Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **2**, March **2015**

A Novel Approach for Detection of Copy Move Forgery using Completed Robust Local Binary Pattern

Salam Abdul-Nabi Thajeel[1,2] and Ghazali Sulong[1]

[1]UTM-IRDA Digital Media Centre (MaGIC-X)
Faculty of Computing
Universiti Teknologi Malaysia,
81310 UTM Skudai, Johor, Malaysia
sath72@gmail.com;ghazali@utmspace.edu.my

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

Received July, 2014; revised November, 2014

Abstract. *Copy-move forgery is one of the most popular tampering artifacts in digital images. Where a part of image content is copied and then pasted to another part of the same image. Despite several established methods for detecting copy-move forgery, perceiving forged areas in the presence of noise, blur and rotated region before pasting are complicated. To solve this problem, we present a Novel approach for detection of copy move forgery using Completed Robust Local Binary Pattern (CRLBP).The proposed method consists of five main steps, where the suspicious image is filtered using a hybrid filter before being divided into overlapping blocks. The CRLBP operator is then applied to produce an invariant rotation descriptor to extract feature for each block and then sorted the feature vectors using lexicographical sorting. The forged regions are identified by comparing the feature vector using Euclidean distances. Finally, we introduced a new technique to reduce false matches which caused by flat region. Experimental results show that the proposed approach is able to detect forged areas efficiently even in the presence of image distortion such as rotation, additive noise, blurring and compression. And can also solve the false match problem. Results with precision and a false positive rate give better performance as compared to other techniques.*

Keywords: Copy move forgery detection, Duplicated region detection, Feature extraction, Digital image forensic, CRLBP

1. **Introduction.** In todays digital epoch, images and videos are exploited as the primary vehicle for transferring information. The visual media possess high capacity for easy articulation, dissemination and storage. All these enabled them as significant routes for information transfer, especially with the advent of information technology and communication devices. Presently, images and videos are considered as one of the vital sources to be used as basic evidence to influence judgment, for instance, in a court of law. In fact, they are often used to certify the truthfulness of the reported news. Nevertheless, the confidence level in the picture may change from time to time due to the possibility of picture manipulation and image forgeries [1]. The number of maliciously tampered images is exponentially escalating since the inception of broad range of powerful computer application softwares. In short, the creation of digital image forgeries became straightforward.

Undoubtedly, the image field is highly benefited from the current development in digital data and information technology. The validity and reliability of digital data faces many issues related to time-by-time expansion in digital imaging [2]. Photoshop, GIMP etc. are some easily available popular digital image processing tools which can be employed for copy-move attack. These tools provide many features and flexibilities for manipulation despite several uncertainties on the integrity and authenticity of digital images [3]. Because of these issues, numerous examples are evidenced in media with tampering images. The digital image forgeries are separated into three categories such as copy-move, image splicing and image retouching. Amongst all these the copy-move or cloning is one of the most basic image manipulation methods. This manipulation necessitates a forger to cover a part of an image and the success depends on the availability of a homogeneous texture (e.g., grass, sand or water). Although different regions of a homogeneous texture appear qualitatively similar but is highly unlikely that they are numerically identical. In the other basic image manipulation of splicing called photomontage, a forger combines regions from different images into a single image. Conversely, the image retouching being a less corrupting type of image forgery does not change the whole image but slightly alters its quality [4]. However, the authenticity of images and videos remain un-trustful in all these relatively easier tampering methods. Determining the authenticity of a digital image is the key issue of image forensics because an image entails the legitimacy of any event that has happened. Truly, proving the clue on whether images are authentic, fake, modified or computer generated remain formidable task.

Robust technological instruments are needed to perform forensic analysis for possible detection of forgeries. The present state-of-the-art for forgery detection methods are largely categorized into active and passive forensics. Watermarking being an active technique solves the image authenticity problem but suffers from many shortcomings. The idea of digital watermarking is to embed information into an image that can be extracted later to verify the authenticity [5]. Generally the active methods that require human intervention (equipped cameras) are inaccurate. These limitations are overcome using several passive authentication methods which do not involve any previous information about the image. In fact, they take advantage of specific detectable changes that forgeries can bring into the image. In contrast, the passive-blind approaches are considered as new means in digital multimedia security because they can operate in the absence of any special operational device. We propose a novel method to detect copy move forgery using CRLBP, this method based on the passive type forensics [4]. Using this method, the features are extracted for detecting copy-move image forgery. The algorithm for the detection composed of five foremost steps .such as preprocessing feature extraction, feature vector sorting, block matching and removal of false matches.

The image in pre-processing comprised the Red, Green and Blue (RGB) ,so it convert to gray scale and then also used hybrid filter to denoising and lastly image division to overlapping blocks. False matches are reduced using method that combines many techniques. Images from standard database CoMoFoD are employed to test efficiency and accuracy of the proposed method. The results are presented, interpreted and compared with other findings. The paper is organized as follows. A short review on copy-move image forgery detection methods is rendered in section 2 and the striking features of CRLBP approach is highlighted in section 3. Section 4 describes our proposed approach and the experimental results are presented in section 5. Section 6 concludes the paper with future worth looking work.

2. **Related Work.** As mentioned before, one of the most prevalent types of image manipulation or tampering method is copy move (cloning). In this type one or more regions

of image are copied and then pasted in another region of the same image. The intent of this type is to duplicate the object or to remove the object in the image. Therefore, all the methods that are used in the copy move forgery detection (CMFD) make an attempt to identify those objects which were cloned and pasted previously. Detection of the duplicated parts is not so easy especially if the attackers try to implement the post-processing operations on copied part before being pasted into another part. Typically, forgers use some techniques such as filtering, rotation, JPEG compression, resizing and add noise to the image. Because of these operations, it is hard to detect copy-move forgery. Ideally, CMFD method is capable of detecting duplicated parts albeit of differences. In other words, a smart forgery detector must be robust enough to identify any form of manipulations.

To accomplish this task, several detecting techniques are developed. They are classified as block-based and key-point-based methods [6]. In the former method the image is firstly divided into small overlapping or non-overlapping blocks to extract the feature from each block. Finally, the blocks are compared against each other to examine their matches. Conversely, the later method searches key-points in the image without dividing it and extract feature around each key point to identify the duplicated blocks [7]. Here we provide the concise overview of previous techniques proposed to solve CMFD. Fridrich [8] introduced a method where the image was divided into overlapping block of the same size and the discrete cosine transform (DCT) was used to extract the coefficient for each block. The detected duplicated regions were dependent on the find matching of the quantization coefficient which was lexicographically sorted. Popescu [9] proposed a similar method by replacing DCT and used principal component analysis (PCA). One of the characteristics of PCA was utilized to make the numbers of features half compared to that of Fridrich. This method is very effective but has weakness such as incapability of detecting the copy regions that were rotated prior to pasting. However, Fridrichs method can detect a copy-move tampering with number of rotation up to five. Mahdian & Saic [10]used the blur moment invariant to detect copy-move region for exposed image containing blurred or added noise .This method fail to detect forged area after rotated or flipped.

In [11] Wang, et al have used Hu moments to copy-move forgery detection. where an efficient algorithm was developed which was robust to different post-processing techniques including as blurring and noisy JPEG compression. Meanwhile, Gaussian pyramid was used to reduce the image dimensions while the image is divided into several fixed sized overlapping blocks. This method is faster compared with [10] but also have the same weakness with the rotated or flipped.

To overcome the effect of rotation on copy-move detection, Ryu et al. [12] established a copy-rotate-move forgery-detection algorithm using Zernike moments. In addition to rotation, the algorithm also invariant to different types of operations such as insensitive to simple noise, blurring and rotation. Nonetheless, the method failed to detect forgery in the image containing flat region and is inaccurate for images enclosing noise. Leida Li [13] used local binary pattern to detect copy-move forgery, where the image was divided into overlapping circular blocks and filtered using low pass filtering before Local Binary Pattern (LBP) was applied to extract features. It produced good results for images exposed with simple additive noise, JPEG compression and robust to region rotation and flipping. Nevertheless, this method is incapable of detecting images exposed to random region rotations. Huang et al. [14] developed a method using SIFT (Scale Invariant Feature Transform) for copy-move forgery detection. It was robust to scale and rotation attacks but sensitive to simple noise and blurring .also it performance poorly on image with small tampered region.

In this view, we propose a new approach to detect copy-move forgery based on CRLBP. This method has some advantages because it not only deals with traditional image processing operations but also involves geometric (rotation) and photometric (noise, blur) transformations. Several techniques are combined to reduce the false positive that occurs due to flat regions.

3. **Completed robust local binary pattern (CRLBP).** Traditional descriptor using LBP has two obvious disadvantages such as noise sensitiveness and tendency to describe dissimilar structural patterns with similar binary code which decreases its ability of discrimination. Various improved versions of LBP including completed local binary pattern (CLBP) and Local Ternary Pattern (LTP) are developed. However, all proposed improved versions of LBP are sensitive to noise.

Therefore we used a new version of LBP named CRLBP that introduced by Zhao et al [15] to extract features in proposed copy move forgery detection.

Zhao et al [15] introduce CRLBP method by combining combined two LBP versions such as CLBP and Robust Local Binary Pattern (RLBP) which carries all the essential characteristics. The new approach is indeed robust to noise and can attain remarkable features categorization accuracy. For the central value in the local area 3*3 pixels is substituted by average local gray level. The average local gray level is comparatively more robust to noise and illumination variation than center gray value. Weighted Local Gray Level (WLG) which is used to obtain the traditional gray value of the center pixel makes CRLBP more stable and strong. The demerits of CLBP and RLBP are highlighted hereinafter.

3.1. **CLBP.** The main disadvantage of LBP is the creation of analogous binary code for several dissimilar structural patterns. Guo et al. [16] introduced an improved version of LBP called CLBP to modify the discriminative capability of the local structure. Fig.1 illustrates the detail framework of CLBP displaying the center gray level, local difference sign magnitude transform (LDSMT) symbolizing every local region in the input image and decomposition of LDSMT into two elements defined as magnitudes (m_p) and signs (s_p), respectively.

(CLBP_C), (CLBP_S) and (CLBP_M) signify three operators as proposed by Guo et al [16]. The center gray level is coded by the CLBP_C upon global thresholding , CLBP_S and CLBP_M are used to code the sign and magnitude components respectively. The signs and magnitude are defined as,

The signs and magnitude are defined as,

$$s_p = s(g_p - g_c), m_p|g_p - g_c| \tag{1}$$

Where g_p, g_c are the gray values for the neighbor and the central pixels.
The $CLBP\_S$ operators yield,

$$CLBP\_S_{P,R} = \sum_{p=0}^{p-1} s(g_p - g_c)2^p \tag{2}$$

where

$$\mathrm{s}(x) = \begin{cases} 1 & , x \geq t \\ 0 & , |x| < t \\ -1 & , x < -1 \end{cases}$$

Where t is the user predefined threshold and R is the radius of the circle. The gray values for both the central and neighbor pixels represented by g_c and g_p (where p=0,...,p-1) with p the total neighbors number. The CLBP_M is expressed as,

$$CLBP\_M_{P,R} = \sum_{p=0}^{p-1} s(m_p - c)2^p, \tag{3}$$

where

$$\mathrm{s}(x) = \begin{cases} 1 & , x \geq 0 \\ 0 & , x < 0 \end{cases}$$

Where c is the threshold which is assigned as the mean value of m_p for complete image.

According to Guo et al. [17], the center pixel also carries distinctive details. Therefore, to get the local central information an operator called CLBP-Center (CLBP_C) is introduced as follows,

$$CLBP\_C_{P,R} = s(g_c - C_I) \tag{4}$$

Where the threshold $C_I$is a set of average grey level of entire image.

The CLBP feature map of the original image is obtained by combining the CLBP_C, CLBP_S and CLBP_M codes and a CLBP histogram is built by mixing them. Significant enhancement is made for differentiating the confusing the designs. Furthermore, the CLBP method resolves some confusion of different patterns in spite of its sensitiveness to noise while the value of a pixel is still used as a threshold directly.

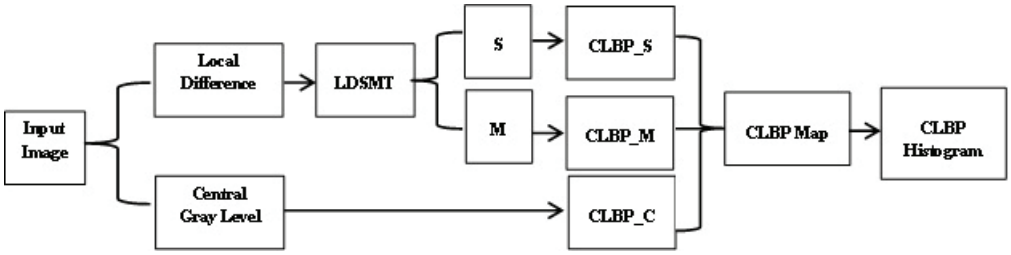

FIGURE 1. Framework of CLBP

3.2. **RLBP.** Chen et al. [15] defined the Average Local Gray Level (ALG) to determine the threshold. This must be invariant to monotonic gray scale transformation and robust to noise. The ALG can be written as,

$$ALG = \frac{\sum_{i=1}^{8}(g_i + g)}{9} \tag{5}$$

Where g is the gray value for the pixel that is located in the center with g_i (i=0,1,...,8) represent the gray value for neighboring pixel. ALG signifying the average gray level of local texture is clearly more robust to noise than the gray value of the center pixel.

The LBP process performed by using ALG as the threshold (alternative of the gray value) is termed as RLBP and given by,

$$RLBP_{P,R} = \sum_{p=0}^{p-1} s(g\_p - ALG\_c)2^p = \sum_{p=0}^{p-1} s\left(g\_p - \frac{\sum_{i=1}^{8} g_c i + g_c}{9}\right)2^p \tag{6}$$

Where g_{ci} (i=0,1,....,8) is the gray value of adjacent pixel of g_c.

Now, RLBP being insensitive to noise, two unlike patterns with comparable LBP code may have different RLBP code due to consideration of neighboring pixels. Thus, RLBP is able to overcome the aforementioned disadvantages possessed by original LBP. However, ALG neglects the particular value of individual pixel. Occasionally, information of central pixel is required. Consequently, the following WLG is defined to keep the balance between information of individual pixel and de-noise,

$$WLG = \frac{\sum_{i=1}^{8}(g_i + \alpha)}{8 + \alpha} \tag{7}$$

Where α is a user determined parameter. WLG is found to be equal to the conventional ALG if $\alpha = 1$. RLBP can be determined from the relation,

$$RLBP_{P,R} = \sum_{p=0}^{p-1} s(g\_p - WLG\_c)2^p = \sum_{p=0}^{p-1} s\left(g\_p - \frac{\sum_{i=1}^{8} g_c i + \alpha g}{8 + \alpha}\right)2^p \tag{8}$$

According to Zhao et [15], RLBP achieves better results for $\alpha = 8$, 9 or 10. Moreover, RLBP exhibits higher sensitivity to noise for $\alpha > 8$. Therefore, α is set as either 1 or 8. RLBP is comparatively more insensitive to noise for $\alpha = 1$ than $\alpha = 8$. In fact, our choice of $\alpha = 8$ in RLBP is found to reveal more stable performance under complex illumination and viewpoint variant conditions, because it extracts gray level information from both individual pixel and local neighboring set.

3.3. **CRLBP.** It is worth-noting that RLBP inherits CLBP effective framework in order to distinguish the confusing patterns of LBP. The magnitude m_p is defined as,

$$m_p = |WLG_p - WLG_c| = \left| \frac{\sum_{i=1}^{8} g_p i + \alpha g_p}{8 + \alpha} - \frac{\sum_{i=1}^{8} g_p i + \alpha g_c}{8 + \alpha} \right| \tag{9}$$

The operator RLBP-Magnitude (RLBP_M) that determines the local difference of WLG is given by [17],

$$RLBP\_M_{P,R} = \sum_{p=0}^{p-1} s(m_p - c)2^p \tag{10}$$

Where the threshold c is chosen as the mean value of the entire image and the center pixel which represents the central gray level of image carry discriminative information. The operator RLBP-Center (RLBP_C) decisive for the local central information can be written as,

$$RLBP\_C_{P,R} = s(WLG_c - C_I) \tag{11}$$

Following [18], the CRLBP method used the same three operators of RLBP, RLBP_M and RLBP_C. These operators are integrated to form the feature map and the histogram of CRLBP. Finally the CRLBP histogram for each block is stored into a single vector of sub-histograms on the behalf of the image block.

4. **Our Proposed Method.** Fig.2 depicts the block diagram of the proposed method for copy-move forgery detection. Which consists of five key steps including preprocessing, feature extraction, feature vector sorting, block matching and false matches removal.

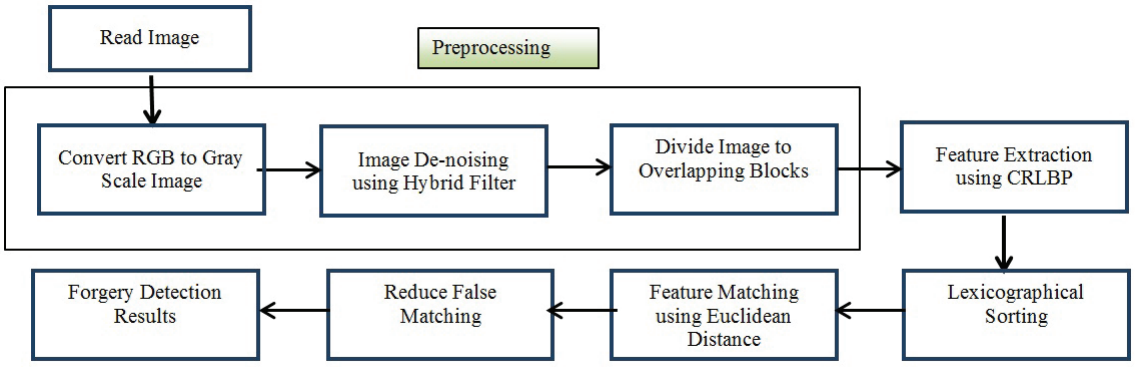

FIGURE 2. Flowchart of the proposed approach

4.1. **Preprocessing.** The main objective of preprocessing is to make the image ready for the feature extraction which includes three stages as follows:

In the first stage, the RGB model of a color image is transformed to grayscale using the relation,

$$Y = 0.299R + 0.587G + 0.114B \tag{12}$$

Where Y is luminance component. In order to minimize the influence of the photometric attacks such as: additive noise, compression and blurring on forgery detection. The hybrid filter is incorporated in proposed CMFD. The hybrid filter comprising of the adaptive mean filter and adaptive wiener filter can successfully remove the Gaussian noise, Rayleigh noise, impulse noise, blurring, salt, pepper noise,and also reduces the effect of JPEG compression simultaneously from the image and provides a clarity to picture while preserving its details. Results show that the use of this type of image denoising is effective in improving the forgery detection performance. A filter with size 5*5 is used. Finally; the image (gray scale image) is divided into overlapping blocks by moving the block over the entire image starting from its top-left to the bottom-right corner. The block size is chosen to be smaller than the minimum size of assumed tampering. For an image with size M*N pixels and overlapping blocks having pixels B*B, the total number of overlapping blocks (TB) yields,

$$TB = (M - B + 1)(N - B + 1) \tag{13}$$

4.2. **Feature extraction.** . In this phase, the features of each block are extracted using CRLBP and stored them in vectors (row feature vector), where the number of vectors is equal to the number of blocks. The image is divided into overlapping blocks of 9*9 pixel and each block is further divided into non-overlapping sub blocks (Cell) of 3*3 pixel . The CRLBP histograms corresponding to each cell is extracted. Then for each overlapping block, the histogram for all cells is combined into single histogram to represent the feature vector of each overlapping block. Finally, the histogram of each overlapping block is saved as the feature vector values. Fig.3 illustrates the feature vector extraction processes.

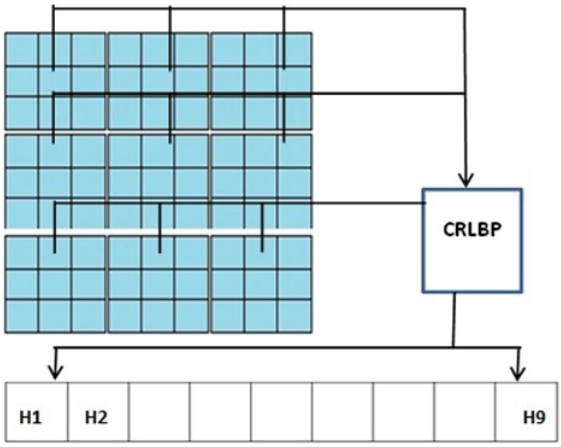

FIGURE 3. Feature vectors extraction from 99 blocks

4.3. **Sorting of feature vector.** Once the features of all blocks are extracted, the next step is to find duplicated blocks by matching the extracted feature vectors. The process is tedious and time consuming due to huge number of feature vectors. To overcome the problem we sort the vectors using lexicographical sort which results in identical or similar row feature vectors become adjacent to facilitate the block matching.

4.4. **Block matching.** In order to locate forged areas we search for duplicated blocks using Eq. 14 and Eq. 15. Where the former indicates the Euclidean distances of feature vectors of two blocks [19], while the latter measures the actual spatial distance between the two blocks.

$$M_{Match(FV_I,FV_{I+j})} = \sqrt{\sum_{k=1}^{p}(Fv_i - Fv_{I+j})^2} \;<\; T_{similar} \tag{14}$$

If Eq.14 is met then the blocks are considered as strong candidates for a duplicated block. Then, the actual block distance is measured using Eq.15 to validate it.

$$D(Blok_i, Blok_{i+J}) = \sqrt{(x_i - x_{i+j})^2 + (y_i - y_{i+j})^2} \;>\; T_{distance} \tag{15}$$

All the matched block pairs are stored in two separate lists called L1 and L2. The entries in these lists are the primary candidates of copy-move; however, some false positives (non-duplicated blocks are detected as duplicated blocks) are still found due to homogeneousness of the image content (flat regions). Thus, the following section deals with the problem.

4.5. **False matching reduction.** We eliminate the above mentioned false positives using a new approach which consists of three steps:

Firstly, for both of L1& L2 we take a pair of candidate block (BL1, BL2) Fig.4, then the eight-connected neighbors of blocks BL1 & BL2 are selected and checked whether the neighbors also found in the candidate list. If they are more than 4 neighbor blocks exist in L1&L2 then the boot blocks (BL1&BL2) remain in the candidate block list, otherwise remove from both lists.

Secondly, the blocks residing on the boundary of the image are excluded: There are many blocks in the border of the image that appear identical but they are false positives

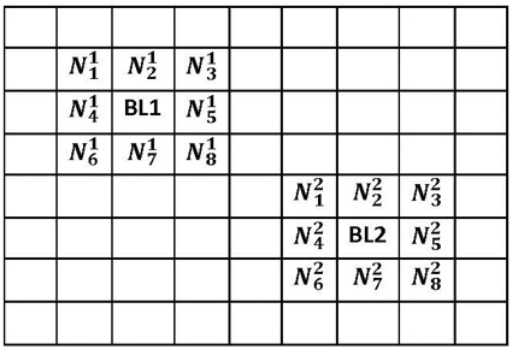

FIGURE 4. False positives removal using connected neighbor block

(non-duplicated blocks are detected as duplicated blocks). Therefore, elimination of these types of blocks is essential to enhance the detection accuracy. Fig.5 shows the exclusion processes.

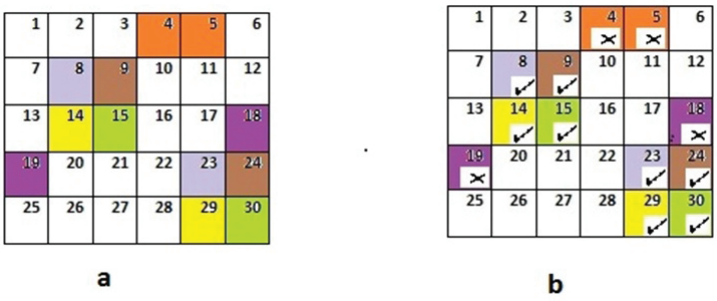

FIGURE 5. Exclusion procedures for the blocks residing on the borders (a) before exclusion (b) after exclusion

Lastly, the duplication maps are generated to visualize the result of forgery detection system. This operation is performed by creating a matrix of zero value (ZM) having a size equal to the test image. The duplicated region value is set to one (white color). A window size of 10*10 pixel is used to exclude the false matching and to move it from the upper left corner to the lower right corner. Each time, the window skips forward by 10 pixels ensuring all the pixels of the image are filtered and each pixel is filtered only once. All pixels of the window are marked as black when the sum of the border pixels in each 10*10 window equals zero and the number of white pixels less than the threshold (NT=25). Conversely, the number of the white pixels is kept constant without performing any filtering. The morphological opening operation is performed on the binary matrix to smoothen out the boundaries of the detected regions and to fill the tiny holes in the map. Fig.6 shows the duplicated maps of some copy-move forged images after the proposed post-processing is applied in removing false matching.

5. **Results and discussion.**

5.1. **Performance Measure.** The proposed method is tested on CoMoFoD database images consisting of five different types of tampered images (attacks):1.multiple copies of same region, 2.multiple copies of different region, 3.Photometric transformations, 4.

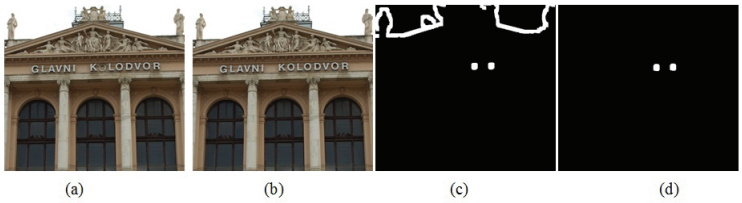

FIGURE 6. Removal of false matching (a) original image, (b) tampered image, (c) an initial result on detection (d) a final result after false positive removal

Rotation, 5.multiple attacks). The performance of the proposed system is measured according to F-measure given below:

$$F - measure = \frac{2 * Precsion * Recall}{Precsion + Recall} \tag{16}$$

$$Precision = \frac{TP}{TP + FP} \tag{17}$$

$$Recall = \frac{TP}{TP + FN} \tag{18}$$

Where F-measure $\in [0, 1]$: 1 denotes the best performance, while 0 indicates worst performance in term of both precision and recall.

where TP is called True Positive which represents the number of pixels that have been correctly detected as forgery, FP known as False Positive which implies the number of pixels with invalid detection (real areas are detected as forger area) and FN is termed as False Negative which is the number of pixels that have not been disclosed as a forged.

5.2. **Experiment.** In this section, we present results of Copy-move forgery detection in different Situation. The results are arranged according to five mentioned attacks.

5.2.1. *Multiple copies of same region.* Figures 7 illustrates an original image (Fig. 7.a) with forged images (Fig. 7.b) using our new approach for multiple copies of same region. Some parts of the original image are detected as copied and pasted multiple times. Fig. 7(c) identified the location of forged areas.

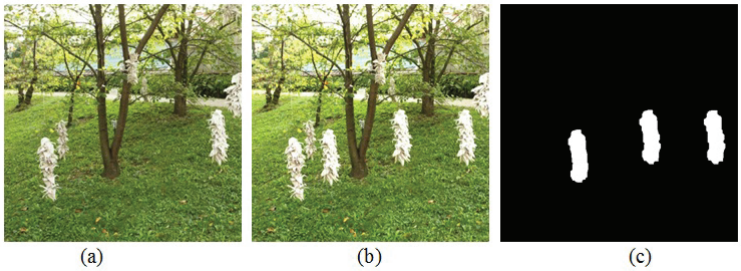

FIGURE 7. Detection of multiple copies of the same region (a) original image, (b)

5.2.2. *Multiple copies of same region.* Figure 8 displays the results of detected multiple copies of different regions. The original and the forged images are shown in Fig. 8 (a) and (b), respectively. Three different parts of the original image are modified. Fig. 8 (c) identified the location of forged areas.

FIGURE 8. Detection of multiple copies of different region (a) original image, (b) tampered image and (c) the detected forged areas

5.2.3. *Photometric transformations.* There are many different types of photometric transformations can be applied on tampered images to hide the tampering traces. The results of proposed CMFD method under the most common attacks such as JPEG compression, noise adding and image blurring are presented. These types of post-processing methods are applied on images of CoMoFoD database. Table 1 summarizes the information and parameters related to the attacks. Figure 9 depicts the detection results when the image is exposed to these attacks.

TABLE 1. Parameters for most common attacks

Attacks Method	Parameters
JPEG compression	factor = [20, 30, 40, 50, 60, 70, 80, 90, 100]
Noise adding	$\mu = 0, \sigma^2$2= [0.009, 0.005, 0.0005]
Image blurring	averaging filter = [3x3, 5x5, 7x7]

5.2.4. *Rotated copy-moved regions.* The primary focus for using CRLBP is to incorporate CRLBP rotation invariance. The proposed method is tested for rotated copy-moved regions and the detected forgery is shown in Fig. 10. In the simulation, the copied regions are rotated at different angles (5, 10, 15, 90, 180 and 270°) before pasting them onto another part of the image.

5.2.5. *Multiple attacks.* In the previous section the performance of the proposed method is examined for the forged region encountered with single attack deformation. However, in reality the tampered area is often affected by multiple attacks such as rotation and noise. Fig. 11 represents the detected forgery using our method for multiple attacks cases. In these experiments, the image that contain copy move forgery is exposed to different attacks such as (rotation, Gaussian noise, Gaussian blurring and JPEG compression) .The F- Measure of the proposed method and methods in [12, 13] are presented in Table 2 and Fig. 12. It can be concluded that the proposed method outperformed on the methods in [12, 13].

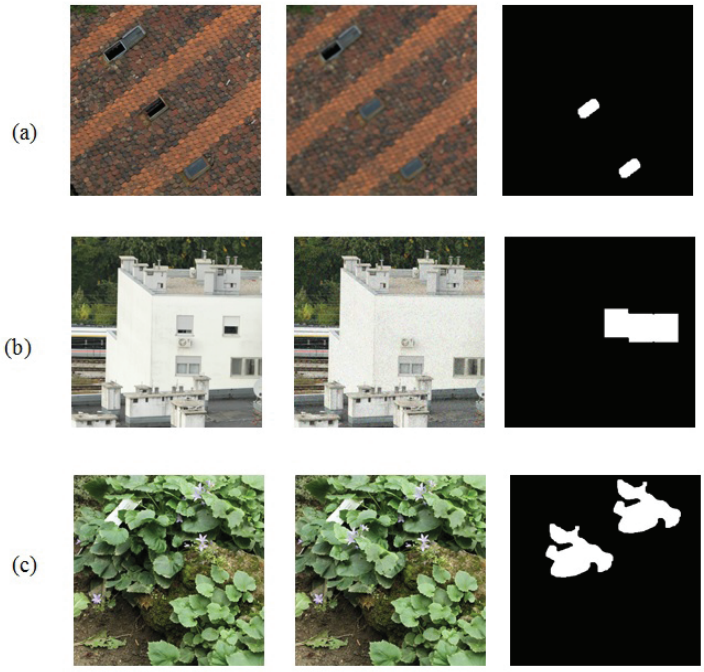

FIGURE 9. Experiment results under photometric attacks. The original images (left), tampered images (middle) and the detected forgery (right). (a) Tampered image with Gaussian blurring ($\mu = 7, \sigma = 35$), (b) tampered image distorted by AWGN, NP = 20 dWB, and (c) tampered image compressed in JPEG format by a quality factor (Q) = 40

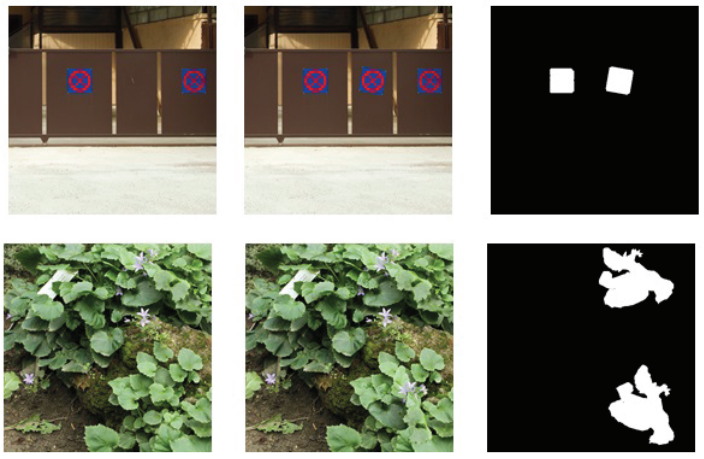

FIGURE 10. Forgery detection for rotated copy-move region. The original images (left), tampered images (middle) and the detected forgery (right)

5.3. **Comparisons with other methods.** In this section, the performance of the proposed method is compared with the method in [12] that used Zernike Moments to extract features and [13] that used LBP to features extraction. Where the images that contain copy move forgery is exposed to single attack such as (rotation, Gaussian noise, Gaussian blurring JPEG compression) or multiple attacks. The F- Measure of the proposed method and methods in [12, 13] are presented in Table 2 according to the attacks. From Table 2,

FIGURE 11. Forgery detection for rotated copy-move region. The original images (left), tampered images (middle) and the detected forgery (right)

we find that the proposed method performs better than the two other methods, especially when the images expose to multiple attacks.

TABLE 2. F-measure of copy-move detection methods with Variety attacks

Attack Type	Rotation	Rotation + JPG Compression	Rotation + Noise	Rotation + Blurring
Proposed method	0.9647	0.9435	0.9154	0.9365
Method[13]	0.9377	0.9231	0.8956	0.9047
Method[12]	0.8736	0.8465	0.7867	0.7989

6. **Conclusions.** Lately, one of the main problems in digital image forensics is the copy-move forgery detection. Numerous techniques have been proposed; however Most of them suffer considerably from common attacks: such as additive noise, blurring, compression and rotation. We introduced a new method based on CR LBP to extract features from overlapping blocks to detect copy-move forgery.

Our experiment revealed that the CRLBP revealed many advantages in terms of robustness, to some noise, and achieves superior results. Hybrid filter is employed in the pre-processing step to enhance image quality for efficient and precise detection. In the post-processing used a new technique consists of three steps to reduce the false positive, this technique made the CMFD accuracy best. Images from standard database CoMoFoD are used to implement our method. Five different types of tampered images according to attacks are used. Overall the performance of our proposed method is very encouraging, especially in dealing with tampered image with additive noise, blurring, compression, rotation and multiple attacks. The proposed method is still time consuming for forgery detection, especially in the high resolution images. So we can reduce the computational cost by applying the DWT (Discrete Wavelet Transform) to reduced dimensional representation of the input image.

Acknowledgment. The authors are thankful to the Ministry of Higher Education (MOHE), Iraq for providing the research grant. The facilities provided by the University Technology Malaysia (UTM), Johor are gratefully acknowledged.

REFERENCES

[1] J. Redi, W. Taktak, and J. Dugelay, Digital image forensics: a booklet for beginners, *Multimed. Tools Appl*, vol. 33, pp. 140, 2011.

[2] S. Sadeghi, H. Jalab, and S. Dadkhah, Efficient Copy-Move Forgery Detection for Digital images, *World Acad. Sci. Eng. Technol*, vol. 71, pp. 543546, 2012.
[3] L. Jing and C. Shao, Image Copy-Move Forgery Detecting Based on Local Invariant Feature, *J. Multimed*, vol. 7, no. 1, pp. 9097, 2012.
[4] G. R. E. J, T. S. Aditya, and M. S. S, Survey on Passive Methods of Image Tampering Detection, *Commun. Comput. Intell. (INCOCCI), 2010 Int. Conf. on. IEEE* , pp. 431436, 2010.
[5] D. Kundur and D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, *Proc. of the IEEE* , vol. 87, no. 7, 1999.
[6] S. Bayram, H. T. Sencar, and N. Memon, An efficient and robust method for detecting copy-move forgery, *IEEE International Conference on Acoustics, Speech and Signal Processing* , pp. 10531056, 2009.
[7] 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, no. 6, pp. 174183, 2013.
[8] A. Fridrich, B. Soukal, and A. Luk, Detection of copy-move forgery in digital images, *Proc. Digit. Forensic Res. Work*, 2003.
[9] A. Popescu and A. Farid, Exposing digital forgeries by detecting duplicated image regions, *Pattern Recognition, 2006. ICPR 2006. 18th Int. Conf. IEEE* , vol. 4, no. 2000, pp. 111, 2004.
[10] B. Mahdian and S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, *Forensic Science International*, vol. 171, no. 23, pp. 1809, 2007.
[11] 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 Autom. Sin*, vol. 35, no. 12, pp. 14881495, 2010.
[12] S. J. Ryu, M. J. Lee, and H. K. Lee, *Detection of copy-rotate-move forgery using Zernike moments*, LNCS6387, Springer, pp. 51-65, 2010.
[13] L. D. Li, S. S. Li, and H. C. Zhu, An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 4656, 2013.
[14] H. L. Huang, W. Q. Guo, and Y. Zhang, Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm, *Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 272276, 2008.
[15] Y. Zhao, W. Jia, R. X. Hu, and H. Min, Completed robust local binary pattern for texture classification, *Neurocomputing* , vol. 106, pp. 6876, 2013.
[16] Z. H. Guo, D. Zhang, and D. Zhang, A completed modeling of local binary pattern operator for texture classification, *IEEE Trans. on Image Processing*, vol. 19, no. 6, pp. 16571663, 2010.
[17] G. H. Zhao, G. M. Wu, Y. Liu, and J. M. Chen, Texture Classification Based on Completed Modeling of Local Binary Pattern, *International Conference on Computational and Information Sciences*, pp. 268271, 2011.
[18] Y. Zhao, D. S. Huang, and W. Jia, Completed local binary count for rotation invariant texture classification, *IEEE Trans. on Image Process*, vol. 21, no. 10, pp. 44924497, 2012.
[19] D. G. Bailey, *An Efficient Euclidean Distance Transform*, LNCS3322, pp. 394408, 2005.