pp. 223-233

[41] Zhong, J., Gan, Y., Young, J., Huang, L., and Lin, P., 2017, "A new block-based method for copy move forgery detection under image geometric transforms," Multimedia Tools and Applications, Vol.76, Issue.13, pp. 14887–14903

[42] Zhang, W., Yang, Z., Niu, S., and Wang, J., 2016, "Detection of Copy-Move Forgery in Flat Region Based on Feature Enhancement," International Workshop on Digital Watermarking IWDW 2016: Digital Forensics and watermarking pp.159-171

[43] Park, C. S., and Choeh, J. Y. 2017, "Fast and robust copy-move forgery detection based on scale-space representation," Multimedia Tools and Applications, pp.1–17

[44] Zhu, Y., Shen, X., and Chen, H., 2016 "Copy-move forgery detection based on scaled ORB," Multimedia Tools and Applications, Vol.75, Issue.6, pp.3221–3233

[45] Zhong, J., and Gan, Y. 2016 "Detection of copy–move forgery using discrete analytical Fourier–Mellin transform," Nonlinear Dynamics, Vol.84, Issue.1, pp.189–202

[46] Yu, L., Han, Q., and Niu, X., 2016 "Feature point-based copy-move forgery detection: covering the non-textured areas," Multimedia Tools and Applications, Vol. 75, Issue.2, pp.1159–1176

[47] Emam, M., Han, Q., and Niu, X., 2016, "PCET based copy-move forgery detection in images under geometric transforms," Multimedia Tools and

Applications, Vol.75, Issue.18, pp.11513–11527

[48] Liu, Y., Guan, Q., and Zhao, X., 2017, "Copy-move forgery detection based on convolutional kernel network," Multimedia Tools and Applications, pp. 1–25

[49] Pandey, R. C., Agrawal, R., Singh, S. K., and Shukla, K.K., 2014, "Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features," Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) pp. 659-666

[50] Tralic, D., Rosin, P. L., Sun, X., and Grgic, S., 2014, "Copy-Move Forgery Detection Using Cellular Automata," Cellular Automata in Image Processing and Geometry pp. 105-125

[51] Khayeat, A. R. H., Sun, X., and Rosin, P. L., 2016 "Improved DSIFT Descriptor Based Copy-Rotate-Move Forgery Detection," Pacific-Rim Symposium on Image and Video Technology Image and Video Technology, pp.642-655

[52] Anand, V., Hashmi, M. F., and Keskar, A. G., 2014, "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods," Asian Conference on Intelligent Information and Database Systems, pp. 530-542

[53] Wang, X.Y., Li, S., Liu, Y.N., Niu, Y., Yang, H.Y., and Zhou, Z., 2017, "A new keypoint-based copy-move forgery detection for small smooth regions," Multimedia Tools and Applications, Vol.76, Issue.22, pp. 23353–23382

[54] Xiu, L. B., Pun, C.M., and Yuan, X.C., 2018, "Multi-scale feature extraction and adaptive matching for copy-move forgery detection," Multimedia Tools and Applications, Vol.77, Issue.1, pp.363–385

[55] Wu, Y. J., Deng, Y., Duan, H.B., and Zhou, L.N., 2014, "Dual tree complex wavelet transform approach to copy-rotate-move forgery detection," Science China Information Sciences, Vol.57, Issue.1, pp.1–12

[56] Oommen, R. S., Jayamohan, M., and Sruthy, S., 2016, "Scale Invariant Detection of Copy-Move Forgery Using Fractal Dimension and Singular Values," Advances in Signal Processing and Intelligent Recognition Systems, pp.559-570

[57] Wang, X.Y., Liu, Y., Xu, H., Wang, P., and Yang, H., 2016, "Robust copy–move forgery detection using quaternion exponent moments," Pattern Analysis and Applications, pp. 1–17

[58] Sheng, Y. Z., Wang, H. J., and Zhang, G. Q., 2013, "Comparison and Analysis of Copy-Move Forgery Detection Algorithms for Electronic Image Processing," Advances in Mechanical and Electronic Engineering, pp. 343-348

[59] Jaberi, M., Bebis, G., Hussain, M., and Muhammad, G., 2014, "Accurate and robust localization of duplicated region in copy–move image forgery," Machine Vision and Applications, Vol. 25, Issue.2, pp.451–475

[60] Sadeghi, S., Dadkhah, S., Jalab, H. A., Mazzola, G., and Uliyan, D., 2017 "State of the art in passive digital image forgery detection: copy-move image forgery," Pattern Analysis and Applications, pp. 1–16

[61] Yang, P., Yang, G., and Zhang, D., 2016, "Rotation Invariant Local Binary Pattern for Blind Detection of Copy-Move Forgery with Affine Transform," International Conference on Cloud Computing and Security, pp. 404-416

[62] Park, C., Kim, C., Lee, J., and Kwon, G. R., 2016, "Rotation and scale invariant upsampled log-polar fourier descriptor for copy-move forgery detection," Multimedia Tools and Applications, Vol.75, Issue.23, pp. 16577–16595

[63] Fridrich, J., Soukal, B.D., and Lukas, A.J., 2003, "Detection of copy-move forgery in digital images," In: Proceedings of Digital Forensic Research Workshop, Cleveland

[64] Popescu, A.C., Farid, and H., 2005, "Exposing digital forgeries by detecting traces of resampling," IEEE Trans Signal Process Vol. 53, pp.758–767

[65] Muhammad, G., Hussain, M., and Bebis, G., 2012, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digit Investig Vol.9,pp.49–57

[66] Yang, B., Sun, X., Chen, X., Zhang, J., and Li, X., 2013, "An efficient forensic method for copy-move forgery detection based on DWT-FWHT," Radio engineering Vol.22, pp.1098–1105

[67] Kakar, P., and Sudha, and N., 2012, "Exposing Postprocessed copy-paste forgeries through transform-invariant features," IEEE Transactions on Information Forensics and Security Vol.7, pp.1018–1028

[68] Chen, B., Shu, H., Coatrieux, G., Chen, G., Sun, X., and Coatrieux, J.L., 2015, "Color image analysis by quaternion-type moments," Journal of Mathematical Imaging and Vision Vol.51, pp.124–144

[69] Amerini, I., Barni, M., Caldelli, R., and Costanzo, A., 2013, "Counter-forensics of SIFT-based copy-move detection by means of keypoint classification," EURASIP Journal on Image and Video Processing, pp.1–17

[70] Amerini, I., Ballan, L., Caldelli, R., Del, A. B., and Serra, G., 2011, "A SIFT-based forensic method for copymove attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security Vol.6, pp.1099–1110

[71] Pan, X., and Lyu, S., 2010, "Region duplication detection using image feature matching," IEEE Transactions on Information Forensics and Security Vol. 5, pp.857–867

[72] Neamtu, C., Barca, C., Achimescu, E., and Gavriloaia, B., 2013, "Exposing copy-move image tampering using forensic method based on SURF," International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–4

[73] Bay, H., Ess, A., Tuytelaars, T., and Van, G. L., 2008, "Speeded-up robust features (SURF)," Computer Vision and Image Understanding, Vol. 110, pp.346–359

[74] Luo, J., and Oubong, G., 2009, "A comparison of SIFT, PCA-SIFT and SURF," International Journal of Image Processing, Vol.3, pp.143–152

[75] Zhu, Y., Shen, X. and Chen, H., 2015, "Copy-move forgery detection based on scaled ORB," Multimedia Tools and Applications, pp.1–13

[76] Gu, B., and Sheng, V.S., 2016, "A robust regularization path algorithm for v-support vector classification," IEEE Transactions on Neural Networks and Learning Systems, pp: 1–8

[77] Gu, B., Sheng, V.S., Tay, K.Y., Romano, W., and Li, S., 2015, "Incremental support vector learning for ordinal regression," IEEE Transactions on Neural Networks and Learning Systems Vol.26, pp.1403–1416

[78] Wen, X., Shao, L., Xue, Y., and Fang, W., 2015, "A rapid learning algorithm for vehicle classification," Information Sciences, Vol.295, pp.395–406

[79] Cozzolino, D., Poggi, G., and Verdoliva, L., 2015, "Efficient dense-field copy–move forgery detection," IEEE Transactions on Information Forensics and Security, Vol. 10, pp.2284–2297

[80] Li, J., Li, X., Yang, B., and Sun, X., 2015, "Segmentation-based image copy-move forgery detection scheme," IEEE Transactions on Information Forensics and Security, Vol. 10, pp.507–518

[81] Bi, X., Pun, C.M., and Yuan, X.C., 2016, "Multi-level dense descriptor and hierarchical feature matching for copy– move forgery detection," Information Sciences, Vol.345, pp.226–242

[82] Kim, H.S., and Lee, H.K., 2003, "Invariant image watermark using zernike moments," IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, pp.766–775

[83] Teh, C.H., and Chin, R.T., 1988, "On image analysis by the methods of moments," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.10, pp.496–513

[84] Solorio, S. B., and Nandi, A.K., 2011, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," Signal Processing, Vol. 91, Issue.8, pp.1759–1770

[85] Al-Qershi, O.M., and Khoo, B.E., 2014, "Enhanced matching method for copy-move forgery detection by means of zernike moments," Digital-forensics and watermarking, Springer, pp. 485–497

[86] Lynch, G., Shih, F.Y., and Liao, H.Y.M., 2013, "An efficient expanding block algorithm for image copymove forgery detection," Information Sciences, Vol.239, pp.253–265

[87] Bentley, J.L., 1975, "Multidimensional binary search trees used for associative searching," Communications of the ACM, Vol.18, pp.509–517

[88] Shivakumar, B., and Baboo, L.D.S.S., 2011, "Detection of region duplication forgery in digital images using surf," IJCSI International Journal of Computer Science Issues, Vol.8

[89] Langille, A., and Gong, M., 2006, "An efficient match-based duplication detection algorithm," The 3rd Canadian conference on computer and robot vision. IEEE, pp. 64–64

[90] Indyk, P., and Motwani, R., 1998, "Approximate nearest neighbors: towards removing the curse of dimensionality," Proceedings of the thirtieth annual ACM symposium on theory of computing, ACM, pp. 604–613

[91] Ryu, S.J., Kirchner, M., Lee, M.J., and Lee, H.K., 2013, "Rotation invariant localization of duplicated image regions based on zernike moments," IEEE Transactions on Information Forensics and Security, Vol.8, pp.1355–1370

[92] Li, Y., 2013, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," Forensic Science International, Vol.224, pp.59–67

[93] Shivakumar, B.L., and Baboo, S., 2010, "Detecting copy-move forgery in digital images: A survey and analysis of current methods," Global Journal of Computer Science and Technology, Vol.10, Issue.7, pp.61–65

[94] Tralic, D., Zupancic, I., Grgic, S., and Grgic, M., 2013, "Comofod-new database for copy-move forgery detection," In: Proc. 55th International Symposium ELMAR, pp. 49–54

[95] Fridrich, J., Soukal, D., and Lukas, J., 2003, "Detection of copy move forgery in digital images," In: Proc. Digital Forensic Research Workshop

[96] Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., and Serra, G., 2011, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, Vol.6, Issue.3, pp.1099–1110

[97] Shivakumar, B.L., and Baboo, S., 2011, "Detection of region duplication forgery in digital images using surf," International Journal of Computer Science Issues, Vol.8, Issue.4, pp.199–205

[98] Bashar, M., Noda, K., Ohnishi, N., and Mori, K., 2010, "Exploring duplicated regions in natural images," IEEE Transactions on Image Processing

[99] Popescu, A., and Farid, H., 2004, "Exposing digital forgeries by detecting duplicated image regions," Tech. rep. tr2004-515, Dartmouth College

[100] Ryu, S.J., Lee, M.J., and Lee, H.K., 2010, "Detection of copy-rotate-move forgery using zernike moments," International Workshop on Information Hiding, pp. 51–65

[101] Wang, J., Liu, G., Li, H., Dai, Y. and Wang, Z., 2009, "Detection of image region duplication forgery using model with circle blocks," International Conference on Multimedia Information Networking and Security, Hubei, pp. 25-29

[102] Christlein, V., Riess, C., Jordan, J., Riess, C., and Angelopoulou, E., 2012, "An evaluation of popular copy-move forgery detection approaches," IEEE Information Forensics and Security, Vol.7, Issue.6, pp.1841–1854

[103] Bayram, S., Sencar, H., and Memon, N., 2009, "An efficient and robust method for detecting copymove forgery," IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 1053–1056

[104] Li, G., Wu, Q., Tu, D., and Sun, S., 2007, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd," IEEE International Conference on Multimedia and Expo, pp. 1750–1753

[105] Kang, X., and Wei, S., 2008, "Identifying tampered regions using singular value decomposition in digital image forensics," International Conference on Computer Science and Software Engineering, New York, Vol. 3, pp. 926–930,

[106] Luo, W., Huang, J., and Qiu, G., 2006, "Robust detection of region-duplication forgery in digital images," IEEE Information Forensics and Security Vol.4, pp.746–749

[107] Solorio, S. B., and Nandi, A.K., 2011, "Exposing duplicated regions affected by reflection, rotation and scaling," International Conference on Acoustics, Speech and Signal Processing, pp. 1880–1883

[108] Lin, H., Wang, C., and Kao, Y., 2009, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, Vol.5, Issue.5, pp.188–197

[109] Wang, J., Liu, G., Zhang, Z., Dai, Y., and Wang, Z., 2009, "Fast and robust forensics for image region-duplication forgery," Acta Automatica Sinica, Vol.35, Issue.12, pp.1488–1495

**AUTHORS PROFILE**

**Ms. Gurpreet Kaur** is an Assistant Professor and has more than 9 years of academic experience.She has done M.Sc (C.S.) degree from Guru Nanak Dev Universiy,Amritsar in 2009 and received MCA degree from Lovely professional University,Jalandhar in 2014.She has published 4 papers in different Journals.Her research interest is in the area of Copy,Move Forgery and Rotation Invariant Forgery Detection using LBP variants.

**Dr. Rajan Manro** is an Associate Professor and has more than 14 years of academic experience. He has done MCA degree from GGNIMT, Ludhiana, Punjab, India, in 2004, the Post-Graduation Diploma in E-Commerce From ITI, Ludhiana, Punjab, India in 2001 and received the M.Phil Degree in Computer Science from Periyar University, Salem, India in 2008.He is certified Oracle -9i (DBA) Professional. He is an author of more than 30 books on different subjects like Java, ASP.Net, Artificial Intelligence, MIS, Expert System and RDBMS. More than 14 papers are published in different Journals and conference proceedings. His research interest is in the areas of Cloud Computing, E-Goverance, A.I. etc. and is presently working on it.