Image Forgery and Detection of Copy Move Forgery in Digital Images: A Survey of Recent Forgery Detection Techniques

Ramandeep Kaur
Assistant Professor
DAV College Jalandhar

ABSTRACT

With the development of Image processing editing tools and software, an image is manipulated very easily. The image manipulation detection is essential for the reason that an image can be employed as legal evidence, in the field of forensics investigations, and also in numerous various other fields. The image forgery detection based on pixels aims to validate the digital image authenticity with no aforementioned information of the main image. There are several means intended for tampering a digital image, for example, copy-move or splicing, resampling a digital image (stretch, rotate, resize), removal as well as the addition of an object from your image. Copy move image forgery detection is utilized to figure out the replicated regions as well as the pasted parts, however forgery detection may possibly vary dependant on whether or not there is virtually any post-processing on the replicated part before inserting the item completely to another party. Typically, counterfeiters utilize many operations like rotation, filtering, JPEG compression, resizing as well as the addition of noise to the main image before pasting, that make this thing challenging to recognize the copy move image forgery. Hence, forgery detector needs to be robust to any or all manipulations and also the latest editing software tools. In the literature part, various researchers portrayed the working scenario of copy-move image forgery utilizing the similarity measures as well as the relationship among the original parts of the image and their pasted parts in the similar image. This research paper illustrates recent issues in the techniques of forgery detection and also all their comparative analysis.

Keywords

Image Forgery, Copy-Move Image forgery, Image Forgery Detection, Tampering, Digital Forensics, Duplication forgery Detection

1. INTRODUCTION

The most up-to-date image resolution technologies have provided forgers the various tools for utilizing and changing the desired content of images keeping the goal in mind of embedding deceitful thing to the digital image with no visible capabilities [1]. Keeping this point in mind, it is recommended by several researchers to determine the authenticity of the image to identify these kinds of actions that exist in several applications, for instance, medical imaging, intelligence services, criminal investigation, journalism and surveillance systems.

Accordingly, techniques of digital image forgery have been produced to legitimize the issues of forgery as an important process in digital image processing [2]. Numerous research studies were directed in diverse disturbing fields to upgrade the present techniques of copy-move image forgery [3], which incorporate adding, or hiding an image region or showing off the information which is not correct [4]. The basic techniques of forgery in digital images can be partitioned into three principle categories: Copy-Move (that is, Cloning), Copy-Paste (that is, Splicing), and Image Retouching as demonstrated in Figure 1. For example, the technique of image retouching is effective in manipulating the base image by altering its image features without making discernible changes of the image content.

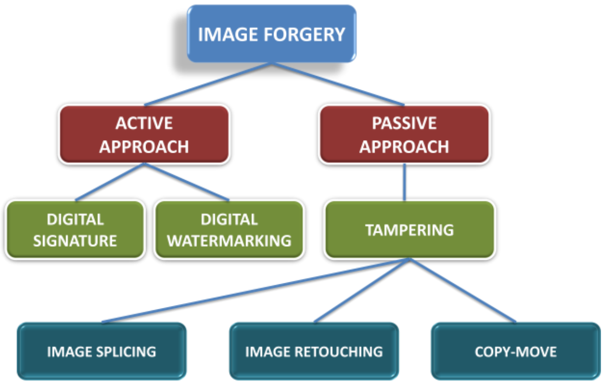

Figure 1-Error! Use the Home tab to apply 0 to the text that you want to appear here.**-1 Classification of Common Image Forgery techniques**

Mostly utilized image tampering technique is usually copy-move image forgery where a portion of the original image is copied and pasted on the same image in to hide the relevant information. Since it is simple and effective to execute that makes it most basic kind of image forgery [4]. A copy-move image forgery is presented in the following Fig.2.

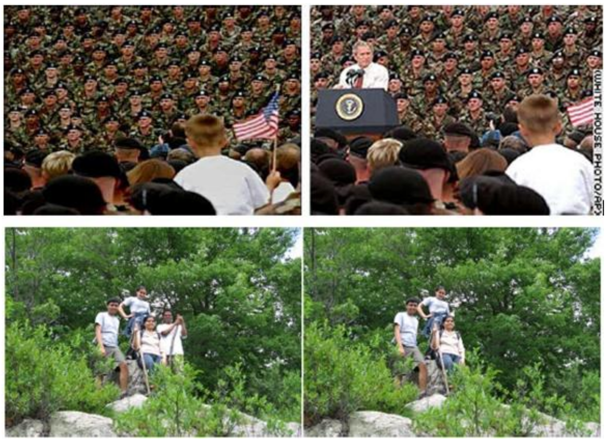

Figure1-2 Example of Copy-Move Image Forgery

Image splicing alternatively, make utilization of primary image with one or more images to create a forged image [5],

[6], these kinds of technique works by incorporating several portion of some other images to the primary image so counterfeiters modify or hide the image content. Moreover, image cloning works by duplicating a specific portion of the image and moving this part to another place of the same image so counterfeiters can duplicate or hide some portion of the image [7]. Consequently, recent efforts in building reliable techniques for image forgery detection have obtained consideration of numerous researchers. Forgery detection technique seen in the literature can be classified into passive methods and active methods [8], [9]. An active image forgery detection technique for example watermarking, this includes embedding the detail of the image in order to portray digital tampering for instance signature, date, name etc. On the other hand passive image forgery detection technique includes detecting forgeries as well as copied materials without taking into account the content of the primary image [10]. The primary objective of this technique is to state how identifying image forgeries usually are achievable with no need of watermark of the original image.

Numerous new image forgery techniques were acquainted by various researchers to depict its workability taking into account the robustness. The key feature of digital image cloning is that, because the copied area is selected from the picture itself, the texture, the noise components and color patterns are perfect with the remaining image. Hence, it is not simple to identify the forgery parts [11], [12]. Additionally, there may be post-processing operations which could possibly make the exposing method harder.

In this paper, the emphasis is on the copy-move (that is, cloning) image forgery detection in conjunction with portraying the issues connected with the detection of forgery. However, I've presented the most recent techniques of forgery detection addressed in the literature.

2. CURRENT ISSUES OF DIGITAL IMAGE FORGERY

As the digital images assume a crucial role in disentangling the method for addressing as well as exchanging ideas flexibly, a consideration has been paid in recent times towards examining the appropriate mechanism for detecting and analyzing image forgery. This consideration was because of the most recent malevolent exercises in which a particular object is copied on the same image. These types of activities can be seen in the case of copy-move image forgery that considers a stands out amongst the most known type of activity which focuses on adding or concealing an object [13],[14]. Numerous scholars have decided that copy-move image forgery works on the grounds of detecting additional noise, texture and color changes and these may be observed in the duplicated area of the image. So, a new technique of copy-move forgery is needed to detect the malicious activities from the digital images [15], [16].

The challenges and issues being addressed in digital image forgery domain are the techniques of forgery detection, social impacts on digital forgeries, and techniques of forgery prevention. The digital image forgeries have numerous implications and perspectives on legal, social, intelligence, technical, security, investigative mechanisms and managerial issues [17],[18]. The forgery detection and creation are related with each other. Figure 2 introduces the workflow of the general image forgery detection methods consists of 4 faces and these four faces are

- Overlapping blocks,
- Feature extraction,
- Block matching, and
- Forgery decision.

The basic utilization of this technique is to identify new forgery in the original image and this task of detecting forgeries is still very challenging. From other point of view, the confidentiality incorporated in the recent forgery approaches introduces a new level of difficulty in forgery detection and forgery creation processes and work like a obstacle to both of the image forgery processes. Figure 2 presents the forgery detection technique consists of 4 faces. This general approach lets you applying different extraction techniques like PCA, DCT, et cetera. It also lets you applying various matching techniques like radix sort and K-D tree.

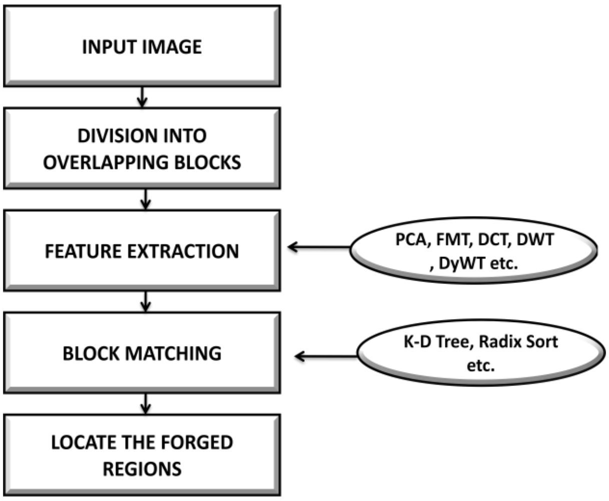
INPUT IMAGE
DIVISION INTO OVERLAPPING BLOCKS
FEATURE EXTRACTION
PCA, FMT, DCT, DWT , DyWT etc.
BLOCK MATCHING
K-D Tree, Radix Sort etc.
LOCATE THE FORGED REGIONS

Figure 2-1 General Approach for Image Forgery Detection

Moreover, the research development in digital forensics has determined the appropriate solutions for handling more wide-ranging issues corresponding to copy-move image forgery. For that reason it's emerging that comprehensive techniques and solutions, generating standardized datasets, evaluation criteria, benchmarks, et cetera are still required to be introduced to recognize the new techniques of reducing the likelihood for digital image forgeries. So, many precise and practical solutions have been developed which research will present in the following section. The basic difficulties which research identified in the literature survey can be classified as:

- Natural category,
- Detection of forgery,
- Flow mapping and
- Identification of source.

2.1 Natural Category

In this natural category, the data of the image includes author name, description, signature, tags, etc are consider as essential features which help to detect the authenticity and originality of the image. Altering these types of data by several forgers may result in forgery. So, the authenticity and originality of images in most of the cases become the difficult task [17], [19]. Researchers have correlated the various natural issues to computer graphics, multimedia, and animation with high-computing devices and algorithms. It is also possible to produce high precision realistic data and images of any sort of events [17], [20]. Differentiating and identifying the image and data captured by realistic computer and acquisition devices is one of the multidimensional problems that need attention.

This comes with the recent digital editing softwares, manipulations and alteration that make these processes easier for the image forgers to hide or add information in the digital images; so, it is a threatening and complex problem [21]. Specific to forgery detection, digital images can be manipulated in different ways just with the help of simple operations such as affine transforms (for example shearing, rotation, scaling and translation), several compensation operations (such as color, contrast adjustments, brightness, blurring and enhancement) and lastly suppression operation (for example compression, filtering, and noise addition) [22]. Furthermore many complex operations are likewise feasible for instance cropping, compositing, matting, blending, as well as photomontage results in visually undetectable artifacts in the digital image [13]. The scientific and automatic method of identifying forged images is the challenging problem for many researchers.

2.2 Detection of Forgery

Methods of forgery detection become much more difficult to deal with the recent techniques of forgery. This is only due to the availability of various digital image editing softwares, manipulation and alteration become very easier for forgers and so image forgery identification becomes the threatening problem [23]. Detection of image forgeries can be altered in several ways just with the help of simple operations such as affine transforms for example shearing, rotation, scaling and translation, several compensation operations such as color, contrast adjustments, brightness, blurring and enhancement and lastly suppression operation (for example compression, filtering, and noise addition [9]. Furthermore many complex operations are likewise feasible for instance cropping, compositing, matting, blending, as well as photomontage results in visually undetectable artifacts in the digital image [24]. The scientific and automatic method of identifying forged images is the challenging problem for many researchers.

2.3 Flow Mapping

Flow mapping helps you to supply more information about the source of the forgery in which the cloned areas can be checked being utilized later on in distinguishing the pasted areas in the identical image. Difficulties to name the origin of the source back to the fast internet availability and easy accessibility of high quality image editing tools which raises the issue of legitimacy of digital resources,, the technology associated with digital resources is usually moving at much speedier rate because of social network websites [25]. Hence discovering the history associated with digital resources turned to a vital issue. A few initiatives associated with finding the flow (linage) associated with data will be made in some sort of networked domain [26]. To find the best answers to solve issues relevant to the legitimacy of the scholarly resources, researchers have shown most of these factors as an impending issue with advanced digital assets [27].

2.4 Source Identification

This source identification category deals with the challenges coupled with recognizing the source of the data that falsifiers generally depend on in pasting and copying the diverse areas in the same image [11]. Such viewpoints are found because of the brand-new models of image acquisition equipment, for example, digital camera, scanners, cell phones, and so forth which usually increase the intricacy in distinguishing the source of the forgery.

3. CURRENT TECHNIQUES OF COPY-MOVE FORGERY

The copy-move forgery detection (CMFD) can classify into either Key-point-based methods or block based methods as shown in Figure 2.

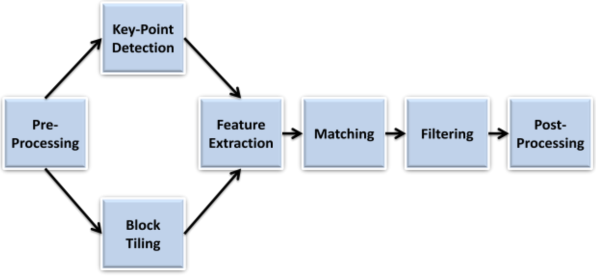

Figure 3-1 Classification of Copy-Move Forgery Detection

3.1 Block-Based Forgery Techniques

Many of the copy-move forgery techniques are rely upon block-based approach; the principle idea of these kinds of approaches of forgery is that as opposed to attempting to detect the whole forged area, this whole image can be tiled into smaller non-overlapping or overlapping blocks. These blocks are then generally compared next to one another so that you can figure out the blocks which are matching. The image regions enclosed by the coordinating blocks are the forged and copied regions. Most of these approaches can easily classify as following.

3.1.1. Moment-Based Methods (Blur, Zernike, HU)

Mahdian & Saic [28] utilized the techniques of blur moment invariants embodies the regions of the image as they can't be influenced by blur degradation as well as additive noise. Their technique starts with tilting the image into blocks of a specific size. They signify every image block by means of blur invariants. The size of the feature vector is of length 2. They utilized PCT (principal component transformation) in order to decrease the dimensionality of the feature vector. For the analysis of block similarity, they utilized the representation of the k-d tree. With the help of specific threshold value, they figure out the blocks which are similar. Once these similar blocks are discovered, they need to be validated. In order to verify this, they have detected the neighborhood of every similar block region which are likewise the same. Two blocks which are similar having non-identical neighborhood are viewed as false positive blocks. By applying this procedure, they properly recognized image copy-move forgery which encompasses cloned regions. They could likewise identify cloned regions having varying contrast values. Nevertheless, there are a few alarms which are not false, which are widespread with lots of the planned procedures. In addition, the algorithms computation time is very moderately high.

Wang, Liu, Zhang, Dai and Wang [16] executed a research on the detection of copy-move forgery through the use of Hu moments. They formulated the algorithm to be more cost-effective as well as robust to help a variety of post-processing methods including lossy JPEG data compression, blurring. They diminished the dimensions of feature vector by utilizing Gaussian pyramid. They tiled image into various fixed size overlapping blocks. They utilized Hu moments towards the image blocks and figured out the eigenvalues. After that, they sorted the values of these vectors in the lexicographic order and a threshold value is selected in order to lessen the false detections. They figured out the matching blocks by utilizing the technique of mathematical morphology. Their procedure is even successful in identifying the copy-move forgery when post-processing is completed.

Mohamadian and Pouyan [29] portrayed new strategy for identifying copy-move forgery by utilizing SIFT algorithm in conjunction with Zernike moments. They utilized SIFT algorithm to implement typical copy-move image forgery detections. However, SIFT can't be utilized to distinguish flat cloned regions. In order to do this, they utilized the technique of Zernike moments. The procedure starts with the extraction of SIFT features. After the process of extraction, they utilized these extracted features to discover matching blocks. To stay away from forgery false alarms, they utilized the method of hierarchical clustering. This includes clustering of extracted feature points right into the structure of the tree based on the threshold value. By this technique, they found themselves be able to diminish false detections as they considered that digital image is tampered or forged just when two groups or clusters tend to be matched up having at least three comparative feature points. Be that as it may, this feature diminishes the likelihood of identifying flat forgeries. Their implemented procedure had the capacity to figure out the geometric transformations carried out. In order to implement flat forgeries, Zernike moments are utilized. At first, they tiled the original image into a few sub-blocks and then calculated the Zernike moments of each sub-block. This involves calculations which are very complex and finally a feature vector is generated with coefficients of Zernike moments. With specific threshold values, they detected the blocks which are matching. Their technique utilized the SIFT algorithm, which has one and only limitation of not ready to recognize copy-move flat forgeries. They conquered this limitation by utilizing Zernike moments.

3.1.2. Dimensionality Reduction-Based Methods

Popescu and also Farid [30] could successfully identify copy-move image forgery by making use of Principal Component Analysis (PCA). Their applied approach resembles DCT technique and also better in catching discriminating features. The target digital image is transformed into the grayscale image from colored image. The image is tiled into various sub-blocks of a specific size, which are then transformed into feature vectors. After that, they sort the vector in the lexicographic order prior to block matching. This approach is far better than the brute-force strategy for detecting matches. PCA method can be efficient at identifying even minimal variations as a result of noise or even lossy data compression. Their approach is only intended for grayscale digital images. On the other hand, the strategy may be made to function for color digital images at the same time by implementing the desired image with very color channel, which usually brings out 3 duplication color maps (RGB). And then PCA technique can be applied to every single map on their own to identify the forgeries. Their approach features a very good efficiency in uncovering copy-move image forgeries and as well offers a fewer number of false image positives. On the other hand, this efficiency falls as the size of the block decreases and as well if the image quality is low.

Ting and Rang-ding [31] utilized SVD (Singular Value Decomposition) in order to detect copy-move image forgeries. Their proposed algorithm is less complex as compared to other methods and is vigorous to post-processing procedures. They utilized the correlation as a similarity criterion between the copied as well as pasted regions and scanned for regions which are identical. Firstly, the input image is tiled into various overlapping sub-blocks of fixed sizes. At that point, they utilized SVD technique to every block and extracted a feature vector having unique singular values for every image sub-block. Utilizing these feature vectors, they discovered the blocks which are matching by converting every block feature vector into the k-d tree. They utilized a threshold value in order to increase the sturdiness and as well wipe out pseudo-matching. An original picture won't have indistinguishable areas by means of coherent orientation. Consequently, the resulted matched blocks are a confirmation for copy-move image forgery. They utilized lines to join 2 identical block regions which usually demonstrate the forged regions. The images are downloaded from the web and utilized their efficient algorithm to discover forgeries. They picked an experimental threshold value. Their robust algorithm effectively identified copy-move image forgeries still when image post-processing is done. On the other hand, it neglects to distinguish that from the 2 matched blocks which image block is pasted and which one is copied. Their proposed algorithm is not powerful against JPEG compression.

A technique proposed by Bashar, Ohnishi, Noda, and Mori [32], utilizes DWT (Discrete Wavelet Transform) and KPCA (Kernel Principal Component Analysis) in order to detect the copy move forgeries. They utilized these strategies due to their powerful block matching feature. They tiled the given image into several overlapping sub-blocks. They figured out the DWT and KPCA vectors for each block. At that point, they put these vectors in a lattice and performed the sorting in a lexicographical order. They utilized the sorted sub-blocks to locate the similar block points and evaluated the offset frequencies. To dodge false detection of blocks, they set a threshold value. They proposed a fresh algorithm for rotation and flip forgery types utilizing geometric transformations and labeling techniques. This algorithm indicated promising enhancements as contrasted with traditional PCA technique. Furthermore, it likewise identifies copy-move forgeries which have an added noise as well as lossy JPEG compression.

A new approach of copy-move forgery is proposed by Zimba and Xingming [33]. Their proposed strategy starts works by transforming color to the grayscale image. At that point, they performed DWT to the whole image. This outputs image sub-bands: low frequency as well as high-frequency sub-bands. Out of these two sub-bands, low frequency bands are sufficient to detect the forgeries. The given image is partitioned into overlapping blocks. They utilized PCA- Eigen Value Decomposition on the image sub-blocks. They set these vectors into the grid and perform the lexicographical sorting. This technique makes the block matching not as much of complex. They then figured out the normalized shift vector and after that they calculated the offset frequency. This frequency is then employed to morphological processing in order to give the concluding results. This technique is more proficient than traditional PCA technique by diminishing the size of the image at the starting of the procedure. Their proposed algorithm can recognize forgeries including rotation of changing degrees. They evaluated morphological processing to evade false identifications. The main limitation is, the copied area ought to be greater than the image block size, and else it can't be recognized. Likewise, their strategy fails to identify forgeries rotation, scaling, and compression.

3.1.3. Intensity-Based Methods

Huang, Luo and Qiu[34] proposed a method for copy-move image forgeries utilizing intensity values of the image. The image is tiled into several overlapping blocks. At that point, the image blocks are then partitioned into 4 directions and 2 equal parts. At that point characteristic block vector is calculated for every image block utilizing AWGN (Additive White Gaussian Noise) operation and are sorted in lexicographical order. Each block pair of similar feature vectors does not require representing the duplicated image blocks. And so, a technique must be created to figure out which image blocks are actually duplicated. In order to perform this, they utilized shift vectors. They fixed a certain value of the shift vector and two image blocks are viewed as equivalent when the value of the shift vector corresponding to that pair surpasses it. Those block pairs are rejected whose value of shift vector are entirely different from the specified value. At that point, they utilized some technique to guarantee whether copy-move forgery is really done or not. Their proposed algorithm has not so good computational complexity and powerful to operations of post-processing. It works well in the cases where the size of the forged regions is usually larger as compared to the size of the block. Even so, the presented algorithm is not able to work in the cases where the digital image is extremely distorted and have expansive smooth regions.

Bravo-Solorio & Nandi [35] directed a study on copy move image forgery detection method to discover falsifications including scaling, rotation and reflection. In this, they have divided the image into image blocks and move the window over it in a raster scan manner. After that feature vectors are calculated that are dependent on color. In this way, they lessen the number of search iterations thus raising the efficiency. Four features are calculated and among them three features are autonomously processed as red, green and blue parts. The last fourth component is the entropy of luminance. They utilized this fourth component to dispose of image blocks with too little textural data. These features are then sorted lexicographically and after that block matching is carried out. Their proposed technique yields a number of matches; thus they utilized refinement to lessen them. They utilized 1-D (one-dimensional) descriptors to diminish memory utilization. These descriptors are tending to be invariant to reflection and rotation. This technique is effective than several strategies regarding computation as well as identifying forged blocks with post-processing.

Lin et al. [23] examined about copy move image forgery identification & detection and suggested a new method. They partitioned the image into various image blocks of the equivalent size which are also then partitioned into 4 sub-blocks. Average intensity is calculated of every singular block by utilizing the 4 sub-block intensities. At that point, relative intensity is computed by calculating the contrast between average and individual intensities. By doing this, they end up with feature vectors. These characteristic vectors tend to be of type integers; subsequently they utilized radix sort strategy rather than lexicographical sorting. They noted the upper left corner of every image block and utilized it to compute a shift vector by discovering the contrast between adjoining component vectors. This calculated shift vector can be accumulative for the areas which are altered and the detection of forgery will be based on this value. Their strategy is productive and fit for distinguishing even Gaussian noise and JPEG compression. Nonetheless, their proposed method fails if the altered image region is pivoted or rotated with different angles.

Wang, Li, Dai, Liu, and Wang [36] diminished the image dimension by utilizing the technique of Gaussian pyramid. In their proposed method image blocks are in circular form and computed the four feature vectors which are then sorted lexicographically sorted. By utilizing positive threshold value, they locate the feature vectors which are matching. They then successfully identified image forgeries as copy move by this technique. By simply fine-tuning the threshold value, they could manage the iterations of feature vectors which are matching. They additionally attempted their technique on the altered pictures with post-processing like lossy JPEG compression, blurring, and rotation. They likewise enhanced the efficiency of the proposed technique to restrict the number of search space of block matching.

Sridevi, Sandeep and Mala [37], employed a technique of copy-move image forgery in a parallel domain. They proposed this technique fundamentally to achieve copy move image forgery in the real-time environment. Different techniques like DWT, PCA as well as SVD have higher computation time; thus they can't be utilized as a part of real-time apps. Their technique starts with isolating the grayscale image into various overlapping blocks of a predefined size. Intensity values as a feature are extracted from every block. The last two areas of the feature vectors save the position of the blocks. This procedure of feature vector extraction is done with the help of the algorithm. For parallel sorting, they created another separate algorithm. This lexicographical sorting is done by utilizing radix sort strategy as a part of a parallel way. This lexicographical sorting guarantees simple identification of similar blocks by discovering the identical features. They discovered the copied image regions by feature matching and these image blocks are then mapped onto the original image by utilizing the positions saved in the vector. There will be a fundamental algorithm which controls every one of these mentioned steps. Their technique has demonstrated performance enhancement over numerous other regular methods. This is refined by diminishing the processing time. They managed the detection of false blocks by fine-tuning the size of the block. Though, their proposed technique can't be tried on the color image.

3.1.4. Frequency-Based Methods

Fridrich et al. [38] utilized DCT (Discrete Cosine Transform) coefficients for the detection of copy-move image forgery. They began the process by splitting the image into various image blocks of a particular size and sliding this window over the image pixels in raster scan order. Pixel values are recorded for each block and stored in the array. This array is then sorted lexicographically to figure out the similar entries in the matrix rows. At that point, this matrix is utilized to locate the copied and forged regions. This strategy is accurate match method. In the method of the robust match, they characterize the image blocks utilizing the quantized coefficients of DCT. You'll find there's a value called Q-factor which selects the steps of the quantization which are included in computing the coefficients of DCT. They picked an appropriate Q-factor value and the proposed array is then again sorted lexicographically prior to matching. The developed algorithm deals with the false positives blocks by coordinating mutual pairs. Nonetheless, the algorithm is not able to discriminate among vast identical textures of an original image.

A research by Zhang, Su, and Feng[39] portrays a robust and efficient algorithm for copy-move image forgery detection taking into account pixel-matching and DWT. Their efficient algorithm can identify duplicated regions in an image. To begin with, DWT is calculated for the entire image in order to get the sub-band. And then, they computed the spatial offset values among the pasted region and the copied region. Next the image is moved with the offset value and is then overlaid with the original image. The replicated region plus the pasted region share the same properties and spatial region. Henceforth, the pixels of the image will be indistinguishable if the copy-move image forgery is implemented on the image. Their approach is robust and efficient for different techniques of copy-move forgery. Although their approach is based on the locale of image forged region. It can't be implemented to pictures which include copy-move region right at the center point of the image. Amid such cases, the picture must be partitioned into sub-blocks and the effective algorithm must be utilized recursively.

Bayram, Sencar & Memon [40] led a study to distinguish copy-move image forgery by utilizing FMT (Fourier-Mellin Transform). They picked FMT as it is generally robust to blurring, lossy JPEG compression, scaling, noise and effects of translation used as post-processing. They segmented the image into a few small sub-images and after that they computed the Fourier transform of the image's sub-blocks. By this, they guaranteed that change is translation invariant. At that point, they re-sampled, then projected and then quantized in order to get the desired feature vectors. These calculated feature vectors are generally made invariant to the rotation to smaller angles of rotation. After that process of a block, matching is executed in order to identify the feature vectors which are similar in nature by utilizing either counting bloom filters or lexicographic sorting. Indeed, even an original image might have numerous blocks which are similar. For this reason, they authenticated forging in the case when you will find a number of connected sub-blocks within the same block distance. This lessens false positives that make the strategy extremely effective. Their approach might identify forgeries including blocks having rotations up to (or equal to) 10 degrees plus a scaling factor of 10%. Their method is also robust to JPEG image compression.

A late study by Li, Li & Wang [41], depicts the block-matching method of copy-move image forgery detection by utilizing Polar Harmonic Transform (PHT). They utilized this new sort of orthogonal moment in order to make features of image blocks and they achieved bock-matching by utilizing PHT block features. They utilized this procedure to identify copy-move image forgeries which include geometric transformations and block rotations. Dissimilar to numerous different schemes which utilize square blocks, these researchers partitioned the given image into numerous circular blocks as PHT can be characterized on a specific unit disc. Subsequently, they utilized the formula in order to get the block image features utilizing PHT. After that, they constructed lexicographically sorted a matrix by utilizing features vector of PHT. The last portion may be the block matching which they achieved with the help of simulations. They executed post-processing operation on the tampered images and attempted to identify forgeries that have rotated image blocks. Their technique was fruitful in distinguishing orthogonally rotated tampered image blocks. Although when the rotation angle was changed, their forgery detection algorithm wouldn't offer appropriate results, however, it may identify the forged regions. They additionally exhibited the identification of forgeries having geometric transformations. Therefore, the performance and execution of PHT protocol is great in distinguishing copy-move image forgeries whereby the pasted image region is normally rotated prior to being pasted. All traditional detections are achieved effectively. The algorithm is better than numerous other offered strategies within normal detections. Though, it isn't so good in identifying image forgeries involving local bending and scaling.

A research conducted by Muhammad, Hussain, Bebis, and Khawaji [14] suggested the robust technique for identifying copy-move image forgery by utilizing DyWT (Dyadic Wavelet Transform). Their strategy depends on the extraction of a high and the low-frequency component corresponding t the given image; after that matching these components by implementing similarity measures over these. DyWT is normally utilized in several detection techniques. Though, DyWT transform is shift invariant. Thus, Mallat & Zhong presented DyWT which is shift invariant in nature. In this sort of waveform, you will find there are absolutely no downsampling as well as no shrinking of image wavelet coefficients such as DyWT. Provided an image, researchers decomposed these by utilizing high-pass and low-pass filters. After that, they utilized robust algorithm in order to calculate the DyWT of the desired image. Total of 4 sub-bands are acquired right at the output and they have the same size when compared to the original image. The researchers first partitioned the original image in order to scale it by 1 by utilizing DyWT. A pair of subbands HH1 and LL1 is obtained. They reduced these types of sub-bands right into 16-by-16-pixel blocks and with an overlapping of eight (or 8) pixels. For that strategy to work effectively, a copy-move image forgery must be carried out on the minimum image size of 16-by-16. They then implemented the matching of HH1 and LL1. LL1 ought to be same and the HH1 ought to be remarkably dissimilar pertaining to forged regions. They utilized this specific in order to identify the copy-move image forgery. In order to figure out the similarity between the blocks they utilized used Euclidean distance as similarity criterion. They computed the Euclidean distance for HH1 and LL1 and after that sorted these two in descending as well as in ascending order respectively. They then compared the calculated values with the threshold value. In case, if values lie below the threshold value then they left those values. And in case, if they figured out that they are equivalent they regarded those to be addressing the particular forged image region. Their technique is robust to a few more methods and provides better results. Even so, the image must be converted into grayscale prior to processing.

A study proposed by Ghorbani, Faraahi and Firouzmand [42] suggested a fresh technique for copy-move image forgery detection. These carried out Quantization Coefficients Decomposition on DCT and DWT coefficients. They first converted the original image into grayscale image. They then applied discrete wavelet transform (DWT) in order to get the 4 sub-bands. For the purpose of forgery detection, they utilized only the sub-bands which are related to low-frequency part. After that, they decomposed the image into few blocks of the same size. The image blocks are usually in the form of overlapping. After they implemented the discrete cosine transform in order to get the DCT feature vectors and afterward QCD is conducted on the DCT vectors. These computed feature vectors are then organized into matrix form. In order to lessen the computational complexity, the matrix is sorted lexicographically. For each set of two adjacent rows, they computed the normalized shift vector. They after that counted the shift vector i.e. how many times it appears. A threshold value is utilized for the count value and the image blocks are called tampered if and only if the count value surpasses the pre-defined threshold value. Their strategy is effective in recognizing forgeries when contrasted with different methods. Nonetheless, this technique can't identify forgeries if the tampered region experiences post-processing like heavy compression, scaling, and rotation. Furthermore, this technique imposes certain constraints on the tampered regions.

Li et al. [43] suggested another technique for copy-move forgery identification. They utilized a grayscale operator call LBP (Local Binary Pattern) to depict the texture of the image. They changed the original image into grayscale image. Nonetheless, it will have noise contaminants, lossy JPEG compression and lots of various other post-processing strategies carried out on the forged image. High-frequency components for such type of images won't be stable. For this reason, they utilized the Gaussian LPF (low pass filter) and as well learned that filtering if implemented more than twice would certainly increase the performance rate of detection. And then, they split the image into many overlapping blocks which are circular in nature. They extracted the block feature vectors by utilizing LBP which is generally rotation invariant. They then put these feature vectors in matrix form in order to discover the blocks which are similar. The matrix is then sorted lexicographically in order to reduce the computation. At that point, they utilized Euclidean distances to figure out the matching blocks. The Euclidean distance is computed for each feature vector and is contrasted with a particular threshold value. The acquired matched blocks are then marked on the given image to show the tampered regions. They distinguished some false regions. To represent that, they utilized filtering to decrease the false positives. They then performed morphological erosion and morphological processing to take out the false positives totally. Their technique is invariant to flipping and rotation. Though, their technique can't distinguish forgeries including rotation at various angles.

Qiao, Liu, Sung, & Ribeiro [44] offered the latest strategy for copy-move forgery detection. Their approach depends on multi-orientation and multi-resolution curvelet transform. This curvelet transform is normally conducted in the frequency domain in order to get the better efficiency. They transformed the original image into a grayscale image. The given grayscale image is divided into a number of sub-bands. At that point, they apportioned every sub-band into a few block and executed ridgelet investigation on them. Ridgelet transform consolidates 1-D wavelet transform and Radon transform. Though, it is computationally very complex in nature. To lessen the computational complexity, they utilized discrete curvelet transform. This employs a pyramid structure with different orientations at different scales, which improves the accuracy and detection performance. Multi-directional decomposition offers precise connection among nearby orientations. They utilized these multioriented pyramids structured feature vectors to implement matching. These feature vectors are then sorted lexicographically in order to reduce the complexity. Their strategy effectively distinguished copied regions after rotations, scaling, and JPEG compression. Though, it can't be employed on images which are compressed. They must be decompressed prior to this technique can be utilized. Likewise, the image must be in grayscale in order to implement this particular research.

3.2 Keypoint-Based Techniques

A study proposed by Huang, Guo & Zhang [45], depicts a technique of identifying copy-move forgery by finding the correlation between pasted region and original region of the image. They presented Scale Invariant Feature Transform (SIFT) algorithm for accurate detection. They initially computed the SIFT key points. They coordinated these with each other in order to discover the image forgeries. In case, you find any matching SIFT points, and then in that case image has copy-move image forgeries. The process of matching was implemented for each key point by recognizing its closest neighbor. They used the threshold value, which is the proportion of nearest neighbors to second nearest neighbors. This makes the algorithm more robust. They faced many difficulties in executing high-scale images. Henceforth, they utilized Best-Bin-First (BBF) search technique, which usually comes from the k-d algorithm, for block matching purpose. This technique distinguishes the most identical vectors with minimum computation and maximum probability. They then took one forged image and afterward repeated the forgery detection method for distinct threshold values. They figured out that the detection accuracy depends on it. An ideal threshold value should be chosen. They then tested the method's robustness by effectively identifying forgeries with post-processing in a tampered image. Their technique is effective in utilizing SIFT algorithm to recognize the copy-move forgery. On the other hand, their procedure isn't useful if the forged region is small in size and SNR (signal to noise ratio) value is quite low.

Bo, Guangjie, Junwen, and Yuewei [46], led a research on copy-move image forgery detection by utilizing Speeded-up Robust Features (SURF) formula, and this formula is designed by Herbert Bay et al. It includes key point description and detection. They utilized Hessian matrix for finding the respective key points as well as Haar wavelets for setting the orientation. They evaluated dominant orientation and then depicted the orientation of the respective descriptor. By taking out square regions around these types of interest points, they created SURF descriptors that are aligned correctly towards dominant orientation. By response weighting of the Haar wavelets, they then enhanced the robustness (or strength) to geometric deformations and localization type errors. They picked Haar wavelets as they are illumination bias invariant. Afterward, SURF descriptors are utilized for the matching purpose. They utilized a threshold value in order to improve the robustness and also prevent false detections. They picked the threshold's empirical value and tried their algorithm on distinctive images and they success. Further, they executed post-processing like blurring, rotation and scaling on the tampered images. They utilized the algorithm in order to test and they were effective in demonstrating its robustness towards post-processing. Their procedure is fruitful in recognizing the forged regions when post-processing is implemented on the images. On the other hand, they could not locate the definite boundaries of the forged region.

A study conducted by Zheng, Zhub and Haoa [47] uncovers another technique for key points matching which is dependent on the key point's position relationship. Key points in the original region and tampered region ought to be consistent and they ought to be distributed equitably on the whole image. This guarantees that similar textures, for example, similar to the sky, additionally create a significant number of key points. Their detection algorithm is designed to scan as well as dispose of the key points initially. This guarantees that noise parameter has no effect on key points. They examined the key points again and discovered the desired features for all essential key points. They designed new algorithm in order to discover the features and then they put these features in a matrix. Their designed algorithm is different from SIFT algorithm in feature determination. By seeing the matrix reliable key points, their algorithm identified copy move forgeries implemented on the image. Their method discovers a set of consistent key points and in addition to it; they marked the candidate key points once they fulfill certain conditions. They then utilize the certain threshold value in order to reduce the false detections. They noticed that the computational time is less furthermore there are fewer number of false image region detection on the big similar texture, for example, similar to the sky. Their technique is effective in these types of detections, however, cannot recognize forgery including post-processing on images like scaling and rotation.

4. CONCLUSION

With the image processing technology advancement, identification of digital (or computerized) image forgery is a fascinating research topic in crime scene investigation science or forensic science. In this paper, a particular type of image forgery that is the Copy-move forgery is explored and an effective forgery detection technique is proposed taking into account of Fourier transform. In this paper, I have examined the issue of copy-move forgery detection. My focus was on extracting and detecting duplicated regions or areas with higher robustness and accuracy.

5. REFERENCES

[1] Pan, X. Z., and Wang, H. M. "The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA", Advanced Materials Research, 2012, Vol. 532, pp. 692-696.

[2] Shivakumar, B., and Baboo, S. S. "Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors", International Journal of Computer Applications, 2011, Vol. 27, No. 3.

[3] Yao, H., Tang, Z., Qiao, T., Zhao, Y., and Mao, H. "Detecting Copy-Move Forgery Using Non-negative Matrix Factorization" , proceedings of Third International Conference on Multimedia Information Networking and Security (MINES), 2011.

[4] Pujari, V. S., and Sohani, M. "A Comparative Analysis On Copy Move Forgery Detection Using Frequency Domain Techniques", International Journal of Global Technology Initiatives, 2012, Vol.1, No. 1, pp. E104-E111.

[5] Chen, L., Ni, J., Lu, W., Sun, W., and Huang, J. "Region duplication detection based on Harris corner points and step sector statistics", Journal of Visual Communication and Image Representation, 2013, Vol. 24, No. 3, pp. 244-254.

[6] Liu, M.-H., and Xu, W.-H. "Detection of copy-move forgery image based on fractal and statistics", Journal of Computer Applications, 2011, Vol. 8.

[7] Yadav, P., Rathore, Y., and Yadu, A. "DWT Based Copy-Move Image Forgery Detection", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 2012, Vol. 1, No.5, pp. 56-58.

[8] Pujari, V. S., and Sohani, M. "A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non Lexicographic techniques", IJECCE, 2012, Vol. 3, No. 1, pp. 136-139.

[9] Shivakumar, B., and Santhosh Baboo, L. D. S. "Detecting copy-move forgery in digital images: a survey and analysis of current methods", Global Journal of Computer Science and Technology, 2010, Vol. 10, No. 7.

[10] Chen, L., Lu, W., and Ni, J. "An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection", International Journal of Digital Crime and Forensics (IJDCF), 2012, Vol. 4, No. 1, pp. 49-62.

[11] Liu, G., Wang, J., Lian, S., & Wang, Z. "A passive image authentication scheme for detecting region duplication forgery with rotation", Journal of Network and Computer Applications, 2011, Vol. 34, No. 5, pp. 1557-1565.

[12] Sridevi, M., Mala, C., & Sanyam, S. "Comparative Study of Image Forgery and Copy-Move Techniques", Springer: Advances in Computer Science, Engineering & Applications, 2012, pp. 715-723.

[13] A merini, I., Barni, M., Caldelli, R., & Costanzo, A., "Counter-forensics of SIFT-based copy-move detection by means of keypoint classification", EURASIP Journal on Image and Video Processing, 2013, Vol. 18, No.1.

[14] Muhammad, G., Khawaji, K., Hussain, M., and Bebis, G. "Blind copy move image forgery detection using dyadic undecimated wavelet transform", Digital Signal Processing, 2011.

[15] Piva, A. "An Overview on Image Forensics", ISRN Signal Processing, 2013.

[16] Wang, J.-W., Zhang, Z., Liu, G.-J., Dai, Y., and Wang, Z. "Fast and robust forensics for image region duplication forgery", Acta Automatica Sinica, 2009, Vol. 35, No.12, pp. 1488- 1495.

[17] Mahdian, B., and Saic, S. "A bibliography on blind methods for identifying image forgery", Signal Processing: Image Communication, 2010, Vol. 25, No. 6, pp. 389-399.

[18] Math, S., and Tripathi, R. "Digital Forgeries: Problems and Challenges", International Journal of Computer Applications, 2010, Vol. 5, No. 12.

[19] Hwang, M. G., and Har, D. H. "A Novel Forged Image Detection Method Using the Characteristics of Interpolation", Journal of Forensic Sciences, 2013, Vol. 58, No.1, pp. 151-162.

[20] Taktak, W., and Dugelay, J.-L. "Digital Image Forensics: A Two-Step Approach for Identifying Source and Detecting Forgeries", The Era of Interactive Media, 2013, pp. 37-51.

[21] Jian-feng, Z. G.-j. Z. "The Application of Electronic Signature Technology in Online Bidding System", Journal of Changzhou Vocational College of Information Technology, 2011, Vol. 4, No. 7.

[22] Chang, I.-C., and Hsieh, C.-J "Image Forgery Using An Enhanced Bayesian Matting Algorithm", Intelligent Automation & Soft Computing, 2011, Vol. 17, No. 2, pp. 269-281.

[23] Lin, H.-J., Wang, C.-W., and Kao, Y.-T. "Fast copy-move forgery detection", WSEAS Transactions on Signal Processing, 2009, Vol. 5, No. 5, pp. 188-197.

[24] Peng, F., Nie, Y.-y., and Long, M. "A complete passive blind image copy-move forensics scheme based on compound statistics features", Forensic Science International, 2011, Vol. 212, No. 1, pp. e21-e25.

[25] Barnes, C., Goldman, D. B., Shechtman, E., and Finkelstein, A. "The generalized patchmatch correspondence algorithm", Computer Vision–ECCV 2010, Springer, 2010, pp. 29-43.

[26] Ghosh, P., Gelasca, E. D., Ramakrishnan, K., and Manjunath, B. "Duplicate image detection in large scale databases", Advances in Intelligent Information Processing: Tools and Applications, 2007, pp. 149-166.

[27] Christlein, V., Riess, C., and Angelopoulou, E. "On rotation invariance in copy-move forgery detection", IEEE International Workshop on Information Forensics and Security (WIFS), 2010.

[28] Mahdian, B., and Saic, S. "Detection of copy– move forgery using a method based on blur moment invariants", Forensic Science International, 2007, Vol. 171, No. 2, pp. 180-189.

[29] Mohamadian, Z., and Pouyan, A. A. "Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions", UKSim, 2013.

[30] Popescu, A. C., and Farid, H. "Exposing digital forgeries by detecting duplicated image regions" Dept. of Comput. Sci., Dartmouth College, Tech. Rep. TR 2004-515, 2004.

[31] Ting, Z., and Rang-ding, W. "Copy-move forgery detection based on SVD in digital image", 2nd International conference on Image and Signal Processing, 2009.

[32] Bashar, M., Noda, K., Ohnishi, N., and Mori, K. "Exploring duplicated regions in natural images", IEEE Transactions on Image Processing, 2010, Vol. 99, No. 1.

[33] Zimba, M., & Xingming, S. "DWT- PCA(EVD) Based Copy-move Image Forgery Detection", International Journal of Digital Content Technology and its Applications, 2011, Vol. 5, No. 1.

[34] Luo, W., Huang, J., and Qiu, G. "Robust detection of region-duplication forgery in digital image", 18th International Conference on Pattern Recognition, ICPR 2006, 2006.

[35] Bravo-Solorio, S., and Nandi, A. K. "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics", Signal Processing, 2011, Vol. 91, No. 8, pp. 1759-1770.

[36] Wang, J., Liu, G., Li, H., Dai, Y., and Wang, Z. "Detection of image region duplication forgery using model with circle block", International Conference on Multimedia Information Networking and Security, MINES'09, 2009.

[37] Sridevi, M., Mala, C., and Sandeep, S. "Copy– move image forgery detection", Computer Science & Information Technology (CS & IT), 2012, Vol. 52, pp. 19-29.

[38] Fridrich, A. J., Soukal, B. D., and Lukáš, A. J. "Detection of copy-move forgery in digital images", Digital Forensic Research Workshop, 2003.

[39] Zhang, J., Feng, Z., and Su, Y. "A new approach for detecting copy-move forgery in digital images", 11th IEEE Singapore International Conference on Communication Systems, 2008.

[40] Bayram, S., Sencar, H. T., and Memon, N. "An efficient and robust method for detecting copy-move forgery", IEEE International Conference on Acoustics, Speech and Signal Processing, 2009.

[41] Li, L., Li, S., and Wang, J. "Copy-move forgery detection based on PHT", World Congress on Information and Communication Technologies, 2012.

[42] Ghorbani, M., Firouzmand, M., and Faraahi, A. "DWT-DCT (QCD) based copy-move image forgery detection", 18th International Conference on Systems, Signals and Image Processing, 2011.

[43] Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J. F., and Pan, J.-S. "An Efficient Scheme for Detecting Copymove Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, 2013, Vol. 4, No. 1, pp. 46-56.

[44] Qiao, M., Sung, A., Liu, Q., and Ribeiro, B. "A novel approach for detection of copy-move forgery", Fifth International Conference on Advanced Engineering Computing and Applications in Sciences, 2011.

[45] Huang, H., Guo, W., and Zhang, Y. "Detection of copy-move forgery in digital images using SIFT algorithm", Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008.

[46] Bo, X., Junwen, W., Guangjie, L., and Yuewei, D. "Image copy-move forgery detection based on SURF", International Conference on Multimedia Information Networking and Security, 2010.

[47] Zheng, J., Haoa, W., and Zhub, W. "Detection of Copy-move Forgery Based on Keypoints' Positional Relationship", Journal of Information and Computational Science, 2012, Vol. 1, No. 3, pp. 53-60.