STATE OF THE ART OF COPY-MOVE FORGERY DETECTION TECHNIQUES: A REVIEW

Salam A.Thajeel [1,2] and Ghazali Bin Sulong [1]

**[1] Faculty of computing , University Technology Malaysia (UTM)
Skudai ,Malaysia**

[2] Computer Science Department , Collage of Education ,The University of Al-Mustansiriyah, Baghdad, Iraq

Abstract

The different methods for processing and detecting forgery in digital images have received growing attention recently. This is due to the availability of up-to-date editing software and sophisticated digital cameras, which simplify the duplication of regions for the forgers where part of an image is pasted to another location to conceal undesirable objects. An example of these methods is copy-move (i.e., Cloning) forgery in digital images. Detection of copy-move forgery to search the copied regions and they're pasted ones, but detection may vary based on whether there has been any post-processing on the copied part before paste it to another party. Generally, forgers apply some operations such as filtering, resizing, rotation, JPEG compression, and noise addition to the original image before pasting, which make it difficult to detect copy-move forgery. Hence, forgery detector should be robust to all manipulations and up-to-date editing software. In the literature, researchers described the working process of copy-move forgery based on the similarity and based on the relationship between the original image parts and pasted one within the same image. This paper highlights current issues in the forgery detection approaches and all their comparative analysis.

Keywords: *digital forensics*, *copy-move forgery, duplication forgery detection, forgery detection,*

1. Introduction

The latest imaging technologies have given forgers require tools for changing and using the contents of digital images to the aim of adding deceptive object to the images with no noticeable features [1]. From this point, it is suggested by many researchers to establish images authenticity to detect these activities which can be found in many applications such as criminal investigation, medical imaging, journalism, intelligence services and surveillance systems.

Therefore, digital forgery detection techniques have been developed to justify the forgery issue as a necessary process in image processing [2]. Several research studies were conducted in different disturbing fields to enhance the current techniques for copy-moving forgery [3], which include hiding or adding a region in the image or displaying incorrect information [4]. The common forgery techniques in digital images can be divided into three main groups: Copy-Paste (i.e., Splicing), Image Retouching, and Copy-Move (i.e., Cloning). For instance, retouching technique which works on manipulating the digital image by changing its features without making noticeable modifications of the content of the image. Meanwhile, image splicing on the other hand, make use of the original image with additional images to generate a tampered copy [5,6], such method work on adding some part of other images to the original image so that forgers hide or modify the content of the image. In addition, image cloning, which works by copying a definite part of an image and shifting it to another part of the same image so that forgers can hide or duplicate some part of the image [7]. Hence, current effort in developing reliable methods for image forgery detection has gained attention of many researchers. Detection method found in the literatures can be categorized into active method and passive method [8, 9]. An active detection method like watermarking, which consists of adding image details in order to describe digital tampering such as name, date, signature, etc. While the passive method consists of detecting forgeries or duplicated objects in images without considering the information of the original images [10]. The main goal of this method is to express how detecting forgeries are possible without any need of original image watermark.

Several new forgery techniques were introduced by different scholars to describe its workability based on the robust. The key characteristic of image cloning is that, since the duplicated region is picked from the image itself, the noise components, texture and color patterns are compatible with the rest of the image. Thus, it is not easy to detect the forgery parts [11,12]. Moreover, there might be post-processing operations that can even make the exposing procedure harder.

In this paper, the focus is on detecting copy-move (i.e., cloning) image forgery along with describing the issues associated with the forgery detection. Nevertheless, we

introduced the latest forgery detection techniques proposed in the literature.

2. CURRENT ISSUES

Since the digital images play a significant role in simplifying the way of representing and transferring ideas flexibly, an attention has been paid recently towards investigating the suitable mechanism for analyzing and detecting forgery in the digital images. This attention was due to the latest malicious activities in which a single object inside the image is duplicated within the same image. Such activities can be seen in the copy-move forgery that considers one of the most known activity aims at including or hiding a [13, 14]. Many scholars have agreed that copy-move forgery works on the premises of detecting added noise, color changes, and texture that can be found within the duplicated area inside the image. Usually it is possible to identify the duplicated object by computing and comparing these premises with the whole image. But new forgery detection techniques are still lacking of up to date malicious activities. Such assumption came from the ability of forgers to change the geometry of the duplicated object easily by modifying the image's features. Therefore, a new copy-move forgery detection technique is needed in order to balance the new malicious activities on digital images [15, 16].

The issues and challenges being addressed in the domain of digital image forgery are forgery detection techniques, digital forgeries of social impacts, and forgery prevention techniques. The digital forgeries have many perspectives and implications on social, legal, technical, intelligence, investigative mechanisms, security, managerial issues [17, 18]. The forgery creation and detection are complimentary to each other. Figure 1 presents the workflow of the common forgery detection technique consists of four faces, these are overlapping blocks, feature extraction, block matching, and forgery decision. The utilization of this method to detect new forgery activities is considered to be useless, the reason back to that foragers have developed a new ways to overlap objects within the original image, this process of forgery creation contributes to the advances and sophistication in forgery detection methods which still a challenging topic. From the other hand, the confidentiality involved in the current forgery approaches presents a new level of complexity in forgery creation and forgery detection processes and acts as a hindrance to both of these processes. Figure 1 shows the general forgery detection approach consists of overlapping blocks, feature extraction, block matching, and forgery decision. This approach allows applying several extraction techniques such as DCT, PCA, etc. It also allows applying different matching techniques such as K-D tree and radix sort.

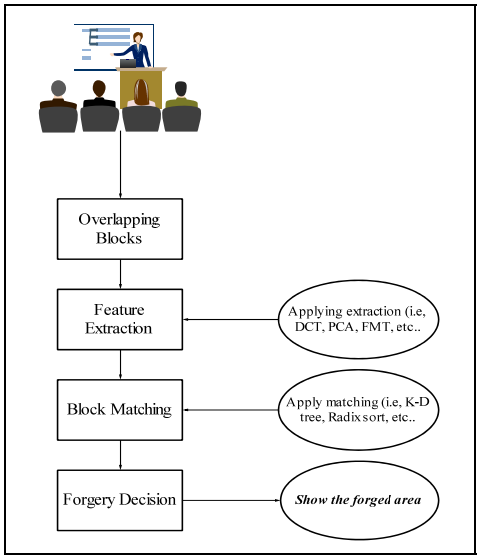

Fig 1. General Forgery Detection approach

Furthermore, the development of research in digital forensics has finally determined the suitable solutions for solving more comprehensive issues related to copy-move forgery. Accordingly it is emerging that generalized solutions and techniques, building standardized data sets, benchmarks, evaluation criteria etc. are still needed to be proposed to realize the new frameworks minimizing the chances for digital forgeries. Thus, many practical and precise techniques, solutions have been proposed which research will introduce in the next section. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification.

2.1 Natural

In this category, the image's data consists of author name, signature, description, tags, and so on are consider an important features that help to assets originality and authenticity of the digital image. Modifying these data by forgers may lead to forgery of information. Therefore, the originality and authenticity of images or data in many cases become challenging problem [17, 19]. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue. It is possible to generate high precision realistic images and data of any events [17, 20]. Identifying and differentiating the data and image acquired

by acquisition devices and realistic computer generated one is a multidimensional problem that has drawn attention of researchers worldwide.
This comes along with the latest digital editing tools, alteration, and manipulation that makes it an easy for the forgers to add or hide information within the digital images, therefore, it becomes a complex and threatening problem [21]. Specific to image forgery detection image can be manipulated in various ways with many simple operations like affine transforms (such as translation, scaling, rotation, shearing) compensation operations (like color, brightness, contrast adjustments, blurring and enhancement) suppression operation (such as filtering, compression and noise addition) [22]. Additionally more complex operations are also possible such as compositing, blending, matting, cropping, and photomontage leading to visually untraceable artifacts in an image [13]. The automatic and scientific method of detecting the forged images has become a big challenging problem for researchers and the same problem is true for every multimedia contents.

2.2 Forgery Detection

Forgery detection methods become much more complicated to deal with the latest forgery techniques. This back to the availability of digital editing tools, alteration, and manipulation become very easy and as a result forgery detection becomes a complex and threatening problem [23]. Image forgery detection can be manipulated in various ways with many simple operations like affine transforms such as translation, scaling, etc., compensation operations such as brightness, colors, contrast adjustments, etc., suppression operation such as noise extraction, filtering, compression, etc., [9]. Furthermore, more complex operations are also possible such as compositing, blending, matting, cropping, photomontage leading to visually untraceable artifacts in an image [24]. The automatic and scientific method of detecting the forged images has become a big challenging problem for researchers and the same problem is true for every multimedia contents.

2.3 Flow Mapping

Flow mapping helps to provide additional information about the forgery source in which the copied regions can be marked to be used later in identifying the pasted regions in the same image. Difficulties to identify the origin of the source back to the high speed accessibility of internet and easy availability of freely available high processing digital
editing tools (image) which increases the problem of authenticity of digital resources, the technology of digital resources is moving at a much faster rate due to social networking sites [25]. Thus finding the history (flow) of digital resources becomes a critical problem. Some efforts of finding the linage (flow) of data are being made in a networked environment [26]. In order to find the proper solutions to solve problems related to the authenticity of the intellectual assets, researchers have demonstrated these aspects as a potential problem with digital resources [27].

2.4 Source Identification

This category concerns about the challenges associated with identifying the data source that forgers usually rely on in copying and pasting the different regions in the same digital image [11]. Such aspects are found due to the new varieties of image acquisition devices such as digital camera, scanners, cell phones, etc. which increase the complexity in identifying the forgery source.

3. CURRENT TECHNIQUES

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

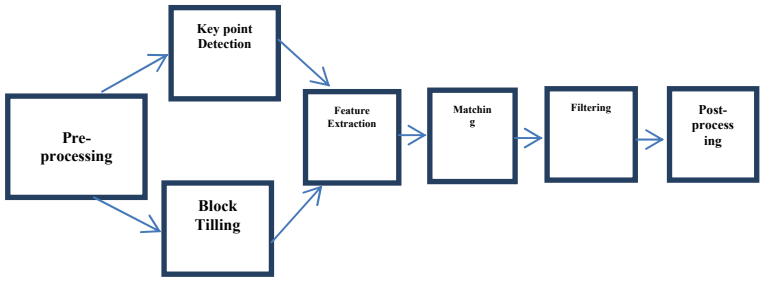

Fig 2. CMFD classification

3.1Block-based methods

Several techniques to detect copy-move forgery are based on block based method,The main idea of these techniques is that rather than trying to identify the entire forged region, the image is divided into small overlapping or non- overlapping blocks. The blocks are compared against each other in order to see which blocks are matched. The regions of the image covered by the matching blocks are the copied and forged regions. these techniques can classify as following

3.1.1 Moment-based (BLUR, HU, and ZERNIKE)

Mahdian and Saic [28] used blur moment invariants to represent image regions because they cannot be affected by blur degradation and additive noise. Their method

begins with tilting of images by blocks of a particular size. They represented each block with blur invariants. The feature vector for each block is of length 72. These are normalized further to improve the duplication detection abilities of the algorithm. They applied principal component transformation (PCT) to reduce the dimension of feature vector. For blocks similarity analysis, they used k-d tree representation. Using a certain threshold value, they found similar blocks. Once the similar blocks are found, they must be verified. They verified this by finding the neighborhood of similar blocks which are also identical. Two similar blocks with non-identical neighborhood are considered as false positive. By using this method, they successfully detected copy-move forgery for images which have blurred duplicated region. They could also detect duplicated regions with changed contrast values. However, there are some false alarms which are common in many of the proposed methods. Also, the computation time of the algorithm is comparatively high.

Wang, Liu, Zhang, Dai and Wang [16] conducted a study on copy-move forgery detection by using Hu moments. They developed the algorithm to be more efficient and also robust to various post-processing techniques such as blurring, lossy JPEG compression. They reduced the dimensions of the image by using Gaussian pyramid. They divided the image into several fixed sized blocks which are overlapping. They applied Hu moments to the blocks and calculated the eigen values. They sorted these vectors lexicographically and an area threshold is selected to reduce false detections. They performed finding matching blocks by using mathematical morphological techniques. Their method is successful in detecting copy-move forgery even when post-processing is done.

Mohamadian and Pouyan [29] described new method of detecting copy-move forgeries by using SIFT algorithm along with Zernike moments. They used SIFT algorithm to perform normal copy-move forgery detections. But SIFT cannot be used to detect flat copied regions. To account for this, they used Zernike moments. The process begins with SIFT feature points extraction. After extraction, they used these feature to find possible matches. To avoid false alarms of forgery, they used hierarchical clustering. This involves clustering of feature points into a tree structure based on certain threshold value. By this method, they were able to reduce false alarms because they considered that image is forged only when two clusters are matched with a minimum of three similar feature points. However, this feature reduces the possibility of detecting flat forgeries. Their method was able to find out the possible geometric transformations performed. To account for flat forgeries, Zernike moments are used. Initially, they divided the image into several sub-blocks and calculated Zernike moments. This involves complex calculations and at the end a feature vector with coefficients of Zernike moments is obtained. With respect to certain threshold values, they determined matching blocks. Their method used the SIFT algorithm, which has only one disadvantage of not able to detect flat copy-move forgeries. They overcame this disadvantage by using Zernike moments.

3.1.2 Dimensionality reduction-based (PCA, SVD, KPCA, and PCA-EVD)

Popescu and Farid [30] were able to efficiently detect copy-move forgery by applying PCA (Principal Component Analysis). Their method is similar to DCT approach and better in capturing discriminating features. The given image is converted from color to grayscale. They divided the image into several small sized blocks, which are represented into vectors. Then they arranged it lexicographically before matching. This is much better than the brute-force method of finding matches. They used PCA method to represent the different blocks in an alternative way. PCA is capable of detecting even minor variations due to noise or lossy compression. Their method is only for grayscale images. However, the method can be made to work for color images as well by processing the image for each color channel, which yields three duplication maps. Then PCA is applied to each map separately to detect the forgeries. Their method has a good efficiency in detecting copy-move forgeries and also gives less number of false positives. However, the efficiency falls as the block size decreases and also if the quality of the image is low.

Ting and Rang-ding [31] proposed a copy-move forgery detection method using Singular Value Decomposition (SVD). Their developed algorithm is computationally less complex and is robust to post-processing techniques. They used the correlation between the copied and pasted regions and searched for identical regions. In the first step, they divided the image into several small overlapping blocks. Then, they applied SVD to every block and extracted unique singular values feature vector for each block. Using these vectors, they found the matching blocks by transforming each block features into k-d tree. They used a threshold value to increase the robustness and eliminate pseudo-matching. A natural image will not have identical regions with coherent orientation. So, the obtained matched blocks are an evidence for copy-move forgery. They used lines to connect two identical blocks in a figure which clearly shows the tampered regions. They downloaded images from internet and used their algorithm to detect forgeries. They chose an empirical value of threshold. Their algorithm successfully detected copy-move forgeries even when post-processing is done on the

images. However, it fails to detect that out of two matched blocks which block is copied and which block is pasted. Their algorithm is not robust against JPEG compression.

A method proposed by Bashar, Noda, Ohnishi and Mori [32], uses Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) for copy-move forgery detection. They used these methods because of their robust block-matching feature. They divided the image into several small-sized blocks. They calculated KPCA-based vectors and DWT vectors for every block. Then they placed these vectors in a matrix and sorted it lexicographically. They used the sorted blocks to find the similar points and calculated their offset frequencies. To avoid false detections, they placed a threshold value for offset-frequency. They developed a new algorithm to detect flip and rotation type of forgeries using labeling technique and geometric transformation. This algorithm showed promising improvements compared to conventional PCA-approach. It also detects forgeries which have an additive noise and lossy JPEG conversation.

Zimba and Xingming [33] proposed a new method of copy-move forgery detection. Their method begins with conversion of color image into grayscale image. Then, they applied DWT to entire image. This gives sub-bands, out of which low frequency sub-band is enough to perform detection process. They divided the image into several overlapping blocks. They performed Principal Component Analysis – Eigen Value Decomposition (PCA-EVD) on the blocks. They placed these feature vectors are placed into the matrix and sorted the entries lexicographically. This method of sorting makes the matching less complex. They calculated the normalized shift vector and then offset frequency. This offset frequency is subjected to morphological processing to give final results. They made this method more efficient than conventional PCA method by reducing the image size in the beginning of the process. Their algorithm can detect duplications involving rotation of varying degrees. They included morphological operations to avoid false detections. The only disadvantage is that the duplicated region should be bigger than the block size, otherwise it cannot be detected. Also, their method fails to detect forgeries involving scaling, rotation and heavy compression.

3.1.3 Intensity-based (LUO, BRAVO, LIN, CIRCLE, and PCMIFD)

A study proposed by Luo, Huang and Qiu[34] describes the method of copy-move forgery detection based on intensities. They divided into several overlapping blocks. Then they divided the blocks into two equal parts and four directions. Then a block characteristic vector is computed for all the blocks using Additive White Gaussian Noise (AWGN) operation and they are lexicographically sorted. Every pair of similar block feature vectors need not represent a duplicated region of image. So, a method has to be developed to determine which pairs actually represent duplicated region. For this, they used shift vector method. They set a particular value of shift vector and two blocks are considered equal only when the shift vector of that pair exceeds it. The highest occurring shift vector is found and the pairs are discarded whose shift vectors are much different from this value. Then they employed some method to ensure whether forgery is actually done or not. Their algorithm has lower computational complexity and robust to post-processing operations. It holds well only when the forged regions are larger than the block size. However, the algorithm fails when the images are highly distorted and have large smooth regions.

Bravo-Solorio and Nandi [35] conducted a study on copy-move detection technique to find forgeries involving reflection, rotation and scaling. They tiled the image as block of pixels by sliding pixel by pixel with a window of particular size in a raster-scan order. They calculated feature vectors which are color-dependent. By this, they reduced the number of searches thereby increasing the efficiency. They calculated four features out of which three features are independently computed as red, green and blue components. The fourth feature is calculated as the entropy of luminance channel. They used this fourth feature to discard blocks with insufficient textural information. These features are listed lexicographically and then matching is performed. Their method produces lot of matches; hence they used refinement to reduce them. They used one-dimensional (1-D) descriptors to reduce memory usage. These 1-D descriptors are invariant to rotation and reflection. This method is efficient than many other methods in terms of computation and detecting tampered regions with post-processing.

Lin et al. [23] studied about copy-move forgery detection and proposed a new technique. They divided into several blocks of equal size which are further divided into four blocks. They calculated the average intensity of a single block by using the intensity of the four sub-blocks. Then relative intensity is calculated by finding the difference between individual intensities and the average intensity. They did this for all the blocks and obtained feature vectors. These feature vectors are integers; hence they used radix sort method instead of lexicographical sorting. They recorded the top-left corner point of each block and used it to calculate a shift vector by finding the difference between adjacent feature vectors. This shift vector is accumulative in nature for the regions which are tampered

and the forgery detection is based on this value. Their method is efficient and capable of detecting even JPEG compression and Gaussian noise. However, their algorithm fails when the tampered region is rotated at some arbitrary angles.

Wang, Liu, Li, Dai and Wang [36] reduced the dimensions of the image by Guassian pyramid method. For the circle block, they calculated four features which are lexicographically sorted. By using a certain threshold value they find the matching feature vectors. They successfully detected copy-move forgeries in the image by this method. By adjusting threshold value, they could control the number of matching feature vectors are obtained. They also tried their method on the tampered images with post-processing like blurring, lossy JPEG compression, rotation. They also improved the efficiency of detecting method to narrow down the number of block-matching search space.

A study by Sridevi, Mala and Sandeep [37], proposes a copy-move forgery detection technique in a parallel environment. They proposed this method mainly to accomplish copy-move forgery detection in real-time. Other methods like PCA, DWT or SVD have high computation time; hence cannot be used in real-time applications. Their method begins with dividing the grayscale image into several overlapping blocks of a specified size. Then intensity features for every block are extracted. The last two locations of the feature vectors store the block position. All this process of extracting the intensity features is taken care by one algorithm. They developed one more algorithm for parallel sorting. This performs the lexicographical sorting using radix sort method in a parallel way. This kind of sorting ensures easy detection of similar blocks by finding the identical features. They found the duplicated regions by matching of features and these blocks are mapped on to the image using the location stored in the vector. There will be a main algorithm which controls all these steps. Their method has shown performance improvement over many other conventional techniques. This is accomplished by reducing the processing time. They controlled the false detection rate by adjusting the block size. However, their method cannot be applied for a color image.

3.1.4 Frequency-based (DCT, DWT, FMT, PHT, DyWT, QCD, LBP, and Curvelet)

Fridrich, Soukal and Lukáš [38] used Discrete Cosine Transform (DCT) coefficients for copy-move forgery detection. They started with dividing the image into several blocks by using a window of particular size and moving it by one pixel along the image. They recorded the pixel values for each block and entered them into an array. They sorted the array lexicographically to find the similar entries in the rows of the matrix. Then, this sorted matrix is used to find the forged regions. This method is exact match method. In robust match method, they represent the blocks using quantized DCT coefficients. There is a Q-factor which decides the quantization steps involved in calculating DCT coefficients. They chose a suitable value of Q-factor and the array is again lexicographically sorted before matching is done. The algorithm developed by them takes care of the false positives by matching even mutual pairs. However, the algorithm cannot discriminate between large identical textures of a natural image.

A study by Zhang, Feng and Su [39], describes an efficient and robust algorithm for copy-move forgery detection based on DWT and pixel-matching. Their algorithm can detect duplicated regions in a grey-scale image. First, they calculated DWT for the whole image to obtain a sub-band. Then, they calculated the spatial offset between the copied region and pasted region. Then the image is shifted with this offset value and is overlaid with the given image. The copied region of the given image and the pasted region of the shifted image share the same spatial region. Hence, the pixels will be identical if at all a copy-move forgery is performed on the image. Their method is efficient and robust for various copy-move forgery techniques. But their method relies very much on the location of the forged region. It cannot be applied to images which has copy-move region at the center of the image. During such cases, the image has to be divided into sub-images and the algorithm must be applied recursively.
Bayram, Sencar and Memon [40] conducted a study to detect copy-move forgery by using Fourier-Mellin Transform (FMT). They chose FMT because it is robust to lossy JPEG compression, blurring, noise, scaling and translation effects applied as post-processing. They divided the image into several small sized blocks and they calculated the fourier transform of each block. By this, they ensured that transform is translation invariant. Then, they re-sampled, projected and quantized to get feature vectors. These feature vectors are made rotation invariant to small rotation angles. Then they are matched to find similar feature vectors by using either Lexicographic sorting or counting bloom filters. Even a natural image can have several similar blocks. Hence, they authenticated forging only when there are a certain number of connected blocks within same distance. This reduces false positives which makes the technique more efficient. Their method could detect forgeries involving blocks with rotations of up to 10 degrees and a scaling of 10%. Their algorithm is robust to JPEG compression as well.

A recent study by Li, Li and Wang [41], describes a block-matching method of copy-move forgery detection by using PHT (Polar Harmonic Transform). They used this new kind of orthogonal moment to generate features of blocks and they accomplished matching using PHT features. They used this technique to find copy-move forgeries which involves block rotations and geometric transformations. Unlike many other schemes which use square blocks, these people divided the image into many circular blocks because PHT can be defined on a unit disc. Then, they used the below shown formula to extract block features using PHT. Then they built a lexicographically sorted matrix by using PHT feature vectors. The final part is the block matching which they accomplished it by simulations. They performed post-processing on the forged images and tried to detect forgeries which have rotated blocks. Their method was successful in ideally detecting orthogonally rotated forged blocks. But when the angle of rotation changed, their detection algorithm did not give ideal results but it could locate the forged parts. They also demonstrated the detection of forgeries with geometric transformations. Hence, the performance of PHT algorithm is good in detecting copy-move forgeries wherein the pasted region is rotated before being pasted. All other traditional detections are accomplished well. Their algorithm is superior to many other proposed methods in normal detections. However, it is not good in detecting forgeries involving scaling and local bending.

A study by Muhammad, Hussain, Khawaji and Bebis [14] explained about a robust method for detecting copy-move forgery using Dyadic Wavelet Transform (DyWT). Their method is based on extracton of low frequency component and a high frequency component; matching them by applying a similarity measure. DyWT is most commonly used in many detection methods. However, it is shift invariant. Hence, Mallat and Zhong introduced DyWT which is shift invariant. In this type of waveform, there is no down-sampling and no shrinking of wavelet coefficients as in DyWT. Given an image, authors decomposed them using a low-pass filter and a high-pass filter. Then, they used atrous algorithm to compute DyWT of that image. Four sub-bands are obtained at the output side and they are of same size as that of the original image. The authors first decomposed the given image to scale one by using DyWT. Two sub-bands, LL1 and HH1 are obtained. They divided these sub-bands into 16x16 pixel blocks with an overlapping of 8 pixels. For the method to work, a copy-move forgery has to be performed on a minimum size of 16x16. Then they performed matching on LL1 and HH1. LL1 should be same and HH1 should be highly dissimilar for forged regions. They used this property to find out copy-move forgery. To find the similarity they used Euclidean distance method. They found out the Euclidean distance for both LL1 and HH1 and sorted them in ascending order and descending order respectively. They compared the values with a preset threshold value. If the values fall short of the threshold value then they discarded those values. If they are found to be equal then they considered those values to be representing the forged region. Their method is superior to several other methods and gives better results. However, the image has to be converted into grayscale before processing.

A study by Ghorbani, Firouzmand and Faraahi [42] presented a new method for copy-move forgery detection. They performed Quantization Coefficients Decomposition on Discrete Cosine Transform and Discrete Wavelet Transform coefficients. They converted the given image into grayscale. Then, they applied DWT in the beginning to obtain four sub-bands. They used only the low frequency sub-band for forgery detection. Then, they divided image into several blocks of same size. The blocks are overlapping in nature. Then, they applied DCT to get DCT feature vectors and then QCD is performed on these DCT vectors. These feature vectors are arranged into matrix. To reduce computational complexity, they sorted the matrix lexicographically. For every pair of adjacent rows in the matrix, they calculated normalized shift vector. They counted the number of times a shift vector appears. A threshold value is set for the count value and the blocks are set to be forged only if the count value exceeds this threshold value. Their method is efficient in detecting forgeries, when compared to other methods. However, this method cannot detect forgeries when the tampered region undergoes post-processing like rotation, scaling and heavy compression. Also this method imposes certain restrictions on the forged areas.

Li et al. [43] proposed a new method for copy-move forgery detection. They used a grayscale operator call Local Binary Pattern (LBP) to describe the image texture. They transformed the given image into grayscale. However, there will be noise contamination, lossy JPEG compression and many other post-processing methods performed on the forged image. For such images, high frequency components will not be stable. Hence, they used a Gaussian low pass filter and also found out that filtering more than twice would increase the detection performances. Then, they divided the image into several overlapping circular blocks. They extracted the feature vectors of the block using LBP which is rotation invariant. They arranged these feature vectors into a matrix to find similar blocks. To reduce the computation they sorted the matrix lexicographically. Then they used Euclidean distances to find out matching blocks. Euclidean distance is estimated for every feature vector and is compared with

a threshold value. The obtained matched blocks are marked on the image to indicate the forged regions. They detected some false regions. To account for that, they used filtering to reduce the false positives. Then they performed morphological processing and morphological erosion to remove the false positives completely. Their method is invariant to rotation and flipping. However, their method cannot detect forgeries involving rotation at different angles.

Qiao, Sung, Liu and Ribeiro [44] presented a new approach for copy-move forgery detection. Their method is based on multi-resolution and multi-orientation curvelet transform. Curvelet transform is usually performed in frequency domain to have a better efficiency. They converted the image into grayscale. In curvelet transform, the grayscale image is decomposed into a set of sub-bands. Then they partitioned each sub-band into several block and performed ridgelet analysis on them. Ridgelet transform combines Radon transform and the 1-D wavelet transform. However, it is computationally complex. To reduce the complexity they used fast discrete curvelet transform. This gives a pyramid structure with multiple orientations at various scales, which increases the detection performance and accuracy. Multi-directional decomposition gives precise relation between adjacent orientations. They used these pyramid structured multi-oriented feature vectors to perform matching. To reduce the computational complexity, they sorted the feature vectors lexicographically. Their method efficiently detected duplicated regions even after JPEG compression, scaling and rotations. However, it cannot be applied on compressed images. They have to be decompressed before this method can be used. Also, the images have to be in grayscale to perform this analysis.

3.2 Keypoint-based methods

A study byHuang, Guo and Zhang [45], describes a method of detecting copy-move forgery by taking the advantage of correlation between the original image region and the pasted region. They introduced SIFT (Scale Invariant Feature Transform) algorithm for precise detection and to make the technique robust against post image processing. They first calculated the SIFT keypoints. They matched these with one another to find forgeries. If any identical SIFT points are found, then the image has copy-move forgeries. Matching process was done for each keypoint by identifying its nearest neighbor. They set a threshold value, which is the ratio of closest to second-closest neighbors. This increases the robustness of the method. They faced difficulties in implementing for high scale images. Hence, they used BBF (Best-Bin-First) search method, which is derived from k-d algorithm, for matching. This method identifies the most similar vectors with maximum probability and minimum computation. They took one tampered image and repeated the detection method for different threshold values. They found out that the accuracy of detection is dependent on it. An optimum threshold value has to be chosen. They tested the robustness of the method by successfully detecting forgeries in a tampered image with post-processing. Their method is successful in using SIFT algorithm to detect the copy-move forgery and is robust post-processing done on the images. However, their method is not efficient when the tampered region is small and SNR value is low.

Bo, Junwen, Guangjie and Yuewei [46], conducted a study on copy-move forgery detection by using SURF (Speeded up Robust Features) algorithm, which is developed by Herbert Bay et al. It involves keypoint detection and description. They used Hessian matrix for detecting the keypoints and Haar wavelets for assigning the orientation. They estimated dominant orientation and described the orientation of the interest point descriptor. By extracting square regions around these interest points, they constructed SURF descriptors which are aligned to the dominant orientation. By weighting the responses with Haar wavelets, they increased the robustness to localization errors and geometric deformations. They chose Haar wavelets because they are invariant to the illumination bias. The SURF descriptors are then used for matching. They used a threshold to increase the robustness and avoid false detections. They chose an empirical value of threshold and tested their algorithm on different images and they were successful. Further, they performed post processing like scaling, rotation and blurring on the forged images. They used the algorithm to test and were successful in showing its robustness for post processing. Their method is successful in locating the tampered regions even when post processing is done on the images. It is robust and speed in detecting. However, they couldn't find the exact boundaries of the tampered region.

A study by Zheng, Haoa and Zhub [47] reveals a new method for keypoints matching based on the position relationship of the keypoints. Keypoints in tampered region and original region should be consistent and they should be distributed evenly over the entire image. This ensures that large similar textures, like sky, also produce considerable number of keypoints. Their algorithm is built to scan and discard the keypoints for the first time. This ensures that noise has no impact on them. They scanned the keypoints again and found the features for all keypoints. They developed new algorithm to find the features and stored these features into a matrix. Their algorithm differs from SIFT in the way of determining

features. By noticing the consistent keypoints in the matrix, their algorithm detected copy-move forgery in the image. Their algorithm finds a pair of consistent keypoints and marks them as candidate keypoints only when they satisfy certain condiditons. They also set a threshold value to reduce the number of false detections. They noted that the computational time is very less and also there are very less number of false detections on a large similar texture like sky. Their algorithm is advantageous in this kind of detections but cannot detect tampering involving post-processing like rotation and scaling.

4. Conclusions

With the rapid progress of image processing technology, detection of digital image forgery is an interesting research topic in forensics science. In this paper, a specific type of forgery which is Copy-move forgery investigated and an efficient detection method proposed based on Fourier transform. In this paper, we have considered the problem of copy-move image forgery detection. Our emphasis was on detecting and extracting duplicated regions with higher accuracy and robustness.

References

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

[2] Shivakumar, B., & Baboo, S. S. (2011). Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors. International Journal of Computer Applications, 27(3).

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

[4] Pujari, V. S., & Sohani, M. (2012b). A Comparative Analysis On Copy Move Forgery Detection Using Frequency Domain Techniques. International Journal of Global Technology Initiatives, 1(1), E104-E111.

[5] Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013). Region duplication detection based on Harris corner points and step sector statistics. Journal of Visual Communication and Image Representation, 24(3), 244-254.

[6] [6] Liu, M.-H., & Xu, W.-H. (2011). Detection of copy-move forgery image based on fractal and statistics. Journal of Computer Applications, 8, 061.

[7] Yadav, P., Rathore, Y., & Yadu, A. (2012). DWT Based Copy-Move Image Forgery Detection. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 1(5), 56-58.

[8] Pujari, V. S., & Sohani, M. (2012a). A Comparative Analysis on Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non Lexicographic techniques. IJECCE, 3(1), 136-139.

[9] [9] Shivakumar, B., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology, 10(7).

[10] Chen, L., Lu, W., & Ni, J. (2012). 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), 4(1), 49-62.

[11] Liu, G., Wang, J., Lian, S., & Wang, Z. (2011). A passive image authentication scheme for detecting region-duplication forgery with rotation. Journal of Network and Computer Applications, 34(5), 1557-1565.

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

[13] A merini, I., Barni, M., Caldelli, R., & Costanzo, A. (2013). Counter-forensics of SIFT-based copy-move detection by means of keypoint classification. EURASIP Journal on Image and Video Processing, 2013(1), 18.

[14] Muhammad, G., Hussain, M., Khawaji, K., & Bebis, G. (2011a). Blind copy move image forgery detection using dyadic undecimated wavelet transform. Paper presented at the Digital Signal Processing (DSP.

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

[16] Wang, J.-W., Liu, G.-J., Zhang, Z., Dai, Y., & Wang, Z. (2009). Fast and robust forensics for image region-duplication forgery. Acta Automatica Sinica, 35(12), 1488-1495.

[17] Mahdian, B., & Saic, S. (2010). A bibliography on blind methods for identifying image forgery. Signal Processing: Image Communication, 25(6), 389-399.

[18] Math, S., & Tripathi, R. (2010). Digital Forgeries: Problems and Challenges. International Journal of Computer Applications, 5(12).

[19] Hwang, M. G., & Har, D. H. (2013). A Novel Forged Image Detection Method Using the Characteristics of Interpolation. Journal of Forensic Sciences, 58(1), 151-162.

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

[21] Jian-feng, Z. G.-j. Z. (2011). The Application of Electronic Signature Technology in Online Bidding System. Journal of Changzhou Vocational College of Information Technology, 4, 007.

[22] Chang, I.-C., & Hsieh, C.-J. (2011). Image Forgery Using An Enhanced Bayesian Matting Algorithm. Intelligent Automation & Soft Computing, 17(2), 269-281.

[23] Lin, H.-J., Wang, C.-W., & Kao, Y.-T. (2009). Fast copy-move forgery detection. WSEAS Transactions on Signal Processing, 5(5), 188-197.

[24] Peng, F., Nie, Y.-y., & Long, M. (2011). A complete passive blind image copy-move forensics scheme based on compound statistics features. Forensic Science International, 212(1), e21-e25.

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

[26] Ghosh, P., Gelasca, E. D., Ramakrishnan, K., & Manjunath, B. (2007). Duplicate image detection in large scale databases. Advances in Intelligent Information Processing: Tools and Applications, Eds. B. Chandra and CA Murthy, 149-166.

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

[28] Mahdian, B., & Saic, S. (2007). Detection of copy–move forgery using a method based on blur moment invariants. Forensic Science International, 171(2), 180-189.

[29] Mohamadian, Z., & Pouyan, A. A. (2013). Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions. Paper presented at the UKSim.

[30] Popescu, A. C., & Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515.

[31] Ting, Z., & Rang-ding, W. (2009). Copy-move forgery detection based on SVD in digital image. Paper presented at the Image and Signal Processing, 2009. CISP'09. 2nd International Congress on.

[32] Bashar, M., Noda, K., Ohnishi, N., & Mori, K. (2010). Exploring duplicated regions in natural images. IEEE Transactions on Image Processing,(99), 1.

[33] Zimba, M., & Xingming, S. (2011). DWT-PCA(EVD) Based Copy-move Image Forgery Detection. International Journal of Digital Content Technology and its Applications, 5(1).

[34] Luo, W., Huang, J., & Qiu, G. (2006). Robust detection of region-duplication forgery in digital image. Paper presented at the Pattern Recognition, 2006. ICPR 2006. 18th International Conference on.

[35] Bravo-Solorio, S., & Nandi, A. K. (2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing, 91(8), 1759-1770.

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

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

[38] Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. Paper presented at the in Proceedings of Digital Forensic Research Workshop.

[39] Zhang, J., Feng, Z., & Su, Y. (2008). A new approach for detecting copy-move forgery in digital images. Paper presented at the Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on.

[40] Bayram, S., Sencar, H. T., & Memon, N. (2009). An efficient and robust method for detecting copy-move forgery. Paper presented at the Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on.

[41] Li, L., Li, S., & Wang, J. (2012). Copy-move forgery detection based on PHT. Paper presented at the Information and Communication Technologies (WICT), 2012 World Congress on.

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

[43] Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J. F., & Pan, J.-S. (2013). An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns. Journal of Information Hiding and Multimedia Signal Processing, 4(1), 46-56.

[44] Qiao, M., Sung, A., Liu, Q., & Ribeiro, B. (2011). A novel approach for detection of copy-move forgery. Paper presented at the ADVCOMP 2011, The Fifth International Conference on Advanced Engineering Computing and Applications in Sciences.

[45] Huang, H., Guo, W., & Zhang, Y. (2008). Detection of copy-move forgery in digital images using SIFT algorithm. Paper presented at the Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on.

[46] Bo, X., Junwen, W., Guangjie, L., & Yuewei, D. (2010). Image copy-move forgery detection based on SURF. Paper presented at the Multimedia Information Networking and Security (MINES), 2010 International Conference on.

[47] Zheng, J., Haoa, W., & Zhub, W. (2012). Detection of Copy-move Forgery Based on Keypoints' Positional Relationship*. Journal of Information and Computational Science, 1(3), 53-60 .

First Author Salam Abdulnabi Thajeel ,he received his B.Cs. Degree in computer science 2000 University of Al-Mustansiriyah,Baghdad, Iraq. M.Sc. Degree in Computer Science Iraqi Commission for Computers & Informatics 2003 ,Bagdad, Iraq, Currently he is a Ph.D. student in University Technology Malaysia.

Second Author Ghazali Bin Sulong , was born in May 21, 1958 Malaysia. He received his pH. D. Computing 1989 University of Wales College of Cardiff (UWCC), Wales, U.K., M.Sc.Computing 1982 University of Wales College Cardiff (UCC), Wales, U.K., B.Sc. Statistic 1979 UKM, Malaysia. Currently he is a Professor in Image Processing in University Technology Malaysia.