I.J. Image, Graphics and Signal Processing, **2016, 6, 29-40**
Published Online June 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.06.04

Copy-Move Image Forgery Detection a Review

Anuja Dixit and R. K. Gupta
Department of Computer Science & Engineering and Information Technology
Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, 474005, India
Email: anu2010cse1@gmail.com

***Abstract*—**Due to the availability of various image processing tools forgery over an image can be performed very easily but very difficult to identify. In copy-move forgery, a segment is copied from the original image and pasted at some other location on the same image to hide significant objects of image or to bring additional information which is originally not present in image. Nowadays, this forgery technique is drawing researcher's attention. Till now many solutions are presented by researchers to detect such type of forgery in images. Several post-processing operations like rotation, alteration in intensity, noise addition, filtering and blurring can be applied over copy-moved segment which makes detection of forgery very difficult. Copy-move forgery detection is mainly based on finding similarity present in an image and establish a relationship between genuine image parts and pasted portion of the image. This paper is centralized towards providing survey to forgery detection techniques based on different block-based methods. In block-based methods image is divided in blocks of fixed dimension and further features are extracted corresponding to each block of image. Forged blocks are identified utilizing the similarity present between feature vectors.

***Index Terms*—**Image forgery, Block matching, Tampered region, Copy-move forgery, Feature extraction, Block-based method.

I. Introduction

Our brain interprets visual imprints very rapidly. When computers were not available easily for everyone, there was possibility to trust what we see. Due to advancement in information technology, digital images can be transmitted from one place to another very easily. Images can explain any incidence in much better manner than thousands of words. A digital image travel through several steps throughout its life cycle. According to need they are tampered. Manipulation to images can be done very easily with the help of image processing tools (Adobe Photoshop, Corel Draw and GIMP). These tools can also be used for enhancing an image (innocent editing) but mainly these are used for changing image data (malicious editing). A person who just have some knowledge about these tools can perform alteration to original image. These manipulations in images can be done for defaming a person or for private profit. Everyday, we passes through several images available on magazines, newspapers, televisions and websites. They are used in various fields like medical, courts of law, criminal investigations etc. Due to easy availability of alteration tools, images cannot be trusted anymore. Images are losing their credibility due to forgery operations. Documents with images must be authenticated before determining any conclusion. Detection of authenticity of an image is very essential. Researches are continuously giving their efforts in finding more efficient algorithm for detecting such forgeries and creating techniques which are robust against post-processing operations. Image forgery can be defined as adding, deleting, changing features of an image. Image forgery results in significant alteration in image information and can change the sense of information shown by the image. Fun-making, rivalry about politics, defaming a person, black-mailing a person in authority for private profit and harassment are sole purpose of image forgery. Image forgery detection is a difficult task for authorities who are dependent on the visual data. These forgeries could be done for malicious purposes.

Image forgery techniques are of three kinds: Copy-Move forgery, Image splicing and image resampling. In copy-move forgery, a portion of original image is copied and it is pasted at different location on the same image. The sole purpose of copy-move forgery is to bring additional data in image which is originally not present. This forgery technique could be applied to cover original information of image by pasting copied segment over it. These manipulation in image change the message reflected by the image. Most of the time, such altered images are used in courts of law as an evidence to prove innocent as guilty or vice versa. The detection of copy-move image forgery is not an easy task because the copied segment is from the same image so the characteristics like noise, color patterns and texture patterns all are compatible to the rest of the image. In addition to it, several post-processing operations are also applied to the copied portion before pasting it to original image which makes the detection of forgery much more difficult task. Various methods for detection of copy-move forgery detection are described in this paper. This review paper is focused on providing working of different block based methods for forgery detection. If complete image is processed at a time then computational cost will be high so image is divided in blocks. Using different techniques features are extracted corresponding to each block of image. Copied and pasted blocks will have similar feature vectors, this principle is exploited for copy-move forgery detection. The outline of this review paper is as follows. In section II, various image forgery

detection techniques are discussed. In section III, copy-move forgery detection methods are described based on their specific classifications. Conclusion derived from this review paper is stated in section IV.

II. Digital Image Forgery Detection Approaches

As various techniques are available to tamper images so there is requirement of such techniques which can contribute in maintaining authenticity and integrity of images. Broadly, Image forgery detection techniques can be categorized into two categories: Active and passive.

Digital signatures and watermarking are active techniques of forgery detection. These techniques are costly because only expensive cameras have such features to embed certain details in original image for identifying tampering.

Passive techniques [1] are also called blind image forgery techniques. These techniques does not demand any prior information about source image. These techniques are focused on how forgery can be detected without the need of any image watermarks. Passive image forgery detection techniques can be categorized into six broad categories. They are pixel-based, geometric-based, source camera identification- based, camera-based techniques, physics-based and format-based techniques.

A. Pixel-Based Technique

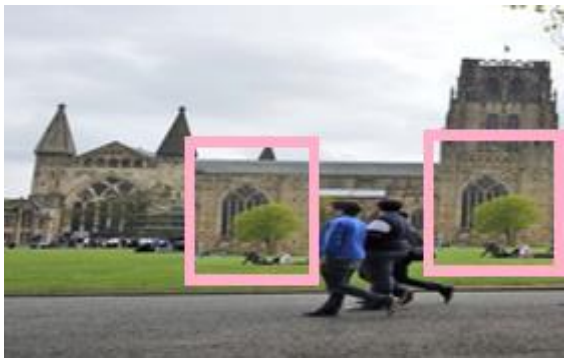
These are the most common techniques based upon statistical changes happened at pixel-level due to forgery. Such techniques also establish a correlation due to tampering in spatial domain or in transformed domain. These methods are widely used for finding the authenticity of images. Usually, forgery detection is based on pixel-level values. These methods are focused on detecting the manipulation in the image on the basis of pixel related characteristics. Usual pixel-based forgery detection techniques are Image splicing, Resampling and copy-move. In this paper our main focus is on analyzing all copy-move forgery detection techniques.

Image splicing: In this method one or more segment of two or more images are copied and pasted to original image. Image splicing is also called copy-paste image forgery.

Image resampling: This method is about producing a high quality image by enhancing its features without noticeable changes in image statistics. Some geometrical transformations like skewing, stretching, flipping etc. can be performed on an image. The interpolation is of greatest importance step in image retouching. These image forgeries cannot be easily detected. Continuous efforts by researchers are being applied in this field for finding more reliable method for forgery detection.

Copy-move forgery: In Copy-move forgery a portion of an original image is used for hiding their own features or adding false information to image as shown in Fig.1. Copy-move forgery is also called cloning.

(a) original Image



(b) Tampered Image

Fig.1. Copy-move forged Image

B. Geometric-Based Technique

In genuine images, the camera center projection on image plane approaches the center of image, this point is also called principal point. When any forgery is done like shifting of object in an image, translation is performed or existing image is combined with other image then the principal point does not remain in its correct position. By utilizing this constraint, projective geometrical principles used for developing forgery detection technique.

C. Source Camera Identification-Based Technique

These techniques are based on identifying image forgery using characteristics of source camera which was used for capturing image.

D. Camera-Based Technique

These techniques are focused on using steps of imaging process in a camera. Various artifacts are present regarding each stage they can be used for forgery detection.

E. Physics-Based Technique

If two images are taken in unlike conditions having different lighting or brightness then there will be differences in image portions (if both are spliced). Such physics- based characteristics can be used in detection of image forgery.

F. Format-Based Technique

If transformation is performed in forged image for the purpose of contraction like JPEG compression such activities makes forgery detection process much harder.

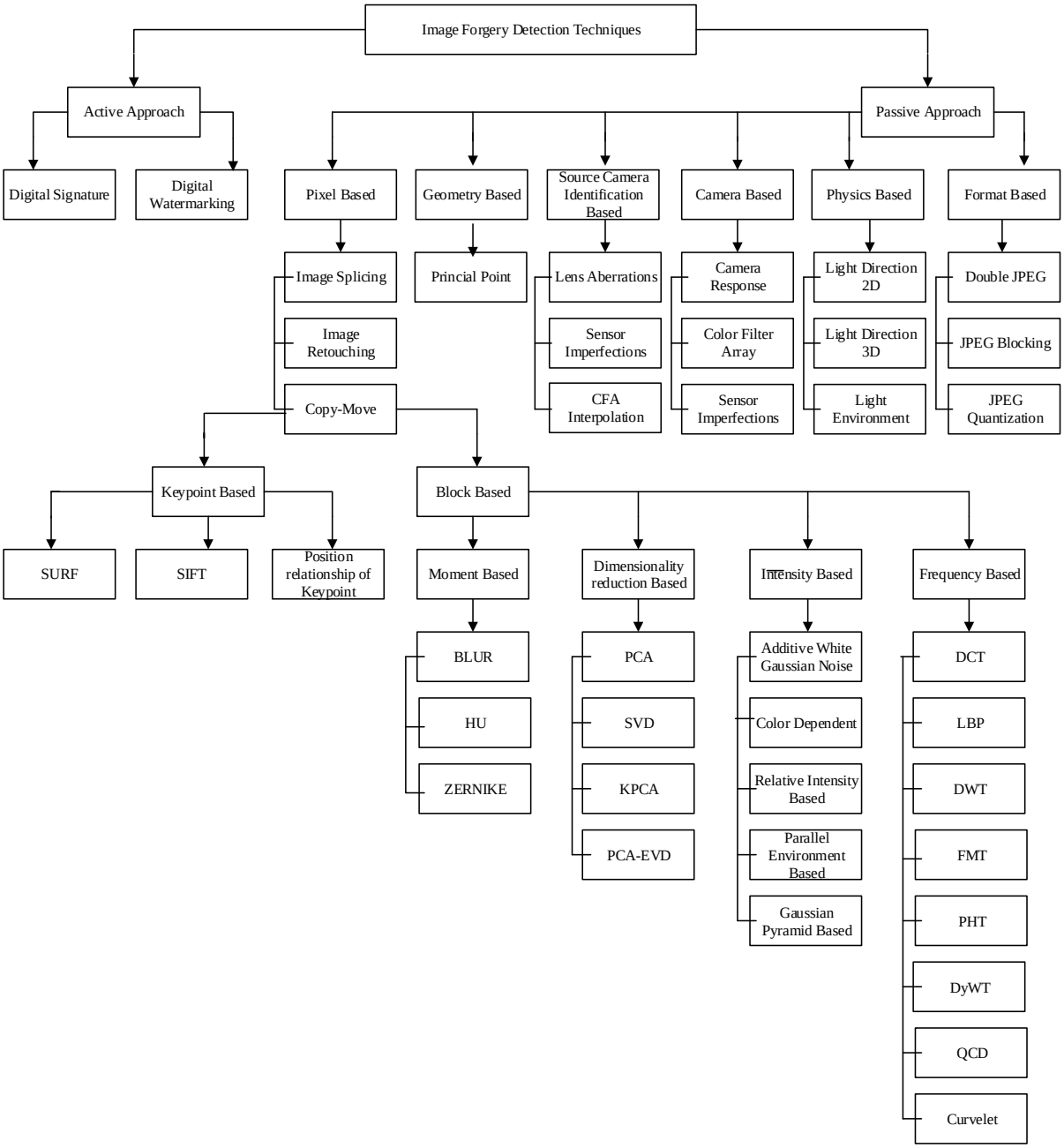


Fig.2. Image Forgery Detection Techniques

From above categorization as shown in Fig. 2 we came to a conclusion that the image forgery detection technique is multidimensional. Various characteristics and features can be used for it. The most effective method among above categories is pixel-based technique in which variation in pixel-level is observed for forgery detection. These techniques neither expect any previous knowledge about transformation performed over image segment nor require any information about how image acquisition has been done.

III. Copy-Move Forgery Detection

Copy-move forgery is based on the concept of copying a segment from the original image and pasting it on the same image for adding or hiding information shown by the image. As in this technique we mainly stress on finding the similar region in the image so there is no scope for finding the forgery on the basis of incompatibilities because the copied segment is from the same image. We concentrate on finding forgery on the basis of compatibilities of segments present in an image.

Hence, the copied region possess strong correlation with the rest of the image that exploited for finding forged section in the image. The main problem with copy-move detection is the computational complexity involved with exhaustive search methods. Copy-Move forgery detection method can be classified into block-based and key point-based methods.

A. Block Based Method

These methods are based on using blocks of image for analyzing the forgery. The main principle of these methods is to divide image in overlapping or non-overlapping blocks rather than analyzing the whole image at a time. After that different techniques are applied on the blocks for extracting features. These extracted features stored in a matrix corresponding to each block. Some sorting technique is applied so that the similar features can lie in proximity. Concept of shift vector is introduced for finding the blocks having similar shifting. Counter value is set for counting the occurrence of blocks with same shifting and on the basis of threshold value the similar regions are detected. On the basis of above principle the forged blocks identified in an image. Block-based techniques can be divided in five categories. They are moment-based, dimensionality reduction-based, frequency-based, intensity-based and texture-based as shown in Fig. 2.

(a). Moment-Based Methods

For detection of copy move forgery different moment-based methods are used by researchers. Mahdian et al. [2] proposed Blur moments for detecting forgery regions. These moments don't get affected by blur degradation and additive noise. First of all image is divided in fixed size blocks then Blur invariants are calculated for each block. Mainly blur moment used here for extraction of features. As the length of feature vector could be high and computation could not be efficient so PCT (Principal Component Transform) is used for reducing the dimension of feature vector. After extraction of feature vector and reducing their dimension next step is to match features. For analyzing the similarity in block features k-d tree representation used. Similar blocks declared using threshold value. After detection of similar blocks they are verified by using the concept that the neighboring blocks of forged region will be similar but similar blocks which have different neighbors considered as false positives. This method is mainly used for detecting those region which are blurred before using them on the same image. This method can also identify regions which are similar but having different contrast values. In this method there is possibility of getting false positives which are usual in different detection methods. This method is not computationally efficient.

Wang et al. [3] proposed a method for detecting copy-move forgery based on Hu moments. In this method first of all size of image is contracted due to use of Gaussian pyramid. After that image is divided in fixed size blocks which are overlapping. For each block Hu moments are computed. After that Eigen values are calculated. These vectors corresponding to each block are stored and lexicographical sorting applied to identify similar vectors. Then threshold value decided for decreasing false detections. Morphological operations used for matching of similar blocks. This algorithm is more efficient and robust to post-processing operations like blurring and lossy JPEG compression.

Mohmadian and pouyan [4], conducted a study on detecting copy-move forgeries using SIFT (Scale Invariant Feature Transform) algorithm with Zernike moments. SIFT algorithm used for detecting normal copy-move portions but this method failed to detect forged flat regions so zernike moments used with this algorithm. Using SIFT algorithm feature points extracted. Extracted features used for finding matching. To avert false matches hierarchical clustering used. In this clustering is done on the basis of threshold value and a tree is constructed on the basis of similarity. In this method they considered that if two clusters are similar with at least three similar feature points then portion is considered as copy moved. SIFT methods are unable to find flat copy-move forgeries to overcome this drawback Zernike moments are used. The image is divided in overlapping blocks and Zernike moments are calculated for each block. This process has high complexity. After applying this method feature vectors along with Zernike moment coefficient is achieved. By using threshold value matching blocks identified.

(b). Dimensionality Reduction-Based Methods

There are several dimensionality reduction based methods one of them is PCA (principal component analysis). This method was proposed by Popescu and Farid [5]. At first if the given image is color image then it is converted to gray-level image. Image divided in fixed size overlapping blocks as shown in Fig.3. Further these blocks are represented in form of vectors. These vectors of block sorted in lexicographical order for matching. PCA is used for representing the blocks of image. PCA method has the ability to find changes occurred due to noise addition and lossy JPEG compression. They applied proposed method only over gray scale images. This method can also be applied over color images using different color channel which yields three different maps. PCA can be applied to these maps separately to detect copy-move forgery. The proposed method has good efficiency and generates less number of false matches. In this method if the block size decreases then efficiency also decreases.

Ting and Rang ding [6] used singular value decomposition for copy-move forgery detection. SVD [7] facilitates matrix factorization as well as can be used for drawing out the geometric and algebraic features from an image. SVD is utilized in many fields like signal processing, data compression and pattern analysis. Given a $\mathrm{P} \times \mathrm{Q}$ matrix. 'h' is rank of $\mathrm{L} \in R^{P \times Q}$. The SVD algorithm assumes that there exists orthogonal matrices $\mathrm{M} \in R^{P \times P}$ and $\mathrm{N} \in R^{Q \times Q}$ such that L is factored as in (1).

$$L = M \sum N^T \tag{1}$$

Where, $\sum \in R^{P\times Q}$ is a $P \times Q$ diagonal matrix as shown in (2).

$$\Sigma = \begin{bmatrix} \sum_h & 0 \\ 0 & 0 \end{bmatrix} \quad (2)$$

Where $\sum_h$ is a square diagonal matrix belongs to $R^{h\times h}$: $\sum_h$ = diag ($\sigma_1, \sigma_2, \ldots\ldots \sigma_h$), This matrix have positive diagonal entries which are called singular values of L and ranked in decreasing order as $\sigma_1 \geq \sigma_2 \geq \cdots . \geq \sigma_h$. Their proposed algorithm is computationally less complex. Here, correlation between copied and forged segment is used to detect forgery. An image is divided into fixed size overlapping blocks. After that SVD is applied on every block and singular values are extracted for each block. These extracted singular values are feature vectors corresponding to each block. On the basis of feature vectors similar blocks are detected. These feature vectors transformed into k-d tree. Using threshold value false matches get reduced. This algorithm is not able to detect that which segment is copied and which is pasted segment and also not robust to JPEG compression.

A dimensionality reduction based method is proposed by Basher et al. [8]. They used Discrete Wavelet Transform (DWT) and Kernel Principle Component Analysis (KPCA) for detection of copy-move forgery. At first the image is divided into fixed sized overlapping blocks then KPCA used for feature extraction from each block. They placed these feature vector in a matrix and lexicographical sorting is performed to identify similar blocks. To avoid false matches threshold value is set for offset frequency. They implemented a novel algorithm for flip and rotation counterfeit using labeling technique and geometric transformation. This algorithm shows better result than conventional PCA method and also robust against additive noise and lossy JPEG compression.

Zimba and Xingming [9] proposed a method based on DWT-PCA (EVD). As DWT divides input image in four sub-bands LL, HL, LH and HH which contains low frequency information, horizontal component, vertical component and diagonal component information respectively. By using DWT there is no need to analyze whole image. All low frequency components which are of more importance are contained in approximation band. Due to this complexity get reduced. Only $1/4^{th}$ of the original number of blocks of fixed size are considered after first level decomposition which belong to approximation band. If an image is divided in blocks of dimension $B \times B$ and input image is of dimension $M \times N$. Total number of blocks in an image will be $(M - B + 1)(N - B + 1)$. As by applying DWT we get four sub-bands and only one of them is analyzed for finding forgery. So, now the number of blocks from which features extracted get reduced to $(\frac{M}{2} - B + 1)(\frac{N}{2} - B + 1)$ after first level of decomposition. Hence, by using DWT complexity reduced. After applying DWT they applied Principal component analysis-Eigen value decomposition (PCA-EVD) on blocks for feature extraction. Extracted feature vectors stored in a row vector. A matrix is formed containing feature vector corresponding to each block. Matrix will have rows equal to the number of blocks of approximation band and number of columns equal to the length of feature vector. Lexicographical sorting is applied on the matrix. Due to sorting similar feature vectors will be in proximity to each other. Shift vector is calculated corresponding to blocks. Each block has it's coordinates as left-top corner location. Shift vector is calculated by subtracting corresponding x and y coordinates of top-left corner of two blocks. These shift vectors are normalized by multiplying with -1 if shift vectors values are negative. Counter value initialized to zero. Whenever blocks having similar shifting are obtained counter value increased by one. Threshold value is set and when the counter value is greater than threshold value those block pairs are considered as copy-move forged region. This method is robust against varying degree of rotation performed over copied part of an image. The disadvantage of this method is that if the forgery size is less than the size of blocks then the forgery could not be detected. This method is also fail to detect regions where scaling is performed on copied part and if heavy compression is applied.

(c). Intensity-Based Techniques

Luo, Huang and Qiu [10] proposed a method for finding copy-move image forgery. This method is based on intensity. In this method image is divided in overlapping blocks of fixed dimensions. Further blocks are divided in two equal parts in four directions. Then for each block a vector is calculated by using Additive White Gaussian Noise (AWGN) operation. AWGN operation is used for feature extraction from each block. These feature vectors stored in a matrix. Lexicographical sorting is applied over vectors so that similar vector occupy the position in neighborhood of each other. To reduce the false matches in image shift vectors are calculated. If similar shift vector is obtained more than a threshold value then corresponding blocks with that shifting considered as forged blocks. Proposed algorithm has less complexity and robust against post-processing operations. Their algorithm works well when the forgery size is greater than the size of overlapping blocks. In some cases where forged region is highly distorted this algorithm failed. Also, if image contain large smooth region in that case algorithm failed to identify actual forged region because of occurrence of false matches.

Bravo-Solorio and Nandi [11] proposed a method for finding copy-move forgery in an image where copied region is manipulated using scaling, rotation and reflection. In this method an image is divided in block of pixels by using a sliding window which slides from top left to right bottom in raster-scan order. Feature extracted from blocks to analyze forgery. To reduce the complexity color dependent features are extracted. Four features extracted from blocks. They are red, green, blue components and fourth one is entropy of luminance channel. As number of features decreased so complexity reduced and efficiency increased. Fourth feature is useful in discarding blocks having inefficient textural

information. Extracted features stored and lexicographical sorting is performed to find similar feature values corresponding to overlapping blocks. This method results in large number of false matches. 1-D descriptors are used for reducing false matches. They are

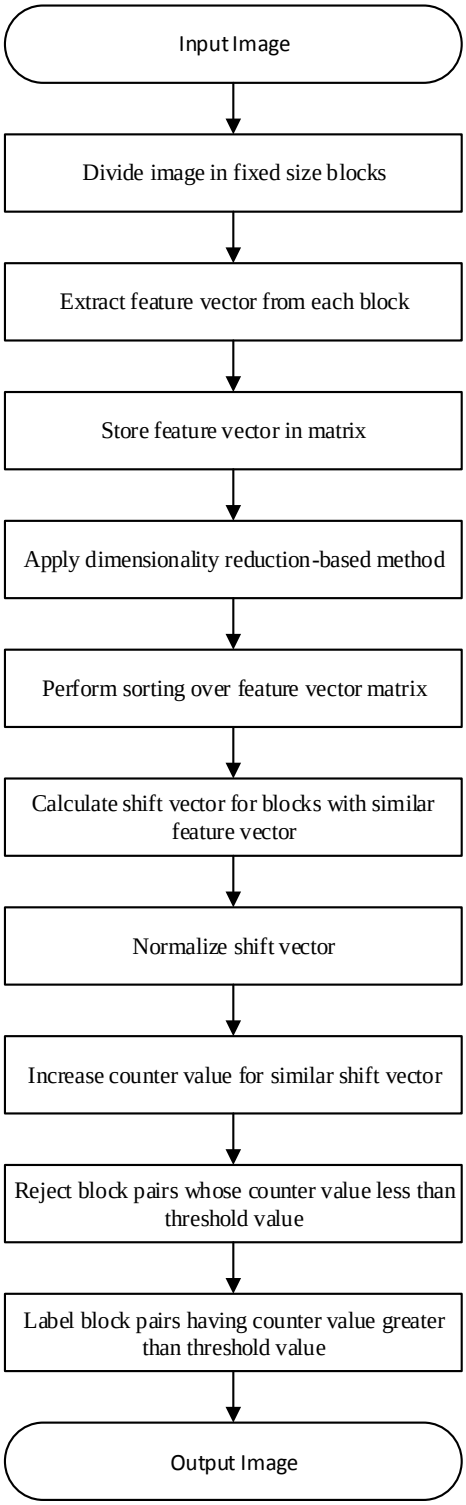


Fig.3. Block-Based Methodology

efficient in reducing memory usage and also invariant to reflection and rotation. This method is better than other forgery detection methods because this method result in less computation and also robust against post-processing operations applied over copied regions.

Lin et al. [12] proposed a new technique for copy-move forgery detection method. In this method image is divided into fixed size blocks. After that each block is further divided in four sub-blocks. For each sub-block intensity is calculated. Average intensity of block calculated by using four sub-blocks. Relative intensity is calculated using difference of individual intensity of each block and their average intensity. They applied this process for each block and feature vectors are obtained. Feature vector corresponding to each block are integer value so radix sort is applied instead of using lexicographical sorting for finding similar feature vectors. For reducing false matches further shift vectors are calculated. Blocks corresponding to highest occurred shift vector labeled as forged blocks. This method is capable of detecting forged region with JPEG compression and Gaussian noise. This method failed where copied region is rotated at different angles.

Wang, Liu, I, Dai and Wang [13] proposed a method using Gaussian pyramid method. In this method the dimension of image is reduced by using Gaussian pyramid. In this algorithm circular blocks are used instead of rectangular or square blocks. Four features are extracted from each circular block. After feature extraction lexicographical sorting is applied. Using threshold value similar blocks could be obtained which reduces false matches. Their method is used for identifying tampered region with post- processing operations like lossy JPEG compression, blurring and rotation.

Sridevi, Mala and Sandeep [14] proposed a method for detecting copy-move forgery detection. This method was developed for real-time applications. Methods like PCA, SVD or DWT have higher complexity, so they cannot be used in real-time applications. In this algorithm input image is grayscale image. Image is divided into fixed size overlapping blocks. Intensity features are extracted from each block. Feature vectors are in form of row vector corresponding to each block. Two additional columns are used in row feature vector for storing location of each block. Lexicographical sorting is performed using radix sort in a parallel way. By sorting similar feature vectors corresponding to similar blocks will be in proximity to each other also containing corresponding block positions. These feature vectors are helpful in locating position of forged block in image. Their method is successful in reducing processing time. False detection rate can be reduced by adjusting block size. Drawback of this method is that it cannot be applied over color images.

(d). Frequency-Based Techniques

Fridrich, Soukal and Lukas [15] proposed a method based on Discrete Cosine Transform (DCT). At first they divided the image in overlapping blocks by using a fixed size sliding window. This window moves by one pixel along the direction top-left to bottom-right. For each block pixel values are stored in a row. A matrix is formed having row with pixel value corresponding to each block.

Lexicographical sorting is performed to find similar blocks. This method is known as exact match method. Another method is robust match method. In this approach DCT coefficient [16] are calculated for each block. Quantization is performed over DCT coefficients to achieve finer results. A suitable value of Q-factor is decided for appropriate quantization. For each block DCT coefficients are calculated and stored in row vector. These feature vectors stored in a matrix. Lexicographical sorting is performed over matrix. Similar blocks found with help of highly occurred shift vectors. The disadvantage with this method is that it cannot differentiate between large identical areas on a natural image.

Zhang, Feng and Su [17] proposed an efficient and robust method based on Discrete Wavelet Transform (DWT). In this approach DWT is applied on the image. Image is divided in four sub-bands by using DWT. Four sub-bands have horizontal, vertical, diagonal components and Fourth sub-band is approximation band. Approximation band is used for identifying forgery in image. This band is divided in overlapping blocks. Features are extracted from the blocks and stored in a row vector. A matrix is formed having rows corresponding to feature vector of each blocks and columns equal to the number of features extracted for a block. Lexicographical sorting is performed to find similar feature vector blocks. Identical blocks will be present if copy-move forgery performed in image. Drawback associated to this method is that if forgery is present at middle of the image then it could not be detected. In this case images have to be divided in sub images and this algorithm should applied recursively.

Bayram, Sencar and Memon [18] proposed a method based on Fourier-Mellin Transform (FMT). FMT has different properties like it is robust against blurring, scaling, translation, noise, JPEG compression and other translations enforced as post-processing over copied portion of the image. In this method first of all image is divided in overlapping blocks after that fourier transform is calculated for each block. Due to use of fourier tansform it is certain that method is invariant to translation. Calculated fourier transform is used as feature vectors after performing resampling, projection and quantization. These feature vectors are operated to make them rotation invariant so that if copied region is rotated to arbitrary angles before pasting then the values of vectors should not change. If these values changed due to arbitrary rotation then forgery cannot be identified for similar regions in image. These feature vectors corresponding to each block are stored in a matrix. Lexicographic sorting is performed to identify similar feature vectors. An original image can also have similar regions in an image. So to reduce such type of false matches distance between blocks is calculated by using Euclidean distance. With this method a bunch of blocks could be identified which have similar shifting. Hence, copy-move forged blocks will be identified. Their method is robust to scaling up to 10% and also can detect forged region rotated up to 10^0. Proposed method is also robust to JPEG compression.

Li and Wang [21] proposed an algorithm based on Polar Harmonic Transform (PHT). In this method PHT is used for feature extraction from blocks. Orthogonal moments are used for generating features from block. PHT can only be defined over a unit disc so blocks are not considered to be square as done in other passive forgery detection method. These feature vectors stored in a row. A matrix stores extracted features of all circular blocks. Lexicographical sorting is applied on matrix to establish the similar feature vectors in proximity of each other. Next step is to detect similar blocks in image this is done by using simulations. For detecting efficiency of the method several images are taken with post-processing operations applied over copied regions. Their method is able to find blocks which are orthogonally rotated to hide forgery in image. If the rotation performed at some arbitrary angles then this method does not yield good results. Although it can locate forged sections in such cases. These researchers showed forgery detection on images having geometrical transformation over copied segment. PHT algorithm holds well where copied region is rotated before pasting it on original image to make a forged image. This method does not provide good results where scaling is performed over copied region and also not holds good in case of local blending.

Muhammad, Hussain, Khawaji and Bebis [22] proposed a method for detecting copy-move forgery based on Dyadic Wavelet Transform (DyWT). Their method used low frequency and high frequency components and by applying similarity measure forged blocks are identified. DyWT is used in various applications to identify forgery in image. DyWT is shift invariant so Mallat and Zhong proposed a method based on the shift invariance property of this transform. Muhhammad et al. used Low pass filter and high pass filters for decomposing input image in sub-bands. Two sub-bands LL1 and HH1 are used for identifying forgery as shown in Fig. 4. They used a block of dimension 16x16 for dividing sub-bands having 8 overlapping pixels. LL1 is achieved by applying low pass filter in both horizontal and vertical direction in image. HH1 is obtained after applying high pass filter in both horizontal and vertical directions. In this method it is assumed that copy-move forgery is performed at least for 16x16 pixels. LL1 sub-band contains similarity features between blocks while HH1 sub-band contain dissimilarity features between blocks. Similarity between blocks are obtained by calculating Euclidean distance as shown in (3).

$$D(x,y) = \sqrt{\frac{1}{N}\sum_{i=1}^{n}(x_{i-}\ y_i)^{\ 2}} \tag{3}$$

X and Y are block pairs. x_i And y_i are corresponding gray values of pixels. $D(x,y)$Gives distance between pair of blocks for both LL1 and HH1 band. N=256 is assumed. After calculating distance between pair of blocks these

distance values are normalized according to maximum distance between blocks on scale 0 to 1. These distance values corresponding to LL1 sub-band and HH1 sub-band are stored in List1 and List2. List1 is sorted in ascending order. All the pair of blocks having distance value>0.7 are discarded. This value is identified as

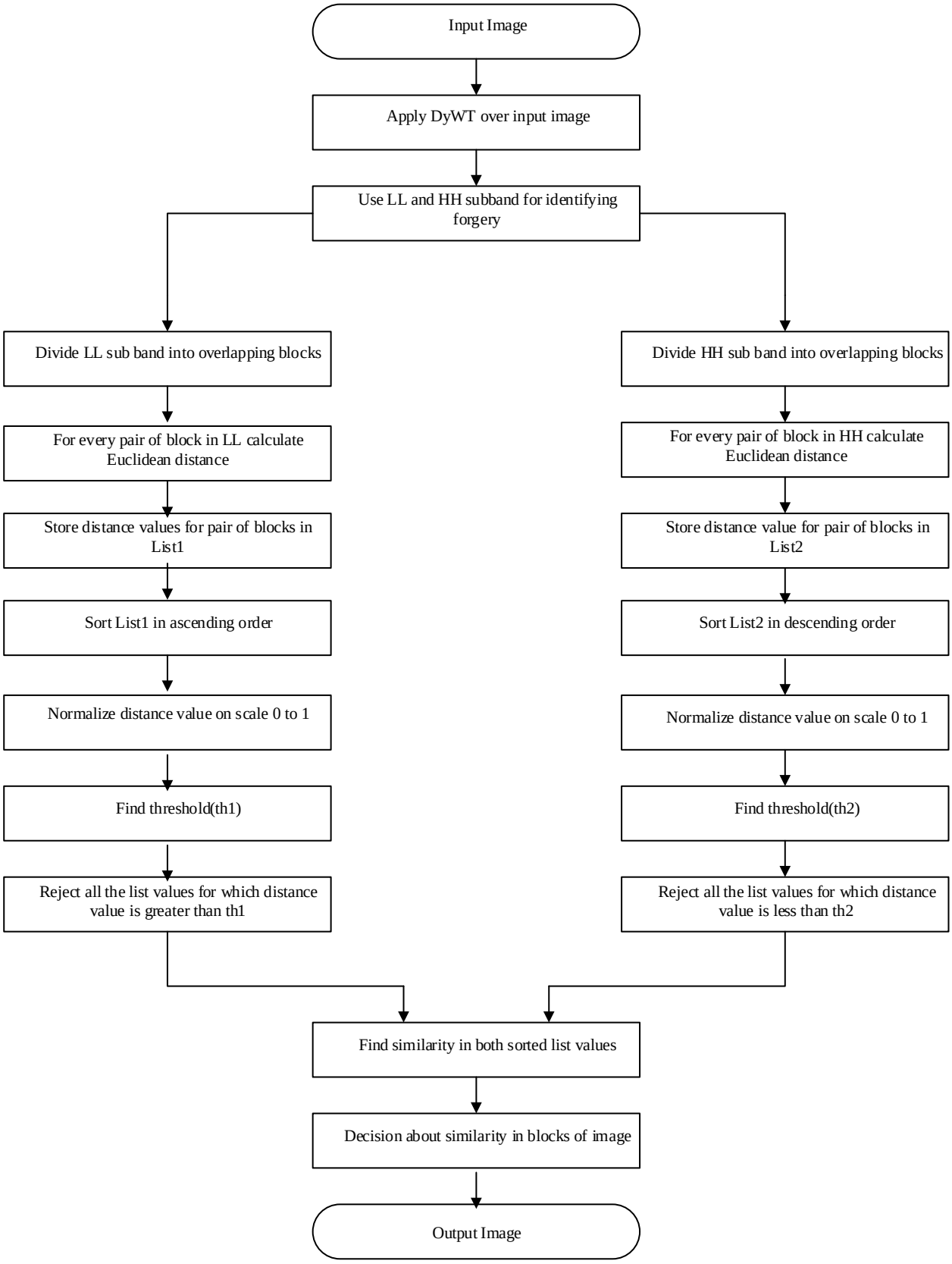


Fig.4. Block-Based method using DyWT

threshold1 (th1). Similarly, in HH1 sub-band Euclidean distances are calculated and they are arranged in decreasing order. A threshold value is set. All the block pairs having distance<0.3 discarded because List2 is concerned about dissimilarity between blocks. This value is referred as threshold2 (th2). On the basis of similarity between the lists forged blocks are identified. If for a block pair (p,q) which is at r^{th} location in List1 and similar values are there for pair of block in List2 at position between $(r-i)^{th}$ and $(r+i)^{th}$ then these block pairs will be identified as copy-moved blocks in image. Value of i may vary from 1 to 15. For $i = 7$ optimum results were obtained. Both list are compared for distance values to avoid false matches. For applying DyWT method first of all we have to convert color image in gray.

A method proposed by Ghorbani, Firouzmand and Faraahi [19] for detection of copy-move forgery. They used Discrete Wavelet Transform for dividing input image into four sub-bands. In this method low pass filter and high pass filter is applied to get four sub-bands which contains the horizontal, vertical, diagonal and a low frequency component sub-band. Low frequency sub-band LL also known as approximation sub-band. As low frequency components are highly rich in information. This sub-band is divided in square blocks by using a sliding window of fixed dimension moving all over the approximation sub-band from top-left corner to bottom-right corner. In this algorithm for feature extraction from square blocks Discrete Cosine Transform (DCT) is used. After achieving DCT coefficients corresponding to each block these coefficients are decomposed using Quantization Coefficient Decomposition (QCD). In this method a quantization table is used for coefficient decomposition having different Quantization factor (Q-factor). As the values of Q-factor increases quantized coefficient decomposition holds much finer values. For each block features are extracted and quantized. These features are stored in a row vector. A matrix is formed storing feature vectors for all blocks. Lexicographical sorting is applied for obtaining similar feature vector at neighboring positions. Shift vectors are calculated for neighboring blocks. On the basis of shifting between blocks similar blocks are identified. This method yields better results than other algorithms but cannot identify forgery if the forged region contain post-processing Operations on copied region like scaling, heavy compression and rotation before pasting them to original image.

Li et al. [20] used a new algorithm for copy-move forgery detection. In this method Local Binary Pattern (LBP) is used for describing image texture. LBP is also known as gray-scale operator. First of all pre-processing is done on the input image to convert it into grayscale image. There could be such forged images which might go through noise addition, lossy JPEG compression and various other transformations as post-processing operations applied over forged segment. High frequency components will not be helpful in forgery detection. Gaussian low pass filter is applied and resulted in conclusion that if filter is applied for number of times then more accurate detection results are obtained. Further image is divided in overlapping blocks which are circular. Features are extracted from each circular block using LBP. LBP is rotation invariant so gives efficient result in detecting forgery if copied region is rotated at arbitrary angles before pasting. These feature vectors are in form of row vectors. Feature vectors stored in a matrix having a row feature vector corresponding to each block. These vectors are lexicographically sorted to avoid computation for finding similar forged blocks. Euclidean distance is calculated for finding distance between blocks. A threshold value is set for finding blocks associated with a similar distance. This method accurately finds the copy-moved blocks. For reducing number of false matches filtering is used. To remove false matches completely morphological processing is applied. This method is invariant to rotation and flipping but fail to identify regions rotated at different angles.

Qiao, Sung, Liu and Ribeiro [23] proposed a new methodology for detection of copy-move forgery. In this algorithm multi-resolution and multi-orientation curvelet transform is used. Basically curvelet transform utilized in frequency domain which yields efficient results. At first color image is divided into sub-bands. Further these sub-bands are divided in several blocks. Ridgelet analysis performed over these blocks to detect copy-move forgery in image. Ridgelet transform is combination of radon Transform and 1-D Wavelet Transform. This method is computationally complex so authors applied fast discrete curvelet transform. By using this method a pyramid structure is obtained which have multiple orientations at multiple scales due to this detection accuracy and Performance enhanced. As due to fast discrete curvelet transform, multi-directional decomposition is obtained which gives accurate relation between neighboring orientations. Pyramid structures are used for extracting features at multiple-orientations. These features are stored for every block in a matrix. Lexicographical sorting is applied for finding similar features which reduce the complexity of finding copy-moved blocks. Their method is able to identify tampered region of image even if JPEG compression, rotation and scaling applied. One constraint with this method is that it cannot be applied on compressed images. At first image should be decompressed if it is compressed. Pre-processing is required over images if image is colored convert it to gray scale image.

B. Keypoint-Based Techniques

These techniques used for copy-move forgery detection on the basis of finding correlation between original image segment and pasted segment(copying from original image and then performing post-processing over copied segment to make it difficult to identify forged region and pasting them over some other location on same image). Huang et al. [24] used SIFT (Scale Invariant Feature Transform) [25] to identify copy-moved regions. This method can identify forgery when post-processing is done over copied segment but failed to identify small size of tampered region. Further, Junwen et

al. [26] proposed SURF (Speeded up Robust Feature) method for copy-move forgery detection. They used Hessian matrix for key-point detection and Haar wavelets used for identifying their orientation. This method is fast in detecting forgery but failed to identify exact boundaries of tampered region.

The main problem in detecting copy-move forgery is because of multiple processes applied over copied region before pasting it over same image to hide forgery. Image processing operations like rotation, scaling, compression, bending, and noise addition made forgery detection very difficult. Computational complexity is also a major problem. If forged region go through rotation and scaling transformations then key point based methods like SIFT is effective in detecting forgery. Key point based methods are also robust to noise and variations in illumination conditions but drawback associated to this method is about unable to detect duplicated flat regions. Zernike moments are capable of detecting flat forged regions but unable to detect scaled copy-moved regions. Methods using block based algorithms are not able to detect duplicated regions with scaling and rotation. Algorithms using circular blocks rather square or rectangular blocks are rotation invariant so can detect forgeries with rotation. Below Table 1 shows the advantages and disadvantages of different methodologies used for detecting copy-move forgery.

IV. Conclusion

Nowadays, performing forgery over images is very easy. Detection of such type of forgery is very interesting topic of research. Copy-move forgery is one of the hot research topic. Various algorithms are proposed by researchers to identify such forgeries in images. In this paper, several methods have discussed. These methods are robust against post-processing operations performed over copied segment. Many algorithms are suggested by researchers based on Fourier transforms but still there is lot of scope in this field to find such methods which can be robust against several post-processing operations simultaneously. Some algorithms gives efficient results when certain assumptions are made. After analyzing several methods used for copy-move forgery detection it is noticed that use of hybrid approach is more successful in providing accurate results with less computational cost. This area of research is growing. Also, there is a need of huge dataset to benchmark the results of forgery detection methods.

Table 1. Advantages and Disadvantages of Moment Based Copy-Move Forgery Detection Techniques.

Author	Method	Advantage	Disadvantage
Mahadian 2007[2]	BLUR	BLUR invariants don't get affected by blur degradation and additive noise.	Computation time is high.
Wang 2009[3]	HU	Robust against blurring and lossy JPEG compression.	High probability of False Matches.
Mohamadian 2013[4]	Zernike	Efficient detection of flat copied regions.	Calculation of Zernike moment is complex.

Table 2. Advantages and Disadvantages of Dimensionality Reduction Based Copy-Move Forgery Detection Techniques.

Author	Method	Advantage	Disadvantage
Popescu 2004[5]	PCA	Small variations due to noise and lossy compression can be detected accurately.	For low quality image, as size of block decreases so does efficiency.
Ting 2009[6]	SVD	Less computation complexity and robust against post processing operations.	Cannot deal with JPEG compression.
Bashar 2010[8]	KPCA	Forgeries with additive noise and JPEG compression can be detected.	Average accuracy is less than other methods which are based on wavelet.
Zimba 2011[9]	PCA-EVD	False matches are less and duplication with varying degree of rotations can be detected.	Unable to detect forgeries with scaling and heavy JPEG compression.

Table 3. Advantages and Disadvantages of Intensity Based Copy-Move Forgery Detection Techniques.

Author	Method	Advantage	Disadvantage
Luo 2006[10]	LUO	Computational complexity is less. This method can withstand against post-processing operations.	Highly distorted images with large smooth region cannot be detected.
Bravo 2011[11]	BRAVO	Rotation and reflection invariant.	Unable to differentiate copy-paste regions of image.
Lin 2009[12]	LIN	Forged regions with Gaussian noise and JPEG compression Can be detected.	When tampered region rotated at different angles this method failed.
Wang 2009[13]	CIRCLE	Forged regions with post-processing operations such as blurring, rotation and JPEG compression can be detected.	Not robust against scaling.
Sridevi 2012[14]	PCMIFD	Efficient for real time applications. False matches are less.	It cannot be used for color images.

Table 4. Advantages and Disadvantages of Frequency Based Copy-Move Forgery Detection Techniques.

Author	Method	Advantage	Disadvantage
Fridrich 2003[15]	DCT	Concept of mutual pairs is used, false matches are very less.	Large size similar textures of natural images cannot be detected.
Zhang 2008[17]	DWT	Image size get reduced due to down sampling.	It cannot detect forged region present at center of image.
Bayram 2009[18]	FMT	Robust to post processing operations such as blurring, noise, JPEG compression, scaling and translation.	It cannot detect regions rotated greater than 10^0 and regions with scaling greater than 10%.
Li 2012[19]	PHT	Forged blocks which are orthogonally rotated can be identified.	In case of scaling and local blending this method does not yield good results.
Muhammad 2011[20]	DyWT	Shift invariant method.	Image should be converted to grayscale as preprocessing step.
Ghorbani 2011[21]	QCD	Computationally efficient.	Forgeries with rotation, scaling and heavy compression over copied region cannot be detected.
Li 2013[22]	LBP	Rotation and flipping invariant method.	Forged region rotated at varying angles cannot be detected.
Qiao 2011[23]	Curvelet	Forged regions with JPEG compression, scaling and rotations can be detected efficiently.	This method cannot be applied over compressed images. Image should be decompressed before analysis.

REFERENCES

[1] S. Agarwal and S. Chand, "Image forgery detection using multi scale entropy filter and local phase quantization", International Journal of Image, Graphics and Signal Processing, vol. 7, pp. 78-85, 2015.

[2] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic Science International, vol. 171, pp.180-189, 2007.

[3] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai and Z. Q. Wang, "Fast and robust forensics for image region duplication forgery," Acta Automatica Sinica, vol. 35, pp.1488-1495, 2009.

[4] Z. Mohamadian and A. Pouyan, "Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions," in 15th International Conference UKSim, 2013.

[5] C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, Hanover, United States, 2004.

[6] Z. Ting and W. Rang-ding, "Copy-move forgery detection based on SVD in digital image," in International Conference on image and signal processing, 2009.

[7] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics,"

in International conference on computer science and software engineering, vol. pp. 926-930, 2008.
[8] M. Bashar, K. Noda, N. Ohnishi and K. Mori, "Exploring duplicated regions in natural images," IEEE Transactions on Image Processing, 2010.
[9] M. Zimba and S. Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection", International Journal of Digital Content Technology and its Applications, Vol. 5, 2011.
[10] W. Luo, J. Huang and G. Qiu, " Robust detection of region-duplication forgery in digital image," in 18th International Conference on Pattern Recognition ICPR, 2006.
[11] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics," in Signal Processing, Vol. 91, pp.1759-1770, 2011.
[12] H. J. Lin, C. W. Wang and Y. T. Kao, "Fast copy-move forgery detection. WSEAS Transactions on Signal Processing," Vol. 5, pp.188-197, 2009.
[13] J. Wang, G. Liu, H. Li, Y. Dai and Z. Wang, "Detection of image region duplication forgery using model with circle block," in International Conference on Multimedia Information Networking and Security (MINES'09), 2009.
[14] M. Sridevi, C. Mala and S. Sandeep, "Copy–move image forgery detection," Computer Science & Information Technology (CS & IT),Vol. 52, pp.19-29, 2012.
[15] J. Fridrich, B. D. Soukal and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Digital Forensic Research Workshop, 2003.
[16] S. Kumar, J. V. Desai and S. Mukherjee, "Copy move forgery detection in contrast variant environment using binary DCT vectors," International Journal of Image, Graphics and Signal Processing, vol. 7, pp. 38-44, 2015.
[17] J. Zhang, Z. Feng and Y. Su, "A new approach for detecting copy-move forgery in digital images," 11th IEEE Singapore International Conference on the Communication Systems, ICCS, 2008.
[18] S. Bayram, H. T. Sencar and N. Memon, "An efficient and robust method for detecting copy-move forgery," IEEE International Conference Acoustics, Speech and Signal Processing, ICASSP, 2009.
[19] L. Li, S. Li and J. Wang, "Copy-move forgery detection based on PHT," World Congress Information and Communication Technologies (WICT), 2012.
[20] G. Muhammad, M. Hussain, K. Khawaji and G. Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform," Digital Signal Processing DSP, 2011.
[21] M. Ghorbani, M. Firouzmand and Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," 18th International Conference Systems, Signals and Image Processing (IWSSIP), 2011.
[22] L. Li, S. Li, H. Zhu, S. C. Chu, J. F. Roddick and J. S. Pan, "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns," Journal of Information Hiding and Multimedia Signal Processing, Vol. 4, pp.46-56, 2013.
[23] M. Qiao, A. Sung, Q. Liu and B. Ribeiro, "A novel approach for detection of copy-move forgery," Fifth International Conference on ADVCOMP (Advanced Engineering Computing and Applications in Sciences, 2011.
[24] H. Huang, W. Guo and Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," Pacific-Asia Workshop Computational Intelligence and Industrial Application, 2008.
[25] S. A. Thajeel and G. B. Sulong, "State of the art of copy-move forgery detection techniques: A Review," International Journal of Computer Science Issues", Vol. 10, pp. 174-183, 2013.
[26] X. Bo, W. Junwen, L. Guangjie and D. Yuewei, "Image copy-move forgery detection based on SURF," International Conference on Multimedia Information Networking and Security (MINES), 2010.

Authors' Profiles

Anuja Dixit is Research scholar pursuing M.Tech in Cyber Secutity from Madhav Institute of Technology & Science, Gwalior, India. She received B.Tech degree in Computer Science & Engineering from University Institute of Engineering & Technology, Kanpur, Uttar Pradesh, India.

R. K. Gupta is currently Professor and Head of computer science & Engineering/Information Technology Department at Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, India. He has received M.Tech degree in Computer Science & Engineering from Indian Institute of Technology, Delhi. He has received Ph.D. degree from Indian Institute of Information Technology and Management, Gwalior. He has guided various thesis at Master's and Ph.D. level. His area of specialization is Data Mining.

How to cite this paper: Anuja Dixit, R. K. Gupta,"Copy-Move Image Forgery Detection a Review", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.6, pp.29-40, 2016.DOI: 10.5815/ijigsp.2016.06.04

